
国家工作人员因私出国（境）

管理平台技术方案

修订记录

版本	修改记录	修改人	日期	备注
0.1	初稿	亢洋	2019-12-11	
0.2	二稿	亢洋、胡儒然	2019-12-12	
0.3	三稿	亢洋、胡儒然、宛根训	2019-12-25	
0.4	四稿	亢洋、宛根训、赵亚强	2020-01-06	
0.5	五稿	宛根训	2020-5-15	2.0 需求讨论和方案合稿
0.6	六稿	宛根训	2020-5-16	各子系统统一风格、系统1、2和6进一步完善后合稿
1.0	1.0 版	宛根训	2020-6-12	浙江出入境和组织部门第二轮现场调研后，各业务系统独立完善基础上进行汇总

目录

一、 总体设计	4
1.1 平台架构.....	4
1.2 业务流程梳理	4
1.2.1 总体业务流程.....	1
1.2.2 登记备案业务流程	2
1.2.3 出国（境）审批管理业务流程	3
1.2.4 证件信息生命周期流程	4
1.3 数据流向.....	5
二、 平台组成	1
2.1 证件保管柜	1
2.1.1 概述	1
2.1.2 总体结构.....	2
2.1.3 功能架构.....	5
2.1.4 功能设计.....	5
2.1.5 数据表设计	67
2.1.6 接口设计	79
2.2 备案审批系统	79
2.2.1 概述	79
2.2.2 总体构架.....	79
2.2.3 功能设计	80
2.3 数据汇聚分发系统	127
2.3.1 概述	127
2.3.2 功能描述	127
2.3.3 功能架构.....	128
2.3.4 功能设计.....	128
2.3.5 数据表设计	129
2.3.6 接口设计	129
2.4 证件保管柜管理系统	130
2.4.1 概述	130
2.4.2 功能描述	130
2.4.3 功能架构.....	131
2.4.4 功能设计	131
2.4.5 数据表设计	144
2.4.6 接口设计	151
2.4.7 接口数据格式	152
2.5 跨网传输系统	162
2.5.1 概述	162
2.5.2 总体设计	162
2.5.3 功能架构.....	163
2.5.4 功能设计	164
2.5.5 接口设计	171
2.6 综合信息管理系统	185

2.6.1 概述	185
2.6.2 总体设计	185
2.6.3 功能架构	186
2.6.4 功能设计	188
2.6.5 事件日志	223
2.6.6 数据库表设计	225
2.7 密钥管理系统	240
2.7.1 概述	240
2.7.2 功能架构	240
2.8 展示系统	241
2.8.1 概述	241
2.9 运维监控系统	242
2.9.1 概述	242
2.9.2 功能架构	242
2.9.3 功能描述	243
三、 服务接口	254
3.1 数据汇聚分发系统接口	254
3.2 跨网传输系统接口	254
3.3 综合信息管理系统接口	254
3.4 出入境查询推送接口	254
3.5 证件和人员信息签名验证接口	254
四、 安全技术方案	254
4.1 安全设计目标	254
4.2 风险评估	255
4.2.1 国家工作人员因私出国（境）管理平台架构	255
4.2.2 威胁和风险分析	257
4.3 安全需求	257
4.3.1 证件保管柜设备认证	257
4.3.2 保障数据传输安全	258
4.3.3 保障数据存储安全	258
4.3.4 公安网平台安全要求	258
4.3.5 保障系统高可用	259
4.4 安全方案	259
4.4.1 数据分级、分类	259
4.4.2 密码设备	259
4.4.3 证件保管柜安全	260
4.4.4 数据安全	260
4.4.5 安全传输协议	261
4.4.6 跨网数据传输	263
4.4.7 公安网系统加固	265
4.4.8 密钥管理系统	265
4.5 安全合规	267
附录 1：标识生成规则	269
附录 2：业务流水号生成规则	270

一、总体设计

1.1 平台架构

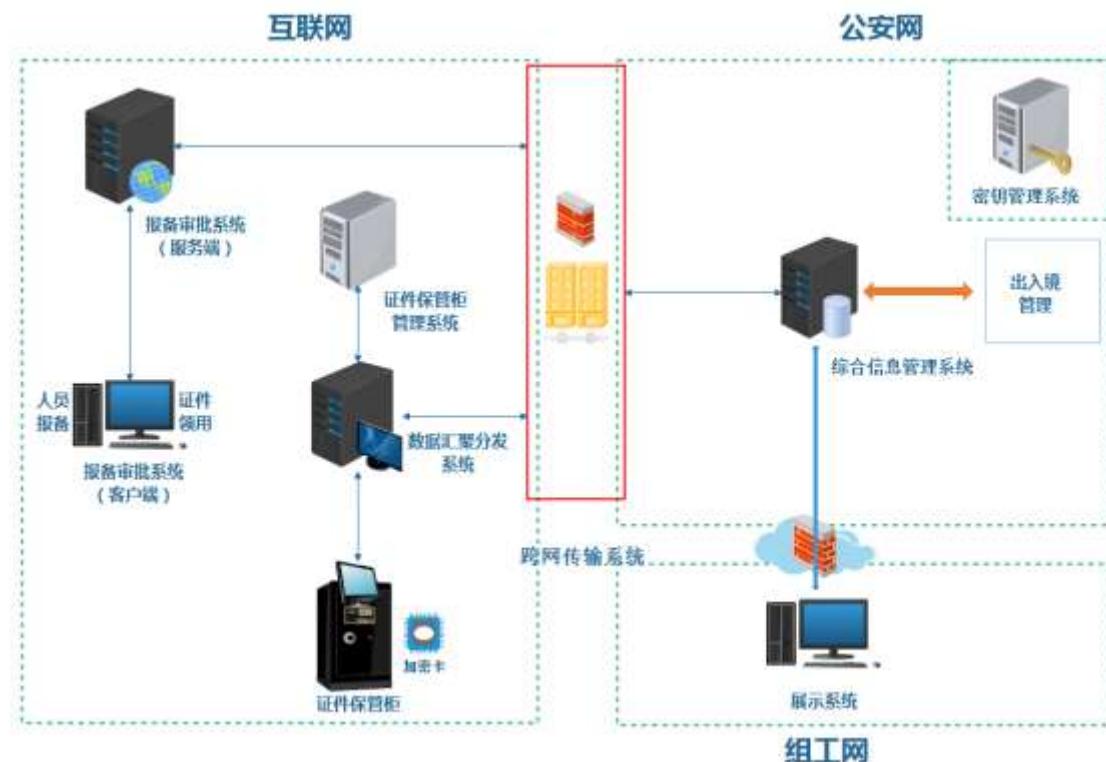
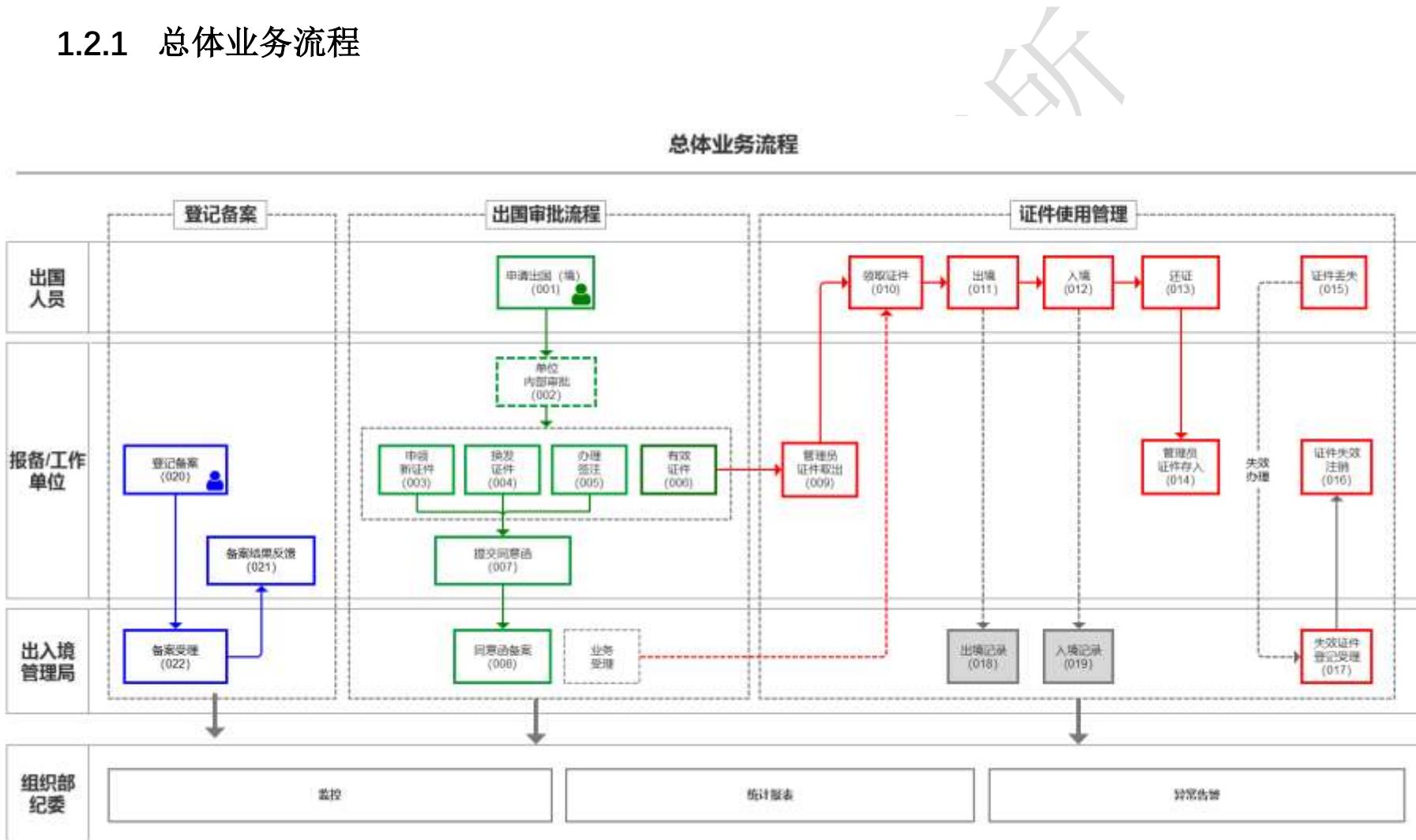


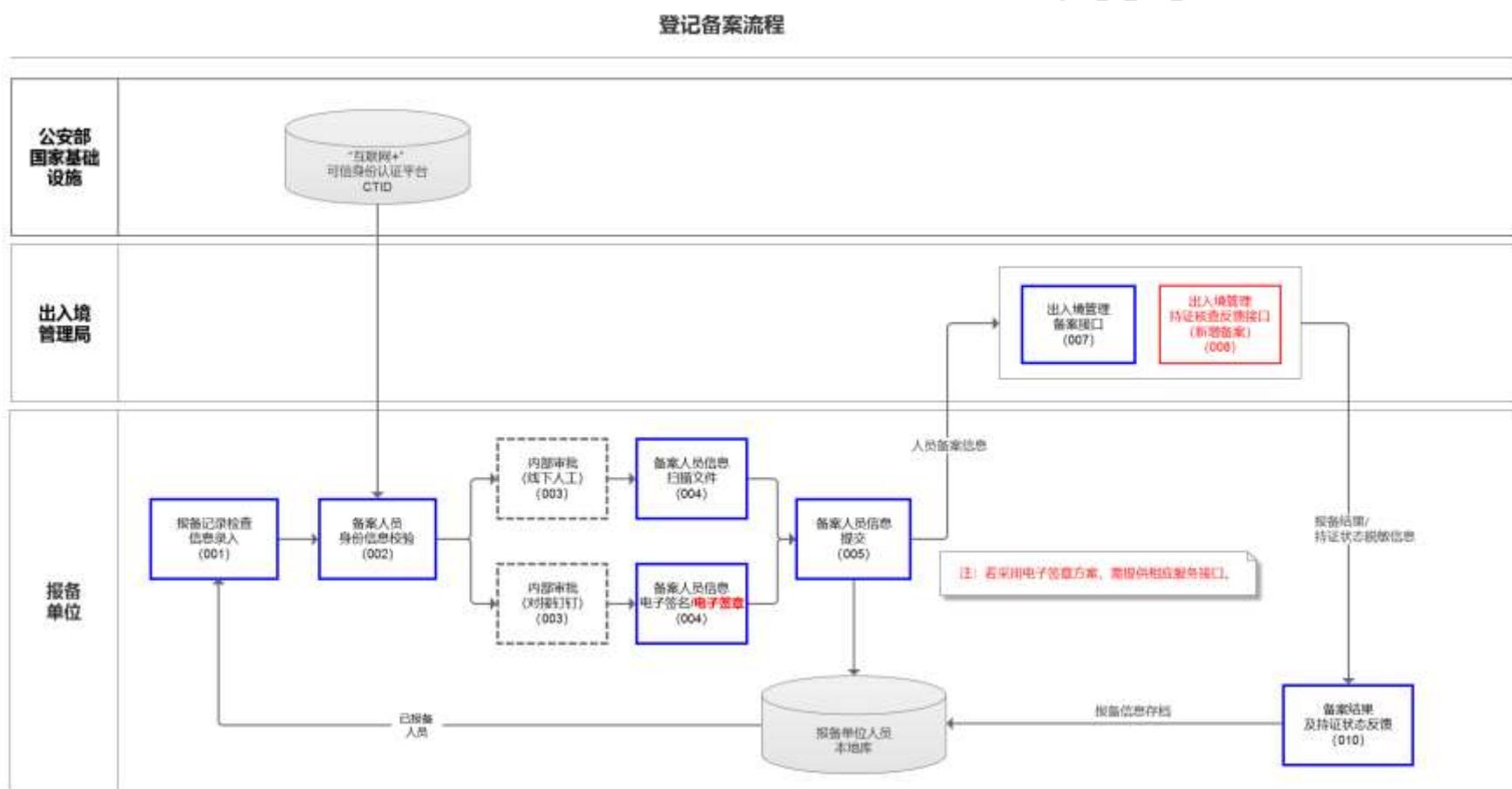
图 1-1 平台架构图

1.2 业务流程梳理

1.2.1 总体业务流程



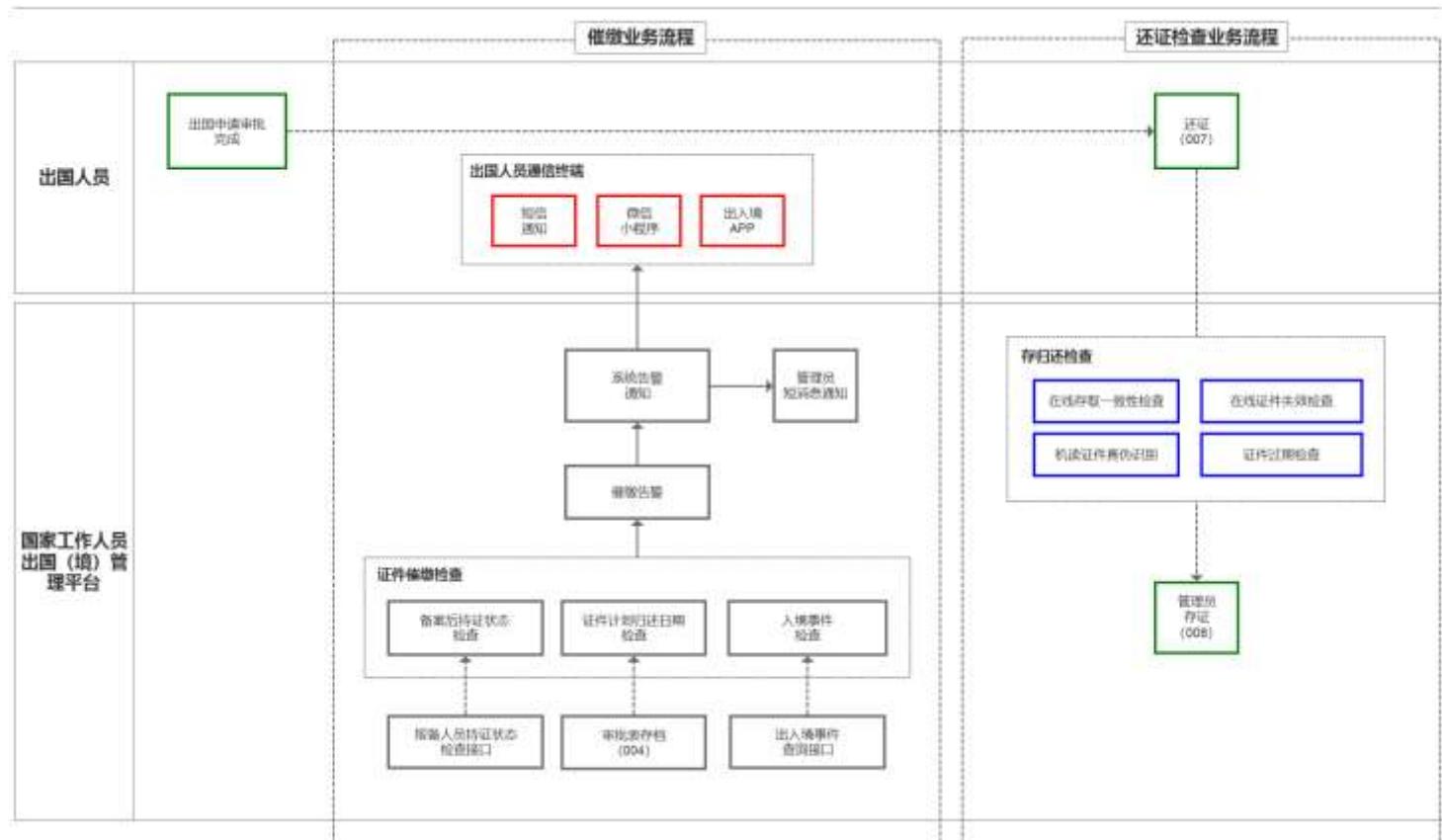
1.2.2 登记备案业务流程



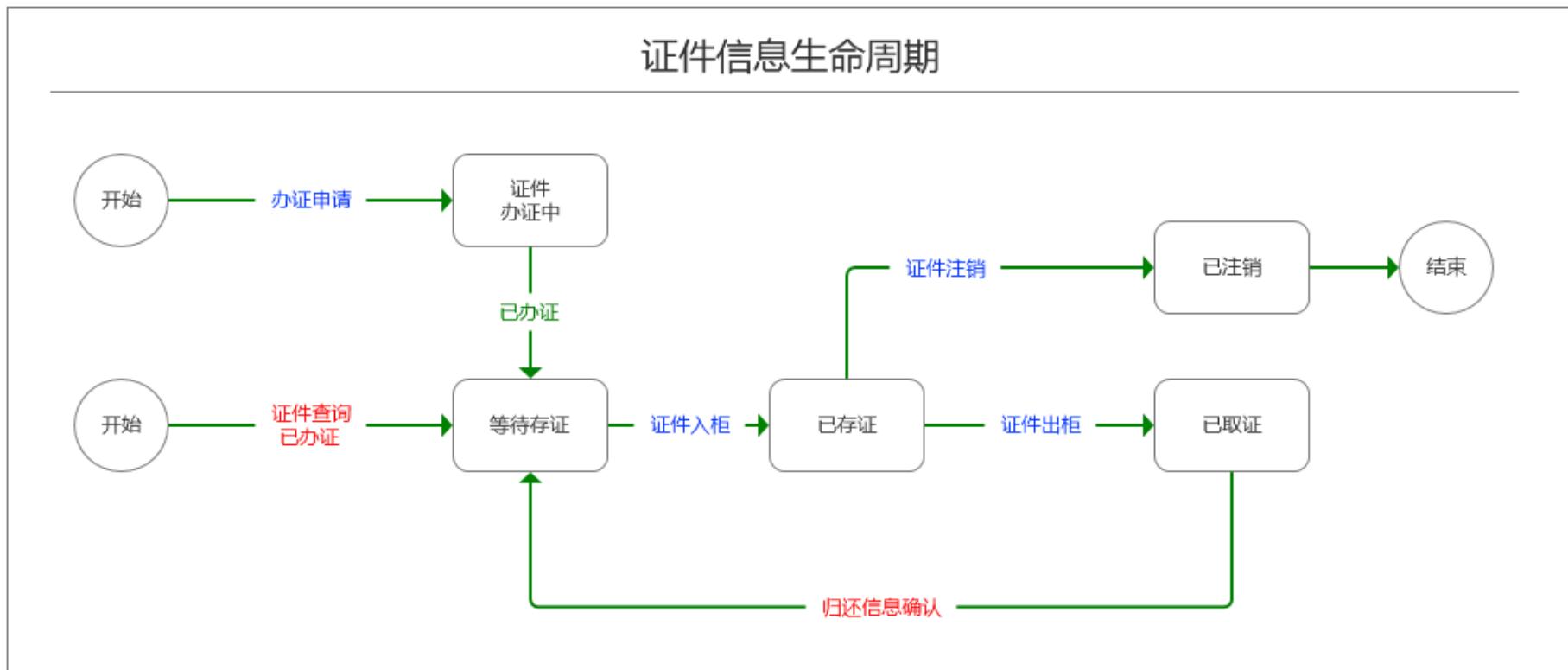
1.2.3 出国（境）审批管理业务流程



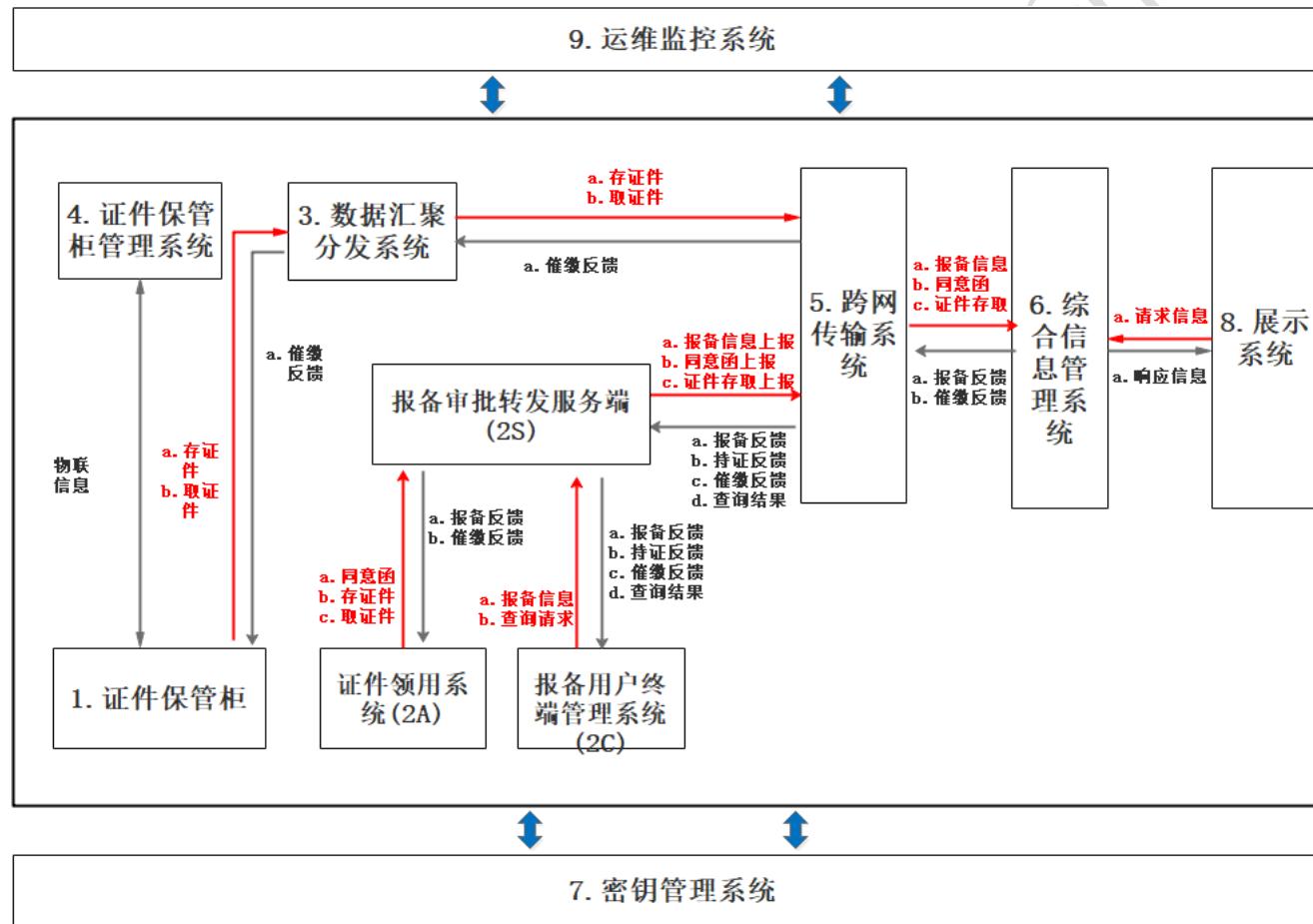
出国（境）审批管理-证件催缴、归还检查



1.2.4 证件信息生命周期流程



1.3 数据流向



二、平台组成



图 2-1 平台组成图

如图 2-1 所示，国家工作人员因私出国（境）管理平台以公安部第一研究所国家发改委人工智能创新发展重大专项基础平台为基础，通过建设应用系统和制定标准规范，为国家工作人员单位用户、出入境管理部门、组织部门和纪检监察部门提供应用，实现国家工作人员和证件的管理。平台包含 9 个独立系统，分别为：证件管理柜、备案审批系统、数据汇聚分发系统、证件管理柜管理系统、跨网传输系统、综合信息管理系统、密钥管理系统、展示系统和运维监控系统共 9 大子系统组成。

2.1 证件保管柜

2.1.1 概述

证件保管柜是集硬件设备和软件功能为一体的智能化终端设备，由证件保管柜设备、证件保管柜控制模块和证件保管柜智能管理模块

三部分组成，实现证件在证件保管柜上的存入和取出，如图 2.1-1。



图 2.1-1 证件保管柜实体图

2.1.2 总体结构

证件保管柜由证件保管柜机具及证件保管柜智能管理软件组成，有智能管理软件实现对证件保管柜机具的各种操作控制及实现证件的智能化管理。

证件保管柜机具：

证件保管柜具备防盗、防拆、防水的特点和离线可操作、断点续传、数据备份等功能，由可扩展型柜体、柜门开关控制板、UPS 电源、4G 模块、指纹模块、多功能证件阅读机具、液晶显示屏一体机等模块组成，主要实现了证件信息、管理员身份信息的采集、证件的物理空间存储、机械的控制和与软件端的通讯及响应，如图表 2.1-2。

组成结构	对应标准	性能要求
机柜箱体		厚度 1 毫米，冷轧板结构，表面酸洗，磷化喷塑。防火，防水，防尘
4G 通信模块		
安全模块	GM/T 0028 密码模块安全技术要求	

证件存放抽屉		
UPS 电源		220V 输入, 12V8A 输出, 通讯接口 485.过载保护
触摸一体机		英特尔 J1900、电容多点触摸、内存 4G, 硬盘 64G、4 个 USB、分辨率 1024*768。4G
多功能证件阅读机具		
控制主板		通讯接口:1 路 RS232,2 路 RS485; 锁控接口: 4 路带状态反馈锁控输出; 继电器输出: 2 路继电器输出; 温湿度接口: 1 路数字接口温湿度采集; 电源: 12V;
门锁		12V 供电, 具备状态反馈, 开锁驱动 (电磁铁或微电机) 承受 150KG 拉力不产生明显变形。



图表 2.1-2 证件保管柜实体侧面图

证件保管柜智能管理软件:

证件保管柜主机（嵌入式板）：运行证件保管柜主机应用界面与证件保管柜后台服务程序。

证件保管柜应用系统：提供操作界面，实现管理员认证、证件出入柜、证件核验的前端业务功能。

证件保管柜主机后台程序：提供证件保管柜后台服务，主要实现了证件保管柜柜体管理、证件数据管理、存取记录、统计分析、催收告警、设备运行监控和系统设置的后台管理功能。如图表 2.1-3，图表 2.1-4。



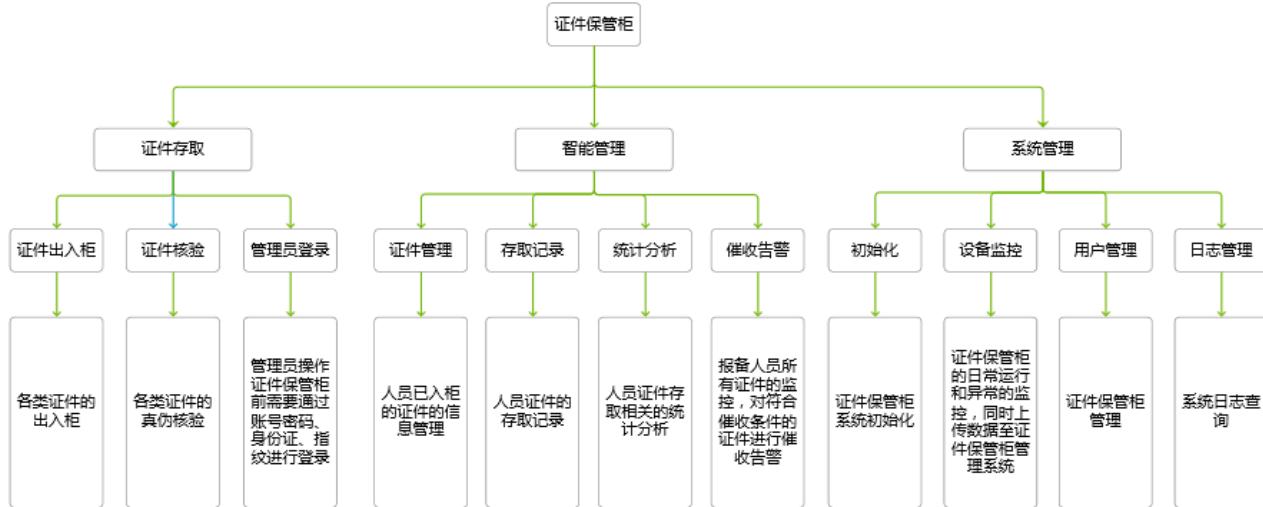
图表 2.1-3 证件保管柜主界面图

		正常 88				空余 18				异常 8				退出										
1	龚林泉	向峥	孟彭楠	葛妍伊	朱唐古	魏付元	贺志瑶	姜浩韩	王寒	李心	杨婧雄	朱唐古	郭瑞敏	吴玄庚	杨涛鸣	洪雨竹	陶爱红	贺雪珊	傅小乐	朱晨程	单碧蓉	黄晓兰	张艳	陈红雪
2	龚林泉	向峥	孟彭楠	葛妍伊	朱唐古	魏付元	贺志瑶	姜浩韩	王寒	李心	杨婧雄	朱唐古	郭瑞敏	吴玄庚	杨涛鸣	洪雨竹	陶爱红	贺雪珊	傅小乐	朱晨程	单碧蓉	黄晓兰	张艳	陈红雪
3	龚林泉	向峥	孟彭楠	葛妍伊	朱唐古	魏付元	贺志瑶	姜浩韩	王寒	李心	杨婧雄	朱唐古	郭瑞敏	吴玄庚	杨涛鸣	洪雨竹	陶爱红	贺雪珊	傅小乐	朱晨程	单碧蓉	黄晓兰	张艳	陈红雪
4	龚林泉	向峥	孟彭楠	葛妍伊	朱唐古	魏付元	贺志瑶	姜浩韩	王寒	李心	杨婧雄	朱唐古	郭瑞敏	吴玄庚	杨涛鸣	洪雨竹	陶爱红	贺雪珊	傅小乐	朱晨程	单碧蓉	黄晓兰	张艳	陈红雪
5	龚林泉	向峥	孟彭楠	葛妍伊	朱唐古	魏付元	贺志瑶	姜浩韩	王寒	李心	杨婧雄	朱唐古	郭瑞敏	吴玄庚	杨涛鸣	洪雨竹	陶爱红	贺雪珊	傅小乐	朱晨程	单碧蓉	黄晓兰	张艳	陈红雪

图表 2.1-4 证件保管柜操作界面图

2.1.3 功能架构

证件保管柜



图表 2.1-5 证件保管柜功能架构图

2.1.4 功能设计

2.1.4.1 证件出入柜

功能描述：

单位下证件保管柜管理员按照一定的证件出入柜规则，将人员证件存入柜中或从柜中取出，后台系统自动生成相关数据进行本地存储并同步至综合信息管理系统。

➤ 证件出柜

管理员登陆系统后，在默认的证件出柜界面中直接输入取证码就可以进行证件出柜操作，如果管理员在没有获取到取证码或者丢失取证码情况下，可以通过另外一种方式，即通过条件搜索到需要出柜的证件，然后进行证件出柜操作。

➤ 证件入柜

首先，管理员可以通过导入本单位原有人员与证件的相关信息初

始化数据，也可以在证件入柜操作流程中进行添加持证人和证件相关数据。管理员登录系统后，在证件保管柜上刷取需要入柜的证件并核验通过后，系统通过抽屉匹配规则和人员匹配规则来确定证件入柜的位置，管理员将证件存入指定的抽屉中即可。

功能流程图：

证件保管柜-证件入柜



图表 2.1-6 证件入柜流程图

证件入柜流程详细设计：

1. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面。



2. 管理员登录系统，具体认证登录流程参考 1.1.4.4 管理员认证，
登录后跳转至主界面。



3. 管理员点击“证件入柜”按钮，进入到证件入柜界面。



4. 管理员根据操作提示将需要入柜的证件放置于证件核验区进行刷取，系统通过证件人员匹配规则（1.通过生成的证件标识匹配证件（匹配不到证件时，系统新建证件记录），再通过证件匹配持证人员。2.当1匹配不到持证人员时，通过证件上的姓名和出生日期进行持证人员匹配（当有多个人员时，默认选择第一个））来匹配该证件的持证人，如果最终能匹配到持证人，进入到6；否则，进入到5。此外，当检测到证件已经过期的，系统提示管理员证件已过期。



5. 由于在柜内数据库中未匹配到的持证人，需要新建持证人才能继续当前证件的入柜操作。管理员按照要求填写新建持证人表单，包括姓名和公民身份号码（可以通过刷身份证自动获取或者手动填写）、手机号和验证码（选填）等。填写完成后，点击“注册”按钮，二次确认后完成新建持证人，同时，后台将证件与新建持证人进行绑定。

证件保管柜

35°C 60% WiFi

返回

该证件持有人还未在本柜内创建对应的记录，
需要先进行人员注册！

开始创建

取消

证件保管柜

35°C 60% WiFi

返回

新建持证人

姓名

张三

公民身份号码

请输入身份证

手机

请输入手机号

验证码

请输入验证码

获取

创建



6. 系统通过抽屉匹配规则，判断当前持证人是都已经绑定的抽屉，如果有；如果没有，系统将计算分配一个新空余抽屉与人员进行绑定（证件与抽屉也进行绑定，用于证件出柜），进入 7。
7. 操作界面显示持证人和证件相关信息并提示管理员将证件放入指定的抽屉当中，管理员打开对应的抽屉，将证件放入抽屉中，关闭抽屉，点击界面中的“入柜完成”按钮，二次确认后完成本次证件入柜操作。

证件保管柜

35°C 60%

返回

证件详情

性别	姓名
男	张三
证件类型	公民身份证号码
电子护照	333038****2655
出生日期	有效期至
1998/5/6	2020/5/6

STEP 1: 请刷取当前人员需要入柜的证件

证件读取成功！
请将证件放置于 1号柜 2行 3列

STEP 2: 确认已将证件放入抽屉

确认入柜



8. 系统后台判断本次入柜的证件是否属于初次入柜（每个新建的证件记录中的“新建记录信息上报标识”默认为否，如果该标识位为否，则表示该证件是初次入柜，否则不是初次入柜），如果是，则需要将证件详情上传至综合信息管理系统中进行校验（等待核验结果返回后，将标志位改成是），同

时，系统调用证件入柜事件接口进行数据上传。

备注说明：

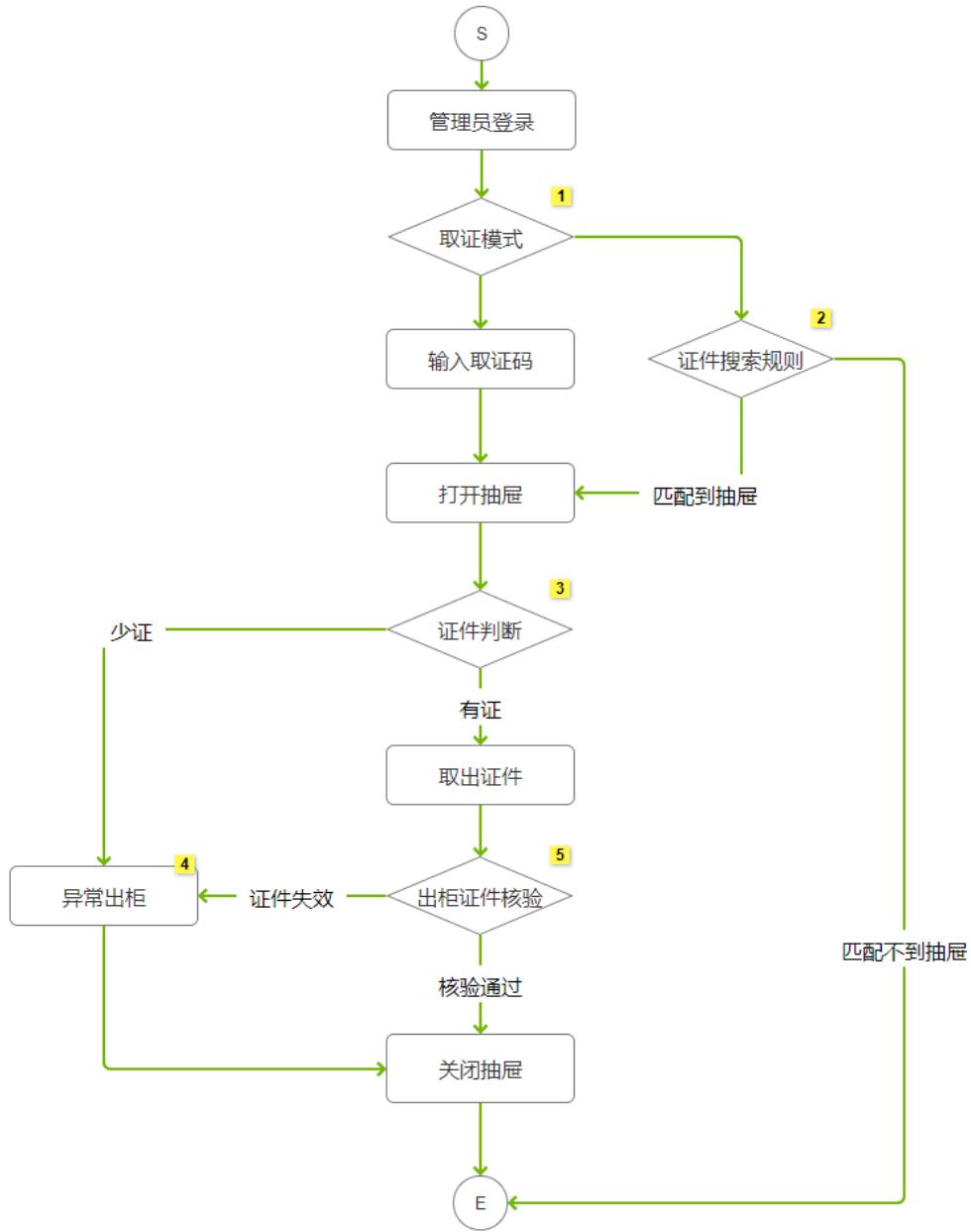
- ◆ 本流程对应的是一个证件的入柜流程，如果是新证件入柜操作则重新开始上述流程。
- ◆ 本流程中通过统一定义的证件编号 Hash (ZJLX • ZJHM) 在数据库中索引证件记录。

核心数据项：

- ◆ 业 务 流 水 号 : 入 柜 : RG+6 位 终 端 编 号 +YYYYMMDDHHMMSS+流水号(6位)+UUID
- ◆ 出柜: CG+6 位终端编号+YYYYMMDDHHMMSS+流水号(6位)+UUID

功能流程图：

证件保管柜-证件出柜



图表 2.1-7 证件出柜流程图

证件入柜流程详细设计：

1. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面。
2. 管理员登录系统，具体认证登录流程参考 1.1.4.4 管理员认证，登录后跳转至主界面。



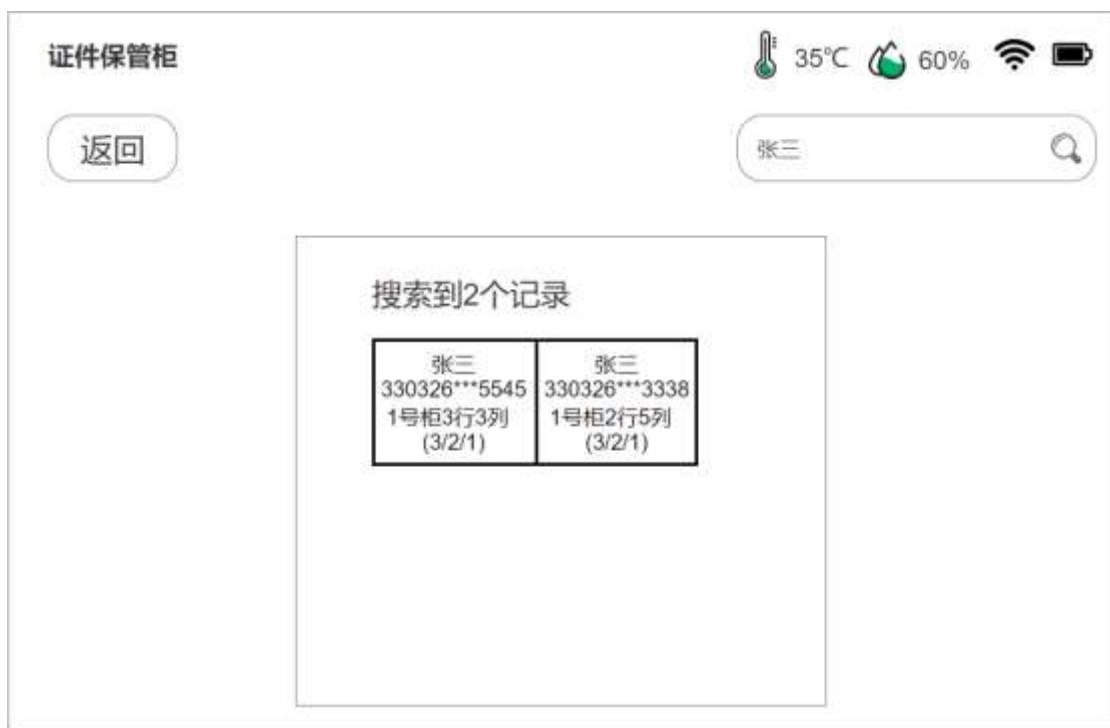
3. 点击“证件出柜”，进入证件出柜界面。



4. 证件出柜有两种模式，一般默认情况下，用户在界面中输入取证码，开始证件出柜，进入步骤 6。如果忘记或者丢失取证码，则可以点击下发的“搜索取证”字样，完成登录后通过搜索证件号码或者人员姓名进行证件出柜流程，进入步骤 4。

