OTA安全管理系统

用户需求说明书

**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 | 2021/12/30 | 雒天承 | 刘鹏 | 刘鹏 | 创建 |
| 2 | V1.1 | 2022/1/4 | 雒天承 | 刘鹏 | 刘鹏 | 根据评审内容修改 |
| 3 | V1.2 | 2022/1/7 | 雒天承 | 刘鹏 | 刘鹏 | 策略管理模块-设置默认策略模版添加后置条件 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

目录

[1 5](#_Toc13807)

[1.1 背景 6](#_Toc7464)

[1.2 业务需求概述 6](#_Toc7104)

[1.3 引用/参考 7](#_Toc26917)

[1.4 术语 7](#_Toc13210)

[2 业务流程模型 7](#_Toc20920)

[2.1 系统用户特征 9](#_Toc32411)

[2.2 业务流程图 10](#_Toc9006)

[3 接口与界面需求 11](#_Toc12526)

[3.1 外部接口 11](#_Toc23991)

[3.2 硬件接口 11](#_Toc15342)

[3.3 软件接口 11](#_Toc32643)

[3.4 用户界面 12](#_Toc13896)

[4 功能需求 13](#_Toc30940)

[4.1 密钥管理（F1） 13](#_Toc31269)

[4.1.1 查看密钥列表（F1-1） 13](#_Toc25132)

[4.1.2 查询密钥（F1-2） 13](#_Toc20899)

[4.1.3 密钥生成（F1-3） 13](#_Toc2824)

[4.1.4 密钥加密导出（F1-4） 14](#_Toc3116)

[4.1.5 公钥复制（F1-5） 14](#_Toc29366)

[4.2 固件管理（F2） 15](#_Toc27497)

[4.2.1 查看固件列表（F2-1） 15](#_Toc32204)

[4.2.2 查询固件（F2-2） 15](#_Toc3297)

[4.2.3 固件导入（F2-3） 15](#_Toc6614)

[4.2.4 固件解析（F2-5） 16](#_Toc23944)

[4.2.5 固件存储（F2-6） 16](#_Toc18219)

[4.2.6 固件加密（F2-7） 16](#_Toc20169)

[4.2.7 固件删除（F2-8） 16](#_Toc592)

[4.2.8 固件导出（F2-9） 17](#_Toc201)

[4.3 策略管理（F3） 17](#_Toc4513)

[4.3.1 查看策略模版列表（F3-1） 17](#_Toc29697)

[4.3.2 查询策略模版（F3-2） 18](#_Toc8471)

[4.3.3 新建策略模版（F3-3） 18](#_Toc9310)

[4.3.4 修改策略模版（F3-4） 18](#_Toc9572)

[4.3.5 删除策略模版（F3-5） 19](#_Toc17016)

[4.3.6 设置默认策略模版（F3-6） 19](#_Toc2230)

[4.4 日志审计（F4） 19](#_Toc9145)

[4.4.1 系统登录日志（F4-1） 19](#_Toc30441)

[4.4.2 用户操作日志（F4-2） 20](#_Toc2140)

[4.4.3 固件处理日志（F4-3） 20](#_Toc3054)

[4.4.4 查询日志（F4-4） 20](#_Toc3749)

[4.5 统计分析（F5） 21](#_Toc32426)

[4.5.1 固件处理数量统计（F5-1） 21](#_Toc9426)

[4.5.2 固件处理策略统计（F5-2） 21](#_Toc29601)

[4.5.3 固件类型统计（F5-3） 21](#_Toc6031)

[4.5.4 业务成功率统计（F5-4） 21](#_Toc15911)

[4.5.5 七日业务情况统计（F5-5） 21](#_Toc2282)

[4.5.6 固件处理用时统计（F5-6） 22](#_Toc19439)

[4.5.7 系统使用情况统计（F5-7） 22](#_Toc15396)

[5 非功能需求 22](#_Toc5674)

[5.1 系统性能 22](#_Toc17618)

[5.2 资源使用率 22](#_Toc3230)

[5.3 可靠性 22](#_Toc23586)

[5.4 易用性 22](#_Toc21072)

[5.5 互用性 23](#_Toc30026)

