**5 密码应用技术方案**

本方案根据{{sysname}}系统密码应用改造要求和相关建设的整体规划，以及密码应用的合规性、正确性和有效性，保证密码应用改造的正确实施部署，来采用此套密码应用技术方案。

## {{img51}}5.1 密码应用技术框架（陈凯）

图 5.1 密码应用技术架构

基于国产密码标准体系和密码管理体系，结合{{sysname}}系统平台的实际情况，基于GB/T 39786-2021《信息系统密码应用基本要求》，建设以保护业务系统的身份认证及数据资产为中心的、自主可控的密码服务体系，通过核心的密码技术、密码模块、密码产品、密码基础设施等产品服务，为网络基础资源、信息设施、计算分析、应用服务、网络通道、接入终端、设备控制等提供身份鉴别、访问控制、数据机密性、完整性、及抗抵赖的密码服务。密码应用技术总体架构如图 5.1所示。

{{sysname}}系统密码应用架构由密码应用层、密码服务层、密码设施层和密码算法层四部分组成。

1、 密码应用层

密码应用层通过调用密码服务平台的一系列服务来保证密码应用安全：

(1) 终端安全密码应用：PC端采用智能密码钥匙解决用户在登录系统和业务操作的身份鉴别，移动端采用手机盾实现用户在登陆系统的身份鉴别，保证了身份的真实性。

(2) 网络和通信安全密码应用，部署SSL VPN和IPSec VPN，实现终端身份鉴别和数据传输加密保护；在PC端部署VPN客户端，建立数据安全传输通道。

(3) 应用和数据安全密码应用，主要为业务应用提供身份验证服务、数据加密服务、完整性验证服务、数据安全存储服务。

(4) 设备和计算安全密码应用，主要对系统内各设备进行管理，对运维人员以及登录设备的用户进行身份鉴别，保证远程管理通道安全，提供访问控制信息完整性保护、日志记录完整性保护和重要程序完整性保护等。

2、 密码服务层

密码服务层为密码应用层提供数据加密服务、时间戳服务、签名验签服务、完整性验证服务、数据库安全服务和身份认证服务等密码应用所需基础服务。

3、 密码设施层

{{51}}

其中：

{{\*list51}}

4、密码算法层

密码算法层为国家标准或国家密码行业标准形式公开发布的算法，包括SM1、SM2、SM3、SM4算法，是商用密码产品的核心算法。

## 5.2 物理和环境安全（董涵宁）

物理和环境安全要求，采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，保护物理访问控制身份鉴别信息。符合该标准的电子门禁系统使用SM4等算法进行密钥分散，实现门禁卡的一卡一密，并基于SM4等算法鉴别人员身份。

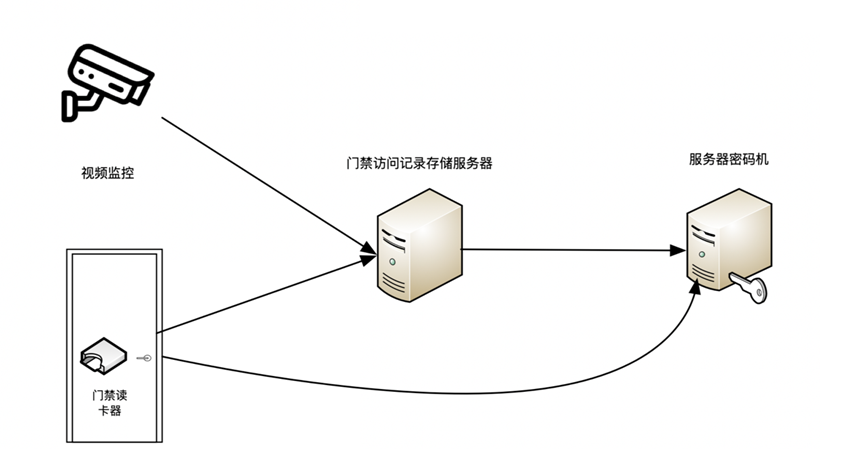


图 5.2 物理环境图

{{?wuli}}

{{jifang}}

{{\*list52}}

{{/wuli}}

表 5.1 物理和环境安全保护对象

|  |  |  |
| --- | --- | --- |
| {{table52}}序号 | 安全层面 | 保护对象 |
| [id] | [level] | [object] |

## 5.3 网络和通信安全（贾红豆、陈凯、曹冉筝）

网络与接入安全密码应用，在应用系统接入边界部署安全网关，配合远程终端在应用系统，对访问应用业务系统的用户进行身份鉴别和权限控制，对传输的数据进行机密性和完整性保护。

