|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OTA安全管理系统项目**  **概要设计说明书**      **天津三源电力智能科技有限公司**  文档修订记录   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **序号** | **版本号** | **修改时间** | **修改人** | **审核人** | **批准人** | **备注** | | 1 | V1.0 | 2022/1/5 | 何恩超 | 孙剑 | 孙剑 | 创建 | | 2 | V1.1 | 2022/1/7 | 何恩超 | 孙剑 | 孙剑 | 根据评审内容调整。 | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |

**目 录**

[1导言 1](#_Toc19687)

[1.1目的 1](#_Toc27822)

[1.2范围 1](#_Toc5536)

[1.3命名规则 1](#_Toc20710)

[1.4术语定义 1](#_Toc20468)

[1.5相关文档 2](#_Toc1693)

[2项目概况 2](#_Toc13272)

[2.1项目描述 2](#_Toc12918)

[3总体结构 3](#_Toc30174)

[3.1总体结构图 3](#_Toc14154)

[3.2功能结构图 3](#_Toc13255)

[3.3用户组成图 4](#_Toc4351)

[3.4业务流程 4](#_Toc636)

[3.4.1加密处理业务流程图 5](#_Toc20233)

[3.5运行环境设计 5](#_Toc4361)

[1 服务器操作环境 6](#_Toc29698)

[3.6设计目标 6](#_Toc12377)

[3.6.1总体原则 7](#_Toc27393)

[3.6.2实用性和先进性 7](#_Toc19890)

[3.6.3标准化、开放性、兼容性 7](#_Toc2193)

[3.6.4高可靠性、稳定性 7](#_Toc7759)

[3.6.5易用性 7](#_Toc31864)

[3.6.6灵活性和可扩展性 8](#_Toc27781)

[3.6.7经济性和投资保护 8](#_Toc691)

[4功能模块设计 8](#_Toc15191)

[4.1业务模块功能分配 8](#_Toc21841)

[4.2模块的具体实现 9](#_Toc23399)

[4.2.1.1密钥管理 9](#_Toc11786)

[4.2.1.2固件管理 9](#_Toc9375)

[4.2.1.3策略管理 11](#_Toc24018)

[4.2.1.4安全审计 12](#_Toc25107)

[4.2.1.5统计分析 12](#_Toc29107)

[5性能设计 15](#_Toc10717)

[5.1系统性能 15](#_Toc22443)

[5.2资源使用率 15](#_Toc26894)

[5.3信息安全 15](#_Toc19310)

[5.4可靠性 16](#_Toc27620)

[5.5易用性 16](#_Toc21044)

[5.6互用性 16](#_Toc11486)

[5.7移植性 16](#_Toc1535)

[5.8扩展性 16](#_Toc18804)

[5.9维护性 17](#_Toc13303)

[5.10合法/合规性 17](#_Toc12663)

[6接口设计 17](#_Toc11988)

[6.1接口设计原则 17](#_Toc3671)

[6.2接口实现方式 17](#_Toc32110)

[6.2.1外系统开放数据库、本系统调用 17](#_Toc2550)

[6.2.2本系统提供接口、本系统调用 18](#_Toc3815)

[7运行设计 18](#_Toc6313)

[7.1运行模块的组合 18](#_Toc10510)

[7.2运行控制 18](#_Toc18577)

[7.3运行时间 18](#_Toc10982)

[8维护设计 18](#_Toc26744)

[8.1出错处理设计 18](#_Toc19588)

[8.1.1出错输出信息 19](#_Toc10958)

[8.2安全保密设计 19](#_Toc3730)

[8.3维护设计 20](#_Toc19853)

