# 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》，信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，信息系统中使用的密码技术应遵循密码相关国家标准和行业标准，信息系统中使用的密码产品、密码服务应符合法律法规的相关要求，否则可能会出现一些安全问题，安全问题一旦被威胁利用后，会导致信息系统面临高等级安全风险。

## 3.1 风险控制需求

3.1.1-3.1.4节分别从物理和环境、网络和通信、设备和计算、应用和数据四个方面进行风险分析，整理密码应用需求，并结合第2章目标信息系统的实际情况，分析出该系统每部分的密码应用需求清单，其中\*号为《信息系统密码应用高风险判定指引》中标注的高风险项，3.1.5节整理密码管理需求。

### 物理和环境安全

1. **风险分析**

{{?risk}}

{{?wlhhjRiskList}}

{{index}}、{{name}}

{{\*description}}

{{/wlhhjRiskList}}

1. **密码应用需求**
2. 身份鉴别的密评三级要求是“宜”，经过上述的风险分析，设备所在机房应部署符合GM/T0036-2014《采用非接触卡的门禁系统密码应用技术指南》标准要求的电子门禁系统对进出机房人员进行身份鉴别。
3. 电子门禁记录数据存储完整性的密评三级要求是“宜”，经过上述的风险分析，设备所在机房应部署符合GM/T 0030-2014《服务器密码机技术规范》标准要求的服务器密码机，对电子门禁记录数据进行完整性保护。
4. 视频监控记录数据存储完整性的密评三级要求是“宜”，经过上述的风险分析，设备所在机房应部署符合GM/T 0030-2014《服务器密码机技术规范》标准要求的服务器密码机，对视频监控记录数据进行完整性保护。

### 网络和通信安全

1. **风险分析**

{{?wlhtxRiskList}}

{{index}}、{{name}}

{{\*description}}

{{/wlhtxRiskList}}

1. **密码应用需求**
2. 身份鉴别的密评三级要求是“应”，经过上述的风险分析，系统应部署符合 GM/T 0024-2014《SSL VPN技术规范》GM/T 0025-2014《SSL VPN 网关产品规范》等标准要求的SSL VPN安全网关搭配使用合规的 USBKey 并在 USBKey 智能密码钥匙和服务端中灌装由具有电子政务电子认证服务资质的 CA 机构签发的数字证书对通信实体进行身份鉴别，保证通信实体身份的真实性。
3. 密评三级要求“宜”做通信过程中数据的完整性。一般在密码基础设施区部署符合GM/T 0024-2014《SSL VPN技术规范》GM/T 0025-2014《SSL VPN 网关产品规范》等标准要求的SSL VPN安全网关，业务应用通过调用该密码设备或产品，使用合规的算法对通信过程中的数据进行完整性保护，实现通信数据防篡改保护。
4. 密评三级要求“应”做通信过程中重要数据的机密性。一般在密码基础设施区部署符合GM/T 0024-2014《SSL VPN技术规范》GM/T 0025-2014《SSL VPN 网关产品规范》等标准要求的SSL VPN安全网关，业务应用通过调用该密码设备或产品，使用合规的算法对通信过程中重要数据进行机密性保护，实现重要数据防窃取保护。
5. 密评三级要求“宜”对网络边界访问控制信息做完整性保护。系统应部署符合GM/T 0024-2014《SSL VPN技术规范》GM/T 0025-2014《SSL VPN 网关产品规范》等标准要求的SSL VPN安全网关，使用合规的算法保证网络边界访问控制信息的完整性。
6. 安全接入认证的密评三级要求是“可”，本系统不涉及此需求，故不做特殊改造。

### 设备和计算安全

1. **风险分析**
2. 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。
3. 远程通道管理安全：本系统现阶段通过非国密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。
4. 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。
5. 重要信息资源安全标记完整性：无重要信息资源安全标记。
6. 日志记录完整性：本系统内各设备未采用密码技术保证其上日志记录完整性，存在设备日志记录被非授权篡改风险。
7. 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。
8. **密码应用需求**

