在线加解密
概要设计说明书

版本号：V1.0

2023-04-29

0、 修订历史

版本号	日期	修订人	修订记录
1.0	2023-04-29	chatty	初稿

1、 简介

1.1、目的

编制的目的是说明对程序系统的设计考虑，包括整体架构设计及描述，核心服务与功能的设计及描述。

1.2、定义和缩写

名词	解释

2、 需求概述

2.1、功能需求描述

- 铜锁在线加解密服务

  负责对数据进行 sm4,sm3,sm2 等加解密和验签等功能。

2.2、非功能需求描述

2.2.1、可移植性

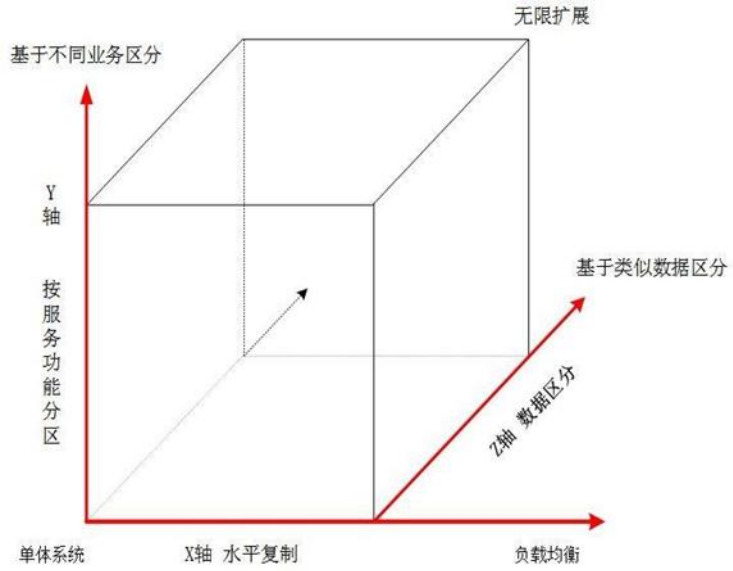
系统开发主要采用 SpringBoot + Vue 前后端分离技术，语言平台是 J2EE 平台系，支持简化的、基于组件开发模型，由于 J2EE 基于 Java 编程语言和 J2SE 平台，它提供了编写一次，随处运行的可移植性。接口的设计除了车厂的个性化需求外，总体上采用通用的 Restful 技术和 Json 文本数据格式，很好的支持系统的可移植性。