# 1导言

本章对该文档的目的、功能范围、术语、相关文档、参考资料、版本更新进行说明。

## 1.1目的

本系统主要为OTA安全管理系统，为终端设备OTA升级包提供安全保护，保证OTA升级过程信息安全。系统分为五个模块，分别为：密钥管理模块、固件加密模块、策略管理模块、安全审计模块、系统管理模块。密钥管理模块可对密钥进行全生命周期管理，并支持密钥的加密导出及公钥复制。固件加密模块可对固件包进行增删改查管理，以及配置相应的策略模板对固件包进行加密或签名操作，加密完成后的固件包可以导出。策略管理模块为固件包处理提供策略模板，可对策略模板进行增删改查管理、设置系统默认模板等。安全审计模块为系统各类审计日志，包括登录日志、操作日志、固件处理日志，可对日志进行查询、导出等操作。系统管理模块包括用户管理、权限管理、机构管理以及系统配置，可进行基本的管理功能以及系统配置项修改功能。

## 1.2范围

本系统的建设主要为开发OTA安全管理系统，系统采用B/S架构，包含服务端后台程序及前端程序的开发，本文档对其中各部分进行了详细的功能定义，本系统的建设应严格遵守本文档中定义的全部内容。

## 1.3命名规则

1. 变量对象命名规则

申明全局变量、局部变量对象的命名规则。

1. 数据库对象命名规则

申明数据库表名、字段名、索引名、视图名对象的命名规则。

## 1.4术语定义

|  |  |  |
| --- | --- | --- |
| **序号** | **术语名称** | **术语定义** |
| 1 | 总体结构 | 软件系统的总体逻辑结构。按照不同的设计方法，有不同的总体逻辑结构。若采用传统的面向功能或面向数据的结构化设计方法，则总体逻辑结构为一树形的功能模块结构图。若采用时尚的面向对象或面向部件（组件）的设计方法，则总体逻辑结构为部件（组件）的组装图。 |
| 3 | 数据结构 | 数据结构包括：关系数据库表的结构、对象数据库表的结构、变量说明。 |
| 4 | 概念数据模型 | 关系数据库的逻辑设计模型，叫概念数据模型。主要内容包括一张逻辑E--R图及其相应的数据字典。 |
| 5 | 物理数据模型 | 关系数据库的物理设计模型，叫物理数据模型。主要内容包括一张物理表关系图及其相应的数据字典。 |
| 6 | 视图 | 在基表之上建立的一张虚表，叫视图，它具有物理表的许多性质，在授权上很有用。 |
| 7 | 角色 | 数据库中享有某些特权操作的用户，叫角色。 |
| 8 | 子系统 | 具有相对独立功能的小系统叫子系统。一个大的软件系统可以划分为多个子系统，每个子系统可由多个模块或多个部件组成。 |
| 9 | 模块 | 具有功能独立、能被调用的信息单元叫模块。模块是结构化设计中的概念。 |
| 10 | 部件（组件） | 具有功能独立、能被调用的、且已包装的信息单元叫部件（组件）部件是面向对象设计中的概念。 |
| 11 | 内部接口 | 软件系统内部各子系统之间、各部件之间、各模板之间的接口，叫内部接口。接口描述包括：调用方式、入口信息、出口信息等。 |
| 12 | 相关文件 | 相关文件是指：当本文件内容变更后，可能引起变更的其它文件。如需求分析报告、详细设计说明书、测试计划、用户手册。 |
| 13 | 参考资料 | 参考资料是指：本文件书写时用到的其它资料。如各种有关规范、模板、标准、准则。 |

## 1.5相关文档

《OTA安全管理系统系统需求规格说明书》

# 2项目概况

## 2.1项目描述

目前车联网行业发展迅速，软件定义汽车的态势明显，ECU固件、TBOX固件、IVI固件、IVI应用程序等各种固件程序、软件程序都以OTA的方式进行升级。OTA升级方式在端-管-云模式的应用场景中发挥着巨大的作用。

由于目前大多数主机厂及物联网厂商在对前端设备的OTA升级过程中并未采取安全措施保证升级包的保密性、完整性，导致不法分子有可能在升级过程中植入非法程序，对用户的人身安全、隐私安全造成威胁。

我司专注物联网、车联网信息安全，经过前期的市场调研、可行性分析以及用户的沟通，立项研发OTA安全管理系统，对OTA升级过程提供安全保护，保证升级包的保密性、完整性，保护用户安全。

