中国科学技术大学

专业硕士学位论文

(工程硕士）



**基于领域驱动的第三方支付清结算系统的设计与实现**

作者姓名： 杨武

专业领域： 软件工程

校内导师： 孙广中 教授

企业导师： 杜经纬 专家工程师

完成时间： 二〇二三 年 九 月 八 日

University of Science and Technology of China

A dissertation for master’s degree

(Master of Engineering)



**Design and Implementation of Third-party Payment and Settlement Systems Based on Domain Driven Design**

Author：Yang Wu

Speciality：Software Engineering

Supervisor：Associate Professor. Sun Guangzhong

Advisor：Senior Engineer. Du jinwei

Finished time: September 8, 2023

中国科学技术大学学位论文原创性声明

本人声明所呈交的学位论文,是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外，论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

作者签名：\_\_\_\_\_\_\_\_\_\_\_ 签字日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

中国科学技术大学学位论文授权使用声明

作为申请学位的条件之一，学位论文著作权拥有者授权中国科学技术大学拥有学位论文的部分使用权，即：学校有权按有关规定向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅，可以将学位论文编入《中国学位论文全文数据库》等有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。本人提交的电子文档的内容和纸质论文的内容相一致。

控阅的学位论文在解除后也遵守此规定。

□公开 □控阅（\_\_\_\_年）

作者签名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 导师签名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

签字日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 签字日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**摘 要**

在移动互联网技术迅速发展和全球移动支付行业持续增长的背景下，我国移动支付市场正在经历前所未有的快速增长，并取得了显著的成就。我国政府高度重视支付清结算行业的发展，支付清结算技术发展迅猛，产业规模不断扩大。第三方支付清算平台在我国支付清算行业中的地位日益重要，其在提供便捷支付服务，推动数字经济发展和普惠金融方面的贡献不可忽视。然而，随着交易规模和业务的不断扩大，第三方支付清结算系统的复杂性、稳定性和扩展性问题面临挑战，而传统的基于数据库开发模式的清结算系统，业务逻辑依赖数据模型而不是业务模型，导致系统与业务逻辑紧密耦合，难以适应市场业务需求的快速变化，系统开发和维护成本居高不下。

滴滴作为领先的出行公司，在国际化转型的过程中，其国际化支付面临着巨大的交易量和复杂的海外支付环境等挑战，对支付架构的迭代效率及扩展性要求苛刻。由于原来的支付系统不能适应当前海量的交易数据，为此需要对其进行重构设计，建设稳定高效的国际支付中台。

为了解决上述问题，本文基于对国内外支付清洁算系统架构的分析与研究，结合滴滴国际支付清结算系统的业务需求，提出了一种基于领域驱动设计的清结算系统设计与实现方案。

清结算系统的工作内容和研究重点如下：

1. 根据领域驱动设计思想，对清结算系统进行需求分析，将系统划分为不同层级和模块，使用建立统一语言（Ubiquitous Language ）分析领域事件、聚合根、实体、值对象、仓库和服务等模型元素，设计清结算领域模型。
2. 根据支付中台清算业务需求，使用UML统一建模语言，分析清结算系统子模块的静态结构和动态结构，设计清结算系统核心类图、顺序图、业务活动图和状态图等图表。
3. 采用主流后端技术，如SpringBoot、MyBatis、Apollo和Rocket等框架技术开发系统，并采用JUnit5测试框架对系统进行测试。

该系统已经部署在实际生产环境中使用，通过配置化功能，系统能够满足不断变化的商户资金结算服务，后期配置维护十分方便，提高了系统的可扩展性；同时采用领域驱动设计的系统以领域模型为核心，能够及时响应市场需求变化，降低了后期系统的开发维护成本。

**关键词：**第三方支付 清结算系统 领域驱动设计

**ABSTRACT**

Against the backdrop of rapid development in mobile internet technology and sustained growth in the global mobile payment industry, China's mobile payment market is experiencing unprecedented growth and has achieved significant success. The Chinese government attaches great importance to the development of the payment clearing industry, with rapid technological advancements and continuous expansion of the industry scale. Third-party payment clearing platforms are becoming increasingly important in China's payment clearing industry, contributing significantly to providing convenient payment services, promoting digital economic development and inclusive finance. However, as transaction volume and business continue to expand, third-party payment settlement systems face challenges regarding complexity, stability and scalability. Traditional database-based settlement systems have business logic that depends on data models rather than business models which results in tight coupling between system and business logic making it difficult for them to adapt quickly to changes in market demand leading to high costs for system development and maintenance.

As a leading transportation company undergoing internationalization transformation process, Didi's international payments carry all its outbound businesses including ride-hailing services, food delivery services as well as financial services facing huge transaction volumes along with complex overseas payments environment posing stringent requirements on iteration efficiency & scalability of its payments architecture. Due to inability of original payments system being able to cope up with current massive transaction data volume; therefore there was a need for reconstruction design towards building stable & efficient International Payment Platform.

To address these issues mentioned above this article proposes a domain-driven design based settlement system design & implementation plan by analyzing domestic & foreign pay-clearing system architectures combined with Didi’s international pay-clearing system’s business needs.

The work content & research focus areas of this settlement system are:

1) Based on domain-driven design thinking analyze requirements for pay-clearing systems dividing it into different levels/modules using Ubiquitous Language (UL) model elements such as domain events/aggregates/entities/value objects/repositories/services etc., designing Pay-Clearing Domain Model

2) Using UML Unified Modeling Language according to payment center clearing business requirements, analyze the static structure and dynamic structure of pay-clearing system sub-modules, design Pay-Clearing System Core Class Diagrams, Sequence Diagrams, Business Activity Diagrams & State Charts etc.

3) Adopt mainstream backend technologies such as SpringBoot, MyBatis, Apollo and Rocket frameworks for developing systems along with JUnit5 testing framework. The system has been deployed in actual production environment using configuration function which can meet continuously changing merchant fund settlement services making it easy for post-configuration maintenance thereby improving the system's scalability; at the same time adopting domain-driven design based on a core domain model that can respond promptly to changes in market demand reducing later stage development & maintenance costs.

**Key Words:** Clearing Settlement System Third-Party Payment Domain-Driven Design.

**目 录**

[摘 要 I](#_Toc20127)

[ABSTRACT II](#_Toc30355)

[第1章 绪论 1](#_Toc31424)

[1.1 系统开发背景 1](#_Toc18764)

[1.2 国内外研究现状 2](#_Toc7905)

[1.2.1 国外应用现状与发展趋势 2](#_Toc8994)

[1.2.2 国内应用现状与发展趋势 3](#_Toc27982)

[1.3 解决的主要问题 4](#_Toc6191)

[1.4 本文主要工作 4](#_Toc4297)

[1.5 论文组织结构 5](#_Toc15096)

[第2章 相关技术及理论 7](#_Toc16744)

[2.1 通信协议与数据格式 7](#_Toc7247)

[2.1.1 超文本传输安全协议 7](#_Toc2404)

[2.1.2 JS对象简谱 7](#_Toc12153)

[2.1.3 抽象语法标记 8](#_Toc306)

[2.2 体系结构与框架 8](#_Toc23626)

[2.2.1 B/S三层架构 8](#_Toc17832)

[2.2.2 开发框架 9](#_Toc5970)

[2.3 国家商用密码算法 10](#_Toc16373)

[2.3.1 SM2非对称加密算法 10](#_Toc22617)

[2.3.2 SM3密码杂凑算法 10](#_Toc22199)

[2.3.3 SM4分组加密算法 11](#_Toc18863)

[2.4 技术标准 12](#_Toc6268)

[2.5 本章小结 12](#_Toc7975)

[第3章 需求分析 13](#_Toc13154)

[3.1 系统概述 13](#_Toc14767)

[3.2 需求导出 13](#_Toc27326)

[3.2.1 通用需求导出 13](#_Toc9443)

[3.2.2 管理员需求导出 14](#_Toc748)

[3.2.3 业务人员需求导出 15](#_Toc9748)

[3.2.4 业务对象需求导出 16](#_Toc7357)

[3.3 功能性需求 16](#_Toc4243)

[3.3.1 安全管理员核心用例 17](#_Toc1297)

[3.3.2 业务员核心用例 19](#_Toc28992)

[3.3.3 业务对象核心用例 20](#_Toc25261)

[3.4 非功能性需求 22](#_Toc29612)

[3.4.1 性能需求 22](#_Toc15175)

[3.4.2 可扩展性与可维护性 22](#_Toc13661)

[3.4.3 易用性与可执行性 23](#_Toc21081)

[3.4.4 安全性需求 23](#_Toc8160)

[3.5 本章小结 24](#_Toc14148)

[第4章 系统概要设计 25](#_Toc26843)

[4.1 系统设计目标和原则 25](#_Toc17859)

[4.2 系统静态结构设计 25](#_Toc3896)

[4.2.1 拓扑结构设计 25](#_Toc12992)

[4.2.2 管理子系统设计 26](#_Toc10015)

[4.2.3 业务子系统设计 27](#_Toc20746)

[4.3 系统动态结构设计 29](#_Toc4706)

[4.3.1 管理子系统动态结构 29](#_Toc21628)

[4.3.2 业务子系统动态结构 30](#_Toc29049)

[4.4 本章小结 31](#_Toc20369)

[第5章 系统详细设计 32](#_Toc14668)

[5.1 详细设计目标 32](#_Toc18051)

[5.2 业务子系统设计 32](#_Toc31831)

[5.2.1 安全认证逻辑设计 32](#_Toc19550)

[5.2.2 系统安全通信设计 33](#_Toc10738)

[5.2.3 安全认证业务设计 35](#_Toc432)

[5.3 安全管理员模块设计 42](#_Toc23737)

[5.3.1 用户证书管理设计 42](#_Toc18880)

[5.3.2 MCA管理设计 44](#_Toc22900)

[5.3.3 业务CA管理设计 45](#_Toc29296)

[5.3.4 系统安全功能设计 47](#_Toc10725)

[5.4 业务员模块设计 49](#_Toc11317)

[5.4.1 RA管理设计 49](#_Toc23403)

[5.4.2 终端证书管理设计 51](#_Toc23241)

[5.4.3 证书模板管理设计 53](#_Toc26460)

[5.4.4 互联信息管理设计 55](#_Toc19594)

[5.4.5 系统业务功能设计 56](#_Toc15229)

[5.5 数据库设计 58](#_Toc5532)

[5.5.1 安全管理员数据模型设计 58](#_Toc19212)

[5.5.2 业务员数据模型设计 62](#_Toc30020)

[5.5.3 安全认证业务数据模型设计 66](#_Toc5423)

[5.6 本章小结 67](#_Toc13255)

[第6章 系统实现与测试 68](#_Toc20287)

[6.1 系统的部署实现 68](#_Toc24059)

[6.2 测试概要 69](#_Toc1741)

[6.2.1 测试概述 69](#_Toc25588)

[6.2.2 测试环境 70](#_Toc405)

[6.3 系统功能测试 71](#_Toc5539)

[6.3.1 测试需求 71](#_Toc11802)

[6.3.2 测试设计 72](#_Toc21637)

[6.3.3 测试结果 77](#_Toc2241)

[6.3.4 优化策略 77](#_Toc20676)

[6.4 系统非功能测试 78](#_Toc30978)

[6.4.1 测试需求 78](#_Toc13353)

[6.4.2 测试设计 79](#_Toc2309)

[6.4.3 测试结果 80](#_Toc20910)

[6.4.4 优化策略 81](#_Toc21353)

[6.5 本章小结 82](#_Toc26306)

[第7章 结 论 83](#_Toc8201)

[7.1 工作总结 83](#_Toc9075)

[7.2 课题展望 83](#_Toc12265)

[7.2.1 不足之处 83](#_Toc6425)

[7.2.2 课题展望 84](#_Toc31172)

[参 考 文 献 85](#_Toc27454)

[致 谢 89](#_Toc25551)

第1章 绪论

1.1 系统开发背景

随着互联网和信息技术高速发展，我国移动支付市场蓬勃发展，并取得显著成绩。2022年，根据中国人民银行的数据，非银行支付机构处理网络支付业务1310241.81亿笔，金额 337.87 万亿元，反映了第三方支付清算平台在我国支付清算行业中的重要地位。2015年12月，中国人民银行发布《非银行支付机构网络支付业务管理办法》，制定了第三方支付机构进行网络支付业务的相关规定。2023年4月，央行指出要强化支付清算体系顶层治理，建设稳定高效的支付清算体系。以上政策和法规都表明了中国政府对支付清算行业的重视，以及对维护其安全、稳定运行的承诺。随着全球新一轮科技和产业革命的蓬勃发展，第三方支付清算行业将迎来新的机会，支付结算规模将不断扩大。

滴滴国际化经过三年多探索，业务遍布全球十多个国家，在中国互联网公司出海中出类拔萃。滴滴国际化支付承载着出行、外卖、金融所有出海业务，面临着每天千万级交易、数亿流水、质量及效率参差不齐的海外支付环境等挑战。然而，原有的支付清算系统并不能满足当前业务的发展需求，需要重新建设一个高效稳定的支付清算系统，以支持各种交易场景下的手续费、税费计费规则和结算提现规则，给商户提供高效稳定的资金结算服务。

清结算系统是支付系统的一个核心子系统，在第三方支付平台中承担着资金清算、结算和提现等资金处理业务，对资金处理准确性、系统可扩展性和可维护性等指标有着严格要求。稳定高效的第三方支付平台清结算系统，可提高平台的资金处理精确度和结算效率，显著提升平台的支付清结算服务能力[[1]](#footnote-0)[1]。然而，传统的基于数据库建模的软件系统，将系统业务与数据库表紧耦合，在业务需求、业务场景和政策多变的支付清算领域中，无法快速响应市场变化和进行敏捷开发，导致系统模块依赖关系复杂，模块职责边界模糊，后期开发和维护成本指数级增长。领域驱动设计作为一种应对复杂系统的软件建模方法，自2003年诞生以来一直受到软件社区的追捧，因其边界上下文（Bound Context，简称 BC）概念能够有效进行微服务边界的划分而在微服务时代广受欢迎。领域驱动是一套完整的软件设计理论，提出了一系列战略设计和战术设计概念，在20多年的实践发展中逐渐形成了领域驱动设计模式（DDDP）。

基于领域驱动的系统设计，能够有效管理系统的复杂性，应对不断变化的业务需求，保持系统的灵活性，具有较高的可扩展性和可维护性。

1.2 国内外研究现状

目前，国外的PayPal、Apple Pay、Google Pay等第三方支付具有广泛的影响力。特别是在欧美市场，这些支付平台被广泛使用。国内的支付宝和微信支付成为主导市场的两大巨头，也在全球范围内发挥着越来越大的影响力。然而，第三方支付的清结算系统架构属于公司内部信息，无法从外部文献资料中获取，并且各个公司根自身业务发展和技术水平采用不同的设计结构。因此，下面只对领域驱动设计进行分析研究。

1.2.1 国外应用现状与发展趋势

领域驱动是一种软件设计方法，它通过统一语言即模型在分析和开发阶段达成共识；通过分层架构划分软件结构；利用领域模型内聚业务规则等方法来解决大型软件开发过程中面临的复杂性问题。

在技术理论方面，领域驱动设计概念（Domain Driven Design，简称 DDD）自2003 年由软件建模大师 Eric Evance [6]首次提出以来，吸引着软件开发者社区的强烈关注,一度被认为是系统建模领域的圣经。越来越多的开发组织开始实践DDD，并出版了相关技术图书介绍其最佳实践。2006年，Jimmy Nilsson[7] 出版《Applying Domain-Driven Design And Patterns》，书中基于Martin Fowler (Patterns of Enterprise Application Architecture) 和Eric Evans (Domain-Driven Design) 对每个DDD原则给出清晰且注释良好的C#代码案例，并首次将领域驱动应用于实际的.NET项目中，为开发者指明了实践道路。2013 年，Vaughn Vernon在《Implementing Domain-Driven Design》中介绍了如何将 DDD 技术落地的实践指南[8]，提出了包括六边形架构、SOA、REST、CQRS、事件驱动等架构模式适应不同的软件建模需求。2015年， [Scott Millett](https://book.douban.com/search/Scott Millett) 在 《Patterns, Principles, and Practices of Domain-Driven Design》中提出使用战略模式构建有效的领域模型，使用战术模式来维护领域模型的一致性[9]，并提供了大量的最佳实践和模式来构建可维护、可扩展的软件系统。2018年，Scott Wlaschin 在《Domain Modeling Made Functional》中首次将 Functional Programming 与DDD 相结合来对现实需求建模[10]，设计出的软件可能比采用面向对象的方式更优雅更简洁。

在技术应用方面，2006年，Harald Wesenberg等人采用领域驱动设计来评估现成的第三方商业软件，发现在领域专家的帮助下，能够全面分析现有业务领域，将隐性的领域知识显示化和共享化，提高了沟通效率，节省了软件分析成本。2007年，挪威石油和天然气公司 Statoil ASA，准备设计一个新系统来支持石油和炼油产品的交易和供应业务。该公司采用领取驱动设计技术结合敏捷软件开发方法对遗留系统进行重构，重构后的系统提高了系统的性能和代码质量。2021 年，[Alam Rahmatulloh](https://ieeexplore.ieee.org/author/37087007622)[14] 等人将DDD应用到物联网监控应用的开发中，并表示采用DDD能很好的划分软件模块、准确定义系统服务，所开发的系统具有良好的扩展性和维护性；同年，PeterOukes[15] 通过研究荷兰土地管理系统发现应用领域驱动设计思想使土地管理系统中的各个模块解耦，通过事件源（Event Sourcing）实现更好的土地登记可追溯性、功能和系统互操作性。欧洲最大的在线时尚零售商之一的Zalando，基于分布式架构，围绕业务领域组织，采用领域驱动设计 (DDD) 实现“高内聚和低耦合”的微服务架构，以持续高质量的软件交付支撑业务持续增长。

