**交通银行股份有限公司**

**TSM可信服务管理平台软件采购项目**

**投标技术方案**

**2021年03月**

目录

[1. 对项目产品的理解 6](#_Toc67944621)

[1.1. 项目名称 6](#_Toc67944622)

[1.2. 项目产品 6](#_Toc67944623)

[1.3. 项目产品设计原则 7](#_Toc67944624)

[1.3.1. 整体性原则 7](#_Toc67944625)

[1.3.2. 继承性原则 7](#_Toc67944626)

[1.3.3. 实用性原则 7](#_Toc67944627)

[1.3.4. 平台化和组件化原则 7](#_Toc67944628)

[1.3.5. 先进性和成熟性原则 8](#_Toc67944629)

[1.3.6. 标准化和开放性原则 8](#_Toc67944630)

[1.3.7. 可维护性和扩展性原则 8](#_Toc67944631)

[1.3.8. 安全性和保密性原则 8](#_Toc67944632)

[1.3.9. 高性能和稳定性原则 9](#_Toc67944633)

[1.4. 缩略语和术语 9](#_Toc67944634)

[1.4.1. 缩略语 9](#_Toc67944635)

[1.4.2. 术语定义 11](#_Toc67944636)

[2. 产品总体设计 12](#_Toc67944637)

[2.1. 系统应用架构 12](#_Toc67944638)

[2.2. 系统技术架构 13](#_Toc67944639)

[2.3. 高可用部署方案 16](#_Toc67944640)

[2.3.1. 单点部署 16](#_Toc67944641)

[2.3.2. 高可用分布式集成部署 16](#_Toc67944642)

[2.3.3. 微服务云与容器虚拟化架构 19](#_Toc67944643)

[2.4. 系统安全等级保护 19](#_Toc67944644)

[2.4.1. 网络安全 19](#_Toc67944645)

[2.4.2. 主机安全 21](#_Toc67944646)

[2.4.3. 应用安全 22](#_Toc67944647)

[2.4.4. 数据安全与备份恢复 23](#_Toc67944648)

[2.5. 产品技术路线 23](#_Toc67944649)

[2.5.1. J2EE技术体系 23](#_Toc67944650)

[2.5.2. 微服务架构 25](#_Toc67944651)

[2.5.3. WS服务接口技术 26](#_Toc67944652)

[2.5.4. 基于UML的模型设计 26](#_Toc67944653)

[2.5.5. PKI/CA安全开发技术 27](#_Toc67944654)

[2.5.6. GP技术规范 28](#_Toc67944655)

[2.6. TSM平台性能指标 30](#_Toc67944656)

[3. 产品功能方案 32](#_Toc67944657)

[3.1. 门户与个人中心 32](#_Toc67944658)

[3.1.1. 用户登录 33](#_Toc67944659)

[3.1.2. 忘记密码 34](#_Toc67944660)

[3.1.3. 个人中心 34](#_Toc67944661)

[3.1.4. 修改密码 34](#_Toc67944662)

[3.1.5. 个人信息 35](#_Toc67944663)

[3.2. 系统配置管理 35](#_Toc67944664)

[3.2.1. 平台机构设置 35](#_Toc67944665)

[3.2.2. SE厂商及类型设置 36](#_Toc67944666)

[3.3. TSM接口配置 37](#_Toc67944667)

[3.3.1. SE-TSM接口配置 37](#_Toc67944668)

[3.3.2. SP-TSM接口配置 38](#_Toc67944669)

[3.4. SE/安全域信息管理 38](#_Toc67944670)

[3.4.1. SE信息管理 38](#_Toc67944671)

[3.4.2. 安全域信息管理 40](#_Toc67944672)

[3.4.3. 安全域密钥配置管理 40](#_Toc67944673)

[3.5. 应用包信息管理 41](#_Toc67944674)

[3.5.1. 应用实例AID分配 41](#_Toc67944675)

[3.5.2. 应用信息管理 41](#_Toc67944676)

[3.6. 个人化信息管理 44](#_Toc67944677)

[3.6.1. 个人化证书信息 44](#_Toc67944678)

[3.6.2. 个人化钱包信息 44](#_Toc67944679)

[3.6.3. 个人化方案配置 45](#_Toc67944680)

[3.6.4. 应用安装适配管理 45](#_Toc67944681)

[3.6.5. 应用安装指令流程设置 48](#_Toc67944682)

[3.6.6. 应用实例化信息管理 49](#_Toc67944683)

[3.7. 接入服务管理 49](#_Toc67944684)

[3.7.1. 证书密钥信息管理 49](#_Toc67944685)

[3.7.2. 接口服务密钥管理 50](#_Toc67944686)

[3.7.3. SE合作商管理 51](#_Toc67944687)

[3.7.4. SE商户信息管理 52](#_Toc67944688)

[3.7.5. SE注册信息管理 52](#_Toc67944689)

[3.8. 统计分析管理 52](#_Toc67944690)

[3.8.1. 应用实例化日统计 52](#_Toc67944691)

[3.8.2. 应用实例化分类汇总 53](#_Toc67944692)

[3.9. 系统权限管理 53](#_Toc67944693)

[3.9.1. 角色管理 53](#_Toc67944694)

[3.9.2. 用户管理 56](#_Toc67944695)

[3.10. 平台维护管理 57](#_Toc67944696)

[3.10.1. 系统参数设置 57](#_Toc67944697)

[3.10.2. 预警设置 57](#_Toc67944698)

[3.10.3. 日志管理 58](#_Toc67944699)

[3.10.4. 服务器监测 58](#_Toc67944700)

[3.11. TSM密码机系统 58](#_Toc67944701)

[3.12. 物联网支付终端注册及认证管理 59](#_Toc67944702)

[3.13. 数币应用支撑中间件 60](#_Toc67944703)

[4. 产品服务接口 61](#_Toc67944704)

[4.1. SE状态查询 61](#_Toc67944705)

[4.2. 应用申请 63](#_Toc67944706)

[4.2.1. 报文功能 63](#_Toc67944707)

[4.2.2. 报文结构 63](#_Toc67944708)

[4.3. 应用加载 64](#_Toc67944709)

[4.3.1. 报文功能 64](#_Toc67944710)

[4.3.2. 报文结构 64](#_Toc67944711)

[4.4. 应用删除 65](#_Toc67944712)

[4.4.1. 报文功能 65](#_Toc67944713)

[4.4.2. 报文结构 65](#_Toc67944714)

[4.5. 应用锁定 66](#_Toc67944715)

[4.5.1. 报文功能 66](#_Toc67944716)

[4.5.2. 报文结构 66](#_Toc67944717)

[4.6. 应用解锁 68](#_Toc67944718)

[4.6.1. 报文功能 68](#_Toc67944719)

[4.6.2. 报文结构 68](#_Toc67944720)

[5. 项目实施方案 70](#_Toc67944721)

[5.1. 项目管理的目的 70](#_Toc67944722)

[5.2. 项目管理措施 71](#_Toc67944723)

[5.3. 项目管理制度 71](#_Toc67944724)

[5.3.1. 决策制度 71](#_Toc67944725)

[5.3.2. 交流制度 72](#_Toc67944726)

[5.3.3. 例会制度 72](#_Toc67944727)

[5.3.4. 问题与争议管理方法 73](#_Toc67944728)

[5.3.5. 失误管理制度 73](#_Toc67944729)

[5.3.6. 工作管理制度 74](#_Toc67944730)

[5.3.7. 项目变更管理 74](#_Toc67944731)

[5.3.8. 计划管理 75](#_Toc67944732)

[5.3.9. 质量保证措施 76](#_Toc67944733)

[5.4. 项目风险管理 76](#_Toc67944734)

[5.4.1. 风险的定义和识别 76](#_Toc67944735)

[5.4.2. 风险的量化和分析 77](#_Toc67944736)

[5.4.3. 风险控制的组织架构和风险控制流程 78](#_Toc67944737)

[5.4.4. 风险对策控制的输入项 79](#_Toc67944738)

[5.4.5. 风险对策实施控制的工具和方法 79](#_Toc67944739)

[5.4.6. 风险对策实施控制输出项 79](#_Toc67944740)

[5.5. 项目组织机构与管理 80](#_Toc67944741)

[5.5.1. 项目进度管理 80](#_Toc67944742)

[5.5.2. 项目组织机构 80](#_Toc67944743)

[5.5.3. 各阶段的任务 84](#_Toc67944744)

[5.5.4. 各阶段开始标识 88](#_Toc67944745)

[5.5.5. 各阶段结束标识 88](#_Toc67944746)

[5.6. 培训方案 88](#_Toc67944747)

[5.6.1. 培训目的 88](#_Toc67944748)

[5.6.2. 培训方式 89](#_Toc67944749)

[5.6.3. 培训要求 90](#_Toc67944750)

[5.6.4. 培训内容及计划 91](#_Toc67944751)

[5.7. 软件质量保障措施 91](#_Toc67944752)

[5.7.1. 制定项目计划 92](#_Toc67944753)

[9.3.2 制定质量保障计划 93](#_Toc67944754)

[9.3.3 制定软件系统测试﹑考核制度 93](#_Toc67944755)

[9.3.4 软件质量控制 94](#_Toc67944756)

[5.8. 应急响应服务 96](#_Toc67944757)

[5.8.1. 应急响应情况分类 96](#_Toc67944758)

[5.8.2. 应急响应处理流程 97](#_Toc67944759)

[5.8.3. 应急响应人员组织管理体系 97](#_Toc67944760)

[5.8.4. 安全事件应急响应措施 97](#_Toc67944761)

[5.9. 项目管理方案 98](#_Toc67944762)

[5.9.1. 项目管理目标 98](#_Toc67944763)

[5.9.2. 项目管理工具 99](#_Toc67944764)

[5.9.3. 项目协调及沟通管理 99](#_Toc67944765)

[6. 售后服务及技术支持 100](#_Toc67944766)

[6.1. 技术支持服务总体说明 100](#_Toc67944767)

[6.1.1. 质量保证期内的售后服务 101](#_Toc67944768)

[6.1.2. 质量保证期外的技术支持与服务 102](#_Toc67944769)

[6.2. 技术支持服务组织 103](#_Toc67944770)

[6.3. 技术支持服务质量控制 104](#_Toc67944771)

[6.3.1. 服务质量保证体制 104](#_Toc67944772)

[6.3.2. 客户投诉处理 105](#_Toc67944773)

[6.4. 技术支持与服务内容 106](#_Toc67944774)

[6.4.1. 现场安装、调试 106](#_Toc67944775)

[6.4.2. 质量保证期及保修服务 106](#_Toc67944776)

[6.4.3. 远程服务 109](#_Toc67944777)

# 对项目产品的理解

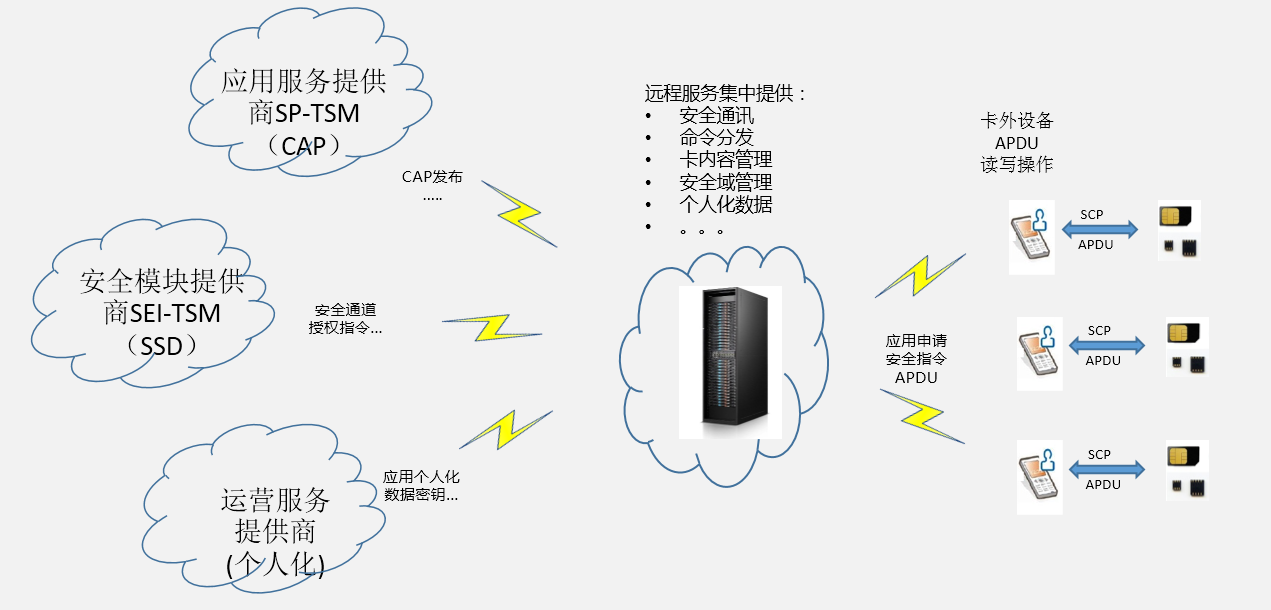
## 项目名称

交通银行股份有限公司TSM可信服务管理平台软件采购项目。

## 项目产品

TSM（Trusted Service Management）可信服务管理，主要因一卡多用及NFC近场通信服务而生，是基于“一卡多应用”技术建立的一套完整的“空中发卡”和应用管理体系。通过TSM平台，发卡机构可安全、高效地将各种安全应用集中在手机或IC卡上，既方便用户携带、使用，又便于自身发卡和管理。

数字货币硬钱包应用依赖于安全芯片SE，数字货币硬钱包应用本质是一种Java Applet的安全应用程序，需要适配多种SE载体（包括IC卡、SIM卡、智能手机、安全模块等），因此需要TSM平台进行远程应用管理，TSM平台在数字货币业务中起到前置平台的作用。



TSM是卡应用业务发展的关键环节，是联系运营机构、账户管理机构、发行机构、应用发行机构以及最终用户的桥梁。

## 项目产品设计原则

### 整体性原则

交通银行股份有限公司TSM可信服务管理平台从建设目标、建设内容到技术架构和实施过程等各个方面，都必须从一个整体的角度去考虑，而不能是孤立的TSM平台。本投标方案在设计过程中至始至终都秉承该原则，将TSM的功能设计内容从一个整体的角度去考虑和分析。这样能够提升业务应用平台工程整体的稳定性，降低业务应用生态集成成果对最终用户的影响。

### 继承性原则

我司在此之前参加了中国人民银行数字人民币硬钱包TSM 系统实施，以及与中国银行、中国电信等相关数币业务的项目产品研发工作。这些信息化工程的建设为在金融领域可信服务管理方面的应用积累了丰富的经验，交通银行股份有限公司TSM可信服务管理平台将继承合理利用以上产品技术的成果，确保TSM可信服务管理平台在交通银行股份有限公司相关业务应用领域发挥更加成熟稳定的系统作用。

### 实用性原则

系统的开发要“以人为本”，充分考虑用户及金融卡各项业务的实际需要，贴近用户的需求与习惯做法，做到功能强大、界面友好和美观、操作简单、使用方便。充分实现信息资源的共享，减少工作人员的工作量（如文字录入工作量），实现各项数据业务的计算机协同工作环境，使平台及应用系统能方便地获得所需的信息。

### 平台化和组件化原则

平台及应用软件设计遵循平台化、组件化设计的原则，以实现三个统一。既坚持面向数据（以数据为核心）、业务（以业务为基础）、面向用户（以人为本的应用），采用平台化、组件化的设计思想，实现统一的数据交换、统一的接口标准、统一的安全保障。

### 先进性和成熟性原则

系统建设要尽能采用最先进的技术、方法、软件、硬件和网络平台，确保系统的先进性，同时兼顾成熟性，使系统成熟与可靠。系统在满足全局性与整体性要求的同时，能够适应未来技术发展和需求的变化，使系统能够可持续发展。

### 标准化和开放性原则

系统的建设要严格按照国家、地方和行业的有关标准与规范，如空间数据分层与编码标准、数据质量与元数据标准、物标显示标准等，并适当考虑与国际接轨。在没有标准与规范的情况下，要参照国家、地方和行业的相关标准与规范，制订相应的标准与规范。系统的分析、设计、实现和测试要严格按照软件工程标准和规范，并尽可能采用开放技术和国际主流产品，以确保系统符合国际上各种开放标准。

### 可维护性和扩展性原则

为了确保系统的可持续发展，系统应具有较强的可维护性和扩展性。当机构调整、人事变动、业务内容与流程变更时，能方便地进行系统流程和功能的调整，以适应系统需求变化；系统能够方便地进行管理与维护，软、硬件的升级不影响正常运作，系统功能、结构以及数据库可方便地扩展；在系统设计时还要充分考虑未来的扩充；当增加新的业务功能需求时，系统要能够灵活扩展新的应用，而不需改变原有技术架构和系统结构。

### 安全性和保密性原则

保证网络环境下数据的安全，防止病毒入侵、非法访问、恶意更改毁坏，采取完备的数据保护和备份机制。为了防止非授权用户的非法入侵和授权用户的越权使用，系统进行岗位化界面设计，从客观上保障工作人员“自司其职”，系统分级分层授权，数据分级分层管理，防止了执行超越权限操作的现象发生。以保证业务信息安全和保密。系统应进行各种级别的权限控制，并具备审核功能，自动记录用户访问的情况和操作过程，以备日后查询。

充分考虑在网络、操作系统、数据库、应用等方面的安全性合理的日志和规章制度。

### 高性能和稳定性原则

在系统设计、开发和应用时，应从系统结构、技术措施、软硬件平台、技术服务和维护响应能力等方面综合考虑，确保系统较高的性能，如在网络环境下对空间图形的多用户并发操作要具有较高的稳定性和响应速度，综合考虑确保系统应用中最低的故障率，确保系统的良好运行。

先进性、科学性、经济性相结合

系统的运行平台和开发平台都采用目前先进成熟的技术实现，系统开发时兼顾到将来的应用扩展，以保持系统的先进性。在构建系统的过程中，全面采用各种新技术，采用国际先进的互联网技术，采用国际先进的网络技术模式，采用国际先进的技术路线，采用国际先进的多层结构体系，采用先进的部件/中间件、XML、WebService、WebGIS（网络地理信息系统）等先进技术，采用基于功能部件开发组织技术等先进技术对系统进行分析和设计。

系统的设计开发在保证其科学性和先进性的同时，合理计划使用系统开发经费，充分利用现有的软硬件资源，做到物尽其用。分步骤分阶段开发时，应当优先开发能迅速产生社会效益和经济效益的系统模块，使之及早投入使用。

## 缩略语和术语

### 缩略语

以下缩略语适用于本规范

|  |  |  |
| --- | --- | --- |
| **缩略语** | **英文** | **中文** |
| AID | Application Identifier | 应用标识符 |
| APDU | Application Protocol Data Unit | 应用协议数据单元 |
| BIP | Bearer Independent Protocol | 独立承载协议 |
| BSS | Business Support System | 业务支撑系统 |
| CAP | Card Application Package | 卡片应用安装包 |
| CAT\_TP | Card Application Toolkit\_Transport Protocol | 卡片应用工具包\_传输协议 |
| CLA | Class byte of the command message | 命令消息的类字节 |
| CRM | Customer Relationship Management | 用户关系管理 |
| IMSI | International Mobile Subscriber Identity | 国际移动用户标识 |
| INS | Instruction byte of the command message | 命令消息的说明字节 |
| ISD | Issuer Security Domain | 主安全域 |
| JSMDP | Java Card Service Manager & Download Platform | Java卡综合业务管理与下载平台 |
| MAC | Message Authentication Code | 消息校验码 |
| P1 | Reference control parameter 1 | 参考控制变量1 |
| P2 | Reference control parameter 2 | 参考控制变量2 |
| PRM | Partner Relationship Management | 合作伙伴关系管理 |
| RID | Registered Application Provider Identifier | 已注册应用商标识 |
| SCP | Secure Channel Protocol | 安全信道协议 |
| SMG | Short Message Gateway | 联通在信网关 |
| SP | Service Provider | 服务提供商 |
| SPSMG | Service Provider Short Message Gateway | 联通在信集中接入网关 |
| SSD | Supplementary Security Domain | 附属安全域 |
| SW | Status Word | 状态字 |
| TAR | Toolkit Application Reference | Toolkit应用标识 |
| TLV | Tag Length Value | TLV结构 |
| UICC | Universal Integrated Circuits Card | 通用集成芯卡片 |
| USAT | (U)SIM Application Toolkit | (U)SIM应用工具框架 |
| (U)SIM | Universal Subscriber Identity Module | （通用）用户标识模块 |
| VAC | Value-added ServiceAuthenticationCenter | 增值业务鉴权中心 |
| PoR |  |  |
| OTA-SMS |  |  |
| OTA-BIP |  |  |
| POS | point of sale | 销售终端 |

### 术语定义

以下术语适用于本规范：

• 业务：业务是指根据用户需求，利用自身或第三方资源向用户提供的具有市场价值的服务内容。在管理上，业务是服务提供商与运营商进行审核管理和分成结算的对象。本规范特指Java卡类业务。

• 业务能力：指基础增值服务，例如：邮件、消息、浏览、流媒体等，可以使用这些业务能力进行组合，构造出特定的业务，满足细分市场后的用户需求。本规范特指Java卡业务。

• 业务引擎：指实现各个业务能力的物理实体，本规范特指Java卡综合业务管理与下载平台，即：JSMDP。

• 产品：产品是指运用营销手段，是用户购买业务的方式，将业务或业务组合附加上销售对象、销售地域、资费计划、销售渠道、服务水平及配套资源六个方面属性后的产物，是向用户最终交付的、用户可以购买的业务或业务组合实例。

