# 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要求三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. 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，否则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. 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，否则存在数据被篡改的风险。
  3. 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，否则存在数据被篡改的风险。

### 3.2.2 密码应用需求

* 1. 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. 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. 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

### 3.3.1 风险分析

(1) 系统现存通信信道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。

(2) 系统现存通信信道未采用密码技术保证通信过程中数据的完整性。

(3) 系统现存通信信道未采用密码技术保证通信过程中重要数据的机密性。

(4) 系统现存通信信道未采用密码技术保证网络边界访问控制信息的完整性。

(5) 系统现存通信信道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，确保接入的设备身份真实性。

### 3.3.2 密码应用需求

(1) 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) 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通信过程中数据的完整性。

(3) 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通信过程中重要数据的机密性。

(4) 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) 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。

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. 系统运维人员未通过安全访问服务设备、安全组件与系统建立连接，未使用密码技术对运维人员进行身份鉴别，存在设备被非授权人员登录风险。
  2. 系统运维人员远程管理设备时，未采用密码技术建立安全的信息传输通道，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. 系统中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，存在系统资源访问控制信息未授权被篡改的风险。
  4. 系统未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，存在设备中重要信息资源安全标记被非授权篡改风险。
  5. 系统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，存在日志记录被非授权篡改风险。
  6. 系统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，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）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，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）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，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）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）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，对设备中的重要信息资源安全标记进行完整性保护。

（5）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，对日志记录进行完整性保护。

（6）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}} | 设备 | 测评对象 |
| [sblx] | [sbmc] | [cpdx] |

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/不适用解释 | 结论 |
| [cpdx] | [zb] | [yq] | [fxdj] | [syqk] | [xtxz] | [jl] |

## 3.5 应用和数据

### 3.5.1 风险分析

* 1. 系统不能保证应用系统用户身份的真实性，应采用密码技术对登录用户进行身份鉴别。
  2. 系统中存在信息系统应用的访问控制信息被未授权篡改的风险，应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。
  3. 系统中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，应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。
  4. 系统应用的重要数据存在重要数据被窃取和非授权篡改风险，应使用密码技术进行传输机密性和完整性、存储机密性和完整性保护。
  5. 系统应采用密码技术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。

### 3.5.2 密码应用需求

（1）应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，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。

（2）应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，对信息系统应用的访问控制信息进行完整性保护，防止被非授权篡改。

（3）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，对信息系统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。

（4）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，应用通过调用该密码设备或产品，对系统应用的重要数据进行传输机密性和完整性、存储机密性和完整性保护，实现重要数据防窃取和防篡改保护。

（5）应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，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}} | 测评对象 |
| [ywyy] | [cpdx] |

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。