5. 进入证件出柜搜索界面，管理员可以通过以下几种方式查找证件：a. 用户点击页面中带有人员姓名的虚拟抽屉查看该抽屉中证件列表，然后切换证件信息进行查找；b. 用户通过上方搜索栏输入人员姓名来查找人员（如果出现同名则显示姓名+公民身份号码（前 6 后 4）来区别，让用户自己选择）下的证件，切换证件信息进行查找；c. 用户直接搜索证件号码来直接查找证件。进入步骤 5。





- 选择好出柜证件后，点击下方“证件出柜”按钮，二次确认后进入步骤 7。



7. 系统匹配到对应的待出柜证件并显示出柜信息，管理员根据操作提示，首先将证件从指定的抽屉中取出，如果此时发现抽屉内缺少本次出柜的证件，进入步骤 8，正常则进入步骤 7。



8. 管理员将证件放置于证件核验区进行刷取核验，如果刷取证件与待出柜证件一致，待出柜证件记录后面自动打钩，提示

“核验通过！”进入步骤 10。如果不一致，则提示证件与待出柜证件不符，请重新刷证。如果证件读取芯片失败，则进入步骤 9。



9. 用户点击“异常出柜”按钮，选择异常出柜的原因，确认后本次证件被标记为异常出柜，进入步骤 9。



10. 管理员关闭抽屉，点击界面中的“我已关闭抽屉，出柜完成”按钮，本次证件出柜流程完成，系统调用证件出柜事件接口进行数据上传。





备注说明：

- ◆ 本流程对应的是一个证件的出柜流程，如果是新的证件出柜则需重新开始上述流程。

2.1.4.2 查询

功能描述：

管理员通过此功能直观地查看当前证件保管柜的各个抽屉的使用状态，同时可以通过刷取人员的身份证件来查询该人员在柜内的所有证件的信息和状态。此外，管理员可以通过此处，进入到智能管理模块中进行进一步的查询和管理。

功能流程：

证件保管柜-查询



证件入柜流程详细设计：

-
11. 管理员来到证件保管柜前进行查询的操作。
 12. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.4 章节中的管理员身份认证流程设计。



13. 管理员身份认证通过登录后，进入主界面，点击“查询”进入查询的操作流程。



14. 操作界面显示当前证件保管柜中抽屉的使用状况（总数、已使用、空余、异常），管理员还可以刷取人员的身份证件，系统通过人员标识索引到柜内人员后，在界面显示该人员的证件列表及证件状态信息，如果证件刷取失败，则提示错误信息，让管理员重新刷证。





15. 管理员还可以点击界面右上方的齿轮图标，进入到系统更多功能列表中，含证件管理、存取记录、统计分析、催收告警、证件盘点、设备监控、用户管理、日志管理。



2.1.4.3 证件核验

功能描述:

通过多功能证件阅读机具识别读取电子旅行证件的信息及验证证件的真伪。

功能流程:

证件保管柜-证件核验



证件入柜流程详细设计:

1. 管理员来到证件保管柜前进行证件核验的操作。
2. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，点击页面下方的核验图标，进入证件核验界

面。



3. 管理员在证件核验区域刷取人员的相关证件，系统通过后台向移民局发起核验请求，证件真伪核验完成后，结果反馈至证件保管柜，操作界面上显示核验结果和证件相关内容信息。此外，如果检测到该证件已过期，系统将进行相关的提示。



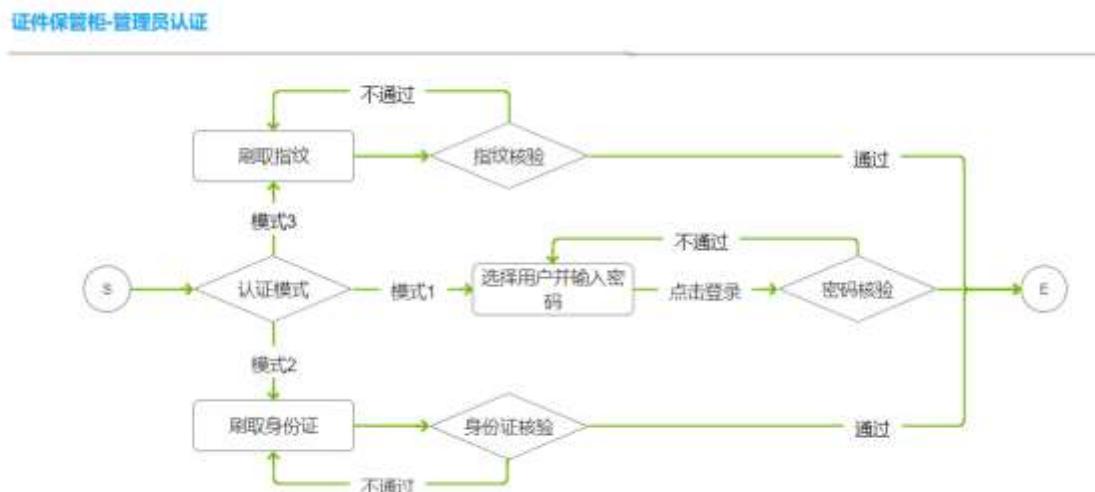
2.1.4.4 管理员认证

功能描述:

管理员登录系统时需要进行身份认证，管理员认证目前分为三种模式，分别是账号密码、刷身份证件和刷指纹登录。

- 模式 1：管理员可以在登录界面选择登录的账号（一般默认是两个账号），点击账号后输入对应的密码，点击“登录”按钮登录。
- 模式 2：管理员通过刷取身份证件，核验通过后自动登录系统。
- 模式 3：管理员通过刷取指纹，核验通过后自动登录系统。

功能流程：



图表 2.1-8 证件核验流程图

证件入柜流程详细设计：

1. 管理员进入到证件保管柜的登录页面，界面上显示三种认证登录的方式，分别是账号密码，刷身份证件和刷指纹。
2. 如果是通过账号密码方式认证登录，管理员可以切换需要登录的账号，输入对应的密码，点击“登录”按钮认证登录即可，如果忘记密码，点击下方的“忘记密码？”字样，进入密码重置页面，通过短信验证重置密码即可；如果是身份证件或者指纹认证登录方式时，管理员直接在证件核验区域或指纹采集区域刷取身份证件或者指纹，核验通过即可登录。



2.1.4.5 证件管理

功能描述:

对单位下已经入柜的人员证件进行信息管理，包括新增、注销证件，及证详情的查看。

➤ 证件新增:

单位进行人员报备后，证件保管柜会定时从综合信息管理系统中获取单位下已报备人员的持证信息（主要获取证件标识），获取到后会在证件保管柜内自动新增对应的证件记录，当证件入柜时获取到证件详情后再补全其余内容。

➤ 证件查看/注销:

管理员可以查看本单位证件保管柜中人员证件的相关信息和状态。

持证人证件丢失或持证人离开工作单位不再在证件保管柜中继续使用时，证件保管柜管理员进行证件注销操作，注销后，对应证件将无法继续在证件保管柜中使用。

对于需要进行注销的证件，人员获取组织部门出具的相关证明（出入境提供的失效证明（移民局小程序，微信，支付宝））证明后提供给管理员，管理员确认后注销该证件，在该证件取出后，后续系统将不在继续为给证件服务。

注销后的证件，不再支持入柜。

功能流程:

证件保管柜-证件查看/注销



证件注销流程详细设计:

1. 管理员根据需求，到证件保管柜前查看或者注销证件。
2. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.3 章节中的管理员身份认证流程设计。



3. 管理员身份认证通过登录后，进入主界面，通过依次点击查询→更多→证件管理，进入证件管理的操作界面。



1. 界面展示证件保管柜上的所有的证件列表，内容包括：证件类型、证件号码、姓名、性别、有效期至、所在位置、状态、操作时间、操作等，点击记录最左边的展开键，可以展开证

件相关的拓展内容（状态为待归还才有），包括：借出理由、借出天数、出发地/目的地、计划归还日期等，还可以通过右上方的查询框，输入相关的查询条件进行查询，如证件号码和人员姓名等。

证件保管柜

返回 证件管理

35°C 60% WiFi

请输入证件号码或者人员姓名

证件类型	证件号码	姓名	性别	有效期至	所在位置	状态	操作时间	操作
▼ 电子护照	E663***355	张三	男	2028-12-14	1号柜4行2列	待归还	2020-05-06 15:33:26	
借出理由	出国玩耍					借出天数	10天	
出发地/目的地	中国/美国					计划归还日期	2020-12-21	
▶ 港台台	T559***478	张三	男	2028-12-14	1号柜4行2列	在柜	1991-01-02	

4. 此外，管理员点击记录中操作的注销按钮，进入到证件注销流程。管理员选择注销理由并在“确认有相关批示”的栏中打钩，点击注销，弹出二次注销确认页面，核对无误后确认，完成本次证件的注销。

证件保管柜

返回 证件管理-注销

35°C 60% WiFi

证件序号	1	证件类型	电子护照
姓名	张三	证件号码	E332***265
★ 注销理由	丢失	★ 确认有相关批示	<input checked="" type="checkbox"/>
操作员	管理员1		

注销



2.1.4.6 存取记录

功能描述:

管理员对单位下人员各类证件的存取记录的查询。

功能流程:

证件保管柜-存取记录



证件注销流程详细设计：

2. 管理员根据需求，到证件保管柜前查看证件存取记录。
3. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.3 章节中的管理员身份认证流程设计。



4. 管理员身份认证通过登录后，进入主界面，通过依次点击查询→更多→存取记录，进入证件存取记录的界面。



证件管理



存取记录



统计分析



催收告警



证件盘点



设备监控



用户管理



日志管理

5. 界面展示证件保管柜上所有证件的存取记录列表，内容包括：姓名、证件类型、证件号码、位置、性别、操作类型、操作时间、经办人等，点击记录最左边的展开键，可以展开证件相关的拓展内容（操作类型为出柜才有），包括：借出理由、借出天数、出发地/目的地、计划归还日期等，还可以通过右上方的查询框，输入相关的查询条件进行查询，如证件号码和人员姓名等。

证件保管柜

返回 存取记录

35°C 60% WiFi

请输入证件号码或者人员姓名

姓名	证件类型	证件号码	位置	操作类型	操作时间	经办人
张三	电子护照	E336***547	1号柜4行2列	出柜	2020-05-06 15:33:26	管理员1
理由	出国玩耍		借出天数	10天		
出发地/目的地	中国/美国		计划归还日期	2020-12-21		
李四	电子护照	E336***547	1号柜4行2列	入柜	2020-05-06 15:33:26	管理员1

2.1.4.7 统计分析

功能描述:

对单位下证件保管柜、证件相关数据的统计分析并展示，如证件保管柜运行状态及抽屉使用率饼型图、最新证件存取记录、证件存取趋势图等，可根据单位用户需求定制。

功能流程:

证件保管柜-统计分析



证件注销流程详细设计:

1. 管理员根据需求，到证件保管柜前查看统计分析。
2. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.3 章节中的管理员身份认证流程设计。



3. 管理员身份认证通过登录后，进入主界面，通过依次点击查询→更多→统计分析，进入证件存取记录的界面。



4. 界面展示证件保管柜运行状态信息（温度、湿度）和抽屉使用率（饼图），证件最新的存取记录列表（滚动播放），下方还有证件存取的趋势图（可按日、月、天）。



2.1.4.8 催收告警 (移到证件领用系统)

功能描述:

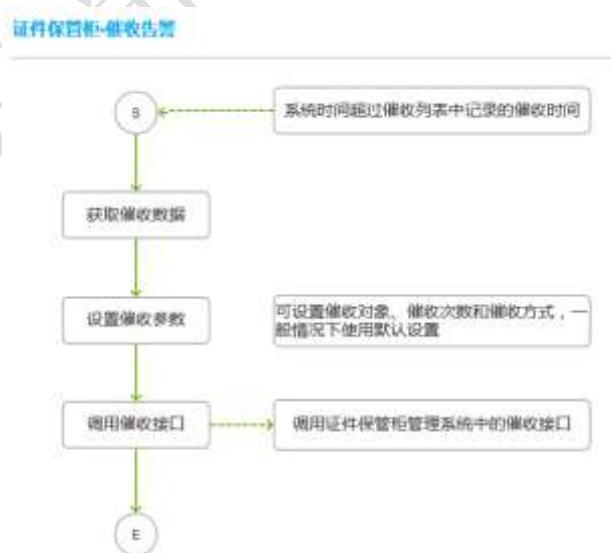
如果系统生成新的催收记录，会自动在操作主界面上进行相关提示（出现催收图标，附带新增催收记录数量），管理员点击后跳转至催收告警的界面，主界面的提示在查看后将自动隐藏。

催收告警还通过一套催收机制来实现对人员证件的催收管理。催收机制包含催收生成规则、催收生命周期、催收触发条件、催收对象、催收次数、催收方式。

催收生成规则	<ol style="list-style-type: none"> 1. 人员证件按照规定的流程正常出库后，默认将证件出库申请中的归还时间作为证件的催收时间，生成待催收记录放入催收列表中，等待生成催收名单发起催收。 2. 证件保管柜从综合信息管理系统获取回来催收信息后，根据系统配置参数，生成对应的待催
--------	--

	将收记录放入催收列表中，等待生成催收名单发起催收。
催收生命周期	待催收→催收中→催收结束
催收触发条件	催收列表中的记录到达催收时间点且催收状态不为催收结束
催收对象	<ol style="list-style-type: none"> 1. 管理员（默认） 2. 持证人（参考） 3. 其他（参考）
催收次数	共 1 次/ 每日 1 次（可配置）
催收方式	<ol style="list-style-type: none"> 1. 小程序 2. 公众号 3. 短信息 4. 其他（如：钉钉待办事件）
催收发起时间	每日早 10:00 - 17:00 之间

功能流程：



图表 2.1-9 催收告警流程图

证件注销流程详细设计：

1. 管理员根据需求，到证件保管柜前查看催收告警信息。
2. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.3 章节中的管理员身份认证流程设计。



3. 管理员身份认证通过登录后，进入主界面，如果当前系统内有新增的催收记录，则会在主界面的右上角显示催收图标(附带新增催收数量)，如果没有，则不显示，管理员点击催收图标跳转到催收告警页面，最新的记录会被标记，退出后标记取消，同时，主界面的催收图标也消失。



序号	姓名	证件类型	证件号码	借出日期	应还日期	逾期
● 1	张三	电子护照	E335***669	2020-05-06	2020-05-16	2天
● 2	李四	电子护照	E335***669	2020-05-06	2020-05-16	2天
3	王五	电子护照	E335***669	2020-05-06	2020-05-16	0天

4. 此外，管理员还可以通过依次点击查询→更多→催收告警，进入催收告警界面，查看更多历史催收告警记录，内容包括：姓名、证件类型、证件号码、借出日期、应还日期、逾期（天数）。管理员还可以通过搜索栏进行条件搜索。

序号	姓名	证件类型	证件号码	借出日期	应还日期	逾期
1	张三	电子护照	E335***669	2020-05-06	2020-05-16	2天
2	李四	电子护照	E335***669	2020-05-06	2020-05-16	2天
3	王五	电子护照	E335***669	2020-05-06	2020-05-16	0天

2.1.4.9 设备监控

功能描述:

对证件保管柜的日常运行和异常的监控，同时调用心跳接口（上报监控数据）和数据采集接口（上报抽屉开关记录）上传数据，通过事件上报接口上传异常监控数据。

证件保管柜定时（10分钟）调用心跳接口向证件保管柜管理系统发送心跳，并从证件保管柜管理系统中获取系统时间进行时间同步，还有根据心跳返回包中的告警配置修改标志位进行判断是否调用版本下载接口来更新证件保管柜中的系统版本。

监控项内容：本地设备的硬件及软件的监控，并上报监控数据到证件保管柜管理系统。

监控项:

	监控项		判断标准	处理
硬件	主控制器			

	视频抓拍	主控制器反馈	本地提醒, 异常上报
	操作超时	主控制器反馈	本地提醒
	尝试过多	主控制器反馈	本地提醒
	归还超时	系统软件计时	本地提醒
	非法领用	系统软件判断, 刷卡与指定用户不符	本地提醒, 异常上报
	断网	系统软件判断	本地提醒, 异常上报
	震动	采集控制板反馈	本地提醒
	温度	采集控制板反馈	本地提醒, 异常上报
	湿度	采集控制板反馈	本地提醒, 异常上报
	防拆	采集控制板反馈	本地提醒, 异常上报
	电压	采集控制板反馈	本地提醒, 异常上报
	非法开门	采集控制板反馈	本地提醒, 异常上报
软件	接口	系统软件反馈	本地提醒, 异常上报
	硬盘存储空间	系统软件反馈	本地提醒, 异常上报

	CPU 负载	系统软件反馈	本地提醒, 异常上报
	内存使用	系统软件反馈	本地提醒, 异常上报
	运行时间	系统软件反馈	本地提醒, 异常上报
	心跳	系统软件反馈	本地提醒, 异常上报
	版本	系统软件反馈	本地提醒, 自动同步

功能流程:



图表 2.1-10 设备监控流程图

证件注销流程详细设计:

1. 管理员根据需求, 到证件保管柜前查看设备监控项相关数据。
2. 管理员触碰证件保管柜上屏幕任意位置, 屏幕从待机模式跳转至登录界面, 具体流程详情参考 2.1.4.3 章节中的管理员身份认证流程设计。



3. 管理员身份认证通过登录后，进入主界面，通过依次点击查询→更多→设备监控，进入设备监控界面。



4. 界面以图表的形式展示证件保管柜上监控项的数据，内容包括：温度、湿度、运行状态、电压、CPU 负载、最新异常记录、各监控项变化趋势（根据监控项拓展）。



2.1.4.10 系统对账

➤ 证件盘点:

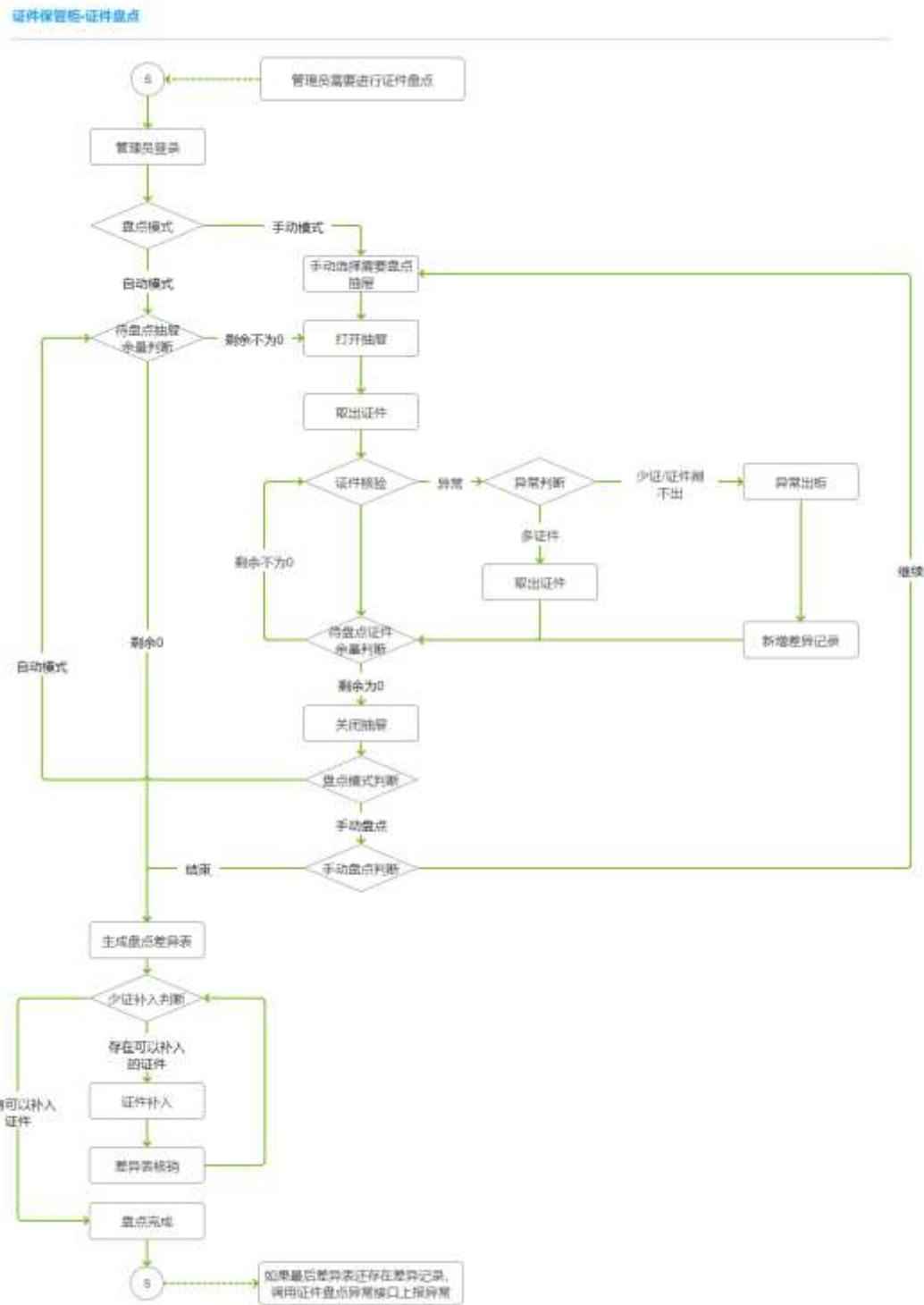
功能描述:

单位根据自身的需求，要求管理员定期进行证件盘点，管理员按照规定的流程，将证件保管柜的各个抽屉中的证件与系统中记录进行盘点核对，如果发现异常，系统新增差异记录，盘点结束后生成差异表，管理员可以根据差异表进行证件补入的操作，完成补入后对应的差异记录会自动核销，如果最后仍存在无法核销的差异记录，则系统生成盘点异常清单上报至综合信息管理系统。

目前证件盘点分为自动盘点和手动盘点两种模式。

- **自动盘点:** 系统对单位下某个证件保管柜中的所有抽屉按照顺序进行证件盘点。
- **手动盘点:** 管理员手动选择某个抽屉进行证件盘点。

功能流程:



证件入柜流程详细设计:

1. 管理员根据单位需求，定期到证件保管柜前进行证件盘点。
2. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.3 章节中的管理员身

份认证流程设计。



3. 管理员身份认证通过登录后，进入主界面，通过依次点击查询→更多→证件盘点，进入证件盘点的业务操作流程。



4. 界面显示证件盘点的两种模式和历史盘点记录，两种盘点模式分别是自动盘点和手动盘点，点击自动盘点模式，进入步

骤 6：点击手动盘点模式进入步骤 5；点击历史盘点，可以查看已经完成盘点的历史记录，点击查看详情。



序号	创建时间	完成时间	差异率	操作人	操作
1	2019-06-05 15:33:25	2019-06-05 15:33:25	2%	管理员1	详情

[返回](#)

历史盘点记录-详情

盘点序号	1	创建时间	2019-06-05 13:22:32
操作人	管理员1	结束时间	2020-06-05 13:22:32
盘点总数	100	正常数	98
异常数	2	正常率	98%

5. 管理员进入手动盘点界面，管理员根据自己的需求，逐一选择抽屉进行盘点操作，选择好抽屉后，进入步骤 8；如果想结束盘点，点击左上方返回按钮退出手动盘点，进入步骤 12。

[返回](#)

手动盘点模式

总数: 100 已盘点: 0 剩余: 100

柜1

请点击选择需要盘点的抽屉





6. 管理员进入自动盘点新建/待续界面，管理员可以选择新建一条自动盘点的记录，也可以选择之前暂停待续的盘点记录，进入开始盘点界面。





7. 系统自动计算柜内需要盘点的抽屉数量，并循环判断待盘点的抽屉数量是否为 0，如果不为 0，系统则按照顺序自动锁定下一个待盘点的抽屉，进入步骤 8；如果数量为 0，则进入步骤 12。
8. 界面展示当前抽屉内待盘点的证件列表和位置信息，提示管理员从抽屉中取出所有证件进行一一核验盘点。

9. 管理员打开抽屉，取出抽屉内所有的证件。
 10. 管理员在证件核验区域依次循环刷取证件进行核验盘点，如果刷取的证件与证件列表中的证件相符，则对应的证件记录后面自动打钩，如果不符，界面提示错误信息，管理员将这本证件取出放在一边，如果管理员发现列表中的证件存在

缺失或者证件失效的情况，在界面上对这些证件进行异常出柜的操作，系统自动在差异表中对应新增一条盘点差异记录。完成后，进入步骤 11。



证件保管柜

35°C 60% WiFi

返回

证件异常出柜

张三 330381*****0114

证件

异常原因



台湾通行证 T33**365

少证 ▶

确定

证件保管柜

35°C 60% WiFi

暂停

自动盘点模式-盘点中

总数: 100 已盘点: 30 剩余: 68 差异: 2

证件异常

李四

330381*****1544

1号柜 4行 2列 共 3 本证件

柜1			
			正在盘点

港澳台通行证 已盘点 ✓

台湾通行证 T33**365 少证

电子护照 已盘点 ✓



11. 如果是自动盘点模式下，则进入步骤 6。如果是手动模式，则进入步骤 5。
12. 系统根据本次盘点中盘点过的所有抽屉的情况，统计生产对应的盘点差异表，管理员可以将此次盘点多出来的证件依次在证件核验区域重新进行刷取，如果能匹配到差异表中的状态为“少证”的记录，则系统提示管理员将证件归还至对应的抽屉中，管理员完成证件补入后，差异表中对应的差异记录自动核销。

证件保管柜

35°C 60%

返回

盘点差异表

序号	位置	人员	公民身份证号码	证件类型	证件号码	差异原因	可操作
----	----	----	---------	------	------	------	-----

1	1号柜 4行 2列	张三	330318****2256	台湾通行证	T33**365	少证	
---	-----------	----	----------------	-------	----------	----	--

2	1号柜 5行 2列	李四	330318****6666	台湾通行证	T33**365	证件失效	
---	-----------	----	----------------	-------	----------	------	--

盘点完成

•) 请将补入的证件放置核验区



证件保管柜

35°C 60%

返回

证件结果

序号	差异序号	1	
----	------	---	--

姓名	李四
----	----

公民身份号码	330381*****1544
--------	-----------------

抽屉位置	1号柜4行2列
------	---------

补入证件	港澳台通行证/G78**355
------	-----------------

补入成功!
请放回证件

确认已将证件放回

[返回](#)

盘点差异表

序号	位置	人员	公民身份证号码	证件类型	证件号码	差异原因	可操作
1	1号柜 4行 2列	张三	330318****2256	台湾通行证	T33**365	少证	已补入
2	1号柜 5行 2列	李四	330318****6666	台湾通行证	T33**365	证件失效	

[盘点完成](#)

•) 请将补入的证件放置核验区



13. 最终，管理员点击界面中的“完成盘点”，弹出二次界面，确认后退出盘点界面。后台进行判断，如果差异表中仍存在未核销的差异记录，则调用接口将此差异表上报至综合信息管理系统，让其修改对应证件的状态，本证件保管柜也修改对应的证件状态，对少证和证件失效的人员进行催收或者其他处理。



➤ 证件对账:

证件对账的功能是将证件保管柜固定时间内发生变化的证件状态和人员状态的数据打包发送到综合信息管理系统中，由其完成数据一致性检查。证件的状态信息原则上以证件保管柜的数据为准。

(1) 数据对账处理逻辑

- ◆ 每天在固定的时间段（20:00~06:00），证件保管柜向综合信息管理系统上报当日变更的证件状态信息和人员状态信息；

(2) 对账数据

对账发送数据：每日增量数据，包含如下数据项

证件状态：

- ◆ 人员标识
- ◆ 证件标识

- ◆ 保存位置（机柜+抽屉）

- ◆ 社会统一信用代码

- ◆ 状态（入柜/出柜）

操作流水：

- ◆ 业务请求时间交易流水日志（*）

操作日志：

- ◆ 业务请求时间交易流水日志（*）

2.1.4.11 系统管理

功能描述：

对证件保管柜中后台管理系统的设置，包括证件保管柜初始化、用户管理、数据备份和日志管理。

➤ 证件保管柜初始化：

1、证件保管柜管理系统新增报备单位信息：社会统一信用代码，单位名称，工作联系人，工作联系电话，开通证件保管柜数量（该单位下允许开通的证件保管柜数量）。

2、新证件保管柜到业主现场，系统启动，从证件保管柜管理系统获取新增报备单位信息名称列表，选择本证件保管柜对应的单位名称，设置本机操作员账号和密码、SIM 卡号、有效期、套餐名，并确认注册开通，同时将注册信息反馈到证件保管柜管理系统。

证件保管柜初始化配置流程 (证件保管柜上线注册)

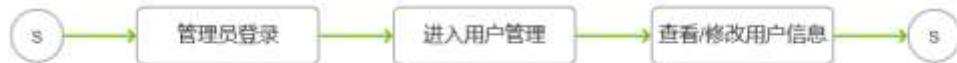


图表 2.1-11 系统管理流程图

➤ 用户管理

用户管理包括了对用户的新增（系统默认有两个管理员账号，上限最高为 5 个）、修改和查询。其中用户的初次新增在证件保管柜初始化中完成。如果管理员在进行管理员认证模式 1 下，忘记账号对应的密码时，可以通过模式 2 认证后登录系统中，在此处的用户管理中进行密码重置。

证件保管柜-用户管理



用户管理流程详细设计：

1. 管理员根据需求，到证件保管柜前进行用户管理操作。
2. 管理员触碰证件保管柜上屏幕任意位置，屏幕从待机模式跳转至登录界面，具体流程详情参考 2.1.4.3 章节中的管理员身份认证流程设计。



3. 管理员身份认证通过登录后，进入主界面，通过依次点击查询→更多→用户管理，进入用户管理的界面。



4. 界面展示证件保管柜上的所有用户列表，内容包括：姓名、账号、角色、创建时间、状态、操作等。管理员可以新增用户（启用用户不超过 3 个（默认是登录页面的 3 个用户），超

过则不允许启用用户），可以点击修改和重置密码。

证件保管柜

返回 用户管理

请输入证件号码或者人员姓名

序号	姓名	账号	角色	创建时间	状态	操作
1	张三	admin	管理员	2020-05-06 15:33:22	启用	
2	李四	admin2	管理员	2020-05-06 15:33:22	启用	

5. 点击新增用户。

证件保管柜

返回 用户管理-新增

姓名	<input type="text"/>	公民身份号码	<input type="text"/>
账号	<input type="text"/>	密码	<input type="text"/>
手机	<input type="text"/>	验证码	<input type="text"/>

6. 点击修改用户信息。

证件保管柜

35°C 60% WiFi

返回 用户管理-修改

姓名 张三 公民身份号码 33038***1526

账号 admin 用户状态 开

手机 188***3695 验证码 发送

确认



7. 点击重置密码。

证件保管柜

35°C 60% WiFi

返回 用户管理-重置密码

新密码

确认新密码

确认



➤ 数据备份恢复：

1、备份（自动）：

1.1、系统具备本地双硬盘数据备份机制，

1.2、系统具备每周定时数据库自动备份机制，保障数据库安全。

2、恢复（手动）：

2.1、本地备份数据恢复。

2.2、通过 6 获取恢复数据。

本地参数配置；

4G 卡的管理（放在 4 上）：

指纹核验功能：启用，不启用（2013 年 1 月新办身份证有指纹（指纹核对为默认选项，可取消））

➤ 日志管理：

日志管理记录了管理人员在系统各个模块中的操作动作记录。

证件保管柜

返回 日志管理

35°C 60% WiFi

请输入证件号码或者人员姓名

动作流水	人员	模块	动作	时间
2020060533225	管理员1	存取记录	查看	2020-05-16 15:33:75
2020060533224	管理员1	证件出柜	关闭抽屉	2020-05-16 15:33:75
2020060533223	管理员1	证件出柜	打开抽屉	2020-05-16 15:33:75

2.1.5 数据表设计

名称	表明	备注
CertificateInfo	证件信息表	
PersonInfo	人员信息表	
DropRecord	证件取出记录表	
PutRecord	证件取出记录表	
m_zjcsxxb_t	证件催缴信息表	
DeviceCabinet	一体机证件保管柜关联表	
IOTDevice	一体机表	
LicenseCabinetInfo	证件保管柜表	
DrawerItem	抽屉与证件关联表	
User	用户表	
Dept	单位表	
Permission	权限表	
Role	角色表	
RolePermission	角色权限表	
UserDevice	用户设备表	
ZzgMsg	证件保管柜信息上报表	

证件信息表 CertificateInfo

代码	名称	类型	非空	主键	规范	备注
DocId	证件 ID	int(11)	√	√	AUTOINCREMENT	
ZJBS	证件标识	varchar (32)				hash (证件类型.证件号码)

RYBS	人员标识	varchar (32)				hash (公民身份号码+姓名)
ZJHM	证件号码	varchar (32)				
DocType	证件类型	varchar(5)			DEFAULT NULL	ZJLX, 需要字典
ChName	中文名字	varchar(64)			DEFAULT NULL	ZWXM
DocNo	证件编号的 Md5 值	varchar(32)			DEFAULT NULL	建议使用证件号码, MD5 有啥用?
EnName	英文名字	varchar(20)			DEFAULT NULL	YWXM
Sex	性别	int(1)			DEFAULT NULL	XB, 需要字典
BirthDate	出生日期	date			DEFAULT NULL	CSRQ
ExpireDate	有效期截止日期	date			DEFAULT NULL	YXQJZRQ
ZP	照片	varchar (32)				
IssueDate	签发日期	date			DEFAULT NULL	
BirthPlace	出生地点	varchar(20)			DEFAULT NULL	
IssuePlace	签发机关	varchar(20)			DEFAULT NULL	
Status	有效状态	int(1)			DEFAULT NULL	有效 过期
PersonID	单位人员 ID	int(11)			DEFAULT NULL	

人员信息表 PersonInfo

代码	名称	类型	非空	主键	规范	备注
PersonId	人员 ID	int(11)	√	√	AUTOINCREMENT	
RYBS	人员标识	varchar (32)				RYBS, hash (公民身份证号 码+姓名)
ChName	姓名	varchar (32)			DEFAULT NULL	
PersonID	公民身份 号码	varchar (32)			DEFAULT NULL	
DWMC	单位名称	varchar(5)				
TYSHXYDM	统一社会 信用代码	varchar(64)				
LXDH	联系电话	varchar(32)				
ZW	职务	varchar(20)				
RYZT	人员状态	int(1)				
BirthDate	出生日期	date			DEFAULT NULL	
Addr	家庭地址	date			DEFAULT NULL	
IssuingAuthori ty	签发机关	varchar (32)			DEFAULT NULL	
PeriodValidity	有效期限	date			DEFAULT NULL	建议改成两个 字段：有效期 起始日期，有 效期截止日期
PeriodValidity	有效期起 始日期	varchar(20)			DEFAULT NULL	

PeriodValidity	有效期截止日期	varchar(20)			DEFAULT NULL	
----------------	---------	-------------	--	--	--------------	--

证件取出记录表 DropRecord

代码	名称	类型	非空	主键	规范	备注
DropRecID	取出记录 ID	int(11)	√	√	AUTOINCREMENT	
ZJQCYWLSH	证件取出流水号	varchar (32)				
ZJBS	证件标识	varchar (32)				一证一号，每个证件唯一的证件 id, hash (证件号+证件类型)
QZYT	取证用途	varchar (32)				
GHJZRQ	归还截止日期	varchar (32)				
DropTime	取出时间	datetime	√			
DropType	取出类型	int(2)			DEFAULT NULL	1: 取出 2: 撤销
UserId	经办人 ID	int(11)	√		DEFAULT 0 UNSIGEND	用户表中用户 ID
DocId	证件 ID	int(11)			DEFAULT 0	
DrawerId	抽屉 ID	int(11)			DEFAULT NULL	
CabinetStrno	证照保管柜序列号	varchar(40)			DEFAULT NULL	
SBXLH	设备序列号	varchar (32)				

证件存入记录表 PutRecord

代码	名称	类型	非空	主键	规范	备注
PutRecID	存入记录 ID	Int(11)	√	√	AUTOINCREMENT	
ZJCRYWLSH	证件存入流水号					
ZJBS	证件标识					一证一号，每个证件唯一的证件 id, hash (证件号+证件类型)
PutTime	存入时间	datetime			DEFAULT NULL	
PutType	存入类型	int(2)			DEFAULT NULL	1 新增 2 归还
UserId	经办人 ID	int(11)	√		DEFAULT '0'	用户表中用户 ID
DocId	证件 ID	int(11)			DEFAULT '0'	
DrawerId	抽屉 ID	int(11)			DEFAULT NULL	
CabinetStrno	证照保管柜序列号	varchar(40)			DEFAULT NULL	
SBXLH	设备序列号	varchar (32)				

证件催缴信息表 m_zjcsxxb_t

代码	名称	类型	非空	主键	规范	备注
CSYWLSH	催收业务流水号					
ZJBS	证件标识					

RYBS	人员标识					
ZJLX	证件类型					
YQTS	逾期天数					
CSLX	催收类型					1:: 逾期 2: 未逾期已入境
ZT	状态					1: 催收中 2: 催收结束

一体机证件保管柜关联表 **DeviceCabinet**

代码	名称	类型	非空	主键	规范	备注
DeviceId	设备 ID	int(11)	√		DEFAULT 0 UNSIGNED	
CabinetId	证件保管柜 ID	int(11)	√		DEFAULT 0 UNSIGNED	

一体机表 **IOTDevice** (证件保管柜中的一体机)

代码	名称	类型	非空	主键	规范	备注
DeviceId	一体机 ID	int(11)	√	√	AUTO INCREMENT	
SerialNo	设备序列号	varchar(40)	√			SBXLH
SerialType	设备型号	int(6)	√		DEFAULT 1	
DevName	设备名称	varchar(64)			DEFAULT NULL	

DeptId	单位 ID	int(6)	√		DEFAULT 1	建议统一社会信用代码绑定单位
TYSHXYDM	统一社会信用代码	varchar (32)				
MaintainId	设备维保单位 ID	int(11)			DEFAULT NULL	
Enable	设备是否启用	varchar(1)	√		DEFAULT '0'	0 停用 1 启用

证件保管柜表 LicenseCabinetInfo

代码	名称	类型	非空	主键	规范	备注
CabinetId	证件保管柜 ID	Int(11)	√	√	AUTOINCREMENT	
CabinetStrno	证件保管柜序列号	varchar(40)	√			
CabinetType	证件保管柜型号	int(6)			DEFAULT 1 UNSIGNED	
CreateTime	创建时间	timestamp			CURRENT_TIMESTAMP	
UpdateTime	更新时间	timestamp			CURRENT_TIMESTAMP	
RowNum	证件保管柜抽屉行数	int(5)	√			
ColNum	证件保管柜抽屉列数	int(5)	√			
Remark	备注信息	varchar(255)			DEFAULT NULL	

Enable	是否启用	varchar(1)			DEFAULT '0'	0 停用 1 启用
DeviceId	一体机 ID	int(11)	√			

抽屉与证件关联表 DrawerItem

代码	名称	类型	非空	主键	规范	备注
DrawerItemId	抽屉与证件关联 ID	int(11)	√	√	AUTOINCREMENT	索引
DrawerId	抽屉 ID	int(11)	√		DEFAULT 0	
DocId	证件 ID	int(11)	√		DEFAULT 0	
Status	存放状态	int(5)	√		DEFAULT 0	1 在柜 2 待还 3 撤销
PlanReturnTime	计划归还时间	datetime	√			
PutTime	实际放入时间	datetime	√			

证照保管柜抽屉表 LicenseDrawer

代码	名称	类型	非空	主键	规范	备注
DrawerID	证照保管柜抽屉 ID	Int(11)	√	√	AUTOINCREMENT	
CabinetId	证件保管柜 ID	int(11)				建议使用设备序列号绑定证件保管柜
DrawerRow	行号	int(5)			DEFAULT	

					NULL	
DrawerCol	列号	int(5)			DEFAULT NULL	
chName	中文名字	varchar(64)			DEFAULT NULL	建议绑定人员标识
personID	身份证号的 Md5 值	int(11)			DEFAULT NULL	建议用国密算法，这这个有必要吗？
state	状态	varchar(1)			DEFAULT '0'	0 空闲 1 正在使用 2 异常 3 证件不齐全

用户表 User

说明：能登录系统进行操作的用户

代码	名称	类型	非空	主键	规范	备注
UserId	用户 ID	Int(11)	√	√	AUTOINCREMENT	
OwnerId	主账号 ID	int(11)			DEFAULT '0'	主账号，该 ID 为 0
UserName	用户名	varchar(255)			DEFAULT NULL	
Password	密码	varchar(255)			DEFAULT NULL	
NickName	昵称	varchar(255)			DEFAULT NULL	
RoleId	角色 ID	int(11)			DEFAULT '0'	
CreateTime	创建时间	timestamp			CURRENT_TIMESTAMP	

UpdateTime	修改时间	timestamp			CURRENT_TIMESTAMP	
DeleteStatus	是否有效	varchar(1)			DEFAULT '0'	0 有效 1 无效
DeptId	部门 ID	int(6)			DEFAULT '1' UNSIGNED	

单位表 Dept (组织架构)

代码	名称	类型	非空	主键	规范	备注
DeptID	单位 ID		√	√	AUTOINCREMENT	
DeptName	单位名称	varchar(45)	√			
DeptCode	单位代码	varchar(45)	√			
TYSHXYDM	统一社会信用代码	varchar (32)				
Pid	父级 id	int(6)	√		UNSIGNED	
Level	层级链	varchar(45)	√			
CreateTime	创建时间	timestamp			CURRENT_TIMESTAMP	
UpdateTime	更新时间	timestamp			CURRENT_TIMESTAMP	
DeleteStatus	是否有效	varchar(1)			DEFAULT '0'	0 有效 1 无效

权限表 Permission

代码	名称	类型	非空	主键	规范	备注
PermissionId	权限 ID	Int(11)	√	√	DEFAULT 0	
MenuCode	归属菜单	varchar(1)			DEFAULT 0	
MenuName	菜单的中文释义	varchar(255)				
PermissionCode	权限的代码	varchar(255)				
PermissionName	本权限的中文释义	varchar(255)				
RequiredPermission	是否本菜单必选权限	tinyint			DEFAULT 2	1 必选 2 非必选

角色表 Role

代码	名称	类型	非空	主键	规范	备注
RoleId	角色 ID	Int(11)	√	√	AUTOINCREMENT	
RoleName	角色名	varchar(20)	√		DEFAULT NULL	
CreateTime	创建时间	timestamp			CURRENT_TIMESTAMP	
UpdateTime	更新时间	timestamp			CURRENT_TIMESTAMP	
DeleteStatus	删除标志位	varchar(1)			DEFAULT '0'	

角色权限表 RolePermission

代码	名称	类型	非空	主键	规范	备注

RolePermissionId	角色权限 ID	Int(11)	√	√	AUTOINCREMENT	
roleID	设备 ID	int(11)	√		DEFAULT NULL	
permissionID	权限 ID	int(11)			DEFAULT NULL	
createTime	创建时间	timestamp			CURRENT_TIMESTAMP	
updateTime	更新时间	timestamp			CURRENT_TIMESTAMP	
deleteStatus	删除标志位	varchar(1)			DEFAULT '0'	

