OTA安全管理系统

产品需求规格说明书

**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 | 2021/12/31 | 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 概述 5](#_Toc32348)

[1.1 背景 5](#_Toc30074)

[1.2 系统目标 6](#_Toc28107)

[1.3 目标系统概述 7](#_Toc21130)

[1.3.1 系统总体结构 7](#_Toc18213)

[1.4 范围/系统界定 8](#_Toc7417)

[1.5 系统假设/约定 8](#_Toc27651)

[1.5.1 假设 8](#_Toc2825)

[1.5.2 约定 8](#_Toc20601)

[1.6 操作环境 8](#_Toc982)

[1.6.1 服务器操作环境 8](#_Toc23848)

[1.7 系统用户特征 9](#_Toc15269)

[1.8 引用/参考 9](#_Toc21186)

[1.9 术语 10](#_Toc24540)

[2 用例 10](#_Toc17066)

[2.1 系统用例 10](#_Toc14238)

[2.1.1 密钥管理模块 10](#_Toc3481)

[2.1.2 固件加密模块 11](#_Toc1626)

[2.1.3 策略管理模块 14](#_Toc8302)

[2.1.4 安全审计模块 16](#_Toc10199)

[2.1.5 系统管理模块 17](#_Toc10398)

[3 接口与界面 18](#_Toc22903)

[2.1硬件接口 18](#_Toc1231)

[2.2软件接口 18](#_Toc719)

[2.3通信接口（可选） 18](#_Toc7079)

[2.4 用户界面 18](#_Toc8134)

[4 功能需求 22](#_Toc20963)

[4.1 系统流程图 22](#_Toc16595)

[4.2 功能一览表 23](#_Toc25118)

[4.3 功能描述 26](#_Toc31258)

[4.3.1 OTA安全管理系统服务端平台 26](#_Toc11263)

[4.4 公共功能描述 70](#_Toc8306)

[4.4.1 系统管理模块（OTA-SRS-SM） 70](#_Toc32164)

[5 非功能需求 74](#_Toc27548)

[5.1 系统性能 74](#_Toc12669)

[5.2 资源使用率 74](#_Toc3890)

[5.3 信息安全 74](#_Toc3066)

[5.4 可靠性 75](#_Toc10266)

[5.5 易用性 76](#_Toc24508)

[5.6 互用性 76](#_Toc2689)

[5.7 移植性 76](#_Toc29730)

[5.8 扩展性 76](#_Toc7330)

[5.9 维护性 76](#_Toc18793)

[5.10 合法/合规性 76](#_Toc3310)

[6 验收标准 77](#_Toc28353)

[7 需求确认 78](#_Toc26192)

[8 附录 79](#_Toc509)

[8.1 密钥算法清单 79](#_Toc23449)

# 

## 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。

在进行需求分析的过程中，识别到以下三方对于此产品的基本需求，本产品的设计将以覆盖下列需求为MVP目标，如下所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

本文对此产品系统需求以及业务流程等方面进行详细梳理及分析。

本文档主要包含如下内容：

1. 明确系统需求，对系统的总体需求进行梳理；
2. 在开始系统开发之前对软件的需求进行全面的了解，辅助开发、测试人员进行后续研发工作；
3. 作为系统设计和实现的依据；
4. 为系统最后的确认和验收提供基准；
5. 作为项目组与客户方之间进行需求交流的基础；

## 系统目标

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。

## 目标系统概述

### 系统总体结构



## 范围/系统界定

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。

## 系统假设/约定

### 假设

* 开发周期：本系统的开发具有充足的时间；
* 开发资源：本系统的开发具有充足的人员及预算资源；
* 验证环境：用户能够提供交付测试的环境用于验证；
* 需求确认：用户能够参与需求的核准；

### 约定

* 设计和实现：本系统基于B/S架构设计；
* 开发语言：服务端后台程序采用JAVA语言编写，前端采用vue.js开发；
* 合规性：系统使用的密码技术均符合相关技术规范；

## 操作环境

### 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 |
| 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 |  |

## 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** |
| --- | --- | --- | --- |
| 功能点A，例如：用户管理 |  |  | √ |
| 功能点A，例如：权限管理 |  |  | √ |
| 功能点A，例如：密钥管理 | √ |  |  |
| 功能点A，例如：固件管理 | √ |  |  |
| 功能点A，例如：全局策略 | √ |  |  |
| 功能点A，例如：固件策略 | √ |  |  |
| 功能点A，例如：操作日志 |  | √ |  |
| 功能点A，例如：登录日志 |  | √ |  |

## 引用/参考

|  |  |  |
| --- | --- | --- |
| **文件名** | **版本号** | **说明** |
| 国密芯片与国密算法应用研究项目采购需求-签字版 | V1.0 | 泛亚项目SOW |
| 吉利汽车研究院（宁波）有限公司-技术协议 | V1.0 | 吉利项目SOW |
| OTA安全管理系统\_用户需求说明书 | V1.0 | 用户需求说明书 |
|  |  |  |

## 术语

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

# 用例

## 系统用例



### 密钥管理模块

|  |  |  |  |
| --- | --- | --- | --- |
| 密钥管理模块 | | | |
| 图例：   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | 用户扮演的角色 | 系统支持的业务活动 | 角色指向活动：能执行  活动指向角色：通知/调用 |  | | | | |
| **用例（业务功能）简述** | | | |
| **业务流程** | **用例名称** | **用例简述** | **业务规则** |
| 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 | 密钥查询 | 1、查看系统中已生成的全部密钥 | 1、可通过对密钥名称、密钥类型过滤查询；  2、密钥名称支持模糊查询；  3、密钥类型支持级联选择； |
| 密钥生成 | 1、手动生成密钥 | 1、手动生成时需配置密钥名称（必须项）；  2、选择密钥类型支持级联选择；  3、密钥的软生成/硬生成方式遵循系统当前密钥管理机制； |
| 密钥删除 | 1、删除已存在的密钥 | 1、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； |
| 密钥导出 | 1、导出非对称密钥公钥 | 1、仅非对称密钥支持导出；  2、点击导出按钮后自动将公钥复制到系统剪贴板 |
| 固件加密处理完成后，需要将加密密钥封装成数字信封导出 | 密钥导入 | 1、系统封装密钥信封时的必要参数 | 1、可通过手动输入或PKI系统查询的方式导入保护密钥； |

### 固件加密模块

|  |  |  |  |
| --- | --- | --- | --- |
| 固件加密模块 | | | |
| 图例：   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | 用户扮演的角色 | 系统支持的业务活动 | 角色指向活动：能执行  活动指向角色：通知/调用 |  | | | | |
| **用例（业务功能）简述** | | | |
| **业务流程** | **用例名称** | **用例简述** | **业务规则** |
| 未命名文件(47) | 固件获取 | 1、系统获取待加密的原始固件包 | 1、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；  2、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；  3、导入时可输入固件包的描述信息（非必须项）；  4、导入时需要选择固件包的解析方式，解析方式根据文件后缀名自动关联出此类文件的所有解析方式供用户选择（必选项）；  5、系统中各固件包名称唯一；  6、通过外部接口导入时需要正确传7相应的接口参数；  8、当固件包名称重复/上传格式错误时导入失败； |
| 查看详情 | 1、查看固件包的相关信息 | 1、可查看固件包解析方式、加密处理策略、加密处理耗时 |
| 固件预处理 | 1、固件加密前预处理 | 1、通过固件导入时选择的解析方式实现；  2、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； |
| 固件存储 | 1、存储原始固件包以及加密后固件包 | 1、支持对接外部存储服务；  2、支持存储到本地路径； |
| 固件导出 | 1. 导出签名后的固件包及签名值； 2. 导出加密后的固件包及密钥信封； 3. 导出签名并加密后的固件包、签名值及密钥信封； | 1. 签名操作导出原始固件包及签名文件； 2. 加密操作导出加密固件包及密钥信封（需导入保护密钥）； 3. 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）； 4. 支持对接外部接口导出； |
| 固件删除 | 1、删除系统内的固件包 | 1、正在处理中的固件包无法删除；  2、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； |
| 固件加密处理 | 1、系统对固件进行加密处理 | 1、可配置加密处理的策略；  2、可统计加密、签名的耗时；  3、支持可视化显示处理的进度；  4、处理失败时可通知用户处理失败； |
| 固件加密处理策略 | 1、系统对固件进行加密处理的策略 | 1、未成功执行加密处理的固件包可配置加密策略；  2、加密中及加密完成的固件包不可配置加密策略； |
| 控制操作 | 1、固件加密的开始、终止操作控制 | 1、未处理过的原始文件可手动进行开始加密操作；  2、加密中的文件可进行终止操作；  3、终止后文件回到原始状态，可再次配置策略模版进行加密操作； |

### 策略管理模块

|  |  |  |  |
| --- | --- | --- | --- |
| 策略管理功能 | | | |
| 图例：   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | 用户扮演的角色 | 系统支持的业务活动 | 角色指向活动：能执行  活动指向角色：通知/调用 |  | | | | |
| **用例（业务功能）简述** | | | |
| **业务流程** | **用例名称** | **用例简述** | **业务规则** |
| 可配置新的策略模版或修改/删除已有的策略模版；可将已有的策略模版配置为默认模版 | 新建策略模版 | 1、新增策略模版 |  |
| 配置策略模版 | 1、配置策略模版内容 | 1、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；  2、配置加密及签名时，各配置项需要遵循固定的联动方式；  3、加密策略中配置了一次一密后，无法手动选择密钥；  4、算法类型及模式的选择为级联选项； |
| 默认策略模版 | 1、设置系统默认策略模版 | 1、在策略模版配置页面实现；  2、默认策略模版全局唯一；  3、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；c.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。 |
| 删除策略模版 | 1、删除系统中已存在的策略模版 | 1、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； |
| 加密策略 | 1、配置加密处理的策略 | 1、包含加密开关、一次一密开关、选择密钥、加密模式；  2、各配置项的配置需要按照先后顺序依次开放禁用/启用；  3、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； |
| 签名策略 | 1、配置签名处理的策略 | 1、包含签名开关、选择签名算法、选择密钥；  2、各配置项的配置需要按照先后顺序依次开放禁用/启用；  3、签名密钥的选择按照签名算法自动关联该类型密钥； |
| 对系统全局策略（存储、协议、接入认证等）进行配置 | 文件服务器 | 1、可配置加密固件包存储的路径 |  |

### 安全审计模块

|  |  |  |  |
| --- | --- | --- | --- |
| 安全审计模块 | | | |
| 图例：   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | 用户扮演的角色 | 系统支持的业务活动 | 角色指向活动：能执行  活动指向角色：通知/调用 |  | | | | |
| **用例（业务功能）简述** | | | |
| **业务流程** | **用例名称** | **用例简述** | **业务规则** |
| 对系统各类安全事件进行日志记录 | 用户登录日志 | 1、日志记录用户登录事件 | 1、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 |
| 操作日志 | 1、日志记录用户对系统操作的事件 | 1、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 |
| 文件日志 | 1、日志记录固件包状态事件 | 1、包含系统时间、文件名称、处理类型、处理结果 |
|  | 查看日志 | 1、查看各类日志 |  |

### 系统管理模块

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| 图例：   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | 用户扮演的角色 | 系统支持的业务活动 | 角色指向活动：能执行  活动指向角色：通知/调用 |  | | | | |
| **用例（业务功能）简述** | | | |
| **业务流程** | **用例名称** | **用例简述** | **业务规则** |
|  | 用户管理 | 1、系统用户的新增、删除、修改、查看 |  |
|  | 权限管理 | 1、给各类用户分配系统权限 |  |

# 接口与界面

### 2.1硬件接口

| **硬件名称** | **硬件类型** | **软硬件交互数据性质** | **通信协议** |
| --- | --- | --- | --- |
| 服务器密码机 | 服务器 | 通过调用加密机接口以硬件方式实现密钥管理、文件加密、密钥导出等业务。传输二进制数据。 | TCP/IP |
| CDN存储服务器 | 服务器 | 通过外部接口传入文件URL，向外部CDN存储服务获取/推送文件 | https |
|  |  |  |  |