2.2.2、灵活性

系统设计时充分考虑了系统的参数化配置，参数配置分为两部分，一部分是参数配置文件，一部分为数据库；大部分参数的修改在不重启系统的情况下可立即有效。

在接口方面，系统支持通过内部标准化的接口服务，为后续扩展提供方便。

2.2.3、模块化设计



微服务拆分方式：Y 轴所示方式，既按照不同的服务方式拆分。

微服务拆分要点：低耦合，高内聚，一个服务完成一个独立功能。

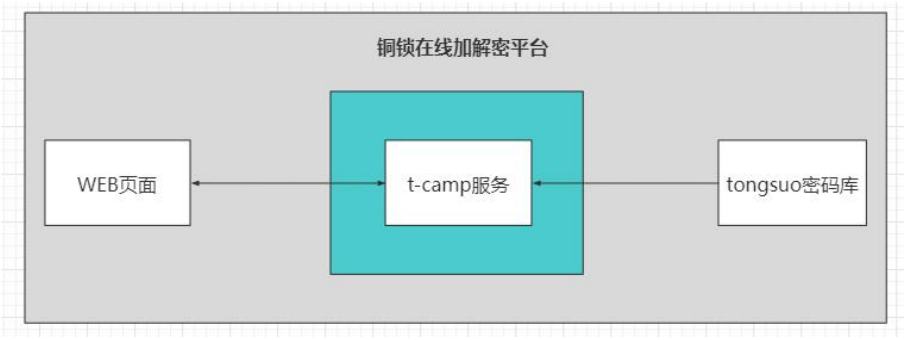
2.2.4、接口标准化

无状态协议 HTTP，具备先天优势，扩展能力很强。可支持安全加密 HTTPS 扩展，目前暂未扩展。

JSON 报文序列化，轻量简单，人与机器均可读，学习成本低，搜索引擎友好，语言无关，各大热门语言都提供成熟的 Restful API 框架。

3、 整体架构设计及描述

3.1、系统交互及描述

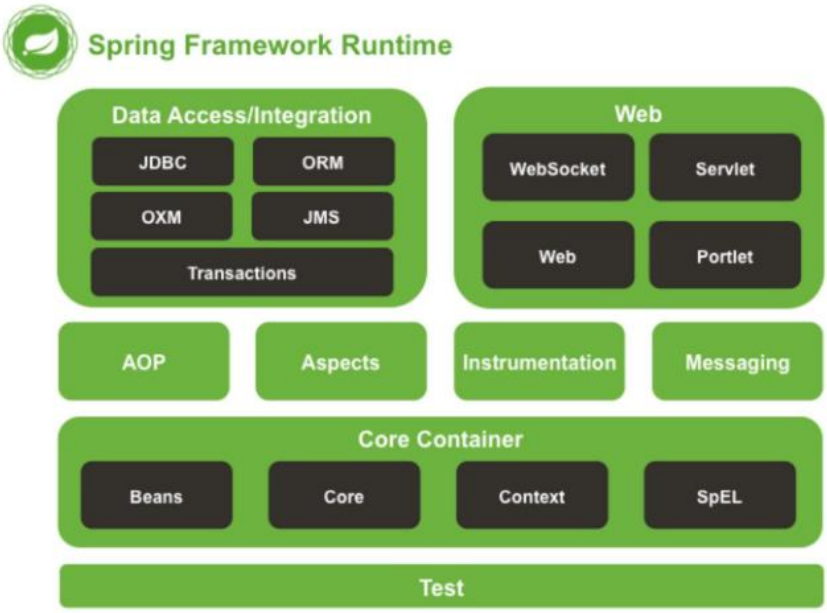


- Web 页面：用户操作页面。
- t-camp 服务：数据处理页面，跨语言转换。
- Tongsuo 密码库：采用 c 实现的加解密数据库，支持多种数据加解密。