以上研究表明，国外在领域驱动设计的理论研究和技术应用方面都处于前沿水平。在20年的理论到实践的发展过程中，已经形成一套完整成熟的软件设计理论和开发方法，在微服务和大型软件开发中有着广泛应用。

1.2.2 国内应用现状与发展趋势

国对领域驱动的关注比较晚，直到2008年才逐渐意识到其重要性，但很少将其应用到实际软件开发中。2008年，王忠等人在分析企业级应用系统开发现状时，提出基于数据库开发设计的软件开发方法已不能很好满足企业级系统开发，从理论层面分析了领域驱动设计软件开发方法的相关概念和开发流程[16]。2009年，郑琴琴结合领域驱动设计的思想开发实现了服装行业共享平台，结果表明领域驱动设计的思想使得平台能够快速响应需求的变化，有利于更好地维护[13]。

随着微服务的爆发，领域驱动因其界限上下文能为微服务的划分提供依据而大火起来。2015年，易立江基于领域驱动设计的思想建立了新型证券交易系统[17]。2017年，胡俊霞将领域驱动设计应用到企业信息化系统中，可解决系统的可维护性和可扩展性[18]。2021年，张帅基于领域驱动思想设计并实习了AGV调度系统，该系统已成功运用于十余个大型智能物流项目，能够满足实际应用需求，并且具有良好的扩展性、稳定性[19]。同年，黄喆基于领域驱动设计的银行存款业务核心系统，提高了银行业务处理的效率和正确性，降低了维护成本[20]。贾子甲等人通过应用系统文献综述的方法对2003年~2019年7月之间发表的领域驱动相关文献进行分析，研究得出领域驱动设计注重业务的领域知识，能够帮助开发者更好地进行软件设计[[2]](#footnote-1)[3]，并指出使用领域驱动设计能清晰地划分领域间的依赖关系、提升架构质量和促进业务专家和技术专家之间的沟通，并且以敏捷方式实现复杂架构的不断演进。

综上所述，国内关于领域驱动设计思想的认可度不断提高，相关理论研究也在不断深入，但实际企业级项目应用还不够广泛，各行各业也在此基础上不断学习和研究。支付清结算业务的特殊性意味着支付清结算核心系统使用领域驱动设计的思想进行开发和设计也是势在必行的。

1.3 解决的主要问题

本课题通过分析和梳理清结算业务的整体流程，理清清结算系统与各业务子系统的关系，将清结算逻辑活动从整个支付系统中独立出来，通过配置化手续费、结算规则和提现规则等，为商户提供各种的资金结算服务。在系统设计上，采用领域驱动设计思想，划分清结算领域模块，定义领域模型，使重构后的系统能够聚焦业务领域，适应快速变化的市场需求。同时，所开发的软件具有可维护性和可扩展性的特点，能节省后期软件开发维护成本。

1.4 本文主要工作

（1）领域驱动设计及其他技术理论研究。

分析研究领域驱动设计的相关理论技术，包括产生背景、基本原理、技术特点和适用场景四个部分，介绍清结算系统使用到的其它技术，为后续系统设计和建模做准备。

1. 清结算系统需求分析及概要设计

根据企业支付清结算业务的发展现状，分析清结算系统的业务需求。通过对业务场景和业务用例的分析，设计系统的功能性和非功能性需求。由于清结算系统是支付系统的核心子系统，故分析了整体的支付系统结构以及清结算与其他系统的依赖关系，然后结合领域驱动设计思想，设计清结算各个子领域的模型结构。

1. 清结算系统详细设计及功能实现

详细设计清结算系统核心模块：数据获取模块、清分模块、结算模块、异常处理模块的核心功能和业务流程，设计每个模块功能的活动图和状态图。

1. 清结算系统测试分析

通过单元测试和集成测试等方式对系统进行代码质量测试，验证系统是否满足业务目标和用例需求。

1.5 论文组织结构

本文共分为七章内容，各章组织内容如下：

第一章是绪论。本章介绍清结算设计开发的社会背景，分析国内外领域驱动设计的研究现状，同时介绍论文主要的工作内容和解决的主要问题。

第二章是理论及相关技术。本章分析研究系统设计与实现阶段采用的理论与相关技术框架，通过对其原理和特性的研究，表明其理论和技术的优点和适用性。

第三章是需求分析。本章从目前企业清结算业务需求出发，通过系统化和结构化的方法详细分析系统中的参与人员角色，从不同类型用户使用系统的角度分析系统需求。

第四章是系统概要设计。本章给出整体的支付架构图和清结算系统模块图，清晰展示清结算系统和各个系统之间的交互关系，对清结算系统内部的流程结构做了详细的设计。同时，介绍了该系统中数据库的逻辑结构和物理结构。

第五章是系统详细设计。本章将从系统模块角度出发，使用UML建模语言，详细设计各模块功能的具体实现，给出各个模块的领域模型、类型结构和流程图标等。

第六章是系统实现与测试。在系统设计并编程完成之后，需要按照前期提出的标准对系统进行的测试，覆盖软件开发测试过程和软件产品测试过程，包括产品功能、质量、技术文档等多方面，由测试结果判断系统的功能与性能是否满足了前期设计要求。

第七章是结论。对本次课题研究的工作成果进行各方面的总结，分析本次设计完成后仍有待改进的地方以及产生这些不足的原因，对未来一个时期内车联网信息安全体系的发展趋势进行展望。

第2章 理论及相关技术

2.1 领域驱动设计理论研究

本章首先研究领域驱动设计的相关理论和技术，分为产生背景、基本原理、技术特点和适用场景四个部分，然后介绍了清结算系统使用到的其它技术，阐述其特点及适用性。

2.1.1 领域驱动产生背景

（1）复杂性挑战

在软件开发中，软件的复杂性包括技术实现的复杂性和软件领域的复杂性，而后者往往是软件成败的关键。2023年，[Tashtoush Yahya](https://scholar.cnki.net/home/search?sw=6&sw-input=Tashtoush Yahya" \t "/Users/yangwu/Documents\\x/_blank)等人采用机器学习算法对软件可读性和软件复杂度进行实证研究，结果表明两者之间相互影响，是软件质量的重要组成部分[21]。2017年，何磊将McCabe圈复杂度和Halstead复杂度用于评估Java软件复杂度，设计实现基于代码复杂度的软件演化评估工具，对复杂度高的模块向开发人员预警，实现对软件复杂度指标的监控预警[22]。对于绝大多数的软件，最复杂的不是技术实现而是软件所研究应用的领域本身，即用户的活动和业务逻辑。在软件设计过程中，应该首先处理领域复杂性，对领域建模，再从领域出发做技术选型和设计。成功软件设计必须系统的处理软件的核心方面，它包括：1）在软件设计中，主要的关注点应该是领域和领域逻辑，而不是技术方法。2）领域驱动设计应该基于领域模型进行设计，并通过模型来处理领域复杂性。

（2）需求分析和设计的分离

在传统的瀑布模型中，软件需求分析和系统设计是分离的。1970年，[Winston W. Royce](https://en.wikipedia.org/wiki/Winston_W._Royce" \o ") 首次在论文中提出瀑布模型，并认为该模型存在重大缺陷，因为测试在开发结束后进行，有可能导致项目失败[23]。美国国防部于94年发布MIL-STD-498（军用标准软件开发和文档），开始明确反对瀑布式方式，转而采用迭代增量式开发[24]。瀑布模型的工作流程首先是领域专家将需求告诉给产品分析师，然后产品分析师消化吸收和抽象后再将需求转述给程序员，最后程序员翻译产品需求设计实现系统。这种单方向的工作模式必定失败的原因是建模过程中缺乏反馈，也即需求和设计的分离。产品分析师完全负责模型的创建，只接受领域专家的输入，然后进行抽象建模，没有从程序员中获得对模型的反馈意见，也没有获得软件先前版本相关人员的实际经验，导致领域知识的单向流动，没有在所有参与人员中获得积累。

1. 软件缺乏抽象

即便是采用迭代的方式开发软件，也不能保证领域知识在团队中得到良好的积累。在《Code Complete》中将抽象作为一种软件设计方法，它使我们以一种简化的观点来考虑复杂的概念，是处理系统复杂度的一种重要手段[24]。然而，现实中常见的场景是，开发者采用直接翻译需求的开发方式来处理软件需求，他们刚刚从领域专家得知某个需求后，就立马进行代码开发，然后将结果展示给领域专家并等待下一个需求。这种直译式的开发虽然能满足当前阶段的软件需求，但是由于缺乏对领域的抽象，开发者无法获得对领域的深入理解，总是限于新需求的被动之中，只知道应该做什么，而忽略了软件背后的领域知识。同时，由于缺乏对软件领域概念的抽象和建模，开发出来的系统只能满足当前使用，不可能从旧的功能整合中获得对系统的新的认识，导致系统缺乏扩展性。

2.1.2 领域驱动基本原理

针对上述软件开发设计的问题，领域驱动设计提出了以下软件建模的基本原理。

（1）基于领域模型的软件建模

领域模型是领域驱动设计的核心，软件建模围绕着领域模型进行设计。领域模型是对大量领域知识的总结概括和领域概念的抽象和简化，它反映了具体领域的核心关注点，是管理领域复杂度的有效方法。同时，领域建模是一个动态活动过程，它要求领域专家和技术专家持续紧密的合作，共同不断的精细化领域模型，分析人员和编程人员对领域知识进行抽象，构建领域模型以便于代码实现，领域专家将自己对领域知识的深入理解反应到领域模型中，保证领域建模是基于真实的业务原则进行的。领域模型作为团队成员的统一交流语言，将彼此对领域知识的认识集中反馈到模型中，降低了对领域知识的误解分歧，同时将需求分析和设计过程有机结合起来。

1. 基于职责分离的软件设计

一个完整的软件系统包含许多模块，各个模块的职责和关注点不同，为了保持领域模型的单一职责和干净独立的领域内涵，需要分离系统中与领域不相关的功能特性。为此，在领域驱动设计中采用分层架构，根据系统职责划分软件层次，隔离关注点，并通过领域元素构建领域模型，使领域模型具有清晰独立的领域含义。

（3）基于重构的领域模型优化

在设计的早期阶段，领域建模往往通过识别需求文档中的名词和动词来进行面向对象设计，把名词设计为对象，动词设计为对象的方法，这种过于简化的设计方法在面向对象的教学中被大家普遍接受。然而，实际上由于开始阶段缺乏对领域知识的深入理解，最初的模型往往停留在对象表面，不能反映领域专家主要的关注点和最本质的领域知识。在对领域模型不断重构优化，不断对领域知识加深理解的过程中，我们会发现新的领域概念，纠正错误的领域对象关系，或者删除多余的领域对象，使得领域模型不断接近领域知识的本质，与领域专家的理解和用户的真实需求保持一致。

2.1.3 领域驱动设计技术方法

领域驱动设计采用分层的设计方法，隔离领域对象和系统功能，同时对领域元素进行分类，明确了每类元素的职责范围，最后通过聚合、工厂和仓储对象管理领域对象的生命周期。

（1）隔离领域对象

为了处理复杂的任务，软件系统一般基于分层架构进行设计，将系统划分不不同层级，每层只关注当前层的任务，并且只依赖下层服务，这样设计的软件能够保持系统的高内聚低耦合特性，便于理解和拓展。领域驱动设计将系统划分为四个层次，分别是用户接口层、应用层、领域层和基础设施层，如图所示。

下面简要介绍每层的具体内容和职责范围。

1. 用户接口层（User Interface Layer）：用户接口层负责向用户展示信息以及接受用户的输入命令。
2. 应用层（Application Layer）：应用层定义了软件应用的具体任务，是很薄的一层，不包含具体的业务逻辑和业务状态，而是通过协调领域对象来实现任务目标，负责领域对象的编排管理。
3. 领域层（Domain Layer）：领域层负责定义业务概念，展示业务状态和业务规则信息。
4. 基础设施层（Infrastructure Layer）：基础设施层为高层提供通用的基础能力，比如消息发送、领域对象的持久化、缓存等能力。同时，其他层也可以通过依赖基础设施层进行间接的交互。

领域驱动设计分层的主要目的是保持领域层的独立性，领域层将领域相关的逻辑集中在同一层，与其他层分离，不关心领域对象的持久化、展示、应用任务等内容，能够专注于领域知识的表达，使得领域模型具有清晰的领域含义。

（2）领域模型元素

为了清晰地表示模型的不同组成部分，领域驱动设计定义了如下模型元素：

1）实体（Entity）

通过唯一标识（Identity）定义的对象称为实体，不同的实体通过唯一标识而不是实体的属性进行区分，同时实体的生命周期具有连续性。在设计实体模型时，实体的类型、职责、属性和关联关系都应该围绕着实体的唯一标识进行设计。通常通过工具UUID或者外部依赖生成全局唯一编号作为实体的唯一标识。

2）值对象（Value Object）

值对象用来描述模型的某个方面，没有概念上的唯一性，不同的值对象通过属性值进行区分。值对象是不可变对象，典型的值对象如数字、字符串、颜色等对象，它们一般作为参数在对象间传递，并且通常是瞬态的（transient），使用的时候被创建，完成后就销毁。值对象可以组合其他值对象或实体形成更大的值对象，同时也可以作为实体对象的属性。

3）服务（SERVICE）

服务以接口的形式表示领域操作，它独立于实体和值对象，并且没有封装状态。当某个处理方法或转换过程不属于某个实体或值对象的职责时，通常将该操作设计为一个无状态的服务，实现实体和值对象的概念完整性。服务按照不同的用途划分到不同的分层中，比如应用层服务负责接受用户输入、向领域服务传递参数和调用基础服务发送通知等，领域层服务调用领域对象来处理领域逻辑，基础服务负责发送邮件、消息通知等。

（3）生命周期管理

为了管理复杂对象的生命周期、维护对象的一致性状态和保持领域模拟的清晰独立，领域驱动设计提出来三种模式，包括聚合、工厂和仓储模式。

1）聚合（Aggreate）

聚合将一组关联实体和值对象组合成一个单元，定义了关联对象的边界和职责。聚合通过聚合根（聚合内部的一个实体）向外界提供访问内部对象的入口，对聚合进行访问控制。在整个聚合生命周期内，聚合根负责维护聚合内部对象的状态一致性和不变性约束（Invariant），防止对关联对象的修改因缺乏同步导致系统出现不一致状态。

2）工厂（Factory）

工厂将复杂对象或聚合对象的创建组装逻辑封装在工厂中，分离了对象的创建和使用职责。工厂位于对象生命周期的开始阶段，在创建聚合对象时强制保证聚合内部关联对象的不变性约束，实现客户端代码与具体类型的解耦。在实践中，一般使用简单工厂、工厂方法和抽象工厂设计模式来创建对象。特别的，工厂的每个创建方法必须是原子性的，并且在方法内维护对象的不变性约束。同时，工厂方法的返回类型应该与具体类型无关，一般设计为父类类型或接口。

3）仓储（Repository）

仓储封装了数据库操作和元数据映射的逻辑，使设计的重点保持在领域模型上，而不是陷于底层数据的操作细节。仓储将领域层与存储层解耦，为客户端提供一个的获取数据和数据生命周期管理的接口。仓储与工厂的关系比较复杂，它们既存在显著的不同点又彼此合作。首先，仓储与工厂的职责不同，工厂负责创建新对象，而仓储负责从数据库或其他数据源中恢复旧对象。其次，仓储与工厂的所处的对象生命周期也不同，工厂位于对象生命周期的开始阶段，而仓储位于对象生命周期的中间和结束阶段。在实践中，一般通过仓储和工厂合作的方式实现对象的创建和保存，如下图3-1和3-2所示。



图3-1 恢复旧对象



图3-2 保存新对象

2.2 相关技术与框架

2.2.1 Spring/SpingBoot

本文采用Spring、SpringBoot开发框架，理由如下：

1. Spring、SpringBoot 是当前主流的Java企业级开发框架，与同类开发框架相比，Spring提供了诸如IOC容器、AOP切面编程、事务管理和MVC模型等高级特性
2. SpringBoot 是Spring约定大于配置的解决方案，内嵌了Tomca或Jetty服务器而不需要单独部署WAR文件，其自动化配置功能使得开发人员可直接创建独立的、生产级别的Spring应用，大大降低了软件系统开发难度。

Spring框架设计结构如图所示：



2.2.2 MyBatis

本文采用MyBatis框架进行数据持久化，理由如下：

1. MyBatis 是一个优秀的持久层框架，它具有定制化 SQL、存储过程以及高级映射等特性。MyBatis 避免了几乎所有的 JDBC 代码和手动设置参数以及获取结果集的过程。MyBatis 可以使用简单的 XML 或注解来配置和映射原生类型、接口和 Java 的 POJO（Plain Old Java Objects，普通 Java 对象）为数据库中的记录。
2. MyBatis 相比 Hibernate 等全自动的 ORM ([Object Relational Mapping](https://en.wikipedia.org/wiki/Object%E2%80%93relational_mapping" \o "))框架，开发者可以根据业务场景自己编写SQL，进行SQL优化。特别适用于需要自由控制 SQL、复杂查询或者有性能要求的场景。因此，MyBatis为开发人员编写和优化SQL提供了更高的灵活性和控制度。

