**3 密码应用需求分析**

**3.1计算平台**

**3.1.1物理环境**

#### 3.1.1.1物理环境风险分析

{{?risk}}

{{?wlhhjRiskList}}

{{index}}、{{name}}

{{\*description}}

{{/wlhhjRiskList}}

{{/risk}}

3、XXX机房（云机房）

【云平台通过了密评】该系统部署在XXX云，云平台已通过密码应用安全性评估，且安全等级不低于此信息系统，其密评报告中对云支撑能力进行了评估，本机房作为被完全评估的支撑能力，能同时支撑云平台和云应用在物理和环境安全层面的密码应用安全，采用云平台测评结论。

#### 3.1.1.2物理环境密码应用需求分析

{XXX机房已采用合规的电子门禁系统和电子监控系统，符合密评要求，无需改造。}

身份鉴别：采用缓解措施，基于生物识别技术（如指纹等）对重要区域进入人员进行身份鉴别；或（2）重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控。缓解措施可降低本指标的高风险程度。

电子门禁记录数据完整性：本方案中，不对电子门禁记录数据进行改造和完整性保护。

视频监控记录数据完整性：本方案中，不对视屏监控记录数据进行改造和完整性保护。

**3.1.2网络环境**

#### 3.1.2.1网络环境风险分析

系统在网络环境涉及以下两条通信信道：①内部用户PC浏览器与业务系统之间的通信信道；②系统业务服务区和数据灾备区之间的专线通信信道；③公众用户移动端 APP与业务系统之间的通信信道；④XXX系统与业务系统之间的通信信道。

1. 内部用户PC浏览器与业务系统之间的通信信道

身份鉴别：通过采用国际算法（算法如RSA2048）的HTTPS方式进行连接，对通信实体未采用合规的方式进行身份鉴别，存在非法设备或非授权人员接入网络的风险。

通信数据完整性：通过采用国际算法（算法）的HTTPS方式进行连接，未采用合规的密码技术保证通信过程中数据的完整性，存在数据传输过程中被非授权篡改的风险。

通信过程中重要数据的机密性：通过采用国际算法（算法）的HTTPS方式进行连接，未采用合规的密码技术保证通信过程中重要数据的机密性，存在数据传输过程中被窃取的风险。

网络边界访问控制信息的完整性：未采用合规的密码技术保证通信过程中网络边界访问控制信息的完整性，存在数据传输过程中被非授权篡改的风险。

安全接入认证：本系统不涉及此需求，不纳入本次测评范围。

1. 系统业务服务区和数据灾备区之间的专线通信信道

身份鉴别：目前系统业务服务区和数据灾备区之间的专线通信信道使用专线进行灾备数据传输，通信前未使用密码技术对通信实体双方进行验证， 存在非法通信实体接入网络的风险。

通信数据完整性：目前系统业务服务区和数据灾备区之间的专线通信信道使用专线进行灾备数据传输，未使用密码技术对灾备数据传输通道进行机密性和完整性保护，存在通信数据在信息系统外部被非授权篡改的风险。

通信过程中重要数据的机密性：目前系统业务服务区和数据灾备区之间的专线通信信道使用专线进行灾备数据传输，未采用合规的密码技术保证通信过程中重要数据的机密性，存在数据传输过程中被窃取的风险。

网络边界访问控制信息的完整性：未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护，存在非法设备从外部接入内部网络，或网络边界被破坏。

安全接入认证：本系统不涉及此需求，不纳入本次测评范围。

1. 公众用户移动端 APP与业务系统之间的通信信道

身份鉴别：目前互联网系统移动端 APP的通信信道使用HTTP协议建立数据传输通道，通信前未使用密码技术对通信实体双方进行验证， 存在非法通信实体接入网络的风险。

通信数据完整性：目前互联网系统移动端 APP的通信信道使用HTTP协议建立数据传输通道，未使用密码技术保证通信过程中数据的完整性，存在数据传输过程中被非授权篡改的风险。

通信过程中重要数据的机密性：目前互联网系统移动端 APP的通信信道使用HTTP协议建立数据传输通道，未采用密码技术保证通信过程中重要数据的机密性，存在数据传输过程中被窃取的风险。

网络边界访问控制信息的完整性：未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护，存在非法设备从外部接入内部网络，或网络边界被破坏。