### 2.2软件接口

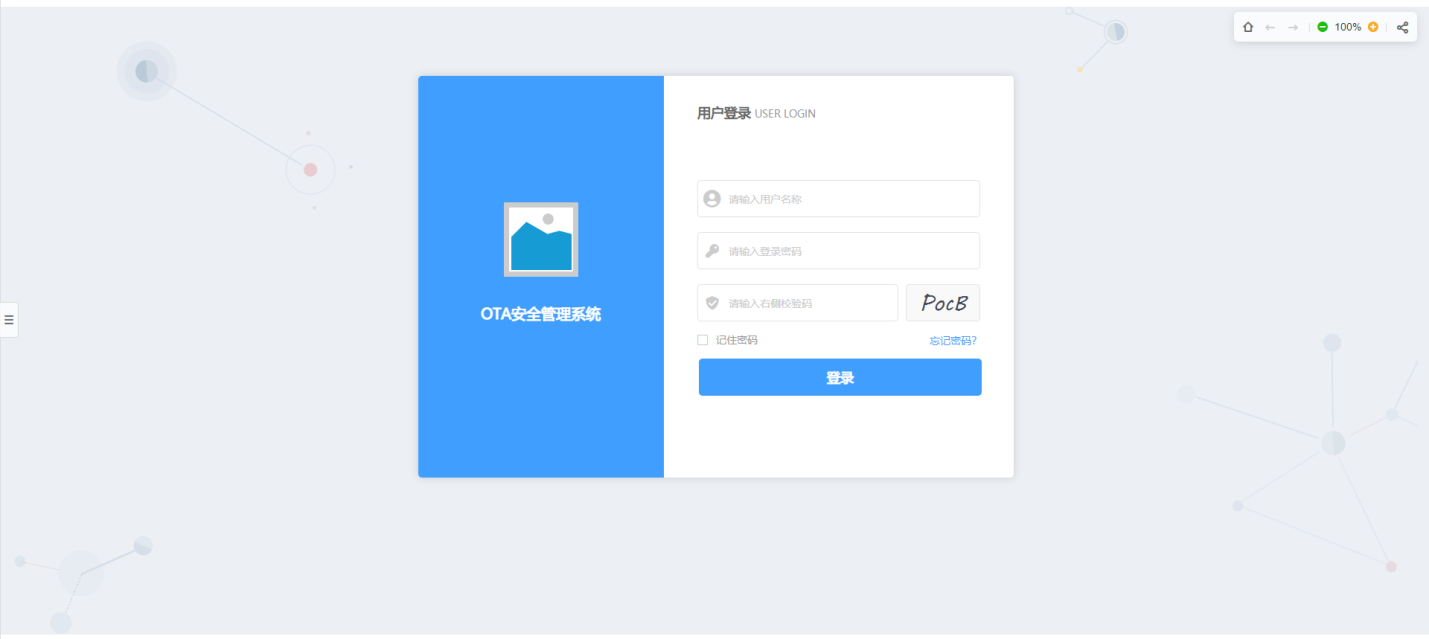
无特殊要求

### 2.3通信接口（可选）

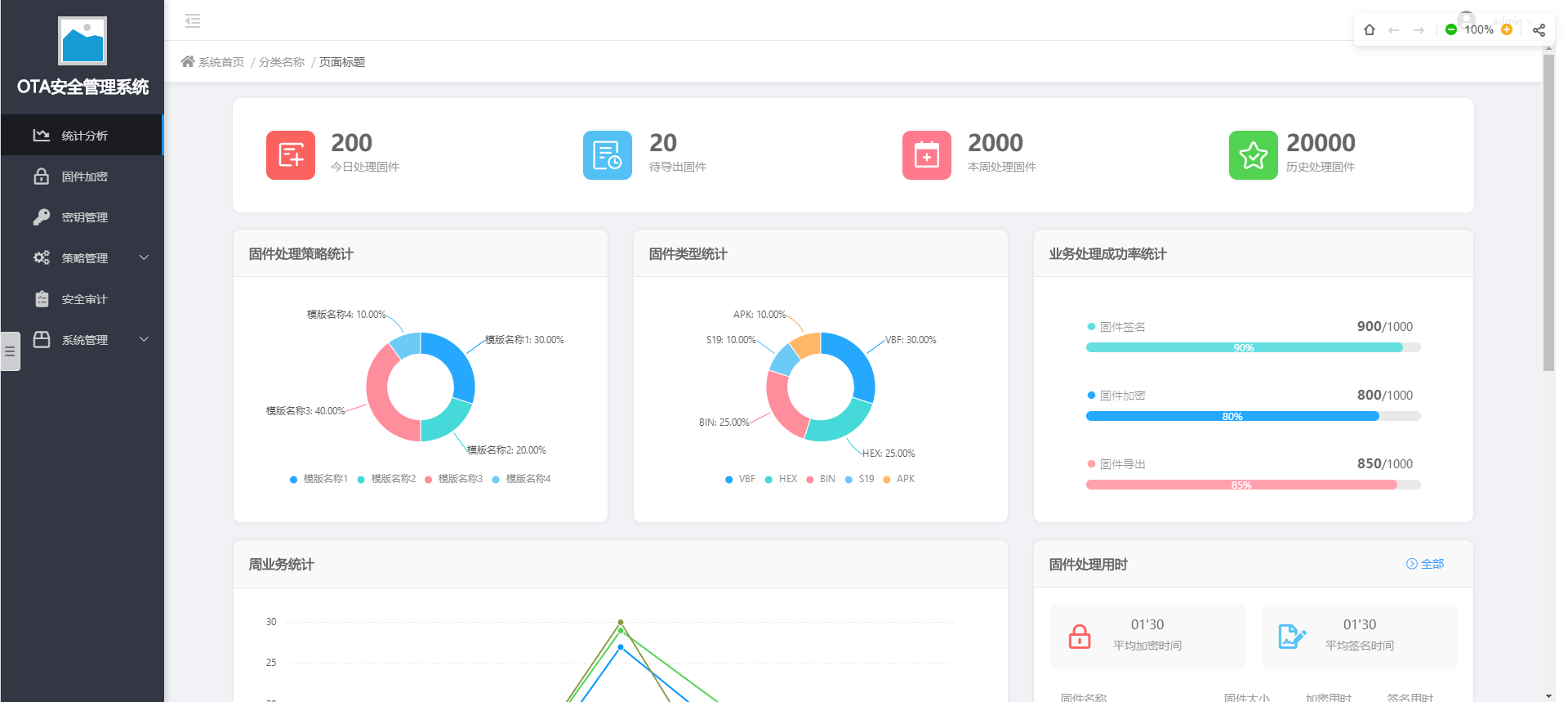
无特殊要求

### 2.4 用户界面

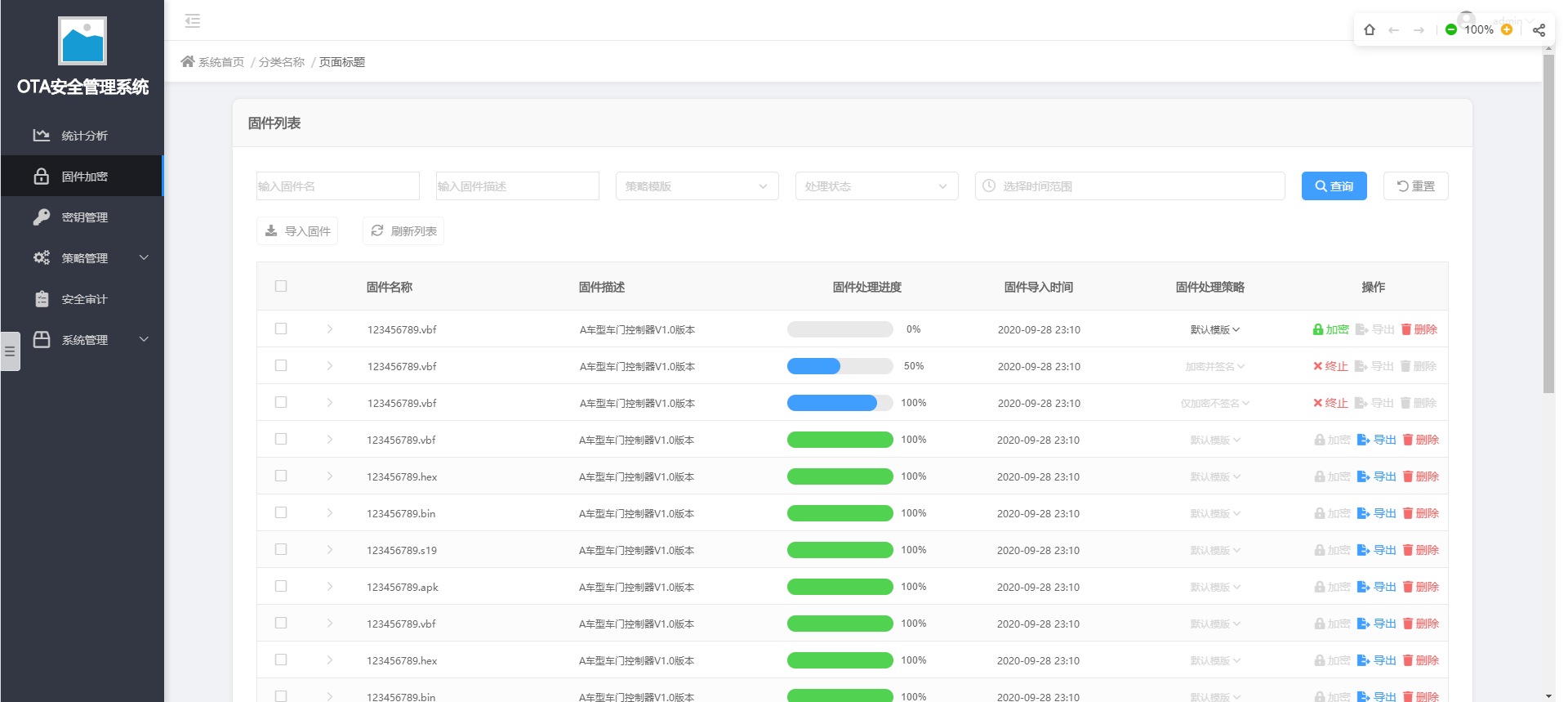
* 系统登录：用户登录Web系统



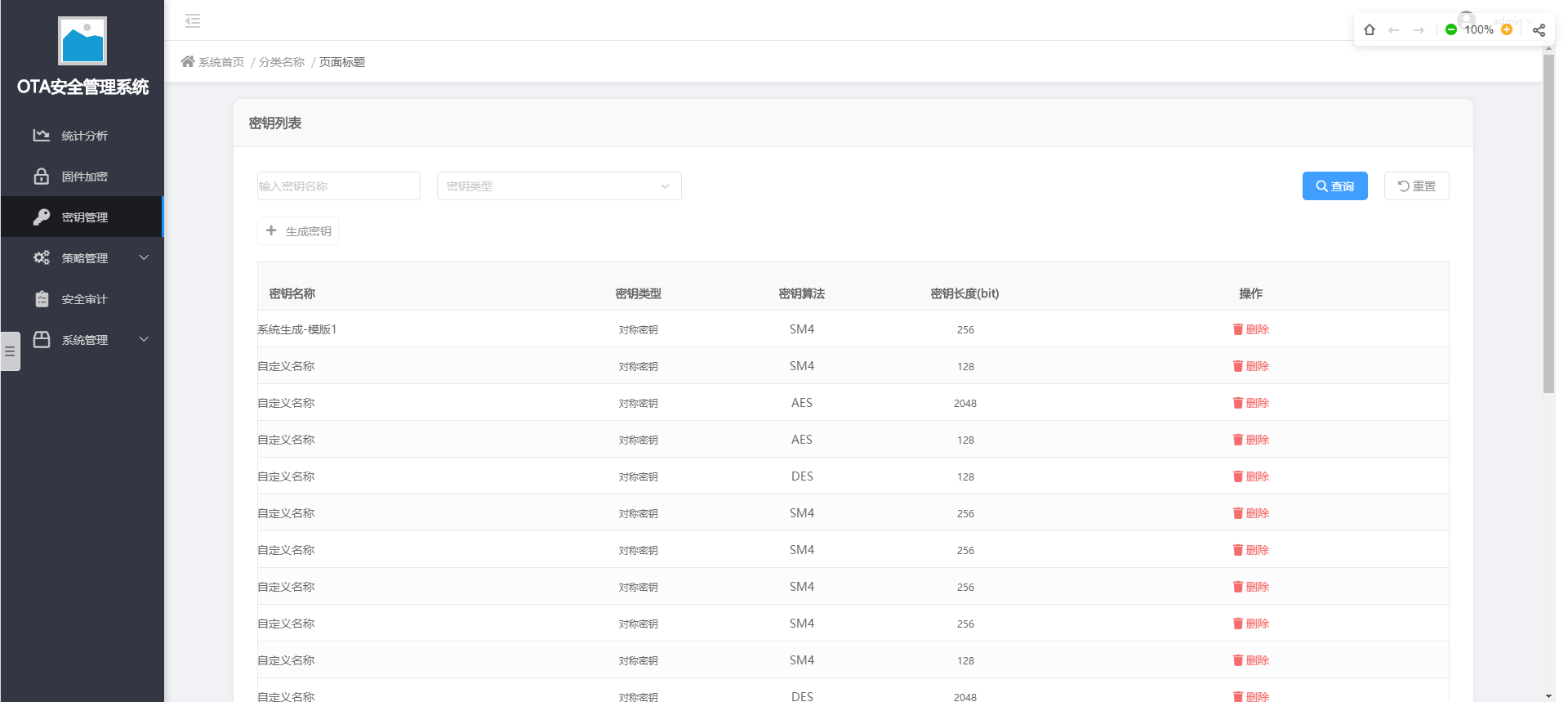
* 系统首页：登录后系统首页，主要为系统数据分析页面，包括对处理策略的统计、加密固件类型的统计、以及相关业务指标的统计；



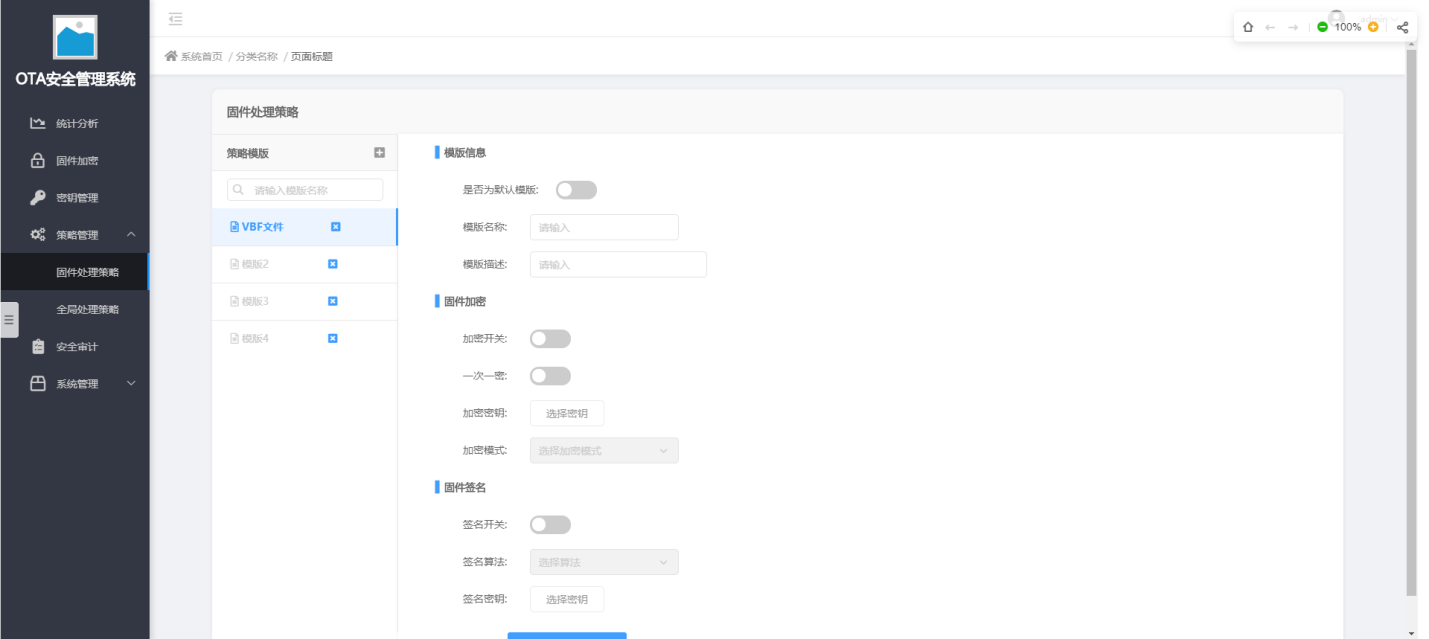
* 固件加密：主要用来显示用户接口以及外部接口对获取到的文件进行加密处理的操作及过程，包括固件的上传、查询、固件列表以及详情查看等；