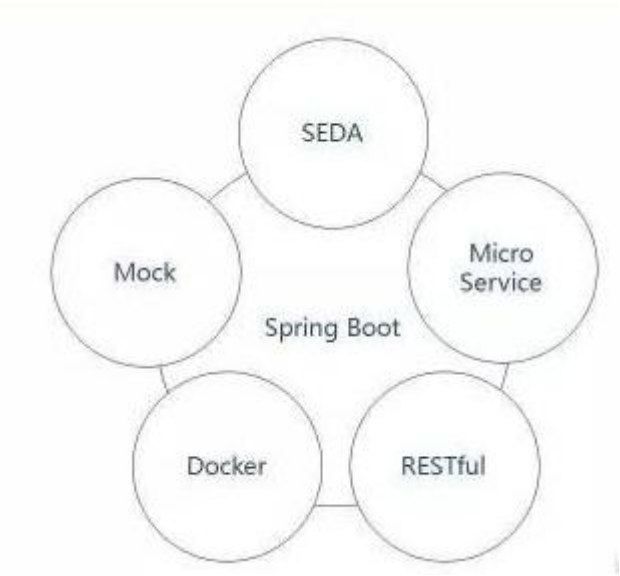
3.2、技术架构及描述

- Springboot 的技术和 spring 的匹配度很高。

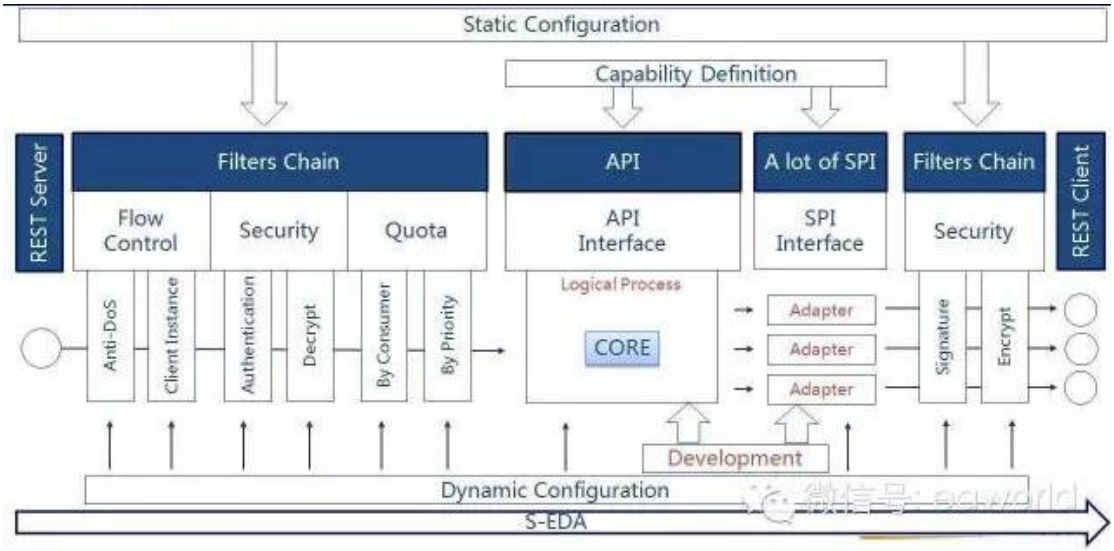
Spring Framework：即通常所说的 spring 框架，是一个开源 Java EE 全功能栈应用程序框架， spring boot 也依赖于此框架。



- Spring Boot 在平台中的定位，其相关技术融合。



- SEDA



整体是采用 SEDA，也就是 Stage-EDA。可以看到，整体是以处理顺序进行展示的，响应过程类似。在处理过程中，主要会有前置过滤，核心功能处理，后置过滤几大部分。

图中的过滤器都是可插拔式的，并且可以根据实际场景进行扩展开发。每个过滤器都是 Stage，比如 ClientInstance 合法性检查、调用鉴权、解密、限流等等。

一个请求 Stage 与 Stage 的转换，实现上是切换不同的线程池，并以 EDA 的方式驱动。

对于业务逻辑的开发者而言，只需要关心 CORE 部分的业务逻辑实现，其他的非功能都由框架进行统一实现。

- Docker 结合度很高

4、 核心服务与功能的设计及描述

4.1、t-camp 服务设计

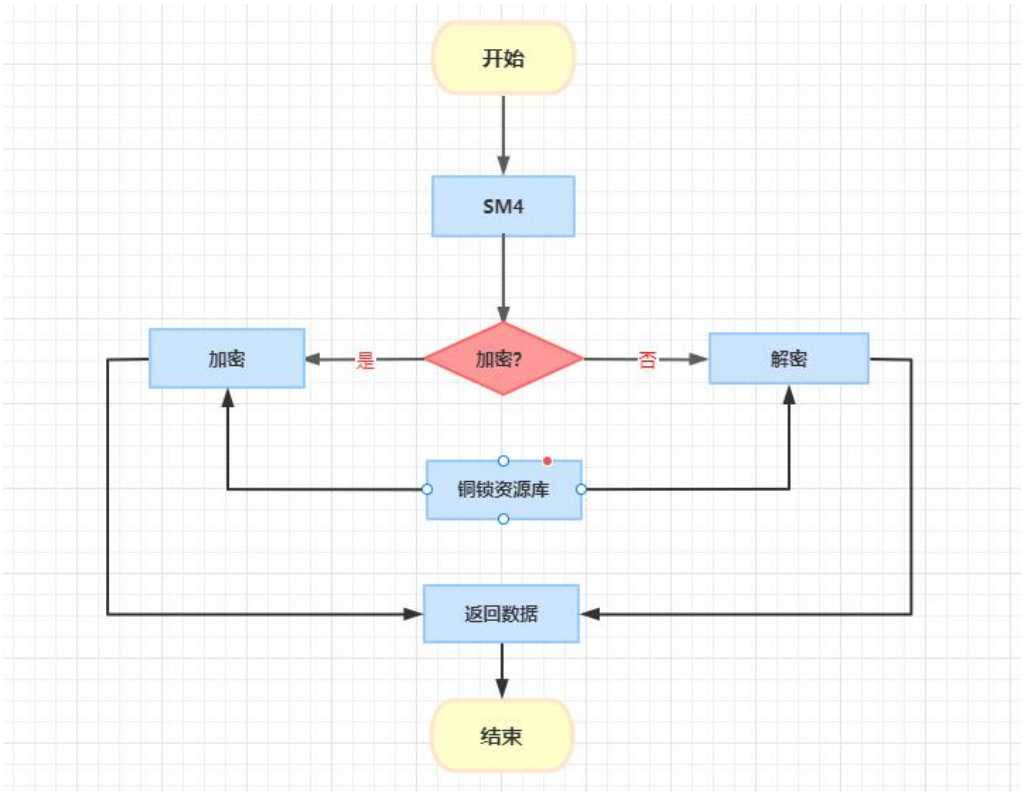
t-camp 服务是核心，web 页面的请求通过调用不同的接口，实现对数据的不同加密方式的加密，其中，sm4 支持数据的加密和解密；sm3 支持数据的加密；sm2 支持文件的签名和验签。