2.2.3 RocketMQ

本文采用RocketMQ消息中间架进行异步通信，理由如下：

1. RocketMQ 是Apache RocketMQ 顶级项目，具有高吞吐、高并发、顺序消息和事务消息、可靠的消息存储和传输、集群和分布式部署等特点。在实际开发中，RocketMQ适用于大规模消息处理、异步处理、应用解耦、流量削峰等场景，已经广泛应用在电商、金融、物联网等领域。在海量交易数据背景下，使用RocketMQ够提高清结算资金结算效率和系统稳定性。
2. 相比于其他消息中间件，RocketMQ拥有更丰富的功能。与 Kafka 相比，RocketMQ 的功能更为丰富，例如支持顺序消息、事务消息。RocketMQ 的可用性和容错性也相对较强，支持消息的事务性提交和回滚，在处理复杂业务逻辑时比较有优势；与 RabbitMQ 相比，RocketMQ 支持更高的并发和吞吐量；与 ActiveMQ 相比，RocketMQ 在处理大规模消息时，性能更优。在金融支付领域和清结算领域，对消息中间件的性能和可靠性要求严苛，而RocketMQ的高并发、顺序消息和事务消息的特点能够满足清结算系统的需求。

2.2.4 Apollo

本文采用Apollo配置中心作为清结算配置管理中心，理由如下：

1. Apollo开源分布式配置中心，提供了诸如分布式、实时更新、版本控制和权限管理等功能，具有使用简单、高可靠性和高可用的优点。在微服务架构中，由于服务数量增多，配置管理的复杂性增加，使用Apollo可以大大简化配置管理的工作。在清结算系统中，商户的手续费配置、交易方式配置、结算方式配置等各种配置通过统一管理在Apollo中，可以大大简化商户结算流程中的配置任务，提高了清结算系统的扩展性和灵活性。
2. 相比于其他配置中心，Apollo具有不同的优点。与 Spring Cloud Config 相比，Apollo 更注重配置的实时性，配置更改后可以立即推送到所有机器。而 Spring Cloud Config 默认情况下，配置更改后需要重启应用或者调用特定的刷新接口才能更新配置。清结算系统对时效性对时效性要求很高，需要及时的获取Apollo结算配置，计算商户交易手续费等各种费用，以提高商户资金结算时效。

2.2.5 XXL-JOB

本文采用XXL-JOB作为清结算任务调度中心，理由如下：

1. XXL-JOB是一款开源的分布式调度平台，提供了任务管理、调度器管理、日志查看、故障转移、执行器管理和通知报警等功能，具有简单易用、调度模式丰富、支持多种任务类型等优点，适用于大数据处理、游戏后台、金融电商项目等需要对任务进行定时调度的场景。在清结算项目中，需要定时清算和结算商户交易金额，需要定时对清结算流程中的异常事件进行重试，因此XXL-JOB分布式任务调度中心能很好的满足系统的定时任务需求。

2.5 本章小结

本章主要介绍了清结算系统开发中所用到的理论和技术，主要分为领域驱动设计理论和相关技术框架两个部分。通过分析对别其他相似技术和框架，剖析了选型技术的特征、优势和适用场景，并结合清结算系统的技术需求，阐述选择这些技术的理由。

第3章 需求分析

3.1 系统概述

为了解决A企业清结算业务的发展与当前支付清结算系统不匹配的问题，需要重新设计一套清结算系统来满足A企业国际化出行、外卖和钱包等上游业务的发展。本文设计了一套基于领域驱动的清结算系统，该系统能够支持商户结算业务相关的费用配置管理、结算配置管理、各种交易类型手续费的清算和结算和异常处理等需求。

本课题根据领域驱动设计思想，识别业务边界上下文，进而划分子域，然后再每个子域模块内设计核心领域构建元素，包括聚合根、领域服务、仓储等元素。同时，为了保证系统的可扩展性和可维护性，系统模块、接口和类的设计采用设计模式中的SOLID五大原则，提高系统复用性，尽可能降低后期开发维护成本。

3.2 需求导出

本次课题设计的清结算系统是支付系统的内部子系统，和清结算系统发生交互的有交易系统、运营系统和账户系统。完整的支付系统如图所示。



交易中心把商户交易数据通过消息中间件MQ异步发送到清结算中心，清结算中心通过订阅MQ获取交易数据，然后对交易数据进行数据处理等操作，为清结算流程准备数据源。运营平台在商户入网过程中，把商户计费配置和结算配置通过清结算中心提供的API下发到清结算配置数据库，为计费流程和结算流程提供相关配置参数。账户系统为了记录商户和平台清结算相关账户余额的变动情况，需要在计费和结算流程中记录相关账户的余额变化。为了保证商户资金安全和商户主体安全，风控系统需要对包含支付相关的商户交易和商户在清算和结算流程中，对交易数据进行风控校验拦截。交易系统、运营系统、账户系统、风控系统和清结算系统的系统依赖图如图所示。



清结算相关子系统交互顺序图如下。从时间先后顺序来看，交易系统首先通过消息中间件异步的将待清分的交易数据发送到清结算系统，清结算系统接收数据后开始进行数据校验和解析，并将解析后的清分对象保存到清结算服务数据库中，作为数据获取和处理阶段完成的结果；运营系统把商户入驻时添加的各种配置规则通过网络保存到清结算数据库中，然后清结算在计费和结算等流程中查询配置计算手续费、税费等费项，并把各种费项更新到清分对象中，最后保存数据库请分表；清结算系统根据结算规则判断结算模式，如果是实时结算，就立即调用账户系统记账服务，变更商户待结算余额，如果是周期结算，只需要把费项累加，待结算日期到达之后触发记账服务。在结算流程中，需要对支付类型的交易数据进行风控拦截处理，防止发生资金损失，如果风控通过，进行结算表数据更新和通知账户系统更新商户现金余额等操作。同时，为了提高清结算系统的稳定性和鲁棒性，定时处理清结算流程中发生的异常事件，根据异常状态机进行状态流转。最后，根据结算配置中的提现规则，将符合条件的商户结算资金转结到商户余额账户中。



3.2.1 领域需求导出

清结算系统需要准确多样的计算手续费，核心特性需求如下：

1. 数据处理：根据交易类型对交易数据进行条件过滤，只保留满足清算条件的交易数据。比如对于支付类交易，清算条件为交易成功且是外部商户。根据交易类型对交易数据进行合法性校验，并组装清分实体落库。
2. 清分计费：根据交易数据中的交易类型和商户计费配置计算手续费、净额等所有费项，更新清分实体和清分表。
3. 账户记账：在是结算类型中，每笔交易在清分后调用账户中心对给类账户进行余额变更。
4. 手续费清算：根据商户交易类型将手续费累加结算明细单，生成手续费结算详情单。
5. 汇总结算：对结算配置为周期结算的交易，定期汇总已清分记账的结算详情单，生成付款结算单和收费结算单并调用账务系统记账。
6. 风控处理：在结算流程中对支付类交易进行风控审核。
7. 异常处理：对清结算流程中发生异常的单号进行自动重试或人工处理。

3.2.2 运营系统需求导出

运营系统的职责为了更好的管理维护商户信息，包含商户审批，交易查询、商户查询、配置管理和报表等功能。运营系统在和清结算系统交互过程中，主要负责清结算配置管理和清结算流水查询。

1. 配置管理：运营系统在商户入网流程中，需要配置商户计费、计税和结算规则，包括配置添加、编辑、查询和验证。当运营人员审核通过后，商户清结算业务相关配置将会下发到清结算配置数据库中。在国际化业务中，清结算系统需要根据运营主题所在时区，进行国际化处理，其中包括时区转换，语言展示等逻辑。为此，运营人员在Apollo配置中心管理商户信息、时区信息、语言等配置，定时统一下发到清结算服务器。
2. 流水查询：清结算系统在处理商户交易金额的整体业务流程中，会产生清分表流水、结算详情表流水和结算表流水。运营系统通过清结算系统提供的API服务，查询对应商户的清结算流水，为商户自身资金对账、结算报表等需求提供数据源。

3.3 功能性需求

根据上部分对需求进行初步分析与导出，整个清结算系统和核心业务在于对商户交易数据进行清算结算，包括运营系统对配置和清结算流水管理。本节根据清结算系统核心业务流程描述系统的功能性需求。系统需求列表如下所示

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 参与者 | 说明 |
| R1 | 清分 | 清结算系统  交易系统 | 对交易数据进行处理 |
| R2 | 计费 | 清结算系统 | 计算各种交易手续费 |
| R3 | 记账 | 账户系统 | 调用账户系统记账 |
| R4 | 结算 | 清结算系统 | 汇总商户结算明细，发起结算流程 |
| R5 | 风控 | 风控系统 | 调用风控系统进行风控拦截 |
| R6 | 异常处理 | 清结算系统 | 处理清结算流程中的异常事件 |
| R7 | 配置管理 | 运营系统 | 管理清结算相关配置 |
| R8 | 流水管理 | 运营系统 | 查询清结算相关流水 |

3.3.1 清结算系统用例

根据上述对功能性需求的分析，可得出下面清结算系统核心用例图。

%3CmxGraphModel%3E%3Croot%3E%3CmxCell%20id%3D%220%22%2F%3E%3CmxCell%20id%3D%221%22%20parent%3D%220%22%2F%3E%3CmxCell%20id%3D%222%22%20value%3D%22%E6%95%B0%E6%8D%AE%E6%A0%A1%E9%AA%8C%22%20style%3D%22ellipse%3BwhiteSpace%3Dwrap%3Bhtml%3D1%3B%22%20vertex%3D%221%22%20parent%3D%221%22%3E%3CmxGeometry%20x%3D%22449%22%20y%3D%222917%22%20width%3D%22108%22%20height%3D%2240.75%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3C%2Froot%3E%3C%2FmxGraphModel%3E



清结算系统核心有5个用例，分别是清分、计费、清算、结算和异常处理，下面通过用例描述表简单介绍每个用例的大致流程。

表3-1 清分用例描述

|  |  |
| --- | --- |
| 用例名称 | 清分 |
| 用例描述 | 清结算系统对交易数据进行清分操作 |
| 主执行者 | 清结算系统 |
| 优先级 | 高 |
| 触发条件 | 清结算系统监听到MQ Topic有数据时 |
| 后置条件 | 创建清分对象 |
| 基本事件流 | （1）从MQ Topic 获取交易Binlog数据  （2）将交易数据解析为Binlog 对象  （3）校验数据字段完整性和合法性  （4）将Binlog转换并组装成清分对象 |
| 异常事件流 | Binlog 数据校验异常 |

表3-2 计费用例描述

|  |  |
| --- | --- |
| 用例名称 | 计费 |
| 用例描述 | 清结算系统对清分对象计算各费项手续费 |
| 主执行者 | 清结算系统 |
| 优先级 | 高 |
| 触发条件 | 清分成功 |
| 后置条件 | 完成手续费、分期费、税费、净额计费 |
| 基本事件流 | （1）清分数据落库  （2）清分前置条件校验  （3）创建计费聚合根对象  （4）根据配置规则匹配计算各费项手续费  （5）计费结果后置校验  （6）更新清分对象，保存数据库 |
| 异常事件流 | 1. 配置异常 2. 重复计费异常 3. 数据库更新异常 |

表3-3 清算用例描述

|  |  |
| --- | --- |
| 用例名称 | 清算 |
| 用例描述 | 清结算系统对清分对象进行清算 |
| 主执行者 | 清结算系统 |
| 优先级 | 高 |
| 触发条件 | 清分成功 |
| 后置条件 | 记账成功，完成清分对象各费项累计 |
| 基本事件流 | （1）计费  （2）交易记账  （3）实际结算，实时对各费项记账  （4）周期结算，创建结算详情单，并累计各费项到结算详情单  （5）创建并保存各费项数据库索引 |
| 异常事件流 | 1. 计费异常 2. 记账异常 3. 数据库更新、唯一键冲突异常 |

表3-4 结算用例描述

|  |  |
| --- | --- |
| 用例名称 | 结算 |
| 用例描述 | 清结算系统对结算详情单进行汇总结算 |
| 主执行者 | 清结算系统 |
| 优先级 | 高 |
| 触发条件 | XXL-JOB 定时任务每小时触发结算流程 |
| 后置条件 | 完成商户各类费项的汇总结算 |
| 基本事件流 | 1. XXL-JOB 定时创建结算单 2. 绑定结算详情单到结算单 3. XXL-JOG 定时触发结算主流程 4. 风控处理 5. 将详情单各个费项累加到结算单上 6. 记账，结算各类费项 |
| 异常事件流 | 1. 记账异常 2. 风控异常 |

表3-5 异常处理用例描述

|  |  |
| --- | --- |
| 用例名称 | 异常处理 |
| 用例描述 | 清结算系统对异常事件进行处理 |
| 主执行者 | 清结算系统 |
| 优先级 | 高 |
| 触发条件 | XXL-JOB 定时触发 |
| 后置条件 | 完成异常事件处理 |
| 基本事件流 | 1. 扫描异常表，构造异常处理聚合根 2. 自动重试，构造清分对象 3. 重新清算 4. 自动重试超过阈值，进行人工处理 |
| 异常事件流 | 无 |

3.4 非功能性需求

3.4.1 性能需求

清结算系统整体性能要求如下：

1. 每秒请求数QPS（Queries Per Second）：清结算主要的流量入口为交易系统推送的交易数据库binlog消息，因此清结算系统QPS必须不小于交易系统binlog消息生产者QPS，当前观测到交易binlog最大QPS为96，所以清结算QPS 满足100就可以;
2. 并发度Concurrency：清结算支持多用户实时结算和周期结算，其清分效率不低于每秒1000 个binlog消息，结算效率不低于每秒500个用户。
3. 响应时间RT（Response-time）：配置查询、修改和清结算流水查询的请求平均响应时间小于50ms；
4. 系统稳定性：可承受日常使用负载量，系统运行稳定无问题。

3.4.2 准确性

清结算系统涉及商户和平台各类账户动账、费用计算和余额提现等业务，因此需要满足资金处理的准确性需求。在 Java 开发平台，使用内置的不可变、任意精度的大整数 BigDecimal 进行数值计算，避免float 和 double 精度不够造成的资金损失问题。资金处理准确性不低于99.99%

3.4.3 可扩展性和可维护性

设计阶段应充分调研和评估清结算业务在3至5年内的发展前景，充分考虑系统升级、扩展、修改的可维护性。系统总体架构应该在未来3年内保持相对稳定，同时必须能够适应不断变化的清结算业务需求。

系统可扩展和可维护性主要通过代码质量和代码复杂度判断系统是否容易扩展和维护。代码质量的主要从设计模式、注释质量、异常处理三分方面考虑。在系统设计方面，总体要求按照高内聚低耦合的软件设计思想，采用SOLID（单一职责SPR、开闭原则OCP、里式替换LSP、接口隔离ISP、依赖倒置DIP）软件设计原则，使系统保持高可扩展性；在代码注释方面，要求不做多余重复的注释，代码能够表明的就不用注释，而类似于方法和类的目的和意图之类的无法通过代码说明的，需要进行简要概括性的注释。因此，每个类、接口、方法应该对其主要内容和意图进行注释说明；在异常处理方面，系统首先根据异常层级分类，然后根据类型进行分类，系统内部异常不能暴露给外部用户，即屏蔽内部异常。同时，为了方便开发人员定位错误，内部系统异常按照类型归类，比如按照MQ异常、参数校验异常、数据库异常、文件和网络IO异常分类。

代码复杂度主要从代码行数、圈复杂度和继承深度来评估。每个类和方法的代码函数分别不应该超过3000行和100行;代码圈复杂度不超过10；类接口继承深度数字越大意味着通过继承重用代码的可能性越大，但也意味着复杂性更高并且代码错误率更高，因此继承深度不超过6。

3.4.4 数据安全性

本系统的数据安全性主要从以下方面衡量。

1. 数据完整性：在业务数据方面，能够对交易系统发送的binlog消息进行业务字段完整性校验；在数据存储方面，能够满足数据库完整性和唯一性约束。

（3）备份和恢复：对商户配置和清结算流水数据进行备份，定时通过网络将数据传送到备用中心；提供本地数据的备份和恢复、按照每天2次进行数据的备份；采用集群部署方式，分散系统压力，避免单点故障，集群机器数不少于3台；备份硬盘至少2块，磁盘空间大小至少在1TB以上。

3.5 本章小结

本章首相介绍了清结算系统和其他支付子系统，概括描述了清结算系统和其他子系统依赖关系。然后对清结算系统的业务流程进行分析，形成最初的业务需求。接着通过用例图和用例规范表简单描述每个用例需求的具体内容和基本流程，确具体的功能性需求。最后描述系统的非功能性需求，形成完整的清结算系统需求。

第4章 系统概要设计

4.1 系统设计目标和方法

清结算系统的主要功能是为商户提供收单服务，即对商户在平台进行的交易金额进行清分结算，在平台收取服务费后把净额结算给商户。整个系统由多个低耦合高内聚的模块构成，同时各个模块相互协调以完成清结算系统任务。为了合理高效的实现该系统，本文采用了如下设计方法：：

