# 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》，3.1节进行基本的、通用的风险分析，整理密码应用需求，3.2-3.5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，3.6节进行密钥的风险分析，并整理密钥管理需求。

## 3.1 通用需求分析

### 3.1.1 风险分析

对所有实现密码运算和密钥管理的密码产品，查看它们的商用密码产品型号证书或认证证书，确认其是否符合密码应用方案中的选型；若密码应用方案中未选定具体产品指标或安全等级，测评人员应当确认其是否属于GM/T 0028-2014要求二级及以上的密码模块或硬件密码产品。

### 3.1.2 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》，选择适当的具有商用密码产品型号证书或认证证书的密码产品。

## 3.2 物理和环境

### 3.2.1 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。

### 3.2.2 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，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“应”，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“应”，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。

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。

### 3.2.3 本系统需求分析清单-物理和环境

表3.1 测评对象表-物理和环境

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

本项目需求分析清单如表3.2所示。

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 | 结论 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

## 3.3 网络和通信

### 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。系统现存接入设备如果未采用密码技术对外部连接到内部网络的设备进行接入认证，则存在非授权设备接入等风险。

### 3.3.2 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”，本三级系统不作此需求，故不做特殊改造。

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。

### 3.3.3 本系统需求分析清单-网络和通信

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 | 结论 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

## 3.4 设备和计算

### 3.4.1 风险分析

* 1. 风险分析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。系统如果不采用密码技术保证设备中重要信息资源安全标记的完整性，则存在设备中重要信息资源安全标记被非授权篡改风险。
  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。

### 3.4.2 密码应用需求

根据上述风险分析，有以下应用需求。

* 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。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，对设备中的重要信息资源安全标记进行完整性保护。
  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。

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。

### 3.4.3 本系统需求分析清单-设备和计算

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 | 结论 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

## 3.5 应用和数据

### 3.5.1 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。如果不采用合规密码技术进行保护，会存在信息系统应用的重要信息资源安全标记被未授权篡改的风险。
  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。

### 3.5.2 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。当前业务应用中没有重要信息资源安全标记，不需要进行完整性保护。
  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。

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；在可能涉及法律责任认定的应用中，未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。

### 3.5.3 本系统需求分析清单-应用和数据

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 | 结论 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

## 3.6 密钥安全管理

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。

### 3.6.1 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。

### 3.6.2 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，评估通过后上线运行。