4.1.1、原理流程图

如下图所示，对于 sm4，当用户页面点击 sm4 时，支持 sm4 加密和解密，正常情况下，用户输入数据，输入加密的 key 即可生成对应的加密数据，拿到加密数据和 key 的用户也可以通过本页面进行数据的 sm4 解密。

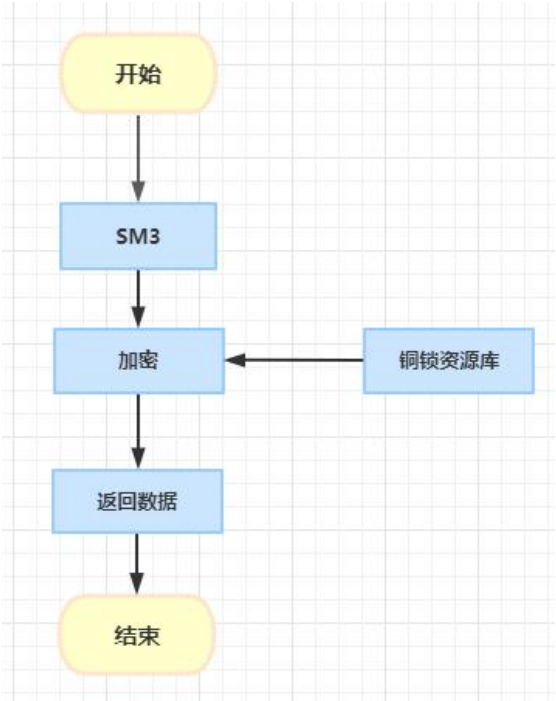
对于异常情况，如果用户的 key 和加密数据二者有一个不符合条件，就无法得到加密前的原始数据。