（1）系统架构选择

系统的构建采用领域驱动设计中的四层架构和CQRS架构结合的方式。对于清分和结算模块，由于业务领域和业务规则复杂，将业务相关逻辑抽象到领域层能够是系统分层设计符合单一职责原则。同时，将业务变化隔离在领域层，使得其他层的功能相对稳定，不需要经常修改，使各层保持高内聚低耦合的特性。对于配置管理和流水查询这些没有负责业务规则的模块，清结算系统单独使用CQRS架构进行设计，从而简化系统整体的复杂度。这种根据模块自身业务特点，采取不同的架构设计的方式，使得系统具有较高的可扩展性。

（2）系统功能设计与实现

清结算系统采用Spring+SpringBoot+MyBatis技术实现系统模块功能。根据业务需求分析，系统分为三个模块，分别是清算模块、结算模块和异常处理模块。

（3）系统测试

系统在实习开发中，对个模块功能采取单元测试方法验证函数功能的正确性，在模块开发完成后，采用集成测试对各模块进行联调，测试是否符合预期。

4.2 系统静态结构设计

4.2.1 系统架构设计

清结算系统作为整个支付系统的核心子系统，需要与其他子系统的协调配合。清结算系统整体架构图见图4-1。



从图中可得，清结算系统需要和交易系统、运营系统账户系统进行交互。清结算系统内部主要分为四个模块：配置和流水模块，即图中的商户收配置、结算管理子模块属于配置模块，交易清分管理和结算单管理属于清分模块；结算模块，包含实时清算、周期清算和周期结算子模块；异常处理单独属于一个模块。系统对外通过API层向运营系统提供配置管理和流水查询服务。

4.2.1 系统功能模块设计

清结算系统主要包含五个模块，分别是清算模块、结算模块、异常处理模块、配置模块和流水模块，每个模块下包含具体的功能子模块。清算模块包含清分模块、计费模块和记账模块；结算模块包含实时结算模块和周期结算模块；异常护理模块包含自动处理模块和人工处理模块；配置模块包含配置下发模块和配置查询模块；流水模块包含清算流水查询、结算流水查询和提现流水查询模块。系统功能模块图如下所示。

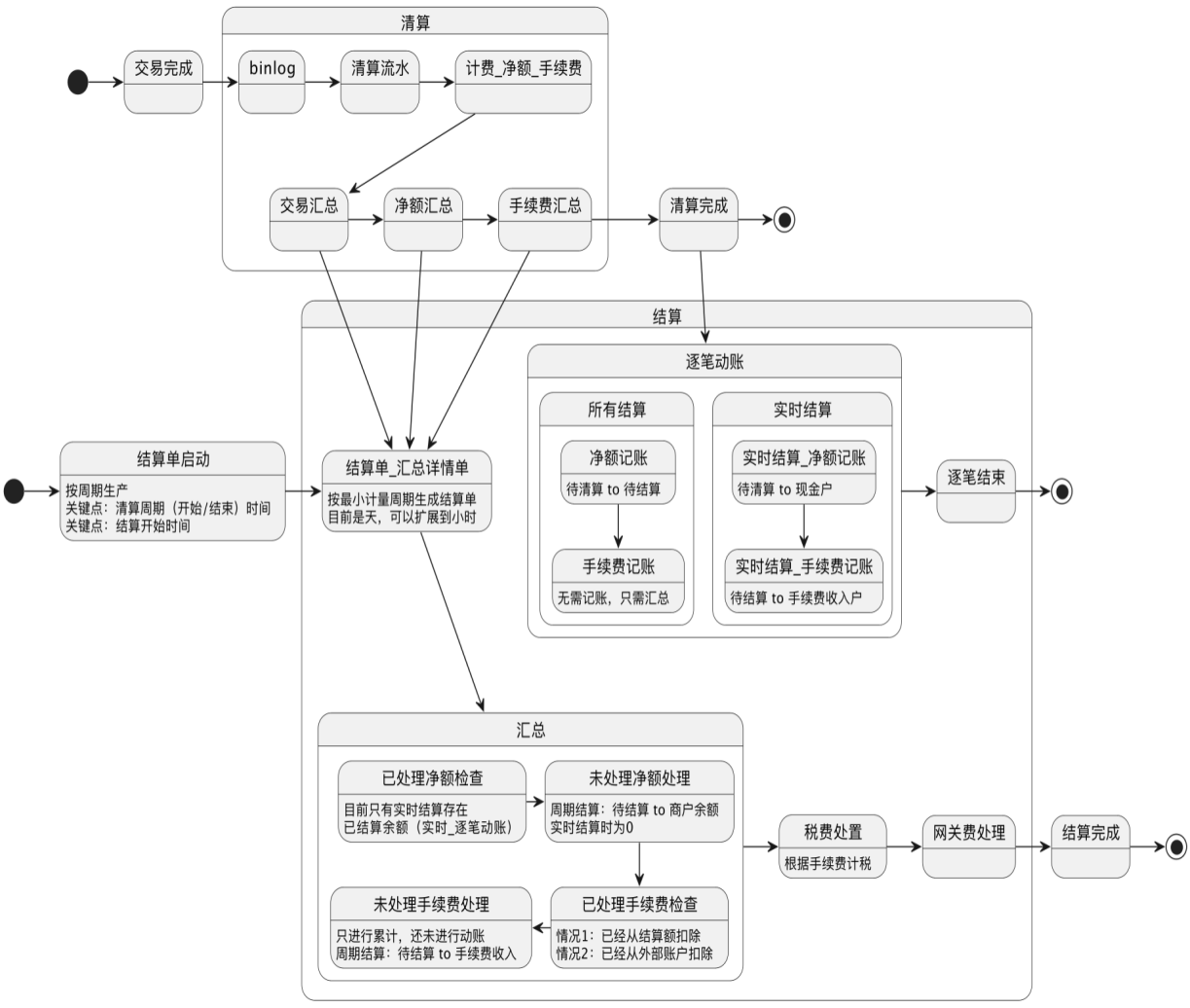


4.3 系统动态结构设计

本节通过系统活动图和数据流图描述清结算系统的动态结构。

4.3.1 清结算系统活动图

清结算系统分为清算和结算两大流程，系统整体活动图如图所示。



从清结算活动图可以看出，清算活动包含如下步骤：

1. 清分：从交易完成开始，对binlog清分，产生清分流水
2. 计费：对清分实体计算净额和手续费。
3. 汇总：对清分实体进行交易汇总、金额汇总和手续费汇总，即汇总到结算汇总详情单上。在此步骤完成需要创建结算汇总详情单，详情单创建逻辑属于重点部分，同时保持事务完整性约束，最后将清算数据关联到结算部分。
4. 记账：清算最后需要进行逐步动账处理，周期结算模式净额记账将商户待清算记账到商户待结算账户，而手续费记账实际上只需要进行汇总；实时结算模式净额记账资金信息流从商户待清算账户转移到商户现金户，而手续费记账资金信息流从待结算户转移到平台手续费收入户，完成清算记账。

结算活动包含如下步骤：

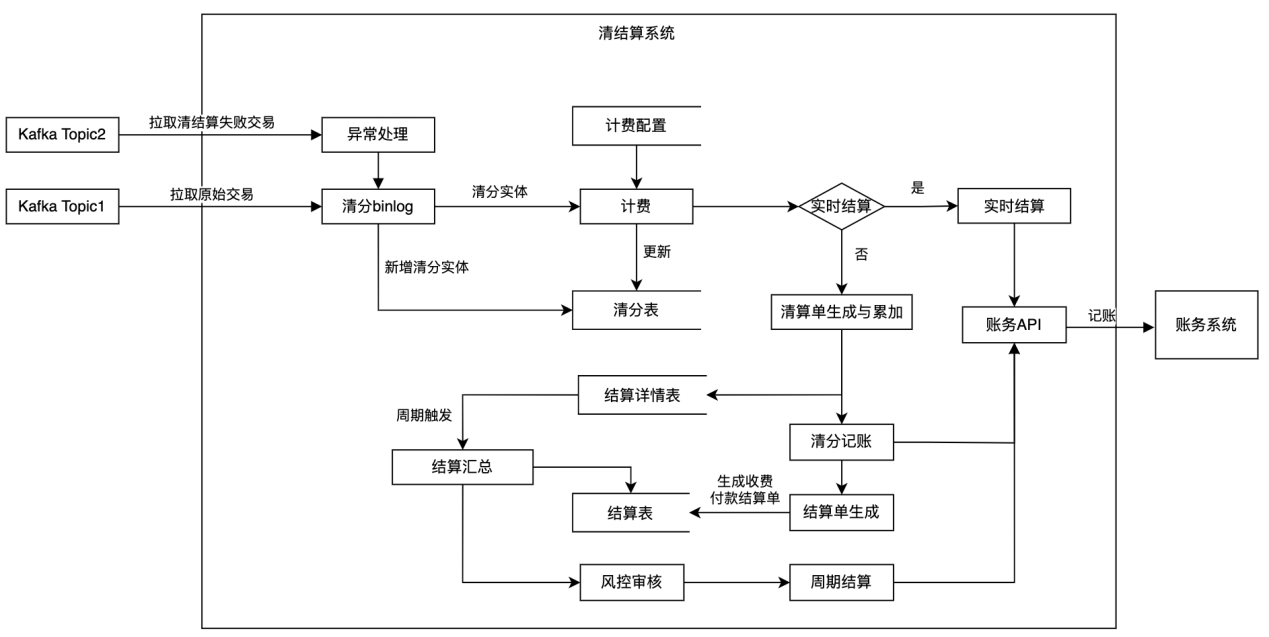
1. 定时任务：XXL-JOB定时任务启动，首先是创建结算单，然后再扫结算汇总详情单，将多个汇总详情单根据主键绑定一个结算单上。

(2) 汇总：将绑定的多个汇总详情单各费项金额累计汇总到结算单中；在汇总时根据结算类型，进行实时结算和周期结算处理，实时结算模式需要进行已处理净额和已处理手续费检查，同时进行记账；周期结算模式需要进行未处理净额和未处理手续费检查，同时进行记账。

(3) 后置处理：最后处理税费和手续费，完成结算流程。

4.3.2 清结算系统数据流图

清结算系统数据流图如图所示。



4.4 本章小结

本章从静态和动态两方面阐述清结算系统概要设计，系统静态结构方面介绍了清结算整体架构和系统功能模块，并分别以架构图和功能模块图表示；系统动态结构方面介绍了清结算活动流程和清结算数据流向，并分别以活动图和数据流图表示。

第5章 系统详细设计

5.1 详细设计目标

本章重点描述清结算系统各模块核心业务功能实现的数据结构和算法，并通过UML类图、泳道图、时序图进行详细设计。最后，对概要设计部分中的ER数据图进行详细设计。

5.2 清算模块设计

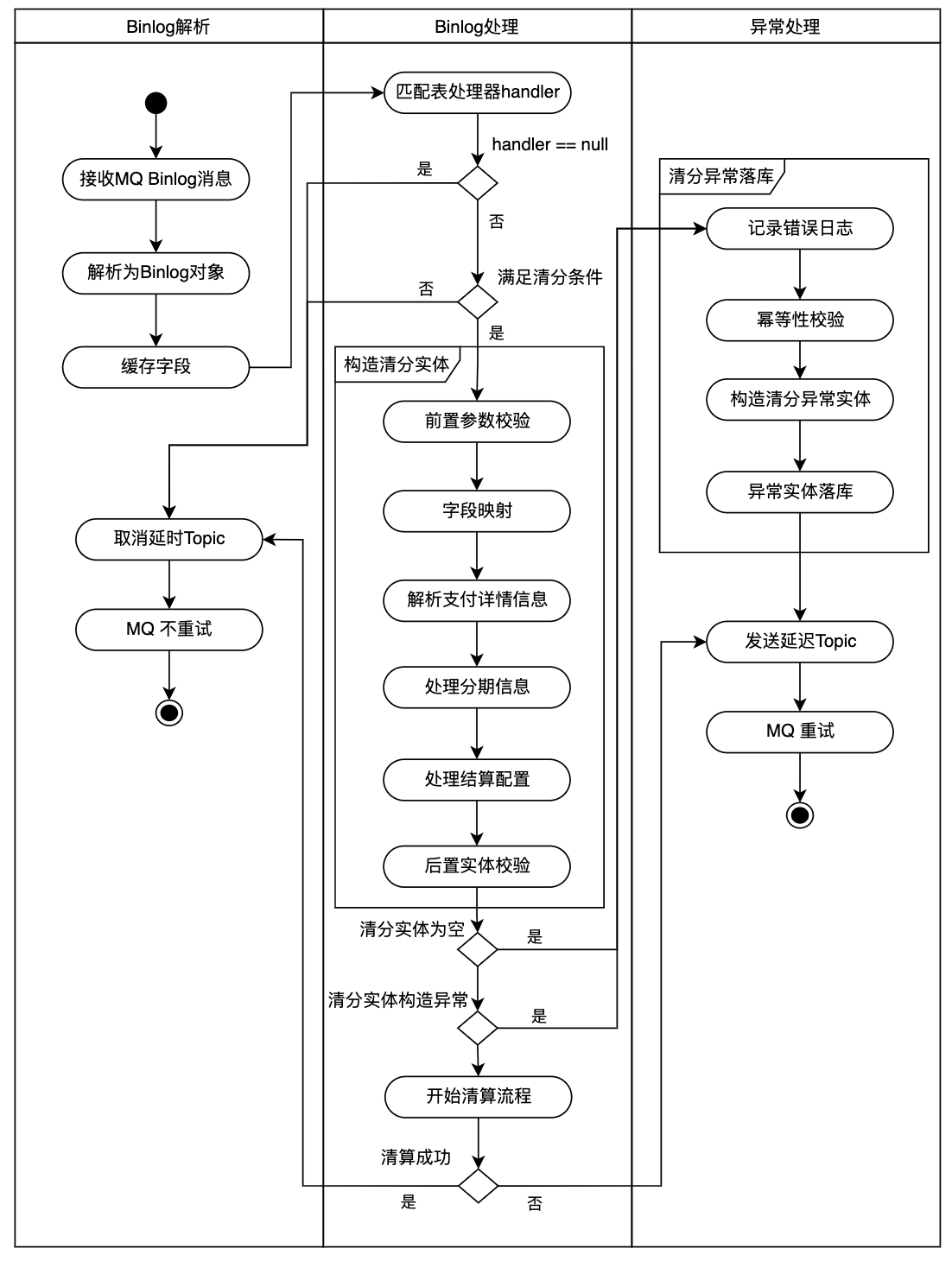
清算模块是清结算系统核心模块之一，其核心子模块包括清分、计费和清算汇总子模块，下面将对核心子模块进行详细设计。

5.2.1 Binlog清分详细设计

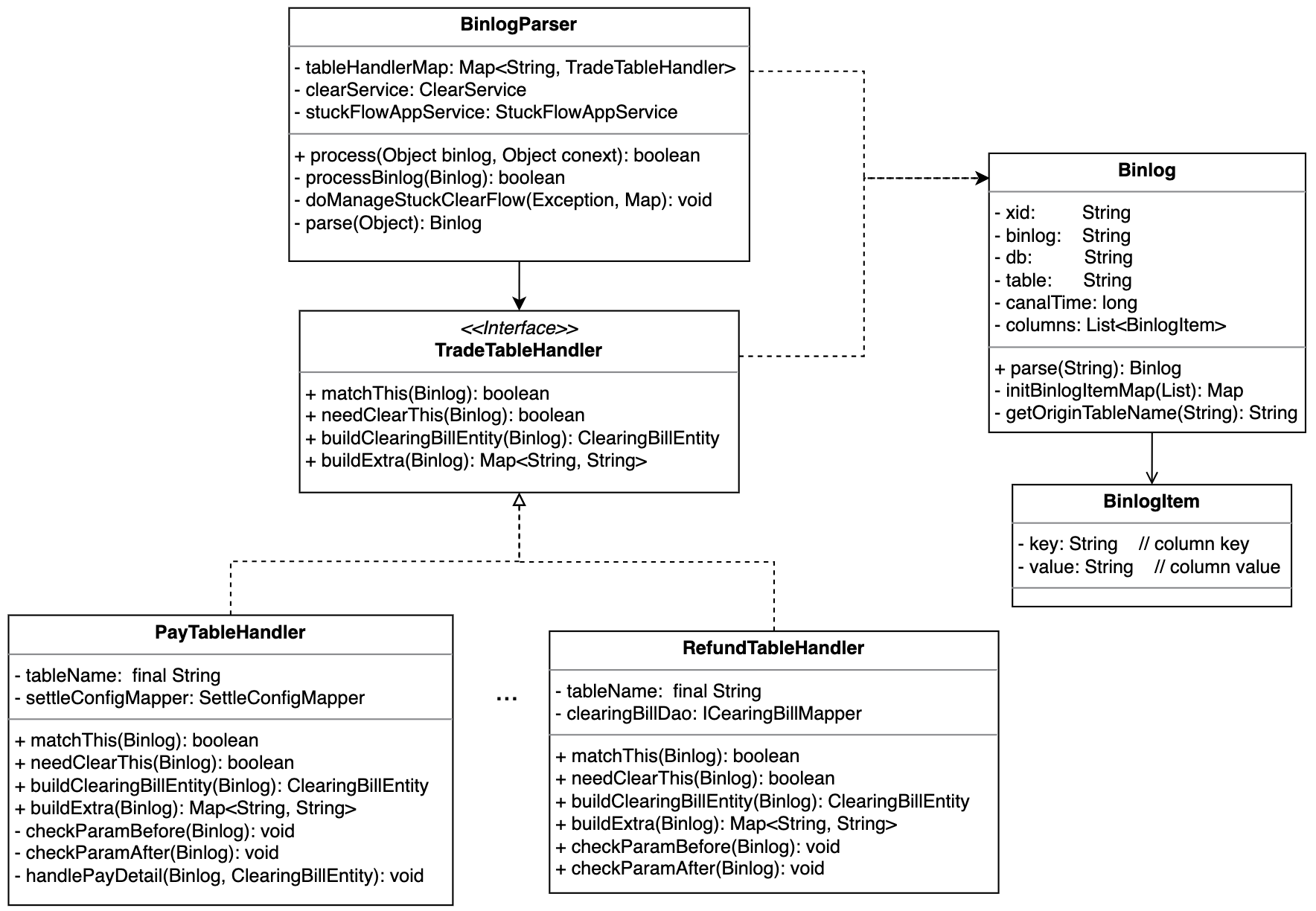
在支付系统中，各个子系统相互协作完成商户支付业务，清结算数据源来自交易系统产生的商户交易信息，保存在交易数据库中。在微服务架构模式下，各个业务子系统根据业务属性进行垂直拆分，每个子系统拥有单独的数据库，彼此之间实现数据隔离。在子系统数据相互隔离的前提下，为了实现系统之间的数据共享以及保持系统之间的解耦，一般通过第三方消息平台进行数据通信和共享。