[5.6 扩展性 23](#_Toc8383)

[5.7 维护性 23](#_Toc12903)

[5.8 合法/合规性 23](#_Toc3525)

[6 需求确认 24](#_Toc9559)

# 

## 背景

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。

## 业务需求概述

|  |  |  |  |
| --- | --- | --- | --- |
| 需求提出人 | 陈涛 | | |
| 所在单位 | 泛亚汽车技术中心有限公司 | | |
| 职位 | 项目经理 | | |
| 高阶需求 | 编号 | 内 容 | 重要度 |
| 1 | 支持不同大小固件数据签名验签 | 高 |
| 2 | 支持不同大小固件数据加解密 | 高 |
| 3 | 可比对不同主控下国密/国际算法软方式/安全芯片方式加解密、签名验签时间等算法性能 | 高 |
| 4 | 支持.hex、.bin、.s19格式文件的加密处理 | 高 |
| 5 | 文件导入、文件加密处理进度的页面呈现 | 中 |

|  |  |  |  |
| --- | --- | --- | --- |
| 需求提出人 | 陈涛 | | |
| 所在单位 | 泛亚汽车技术中心有限公司 | | |
| 职位 | 项目经理 | | |
| 高阶需求 | 编号 | 内 容 | 重要度 |
| 1 | 支持不同大小固件数据加解密 | 高 |
| 2 | 支持通过外部接口获取、上传数据 | 高 |
| 3 | 支持对接客户PKI系统查询证书公钥 | 高 |
| 4 | 加密密钥支持以PKCS#7密钥信封格式输出 | 高 |
| 5 | 支持.vbf格式文件的加密处理 | 高 |

|  |  |  |  |
| --- | --- | --- | --- |
| 需求提出人 | 雒天承 | | |
| 所在单位 | 天津三源电力智能科技有限公司 | | |
| 职位 | CTO | | |
| 高阶需求 | 编号 | 内 容 | 重要度 |
| 1 | 支持多种数据导入、导出方式（本地操作、外部调用） | 高 |
| 2 | 支持多种签名、加密方式，可自由配置加密策略 | 高 |
| 3 | 支持主流ECU升级文件格式的解析处理 | 高 |
| 4 | 支持对主要业务指标的统计分析，以及页面呈现效果 | 高 |
| 5 | 支持对.apk格式文件的加密处理 | 中 |

## 引用/参考

|  |  |  |
| --- | --- | --- |
| **文件名** | **版本号** | **说明** |
| *泛亚SOW* |  |  |
| *吉利TSM开发协议* |  |  |
|  |  |  |
|  |  |  |

## 术语

| **业务名词/术语** | **描述** |
| --- | --- |
| *密钥* |  |
| *密钥信封* |  |
| *保护公钥* |  |
| *LMK* |  |

