# 5 密码应用技术方案

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况，项目预算及拟采购的密码产品，设计密码应用技术方案，保障密码应用的合规性、正确性和有效性。

其中，5.1节介绍密码应用技术框架和整体架构，5.2-5.5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介绍典型的密码应用技术方案，以及结合本系统实际情况、采用的密码产品、设计的密码应用解决方案，5.6节介绍密钥管理方案，5.7节介绍密码应用部署，5.8节介绍本项目拟采购的密码软硬件产品，5.9节从物理和环境、网络和通信、设备和计算、应用和数据四个方面，做商用密码应用的技术部分安全与合规性分析，其中\*号为《信息系统密码应用高风险判定指引》中标注的高风险项。

## 5.1 密码应用技术框架

基于国产密码标准体系和密码管理体系，结合目标信息系统的实际情况，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。

图 5.1 密码应用技术架构

{{sysname}}密码应用架构分为密码算法层、密码设施层、密码基础服务层和密码应用层，密码应用层包括用户终端安全密码应用、网络接入网络和通信安全密码应用、业务安全密码应用和数据安全密码应用、平台管理安全密码应用设备和计算安全密码应用四部分。

1. 密码基础服务层

{{51}}

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：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，保证了身份的真实性。
  2. 网络接入安全密码应用，部署可信浏览器、SSL VPN、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. 系统业务安全密码应用，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。

3、密码设施层

基于各密码产品构建的密码基础服务层的主要功能是为上层应用提供密码基础服务支撑，实现上层应用的密码安全增强。该平台使用符合国家密码法规和标准规定的商用密码算法，使用经过国家密码管理局核准的密码产品，遵循“GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》”以及相关“密评”规范。

密码设施层整合服务器密码机、签名验签服务系统、通用统一密码等产品能力，打造服务化、场景化，易于行业快速对接集成的密码服务能力，对外统一提供密码服务、集约化建设，密码服务可弹性扩展。

以下密码产品均满足GB/T 37092-2018《信息安全技术 密码模块安全要求》或GM/T 0028-2014《密码模块安全技术要求》密码模块二级及以上。

{{\*s582}}

## 5.2 物理和环境安全

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》：采用基于密码技术的电子门禁系统和视频监控系统，对设备机房出入人员的身份进行鉴别，并对电子门禁系统进出记录数据和视频监控音像记录数据进行完整性保护。

{{?solution}}

{{?wlhhjFAList}}

{{index}}、{{name}}

{{\*description}}

{{/wlhhjFAList}}

## 5.3 网络和通信安全

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。具体如表5.2所示，架构图如图5.2所示。



图 5.2 网络和通信安全架构图

{{?wlhtxFAList}}

{{index}}、{{name}}

{{\*description}}

{{/wlhtxFAList}}

## 5.4 设备和计算安全

在设备和计算安全中主要是指运维人员在对业务系统进行运维时，需要对运维人员身份鉴别，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。具体如表5.3所示，架构图如图 5.3所示。



图 5.3 设备和计算安全架构图

{{?sbhjsFAList}}

{{index}}、{{name}}

{{\*description}}

{{/sbhjsFAList}}

## 5.5 应用和数据安全

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，具体如表5.4所示，架构图如图 5.4所示。



图 5.4 应用和数据安全架构图

{{?yyhsjFAList}}

{{index}}、{{name}}

{{\*description}}

{{/yyhsjFAList}}

{{/solution}}

## 5.6 密钥管理

1) 密钥管理

表 5.5 密钥管理表

| **序号** | **密钥名称** | **算法** | **用途** | **存储位置** |
| --- | --- | --- | --- | --- |
| 1 | 重要数据传输机密性保护密钥 | SM4 | 用于保护SSL通道中重要业务数据的传输机密性 | 临时协商，用完销毁 |
| 2 | 重要数据传输链路身份鉴别私钥 | SM2 | 用于建立链路时SSL客户端和服务端的身份鉴别 | 服务端在密码卡、客户端在UKEY |
| 3 | 重要数据传输链路身份鉴别公钥 | SM2 | 以证书形式使用，用于建立链路时SSL客户端和服务端的身份鉴别 | 服务端在密码卡、客户端在UKEY |
| 4 | 重要数据传输链路密钥协商私钥 | SM2 | 用于SSL客户端和服务端的密钥协商 | 服务端在密码卡、客户端在UKEY |
| 5 | 重要数据传输链路密钥协商公钥 | SM2 | 以证书形式使用，用于SSL客户端和服务端的密钥协商 | 服务端在密码卡、客户端在UKEY |
| 6 | 用户签名私钥 | SM2 | 系统管理员登录应用系统 | Ukey |
| 7 | 用户签名公钥 | SM2 | 以证书形式使用，用于系统管理员登录应用系统 | Ukey |
| 6 | 应用系统主密钥 | SM4 | 用于通过密钥分散技术，派生重要数据存储完整性保护密钥和重要数据存储机密性保护密钥 | 密码应用中间件数据库 |
| 7 | 应用系统主密钥保护密钥 | SM4 | 用于保护应用系统主密钥 | 服务器密码机 |
| 8 | 重要数据存储完整性保护密钥 | HMAC | 用于保护身份鉴别信息、重要业务数据、日志数据的存储完整性 | 临时分散，用完销毁 |
| 9{{table512}} | 重要数据存储机密性保护密钥 | SM4 | 用于保护身份鉴别信息、重要业务数据的存储机密性 | 临时分散，用完销毁 |
| [id] | [name] | [sf] | [yt] | [location] |