# 3总体结构

## 3.1总体结构图



## 3.2功能结构图

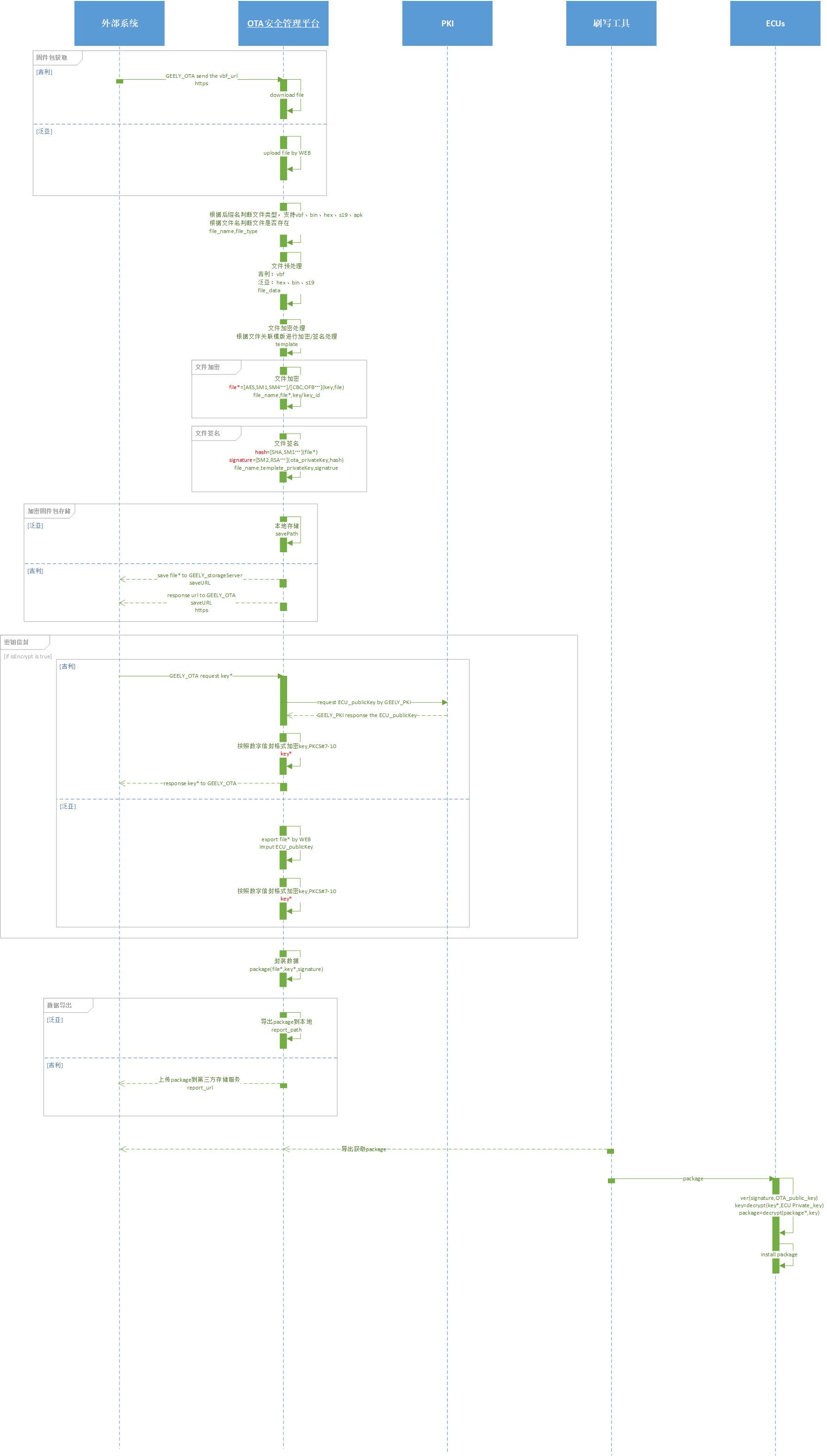


## 3.3用户组成图



## 3.4业务流程

### 3.4.1加密处理业务流程图

**

## 3.5运行环境设计

### 服务器操作环境

|  |  |
| --- | --- |
| 分类 | 选型原则 |
| 技术选型 | * CentOS 7.6 * Java EE 8 * Servlet 3.0 * Apache Maven 3 * Spring Boot 2.1 * Spring Framework 5.1 * Spring Security 5.1 * Apache MyBatis 3.4 * Hibernate Validation 6.0 * Alibaba Druid 1.1 * Vue 3.0 * Axios 0.18 |
| 部署模式 | 前后端分离式集群部署 |
| 开发平台 | Windows 10 64Bit |
| 运行平台 | Centos7等主流服务器操作系统 |
| 容器中间件 | JDK 1.8.0\_281 (x64版本) nginx-1.15.10、 |
| 数据库 | mysql-5.7.21-linux-glibc2.12-x86\_64 |
| 开源组件 |  |

## 3.6设计目标

本系统主要为OTA安全管理系统，为终端设备OTA升级包提供安全保护，保证OTA升级过程信息安全。系统分为五个模块，分别为：密钥管理模块、固件加密模块、策略管理模块、安全审计模块、系统管理模块。密钥管理模块可对密钥进行全生命周期管理，并支持密钥的加密导出及公钥复制。固件加密模块可对固件包进行增删改查管理，以及配置相应的策略模板对固件包进行加密或签名操作，加密完成后的固件包可以导出。策略管理模块为固件包处理提供策略模板，可对策略模板进行增删改查管理、设置系统默认模板等。安全审计模块为系统各类审计日志，包括登录日志、操作日志、固件处理日志，可对日志进行查询、导出等操作。系统管理模块包括用户管理、权限管理、机构管理以及系统配置，可进行基本的管理功能以及系统配置项修改功能。