清分模块采用阿里巴巴MySQL binlog 增量订阅和消费组件canal将交易系统的binlog数据同步到消息中间件RocketMQ 中，然后订阅RocketMQ获取交易数据。交易系统根据业务交易类型将交易数据保存到对应的数据库表中，比如支付表，退款表和拒付表等。因此，清分模块需要按照表的交易类型进行分类处理。同时，清结算接收到的是二进制日志数据，不满足自身业务数据需求，需要进行数据格式转换。其次，为了防止对错误数据或者缺失数据进行后续计费逻辑而导致的大量异常重试堆积，需要提前进行数据字段校验。最后，为了保持系统健壮性，需要对异常数据进行重试处理。

根据上述分析，清分模块主要的逻辑分为数据解析和字段校验和异常处理三部分。数据解析部分主要任务是定义Binlog对象，将二进制数据解析为Binlog对象，最后做一些缓存；字段校验部分主要内容是匹配表处理器hanler，判断数据是否满足清算条件，最后进行参数校验和构造清分对象。异常处理逻辑包含binlog 解析和校验部分的异常，对于binlog解析异常，清分模块不需要进行重试；对于字段校验异常，首先需要将异常数据落库，其次需要发送到RocketMQ延迟队列进行重试处理。清分模块泳道图如图所示。

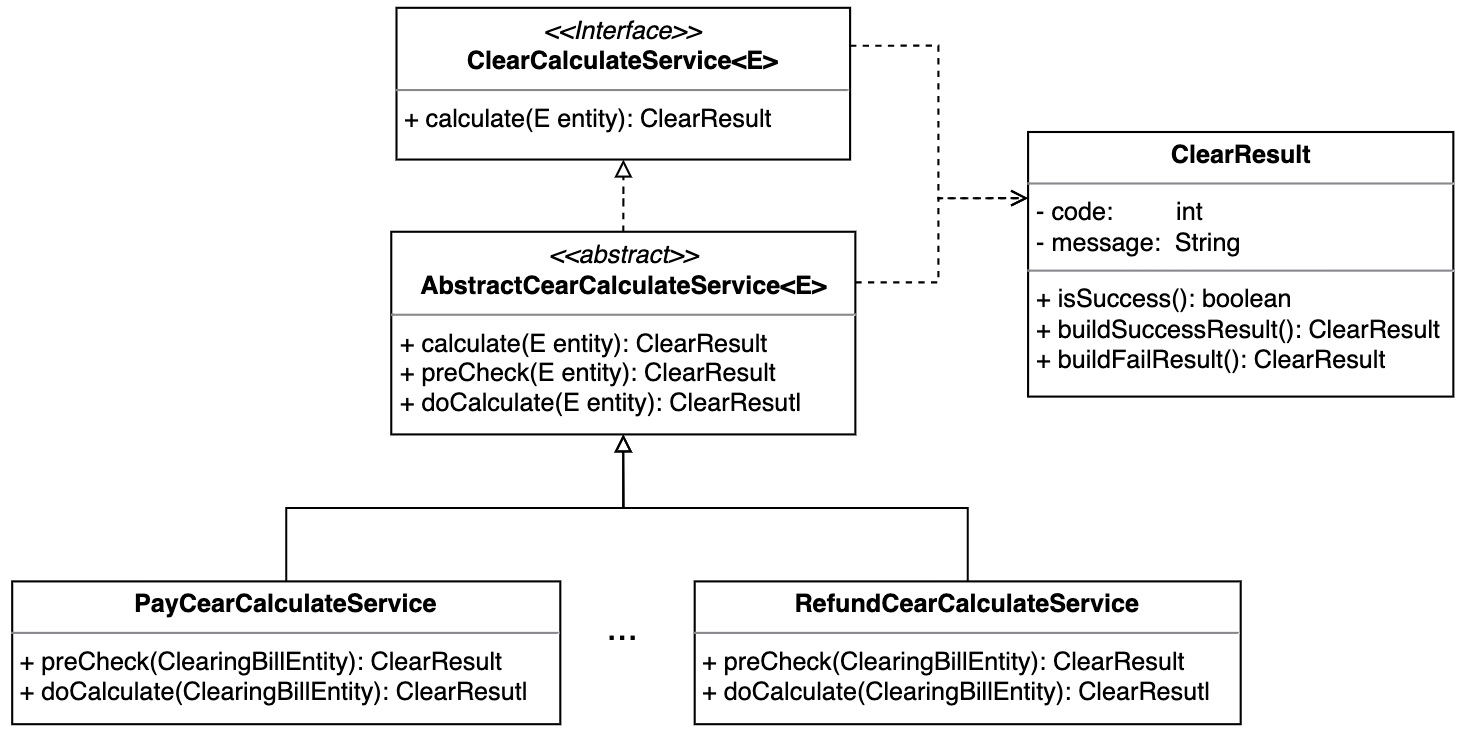


在Binlog处理中，需要根据交易类型匹配合适的表处理器handler，然后通过 handler 完成下面的清分条件判断和构造清分实体逻辑，使Blinog处理逻辑集中对应的handler中，与主流程解耦。通过分析发现，根据类型匹配handler明显可以通过面向对象的多态技术实现条件匹配。因此，这里通过接口和继承实现多态行为，不同交易类型的实现类handler 继承TradeTableHander接口，实现不同的处理逻辑，避免在主流程中进行if 条件判断。最后，根据领域驱动设计中的充血模型思想，将Blinog解析的逻辑放在Binlog对象中，调用者BinlogParser只需要进行参数类型转换和异常处理，然后委托给Binlog处理，使得对象不仅仅是数据容器，而是包含具体的业务逻辑的领域实体。Binlog处理类图如图所示。

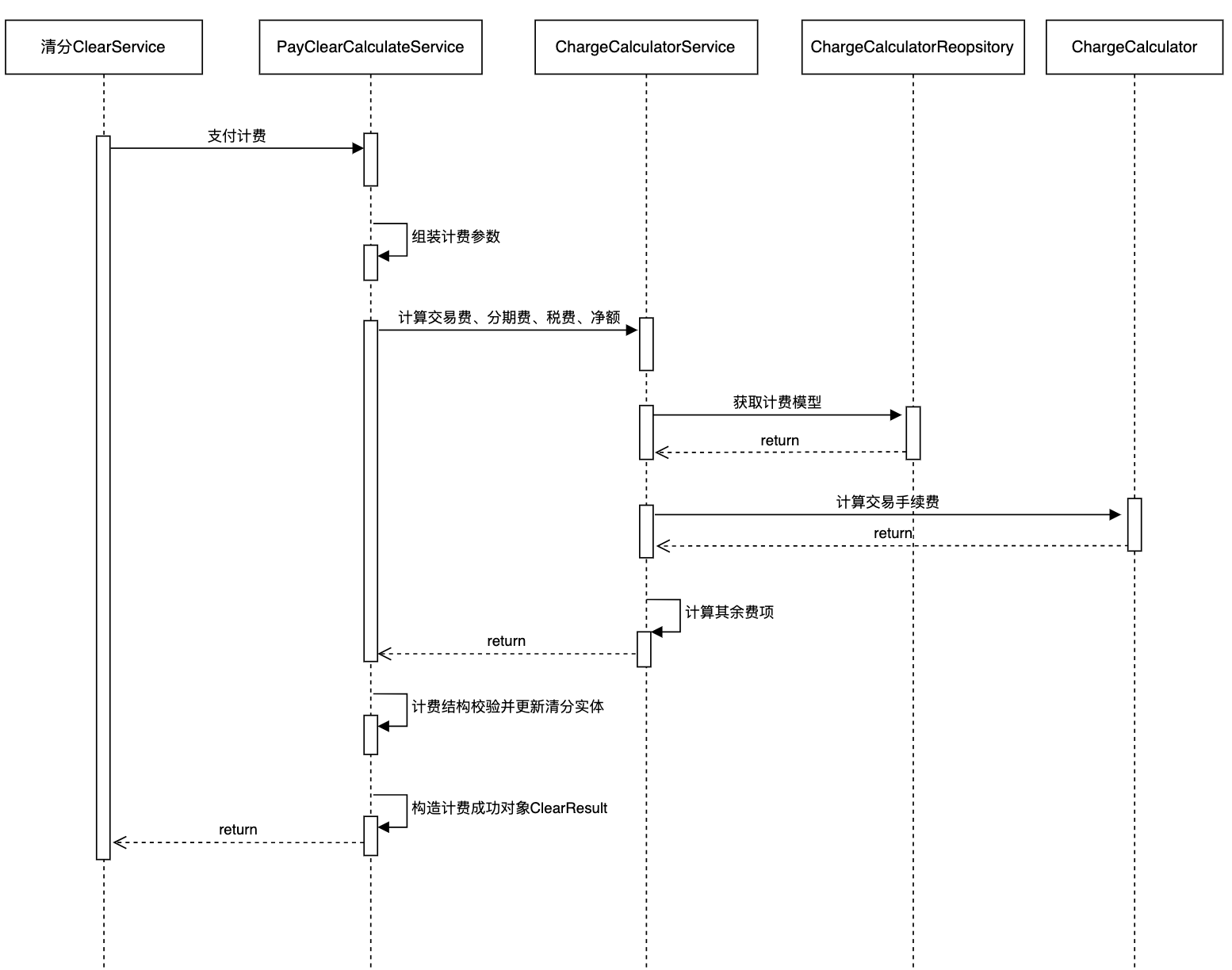


5.2.2 计费详细设计

计费模块的核心目标就是计算商户一笔交易的各种手续费。然而，作为第三方支付平台，所服务的商户数多达几十万、数百万，并提供数十种交易服务，计费服务必须能合理高效的对数量庞大的商户、丰富的交易类型以及不同商户的计费配置进行手续费计算。为此，清结算系统将商户结算配置抽离出来，单独配置和保存，整个计费流程根据商户的计费配置进行处理。为了解决不同交易类型，计费逻辑不同的问题，计费模块通过接口和抽象类和子类继承的方式，使得每种交易类型对应一种计费服务。类图如图所示。

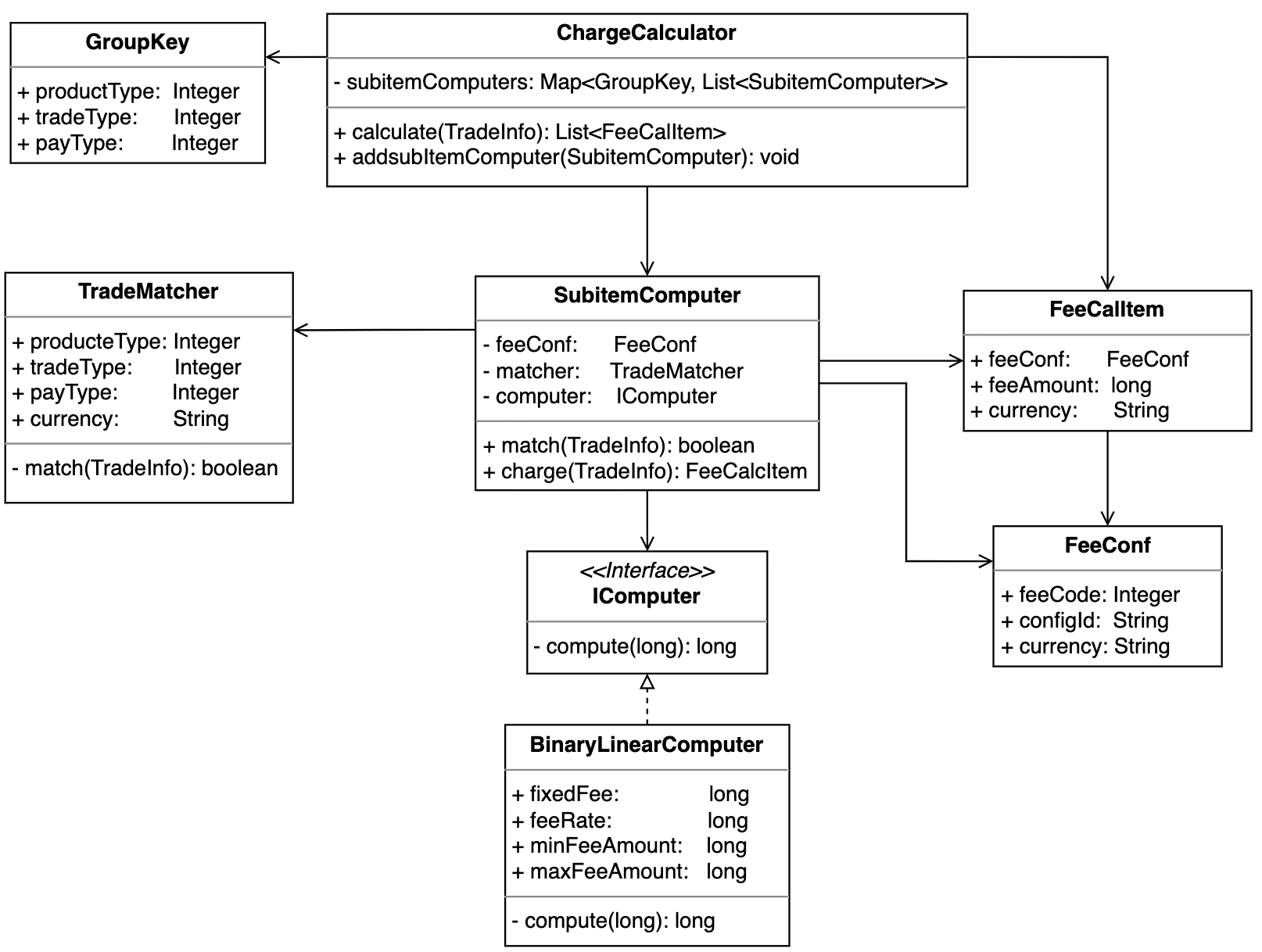


ClearCalculateService 作为计费统一接口，定义了清分操作calculate 方法签名。为了保持通用，calculate 入参为泛型，返回结果为值对象ClearResult。抽象类AbstractCearCalculateService实现该接口，并添加参数预校验方法preCheck和计费方法doCalculate，分别判断入参是否满足计费条件和负责具体的计费逻辑。子类继承该抽象类，覆盖doCalculate方法，添加计费逻辑。为了简化计费流程，calculate方法采用设计模式的模版方法，统一了计费的标准流程。具体流程为：先参数校验，校验成功后再计费，否则返回失败的ClearResult对象。PayCearCalculateService和RefundCearCalculateService分别为支付计费服务和退款计费服务，内部将计费服务委托给ChargeCalculatorService这个实际的收费服务，得到计费列表后再更新清分实体。这样处理的原因是划分收费服务边界上下文，使得收费服务保持独立，与清分上下文解耦，使得模块间的职责边界更加清晰，符合高内聚低耦合的编码原则。ChargeCalculatorService分别负责支付和退款交易的收费服务，对于支付交易，需要计算交易手续费、分期费、税费和净额；对于退款交易，需要计算退款手续费、退分期费、退税费和退净额。支付计费整体的交互时顺序如图所示。