2) 密钥生命周期

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | 重要数据传输机密性保护密钥 | SSL VPN客户端和服务端通过重要数据传密钥协商公私钥协商产生 | 临时协商、用完销毁 | 不涉及 | 不涉及 | VPN内部使用 | 不涉及 | 不涉及 | 临时协商、用完销毁 |
| 2 | 重要数据传输链路身份鉴别私钥 | VPN密码卡内部产生 | VPN密码卡内部存储 | 不涉及 | 不涉及 | VPN内部使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 3 | 重要数据传输链路身份鉴别公钥 | VPN密码卡内部产生 | VPN密码卡内部存储 | 不涉及 | 以公钥证书形式导入导出 | 以公钥证书形式使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 4 | 重要数据传输链路密钥协商私钥 | 由CA生产 | VPN密码卡内部存储 | 不涉及 | 不涉及 | VPN内部使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 5 | 重要数据传输链路密钥协商公钥 | 由CA生产 | VPN密码卡内部存储 | 不涉及 | 以公钥证书形式导入导出 | 以公钥证书形式使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 6 | 用户签名私钥 | 由ukey产生 | Ukey内部存储 | 不涉及 | 不涉及 | Ukey内部使用 | 不涉及 | 不涉及 | Ukey内部销毁 |
| 7 | 用户签名公钥 | 由ukey产生，由CA签发为公钥证书形式 | 以公钥证书形式存储 | 以公钥证书形式分发 | 以公钥证书导入导出 | 以公钥证书形式使用 | 不涉及、由CA备份和恢复 | 不涉及、 由CA归档 | 不涉及、 由CA销毁 |
| 8 | 应用系统主密钥 | 由密钥管理系统产生 | 密钥管理系统内部存储；  密码应用中间数据库密文存储； | 密钥管理系统使用密码应用中间平台根证书加密后分发至密码应用中间件；  密码应用中间将密文形式的应用系统主密钥分发至服务器密码机； | 不涉及 | 服务器密码机内部使用 | 密钥管理系统内部备份恢复 | 密钥管理系统内部归档 | 密钥管理系统内部销毁；密码应用中间件内部销毁 |
| 9 | 应用系统主密钥保护密钥 | 由服务器密码机内部产生 | 由服务器密码机内部存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部备份恢复 | 不涉及 | 服务器密码机内部销毁 |
| 10 | 重要数据存储完整性保护密钥 | 由服务器密码机通过应用系统主密钥进行密钥分散内部产生 | 临时分散，用完销毁 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 临时分散，用完销毁 | 临时分散，用完销毁 | 临时分散，用完销毁 |
| 11{{table513}} | 重要数据存储机密性保护密钥 | 由服务器密码机通过应用系统主密钥进行密钥分散内部产生 | 临时分散，用完销毁 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 临时分散，用完销毁 | 临时分散，用完销毁 | 临时分散，用完销毁 |
| [id] | [name] | [production] | [storage] | [ff] | [drhdc] | [use] | [bfhhf] | [gd] | [xh] |

## 5.7 密码应用部署

密码应用部署拓扑图如图5.5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 5.5 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、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

通过上述分析，该目标系统的密码应用改造所需的密码产品所包括硬件、软件以及相关的服务，如表5.6所示。

表 5.6 密码软硬件产品清单表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号{{table57}} | 产品名称 | 部署位置 | 主要用途 | 数量  (台/套) | 备注 |
| [id] | [name] | [location] | [function] | [num] | [remark] |

## 5.9 安全与合规性分析

### 5.9.1 物理和环境安全

物理与环境安全与合规性分析结果如表5.7所示：

表 5.7 安全与合规性分析表-物理和环境

|  |  |  |  |
| --- | --- | --- | --- |
| **指标点{{table58}}** | **测评对象** | **测评指标预测符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评预测结果（符合/部分符合/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |

### 5.9.2 网络和通信安全

网络和通信安全与合规性分析结果如表5.8所示：

表 5.8 安全与合规性分析表-网络和通信

|  |  |  |  |
| --- | --- | --- | --- |
| **指标点{{table59}}** | **测评对象** | **测评指标预测符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评预测结果（符合/部分符合/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |

### 5.9.3 设备和计算安全

设备和计算安全与合规性分析结果如表5.9所示：

表 5.9 安全与合规性分析表-设备和计算

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元{{table510}}** | **测评对象** | **测评指标预测符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评预测结果（符合/部分符合/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |

### 5.9.4 应用和数据安全

应用和数据安全与合规性分析结果如表5.10所示：

表 5.10 安全与合规性分析表-应用和数据

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元{{table511}}** | **测评对象** | **测评指标预测符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评预测结果（符合/部分符合/不符合/不适用）** |
| [zb] | [cpdx] | [cpzb] | [dycp] |