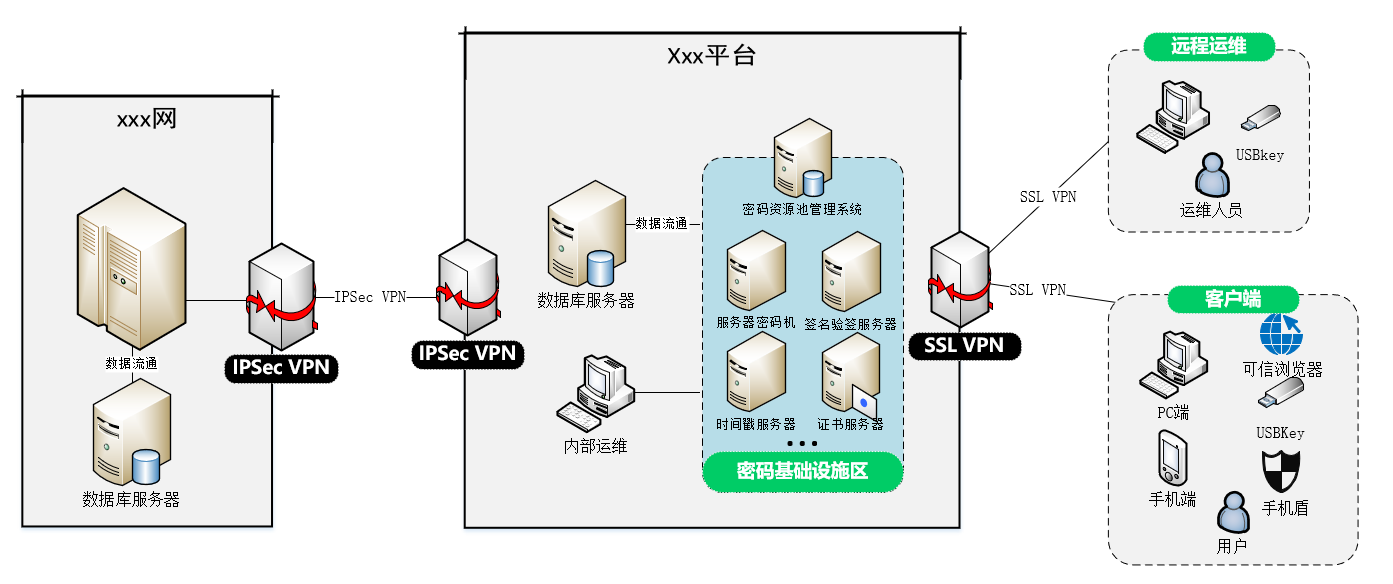


图 5.3 网络和通信安全架构图

{{?wangluo}}

{{tongdao}}

{{\*list53}}

{{/wangluo}}

表 5.2 网络与通信安全保护对象

|  |  |  |
| --- | --- | --- |
| {{table53}}序号 | 安全层面 | 保护对象 |
| [id] | [level] | [object] |

## 5.4 设备和计算安全（卢焱、王晨、曹冉筝）

在设备和计算安全中主要是指管理员在对业务系统进行运维时，需要对运维管理员身份鉴别，保障网络环境中主机系统以及存储资源以及其上所承载的应用程序等重要数据的机密性和完整性。架构图如图 5.6所示：



图 5.4 设备和计算安全架构图

{{?jisuan}}

{{shebei}}

{{\*list54}}

{{/jisuan}}

表 5.3 设备与计算安全保护对象

|  |  |  |
| --- | --- | --- |
| {{table54}}序号 | 安全层面 | 保护对象 |
| [id] | [level] | [object] |

## 5.5 应用和数据安全（冯天浩、张海政、刘双平）

针对在应用和数据安全层面的密码应用需求，本节提出对应的功能设计，主要包括身份鉴别、访问控制信息完整性、重要数据传输完整性、重要数据传输机密性、重要数据存储机密性、重要数据存储完整性、不可否认性，应用和数据安全架构图如图 5.7所示。



图 5.5 应用和数据安全架构图

{{?yingyong}}

{{yewu}}

{{\*list55}}

{{/yingyong}}

表 5.4 应用与数据安全保护对象

|  |  |  |
| --- | --- | --- |
| {{table55}}序号 | 安全层面 | 保护对象 |
| [id] | [level] | [object] |

## 5.6 密**钥管**理

描述系统中各密钥全生命周期涉及的密钥管理方案和使用的独立的密钥管理设备、设施（若有）。

1. 密钥管理（还没设计）

表 5.5 密钥管理表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **算法** | **用途** | **存储位置** |
| 1 | {用户密钥} | {SM4} | {对数据加密密钥进行加密} | 服务器密码机 |

1. 密钥生命周期（还没设计）

表 5.6 密钥生命周期表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **生产** | **存储** | **分发** | **导入和导出** | **使用** | **备份和恢复** | **归档** | **销毁** |
| 1 | 用户CA公钥 | 不涉及，由CA生产 | 以证书形式存储 | 以证书形式离线分发 | 以证书形式离线导入和导出 | 以证书形式使用 | 不涉及、由CA备份和恢复 | 不涉及、 由CA归档 | 不涉及、 由CA销毁 |

**5.7 密码应用部署（贾红豆）**

密码应用部署拓扑图如所示：

1. 客户端在PC端配发USBKey智能密码钥匙。授权用户通过PC端登录，采用SM2数字证书认证机制，使用USBKey，与安全通道中的SSL VPN安全网关之间，实现双向身份认证，确保授权用户身份的真实性。