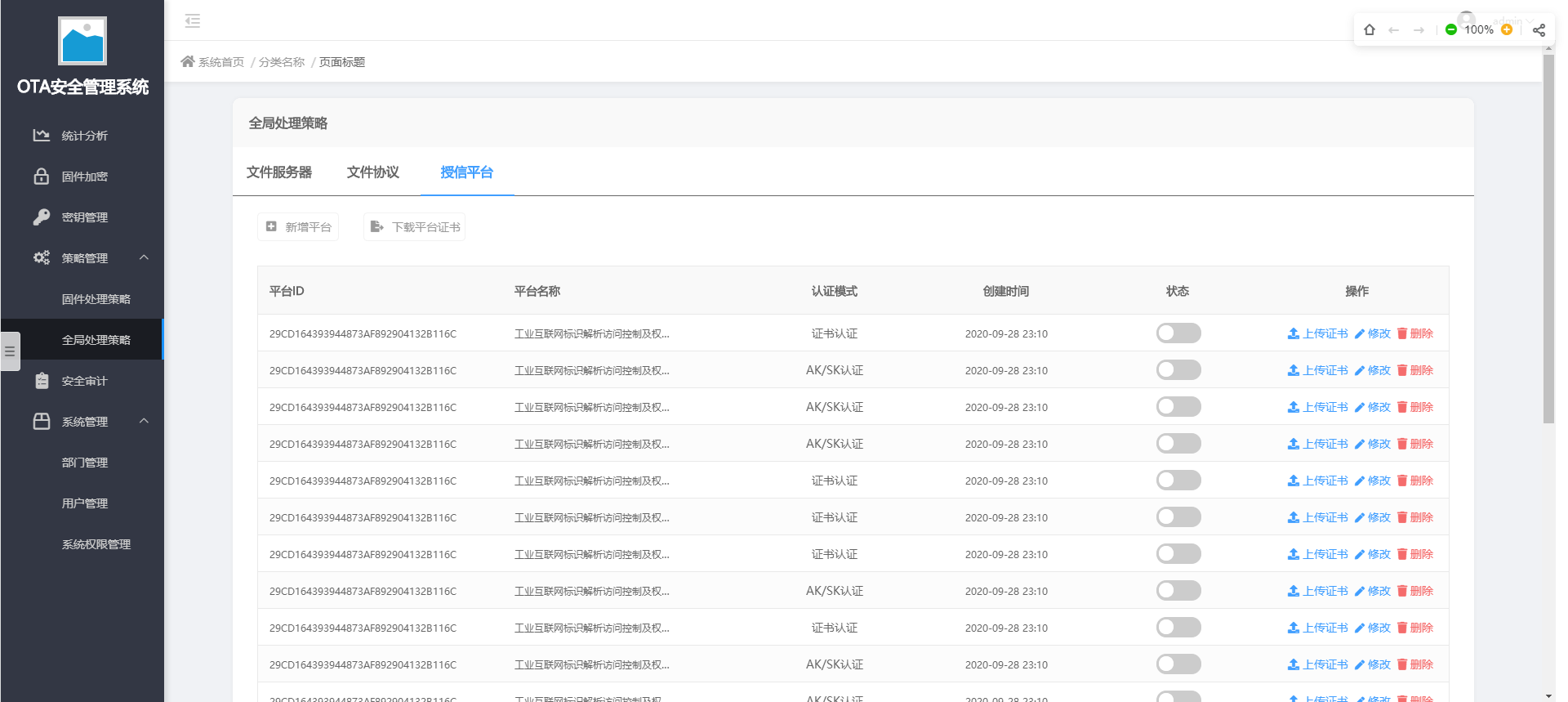


* 密钥管理：主要用来显示系统内存储的密钥以及对密钥的全生命周期管理；

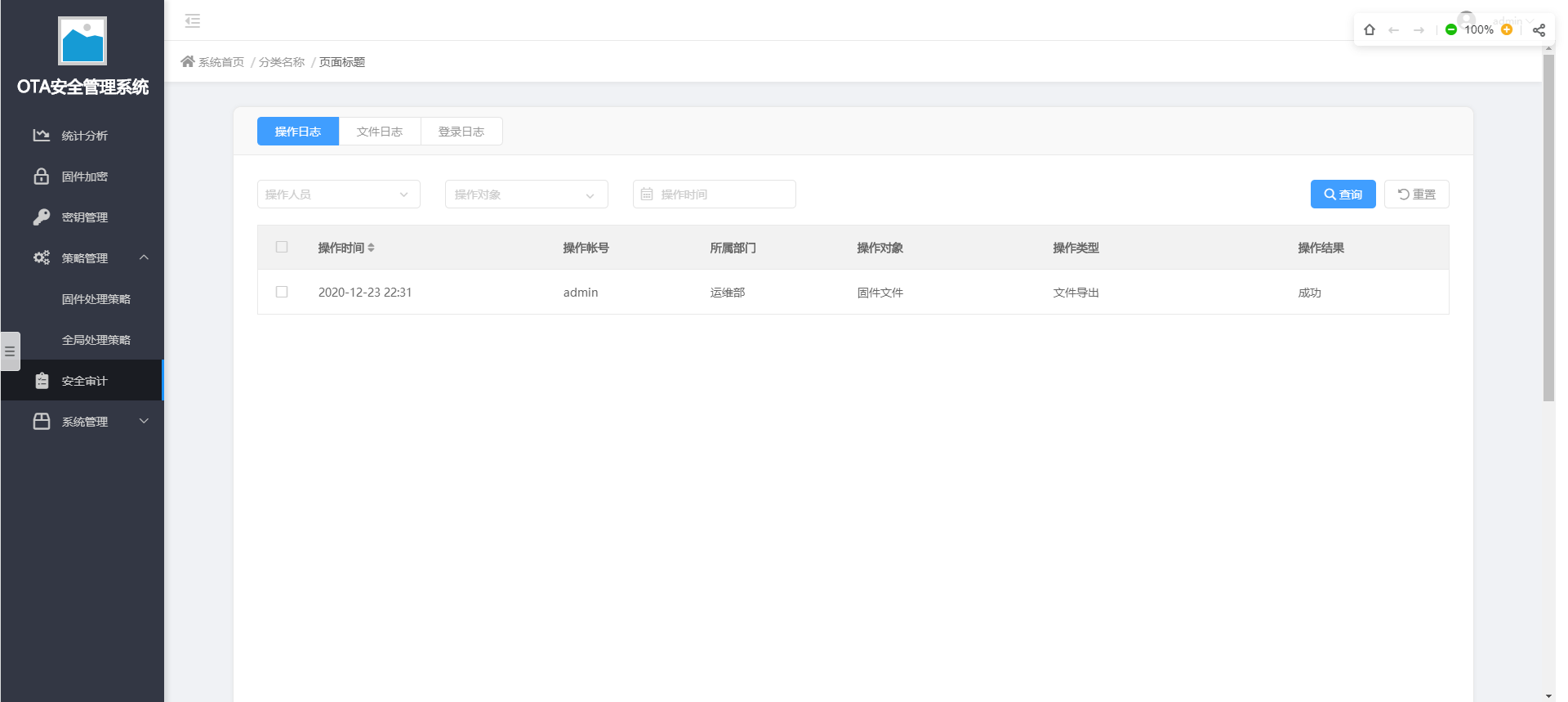


* 策略管理：主要用于管理系统策略，包含固件处理策略和全局策略两个子模块，固件处理策略包含策略模板的新增、删除、查询以及对模板策略的详细配置；全局策略包含文件存储服务、授信平台等配置；

