# 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。

### 3.1.1 物理和环境安全

1. **风险分析**
   1. 物理和环境安全中的身份鉴别是指：设备所在机房应使用密码技术对进入机房人员进行身份鉴别，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在非授权人员进入物理环境，对软硬件设备和数据进行直接破坏的风险。
   2. 物理和环境安全中的电子门禁记录数据存储记录完整性是指：设备所在机房应使用密码技术对电子门禁记录进行数据完整性保护，属于《信息系统密码应用高风险判定指引》认定的非高风险项，如果不采用合规密码技术进行保护，会存在数据被篡改的风险。
   3. 物理和环境安全中的视频监控记录数据存储记录完整性是指：设备所在机房应使用密码技术对视频监控记录进行数据完整性保护，属于《信息系统密码应用高风险判定指引》认定的非高风险项，如果不采用合规密码技术进行保护，会存在数据被篡改的风险。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未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为高风险项，现有系统在高风险项层面不能满足要求，存在较大风险。

1. **密码应用需求**
   1. 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/T 0036-2014 标准要求的密码产品，对进出机房人员进行身份鉴别。
   2. 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密码相关国家、行业标准要求的电子门禁系统，对电子门禁记录数据进行完整性保护。
   3. 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密码相关国家、行业标准要求的视频监控系统，对视频监控音像记录数据进行完整性保护。

具体情况如下所示：

表 3.1 测评对象表-物理和环境安全

|  |
| --- |
| **测评对象{{table31}}** |
| [jfmc] |

表 3.2 密码应用需求分析表-物理和环境

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象{{table32}} | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 预测结果 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

### 3.1.2 网络和通信安全

1. **风险分析**
   1. 网络和通信安全中的身份鉴别是指：系统现存通信信道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，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在非法通信实体介入网络通信的风险。
   2. 通信过程中数据的完整性是指采用密码技术保证信息系统与其他实体通信过程中数据的完整性，如果不采用合规密码技术进行保护，会存在通信过程中数据被非授权篡改的风险。
   3. 通信过程中重要数据的机密性是指采用密码技术保证信息系统与其他实体通信过程中重要数据的机密性，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在通信过程中重要数据被窃取的风险。
   4. 网络边界访问控制信息的完整性是指采用密码技术保证网络边界访问控制信息的完整性，不属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在网络边界访问控制信息被篡改的风险。
   5. 网络和通信安全中的安全接入认证是指：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。本系统不涉及安全接入认证。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未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、未采用密码技术保证通信过程中重要数据的机密性为高风险项，现有系统在高风险项层面不能满足要求，存在较大风险。

1. **密码应用需求**
   1. 身份鉴别的密评三级要求是“应”，经过上述的风险分析，系统应部署符合密码相关国家、行业标准要求的密码设备或产品对通信实体进行身份鉴别，保证通信实体身份的真实性。
   2. 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密码相关国家、行业标准要求的密码设备或产品，业务应用通过调用该密码设备或产品，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。
   3. 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密码相关国家、行业标准要求的密码设备或产品，业务应用通过调用该密码设备或产品，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。
   4. 密评三级要求“宜”对网络边界访问控制信息做完整性保护。系统应部署符合密码相关国家、行业标准要求的密码设备或产品保证网络边界访问控制信息的完整性。
   5. 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。

具体情况如下所示：

表 3.3 测评对象表-网络和通信

|  |  |  |
| --- | --- | --- |
| **途经不受保护的网络类型{{table33}}** | **通信主体** | **测评对象** |
| [wllx] | [txzt] | [cpdx] |

表 3.4 密码应用需求分析表-网络和通信

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象{{table34}} | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 预测结果 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

### 3.1.3 设备和计算安全

1. **风险分析**
   1. 设备和计算安全中的身份鉴别是指：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，属于《信息系统密码应用高风险判定指引》认定的高风险项。系统运维人员如果不通过安全方式与系统建立连接或未使用合规的密码技术对运维人员进行身份鉴别，则存在设备被非授权人员登录风险。
   2. 设备和计算安全中的远程通道管理安全是指：远程管理设备时，采用密码技术建立安全的信息传输通道，属于《信息系统密码应用高风险判定指引》认定的高风险项。系统运维人员远程管理设备时，如果不采用密码技术建立安全的信息传输通道，则存在信息传输通道被未授权使用或传输数据未授权被获取和篡改等风险。
   3. 设备和计算安全中的系统资源访问控制信息的完整性是指：采用密码技术保证系统资源访问控制信息的完整性，属于《信息系统密码应用高风险判定指引》认定的非高风险项。系统中如果未采用密码技术对系统资源访问控制信息进行完整性保护，则存在系统资源访问控制信息未授权被篡改的风险。
   4. 设备和计算安全中的重要信息资源安全标记的完整性是指：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，属于《信息系统密码应用高风险判定指引》认定的非高风险项。本系统不涉及重要信息资源安全标记。
   5. 设备和计算安全中的日志记录的完整性是指：采用密码技术保证日志记录的完整性，属于《信息系统密码应用高风险判定指引》认定的非高风险项。系统如果未采用密码技术对应用服务器、数据库服务器等设备日志记录进行完整性保护，则存在日志记录被非授权篡改风险。
   6. 设备和计算安全中的重要可执行程序完整性、重要可执行程序来源真实性是指：采用密码技术对重要可执行程序进行完整性保护，并对其来源行真实性验证，属于《信息系统密码应用高风险判定指引》认定的非高风险项。系统如果未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，则存在重要可执行程序被非授权篡改、来源不可信风险。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未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；远程管理设备时，未采用密码技术建立安全的信息传输通道为高风险项，现有系统在高风险项层面不能满足要求，存在较大风险。

