## 5.2方案详细设计

北京市医疗系统密码应用建设是从物理和环境安全、网络和通信安全、设备和计算安全和应用和数据安全五个方面进行建设。

### 5.2.1物理和环境安全

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。

1. 身份鉴别：采用基于密码技术的遵循GM/T 0036要求的电子门禁系统
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，
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，

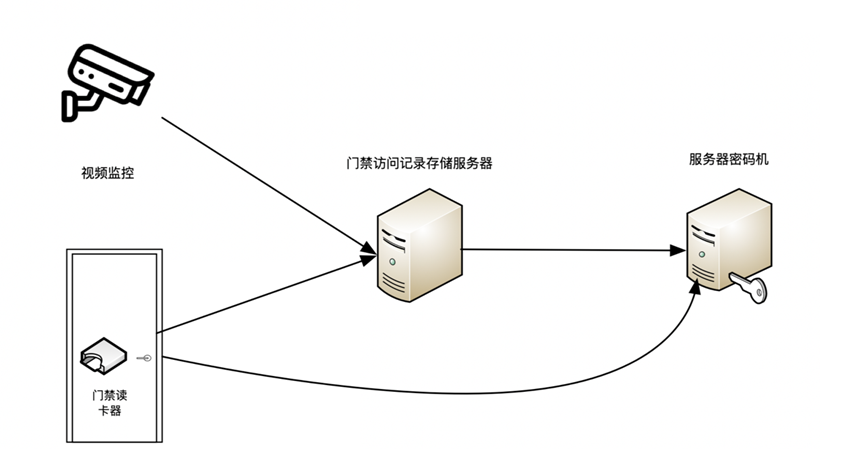


图 5.4 物理环境图

表 5.3 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 | 通州机房 |

表 5.4 指标适用情况及论证说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全层面 | 指标要求 | 应用要求 | 适用情况 | 不适用性  论证说明 |
| 物理和环境安全 | 8.1 a) 宜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。 | 宜 | 适用 | 无 |
| 8.1 b) 宜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。 | 宜 | 适用 | 无 |
| 8.1 c) 宜采用密码技术保证视频监控音像记录数据的存储完整性。 | 宜 | 适用 | 无 |

### 5.2.2网络和通信安全

网络与接入安全密码应用，在应用系统接入边界部署IPSec VPN和SSL VPN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。