安全接入认证：本系统不涉及此需求，不纳入本次测评范围。

1. {{sysname}}与业务系统之间的通信信道

{{sysname}}与业务系统之间的通信信道不涉及敏感数据的传输，故本次密码应用建设不进行改造。

#### 3.1.2.2网络环境需求分析

1. 内部用户PC浏览器与业务系统之间的通信信道

身份鉴别：通过部署合规的SSL VPN产品，建立单向的商密SSL传输通道，对通信实体进行身份鉴别，保证通信实体身份的真实性；

通信过程中数据的完整性：通过部署合规的SSL VPN产品，建立商密SSL传输通道，通过SSL VPN技术对通信数据进行完整性保护；

通信过程中重要数据的机密性：通过部署合规的SSL VPN产品，建立商密SSL传输通道，通过SSL VPN技术对通信过程中的重要数据进行机密性保护；

网络边界访问控制信息做完整性：通过部署合规的SSL VPN产品，建立商密SSL传输通道，通过SSL VPN技术对防火墙的访问控制列表、边界路由的访问控制列表等网络边界访问控制信息进行完整性保护；

安全接入认证：本系统不涉及此需求，故不做特殊改造。

1. 系统业务服务区和数据灾备区之间的专线通信信道

身份鉴别：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等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；

通信过程中数据的完整性：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制对通信数据进行完整性保护；

通信过程中重要数据的机密性：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于密码算法的解密功能实现通信过程中重要数据的机密性保护；

网络边界访问控制信息做完整性：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对IPsec VPN中的访问控制列表进行完整性保护。

安全接入认证：本系统不涉及此需求，故不做特殊改造。

1. 公众用户移动端 APP与业务系统之间的通信信道

身份鉴别：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等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；

通信过程中数据的完整性：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制对通信数据进行完整性保护；

通信过程中重要数据的机密性：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于密码算法的解密功能实现通信过程中重要数据的机密性保护；

网络边界访问控制信息做完整性：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对SSL VPN安全网关、防火墙、边界路由中的访问控制列表进行完整性保护；

安全接入认证：本系统不涉及此需求，故不做特殊改造。

**3.1.3设备环境**

#### 3.1.3.1设备环境风险分析

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。

远程通道管理安全：本系统现阶段通过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。

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。

重要信息资源安全标记完整性：无重要信息资源安全标记。

日志记录完整性：本系统内各设备未采用密码技术保证日志记录的完整性，存在日志记录被非授权篡改的风险。

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。

#### 3.1.3.2设备环境需求分析

本系统在设备和计算安全层面的测评对象共分为三类，分别为堡垒机、通用设备、密码设备。其中，通用设备包括：应用服务器和数据库服务器以及数据库管理系统；密码设备包括【服务器密码机、签名验签服务器、国密安全密码应用中间件、SSL VPN安全网关、密钥管理系统】。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三类测评对象有以下密码应用需求。

1、堡垒机

1. 身份鉴别：采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性。

{在密码基础设施区部署堡垒机，给运维人员配发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），首先通过SSL VPN安全网关接入内网，再登录堡垒机进行设备的运维管理，SSL VPN安全网关的身份鉴别措施可有效缓解运维人员登录堡垒机的身份鉴别风险，因此不对堡垒机进行改造。（不改造堡垒机）}

1. 远程管理通道安全：采用密码技术建立安全的信息传输通道，实现对远程管理人员的身份鉴别，以及传输数据的机密性和完整性保护。

{在网络边界处部署已通过商用密码产品认证的SSL VPN安全网关登录堡垒机，先通过国密SSL协议建立运维人员到内网的安全传输通道，再使用堡垒机自签的证书，通过非国密HTTPS协议建立运维人员到堡垒机的安全传输通道。（不改造堡垒机）}

1. 系统资源访问控制信息完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等进行完整性保护。
2. 重要信息资源安全标记完整性：设备不涉及重要信息资源安全标记，此项不适用。
3. 日志记录完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的日志记录进行完整性保护。

{由于堡垒机不支持日志记录调出，本次项目暂不考虑对堡垒机的日志记录完整性进行密码应用建设。（不改造）}

1. 重要可执行程序完整性、重要可执行程序来源真实性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的重要可执行程序进行完整性保护并实现其来源的真实性保护。

{由于堡垒机技术上无法实现，本次项目暂不考虑对堡垒机重要可执行程序完整性和重要可执行程序来源真实性进行密码应用建设。（不改造）}

2、通用设备

1. 身份鉴别：采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性。

{使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机利用用户名+口令对通用类产品进行运维过程中的身份鉴别。（不改造堡垒机）}