# 业务流程模型

总体业务结构如下图所示。



## 系统用户特征

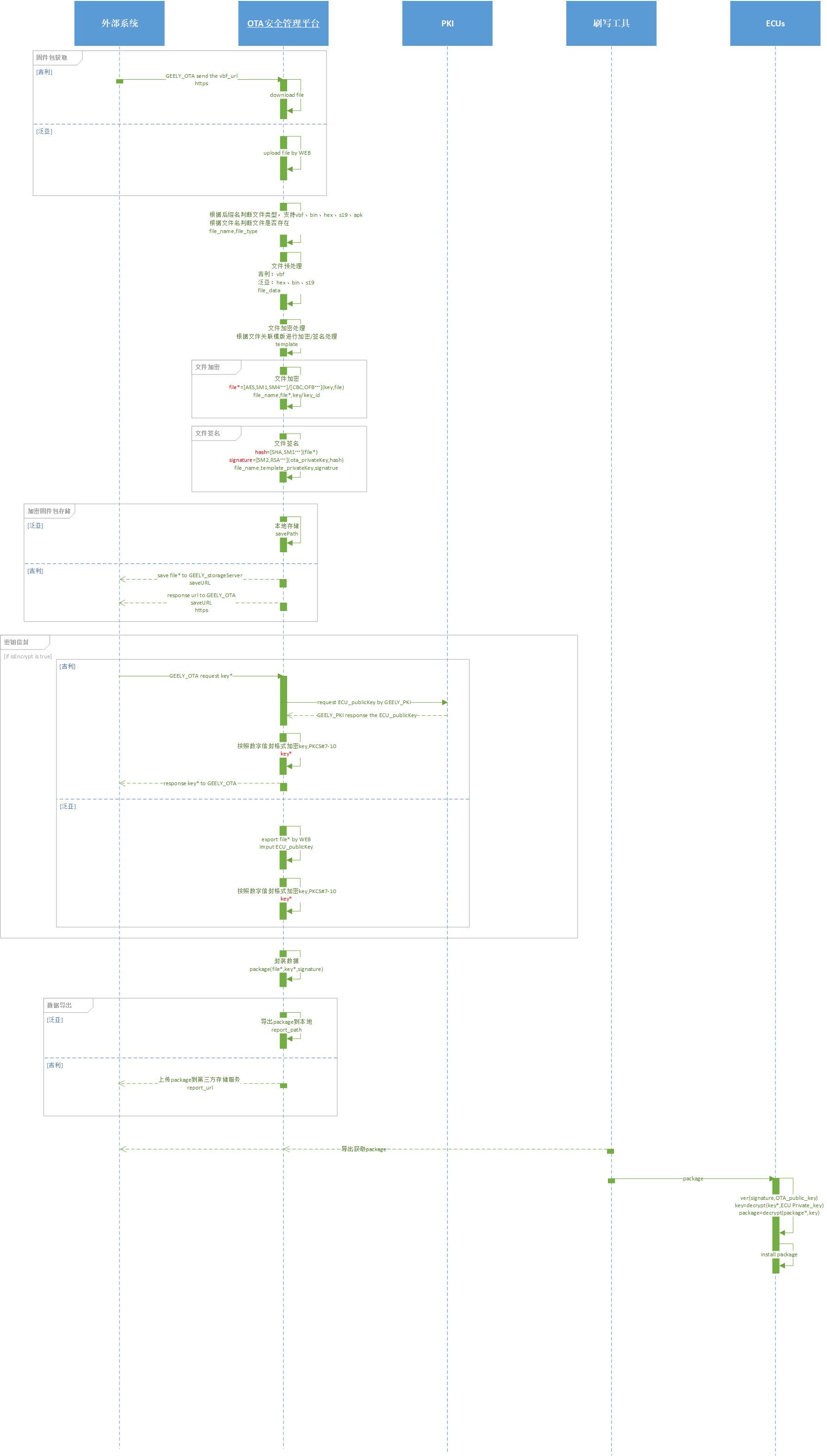
业务操作员：负责业务功能操作

系统管理员：负责分配角色账号

审计员：对操作日志进行审核

| **角色**  **功能** | **业务操作员** | **审核人员** | **系统管理员** |
| --- | --- | --- | --- |
| 用户管理 |  |  | √ |
| 权限管理 |  |  | √ |
| 密钥管理 | √ |  |  |
| 固件管理 | √ |  |  |
| 全局策略 | √ |  |  |
| 固件策略 | √ |  |  |
| 操作日志 |  | √ |  |
| 登录日志 |  | √ |  |

## 业务流程图

**

# 接口与界面需求

## 外部接口

本系统与外部系统无业务关联，无外部接口需求

## 硬件接口

本系统不涉及硬件模块，无硬件接口需求

## 软件接口

本系统采用B/S架构设计，系统与数据库再同一局域网环境采用TCP/IP协议通信，前端开发采用Vue.js实现前后端分离，前端UI界面调用后端的各种数据及业务接口，用于页面的数据展示及交互操作。