• 合作伙伴：广义的合作伙伴是指和银行存在伙伴关系的实体。这里主要是指对SP/CP、SI以及各种服务类合作伙伴的统称。

• Toolkit应用：特殊的应用，此类应用可以与终端交互，指示终端执行主动式命令。

• Applet类：由Java语言编写的Java类，此Java类经转换并下载到卡上后，可以由此类安装卡上应用。

• CAP包：由Java语言编写并经转化的含有1个或多个Java类的Java包。

• 类库：不含有Applet类的CAP包。

• 安装包：含有Applet类的CAP包，也称为：非类库。

• 上行请求：由移动用户在手机终端上或各种门户上发起的业务使用请求。

• 主动式命令：由卡上应用主动发送到终端，由终端执行的命令。

• 主动PUSH：由平台主动发起的向用户提供服务的业务使用请求。

• 应用实例：应用版本所对应的Applet实例。

• 包AID：等同Package AID。

• 实例AID：等同Instance AID。

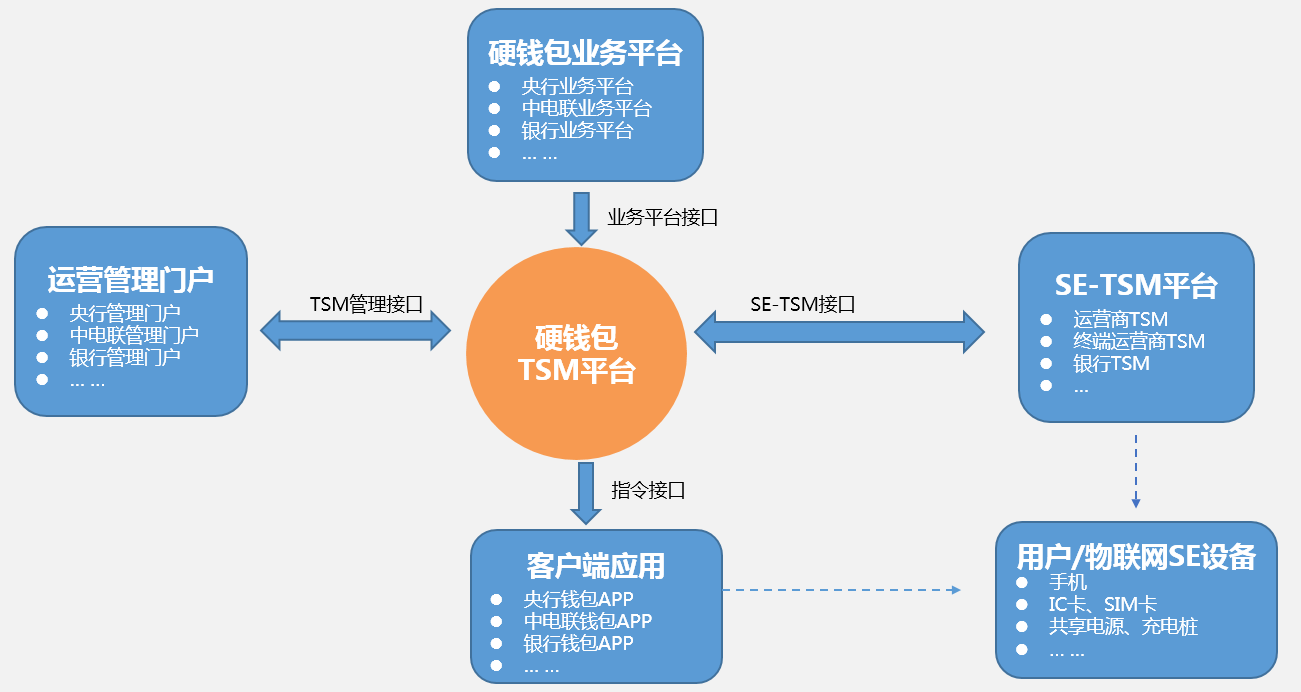
# 产品总体设计

TSM可信服务平台提供针对数币硬钱包的账户开立、个人化数据下发、远程管理、安全分发、密钥管理等支撑性服务平台。平台符合央行数字人民币标准规范，针对金融机构的硬钱包开立、钱包证书个人化、激活等进行安全保障分发支持。

## 系统应用架构

为满足DCEP项目中业务平台、SE平台及客户端三方的需求，需要一个可信服务管理平台(Trusted Service Manager)，以下简称TSM，来提供应用发行管理和安全模块管理等服务。

硬钱包TSM平台主要负责与三方（业务平台、SEI-TSM平台、客户端）接口的互通，实现SE管理、安全域管理、应用管理及应用个人化管理、平台管理、密钥管理、接入管理。



TSM 系统：银行机构可作为一个可信的第三方实体，被整个数字货币生态系统中的其他参与者所信任，将不同的安全载体发行方和不同的应用提供方连接在一起，主要提供用户管理、安全载体管理、辅助安全域管理、应用发现、应用开通、应用下载、应用个人化及应用生命周期管理等功能。

安全载体发行方：负责发展数字货币用户并承担安全载体成本的机构。

应用提供方：提供安全载体应用或服务给最终用户的实体。

芯片应用客户端：与TSM 系统和用户交互，实现安全载体管理、应用的发现、下载、个人化及管理的客户端程序。

安全载体：由银行、通信运营商或其它行业机构发行，可以以某种形态安放于手机内，

安全存放应用和数据的硬件单元。

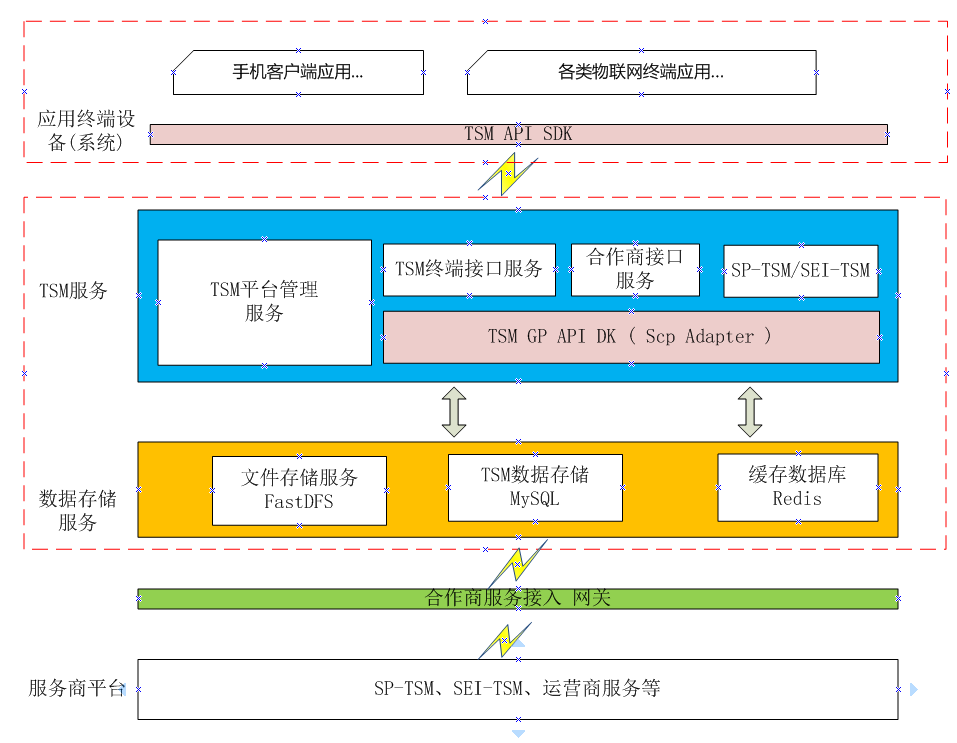
安全载体制造商：按照安全载体发行方的要求生产安全载体的厂商，所生产的安全载体内

预置安全载体发行方要求的安全域和应用。

## 系统技术架构

系统结构

TSM服务平台由平台存储服务、管理服务、GP指令包、平台对外接口服务等组成，如下图



* 数据存储服务：

支持分布式文件存储、和平台管理数据存储，同时为平台接口服务提供主流缓存数据库存储模式；

* TSM平台管理服务

TSM管理服务包括平台系统后台维护管理、安全域、应用发布包配置管理，以及服务接入认证管理等

* GP指令包

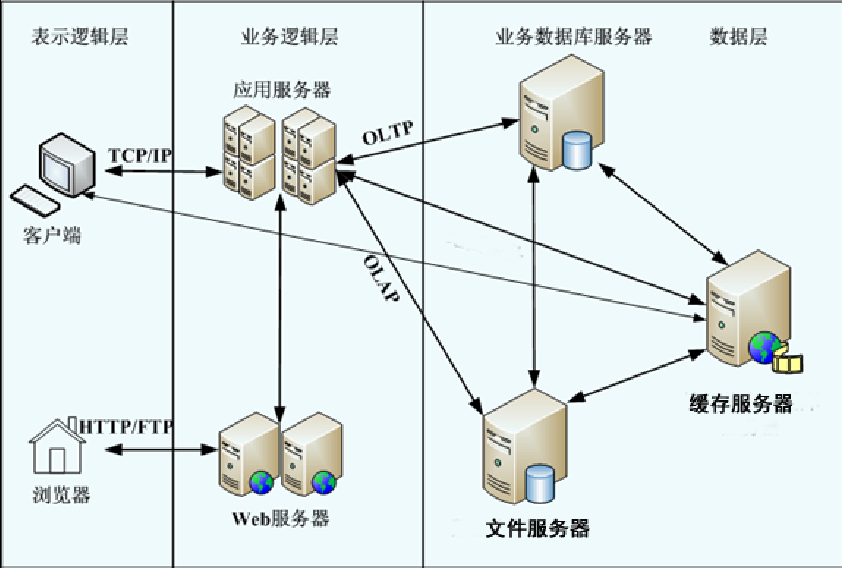
按照GP规范，根据服务请求参数和平台相关配置参数生成相关GP指令及指令分发；。

* 平台对外接口服务

根据实际应用场景需求，TSM平台提供与运营服务商、应用服务商，以及SP、SEI等外部TSM系统对接服务；

逻辑结构

为了实现系统具有业务变化的适应性、高度的安全性、大容量数据存储处理等技术特点，在系统的技术框架中采用三层或多层体系架构，可根据未来业务发展引入数据仓库技术。系统把业务逻辑、表示逻辑和数据资源分为三个不同的处理层次：



多层体系架构示意图

表示逻辑（客户层）为第一层：它的主要功能是实现用户交互和数据表示，为以后的处理收集数据，向第二层的业务逻辑请求调用核心服务处理，并显示处理结果；

业务逻辑（应用服务器组件）为第二层：实现核心业务逻辑服务，管理并接受客户的服务请求，向资源管理器提交数据操作请求，并将处理结果返回请求者——即客户或其他服务器。

数据资源（资源管理器）为第三层：包括数据库和各种文件（如多媒体文件），负责管理应用系统的数据资源，完成数据操作。应用服务器组件在完成服务的过程中通过资源管理器存取它管理的数据，或者请求资源管理器的数据服务。

基于SOA的思想，系统的应用架构分为三个大的层次架构，内容展现与Web应用界面层、核心应用层、系统与基础服务层；整个应用系统设计、开发和部署基于统一的开发环境。

最终应用层的展现方式分为两种，一种是浏览器（Browser），主要用于管理和监控类的业务系统；另一种是客户端程序，如移动终端等。

## 高可用部署方案

TSM平台根据实际应用规模和维护管理方式，可以选择**单点运行部署，分布式集群部署，Cloud云部署**；

### 单点部署

针对小规模应用，平台满足单台高性能服务器单机部署模式。即：Nginx+Redis+MySQL服务平台模式。适应快速实施，接入服务。

### 高可用分布式集成部署

双层高可用架构进行集成部署。系统架构示意如下图所示。其中：

* 网络层：

部署1台负载均衡设备，用于接收用户的HTTP访问请求。该设备由系统运维方提供。

* 业务层：分为核心业务域和数据存储域

**应用服务域**

部署3台应用服务器，采用集群方案。每台服务中将分别部署以下服务：

Nginx服务器。

TSM平台Web门户网站。

TSM平台后台系统服务。

TSM平台APP接口服务。

**数据存储域：**

部署2台数据服务器，采用主备方案。每台服务器中将分别部署以下服务：

Keepalive中间件。

Mysql数据库服务。

NFS网络文件服务。

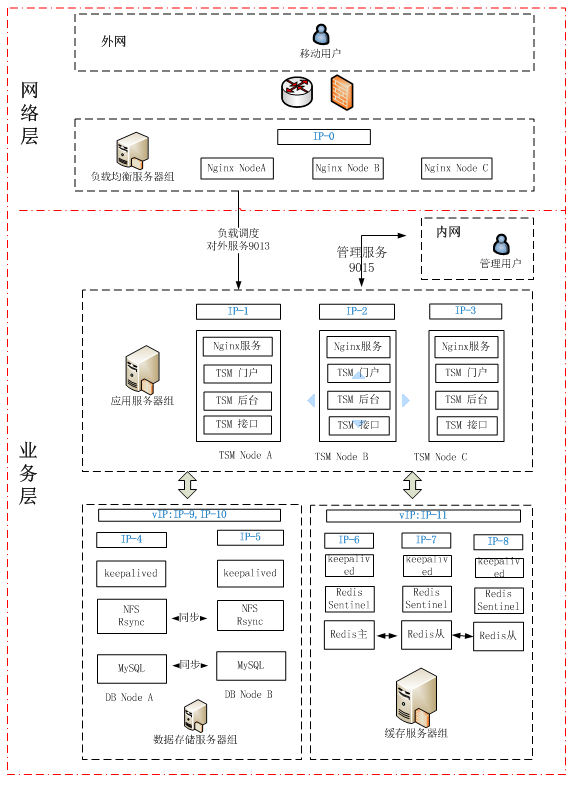
Rsync服务。

用于提供数据库和网络文件共享服务。该域内服务器该服务器仅与应用服务器进行内网通信。

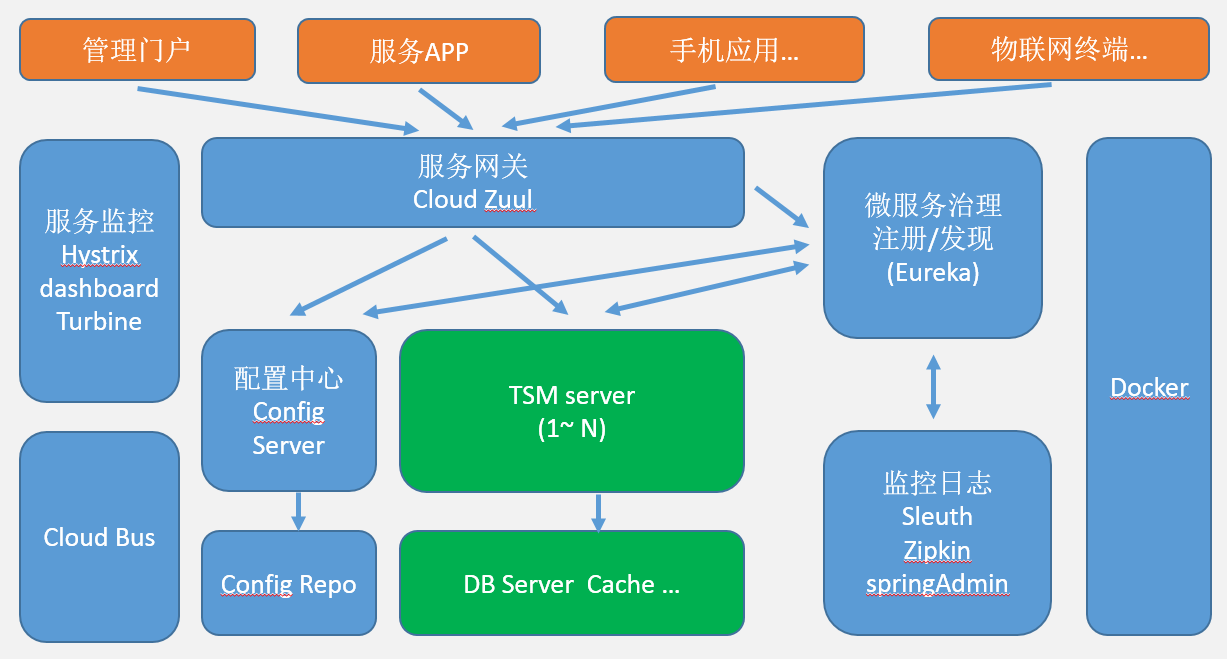
数据缓存域：部署3台数据缓存服务器，采用主备方案。每台服务中将分别部署以下服务：

Redis缓存服务器。用于提供数据缓存服务服务。

Keepalived中间件，该域内服务器该服务器仅与应用服务器进行内网通信。



### 微服务云与容器虚拟化架构

 支持SpringCloud微服务架构发布与Docker容器虚拟化部署。满足弹性扩容与高可用部署。

Spring Cloud是一系列框架的[有序集合](https://baike.baidu.com/item/%E6%9C%89%E5%BA%8F%E9%9B%86%E5%90%88/994839)。利用Spring Boot的开发便利性巧妙地简化了分布式系统基础设施的开发，包括服务发现注册、配置中心、消息总线、负载均衡、断路器、数据监控等，都可以用Spring Boot的开发风格做到一键启动和部署。

## 系统安全等级保护

信息系统安全等级保护技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确的配置其安全功能来实现，TSM系统按照等级保护三级要求进行规划设计。

基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面考虑。TSM软件系统主要措施如下：

### 网络安全

* 访问控制

部署边界防火墙。通过仔细配置防火墙完成边界访问控制；TCP访问明确私有端口，以防恶意攻击；根据基本要求对隔离设备以及网络设备等制定相应的ACL策略。包括：访问控制粒度、用户数量等。

根据要求在配置防火墙等隔离设备的策略时要满足相应要求，包括：端口级的控制粒度；常见应用层协议命令过滤；会话控制；流量控制；连接数控制；防地址欺骗等。

* 安全审计

在业务服务器区交换机旁路部署网络审计系统（数据库），在互联网边界旁路部署网络审计系统（互联网），记录用户网络行为、网络设备运行状况、网络流量等，审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

审计功能具备报表生成功能，同时采用日志服务器进行审计记录的保存，避免非正常删除、修改或覆盖。

* 结构安全

根据高峰业务流量，关键设备选择高端设备，核心交换设备和接入设备带宽能够支撑业务高峰的数据量，核心交换、重要系统应用服务器均已采用冗余设备部署；

绘制了详细网络拓扑图，并根据业务、部门、信息系统类别等合理划分了安全域。

主要网络设备的处理能力以及各部分带宽均需满足业务高峰需要；

合理规划路由及VLAN，在业务终端与业务服务器之间建立安全路径；在系统内、外通过防火墙进行有效隔离，保证重要网段与其他网段之间进行可靠的隔离；

网络设备规划带宽优先级，保证在网络发生拥堵的时候优先保护重要主机。

* 恶意代码防范

互联网边界部署AV防病毒网关，进行网关级的恶意代码的检测与清除，并定期升级恶意代码库。

* 网络设备防护

根据基本要求配置网络设备自身的身份鉴别与权限控制；包括：登陆地址、标识符、口令的复杂度（3种以上字符、长度不少于8位）、失败处理，传输加密等方面。对网络设备进行安全加固。对设备的管理员等特权用户进行不同权限等级的配置，实现权限分离。

### 主机安全

* 身份鉴别

根据基本要求配置用户名/口令；采用3种以上字符、长度不少于8位的口令；启用登陆失败处理、传输加密等措施；保证用户名的唯一性。建立PKI/CA体系，对主机管理员登录时进行身份鉴别。

* 访问控制

根据基本要求进行主机访问控制的配置，包括：功能启用、特权用户权限分离、默认账号和口令的修改，无用账号的清除等；

通过安全加固措施制定严格用户权限策略，保证账号、口令等符合安全策略；

对管理员进行分级权限控制，并根据最小权限原则仅授予管理用户所需的最小权限。

对重要服务器上的信息（文件、数据库等）进行标记，并设定访问控制策略进行访问控制，实现强制访问控制。

* 安全审计

部署内网安全管理系统，利用审计功能进行文件操作审计、外挂设备操作审计、非法外联审计、IP地址更改审计、服务与进程审计等；

根据基本要求记录用户行为，资源状况等，审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果，并保护好审计结果。

审计范围包括重要客户端；同时能够生成审计报表。

* 剩余信息防护

通过对操作系统及数据库系统进行安全加固配置，及时清除剩余信息的存储空间。

* 恶意代码防护

部署终端防病毒软件，及时进行升级更新；进行漏洞扫描，及时进行系统补丁更新。由升级服务器进行病毒软件和病毒库升级；对升级包进行杀毒检查，采用光盘等不可修改介质进行传递，在测试机上测试没问题后，再发放给终端进行升级。

### 应用安全

* 身份鉴别

根据基本要求配置用户名/口令；设计专用软件模块进行身份鉴别；

采用3种以上字符、长度不少于8位的口令；设计登陆失败处理措施，采取结束会话、限制非法登录次数和自动退出等措施；保证系统用户名的唯一性。

进行PKI体系建设，采用CA证书方式进行身份鉴别。

* 访问控制

根据基本要求进行访问控制的配置，包括：权限定义、默认账号的权限管理、控制粒度的确定等；

通过安全加固措施制定严格用户权限策略，保证账号、口令等符合安全策略；

通过防火墙制定符合基本要求的ACL策略。

根据系统重要资源的标记以及定义的安全策略进行严格的访问控制。

* 安全审计

应用系统开发应用审计功能，根据基本要求记录系统重要安全事件的日期、时间、发起者信息、类型、描述和结果等，并保护好审计结果。部署数据库审计系统对用户行为、用户事件及系统状态加以审计，从而把握数据库系统的整体安全。对审计记录数据进行统计、查询、分析及生成审计报表。

* 通信完整性

应用系统开发数据完整性校验功能，采用消息摘要机制确保完整性校验；

采用PKI体系中的完整性校验功能进行完整性检查，保障通信完整性。

* 通信保密性

采用PKI体系的加密功能保障通信保密性。

* 软件容错

进行代码审核，对输入数据进行检查，保证符合规定；应用系统需进行自动保护功能设计，故障后可以恢复。

### 数据安全与备份恢复

* 数据完整性

应用系统采用MD5等数据校验技术对数据进行完整性检查；数据受到破坏后通过备份策略进行数据恢复；配置存储系统对系统管理数据、鉴别信息和重要业务数据存储过程中的完整性进行检测与恢复