用户设备表 **UserDevice**

代码	名称	类型	非空	主键	规范	备注
UserId	用户 ID	Int(11)	√		DEFAULT 0 UNSIGNED	
DeviceId	一体机 ID	int(11)	√		DEFAULT 0 UNSIGNED	

设备上报信息表 **ZzgMsg**

代码	名称	类型	非空	主键	规范	备注
MsgID	上报信息 ID	Int(11)	√	√	AUTOINCREMENT	
MsgTime	消息接收时间	timestamp			CURRENT_TIMESTAMP	
DeviceId	一体机 ID	int(11)	√			
CabinetId	证件保管柜 ID	int(11)	√			

MsgType	消息类型	int(11)			DEFAULT 0	
ZzgStatus	证照柜状态	int(5)			DEFAULT 0	
Msg	消息字符串	varchar(128)			DEFAULT NULL	

2.1.6 接口设计

无

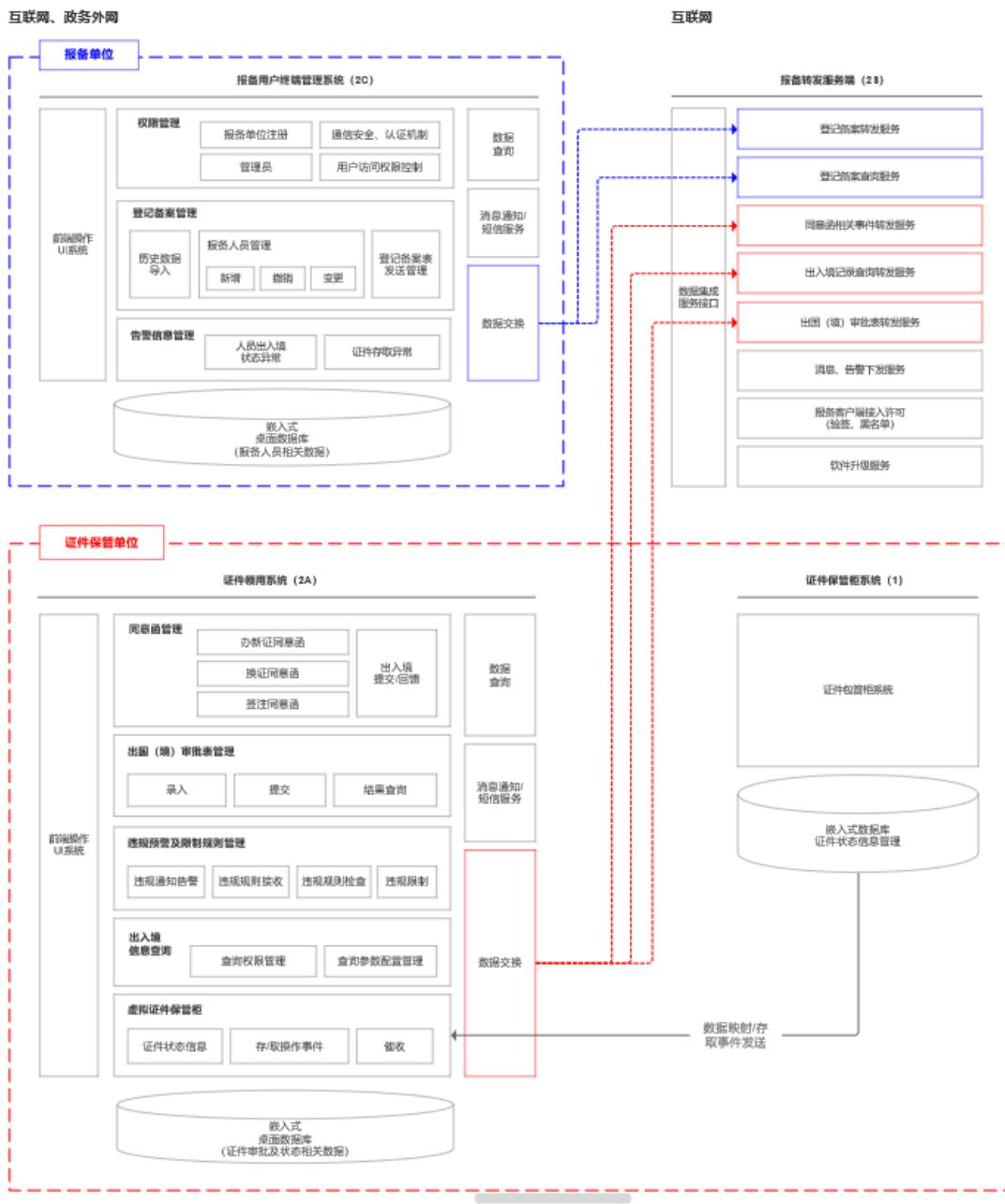
2.2 备案审批系统

2.2.1 概述

报备审批管理系统主要实现国家工作人员因私出国（境）所需的人员登记备案，证件受理（新证，换证，撤销）、证件领取审批及证件查询请求等相关业务功能。

2.2.2 总体构架

系统构架：系统采用 C/S 的构架，由报备用户终端管理系统（2C），证件领用系统（2A），报备审批后台系统（2S）共同组成。



2.2.3 功能设计

2.2.3.1 报备用户终端管理系统 (2C)

2.2.3.1.1 概述

登记报备用户终端系统用于报备单位的报备人员信息管理。同时，支持从报备终端向出入境管理部门提交报备人员信息，并接收来自出

入境部门的报备反馈信息。

2.2.3.1.2 功能描述

(1) 报备单位注册：用户安装登记报备系统之后，需要经过系统运营部门的信息核实，并向用户发放应用 ID, UKey 或者加密卡等设备，用于系统的应用激活。应用注册功能用于激活用户终端应用，达到可用状态。

(2) 管理员信息注册：当用户应用注册之后，需要报备单位指定的管理员需要向系统上报管理员身份信息，如：姓名、身份证号、手机号等。

(3) 报备人员管理：用于添加本单位的报备人员信息以及该人员的报备记录，并存储与本地数据库中。

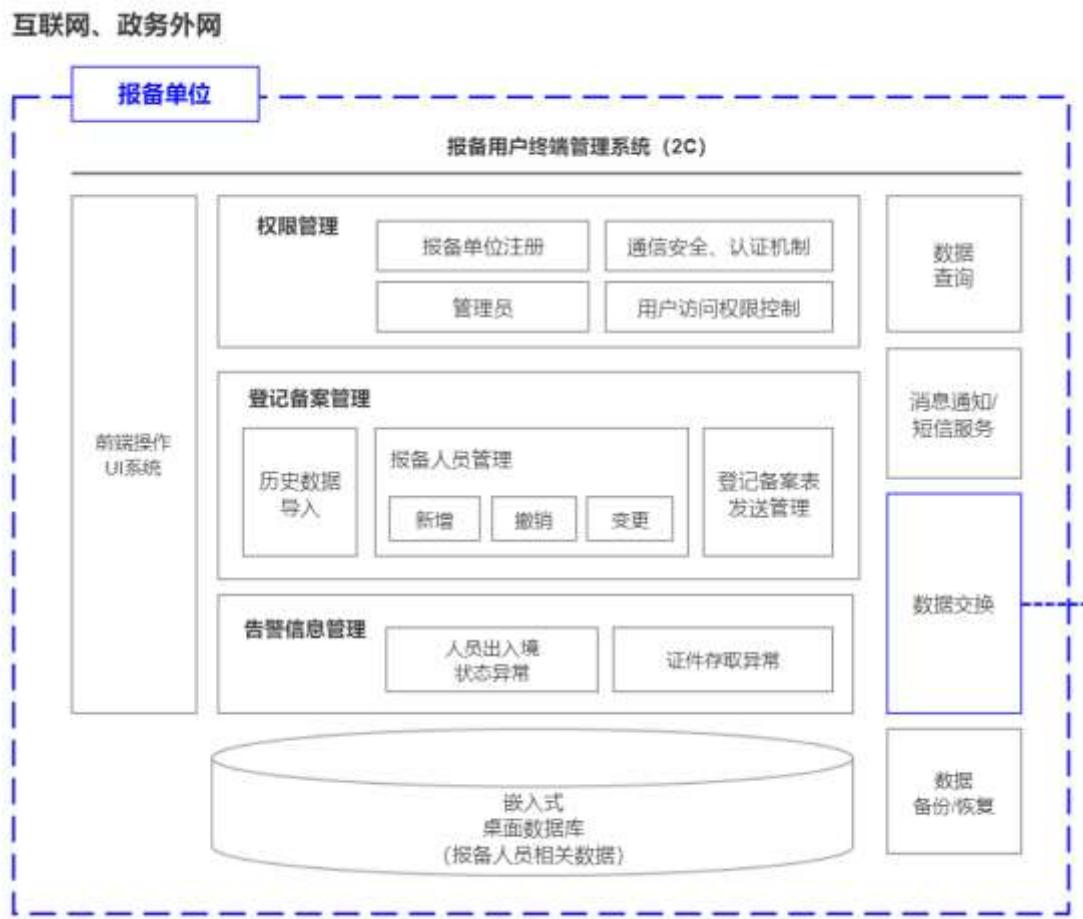
(4) 登记报备表发送管理：用于向出入境发送报备人员信息表，完成在线报备工作，登记报备表包含：新增报备人员和撤销报备人员。

(5) 报备人员历史数据导入：支持从出入境管理部门提供你的本单位报备人员信息及持证信息导入到系统中。

(6) 人员出入境状态和证件存取异常告警：报备单位可以接收“登记报备系统服务端（2S）”系统发送的人员出入境异常、证件存取异常、以及催缴信息。

(7) 告警信息短消息配置：允许报备系统配置短消息服务，用于向已报备人员发送证件催缴和报备流程相关通知信息。

2.2.3.1.3 功能架构



图表 2.2-1 报备用户终端功能架构图

2.2.3.1.4 功能设计

2.2.3.1.4.1 报备单位注册

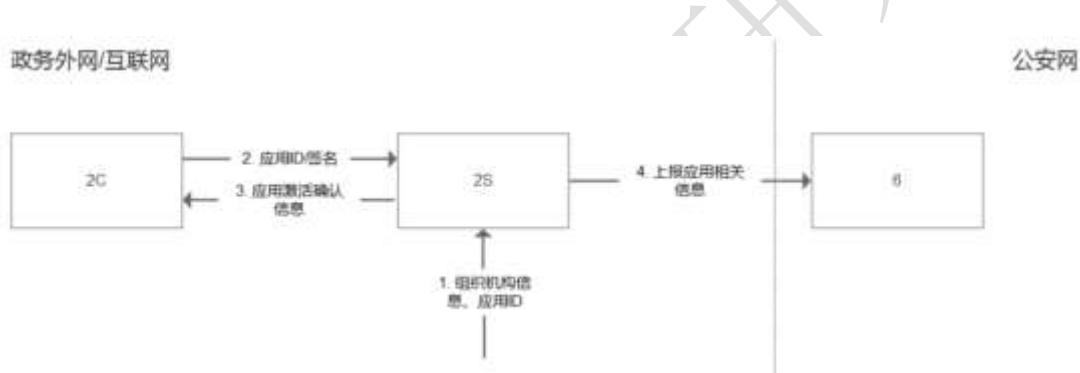
功能描述

用户安装登记报备系统之后，需要经过系统运营部门的信息核实，并向用户发放应用 ID，UKey 或者加密卡等设备，用于系统的应用激活。应用注册功能用于激活用户终端应用，达到可用状态。**(单位信息置于 UKEY 中，激活是一次性的)**



图 2.4.4-1 报备单位注册激活

数据流图



图表 2.4.4-2 报备应用激活数据流转图

(1) 在签发加密卡/U 盾时，录入报备单位基本信息同时生成对应的应用激活 ID 和秘钥，将加密卡/U 盾以及激活 ID 和秘钥交给报备单位。

(2) 客户插入 U 盾后，启动报备应用输入应用激活 ID 和秘钥后，应用对激活 ID 和秘钥进行加密并签名并发送给应用服务器

(3) 应用服务器收到激活信息后，对签名进行验签确认合法接入性，然后对数据进行解密，验证通过后，确认激活信息。

(4) 应用服务器同步报备应用客户激活信息给综合信息管理平

台。

2. 2. 3. 1. 4. 2 管理员注册

功能描述

当用户应用注册之后，报备单位指定的管理员需要向系统上报管理员身份信息，如：姓名、身份证号、手机号等。

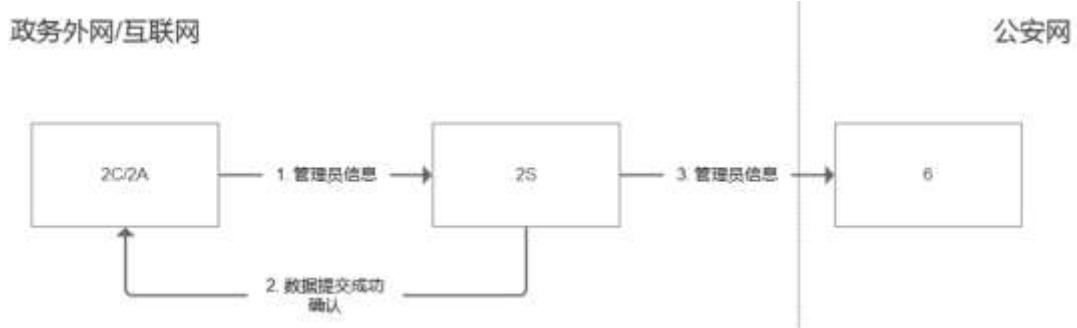
This screenshot shows the 'Administrator Basic Information' registration page. On the left, there is a dark sidebar with the 'AntDesign' logo and a navigation menu containing items like '配属管理', '报备单位', '报备事项管理', '登记事项管理', and '报备流程管理'. The main content area has a light blue header bar with tabs for '基本信息' (Basic Information), '修改密码' (Change Password), and '配置地图' (Configure Map). The '基本信息' tab is active. It contains fields for '用户名' (Username) with value 'admin', '姓名' (Name) with placeholder '请输入姓名', '身份证号码' (ID Card Number) with placeholder '身份证号码' and note '身份证号码必须为18位', '公民身份号码' (Citizen ID Number) with placeholder '公民身份号码', '手机号码' (Mobile Phone Number) with value '18812345678', and a '验证码' (Verification Code) input field with placeholder '请输入验证码'. A blue '提交' (Submit) button is located at the bottom right.

图 2. 4. 4-3 管理员基本信息

This screenshot shows the 'Administrator Change Password' page. The layout is similar to the previous one, with a dark sidebar on the left and a light blue header bar with tabs for '基本信息' (Basic Information), '修改密码' (Change Password), and '配置地图' (Configure Map). The '修改密码' tab is active. It features three input fields: '旧密码' (Old Password), '新密码' (New Password), and '确认新密码' (Confirm New Password). Below these fields is a blue '立即修改' (Immediately Modify) button.

图 2. 4. 4-4 管理员修改密码

数据流图



图表 2.4.4-6 管理员数据流图

2.2.3.1.4.3 报备人员管理

功能描述

用于添加本单位的报备人员信息以及该人员的报备记录，并存储与本地数据库中。

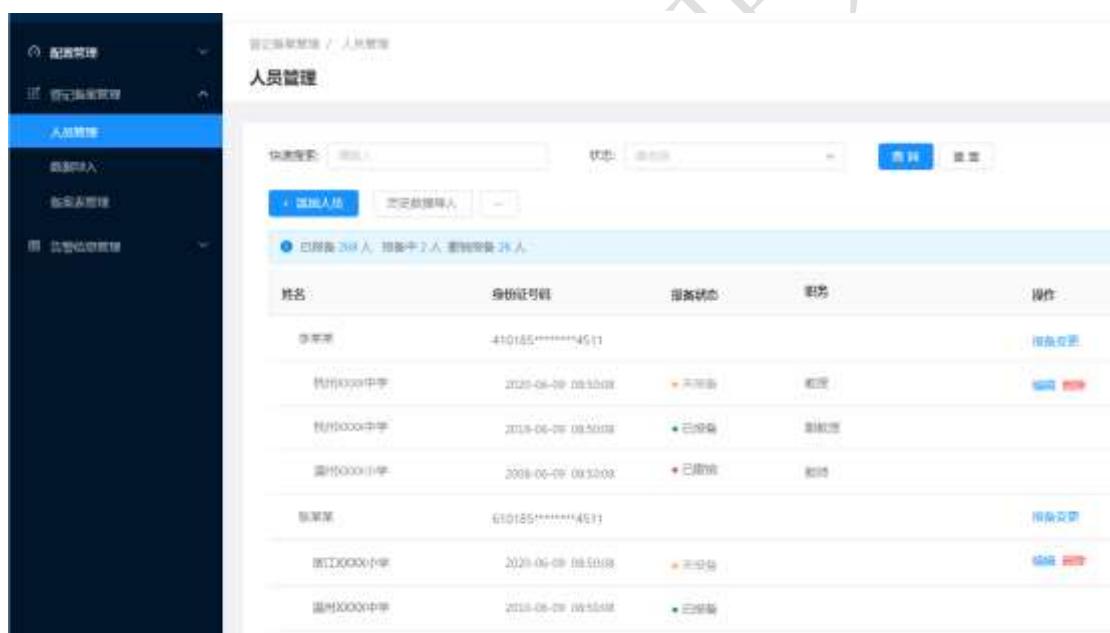


图 2.4.4-7 人员管理

AntDesign

配置管理 / 登记报备管理 / 添加人员

添加人员

人员信息录入

姓名:

身份证号码:

单位名称:

单位代码:

电话号码: -

手机:

操作:

图 2.4.4-8 添加人员

2.2.3.1.4.4 登记报备表发送管理

功能描述

用于向出入境发送报备人员信息表，完成在线报备工作，登记报备表包含：新增报备人员和撤销报备人员。

AntDesign

配置管理 / 登记报备管理

备案表管理

操作:

备案业务流水号	报备状态	创建日期	完成日期	操作
911101000021012214	● 未报备	2016-09-21 08:55:08	2016-09-21 08:55:08	<input type="button" value="编辑"/> <input type="button" value="删除"/>
911101000021012219	● 进行中	2016-09-21 08:50:08	2016-09-21 08:50:08	
911101000021012200	● 已报备	2016-09-21 08:50:08	2016-09-21 08:50:08	
911101000021012210	● 已报备	2016-09-21 08:50:08	2016-09-21 08:50:08	
911101000021012205	● 已报备	2016-09-21 08:50:08	2016-09-21 08:50:08	

图 2.4.4-9 备案表管理

图 2.4.4-10 备案表提交

数据流图



图表 2.4.4-13 报备人员及报备记录数据流图

2.2.3.1.4.5 报备人员历史数据导入

功能描述

支持从出入境管理部门提供你的本单位报备人员信息及持证信息导入到系统中。



图 2.4.4-11 历史数据导入成功



图 2.4.4-12 历史数据导入失败

2.2.3.1.4.6 人员出入境状态和证件存取异常告警

功能描述

报备单位可以接收“登记报备系统服务端（2S）”系统发送的人员出入境异常、证件存取异常、以及催缴信息。



图 2.4.4-5 告警催缴

2.2.3.1.4.7 告警信息短消息配置

功能描述

允许报备系统配置短消息服务，用于向已报备人员发送证件催缴和报备流程相关通知信息



图 2.4.4-5 管理员短信 API 配置

2.2.3.1.5 数据结构

数据库表清单

名称	代码	备注
m_djba_yhxx_t	用户信息表	
m_djba_zzjgxx_t	组织机构信息表	
m_djba_bbdwxx_t	报备单位信息表	
m_djba_bbryxx_t	报备人员信息表	
m_djba_bbjl_t	人员报备记录表	
m_djba_baxx_t	登记备案信息表	
m_djba_gjxxjl_t	告警信息记录表	

(1) m_djba_yhxx_t 【用户信息表】

代码	名称	数据类型	主键	备注
ID	用户 ID	VARCHAR(32)		
MM	密码 HASH	VARCHAR(32)		
XM	姓名	VARCHAR(32)		密文
GMSFHM	公民身份证号码	VARCHAR(32)		密文
SJHM	手机号码	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmm mss
ZXGXSJ	最新更新时间	DATETIME		

(2) m_djba_zzjgxx_t 【组织机构信息表】

代码	名称	数据类型	主键	备注
ZZJGDM	组织机构代码	VARCHAR(32)	是	
DWMC	单位名称	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(3) m_djba_bbdwxx_t 【报备单位信息表】

代码	名称	数据类型	主键	备注
ZZJGDM	组织机构代码	VARCHAR(32)		
APPID	应用 ID	VARCHAR(32)	是	
DWMC	单位名称	VARCHAR(32)		
LXFS	联系方式	VARCHAR(32)		
LXDZ	联系住址	VARCHAR(32)		
FFZT	服务状态	VARCHAR(32)		
DXAPI	短信 API	VARCHAR(128)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(4) m_djba_bbryxx_t 【报备人员信息表】

代码	名称	数据类型	主键	备注
XM	姓名	VARCHAR(32)		密文
GMSFHM	公民身份证号 码	VARCHAR(32)		密文
RYID	人员 ID	VARCHAR(32)		
SJHM	手机号码	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(5) m_djba_bbjl_t 【人员报备记录表】

代码	名称	数据类型	主键	备注
ID	报备记录 ID	VARCHAR(32)	是	
BBYWLSH	报备业务流水号	VARCHAR(32)		
BBLX	报备类型	VARCHAR(32)		1 报备, 2 撤销
BBZT	报备状态	VARCHAR(32)		1 未报备 2 报备中 3 已报备 4 撤销中 5 已撤销
GMSFHM	公民身份证号 码	VARCHAR(32)		密文
ZZJGDM	组织机构代码	VARCHAR(32)		
SPDWDM	审批单位住址机构代码	VARCHAR(32)		
ZW	职务	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(6) m_djba_baxx_t 【登记备案信息表】

代码	名称	数据类型	主键	备注
BBYWLSH	报备业务流水号	VARCHAR(32)	是	
BBSPD	报备审批单	VARCHAR(3072)		
TJZT	提交状态	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(7) m_djba_gjxxjl_t 【告警信息记录表】

代码	名称	数据类型	主键	备注
GJYWLSH	告警业务流水号	VARCHAR(32)		
RYID	人员 ID	VARCHAR(32)		
GJLX	告警类型	VARCHAR(32)		
YQTS	逾期天数	VARCHAR(32)		
GJXX	告警信息描述	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

2.2.3.1.6 接口设计

无。

2.2.3.2 证件领用系统（2A）

2.2.3.2.1 概述

证件领用系统是单位工作人员各种出入境证件的保管和领用的系统，系统实现出国（境）审批表，多种证件办理同意函（新增，换证，签注）的电子化，并将相关数据，文件上报出入境管理局，实现工作人员办证，领证快捷化，自动化。

2.2.3.2.2 功能描述

1、**出国（境）审批表管理：**主要是管理本单位工作人员出国（境）审批表，系统依据申请人相关信息及持证信息自动判断申请人是否需要同时办理相关的证件受理同意函，并打印审批表，提交领导签字后，将审批表及相关数据存档。

2、**同意函管理：**辅助单位实现同意函的数字化管理，包括：(1) 同意函的模板管理，单位工作人员提出出国申请后，系统根据申请人录入信息和持证信息，生成同意函模板；(2)支持纸质同意函的上报，可以支持单位纸质同意函电子化和信息的上报；(3) 对接单位 OA 系统，实现同意函的数字化及自动上报。

3、**虚拟证件柜：**在单位没有配置实体证件柜时，提供虚拟证件保管柜，辅助实现存取证件的信息上报。管理员通过虚拟证件柜来实现证件的领取，存入操作，当有实体证件柜时，可以将实体证件柜接入系统，实现证件存取操作。

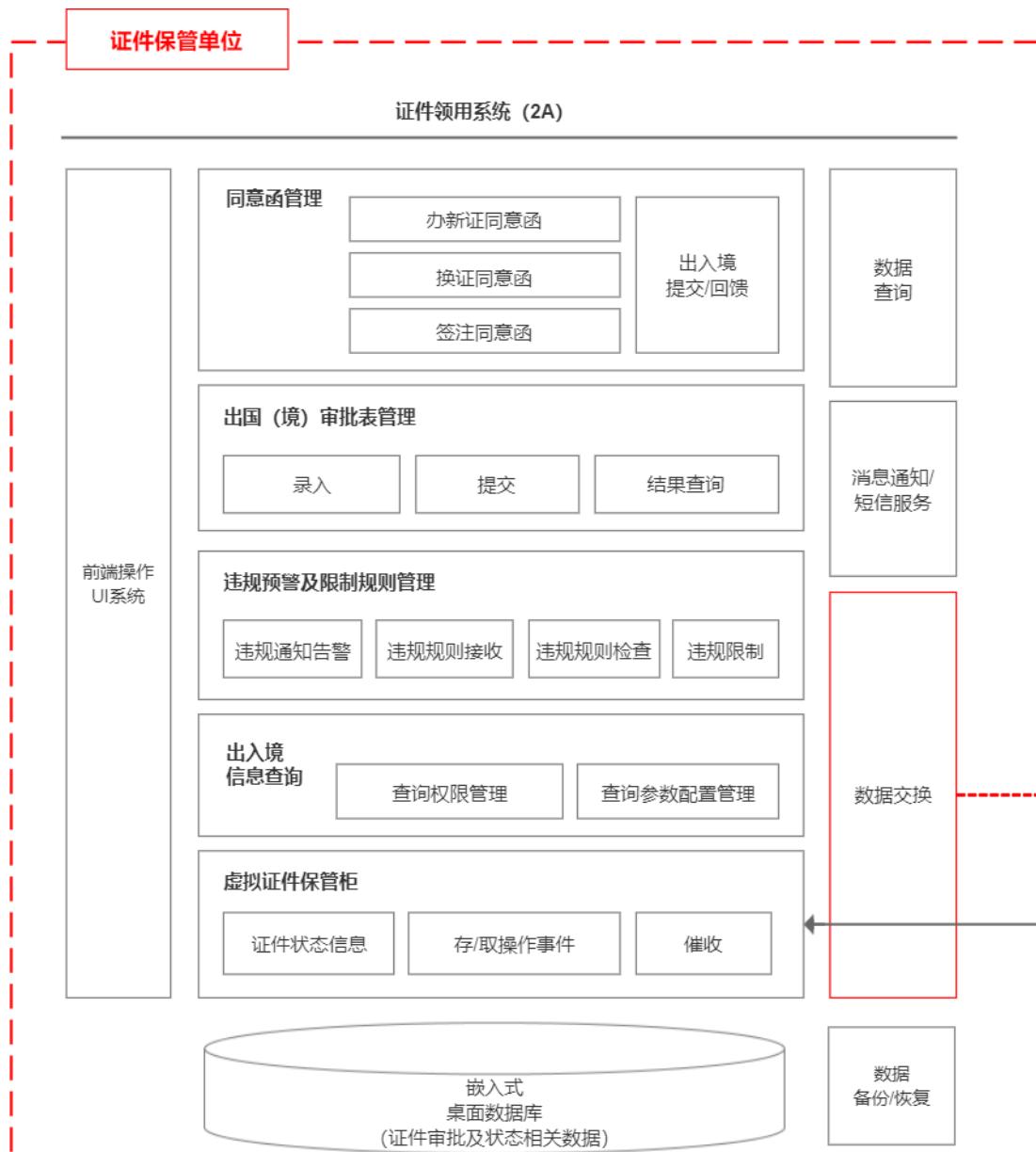
4. **人员出入境状态和证件存取异常告警：**报备单位可以接收“登

记报备系统服务端（2S）”系统发送的人员出入境异常、证件存取异常、以及催缴信息。

5、告警信息短消息配置：允许报备系统配置短消息服务，用于向已报备人员发送：

- (1) 证件催缴告警；
- (2) 和出入境业务流程（办证、换证、签注）相关通知信息；
- (3) 证件即将过期提醒。

2.2.3.2.3 功能架构



2.2.3.2.4 功能设计

2.2.3.2.4.1 出国（境）审批表管理

功能描述：

出国（境）审批表管理主要是管理本单位工作人员出国（境）审批表，系统依据申请人相关信息及持证信息自动判断申请人是否需要同时办理相关的证件受理同意函，并打印审批表，提交领导签字后，将审

批表及相关数据存档。

出国（境）审批表：填写和导入单位出国境需求人员信息：

出国（境）审批表

导出 导入

序号	姓名	身份证号码	报备类型	出生日期	工作单位	人事主管单位	单位职务
1	张三	1234567890012345678	报备	2000-02-02	xxxxxx	xxxxxx	xxxxx
+ [新增]							

因私出国（境）人员信息

身份证号	手机号:
姓: 名:	工作时间:
性别: <input checked="" type="radio"/> 男 <input type="radio"/> 女	职称/职称:
出生日期:	单位职务:
籍贯:	政治面貌:
民族:	健康状况:
出国(境)时间:	出国(境)目的地:
上次出国(境)时间:	上次出国(境)地点:
申请出国(境)事由:	工作简历
国内直系亲属及主要社会关系	国外直系亲属及主要社会关系

保存 上一个 下一个

组包打印：将相关信息分组并打印纸质审批单。

组包打印 重新打印

身份证号: 姓名: 查询

序号 姓名 身份证号码 性别 出生日期 工作单位 人事主管单位 职级/职称 户口所在地

1 张三 1234567890012345678 男 2000-02-02 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

<<上页 1 下页>> 共1条

全选/取消 组包打印

区管干部因私出国（境）审批单

姓名	性别	出生日期	民族	籍贯	现住
代办人姓名	工作时间	单位职务	健康状况	入党时间	
代办人手机号		工作单位			
代理人手机号					
本人手机号					
本人身份证号					
国内直系亲属及主要社会关系		国外直系亲属及主要社会关系			
出境（境）目的	赴港（境）时间	赴港（境）外停留时间	同行人员	上次因私出境（境）时间	上次因私出境（境）地点
申请出国（境）事由	本人签名: _____ 年 月 日				

电子档案：对纸质审批单进行电子照片采集。

电子档案采集

组包号:

组包时间: 2020-03-10 18:10:29

2020-06-10 18:10:29

查询

序号 组包号 类别 状态 组包人页数 1 组包人 组包时间 操作

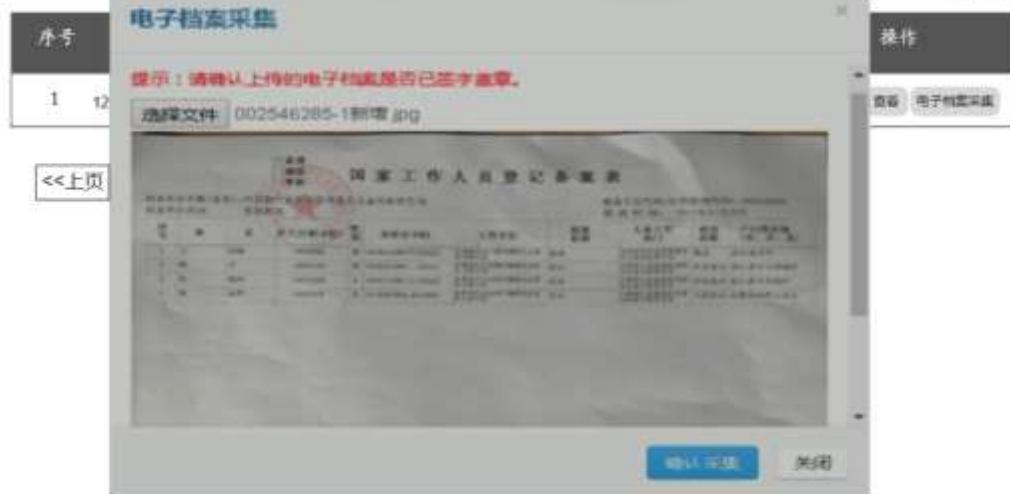
1 1234567890012345678 待证 已组包 1 XXXXXXXX 2020-06-10 18:10:29

查看 电子档案采集

<<上页 1 下页>> 共1条

电子档案采集

组包号: [] 组包时间: [2020-03-10 18:10:29] [2020-06-10 18:10:29] [查询]



审批表上报：将相关申请数据及电子照片保存并上报系统后台。

审批表上报

组包号: [] 组包时间: [2020-03-10 18:10:29] [2020-06-10 18:10:29] [查询]

序号	组包号	类别	状态	组包人员数量	组包人	组包时间	操作
1	1234567890012345678	领证	已组包	1	xxxxxx	2020-06-10 18:10:29	[查看, 上报]

[<<上页] [1] [下页>>] [共1条]

查询统计：查询本单位审批表情况。

查询统计

组包号: 组包时间:

业务类别:

状态:

序号	组包号	类别	状态	组包人员数量	组包人	组包时间	操作
1	1234567890012345678	检测	已入库	1	xxxxxx	2020-06-10 18:10:29	<input type="button" value="查看"/>

共1条

2.2.3.2.4.2 同意函管理

功能描述:

单位工作人员提出出国申请后，系统自动分析该申请人的持证信息，并给出相应函件处理模式，方便工作人员直接处理。

同意函登记：编辑系统自动生成的同意函或手工新增同意函信息。

同意函

序号 姓名 身份证号码 工作单位 职务 登记单位 登记人 登记时间

1 张三 1234567890012345678 XXXXXXXXXX 财务 XXXXXXXX XXXXXX XXXXXX

申办出入境证件人员信息

身份证号:

职务:

姓名:

工作单位:

办证种类:

护照

往来港澳通行证及香港签注

往来港澳通行证及澳门签注

往来台湾通行证及签注

特殊说明:

提示: 签注默认为一年一次有效港澳旅游签注(团队或个人)或六个月一次有效赴台旅游
签注(团队或个人), 允许办理其他种类签注的, 应在特殊说明中注明。

登记人:

登记单位:

登记时间:

联系电话:

管辖单位: XXX公安局出入境管理局

保存

组包打印: 选择同意函并打印, 进行纸质同意函审批操作。

组包打印 重新打印

身份证号:

姓名:

查询

序号	姓名	身份证号码	工作单位	职务	登记单位	登记人	登记时间
----	----	-------	------	----	------	-----	------

1

张三 1234567890012345678

XXXXXXXXXX

副高

xxxxxx

xxxxxx

xxxxxx

组包打印

关于同意吕小华
申办出入境证件的函

编号: T00254500420171130X10010003

嘉兴市公安局出入境管理局:

同志(身份证号码:)系嘉兴市第三中学(单位全称)的副高(职务)。按照干部管理权限,我单位同意该人申办:

- 普通护照 往来港澳通行证及香港签注
 往来港澳通行证及澳门签注 往来香港通行证及签注

组织、人事部门联系人姓名: 俞敏娟

联系电话: 17788560744

负责人签名: 公章:

日期: 年 月 日

备注: 1、登记备案国家工作人员申请出入境证件须提交此函,如有涂改,本函无效。
2、登记备案单位须在同意办理的出入境证件类型前打“√”,再不同意办理的证件类型前打“×”。
3、本函自开具之日起3个月内有效。
4、因受理往来港澳和台湾签注申请涉及出入境次数问题,如有关组织人事部门无特别说明,公安机关为登记备案国家工作人员办理因私事赴港澳台签注时均签发一次出入境有效签注。特别说明:

(请文字说明并加盖公章)

组包打印 重新打印

组包号:

组包时间: 2020-03-10 18:10:29

2020-06-10 18:10:29

查询

序号	组包号	类别	状态	组包人员数量	组包人	组包时间	操作
1	1234567890012345678	同意函	已组包	1	xoooox	2020-06-10 18:10:29	重新打印

电子档案：对打印并领导审批完成的同意函进行拍照，生成图片数据。

电子档案采集

组包号:	2020-03-10 18:10:29	2020-06-10 18:10:29	查询				
序号	组包号	类别	状态	组包人员数量	组包人	组包时间	操作
1	1234567890012345678	同意函	已组包	1	xxxxxx	2020-06-10 18:10:29	查看 电子档案采集



同意函上报：将审批完成的同意函及电子数据一起上报系统后台。

同意函上报

组包号:	2020-03-10 18:10:29	2020-06-10 18:10:29	查询				
序号	组包号	类别	状态	组包人员数量	组包人	组包时间	操作
1	1234567890012345678	同意函	已组包	1	xxxxxx	2020-06-10 18:10:29	查看 上报

查询统计：查询和统计本单位同意函上报情况。

查询统计

组包号:	<input type="text"/>	组包时间:	2020-03-10 18:10:29	2020-06-10 18:10:29			
业务类别:	<input type="text"/> 请选择...	状态:	<input type="text"/> 请选择...	<input type="button" value="高级"/>	<input type="button" value="查询"/>		
序号	组包号	类别	状态	组包人员数量	组包人	组包时间	操作
1	1234567890012345678	商誉清	已入库	1	xxxxxx	2020-06-10 18:10:29	<input type="button" value="查看"/>

2.2.3.2.4.3 数据查询

功能描述:

数据查询模块主要实现本单位报备人员的持证信息及出入境信息的查询。

持证信息查询: 查询本单位报备人员的持证信息:

持证信息查询									
身份证号:	<input type="text"/>	姓名:	<input type="text"/>	证件类别:	<input type="text"/> 请选择...	状态:	<input type="text"/> 请选择...		
<input type="button" value="高级"/>	<input type="button" value="查询"/>	序号	身份证号	姓名	证件类型	证件号码	有效期		
		1	330110****0021	张三	港澳台证	22****32	2020-05-10	01-02-01	2020-06-10 18:10:29

出入境查询: 查询本单位报备人员的出入境信息(暂未开放)。

2.2.3.2.4.4 人员出入境状态和证件存取异常告警

功能描述

报备单位可以接收“登记报备系统服务端（2S）”系统发送的人员出入境异常、证件存取异常、以及催缴信息。



图 2.2.4-4 业务告警信息

2.2.3.2.4.5 告警信息短消息配置

功能描述

允许报备系统配置短消息服务，用于向已报备人员发送：

- (1) 证件催缴告警；
- (2) 和出入境业务流程（办证、换证、签注）相关通知信息；
- (3) 证件即将过期提醒。

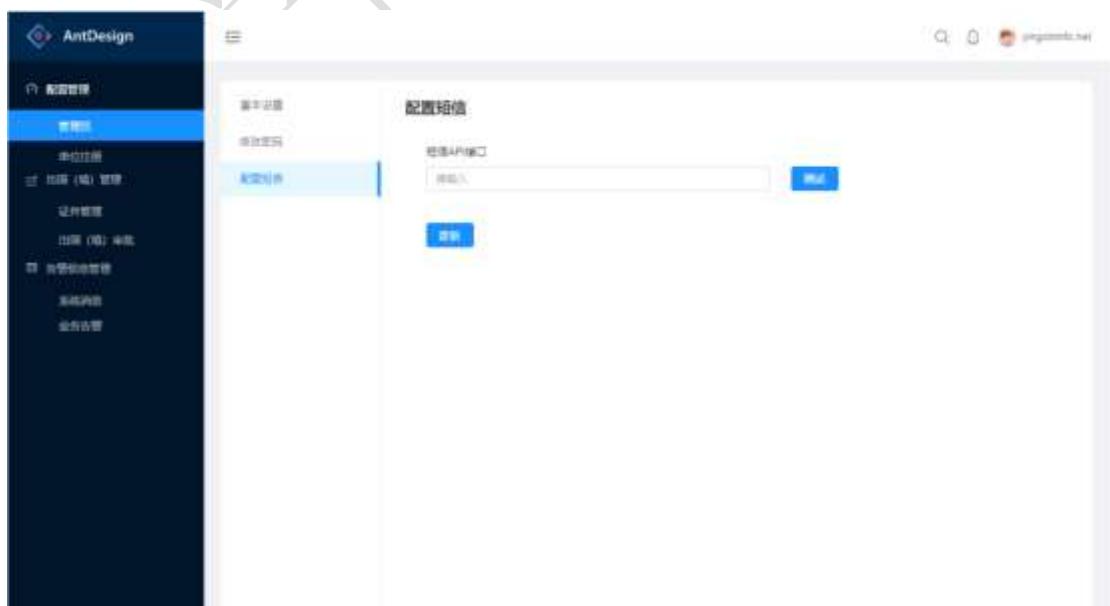


图 2.2.4-4 短信验证码配置

2.2.3.2.5 数据结构

数据库表清单

名称	代码	备注
m_zjly_yhxxb_t	单位用户信息表	
m_zjly_dwxxt	单位信息表	
m_zjly_bbryxx_t	报备人员信息表	
m_zjly_gjxxjl_t	告警信息记录表	
m_zjly_zjxx_t	证件信息表	
m_zjly_zjqcq_t	证件存取事件表	
m_zjlx_cgjsp_t	出国境审批表	
m_zjly_tyh_t	同意函表	

(1) m_zjly_yhxxb_t 【单位用户信息表】

代码	名称	数据类型	主键	备注
ID	用户 ID	VARCHAR(32)		
MM	密码 HASH	VARCHAR(32)		
XM	姓名	VARCHAR(32)		密文
GMSFHM	公民身份证号码	VARCHAR(32)		密文
SJHM	手机号码	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(2) m_zjly_dwxx_t 【单位信息表】

代码	名称	数据类型	主键	备注
ZZJGDM	组织机构代码	VARCHAR(32)		
APPID	应用 ID	VARCHAR(32)	是	
DWMC	单位名称	VARCHAR(32)		
LXFS	联系方式	VARCHAR(32)		
LXDZ	联系住址	VARCHAR(32)		
FFZT	服务状态	VARCHAR(32)		
DXAPI	短信 API	VARCHAR(128)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(3) m_zjly_bbryxx_t 【报备人员信息表】

代码	名称	数据类型	主键	备注
XM	姓名	VARCHAR(32)		密文
GMSFHM	公民身份证号码	VARCHAR(32)		密文
RYID	人员 ID	VARCHAR(32)		
SJHM	手机号码	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(4) m_zjly_gjxxjl_t 【告警信息记录表】

代码	名称	数据类型	主键	备注
GJYWSH	告警业务流水号	VARCHAR(32)		
RYID	人员 ID	VARCHAR(32)		
GJLX	告警类型	VARCHAR(32)		
YQTS	逾期天数	VARCHAR(32)		
GJXX	告警信息描述	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(5) m_zjly_zjxx_t 【证件信息表】

代码	名称	数据类型	主键	备注
RYID	人员 ID	VARCHAR(32)		
ZJID	证件 ID	VARCHAR(32)		
ZJLX	证件类型	VARCHAR(32)		
ZJHM	证件号码	VARCHAR(32)		
XM	姓名	VARCHAR(32)		
CSRQ	出生日期	VARCHAR(32)		
YXQZ	有效期至	VARCHAR(32)		
ZJZT	证件状态	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(6) m_zjly_zjcq_t 【证件存取事件表】

代码	名称	数据类型	主键	备注
ZJCQYWLSH	证件存取业务流水号	VARCHAR(32)		
ZJID	证件 ID	VARCHAR(32)		
CQSJ	存取事件	VARCHAR(32)		1. 存入 2 取出
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(7) m_zjlx_cgjsp_t 【出国境审批表】