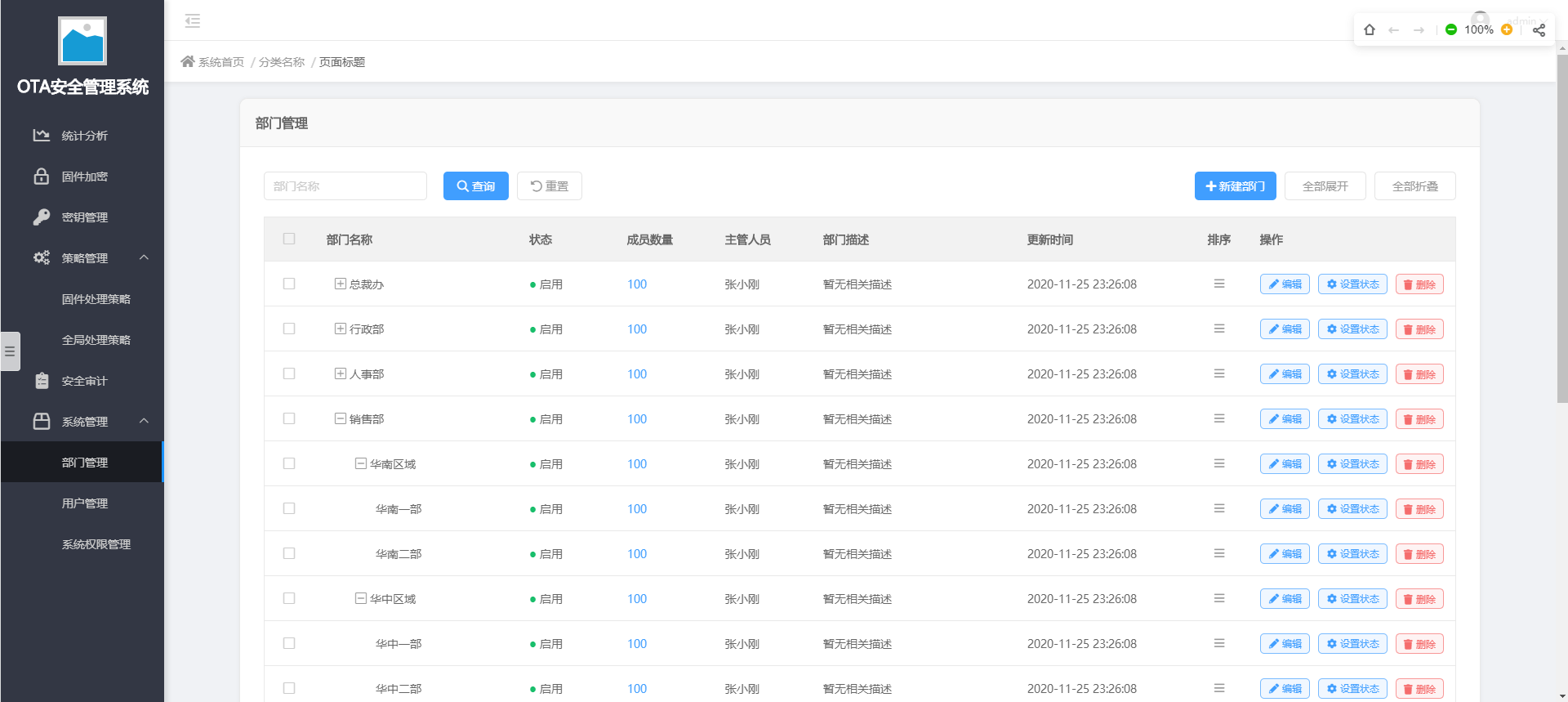


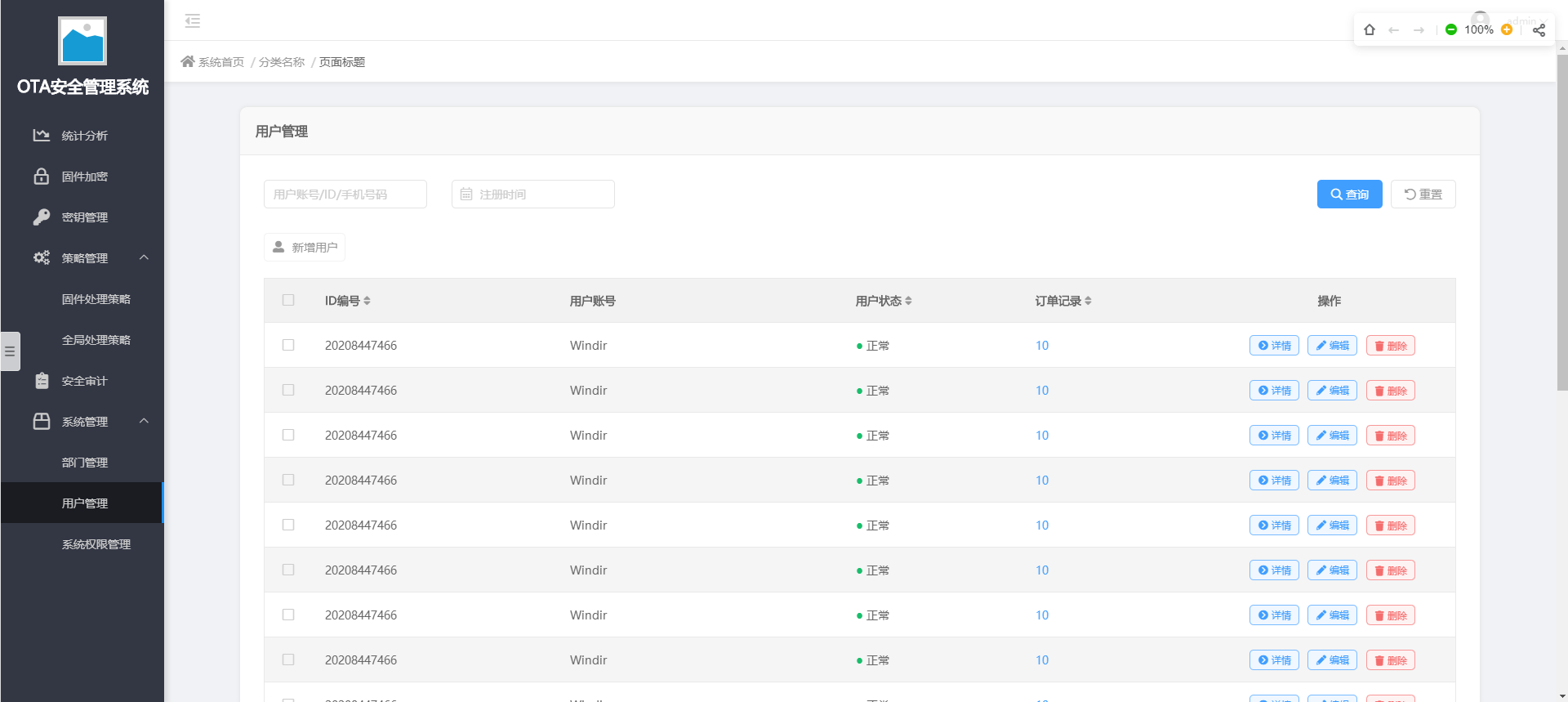


* 安全审计：用于查看系统各类日志，包括用户操作日志、文件日志以及登录日志。



* 系统管理：用于对部门、用户以及权限的管理，包含部门管理、用户管理、权限管理三个子模块，可对组织架构、系统用户、角色及权限做相关配置；

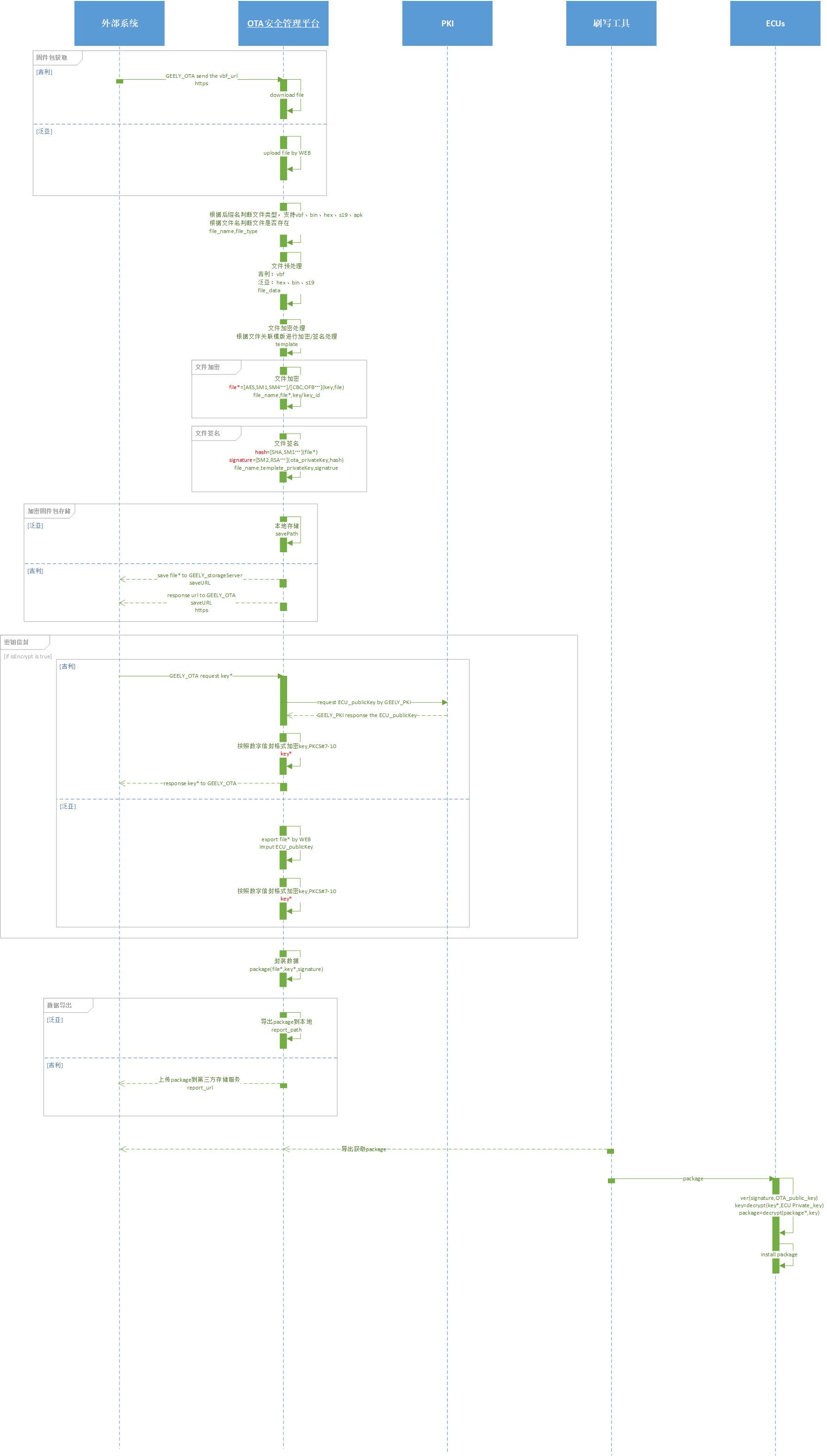




# 功能需求

## 系统流程图

系统核心业务流程，包括固件的获取/导入、固件加密/签名处理、固件上传/导出；

**

## 功能一览表

*【显示出业务和系统功能的关系，以及优先级(高、中、低)。】*

|  |  |  |  |
| --- | --- | --- | --- |
| **功能编号** | **系统功能名称** | **对应业务需求描述** | **优先级** |
| **OTA-SRS-KM-01** | **密钥列表** | F1-1 | **高** |
| **OTA-SRS-KM-02** | **密钥查询** | F1-2 | **高** |
| **OTA-SRS-KM-03** | **密钥生成** | F1-3 | **高** |
| **OTA-SRS-KM-04** | **保护密钥导入** | F1-4 | **低** |
| **OTA-SRS-KM-05** | **密钥导出** | F1-4 | **高** |
| **OTA-SRS-KM-06** | **密钥删除** | **——** | **低** |
| **OTA-SRS-KM-07** | **公钥复制** | F1-5 | **高** |
| **OTA-SRS-FW-01** | **固件列表** | F2-1 | **高** |
| **OTA-SRS-FW-02** | **固件查询** | F2-3 | **高** |
| **OTA-SRS-FW-03** | **固件详情** | F2-2 | **高** |
| **OTA-SRS-FW-04** | **固件导入** | F2-4 | **高** |
| **OTA-SRS-FW-05** | **固件解析** | F2-5 | **高** |
| **OTA-SRS-FW-06** | **固件加密** | F2-7 | **高** |
| **OTA-SRS-FW-07** | **固件存储** | F2-6 | **高** |
| **OTA-SRS-FW-08** | **固件导出** | F2-9 | **高** |
| **OTA-SRS-FW-09** | **固件删除** | F2-8 | **高** |
| **OTA-SRS-TP-01** | **策略模版列表** | F3-1 | **高** |
| **OTA-SRS-TP-02** | **查询策略模版** | F3-2 | **高** |
| **OTA-SRS-TP-03** | **新建策略模版** | F3-3 | **高** |
| **OTA-SRS-TP-04** | **修改策略模版** | F3-4 | **高** |
| **OTA-SRS-TP-05** | **配置默认策略模版** | F3-6 | **高** |
| **OTA-SRS-TP-06** | **删除策略模版** | F3-5 | **高** |
| **OTA-SRS-GC-01** | **文件服务器** | F2-6 | **低** |
| **OTA-SRS-LOG-01** | **系统登录日志** | F4-1 | **高** |
| **OTA-SRS-LOG-02** | **用户操作日志** | F4-2 | **高** |
| **OTA-SRS-LOG-03** | **固件日志** | F4-3 | **高** |
| **OTA-SRS-LOG-04** | **查看日志** | F4-1、F4-2、F4-3 | **高** |
| **OTA-SRS-LOG-05** | **查询日志** | F4-4 | **高** |
| **OTA-SRS-SM-01** | **用户管理** | **F7** | **高** |
| **OTA-SRS-SM-02** | **机构管理** | **F6** | **高** |
| **OTA-SRS-SM-03** | **权限管理** | **F5** | **高** |
| **OTA-SRS-SM-04** | **授信平台管理** | **——** | **低** |
| **OTA-SRS-DV-02** | **固件处理数量统计** | F8-1 | **高** |
| **OTA-SRS-DV-03** | **固件处理策略统计** | F8-2 | **高** |
| **OTA-SRS-DV-04** | **固件类型统计** | F8-3 | **高** |
| **OTA-SRS-DV-05** | **业务处理成功率统计** | F8-4 | **高** |
| **OTA-SRS-DV-06** | **七日业务处理情况** | F8-5 | **高** |
| **OTA-SRS-DV-07** | **固件处理用时（单固件）** | F8-6 | **高** |
| **OTA-SRS-DV-08** | **固件处理用时（平均值）** | F8-6 | **高** |
| **OTA-SRS-DV-09** | **系统使用情况** | F8-7 | **高** |
| **OTA-SRS-DV-10** | **操作日志** | **F8** | **高** |
| **OTA-SRS-DV-11** | **系统监控-负载预警** | F8-7 | **低** |

## 功能描述

### OTA安全管理系统服务端平台

#### 密钥管理模块（**OTA-SRS-KM**）

##### 密钥列表（**OTA-SRS-KM**-01）

###### 流程图

无

###### 前提条件

1. 业务操作员权限

###### 输入

无

###### 处理步骤

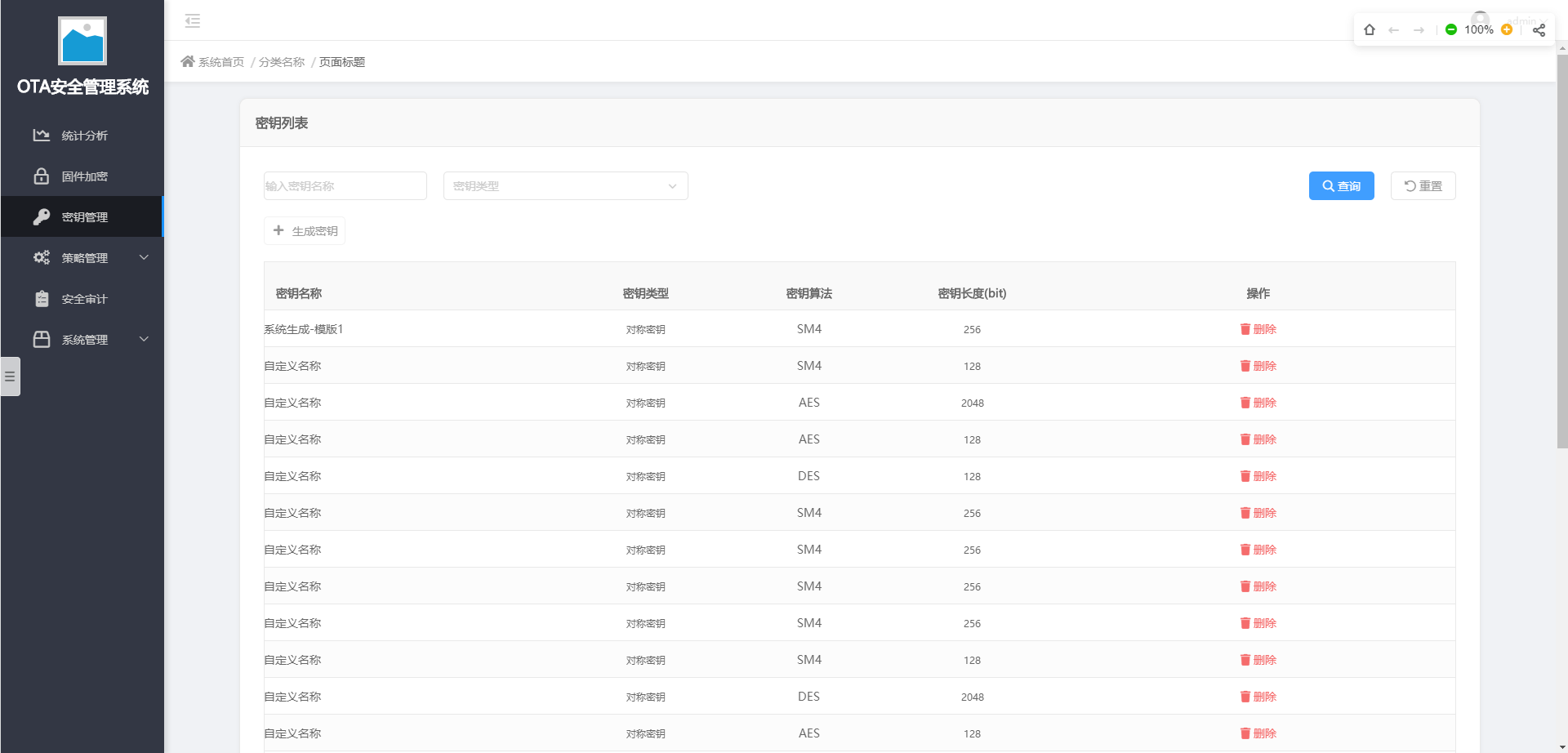
1. 业务操作员进入密钥管理模块；

###### 输出

密钥列表展示内容字段：

* 密钥名称
* 密钥类型
* 密钥算法
* 密钥长度
* 密钥操作【复制】

原型



###### 规约

1. 密钥名称为生成密钥时输入的名称，系统一次一密自动生成的密钥名称为：模版名称-系统生成；
2. 密钥长度单位为bit；
3. 固件操作按钮显示规则：
4. 仅非对称密钥复制按钮可见

##### 密钥查询（**OTA-SRS-KM**-02）

###### 流程图

无

###### 前提条件

1. 业务操作员权限；

###### 输入

1. 密钥名称
2. 密钥类型；

###### 处理步骤

1. 业务操作员进入密钥管理页面；
2. 在过滤器中输入密钥名称关键字或者选择密钥类型
3. 点击查询按钮；
4. 系统根据过滤器过滤出所查询的密钥信息；

###### 输出

密钥列表中展示所查询的密钥信息；

###### 规约

1. 密钥名称过滤器支持关键字模糊匹配；
2. 密钥类型的选择采用级联选项框，选项框选项为密钥类型，通过密钥类型、密钥算法做级联选项框默认选项为选择提示语

##### 密钥生成（**OTA-SRS-KM-03**）

###### 流程图

**

###### 前提条件

1. 业务操作员权限；
2. 安全组件调通；

###### 输入

1. 密钥名称
2. 密钥配置参数：密钥类型、算法类型、加密模式、密钥长度

###### 处理步骤

1. 业务操作员登录系统进入密钥管理模块，在页面中点击生成密钥按钮
2. 弹框中输入密钥名称以及选择密钥配置相关参数；
3. 系统接收输入参数后，向安全组件发送【密钥生成】请求；
4. 安全组件接收到请求后，生成密钥，此处称为业务密钥；
5. 安全组件生成密钥后，返回【密钥密文】（此密钥密文由安全组件LMK加密得到）；
6. 系统接收到【密钥密文】后将密钥相关信息储存至数据库；
7. 反馈执行结果；

###### 输出

返回成功：提示处理成功，返回密钥列表，列表及数据库中新增密钥条目。

返回失败：提示失败以及失败原因【安全组件通信异常】；

###### 规约

1. 密钥名称：必填项，可重复，字符串类型，0~255byte；
2. 密钥配置参数为级联选项框；

原型图



##### 密钥信封（**OTA-SRS-KM-05**）

通过PKCS#7数字信封格式将固件包的签名值、加密密钥导出，在固件包导出内部实现，最终和固件包一起导出下载。

###### 流程图

**

###### 前提条件

1. 业务操作员权限；
2. 进行固件包导出操作；
3. 安全组件已正常部署；

###### 输入

1. 保护密钥；

###### 处理步骤

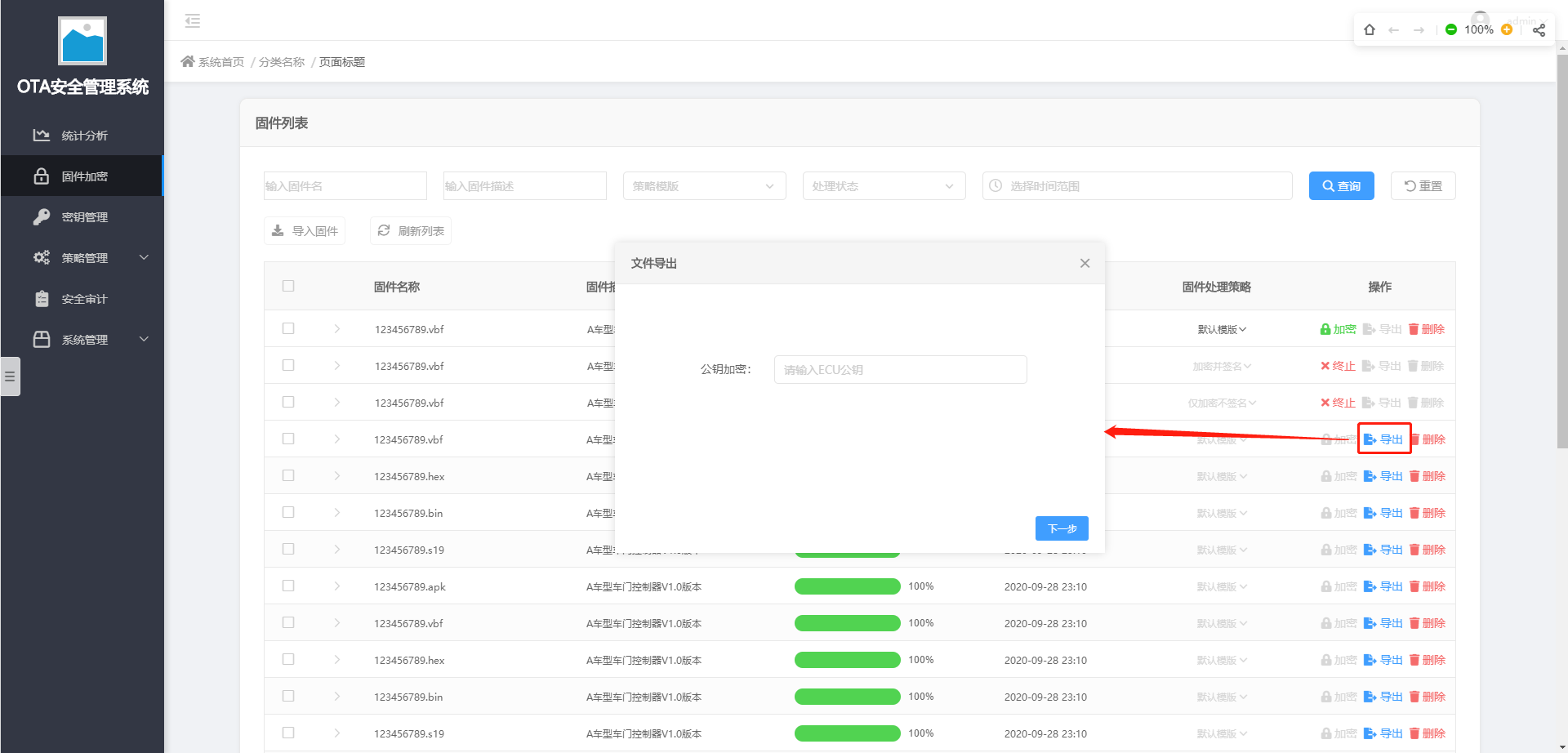
1. 业务操作员进行固件包导出操作；
2. 系统判断该固件包处理类型；
3. 获取保护密钥、查询加密密钥密文、查询签名密钥密文；
4. 向安全组件传入参数请求制作P7密钥信封；
5. 安全组件返回P7密钥信封；
6. 打包压缩；
7. 反馈处理结果；

###### 输出

返回成功：提示操作成功，页面弹出下载；

返回失败：提示失败及失败原因【保护密钥格式错误、未查找到加密密钥或签名密钥、安全组件通信异常】；

原型图



###### 规约

1. 密钥信封以文件一起打包压缩，压缩格式为zip
2. 密钥信封格式为标准PKCS#7格式
3. 若固件包加密，加密密钥需要用保护密钥做加密；
4. 输入保护公钥的格式必须符合X.509定义的公钥格式

##### 公钥复制（**OTA-SRS-KM**-07）

复制系统中非对称密钥的公钥到剪切板。

###### 流程图

无

###### 前提条件

1. 业务操作员权限；
2. 系统中有密钥；
3. 该密钥类型为非对称密钥；

###### 输入

无

###### 处理步骤

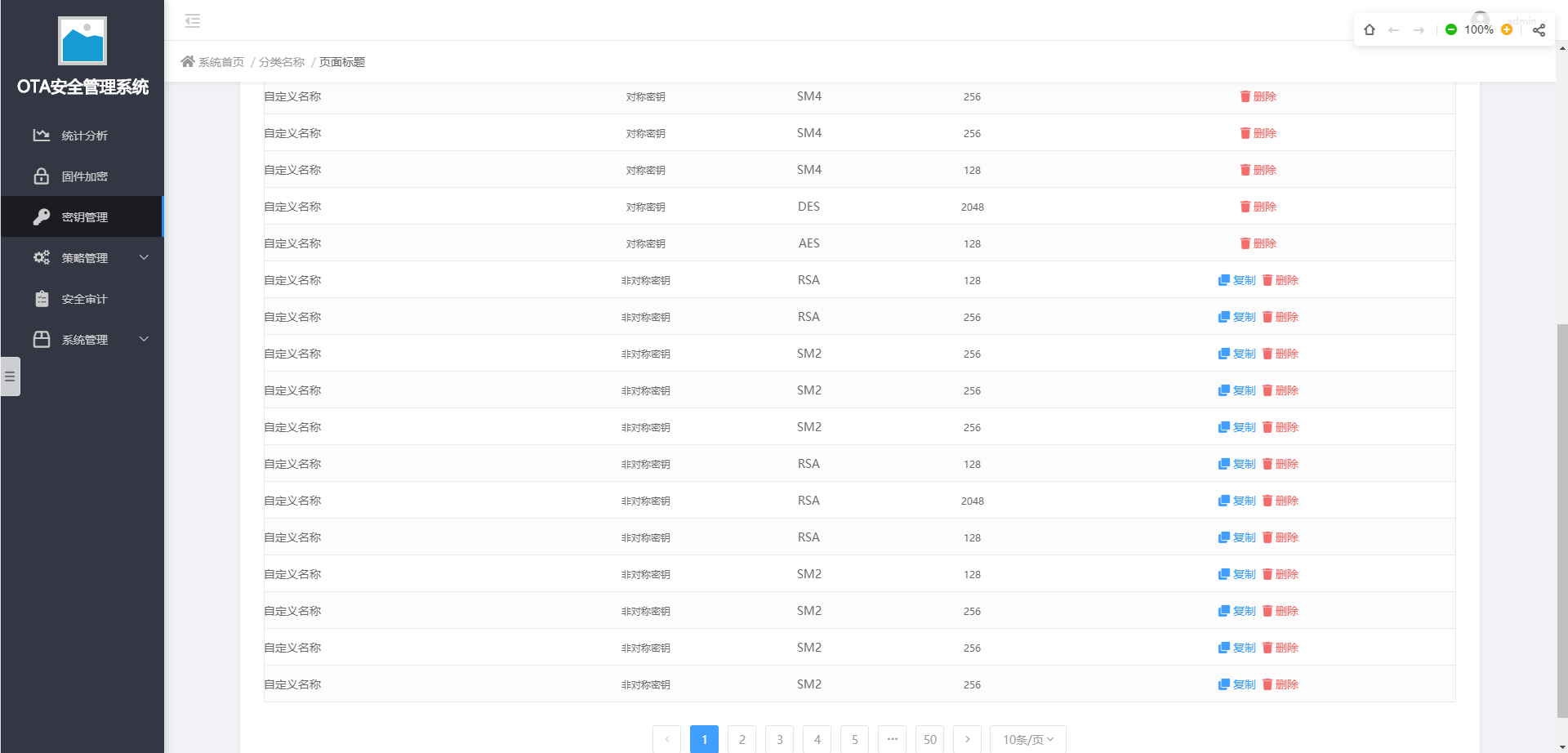
1. 业务操作员进入密钥管理模块；
2. 在密钥列表的操作列对非对称密钥点击复制操作按钮；
3. 系统查找密钥相关信息；
4. 系统将公钥复制在剪切板；
5. 反馈操作结果；