### 3.6.1总体原则

1、统一总体设计：遵循“统一设计、统一规划、统一实施，统一建设”的原则，加强规范化、标准化，确保各建设项目的实施过程符合总体架构设计。

2、符合标准要求：符合信息安全、汽车行业相关规范标准标准规范。

3、整合现有资源：充分利用现有技术能力和现有技术框架。

### 3.6.2实用性和先进性

采用先进成熟的技术满足用户使用需求，兼顾其他相关的管理需求，使整个系统在相当一段时期内保持技术的先进性，而不至于落后，以适应现代科技和信息化技术快速发展的大趋势和大方向。同时，用户在短时间内不必再为系统的升级而开销，有效的保护了用户投资。在保证系统先进性的前提下，也要充分考虑系统的实用性，毕竟只先进不实用的系统不是用户真正需要的，最大程度的满足用户建设需要、贴合用户使用需求，才能满足用户的实用性要求。

### 3.6.3标准化、开放性、兼容性

选择标准、开放的技术和应用标准，软件协议上真正实现开放，同时基于开放式标准，坚持统一规范的原则，实现标准化、模块化，从而为未来系统的开放、兼容、发展奠定基础。

### 3.6.4高可靠性、稳定性

业务系统的运行，高可靠性是第一位的。要对系统架构进行高可靠性的设计和建设。采用冗余、分布式、集群、热备等相关的技术手段，为整个系统的稳定运行保驾护航。

### 3.6.5易用性

系统建成后是否能让用户使用人员很快上手，这直接关系到系统的使用效率。因此，在系统建设中，必须坚持系统的易用性原则。在系统的操作和控制方式上，尽可能通过技术手段，使得操作人员可以快速掌握系统的使用。

### 3.6.6灵活性和可扩展性

考虑到未来业务的调整及快速发展，系统结构要层次化、模块化，易于未来应用的扩展。现代化的系统应该是一个不断发展、与时俱进的系统，所以它必须具有良好的灵活性和可扩展性，能够根据用户不断发展的业务需要，方便灵活的进行扩展和升级，并提供技术升级、设备更新的灵活性。

### 3.6.7经济性和投资保护

应以较高的性能价格比构建系统，无论是技术的选择上还是系统的构建上，使资金的产出投入比达到最大值。能以较低的成本、较少的人员投入来维持系统的正常运转，以体现系统的高效能与高效益。并且在不影响系统改造目标的前提下，尽可能保留和延长现有系统运行，以充分利用以往资金与技术方面的投入。