* 数据保密性

在系统内部传输管理数据、鉴别信息和重要业务数据，不涉及外部传输，暂无需加密

* 备份与恢复

根据基本要求对重要数据进行定期备份；进行每天数据备份且介质存放与场外；主要安全域均采用双机冗余部署，保证系统的高可用性。

## 产品技术路线

### J2EE技术体系

为新建系统的可移植性、独立性、安全性提供了保障，并且提供了并发的机制，具有很高的性能；其次，它最大限度地利用了网络、具有安全性、机动性、可伸缩性和跨平台性。

TSM系统所采用的J2EE技术构架的选择非常重要。一般来说，构建大型应用系统需要具备以下特征：

（1）支持多层构架，表示层、业务层、数据库访问层分开；

（2）独立于特定的硬件平台和操作系统；

（3）支持各种类型的数据库系统；

（4）良好的安全性；

（5）分布式事务功能；

（6）支持消息服务；

（7）支持组件化开发；

（8）支持集群和失效转移，提供良好的可扩展性和容错性；

（9）支持XML技术；

（10）支持Web Service和EAI；

（11）具有良好的可扩展性。

J2EE是由Sun公司领导，各厂商共同制定并得到广泛认可的工业标准，是帮助企业和一个组织方便地实现具有更强的伸缩性、开放性、安全性的网络应用的最具影响力的技术构架。J2EE支持基于组件的应用系统开发，基于J2EE的Web应用服务器是应用最广的、最有应用前景的中间件软件平台。

J2EE提供了一个企业级的计算模型和运行环境以用于开发和部署多层体系结构的应用。它通过提供企业计算环境所必需的各种服务，使得部署在J2EE平台上的多层应用可以实现高可用性、安全性、可扩展性和可靠性。它的优越性在于：计算平台支持Java语言，使得基于J2EE标准开发的应用可以跨平台地移植；Java语言非常安全、严格，这使开发者可以编写出非常可靠的代码；J2EE提供了企业计算中需要的所有服务，且更加易用；J2EE中多数标准定义了接口，例如JNDI、JDBC、Java Mail等，因此可以和许多厂商的产品配合，容易得到广泛的支持；J2EE树立了一个广泛而通用的标准，大大简化了应用开发和移植过程。

J2EE是主流的技术体系，J2EE已成为一个工业标准，围绕着J2EE有众多的厂家和产品，其中不乏优秀的软件产品，合理集成以J2EE为标准的软件产品构建大型应用服务平台，可以得到较好的稳定性、高可靠性和扩展性。

J2EE架构示意图

J2EE技术的基础是JAVA语言，JAVA语言的与平台无关性，保证了基于J2EE平台开发的应用系统和支撑环境可以跨平台运行。

基于J2EE技术的应用服务器（Application Server）主要是用来支持开发基于Web的三层体系结构应用的支撑平台。

### 微服务架构

微服务架构是一项在云中部署应用和服务的新技术。大部分围绕微服务的争论都集中在容器或其他技术是否能很好的实施微服务，而红帽说API应该是重点。

微服务可以在“自己的程序”中运行，并通过“轻量级设备与HTTP型API进行沟通”。关键在于该服务可以在自己的程序中运行。通过这一点我们就可以将服务公开与微服务架构（在现有系统中分布一个API）区分开来。在服务公开中，许多服务都可以被内部独立进程所限制。如果其中任何一个服务需要增加某种功能，那么就必须缩小进程范围。在微服务架构中，只需要在特定的某种服务中增加所需功能，而不影响整体进程的架构。

TSM 平台采用Springboot及SpringCloud服务框架设计；满足多种分布式高可用服务及微服务部署；

* 满足高内聚低耦合的设计原则。

服务解耦将原有的巨大的单体应用拆分为多个独立的微服务，使得每个服务模块更专注于独自的业务处理。

* 服务之间彼此隔离

通过轻量级的通讯机制进行交互，使得开发时无需关注具体的开发环境，只需要协商好通讯机制即可。

* 支持根据不同的应用需求规划部署环境

对于访问量大的服务可以增加服务的部署数量，访问量小的服务适当的减少部署数量。

* 支持更高的扩展性能

服务之间的耦合性降低，无论从功能上，还是架构上，我们都可以进行更为灵活的扩展，而不影响其他服务。

### WS服务接口技术

Web Service可以执行从简单的请求到复杂业务处理的任何功能。系统一旦部署以后，其他Web Service应用程序可以发现并调用它部署的服务；Web services要使用两种技术： XML和SOAP，XML提供在web上传送结构化数据的方式，Web services以一种可靠的自动的方式操作数据，XML可以使web services十分方便的处理数据，它可以使内容与表示方式进行分离； SOAP使用XML消息调用远程方法，这样web services可以通过HTTP协议的post和get方法与远程机器交互。通过web services可实现了综合应用系统与其他系统的互联互通。

### 基于UML的模型设计

基于UML的设计应用中，面向对象软件开发一般都采用迭代增量式的开发过程，这种方法不是在项目结束时一次性提交软件，而是分块逐次开发和提交。每一次迭代都包含了软件生命周期的所有阶段，即：分析、设计、实现和测试阶段。

面向对象的迭代式软件开发方法可以尽早发现项目的风险，并在软件开发过程中对这些风险进行有效的控制，从而保证达到项目的工程实施保证。

标准建模语言UML由五类图来描述应用系统的业务实现过程，即：

用例图，从用户角度描述系统功能,并指出各功能的操作者。

静态图(Static diagram)，包括类图、对象图和包图。类图描述系统中类的静态结构。

行为图(Behavior diagram)，描述系统的动态模型和组成对象间的交互关系，状态图描述类的对象所有可能的状态以及事件发生时状态的转移条件，对类的补充。

交互图(Interactive diagram)，描述对象间的交互关系顺序图显示对象之间的动态合作关系,它强调对象之间消息发送的顺序,同时显示对象之间的交互；合作图描述对象间的协作关系,合作图跟顺序图相似,显示对象间的动态合作关系。

实现图( Implementation diagram )，构件图描述代码部件的物理结构及各部件之间的依赖关系。

通过这些框图实现了系统设计的可视化建模，将模型中的信息用标准图形元素直观地显示，形成构建系统的蓝图，便于系统的维护和修改。主要目的：

用户可以直观地了解用户与系统之间的交互；

分析人员可以看到模型对象之间的交互；

开发人员可以了解开发的对象之间的任务；

测试人员可以看到对象之间的交互和编制测试方案；

项目管理人员可以看到整个系统及各部分的交互；

通过使用一个共同的图形语言，改进跨团队的沟通。

### PKI/CA安全开发技术

充分利用PKI/CA安全体系提供的安全保障，通过用户身份认证、信息的保密性、完整性和不可抵赖性，实现对应急指挥数据的安全访问，实现信息的传输、存储和访问的安全性。

PKI 就是 Public Key Infrastructure 的缩写，翻译过来就是公开密钥基础设施。它是利用公开密钥技术所构建的，解决网络安全问题的，普遍适用的一种基础设施。PKI通过延伸到用户本地的接口，为各种应用提供安全的服务，如认证、身份识别、数字签名、加密等。有了 PKI，安全应用程序的开发者不用再关心那些复杂的数学运算和模型，而直接按照标准使用一种接口。用户也不用关心如何进行对方的身份鉴别而可以直接使用标准的接口。

PKI 中最基本的元素就是数字证书。所有安全的操作主要通过证书来实现。 PKI 的硬设备还包括签置这些证书的证书机构(CA)，登记和批准证书签置的登记机构(RA)，以及存储和发布这些证书的电子目录。PKI中还包括证书策略，证书路径以及证书的使用者。所有这些都是 PKI 的基本元素。许多这样的基本元素有机地结合在一起就构成了PKI。

在PKI体系 中，CA（Certificate Authority，认证中心）和数字证书是密不可分的两个部分。认证中心又叫CA中心，它是负责产生、分配并管理数字证书的可信赖的第三方权威机构。认证中心是PKI安全体系的核心环节，因此又称作PKI/CA。认证中心通常采用多层次的分级结构，上级认证中心负责签发和管理下级认证中心的证书，最下一 级的认证中心直接面向最终用户。

数字证书，又叫“数字身份证”、“数字ID”，是由认证中心发放并经认证中心数字签名的，包含公开密钥拥有者以及公开密钥相关信息的一种电子文件，可以用来证明数字证书持有者的真实身份。

数字证书采用公开密钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己 设定一把特定的、仅为本人所知的专有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，用于加密和验证签名。当发送一份保密 文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过使用数字证书，使用者可以得到如 下保证：信息除发送方和接收方外不被其它人窃取；信息在传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己的信息不能抵赖； 信息自数字签名后到收到为止，未曾作过任何修改，签发的文件是真实文件。

### GP技术规范

GlobalPlatform卡片架构由一系列组件构成，为卡上的应用和卡外管理系统之间提供了一套独立于硬件和厂商的接口。下面的图例展现了卡片架构的各个组件，该卡片上运行着若干来自发卡方的应用，若干来自应用提供方的应用，以及若干提供全局服务(如CVM服务)给其他应用的应用。

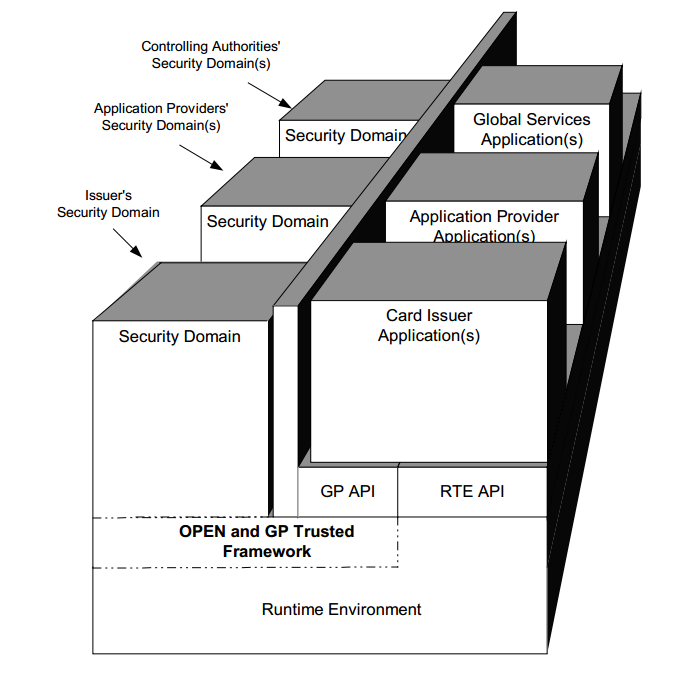
所有这些应用必须在一个安全的运行时环境中实现，该运行时环境提供了一套硬件中立的应用编程接口以支持应用的可移植性。 GlobalPlatform并不强制规定运行时环境的实现技术。卡片管理器作为GlobalPlatform架构中的首要组件起到了 GlobalPlatform卡片中心管理者的作用，特定的密钥和安全管理应用被称作安全域，负责确保发卡方和其他安全域提供者之间的密钥的完全隔离。

作为卡外授权机构的卡片内代表的安全域，依据现有的三种授权机构，可以划分为三种主流类型：

发卡方安全域（主安全域，ISD），卡片上首要的、强制性存在的安全域，是卡片管理者(通常是发卡方)在卡片内的代表；

补充安全域（辅助安全域，SSD），卡片上次要的、可选择地存在的安全域，是应用提供方或发卡方以及它们的代理方在卡片内的代表；

授权管理者安全域，一种特殊类型的补充安全域，授权管理者负责将某种安全策略贯彻到所有加载到卡片的应用代码上，授权管理者安全域就是授权管理者在卡片内的代表，卡片上可能存在多个这样的安全域。



GlobalPlatform架构意图运行在一个安全的多应用运行时环境之上。该运行时环境负责向所有应用提供一套硬件中立应用编程接口，一种能确保各个应用的代码和数据能相互区隔的、安全的存储和执行空间分配机制，并提供服务来完成卡片和卡外实体之间的通信。考虑到处理复位应答或请求应答时对通信协议、逻辑通道以及命令序列等方面的支持的差别， GlobalPlatform卡片应该尊循恰当的标准，包括ISO/IEC 7816-3, ISO/IEC 7816-4, ISO/IEC 14443-3 and ISO/IEC 14443-4。

## TSM平台性能指标

测试环境参照

|  |  |
| --- | --- |
| 资源 | 描述 |
| 操作系统 | Windows，Intel(R) Core(TM)i5-8500 CPU @ 3.00GHz 3.00GHz单CPU两核 |
| JDK | 1.8.0\_231 |
| 压测软件 | Jmeter5.2.1 |
| 性能监控工具 | ServerAgent、nmon、top |

性能指标参数：



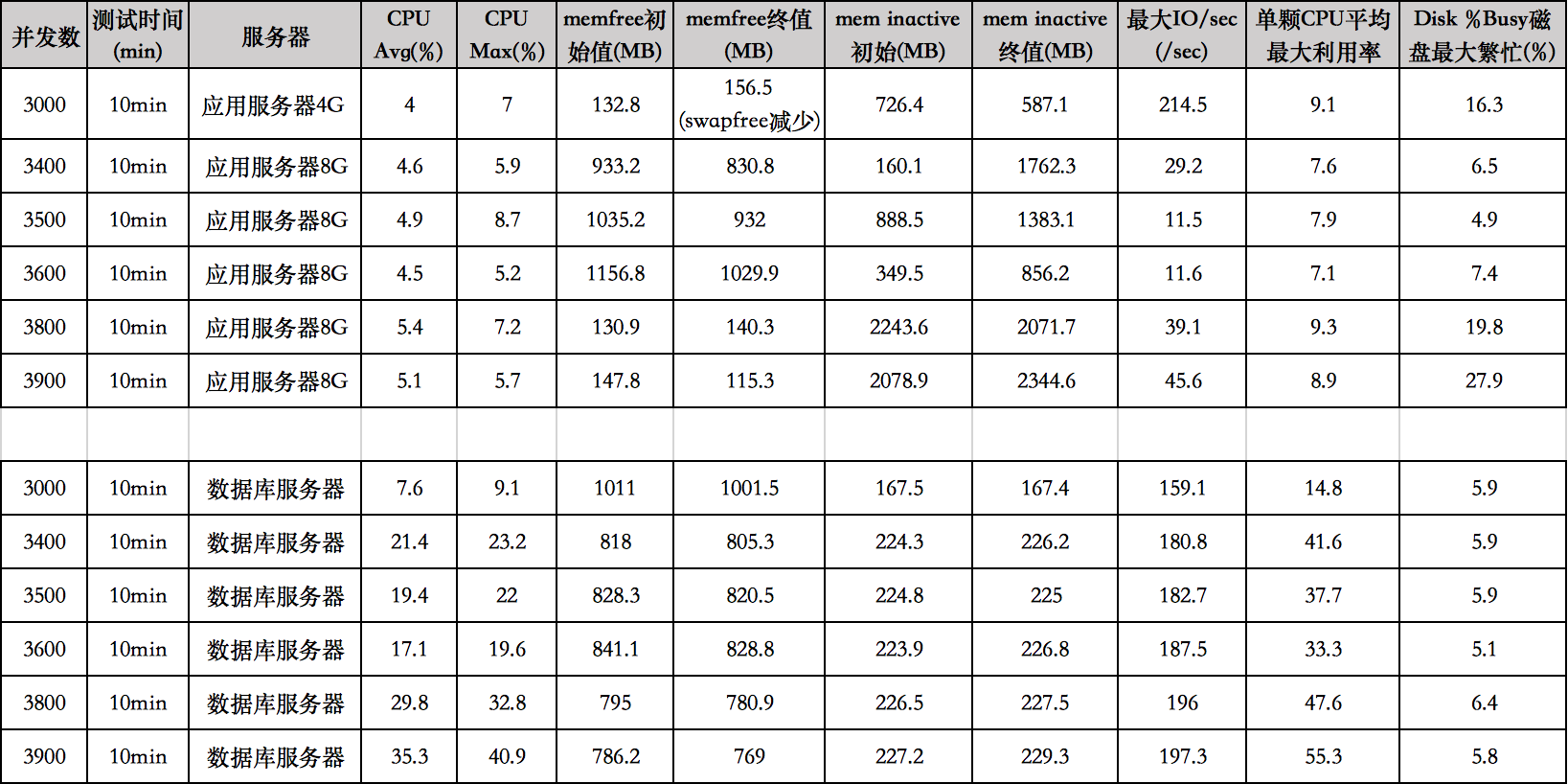
1.在服务器内存4G时，10分钟启动3000个用户进行应用申请和下载，应用申请的平均响应时间和95%响应时间在45ms以下，应用下载的平均响应时间和95%响应时间在5ms以下；

2.服务器内存8G时，10分钟启动3400个用户，应用申请的平均响应时间和95%响应时间在90ms以下，应用下载的平均响应时间和95%响应时间在5ms以下。

3.服务器内存8G时，10分钟分别启动3500、3600个用户进行应用申请和应用下载，应用申请的平均响应时间和95%响应时间都在100ms以下，应用下载的平均响应时间和95%响应时间在6ms以下；

4.服务器内存8G时，10分钟分别启动3800、3900个用户进行应用申请和应用下载，应用申请的平均响应时间在100ms以下，应用下载的平均响应时间在5ms以下。

服务器性能监控



测试应用服务器内存4G时10分钟3000用户进行应用申请和应用下载，测试应用服务器内存8G时10分钟内进行3400、3500、2600、3800、3900用户的应用申请和应用下载。

测试结果如下：

1. 测试10分钟3000个用户量（应用服务器内存4G）

A.应用服务器CPU平均利用率4%，最大利用率7%；测试过程中内存不足，使用到了swap；最大IO/sec采集值214.5；单颗CPU利用率最大9.1%；Disk %Busy磁盘最大繁忙16.3%；

B.数据库服务器CPU平均利用率7.6%，最大利用率9.1%；可用内存从1011M到1001.5M，减少10.5M；最大IO/sec采集值159.1；单颗CPU利用率最大14.8%；Disk %Busy磁盘最大繁忙5.9%；

1. 测试10分钟3400个用户量（应用服务器内存8G）

A.应用服务器CPU平均利用率4.6%，最大利用率5.9%；可用内存从933.2M到830.8M，减少102.4M；最大IO/sec采集值29.2；单颗CPU利用率最大7.6%；Disk %Busy磁盘最大繁忙6.5%；

B.数据库服务器CPU平均利用率21.4%，最大利用率23.2%；可用内存从818M到805.3M，减少12.7M；最大IO/sec采集值180.8；单颗CPU利用率最大41.6%；Disk %Busy磁盘最大繁忙5.9%；

1. 测试10分钟3500个用户量

A.应用服务器CPU平均利用率4.9%，最大利用率8.7%；可用内存从1035.2M到932M，减少102.8M；最大IO/sec采集值11.5；单颗CPU利用率最大7.9%；Disk %Busy磁盘最大繁忙4.9%；

B.数据库服务器CPU平均利用率19.4%，最大利用率22%；可用内存从828.3M到820.5M，减少7.8M；最大IO/sec采集值182.7；单颗CPU利用率最大37.7%；Disk %Busy磁盘最大繁忙5.9%；

4.测试10分钟3600个用户量

A.应用服务器CPU平均利用率4.5%，最大利用率5.2%；可用内存从1156.8M到1029.9M，减少126.9M；最大IO/sec采集值11.6；单颗CPU利用率最大7.1%；Disk %Busy磁盘最大繁忙7.4%；

B.数据库服务器CPU平均利用率11.7%，最大利用率19.6%；可用内存从841.1M到828.8M，减少12.3M；最大IO/sec采集值187.5；单颗CPU利用率最大33.3%；Disk %Busy磁盘最大繁忙5.1%；

5.测试10分钟3800个用户量

A.应用服务器CPU平均利用率5.4%，最大利用率7.2%；可用内存从130.9M到147.3M，内存平稳；最大IO/sec采集值39.1；单颗CPU利用率最大9.3%；Disk %Busy磁盘最大繁忙19.8%；

B.数据库服务器CPU平均利用率29.8%，最大利用率32.8%；可用内存从795M到780.9M，减少14.1M；最大IO/sec采集值196；单颗CPU利用率最大47.6%；Disk %Busy磁盘最大繁忙6.4%；

6.测试10分钟3900个用户量

A.应用服务器CPU平均利用率5.1%，最大利用率5.7%；可用内存从147.8M到115.3M，内存平稳；最大IO/sec采集值45.6；单颗CPU利用率最大8.9%；Disk %Busy磁盘最大繁忙27.9%；

B.数据库服务器CPU平均利用率35.3%，最大利用率40.9%；可用内存从786.2M到769M，减少7.2M；最大IO/sec采集值197.3；单颗CPU利用率最大55.3%；Disk %Busy磁盘最大繁忙5.8%；

# 产品功能方案

## 门户与个人中心

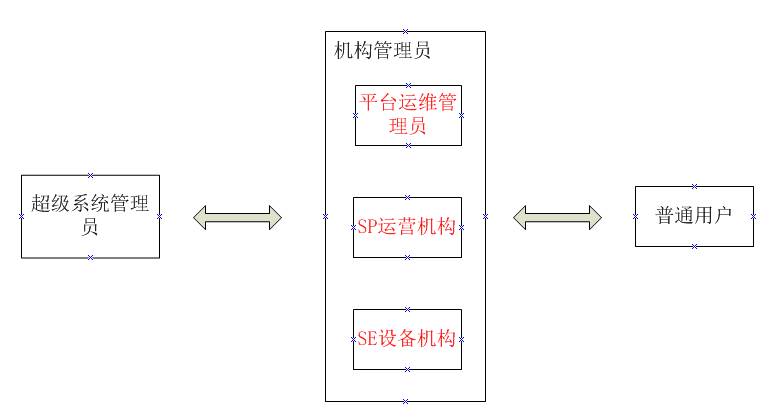
平台前端门户，包括管理员门户、普通用户门户功能菜单及操作。

平台的管理员门户提供给超级管理员、机构管理员使用。

针对不同角色系统分配相应权限与访问范围，如机构管理员只能进行部分权限的访问及管理，超级管理员可访问所有权限并进行授权管理。对于不同管理员的登录，系统可根据用户名和密码对管理员类型进行识别认证，并针对不同的角色提供相应的权限范围内的门户菜单。