代码	名称	数据类型	主键	备注
SPBYWLSH	出国(境)审批业务流水号	VARCHAR(32)		
RYID	人员 ID	VARCHAR(32)		
ZJID	证件 ID	VARCHAR(32)		
CFSJ	出发时间	VARCHAR(32)		
FHSJ	返回时间	VARCHAR(32)		
MDD	目的地	VARCHAR(32)		
SPDWJ	审批表 PDF 文件	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

(8) m_zjly_tyh_t 【同意函表】

代码	名称	数据类型	主键	备注
SPBYWLSH	出国(境)审批业务流水号	VARCHAR(32)		
TYHYWLSH	同意函业务流水号	VARCHAR(32)		
CRJYWLX	出入境业务类型	VARCHAR(32)		1. 办新证 2. 换发 3. 签发
TYHWJ	同意函 PDF 文件	VARCHAR(32)		
RKSJ	入库时间	VARCHAR(14)		YYYYMMDDhhmmss
ZXGXSJ	最新更新时间	DATETIME		

2.2.3.2.6 接口设计

无。

2.2.3.3 报备转发服务端 (2S)

2.2.3.3.1 概述

登记备案转发服务、登记备案查询服务、同意函相关事件转发服务、出入境记录查询转发服务、出国（境）审批表转发服务、消息、告警下发服务、报备客户端接入许可（验签、黑名单）、软件升级服务。

总体架构

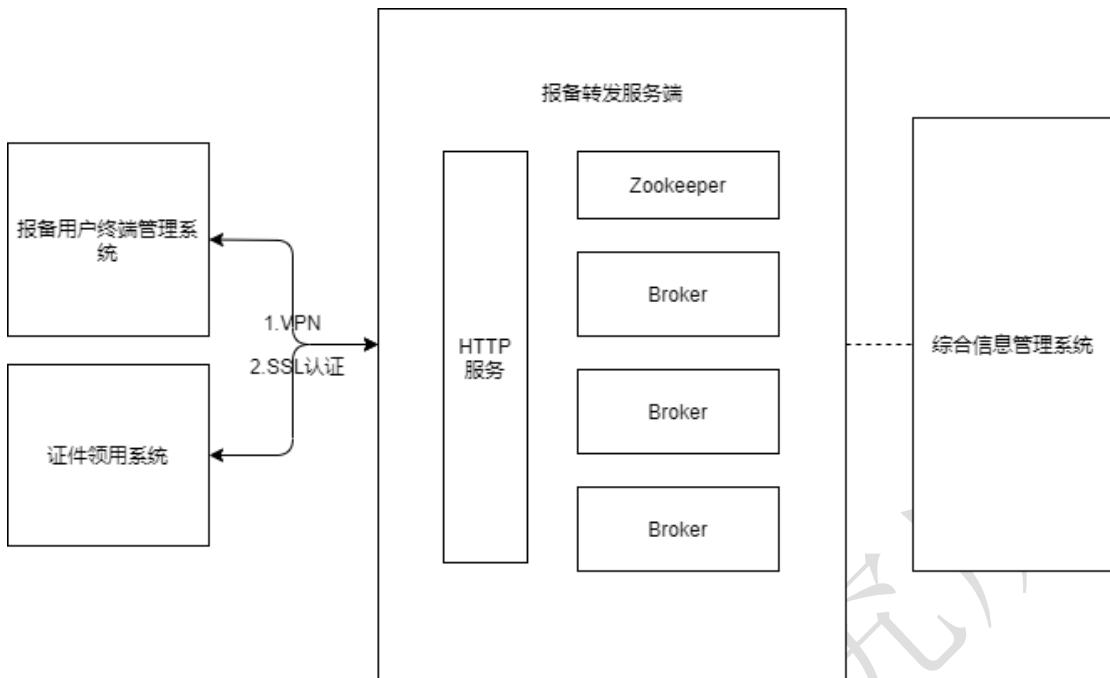


图 2.3.1-1 功能架构

2.2.3.3.2 功能描述

1. 登记备案转发服务

报备系统的人员报备信息提交到本系统中，再上传到公安网的管理平台最后上报给出入境系统，管理平台反馈人员报备状态和持证信息传回证件领用系统和报备用户终端管理系统。

2. 登记备案查询服务

出入境管理系统提供接口用于各单位查询备案人员，调用流程从报备用户终端管理系统发起，上传到本系统中再转发给公安网综合信息管理系统去调用出入境接口完成查询，结果反馈给报备用户终端管理系统。

3. 出国（境）审批表转发

备案人员因私出国（境）申领证件的，需要在证件领用系统中发

起申请并上传纸质审批表电子扫描件。出国（境）请求发送到本系统后进行转发上报给公安网综合信息管理系统最终会提交给出入境系统，结果层层返回给证件领用系统。

4. 同意函转发

证件办理流程中，涉及到新证件办理、证件换领、通行证签注时需要提交相关同意函。同意函信息在证件领用系统中生成，并提交到本系统，转发给公安网综合信息管理系统和出入境系统进行确认才能办理证件业务。

5. 出入境记录查询转发

管理单位需要发起人员出入境记录查询业务时，将相关查询请求发送到本系统，通过本系统调用出入境接口进行查询，异步查询结果反馈给查询单位。

6. 消息、告警下发

备案人员取出证件后，综合信息管理系统会定期通过出入境系统查询人员出入境状态，当出现入境记录、超期记录或逾期未上缴记录就会生成相关催缴信息或告警信息发送到本系统，由本系统下发这类信息到证件保管单位进行催缴处理。

7. 报备客户端接入许可

证件领用系统初次上线时需要连接本系统，根据应用 id、ukey 信息和数据签名校验客户端系统合法性，通过校验的系统允许接入系统提供服务。

8. 软件版本校验及更新

备案登记客户端与证件领用客户端定时进行版本校验，发现新版本时会进行消息提醒，并提供下载功能。

2.2.3.3 功能架构

考虑到本系统与其他上下游（登记备案用户终端、证件领用管理终端、综合信息管理系统、出入境系统）交互主要是异步通信，证件领用系统作为下游存在非长期开机的情况，并且与出入境系统的通信存在跨网络传输的场景。为了保障数据安全不被泄露，以及通信数据准确无误，设计本系统和证件领用系统之间通过 http 服务+消息队列的方式进行网络通信。



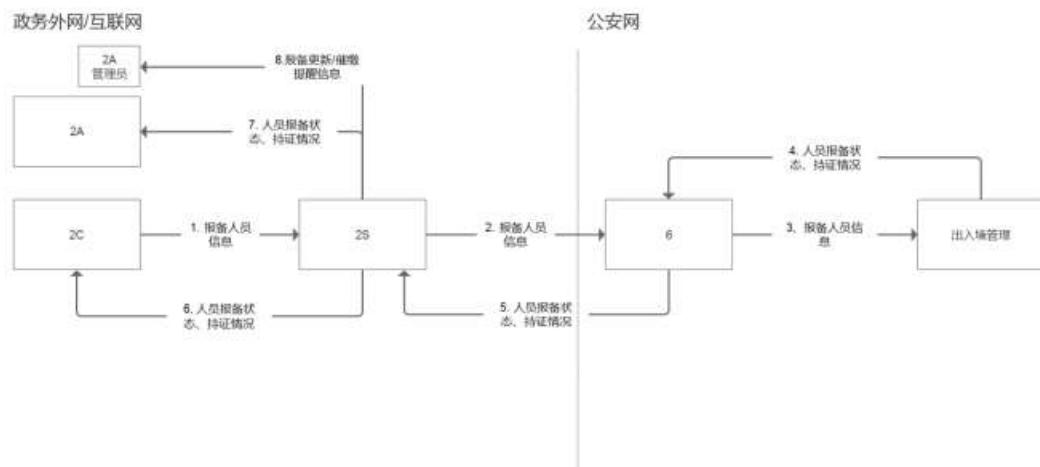
图 2.3-1 报备转发服务端

2.2.3.3.4 功能设计

1. 登记备案转发服务

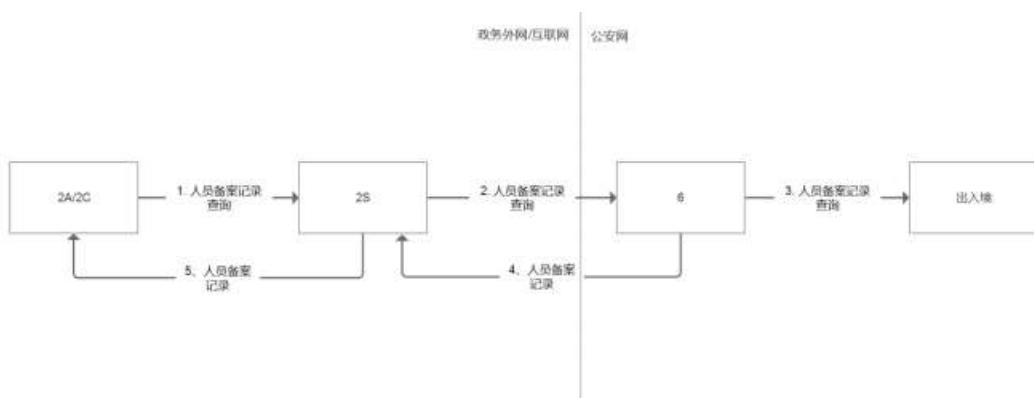
证件领用系统调用 http 接口传送备案信息到本系统，立即返回接收成功标识。本系统将报备信息上报给综合信息管理系统最终提交给

出入境系统，待综合信息管理系统得到报备反馈信息（人员报备状态、人员持证情况）后通过网闸文件交换方式传输到本系统中，生成对应的报备结果反馈信息发布到消息队列中，报备用户终端管理系统和证件领用系统都可以通过订阅消息队列频道的方式获得报备反馈信息。后续即可开始报备状态更新，证件催缴等流程。



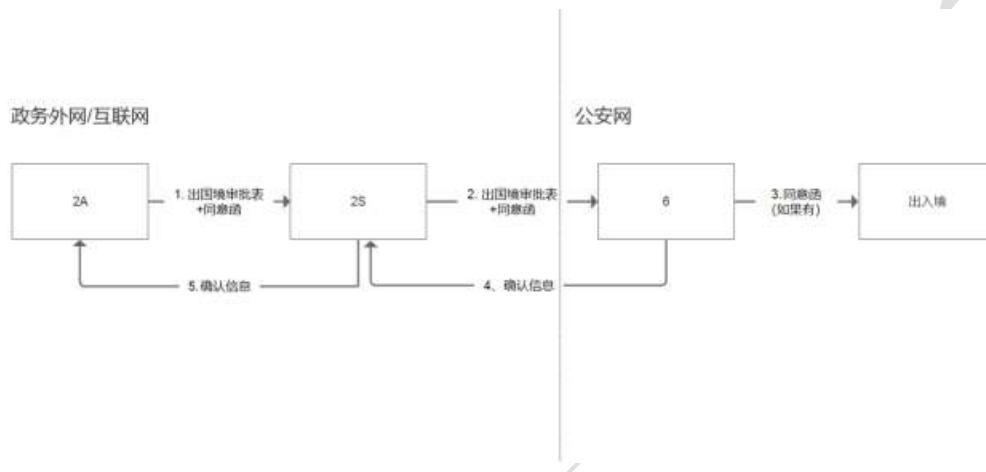
2. 登记备案查询服务

报备用户终端管理系统通过 http 接口（或订阅机制）发送登记备案查询服务请求到达本系统，再通过网闸交互数据到综合信息管理系统进行登记备案查询业务，异步结果通过网闸交互数据返回本系统，发布到消息队列中，报备用户终端管理系统通过订阅方式接收查询结果。



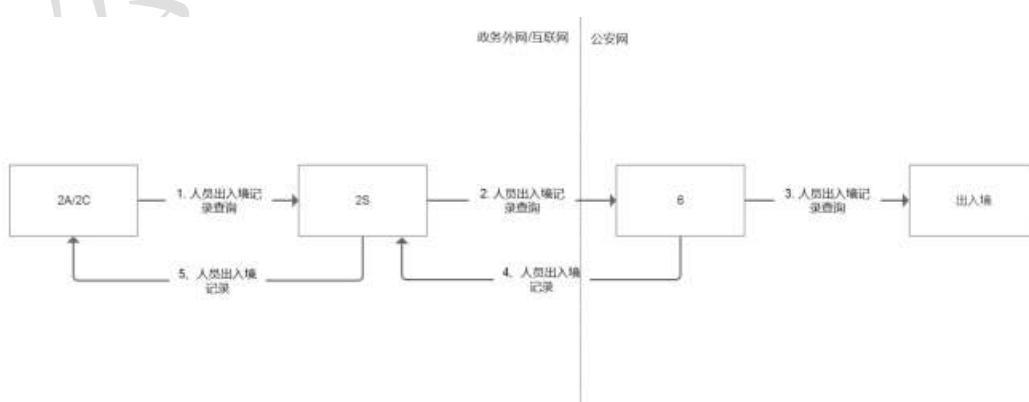
3. 同意函相关事件转发

证件领用系统通过 http 接口发送同意函相关事件请求到本系统，再通过网闸交互传递给综合信息管理系统，根据业务需要发送给出入境系统。综合信息管理系统生成的返回结果通过网闸交互传递到本系统，发布到消息队列中，证件领用系统通过订阅方式获得返回结果。



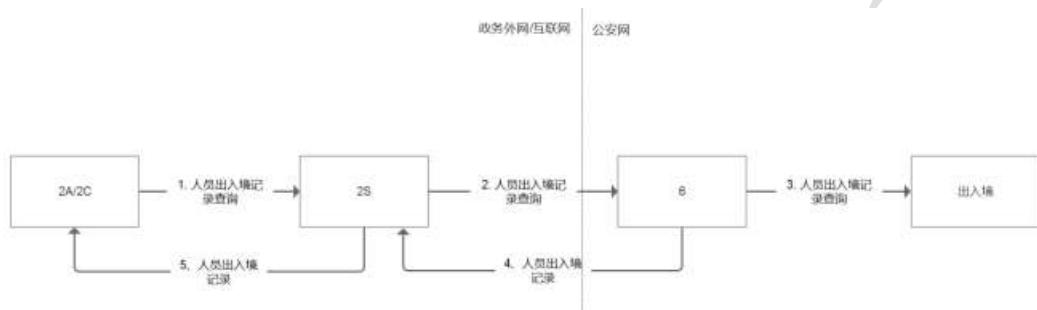
4. 出入境记录查询转发

管理单位（证件领用系统、报备用户终端管理系统）发起人员出入境记录查询业务时，将相关查询请求通过 http 接口发送到本系统，本系统通过网闸交互传递给综合信息管理系统调用出入境接口进行查询，结果通过网闸交互传递给本系统，再通过消息队列反馈给查询单位。



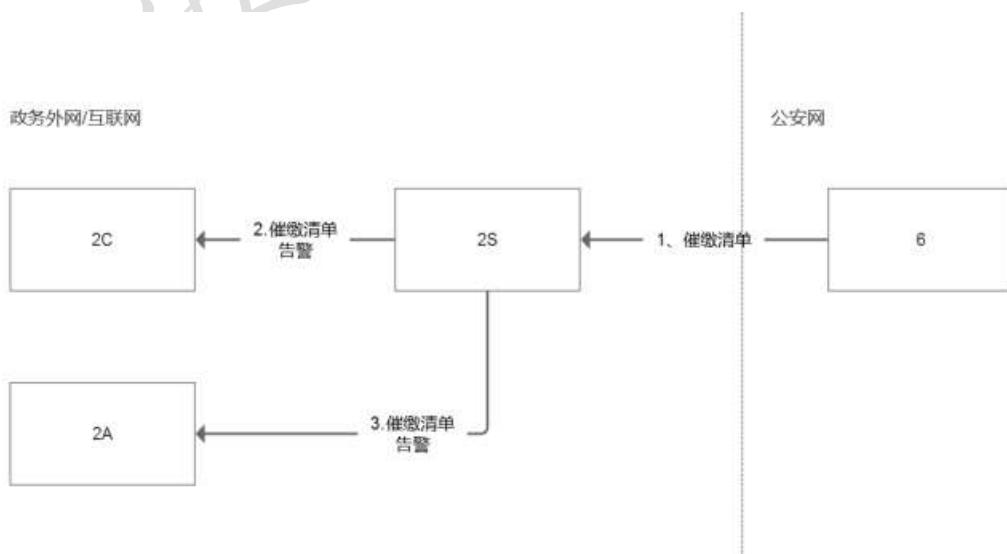
5. 出国（境）审批表转发

管理单位（证件领用系统、报备用户终端管理系统）发起人员出入境记录查询业务时，将相关查询请求通过 http 接口发送到本系统，本系统通过网闸交互传递给综合信息管理系统调用出入境接口进行查询，结果通过网闸交互传递给本系统，再通过消息队列反馈给查询单位。



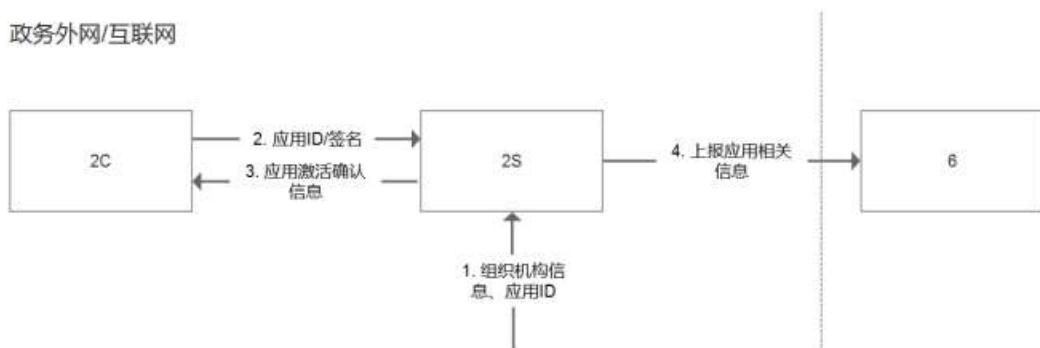
6. 消息、告警下发

综合信息管理系统生成证件催缴信息、异常告警信息之后，通过网闸数据交互传递给本系统，登记备案用户端和证件领用终端通过订阅方式获取消息和告警信息，同时本系统通过短信方式通知证件领用系统和报备用户终端管理系统管理员进行处理。



7. 报备客户端接入许可

报备用户终端管理系统初次启动，调用 http 接口发送系统注册请求到本系统，本系统对请求中的组织机构代码、应用 id 和数据签名校验请求来源是否合法，立即 http 响应校验结果。并通过网闸交互方式上报合法客户端信息给综合信息管理系统。



2.2.3.3.5 接口设计

(1) 应用接入许可（激活）接口（2A,2C）

请求数据 (body)

```
{
    "appid": "平台签发的绑定 UKEY 的应用 ID",
    "sign": "签名",
}
```

响应数据 (body)

```
{
    "desc": "错误描述",
    "code": "响应码"
}
```

(2) 管理员注册接口 (2A,2C)

[疑问：本地管理还是 2S 验证用户登录]

请求数据 (body)

```
{  
    "xm" : "",  
    "gmsfhm" : "",  
    "sj" : "",  
    "yzm" : "",  
}
```

响应数据 (body)

```
{  
    "desc" : "错误描述",  
    "code" : "响应码"  
}
```

(3) 验证码发送接口 (2A,2C)

请求数据 (body)

```
{  
    "sj" : "手机号码"  
}
```

响应数据 (body)

```
{  
    "desc" : "错误描述",
```

```
        "code" : "响应码"  
    }  
}
```

(4) 应用版本检查接口 (2A,2C)

请求数据 (GET 请求)

无

响应数据 (body)

```
{  
    "version" : "1.6.2" ,  
    "desc" : "错误描述" ,  
    "code" : "响应码"  
}
```

(5) 应用版本更新接口 (2A,2C)

请求数据 (GET)

无

响应数据 (body)

文件流

(6) 报备单位组织机构提交接口 (2C)

请求数据 (body)

```
{  
    "appid" : "" ,  
    "bbdwzzjgdm" : "报备单位组织机构代码" ,
```

```
        "zzjgdm": "下属组织机构代码",
        "zzjgmc": "下属组织机构名称",
    }
```

响应数据 (body)

```
{
    "desc": "错误描述",
    "code": "响应码"
}
```

(7) 登记备案信息提交接口 (2C)

请求数据 (body)

```
{
    "appid": """",
    "bbywlsh": "报备业务流水号",
    "bbspbwj": "BASE64(报备文件审批表)",
    "wjszqm": "文件数字签名",
    "xzbb": "[{
        "xm": """",
        "gmsfhm": """",
        "zzjgdm": "组织机构代码",
        "sj": "手机号码",
        "spdwwzzjgdm": "审批单位组织机构代码",
        "zw": ""
    }]
}
```

```
        } ] ,  
        cxbb : [ {  
            "xm" : " " ,  
            "gmsfhm" : " " ,  
            "zzjgdm" : "组织机构代码" ,  
            "sj" : "手机号码" ,  
            "spdzzjgdm" : "审批单位组织机构代码" ,  
            "zw" : "职务" ,  
        } ]  
    }  
}
```

响应数据 (body)

```
{  
    "desc" : "错误描述" ,  
    "code" : "响应码"  
}
```

(8) 登记备案结果及人员持证状态消息订阅 (2A,2C)

响应数据 (body)

```
{  
    "bbywlsh" : "报备业务流水号" ,  
    "bbjg" : [ {  
        "ryid" : "人员 ID" ,  
        "bbzt" : "报备状态" ,  
    }
```

```
        "zjlb": [{"  
            "zjlx": "证件类型",  
            "zjhm": "证件号码",  
        }]  
    },  
    "code": "响应码",  
    "desc": ""  
}
```

(9) 人员出入境异常及证件状态异常消息订阅 (2A, 2C)

响应数据 (body)

```
{  
    "yc": [{"  
        "yclx": "异常类型",  
        "ryid": "人员 ID",  
        "zjid": "证件 ID",  
        "ycessm": "异常信息说明"  
    }]  
}
```

(10) 证件催缴信息订阅 (2A, 2C)

响应数据 (body)

```
{  
    "cj": [{"  
        "cjid": "催缴 ID",  
        "zjid": "证件 ID",  
        "ycessm": "异常信息说明",  
        "cjsj": "催缴时间",  
        "cjsm": "催缴说明",  
        "cjsl": "催缴状态",  
        "cjsr": "催缴人"  
    }]  
}
```

```
        "ryid" :"" ,  
        "zjlx" :"证件类型" ,  
        "zjhm" :"证件号码(脱敏)" ,  
        "yqts" :"逾期天数"  
    }]  
}
```

(11) 出国(境)审批表提交接口 (2A)

请求数据 (body)

```
{  
    "cgspywlsh" :"出国(境)审批业务流水号" ,  
    "xm" :"" ,  
    "gmsfhm" :"" ,  
    "sj" :"手机号码" ,  
    "zzjgdm" :"组织机构代码" ,  
    "mdd" :"目的地" ,  
    "cfsj" :"出发时间" ,  
    "fhsj" :"返回时间" ,  
    "cgsy" :"出国事由" ,  
    "zjlx" :"证件类型" ,  
    "zjhm" :"证件号码可为空" ,  
    "spbwj" :"BASE64(审批表扫描件 pdf) "
```

}

响应数据（body）

{

“code”：“响应码”，

“desc”：“””

}

（12）同意函提交接口（2A）

请求数据（body）

{

“cgspywlsh”：“出国（境）审批业务流水号”，

“tyhywlsh”：“同意函业务流水号”，

“crjyw1x”：“出入境业务类型-新办证件、签注、换发”

“tyhwj”：“BASE64(同意函扫描件 pdf) ”

}

响应数据（body）

{

“code”：“响应码”，

“desc”：“””

}

（13）出国境审批及同意函结果订阅

{

“yw1sh”：“出国（境）审批业务流水号”，

```
        "jg": "结果"  
    }  
}
```

(14) 证件存取事件接口 (2A)

请求数据 (body)

```
{  
    "ywls": "证件存取业务流水号",  
    "zzjgdm": "组织机构代码",  
    "zjhm": "证件号码",  
    "cqsj": "存取事件"  
}
```

响应数据 (body)

```
{  
    "code": "响应码",  
    "desc": ""  
}
```

(15) 证件注销接口 (2A)

请求数据 (body)

```
{  
    "ywls": "证件注销业务流水号",  
    "zzjgdm": "组织机构代码",  
    "zjid": "证件 id",  
}
```

```
        "zxhzwj": "注销回执 PDF 文件"
    }
```

响应数据 (body)

```
{
    "code": "响应码",
    "desc": ""
}
```

2.3 数据汇聚分发系统

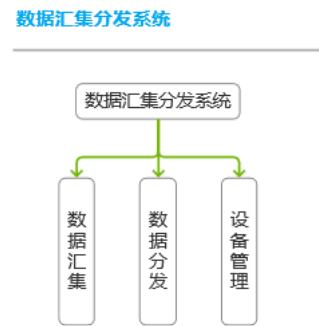
2.3.1 概述

数据汇聚分发系统是“国家工作人员因私出国（境）管理平台”前端系统（证件保管柜，证件保管柜管理系统，报备审批系统）之间及与跨网传输系统建立安全的数据通道。系统包括：通信协议、安全机制、密钥体系、签名验证服务器设备接口。

2.3.2 功能描述

- ◆ 与设备建立安全通信通道，使用数字信封传输敏感信息与跨网传输系统建立安全数据通道。
- ◆ 接收设备的存入、取出数据与证件存取信息，将数据透明转发到跨网传输系统。

2.3.3 功能架构



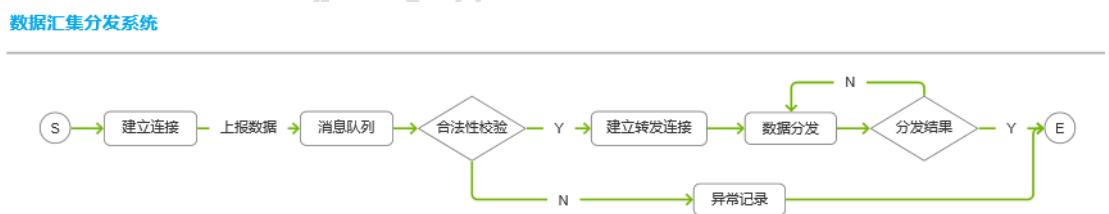
图表 2.3-1 数据汇聚分发系统功能架构图

2.3.4 功能设计

功能描述:

数据汇聚系统负责的是数据接收和转发的操作，对接收的数据需先进行数据来源有效性校验（与系统已开通的设备进行校验），校验通过后进入消息队列，通过分发规则进行数据分发操作，并反馈反复结果。

功能流程:



图表 2.3-2 数据汇聚流程图

消息队列：性能要求？部署？

功能分发规则:

序号	数据来源	数据类型	接收系统	安全	数据项
----	------	------	------	----	-----

1	证件保管柜	业务类数据 (证件信息, 人员信息, 证件存取等)	综合信息管理系统	签名/验签	证件信息, 人员信息, 报备信息, 机柜信息
2	证件保管柜	机柜类数据 (机柜信息, 抽屉状态)	证件保管柜管理系统	加密/解密	机柜信息, 抽屉状态, 抽屉运行日志, 操作日志, 异常信息
3	报备用户终端系统				

2.3.5 数据表设计

2.3.6 接口设计

序号	接口名称	数据源	目的系统	接口类型	消息协议	安全模式	数据实体
1	ReportPutZZ	证件保管柜	数据汇聚分发系统	Restful	JSON		{ DeviceID//String 设备序列号 ZZGSN //String 证件保管柜序列号 Row //int 抽屉行 Column //int 抽屉列 PassportData//BASE64 编码数字信封加密证件信息 }
2	ReportDropZ	证件保	数据汇聚分	Restful	JSON		{

	Z	管柜	发系统				DeviceID//String 设备序列号 ZZGSN //String 证件保管柜序列号 Row //int 抽屉行 Column //int 抽屉列 DropData //BASE64 编码数字信封加密信息 }
--	---	----	-----	--	--	--	---

2.4 证件保管柜管理系统

2.4.1 概述

证件保管柜管理系统主要实现证件保管柜的管理和运行维护功能。系统采用 C/S 结构。

2.4.2 功能描述

- 证件保管柜接入报备：系统对新增证件保管柜的单位信息（社会信用统一代码，单位名称，工作联系人，工作联系方式）在证件保管柜管理系统进行接入报备，新证件保管柜接入系统后，获取报备列表进行系统注册，并将注册信息反馈给证件保管柜管理系统。

-
- 版本管理：由于我们现在处于开发阶段，存在频繁发布设备版本的情况。当项目稳定后，会采取设备管理的方式来发布新版本；
 - 性能监控：主要是对服务器 CPU、内存及服务的监控，并通过阈值进行告警，并将报警记录进行周期性存档；
 - 故障管理：对证件保管柜的运行状态,抽屉使用情况，进行监控，对异常、故障等情况进行设备运维安排。主要来源有 3 部分，一为性能监控的报警记录来源、二是人工作业维护计划的问题发现，或者来自内部反馈或者用户反馈，一可以自动记录，二可以手工填报，然后进行汇总，并以图形或者报表的形式直观化反映出故障的来源及状况。

2.4.3 功能架构



图表 2.4-1 证件保管柜管理系统功能架构图

2.4.4 功能设计

2.4.4.1 设备管理

2.4.4.1.1 功能描述：

负责系统证件保管柜的接入开通和管理，主要包括新证件保管柜初始化、设备管理、版本管理。

A、设备信息：

证件保管柜管理系统-设备信息：设备名称、设备序列号、设备型号、容量规格、单位名称、位置、创建时间、状态和操作（详情和修改）。

The screenshot displays two pages of a management system:

Top Page (设备信息):

- Left Sidebar:** Includes categories like Equipment Management, Equipment Allocation, Unit Management, and various levels of storage.
- Header:** Shows navigation paths (一级菜单 / 二级菜单 / 三级菜单) and user information (momo, 登录).
- Content:** A table listing equipment details:

设备名称	设备序列号	设备型号	容量规格	单位名称	位置	创建时间	状态	操作
证件保管柜	XJH-Q2555061	XJ-123-100	1.0.3	电子技术有限公司	浙江杭州西湖区	2020-03-06	已启用	详情 编辑
证件保管柜	XJH-Q2555071	XJ-123-100	1.0.3	易信科技有限公司	浙江杭州西湖区	2020-03-06	已启用	详情 编辑
证件保管柜	XJH-Q2555081	XJ-123-100	1.0.3	易信科技有限公司	浙江杭州西湖区	2020-03-06	已启用	详情 编辑
证件保管柜	XJH-Q2555091	XJ-123-100	1.0.3	易信科技有限公司	浙江杭州西湖区	2020-03-06	已启用	详情 编辑
证件保管柜	XJH-Q2555101	XJ-123-100	1.0.3	易信科技有限公司	浙江杭州西湖区	2020-03-06	已启用	详情 编辑
- Bottom Page (设备信息详情页):**

This page provides a detailed view of a specific equipment item:

- Left Sidebar:** Same as the top page.
- Content:** Displays the following sections:
 - 设备基础信息:** Includes device name (证件保管柜), serial number (XJH-Q2555061), model (XJ-123-100), size (200mm*100mm*50mm), creation time (2020-03-06 11:00:00), and status (已使用).
 - 单位信息:** Shows unit name (电子技术有限公司), address (浙江杭州西湖区万塘路18号), and remarks (无).
 - 质保信息:** Shows guarantee unit (杭州安泰集团有限公司), contact person (李四), phone (18812345678), guarantee period (三年), and end date (2022-06-06).



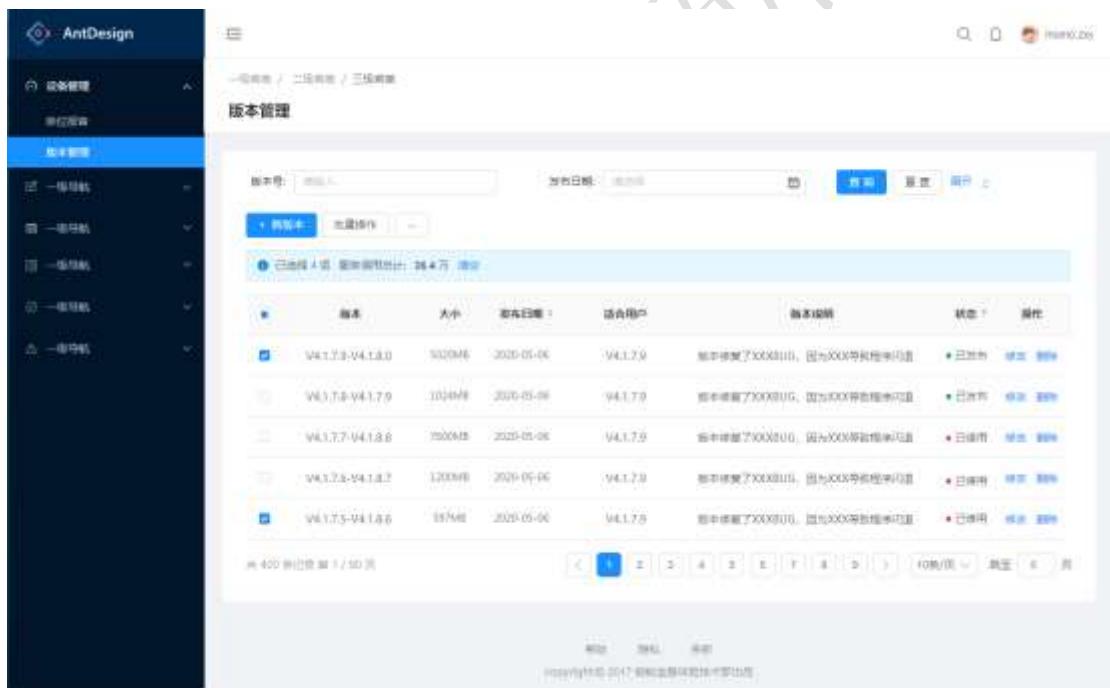
B、单位报备:

证件保管柜管理系统-报备单位: 社会统一信用代码, 单位名称, 工作联系人, 联系方式, 维保单位, 维保联系人, 维保联系方式、状态和操作（修改、删除）。

社会统一信用代码	单位名称	单位联系人	联系方式	维保单位	维保联系人	联系方式	状态	操作
3302295421231232	杭州盈创电子技术有限公司	张三	13433333333	杭州维保公司	王二	13433333333	●未开通	修改 删除
332312324563433	杭州盈创技术有限公司	李四	13333333333	杭州维保公司	王二	13333333333	●已开通	修改 删除
345345345453454	杭州盈创技术有限公司	王五	18888888888	杭州维保公司	王二	18888888888	●已开通	修改 删除
3370707575675425	杭州盈创技术有限公司	赵六	18888888888	杭州维保公司	王二	18888888888	●已开通	修改 删除
33090978980756	杭州盈创技术有限公司	二哥	13333333333	杭州维保公司	王二	13333333333	●已开通	修改 删除



C、版本管理：客户端版本管理及升级服务。

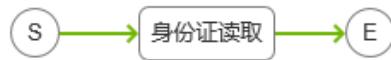




2.4.4.1.2 功能流程

证件保管柜初始化流程：

证件保管柜初始化流程



图表 2.4-2 证件保管柜初始化流程图

数据表结构

2.4.4.2 运行维护

2.4.4.2.1 功能描述:

A、数据采集

数据采集模块主要负责接收和处理证件保管柜所上发的各类数据，包括监控数据，异常数据，故障数据等，全实时数据上报保存。系统保存所有上报数据，告警信息后加快上报规则。

1、注册信息、心跳、

2、监控信息（柜子开启，关闭，异常数据）

	监控项	判断标准	正常	异常	处理
硬件	网络				
	电源				
	温度				
	湿度				
	机柜开门				
	接口				
	硬盘存储空间				
	CPU 负载				
	内存使用				
	运行时间				
	心跳				
	版本				

B、设备监控

设备监控：查看系统中各个设备的运行状态，包括 IP 地址、系统版本、温度、识读、磁盘、内存、CPU、心态状态、抽屉使用状况和设备操作记录等。

The screenshot shows the 'Device Monitoring' page. On the left is a dark sidebar with a navigation tree: '设备管理' (Equipment Management) -> '设备监控' (Equipment Monitoring). The main content area has a title '设备监控' (Equipment Monitoring). It includes a search bar for '设备序列号' (Equipment Serial Number), '单位' (Unit), and '操作员' (Operator). Below the search is a button labeled '已选择 4 条' (4 selected) and a blue '搜索' (Search) button. A table lists four equipment items with columns: '设备名称' (Equipment Name), '设备序列号' (Equipment Serial Number), and '操作员' (Operator). The table rows are: 1. 证件保管组 XJH2251851 电子技术有限公司; 2. 证件保管组 XJH2251851 高新技术有限公司; 3. 证件保管组 XJH2251851 高新技术有限公司; 4. 证件保管组 XJH2251851 信息产业有限公司. To the right of the table is a '设备监控场景图' (Equipment Monitoring Scenario Chart) showing a line graph of temperature and humidity over time. Below the chart is a table for '设备操作记录' (Equipment Operation Record) with columns: '操作员' (Operator), '操作类型' (Operation Type), '内容' (Content), '操作员' (Operator), and '操作时间' (Operation Time). The table shows one record: '王海涛' (Wang Haotao) performed an '增加' (Add) operation on '证件保管组' (Document Management Group) at 2020-01-06 15:45:01.

C、告警查看

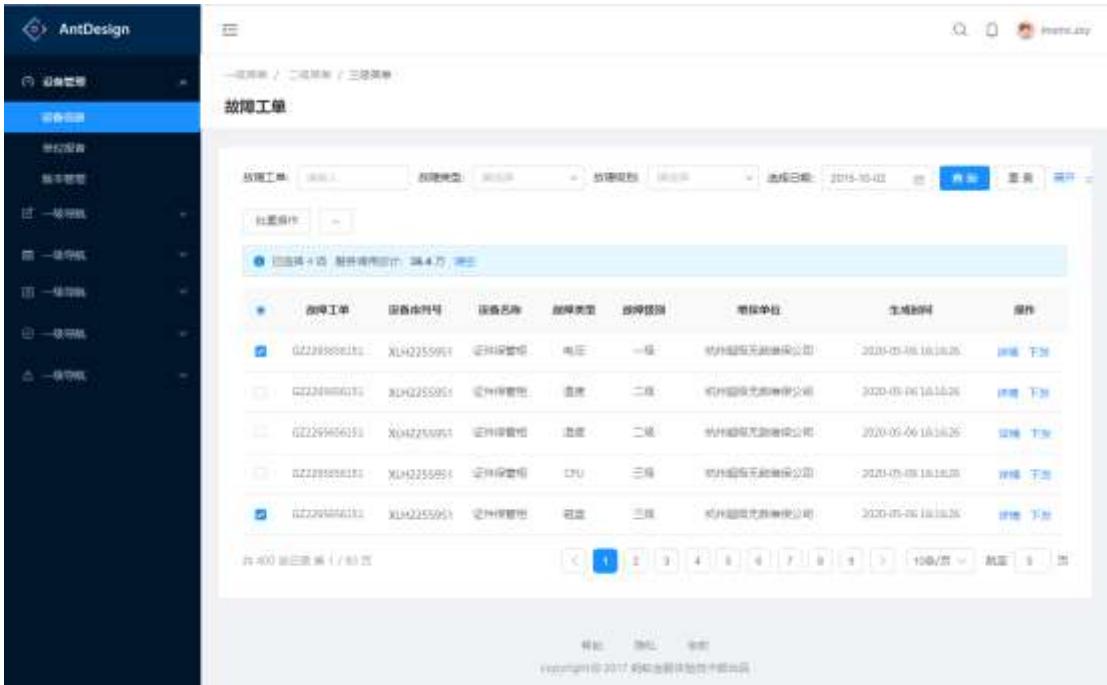
告警查看：查看系统接收到的告警记录，包括设备信息、告警类型、告警内容、上报时间等，可以点击查看详情生产故障工单。

The screenshot shows the 'Alert View' page. The left sidebar is identical to the previous page. The main content area has a title '告警查看' (Alert View). It includes a search bar for '设备序列号' (Equipment Serial Number), '告警类型' (Alarm Type), and '选择日期' (Select Date). Below the search is a blue '搜索' (Search) button. A table lists five alarm records with columns: '告警名称' (Alarm Name), '告警序列号' (Alarm Serial Number), '设备型号' (Equipment Model), '告警类型' (Alarm Type), '告警内容' (Alarm Content), '上报时间' (Report Time), and '操作' (Operation). The table rows are: 1. 证件保管组 XJH2251851 0-225-100 电压 电源电压过低, 目前CPU正常 2020-01-04 14:56:34 [详情] [生成故障工单]; 2. 证件保管组 XJH2251851 0-225-100 温度 环境温度过高, 经过阈值上限(30°C) 2020-01-06 14:18:26 [详情] [生成故障工单]; 3. 证件保管组 XJH2251851 0-225-100 湿度 相对湿度过大, 超过阈值上限(90%) 2020-01-06 14:24:28 [详情] [生成故障工单]; 4. 证件保管组 XJH2251851 0-225-100 CPU 电源CPU负载过高, 正常(0%) 2020-01-06 14:25:36 [详情] [生成故障工单]; 5. 证件保管组 XJH2251851 0-225-100 电源 电源设备温度异常, 且温度上升 2020-01-06 14:28:21 [详情] [生成故障工单]. At the bottom are buttons for '跳转' (Jump), '排序' (Sort), and '重置' (Reset).