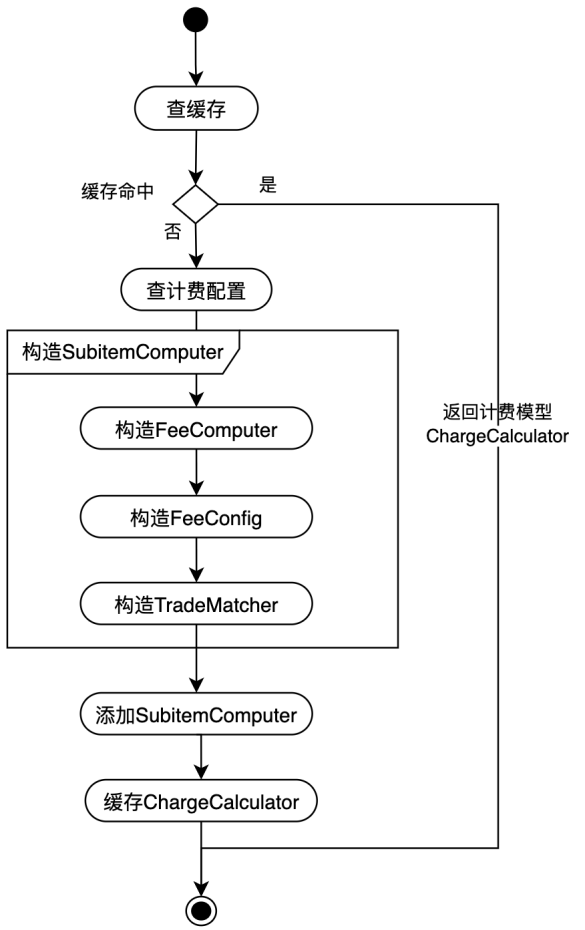
从上图可知，PayCearCalculateService主要任务是组转计费参数，即根据分服务传递的清分实体ClearingBillEntity抽取出ChargeCalculatorService需要的计费参数实体TradeInfo，然后调用ChargeCalculatorService进行计费；支付计费的逻辑分为两部分，前置计费和后置计费。前置计费即交易手续费计费，需要先计算，后置费项在手续费基础上计算。ChargeCalculatorService首先从仓库ChargeCalculatorRepository中获取计费模型，然后把交易手续费计算逻辑委托给计费模型ChargeCalculator，然后再计算其他费项。下面首先介绍计费模型的类图和计费仓库获取计费模型的逻辑，最后再介绍计费模型中的计费逻辑。

ChargeCalculator模型计算交易手续费是计费模块的热点代码，需要处理大批量计费请求。同时，计费模型需要根据商户配置中的费率和计算方式计算，即通过配置转换成相应的计费实体。对此，根据领域驱动设计思想，设计计费模型、计费仓库和计费服务。ChargeCalculator类图如下所示。



ChargeCalculator领域模型包含一个分组的子项计算器map，用来做缓存。其中的calculate方法被ChargeCalculatorService调用，接受计费参数对象TradeInfo，返回一个费项计费列表。每个费项列表值对象FeeCalItem根据费项配置FeeConf、该费项金额feeAount和币种组成。费项配置值对象FeeConf由该费项编码feeCode、商户配置ID configId 和费项币种组成。费项计算器由三部分组成，分别是费项配置FeeConf、计费匹配器TradeMatcher和计算器IComputer。计费配置器中的match方法根据参数中的产品类型、交易类型、支付类型和币种进行匹配，匹配成功才进行计算。计算器根据配置中的费基、费率、最小费用和最大费用计费，而具体的计算方式由子类决定。BinaryLinarComputer 表示按照 a + bx 方式计费，a表示费基，b表示费率，x表示支付金额，计费结果满足最小和最大费用限制。

在领域驱动设计中，仓库给调用实体提供了一个内存对象的抽象视图，实体可以直接从仓库中获取目标对象，而不需要关系目标对象的创建逻辑和底层数据库存储和映射相关的细节，保证了领域逻辑的独立性。ChargeCalculatorRepository首先根据商户id查内存缓存，如果缓存命中，直接返回商户计费模型，缓存过期时间设置为1分钟；如果缓存未命中则通过查询商户计费配置，获取商户所有的配置对象ChargeConfigEntity，然后根据配置构造子项计算器SubitemComputer，再把子项计算器添加到计费模型中，最后更新缓存并返回ChargeCalculator计费模型。ChargeCalculator添加子项计算器是根据GroupKey进行分组，把相同分组的子项计算器添加到计费实体map中。仓库获取计费模型ChargeCalculator的活动图如下。



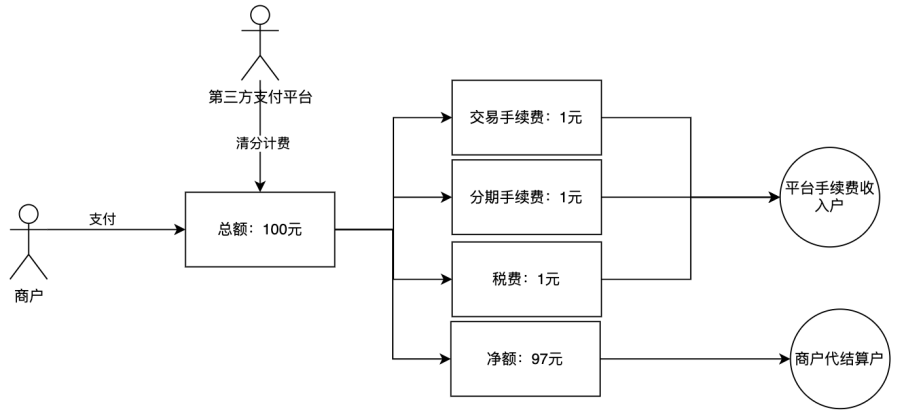
ChargeCalculatorService在通过仓库获取计费模型后，就调用计费模型的计费方法获取交易手续费，即计费模型只负责计算交易手续费，ChargeCalculatorService负责计算其他后置费项。计费模型ChargeCalculator计费流程为：

1. 根据入参获取分组Key
2. 从map中获取该笔交易的所有子项计费器，因为一个商户可能配置了多种交易手续费，每种手续费计算对应一个子项计费器SubitemComputer
3. 判断计费参数是否存在子项计费器
4. 子项计费器列表首先匹配计费参数，即如果计费参数命中多个计费器，多个计费器单独计费，SubitemComputer match方法将匹配逻辑委托给SubitemComputer中的匹配器TradeMatch，TradeMatch再根据匹配策略IMatcherPolicyUtil接口中定义的策略进行匹配，如果匹配成功，然后charge方法将计费方式委托给SubitemComputer中的IFeeComputer计算器，TradeMatch和FeeComputer在构造SubitemComputer时初始化，最后完成计费。
5. 验证计费结果，查看是否存在重复计费

计费领域模型ChargeCalculator计费的核心思想是将子项匹配和计算逻辑全部委托给子项计费器，自己只负责流程编排。其伪代码如下：

|  |  |
| --- | --- |
| 1 | List<FeeCalItem> calculate(TradeInfo info) { |
| 2 | GroupKey key ← new GroupKey(info) |
| 3 | List<SubitemComputer> computers ← map.get(key) |
| 4 | if computers == null then |
| 5 | return new ArrayList<>() |
| 6 | List<FeeCalItem> feeList ← computers.filter(e->e.match(info)).map(c -> c.charge(info)) |
| 7 | feeList.groupBy(e -> e.config().feeCode()).forEach((k,v) -> { |
| 8 | if v.size() > 1 then |
| 9 | throw RuntimeException(“重复计费: ” + k) |
| 10 | } |
| 11 | return feeList |
| 12 | } |

根据概要设计中的数据流图，计费是按逐笔进行计费的，一笔交易的计算的结果是按照费项粒度保存在清分表中。比如，商户支付了100元的交易金额，平台根据配置需要收交易手续费、分期费、税费，并计算净额，如图所示：

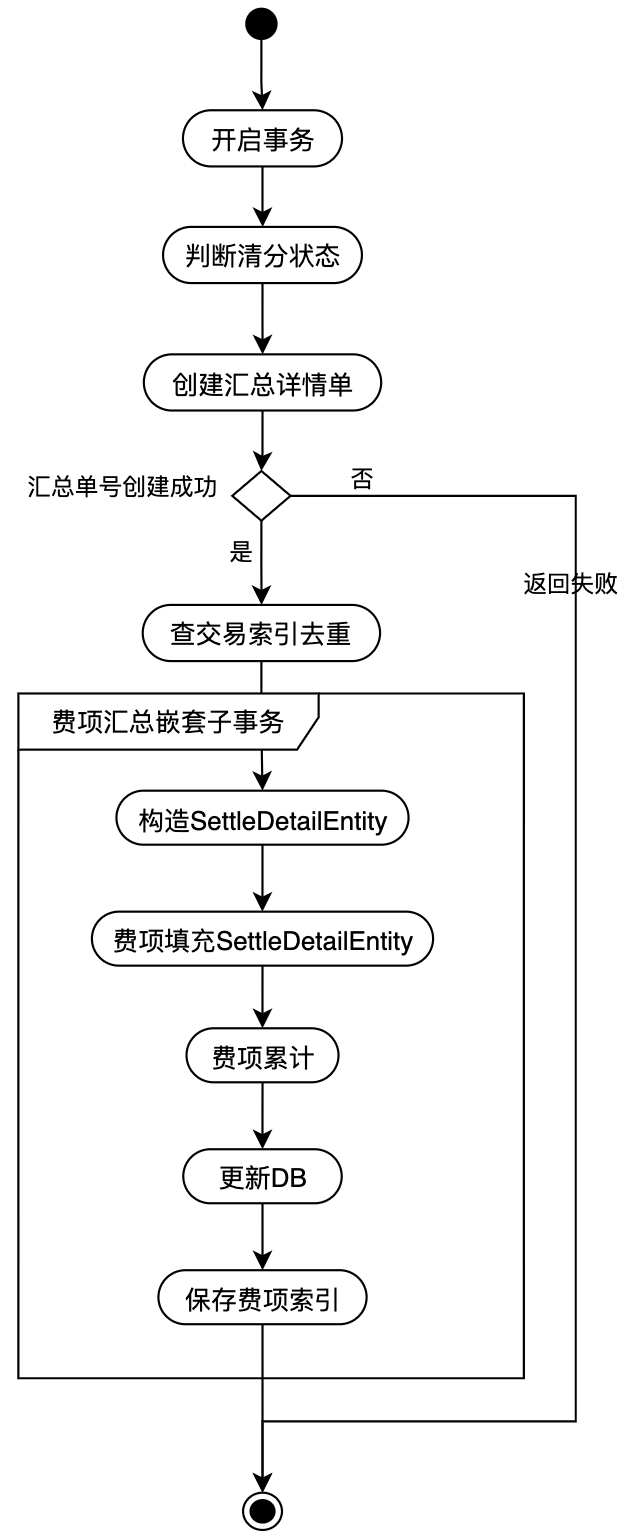


第三方支付平台为商户提供收单服务，通过清结算系统计算各种手续费，然后将手续费收入计入平台手续费收入户，将净额计入平台商户待结算户，然后通过结算流程按结算配置结算给商户。

5.2.2 清算汇总详细设计

计费模块逐笔计费，将商户各类交易的费项结果保存在清分表中，即清分表唯一键为商户和交易类型，但是结算时间一般以天或周为级别，比如按工作日、自然日、单周、或双周结算。为了满足商户不同的业务需求和现金流管理策略，第三方支付平台为商户提供多种结算模式，在商户入网时签约某种结算模式，然后平台在运营系统的配置下发给清结算系统。所以，在清分模块需要汇总商户一天内同类型交易的费项，并保存到结算详情表中。

汇总流程主要分为两大部分，第一部分是创建用于汇总费项的结算明细单号DetailId，第二部分为费项汇总部分。整体汇总流程状态图如下：



1. 汇总流程首先开启Spring事务，保证整个操作流程满足事务ACID属性；
2. 校验清分实体ClearingBillEntity状态是否符合汇总前置状态；
3. 根据商户id、产品类型productType、交易类型tradeType和交易完成时间tradeFinishTime，调用结算服务settleService的createDetailId方法创建汇总详情单，并返回结算明细单号DetailId；
4. 为了避免商户同一笔交易重复汇总，根据商户交易号tradeId和交易类型tradeType查询清分索引表去重；
5. 如果去重校验通过，开启一个新的Spring嵌套子事务，进行费项累计；首先创建内存结算详情实体SettleDetailEntity，然后然后根据结算模式将该笔交易计费后的各类费项结果保存到实体中的对应字段中；对于实时结算模式，因为实时结算已经调用账户服务记账了，所以各费项分别累计到已处理交易手续费、已处理分期手续费、已处理税费和已处理净额字段中；同样，对于周期结算模式，因为需要延期结算，为了和实时结算模式区分，费项需要分别累积未处理交易手续费、未处理分期手续费、未处理税费和未处理净额字段；最后到通过MyBatis update进行各费项累计并更新实体到数据库结算详情表；
6. 为了保存费项累计记录，需要为各类费项创建清分索引，保存交易单号、交易类型、费项编码、商户号、结算详情单号等信息，保证（2）中重复交易不会重复累计费项，同时关联了结算详情单号，为后续商户对账提供数据查询支持。

要组成部分，内部含有分别和认证授权机构（ECA）、假名证书机构（PCA）、应用证书机构（ACA）相对应的认证授权机构（AAA）、假名证书注册机构（PRA）、应用证书注册机构（ARA），用于代V2X设备进行各式业务的申请。此外，该系统还设有异常行为检测机构及链接机构，负责识别异常行为或错误，并向上提供撤销信息。只有合理合法的申请才会被其受理并代之向安全认证系统申请。

图5.1为安全认证过程的逻辑结构图。

业务逻辑

图5.1 安全认证逻辑结构图

综上，利用车联网平台中的系统间协作，本系统实现了对车联网智能设备相关安全认证管理功能的提供。这种间接提供服务的方式虽然延长了部分业务时间，但是却大大提升了系统本身处理业务的效率，保障了整个车联网平台的安全性。此外，签发的证书经过多级机构的认证审核，保证了车联网设备使用这些证书进行通信时的数据安全。

5.2.2 系统安全通信设计

智能设备是通过注册审批系统（PRA）向本安全认证管理系统（PCA）申请安全认证业务的。为保障信息交互顺利，需要对两个系统之间的通信过程进行设计。根据上节设计内容及SSL协议无法适配国产的SM系列密码算法，故而传统的HTTPS协议无法胜任国产车联网平台的相关要求。因此，本系统选择国家标准规定的运用国密SSL协议的HTTPS通信方式。

国密SSL协议的通信流程大致和传统SSL协议一致，但服务端在双方握手的过程中采用签名证书与加密证书同存的双证书形式。RA系统管理端与CA系统服务端的通信建立时序图如图5.2所示。

SSL握手

图5.2 国密SSL通信时序图

由图可见通信建立的详细步骤：

1. RA系统先向CA系统的服务端发送包括了加密套件和随机数的ClientHello消息，服务端收到后选择合适的加密套件、生成随机数，向RA回复ServerHello消息。
2. 服务端继续发送消息，依次发送包含自身双证书的Certificate消息、表征申请密钥交换的ServerKeyExchange消息以及索取对方证书完成双向认证的CertificateRequest消息。
3. 在确认收到对方发送的所有消息后，管理端会首先发出ClientCertificate消息回复服务端的证书请求，而后回复ClientKeyExchange完成密钥交换，最后发送CertificateVerify消息让服务端鉴别RA是否为证书的合法持有者。
4. 最后，服务端和客户端各自完成密码规格变更，为验证密钥交换过程是否成功发送Finished消息给对方，双方收到后即确认握手的完整性，通信成功建立。

通信建立后，RA即可向CA系统提出业务申请。请求与响应报文的报文头与正文内容都须是ASN.1序列化后的相关数据。ASN.1的编码技术支持可扩展信息在无线网络中低延迟、高效率的传输。由于车联网服务端接口用于同车联网体系中其他的机构进行数据交互，故而使用ASN.1可以不受语言、框架的限制，达到车联网体系的兼容与交互。如传输中的证书在ASN.1描述为：

|  |  |
| --- | --- |
| 1 | CertificateBase ::= SEQUENCE { |
| 2 | version Uint8(3), |
| 3 | type CertificateType, |
| 4 | issuer IssuerIdentifier, |
| 5 | toBeSigned ToBeSignedCertificate, |
| 6 | signature Signature OPTIONAL, |
| 7 | } |

综上所述，通过运用国密SSL协议的HTTPS通信方式以及ASN.1序列化报文内容，系统的通信能力适配了国密系列算法，且满足了车联网平台的信息高效传输要求。

5.2.3 安全认证业务设计

1. 安全证书

根据前文所提出的设计思路，本系统中进行业务相关的格式设计时既需要满足相关标准，又需要满足车联网安全需求。通过对比x.509证书及ITS证书的优缺点，结合证书在系统中的具体用途，设计证书的基本格式如表5.1所示。

本文中，业务子系统对外提供安全认证相关服务的证书类型有以下四种：注册证书、假名证书、应用证书和身份证书。

（1）注册证书由注册CA签发给OBU和RSU。OBU或RSU向注册机构申请认证通过后，注册CA会为其签发注册证书。一个设备只能拥有一张注册证书。V2X设备获得注册证书后，才可以向PCA申请假名证书或向ECA申请应用证书和身份证书。

（2）假名证书由假名CA签发给OBU。OBU使用假名证书签发其播发的主动安全消息。为保护用户隐私，需要使用一定的手段对隐私信息进行加密保护，且假名证书到期后直接作废。为避免泄露车辆重要安全信息，OBU可拥有多个假名证书，用于定期切换使用。

（3）应用证书由应用CA签发给RSU，用于特定的车联网应用。RSU和VSP使用应用证书签发其播发的应用消息，例如限速区域、道路拥堵状态等消息。为实现不同应用的区分与识别，RSU的一个应用对应获得一张身份证书。

（4）身份证书由应用CA签发给OBU，用于特定的车联网应用。OBU使用身份证书向RSU证明其身份，以获得后者提供的特殊车联网应用服务，例如救护车与红绿灯进行交互，并控制后者的状态。为实现不同应用的区分与识别，OBU的一个应用对应获得一张身份证书。