本系统在设备和计算安全层面的测评对象共分为四类，分别为堡垒机、通用类产品、整机类密码产品、系统类密码产品。其中，整机类密码产品包括【手动填入】；通用类产品包括：应用服务器和数据库服务器以及数据库管理系统；系统类密码产品包括：【手动填入】。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四类测评对象有以下密码应用需求。

堡垒机：

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）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。
2. 远程管理通道安全：需部署符合密码相关国家、行业标准要求的国密堡垒机，通过堡垒机以及合规的协议建立运维人员到堡垒机的远程管理通道。
3. 系统资源访问控制信息完整性：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系统资源访问控制信息的完整性，防止被非授权篡改。
4. 重要信息资源安全标记完整性：无重要信息资源安全标记。
5. 日志记录完整性：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系统的日志记录的完整性，防止其被篡改。
6. 重要可执行程序完整性、重要可执行程序来源真实性：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系统的重要可执行程序完整性以及来源的真实性。

通用类产品：

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。
2. 远程管理通道安全：需部署符合密码相关国家、行业标准要求的国密堡垒机，由堡垒机通过合规的协议建立运维人员到应用服务器、数据库服务器以及数据库管理系统的远程管理通道。
3. 系统资源访问控制信息完整性：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资源访问控制信息的完整性，防止被非授权篡改。
4. 重要信息资源安全标记完整性：无重要信息资源安全标记。
5. 日志记录完整性：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。
6. 重要可执行程序完整性、重要可执行程序来源真实性：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。

整机类密码产品：

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。
2. 远程管理通道安全：需部署符合密码相关国家、行业标准要求的国密堡垒机，由堡垒机通过合规的协议建立运维人员到整机类密码产品的远程管理通道。
3. 系统资源访问控制信息完整性：整机类密码产品均已通过商用密码产品检测认证，其自身已具有安全防护能力，通过产品自身的安全防护机制可实现系统资源访问控制信息的完整性。
4. 重要信息资源安全标记完整性：无重要信息资源安全标记。
5. 日志记录完整性：整机类密码产品均已通过商用密码产品检测认证，其自身已具有安全防护能力，通过产品自身的安全防护机制可实现日志记录的完整性。
6. 重要可执行程序完整性、重要可执行程序来源真实性：整机类密码产品均已通过商用密码产品检测认证，其自身已具有安全防护能力，通过产品自身的安全防护机制可实现重要可执行程序完整性以及来源的真实性。

系统类密码产品：

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。
2. 远程管理通道安全：需部署符合密码相关国家、行业标准要求的国密堡垒机，由堡垒机通过合规的协议建立运维人员到系统类密码产品的远程管理通道。
3. 系统资源访问控制信息完整性：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系统类密码产品的系统资源访问控制信息的完整性，防止被非授权篡改。
4. 重要信息资源安全标记完整性：无重要信息资源安全标记。
5. 日志记录完整性：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系统类密码产品的日志记录的完整性，防止其被篡改。
6. 重要可执行程序完整性、重要可执行程序来源真实性：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系统类密码产品的重要可执行程序完整性以及来源的真实性。