D、故障工单

故障工单：通过告警信息系统自动生成或者从告警查看中选择告警记录选择生产故障工单，并落实故障处理，并对故障问题的处理进

行后续跟踪。



E、维保管理

维保管理：对设备维保信息，维保单位进行管理和配置。

2.4.4.2.2 功能流程

数据采集流程

证件保管柜初始化流程



图表 2.4-3 证件保管柜数据采集流程图

故障维护流程

故障维护流程



图表 2.4-3 运行维护流程图

版本管理流程

证件保管柜管理系统-设备管理-版本管理

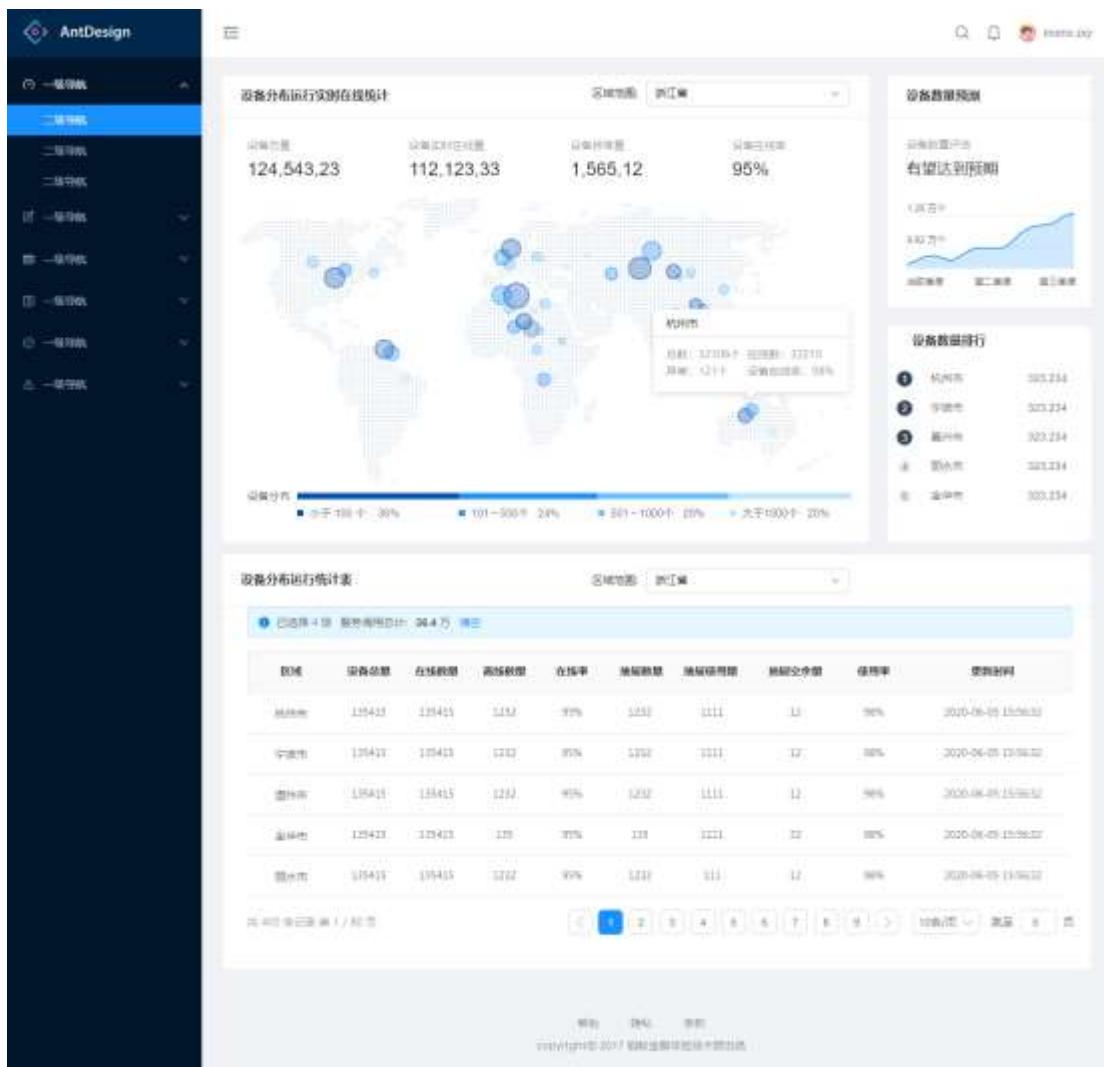


图表 2.4 -5 版本管理流程图

2.4.4.3 统计分析

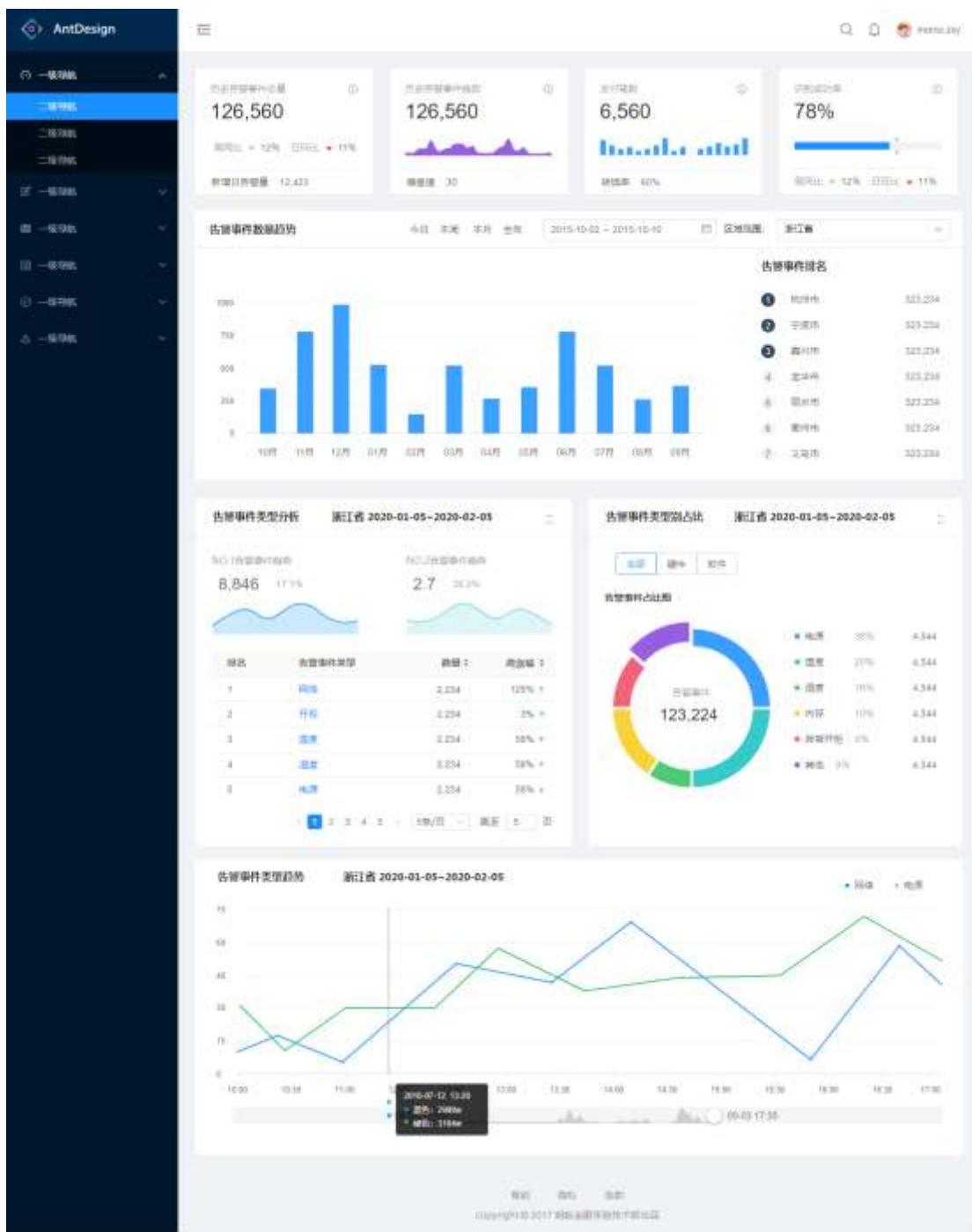
2.4.4.3.1 功能描述

A、设备统计：系统设备总量，抽屉总量，分布情况等信息的统计，用户可以选择不同的区域进行查询。



B、运维统计：系统故障信息，运维工单，运维周期等信息的统计。

C、告警统计：统计分析上报的所有告警事件，按地区、时间等维度生产相应的统计分析图标。



2.4.4.3.2 功能流程

2.4.4.4 系统管理

2.4.4.4.1 功能描述

A、用户管理：系统平台操作用户的分配及管理。

The screenshot shows the 'User Management' page of a system. On the left is a dark sidebar with a tree menu for '设备管理' (Equipment Management) and '权限管理' (Permission Management). The '权限管理' node is currently selected. The main area has a title '用户管理' and a search bar. Below is a table with the following data:

用户名	角色	创建时间	更新时间	状态	操作
admin	超级管理员	2020-05-01 12:33:15	2020-05-01 12:33:15	已启用	修改 登录日志 锁定
admin1	管理员	2020-05-01 12:33:15	2020-05-01 12:33:15	已启用	修改 登录日志 锁定
admin2	管理员	2020-05-01 12:33:15	2020-05-01 12:33:15	已启用	修改 登录日志 锁定
admin3	普通用户	2020-05-01 12:33:15	2020-05-01 12:33:15	已启用	修改 登录日志 锁定
admin4	普通用户	2020-05-01 12:33:15	2020-05-01 12:33:15	已启用	修改 登录日志 锁定

At the bottom are buttons for '添加新用户' (Add New User), a search bar, and a footer with copyright information.

B、权限管理：系统用户权限的分配及管理。

The screenshot shows the 'Permission Management' page. The sidebar has the same structure as the previous screen. The main area displays a tree view of permissions categorized by role:

- 超级管理员 (Super Admin):
 - 设备管理 (Equipment Management):
 - 采集管理 (Collection Management): 读取、写入、修改
 - 单位设备 (Unit Equipment): 读取、修改
 - 故障管理 (Fault Management): 读取、修改
 - 统计分析 (Statistical Analysis):
 - 设备统计 (Equipment Statistics): 读取、写入
 - 故障统计 (Fault Statistics): 读取
- 管理员 (Administrator):
 - 设备管理 (Equipment Management):
 - 采集管理 (Collection Management): 读取、写入、修改
 - 单位设备 (Unit Equipment): 读取、修改
 - 故障管理 (Fault Management): 读取、修改
- 普通用户 (Normal User):
 - 设备管理 (Equipment Management):
 - 采集管理 (Collection Management): 读取、写入
 - 单位设备 (Unit Equipment): 读取

C、参数配置：系统运行的基本参数的管理，如设备心跳间隔。



D、系统日志：系统运行日志的查看及管理。



E、数据备份：系统数据的备份管理。

备份机制：1、系统每日定时自动备份一次数据库到本地。

2、系统每周定时



2.4.4.4.2 功能流程

2.4.5 数据表设计

2.4.5.1 数据库表结构设计

名称	表明	备注
m_sbxx_t	设备表	
m_zjbgg_t	证件保管柜表	
m_zjbggct_t	证件保管柜抽屉表	
d_sbxh_t	设备型号表	
m_bbdw_t	报备单位表	
d_qgdqdm_t	全国地区代码表	
m_wbdw_t	维保单位信息表	
m_bbgl_t	版本管理表	
m_sjcj_t	数据采集表	

m_sjsb_t	事件上报表	
m_gjsj_t	告警事件表	
m_sbxt_t	设备心跳表	
m_sjbf_t	数据备份表	

1、设备表 m_sbxx_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
sbxlh	设备序列号	varchar(64)				
sbmc	设备名称	varchar(64)				
sbxh	设备型号	varchar(64)				
cjsj	创建时间	datetime				
gxsj	更新时间	datetime				
dwID	单位 ID	int(11)				
wbdwID	维保单位 ID	int(11)				
sbzt	设备状态	int(2)				0: 启用; 1: 禁用

2、证件保管柜表 m_zjbgg_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
zjbggxlh	证件保管柜序列号	varchar(64)				
zjbggxh	证件保管柜型号	varchar(64)				

cjsj	创建时间	datetime				
gxsj	更新时间	datetime				
cthsl	抽层数	int(11)				
ctls	抽屉列数	int(11)				
bz	备注	varchar(64)				
zjbggzt	证件保管柜状态	int(11)				0: 启用; 1: 禁用; 2: 异常
sbID	设备 ID	int(2)				

3、证件保管柜抽屉表 m_zjbggct_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
cthsl	抽层数	int(11)				
ctls	抽屉列数	int(11)				
zjbggID	证件保管柜 ID	int(11)				
ctzt	抽屉状态	int(2)				0: 正常; 1: 异常

4、设备型号表 d_sbkh_t

代码	名称	类型	非空	主键	规范	备注
sbkh	设备型号	varchar(64)	√	√		
sbgg	设备规格	varchar(64)				

5、报备单位表 m_bbdw_t

代码	名称	类型	非空	主键	规范	备注

ID	ID	int(11)	√	√		
tyshxydm	统一社会信用代码	varchar(64)				
dwmc	单位名称	varchar(64)				
ssqy	所属区域	varchar(6)				区域代码 110000
xxdz	详细地址	varchar(64)				
dwlxr	单位联系人	varchar(64)				
gmsfhm	公民身份号码	varchar(64)				
lxfs	联系方式	varchar(64)				
cjsj	创建时间	datetime				
gsj	更新时间	datetime				
dwzt	单位状态	int(2)				0: 注册; 1 未注册
jmk	加密卡	varchar(64)				
sbID	设备 ID	int(11)				

6、全国地区代码字典表 d_qgdqdm_t

代码	名称	类型	非空	主键	规范	备注
qydm	区域代码	varchar(6)				
qymc	区域名称	varchar(32)				

7、维保单位信息表 m_wbdw_t

代码	名称	类型	非空	主键	规范	备注

ID	ID	int(11)	√	√		
wbdwmc	维保单位名称	varchar(64)				
wbdwdz	维保单位地址	varchar(64)				
wbdwlxr	维保单位联系人	varchar(6)				
lxfs	联系方式	varchar(64)				

8、版本管理表 m_bbgl_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
bbmc	版本名称	varchar(64)				
bbdx	版本大小	varchar(64)				
fbrq	发布日期	date				
shyh	适合用户	varchar(64)				
bbsm	版本说明	varchar(64)				
bbzt	版本状态	int(2)				0: 已发布; 1 未发布
ccdz	存储地址	varchar(64)				

9、数据采集表 m_sjcj_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
czy	操作员	varchar(64)				

sbID	设备 ID	int(11)				
zjbggID	证件保管柜 ID	int(11)				
zjbggctID	证件保管柜 抽屉 ID	int(11)				
czlx	操作类型	int(2)				0: 出柜; 1: 入柜; 2: 注销
sjz	数据值	varchar(64)				操作的详细内容

10、事件上报表 m_sjsb_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
sbID	设备 ID	int(11)				
sj	时间	datetime				
sjlx	事件类型	varchar(64)				0: 告警; 1: 短信
sjnr	事件内容	varchar(64)				事件类型+事件明细（网络-网络波动）

11、设备心跳表 m_sbxt_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
sbID	设备 ID	int(11)				
IPdz	IP 地址	varchar(64)				
sj	时间	varchar(64)				0: 告警; 1:

						短信
sd	温度	varchar(64)				事件类型+事件 明细（网络-网 络波动）
wd	湿度	varchar(64)				
CPU	CPU	varchar(64)				
nc	内存	varchar(64)				
cp	磁盘	varchar(64)				

12、告警事件表 m_gjsj_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
sbID	设备 ID	int(11)				
gjlx	告警类型	varchar(64)				电压、温度、 湿度等等
gjnr	告警内容	varchar(64)				检测到断电， 目前 UPS 供电
sj	时间	datetime				
sfscgd	是否生成工 单	int(2)				0: 是; 1 否

13、数据备份表 m_sjbf_t

代码	名称	类型	非空	主键	规范	备注
ID	ID	int(11)	√	√		
sjbb	数据版本	varchar(64)				
sjzt	数据状态	int(2)				0: 已备份; 1: 未备份

bfsj	备份时间	date				
bflj	备份路径	varchar(64)				

2.4.6 接口设计

序号	接口名称	数据源	目的系统	接口类型	消息协议	安全模式	数据实体	传输方式
1	设备初始化接口	证件保管柜	证件保管柜管理系统	服务调用	Json		统一社会信用代码，设备序列号，单位名称，工作联系人，工作联系电话，管理员账号，保管柜加密卡 ID，管理员身份唯一 ID	
2	心跳接口	证件保管柜	证件保管柜管理系统	服务调用	Json		设备 ID，IP 地址，时间，版本，温度，湿度，cpu 占用，内存占用，磁盘占用，告警配置修改标志	
3	数据采集接口	证件保管柜	证件保管柜管理系统	服务调用	Json	签名/验签	设备 ID，抽屉 ID，操作员，数据类型，数据值	同步
4	数据同步接口	证件保管柜管理系统	证件保管柜	服务调用	Json	数据加密/解密	同步数据信息，时钟，保管柜告警阈值	
5	事件上报接口	证件保管柜	证件保管柜管理系统	服务调用	Json		告警，报备结果，短信验证	
6	版本下载接口	证件保管柜	证件保管柜管理系统	服务调用	FTP		新版本证件保管柜软件	

2.4.7 接口数据格式

(1) 服务地址定义

[http://\[host\]:\[port\]/xxx/\[ver\]/xxx](http://[host]:[port]/xxx/[ver]/xxx)

说明：

[host]： 认证服务 IP 或者域名；

[port]： 认证服务端口号；

[ver]： 认证服务 API 版本

(2) 服务协议规格

请求协议： http

请求方法： post

上传数据： body=json 字符串

内容类型： Content-Type = application/json, charset=utf-8

(3) 设备初始化接口业务数据格式

设备初始化数据（data）：

序号	字段	类型	字段名	必填	说明
1	tyshxydm	String	统一社会信用代码	是	
2	sbxlh	String	设备序列号	是	证件保管柜的唯一 ID
3	dwmc	String	单位名称	是	
			单位地址	否	
4	gzlxr	String	工作联系人	是	
5	gzlxdh	String	工作联系电话	是	
6	jmkid	String	加密卡 ID	是	
7	glylb	JSONArray	管理员列表	是	

8		glyzh		String	管理员账号	是	
9		rybs		int	人员标识	是	管理员的唯一 ID Hash(公民身份证号码 + 姓名)
10	zjbghzxx			JSONArray	证件保管柜汇总信息		
11		sbxlh		String	设备序列号	是	证件保管柜的唯一 ID
12		zjgxlh		String	证件柜序列号	是	
13		cth		String	抽屉行	是	
14		ctl		String	抽屉列	是	
15		cfzjs		String	存放证件数	是	
16		cfzjlb		JSONObject	存放证件列表	是	
17			rybs	int	人员标识	是	人员的唯一 ID Hash(公民身份证号码 + 姓名)
18			rybbzt	int	人员报备状态		1: 已报备, 2: 未报备,
19			hzcfzt	int	护照存放状态		1: 已存放, 2: 被领出, 3: 未办理

20			gatxzcftz	int	港澳通信证存放状态		1: 已存放, 2: 被领出, 3: 未办理
21			dljmwlwt xzcfzt	int	大陆居民往来 台湾通行证存放状态		1: 已存放, 2: 被领出, 3: 未办理

业务数据报文示例:

```
{
    "tyshxydm":"",
    "sbxlh":"",
    "dwmc":"",
    "gzlxr":"",
    "gzlxdh ":""
    "jmkid":"",
    "glylb": [
        {
            "glyzh":"",
            "rybs":""
        }
    ],
    "zjbghhzxx": [
        {
            "sbxlh":"",
            "zjgxlh":"",
            "cth":"",
            "ctl":"",
            "cfzjs":"",
            "cfzjlb": {

```

```

    "rybs":"",
    "rybbzt":"",
    "hzcfzt":"",
    "gatxzcfzt":"",
    "dljmwlwtxzcfzt":""
}
}
]
{
...
}

```

设备初始化响应数据（data）

序号	字段	类型	字段名	必填	说明
	fkjg	String	反馈结果	是	
	nrms	String	内容描述	是	

示例

```
{
    "fkjg":"",
    "nrms":""
}
```

(4) 心跳接口业务数据格式

心跳接口业务数据（data）：

序号	字段	类型	字段名	必填	说明
1	sbxlh	String	设备序列号	是	证件保管柜的唯一 ID
2	sbipdz	String	设备 IP 地址	是	

3	czsj	String	操作时间	是	时间戳
4	sbbb	String	设备版本	是	
5	sbwd	String	设备温度	是	
6	sbsd	String	设备湿度	是	
7	clqzy	String	处理器占用	是	
8	nczy	String	内存占用	是	
9	cpzy	String	磁盘占用	是	

业务数据报文示例：

```
{
    "sbxlh ":"",
    "sbipdz ":"",
    "czsj":"",
    "sbbb ":""
    "sbwd ":""
    "sbsd ":""
    "clqzy ?>"
    "nczy"
    "cpzy "
}
```

心跳接口响应数据 (data)

序号	字段	类型	字段名	必填	说明
1	fkjg	String	反馈结果	是	
2	szjzxx	String	时钟校准信息	是	

3	ksjbbh	String	可升级版本号	是	
4	gjpzgbz	int	告警配置更新标志	是	
5	zfsjbz	int	转发数据标志	是	2 通过 4 发往 1

示例

```
{
    "fkjg":"",
    "szjzx ":"",
    "ksjbbh":"",
    "gjpzgbz":""
}
```

(5) 数据采集接口业务数据格式

数据采集接口数据（data）：

序号	字段	类型	字段名	必填	说明
1	sbxlh	String	设备序列号	是	证件保管柜的唯一 ID
2	zjgxlh	String	证件柜序列号	是	
3	cth	String	抽屉行	是	
4	ctl	String	抽屉列	是	
5	czsj	String	操作时间	是	时间戳
6	czyzh	String	操作员账号	是	
7	czlx	String	操作类型	是	1: 出柜, 2: 入柜, 3: 注销, 4: 撤销

8	zjlx	String	证件类型	是	
9	ctzt	String	抽屉状态	是	当前抽屉存证状态

业务数据报文示例:

```
{
    "sbxlh":"",
    "zjgxlh":"",
    "cth":"",
    "ctl":"",
    "czsj":"",
    "sjsbsj":"",
    "czyzh":"",
    "czlx":"",
    "zjlx":"",
    "ctzt":""
}
```

数据采集接口响应数据 (data)

序号	字段	类型	字段名	必填	说明
	fkjg	String	反馈结果	是	
	nrms	String	内容描述	是	

示例

```
{
    "fkjg":"",
    "nrms"
}
```

```
"nrms":""  
}
```

(6) 数据同步接口业务数据格式

数据同步接口数据（data）：

序号	字段	类型	字段名	必填	说明
1	sbxlh	String	设备序列号	是	证件保管柜的唯一 ID
2	czsj	String	操作时间	是	时间戳
3	czlx	String	操作类型	是	1: 告警配置更新, 2: 版本更新, 3 柜状态更新(开机同步一次、之后 24 小时同步一次)4: 数据转发

业务数据报文示例：

```
{  
    "sbxlh ":"",  
    "czsj ":""  
    "czlx ":""  
}
```

数据同步接口响应数据（data）

序号	字段	类型	字段名	必填	说明
	fkjg	String	反馈结果	是	
	czlx	String	操作类型	是	1: 告警配置更新, 2: 版本

					更新, 3 柜状态更新(开机同步一次、之后 24 小时同步一次), 4: 数据转发
	czsj	String	操作数据	是	1: 告警配置更新, 2: 版本更新配置信息, 3 柜状态更新(开机同步一次、之后 24 小时同步一次), 4: 数据转发内容

示例

```
{
    "fkjg":"",
    "czlx":"",
    "czsj ":""
}
```

(7) 事件上报接口业务数据格式

事件上报接口数据 (data) :

序号	字段		类型	字段名	必填	说明
1	sbxlh		String	设备序列号	是	证件保管柜的唯一 ID
2	czsj		String	操作时间	是	时间戳
3	czlx		String	操作类型	是	事件类型 (1:

						告警, 2: 报备 结果 3: 短信 验证)
4	czsj		String	操作数据	是	时间类型+事 件明细

业务数据报文示例:

```
{
    "sbxlh ":"",
    "czsj ":""
    "czlx ":""
    "czsj ":""
}
```

事件上报接口响应数据 (data)

序号	字段	类型	字段名	必填	说明
1	fkjg	String	反馈结果	是	
2	czsj	String	操作数据	是	事件(1: 告警 反馈, 2: 报备 结果反馈 3: 短信验证码 反馈)

示例

```
{
    "fkjg":"",
    "czsj ":""
}
```

2.5 跨网传输系统

2.5.1 概述

跨网传输系统构建互联网到公安网的安全传输通道，负责将证件保管柜、报备审批系统、证件保管柜管理系统生成的人员报备和证件存取记录汇集到公安网存储，并提供数据的完整性和来源验证。

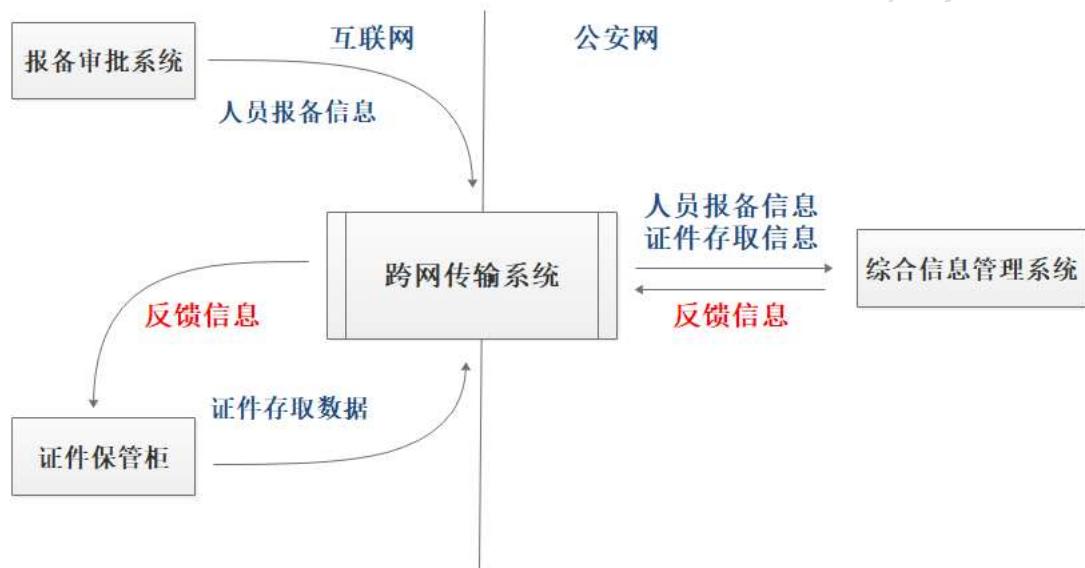


图 2.5-1 跨网传输系统架构图

2.5.2 总体设计

2.5.2.1 设计原则

- ◆ 采用基于 HTTP 协议的 Restful 服务接口，接口调用者和跨网传输服务器交互在请求之间无状态通信
- ◆ 系统设计以高并发、高可靠性为设计目标
- ◆ 系统支持水平传输能力扩展
- ◆ 实时报告系统运行状态、告警通知
- ◆ 基于成熟系统标准化业务组件设计

2.5.2.2 系统性能指标设计

并发指标：1000 次/秒服务调用请求数次

时间指标：1000 次/秒并发情况下，单次请求不大于 1 秒

2.5.3 功能架构

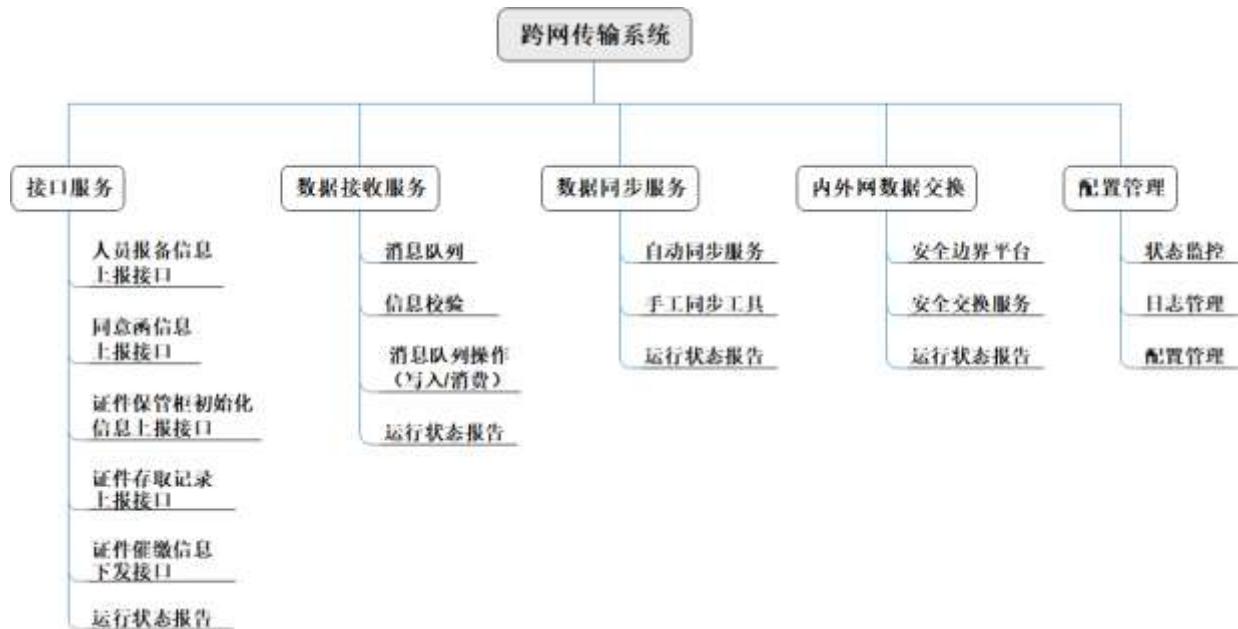


图 2.5-2 跨网传输系统功能架构图

跨网传输系统由接口服务、数据接收服务、数据同步服务、内外网数据交换服务和配置管理 5 部分组成。

接口服务：提供 HTTP 协议 Restful 风格 API 接口供外部系统调用。

数据接收服务：数据接收服务快速将每个接口服务采集的跨网上传数据进行验签和有效性校验，异步写入消息队列。

数据同步服务：提供自动同步服务和手动同步工具，将从消息队列中消费日志信息，触发安全交换系统的数据交换服务，实现数据在公安网内的持久化存储和流转。

内外网数据交换：完成 Http Restful 接口请求数据从互联网向公

安网的单向传输。

配置管理：系统配置参数、日志信息的管理和各子模块运行状态的展现。

2.5.4 功能设计

2.5.4.1 接口服务

提供 HTTP 协议 Restful 风格 API 接口，提供外部系统（汇聚分发系统）的调用，根据不同的接口异步并发写入消息队列。

跨网传输系统主要包含人员报备信息上报、同意函上报、证件保管柜初始化信息上报和证件保管柜存取记录上报 4 个上报接口，一个反馈信息下发接口，各接口的主要设计方式如下：

编号	接口名称	源系统	目的系统	接口类型	消息协议	传输协议	安全模式	数据实体	传输方式
1	人员报备信息上报接口	报备受理系统->数据汇聚分发系统	跨网传输系统	服务调用	JSON	http	签名/验签	报备人员信息（含单位信息）	同步
2	同意函上报接口	报备受理系统->数据汇聚分发系统	跨网传输系统	服务调用	JSON	http	签名/验签	电子版同意函+签名信息（出入境验签）	同步
3	证件保管柜初始化信息上报接口	证件保管柜管理系统	跨网传输系统	服务调用	JSON	http	签名/验签	柜信息和单位信息	同步
4	证件保管柜存取记录上报接口	护照保管柜->数据汇聚分发系统	跨网传输系统	服务调用	JSON	http	签名/验签	柜存储证件信息、柜内容信息	同步
5	反馈信息下发接口	数据汇聚分发系统	跨网传输系统	服务调用	JSON	http	签名/验签	一体化信息管理系统回推数据	同步

2.5.4.2 数据接收服务

数据接收服务快速将每个接口服务采集的跨网上传数据进行验签和有效性校验，异步写入消息队列。

数据接收服务流程图如下所示：

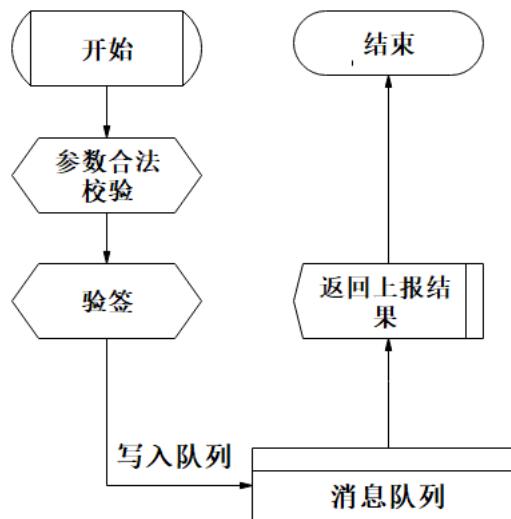


图 2.5-3 数据接收服务流程图

(1) 消息队列

日志消息队列采用 RocketMQ 进行设计。RocketMQ 是开源的分布式消息中间件，具有标准的程序接口和协议，具有高性能、高可靠、高实时、分布式特点，Producer、Consumer、队列都可以分布式，Producer 向一些队列轮流发送消息，队列集合称为 Topic，Consumer 如果做广播消费，则一个 consumer 实例消费这个 Topic 对应的所有队列，如果做集群消费，则多个 Consumer 实例平均消费这个 topic 对应的队列集合，能够保证严格的消息顺序，提供丰富的消息拉取模式，高效的订阅者水平扩展能力，实时的消息订阅机制，亿级消息堆积能力，依赖很少。

◆ NameServer

NameServer 的作用是注册中心，类似于 Zookeeper，但又有区别于它的地方。每个 NameServer 节点互相之间是独立的，没有任何信

息交互，也就不存在任何的选主或者主从切换之类的问题，因此 NameServer 与 Zookeeper 相比更轻量级。单个 NameServer 节点中存储了活跃的 Broker 列表（包括 master 和 slave），这里活跃的定义是与 NameServer 保持有心跳。

单个 Consumer 和一台 Nameserver 保持长连接，定时查询 topic 配置信息，如果该 Nameserver 挂掉，消费者会自动连接下一个 Nameserver，直到有可用连接为止，并能自动重连。与 Nameserver 之间没有心跳。

单个 Consumer 和与其关联的所有 broker 保持长连接，并维持心跳，失去心跳后，则关闭连接，并向该消费者分组的所有消费者发出通知，分组内消费者重新分配队列继续消费。

◆ Broker

Broker 是具体提供业务的服务器，单个 Broker 节点与所有的 NameServer 节点保持长连接及心跳，并会定时将 Topic 信息注册到 NameServer，顺带一提底层的通信和连接都是基于 Netty 实现的。

Broker 中分 master 和 slave 两种角色，每个 master 可以对应多个 slave，但一个 slave 只能对应一个 master，master 和 slave 通过指定相同的 Brokername，不同的 BrokerId（master 为 0）成为一个组。master 和 slave 之间的同步方式分为同步双写和异步复制，异步复制方式 master 和 slave 之间虽然会存在少量的延迟，但性能较同步双写方式要高出 10% 左右。

◆ Producer

单个 Producer 和一台 nameserver 保持长连接，定时查询 topic 配置信息，如果该 nameserver 挂掉，生产者会自动连接下一个 nameserver，直到有可用连接为止，并能自动重连。与 nameserver 之间没有心跳。

单个 Producer 和与其关联的所有 broker 保持长连接，并维持心

跳。默认情况下消息发送采用轮询方式，会均匀发到对应 Topic 的所有 queue 中。

(2) 参数合法性校验

对服务接口传入的参数信息进行合法性校验，校验未通过进入统一异常处理模块处理并返回，校验通过后进行下一步操作。

(3) 验签

和用户方确定统一的签名/验签规范，通过调用密钥管理系统的签名验证服务，对服务调用方传入的参数信息进行验签，确保接口调用的合法性和参数完整性。验签未通过进入统一异常处理模块处理并返回，验签通过后进行下一步操作。

(4) 写入消息队列

根据不同的接口获取不同的队列，将信息异步写入消息队列，写入异常时进入统一异常处理模块处理并返回，写入正常则返回正确返回。

(5) 服务运行状态报告

对监控服务提供线程池使用情况，连接池使用情况，队列使用情况，根据资源使用情况，以便于运维监控作出应用风险预警。

2.5.4.3 数据同步服务

数据同步服务包含自动同步服务和手动同步工具，将从消息队列中消费日志信息，触发安全交换系统的数据交换服务，实现数据在公安网内的持久化存储和流转，同步流程如下：

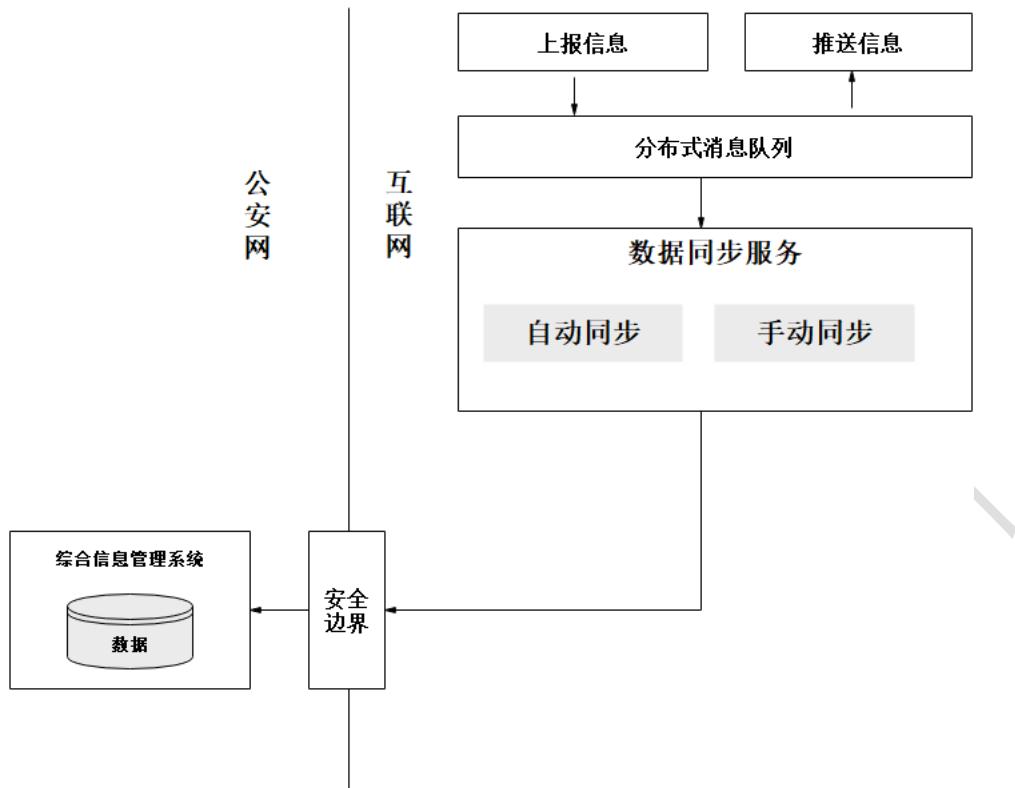


图 2.5-4 数据同步服务流程图

自动同步服务：自动同步服务对存储在消息队列中的上报数据进行消费，通过调用数据交换系统跨网调用综合信息服务系统提供的各类服务接口，实现数据的汇集，并将消息队列中成功消费的信息删除。

手动同步工具：手动同步工具提供导入和导出功能，可以根据配置信息将消息队列中未经消费的数据迁移到公安网内，并输出数据对账报告，作为安全交换系统故障时的应急响应方式。

2.5.4.4 内外网数据交换

建设互联网到公安信息网的数据交换系统，建立安全传输通道，完成国家工作人员单位应用过程的报备、审批信息和证件存取记录从互联网到公安网的汇集。既可规避互联网安全威胁对公安信息网的影响，又可以完成公安信息网与互联网信息资源的融合，实现国家工作人员出国（境）一体化管理。

安全交换系统由互联网到公安网的安全边界平台和安全交换服

务两部分组成。

(1) 安全边界平台

按照《公安信息通信网边界接入平台安全规范—公网信息采集部分》(2013年11月)设计和建设安全边界平台，实现互联网到公安网的单向数据传输，主要包括：路由接入区、边界保护区、应用服务区和安全隔离区等四个部分及单向导出隔离域，构架如图所示：

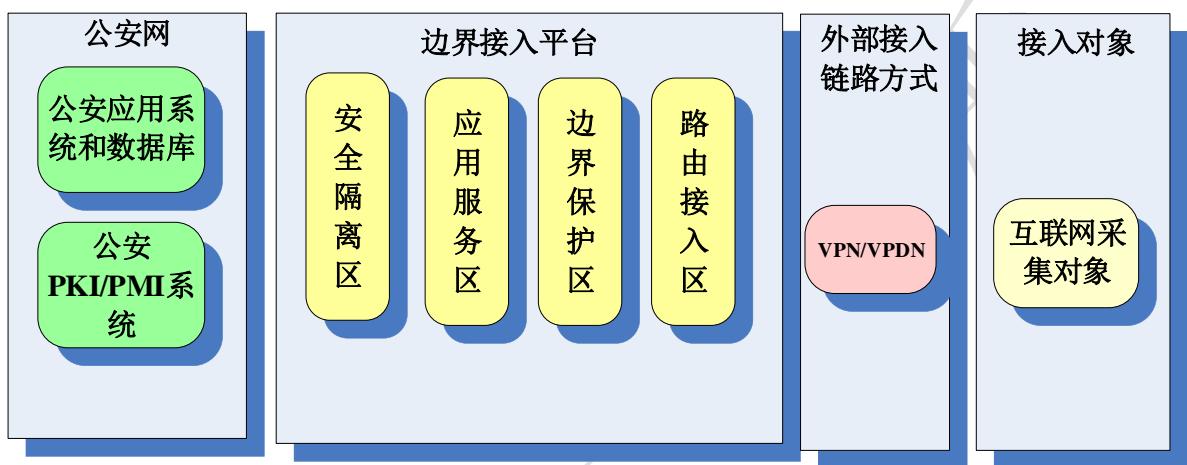


图 2.5-5 安全边界平台架构图

◆ 路由接入区

该区域实现各个外部链接与接入平台之间的连接。

该区域主要安全功能为：实现路由访问控制，将来自不同接入对象或不同外部链路的数据流按照接入平台的安全策略加以区分。

◆ 边界保护区

该区域主要实现对接入平台的边界保护。

该区域主要安全功能为：实现身份认证、访问控制和权限管理，数据机密性和完整性保护，防御网络攻击和嗅探。通过综合审计技术实现对数据行为追溯和分析。

◆ 应用服务区

该区域主要处理各类与应用相关的操作，是公安网对外信息发布、

信息采集和数据交换的中间区域。

该区域主要安全功能为：作为外部终端网络连接的终点，实现应用级身份认证、访问控制、应用代理、数据暂存等功能。防止对公安网的非法访问和信息泄露。对此区域，应加强对服务器等设备的安全保护，应具有病毒、木马保护功能，防止病毒传播和非法控制。

◆ 安全隔离区

该区域实现公安网与应用服务区的安全隔离和信息交换。

该区域主要安全功能为：实现公安网与应用服务区的安全网络隔离，根据安全策略，对出入内网的数据分别进行协议剥离、格式检查和过滤，实现公安网和应用服务区之间的安全数据交换，保障内网的安全。

◆ 安全监测与管理区

该区域实现整个接入平台的安全监测、管理与维护。

该区域主要安全功能为：对接入平台运行情况进行安全监测与审计；对接入平台及业务信息进行注册管理，各种安全策略管理，流量监测，统计分析，安全审计等；接入平台内网络设备、安全设备的配置管理及日常运行维护；补丁升级，漏洞扫描与病毒防范。

（2）安全交换服务

通过部署请求服务系统，将 SOAP、XML-RPC 和 RESTful 请求或应答转为 XML 文件，同时实现对基于 SOAP 协议请求数据进行安全格式检查和请求数据与 XML 文件之间的转换，实现数据落地传输，满足业务和安全性需求。