1. 远程管理通道安全：采用密码技术建立安全的信息传输通道，实现对远程管理人员的身份鉴别，以及传输数据的机密性和完整性保护。

{使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机，由堡垒机使用无高风险的SSH2协议对通用设备进行运维的过程中远程管理通道安全的保护。（堡垒机不改造）}

1. 系统资源访问控制信息完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等进行完整性保护。
2. 重要信息资源安全标记完整性：设备不涉及重要信息资源安全标记，此项不适用。
3. 日志记录完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的日志记录进行完整性保护。

{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。}

1. 重要可执行程序完整性、重要可执行程序来源真实性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的重要可执行程序进行完整性保护并实现其来源的真实性保护。

{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。}

3、整机类密码设备

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。

{设备登录人员使用Ukey登录，采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性}

1. 远程管理通道安全：{密码设备通过堡垒机运维，堡垒机与密码设备之间需采用国密技术或密码技术构建安全的远程管理通道。}

{设备本地运维，不涉及远程管理通道，该指标作为不适用项处理。}

{使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机，由堡垒机使用无高风险的HTTPS协议对各密码设备进行运维的过程中的远程管理通道安全的保护。（堡垒机不改造）}

1. 系统资源访问控制信息完整性：上述密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备访问控制信息的保护。
2. 重要信息资源安全标记完整性：上述密码设备不涉及重要信息资源安全标记，该指标不适用。
3. 日志记录完整性：上述密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备日志信息的保护。
4. 重要可执行程序完整性、重要可执行程序来源真实性：上述密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对重要可执行程序完整性、真实性的保护。

4、系统类密码产品（国密安全密码应用中间件）

1. 身份鉴别：运维人员通过堡垒机使用USBKey（内有数字证书认证系统签发的国密SM2证书）登录到系统类密码产品，配合已通过商用密码产品检测认证的签名验签服务器，在登录时验证运维人员USBKey中的国密数字证书实现运维人员登录系统类密码产品的身份鉴别。
2. 远程管理通道安全：运维人员使用USBKey（内有数字证书认证系统签发的国密SM2证书）登录运维SSL VPN安全网关，再由堡垒机使用无高风险的HTTPS协议对系统类密码产品进行运维管理，从而搭建安全的远程管理通道，实现对系统类密码产品运维的过程中的远程管理通道安全的保护。
3. 系统资源访问控制信息完整性：系统类密码产品（国密安全密码应用中间件）已通过商用密码产品检测认证，通过对接服务器密码机，由国密安全密码应用中间件管理后台将应用主密钥和密钥ID传入服务器密码机，服务器密码机通过应用主密钥和密钥ID分散得到完整性保护密钥，使用完整性保护密钥基于HMAC-SM3算法对访问控制信息计算MAC值，并将访问控制信息和MAC值存储在国密安全密码应用中间件数据库中，查询或使用时，服务器密码机通过应用主密钥和密钥ID重新分散得到完整性保护密钥，对要查询或使用的访问控制信息和MAC值进行校验，实现系统资源访问控制信息的完整性保护。
4. 重要信息资源安全标记完整性：不涉及重要信息资源安全标记。
5. 日志记录完整性：系统类密码产品（国密安全密码应用中间件）已通过商用密码产品检测认证，通过对接服务器密码机，由国密安全密码应用中间件管理后台生成日志，并将应用主密钥和密钥ID传入服务器密码机，服务器密码机通过应用主密钥和密钥ID分散得到完整性保护密钥，使用完整性保护密钥基于HMAC-SM3算法对日志计算MAC值，并将日志和MAC值存储在国密安全密码应用中间件数据库中，查询或使用时，服务器密码机通过应用主密钥和密钥ID重新分散得到完整性保护密钥，对要查询或使用的日志和MAC值进行校验，实现日志记录的完整性保护。系统类密码产品已通过商用密码产品检测认证。
6. 重要可执行程序完整性、重要可执行程序来源真实性：系统类密码产品（国密安全密码应用中间件）难以通过密码技术实现相关保护，系统中重要可执行程序均从官方渠道获取，且在安装前对程序进行验证，保证其没有受到篡改。在一定程度上降低重要可执行程序完整性、重要可执行程序来源真实性保护的安全风险。因此本项目暂不采用密码技术对系统类密码产品（国密安全密码应用中间件）的重要可执行程序完整性、重要可执行程序来源真实性进行保护。系统类密码产品已通过商用密码产品检测认证。