普通用户门户提供给各运营机构的业务人员使用。针对不同角色，系统分配相应权限和访问范围，如央行用户只能访问央行上传的应用对应的数据。对于不同用户的登录，系统可根据注册时的角色选择进行识别认证，并针对不同的角色提供相应的权限范围内的门户菜单。

TSM系统后台管理主要面向系统管理用户和各机构管理用户，不同角色管理员面向的应用场景及权限各异，管理员用户权限如下：



### 用户登录

系统后台管理前端所有功能页要求必须登录后才能授权访问，长时不操作自动失效，系统退出显示重新登录。

登录输入：用户名，密码，图形验证码；

验证码时效时间1分钟，为系统随机生成，图形显示不清楚，点击图形重新生成。



用户密码前端页面进行加密传输；

### 忘记密码

系统通过预留邮箱或手机短信找回密码，认证激活成功后，系统将个人密码恢复初始设置，用户登录后自行更改。

### 个人中心

系统根据用户角色类型和权限，显示个人Home页信息，和个人信息功能服务，包括

展示用户个人基本信息

对于部分个人信息提供修改功能

提供密码修改服务

### 修改密码

修改密码功能为 个人信息服务功能，密码修改逻辑为：



说明：

1、 点击个人中心-密码修改，进入密码修改界面

2、 输入项：原密码、新密码、确认新密码；

3、 点击确认按钮，提示密码修改成功，页面跳转至登录页

### 个人信息

显示个人信息管理，包含以下内容：

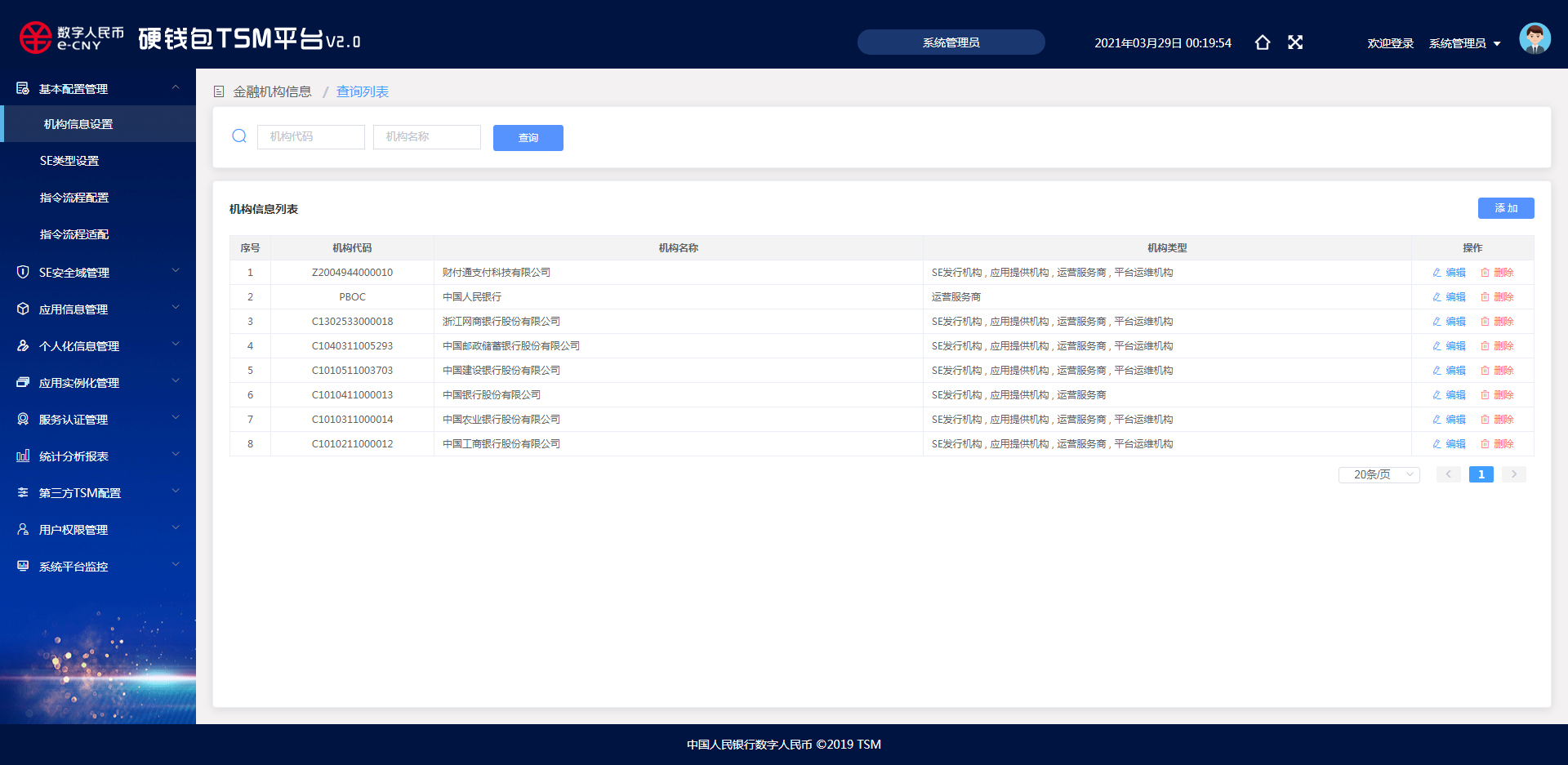


## 系统配置管理

### 平台机构设置

每个管理用户必须有机构属性，是系统角色权限设置的基础，系统设定，只有系统超级管理员和平台管理员可以预先设置机构信息。

机构主要信息内容：



主要操作：查询、新增、编辑、删除、列表内容；设置机构管理员等；

### SE厂商及类型设置

本模块可对SE类型进行维护，包括添加、编辑、删除。

SE厂商及类型信息按照三级级联管理；信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 参数名称 | 内容说明 | 必要性 | 备注 |
| 1 | 载体 | 1 SIM卡  2 手机  3 其他 | M | 管理员可编辑维护 |
| 2 | 厂商 | 厂商及对应字段：（示例）  1 华为：8011  2 小米：8015  3 三星：8016  4 …… | M | 管理员可编辑维护 |
| 3 | 型号 | 厂商下对应的型号 | O | 管理员可编辑维护 |



## TSM接口配置

### SE-TSM接口配置

与第三方SE-TSM平台对接接口配置。

配置信息：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 参数名称 | 内容说明 | 必要性 | 备注 |
| 1 | 接口代码 |  |  |  |
| 2 | 接口名称 |  |  |  |
| 3 | SE提供机构 |  |  |  |
| 4 | SE厂商 |  |  |  |
| 5 | SE介质类型 |  |  |  |
| 6 | SE型号 |  |  |  |
| 7 | SETSM接口地址 | SETSM接口地址URL | Y |  |
|  | 接口参数 | 接口参数 |  |  |
| 8 | 服务协议类型 | 接口服务类型 | Y | http |
| 9 | 数据协议格式 |  | Y | json |
| 10 | 数据协议结构 | 数据协议样本结构 |  |  |
| 11 | 参数映射关系 | 接口字段映射对应关系 |  |  |

### SP-TSM接口配置

与第三方SP-TSM平台对接接口配置。

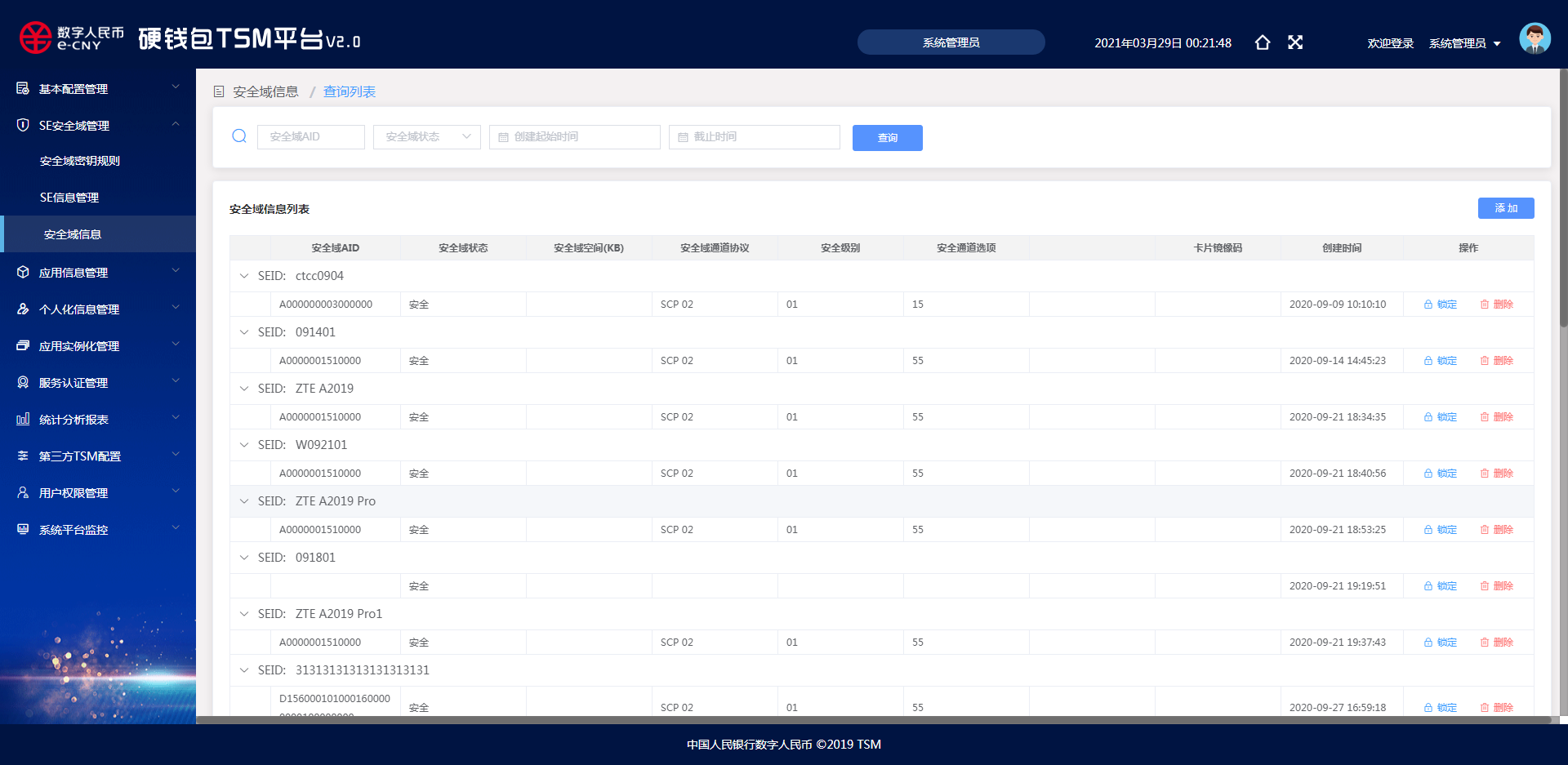
配置信息：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 参数名称 | 内容说明 | 必要性 | 备注 |
| 1 | 接口代码 |  |  |  |
| 2 | 接口名称 |  |  |  |
| 3 | SP提供机构 |  |  |  |
| 4 | 服务类型 | 服务类容类型 |  | 应用，个人化， |
| 5 | SPTSM接口地址 | SPTSM接口地址URL | Y |  |
| 6 | 接口参数 | 接口参数 |  |  |
| 6 | 服务协议类型 | 接口服务类型 | Y | http |
| 7 | 数据协议格式 |  | Y | json |
| 8 | 数据协议结构 | 数据协议样本结构 |  |  |
| 9 | 参数映射关系 | 接口字段映射对应关系 |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |

## SE/安全域信息管理

### SE信息管理

SE（Secure Element）指具备硬件保护机制的数据存储安全设备，通常以安全芯片、智能卡等形态体现。本功能模块可对SE信息管理，具体包括以下功能：添加（手动导入、接口获取）、维护（编辑、锁定、解锁、删除、查看）。



* SE状态管理

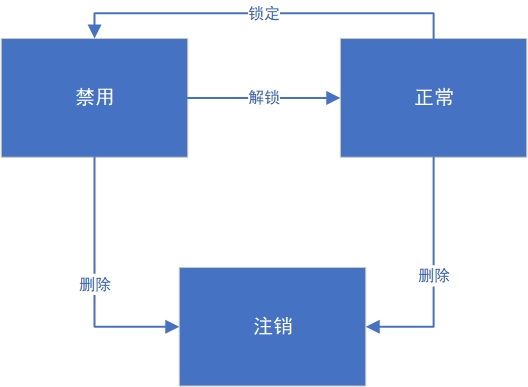


图9：SE状态迁移

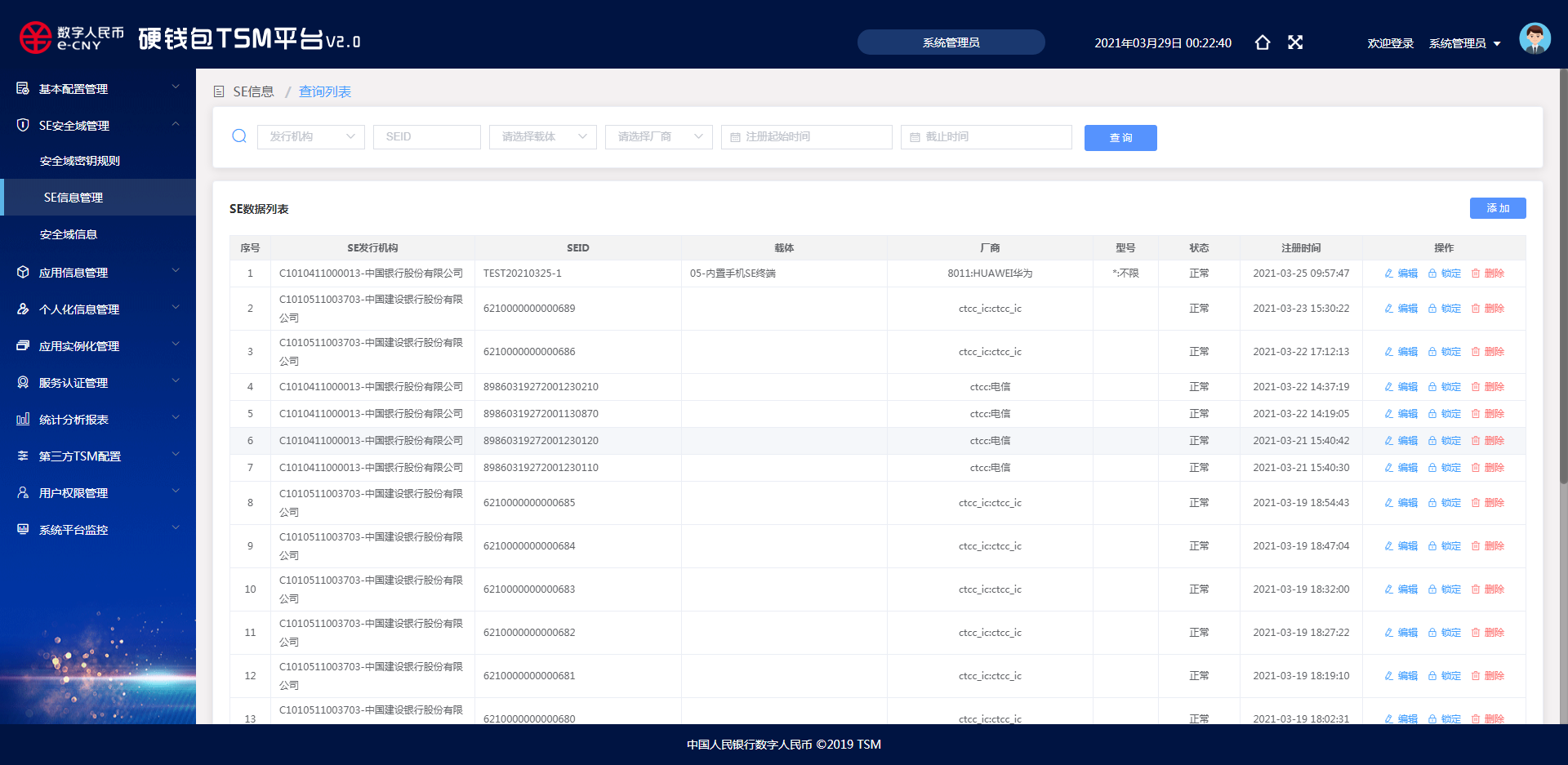
说明：

* SE添加后（通过手动或接口获取）为正常状态
* 正常状态的SE，管理员可进行锁定、删除，SE锁定后状态变为禁用，删除后状态变为注销
* 禁用的SE，管理员可进行解锁、删除，解锁后状态变为正常
* SE锁定后，其关联的安全域和应用也同步锁定变为禁用状态
* SE解锁后，因其锁定变为禁用状态的安全域和应用也同步解锁变为正常状态
* SE删除后，其关联的安全域和应用也同步删除变为注销状态

### 安全域信息管理

安全域代表了SE设备外各类角色在SE上的权力。本功能模块可对安全域信息管理，具体包括以下功能：添加（手动导入、接口获取）、维护（编辑、查看、锁定、解锁、删除）。注：安全域信息的添加、编辑操作在SE信息管理模块进行，在安全域信息管理列表页不再提供添加、编辑入口。

数据信息



### 安全域密钥配置管理

本功能模块根据 SE类型配置秘钥分散规则或秘钥来源方式。

AM模式下，安全域秘钥管理方案:预置秘钥模式，平台分散规则生成模式，加密机分散规则加密模式；

* 预置秘钥模式

根据指定的SE安全域类型预置三只密钥信息，缺点：秘钥保护差；

* 平台分散规则生成模式

根据分散因子、初始秘钥值，根据选择的分散规则计算三只密钥，缺点：秘钥保护较弱；

* 加密机分散规则加密模式

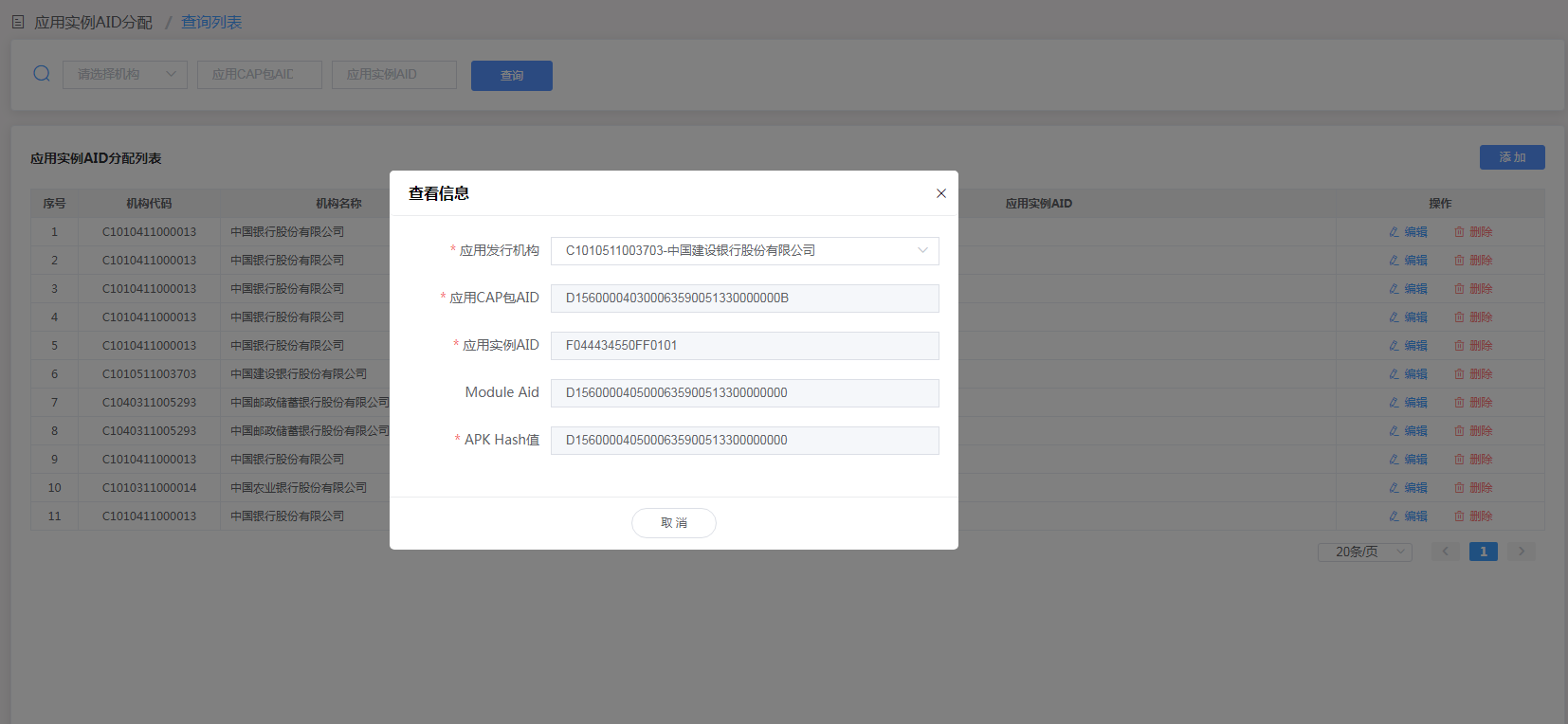
由平台提供分散因子，加密机密管系统，存储初始秘钥值、分散规则计算三只密钥；加密机根据密钥值计算将APDU原始指令进行加密，生成APDU安全指令，进行分发。