请求服务业务流程

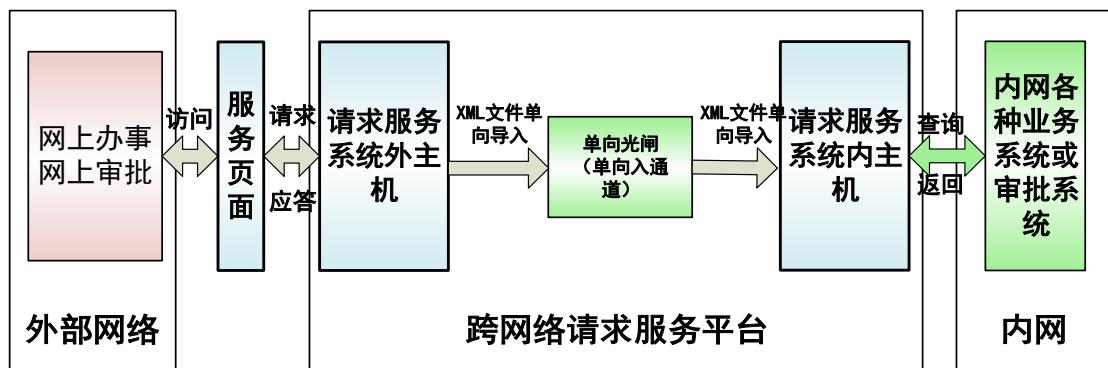


图 2.5-6 请求服务流程图

外部用户先向请求服务系统外主机发起服务请求，外主机将服务请求转换为 XML 文件，通过单向入通道单向导入到内网的请求服务系统内主机，而内主机将 XML 文件转换为服务请求，访问内网各种业务系统或者数据库系统获取返回结果，然后通过文件转换、单向导出，将结果传递给外部用户。

2.5.4.5 配置管理

状态监控：配合监控系统，可实时监控跨网传输系统各业务模块的运行状态，发现异常实时预警。

配置管理：提供参数配置界面，可以查看跨网传输系统可变更参数，支持参数的修改和保存，修改后可以生效。

日志管理：同步日志数据的查看、查询、导出和删除。

2.5.5 接口设计

2.5.5.1 人员报备信息上报接口

和综合信息系统接口服务保持一致

2.5.5.2 同意函上报接口

和综合信息系统接口服务保持一致

2.5.5.3 证件保管柜初始化信息上报接口

和综合信息系统接口服务保持一致

2.5.5.4 对账数据上报接口

数据上报-对账数据

http://[host]:[port]/yth_g1xt/api/[ver]/sjsb-dzsj

【说明】 功能：接收数据汇聚分发系统上报的对账数据包，完成数据验签和跨网传输。

[host]：服务 IP 或者域名

[port]：服务端口号

[ver]：服务 API 版本 v1

【请求协议】

【请求方法】

【内容类型】 Content-Type: application/json, charset=utf-8

◆ 请求数据

◆ 响应数据

2.5.5.5 证件保管柜存取记录上报接口

数据上报-证件存取

http://[host]:[port]/yth_g1xt/api/[ver]/sjsb-zjcq

【说明】 功能：接收数据汇聚分发系统上报的数据包，完成数据验签和跨网传输。

[host]：服务 IP 或者域名

[port]：服务端口号

[ver]： 服务 API 版本 v1

【请求协议】

【请求方法】

【内容类 Content-Type: application/json, charset=utf-8 型】

◆ 请求数据

字段	类型	必填	说明
version	String	是	协议版本
mstype	String	是	业务数据消息类型
c	JSONObject	是	控制信息
coding	String	是	数据编码，如 b64
reqid	String	是	请求 id(抗重放)

	time	String	是	请求时间戳(抗重放)
	sid	String	是	会话 id(抗 Dos)
	ai	String	是	安全机制
	ki	String	是	应用密钥索引
	ei	String	是	安全模块 id
s		JSONObject	是	加密信息
	env	String	否	数字信封 (含接收者证书 id) 或会话密钥
	sig	String	否	原始签名或 mac (含公钥和算法)
	rsig	String	否	转发签名或 mac (含公钥标识和算法)
bdata		JSONObject		请求业务数据 (明文或加密)
	ywlsh	String	是	上报数据业务流水号
	sbttime	String	是	数据上报时间
	zjdata	String	否	上报证件信息，BASE64 编码数字信封加密证件信息。证件信息包含证件类型、证件号码、身份证证号、中文姓名、英文姓名、出生日期、性别、有效期限至 8 个字段，每个字段定长，不足部分用'\0'填充
	optype	String	是	操作证件柜类型: 11 存入； 12 归还 21 借出； 22 取出
	optime	String	是	操作证件柜时间

retdate	String	否	归还日期, optype 为 21 和 22 时该字段生效
Deviceid	String	是	设备序列号
ZZGSN	String	是	证件柜序列号
Row	int	是	抽屉行
Column	int	是	抽屉列

示例：

```
{  
    "code": "",  
    "desc": "",  
    "field": "",  
    "version": "",  
    "mstype" : "",  
    "c": {  
        "coding": "b64",  
        "reqid": "",  
        "ai": "",  
        "ki": "",  
        "ei": ""  
    },  
    "s": {  
        "env": ""},
```

```
"sig": "",  
"rsig": ""  
},  
"bdata": {  
    "ylsh": "",  
    "sbtme": "",  
    "zjdata": "",  
    "optype": "",  
    "optime": "",  
    "retdate": "",  
    "Deviceid": "",  
    "ZZGSN": "",  
    "Row": "",  
    "Column": ""  
}  
}
```

◆ 响应数据

字段	类型	必填	说明
ylsh	String	是	业务编号
status	Boolean	是	服务状态, true 表示访问请求处理无异常, false 表示业务处

		理中出现问题
error_code	String	接口正常错误码为 0, 接口调用不正常时根 据错误内容返回不同 错误码（开发过程中 定义详细的错误代码 表）。
error_msg	String	接口调用正常错误描 述为空字符串，接口 调用不正常时根据不 同错误返回不同错误 描述。（开发过程中定 义详细的错误描述）。
	否	
	否	

示例：

```
{
  "status":true,
  "error_code":"",
  "error_msg":""
}
```

2.5.5.6 人员报备结果反馈接口

数据反馈-报备结果反馈

[http://\[host\]:\[port\]/yth_g1xt/api/\[ver\]/sjfk-bbjg](http://[host]:[port]/yth_g1xt/api/[ver]/sjfk-bbjg)

【说明】 功能：接收报备审批系统的请求，向接收报备审批系

统反馈综合信息管理系统人员报备处理结果。

[host]: 服务 IP 或者域名

[port]: 服务端口号

[ver]: 服务 API 版本 v1

【请求协议】

【请求方法】

【内容类型】 Content-Type: application/json, charset=utf-8

◆ 请求数据

字段	类型	必填	说明
version	String	是	固定值 “1”
mstype	String	是	业务数据消息类型
c	JSONObject	是	控制信息
coding	String	是	数据编码, 如 b64
reqid	String	是	请求 id(抗重放), 随机
time	String	是	请求时间戳(抗重放), 客户端时间戳
sid	String	是	会话 id(抗 Dos), 空
ai	String	是	固定值 “Sig” (数字签名机制)
ki	String	是	空

				安全模块 id, 报备管理系统客户端
ei	String	是		Ukey 设备号
s	JSONObject	是		加密信息
	env	String	否	空
	sig	String	否	原始签名
	rsig	String	否	空
bdata	JSONObject			请求业务数据（明文或加密）
	ryblsh	String	是	人员报备业务流水号

示例：

```
{
    "version": "1",
    "mstype" : "",
    "c": {
        "coding":"b64",
        "reqid":"",
        "ai":"Sig",
        "ki":"",
        "ei":"",
        },
    "s": {
        "env":"",
        "sig":"",
        "rsig":""
        },
    "bdata": {
        ywlsh:""
        }
}
```

◆ 响应数据

字段	类型	必填	说明
----	----	----	----

version	String	是	固定值 “1”
mstype	String	是	业务数据消息类型
c	JSONObject	是	控制信息
coding	String	是	数据编码, 如 b64
reqid	String	是	请求 id(抗重放), 随机
time	String	是	请求时间戳(抗重放), 客户端时间戳
sid	String	是	会话 id(抗 Dos), 空
ai	String	是	固定值 “Sig” (数字签名机制)
ki	String	是	空
ei	String	是	安全模块 id, 报备管理系统客户端 Ukey 设备号
s	JSONObject	是	加密信息
env	String	否	
sig	String	否	原始签名
rsig	String	否	
bdata	JSONObject		请求业务数据 (明文或加密)
status	Boolean	是	服务状态, true 表示访问请求处理无异常, false 表示业务处理中出现问题
error_code	String	否	接口正常错误码为 0, 接口调用不正常时根据错误内容返回不同错误码 (开发过程中定义详细的错误代码表)。
error_msg	String	否	接口调用正常错误描述为空字符串, 接口调用不正常时根据不同错误返回不同错误描述。(开发过程中定义详细的错误描述)。
bbtlsh	String	是	人员报备业务流水号

bbjg String 是 综合信息管理系统反馈的报备结果信息，使用安全模块 id 加密的数据

示例：

```
{  
    "version": "1",  
    "mstype" : "",  
    "c": {  
        "coding": "b64",  
        "reqid": "",  
        "ai": "Sig",  
        "ki": "",  
        "ei": ""  
    },  
    "s": {  
        "env": "",  
        "sig": "",  
        "rsig": ""  
    },  
    "bdata": {  
        "ywls": "",  
        "status": "",  
        "error_code": "",  
        "error_msg": "",  
        "bb1sh": "",  
        "bbjg": ""  
    }  
}
```

2.5.5.7 催缴信息反馈接口

数据反馈-催缴信息反馈

[http://\[host\]:\[port\]/yth_g1xt/api/\[ver\]/sjfk-cjxx](http://[host]:[port]/yth_g1xt/api/[ver]/sjfk-cjxx)

【说明 功能： 接收证件保管柜发送的请求，向护照保管柜

反馈综合信息管理系统碰撞发现的催缴信息。

[host]：服务 IP 或者域名

[port]: 服务端口号

[ver]: 服务 API 版本 v1

【 请求 协议】

【 请求 方 POST
法】

【 内 容 类 Content-Type: application/json, charset=utf-8
型】

◆ 请求数据

字段	类型	必填	说明
version	String	是	固定值 “1”
mstype	String	是	业务数据消息类型
c	JSONObject	是	控制信息
coding	String	是	数据编码, 如 b64
reqid	String	是	请求 id(抗重放), 随机
time	String	是	请求时间戳(抗重放), 客户端时间戳
sid	String	是	会话 id(抗 Dos), 空
ai	String	是	固定值 “Sig” (数字签名机制)
ki	String	是	空
ei	String	是	安全模块 id, 报备管理系统客户端 Ukey 设备号

s		JSONObject	是	加密信息
	env	String	否	空
	sig	String	否	原始签名
	rsig	String	否	空
bdata		JSONObject		请求业务数据（明文或加密）
	orgid	String	是	统一社会信用代码
	devid	String	是	证件柜序列号

示例：

```
{
    "version": "1",
    "mstype" : "",
    "c": {
        "coding":"b64",
        "reqid":"",
        "ai":"Sig",
        "ki":"",
        "ei":""
    },
    "s": {
        "env":"",
        "sig":"",
        "rsig":""
    },
    "bdata": {
        "orgid":"",
        "odevid":""
    }
}
```

◆ 响应数据

字段		类型	必填	说明
version		String	是	固定值 “1”
mstype		String	是	业务数据消息类型

c		JSONObject	是	控制信息
	coding	String	是	数据编码, 如 b64
	reqid	String	是	请求 id(抗重放), 随机
	time	String	是	请求时间戳(抗重放), 客户端时间戳
	sid	String	是	会话 id(抗 Dos), 空
	ai	String	是	固定值 “Sig” (数字签名机制)
	ki	String	是	空
	ei	String	是	安全模块 id, 报备管理系统客户端 Ukey 设备号
s		JSONObject	是	加密信息
	env	String	否	
	sig	String	否	原始签名
	rsig	String	否	
bdata		JSONObject		请求业务数据 (明文或加密)
	status	Boolean	是	服务状态, true 表示访问请求处理无异常, false 表示业务处理中出现问题
	error_code	String	否	接口正常错误码为 0, 接口调用不正常时根据错误内容返回不同错误码 (开发过程中定义详细的错误代码表)。
	error_msg	String	否	接口调用正常错误描述为空字符串, 接口调用不正常时根据不同错误返回不同错误描述。(开发过程中定义详细的错误描述)。
	cjxx	String	是	综合信息管理系统反馈的催缴信息, 使用安全模块 id 加密的数据

示例:

{

```
"version": "1",
"mstype" : "",
"c": {
    "coding": "b64",
    "reqid": "",
    "ai": "Sig",
    "ki": "",
    "ei": ""
},
"s": {
    "env": "",
    "sig": "",
    "rsig": ""
},
"bdata": {
    "ywlsj": "",
    "status": "",
    "error_code": "",
    "error_msg": "",
    "cjxx": ""
}
}
```

2.6 综合信息管理系统

2.6.1 概述

面向各组织部门提供报备人员、相关证件的状态信息的汇聚服务和数据查询服务。

2.6.2 总体设计

2.6.2.1 设计原则

- ◆ 数据交换与数据查询的计算资源分离，有助于未来量化计算资源扩展方案
- ◆ 每个集群至少双机双活运行，确保单机故障服务有效
- ◆ 通过应用负载均衡完成压力分配

按部署架构，综合信息管理系统的分为如下集群服务：

- ◆ 数据交换服务集群：用于完成数据交换相关的操作，包括事件处理、响应、第三方接口查询。根据应用压力配置服务器计算资源，通过应用负载完成计算压力分配。
- ◆ 数据查询服务集群：用于向其他用户提供数据基础查询服务，包括人员情况，证件情况，事件记录等信息。根据应用压力配置服务器计算资源，通过应用负载完成计算压力分配。
- ◆ 数据库存储集群：用于储存人员信息、事件信息、回馈结果、交易记录等信息。采用高可用架构设计。
- ◆ 系统日志存储查询：用于存储采集的日志，采用业界典型的 ELK 解决方案
- ◆ 运维支撑服务系统：参考“运维系统”相关设计

2.6.2.2 系统运行环境

操作系统：CentOS 6.5

Java 环境：Java JDK 1.8

2.6.2.3 标准开发组件

Springboot 2.0 +SpringCloud

2.6.3 功能架构

综合信息管理系统主要包含数据交换、数据查询、外部数据服务接口集成，包含数据签名/验签，加密/解密，并发访问控制、数据和发行校验，数据交换任务池管理，报备、撤销、入柜出柜事件流程动态流转。

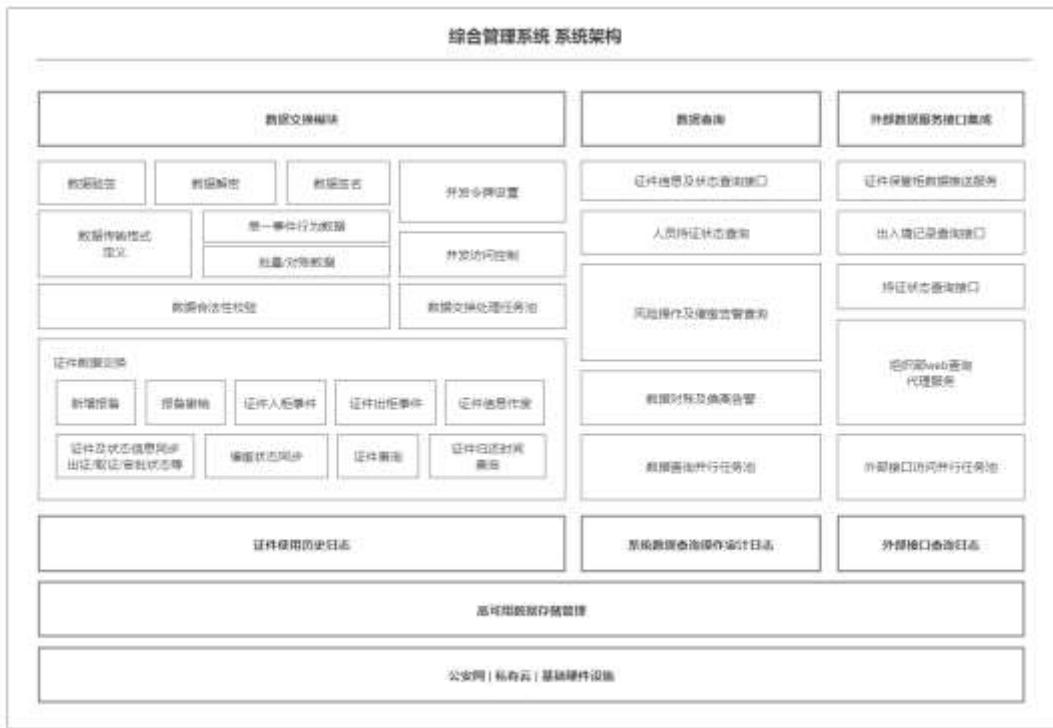


图 2-6-1 系统功能架构

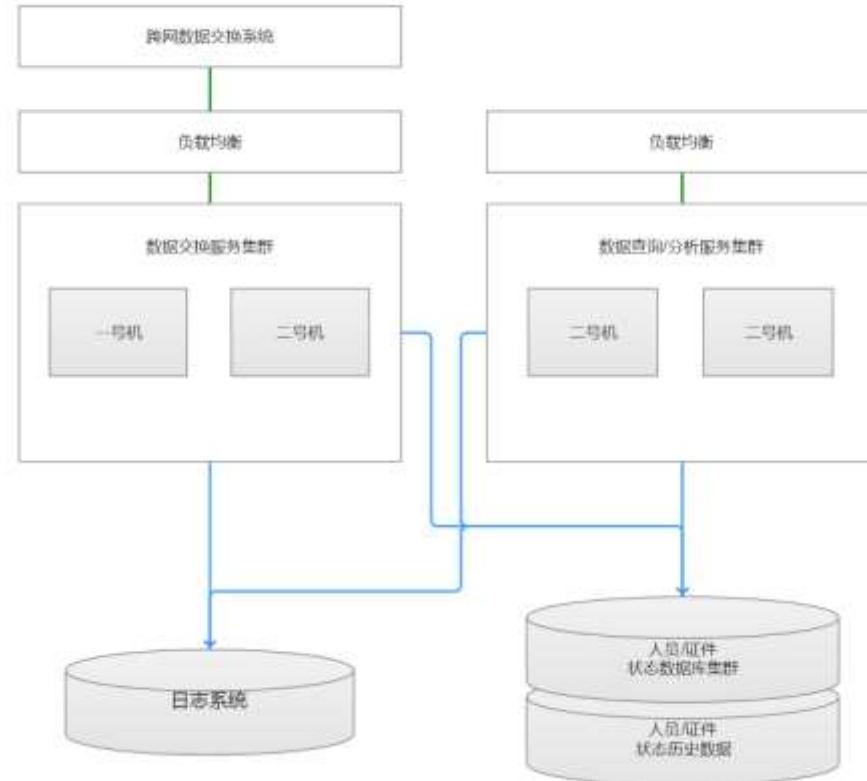


图 2-6-2 系统部署架构图

2.6.4 功能设计

2.6.4.1 数据交换子系统

2.6.4.1.1 功能模块

(1) 登记备案

登记备案模块接收上传的人员登记备案信息并保存到数据库中，然后访问出入境人员报备接口，并通过出入境证件查询功能模块查询报备人员是否已经持有出入境证件，更新对应人员的证件信息，同时进行反馈和证件催缴。

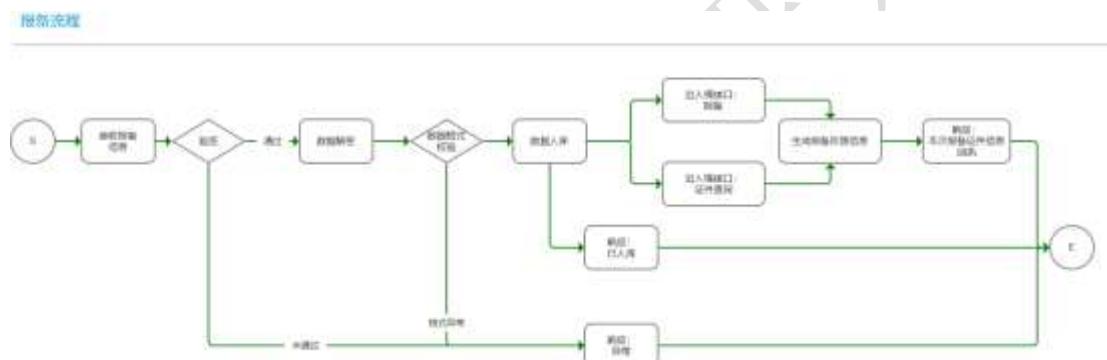


图 2-6-3 登记备案流程图

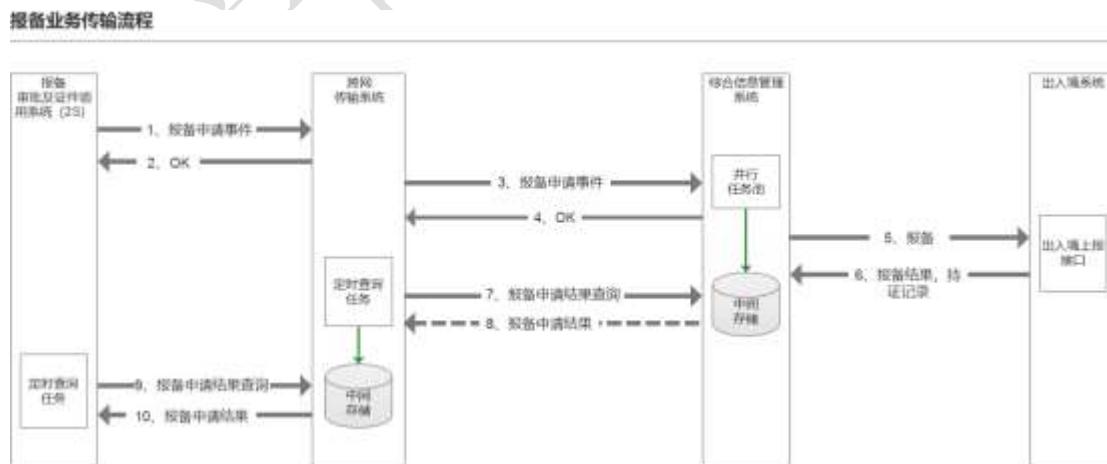


图 2-6-4 登记备案时序图

撤销报备和同单位报备信息变更时，上传的人员登记备案信息并保存到数据库中，然后访问出入境人员报备接口，返回报备结果。

同单位报备变更流程

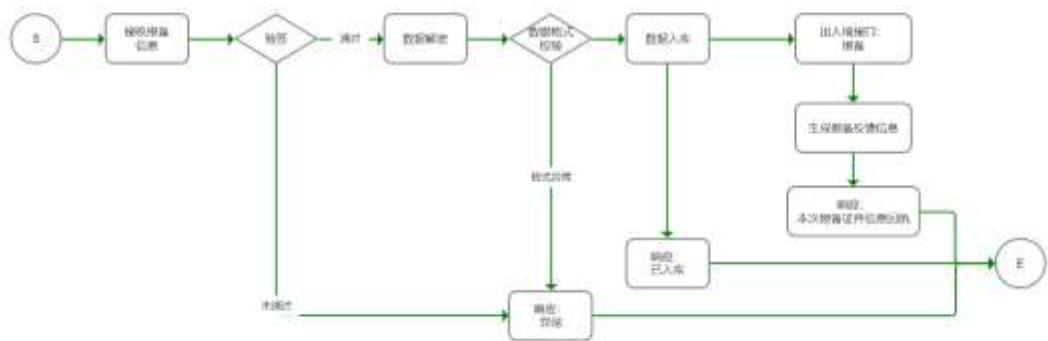


图 2-6-4 撤销备案和同单位变更备案流程图

(2) 同意函报备（办新证/换发/签注）

收到办新证申请/换发申请/签注申请同意函信息后，将同意函文件和信息入库，同时将信息提交给出入境接口。

同意函处理流程

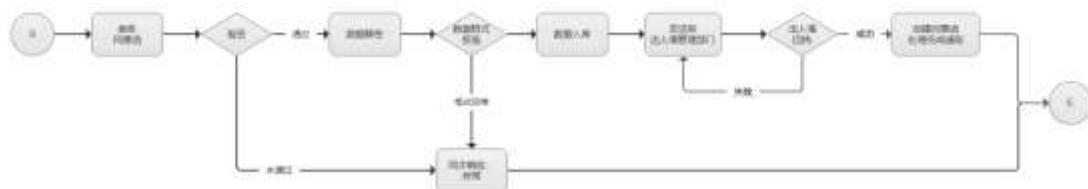


图 2-6-5 同意函处理流程

办证同意函报备传输流程

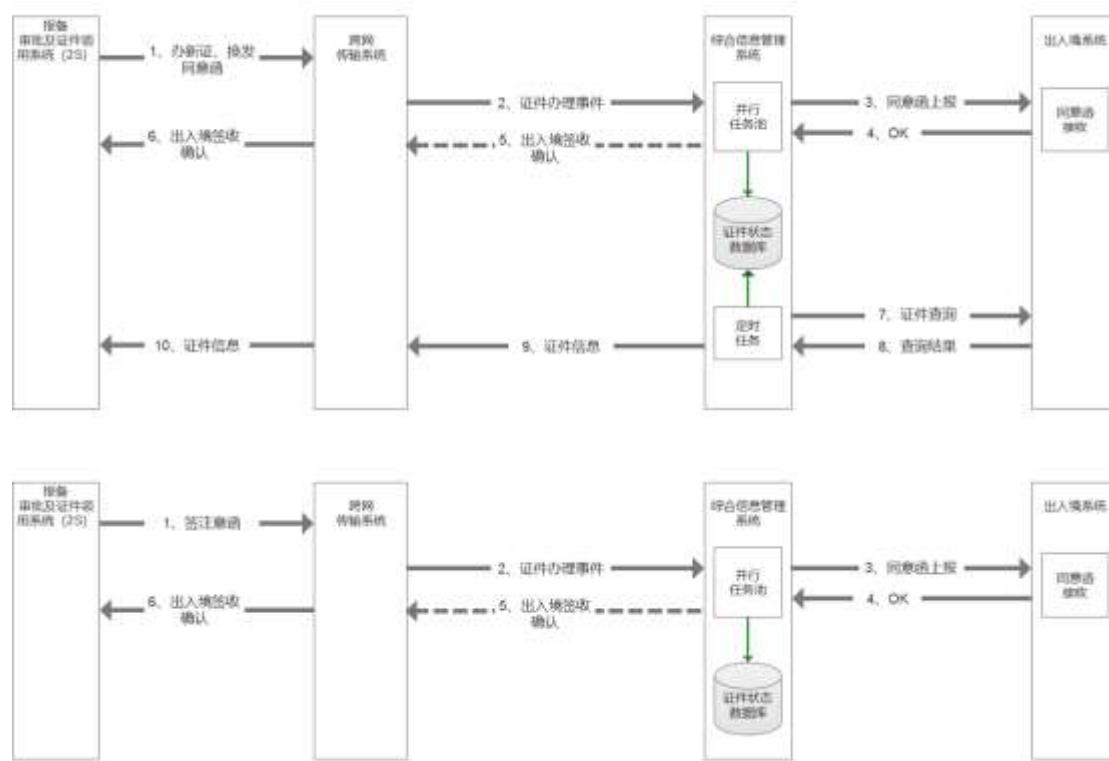


图 2-6-6 同意函处理时序图

(3) 证件入柜

接收证件入柜信息后，更新数据库中证件状态信息，同时进行反馈

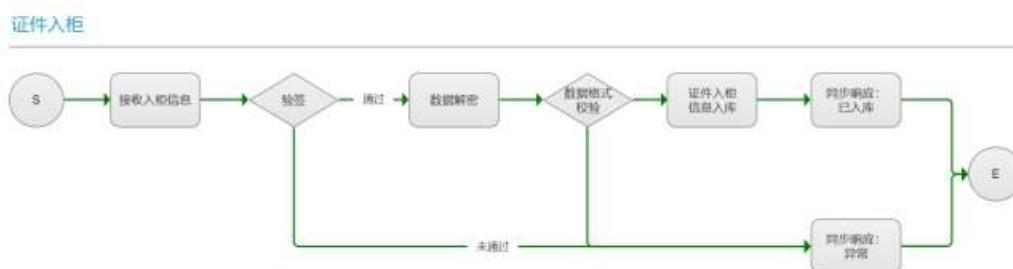


图 2-6-7 证件入柜流程图

入柜业务传输流程

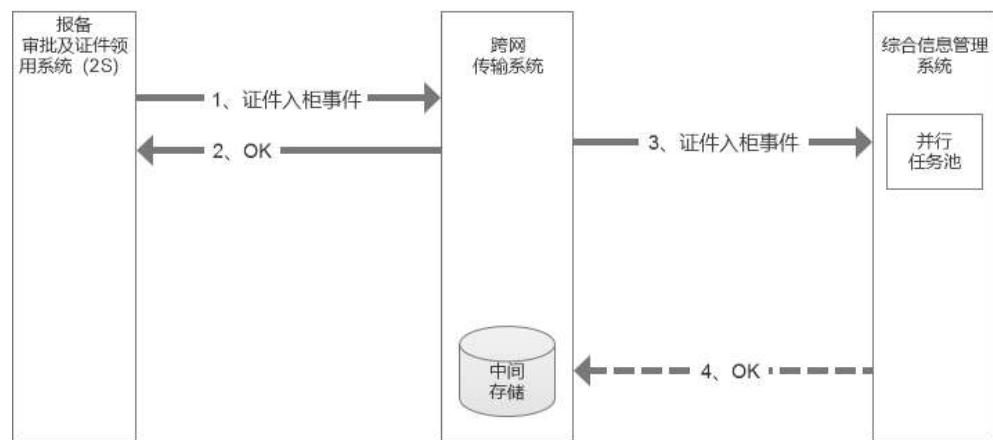


图 2-6-8 证件入柜流程图

(4) 证件出柜

接收证件出柜信息，更新数据库中证件状态信息后，开始定时调用出入境证件查询功能模块，检测证件关联人员的出境再入境记录，查询到入境记录后标记数据库中证件的状态为待入库状态，并进行反馈。

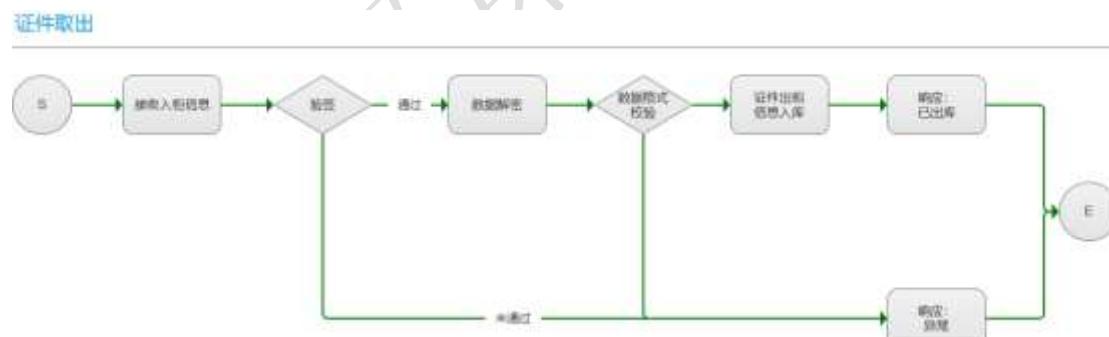


图 2-6-9 证件出柜流程图

出柜业务传输流程

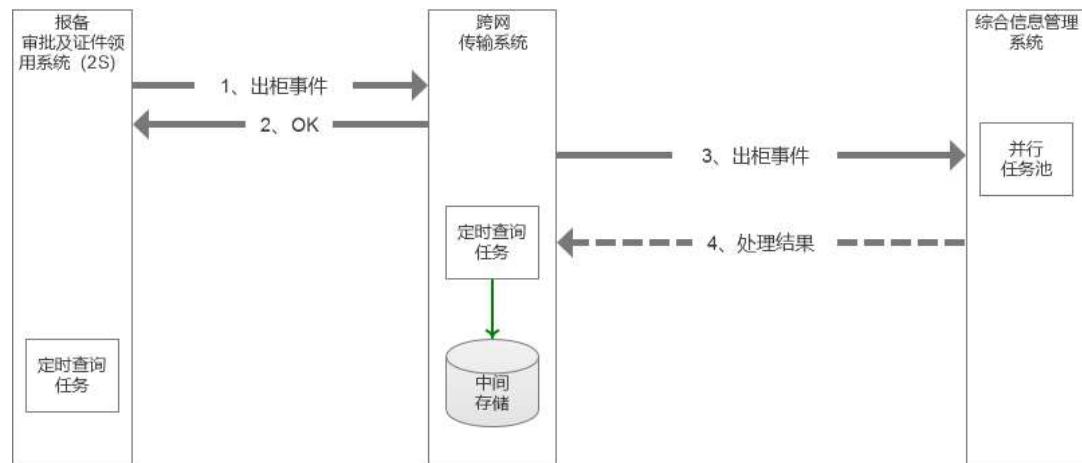


图 2-6-10 证件出柜时序图

(5) 证件注销

接收上传的证件注销信息，修改数据库中证件状态信息，异步反馈证件注销回执。



图 2-6-11 证件注销流程图

证件注销业务传输流程

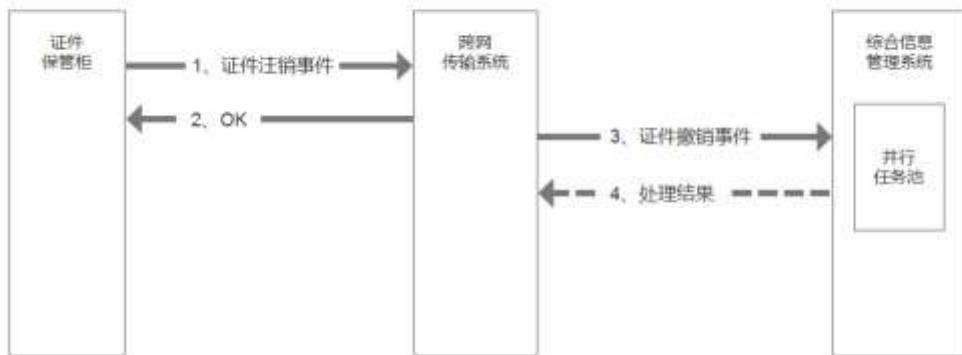


图 2-6-12 证件注销时序图

(6) 应用注册激活

接收到登记备案应用系统和证件领用系统的激活信息后，将激活信息（应用 ID 和组织机构信息）存入数据库。



图 2-6-13 应用注册激活流程

(7) 组织机构信息登记

接收到登记备案应用系统填报的下属工作单位组织机构信息后，将组织机构信息存入数据库。

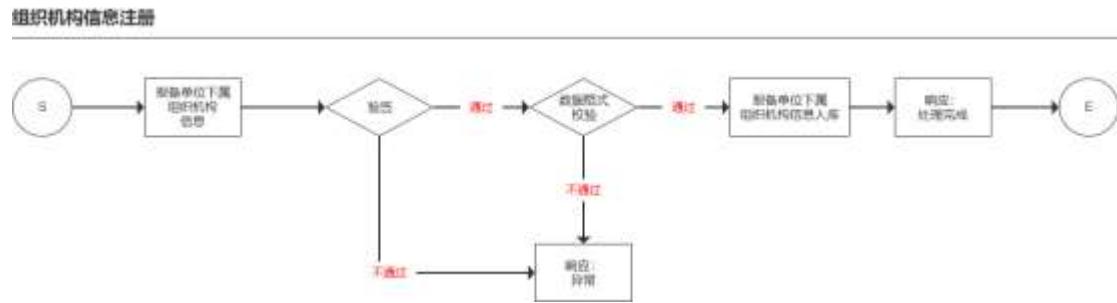


图 2-6-14 组织机构信息登记流程

(8) 终端管理员身份信息登记

接收到登记备案应用系统和证件领用系统的管理员身份信息信息后，存入数据库。



图 2-6-15 终端管理员身份信息登记流程

2.6.4.1.2 接口数据格式

(1) 服务地址定义

[http://\[host\]:\[port\]/xxx/\[ver\]/xxx](http://[host]:[port]/xxx/[ver]/xxx)

说明：

[host]：认证服务 IP 或者域名；

[port]：认证服务端口号；

[ver]：认证服务 API 版本

(2) 服务协议规格

用户向服务器发送认证请求规格：

请求协议: http

请求方法: post

上传数据: body = json 字符串

内容类型: Content-Type = application/json, charset=utf-8

(3) 请求整包数据结构

序号	字段	类型	字段名	必填	备注
	version	String	协议版本	是	
2	mstype	String	业务数据消息类型	是	
	c	JSONObject	控制信息	是	
	coding	String	数据编码, 如 b64	是	
	reqid	String			
	reqtime	String	请求时间戳(抗重放)	是	
	sid	String	会话 id(抗 Dos)	是	
	ai	String	安全机制	是	
	ki	String	应用密钥索引	是	
	ei	String	安全模块 id	是	
s		JSONObject	秘钥信息	是	s
	env	String	数字信封 (含接收者证书 id) 或会话密钥	是	
	sig	String	原始签名或 mac (含公钥和算法)	是	
	rsig	String	转发签名或 mac (含公钥标识和算法)	是	

	bdata		JSONObject	请求业务数据	是	
		ywlsh	String	业务流水号		
		data	String	加密数据（BASE64 编码）		

业务数据报文示例:

```
{
    "version": "",  

    "mstype": "",  

    "c": {  

        "coding": "b64",  

        "reqid": "",  

        "ai": "",  

        "ki": "",  

        "ei": ""  

    },  

    "s": {  

        "env": "",  

        "sig": "",  

        "rsig": ""  

    },  

    "bdata": "业务数据"
}
```

响应整包数据结构:

序号	字段	类型	字段名	必填	备注
	version	String	协议版本	是	

2	mstype		String	业务数据消息类型	是	
	code		String	响应码		
	desc		String	响应说明		
	field		String			
	c		JSONObject	控制信息	是	
		coding	String	数据编码, 如 b64	是	
		reqid	String		是	
		ai	String	安全机制	是	
		ki	String	应用密钥索引	是	
		ei	String	安全模块 id	是	
	s		JSONObject	秘钥信息	是	s
		env	String	数字信封(含接收者证书 id)或会话密钥	是	
		sig	String	原始签名或 mac(含公钥和算法)	是	
	bdata		String	请求业务数据	是	

```
{
    "code":,
    "desc":"",
    "field":"",
    "version":"", // 协议版本
    "mstype ":"", // 业务数据消息类型
    "c":{
```

```
"coding": "", // 数据编码 ("b64")  
"reqid": "", // 请求 id  
"ai": "", // 安全机制 ("认证机制+加密机制" 的组合)  
"ki": "", // 密钥索引  
"ei": "" // 安全模块 id  
},  
"s": {  
    "env": "", // 数字信封 (含接收者证书 id) 或会话密钥  
    "sig": "" // 原始签名 (含公钥标识和算法)  
},  
"bdata": {  
    ... // 业务数据  
}  
}
```

(4) 详细接口参数说明

◆ 应用接入许可 (激活) 接口

请求数据 (body)

字段	类型	字段名	必填	说明
appid	String			
zzjgdm	String	组织机构代码		
zzjgmc	String	组织机构名称		
lxdh	String	联系电话		
dz	String	地址		

fwzt	String	服务状态		
------	--------	------	--	--

{
 “appid”：“平台签发的绑定 UKEY 的应用 ID”，
 “zzjgdm”：“组织机构代码”，
 “zzjgmc”：“组织机构名称”，
 “lxdh”：“联系电话”，
 “dz”：“地址”，
 “fwzt”：“服务状态”
}

响应数据 (body)

{
 “desc”：“错误描述”，
 “code”：“响应码”
}

◆ 管理员身份信息接口

请求数据 (body)

字段	类型	字段名	必填	说明
zzjgdm	String	组织机构代码		
xm	String	应用 ID		密文
gmsfhm	String	公民身份号码		公民身份号码
sj	String	手机号码		手机号码

{

```
        "zzjgdm" : " "
        "xm" : "姓名",
        "gmsfhm" : "公民身份号码",
        "sj" : "手机号",
    }
```

响应数据 (body)

```
{
    "desc" : "错误描述",
    "code" : "响应码"
}
```

◆ 报备单位组织机构提交接口

请求数据 (body)

字段	类型	字段名	必填	说明
appid	String	应用 ID		
bbdwzzjgdm	String	报备单位组织机构代码		
zzjgdm	String	组织机构代码		
zzjgmc	String	组织机构名称		

```
{
    "appid" : " ",
    "bbdwzzjgdm" : "报备组织机构代码",
    "zzjgdm" : "组织机构代码",
    "zzjgmc" : "组织机构名称",
```

}

响应数据（body）

{

“desc”：“错误描述”，

“code”：“响应码”

}

◆ 登记备案信息提交接口

请求数据（body）

字段	类型	字段名	必填	说明
zzjgdm	String	组织机构代码		
bbrys1	int	报备人员数量	是	
spdwj	String	审批单 PDF 文件	是	BASE64
bbywlsh	String	报备业务流水号	是	
spdwjqm	String	审批单文件签名	是	BASE64
bbry1b	JSONArray	报备人员列表	是	
	rybs	人员标识	是	人员的唯一ID Hash(公民身份证号码 + 姓名)
	xm	姓名		密文
	gmsfh	公民身份号码		密文

	m				
	1xdh	String	联系电话		
	zzjgd m	String	组织机构代码		
	bblx	String	报备类型		bbxz(新增)、 bbcx(撤销)
	zw	String	职务		
	zjhzc	String	职级或职称		

示例

```
{  
    "appid": "",  
    "bbrysl": 10  
    "bbywlsh": "报备业务流水号",  
    "spdwj": "BASE64(报备文件审批表)",  
    "spdwjqm": "BASE64(审批文件数字签名)",  
    "bbrylb": [{"  
        "rybs": "",  
        "xm": "",  
        "gmsfhm": "",  
        "zzjgdm": "组织机构代码",  
        "1xdh": "手机号码",  
        "zw": "",  
        "zzjgdm": "",  
        "zjhzc": "",  
        "bblx": ""  
    }]
```

```
    }]  
}
```

响应数据（body）

```
{  
    "desc": "错误描述",  
    "code": "响应码"  
}
```

◆ 登记备案结果反馈查询接口

字段		类型	字段名	必填	说明
bbywlsh		String	报备业务流水号		
zzjgdm		String	组织机构代码		
bbjg					
	ryid	String	人员 ID		
	bbzt	String	报备状态		
	bblx	String	报备类型		
	zjlb				
		zjlx	证件类型		
		zjhm	证件号码		

```
{  
    "bbywlsh": "报备业务流水号",  
    "zzjgdm": "",  
    "bjlx": "居民身份证",  
    "bjhm": "110101198801011234",  
    "ryid": "100000000000000000",  
    "bbzt": "已报备",  
    "bblx": "居民身份证",  
    "zjlx": "居民身份证",  
    "zjhm": "110101198801011234",  
    "bjlx": "居民身份证",  
    "bjhm": "110101198801011234",  
    "bz": "正常",  
    "zzjgdm": ""  
}
```

```
“bbjg” :[{
    “ryid” :”人员 ID” ,
    “bbzt” :”报备状态” ,
    “bblx” :”报备类型” ,
    “zjlb” :[{
        “zjlx” :”证件类型” ,
        “zjhm” :”证件号码” ,
    }]
}],  
“code” :”响应码” ,  
“desc” :””  
}]
```