表5.1 安全证书基本格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 数据域1 | 数据域2 | 是否必选 | 说明 |
| 版本 |  | version | 是 | 证书结构版本，本文采用标准对应的版本号为3 |
| 类型 |  | type | 是 | 证书结构类型 |
| 签发者 |  | issuer | 是 | 自签证书或签发此证书的 CA 证书的 HashedId8 值 |
| 签名数据 | toBeSigned | id | 是 | 证书标识 |
| cracaId | 是 | CRL-CA标识HashedId3，若不使用设置为全零 |
| crlSeries | 是 | CRL序列号，若不使用设置为全零 |
| validityPeriod | 是 | 有效期 |
| region | 否 | 有效地理范围 |
| assuranceLevel | 否 | 信任级别 |
| appPermissions | 是 | 应用数据签名权限 |
| certIssuePermissions | 否 | 适用于 CA 证书，描述可签发的证书种类和权限范围 |
| certRequestPermissions | 否 | 适用于注册证书，描述可申请的证书种类、权限范围 |
| canRequestRollover | 否 | 是否能够用于请求同等权限的证书 |
| encryptionKey | 否 | 加密公钥 |
| verifyKeyIndicator | 是 | 验证公钥，采用其他结构的证书结构时，可以是相关数据 |
| 签名值 |  | signature | 否 | 证书结构类型为显式证书时，此字段为必填字段，用于存储证书的签名值 |

证书的生成采用国密系列算法。国密系列算法在安全性和效率上不逊于国际通用算法，并且具有我国独立知识产权，十分适合用于国内信息安全方面的系统。证书的生成遵循以下流程：

1. 生成空白证书模板；
2. 生成SM2算法的密钥对；
3. 对CA证书使用SM3算法进行Hash计算，将值填入签名者一栏；
4. 根据系统要求填写证书标识、有效期、信任级别等签名数据；
5. 对签名数据字段进行正则八位字节编码规则（COER）进行编码；
6. 使用SM2签名算法和CA的私钥对编码后数据进行计算；
7. 计算结果填入signature字段作为证书的签名值。

根据上文的设计，通过使用国密算法签发给智能设备多种类型的证书并约定不同证书的使用途径，本系统保证了车联网中的智能设备的信息安全，让数据可以在车联网中安全可靠的传输。

2. 证书撤销列表

证书撤销列表（CRL）由CA系统根据RA系统中的异常行为管理机构上报的异常情况进行生成与发布。其主要用于终端授权证书的撤销，出现在列表上的证书将被视为无效证书，使用无效证书传输的信息被各设备视作不安全数据。结合已设计的安全认证技术及证书结构，CRL的具体结构设计如表5.2。

表5.2 证书撤销列表基本格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 数据域1 | 数据域2 | 是否必选 | 说明 |
| 版本 |  | version | 是 | version 是 CRL 的版本号，本标准对应的版本号是 1 |
| 序列号 |  | crlSeries | 是 |  |
| 签发者 |  | issuer | 是 | 签发此证书的CRL CA 的证 书的HashedId8 值 |
| 签发时间 |  | issueDate | 是 | CRL 的发布时间 |
| 下次签发时间 |  | nextCrl | 是 | 包含预期发出具有相同 crlSeries 和crlCraca 的下一个 CRL 的时间 |
| 优先级信息 |  | priorityInfo | 是 | 所包含的信息可协助存储空间有限的 设备确定要保留哪些撤销信息以及丢 弃哪些撤销信息 |
| 正文选择结构体 | typeSpecific | fullHashCrl | 是 | 包含一个完整的基于散列值的 CRL |
|  |  | deltaHashCrl | 否 | 包含基于增量散列的 CRL |
|  |  | fullLinkedCrl | 否 | 包含所有已撤销证书的个体或群组链接数据的列表 |
|  |  | deltaLinkedCrl | 是 | 包含所有已撤销证书的个体和/或群组链接数据的列表 |

由上表可以看到，CRL主要由版本、序列号、签发者、签发时间等部分组成，正文部分可以根据需求情况选择对应的结构体。证书撤销机制如下：

1. 异常行为管理机构识别到异常信息；
2. RA系统核实有问题后上报CA系统；
3. CA系统根据数据库相关信息生成对应CRL，同时更改其信息；
4. RA系统申请下载当前CRL；
5. RA系统根据CRL内容撤销对应证书的安全信任级别。

3. 证书申请业务

证书申请业务为RA系统代车联网智能设备向CA系统提出申请，请求获得管理机构签发的证书。通过前文所述方式发送申请报文，CA系统服务端收到后对其进行处理并返回相应结果。接下来以注册证书的申请下载为例进行详细设计。

当收到注册证书申请请求后，系统首先会对消息进行格式转换，并校验消息包含的参数是否合法。确认无问题后申请方的身份证书是否正常，核查通过之后再检查注册CA的状态以及注册CA的业务证书是否仍有效。当这些检查都通过后再判断是否已为此对象签发过注册证书。若尚未签发，则进入签发阶段，检查数据库保存的证书公钥是否唯一、处理有效期是否满足，同时读取相应证书模板，一切正常则生成证书。过程中发现任何异常都将中止业务并返回响应消息告知异常原因。生成证书之后，将有关信息存入数据库的终端证书信息表及终端证书实体表中留档，而后将证书及其它信息转为响应消息并返回。

证书申请下载时业务子系统的伪代码如下所示。

输入：EC证书申请下载消息requestApplyMessage；

输出：业务响应消息responseApplyMessage。

RequestAndDownloadEC

|  |  |
| --- | --- |
| 1 | reqBody ← requesApplytMessage.getBody() |
| 2 | req ← toJavaObject(reqBody) |
| 3 | if req.checkParamEmpty() = 0 then |
| 4 | responseApplyMessage ← toResponseMessage(param error) |
| 5 | return responseApplyMessage |
| 6 | end |
| 7 | flag ← checkRaInfo(req) and checkCaStatus(req) and checkCaCertStatus(req) |
| 8 | if flag = 0 then |
| 9 | responseApplyMessage ← toResponseMessage(ca error) |
| 10 | return responseApplyMessage |
| 11 | end |
| 12 | if checkCertNotExist(req) = 0 then |
| 13 | responseApplyMessage ← toResponseMessage(exist error) |
| 14 | return responseApplyMessage |
| 15 | end |
| 16 | flag ← checkKey(req) and checkTemplate(req) and checkValidity(req) |
| 17 | if flag = 0 then |
| 18 | responseApplyMessage ← toResponseMessage(validity error) |
| 19 | return responseApplyMessage |
| 20 | end |
| 21 | else |
| 22 | if template.selectTemplate(req.templateName) then |
| 23 | cert ← template.newCert(req) |
| 24 | cert.key ← sm2.genKeyPair() |
| 25 | cert.signer ← sm3.hash(ecaCert) |
| 26 | codeData ← coerCode(cert.sign) |
| 27 | cert.signature ← sm2.signAlg(codeData,ecaScrKey) |
| 28 | end |
| 29 | certInfo ← toCertInfo(cert,req) |
| 30 | certCertEntity ← toCertEntity(cert,sm3.hash(cert)) |
| 31 | responseApplyMessage ← toResponseMessage(certInfo,certEntity) |
| 32 | end |
| 33 | return responseApplyMessage |

4. 证书作废业务

证书作废流程发生在RA收到车联网设备的作废申请后，由RA向ECA提出申请，在校验过参数无误之后检查注册CA的状态以及有效的证书实体信息以及是否存在此种申请。当这些检查都通过后，更改数据库中证书信息表的证书状态，保持证书的实体信息不变并将实体信息写入证书作废表，并生成响应数据反馈给RA。流程中任意环节审查不通过则返回相应的失败结果通知RA。

证书作废时业务子系统的伪代码如下所示。

输入：EC证书作废申请消息requestCancelMessage；

输出：业务响应消息responseCancelMessage。

CancelEC

|  |  |
| --- | --- |
| 1 | reqBody ← requestCancelMessage.getBody() |
| 2 | req ← toJavaObject(reqBody) |
| 3 | if req.checkParamEmpty() = 0 then |
| 4 | responseCancelMessage ← toResponseMessage(param error) |
| 5 | return responseCancelMessage |
| 6 | end |
| 7 | flag ← checkRaInfo(req) and checkCaStatus(req) and checkCaCertStatus(req) |
| 8 | if flag = 0 then |
| 9 | responseCancelMessage ← toResponseMessage(ca error) |
| 10 | return responseCancelMessage |
| 11 | end |
| 12 | if checkCertNotExist(req) = 1 then |
| 13 | responseCancelMessage ← toResponseMessage(exist error) |
| 14 | return responseCancelMessage |
| 15 | end |
| 16 | certInfo ← getCertInfo(req) |
| 17 | certEntity ← getCertEntity(req) |
| 18 | certInfo.setCertStatus(‘cancel’) |
| 19 | certRevoke ← newCertRevoke(certInfo,certEntity) |
| 20 | responseCancelMessage ← toResponseMessage(certRevoke) |
| 21 | return responseCancelMessage |

5. 证书验证业务

当收到证书验证请求后，系统会校验申请方相关参数，正确无误后方允许进入下一步。首先查验申请方的信任级别是否满足要求，以及数据库是否处于正常的对外开放的状态。过程中发现任何异常都将中止业务并返回响应消息告知异常原因。以上条件均满足后，开始对数据库的查询。若查询结果为空，则返回无相关证书信息的失败结果，否则读取符合条件的证书相关资料，返回包含所验证证书详细信息的报文。

证书验证业务的系统伪代码如下所示。

输入：EC证书验证消息requestVerifyMessage；

输出：业务响应消息responseVerifyMessage。

QueryEC

|  |  |
| --- | --- |
| 1 | reqBody ← requestVerifyMessage.getBody() |
| 2 | req ← toJavaObject(reqBody) |
| 3 | if req.checkParamEmpty() = 0 then |
| 4 | responseVerifyMessage ← toResponseMessage(param error) |
| 5 | return responseVerifyMessage |
| 6 | end |
| 7 | flag ← checkRaInfo(req) and checkTrustLevel(req) |
| 8 | if flag = 0 then |
| 9 | responseVerifyMessage ← toResponseMessage(identity error) |
| 10 | return responseVerifyMessage |
| 11 | end |
| 12 | if checkDataBase() = 0 then |
| 13 | responseVerifyMessage ← toResponseMessage(database error) |
| 14 | return responseVerifyMessage |
| 15 | end |
| 16 | flag ← queryCert(req) = 0 |
| 17 | if flag = 0 then |
| 18 | responseVerifyMessage ← toResponseMessage(illegal cert) |
| 19 | end |
| 20 | else |
| 21 | responseVerifyMessage ← toResponseMessage(queryCert(req)) |
| 22 | end |
| 23 | return responseVerifyMessage |

6. 证书更新业务

证书更新业务为RA系统代车联网智能设备向CA系统提出申请，请求管理机构更新已签发的证书。RA发送申请更新的报文，CA系统服务端收到后对其进行处理并返回相应结果。接下来以注册证书的更新下载为例进行详细设计。

当收到注册证书更新请求后，系统首先会对消息进行格式转换，并校验消息包含的参数是否合法。确认无问题后申请方的身份证书是否正常，核查通过之后再检查注册CA的状态以及注册CA的业务证书是否仍有效。当这些检查都通过后再判断是否已为此对象签发过注册证书。若已有注册证书，则进入签发阶段，检查数据库保存的证书公钥是否唯一、处理有效期是否满足，同时读取相应证书模板，一切正常则生成证书。生成证书之后，将有关信息存入数据库的终端证书信息表及终端证书实体表中留档，而后将证书及其它信息转为响应消息并返回。过程中发现任何异常都将中止业务并返回响应消息告知异常原因。

证书更新下载时业务子系统的伪代码如下所示。

输入：EC证书更新下载消息requestUpdateMessage；

输出：业务响应消息responseUpdateMessage。

UpdateAndDownloadEC

|  |  |
| --- | --- |
| 1 | reqBody ← requestUpdateMessage.getBody() |
| 2 | req ← toJavaObject(reqBody) |
| 3 | if req.checkParamEmpty() = 0 then |
| 4 | responseUpdateMessage ← toResponseMessage(param error) |
| 5 | return responseUpdateMessage |
| 6 | end |
| 7 | flag ← checkRaInfo(req) and checkCaStatus(req) and checkCaCertStatus(req) |
| 8 | if flag = 0 then |
| 9 | responseUpdateMessage ← toResponseMessage(ca error) |
| 10 | return responseUpdateMessage |
| 11 | end |
| 12 | if checkCertNotExist(req) = 0 then |
| 13 | responseUpdateMessage ← toResponseMessage(exist error) |
| 14 | return responseUpdateMessage |
| 15 | end |
| 16 | flag ← checkKey(req) and checkTemplate(req) and checkValidity(req) |
| 17 | if flag = 0 then |
| 18 | responseUpdateMessage ← toResponseMessage(validity error) |
| 19 | return responseUpdateMessage |
| 20 | end |
| 21 | else |
| 22 | if template.selectTemplate(req.templateName) then |
| 23 | cert ← template.newCert(req) |
| 24 | cert.key ← sm2.genKeyPair() |
| 25 | cert.signer ← sm3.hash(ecaCert) |
| 26 | codeData ← coerCode(cert.sign) |
| 27 | cert.signature ← sm2.signAlg(codeData,ecaScrKey) |
| 28 | end |
| 29 | certInfo ← toCertInfo(cert,req) |
| 30 | certCertEntity ← toCertEntity(cert,sm3.hash(cert)) |
| 31 | responseUpdateMessage ← toResponseMessage(certInfo,certEntity) |
| 32 | end |
| 33 | return responseUpdateMessage |

5.3 安全管理员模块设计

安全管理员模块主要为安全认证与管理业务中的安全管理员所设计，下辖四个子模块：MCA管理、用户证书管理、业务CA管理及系统安全管理，它们又包括不同的子功能。

本节结合UML图介绍这些模块的详细设计与难点解决情况,重点阐述本模块的静态设计思路与动态设计思路。

5.3.1 用户证书管理设计

在用户证书管理模块，AdminInfo类是实体类，表征用户证书的各项关键信息；FileLogger类负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由AdminController类实现。新增用户证书功能由createAdmin()方法实现，更新用户证书功能由updateAdmin()方法实现，查询用户证书功能由queryAdmin()方法实现，作废用户证书功能由deleteAdmin()方法实现。Service层的功能由AdminService类实现。类中和Controller层类似提供了可以实现新增、更新、查询详情、废弃工作的函数方法。AdminDao类为上层类提供了与数据库进行信息交互的接口，以便完成数据的读写。

用户证书管理相关的功能类图设计如图5.3所示。

用户证书管理模块的功能时序图设计如图5.4所示。安全管理员在管理端执行用户证书管理操作，选择界面的不同功能，根据提示输入证书主题、用途、有效期、算法等参数后，管理端将这些信息传递到服务端。服务端先对各项参数进行校对，确认数据合法后将向数据库请求执行相关数据处理操作。数据库执行完毕后将结果反馈给服务端，服务端将操作的结束信息反馈给管理端，并将此次行为录入系统日志中，最终管理端在界面上告知管理员操作成功。

用户证书类图

图5.3 用户证书管理类图

用户证书时序图

图5.4 用户证书管理时序图

5.3.2 MCA管理设计

MCA管理相关的功能类图设计如图5.1所示。在MCA管理模块，McaInfo类是实体类，表征MCA的各项关键信息；FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由McaController类实现。更新MCA信息功能由updateMcaInfoByType()方法实现，更新MCA身份证书功能由updateMcaIdCert()方法实现。Service层的功能由McaService类实现。类中提供了查询函数用于找到制指定要修改的MCA信息，initMca()和updateMcaIdCert()两个更新函数分别执行更新MCA信息和更新MCA身份证书的功能。McaDao类为上层类提供了与数据库进行信息交互的接口，以便将更新的信息写入数据库表中。

用户证书管理相关的功能类图设计如图5.5所示。

MCA类图

图5.5 MCA管理类图

MCA管理模块的功能时序图设计如图5.6所示。

安全管理员在管理端执行MCA信息更新操作，按界面提示输入需要更新的参数后，管理端将这些信息传递到服务端。服务端先对各项参数进行校对，确认数据合法后将更新参数写入数据库。数据库执行完毕更新语句后将结果反馈给服务端，服务端将操作的结束信息反馈给管理端，同时将此次行为记入系统日志中，最终管理端在界面上展示操作成功的提示。执行MCA身份证书更新的操作与之类似，管理员在界面上进行证书更新的请求，服务端收到请求且校验无误后令数据库执行证书内容的更新操作，然后反馈结果并记入日志。

MCA时序图

图5.6 MCA管理时序图

5.3.3 业务CA管理设计

在业务CA管理模块，OcaInfo表征业务CA的各项关键信息；FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由OcaController类实现。业务CA的基础操作的新增、作废、修改功能分别由createOca()、deleteOca()和updateAdmin()方法实现，查询CA详情和列表功能由queryOca()方法实现。此外，为实现业务证书的签发和导入，还设有issueSubOca()和importSubOca()两种方法。

Service层的功能由OcaService类与TemplateService类共同提供。OcaService类负责封装与业务证书信息和证书实体相关的服务，TemplateService类负责封装与证书模板相关的服务。TemplateDao类与OcaDao类为上层提供了与数据库进行信息交互的接口。业务CA管理相关的功能类图设计如图5.7所示。