### 应用和数据安全

1. **风险分析**

{{?yyhsjRiskList}}

{{index}}、{{name}}

{{\*description}}

{{/yyhsjRiskList}}

{{/risk}}

1. **密码应用需求**
2. 密评三级要求“应”做身份鉴别。一般在密码基础设施区部署符合符合GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》标准要求的签名验签服务器，为用户配发基于SM2数字证书的USBKey进行登录，USBKey中灌装由具有电子政务电子认证服务资质的 CA 机构签发的数字证书，实现对登录用户的安全身份鉴别，保证应用系统用户身份的真实性，防止非授权人员登录。
3. 密评三级要求“宜”做访问控制信息的完整性。一般在密码基础设施区部署符合GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，通过该密码设备或产品使用HMAC-SM3算法对系统中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。
4. 密评三级要求“宜”做重要信息资源安全标记完整性。一般在密码基础设施区部署符合GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，业务应用通过调用该密码设备或产品，对业务应用的重要信息资源安全标记进行完整性保护，防止被非授权篡改。本系统不涉及重要信息资源安全标记，故不做特殊改造。
5. 密评三级要求“应”做重要数据传输机密性。一般在密码基础设施区部署符合GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，业务应用通过调用该密码设备或产品，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。
6. 密评三级要求“宜”做重要数据传输完整性。一般在密码基础设施区部署符合GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，业务应用通过调用该密码设备或产品，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。
7. 密评三级要求“应”做重要数据存储机密性。一般在密码基础设施区部署符合GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，业务应用通过调用该密码设备或产品，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。
8. 密评三级要求“宜”做重要数据存储完整性。一般在密码基础设施区部署符合GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，业务应用通过调用该密码设备或产品，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。
9. 密评三级要求“宜”做不可否认性。一般在密码基础设施区部署符合GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》标准要求的签名验签服务器和符合GM/T 0033-2014《时间戳接口规范》标准要求的时间戳服务器，业务应用通过调用该密码设备或产品，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

### 3.1.5 密码安全管理

本小节针对密码安全管理中存在的风险提出了对应的密码应用需求，如下。

1. **风险分析**

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

1. **密码应用需求**

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

## 3.2 需求分析

通过深入分析{{sysname}}的安全风险，以及《基本要求》针对本系统网络安全保护等级提出的密码应用要求，对系统的密码应用需求分析如表3.9所示。

表 3.9 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 | 保证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 | 实现电子门禁系统进出记录和视频监控音像记录的完整性，防止被非授权篡改 |
| 视频监控记录数据存储完整性 |
| 网络和通信安全 | 身份鉴别 | 实现对通信实体的身份鉴别，保证通信实体身份的真实性 | 无 |
| 通信数据完整性 | 实现通信数据的完整性，防止数据被非授权篡改 | 无 |
| 通信过程中重要数据的机密性 | 实现通信过程中重要数据的机密性，防止重要数据泄漏 | 无 |
| 网络边界访问控制信息的完整性 | 实现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 | 不适用 | 本系统不涉及安全接入认证 |
| 设备和计算安全 | 身份鉴别 | 实现对运维人员和系统管理员的身份鉴别，防止非授权人员登录 | 无 |
| 远程管理通道安全 | 建立安全的信息传输通道，防止信息传输通道被非授权使用，或传输数据被非授权获取或篡改 | 无 |
| 系统资源访问控制信息完整性 | 实现系统资源访问控制信息的完整性保护，防止被非授权篡改 | 无 |
| 重要信息资源安全标记完整性 | 不适用 | 本系统无重要信息资源敏感标记 |
| 日志记录完整性 | 实现日志记录的完整性保护，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 | 实现对重要可执行程序的完整性保护，并对其来源进行真实性验证 | 无 |
| 应用和数据安全 | 身份鉴别 | 实现对登录用户的安全身份鉴别，保证应用系统用户身份的真实性 | 无 |
| 访问控制信息完整性 | 实现系统应用的访问控制信息的完整性保护，防止被篡改 | 无 |
| 重要信息资源安全标记完整性 | 不适用 | 本系统无重要信息资源安全标记 |
| 重要数据传输机密性 | 实现对系统应用的重要数据的传输机密性和完整性、存储机密性和完整性保护，防止重要数据被窃取或篡改 | 无 |
| 重要数据传输完整性 |
| 重要数据存储机密性 | 无 |
| 重要数据存储完整性 |
| 不可否认性 | 不适用 | 本系统不涉及不可否认性 |