◆ 出国（境）审批表提交接口

请求数据（body）

字段	类型	字段名	必填	说明
cgspry wlsh	String	出国（境） 审批业务 流水号		
rybs	String	人员标识	是	每个人唯一的人员标识， hash（公民身份号码+姓名）
xm	String	姓名	是	
gmsfh	String	公民身份号	是	

m		码		
1xdh	String	联系电话	是	
dwmc	String	单位名称	是	
zw	String	职务	是	
rsbml xr	String	人事部门联 系人姓名	是	人事负责人姓名
rsbml xrlxd h	String	人事部门联 系人联系电 话	是	
tysj		同意时间	是	
spbwj	String	审批表扫 描件 pdf	是	审批表扫描件 pdf
tyhwj qm	String	审批表扫 描件 pdf 文件签名	是	审批表扫描件 pdf 文 件签名

{

“cgspywlsh”：“出国（境）审批业务流水号”，

“xm”：“”，

“gmsfhm”：“”，

“sj”：“手机号码”，

“zzjgdm”：“组织机构代码”，

“mdd”：“目的地”，

“cfsj”：“出发时间”，

“fhsj”：“返回时间”，

“cgsy”：“出国事由”，

```
        "zjlx": "证件类型",
        "zjhm": "证件号码可为空",
        "spbjw": "BASE64(审批表扫描件 pdf)"
    }
```

响应数据 (body)

```
{
    "code": "响应码",
    "desc": ""
}
```

◆ 同意函提交接口

请求数据 (body)

字段	类型	字段名	必填	说明
cgspywlsh	String	出国(境) 审批业务 流水号		
tyhywlsh	String	同意函业 务流水号		同意函业务流水号
crjyw1x	Int	出入境业 务类型-新 办证件、签 注、换发		出入境业务类型-新 办证件、签注、换发
tyhwj	String	BASE64(同 意函扫 描件 pdf)		BASE64(同意函扫描 件 pdf)
tyhwjqm	String	同意函扫 描件 pdf 签名		同意函扫描件 pdf 签 名

```
{  
    "cgspywlsh" : "出国（境）审批业务流水号" ,  
    "tyhywlsh" : "同意函业务流水号" ,  
    "crjyw1x" : "出入境业务类型-新办证件、签注、换发"  
    "tyhwj" : "BASE64(同意函扫描件 pdf) "  
}
```

响应数据 (body)

```
{  
    "code" : "响应码" ,  
    "desc" : ""  
}
```

◆ 出国境审批及同意函结果

字段	类型	字段名	必填	说明
cgspywlsh	String	出国（境）审批业务流水号		业务流水号(拼接组织机构代码)
jg	String	同意函&审批表提交结果		同意函&审批表提交结果

```
{  
    "cgspywlsh" : "出国（境）审批业务流水号" ,  
    "jg" : "结果"  
}
```

◆ 证件存取事件接口

请求数据 (body)

字段	类型	字段名	必填	说明
ywlsh	String	出国（境） 审批业务 流水号		业务流水号
zzjgd m		组织机构 代码		组织机构代码
zjhm		证件号码		证件号码
cqsj		存取事件		存取事件

```
{  
    "ywlsh": "证件存取业务流水号",  
    "zzjgdm": "组织机构代码",  
    "zjhm": "证件号码",  
    "cqsj": "存取事件"  
}
```

响应数据 (body)

```
{  
    "code": "响应码",  
    "desc": ""  
}
```

◆ 证件注销接口

请求数据 (body)

字段	类型	字段名	必填	说明
ywlsh	String	业务流水号		业务流水号

zzjgd m	String	组织机构 代码		组织机构代码
zjid	String	证件 id		证件 id
zxhzw j	String	注 销 回 执 PDF 文件		注销回执 PDF 文件

{

“yw1sh”：“证件注销业务流水号”，

“zzjgdm”：“组织机构代码”，

“zjid”：“证件 id”，

“zxhzwj”：“注销回执 PDF 文件”

}

响应数据（body）

{

“code”：“响应码”，

“desc”：“”

}

◆ 异常告警接口

字段		类型	字段名	必填	说明
cj		JsonArr ay	催缴列表		
	zzjgdm	String	组织机构 代码		
	ryid	String	人员 ID		

	zjlx	String	证件类型		
	zjhm	String	证件号码 (脱敏)		
	yqts	String	逾期天数		
	gjscsj	String	告警生成时 间		
yc		JsonArr ay	异常列表		
	zzjgdm	String	组织机构 代码		
	yclx	String	异常类型		
	ryid	String	人员 ID		
	zjid	String	证件 ID		
	ycsm	String	异常信息说 明		

{

“cj” :[{
 “zzjgdm” :” ” ,
 “ryid” :”” ,
 “zjlx” :” 证件类型” ,
 “zjhm” :” 证件号码 (脱敏)” ,
 “yqts” :” 逾期天数” ,
 “gjscsj” :” 告警生成时间”
}],

```
“yc” : [ {  
    “zzjgdm” : ” ” ,  
    “yclx” : ” 异常类型 ” ,  
    “ryid” : ” 人员 ID ” ,  
    “zjid” : ” 证件 ID ”  
    “yccsm” : ” 异常信息说明 ”  
}, ]  
}
```

2.6.4.1.3 签名验签

(1) 签名

1. 原文信息通过摘要算法生成摘要信息
2. 使用私钥对摘要信息进行加密生成数字签名



图 2-6-14 签名

输入：原始数据

输出：数据签名

详见模块 7（密钥管理系统）

(2) 验签

-
1. 使用公钥对数据签名进行解密获取摘要信息
 2. 使用摘要算法将明文生成摘要
 3. 对摘要信息进行比对，一致验签通过（合法），不一致验签未通过（非法）

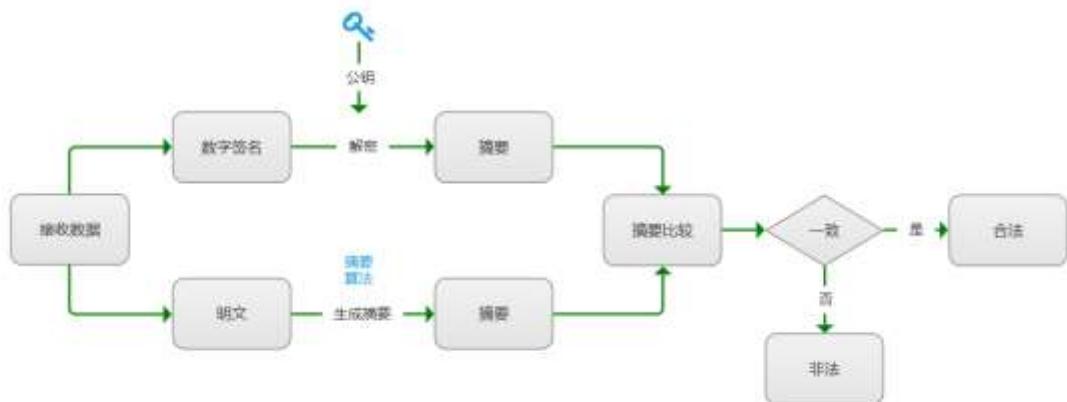


图 2-6-15 验签

输入：原始数据，签名

输出：验签结果

详见模块 7（密钥管理系统）

2.6.4.1.4 加密解密

公钥和私钥配对的，用公钥加密的文件，只有对应的私钥才能解密。当然也可以反过来，用私钥加密，用对应的公钥进行解密。

(1) 加密

详见模块 7（密钥管理系统）

(2) 解密

详见模块 7（密钥管理系统）

2.6.4.1.5 并行任务处理

(1) 数据交换并行任务线程池

核心线程（corePool）：核心线程始终开启，随时等待接收并及时处理请求任务，同时会限制线程的数量。当有新任务提交时，首先检查核心线程数，如果核心线程都在工作，而且数量也已经达到最大核心线程数，则不会继续新建核心线程，而会将任务放入等待队列。

等待队列（workQueue）：等待队列用于存储当核心线程都在忙时，继续新增的任务，核心线程在执行完当前任务后，也会等待队列拉取任务继续执行，这个队列一般是线程安全的阻塞队列，它的容量也可以根据需求业务来定制。

非核心线程：当等待队列已满，如果当前线程数没有超过最大线程数，则会新建线程执行任务。

线程活动保持时间（keepAliveTime）：线程空闲下来之后，保持线程存活的持续时间，超过这个时间还没有任务执行，该工作线程结束。

饱和策略（RejectedExecutionHandler）：当等待队列已满，线程数也达到最大线程数时，线程池会根据饱和策略来执行后续操作，默认的策略是抛弃要加入的任务。

（2）并行任务处理原则

◆ 人员报备、注销、办证事件并行任务线程池

✓ 用于处理人员报备、注销、办证事件相关的批量任务，此类任务包含审批函照片、审批签名相关信息，以及出入境查询相关查询任务；

✓ 使用及配置原则：尽可能提高并能任务处理能力，尽快完成数据校验和入库工作。

◆ 取证、入柜事件并行任务线程池

-
- ✓ 用于处理取证、入证操作的简单任务；
 - ✓ 使用及配置原则：尽可能提高并能任务处理能力，尽快完成数据校验和入库工作。
 - ◆ 出入境记录及证件信息反馈并行任务线程池
 - ✓ 用于处理境相关的异步任务的响应任务。
 - ✓ 使用及配置原则：尽可能提高并能任务处理能力，尽快完成发送工作。
 - ◆ 出入境查询并行任务线程池
 - ✓ 用于处理出入境查询相关任务
 - ✓ 使用及配置原则：限制出入境查询任务的并行数量，确保向出入境查询系统输出的压力在合理范围之内。

2.6.4.1.6 并发访问控制

并发访问控制采用令牌桶技术，在认证请求在传输时，为了防止网络拥塞，确保系统响应时间，需限制流出网络的流量，使流量以比较均匀的速度向外发送。令牌桶算法就实现了这个功能，可控制服务器处理请求的数目，并允许短时间突发数据的发送。

本系统采用大小固定的令牌桶可自行以恒定的速率源源不断地产生令牌。如果令牌不被消耗，或者被消耗的速度小于产生的速度，令牌就会不断地增多，直到把桶填满。后面再产生的令牌就会从桶中溢出。最后桶中可以保存的最大令牌数永远不会超过桶的大小。系统针对用户访问流量进行了控制，用户进行认证时，先从令牌桶里取得

令牌，若在 200ms 内没有取得令牌，则被拒绝认证。

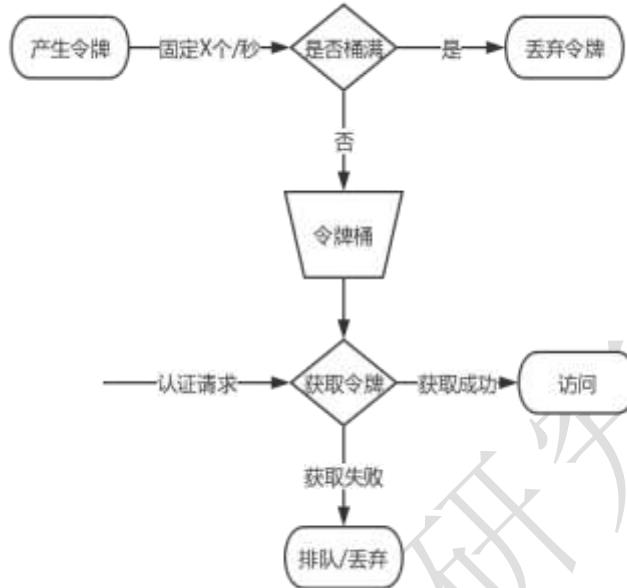


图 2-6-16 令牌桶流程图

2.6.4.2 证件催缴报告推送系统

2.6.4.2.1 功能说明

证件催缴报告模块用于推送催缴证件清单。当证件触发了如下两个事件之后，证件将会设置为“等待入柜”状态，

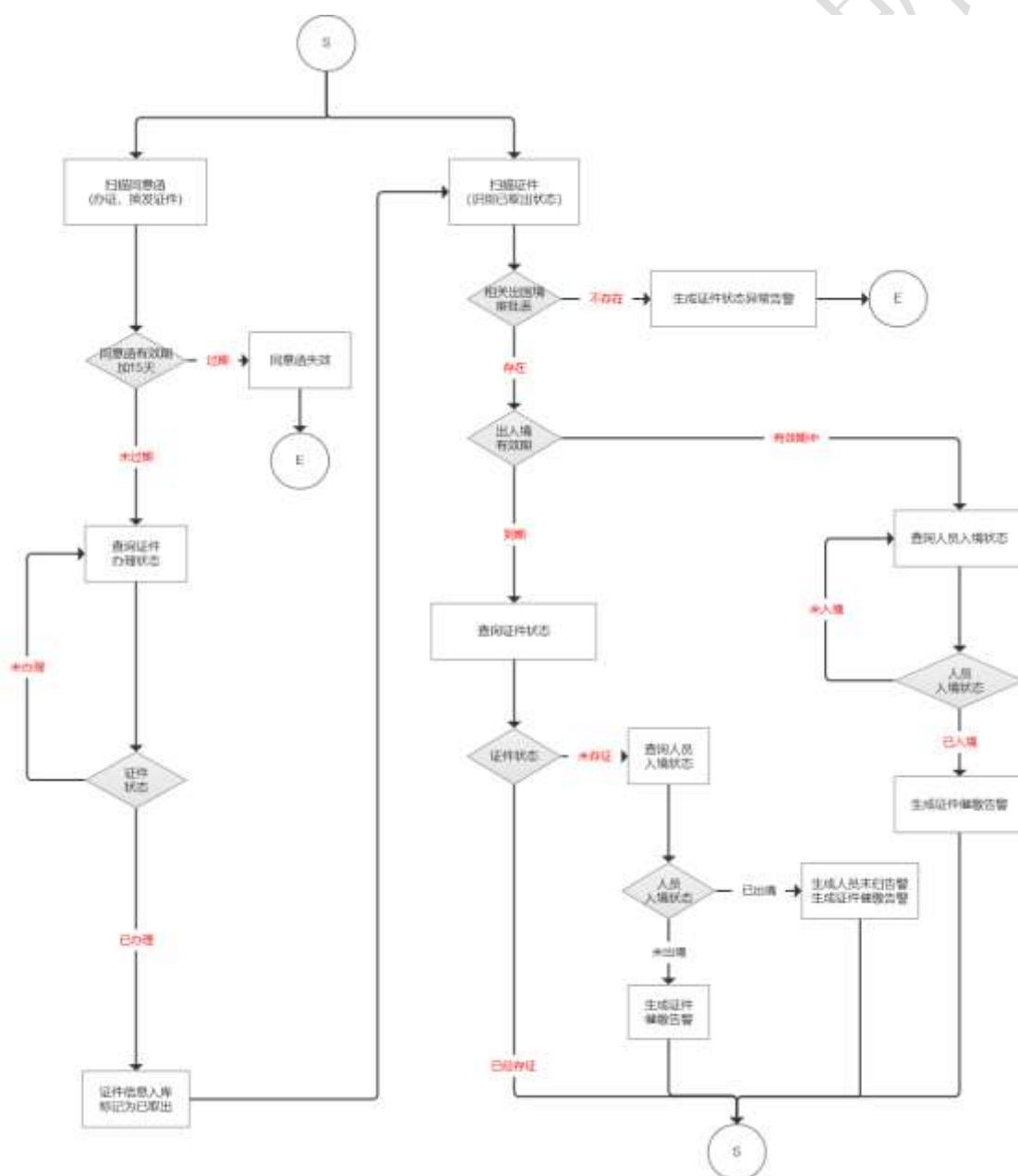
- 当证件被取出后，该证件触发了“入境事件”；
- 当证件被取出后，该证件触发了“已到归还日期”。

当证件进入“等待入柜”状态之后，将被列入催缴报告模块的监测范围，当超过状态后的某一段事件之后将会被列入当日的催缴清单。

定时任务扫描同意函（办新证、换发证件）如果同意函有效期已

超出 15 天（办证周期），则更改同意函状态并结束任务，如在有效期内则查询证件办理状态，如果证件处于尚未办理状态则继续扫描，如果扫描到已办理则登记证件信息并标记为已取出。

定时任务扫描证件，识别出已取出的证件，扫描对应的出国（境）审批表是否存在，不存在告警，存在时查询审批是否已过期，在有效期内。



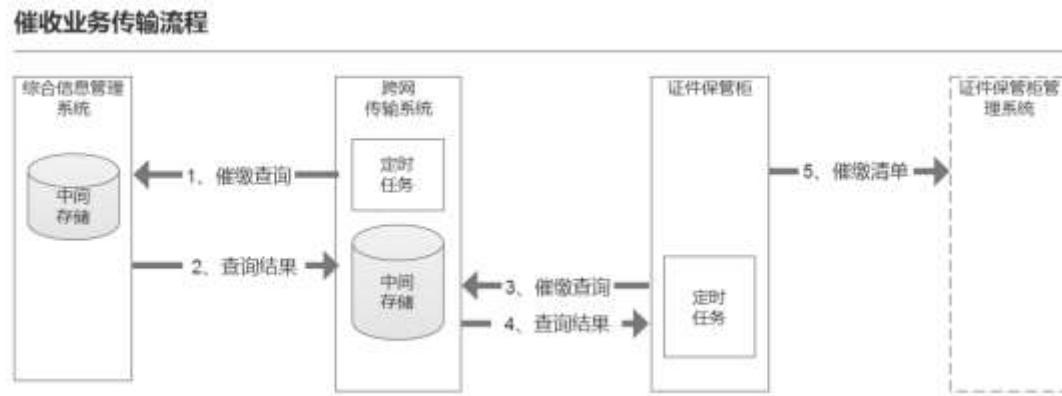


图 2-6-17 催缴查询时序图

2.6.4.2.2 结构格式

组织标识、人员标识、证件类型、证件标识、逾期时间（天）

2.6.4.3 数据管理子系统

2.6.4.3.1 人员及证件生命周期管理

人员状态和证件的状态建议采用有限状态机进行描述（FSM），基于事件驱动状态的变更。有限状态机（FSM）是一种用来进行对象行为建模的工具，其作用主要是描述对象在它的生命周期内所经历的状态序列，以及如何响应来自外界的各种事件。有限状态机（FSM）能采取某种操作来响应一个外部事件。具体采取的操作不仅能取决于接收到的事件，还能取决于各个事件的相对发生顺序。为一个事件而响应的行动不仅取决于事件本身，还取决于机器的内部状态。另外，采取的行动还会决定并更新机器的状态。

数据交换的业务逻辑，将遵循报备人员证明周期状态逻辑以及证件生命周期的有限状态机（FSM）描述，以事件为驱动设置其状态，以确保与证件保管柜状态的一致性。

系统关于事件的处理逻辑，请参考数据交换接口中的事件处理流程。

(1) 报备人员生命周期



图 2-6-18 报备人员生命周期

状态：

- 报备中：系统向出入境提交报备信息，未收到返回信息之前的人员状态。
- 已报备：已经在出入境管理局报备成功的人员状态。
- 报备变更中：同单位报备信息变更中的状态
- 报备撤销中：系统向出入境提交撤销报备信息，未收到返回信息之前的人员状态。
- 报备已注销：已经在出入境管理局撤销报备的人员状态。

事件：

- 报备：系统接收到报备申请事件时执行“报备事件处理流程”，流程执行成功后，创建人员记录并设置人员状态为“已

报备”。

- 报备变更：系统接收到同单位报备信息变更时执行“报备信息变更处理流程”，流程执行中时进入“报备变更中”状态，出入境返回结果为成功，更新报备人信息并设置人员状态为“已报备”，出入境返回结果为失败，不更改报备人信息，恢复变更前的“已报备”状态。
- 撤销报备：系统接收到报备申请事件时执行“报备事件处理流程”，流程执行成功后，将人员记录并设置人员状态为“已注销”。

(2) 证件生命周期

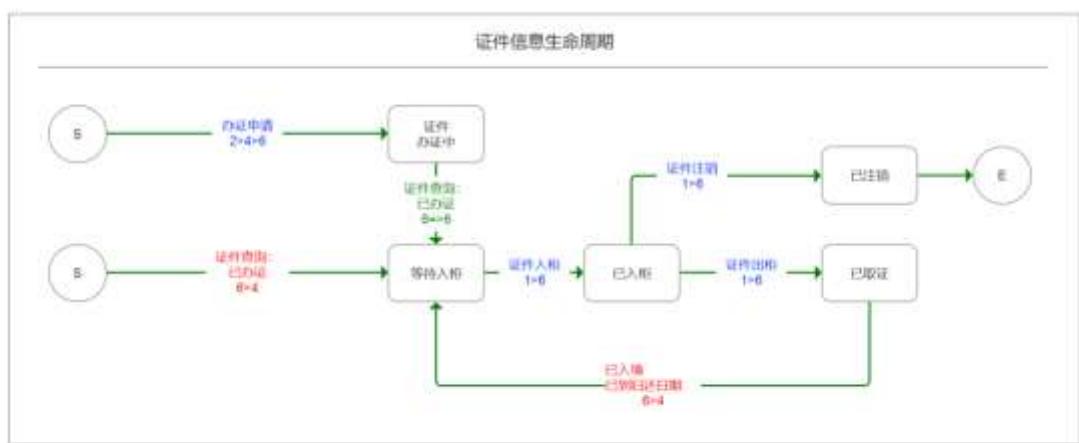


图 2-6-19 证件生命周期状态流转

状态：

- 办证中：证件正在办理中；

-
- 等待入柜：证件已经被取出之后，到达归还日期或者满足归还条件（已入境、证件办理完成未入柜）；
 - 已入柜：证件保存在证件保管柜中；
 - 已取证：证件已经被取出，但未到归还时间；
 - 已注销：证件过期、丢失、损坏等其他失效情况。

事件：

- 办证事件：当人员报备成功后，系统接收到了“办证申请事件”；
- 证件查询已办证：当人员报备成功后，系统定时巡查出入境证件查询接口，当证件为“已办理”时，触发该事件；
- 证件入柜：当系统收到“证件入柜”事件；
- 证件出柜：当系统收到“证件出柜”事件；
- 证件注销：当系统收到“证件注销”事件；
- 已入境：当证件已经被取出后，系统定时巡查出入境证件查询接口，当该证件入境时触发该事件；
- 已到归还日期：当证件已经被取出后，系统定时巡查证件归还日期，当归还期到时触发该事件。

说明：当人员生命周期变为“报备已撤销”后，所有相关证件生命周期设置为“已注销”状态。

2.6.4.3.2 查询用户管理（OAuth2）

（1）系统管理员

系统管理员登录系统后将进入后系统管理服务页面。系统管理员可以进行查询用户账户创建与控制，权限分配，配置参数管理，系统认证统计查看功能。

（2）查询用户

查询用户账号是由系统管理员创建。登录系统后将进入平台门户页面。应用管理账户可以查看属于本组织机构及下属单位的证件使用记录、出入境记录、告警信息等统计信息。

2.6.4.4 数据查询服务子系统

2.6.4.4.1 数据分析统计报表查询子系统

（1）报备人员及证件信息查询（包括人的状态和证的状态）

接收到请求后，查询对应人员的登记报备信息和证件信息并反馈给展示系统。

（2）人员出入境记录查询

接收到人员出入境查询需求时，访问出入境记录查询接口，并将结果反馈给展示系统。

（3）组织机构查询

接收到组织机构查询请求时，可以根据要查询的组织机构代码查询到对应组织的报备单位信息。

(4) 风险操作及催缴告警

2.6.4.4.2 组织报备状态记录管理

(1) 组织查询证件使用情况

2.6.4.5 出入境数据查询接口

2.6.4.5.1 出入境报备推送接口

2.6.4.5.2 出入境办证推送接口

2.6.4.5.3 出入境证件查询接口

人员报备业务场景：报备数据入库后，综合信息管理系统调用证件办理查询时会调用一次出入境查询接口，查询该人员是否已经持有出入境证件，标记已经办理的出入境证件状态为待入库状态，同时进行反馈

办证申请场景：综合信息管理系统证件办理状态查询时，会定时调用出入境查询接口，检测到如果有新的出入境证件办理成功，将证件信息入库并标记状态为待入库状态，同时进行反馈。

2.6.4.5.4 个人出入境记录查询接口

2.6.4.5.5 出入境证件丢失通报推送接口

2.6.4.5.6 包括多个备用访问站点以及配置方案

2.6.4.5.7 查询结果功能描述

2.6.4.6 系统运行状态报告

应用监控能够实时获取前台门户系统服务运行状态，线程池使用情况，连接池使用情况，队列使用情况，根据资源使用情况，作出对

应风险预警。

Actuator 组件提供了监控和管理 spring boot 应用的 HTTP 或者 JMX 端点，引入依赖之后，将自动的拥有审计、健康检查、Metrics 监控功能、指标收集、HTTP 跟踪等，帮助我们监控和管理 SpringBoot 应用、Bean 加载情况、环境变量、日志信息、线程信息，JVM 堆信息等。

2.6.5 事件日志

2.6.5.1 事件日志定义：

系统运行状态发生变化时的系统日志

数据库数据发生变化时的操作日志

查询数据库时记录的审计日志

2.6.5.2 事件日志功能：

向运维服务人员提供系统异常信息查询，帮助定位系统错误信息

保留数据库 crud 操作日志，用于数据对账和操作审计

2.6.5.3 日志系统架构

整体上使用 ElasticSearch 技术栈搭建日志系统。使用 Logstash 组件统一收集系统各节点的日志，可选采集项包含操作系统日志、数据库日志、中间件日志和软件系统自定义日志等，Logstash 完成日志初步处理后发送给 Elasticsearch 集群进行分析和存储，前端使用 Kibana 组件提供数据可视化展示查询功能。

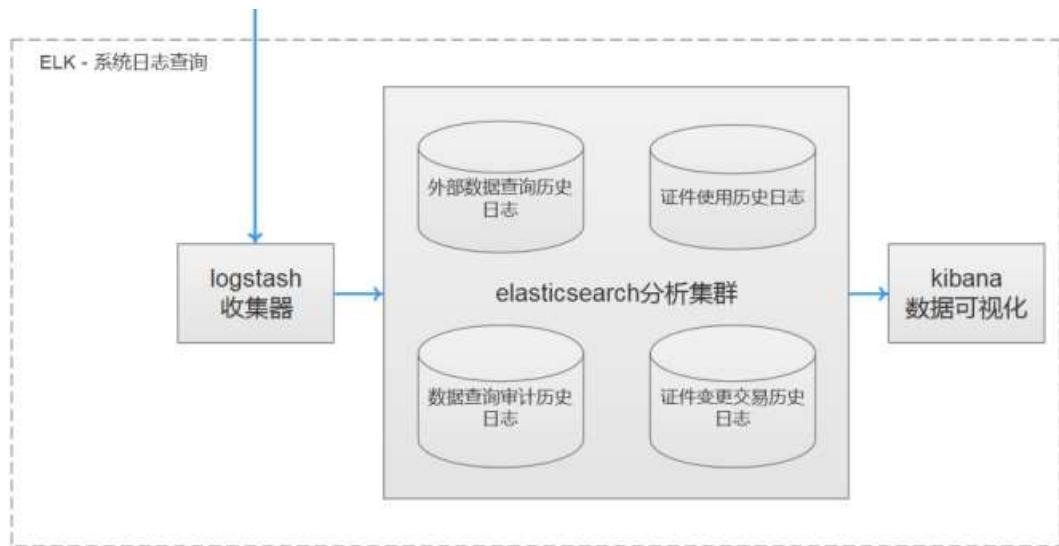


图 2-6-20 日志系统架构图

2.6.5.4 日志类型

2.6.5.4.1 证件使用历史日志

证件使用历史记录记录了系统发生证件办理、证件出柜、证件入柜和证件作废事件时的事件日志。日志项：操作时间、时间类型、证件 id

2.6.5.4.2 数据查询操作审计日志

数据查询操作审计日志记录了前端数据查询子系统进行查询操作时的审计日志。日志项：查询时间、查询类型、查询用户、查询对象

2.6.5.4.3 外部接口查询日志

外部接口查询日志记录数据交换子系统调用出入境数据查询接口时生成的接口查询日志。日志项：查询时间、查询类型、查询对象

2.6.5.4.4 系统日志

系统日志保存了综合信息管理系统各个服务器节点、中间件和应用的运行日志。日志格式根据来源的格式确定。

啊啊啊
啊啊啊

2.6.6 数据库表设计

2.6.6.1 数据库集群存储架构设计

2.6.6.2 数据库表结构设计

名称	表名	备注
m_bbdwxx_t	单位信息表	
m_yhxxb_t	管理员信息表	
m_zzjgxx_t	组织机构信息表	
m_zjxx_t	证件信息表	
m_ryxx_t	人员信息表	
m_baobei_t	报备事件流水表	
m_cgsp_t	出国（境）审批事件流水表	
m_tyhxx_t	同意函信息表	
m_zjcq_t	证件存取事件流水表	
m_zjzx_t	证件注销事件流水表	
m_rybbjg_t	人员报备结果	
m_czztfk_t	持证状态反馈表	
m_cjxxfk_t	催缴信息反馈表	
m_ycxx_t	异常信息表	

m_zjztdzpl_t	证件状态对账偏离表	
m_dzsjp1_t	对账事件偏离表	
d_bb1x_t	报备类型字典表	报备、撤销、更改
d_zjzt_t	证件状态字典表	等待入柜、入柜、出柜、办证中
d_zjlx_t	证件类型字典表	护照、港澳通行证、赴台证
d_rybbzt_t	人员报备状态字典表	报备中、已报备、报备撤销中
d_rycrj_t	人员出入境状态字典表	

(1) m_bbdwxx_t 【单位信息表】

代码	名称	数据类型	主键	备注
APPID	应用 ID	VARCHAR(32)	是	
TYSHXYDM	统一社会信用代码	VARCHAR(32)		
DWMC	单位名称	VARCHAR(32)		
LXFS	联系方式	VARCHAR(32)		
LXDZ	联系住址	VARCHAR(32)		
FFZT	服务状态	VARCHAR(32)		
DXAPI	短信 API	VARCHAR(128)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(2) m_yhxxb_t 【管理员信息表】

代码	名称	数据类型	主键	备注
ID	用户 ID	VARCHAR(32)		
TYSHXYDM	统一社会信用代码	VARCHAR(32)		
APPID	应用 ID	VARCHAR(32)		
MM	密码 HASH	VARCHAR(32)		
XM	姓名	VARCHAR(32)		密文
GMSFHM	公民身份证号码	VARCHAR(32)		密文
SJHM	手机号码	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(1) m_zzjgxx_t 【组织机构信息表】

代码	名称	数据类型	主键	备注
BBDWZZJGDM	报备单位组织机构代码	VARCHAR(32)		
ZZJGDM	组织机构代码	VARCHAR(32)	是	
DWMC	单位名称	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(2) m_zjxx_t 【证件信息表】

代码	名称	数据类型	主键	备注
ZJBS	证件标识	VARCHAR(32)	是	hash (证件类型.证件号码)
RYBS	人员标识	VARCHAR(32)		hash (公民身份证号+姓名)
ZJLX	证件类型	CHAR(3)		字典表 参照《常用证件代码 GA-T 517-2004》 414 普通护照 513 往来港澳通行证 517 大陆居民往来台湾通行证
ZJHM	证件号码	VARCHAR(9)		
ZWXM	中文姓名	VARCHAR(45)		
YWXM	英文姓名	VARCHAR(45)		
XB	性别	CHAR(1)		1 男, 2 女
CSRQ	出生日期	CHAR(8)		YYYYMMDD
YXQJZRQ	有效期截止日期	CHAR(8)		YYYYMMDD
CSDD	出生地点	VARCHAR(45)		
QFRQ	签发日期	CHAR(8)		港澳证中是有效期起始日期, YYYYMMDD
QFDD	签发地点	VARCHAR(45)		
QFJG	签发机关	VARCHAR(45)		

ZP	照片地址	VARCHAR(128)		Obs-url
SJLY	数据来源	CHAR(3)	Defualt ‘hzg’	
ZJZT	证件状态	VARCHAR(32)		需要有字典表
SBXLH	设备序列号	VARCHAR(40)		
ZJGXDH	证件柜序列号	VARCHAR(40)		
CTH	抽屉行	VARCHAR(3)		
CTL	抽屉列	VARCHAR(3)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZJXGSJ	最近修改时间	CHAR(14)		YYYYMMDDHHmmss

(3) m_ryxx_t 【人员信息表】

代码	名称	数据类型	主键	备注
XM	姓名	VARCHAR(45)		
RYBS	人员标识	VARCHAR(32)	是	
GMSFHM	公民身份号码	VARCHAR(18)		
DWMC	单位名称	VARCHAR(108)		
TYSHXYDM	统一社会信用代码	CHAR(18)		
LXDH	联系电话	VARCHAR(11)		
ZW	职务	VARCHAR(45)		
ZJHZC	职级或职称	VARCHAR(45)		
RYZT	人员状态	VARCHAR(32)		

RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZJXGSJ	最近修改时间	CHAR(14)		YYYYMMDDHHmmss

(4) m_bbsjls_t 【报备事件流水表】

代码	名称	数据类型	主键	备注
YWLSH	报备业务流水号	VARCHAR(32)	是	UUID
BBSJ	报备时间	DATETIME		
BBRS	报备人数	INT		
TYSHXYDM	统一社会信用代码	VARCHAR(32)		
SPBBCDZ	审批表保存地址	VARCHAR(32)		同意函图片地址
SPBQMZ	审批表签名值	VARCHAR(1024)		
CZR	操作人	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZJXGSJ	最新修改时间	CHAR(14)		YYYYMMDDHHmmss

(5) m_cgsp_t 【出国（境）审批事件流水表】

代码	名称	数据类型	主键	备注
YWLSH	业务流水号	VARCHAR(32)	是	
TYSHXYDM	统一社会信用代码	VARCHAR(32)		
RYBS	人员标识	VARCHAR(32)		
SJSBSJ	数据上报时间	DATETIME		
CGJSPBDZ	出国境审批表地址	VARCHAR(32)		同意函图片地址 (URL OBS)

CGJSPBQMZ	出国境审批表文件签名值	VARCHAR(1024)		签署人 UKey 对同意函进行签名 (确认签署人)
CGJSPTYSJ	出国境审批同意时间	DATETIME		
CGJSPSXSJ	出国境审批失效时间	VARCHAR(32)		加 15 天 (共 45 天)
RSBMLXRXM	人事部门联系人姓名	VARCHAR(32)		
RSBMLXRLXDH	人事部门联系人联系电话	VARCHAR(32)		人事部门联系人联系电话
CZR	操作人	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZJGXSJ	最新更新时间	DATETIME		

(6) 同意函信息表

代码	名称	数据类型	主键	备注
YWLSH	业务流水号	VARCHAR(32)		
CGJYWLSH	出国(境)审批业务流水号	VARCHAR(32)		
TYH	同意函 PDF 文件地址	VARCHAR(32)		
ZJLX	证件类型	VARCHAR(32)		
CRZYWLX	出入境业务类型	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(7) m_zjqc_t 【证件存取事件流水表】

代码	名称	数据类型	主键	备注
YWLSH	证件存取业务流水号	VARCHAR(32)	是	存取事件业务流水号
ZJBS	证件标识	VARCHAR(32)	是	一证一号, 每个证件唯一的证件 id, hash (证件号+证件类型+有效期)
SJSBSJ	数据上报时间	DATETIME		格式 : YYYYmmDDHHMMSS
CZR	操作人	VARCHAR(32)		柜子保管人
CZSJ	操作时间	DATETIME		YYYYmmDDHHMMSS
CZLX	操作类型	VARCHAR(32)		11 存入, 12 取出
QZYT	取证用途	VARCHAR(32)		
GHJZRQ	归还截至日期	DATETIME		取出时该字段生效
SBXLH	设备序列号	VARCHAR(40)		
ZJGXLH	证件柜序列号	VARCHAR(40)		
CTH	抽屉行	VARCHAR(3)		
CTL	抽屉列	VARCHAR(3)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZJXGSJ	最近修改时间	CHAR(14)		YYYYMMDDHHmmss

(8) m_zjzx_t 【证件注销事件流水表】

代码	名称	数据类型	主键	备注
YWLSH	证件注销业务流水号	VARCHAR(32)	是	
ZJBS	证件标识	VARCHAR(32)		

ZXYY	注销原因	VARCHAR(32)		
ZXZMWJDZ	注销证明文件地址	VARCHAR(32)		内部存档
ZXZMWJQM	注销证明文件签名	VARCHAR(32)		内部存档
SJSBSJ	数据上报时间	DATETIME		
CZR	操作人	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
GXSJ	更新时间	CHAR(14)		YYYYMMDDHHmmss

(9) m_rybbjg_t 【人员报备结果】

代码	名称	数据类型	主键	备注
RYBS	人员标识	VARCHAR(32)	是	hash(公民身份证号码+姓名)
YWLSH	报备业务流水号	VARCHAR(32)	是	人员报备事件流水号
BBLX	报备类型	VARCHAR(32)		
BBSM	报备说明	VARCHAR(32)		
BBZT	报备状态	VARCHAR(32)		
BBJGFHSJ	报备结果返回时间	CHAR(14)		YYYYMMDDHHmmss
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(10) m_czztfk_t 【持证状态反馈表】

代码	名称	数据类型	主键	备注
YWLSH	报备业务流水号	VARCHAR(32)	是	社会信用代码+UUID

RYBS	人员标识	VARCHAR(32)	是	
ZJBS	证件标识	VARCHAR(32)	是	
ZJLX	证件类型	VARCHAR(32)		
FKSJ	反馈时间	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(11) m_c_jxxfk_t 【催缴信息反馈表】

代码	名称	数据类型	主键	备注
CJYWLSH	催缴业务流水号	VARCHAR(32)	是	
ZJBS	证件标识	VARCHAR(32)		
TYSHXYDM	统一社会信用代码	VARCHAR(32)		
SBXLH	设备序列号	VARCHAR(32)		
ZJLX	证件类型	VARCHAR(32)		
YQTS	逾期天数	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(12) m_ycxx_t 【异常信息表】

代码	名称	数据类型	主键	备注
TYSHXYDM	统一社会信用代码	VARCHAR(32)		

YXLX	异常类型	VARCHAR(32)		
RYID	人员 ID	VARCHAR(32)		
ZJID	证件 ID	VARCHAR(32)		
YCSM	异常信息说明	VARCHAR(32)		
RKSJ	入库时间	DATETIME		
ZXGXSJ	最新更新时间	DATETIME		

(13) m_zjztdzpl_t 【证件状态对账偏离表】

代码	名称	数据类型	主键	备注
DZYWLSH	对账业务流水号	VARCHAR(32)	是	
ZJBS	证件标识	VARCHAR(32)	是	
RYXM	人员姓名	VARCHAR(32)		
ZJLX	证件类型	VARCHAR(32)		
ZJH	证件号	VARCHAR(32)		
TYSHXYDM	统一社会信用代码	VARCHAR(32)		
BGGZT	保管柜状态	VARCHAR(32)		
XTZT	系统状态	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(14) m_dzs_jpl_t 【对账事件偏离表】

代码	名称	数据类型	主键	备注
DZYWLSH	对账业务流水号	VARCHAR(32)	是	
ZJBS	证件标识	VARCHAR(32)	是	
CZLX	操作类型	VARCHAR(32)		入库 or 出库
SJYSZXZSJ	事件原始执行时间	CHAR(14)		YYYYMMDDHHmmss
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(15) d_bb1x_t 【报备类型字典表】

代码	名称	数据类型	主键	备注
DM	代码	CHAR(3)		
MC	名称	VARCHAR(32)		
MS	描述	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(16) d_zjzt_t 【证件状态字典表】

代码	名称	数据类型	主键	备注
DM	代码	CHAR(3)		

MC	名称	VARCHAR(32)		
MS	描述	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(17) d_zjlx_t 【证件类型字典表】

代码	名称	数据类型	主键	备注
DM	代码	CHAR(3)		
MC	名称	VARCHAR(32)		
MS	描述	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(18) d_rybbzt_t 【人员报备状态字典表】

代码	名称	数据类型	主键	备注
DM	代码	CHAR(3)		
MC	名称	VARCHAR(32)		
MS	描述	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

(19) d_rycrj_t 【人员出入境状态字典表】

代码	名称	数据类型	主键	备注
DM	代码	CHAR(3)		
MC	名称	VARCHAR(32)		
MS	描述	VARCHAR(32)		
RKSJ	入库时间	CHAR(14)		YYYYMMDDHHmmss
ZXGXSJ	最新更新时间	CHAR(14)		YYYYMMDDHHmmss

2.6.6.3 数据对账设计

数据对账功能是完成固定时间内发生变化的证件状态和人员状态的数据一致性检查。证件的状态信息原则上以保管柜的数据为准。

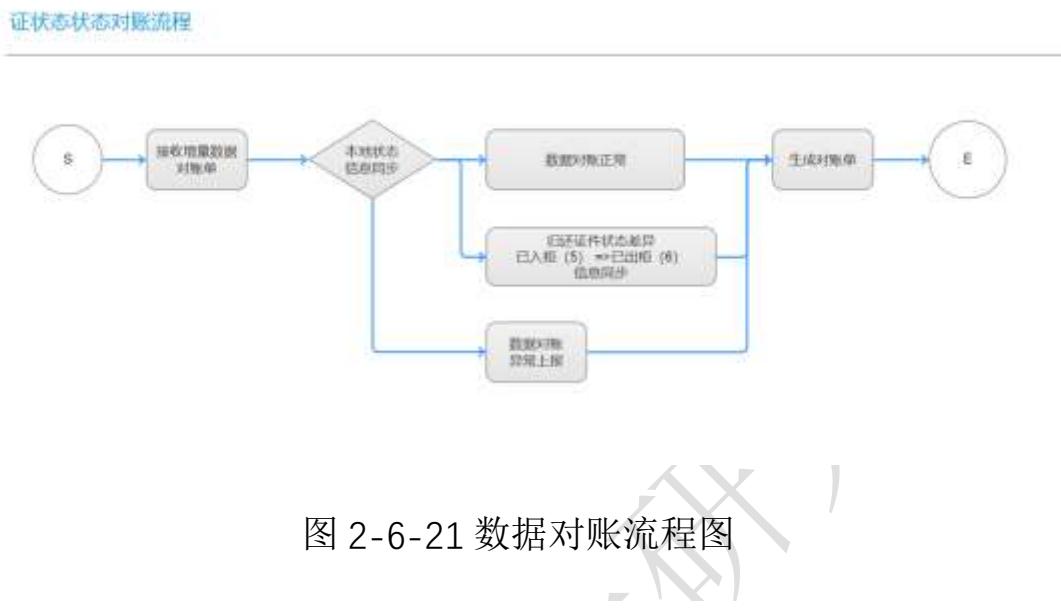
(3) 数据对账处理逻辑

- ◆ 每天在固定的时间段（20:00~06:00），保管柜向综合信息管理系统上报当日变更的证件状态信息和人员状态信息；
- ◆ 综合信息管理系统完成对账工作，并标记差异数据，符合数据自动同步条件差异会被自动同步，其他差异将会被填入对账响应清单；
- ◆ 对账清单需交由单位管理员和系统运维人员处理。