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **接口分类** | **接口名称** | **接口功能** |
|  | 内部接口 | 系统基础信息 | 用于公共表单页面数据展示 |
|  | 内部接口 | 固件基础信息数据 | 获取数据库中保存的固件基础信息 |
|  | 内部接口 | 上传固件文件 | 从客户端向服务端上传固件文件 |
|  | 内部接口 | 提交固件配置信息 | 从客户端向服务端提交固件的配置信息 |
|  | 内部接口 | 修改固件绑定策略 | 从客户端向服务端提交固件绑定策略修改请求 |
|  | 内部接口 | 固件加密 | 从客户端向服务端提交固件加密请求 |
|  | 内部接口 | 密钥基础信息数据 | 获取数据库中保存的密钥基础信息 |
|  | 内部接口 | 提交密钥配置信息 | 从客户端向服务端提交密钥的配置信息 |
|  | 内部接口 | 策略模板基础信息数据 | 获取数据库中保存的策略模板基础信息 |
|  | 内部接口 | 提交策略模板配置信息 | 从客户端向服务端提交策略模板的配置信息 |
|  | 内部接口 | 删除策略模板 | 从客户端向服务端提交删除策略模板请求 |
|  | 内部接口 | 固件处理日志数据 | 获取数据库中保存的固件处理日志 |
|  | 内部接口 | 固件导出记录数据 | 获取固件导出记录 |
|  | 内部接口 | 系统操作日志数据 | 获取数据库中保存的系统操作日志 |
|  | 内部接口 | 用户登录日志数据 | 获取数据库中保存的用户登录日志 |
|  | 内部接口 | 加密模式下拉列表数据 | 用于添加策略模板页面中加密模式选择的下拉列表数据展示 |
|  | 内部接口 | 一次一密下拉列表数据 | 用于添加策略模板页面中一次一密参数选择的下拉列表数据展示 |
|  | 内部接口 | 签名算法下拉列表数据 | 用于添加策略模板页面中签名算法选择的下拉列表数据展示 |
|  | 内部接口 | 密钥选择下拉列表数据 | 用于添加策略模板页面中加密密钥、签名密钥选择的下拉列表数据展示 |
|  | 内部接口 | 策略模板下拉列表数据 | 用于固件列表页面中策略模板选择的下拉列表数据展示 |
|  | 内部接口 | 固件解析类型下拉列表数据 | 用于导入固件页面中固件解析处理器选择的下拉列表数据展示 |
|  | 内部接口 | 操作结果下拉列表数据 | 用于固件处理日志、系统操作日志、用户登录日志页面中操作结果选择的下拉列表数据展示 |
|  | 内部接口 | 系统操作类型下拉列表数据 | 用于系统操作日志页面中操作类型选择的下拉列表数据展示 |
|  | 内部接口 | 固件处理数量统计 | 获取系统处理固件的总数量，包括当日处理数量、周处理数量、历史处理数量，用于统计分析页面的数据展示 |
|  | 内部接口 | 待处理固件数量统计 | 获取系统待处理固件的数量，用于统计分析页面的数据展示 |
|  | 内部接口 | 固件处理策略统计 | 获取系统中各个策略模板的使用次数占比，用于统计分析页面的数据展示 |
|  | 内部接口 | 固件类型统计 | 获取系统中的不同固件类型数量占比，用于统计分析页面的数据展示 |
|  | 内部接口 | 业务处理成功率统计 | 获取系统处理各种业务的成功率，用于统计分析页面的数据展示 |
|  | 内部接口 | 业务处理成功/失败次数统计 | 获取系统处理各种业务的成功数量与失败数量，用于统计分析页面的数据展示 |
|  | 内部接口 | 七日业务处理次数统计 | 获取系统处理各种类型业务的次数，用于统计分析页面的数据展示 |
|  | 内部接口 | 固件处理用时数据 | 获取系统对固件进行不同处理的耗时，用于统计分析页面的数据展示 |
|  | 内部接口 | 系统状态 | 获取当前系统环境运行状态，包括磁盘使用率、CPU使用率、内存使用率，用于统计分析页面的数据展示 |

## 用户界面

* 一致性：界面元素及交互按钮风格保持一致；
* 简易性：结构清晰，布局及设计简洁合理；
* 界面语言：语言描述准确易懂，应减少争议性；
* 人性化：界面交互符合使用常理，降低用户学习成本；