## 应用包信息管理

### 应用实例AID分配

应用实例AID参数统一配置管理。

数据信息：



### 应用信息管理

本功能模块可对应用信息管理，具体包括以下功能：添加、维护（编辑、锁定、解锁、删除、查看）

* 应用信息数据逻辑

应用服务机构 分别提供 各自应用版本及CAP文件。

* 应用数据信息应包括以下参数



* 应用包信息
* 应用状态迁移



图11：应用状态迁移

说明：

管理员上传应用不需要审核过程，添加应用提交，初始状态为审核通过

应用在审核中状态下，管理员可进行拒绝和通过操作，分别对应审核失败状态和审核通过状态；不允许用户对审核中状态的应用进行编辑、删除。

应用在审核失败状态下，管理员及用户可进行编辑、删除操作

应用在审核通过的状态下，管理员可以进行编辑、锁定、删除，分别对应审核中、禁用、注销状态；用户可进行编辑、删除

应用在禁用状态下，管理员可以进行编辑、应用查看、删除、解锁，用户不可以对此应用进行编辑、删除

应用在注销状态下，仅管理员可见

* 审核

管理员对用户上传应用进行审核，操作包括通过、不通过、审核意见，后台处理流程如下：

1、用户提交上传应用信息后，应用列表中将显示此条应用信息，状态为审核中

2、审核中的应用管理员可对其进行审核操作

3、审核通过时不需填写审核意见

4、审核不通过时必须填写审核意见，审核意见将存为这条应用数据的参数，当用户点击审核失败状态的应用时，可以查看审核意见

* 锁定与解锁

管理员可以对应用进行锁定操作。处于锁定状态的应用遵循以下原则：

用户不能通过平台对锁定状态下的应用进行编辑、删除操作

管理员可对锁定状态下的应用进行信息的查看、编辑、删除、解锁操作

* 界面操作

点击左侧菜单栏-应用管理，进入应用管理数据页面

页面包含：查询、添加、编辑（包含管理员审核操作）、删除，锁定与解锁及列表内容

查询条件：关键字：应用名称、应用AID、应用状态，联合查询条件：上线时间（选择日期范围，默认为空）

添加：点击“添加”按钮，进入添加/编辑页面，弹框显示新增应用数据列表（\*为必填项），点击确认即完成添加应用动作，同时在应用信息列表中更新一条数据。

编辑: 点击列表“操作”栏中“编辑”按钮后，新页面显示应用详细信息，管理员可进行编辑、审核通过、审核驳回、审核意见填写操作，用户可进行编辑操作。其中，只有上线时间、下载次数不能编辑。

删除：点击列表“操作”栏中“删除”按钮，完成删除应用信息动作，同时应用信息列表中更新减少一条数据。

锁定与解锁：点击列表最右侧操作栏中的锁定动作，此应用被锁定，应用状态显示为“已锁定”， 此时不能对这个应用进行任何操作。同时操作栏中显示 “解锁”（表示此应用处于可解锁状态），点击“解锁”动作，应用解除锁定，应用状态为“已解锁”。

## 个人化信息管理

### 个人化证书信息

本模块可对运营机构的证书进行添加、维护（编辑、查看、删除）

* 数据内容：
* 操作流程

导入证书

1、 用户可导入机构证书

2、 导入的机构证书编号不能重复，只有管理员将导入的机构证书删除后，才可以再次导入这条机构证书

3、 导入的方式为手动录入信息（如果后期需要导入多条证书信息，可支持通过EXCEL批量导入）

### 个人化钱包信息

应用个人化将钱包信息、SE信息、机构信息写入应用。本模块可对个人化信息进行添加（手动添加、接口获取）、维护（编辑、查看、删除）。

* 数据信息内容



导入个人化信息

1、 用户可导入个人化信息

2、 导入的钱包ID不能重复，只有管理员导入的钱包ID删除后，才可以再次导入这条个人化信息

3、 导入的方式为手动录入信息（若需要导入多条个人化信息，可支持通过EXCEL批量导入）

### 个人化方案配置

配置 不同服务机构提供的应用版本对应的个人化数据配置项。实现不同应用的个人化信息项差异化管理。

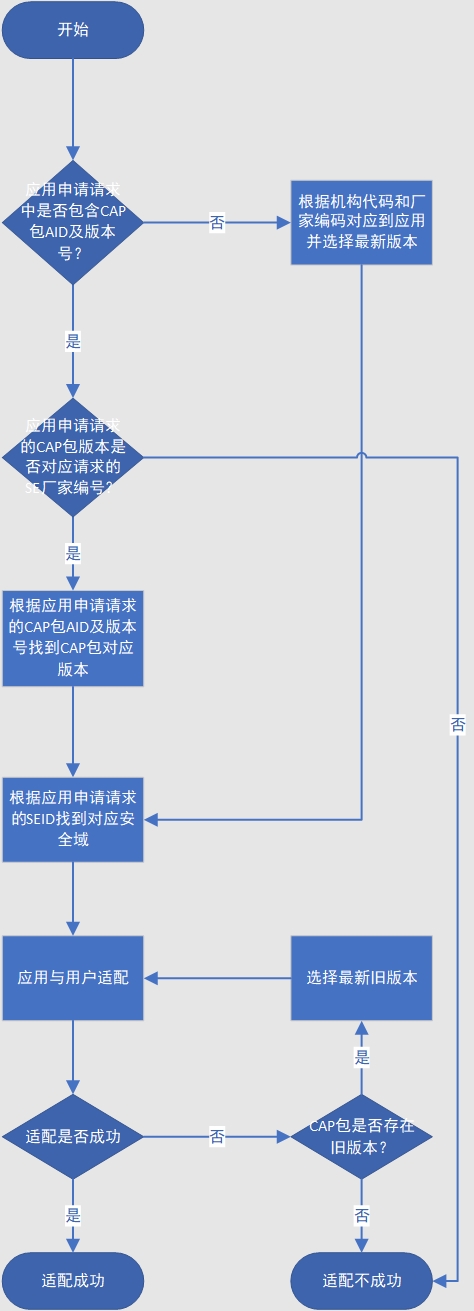
### 应用安装适配管理

可为同一应用的不同版本配置相应的用户适配信息，以满足应用对SE兼容性的要求

* 数据信息内容：



* 流程



流程说明：

1、 平台收到用户应用申请下载的请求，首先判断申请请求中是否包含CAP包AID及版本号，若不包含则根据机构代码和厂家编号找到应用，并选择最新应用CAP包；若包含则判断申请请求的CAP包版本是否对应请求的SE厂家编号。若不对应则适配不成功，返回“申请下载应用无法适配当前SE设备”；若对应，则找到对应版本的CAP包

2、 平台根据应用申请请求的SEID找到对应的安全域，进行适配

3、 若适配不成功，则判断所请求CAP包是否存在旧版本，若存在则选择最新旧版本，再次进入应用适配环节，进入循环操作，直到应用适配成功或失败；若不存在旧版本，则适配不成功，返回“申请下载应用无法适配当前SE设备”

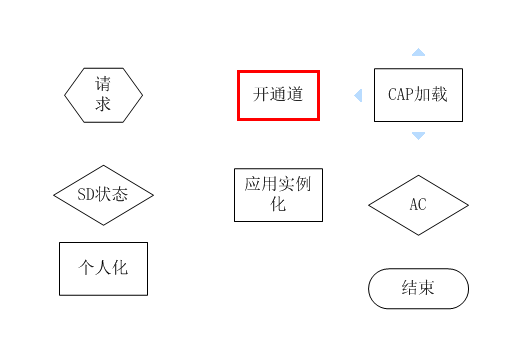
### 应用安装指令流程设置

针对不同的厂商SE类型，服务商应用类型，配置应用安装、激活、个人化，删除、锁定/解锁，应用升级等操作项的 APDU指令流程编排。

主要配置内容：定义指令包，编排逻辑流程。

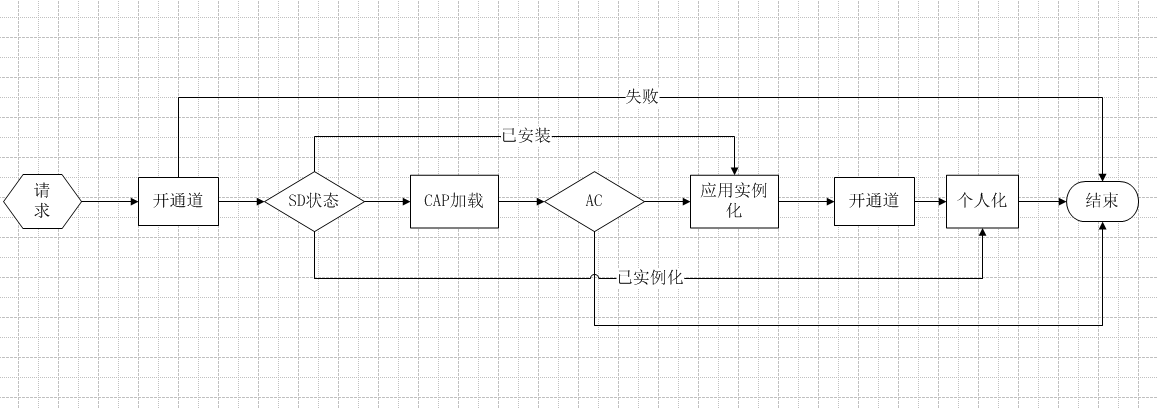
* **指令包定义：**

指令包是可以编排在一个指令批次中多个APDU指令集合，平台根据GP规范预先定制，或根据实际具体应用场景定制封装。



…

* **指令流程编排**



针对不同SE、SP提供商发布的SE及应用包可以个性化定制指令分发编排流程。

### 应用实例化信息管理

查询已安装激活的 SE、应用、个人化记录情况，可以查看相关过程状态和激活过程日志等。

## 接入服务管理

本模块是针对SE、设备等接口进行接入服务的认证管理；

### 证书密钥信息管理

管理分发服务接入证书；



* *界面操作*

点击左侧菜单栏-服务认证管理-证书秘钥信息管理，进入管理数据页面

页面包含：查询、添加、查看、编辑、删除、列表内容

查询条件：关键字：证书编号、机构名称，联合查询条件：创建时间（选择日期范围，默认为空）

添加：点击“添加”按钮，进入添加/编辑页面，显示新增数据列表（\*为必填项），点击确认即完成添加证书信息动作，同时在证书信息列表中更新一条数据。

编辑: 点击列表“操作”栏中“编辑”按钮后，新页面显示证书信息详细信息，可进行编辑操作。

删除：点击列表“操作”栏中“删除”按钮，完成删除证书信息动作，同时证书信息列表中更新减少一条数据

### 接口服务密钥管理

管理分发服务接入证书；

* 界面操作

点击左侧菜单栏-服务认证管理-接口服务秘钥信息管理，进入管理数据页面

页面包含：查询、添加、查看、编辑、删除、列表内容

查询条件：关键字：接口编号、接口名称，联合查询条件：创建时间（选择日期范围，默认为空）

添加：点击“添加”按钮，进入添加/编辑页面，显示新增数据列表（\*为必填项），点击确认即完成添加信息动作，同时在信息列表中更新一条数据。

编辑: 点击列表“操作”栏中“编辑”按钮后，新页面显示信息详细信息，可进行编辑操作。

删除：点击列表“操作”栏中“删除”按钮，完成删除信息动作，同时信息列表中更新减少一条数据。

### SE合作商管理

管理合作商信息及可接入服务ID，证书等信息；

* 数据管理

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 参数名称 | **内容说明** | **必要性** | **备注** |
| 1 | 合作商代码 | 接口唯一标识，平台生成 | M |  |
| 2 | 合作商名称 | 接口名称 | M |  |
| 3 | 有效期 | 默认1年 | M | 可空，视实际需要 |
| 4 | 授权计数 | SE认证授权次数,默认不限 | M | 可空，视实际需要 |
| 5 | 接服务证书 |  |  |  |
| 6 | 接入服务ID |  |  |  |
| 7 | 接入服务Key |  |  |  |

* 界面操作

点击左侧菜单栏-服务认证管理-合作商信息管理，进入页面

页面包含：查询、添加、查看、编辑、删除、列表内容

查询条件：关键字：编号、接口名称，联合查询条件：创建时间（选择日期范围，默认为空）

添加：点击“添加”按钮，进入添加/编辑页面，显示新增数据列表（\*为必填项），点击确认即完成添加信息动作，同时在信息列表中更新一条数据。

编辑: 点击列表“操作”栏中“编辑”按钮后，新页面显示信息详细信息，可进行编辑操作。

删除：点击列表“操作”栏中“删除”按钮，完成删除信息动作，同时信息列表中更新减少一条数据。

### SE商户信息管理

管理合作商户信息及可接入服务ID，证书等信息；

* 界面操作

点击左侧菜单栏-服务认证管理-商户信息管理，进入页面

页面包含：查询、添加、查看、编辑、删除、列表内容

查询条件：关键字：编号、接口名称，联合查询条件：创建时间（选择日期范围，默认为空）

添加：点击“添加”按钮，进入添加/编辑页面，显示新增数据列表（\*为必填项），点击确认即完成添加信息动作，同时在信息列表中更新一条数据。

编辑: 点击列表“操作”栏中“编辑”按钮后，新页面显示信息详细信息，可进行编辑操作。

删除：点击列表“操作”栏中“删除”按钮，完成删除信息动作，同时信息列表中更新减少一条数据。

### SE注册信息管理

本模块是查看远程合作商 SE注册认证信息，主要信息如下：

## 统计分析管理

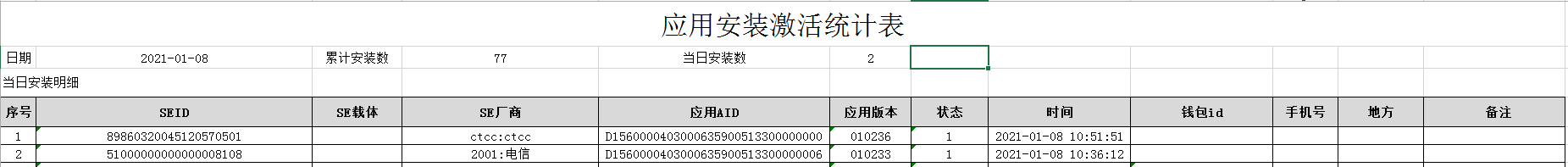
### 应用实例化日统计

按机构，SE类型、统计当日开卡数量及明细；



### 应用实例化分类汇总

按机构，SE类型、时间段统计开卡数量及明细；



## 系统权限管理

### 角色管理

管理员可在此功能模块中进行角色添加、删除、权限编辑（权限配置）。

* 数据管理

1 角色信息列表

|  |  |  |
| --- | --- | --- |
| 序号 | 参数名 | 说明 |
| 1 | 角色ID | 平台分配 |
| 2 | 角色名称 | 默认角色：  1 超级管理员  2 普通管理员  3 普通用户  4 未配置（可创建新角色） |
| 3 | 角色描述 | 长度不超过xx字符 |
| 4 | 角色权限 | 1、web门户登录  2、管理员账号管理  3、用户账号管理  4、角色管理  5、机构管理  6、SE信息管理  7、SE类型管理  8、安全域信息管理  9、应用信息管理  10、应用适配管理  11、应用个人化信息管理  12、证书管理  13、操作日志管理  14、服务器监测  15、预警设置 |

2 角色权限管理列表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 权限内容 | | | 超级管理员  （Y/N） | 普通管理员  （Y/N） | 普通用户（Y/N） |
| 1 | web门户登录 | | | Y | Y | Y |
| 2 | 管理员账号管理 | | | Y | N | N |
| 3 | 用户账号管理 | | | Y | Y | N |
| 4 | 角色管理 | 添加 | | Y | N | N |
| 权限编辑 | | Y | N | N |
| 删除 | | Y | N | N |
| 5 | 机构管理 | | | Y | N | N |
| 6 | SE信息管理 | | 添加 | Y | Y | Y |
| 检索 | Y | Y | Y |
| 编辑 | Y | Y | Y |
| 查看 | Y | Y | Y |
| 锁定/解锁 | Y | Y | N |
| 删除 | Y | Y | N |
| 7 | SE类型管理 | | 添加 | Y | Y | N |
| 检索 | Y | Y | N |
| 编辑 | Y | Y | N |
| 查看 | Y | Y | N |
| 删除 | Y | Y | N |
| 8 | 安全域信息管理 | | 添加 | Y | Y | Y |
| 检索 | Y | Y | Y |
| 编辑 | Y | Y | Y |
| 查看 | Y | Y | Y |
| 锁定/解锁 | Y | Y | N |
| 删除 | Y | Y | N |
| 9 | 应用信息管理 | | 添加 | Y | Y | Y |
| 检索 | Y | Y | Y |
| 编辑 | Y | Y | Y |
| 查看 | Y | Y | Y |
| 锁定/解锁 | Y | Y | N |
| 删除 | Y | Y | N |
| 审核 | Y | Y | N |
| 10 | 应用适配管理 | | 检索 | Y | Y | Y |
| 编辑 | Y | Y | Y |
| 查看 | Y | Y | Y |
| 删除 | Y | Y | Y |
| 11 | 应用个个人化信息 | | 添加 | Y | Y | Y |
| 检索 | Y | Y | Y |
| 编辑 | Y | Y | Y |
| 查看 | Y | Y | Y |
| 删除 | Y | Y | N |
| 12 | 证书管理 | | 添加 | Y | Y | Y |
| 检索 | Y | Y | Y |
| 编辑 | Y | Y | Y |
| 查看 | Y | Y | Y |
| 删除 | Y | Y | N |
| 13 | 操作日志管理 | | | Y | Y | N |
| 14 | 服务器监测 | | | Y | Y | N |
| 15 | 预警设置 | | | Y | Y | N |

说明：

“Y”表示具备该项功能的权限

“N”表示不具备该项功能的权限

* 界面操作

点击左侧菜单栏平台用户管理-角色管理，进入角色管理页面

页面包含：查询、新增、编辑、删除、列表内容

查询：角色名称

新增：按钮位于查询条件栏右侧，点击新增，弹出新增角色弹窗

新增页面包含：

输入框：角色名称：必填；角色描述：选填；

复选框：权限名称

按钮：全选、重置、确定

编辑：点击列表中某条数据操作栏中的编辑动作，弹出编辑页面弹窗，可对信息进行修改编辑。

删除：点击列表中某条数据操作栏中的删除动作，此角色及权限配置数据被删除。

### 用户管理

提供管理员对于该管理员所在机构下普通用户的账号信息的增删改查

* 用户账号列表包含以下参数：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数名** | **说明** | **是否可编辑** |
| 1 | 用户ID | 平台分配（不展示） | N |
| 2 | 邮箱 | 用户邮箱 | Y |
| 3 | 登录名 | 管理员添加时填写 | Y |
| 4 | 所属机构 |  | N |
| 5 | 创建时间 | 首次注册激活时间 如2015/11/18 17:28 | N |
| 6 | 最后登录时间 | 最后一次登录时间 如2015/11/18 17:28 | N |
| 7 | 账号状态 | 1、正常 账号注册并激活成功  2、禁用 账号被禁用  3、待激活 账号注册但未激活 | Y |

* 界面操作

管理员点击左侧菜单栏-平台用户管理-账号管理-用户账号管理，进入用户账号管理页面

页面包含：批量创建、查询、编辑、删除、禁用与启用、列表内容

批量创建：批量添加普通用户，EXCEL形式导入，填写信息：登录名、邮箱、所属机构、密码,所有信息需要符合所填写数据规则

查询

关键字查询：登录名、邮箱

联合查询条件：最后登录时间，例如2015.10.01-2015.10.03

编辑：点击列表中数据操作栏中的编辑动作，弹出该条数据的编辑弹窗，部分信息为可编辑状态（见信息列表）

禁用与启用：点击列表中某条数据操作栏中的禁用动作，用户账号被禁用（账号此时不能登录，提示“用户状态异常，请联系管理员”），同时按钮变成“启用”，点击启用按钮，用户账号被启用。

## 平台维护管理

### 系统参数设置

设置系统全局运行控制参数。

### 预警设置

提供平台告警设置功能，主要针对上述三个指标设定预警门限，并配置通知Email收件邮箱。

点击左侧菜单栏平台管理-预警设置，进入预警设置页面

可对个参数进行编辑、删除及新增预警门限等

预警设置参数表

|  |  |  |
| --- | --- | --- |
| 序号 | 参数名 | 说明 |
| 1 | CPU告警值（%） |  |
| 2 | 内存告警值（%） |  |
| 3 | 硬盘告警值（%） |  |
| 4 | 警告接收邮箱 |  |
| 5 | 创建时间 | 首次创建或修改时间 |

告警Email内容

您好！

硬钱包TSM平台提醒您，CPU告警值已达到xxxx，请您及时维护，保持系统正常运行

### 日志管理

本模块提供平台所有用户（包括管理员）操作日志数据的查询、导出。

### 服务器监测

提供系统服务器状态的实时监控功能，通过折线或条形图形式，展示最近一小时CPU使用率、硬盘使用率及内存使用率。

点击左侧菜单栏平台管理-服务器监测，进入实时监控页面

监测数据包括CPU使用率、内存使用率、硬盘使用率



## TSM密码机系统

在硬钱包应用的生命周期中，禁止各类密钥（包括不限于个人化密钥、应用密钥、会话密钥）的明文或可用于生成明文的全部要素出现在TSM 系统的存储介质上（包括不限于CPU 寄存器、缓存、内存、外存），使用相关密钥的操作应在行内的硬件密码设备上完成。

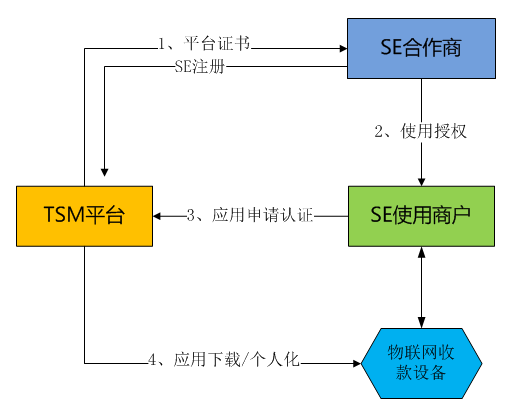
数字货币硬钱包可以使用专用加密机为数币支撑业务提供专用加解密接口，满足密码运算逻辑深度封装，高安全性和密码规则可定制化等方面需求。