# 4功能模块设计

具有功能独立、能被调用的信息单元叫模块。模块是结构化设计中的概念，部件是面向对象设计的概念。

模块功能分配的目的，就是为了将具有相同功能的模块合并，从中提取公用模块，形成公用部件，作为本系统的公用资源，甚至作为公司级组织的公用资源，从而优化系统设计，加快开发速度，提高开发质量。

## 4.1业务模块功能分配

|  |  |  |  |
| --- | --- | --- | --- |
| **模块编号** | **模块名称** | **模块详细功能分配** | **模块的接口标准** |
| M 1 | 密钥管理模块 |  |  |
| M 2 | 固件加密模块 |  |  |
| M 3 | 策略管理模块 |  |  |
| M 4 | 安全审计模块 |  |  |
| M 5 | 系统管理模块 |  |  |
| M 6 | 统计分析 |  |  |

## 4.2模块的具体实现

### 4.2.1.1密钥管理

* **业务描述**

用于固件的加密、签名密钥的管理。可查询系统中已存在的密钥，可在页面中点击生成按钮选择密钥类型手动生成新密钥，可删除没用的密钥，可导出非对称密钥的公钥。

* **功能描述**

主要包括：密钥查询、密钥生成、密钥删除、密钥导出、密钥导入功能。。

1. **密钥查询**

可通过对密钥名称、密钥类型过滤查询、密钥名称支持模糊查询、密钥类型支持级联选择；

1. **密钥生成**

通过页面密钥参数指定可以生成多种类型的密钥（对称密钥、非对称密钥）。手动生成时需配置密钥名称（必须项）；选择密钥类型支持级联选择；密钥的软生成/硬生成方式遵循系统当前密 钥管理机制；

1. **密钥删除**

删除指定密钥。当密钥没有任何固件/模版使用时可删除，否则删除失败，页面提示失败原因；

1. **密钥导出**

仅非对称密钥支持导出，点击导出按钮后自动将公钥复制到系统剪贴板

* **使用对象**

业务操作员

### 4.2.1.2固件管理

* **业务描述**

通过上传指定格式的固件，对固件解析处理，选取指定策略对固件文件进行加密、签名或者既加密又签名处理。未处理的或者处理完成的固件可以进行删除处理，处理后的固件的可以导出原始文件或则密文或签名信封。

* **功能描述**

主要包括：固件获取、查看详情、固件预处理、固件存储、固件导出、固件删除、固件加密处理、固件加密处理策略功能。

1. **固件获取**

可通过页面手动上传或外部接口调用方式传入原始固件包；导入时支持对固件包文件类型进行判断，仅支持vbf、hex、bin、s19、apk五种类型。

1. **查看详情**

可查看固件包解析方式、加密处理策略、加密处理耗时

删除指定密钥。当密钥没有任何固件/模版使用时可删除，否则删除失败，页面提示失败原因；

1. **固件预处理**

通过固件导入时选择的解析方式实现；支持根据文件后缀名自动关联系统对此类格式文件支持的所有解析方式；

1. **固件存储**

支持存储到本地路径；

1. **固件导出**

签名操作导出原始固件包及签名文件；加密操作导出加密固件包及密钥信封（需导入保护密钥）；签名并加密操作导出加密固件包、签名值及密钥信封（签名值在密钥信封内）；支持对接外部接口导出；

1. **固件删除**

正在处理中的固件包无法删除；删除后除相关日志记录之外，原始固件包、加密固件包、签名值等信息均不保留；

1. **固件加密**

可配置加密处理的策略；可统计加密、签名的耗时；支持可视化显示处理的进度；处理失败时可通知用户处理失败；

1. **固件加密处理策略**

* **使用对象**

业务操作员

### 4.2.1.3策略管理

* **业务描述**

固件在进行加密时可以选取不同的策略，实现使用不同的策略（加密、签名、加密又签名）或者不同的密钥（不同的加密密钥对文件加密、不同的签名密钥，对文件签名）对文件进行处理。