**3.2业务应用**

**3.2.1业务应用风险分析**

身份鉴别：通过PC浏览器访问业务系统的内部员工，目前采用用户名+口令的方式登录业务系统，未采用合规的密码技术对登录用户进行身份鉴别，存在非授权人员登录的风险。

访问控制信息完整性：系统中未采用密码技术对访问控制信息进行完整性保护，存在访问控制信息被篡改的风险。

重要信息资源安全标记完整性：本系统无重要信息资源安全标记，此项不适用。

重要数据存储机密性：系统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，存在重要数据在存储过程中被窃取的风险。

重要数据存储完整性：系统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性。存在重要数据在存储过程中被非授权篡改的风险。

重要数据传输机密性：系统未采用合规的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，存在重要数据在传输过程中被窃取的风险。

重要数据传输完整性：系统未采用合规的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，存在重要数据在传输过程中被非授权篡改的风险。

不可否认性：本系统不涉及法律责任认定的应用场景，在本次密码应用改造及测评时，作不适用项处理。

{系统未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。}

**3.2.2业务应用需求分析**

身份鉴别：通过PC浏览器访问业务系统的内部员工，应采用合规的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，防止非授权人员登录。

{采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，在XXXX用户登录系统时对登录用户进行身份鉴别。（选择实际使用到的密码技术）}{XX{用户类型，如普通用户}{通过XX系统（第三方系统名称，如省统一身份认证平台）登录，}使用{账号口令+手机短信验证码/扫码/刷脸}方式登录业务系统，降低了应用和数据安全层面用户身份鉴别的风险。}

访问控制信息完整性：应采用密码技术对访问控制信息进行完整性保护，防止访问控制信息被篡改。

{采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对应用系统的权限、标签等能够决定系统应用访问控制的措施等信息进行完整性保护。}

重要信息资源安全标记完整性：本系统不涉及重要信息资源安全标记，故不做特殊改造。

重要数据传输机密性：应通过调用合规的密码设备或产品，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。

{采用密码技术的加解密功能，对系统重要数据进行传输过程中的机密性保护。}（只有在应用层面传输做了数字信封，才能描述重要数据进行了应用层面的传输机密性保护）

{依赖网络层构建的安全通道缓解。}（数据传输不进行改造，通过网络层缓解）

重要数据传输完整性：应通过调用合规的密码设备或产品，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。

{采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对信息系统应用中重要数据进行传输过程中的完整性保护。}（只有在应用层面传输做了数据源的完整性保护，才能描述重要数据进行了应用层面的传输完整性保护）

{依赖网络层构建的安全通道缓解。}（数据传输不进行改造，通过网络层缓解）

重要数据存储机密性：应通过调用合规密码设备或产品，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。

{采用密码技术的加解密功能，对系统中重要数据进行存储过程中的机密性保护。}

重要数据存储完整性：应通过调用合规的密码设备或产品，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。

{采用密码技术的加解密功能，对系统中重要数据进行存储过程中的机密性保护。采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对系统的重要业务日志做完整性保护}

不可否认性：本系统不涉及法律责任认定的应用场景，在本次密码应用改造及测评时，作不适用项处理。

{采用基于公钥密码算法的数字签名机制等密码技术，对XXX{示例：系统用户的事项申请行为、业务办理审批行为}等关键行为进行签名，实现数据原发行为和数据接收行为的不可否认性。}

**3.3安全管理**

**3.3.1安全管理风险分析**

单位根据等保2.0管理要求，目前虽然已经制定了通用的《某部信息 安全管理制度汇编 》，但该安全管理制度汇编内容仅涉及安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等5个方面的安全管理要求。未对密码应用的管理制度、人员管理、建设运行和应急处置等方面制定专用的密码应用管理制度。

未依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的安全管理要求，制定密码相关管理制度，不利于在本系统中落实密码相关国家政策要求，不利于发挥密码在信息系统安全中的基础支撑作用。

**3.3.2安全管理需求分析**

需依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，从管理制度、人员管理、建设运行、应急处置等4个方面制定并建设密码应用管理保障体系。需制定本系统的密码应用方案，并委托密评机构对密码应用方案进行评估，评估通过后按照本方案完成系统密码应用建设，委托合规的第三方测评机构依据密码应用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。