图 5.6 密码应用部署拓扑图

1. 安全通道部署SSL VPN安全网关，系统运维人员配发智能密码钥匙，由CA机构签发SM2数字证书，实现客户端与SSL VPN安全网关之间的双向身份认证。运维人员通过安装SSL VPN客户端实现安全接入。
2. 服务端包括交换机以及密码基础设施区，密码基础设施包括服务器密码机、签名验签服务器、时间戳服务器、证书认证系统、国密安全密码应用中间件为上层提供各种密码服务：服务器密码机可以提供加解密服务和密钥管理服务；签名验签服务器可以提供签名验签服务，实现身份验证；时间戳服务器的时间戳签发服务可以为操作节点签发时间戳，实现操作行为可追溯；证书认证系统为用户的身份鉴别提供真实性服务；国密安全密码应用中间件可以提供重要数据存储的机密性与完整性保护。

## 5.8 密码软硬件产品清单（刘双平）

通过上述分析，{{sysname}}系统的实现所需的密码产品所包括硬件、软件以及相关的服务如表5.7所示。

表 5.7 系统密码软硬件清单表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **{{table58}}序号** | **产品名称** | **部署位置** | **使用的密码算法** | **数量** | **用途** |
| [id] | [name] | [location] | [algorithm] | [num] | [function] |

**5.9 安全与合规性分析**

{{sysname}}系统的安全与合规性分析如表5.8所示。

表 5.8 安全与合规性分析表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性  （符合/不适用） | 说明  （针对不适用项说明原因及替代性措施） |
| 物理和环境安全 | 身份鉴别 | 采用安全门禁系统实现进入人员身份鉴别 | 符合 | 无 |
| 电子门禁记录数据完整性 | 部署服务器密码机，使用HMAC对电子门禁记录数据和视频记录数据进行完整性保护 |
| 视频监控记录数据完整性 |
| 密码服务 | 密码应用技术服务 |
| 密码产品 | 服务器密码机 |
| 网络和通信安全 | 身份鉴别 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现通信实体身份鉴别，保证通信实体身份的真实性 | 符合 | 无 |
| 通信数据完整性 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现通信数据的机密性和完整性保护 | 符合 | 无 |
| 通信过程中重要数据的机密性 |
| 网络边界访问控制信息的完整性 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现网络边界访问控制信息的完整性保护 | 符合 | 无 |
| 安全接入认证 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现安全接入 | 符合 | 无 |
| 密码服务 | 数字证书认证服务 | 符合 | 无 |
| 密码产品 | SSL VPN、IPSec VPN、智能密码钥匙 | 符合 | 无 |
| 设备和计算安全 | 身份鉴别 | 在本系统运维人员PC端，配发USBKey，在密码基础设施区部署签名验签服务器，用户登录应用时验证人员数字签名，实现对登录应用用户的安全身份鉴别，防止非授权人员登录 | 符合 | 无 |
| 远程管理通道安全 | 采用遵循密码相关国家标准和行业标准的VPN技术，使用密码产品SSL VPN安全网关搭建安全的远程管理通道 | 符合 | 无 |
| 系统资源访问控制信息完整性 | 在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护 | 符合 | 无 |
| 重要信息资源安全标记完整性 | - | 不适用 | 本系统不涉及重要信息资源的敏感标记 |
| 日志记录完整性 | 在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC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 | 符合 | 无 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性 | 符合 | 无 |
| 密码服务 | 数字证书认证服务、密钥管理服务 | 符合 | 无 |
| 密码产品 | SSL VPN安全网关、USBKey、服务器密码机、签名验签服务器 | 符合 | 无 |
| 应用和数据安全 | 身份鉴别 | 在本系统应用用户人员PC 端采用USBKey登录，在基础设施区部署签名验签服务器，用户登录应用时验证人员数字签名，实现对登录应用用户的安全身份鉴别，防止非授权人员登录 | 符合 | 无 |
| 访问控制信息完整性 | 在密码基础设施区部署服务器密码机，使用HMAC对系统应用的访问控制信息进行完整性保护，防止访问控制信息被篡改 | 符合 | 无 |
| 重要信息资源安全标记完整性 | - | 不适用 | 本系统不涉及重要信息资源的敏感  标记 |
| 重要数据传输机密性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2及SM3算法进行会话密钥交互，采用SM4算法对传输的数据信息进行机密性保护，防止其被非授权窃取 | 符合 | 无 |
| 重要数据存储机密性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用SM4算法对数据信息存储进行机密性保护，防止其被非授权窃取 | 符合 | 无 |
| 重要数据传输完整性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2算法进行会话密钥交互，采用HMAC算法对传输的数据信息进行完整性保护，防止其被非授权篡改 | 符合 | 无 |
| 重要数据存储完整性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用HMAC对数据信息存储进行完整性保护，防止其被非授权篡改 | 符合 | 无 |
| 不可否认性 | 在基础设施区部署时间戳服务器，在系统中重要数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性 | 符合 | 无 |
| 密码服务 | 密码应用技术服务 | 符合 | 无 |
| 密码产品 | 服务器密码机、国密安全密码应用中间件、签名验签服务器、时间戳服务器、可信浏览器、USBKey | 符合 | 无 |