* **功能描述**

主要包括：新建策略模板、配置策略模板、默认策略模板、删除策略模板、加密策略、签名策略、功能。。

1. **新建策略**

通过新建的方式新建一个策略模板。

1. **配置策略模板**

可配置是否为默认模版、加密策略、签名策略、加密或签名使用的密钥；配置加密及签名时，各配置项需要遵循固定的联动方式；加密策略中配置了一次一密后，无法手动选择密钥；算法类型及模式的选择为级联选项；

1. **默认策略模板**

在策略模版配置页面实现；默认策略模版全局唯一；设置为默认策略模版后，a.系统新获取的固件包将使用新默认模版；b.系统内已存在但未执行过加密处理的固件包将使用新默认模版；系统内已存在且成功执行过加密处理的固件包不会使用新模版。

1. **删除策略模版**

删除模版后将自动解除该模版关联的所有密钥及待处理文件；

1. **加密策略**

包含加密开关、一次一密开关、选择密钥、加密模式；各配置项的配置需要按照先后顺序依次开放禁用/启用；开启一次一密后，无法手动选择密钥，系统每次加密时会自动生成随机数密钥；

1. **签名策略**

包含签名开关、选择签名算法、选择密钥；各配置项的配置需要按照先后顺序依次开放禁用/启用；签名密钥的选择按照签名算法自动关联该类型密钥；

* **使用对象**

业务操作员

### 4.2.1.4安全审计

* **业务描述**

对系统各类安全事件进行日志记录。

* **功能描述**

主要包括：用户登录日志、操作日志、文件日志、查看日志功能。。

1. **用户登录日志**

日志记录用户登录事件。包含用户登录时间、登录终端类型、登录IP地址、登录用户帐号。

1. **操作日志**

日志记录用户对系统操作的事件；包含操作时间、操作帐号、用户归属部门、操作对象、操作类型、操作结果

1. **文件日志**

日志记录固件包状态事件。包含系统时间、文件名称、处理类型、处理结果

1. **查看日志**

查看各类日志

* **使用对象**

审计员

### 4.2.1.5统计分析

4.2.1.6.1**固件处理数量统计**

* **业务描述**

页面显示固件处理数量统计分析结果。

* **功能描述**

主要包括：按照今日处理固件数量、待处理固件数量、本周处理固件数量、历史处理固件数量进行统计分析。

今日处理固件数:按照操作历史中，处理时间当天的记录

本周处理固件数量:按照操作历史中，处理时间为本周内的的记录；

历史处理固件数量:按照操作历史中，处理时间为当前时间以前的记录，

待处理固件数量：所有未处理的数据。

* **使用对象**

**业务操作**员

4.2.1.6.2**固件处理数量统计**

* **业务描述**

统计对比系统中各策略模版使用次数。

* **功能描述**

统计对比系统中各策略模版使用次数

* **使用对象**

**业务操作**员

4.2.1.6.3**固件处理数量统计**

* **业务描述**

统计对比系统处理的各种类型固件的数量。

* **功能描述**

统计对比系统处理的各种类型固件的数量

* **使用对象**

**业务操作**员

4.2.1.6.4**固件处理成功率统计**

* **业务描述**

统计系统处理签名、加密、导出成功率。

* **功能描述**

统计系统处理签名、加密、导出成功率。

**使用对象**

**业务操作**员

4.2.1.6.5**七日业务处理情况**

* **业务描述**

统计系统七日内处理。按照当前时间往前推算7日内数据

* **功能描述**

统计系统七日内处理。按照当前时间往前推算7日内数据

**使用对象**

**业务操作**员

4.2.1.6.6固件**处理用时统计（单个）**

* **业务描述**

统计系统中各个固件的处理耗时，对已经处理的固件数据记录，展示每个固件的用时消耗。

* **功能描述**

统计系统中各个固件的处理耗时，对已经处理的固件数据记录，展示每个固件的用时消耗。

**使用对象**

**业务操作**员

4.2.1.6.7固件**处理用时统计（平均值）**

* **业务描述**

统计系统处理加密、签名的平均耗时，对固件加密、固件签名分别取平均处理时间。

* **功能描述**

统计系统处理加密、签名的平均耗时，对固件加密、固件签名分别取平均处理时间。

**使用对象**

**业务操作**员

4.2.1.6.8**系统使用情况**