(4) 数据自动同步

综合管理系统仅对满足如下条件的对账差异数据进行自动同步：

当上报数据为“已入柜”，本地数据库为“已取出”状态时，综合管理系统会将证件的状态设置为“已入柜”



对账业务传输流程

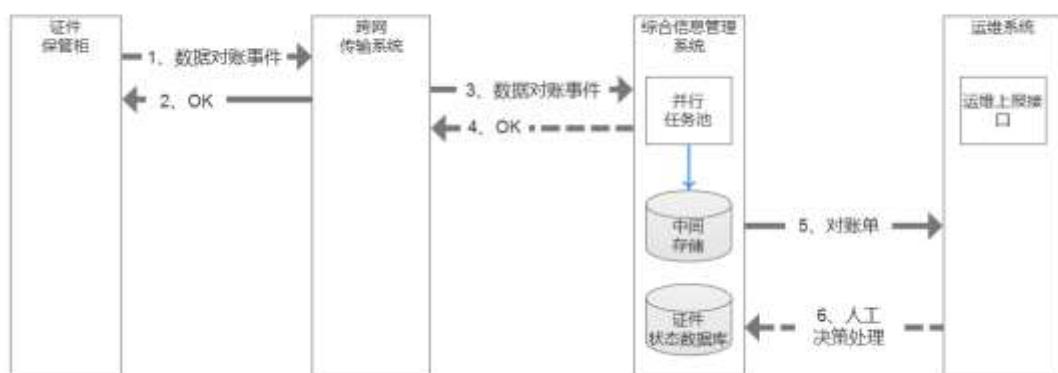


图 2-6-22 数据对账时序图

(5) 对账数据

对账接收数据：每日增量数据，包含如下数据项

证件状态：

◆ 人员标识

-
- ◆ 证件标识
 - ◆ 保存位置（机柜+抽屉）
 - ◆ 社会统一信用代码
 - ◆ 状态（入柜/出柜）

操作流水：

- ◆ 业务请求时间交易流水日志（*）

数据对账偏离表：

证件状态偏离						
对账业务流水号	人员姓名	证件标识	统一社会信用代码	保管柜状态	系统状态	是否修复成功？
操作日志偏离						
业务流水号 1		操作类型		执行时间		执行
业务流水号 2		操作类型		执行时间		执行

2.7 密钥管理系统

2.7.1 概述

“密钥管理系统”主要负责生成、管理护照柜的数字证书和数据保护密钥；初始化模块完成密钥承载安全模块和签名验证服务器的证书和密钥初始化工作。

2.7.2 功能架构

密钥管理系统功能架构参见 4.4.8 节。

2.8 展示系统

2.8.1 概述

在组工网内提供 WEB 页面，供组织部门进行国家工作人员因私出国（境）情况查询和统计，包括出入境历史记录查询，出境国家分布、频次等统计分析。（需进一步调研组织管理相关部门相关需求并进行后续设计）。



图 2-8-1



图 2-8-2

2.9 运维监控系统

2.9.1 概述

运维管理系统负责监控和维护整个管理平台服务器、交换机等各类设备的运行状态，以及各个子系统和功能模块的应用服务状态，从而保障整个系统的运行稳定。

2.9.2 功能架构

运维管理系统采用基础架构、服务支撑和保障、服务应用三层架构设计，设计图见图 2.9-1。



图 2.9-1 架构设计

1. 基础架构

基础软硬件，包括各类传感器、检测中间件和监测工具。

2. 服务支撑和保障

- ◆ 基础监控，是指对服务器、交换机等 IT 资源的监控，以及风火水电等基础设施的监控。
- ◆ 安全监控，是指对网络安全设备、系统安全等方面进行监管。
- ◆ 应用监控，是指对平台服务的监控。

-
- ◆ 运维数据库配置，是指对存储运维数据的数据库进行配置。

3. 服务应用

- ◆ 展示模块，主要是对运维管理情况的展示，包括功能展示、性能展示、故障预警和报警等。
- ◆ 控制模块，主要是对运维管理节点远程控制的操作。
- ◆ 配置管理，主要是对运维管理系统的配置、应用服务的配置进行管理。
- ◆ 服务管理，主要是对故障登记、统计报表、更新、升级等运维服务的管理。

2.9.3 功能描述

2.9.3.1 应用服务监控告警系统

主要实现对整个管理平台系统内各个集群主机和服务状态信息的采集、汇聚、分析、告警四大功能，从各个子系统服务接口采集服务状态和性能信息，汇聚到监控系统服务器中进行识别判断，对于触碰告警规则的异常服务和主机进行告警通知，最终将主机状态、服务状态的信息记录和告警记录保存在数据库中，并可进行展示、查询和性能分析。

(1) 采样接口访问模块

各个应用服务系统提供监控测试调用数据包、调用接口、调用方法和返回值对照表。生成用于调用各个服务接口的测试用例，并确保此测试数据不会对服务的性能造成影响。如表中 2.9-1 所示信息：

表 2.9-1 采样接口访问事例

服务名称	集群地址及端口	集群下各节点地址及端口	请求方式	请求路径	测试用例（需要能够反复测试）	预期测试结果
例： 业 务 调 度 服 务	集群地址： 15.1.10.25 0:8000	节 点 1 : 15.1.10.1:8000 节 点 2 : 15.1.10.2:8000	Get	http://ip: port/vi/lo gin	user=xxxx&pass word=12345678	{result: " success " , token : "XXXXXX XXXXXX" }

(2) 监控任务服务模块

监控任务服务模块负责所有服务状态的采集，需要监控服务可以访问到所有的集群服务节点，对每个服务的接口进行测试，获取返回结果，并判断返回结果是否正确，服务当前状态是否正常，需要在一定时间内完成对数据的收集，定时对所有服务进行轮循测试。

(3) 时序数据库模块

时序数据库模块负责把收集到的各个子系统监控数据保存到时间序列数据库中，时间序列数据库是一类专门用于记录监控信息的数据库，其特点之一是自动按时间顺序保存监控信息，易于按照某个时间段查询数据内容，二是时序数据库的写入性能非常高，适合保存大量主机集群的监控信息。监控数据存储模块工作流程图如图 2.9-2 所示。

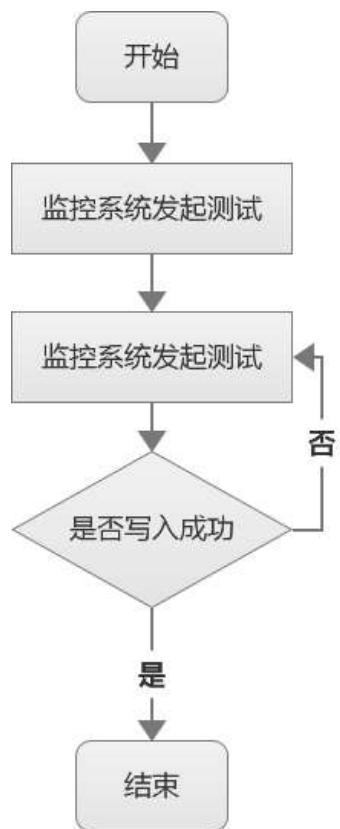


图 2.9-2 监控数据存储模块流程图

(4) 告警规则分析模块

告警规则分析模块是监控系统的核心功能，当系统内出现有主机或服务状态异常时，数据采集模块可以采集到相关的异常信息，送到告警模块进行服务告警，采用微信平台的方式通知对应的负责人处理系统异常情况。监控数据告警模块工作流程图如图 2.9-3 所示。

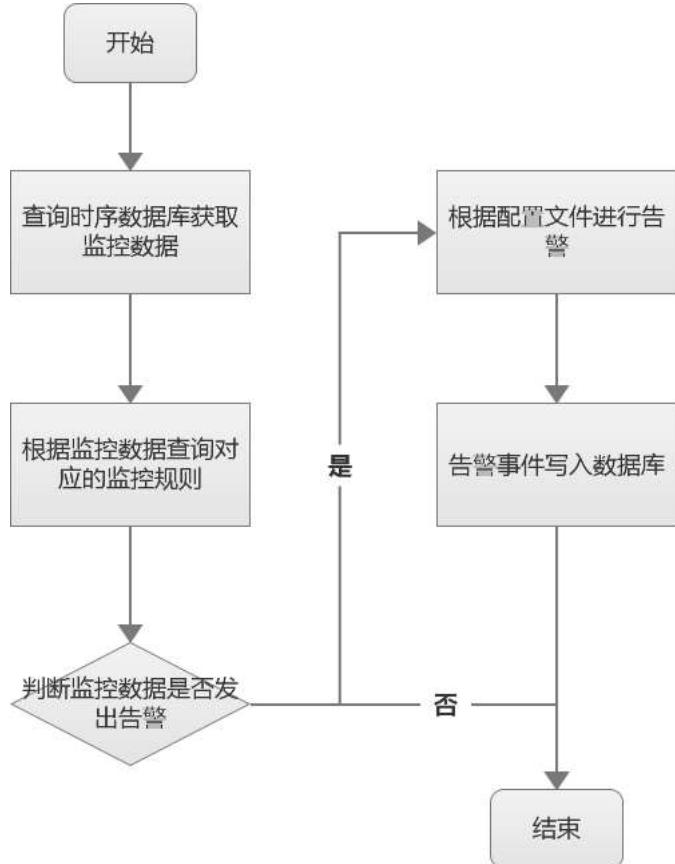


图 2.9-3 数据报警模式流程图

(5) 监控数据告警模块

监控数据告警模块是在判定服务发生异常时进行报警，将告警信息展示到展示页面，同时微信通知运维人员及时响应，将告警信息上传到平台。并向平台提供服务集群状态信息获取接口。

2.9.3.2 外部拨测系统

随着平台的投入使用，平台业务需求增长，对平台网络的通畅、稳定性提出更高的要求。管理平台几乎每时每刻都在运行，如果网络或业务出现问题不能及时发现，将会对平台造成巨大影响。为确保运维工程师在出现问题时及时知晓，快速定位问题原因，保障平台网络的平稳，需要建设网络服务质量拨测系统，收集并分析测试数据，监控平台网络链路是否通畅。同时也对业务进行拨测，监测平台运行状况。并及时向告警平台发送告警信息，帮助运维人员更好地维护平台。

服务。

(1) 网络自动拨测功能

网络拨测发送服务启动后，自动启动自动网络评测功能。并将测试结果记录到数据库中。如果测试结果异常，系统会进行告警（告警信息在前端页面展示，同时微信推送给指定人员）。平台网络自动拨测流程图，如图 2.9-4：

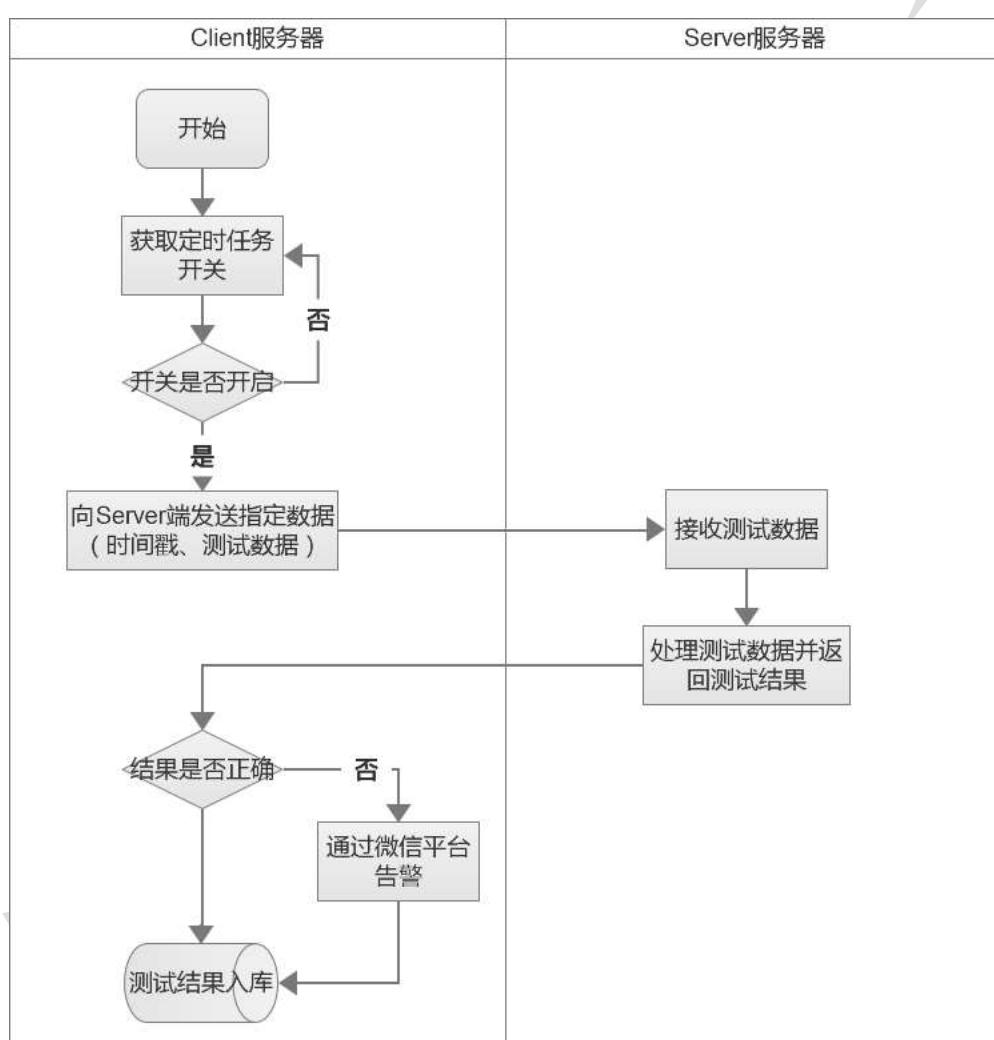


图 2.9-4 网络自动拨测流程图

(2) 网络手动拨测功能

在运维系统操作界面，可用手动启动网络拨测任务。待拨测任务结束后，系统操作界面显示测试结果，并将测试结果保存到数据库中。
(手动拨测不推送告警提示)

网络手动拨测流程图，如图 2.9-5：

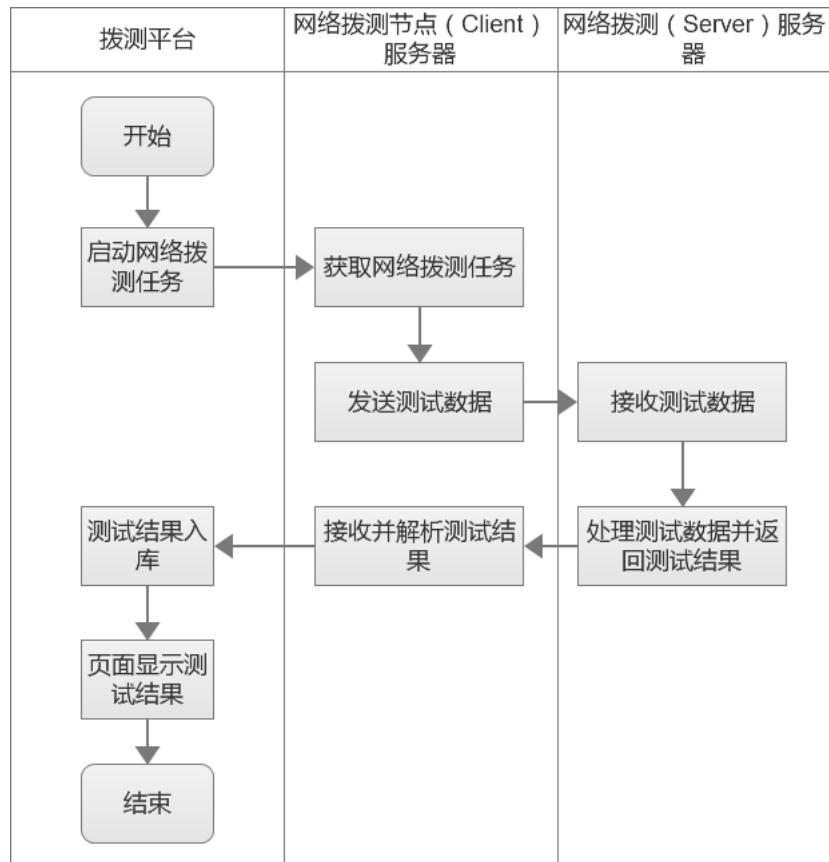


图 2.9-5 平台网络手动测试流程图

(3) 网络拨测结果查询

可以根据时间范围、网络类型、测试结果对网络拨测记录进行查询并显示在操作界面中。

网络拨测结果查询，如图 2.9-6：

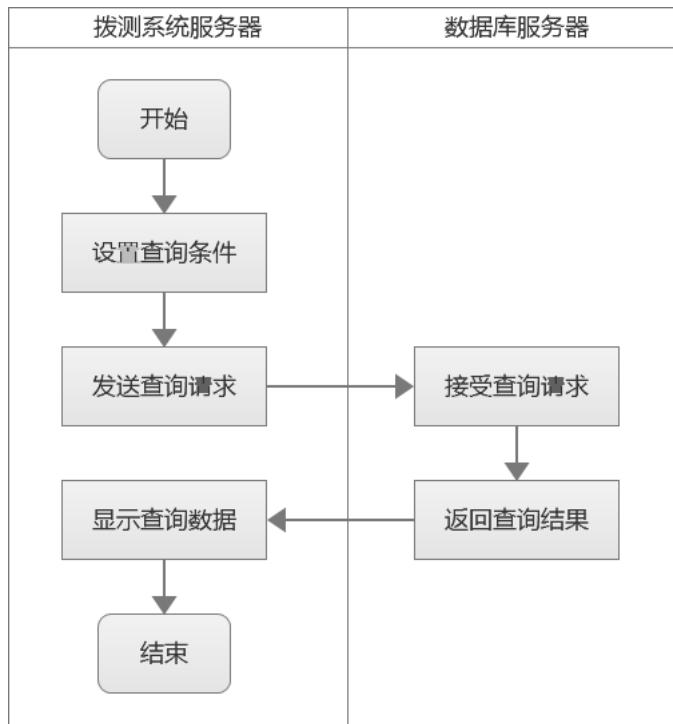


图 2.9-6 网络测试结果查询

2.9.3.3 网络链路流量监控系统

主要是针对网络运维而设计的一体化流量分析处理监控系统。通过对网络各关键节点流量的统一采集、统一分析处理，实现对网络流量、网络传输质量的可视化监控与分析；同时还能够对流量进行深度解析，产生各维度的运维关键指标数据，从而为运维大数据系统提供高价值数据，为自动化运维提供历史数据。

(1) 网络链路配置和解析功能

配置功能是用于配置网络节点和网络节点间的访问链路，通过配置 ip+port 方式指定网络节点，通过服务端网络节点+客户端 ip 制定网络链路。

分布式大型系统的节点往往多而复杂，应用的调用关系更加错综复杂，通过配置到系统中，进行统一管理识别。

网络链路解析功能是通过配置网络链路节点与实际调用关系，规划各网络节点之间的调用关系拓扑图。

(2) 网络链路信息汇聚

根据链路配置信息，通过定时获取网络链路的实时关键指标信息，将其存入时序数据库中，为后期的链路分析提供数据基础。

(3) 网络链路性能分析

网络链路性能分析是将获取到的应用数据进行整合，进一步的探索数据的价值，对数据进行多时段、多指标的综合分析。

(4) 告警检测

通过对服务的各项关键指标的进行实时检测，判断网络链路上各节点的状态，并且将异常状态记录到数据库。

(5) 网络链路实时状态

通过对链路配置信息的解析，绘制全链路状态实时拓扑图，并定时刷新。

(6) 网络链路状态趋势图

通过对于网络链路数据的实时分析定制数据近期的状态变化图。

(7) 告警配置及告警

为网络链路的各个节点及通道配置相关关键参数的告警阈值，从而定制化的设定告警的策略，极大的贴合运维需求。

2.9.3.4 日志快速查看服务

日志快速查看服务是为运维人员提供跨机器日志数据快速定位，查看并下载的一个运维工具。当服务出现错误时，运维人员可快速查看各个集群机器的错误日志，快速定位到错误产生原因，极大的缩减运维人员查找错误日志的耗时。日志查看系统流程设计如图 2.9-7。

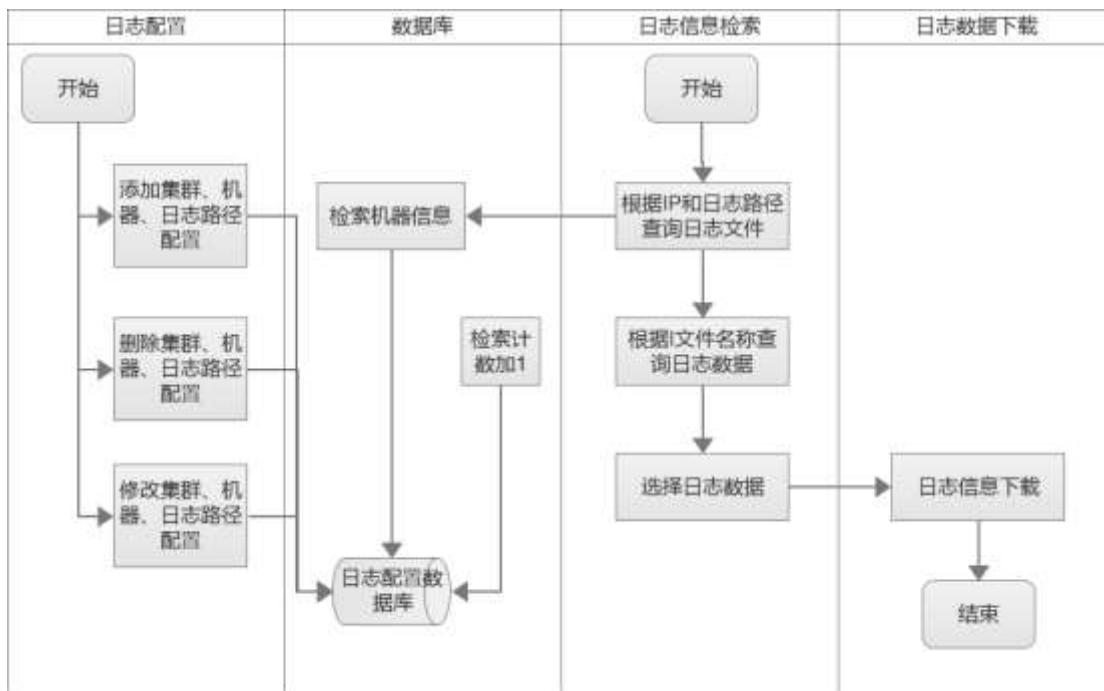


图 2.9-7 日志查看流程图

(1) 日志路径校验功能

输入机器 ip 和日志路径，根据 ip 查询机器配置库，查询出机器用户名、密码，调用 ssh 连接方法，验证该服务器是否有此路径，如果路径存在，检索该路径下所有文件、文件夹名称、创建时间以及文件大小；如果路径不存在，提示机器不存在此路径。

(2) 日志数据检索功能

查询出需要查看的日志文件后，后台先判断文件大小，如果文件大于 1MB，默认查询日志文件倒叙 200 行内容；如果文件小于 1MB，默认查询文件全部内容。如果默认查询没有查询到想要的数据，提供关键字、开始行数、结束行数、正序倒叙检索，这些检索条件可任意组合进行查询，并将检索条件一并在前端显示。前端页面提供选项卡功能，可显示多页面内容。

(3) 日志检索记录功能

每次日志文件检索都会将本次检索的 ip 和日志路径存储到检索历史库，如果库中没有该记录，将该记录存储到检索历史库，并将检

索次数计数设为 1；如果库中有此条记录，该记录的检索次数计数加 1。前端默认展示检索历史计数最高的 5 条(该条数可通过修改配置文件进行修改)数据，供使用人员更快速的检索常用日志文件。

(4) 日志数据下载功能

选择需要下载的日志内容，调用浏览器的下载功能，将选中的日志内容下载成 Excel，Excel 下载路径可选择。

2.9.3.5 自动化部署系统

主要是为运维人员在服务变更过程中提供标准化的流程，简化变更过程中的重复操作，降低操作过程中的误操作风险，同时加强对用户操作的细致化管理，降低安全风险，提供统一的服务管理平台。

(1) 服务目录管理

服务目录管理为所有约定的服务提供一个一致信息源，并确保具有相应访问权限的人可以使用这些信息，确保服务目录生成并得到维护，同时包含所有已经运营和正准备运营的服务的准确性。

服务目录成功写入以后，可以查询受控服务器的服务部署信息（包括部署服务器 IP 地址，服务集群名称，服务名称，服务版本号，服务状态等信息），并且可以控制服务的更新状态（主要指版本更新）。服务在“锁定”状态时，不允许用户对服务进行更新。只有服务在“等待更新”状态时才允许用户通过本系统对服务进行更新。

(2) 安装包管理

对服务部署需要的安装包进行管理，实现安装包的上传部署，启动，停止，重启，卸载与回滚等功能。

服务的部署与更新，必须通过运维管理员先将待修改服务的“更新状态”设置为“等待更新”，应用管理员才可以在远程部署与更新页面，看到需要部署或者更新的服务。此功能解决了因应用管理员没

有通知运维管理员，而直接修改集群内服务器上面服务的情况，导致运维管理员对当前服务器运行的服务部署与更新不了解的情况。

(3) 计算机密码管理

通过对服务器账户和密码的管理，可避免未授权的情况下部署和更新服务，以至于改变平台生产环境。

(4) 操作审计日志

运维管理员可以在审计日志浏览页面，查询各项操作的记录日志，方便运维管理员实现精确追踪、还原操作人员行为审计。对于安全分析、资源变更追查，合规审查有非常重要的作用。

2.9.3.6 监控信息汇聚平台

主要是汇聚平台各个系统的数据进行统一的汇聚展示，针对运维系统众多的分支系统，各自有自己的功能，对系统整体运行情况详尽统计，同时解决运维人员需要查看的内容过多占用了大量精力。

信息汇聚接口包括：

- ◆ 基础设施监控接口
- ◆ 应用监控接口
- ◆ 安全监控接口
- ◆ 网络监控接口
- ◆ 子系统概况信息接口

上述信息统一汇聚展示，统一告警，统一记录。

三、服务接口

3.1 数据汇聚分发系统接口

参见各业务子系统设计。

3.2 跨网传输系统接口

参见各业务子系统设计。

3.3 综合信息管理系统接口

参见各业务子系统设计。

3.4 出入境查询推送接口

参见各业务子系统设计。

3.5 证件和人员信息签名验证接口

参见各业务子系统设计。

四、安全技术方案

4.1 安全设计目标

(1) 合规性

设计方案必须符合信息安全等级保护、密码法相关要求、与隐私数据相关的标准和法律以及公安行业要求等法律和规定。

(2) 安全性

设计方案必须结合业务系统的实际环境和安全需求采取适当的安全保护措施，体现“重点保护、适度安全”的原则。

(3) 高性能

设计方案必须满足业务应用系统对业务性能的要求，不能因为安全设计和安全措施的实施导致原有业务应用系统在性能方面的明显下降。

(4) 高可靠

设计方案必须从功能和结构上满足应用系统对可靠性和稳定性的要求，尤其注重增强系统的冗余和备份机制。

(5) 可扩展

平台结构和产品保证适度的弹性和可发展能力，适应业务未来一定时期阶段业务的变化和发展。

4.2 风险评估

4.2.1 国家工作人员因私出国（境）管理平台架构

“国家工作人员因私出国（境）管理平台”涉及四类网络环境：

- (1) 证件保管柜（单位本地网络）；
- (2) 互联网；
- (3) 公安网；
- (4) 组工网。



图 4-1：国家工作人员因私出国（境）管理平台架构图

“国家工作人员因私出国（境）管理平台”包含 9 个系统：

- (1) 证件保管柜；
- (2) 报备审批系统；
- (3) 数据汇聚分发系统；
- (4) 证件保管柜管理系统；
- (5) 跨网传输系统；
- (6) 综合信息管理系统；
- (7) 密钥管理系统；
- (8) 展示系统；
- (9) 运维系统。

4.2.2 威胁和风险分析

外部的威胁主体可能影响系统的机密性、完整性和可用性。

经过分析，系统的威胁主要包括：

- (1) 证件保管柜本地数据泄露；
- (2) 互联网传输中数据泄露或篡改；
- (3) 系统业务组件失效不可用。

其中，系统性的数据泄露对管理平台的影响最大；其次，局部数据泄露、出现伪造证件保管柜、系统级组件失效不可用也会对管理平台带来一定威胁。

4.3 安全需求

系统安全需求由业务需求和风险决定，包括：

- (1) 证件柜安全；
- (2) 数据存储安全；
- (3) 数据传输安全；
- (4) 互联网系统平台安全；
- (5) 隐私数据泄露风险；
- (6) 系统可用性风险。

4.3.1 证件保管柜设备认证

“证件保管柜管理系统”仅允许合法的、经认证的证件保管柜接入。因此，合法“证件保管柜”需要通过系统的身份认证。

“跨网传输系统”仅接收具有合法身份的证件保管柜产生的证件和人员信息，因此每个证件保管柜产生和上报的证件和人员信息都要能够认证和溯源。

以上要求防止伪造和假冒的证件保管柜连入系统中。

4.3.2 保障数据传输安全

“证件保管柜”产生的证件和人员信息需要以密文形式传输，通过“数据汇聚分发系统”和“跨网传输系统”到公安网内的“综合信息管理系统”存储并使用。

数据在互联网的传输过程中要保障机密性和完整性。

4.3.3 保障数据存储安全

“国家工作人员因私出国（境）管理平台”中要避免证件和人员信息通过互联网或证件保管柜本地网络泄露。

数据的存储中要保障机密性和高效的备份机制。

4.3.4 公安网平台安全要求

互联网端“跨网传输系统”和公安网端“综合信息管理系统”是“国家工作人员因私出国（境）管理平台”的重要组成部分，其自身在网络、设备、管理、策略、数据等多个方面要具备相应安全能力和级别，以保障“国家工作人员因私出国（境）管理平台”业务功能正常运转。

4.3.5 保障系统高可用

“国家工作人员因私出国（境）管理平台”高可用性主要要求：

- 1、证件保管柜支持网络连接失效状态下使用；
- 2、数据汇聚分发系统的架构按照高可用设计；

跨网传输系统的架构按照高可用设计。

4.4 安全方案

4.4.1 数据分级、分类

系统涉及两级、三类数据：

- (1) 公开数据（状态和同步信息）；
- (2) 专有数据（证件信息、人员和组织信息等）。

专有数据不能在互联网环境存储和明文传输，必须要安全处理并传输到公安网内存储；公开数据可以不受限制在互联网环境存储和传输。

4.4.2 密码设备

4.4.2.1 安全模块

安全模块为证件保管柜提供本地数据保护、数字信封、数字签名、数据验证等功能；安全模块的形态包括低功耗加密卡、UKey等。

4.4.2.2 签名验证服务器

签名验证服务器为平台提供数据保护、数字信封、数字签名、数据验证等功能。

4.4.3 证件保管柜安全

(1) 数据安全

“证件保管柜”主板上嵌入安全芯片，芯片包含：数据加密、Mac 密钥和身份认证密钥。密钥用以保护“证件保管柜”内部存储的证件和人员信息，并可以识别、排除非法“证件保管柜”接入“证件保管柜管理系统”。

(2) 物理安全

“证件保管柜”柜体结构采用加固设计，实现防拆卸和较强的抗损坏能力。

(3) 系统安全

“证件保管柜”内采用专用的安全操作系统，系统资源优化，并对内部配置实现了一定的安全基线。

4.4.4 数据安全

(1) 证件和人员信息加密

“证件保管柜”产生的证件和人员信息通过数字信封技术打包为符合《GMT0010-SM2 密码算法加密签名消息语法规范》数字信封类格式，上传到“证件保管柜管理系统”中。

“证件保管柜管理系统”不具有将证件和人员信息解密的能力。

“证件保管柜管理系统”将打包的证件和人员信息通过“数据汇聚分发系统”转发给“跨网传输系统”，最终再进入公安网内“综合信息管理系统”存储并提供给组织部使用。

(2) 证件和人员信息认证

“证件保管柜”产生的证件和人员信息通过数字信封技术打包为加密格式后，还要利用安全模块生成并附带数字签名，一起上传到“证件保管柜管理系统”中；数字签名用以表示本条证件和人员信息来源于当前“证件保管柜”。

“证件保管柜管理系统”接收到打包的证件和人员信息后，用“数据汇聚分发系统”中的签名验证服务器再生成一个数字签名并附带到接收到的证件和人员信息后，转发给“跨网传输系统”；新生成的数字签名用以表示本条证件和人员信息由当前签名验证服务器转发。

“跨网传输系统”接收到每条证件和人员信息后，可以通过上述两个数字签名分别验证每条信息是由哪个“证件保管柜”生成、哪个签名验证服务器转发，掌握信息的全部生成和转发路径。

4.4.5 安全传输协议

管理平台各组件在互联网上利用 HTTP 协议传输应用数据，数据格式中包含机密性和完整性机制，格式如下。

4.4.5.1 请求格式

```
{  
    "version": "", // 协议版本  
    "mstype": "", // 业务数据消息类型  
    "c": {  
        "coding": "b64", // 数据编码  
        "reqid": "", // 请求 id(抗重放)  
        "time": "", // 时间戳(抗重放)  
        "sid": "", // 会话 id(抗 Dos)  
        "ai": "", // 安全机制  
        "ki": "", // 应用密钥索引  
        "ei": "" // 安全模块 id  
    },  
    "s": {  
        "env": "", // 数字信封(含接收者证书 id)或会话密钥  
        "sig": "", // 数字签名或 MAC  
        "rsig": "" // 转发数字签名或 MAC  
    },  
    "bdata": {  
        ... // 业务数据(明文或加密)  
    }  
}
```

4.4.5.2 响应格式

```
{  
    "code": ,  
    "desc": "",  
    "field": "",  
    "version": "", // 协议版本
```

```
    "mstype": "", // 业务数据消息类型
    "c": {
        "coding": "", // 数据编码 ("b64")
        "reqid": "", // 请求 id
        "ai": "", // 安全机制 ("认证机制+加密机制" 的组合)
        "ki": "", // 密钥索引
        "ei": "" // 安全模块 id
    },
    "s": {
        "env": "", // 数字信封 (含接收者证书 id) 或会话密钥
        "sig": "" // 原始签名 (含公钥标识和算法)
    },
    "bdata": {
        ... // 业务数据 (明文或加密)
    }
}
```

4.4.6 跨网数据传输

“跨网传输系统”实现下列数据传输通路：

- (1) 互联网到公安网的单向数据通路，实现互联网内的证件和人员信息传入公安网；
- (2) 公安网到组工网的双向通路，实现组织部内业务系统查询和操作公安网内存储的证件和人员信息。

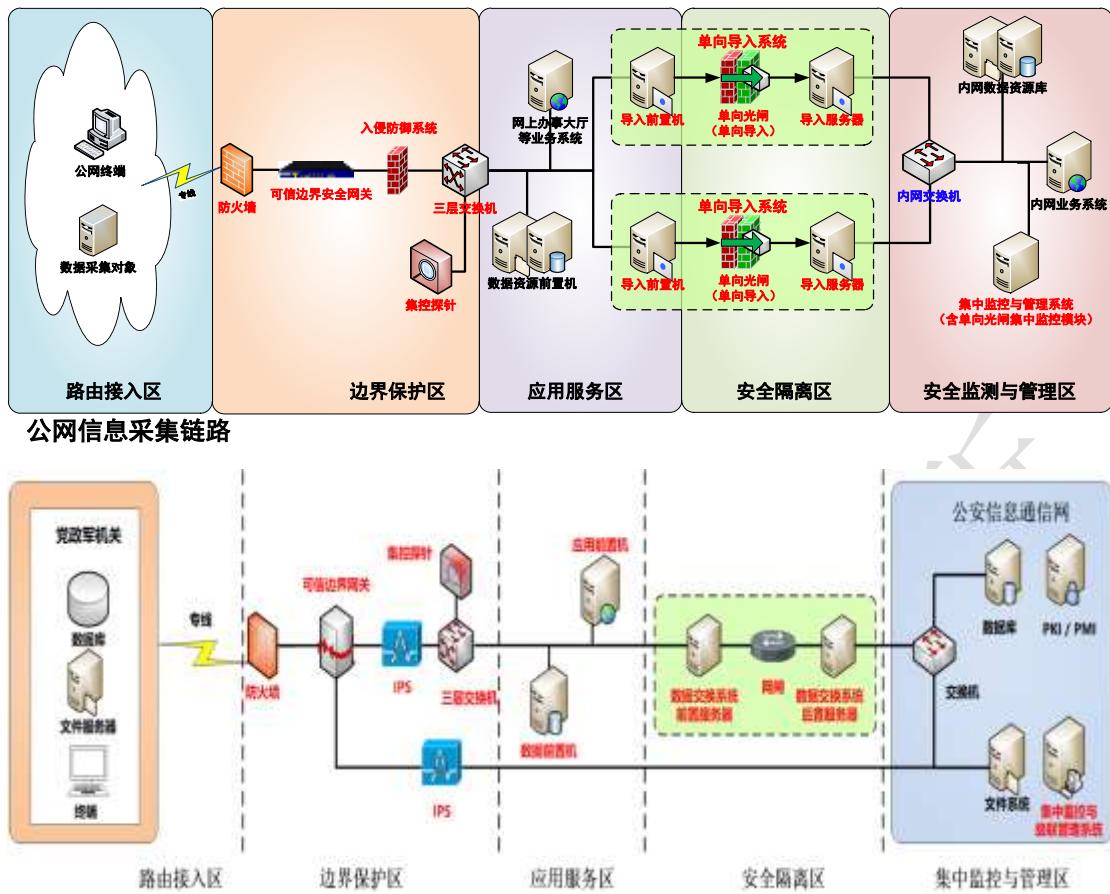


图 4-2：跨网传输系统架构

“跨网传输系统”中组工网与公安网数据交换通路依照《公安信息通信网边界接入平台安全规范（试行）》（2007年10月）设计和建设。

“跨网传输系统”中互联网与公安网数据交换通路依照《公安信息通信网边界接入平台安全规范—公网信息采集部分》（2013年11月）设计和建设。

“跨网传输系统”遵循《GB/T 22239 信息安全技术 网络安全等级保护基本要求》第三级标准设计和建设；

4.4.7 公安网系统加固

针对数据存储、传输和应用三个风险环节，公安网内“综合信息管理系统”设计、实施了一套数据安全加固策略，包括：

- (1) 分级存储、物理隔离、数据加密、个人信息去标识等；
- (2) 安全域隔离、单向边界交换、数据处理管控、数据传输保护等；
- (3) 身份鉴别和访问控制、数据脱敏、数据爬取防护、安全监控和审计等。

4.4.8 密钥管理系统

密钥管理系统的功能是：

- (1) 建立根密钥和密钥体系；
- (2) 安全模块模块和签名验证服务器签名证书生成、分发和管理；
- (3) 安全模块模块和签名验证服务器内加密密钥和 Mac 密钥的生成、分发和管理；
- (4) 实现主密钥备份和密钥树恢复机制；
- (5) 实现安全模块模块损失后的补发密钥和证书；

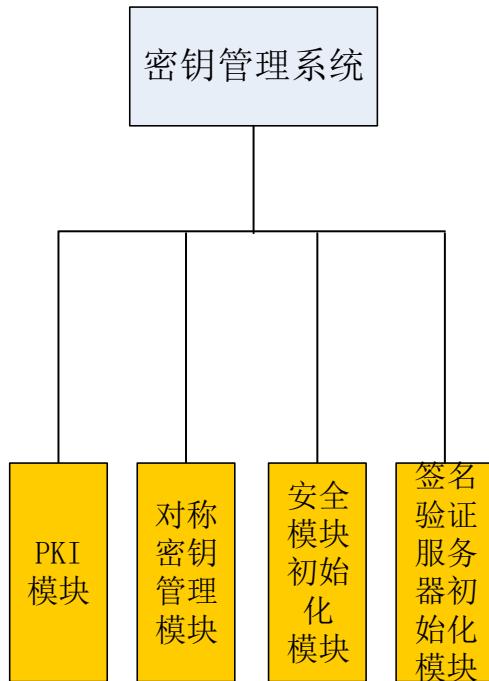


图 4-3：密钥管理系统功能组成

“密钥管理系统”主要负责生成、管理护照柜的数字证书和数据保护密钥；

初始化模块完成密钥承载安全模块和签名验证服务器的证书和密钥初始化工作。

4.4.8.1 PKI 模块

PKI 模块实现安全模块模块和签名验证服务器签名证书生成、分发和管理。安全模块模块和签名验证服务器解决证件保管柜身份认证，以及信息传输认证和溯源。

PKI 模块包含 CA 和 RA 等功能单元。RA 包括四类证书申请模板：（1）签名验证服务器签名证书模板；（2）签名验证服务器加密证书模板；（3）低功耗加密卡签名证书模板；（4）UKey 签名证书模块。CA 首先初始化根证书，之后进入工作状态，可以对 RA 的证书

申请进行签发。

4.4.8.2 对称密钥管理模块

对称密钥管理模块实现安全模块模块和签名验证服务器内加密密钥和 Mac 密钥的生成、分发和管理；对称密钥管理模块解决证件保管柜本地数据机密性，Mac 密钥实现数据验证。对称密钥管理模块包含密码机和密钥管理服务程序。

密钥管理服务根据签名验证服务器、安全模块模块的设备参数计算生成相应的加密密钥和 Mac 密钥，通过不同的驱动程序写入签名验证和安全模块的相应位置；密钥管理服务配套密码机作为密钥存储和备份恢复机制。

4.4.8.3 安全模块初始化模块

安全模块初始化模块为低功耗加密卡和 Ukey 生成私钥和数字证书、本地数据保护密钥、Mac 密钥。

4.4.8.4 签名验证服务器初始化模块

签名验证服务器初始化模块为签名验证服务器生成私钥和数字证书、本地数据保护密钥、Mac 密钥。

4.5 安全合规

“国家工作人员因私出国（境）管理平台”建设遵循《GB/T 22239 信息安全技术 网络安全等级保护基本要求》；
“国家工作人员因私出国（境）管理平台”密码设计和使用遵循《GM/T 0054-2018 信息系统密码应用基本要求》；

“国家工作人员因私出国（境）管理平台”敏感数据定性依照《GB/T 35273 信息安全技术-个人信息安全规范》和《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。

“跨网传输系统”中数据交换通路依照《公安信息通信网边界接入平台安全规范（试行）》（2007年10月）以及《公安信息通信网边界接入平台安全规范—公网信息采集部分》（2013年11月）设计和建设。

附录 1：标识生成规则

平台内各业务系统统一遵从标识生成规则，进行人员、证件和单位的统一标识。

人员标识生成规则：hash（GMSFHM 和 ZWXM 的拼接），其中
GMSFHM 为“公民身份号码”，ZWXM 为“中
文姓名”

证件标识生成规则：hash(ZJLX. ZJHM)，其中 ZJLX 为“证件类
型”，采用《常用证件代码 GA-T 517-
2004》标准，ZJHM 为“证件号码”

单位标识规则：单位的统一社会信用代码

附录 2：业务流水号生成规则

云安部
研究所