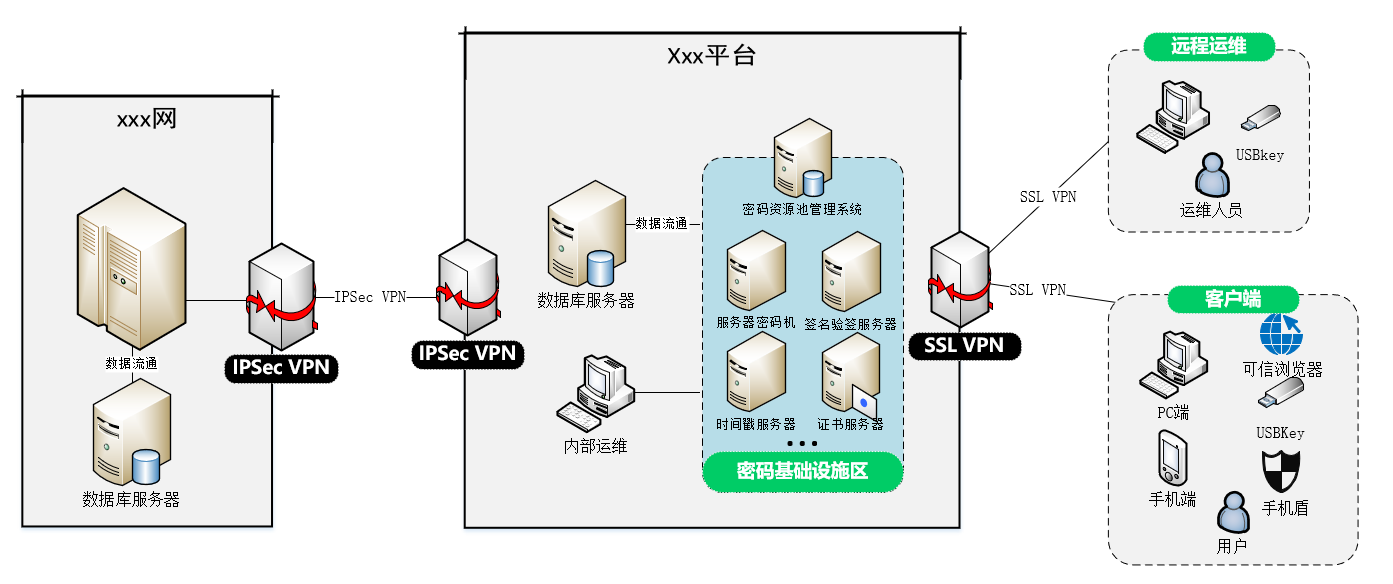


图 5.5 网络和通信安全架构图

1. XXX网IPSec VPN与IPSec VPN之间的通信信道
   1. 身份鉴别：在本地机房部署IPSec VPN安全网关，实现通信实体的身份鉴别，防止与假冒实体通信。
   2. 通信数据完整性和通信过程中重要数据的机密性：部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信数据完整性和通信过程中重要数据的机密性。
   3. 网络边界访问控制信息的完整性：部署的IPSec VPN安全网关已通过商用密码机构认证，可保证网络边界访问控制信息的完整性。
   4. 安全接入认证：部署的IPSec VPN安全网关已通过商用密码机构认证，可保证安全接入。
2. 互联网VPN客户端与运维SSL VPN之间的运维通信信道
   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网关连接到统计内部信息网，并向运维人员配发USBKey，实现对远程运维人员的安全身份鉴别，防止与假冒实体通信。
   2. 通信数据完整性和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，可保证通信数据完整性和通信过程中重要数据的机密性。
   3. 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，可保证网络边界访问控制信息的完整性。
   4. 安全接入认证：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。
3. 移动端与前台应用系统之间的通信信道
   1. 身份鉴别：移动端用户登录到移动业务系统，采用SSL VPN移动安全接入网关实现基于数字证书的身份鉴别，防止非授权人员登录。
   2. 通信数据完整性和通信过程中重要数据的机密性：在本地机房部署SSL VPN安全网关实现移动端与业务系统之间通信数据的机密性和完整性保护。
   3. 网络边界访问控制信息的完整性：在本地机房部署SSL VPN网关，利用SSL VPN网关本身的机制完成对访问控制信息进行完整性保护。
   4. 安全接入认证：移动用户通过移动终端登录到移动业务系统，采用SSL VPN移动安全接入网关实现基于数字证书的身份鉴别。
4. 互联网VPN客户端与内网SSL VPN之间的通信信道
   1. 身份鉴别：员工通过PC终端登录到业务系统，采用SSL VPN移动安全接入网关实现基于数字证书的身份鉴别，防止非授权人员登录。
   2. 通信数据完整性和通信过程中重要数据的机密性：在本地机房部署SSL VPN 安全网关实现移动端与业务系统之间通信数据的机密性和完整性保护。
   3. 网络边界访问控制信息的完整性：在本地机房部署SSL VPN网关，利用SSL VPN网关本身的机制完成对访问控制信息进行完整性保护。
   4. 安全接入认证：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 5.5 网络与通信安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 网络与通信安全 | xx网IPSec VPN与IPSec VPN之间的通信信道 |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |

表 5.6 指标适用情况及论证说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全层面 | 指标要求 | 应用要求 | 适用情况 | 不适用性  论证说明 |
| 网络和通信安全 | 8.2 a) 应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。 | 应 | 适用 | 无 |
| 8.2 b) 宜采用密码技术保证通信过程中数据的完整性。 | 宜 | ☑适用  □不适用 | 无 |
| 8.2 c) 应采用密码技术保证通信过程中重要数据的机密性。 | 应 | 适用 | 无 |
| 8.2 d) 宜采用密码技术保证网络边界访问控制信息的完整性。 | 宜 | ☑适用  □不适用 | 无 |
| 8.2 e) 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。 | 可 | ☑适用  □不适用 | 无 |