# 功能需求

## 密钥管理（F1）

### 查看密钥列表（F1-1）

#### 业务描述

查看密钥列表主要是查看系统中所有的密钥信息以及可进行的相关操作

#### 功能描述

主要包含功能按钮：添加密钥、查询、公钥复制

主要包含字段：密钥名称、算法分类、算法类型、密钥长度、创建时间；

#### 使用对象

业务操作员

### 查询密钥（F1-2）

#### 业务描述

查询密钥主要是根据特定信息过滤查找系统中的密钥

#### 功能描述

查找过滤项：密钥名称、密钥类型

主要包含字段：密钥名称、算法分类、算法类型、密钥长度、创建时间；

#### 使用对象

业务操作员

### 密钥生成（F1-3）

#### 业务描述

密钥生成主要是为固件包的加密或签名处理生成所需的密钥，可以根据具体需要使用的算法类型、密钥类型、密钥长度、填充方式等要求生成对应的密钥。

#### 功能描述

UI界面点击添加密钥按钮，填写表单信息并提交；

表单项：密钥名称、算法类别；

算法类别可支持：

对称算法：AES

非对称算法：SM2、RSA、ECC

可支持的国密算法：

对称算法：SM4

非对称算法：SM2

#### 使用对象

业务操作员

### 密钥加密导出（F1-4）

#### 业务描述

密钥加密导出主要是针对做对称加密的固件包导出，加密固件包导出后在外部使用需要进行解密，解密需要使用该固件包的加密密钥，所以需要将系统做加密的密钥一同导出，由于密钥明文导出不安全，所以需要使用非对称密钥公钥进行加密，此功能就是在加密固件导出时，向系统输入一个非对称密钥公钥，系统使用该公钥对加密密钥进行加密后导出，外部系统可使用私钥进行解密获取到加密密钥。

#### 功能描述

进行加密操作的固件包导出时可手动输入一个非对称密钥公钥作为保护公钥，保护公钥用于对固件包加密密钥进行加密，并且以密钥信封形式导出，密钥信封遵循PKCS#7标准结构。