* **业务描述**

查看系统磁盘、CPU、内存当前使用情况

* **功能描述**

查看系统磁盘、CPU、内存当前使用情况

**使用对象**

**业务操作**员

4.2.1.6.9**操作日志**

* **业务描述**

查看系统操作日志内容列表

* **功能描述**

查看系统操作日志内容列表

**使用对象**

**业务操作**员

# 5性能设计

## 5.1系统性能

系统应提供快速响应的能力，针对固件包导入、固件包加密、固件包导出等业务，并发性能需达到2000tps，响应时间小于1000ms。平均加密速率不小于100MB/s，平均签名速率不小于200MB/s。

## 5.2资源使用率

在2000用户并发压力下，系统的CPU使用率不应超过70%，内存使用率不应超过80%。

## 5.3信息安全

|  |  |  |
| --- | --- | --- |
| **需求属性** | **需求描述** | **备注** |
| 1强认证 | 系统使用本身的认证机制，需满足强密码策略和锁定策略，并在保证基础用户体验的情况下，选择合适的图形验证码和短信验证码； |  |
| 2 访问控制最小化 | 2.1 系统合理划分各种类型的权限管理，包括管理员、审计员、操作员，保证三权分立； | 必选 |
| 2.2 系统权限控制的管理粒度达到表单的角色级别（或单个用户的增删改查） | 明确系统权限的控制粒度，选择需求中一种或两种。 |
| 3 会话的安全性 | 3.1 系统会话标识随机并唯一，登录后重新分配，并对会话的失效周期进行定义 | 必选 |
| 4 日志安全审计 | 4.1 系统日志需以功能模块方式提供，日志记录覆盖每个用户，无论是内部用户或外部用户，记录应对重要的操作行为（登入登出、权限变更、数据导入导出等其他必要的操作）进行记录，并具有筛选功能；日志记录的内容应包含日期、时间、用户标识、行为的过程和结果等 | 必选，其他必要的操作行为记录可根据应用系统的不同业务定义，对业务审计有需求的内容，各编制人员可自行补充； |
| 4.2 日志记录的管理权限不应对基础用户提供，对开放给审计员，并禁止提供删除和修改的功能。 | 必选 |
| 5 软件容错 | 5.1 系统具备容错设计，提供可用性，对异常或错误的页面或功能进行跳转； | 必选 |
| 6 数据安全 | 6.1 应考虑系统数据的保密性和完整性，包括数据的传输加密https，敏感数据存储加密 | 必须 |
| 7 输入输出安全性 | 5.4.7.1 应用系统应对所有类型的用户输入做校验，尤其是那些用于数据库操作、系统命令执行、程序命令执行、显示到页面的重要参数，并记录拒绝后的错误日志。 | 必须 |
| 5.4.7.2 应用系统应对输出参数做严格的限制，保证非功能必须的参数不在输出的参数中，防止多余信息引起的数据泄露。 | 必须 |

## 5.4可靠性

系统应保证可靠运行，可支持全天候24小时处理事务能力。系统可提供可靠的长时间工作，年故障停止服务次数少于 1次，故障停机时间小于120 分钟。

## 5.5易用性

系统必须提供良好的用户界面以方便用户操作。进行系统界面设计时，应符合KISS（keep it simple and stupid，简单易用）原则。

所有系统级和应用级的错误，包括用户的输入错误都能有友好的出错提示页面。

## 5.6互用性

系统提供设计良好的接口，供第三方系统/APP调用。

## 5.7移植性

系统可以灵活的部署在LINUX、Windows等主流操作系统上。

## 5.8扩展性

系统应采用的是模块化的设计方法，每个模块之间相互独立性较高，方便对功能模块的修改以及新增新的业务模块。

## 5.9维护性

系统应提供系统运行日志和业务日志，以方便维护人员及时处理系统的问题。同时，应提供系统配置信息的页面修改功能，以方便维护人员对经常需要修正的相关配置信息进行修改。

## 5.10合法/合规性

|  |  |  |
| --- | --- | --- |
| 法律法规名称 | 选择情况 | 备注 |
| WP29 R156 | 可选 |  |

# 6接口设计

## 6.1接口设计原则

* 使用简单、快捷，通用性好，可靠性高；
* 充分考虑接口所涉及的各个系统的应用扩展情况，能灵活地支撑需求变化；
* 保证接口数据在接口所涉及的各个系统间的一致性；
* 接口数据能够自动导出和导入；
* 在数据交互过程中，应具有传送和接收后的确认过程。