### 5.2.3设备和计算安全

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



图 5.6 设备和计算安全架构图

1. **身份鉴别：**本系统由经批准的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：**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。
3. **系统资源访问控制信息完整性：**在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。
4. **重要信息资源安全标记完整性：**本系统不涉及重要信息的敏感标记。
5. **日志记录完整性：**在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC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。
7. **密码服务：**数字证书认证服务、密钥管理服务。
8. **密码产品：**SSL VPN安全网关、服务器密码机、签名验签服务器、智能密码钥匙。

设备和计算安全层面所使用的密码算法、密码技术、密码服务、密钥管理，需采用符合GM/T 0030-2014《服务器密码机技术规范》、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》的USBKey、服务器密码机实现。

表 5.7 设备与计算安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 设备与计算安全 | 国密堡垒机 |
| 2 | 服务器密码机 |
| 3 | 签名验签服务器 |
| 4 | 应用服务器 |
| 5 | 数据库服务器 |
| 7 | 时间戳服务器 |
| 8 | 安全电子签章系统 |

表 5.8 指标适用情况及论证说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全层面 | 指标要求 | 应用要求 | 适用情况 | 不适用性  论证说明 |
| 设备和计算安全 | 8.3 a) 应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。 | 应 | 适用 | 无 |
| 8.3 b) 远程管理设备时，应采用密码技术建立安全的信息传输通道。 | 应 | 适用 | 无 |
| 8.3 c) 宜采用密码技术保证系统资源访问控制信息的完整性。 | 宜 | ☑适用  □不适用 | 无 |
| 8.3 d) 宜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。 | 宜 | □适用  ☑不适用 | 本系统不涉及重要信息资源安全标记 |
| 8.3 e) 宜采用密码技术保证日志记录的完整性。 | 宜 | ☑适用  □不适用 | 无 |
| 8.3 f) 宜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。 | 宜 | ☑适用  □不适用 | 无 |

### 5.2.4应用和数据安全

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



图 5.7 应用和数据安全架构图

1. **身份鉴别：**在本系统应用用户人员PC端采用USBKey登录，用户C在移动端安装手机盾通过微信公众平台，采用手机验证码的方式验证人员身。在密码基础设施区部署签名验签服务器，其他XX单位职工用户通过移动端上安装的微信小程序或企业微信登录应用时验证人员数字签名，实现对用户A、用户B、用户C、系统管理员、系统运维人员在登录系统和业务操作时的身份鉴别，防止非授权人员登录。
2. **访问控制信息完整性：**在密码基础设施区部署服务器密码机，使用HMAC对系统应用的访问控制信息进行完整性保护，防止访问控制信息被篡改。
3. **重要信息资源安全标记完整性：**无（根据系统定义的安全标记进行有针对性的防护）
4. **重要数据传输机密性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2及SM3算法进行会话密钥交互，采用SM4算法对传输的数据信息进行机密性保护，防止其被非授权窃取。
5. **重要数据存储机密性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用SM4算法对数据信息存储进行机密性保护，防止其被非授权窃取。
6. **重要数据传输完整性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2算法进行会话密钥交互，采用HMAC算法对传输的数据信息进行完整性保护，防止其被非授权篡改。
7. **重要数据存储完整性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用HMAC对数据信息存储进行完整性保护，防止其被非授权篡改。
8. **不可否认性：**在基础设施区部署时间戳服务器，在系统中重要数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性。
9. **密码服务：**密码应用技术服务
10. **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。

表 5.9 应用与数据安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 应用与数据安全 | Xx业务系统应用 |

表 5.10 指标适用情况及论证说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全层面 | 指标要求 | 应用要求 | 适用情况 | 不适用性  论证说明 |
| 应用和数据安全 | 8.4 a) 应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。 | 应 | 适用 | 无 |
| 8.4 b) 宜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。 | 宜 | ☑适用  □不适用 | 无 |
| 8.4 c) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。 | 宜 | □适用  ☑不适用 | 本系统不涉及重要信息资源安全标记 |
| 8.4 d) 应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。 | 应 | 适用 | 无 |
| 8.4 e) 应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。 | 应 | 适用 | 无 |
| 8.4 f) 宜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。 | 宜 | ☑适用  □不适用 | 无 |
| 8.4 g) 宜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。 | 宜 | ☑适用  □不适用 | 无 |
| 8.4 h) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。 | 宜 | ☑适用  □不适用 | 无 |