###### 输出

返回成功：提示操作成功，公钥已复制在剪切板，用户可粘贴自行使用；

返回失败：提示失败；

原型图



###### 规约

*【描述此功能在业务或数据上的约束条件。例如：用户名必须是8位字母或数字组成。】*

1. 只有非对称密钥可进行复制操作；
2. 复制到系统剪切板的为公钥；
3. 采用公钥明文方式复制；

#### 固件管理模块（**OTA-SRS-FW**）

##### 固件列表（**OTA-SRS-FW**-01）

展示系统中已存在的固件信息。

###### 流程图

无

###### 前提条件

1. 业务操作员权限

###### 输入

无

###### 处理步骤

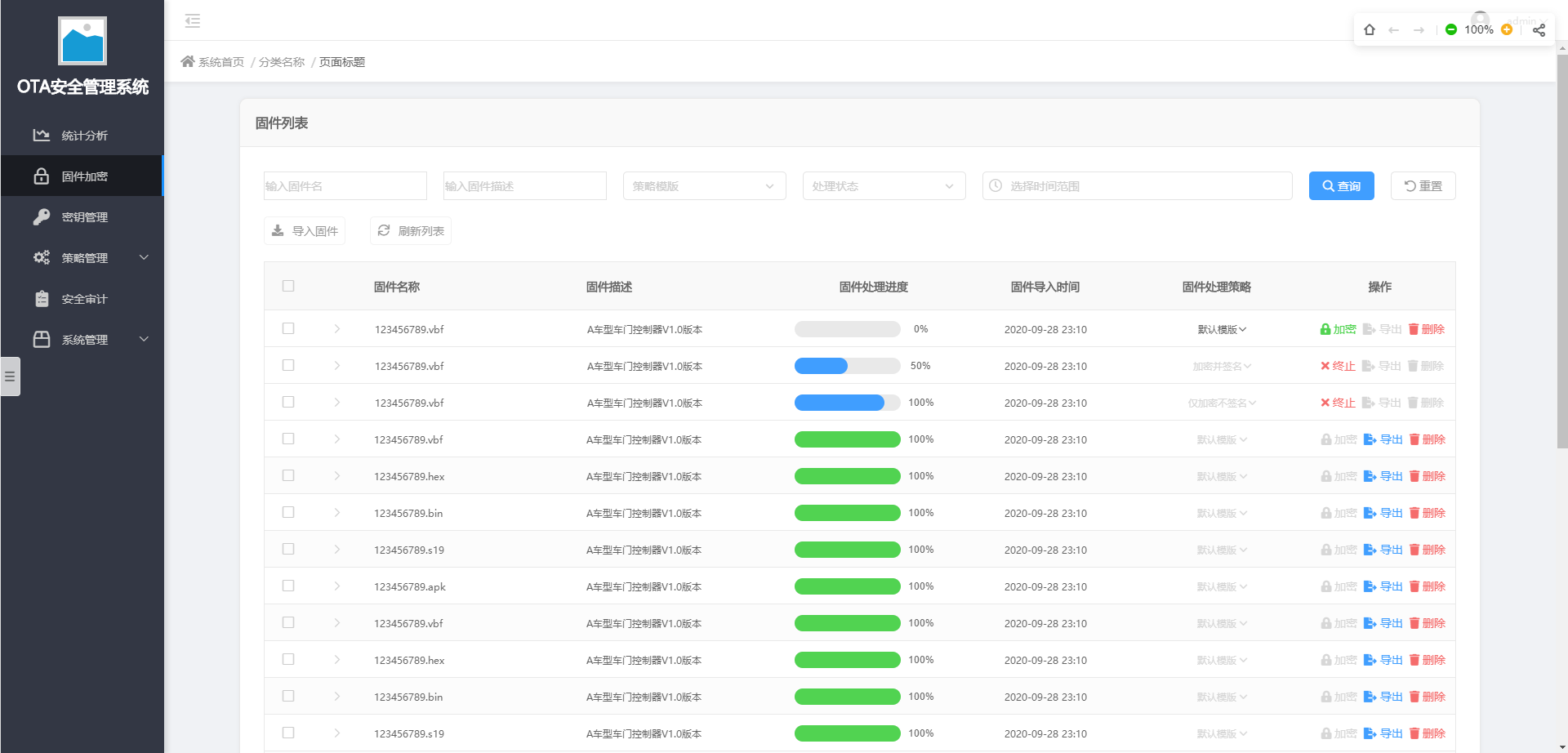
1. 业务操作员进入固件加密模块；

###### 输出

固件列表展示内容字段：

* 固件名称
* 固件描述
* 固件处理进度
* 固件导入时间
* 固件处理策略
* 固件操作【加密、导出、删除、查看详情】

原型图



###### 规约

1. 固件名称采用文件名+后缀名格式显示
2. 固件处理进度进度条显示规则：未处理 灰色0%；处理中 蓝色 百分比进度；处理失败 红色 100%；处理成功 绿色100%；
3. 固件导入时间显示规则：YY-MM-DD hh-mm；
4. 固件处理策略显示规则：采用选项框方式显示，选项框内容为系统中已存在的全部策略模版名称，选择规则如下：
   * + 1. 新导入的固件，默认选择系统默认的策略模版；
       2. 未处理状态、处理失败状态的固件，可选择其他策略模版；
       3. 正在处理以及处理成功的固件，不可选择策略模版；
5. 固件操作按钮显示规则：
6. 未处理状态的文件，加密和删除按钮可用，导出按钮不可用；
7. 处理中的文件，加密、导出、删除按钮均不可用；
8. 处理失败的文件，加密和删除按钮可用，导出按钮不可用；
9. 处理成功的文件，导出和删除按钮可用，加密按钮不可用；

##### 固件查询（**OTA-SRS-FW**-02）

固件列表中查询指定固件。

###### 流程图

无

###### 前提条件

1. 业务操作员权限

###### 输入

过滤器：

1. 固件名称
2. 固件描述
3. 策略模版
4. 处理状态
5. 导入时间

###### 处理步骤

1. 业务操作员进入固件加密模块；
2. 在过滤器中输入查询信息，点击查询按钮；
3. 固件列表根据过滤器查找相应内容并展示；

###### 输出

固件列表展示所查询的固件信息

###### 规约

1. 固件名称过滤器支持关键字模糊匹配；
2. 固件描述过滤器支持关键字模糊匹配；
3. 策略模版采用选项框，选项列举系统内已创建的策略模版名称；
4. 处理状态采用选项框，选项为【未处理、处理中、处理完成】；
5. 时间选择器可选时间范围；

##### 查看固件详情（**OTA-SRS-FW**-03）

查看固件相关的详细信息。

###### 流程图

无

###### 前提条件

1. 业务操作员权限
2. 固件列表中有条目

###### 输入

无

###### 处理步骤

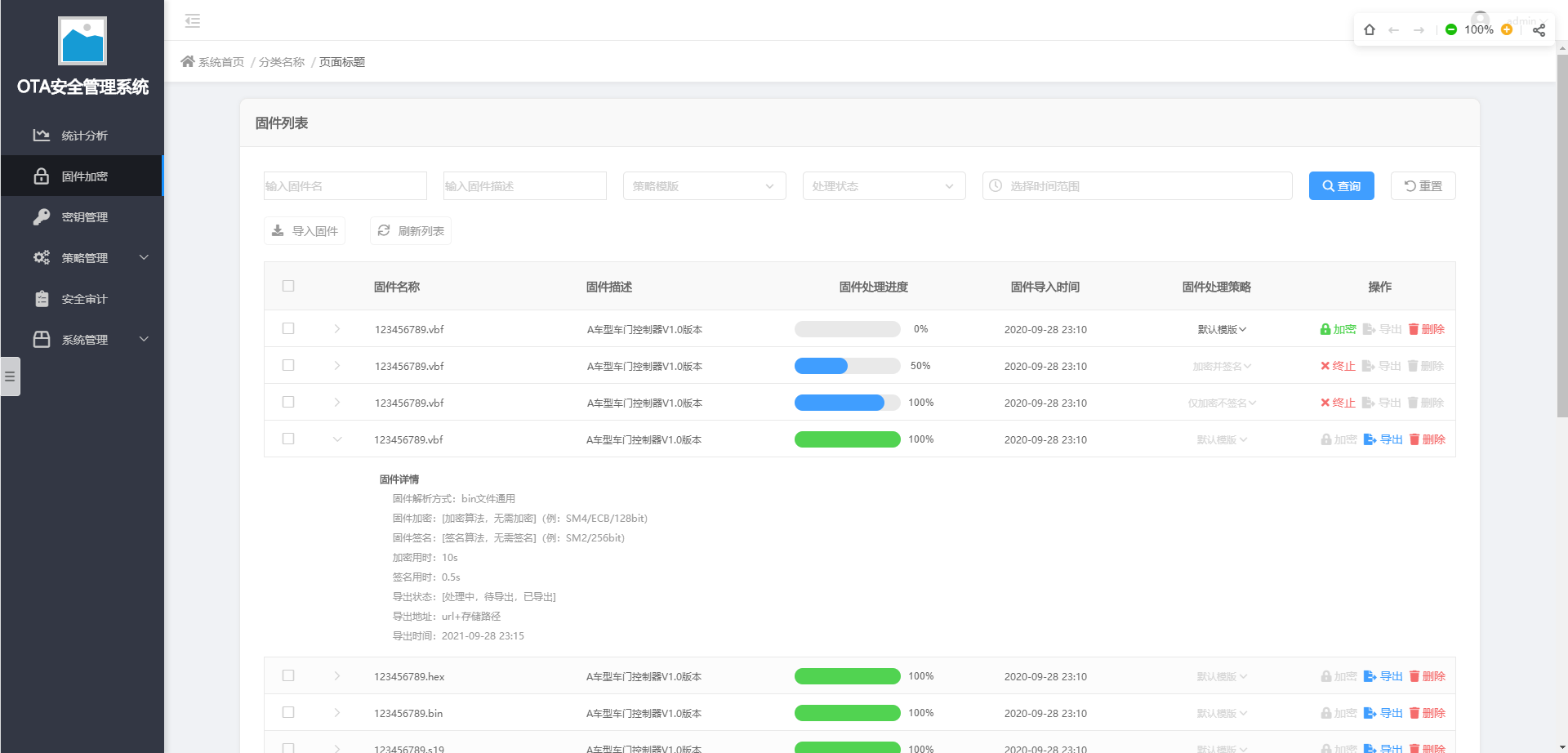
1. 业务操作员进入固件加密模块；
2. 点击固件列表中查询按钮；

###### 输出

固件详情，包含以下信息：

* 固件解析方式（解析器名称）
* 固件加密方式（读取关联的策略模版）
* 固件签名方式（读取关联的策略模版）
* 加密用时（单位：s）
* 签名用时（单位：s）

原型图



###### 规约

无

##### 固件导入（**OTA-SRS-FW**-04）

将原始固件包通过Web导入系统。

###### 流程图

**

###### 前提条件

1. 业务操作员权限；
2. 已配置好原始固件包的存储路径，且路径存在、有写入权限、磁盘空间充足；

###### 输入

1. 合法固件包、固件包解析方式、固件描述信息（非必填）；

###### 处理步骤

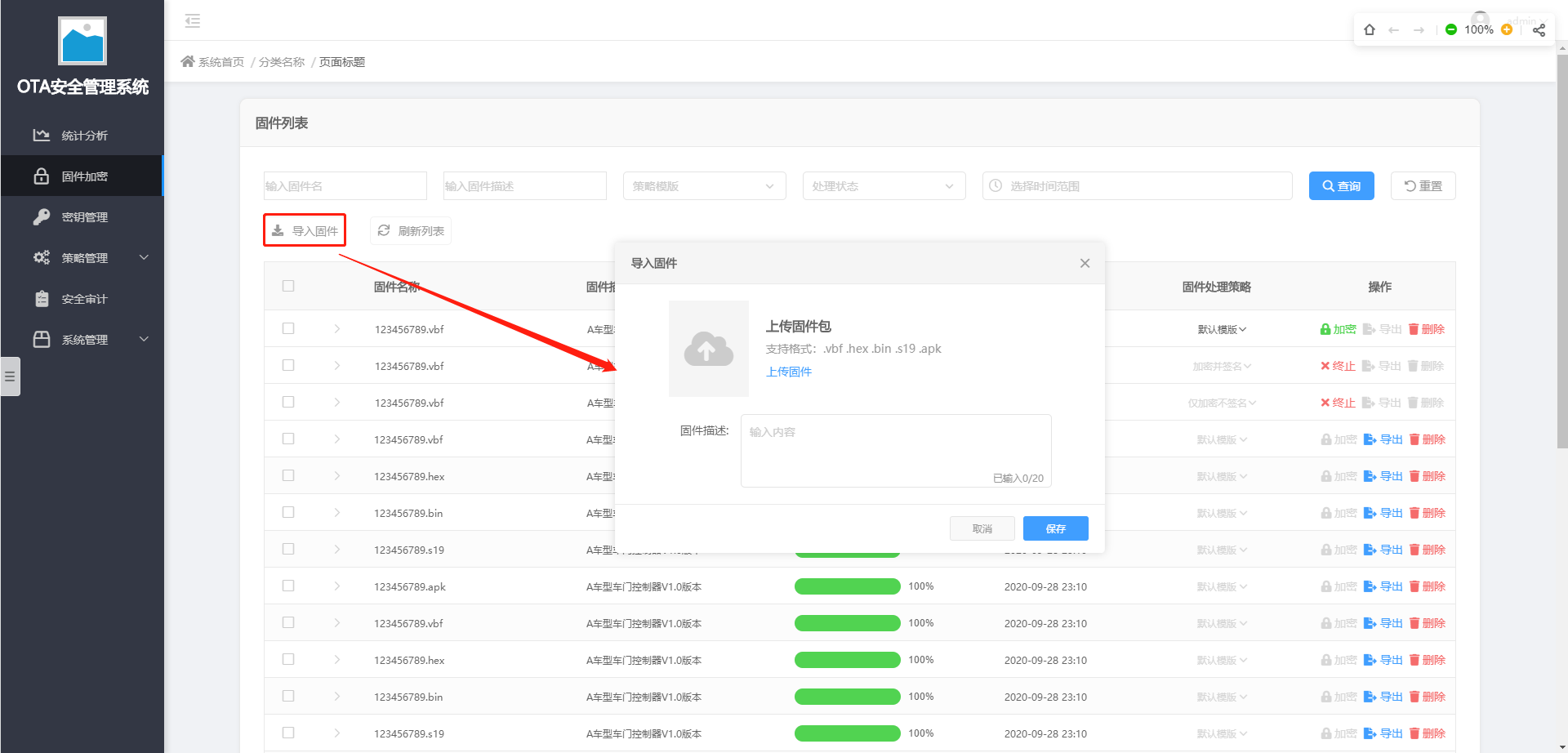
1. 业务操作员进入固件加密模块，点击导入固件按钮；
2. 弹出导入固件窗口；
3. 业务操作员上传固件包；
4. 系统根据后缀名校验固件包合法性；
5. 若固件包合法，显示固件解析方式选择框；
6. 业务操作员选择一种解析方式；
7. 业务操作员输入固件描述信息；
8. 业务操作员点击保存按钮；
9. 系统将固件包存储在指定目录，并存储固件包相关信息到数据库；
10. 反馈处理结果