## 物联网支付终端注册及认证管理

物联网收款设备认证服务系统是SE发行合作商、数币收款设备使用商及硬钱包应用服务提供商之间建立可信安全的SE设备管理注册、应用申请的认证服务系统。

通过发放平台证书、服务访问授权进行数据加密传输、SE认证检测激活控制管理。

该认证服务系统是针对 数币收款设备量身定制认证系统。



**产品主要功能包括：**

* + 平台证书秘钥管理
  + 接口服务秘钥管理
  + SE合作商管理
  + SE使用商户管理
  + SE注册管理
  + 收款设备、SE模块认证管理
  + 应用申请、开卡授权管理
  + 支持国密算法、证书、数据传输加密等

## 数币应用支撑中间件

数币应用支撑中间件包括符合央行硬钱包规范的SE钱包应用（Applet），以及配套的终端应用插件SDK，可支撑数币硬钱包与TSM平台、业务平台交互完成硬钱包账户开立、激活、充值、支付、收款、转账等标准功能实现。

**产品功能包括：**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能** | **数币硬钱包支撑中间件** |
| 1 | 钱包应用安装及个人化接口 | 支持 |
| 2 | 钱包应用删除接口 | 支持 |
| 3 | 钱包应用更新接口 | 支持 |
| 4 | 钱包应用版查询接口 | 支持 |
| 5 | 钱包注册接口 | 支持 |
| 6 | 钱包激活接口 |  |
| 7 | 钱包名称更新接口 | 支持 |
| 8 | 钱包注销接口 | 支持 |
| 9 | 钱包充值接口 | 支持 |
| 10 | 钱包提现接口 | 支持 |
| 11 | 同步接口 | 支持 |
| 12 | 交易结果查询接口 | 支持 |
| 13 | 在线交易接口 |  |
| 14 | 离线支付接口 | 支持 |
| 15 | 离线收款接口 | 支持 |
| 16 | 获取交易流水接口 | 支持 |
| 17 | 取DC/EP响应数据接口 | 支持 |
| 18 | 钱包凭证上送 |  |
| 19 | 钱包密码验证 |  |

数币硬钱包应用插件SDK是在数币硬钱包SE应用的基础上，提供对数币硬钱包的本地管理（开立、激活、充值、支付、收款、转账）等功能，SE插件可通过蓝牙、NFC等通信协议实现插件应用与硬钱包卡、收付款模组进行连接并管理。

# 产品服务接口

## SE状态查询

SE状态查询请求报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **描述** |
|  | MsgBody | msgBody | [1..1] |  |  |
|  | -ProcessID | proID | [0..1] | Max32Text |  |
|  | -InstAid | instAid | [0..1] | Max32Text |  |
|  | -PayEnvironmentIdentification | payEnvID | [1..1] | Max4Text |  |
|  | -TerminalUnqueIdentification | tmnlID | [0..1] | Max64Text |  |
|  | -SafeDeviceIdentification | safeDevID | [0..1] | Max64Text |  |
|  | -SafeEquipmentIdentification | safeEqID | [1..1] | Max64Text |  |
|  | -SeIssuer | seIssuer | [1..1] | Max4Text |  |
|  | -OperCode | operCode | [1..1] | Max6Text |  |
|  | -BatchSize | batSize | [1..1] | Max2NumericText |  |
|  | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
|  | -Responselistcount | respListCon | [1..1] | Max2NumericText |  |
|  | -Responselist | respList | [0..n] |  |  |
|  | --Response | resp | [0..1] | Max512Text |  |

SE状态查询应答报文

| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | ProcessStatus | procSts | [1..1] | Max5Text |  |
| 2 | ProcessCode | procCd | [1..1] | Max4Text |  |
| 3 | ProcessInformation | procInf | [0..1] | Max105Text |  |
| 4 | MsgBody | msgBody | [1..1] |  |  |
| 5 | -ProcessID | proID | [0..1] | Max32Text |  |
| 6 | -BatchSeq | batSeq | [0..1] | Max2NumericText |  |
| 7 | -Commandlistcount | comdListCon | [0..1] | Max2NumericText |  |
| 8 | -Commandlist | comdListCon | [0..n] |  |  |
| 9 | --Command | commd | [1..1] | Max512Text |  |
| 10 | -ResultNumber | resultNum | [0..1] | Max3NumericText |  |
| 11 | -AppletList | appletList | [0..1] |  |  |
| 12 | --Object 1 |  | [1..1] |  |  |
| 13 | ---InstAid | instAid | [0..1] | Max32Text |  |
| 14 | ---CapAID | capAID | [1..1] | Max32Text |  |
| 15 | ---AppState | appState | [1..1] | Max2Text |  |
| 16 | ---WalletId | walletId | [0..1] | Max16Text |  |
| 17 | ---AppVer | appVer | [1..1] | Max8Text |  |
| 18 | ---LatestVer | latestVer | [0..1] | Max8Text |  |
| 19 | …… | …… | …… | …… |  |
| 20 | --Object n |  | [0..1] |  |  |
| 21 | -SSDList | ssdList | [0..1] |  |  |
| 22 | --Object 1 |  | [0..1] |  |  |
| 23 | ---InstAid | instAid | [0..1] | Max32Text |  |
| 24 | ---CapAID | capAID | [1..1] | Max32Text |  |
| 25 | ---AppState | appState | [1..1] | Max2Text |  |
| 26 | ---AppVer | appVer | [1..1] | Max8Text |  |
| 27 | ---LatestVer | latestVer | [0..1] | Max8Text |  |
| 28 | …… | …… | …… | …… |  |
| 29 | --Object n |  | [0..1] |  |  |

## 应用申请

### 报文功能

钱包生态平台App发起硬件钱包应用申请，获取服务关联码和应用实例AID，后续根据服务关联码进行应用加载。

### 报文结构

应用申请请求报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
| 1 | MsgBody | msgBody | [1..1] |  |  |
| 2 | -AppAid | appAid | [0..1] | Max32Text |  |
| 3 | -AppVersion | appVer | [0..1] | Max8Text |  |
| 4 | -PayEnvironmentIdentification | payEnvID | [1..1] | Max4Text |  |
| 5 | -TerminalUnqueIdentification | tmnlID | [0..1] | Max64Text |  |
| 6 | -SafeDeviceIdentification | safeDevID | [0..1] | Max64Text |  |
| 7 | -SafeEquipmentIdentification | safeEqID | [1..1] | Max64Text |  |
| 8 | -SeIssuer | seIssuer | [1..1] | Max4Text |  |
| 9 | -InstructingParty | instgPty | [1..1] | Max14Text |  |
| 10 | -AidMode | aidMode | [1..1] | Max1Text |  |

其中，DC/EP金融机构编码为特征组合码，参照JR/T 0124—2014，长度为十四位，分别为大写拉丁字母或阿拉伯数字。编码分为六段，从左至右分别为：一位金融机构一级分类码；一位金融机构二级分类码；四位金融机构三级分类码；两位地区代码；五位顺序码；一位校验码：

应用申请应答报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
| 1 | ProcessStatus | procSts | [1..1] | Max5Text |  |
| 2 | ProcessCode | procCd | [1..1] | Max4Text |  |
| 3 | ProcessInformation | procInf | [0..1] | Max105Text |  |
| 4 | MsgBody | msgBody | [1..1] |  |  |
| 5 | -ProcessID | proID | [1..1] | Max32Text |  |
| 6 | -InstAid | instAid | [1..1] | Max32Text |  |

## 应用加载

### 报文功能

钱包生态平台App通过关联服务码向TSM请求应用加载指令。

### 报文结构

应用加载请求报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
|  | MsgBody | msgBody | [1..1] |  |  |
|  | -ProcessID | proID | [0..1] | Max32Text |  |
|  | -InstAid | instAid | [1..1] | Max32Text |  |
|  | -PayEnvironmentIdentification | payEnvID | [1..1] | Max4Text |  |
|  | -TerminalUnqueIdentification | tmnlID | [0..1] | Max64Text |  |
|  | -SafeDeviceIdentification | safeDevID | [0..1] | Max64Text |  |
|  | -SafeEquipmentIdentification | safeEqID | [1..1] | Max64Text |  |
|  | -SeIssuer | seIssuer | [1..1] | Max4Text |  |
|  | -BatchSize | batSize | [1..1] | Max2NumericText |  |
|  | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
|  | -ResponseListCount | respListCon | [1..1] | Max2NumericText |  |
|  | -ResponseList | respList | [0..n] |  |  |
|  | --Response | resp | [1..1] | Max512Text |  |

应用加载应答报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
| 1 | ProcessStatus | procSts | [1..1] | Max5Text | 业务处理状态 |
| 2 | ProcessCode | procCd | [1..1] | Max4Text | 处理码 |
| 3 | ProcessInformation | procInf | [0..1] | Max105Text | 业务处理信息 |
| 4 | MsgBody | msgBody | [1..1] |  | 业务数据 |
| 5 | -BatchSeq | batSeq | [1..1] | Max2NumericText | 当前业务下发命令的批次号 |
| 6 | -CommandListCount | comdListCon | [1..1] | Max2NumericText | 本次命令的个数，当返回00或0时表示指令已结束。 |
| 7 | -CommandList | comdList | [0..n] |  |  |
| 8 | --Command | commd | [1..1] | Max512Text | NNXXXX |

## 应用删除

### 报文功能

请求应用删除。

### 报文结构

应用删除请求报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
|  | MsgBody | msgBody | [1..1] |  |  |
|  | -ProcessID | proID | [0..1] | Max32Text |  |
|  | -InstAid | instAid | [0..1] | Max32Text |  |
|  | -AppAid | appAid | [0..1] | Max32Text |  |
|  | -PayEnvironmentIdentification | payEnvID | [1..1] | Max4Text |  |
|  | -TerminalUnqueIdentification | tmnlID | [0..1] | Max64Text |  |
|  | -SafeDeviceIdentification | safeDevID | [0..1] | Max64Text |  |
|  | -SafeEquipmentIdentification | safeEqID | [1..1] | Max64Text |  |
|  | -SeIssuer | seIssuer | [1..1] | Max4Text |  |
|  | -OperCode | operCode | [1..1] | Max6Text |  |
|  | -BatchSize | batSize | [1..1] | Max2NumericText |  |
|  | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
|  | -Responselistcount | respListCon | [1..1] | Max2NumericText |  |
|  | -Responselist | respList | [0..n] |  |  |
|  | --Response | resp | [0..1] | Max512Text |  |

应用删除应答报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **备注** |
| 1 | ProcessStatus | procSts | [1..1] | Max5Text | 业务处理状态 |
| 2 | ProcessCode | procCd | [1..1] | Max4Text | 处理码 |
| 3 | ProcessInformation | procInf | [0..1] | Max105Text | 业务处理信息 |
| 4 | MsgBody | msgBody | [1..1] |  |  |
| 5 | -ProcessID | proID | [0..1] | Max32Text |  |
| 6 | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
| 7 | -Commandlistcount | comdListCon | [1..1] | Max2NumericText |  |
| 8 | -Commandlist | comdListCon | [0..n] |  |  |
| 9 | --Command | commd | [1..1] | Max512Text |  |

## 应用锁定

### 报文功能

请求应用锁定

### 报文结构

应用锁定请求报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **描述** |
|  | MsgBody | msgBody | [1..1] |  | 业务数据 |
|  | -ProcessID | proID | [0..1] | Max32Text |  |
|  | -InstAid | instAid | [1..1] | Max32Text |  |
|  | -PayEnvironmentIdentification | payEnvID | [1..1] | Max4Text |  |
|  | -TerminalUnqueIdentification | tmnlID | [0..1] | Max64Text |  |
|  | -SafeDeviceIdentification | safeDevID | [0..1] | Max64Text |  |
|  | -SafeEquipmentIdentification | safeEqID | [1..1] | Max64Text |  |
|  | -SeIssuer | seIssuer | [1..1] | Max4Text |  |
|  | -OperCode | operCode | [1..1] | Max6Text |  |
|  | -BatchSize | batSize | [1..1] | Max2NumericText |  |
|  | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
|  | -Responselistcount | respListCon | [1..1] | Max2NumericText |  |
|  | -Responselist | respList | [0..n] |  |  |
|  | --Response | resp | [0..1] | Max512Text |  |

应用锁定应答报文

| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **描述** |
| --- | --- | --- | --- | --- | --- |
| 1 | ProcessStatus | procSts | [1..1] | Max5Text |  |
| 2 | ProcessCode | procCd | [1..1] | Max4Text |  |
| 3 | ProcessInformation | procInf | [0..1] | Max105Text |  |
| 4 | MsgBody | msgBody | [1..1] |  |  |
| 5 | -ProcessID | proID | [0..1] | Max32Text |  |
| 6 | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
| 7 | -Commandlistcount | comdListCon | [1..1] | Max2NumericText |  |
| 8 | -Commandlist | comdListCon | [0..n] |  |  |
| 9 | --Command | commd | [1..1] | Max512Text |  |

## 应用解锁

### 报文功能

请求应用解锁

### 报文结构

应用解锁请求报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **描述** |
|  | MsgBody | msgBody | [1..1] |  | 业务数据 |
|  | -ProcessID | proID | [0..1] | Max32Text |  |
|  | -InstAid | instAid | [1..1] | Max32Text |  |
|  | -PayEnvironmentIdentification | payEnvID | [1..1] | Max4Text |  |
|  | -TerminalUnqueIdentification | tmnlID | [0..1] | Max64Text |  |
|  | -SafeDeviceIdentification | safeDevID | [0..1] | Max64Text |  |
|  | -SafeEquipmentIdentification | safeEqID | [1..1] | Max64Text |  |
|  | -SeIssuer | seIssuer | [1..1] | Max4Text |  |
|  | -OperCode | operCode | [1..1] | Max6Text |  |
|  | -BatchSize | batSize | [1..1] | Max2NumericText |  |
|  | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
|  | -Responselistcount | respListCon | [1..1] | Max2NumericText |  |
|  | -Responselist | respList | [0..n] |  |  |
|  | --Response | resp | [0..1] | Max512Text |  |

应用解锁应答报文

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **报文要素** | **字段名** | **属性** | **类型** | **描述** |
| 1 | ProcessStatus | procSts | [1..1] | Max5Text |  |
| 2 | ProcessCode | procCd | [1..1] | Max4Text |  |
| 3 | ProcessInformation | procInf | [0..1] | Max105Text |  |
| 4 | MsgBody | msgBody | [1..1] |  |  |
| 5 | -ProcessID | proID | [0..1] | Max32Text |  |
| 6 | -BatchSeq | batSeq | [1..1] | Max2NumericText |  |
| 7 | -Commandlistcount | comdListCon | [1..1] | Max2NumericText |  |
| 8 | -Commandlist | comdListCon | [0..n] |  |  |
| 9 | --Command | commd | [1..1] | Max512Text |  |

# 项目实施方案

## 项目管理的目的

基于对成功项目的管理经验，我们总结为以下几点：

1．提高项目运作的规范性

2．提高异地项目运做的可控性

3．使项目按时验收

4．降低项目成本

5．提高客户满意度

6．确保项目质量

## 项目管理措施

针对本项目将成立项目领导小组，成员由甲乙双方的领导、项目管理方法咨询专家(项目经理)等经验丰富的专家及双方项目经理组成。下设工程实施组，技术和质量控制组，专家组，商务组，培训组等。项目决策机构为项目领导小组；

项目经理设在项目领导小组内，是项目进度的推进者，同时是任务及成果的提交与转交者；技术和质量控制组负责技术和质量的控制管理，并向项目领导小组通告项目风险与进度状况。

此时，项目经理工作的主要特点为：

1．领导组织协调小组，做好对客户及公司内部的沟通及项目进展通告工作。及时获得成果及向客户提交成果。将任务书汇总，由领导小组调用内部相应阶段所需资源完成任务，并将成果及时转交给客户。

2．所有的工作方法均由专家组负责。

3．按照项目计划日程表执行项目。在项目进行的各个阶段，每个部门分别任命相关人员对相应阶段的任务负责。整个项目在公司系统集成应用体系的所有部门配合下，在项目经理的沟通、串联下，按照计划有条不紊地进行。同时，技术和质量控制组从另一个角度对项目进行跟踪监控，从而保证项目的质量与进度。

从上述中可看出，我们的实施方法改变了传统的项目管理中完全依赖于项目经理个人或几个人的状况，参加项目的每一个成员都在项目领导小组严格的规范下完成自己的任务。

## 项目管理制度

项目工作方法、制度是确保项目成功的基石，项目工作管理是面向目标和目的、面向规范工作过程之管理。因此，目标目的的严肃性必须严格强调，工作过程的规范化应得到首要的尊重。

### 决策制度

1．针对项目经理的原则

对于项目实施过程中的日常工作，一般由项目经理加以决策，然后提交给项目领导小组。经过项目领导小组例会确认无误，则该决定生效，异议应以书面方式表达。

2．最高权力机构准则

项目领导小组是项目实施过程中的最高决策机构，对重大问题具有决策权。

3．决策书面准则

一切决策应有书面文件，并且在项目协调组备案。

### 交流制度

1．问题及早提出准则

对自己承担责任的工作，必须及时发现不能恰当完成的因素，并及时向项目经理或有关责任人书面报告，否则不能恰当完成任务的责任在于任务的承担人。

2．及时澄清准则

对所承接的工作，如没有拒绝，则代表接受人已经完全了解工作环境、工作结果要求等多个要素。如果在呈交结果时，与任务要求有出入，则不可以以任何理由解释责任，失败责任在接受人。因此，接受人应及时与任务分派人澄清任务的全部因素。

3．提醒道义准则

所有项目组成员，如发现项目进展隐患，应及时向项目经理或其他人员提醒。不提醒是没有道义的。提醒可以以书面或口头方式。提醒时也要注意不要追究相关人员的后续工作（因为工作安排有各自的计划与方式）。

### 例会制度

与项目相关的例会结束后，均形成会议纪要，上报与会人员及客户经理。

1．周例会

每周五下午，由项目经理组织在现场的双方项目组成员参加周例会。总结上周工作，形成项目周报。周报必须通过合理渠道上报领导小组。项目周报的内容包括：上周工作进展报告、本周工作计划、本周任务分派报告。

2．月例会

每月的第一个星期五，由项目领导小组组织各工作组召开项目例会，总结这段时间的工作，会后形成会议纪要、项目月报。

3．问题的提交

参见“问题与争议管理方法”一节的相关内容。

4．审批与确认

审批或确认人在收到问题后的三个工作日内向提出人给出书面回复。

5．报告体系

报告格式遵循项目管理规范。

### 问题与争议管理方法

1．问题及早报告原则

对于一个问题，问题发起人必须在问题发生的二日之内，向项目经理提交报告。问题没有及早报告，导致的项目影响，由延误报告人承担。

2．报告方式

如报告人认为口头报告即可，可以采用口头报告，但是如果口头报告没有使问题得以解决，则视同报告人没有作报告。

3．争议管理

在项目中，任何不能达成一致的观点均为争议，争议应立即向项目的上级单位呈报，并报项目领导小组。争议应由可以协调争议各方的机构加以裁决，并对裁决承担责任。争议裁决人由项目经理选择争议的最高仲裁机构为项目领导小组。

如项目领导小组仍不能达成一致意见，则遵循“谁决策谁承担决策失误给对方和项目带来的损失”之原则。

### 失误管理制度

失误可能是多方面的，失误的及早发现是项目成功的基本保障。对失误的严肃性是项目管理的基本要素。因此，每个项目成员均要给予极大重视。对以下各个事件，必须做出失误分析。如：计划有重大改动；经费有较大变化；质量不符；进度不符；成果不符；其它重大事件。

项目经理应每月给出失误分析报告，并有每一失误的详细分析报告，此报告应提交相关人员。如果失误分析报告看不出项目有重大影响，而项目实际有重大问题，则为项目经理之责任。

### 工作管理制度

项目的管理对象主要有：

 目标

 任务

 资源

 质量

 成果

 进度

这些要素通过项目组的工作加以实现，对项目组成员的工作管理是：及早发现问题的重要渠道是落实责任与激励的主要依据。因此，工作管理制度必须全面执行。工作管理制度的对象为：各项目机构和成员承担的工作。

一个项目目标可分解成各阶段目标，每一阶段目标由一个或多个任务（可带子任务）去完成。工作管理是对：工作目标及相关任务、已分派任务、待分配任务、疑难事项等进行管理。疑难事项应立即提交项目经理，项目经理应持有疑难事情管理清单，清单的任何变化必须立即提交项目领导小组。

### 项目变更管理

在项目实施过程中，项目的变更是必然存在的，并且合理的变化是应予以允许和尊重的。因此，项目变更的管理目的在于忠实地记录项目演变的过程，有利于项目的跟踪管理，是项目管理工作的重要组成部分。

针对项目实施过程中出现的各种变更，将依据系统集成项目管理规范之项目变更管理规范执行，其基本过程如下：

项目相关各方有权对需求、工作任务、进度要求、人员调动、经费等提出项目变更请求，项目变更提出方或发现方需填写项目变更报告，说明变化前的状态、变化原因、变化的内容，并提交项目经理。

如果项目变更被拒绝，项目经理应该负责解释原因，并填入项目变更报告。

如果项目变更被接受，项目经理分析由于该项目变更对工作量、费用、进度、人员安排等方面的影响，并将此内容填入项目变更报告。如该变化涉及第三方，则项目经理必须将项目变更报告提交他们，并取得一致意见。如遇到重大的项目变更，项目经理还必须将项目变更报告提交项目领导小组，提请项目领导小组对该项目变更进行讨论和决策。

