**3 密码应用需求分析**

本节主要对本系统进行风险分析，最终得到针对本系统的密码应用需求分析清单。

**3.1 风险控制需求**

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面，对本系统进行风险分析，给出本系统密码应用需求。

**3.1.1 物理和环境安全（董涵宁）**

1. 风险分析

{{311a}}

1. 密码应用需求

{{311b}}

**3.1.2 网络和通信安全（贾红豆）**

1、风险分析

(1) XXX网IPSec VPN与IPSec VPN之间的通信信道

XXX网IPSec VPN客户端与IPSec VPN之间的通信信道未采用密码技术进行身份鉴别，未采用密码技术保证通信过程中数据的完整性和机密性，未采用密码技术保证网络边界访问控制信息的完整性。

(2) 互联网VPN客户端与运维SSL VPN之间的运维通信信道

互联网VPN客户端与运维SSL VPN之间的运维通信信道未采用密码技术进行身份鉴别，未采用密码技术保证通信过程中数据的完整性和机密性，未采用密码技术保证网络边界访问控制信息的完整性。

(3) 移动端与前台应用系统之间的通信信道

移动端与前台应用系统之间的通信信道未采用密码技术进行身份鉴别，未采用密码技术保证通信过程中数据的完整性和机密性，未采用密码技术保证网络边界访问控制信息的完整性。

(4) 互联网VPN客户端与内网SSL VPN之间的通信信道

互联网VPN客户端与内网SSL VPN之间的通信信道未采用密码技术进行身份鉴别，未采用密码技术保证通信过程中数据的完整性和机密性，未采用密码技术保证网络边界访问控制信息的完整性。

2、 密码应用需求

(1) XXX网IPSec VPN与IPSec VPN之间的通信信道

通过上述风险分析，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，实现身份鉴别，保证通信实体身份的真实性；保证通信过程中数据的完整性和机密性；保证网络边界访问控制信息的完整性；保证接入的设备身份真实性。

(2) 互联网VPN客户端与运维SSL VPN之间的运维通信信道

通过上述风险分析，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，实现身份鉴别，保证通信实体身份的真实性；保证通信过程中数据的完整性和机密性；保证网络边界访问控制信息的完整性；保证接入的设备身份真实性。

(3) 移动端与前台应用系统之间的通信信道

通过上述风险分析，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，实现身份鉴别，保证通信实体身份的真实性；保证通信过程中数据的完整性和机密性；保证网络边界访问控制信息的完整性；保证接入的设备身份真实性。

(4) 互联网VPN客户端与内网SSL VPN之间的通信信道

通过上述风险分析，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，实现身份鉴别，保证通信实体身份的真实性；保证通信过程中数据的完整性和机密性；保证网络边界访问控制信息的完整性；保证接入的设备身份真实性。

**3.1.3 设备和计算安全（卢焱）**

1. 风险分析

{{313a}}

1. 密码应用需求

根据上述风险分析，有以下应用需求。

{{313b}}

**3.1.4 应用和数据安全（张海政）**

1. 风险分析

{{314a}}

1. 密码应用需求

{{314b}}

**3.1.5 密码安全管理（董涵宁）**

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

{{315}}

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，评估通过后上线运行。

**3.2 密码应用需求分析清单**

通过深入分析{{sysname}}系统的安全风险，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 3.5所示。

表 3.5 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 | 采用密码技术对从外网连接到内部网络的设备进行接入认证，确保接入设备的身份真实性，防止非授权人员接入 | 无 |
| 设备和计算安全 | 身份鉴别 | 实现对运维人员的身份鉴别，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 | 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 | 无 |