###### 输出

返回成功：反馈成功，列表及数据库新增相关条目；

返回失败：提示失败以及失败原因【不支持的文件类型、已存在同名固件包、未选择处理方式、磁盘空间不足】；

原型图



###### 规约

1. 对固件包格式的校验，只校验文件后缀名；
2. 系统支持的固件包格式：vbf、hex、bin、s19、apk；
3. 固件名称：必填项，不可重复，字符串类型，0~255byte；
4. 固件描述信息：字符串类型，0~1000byte；
5. 解析方式根据固件包后缀名自动关联出系统支持的此后缀名的所有解析器；
6. 上传固件支持文件选择以及拖拽方式；
7. 固件导入需要支持同一款ECU控制器多个固件包的导入。

##### 固件解析（**OTA-SRS-FW**-05）

原始固件包的解析。

###### 流程图

**

###### 前提条件

1. 业务操作员权限
2. 完成固件包导入
3. 系统支持此格式的解析

###### 输入

无

###### 处理步骤

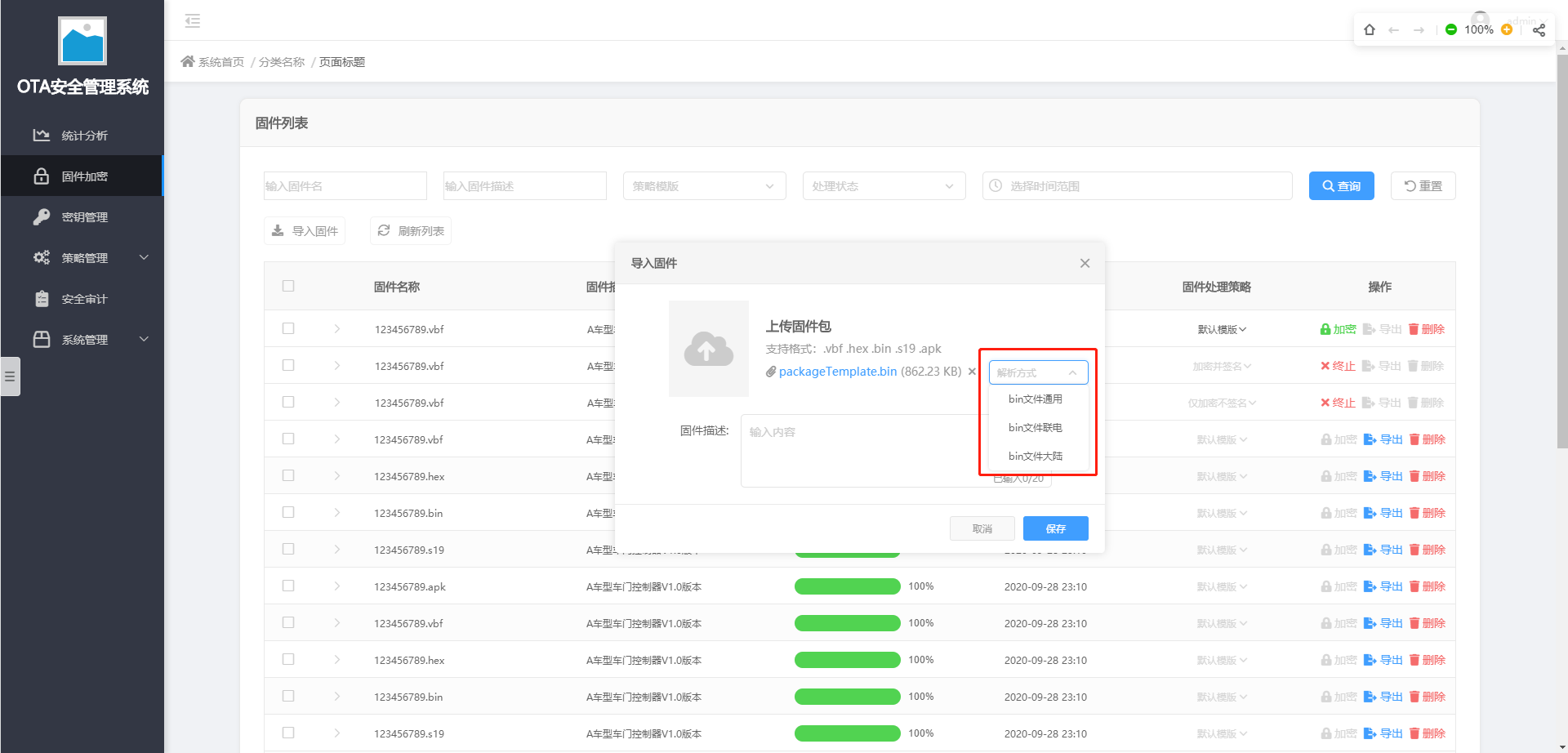
1. 业务操作员成功导入原始固件包
2. 业务操作员进行固件包加密操作
3. 系统根据导入时选择的解析器进行固件包解析
4. 解析成功后进行后续处理

###### 输出

解析成功：进行后续加密处理；

解析失败：提示加密处理失败，日志记录失败原因【固件包解析错误】

原型图



###### 规约

1. 固件解析方式的配置为原始固件包导入时根据页面提示选择解析器，后续不可修改
2. 同一后缀名的固件可能有多种不同解析方式，应在解析器选项框中支以解析器名称区分选择，***例如：hex-通用版本、hex-联成版本、hex-博世版本……***
3. 当前版本支持解析的固件包格式：hex、bin、s19（当前版本三种格式的解析器均为通用版本）

##### 固件加密（**OTA-SRS-FW**-06）

对原始固件包按照一定的策略进行加密处理。

###### 流程图

**

###### 前提条件

1. 业务操作员权限
2. 固件包为未处理状态
3. 固件包关联策略模版

###### 输入

无

###### 处理步骤

1. 业务操作员对未处理状态的固件点击加密按钮
2. 系统读取固件包关联的策略模版
3. 固件包解析
4. 按模版定义的加密策略进行处理
5. 反馈处理进度以及处理结果

###### 输出

加密中：页面进度条反馈处理进度百分比，固件状态变为处理中；

加密成功：页面反馈成功，进度条显示100%，固件状态变为已完成；

加密失败：页面反馈处理失败，进度条红色显示，固件状态变为未处理，失败原因写入日志记录；

###### 规约

1. 当前版本支持以下对固件签名和加密策略：

* 签名

1. 是否签名
2. 签名算法选择
3. 签名密钥选择

* 加密

1. 是否加密
2. 是否一次一密
3. 加密算法选择
4. 加密密钥选择（一次一密不可用）
5. 加密模式选择（一次一密不可用）
6. 新导入的固件自动关联系统默认策略模版

##### 固件存储（**OTA-SRS-FW**-07）

原始固件包、加密固件包的存储，固件导入及固件加密内部逻辑。

###### 流程图

**

###### 前提条件

1. 配置好原始固件包及加密固件包的本地存储路径
2. 业务操作员进行固件导入或固件加密操作
3. 磁盘空间充足

###### 输入

无

###### 处理步骤

*无*

###### 输出

存储成功：文件正常存储在相应目录；

存储失败：提示文件上传失败或加密处理失败及失败原因【存储路径不存在、磁盘剩余空间不足】

###### 规约

1. 固件的存储均采用本地存储方式；
2. 存储路径在配置文件中配置；

##### 固件导出（**OTA-SRS-FW**-08）

将加密后的固件包以固件包+P7密钥信封文件打包的方式导出下载。

###### 流程图

**

###### 前提条件

1. 业务操作员权限
2. 固件加密处理完成

###### 输入

1. 保护密钥（若固件加密）

###### 处理步骤

1. 业务操作员对处理完成的固件点击导出按钮
2. 若固件做了加密，则需要输入一个保护密钥，若没做加密则无需输入
3. 系统根据固件处理类型封装相应的P7信封
4. 系统将加密固件包或原始固件包与P7信封一起打包
5. 反馈处理结果以及下载提示

###### 输出

导出成功：弹出文件下载页面，下载完成后解压zip包，得到固件包和P7信封文件；

导出失败：提示固件导出失败及失败原因【生成密钥信封失败】

###### 规约

1. 若原始固件包做了加密，则导出的固件包为加密固件包，若没有加密，导出的固件包为原文件；
2. 固件包与密钥信封打包的格式为zip

##### 固件删除（**OTA-SRS-FW**-09）

删除系统中保存的固件包。

###### 流程图

无

###### 前提条件

1. 业务操作员权限
2. 固件包状态非处理中

###### 输入

无

###### 处理步骤

1. 业务操作员点击固件操作中的删除按钮
2. 系统弹框确认删除
3. 业务操作员确认删除固件
4. 删除原始固件包及加密固件包
5. 反馈操作结果

###### 输出

删除成功：反馈操作成功，固件列表中删除相应条目，若删除的固件为未处理状态，则原始固件包存储目录中删除此文件；若删除的固件做了加密且为已完成状态，则原始固件包和加密固件包的存储目录中删除此文件；

删除失败：反馈操作失败

###### 规约

1. 只可删除非处理中的固件
2. 删除操作只删除列表条目及对应的文件，不删除相关的日志记录

#### 策略管理模块（OTA-SRS-TP）

##### 策略模版列表（OTA-SRS-TP-01）

展示系统中已存在的策略模版信息。

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限

###### 输入

*无*

###### 处理步骤

1. 业务操作员进入策略管理模块；

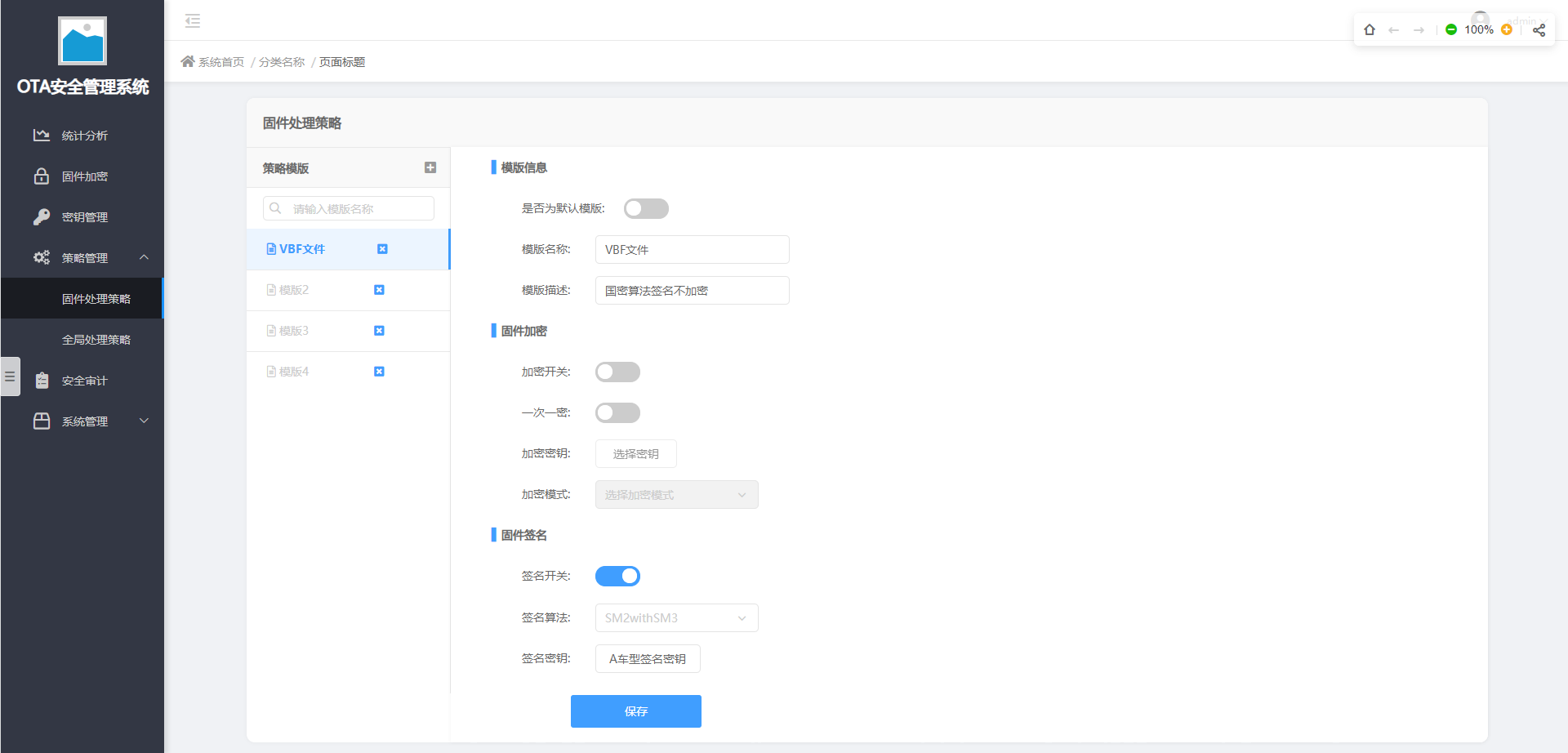
###### 输出

策略模版名称

策略模版内容

* 模版信息
  + - 是否为默认模版
    - 模版名称
    - 模版描述
* 固件加密
  + - 加密开关
    - 一次一密开关
      * 密钥类型选择
    - 加密密钥选择
    - 加密模式选择
* 固件签名
  + - 签名开关
    - 签名算法选择
    - 签名密钥选择

原型图



###### 规约

无

##### 查询策略模版（OTA-SRS-TP-02）

查询系统中的策略模版。

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限

###### 输入

1. 模版名称

###### 处理步骤

1. 业务操作员进入策略管理模块；
2. 在过滤器中输入查询信息，点击查询按钮；
3. 模版列表根据过滤器查找相应内容并展示；

###### 输出

所查询的策略模版

###### 规约

模版名称过滤器支持关键字模糊匹配

##### 新建策略模版（OTA-SRS-TP-03）

新建策略模版。

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限

###### 输入

* 是否设置为默认模版（默认不设置）
* 模版名称（必填）
* 模版描述（必填）
* 设置是否加密（默认不设置）
* 设置是否一次一密（默认不设置）
* 选择密钥类型
* 选择加密模式
* 设置是否签名（默认不设置）
* 选择签名算法
* 选择签名密钥