1. **密码应用需求**
   1. 根据密评三级要求，“应”对登录设备的用户进行身份鉴别。经过上述风险分析，在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，并针对运维人员提供相应密码技术产品或设备的支撑，对运维人员进行身份鉴别，防止非授权人员登录
   2. 根据密评三级要求，“应”保证远程管理通道安全。经过上述风险分析，在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，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篡改。
   3. 根据密评三级要求，“宜”保证系统资源访问控制信息的完整性。经过上述风险分析，在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，对系统资源访问控制信息进行完整性保护，防止被非授权篡改。
   4. 根据密评三级要求，“宜”保证设备中的重要信息资源安全标记的完整性。本系统不涉及重要信息资源安全标记，故不做特殊改造。
   5. 根据密评三级要求，“宜”保证日志记录的完整性。经过上述风险分析，在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，对日志记录进行完整性保护。
   6. 根据密评三级要求，“宜”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。经过上述风险分析，在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，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。

具体如下所示：

表 3.5 测评对象表-设备和计算

|  |  |  |
| --- | --- | --- |
| **设备类型{{table35}}** | **测评对象** | **说明** |
| [sblx] | [cpdx] | [sm] |

表 3.6 密码应用需求分析表-设备和计算

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象{{table36}} | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 预测结果 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

### 3.1.4 应用和数据安全

1. **风险分析**
   1. 身份鉴别是指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，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，则存在非授权人员登录的风险。
   2. 访问控制信息的完整性是指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，属于《信息系统密码应用高风险判定指引》认定的低风险项，如果不采用合规密码技术进行保护，会存在访问控制信息被未授权人员非法窃取或篡改的风险。
   3. 重要信息资源安全标记完整性是指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，不属于《信息系统密码应用高风险判定指引》认定的高风险项。安全标记主要是指对主体（如用户）与客体（如数据对象）都标上安全等级，系统根据访问主体和被访问数据资源的安全标记进行访问许可的判定，一般用于强制访问控制。本系统不涉及重要信息资源安全标记。
   4. 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密码相关国家、行业标准要求的密码设备或产品，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。
   5. 重要数据传输完整性是指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，不属于《信息系统密码应用高风险判定指引》认定的高风险项。如果不采用合规密码技术进行保护，会存在重要数据在传输过程中被非授权篡改的风险。
   6. 重要数据存储机密性是指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，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在重要数据在存储过程中被窃取的风险。
   7. 重要数据存储完整性是指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，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在重要数据在存储过程中被非授权篡改的风险。
   8. 不可否认性是指在可能涉及法律责任认定的应用中，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，属于《信息系统密码应用高风险判定指引》认定的高风险项，如果不采用合规密码技术进行保护，会存在数据发送者或接受者不承认发送或接受的数据，或者否认所做的操作风险。本系统不涉及不可否认性。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未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；未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；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；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，现有系统在高风险项层面不能满足要求，存在较大风险。

1. **密码应用需求**
   1. 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密码相关国家、行业标准要求的密码设备或产品，业务应用通过调用该密码设备或产品，对登录人员进行身份鉴别，防止非授权人员登录。
   2. 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密码相关国家、行业标准要求的密码设备或产品，业务应用通过调用该密码设备或产品，对业务应用的访问控制信息进行完整性保护，实现访问控制信息防窃取保护。
   3. 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密码相关国家、行业标准要求的密码设备或产品，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。
   4. 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密码相关国家、行业标准要求的密码设备或产品，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。
   5. 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密码相关国家、行业标准要求的密码设备或产品，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。
   6. 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密码相关国家、行业标准要求的密码设备或产品，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。
   7. 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密码相关国家、行业标准要求的密码设备或产品，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。
   8. 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密码相关国家、行业标准要求的密码设备或产品，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。

具体如下所示：

表 3.7 测评对象表-应用和数据

|  |  |  |  |
| --- | --- | --- | --- |
| **业务应用{{table37}}** | **数据类型** | **测评对象** | **保护需求** |
| [ywyy] | [sjlx] | [cpdx] | [bhxq] |

表 3.8 密码应用需求分析表-应用和数据

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象{{table38}} | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 预测结果 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

### 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 |