## 6.2接口实现方式

根据外部系统的不同情况，在接口实现上会出现不同的方式。

### 6.2.1外系统开放数据库、本系统调用

若其他系统没有提供接口，但是本系统需要使用这些系统中生产的数据，我们需要直接在外系统的数据库的基础上开发一些新的接口，通过在前置机上部署新的接口提供服务给本系统使用。

### 6.2.2本系统提供接口、本系统调用

此方式主要为内部接口。

# 7运行设计

## 7.1运行模块的组合

客户端程序在有输入时启动接收数据模块，通过各模块之间的调用，读入并对输入进行格式化。在接收数据模块的得到充分数据时，将调用网络传输模块，将数据通过网络送到服务器，并等待接收服务器返回的信息。接收到返回信息后随即调用数据输出模块，对信息进行处理，产生相应的输出。

服务器端程序的网络数据接口模块必须始终处于活动状态。接收到数据后，调用数据处理、查询模块对数据库进行访问，完成后调用网络发送模块，将信息返回客户端。

## 7.2运行控制

首先为用户分配账户和密码，用户在经过认证后登录系统，在分配账户是进行了权限和角色的分配。

## 7.3运行时间

在软件需求分析中，对运行时间的要求为必须对做出的操作有较快的反应。网络硬件对运行时间的影响最大。

服务器的性能将对影响对数据库的访问时间，即客户机操作的等待时间，所以必须使用高性能的服务器。

# 8维护设计

## 8.1出错处理设计

* 出错信息提示

程序在运行时主要会出现两种错误：由于输入信息，或无法满足要求时产生的错误，称为软错误。由于其他问题，如网络传输超时等，产生的问题，称为硬错误。

对于软错误，须在操作成功判断及输入数据验证模块由数据进行数据分析，判断错误类型，再生成相应的错误提示语句，送到输出模块中。

* 出错处理对策

所有服务器都必须安装不间断电源，以防止停电或电压不稳定造成数据丢失的损失。若突然断电，对客户机将不会有太大的影响；对于服务器，可采用日志文件，对事务进行回滚处理，对数据进行恢复。

在网络传输方面，可考虑建立一条成本较低的备份网络，以保证当主网络断路时数据的通信。

在硬件方面要选择教可靠、稳定的服务器，保证系统运行时的可靠性。

### 8.1.1出错输出信息

#### 8.1.1.1导入重复报错

输出信息：:::;;;;固件文件名称已存在



#### 8.1.1.2导出报错

输出信息：导出:::;;;;解析公钥失败



#### 8.1.1.4固件处理失败

输出信息：进度条提示



## 8.2安全保密设计

* 在用户登录系统时进行身份验证，只允许合法用户进入系统。
* 增加弱口令判断机制，用户输入简单的用户名密码，不能设置。
* 在数据接口方面，通过token进行验证，保证数据传输过程可控。
* 对于存储到数据库中的一些关键敏感信息(如密码等信息)，按要求进行加密。
* 加密存储的各项运行参数和业务参数作为商业机密数据，在未经授权时任何人员都应无法查看和存取。
* 对于加密存储到数据库的关键敏感信息，在客户端和服务器之间传递时应进行加密传输。
* 网络层面的安全，通过省电子政务云平台提供安全防护策略，保障网络应用的安全可靠。同时，做好软件应用层面的经常性检查，及时打好系统补丁和Bug修复。

## 8.3维护设计

为了系统维护的方便，在程序内部设计了日志监控模块，监测用户登录日志、操作日志以及报错日志。