###### 处理步骤

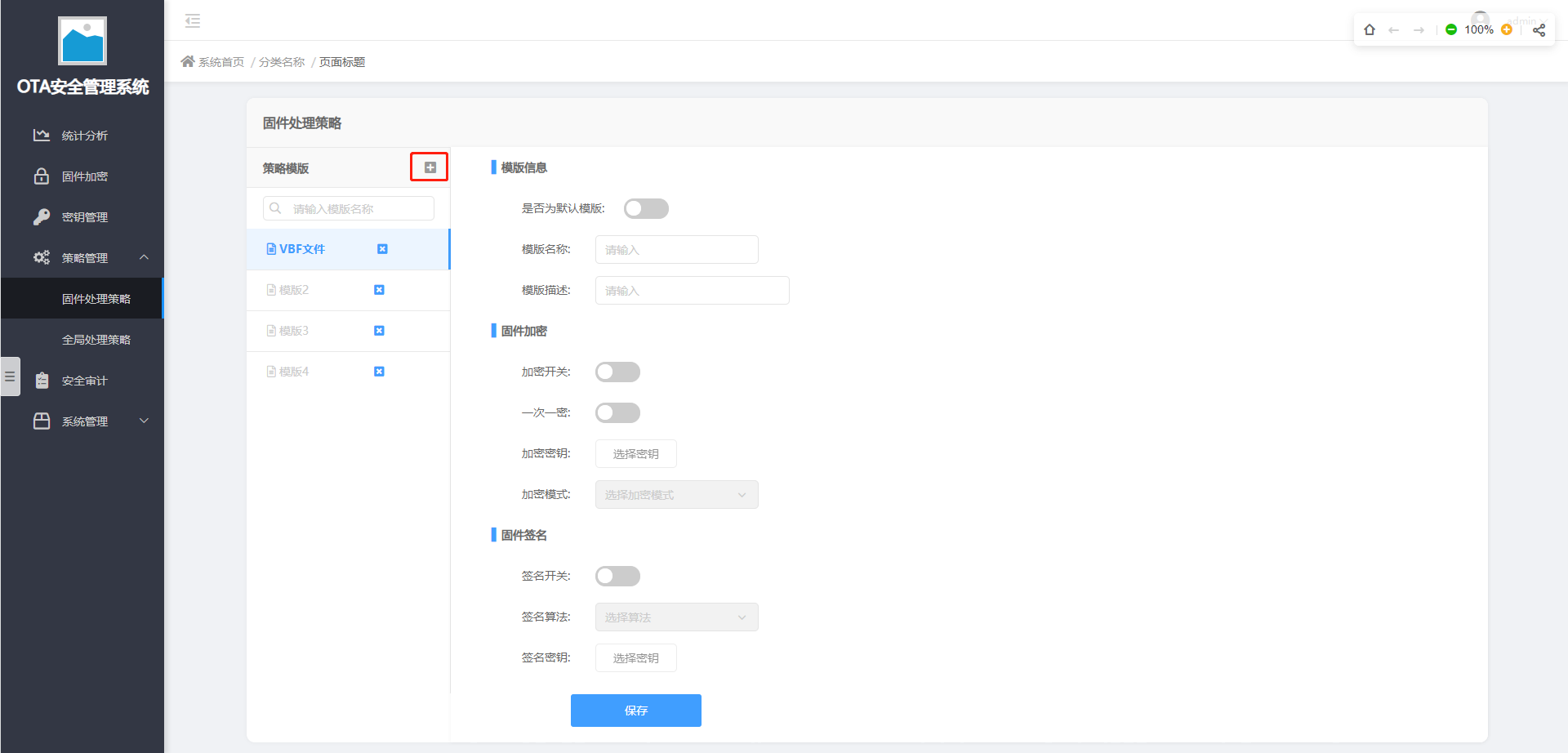
1. 业务操作员进入策略管理模块；
2. 点击新增策略模版按钮
3. 配置策略模版内容
4. 点击保存
5. 系统反馈结果

###### 输出

返回成功：提示处理成功，返回模版列表，列表及数据库中新增模版条目。

返回失败：提示失败以及失败原因【名称重复、必填项没填】；

原型图



###### 规约

1. 模版名称：必填项，不可重复，字符串类型，0~255byte
2. 模版描述信息：字符串类型，0~1000byte
3. 配置项隐藏/显示：

各配置字段可见性按照一定规则打开或关闭，详见原型

1. 配置项可用/禁用：

各配置字段可用性按照一定规则打开或关闭，详见原型

1. 选择加密/签名算法采用级联选项框
2. 选择加密/签名密钥根据算法自动关联出系统中相应的密钥

##### 修改策略模版（OTA-SRS-TP-04）

修改策略模版配置。

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限
2. 存在策略模版
3. 当前模版关联的固件包状态非处理中

###### 输入

* 是否设置为默认模版（默认不设置）
* 模版名称（必填）
* 模版描述（必填）
* 设置是否加密（默认不设置）
* 设置是否一次一密（默认不设置）
* 选择密钥类型
* 选择加密模式
* 设置是否签名（默认不设置）
* 选择签名算法
* 选择签名密钥

###### 处理步骤

1. 业务操作员进入策略管理模块；
2. 点击修改策略模版按钮
3. 修改策略模版内容
4. 点击保存
5. 系统反馈结果

###### 输出

修改成功：提示处理成功，返回模版列表，列表及数据库中数据更新，修改后配置生效；

修改失败：提示失败以及失败原因【名称重复、必填项没填、模版正在使用中】；

###### 规约

1. 修改后的配置只对未处理状态的固件生效，已处理完成的固件不会生效；
2. 待修改的模版没有关联的正在处理中的固件，否则不可修改；
3. 直接在页面修改后保存即可完成修改；

##### 默认策略模版（OTA-SRS-TP-05）

将策略模版设置为系统默认模版。

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限
2. 当前模版非默认模版

###### 输入

* 是否设置为默认模版（默认不设置）

###### 处理步骤

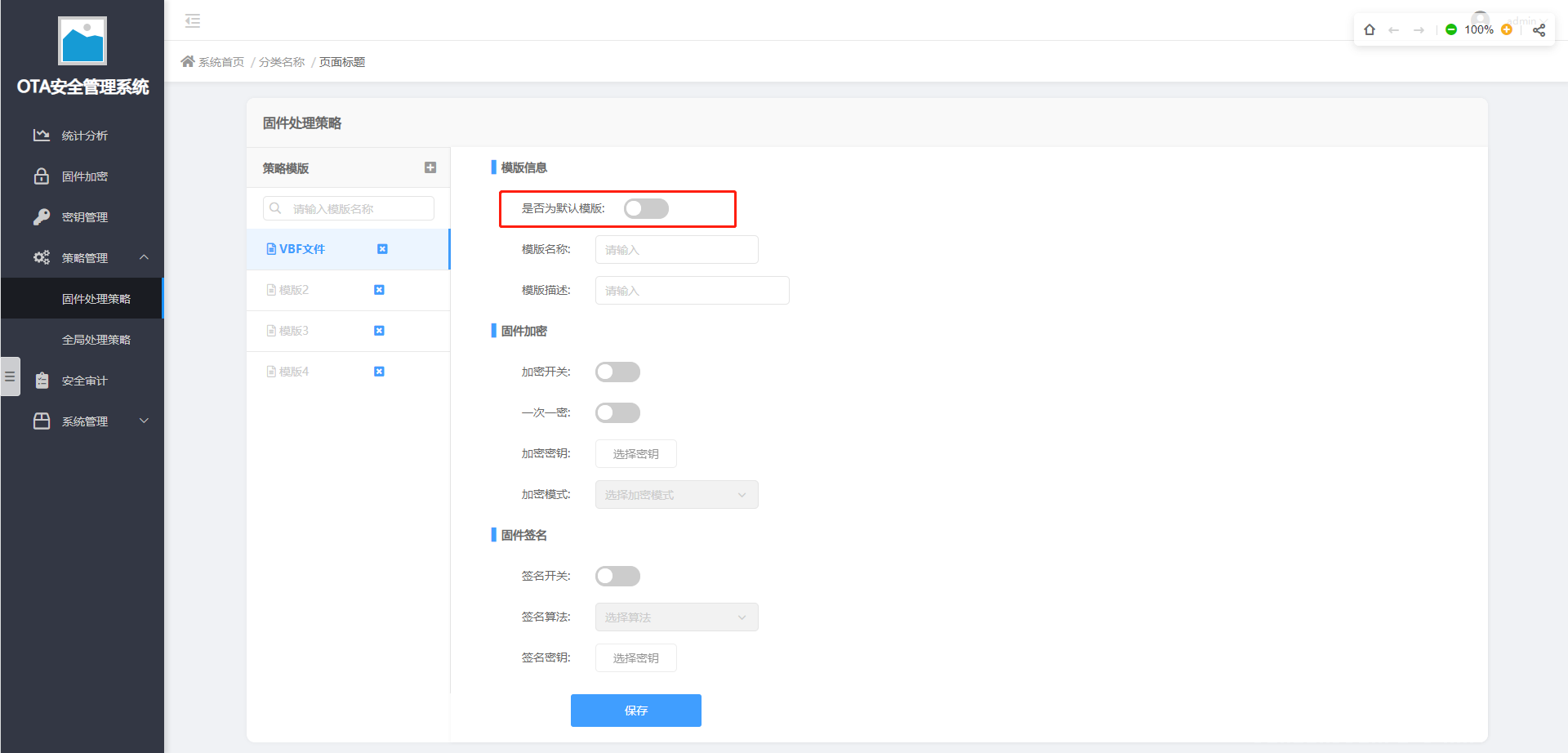
1. 业务操作员进入策略管理模块；
2. 在新增模版或修改模版页面中打开默认模版；
3. 点击保存
4. 系统反馈结果

###### 输出

设置成功：提示处理成功，返回模版列表，列表及数据库中数据更新，修改后配置生效；

设置失败：提示失败；

原型图



###### 规约

1. 默认模版全局唯一，设置新的默认模版后旧模版自动解除默认状态；
2. 文件导入后自动关联系统默认模版
3. 新的默认模版只对后续导入的文件生效，已导入的文件不会自动修改关联模版；

##### 删除策略模版（OTA-SRS-TP-06）

删除策略模版。

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限
2. 当前模版非默认模版
3. 当前模版关联的固件包状态非处理中

###### 输入

*无*

###### 处理步骤

1. 业务操作员进入策略管理模块；
2. 在模版列表中点击删除按钮；
3. 提示是否删除，删除模版将自动解除模版与固件、密钥的关联；
4. 业务操作员确认操作
5. 系统反馈结果

###### 输出

删除成功：提示处理成功，返回模版列表，列表及数据库中数据删除相应条目，文件及密钥自动解除关联；

设置失败：提示失败及失败原因【模版为系统默认模版、模版正在使用中】；

###### 规约

1. 系统默认模版不可删除；
2. 待删除的模版没有关联的正在处理中的固件，否则不可删除；
3. 删除后自动解除固件及密钥与模版的关联关系

#### 安全审计模块（OTA-SRS-LOG）

##### 系统登录日志（OTA-SRS-LOG-01）

记录系统用户登录信息。

###### 流程图

*无*

###### 前提条件

1. 配置系统用户
2. 业务操作员权限

###### 输入

无

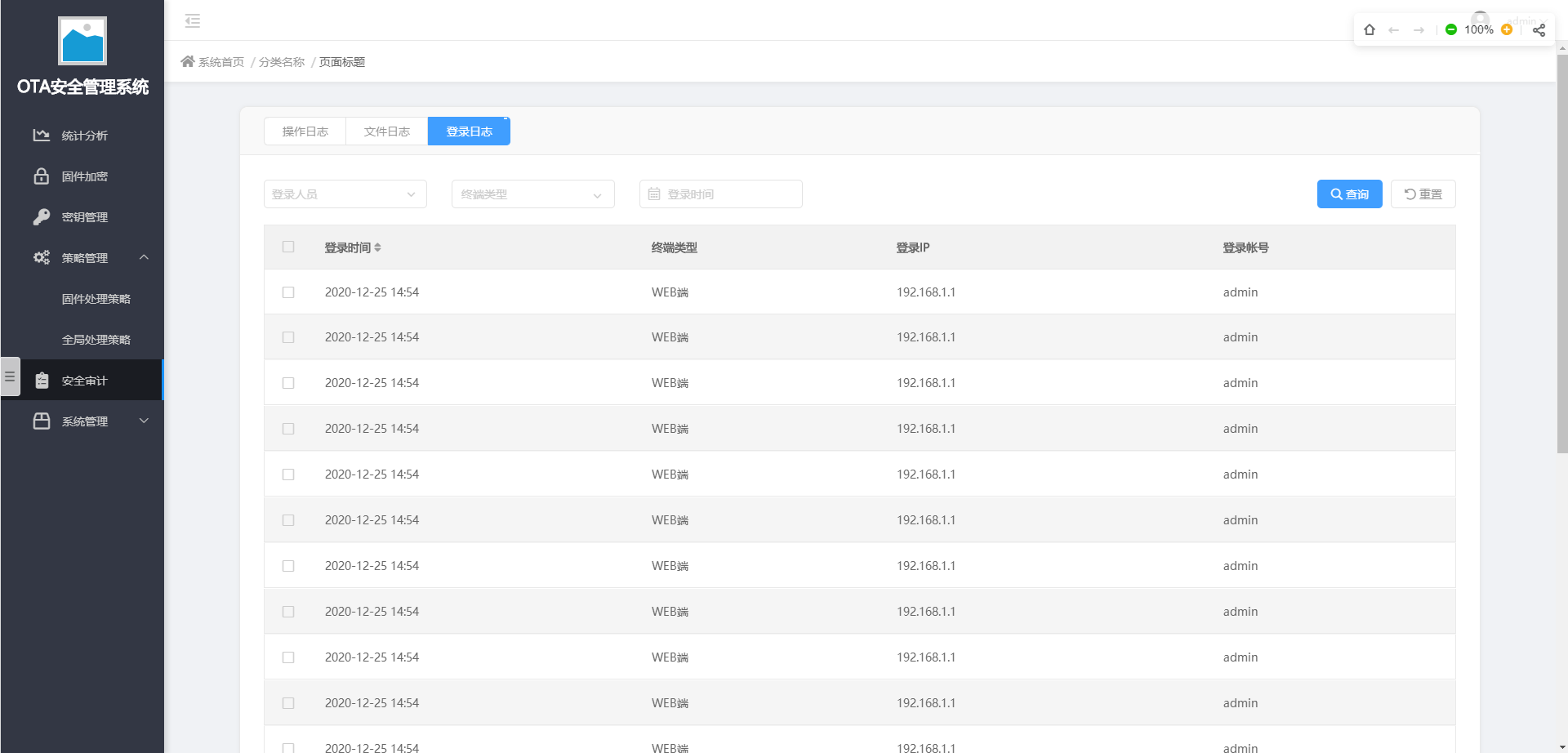
###### 处理步骤

无

###### 输出

系统登录日志列表

原型图



###### 规约

1. 日志记录字段如下：

* 登录时间（YY-MM-DD hh-mm）
* 登录终端类型
* 登录IP
* 登录帐号
* 帐号角色

##### 用户操作日志（OTA-SRS-LOG-02）

记录用户操作信息。

###### 流程图

*无*

###### 前提条件

1. 配置系统用户
2. 用户登录系统
3. 用户执行操作

###### 输入

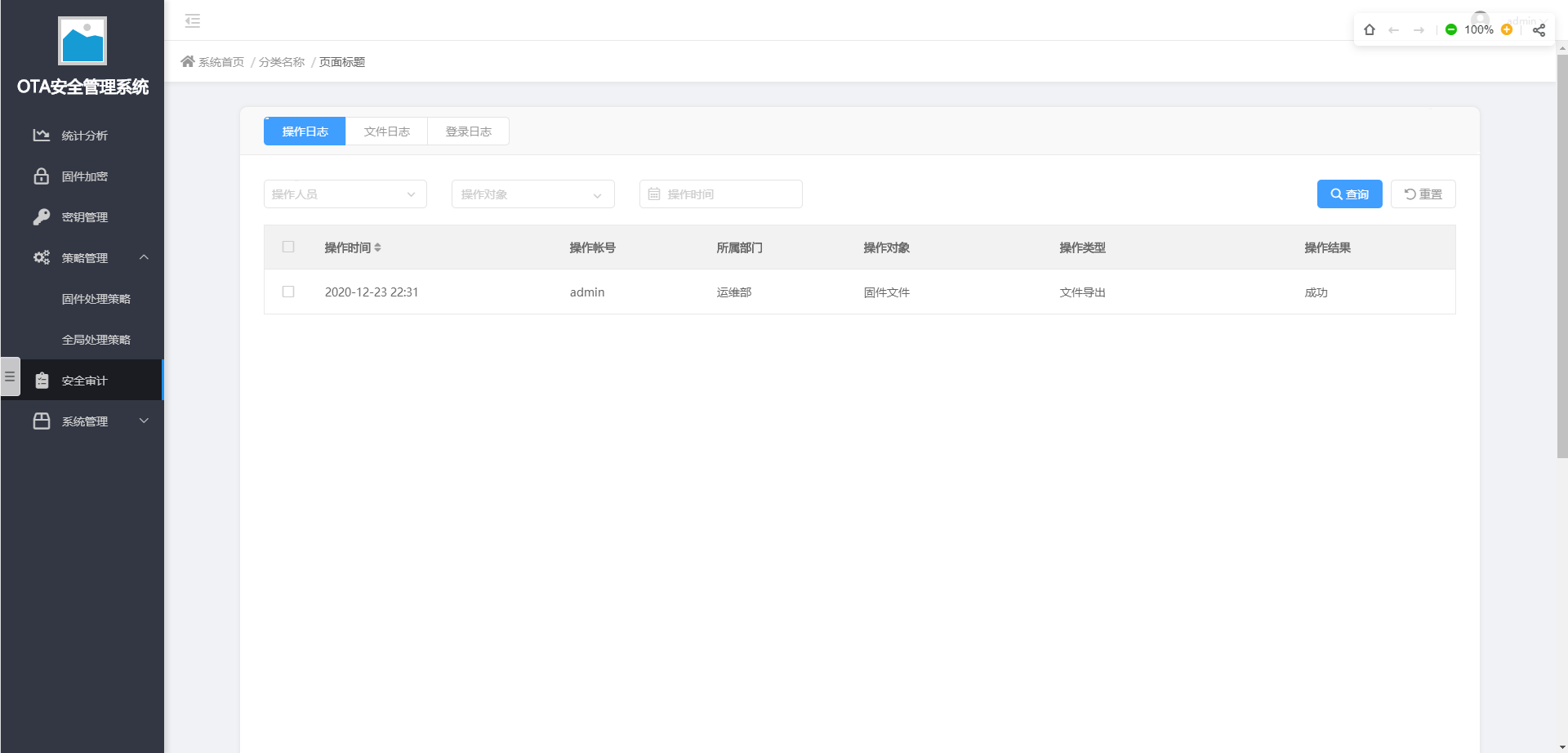
无

###### 处理步骤

无

###### 输出

用户操作日志列表



###### 规约

1. 日志记录字段如下：

* 操作时间（YY-MM-DD hh-mm）
* 操作帐号
* 用户所属部门
* 操作对象【固件文件、策略模版、系统配置、密钥】
* 操作类型
  + - 固件文件：【固件导入、固件加密、固件导出、固件删除】
    - 策略模版：【新增策略模版、修改策略模版、删除策略模版】
    - 系统配置：【新增用户、新增部门、修改用户帐户信息、修改部门、修改权限】
    - 密钥：【生成密钥、复制公钥】
* 操作结果【成功、失败】