对于极端异常情况，如果系统出现问题，会返回系统异常描述。



如下图所示，对于 sm3，当用户点击 sm3 时，能够进入到 sm3 加密页面，该页面只支持数据的加密，加密后数据会生成在加密框中。

对于极端异常情况，如果系统出现问题，会返回系统异常描述。

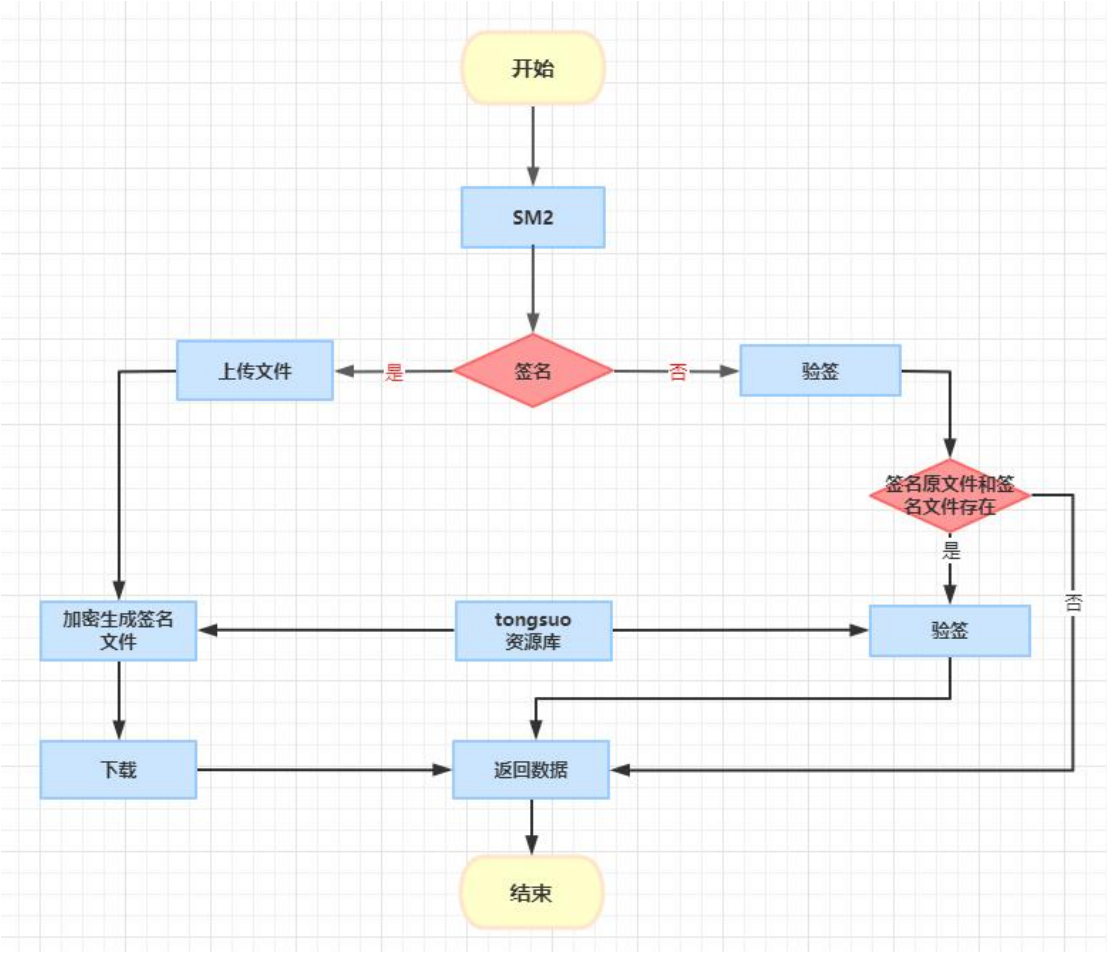


如下图所示，对于 sm2，可支持用户的文件签名和验签。

对于签名，用户在上传原文件后，服务调用 tongsuo 密码库对数据进行签名，并将签名文件返回个前端，供用户下载使用。

对于验签，需要用户上传原文件和签名文件，上传后用户点击验签按钮，系统会给出签名 ok 或者 error 的提示。Ok 表示验签通过，error 表示验签不通过。

对于极端异常情况，如果系统出现问题，会返回系统异常描述。



4.1.2、流程描述

1. 用户可以在页面端选择三种加解密页面。

2. 不同页面可实现不同的数据加解密功能。

3. 点击按钮即可获取对应的数据。

4.2、异常设计

项目采用统一的异常拦截器，不将异常抛出给客户。而是转化成错误码返回给客户端。

返回值	信息	描述
200	操作成功	Valied OK
300	操作失败	Valied Error
4000	输入参数错误	
4001	身份认证失败	
4003	访问被拒绝	
4004	资源未找到	
4005	不支持的请求方法	
500	系统异常	