#### 使用对象

业务操作员

### 公钥复制（F1-5）

#### 业务描述

公钥复制主要是将系统中生成的非对称密钥的公钥复制导出使用

#### 功能描述

点击UI界面中的复制按钮，可将非对称密钥的公钥复制到系统剪切板

#### 使用对象

业务操作员

## 固件管理（F2）

### 查看固件列表（F2-1）

#### 业务描述

查看固件列表主要是查看系统中所有固件的信息以及可进行的相关操作

#### 功能描述

主要包含功能按钮：导入固件、选择策略模板、加密、导出、删除、查看详情；

主要包含字段：固件名称、固件描述、固件处理进度、固件导入时间、固件策略模板；

固件详情包含字段：固件解析方式、固件加密方式、固件签名方式、加密用时、签名用时；

#### 使用对象

业务操作员

### 查询固件（F2-2）

#### 业务描述

查询固件主要是根据特定信息过滤查找系统中的固件

#### 功能描述

查找过滤项：固件名称、固件描述、策略模板、处理状态、导入时间范围

主要包含字段：固件名称、固件描述、固件处理进度、固件导入时间、固件策略模板；

#### 使用对象

业务操作员

### 固件导入（F2-3）

#### 业务描述

固件导入主要是将未处理的原始固件文件手动导入到系统中

#### 功能描述

UI界面点击导入按钮，填写表单信息提交；

表单项：固件文件、固件解析处理器、固件描述；

固件包支持格式：.hex、.bin、.S19、.vbf、.apk

流程：点击导入按钮---选择固件包上传---解析后缀名---选择解析处理方式---输入描述信息（可选）---导入成功

后置条件：固件包导入后默认关联系统默认策略模板

#### 使用对象

业务操作员

### 固件解析（F2-5）

#### 业务描述

固件包有多种格式，需要根据不同格式的固件包使用不同的解析方式进行加密处理

#### 功能描述

固件包导入时，可根据固件包后缀名自动匹配固件包的解析方式

系统支持解析方式：hex

### 固件存储（F2-6）

#### 业务描述

导入源固件包，以及固件包加密后，需要以文件形式存储在服务器本地

#### 功能描述

系统可配置相应存储路径用来存储源固件包、加密后固件包文件

### 固件加密（F2-7）

#### 业务描述

固件加密为系统核心功能，主要是对固件包进行加密或签名，可根据策略模板的配置内容，对固件包进行相应的处理。

#### 功能描述

UI界面中点击加密按钮，系统根据固件关联的策略模板进行加密处理，并在页面中实时反馈加密处理的进度。

流程：点击加密按钮---读取关联策略模板---加密计算---加密---实时监控进度---完成

#### 使用对象

业务操作员

### 固件删除（F2-8）

#### 业务描述

当误传入一个固件包或固件包不再使用时，需要将系统中的存储的固件包删除，以节省系统资源占用。

#### 功能描述

UI界面中点击删除按钮，可删除当前固件包。

前提条件：要删除的固件包非处理中状态。

后置条件：将系统本地相应目录中存储的文件删除，但不删除该文件的相关日志记录。

#### 使用对象

业务操作员

### 固件导出（F2-9）

#### 业务描述

当固件包处理完成后，可将固件包下载导出。

#### 功能描述

UI界面中点击导出按钮，导出固件包。

导出条件：

加密固件包导出：需要输入一个非对称密钥公钥作为保护密钥；

签名固件包导出：无要求

导出文件内容：处理后的固件包，PKCS#7文件

导出格式：.zip压缩包

导出方式：页面弹出下载提示

#### 使用对象

业务操作员

## 策略管理（F3）

### 查看策略模版列表（F3-1）

#### 业务描述

查看策略模板列表主要是查看系统中所有策略模板的信息以及可进行的相关操作

#### 功能描述

主要包含功能按钮：新增、修改、删除、查询；

主要包含字段：策略模板名称、是否默认模板、加密处理、一次一密、加密密钥算法、加密密钥长度、加密模式、加密填充模式、签名处理、密钥签名算法；

#### 使用对象

业务操作员

### 查询策略模版（F3-2）

#### 业务描述

查询策略模板主要是根据特定信息过滤查找系统中的策略模板

#### 功能描述

查找过滤项：策略模板名称；

主要包含字段：策略模板名称、是否默认模板、加密处理、一次一密、加密密钥算法、加密密钥长度、加密模式、加密填充模式、签名处理、密钥签名算法；；

#### 使用对象

业务操作员

### 新建策略模版（F3-3）

#### 业务描述

当需要使用新的策略对固件包进行加密处理时，可在系统中创建新的策略模板

#### 功能描述

UI界面点击新增按钮，填写表单内容并提交；

表单项：是否默认模板、策略模板名称、是否加密处理、是否一次一密、加密密钥选择、加密模式、一次一密参数、是否签名处理、签名算法、签名密钥；

### 修改策略模版（F3-4）

#### 业务描述

当需要对已有的策略进行修改时，可在系统中修改已有的策略模板

#### 功能描述

UI界面点击修改按钮，修改表单内容并提交；

表单项：是否默认模板、策略模板名称、是否加密处理、是否一次一密、加密密钥选择、加密模式、一次一密参数、是否签名处理、签名算法、签名密钥；

前置条件：被修改的策略模板没有关联正在处理中的固件包；

后置条件：修改完成后，关联的已处理完成的固件包，处理方式信息不发生改变；关联的未处理的固件包，将按照新的策略进行处理。

### 删除策略模版（F3-5）

#### 业务描述

当策略模板不再使用时，可删除该策略模板

#### 功能描述

UI界面点击删除按钮，删除策略模板。

前置条件：被删除的策略模板没有关联正在处理中的固件包；