##### 固件处理日志（OTA-SRS-LOG-03）

记录固件处理信息。

###### 流程图

*无*

###### 前提条件

1. 系统中有固件
2. 对固件进行各种操作

###### 输入

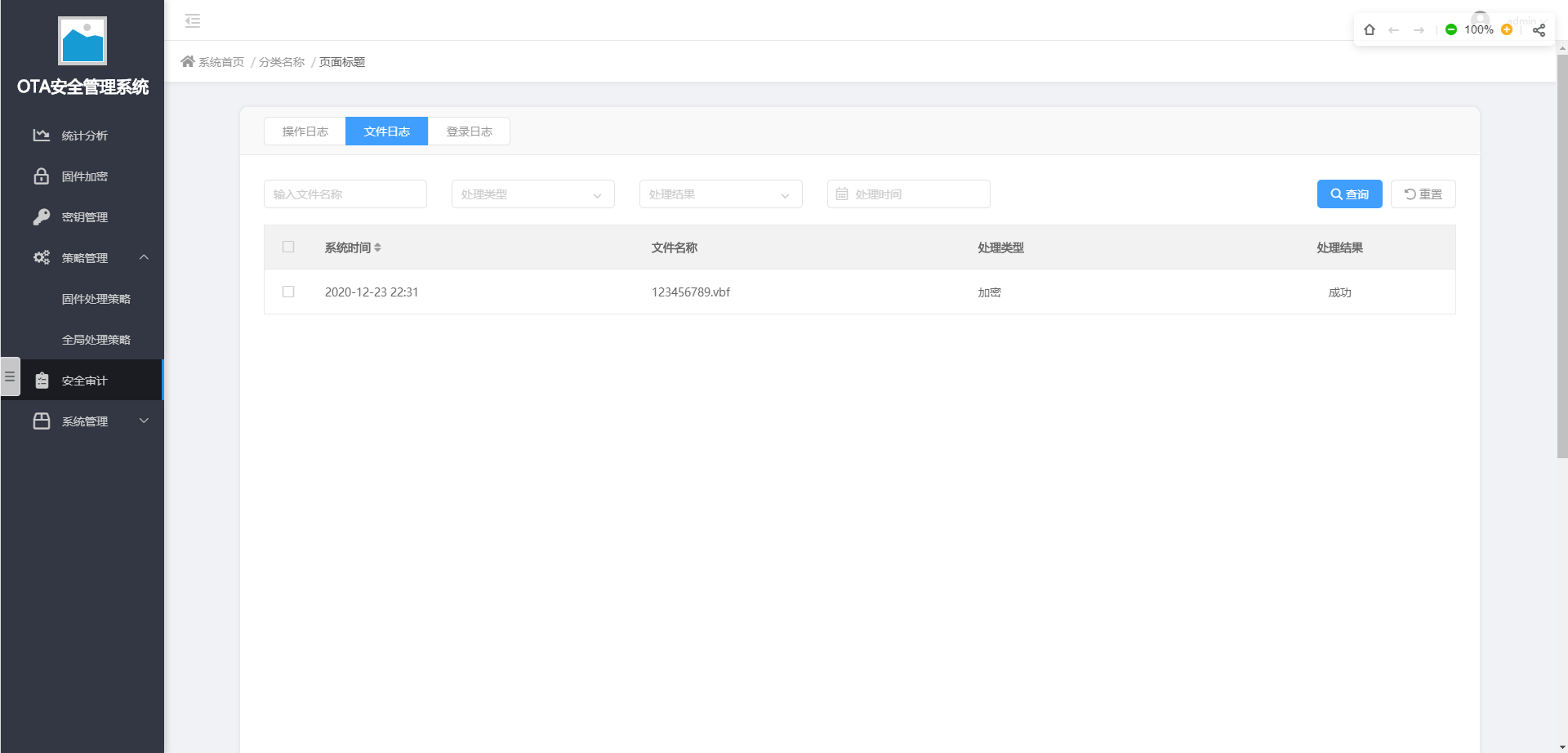
无

###### 处理步骤

无

###### 输出

固件处理日志列表



###### 规约

1. 日志记录字段如下：

* 操作时间（YY-MM-DD hh-mm）
* 固件名称
* 处理类型【导入、加密、签名、导出、删除】
* 处理帐号
* 处理结果【成功、失败】

1. 一条导出记录可点击查看此文件的更多导出记录，更多导出记录可查看以下信息：

* 导出时间
* 导出帐号
* 导出结果

##### 查询日志（OTA-SRS-LOG-05）

查询各类审计日志。

###### 流程图

*无*

###### 前提条件

1. 安全审计员权限

###### 输入

* 系统登录日志
  + - 登录人员
    - 终端类型【WEB端】
    - 登录时间
* 用户操作日志
  + - 操作人员
    - 操作对象【固件、策略模版、系统配置、密钥】
    - 操作时间
    - 操作结果【成功、失败】
* 固件日志
  + - 固件名称
    - 处理类型【导入、加密、签名、导出、删除】
    - 处理结果【成功、失败】
    - 操作时间

###### 处理步骤

1. 安全审计员进入安全审计模块；
2. 查询各类日志内容，在过滤器中输入查询条件
3. 点击查询按钮
4. 系统反馈查询结果

###### 输出

根据过滤器查询条件显示相应日志内容

###### 规约

1. 时间选择器可选时间范围
2. 名称过滤器支持关键字模糊匹配

#### 统计分析模块（OTA-SRS-DV）

##### 统计分析（OTA-SRS-DV-01）

页面显示各类统计分析结果

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 点击导航按钮：统计分析

###### 输出

1. 固件处理数量统计
   * 1. 今日处理固件数量
     2. 待导出固件数量
     3. 本周处理固件数量
     4. 历史处理固件数量
2. 固件处理策略统计
3. 固件类型统计
4. 业务处理成功率统计
5. 七天业务处理情况
6. 固件处理用时统计
7. 系统监控
8. 操作日志

原型图



###### 规约

1. 统计分析页面作为系统登录后内容区域默认显示页面
2. 统计图布局格式及显示效果参考原型设计
3. 每次进入页面时刷新统计结果（非定时及实时刷新）

##### 固件处理数量统计（OTA-SRS-DV-02）

统计系统今日处理固件数量、本周处理固件数量、历史处理固件数量、待处理固件数量

###### 流程图

**

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准
2. 今日处理固件、本周处理固件、历史处理固件均统计处理完成的固件（成功或失败均算处理完成）
3. 待处理固件统计未处理状态的固件

##### 固件处理策略统计（OTA-SRS-DV-03）

统计对比系统中各策略模版使用次数

###### 流程图

见4.3.1.6.2.1

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准
2. 只计算处理完成的固件（成功或失败）
3. 不显示0.00%的数据

##### 固件类型统计（OTA-SRS-DV-04）

统计对比系统处理的各种类型固件的数量

###### 流程图

见4.3.1.6.2.1

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 见流程图

###### 输出

页面显示统计图表

###### 规约

同4.3.1.6.3.6

##### 业务处理成功率统计（OTA-SRS-DV-05）

统计系统处理签名、加密、导出的成功及失败次数

###### 流程图

见4.3.1.6.2.1

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准
2. 固件加密及固件签名只计算处理完成的固件（成功或失败）
3. 固件导出在处理完成固件的基础上统计导出成功的固件（页面弹出下载提示即认为固件导出成功）

##### 七日业务处理情况（OTA-SRS-DV-06）

统计系统七日内处理

###### 流程图

见4.3.1.6.2.1

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准
2. 固件加密及固件签名只计算处理完成的固件（成功或失败）
3. 固件导出在处理完成固件的基础上统计导出成功的固件
4. 显示七天内数据（最新为当前日期）

##### 固件处理用时（单固件）（OTA-SRS-DV-07）

统计系统中各个固件的处理耗时

###### 流程图

见4.3.1.6.2.1

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准
2. 只计算处理成功的固件
3. 加密并签名的固件，单独计算加密和签名的用时
4. 以固件导入时间排序显示系统中前五个固件的处理用时

##### 固件处理用时（平均值）（OTA-SRS-DV-08）

统计系统处理加密、签名的平均耗时

###### 流程图

见4.3.1.6.2.1

###### 前提条件

1. 业务操作员权限
2. 有相关业务数据

###### 输入

无

###### 处理步骤

1. 见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准
2. 只计算处理成功的固件处理用时均值

##### 系统使用情况（OTA-SRS-DV-09）

查看系统磁盘、CPU、内存当前使用情况

###### 流程图

**

###### 前提条件

1. 业务操作员权限
2. 有查看系统资源权限

###### 输入

无

###### 处理步骤

见流程图

###### 输出

页面显示统计图表

###### 规约

1. 统计结果及展示方式以原型图为准

##### 操作日志（OTA-SRS-DV-10）

显示系统操作日志

###### 流程图

*无*

###### 前提条件

1. 业务操作员权限

###### 输入

无

###### 处理步骤

1. 点击导航按钮：统计分析

###### 输出

统计分析页面操作日志板块显示系统操作日志

###### 规约

1. 展示方式以原型图为准
2. 以操作时间排序显示7条日志

## 公共功能描述

### 系统管理模块（OTA-SRS-SM）

#### 机构管理（OTA-SRS-SM-02）

查询各类审计日志。

##### 流程图

*无*

##### 前提条件

1. 安全审计员权限

##### 输入

* 系统登录日志
  + - 登录人员
    - 终端类型【WEB端】
    - 登录时间
    - 认证结果（当前版本暂不支持）
* 用户操作日志
  + - 操作人员
    - 操作对象【固件、策略模版、系统配置、密钥】
    - 操作时间
    - 操作结果【成功、失败】
* 固件日志
  + - 固件名称
    - 处理类型【导入、加密、签名、导出、删除】
    - 处理结果【成功、失败】
    - 操作时间

##### 处理步骤

1. 安全审计员进入安全审计模块；
2. 查询各类日志内容，在过滤器中输入查询条件
3. 点击查询按钮
4. 系统反馈查询结果

##### 输出

根据过滤器查询条件显示相应日志内容

##### 规约

1. 时间选择器可选时间范围
2. 名称过滤器支持关键字模糊匹配

#### 用户管理（OTA-SRS-SM-01）

查询各类审计日志。

##### 流程图

*无*

##### 前提条件

1. 安全审计员权限

##### 输入

* 系统登录日志
  + - 登录人员
    - 终端类型【WEB端】
    - 登录时间
    - 认证结果（当前版本暂不支持）
* 用户操作日志
  + - 操作人员
    - 操作对象【固件、策略模版、系统配置、密钥】
    - 操作时间
    - 操作结果【成功、失败】
* 固件日志
  + - 固件名称
    - 处理类型【导入、加密、签名、导出、删除】
    - 处理结果【成功、失败】
    - 操作时间

##### 处理步骤

1. 安全审计员进入安全审计模块；
2. 查询各类日志内容，在过滤器中输入查询条件
3. 点击查询按钮
4. 系统反馈查询结果

##### 输出

根据过滤器查询条件显示相应日志内容

##### 规约

1. 时间选择器可选时间范围
2. 名称过滤器支持关键字模糊匹配

#### 权限管理（OTA-SRS-SM-03）

系统支持三种角色权限：业务操作员、安全审计员、系统管理员。

##### 流程图

##### 前提条件

1. 安全审计员权限

##### 输入

* 系统登录日志
  + - 登录人员
    - 终端类型【WEB端】
    - 登录时间
    - 认证结果（当前版本暂不支持）
* 用户操作日志
  + - 操作人员
    - 操作对象【固件、策略模版、系统配置、密钥】
    - 操作时间
    - 操作结果【成功、失败】
* 固件日志
  + - 固件名称
    - 处理类型【导入、加密、签名、导出、删除】
    - 处理结果【成功、失败】
    - 操作时间

##### 处理步骤

1. 安全审计员进入安全审计模块；
2. 查询各类日志内容，在过滤器中输入查询条件
3. 点击查询按钮
4. 系统反馈查询结果

##### 输出

根据过滤器查询条件显示相应日志内容

##### 规约

1. 时间选择器可选时间范围
2. 名称过滤器支持关键字模糊匹配

# 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%。

## 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 |

## 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。

## 移植性

系统可以灵活的部署在LINUX、Windows等主流操作系统上。

## 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 |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 验收标准

1. 系统功能完全符合客户需求，系统操作方便简单，符合客户的业务操作流程。
2. 系统性能符合客户对系统性能的要求，系统运行稳定，符合客户的安全要求。
3. 系统页面整洁美观，符合客户的审美效果。

# 需求确认

|  |  |
| --- | --- |
| 需求确认 | |
| 需求文档 | OTA安全管理系统《产品需求规格说明书》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，双方同意后续的开发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：**2022.1.4** |

# 附录

## 密钥算法清单

|  |  |  |
| --- | --- | --- |
| 算法名称 | 算法模式或者类型 | 密钥长度&IV长度 |
| SM4算法  （国密算法） | ECB模式  CBC模式  OFB模式  CFB模式  CTR模式  GCM模式 | 密钥：128Bit  IV：128Bit |
| AES128算法 | ECB模式  CBC模式  OFB模式  CFB模式  CTR模式  GCM模式 | 密钥：128Bit  IV：128Bit |
| AES192算法 | ECB模式  CBC模式  OFB模式  CFB模式  CTR模式  GCM模式 | 密钥：192Bit  IV：128Bit |
| AES256算法 | ECB模式  CBC模式  OFB模式  CFB模式  CTR模式  GCM模式 | 密钥：256Bit  IV：128Bit |
| SM3算法  （国密算法） | - | 结果：256Bit |
| SHA192算法 | - | 结果：192Bit |
| SHA224算法 | - | 结果：224Bit |
| SHA256算法 | - | 结果：256Bit |
| SHA384算法 | - | 结果：384Bit |
| SHA512算法 | - | 结果：512Bit |
| SM2算法  （国密算法） | Prime256 | 密钥：公钥512Bit 私钥256Bit |
| RSA算法 | \*RSA1024  RSA2048  RSA3072  RSA4096 | 密钥：公钥1024Bit 私钥1024Bit  密钥：公钥2048Bit 私钥2048Bit  密钥：公钥3072Bit 私钥3072Bit  密钥：公钥4096Bit 私钥4096Bit |
| ECC算法 | Prime192V1  Prime224V1  Prime256V1  Prime384V1  Prime521V1 | 密钥：公钥384Bit 私钥192Bit  密钥：公钥448Bit 私钥224Bit  密钥：公钥512Bit 私钥256Bit  密钥：公钥768Bit 私钥384Bit  密钥：公钥1042Bit 私钥521Bit |

\* 不建议继续使用。