项目经理在接到变化提出方请求后2个工作日之内，应给予变化提出方明确答复。对于提交项目领导小组讨论决策的项目变更，项目领导小组应在接到变化提出方请求后5个工作日内给予明确答复。

参与项目合作的相关各方在项目变更报告单上签字认可后，该项目变更生效，项目经理执行变化实施。

项目经理根据项目变更报告单中进度的变化情况，修改项目进度计划，调整项目组人员组织结构，以及项目组成员的工作安排，修改项目预算等。对于重大的项目变更，项目经理应将项目变更报告提交项目协调组，协调人员对于项目变更所引起的商务问题与客户进行协商。

将项目变更报告单以及该变化所引起的进度计划、计划预算、人员组织结构、工作说明书等方面修改版本的提交项目相关各方。

对于由于项目变更所产生的项目文档修改，遵照工程项目管理规范之项目变更管理实施规范执行。

项目组成员以及项目相关人员有义务及时发现各种项目变更，并通报项目经理。

项目经理有责任追踪项目变更的各项工作过程，直至变化管理工作完成，项目按新的项目计划执行。

对所有项目变更必须进行管理，并忠实记录项目变更过程。及时合理地调整因项目变更引起的进度、预算、人员、工作内容等。

### 计划管理

项目计划是项目实施工作的执行依据，在项目实施工作开始之前，项目经理必须提交项目计划，否则不允许执行下一步工作。

项目计划必须经合作双方认真讨论确定，保证计划的可行性。

项目计划在确定之后，必须予以公布，告知相关各方，以便对项目计划执行情况的监督。

项目计划分为总体计划、阶段计划、月计划、周计划。阶段跨度在2个月以上时，项目经理必须制定月计划，阶段跨度在2个月以内时，项目经理可以以阶段计划代替月计划。

项目计划包括进度计划、人力计划、资源计划、资金费用计划。

项目总体计划及其变化必须经项目领导小组批准。

项目计划必须以明确工作目标和工作任务为前提，因此各类计划应按阶段、按工作目标和任务的明确落实为下阶段各类计划的制定开始日。

进度计划中应包括项目组工作安排和对于与项目有关的其他各方的工作安排。

项目经理在完成项目计划之后，方可根据项目计划，分派工作任务。

### 质量保证措施

依据项目质量控制与管理规范，在整个项目管理过程的每一个重要环节均有完善的质量保证方法和工作规范。

## 项目风险管理

### 风险的定义和识别

风险定义和识别包含两方面内容：识别哪能些风险可能影响项目进展及记录具体风险的各方面特征。风险识别不是一次性行为，而应有规律的穿整个项目中。

风险识别包括识别内在风险及外在风险。内在风险指项目工作组能加以控制和影响的风险，如人事任免和成本估计等。外在风险指超出项目工作组等控力和影响力之外的风险，如市场转向或政府行为等。

严格来说，风险仅仅指遭受创伤和损失的可能性，但对项目而言，风险识别还牵涉机会选择（积极成本）和不利因素威胁（消极结果）。

项目风险识别应凭借对“因”和“果”（将会发生什么导致什么）的认定来实现，或通过对“果”和“因”（什么样的结果需要予以避免或促使其发生，以及怎样发生）的认定来完成。

风险认定过程应在另一个相关领域中确定一个要求，以便进行进一步运作。比如：如果工作分析结构图不够细致，就无法进行充分的风险识别。风险常常被做为系统规定参数或假定值输入其它过程。

### 风险的量化和分析

风险的量化

风险量化涉及到对风险和风险之间相互作用的进行评估，用这个评估结果分析项目可能产生的风险。这首先需要决定哪些风险值得反应。风险由于包括诸多因素而较复杂，这里就部分因素列举如下：

机会和困难能够以出乎意料的方式相互作用（比如：计划的延迟会造成不得不考虑新的战略以缩短整个项目周期）。

一个单纯的风险事件能造成多重后果。（比如：主要关键程序的开发延误会造成成本超支、计划延迟、多支付薪水以及产品质量低劣等。）

某个项目涉及人员的机会（如降成本）却往往意味着对其它项目涉及人员的威胁（不得不降低利润）。

风险对策研究和分析

风险对策研究和分析包括对机会的跟踪进度和对危机的对策的定义。对危胁的对策大体分以下三点：

避免——排除特定危胁往往靠排除危胁起源。项目管理队伍绝不可能排除所有风险，但特定的风险事件往往是可以排除的。

减缓——减少风险事件的预期资金投入来减低风险发生的概率（如为避免项目产出的产品报废而使用专利技术），以及减少风险事件的风险系数（如买投保），或两者双管齐下。

吸纳——接受一切后果。这种接受可以是积极的（如制定预防性计划来防备风险事件的发生），也可以是消极的（如某些工程运营超支则接受低于预期的利润）。

### 风险控制的组织架构和风险控制流程

对于项目风险控制，应该在项目经理领导下，成立项目风险控制小组。小组的成员包括：项目的甲方、乙方、分包商、行业专家。设立风险控制组组长的岗位，负责组织、协调、管理、控制项目风险。下图为项目风险控制的操作流程概念图。

项目风险控制包括实施风险管理方案以便在项目过程中对风险事件做出回应。当风险发生时，需要重复进行风险识别，风险量化以及风险对策研究一整套基本措施。就算最彻底和最复杂的分析也不可能准确识别所有风险以及其发生概率，理解这一点是很重要的，因此控制和重复是必要的。

### 风险对策控制的输入项

（1）实际风险事件。

有些已识别了的风险事件会发生，有些则不会。发生了的风险事件是实际风险事件或说是风险的起源，而项目管理人员应总结已发生的风险事件以便进行进一步的对策研究。

（2）附加风险识别。

当项目进程受到评价和总结时，事先未被识别的潜在风险事件或风险的起源将会浮出水面。

### 风险对策实施控制的工具和方法

（1）工作区：对消极的风险事件而言，工作区是一种不列入方案的对策。所谓不列入方案是指在感觉上它并未定义在风险事件发生前。

（2）附加风险策略研究。如果风险事件未被预料到，或后果远大于预料，那么计划的风险策略将会不充分，这时就有必要再次重复进行风险对策研究甚至风险管理程序。

### 风险对策实施控制输出项

（1）校正行为：校正行为首先包括实施已计划的风险对策（比如实施预防性计划或工作区计划）。

（2）实时调整风险管理计划。一个预料之中的风险事件发生或没发生，对实际风险事件后果的评估，对风险系数和风险机率的评估，以及风险管理方案的其它方面，都应进行实时的更新调整。

## 项目组织机构与管理

### 项目进度管理

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 阶段 | 阶段成果 | 周期  （合同签订T日） |
|  | 需求阶段 | 总体方案  需求分析说明书 | T+1周 |
|  | 设计阶段 | 系统设计说明书  (概要设计，详细设计数据库设计) | T+2周 |
|  | 开发阶段 | 程序清单  软件运行包  部署文档 | T+3周 |
|  | 测试阶段 | 测试计划、测试大纲，测试报告 | T+2周—T+4周 |
|  | 运行部署及交付 | 操作手册、培训 | T+1周 |
|  | 运维 | 运维手册 | 合同服务期 |

注：各里程碑完成时间以甲方阶段性项目实施计划为准。

### 项目组织机构



图表-项目组织结构图

项目组职责分工如下：

* 项目领导组：

项目领导组是项目实施中双方协同工作的最高管理机构，主要职责是监督和协调项目的实施和进展，定期审核项目经理就项目进展执行情况的书面报告，对项目中存在的问题做出决策，协调解决重大问题和突发事件及对项目经理的任免。

我们建议成立指挥中心的主管领导直接控制，各相关业务部门领导参与的项目领导机构，承建方同样委派一名项目总监，双方联合组成项目领导组。制订定期的项目进展汇报制度，一方面，对项目组起到一个督促作用，另一方面，以规范的方式确立项目的权威性和重要性，并集中解决一些棘手的问题。

* 风险评估组：

由信息指挥中心技术负责人（或第三方监理机构）及承建方技术总监组成，对工程实施过程中出现的各种风险因素进行评估、控制，降低项目实施风险。

* 需求分析组：

由信息指挥中心相关部门的技术人员和业务人员与承建方的技术人员组成，对系统各项业务需求做出总体描述，提交技术和业务部门共同论证，形成正式业务需求。

负责在项目实施期间，参加和指导业务需求分析，咨询解答项目实施中的问题，以及与的有关业务人员讨论协商有关的业务问题。

公司将抽调资深的业务方面的专家，参与需求分析和业务流程的设计，对相关问题提出建议。

* 项目经理：

公司项目经理将负责整个项目的日常管理。提供信息项目组和公司间的沟通渠道，协调、跟踪、管理、汇报项目的实施状况，保证项目按计划完成，保证项目质量。

其主要任务为：

担任公司与信息项目组项目经理的沟通渠道，协调项目实施。

制定详细项目计划，估计项目的规模、工作量和进度，安排项目组的工作任务，确定项目成功实施的关键任务。

协调建立项目实施环境。

项目的跟踪和监控，包括定期召开项目组的例会，跟踪和检查项目的进展情况；组织阶段点和里程碑处开发活动及其成果的评审；控制项目的变更活动；进行风险管理；定期对项目跟踪活动进行总结，并向公司和信息项目领导小组汇报。

遇到重大问题时，提交项目领导组研究决定。必要时召开项目协调会议。

* 质量保证组SQA：

由公司专门的质量保证人员（SQA）担任。质量保证是一种有计划的、贯穿于整个项目生命周期的质量管理方法，其目的是提供一种有效的人员组织形式和管理方法，客观地检查和监控“过程质量”和“产品质量”。对于在质量保证活动中发现的与规范不符合的问题尽量在软件项目内部解决，对于项目内部无法解决的问题，软件质量保证组可以把问题提升到项目领导组以求得解决。

* 技术开发组：

主要由承建方的技术工程师构成，负责系统总体设计、子系统详细设计、编码等工作。

完成系统实施过程中的分析设计、开发实现，以及后期的维护支持工作。

技术开发组的成员按照负责的任务范围进行划分，作到配合工作，以保证系统从设计、开发直至安装、运行及维护过程的技术支持能力。

公司承诺将委派技术水平高，经验丰富的技术人员参加项目的开发。

* 技术支持组：

主要由承建方的技术工程师构成，负责对开发人员、用户进行技术支持工作，包括：负责系统软件及开发工具技术支持、技术培训支持。用户相关部门的技术人员负责系统的日常维护和管理。完成整个项目过程中的所有文档、资料、技术报告、软件介质的管理。对系统采用的第三方产品的技术支持及协调工作，对用户提供应用系统的产品的技术支持工作。

* 系统集成组：

主要由承建方的技术工程师技术人员组成，负责信息项目中所有网络硬件、服务器主机、操作系统、数据库、应用服务器等所有软硬件平台的安装、调试、实施及对用户的培训，并负责应用系统开发后系统总体集成。

* 测试组：

主要由承建方的技术人员构成，负责制定测试计划、搭建测试环境、编写系统测试方案和设计、根据项目需求规格说明书编写和执行测试用例，在测试过程中填写测试缺陷报告，定期通过测试缺陷报告库中的数据反映的信息总结和分析测试进展状况，并及时向项目经理以及其他相关人员进行汇报。测试组要负责系统全面的测试工作，在测试安排上建议信息项目有关业务和技术人员也派人参加进来，并由业务人员和技术人员一起做功能性、界面友好性以及易用性等方面的用户测试，测试组中的技术人另外需要负责做性能、压力等测试。

上述组织结构及职责划分根据项目进展情况由项目领导组及项目经理负责启动并调整，双方应在项目实施阶段保持人员的稳定性，确保项目按计划实施。

* 配置管理组（SCM）：

配置管理组由公司专门的配置管理人员担任。实施配置管理的目的是，建立和维护在项目的整个生命周期中软件产品的完整性和可追溯性。通过标识配置项、建立基线、版本控制和变更控制、保证变更被适当地实施，使开发人员、测试人员、项目管理者、质量保证人员以及客户能方便地通过软件配置管理获得有用的信息。

### 各阶段的任务

|  |  |
| --- | --- |
| 方案确认  会签表 | 项目方案确定阶段会签表得到批准后，项目即正式进入开发实施阶段。 |
|  |  |
| 项目组重构 | 根据实际情况，项目组的人员组成可能会有变动。项目经理应与相关人员一起及时填写资源调用申请表。必要时项目组内应修改项目目标及成员职责。 |
|  |  |
| 设备软件采购齐套  设备软件安装调试验收培 训  ISO9001 | 项目商务组开始按计划进行设备、软件的采购、齐套工作。  项目实施组开始按计划进行设备、软件的安装、调试、培训和验收工作。  项目开发组开始按计划进行开发、测试工作。 |
|  |  |
| 软件/设备  验收单  实施记录  软件错误  报告单 | 实施的过程中，实施人员应保留必要的实施记录。  每项服务完成后或设备到货后，应让客户出具软件/设备/服务验收单。  对于现场发现的软件错误，实施工程师应及时填写软件错误报告单。 |
|  |  |
| 联机调试/系统测试 | 开发实施工作结束后，项目测试组应会同开发实施人员做一次系统的联机调试/系统测试，把系统同《验收规范》做一个比较。 |
|  |  |
| 系统测试  报告 | 项目测试经理及时提交项目联机调试报告。 |
|  |  |
| 联调评审 | 项目经理应组织客户和项目组一起评审系统测试报告。  目的：保证交给客户试运行的系统是符合要求的  评审材料：系统测试报告及相关材料  时间：根据项目情况，可以与其它评审一起进行  签收：项目经理、客户项目经理  参加：由项目测试经理和项目经理协商决定  输出：评审会签表（含问题清单）、评审记录、联调报告 |
|  |  |
| 系统启动  准备  需求冻结 | 评审若没通过，项目组应继续调试系统。  评审若通过，项目组会同客户一起做系统启动前的准备工作。项目经理应与客户协商达成协议，最终冻结需求。客户的需求更改，可以到下一期工程再更改，或进行合同变更。 |
|  |  |
| 保驾运行 | 客户在项目组人员的保驾下运行该系统。客户遇到问题时，保驾人员负责及时解决。 |
|  |  |
| 错误报告单  错误报告单 | 在保驾运行阶段，无论是我们的保驾人员还是客户发现了软件的错误，都应及时填写错误报告单。 |
|  |  |
| 项目人员验证  授权人员批准 | 对于客户发现的错误，保驾人员要首先争取现场验证，以了解更多信息。  对于所有的软件错误，项目组都应先争取授权人员批准，以确定是否更改。 |
|  |  |
| ISO9001/cmm | 如果不改，由保驾人员与客户沟通。  如果更改，由项目开发组执行。 |
|  |  |
| 用户文档  （改进版） | 在保驾运行过程中，项目组及时组织人员编写用户文档，如操作说明书，维护说明书等。 |
|  |  |
| 项目总结  报告 | 在保驾运行期间，项目经理会同项目组相关人员编写项目总结报告。包括：  1、项目目标完成情况总结  2、项目财务分析  3、项目进度与计划比较分析（mpp文档）  4、项目变更总结  5、项目所用产品情况总结  6、项目开发的新功能总结  7、项目设备/软件采购总结  8、项目验收总结  9、项目评审及里程碑事件总结  10、项目问题&对策总结  11、客户满意度分析&总结  12、项目组信息流管理总结  13、项目经验教训总结  14、优秀成员点评 |
|  |  |
| 项目验收  报告 | 在保驾运行即将结束时，项目经理组织相关人员编写项目验收报告。然后与客户协商验收事宜。  评审若通过，项目组会同客户一起做系统启动前的准备工作。项目经理与客户协商达成协议，最终冻结需求。客户的需求变改，在下一期工程中更改，或者立即实施合同变更。 |
|  |  |
| 项目验收 | 在保驾运行快结束时，项目经理应开始与客户项目组协商验收事宜。如系统问题较多，则根据优先级安排人改进。若达到了验收规范，就应与客户项目组及早确定验收会议安排。  如果没通过验收，项目经理根据问题所在，安排人限期解决。如果通过，则双方在验收报告上签字。 |
| 维护通知书 |  |
|  | 验收通过后，公司商务人员及时发给客户正式的维护通知书，告知客户从验收通过之日起，项目进入合同规定的维护期。 |
|  |  |
| Close meeting | 项目经理根据计划召集管理评审——CLOSE MEETING，以评审项目工作，并决定是否结束项目，并交接给服务体系。  目的：  1、正式关闭项目  2、与维护人员交接  3、与维护系统的交接  4、评审项目目标完成情况  5、项目组的评定。  所需文档：项目总结报告及相关文档  召集：项目经理  参加：用户、项目组主要成员，相关领导及管理人员  议程：  1、项目经理介绍情况（简介、目标实现情况、过程）  2、项目经理报告经验教训  3、项目经理报告总结报告的其它重要内容  4、评审人员提问及会议讨论  5、项目发起人宣布结论：项目评价  输出：  1、会议记录  2、遗留问题清单及安排  3、项目评价  4、项目结项公告 |
|  |  |
| 项目  结项公告 | 如果会议决定关闭项目，则项目经理把全部项目资料交运营管理部备案。  运营管理部根据会议结果，拟订并发布项目结项公告。项目进入维护阶段，由服务体系负责。  结项公告内容包括：  1、项目结项时间  2、项目主要目标完成情况  3、感谢支持和配合 |

### 各阶段开始标识

当用户确认并同意该项目实施方案，同时在该阶段评审汇签表上签字后，项目即告正式进入开始阶段。

### 各阶段结束标识

当用户在相关管理评审会签表上签字确认后，项目即从该阶段进入下一个阶段。

## 培训方案

### 培训目的

在项目实施过程中，本着全面共享知识与经验的宗旨，除贯穿实施全过程的用户传帮带外，还会针对工程中的软件配置提出一整套系统的培训方案，以达到如下目的：

通过对本工程的技术协作及系统运行维护人员的培训，使本工程的使用人员能够切实理解和掌握业务系统、计算机软件、数据库等各种基础知识，熟练管理以及维护操作，保证系统完工后能够正常运转，并得到优化的执行。

通过对系统使用者的操作培训，使其熟练使用业务系统，充分发挥系统的作用。

### 培训方式

培训方式采用集中培训，现场培训，热线支持和发放宣传材料等相结合的方式，针对不同层次的人员，开设不同的培训课程。

* 集中授课培训方式：

集中授课培训方式主要是在系统安装调试完毕后，试运行前或正式开通运行前的授课培训，分别针对系统维护人员和系统操作人员，开设集中培训课程。重点是系统维护人员和系统操作人员，采用集中授课的方式，进行培训。

* 现场培训方式：

现场培训方式是指在软件产品到货后和软件系统开发完成后，在系统安装、调试阶段，通过现场实际操作和面对面的单独讲解的方式，使得系统操作人员、系统维护人员能够更深层次的掌握系统各设备的使用、维护以及各种日常操作等。特别时针对项目系统的安装、调试和排错等内容，进行现场指导培训往往比授课讲解的方式更容易让学员记忆、理解和掌握。在项目实施过程中，使用本系统的技术人员可以在培训教师的指导下，对系统进行实际地安装、调试和故障排除。在基础理论培训的基础上，为以后的系统维护工作打下良好的基础。现场培训在实施过程中于用户实施现场进行。在安装前，我方将对用户方技术人员进行初步培训，并通过试验性安装等现场培训手段加强用户技术人员对系统安装调试培训的效果，同时，在安装过程中，用户技术人员可与我方共同参与安装、检测、排除故障等内容的实践。

* 热线支持方式：

通过我公司服务热线提供即时操作咨询。

* 宣传材料方式：

为了扩大宣传的范围，可印制宣传材料在相应的职能部门向用户发放，以便操作人员随时查阅。

### 培训要求

为保证培训的质量，需要客户方配合工作。客户方与实施方共同安排好培训场地及相关境；客户应做好参加培训学员的组织管理工作，包括通知、报到签到工作，安排作息时间等，保证参加培训的学员具备参加培训的资格，以保证培训工作的质量。在培训结束后，将进行考试，对于考试成绩优秀和不合格的技术人员，用户培训工作负责人和我公司的培训负责人应共同制定奖励措施和补救措施，如培训上岗制度等，以保证培训工作的质量。

### 培训内容及计划

根据以上方案，我公司将对用户方的用户和系统管理维护人员等分别进行培训，计划如下（可根据项目实施的实际要求进行变更调整）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **培训项目名称** | **培训内容**  **描述** | **培训**  **人数** | **培训**  **天数** | **培训**  **地点** |
| **1** | **用户培训** | **1、TSM基础知识培训**  **2、TSM系统结构、工作原理**  **3、TSM系统功能操作培训**  **4、常见故障及排除方法培训** | **操作人员**  **培训人数由买方确定** | **1** | **培训地点由买方负责提供，**  **授课方式由买方确定** |
| **2** | **系统管理人员培训** | **1、中间件安装与配置**  **2、数据库安装与配置**  **3、系统安装与配置**  **4、系统权限与角色配置** | **应用系统管理员**  **培训人数由买方确定** | **1** | **培训地点由买方负责提供，**  **授课方式由买方确定** |

## 软件质量保障措施

软件质量保障工作的目的对本系统的实施过程规定各种必要的质量保障措施，以保证项目组所交付的产品能够满足招标书中规定的各项具体需求，同时提供适当的项目可视性评测文档，能够对项目执行的各个阶段有客观的、量化的了解和认识。

软件质量保障措施包括：

### 制定项目计划

软件质量保障活动在项目一启动时就要开始，在策划阶段SQA（质量保证人员）要与项目组通力协作，并在需要时给项目组提供指导和帮助。

当项目与质量管理部为项目所属的部门经理下发《任务通知书》后，项目与质量管理部经理可与项目所属部门经理协商确定项目的SQA人员。

SQA人员还需帮助项目经理针对项目的具体情况对公司的标准软件过程进行裁剪，协助项目经理定义项目的软件过程，为工作产品确定验收标准，并参与项目计划的制定。当项目计划制定完成后，SQA人员还要验证项目计划的可行性。同时SQA人员也可提供项目组所需的技术支持，如项目组决定采用Delphi估算方法对项目的工作量进行估算时，SQA人员可以对参加估算的人员进行有关Delphi估算方法的培训，并以协调人的身份参加估算会议。