后置条件：删除后，关联的固件包自动关联到默认策略模板；已处理完成的固件包，处理方式信息不发生改变。

### 设置默认策略模版（F3-6）

#### 业务描述

可手动设置一个策略模板作为默认策略模板，固件导入后自动关联默认策略模板。

系统首次部署时提供默认的策略模板，模板配置采用系统默认配置。

#### 功能描述

系统首次部署：默认策略模板采用系统默认配置项：

是否默认：是

策略模板名称：默认模板

是否加密：是

是否一次一密：是

一次一密参数：SM4-128-CBC-PKCS7

是否签名：否

修改默认策略模板：

修改页面中选中默认模板，保存即可。

后置条件：修改默认策略模板后，原默认策略模板自动变为非默认状态；修改默认策略模板后，系统中已导入的固件不受影响，后续导入的固件自动关联默认策略模板。

## 日志审计（F4）

### 系统登录日志（F4-1）

#### 业务描述

系统审计员需要定期或在发生安全事故后，对系统的使用情况进行审计，可查看系统登录日志查看系统使用人员使用的时间、IP、地点、等是否符合规定，从而识别安全风险。

#### 功能描述

主要功能按钮：查询日志

主要包含字段：用户名称、登录地址、登录地点、浏览器、操作系统、登录状态、操作信息、登录日期。

### 用户操作日志（F4-2）

#### 业务描述

系统审计员需要定期或在发生安全事故后，对系统的使用情况进行审计，可查看用户操作日志查看系统使用者进行的各种类型操作以及操作时间、主机IP、操作结果等信息，确定人员操作是否符合要求。

#### 功能描述

主要功能按钮：查询

主要包含字段：系统模块、操作类型、操作账号、主机IP、操作地点、操作结果、操作时间，操作详情。

### 固件处理日志（F4-3）

#### 业务描述

系统审计员需要定期或在发生安全事故后，对系统的使用情况进行审计，可查看固件处理日志查看固件处理的相关信息。

#### 功能描述

主要功能按钮：查询，查看导出历史

主要包含字段：固件名称、处理类型、处理时间、处理结果、操作原因、操作账号、导出历史。

### 查询日志（F4-4）

#### 业务描述

查询策略模板主要是根据特定信息过滤查找系统中的各种日志

#### 功能描述

按照登录地址、用户名称、登录状态、登录时间可查询用户登录信息；

按照系统模块、操作账号、操作类型、操作结果、操作时间可查询用户操作信息；

按照固件名称、处理类型、操作结果、处理时间可查询固件处理信息。

## 统计分析（F5）

### 固件处理数量统计（F5-1）

#### 业务描述

页面显示固件处理数量统计分析结果。

#### 功能描述

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。

### 固件处理策略统计（F5-2）

#### 业务描述

页面显示固件处理策略统计分析结果。

#### 功能描述

按照每一种固件处理策略处理固件数量各占全部已处理固件数量的百分比进行统计分析。

### 固件类型统计（F5-3）

#### 业务描述

页面显示固件类型统计分析结果。

#### 功能描述

按照每一种固件类型数量占全部固件数量的百分比进行统计分析。

### 业务成功率统计（F5-4）

#### 业务描述

页面显示各种业务处理成功率的统计分析结果。

#### 功能描述

分析统计固件签名、固件加密、固件导出业务处理成功的数量占各业务处理总数量的百分比。

### 七日业务情况统计（F5-5）

#### 业务描述

页面显示七日内的各种业务处理数量的统计结果。

#### 功能描述

分别统计七日内固件签名、固件加密、固件导出每种业务处理的数量。

### 固件处理用时统计（F5-6）

#### 业务描述

页面显示各个固件处理用时的统计结果。

#### 功能描述

按照固件名称 、固件大小、加密用时、签名用时统计各固件处理业务的所用时长。

### 系统使用情况统计（F5-7）

#### 业务描述

页面显示系统使用情况的统计结果。

#### 功能描述

按照磁盘使用情况、CPU使用率、内存使用率进行统计分析。

# 非功能需求

## 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。

## 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%。

## 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。

## 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。

## 互用性

系统提供设计良好的接口，供第三方系统/APP调用。

## 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。

## 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。

## 合法/合规性

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

# 需求确认

|  |  |
| --- | --- |
| 需求确认 | |
| 需求文档 | OTA安全管理系统《用户需求说明书》v1.2 |
| 文档说明 | 1.本需求文档建立在双方对需求的共同理解的基础之上，本需求文档描述的功能完全符合用户的需求，双方同意后续的工作根据该需求文档开展。  2.如果需求发生变化，双方将对需求的变更的影响，重新协商成本、资源和进度等。  3.本承诺书具有商业合同的等同效果。 |
| 用户确认 | 签字：陈涛 日期：**2022.1.7** |