SQA人员要确保项目策划过程的有效执行，并检查这些活动与相关程序文件要求的一致性。

### 9.3.2 制定质量保障计划

SQA人员在参与制定项目策划的同时制定软件质量保障计划。

软件质量保证计划应包括如下内容：

1、明确质量保证的目的、范围及质量保证计划与其它项目计划的关系；

2、描述软件质量保证的组织、权限和责任；

3、描述质量保证人员如何参与支持项目策划和开发活动；

4、确定SQA人员实施评审的过程，其中应写明需要评审的过程、该过程的进入退出条件以及评审时需要的相应检查列表；

5、确定SQA人员实施审计的工作产品，其中应写明需要审计的工作产品及审计时所需规范；

6、制定有关处理不符合项的规程；

7、确定SQA人员向相关小组汇报有关活动的方法和频度；

8、制定项目SQA活动的进度表；

9、SQA组的资源需求（包括人员、工具、设备、设施和培训）；

10、软件质量保证计划编写完成后，应与其他项目计划一道进行审批；

11、批准后的软件质量保证计划应通知到所有相关的组和个人。

### 9.3.3 制定软件系统测试﹑考核制度

1、拟制测试大纲，并严格按测试大纲进行系统测试。

2、详细记录系统测试过程，并保留记录。对于测试中发现的问题认真记录并形成问题报告。指定专人对问题进行跟踪、解决。

3、系统测试后，检验人员要依据检验规范写出检验报告，保证产品满足用户的要求。

### 9.3.4 软件质量控制

对软件的质量控制贯穿软件开发的全过程，主要包括以下内容：

1、需求评审

(1) 向业主、监理机构提交需求调研的相关文档，包括《会议调研报告》和《需求规格说明书》。

(2) 如果用户认可本轮需求基本满足了其使用要求，签字认可结束本次迭代的需求工作，否则需要进一步修改原型，重新开始本阶段。

2、详细设计评审

(1) 业主组织用户代表对《需求规格说明书》进行评审。

(2) 评审通过后，用户签字认可结束详细设计阶段，否则需要进一步修改详细设计。

3、测试

为保证系统质量，在项目中将测试纳入质量保证活动，主要进行关键模块代码的代码走查和系统测试。

(1) 关键模块的代码走查

遵循“项目质量保证大纲”中的有关规程，在系统开发过程中，质量保证组组织人员以通过评估后的“软件设计说明”文档为依据，对软件开发组提供的关键代码模块实施代码走查，看其是否正确地实现了“软件设计说明”文档中描述的相应模块的设计，与其他有关模块的接口设计以及其他特性（如模块的规模、输入输出等）。

代码走查结束后提交问题报告，质量保证组对问题的修改进行追踪控制。

(2) 系统测试

遵循项目“质量保证大纲”中的有关规程，以通过评估后的“系统需求规格说明”文档和软件开发组提供的用户手册等为依据，对整个系统进行功能、性能的检测。

在实施测试前，测试人员应编写测试说明（包括测试规程、数据样本），测试说明应覆盖全部“系统需求规格说明”。

质量保证组组织人员对《测试说明》进行评审。

测试人员依据评审过的《测试说明》对整个系统进行测试，记录测试过程中的问题，在一轮结束后提交问题报告。以下是控制测试流程的 主要措施：

(1) 错误的跟踪与记录

对测试中发现的每一个错误均按专门的格式记录在数据库中。测试记录包括对错误的详细描述、错误发生的条件和现象、错误分类（需求错误、设计错误、编码错误、接口错误、数据库错误、通信错误等）、严重性（灾难性、破坏性、性能性、一般性、便利性、轻微性）、状态（新建、已修改、重测失败、完成）等信息。利用缺陷跟踪管理工具跟踪错误，避免遗漏和混乱。

(2) 问题的提交、修改与回归测试

一轮测试中发现的问题分批返给系统开发组。一轮测试完成后提交完整的测试记录，并对发现的错误进行分类、统计和分析，形成软件问题报告。严重错误将及时报告给项目质保部门。一轮测试完成之前不接受系统开发组提供的更新版本。

开发组完成修改工作后，修改说明书提交测试方进行回归测试。修改说明书应详细说明修改了的错误、更新了的组件、可能受修改影响的组件等。未能修改的错误应说明原因，必要时交质保部门决策。

测试组收到更新版本后，开始作下一轮回归测试。回归测试是全面回归测试，以确认修改是否引入新的错误。

(3) 确定测试状况

根据完善的测试计划和测试用例说明以及详细的测试记录，可以确定测试状况，了解哪些测试用例已经测过，哪些还未测过，已测过的功能或部件所花费的时间和代价等，从而有效地掌握测试的进程。测试组每轮测试结束后将测试现状和进度向质量保证组报告。

## 应急响应服务

### 应急响应情况分类

当应用系统出现下列情况之一，就需要进行应急响应情况处理：

1、应用系统24小时内不能正常运行，严重影响项目涉及的相关单位的日常业务；

2、发生灾难性事件，由人为灾难或自然灾害的发生造成的应用系统不能正常运行，严重影响相关单位业务工作的正常运行；

3、爆发大规模病毒事件，造成了涉及的应用系统不能正常运行，且36小时内不能恢复正常运行导致的系统瘫痪，严重影响相关单位业务工作的正常运行。

### 应急响应处理流程

应急响应预案是本公司按照故障排除服务制定在系统严重故障造成某些应用无法正常运行等突发情况下制定的应急响应处理流程。当出现人为或自然灾害造成的严重影响相关单位业务工作正常运行并一时难以恢复的系统破坏性事件，本公司将启动按照应急响应预案，主要包括人员组织分工、应急处理流程及应急措施和故障恢复等内容，并进行仿真环境下的演练。

### 应急响应人员组织管理体系

对于上述系统严重故障情况，本公司有着一套成熟高效的应急响应人员组织管理体系：

提供24小时开机的服务工程师和项目经理；

由公司领导、项目经理和售后技术支持与维护服务负责人组成的应急响应领导小组；

应急响应领导小组每天向公司领导汇报项目处理进展，每小时更新应急响应处理的相关记录。

应急响应小组能快速调动相关资源，与其他设备提供商和应用软件提供商联合起来分析解决问题，防治处理环节出现延时，及时排除故障，保证系统正常运行。

### 安全事件应急响应措施

具体流程包括以下内容：

(1) 安全应急流程建立—建立安全基线

(2) 事件识别

(3) 缩小事件影响范围

(4) 事件解决

(5) 后续报告与处理机制

(6) 补救措施

## 项目管理方案

我公司在成功实施ISO9001以及CMM后，已形成了自己独特的项目与质量管理体系，对项目过程中的策划活动、跟踪与监控过程、软件配置管理、软件质量保证、同行评审等活动的实施过程都进行了规定，以加强对项目的管理和控制，保证产品质量。本项目将采用这些规定的过程对项目的实施进行管理和控制。

考虑到本项目所处行业的特殊性以及建设期的紧迫性，而且需要充分保证开发项目的质量，并满足客户的要求，因此有必要结合项目本身的特点对项目管理过程作一个系统的阐述，具体说明如下：

### 项目管理目标

本项目的项目管理方案遵循用户方提出的管理要求及我公司质量管理体系的规定，结合ISO9001和CMMI三级的要求来实施项目管理。

项目策划活动包括明确项目范围、确定项目的组织结构、选择项目的生命周期模型、定义项目的实施过程、对项目任务进行拆分并识别项目工作产品、进行估算（规模、工作量、进度估算等）、制定险管理计划、培训计划等活动。项目策划的结果将形成文档化的项目计划，包括软件开发计划、配置管理计划、质量保证计划、培训计划等。这些计划将被提交给用户方以及公司高层管理人员进行审批，我方将按照批准后的项目 计划开始项目的实施工作。

### 项目管理工具

实施工程所需要的工具很多，包括过程和项目管理工具、需求分析工具、设计与构建工具、配置工具、软件质量工具等类型的工具。

项目在开发和管理过程中，将选择成熟的项目管理工具或者开发工具来提高工作效率，并对建模工具提出要求：

参照工程的总体进度计划，采用Microsoft Project编制分计划；

软件的设计建模过程中，要选择支持UML语言规范的工具。如：Rational ROSE。

### 项目协调及沟通管理

**1、与业主的配合措施**

实施中主动征求业主的意见，接受业主的指导、协调管理。

签订廉政协议、安全生产文明实施协议，交纳安全生产文明实施保证金。

建立工作联系制度，按时参加项目联络会议，沟通项目情况，及时向业主建设进度和建设中出现的问题。

优质高效安全地完成实施任务，让业主放心，让接管单位满意。

在业主组织的实施协调会议上，及时汇报实施中所出现的问题，协同各方专家分析、解决问题。认真落实每次协调会会议精神。

**2、与监理单位的配合措施**

实施中严格执行项目质量监理工作的各项规定。

主动配合监理工程师的工作，自觉接受监理工程师的检查指导，随时听从监理工程师代表业主对我单位项目实施和管理的意见。

及时正确地向监理单位上报各种报表，不影响监理的日常工作。

积极参加由监理主持的项目协调会，并提出有利于项目实施的意见。

积极配合监理，做好项目实施过程中的质量检验工作。

不虚报数量，如实做好项目计量，取得监理认可。

# 售后服务及技术支持

## 技术支持服务总体说明

本项目相关的技术支持与售后服务将由我司的技术支持与售后服务中心统一提供。我司技术支持与售后服务中心（以下简称“支持中心”）是公司专门为系统集成项目所设的常设服务机构，支持中心具备专业的服务水准、专业设备和实验环境，以及覆盖全国主要大中城市的本地服务团队、备件库，同时具有稳定的技术支持队伍，并通过了ISO9001质量体系认证。

在项目建设过程中，我公司将与用户和运行维护单位进行密切沟通，充分考虑用户使用和系统长期运行维护的需要，并且根据业主要求，提供与工程建设相关的技术服务。

在系统试运行阶段，我公司将派至少一名工程师在专职进行全程跟踪，提供全面技术支持服务，确保试运行的顺利进行，达到检验系统、完善系统的目的。在系统竣工验收，进行正式运行后，我公司将提供 支持服务。

技术支持服务具体期限及支持方式见下：

### 质量保证期内的售后服务

在系统保修期内，公司提供的技术支持与售后服务内容主要包括：电话支持、远程支持、现场服务、设备维修与更换、系统故障报告和预防、软件版本升级与增强、后期技术培训等。公司将通过7×24小时热线电话、传真、电子邮件等多种灵活的联系手段为用户提供全时的响应服务。同时，公司在项目单位所在地均设有本地分支机构，通过以上分支机构的本地技术支持服务团队，公司能够向用户提供及时、有效的现场支持服务。

1、质量保证期：质量保证期为系统最终验收后36个月（三年），其中免费现场技术支持期限为36个月（三年）。

2、质保期内，我公司提供免费的技术支持服务，解决所提供软件系统及其附件、安装介质的任何故障，并根据用户的使用要求，不断修改、完善系统。

3、质保期内，提供7X24小时的实时技术支持响应，每年提供1次系统巡检，并提供书面巡检报告。

4、质保期内，系统发生故障时，对本地用户（武汉市内）我们将在1小时内作出实质性响应，在2小时内提供解决此类问题的紧急预案方案，在8小时内到现场解决故障问题恢复系统正常运行，故障处理完后提供故障分析及处理报告。

5、质保期内，对我方开发的软件和自有产品，提供免费升级；对采购的软件产品，依照招标要求，我方将提供3年的免费升级。

6、质保期内，若用户系统需要迁移，我们将提供免费安装部署服务，若因迁移服务造成系统运行异常或故障，由我们负责免费修复。

7、在质保期内，我方如不能在上述承诺响应时间内作出反应和修复故障，则每超出一天按照合同总价的0.1%提供赔偿。

### 质量保证期外的技术支持与服务

质量保证期后，公司承诺提供以下技术支持服务：

1、免费维护期后，提供优惠的软件系统升级支持。对于我方开发的软件，我们将优惠为客户进行软件版本升级服务。对于第三方厂家提供的系统软件、应用软件版本升级时，只收取成本费。

2、永久提供免费热线技术支持。

3、免费维护期后，我方有义务在系统的建设、升级、维护和日常运行管理方面继续给予技术协作和咨询，继续为系统使用单位提供维护服务。如用户需要进行工作量较大的系统迁移或复杂的应用安装，或建设新应用系统需要与我方设计开发的软件进行联调对接等工作需要我方支持时，我们可以提供技术咨询服务，也可以以优惠的价格提供的现场技术服务。

4、保修期满后，公司将以优惠的价格继续为本项目提供全面的技术支持与服务，其内容将主要包括7×24小时的热线电话支持、远程支持、现场服务、设备维修与更换、系统故障报告和预防、软件版本升级与增强、技术后援支持、系统专项维护、系统功能扩充或改造、技术培训等。由于保修期后的服务价格及技术状况的不确定性，我们承诺将继续根据用户的需要以最优惠的价格提供上述服务。保修期后技术支持与服务的方式、范围、响应时间等参照保修期内的技术支持的方式、范围、响应时间等执行。

## 技术支持服务组织

项目验收后，其技术支持与售后服务将由公司支持与售后服务中心承担。

通过服务机构整合和覆盖，我们已经建立了全国分布式的服务体系，能够为全国性、地区性大客户提供全面的技术支持和专业服务。服务体系不仅向我们现有的和潜在的重要客户提供技术咨询、承担我们与客户签定的重要项目合同的实施及技术服务，同时也面向各行各业的关键应用、根据与客户签定的技术服务合同的要求提供专业技术服务。我们的服务体系能够向用户提供每周7天、每天24小时的专业技术支持。

公司技术支持与售后服务中心是公司专门为项目技术支持所设的常设机构。服务体系目前有近200名专业技术服务人员，其中华中地区有约80人，平时中心由1名中心经理、多名软、硬件件技术专家组成的一线工程师以及二线工程师（职责分工见“支持中心工作规范”）组成，将在系统验收后服务期内作为受理和响应人员与项目组成员共同提供支持服务，他们是客户与公司的接口，该中心有责任与义务处理售后服务中出现的任何问题，并将协调公司其它部门的关系，很好地完成售后服务的各项任务。

作为服务体系的代表和核心，技术服务中心是我们主要面向具有关键任务应用的客户提供专业技术服务的专门机构。

技术服务中心由设在北京的服务管理部、网络技术服务部、主机和数据库技术服务部、信息安全技术服务部、售前技术支持部及分布在全国的八个区域分支机构等部门组成。其中，服务管理部负责对各地服务工程师、设备保修/维修人员向用户提供的服务进行管理和监督，同时通过服务跟踪系统监控服务响应的过程、时效和客户的反馈；其他各部门提供相应专业技术的支持和服务。

技术服务中心对用户的服务通过两级方式实现：由分布于全国各地的技术服务工程师提供一线技术支持和服务，以便尽可能提高响应效率；位于技术服务中心的各专业技术部门提供后台支持，并在必要或紧急的情况下配合本地服务工程师对客户提供直接服务。

技术服务中心的服务工程师中大部分都是具有多年关键应用工程项目实施和技术支持及服务背景的资深技术专家。曾经承担过许多大型项目的售前、售后技术支持和服务。

## 技术支持服务质量控制

### 服务质量保证体制

客户服务部门专门负责接收客户的各类问题，将问题进行分类、转发给相关部门、负责跟踪问题解决的过程、调查客户满意度；

建立专门的项目风险维护基金, 为所有软件维护项目提供资金支持，平衡个别项目服务费不足的矛盾，业务管理部负责管理公司项目风险维护基金的使用、协助解决客户投诉。

建立完善的维护服务过程文档，维护人员都按照标准化的方法进行工作，为每一次维护服务都建立了服务质量记录，记载了解决问题的过程、结果和客户满意程度。

### 客户投诉处理

公司建立完善的客户投诉处理制度，处理客户以书面、电话或其它形式直接向公司人员或公司部门明确表示不满或索赔，起诉等事件，并作为对部门或人员的考核依据。

服务品质将由客户服务中心提供保障，服务中心设立有热线投诉电话，网点和中心对服务支持有任何不满时，均可直接向该中心投诉。该中心将详细记录投诉内容，并保障48小时内将处理结果通报投诉者。接到客户投诉后，客户服务中心将详细记录投诉内容，并保障48小时内将处理结果通报客户。

客户投诉管理流程：

1、公司任一部门或任一员工接到客户投诉信息后应该立即接待，详细记录事由及对方联系方式，及时交由客户服务部处理。

2、客户服务部对接到的客户投诉信息及时进行分析，在一个工作日内对客户做出电话反馈，同时确定投诉的责任部门，并做立项登记，填写《客户投诉立项登记表》。

3、客户服务部负责成立专门处理小组并报公司总经理室确定小组负责人，启动处理，全面协调内外部关系。

4、处理小组成立后，负责人应在最短时间内给客户慰问电话，表示公司对此事的重视与关注，同时告之客户解决渠道和联系方式，表明公司已经正式受理此事，投诉已在处理之中。

5、处理小组负责投诉级别的判定。

6、客户服务部门全程参与投诉处理，对于一般事故以上（含一般事故）的投诉客户服务部至少一个月与客户联系一次，并视必要程度增加与对方的联系频度，掌握处理进度的最新动向，认真填写《客户投诉处理跟踪表》，并适时向软件公司总经理室汇报处理情况或申请决策支持。

7、客户投诉处理结束后，由客户服务部组织人员对客户进行回访，向公司总经理室提交处理总结，并做结项登记，填写《客户投诉结项登记表》。

## 技术支持与服务内容

### 现场安装、调试

在项目建设后期，本公司负责形成系统的软件包；提交项目验收所需技术文档；到现场安装调试；协助业主方开展试运行工作，直至全系统投入业务运行。

### 质量保证期及保修服务

项目验收后，本公司提供范围免费售后技术支持，本公司有责任与义务处理售后技术支持中出现的任何问题，并将协调公司其他部门的关系，妥善完成服务中的各项任务。

#### 定期跟踪

系统上线运行后，公司除了定期通过电话跟踪系统的使用情况和存在的问题之外，还将定期派遣技术人员听取意见和建议，解决存在的问题。通过和系统管理员一起对系统运行日志等信息进行分析，了解系统的运行情况，及早发现系统可能存在的问题隐患。

#### 状态报告和故障预测

在保修期内，在征得用户同意的条件下，本公司工程师可现场对设备进行检查，对网络现状做出评估，预测可能出现的故障，并提出预防策略以及提高网络性能的优化建议。

#### 优化系统

虽然在系统测试时做过性能优化，但在实际运行时，公司还将根据业务运行情况、网络情况，继续对CPU、内存、系统参数提供优化建议，确保系统随着业务的发展能够持续、稳定、高效地运行。

#### 应用系统维护

应用系统维护包括对应用系统的维护、应用系统运行中的关键日期的技术支持、应用系统集成工作进行纠错性维护和适应性维护。

对应用系统的维护包括对错误的诊断排除、对验收报告中明确需要在维护阶段完善的业务功能的实现；在关键日期之前，应用系统责任工程师应配合服务中心的业务测试人员对关键程序做模拟测试，抽样检查应用系统数据的正确性，并在关键日期当日在操作现场，协助业务人员核对结果。

#### 故障排除服务

为客户提供远程和现场的故障诊断和故障处理服务，包括设备的故障诊断及处理、基础软件的故障诊断及处理、应用系统的故障诊断及处理、 接入网络系统的故障诊断及处理等。

提供7\*24小时故障处理支持，故障处理时限：

|  |  |  |  |
| --- | --- | --- | --- |
| 主要故障情况分类 | 响应方式 | | |
| 电话响应 | 人员到现场 | 故障排除时间 |
| 产品主要功能不可用 | 30分钟内 | 2小时内 | 到现场后2小时内 |
| 产品主要功能运行缓慢 | 30分钟内 | 2小时内 | 到现场后4小时内 |
| 产品次要功能不可用 | 1小时内 | 4小时内 | 1个工作日内 |

#### 应急响应服务

制定在设备严重故障造成某些应用无法正常运行等突发情况下，应用系统的应急预案，应包括人员组织分工、应急报告流程、故障分类及应急措施和故障恢复等内容，并进行仿真环境下的演练。

对于严重的故障启动应急处理流程，在最快的时间内排除故障，解决问题。

### 远程服务

在网络信息时代，远程支持服务是售后技术支持与维护服务的一个重要组成部分。本公司拥有一批经验丰富的售后工程师，并且在多年积累的基础上建立了内容丰富的故障数据库，能够帮助用户快速找到故障原因并找到解决的办法。

远程支持服务可以通过电话、传真或互联网技术等方式，为用户解决产品相关的问题，保证做到7×24小时维护响应。

#### 热线服务

为了更好的服务于用户，如果客户的系统发生故障或者需要技术咨询服务的时候，公司客户服务中心得到通知后立即会通过电话了解情况并提供远程技术服务，最迟在1小时以内做出反应、4小时内做出答复。

#### 其它远程服务

对于在热线电话中无法解决的问题，售后服务人员会根据情况采取以下方式给予及时回复：

*  Email或传真等方式

如果需要以电子文件的方式提供，售后服务人员会根据用户提供的Email地址或传真等方式，最迟在1小时以内做出反应、4小时内做出答复。

响应的内容一般包括：非紧急情况下的升级或更新软件的提供，用户需要的产品说明、操作指南等文件及其他。

*  远程在线诊断和故障排除、预测：

对于电话咨询解决不了的问题，经用户授权我们可通过电话或Internet远程登录到用户网络系统进行免费的系统优化、参数调整、故障诊断和故障排除。为保证本系统的安全性，此方式可以临时申请和完成后即刻取消权限。

在保修期内，在征得用户同意的条件下，本公司工程师可定期通过远程方式监测用户网络系统的运行状况，或现场对设备进行检查，对网络现状作出评估，预测可能出现的故障，并提出预防策略以及提高网络性能的优化建议。