图5.7 业务CA管理类图

进行CA证书导入时，安全管理员选择一条记录，点击导入按钮，输入相关信息，管理端将导入的内容传递到服务端。服务端调用数据库中模板进行校验，确认导入证书格式合法，然后将其写入数据库。数据库执行完毕后将结果反馈给服务端，服务端将操作的结束信息反馈给管理端，页面提示导入成功；同时将此次行为的相关信息录入系统日志中。

进行业务CA的证书签发时，安全管理员选择根CA，点击签发按钮，选择或输入相关信息，点击确认，服务端收到管理端的数据之后会调用现有的模板，将管理员输入的内容填入模板中而后使用国密算法进行签名，生成一张证书，而后将证书存入数据库中，并使管理端告知管理员，证书已签发、可下载，并将本次操作记入日志中。

进行业务CA的新增、查询、停/启用等管理操作时，安全管理员选择相应功能，在管理端根据提示输入主题、类型、服务状态、密钥索引等必要参数。服务端先对各项参数进行校验，确认数据正常后将命令数据库执行相关操作。数据库执行完毕后将结果反馈给服务端，同时服务端将此次行为的相关信息录入系统日志中。最终收到服务端通知的管理端在界面上告知管理员操作结果。

业务CA管理模块的时序图设计如图5.8所示。

业务CA时序图

图5.8业务CA管理时序图

5.3.4 系统安全功能设计

在系统安全模块，Shamir是与门限信息相关的实体类，SafetyAdmin类是与安全管理员信息相关的实体类。FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由ShamirController类实现。updateShamir()实现密钥持有者更新功能，acivateSystem()实现激活系统功能，updateSafeAdminPwd()实现安全管理员口令更新功能。

Service层的功能由ShamirService类与SafeAdminService类共同提供。ShamirService类负责门限信息更新的方法，SafeAdminService类负责封装与安全管理员信息相关的服务。ShamirDao类与SafeAdminDao类分别为上层提供了与门限信息表和安全管理员信息表进行数据交互的接口。

系统安全相关的功能类图设计如图5.9所示。

安全管理员其它类图

图5.9 系统安全功能类图

以系统安全模块中的密钥持有者更新为例，其功能时序图设计如图5.10所示。安全管理员在管理端进行密钥持有者更新的操作，根据提示输入密钥持有者名称、口令、存储介质、设备口令等修改参数后，管理端将需要修改的密钥持有者信息传递到服务端。为了系统安全，服务端首先关闭相关的门限，确认数据合法后将向数据库请求执行相关数据更新操作。数据库执行完毕后将结果反馈给服务端，服务端将操作的结束信息反馈给管理端，此时系统进行门限恢复操作，开放进出许可；同时将此次行为的相关信息录入系统日志中。最终管理端在界面上告知管理员更新成功。

安全管理员其它时序图

图5.10 密钥持有者更新时序图

5.4 业务员模块设计

业务员模块主要为安全认证与管理业务中的业务员所设计，下辖五个子模块：RA管理、终端证书管理、证书模板管理、互联信息管理及系统业务功能，每个模块又包括详细实现模块业务的子功能。本节将介绍这五个子模块的详细设计与难点解决情况。

5.4.1 RA管理设计

在RA管理模块，RaInfo类是实体类，表征用户证书的各项关键信息；FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由RaController类实现。类中包含六个函数，实现模块的各项功能。新增RA功能由createRa()方法实现；更新用户证书功能由updateRa()方法实现；查询用户证书功能由queryRa()方法实现；作废用户证书功能由deleteRa()方法实现；RA授权功能由updateRaPermission()方法实现；RA状态切换功能由updateRaStatus()方法实现。Service层的功能由RaService类实现。类中和Controller层类似封装了可以实现模块功能的函数方法。RaDao类为上层类提供了与数据库进行信息交互的接口，以便完成Ra信息表中数据的读写。

RA管理相关的功能类图设计如图5.11所示。

RA类图

图5.11 RA管理类图

业务CA管理模块的时序图设计如图5.12所示。

进行RA的新增、查询等管理操作时，业务员选择相应功能，在RA管理页面上根据提示输入名称、主题、序列号、IP类型等参数。服务端先对各项参数进行校验，确认数据正常后将命令数据库执行相关操作。数据库执行完毕后将结果反馈给服务端，同时服务端将此次行为的相关信息录入系统日志中。最终收到服务端通知的管理端在界面上告知业务员操作结果。

进行RA授权时，业务员在界面上选择一个RA，点击授权按钮，输入相关信息，管理端将导入的内容传递到服务端。服务端判断此授权是否违背了业务条例，确认无误后向数据库发出写入请求。数据库执行完毕后将结果反馈给服务端，服务端将操作的结束信息反馈给管理端，同时将此次行为的相关信息录入系统日志中。最终管理页面提示授权成功。

进行RA的状态更改时，业务员选择相应的RA，点击停用/启用按钮，在弹出的提示框中点击确认，服务端收到管理端的请求，调用数据库更改相关RA的状态参数，完成后反馈并使管理端告知管理员，RA状态已更改，并将本次操作记入日志中。

RA时序图

图5.12 RA管理时序图

5.4.2 终端证书管理设计

在终端证书管理模块，实体类包含CertInfo类、CertEntity类和CertRevoke类，CertInfo表征业务CA的各项关键信息；CertEntity记录了业务CA证书的实体信息；CertRevoke表征被作废的终端证书信息。FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由TerminalCertController类实现。对终端证书的查询功能由queryTerminalCert()函数实现，对终端证书的作废功能由cancelTerminalCert()函数实现。

Service层的功能由TerminalCertService类实现。类中封装了和Controller层同名的函数方法，用以提供处理服务。Dao层的功能由TerminalCertSDao类实现，它为上层提供了对数据库中相关证书进行查询与作废的接口。

终端证书管理相关的功能类图设计如图5.13所示。



图5.13 终端证书管理类图

终端证书管理模块的时序图设计如图5.14所示。

业务员进行终端证书的查询操作时，在界上面输入检索条件后，管理端将这些信息传递到服务端。服务端根据这些限制条件从数据库中获取相应的证书信息。获得数据后，服务端将数据反馈给管理端，同时将此次行为记入系统日志中。最终管理端在界面上将查询结果的重要信息以列表的形式展示出来，点击每条信息可查看该证书的详情。

业务员在进行终端证书的作废操作时需要先通过查询功能找到该信息，而后在界面上点击其信息栏右侧的作废按钮，确认之后管理端向服务端发出作废申请，服务端接收到请求后将数据库中的对应证书标记为已作废，并在证书作废表中添加上此证书的相关信息，而后反馈给管理端，管理端提示业务员操作成功。

终端证书时序图

图5.14 终端证书管理时序图

5.4.3 证书模板管理设计

在证书模板管理模块，Template类是实体类，表征证书模板的各项关键信息；FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统工作的相关过程，汇总成为日志信息。

Controller层的功能由TemplateController类实现。类中包含四个函数，实现模块的各项功能。新增模板功能由createTemplate()方法实现；更新现有模板功能由updateTemplate()方法实现；查询证书模板功能由queryTemplate()方法实现；删除模板功能由deleteTemplate()方法实现。Service层的功能由TemplateService类实现。类中和Controller层类似封装了可以实现模块功能的函数方法。TemplateDao类为上层类提供了与数据库进行信息交互的接口，以便完成证书模板表中数据的读写。

证书模板管理相关的功能类图设计如图5.15所示。

证书模板类图

图5.15 证书模板管理类图

证书模板管理模块的功能时序图设计如图5.16所示。业务员在管理端执行如新增、修改等证书模板管理操作时，选择界面上的不同功能，根据要求输入或选择名称、有效期、类型等参数，管理端将这些信息传递到服务端。服务端先对各项参数进行预处理，将处理后的数据转为SQL语句向数据库发出指令。数据库执行指令完毕后将结果反馈给服务端，服务端将操作的结束信息反馈给管理端，同时将此次行为的相关信息录入系统日志中，最终管理端在界面上告知业务员操作结果。

证书模板时序图

图5.16 证书模板管理时序图

5.4.4 互联信息管理设计

在互联信息管理模块，InterConnectionInfo类是实体类，在系统中记录互联系统的相关信息；FileLogger类是记录日志而设置的工具类，在系统执行用户的操作时负责记录系统的工作日志。

Controller层的功能由InterConnectionController类实现。新增互联信息由createInterConnectionInfo()方法实现；删除互联信息由deleteInterConnectionInfo()方法实现；更新互联信息由updateInterConnectionInfo()方法实现；查询互联信息由queryInterConnectionInfo()方法实现。

Service层的功能由InterConnectionService类实现。类中和Controller层类似封装了可以实现模块功能的函数方法。Dao层功能由InterConnectionDao类实现，它为上层类提供了与数据库进行信息交互的接口，以便完成互联信息表数据的读写。

互联信息管理相关的功能类图设计如图5.17所示。

互联信息类图图5.17 互联信息管理类图

互联信息管理模块的功能时序图设计如图5.18所示。

业务员在互联信息配置的管理端页面上，选择相应的管理功能，根据系统要求和选项输入必要参数。服务端先对输入的互联信息进行格式、内容等方面的核对，确认数据合法后调用与数据库的接口，对数据库执行读取或写入的操作。数据库执行完毕后将结果反馈给服务端。服务端在完成所有工作后反馈管理端，使其在界面上通知管理员操作结果，同时还会调用日志工具将此次行为的相关信息录入系统日志中。

互联信息时序图

图5.18 互联信息管理时序图

5.4.5 系统业务功能设计

在系统业务功能模块，HardwareUtil类是为了获取系统硬件相关信息而设置的工具类，负责读取系统的内存、硬盘、CPU等使用情况；FileLogger类是记录日志而设置的工具类，将系统工作的相关过程汇总成为日志信息。

Controller层的功能由SystemController类实现。CRL配置功能由updateCrl()函数实现，证书归档策略配置由updateCertArchiveTime()函数实现，终端证书统计功能由queryCertNumber()函数实现，业务CA查询功能由queryOca()函数实现，CRL配置功能由queryDeviceInfo()函数实现。

Service层的功能由OcaService类与TerminalCertService类共同提供。OcaService类负责封装CRL配置、业务CA查询相关的服务，TerminalCertService类负责封装与证书归档策略、终端证书统计相关的服务。

Dao层的功能由OcaDao类与TerminalCertDao类共同实现。分别为上层提供了与业务CA信息表和终端证书信息表进行数据交互的接口。

系统业务相关的功能类图设计如图5.19所示。

系统业务类图 新

图5.19 系统业务类图

系统业务功能模块的功能时序图设计如图5.20所示。业务员在管理端执行如CRL配置、证书归档策略配置等系统业务操作时，业务员可以通过相关页面上提供的空栏输入目标的配置内容，管理端会将这些数据传递给服务端。服务端获得数据之后对数据进行处理，而后调用数据库，将配置的信息写入对应的数据表单之中，完成配置修改。服务端将完成信息反馈给管理端，由管理端告知业务员操作成功，并将本次行为记录进系统日志中。当业务员点击进入硬件信息详情页面时，服务端会自动调用函数抓取内存、硬盘、CPU等重要硬件的当前状态，并在管理端页面以统计图的形式直观地向业务员展示出来。

业务其它时序图

图5.20 系统业务时序图

5.5 数据库设计

本文所设计的车联网安全认证管理系统包含大量数据。为有效对这些信息进行存储，采用关系型数据库MySQL对系统进行数据管理。在设计时既要考虑到数据的安全同时也要兼顾数据存取的效率。

根据本章前面几节的详细设计内容，本节将选取与系统核心功能有关的数据关系，做出如下的数据库逻辑结构设计。

5.5.1 安全管理员数据模型设计

安全管理员模块：安全管理员与用户证书、MCA、业务CA及门限信息相关的E-R关系图如图5.21所示，安全管理员可以对数据库中保存的用户证书、门限信息等安全相关数据进行管理。

安全管理员ER图5.21 安全管理员模块E-R图

根据数据模型，可以对安全管理员模块的相关数据表单进行如下设计：

（1）管理员信息表，主要存储管理员相关信息。其中主要属性包括ID、名称、管理员证书主题、角色、权限、邮箱、地址、手机、座机、状态、口令。详细说明如表5.3所示。

表5.3 管理员信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 自增 |
| NAME | 名称 | VARCHAR(64) | 非空 |  |
| SUBJECT | 管理员证书主题 | VARCHAR(255) | 非空 |  |
| ROLR | 角色 | VARCHAR(2) | 非空 | 该管理员在对应OCA下的角色 |
| PERMISSION | 权限 | VARCHAR(2048) |  |  |
| EMAIL | 邮箱 | VARCHAR(128) |  |  |
| ADDRESS | 地址 | VARCHAR(128) |  |  |
| CELLPHONE | 手机 | VARCHAR(11) |  |  |
| TELPHONE | 座机 | VARCHAR(20) |  |  |
| OPRSTATUS | 状态 | NUMERIC(1) | 非空 | 0无效 1有效 |
| PWD | 口令 | VARCHAR(128) |  | 作为预留，用key登录不需要 |

（2）业务CA信息表，主要存储业务CA的相关信息。其中主要属性包括ID、内部名称、证书主题、证书标准、CA类别、曲线类型、生效时间、失效时间、CRL名称、密码设备名称、签名算法、密钥长度、模板名称等。详细说明如表5.4所示。

表5.4 业务CA信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 自增 |
| OCANAME | OCA内部名称 | VARCHAR(64) | 唯一索引,非空 | OCA内部名称； 字段值作为证书表的列表分区字段，全部大写存储 |
| SUBJECT | 证书主题 | VARCHAR(255) | 非空 |  |
| CRLNAME | CRL名称 | VARCHAR(128) |  |  |
| CERTSTANDARD | 证书标准 | VARCHAR(32) | 非空 |  |
| CATYPE | CA类别 | VARCHAR(2) | 非空 |  |
| CURVENAME | 曲线类型 | NUMERIC(1) | 非空 | 曲线名称0:SM2,1:P256,2:P256rl |
| NOTBEFORE | 生效时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| NOTAFTER | 失效时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| CRLINTERVAL | 过期多长证书进行归档 | NUMERIC(10) |  | 发布CRL间隔，单位分钟 |
| ARCHIVETIME | CRL发布间隔周期 | NUMERIC(5) |  | 过期多长证书被自动归档.单位天 |
| HSM | 密码设备名称 | VARCHAR(10) | 非空 |  |
| SIGNALG | 签名算法 | VARCHAR(16) | 非空 | 默认SM3withSM2 |
| KEYSIZE | 密钥长度 | NUMERIC(4) | 非空 |  |
| KEYINDEX | 密钥编号 | NUMERIC(4) | 非空 |  |
| KEYPWD | 密钥口令 | VARCHAR(64) | 非空 | SM4加密后的密钥口令 |
| OCASTATUS | OCA状态 | NUMERIC(1) | 非空 | 0：为完成初始化 1：运行 |
| CERTURL | CRL服务器地址 | VARCHAR(128) |  |  |
| PASSWORD | CRL服务器用户口令 | VARCHAR(64) |  |  |
| USERNAME | CRL服务器用户名 | VARCHAR(32) |  |  |
| TEMPLATENAME | 模板名称 | VARCHAR(50) | 非空 |  |

（3）业务CA证书实体表，主要存储业务CA证书的实体数据。其中主要属性包括ID、证书主题、CA类型、证书实体、证书实体哈希、上级证书主题、加入时间、证书状态。详细说明如表5.5所示。

表5.5 业务CA证书实体表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 |  |
| SUBJECT | 证书主题 | VARCHAR(255) | 普通索引,非空 |  |
| CATYPE | CA类型 | VARCHAR(2) | 非空 | 00 : 根机构 01 注册机构 02 授权机构 03 注册证书 04 授权证书 05 CRLSigner |
| SUPCASUBJECT | 上级CA主题 | VARCHAR(255) |  |  |
| CERTENTITY | 证书实体 | VARCHAR(2048) | 非空 | Base64编码的证书实体 |
| CERTHASH | 证书哈希 | VARCHAR(64) | 非空 | 证书使用SM3哈希后的值，16进制保存 |
| ADDTIME | 加入时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| CERTSTATUS | 证书状态 | NUMERIC(1) | 非空 | 0作废,1有效 |

（4）用户证书信息表，主要用户证书相关数据。其中主要属性包括ID、证书序列号、证书主题、证书用途、生效时间、失效时间、证书实体信息。详细说明如表5.6所示。

表5.6 用户证书信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 自增 |
| CERTSN | 证书序列号 | VARCHAR(20) | 非空  唯一索引 |  |
| SUBJECT | 用户证书主题 | VARCHAR(255) | 非空  唯一索引 |  |
| TYPE | 证书用途 | NUMERIC(1) | 非空 | 0:系统证书 1：登录证书 |
| NOTBEFORE | 生效时间 | NUMERIC(20) | 非空 | 毫秒值 |
| NOTAFTER | 失效时间 | NUMERIC(20) | 非空 | 毫秒值 |
| CERT | 证书实体信息 | VARCHAR(2048) | 非空 | 证书实体信息以Base64编码存储 |

（5）门限信息表，主要存储门限相关数据。其中主要属性包括ID、证书主题、业务CA名称、证书类型、证书实体、证书实体哈希、加入时间、周期数据、周期种子值、LA身份信息。详细说明如表5.7所示。

表5.7 门限信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| KEYHASH | SM3哈希后的秘闻片段值 | VARCHAR(64) | 主键 | 密钥被SM3哈希运算后的16进制，全部大写保存 |
| SHAMIRN | 最大密钥持有者 | NUMERIC(2) | 非空 |  |
| SHAMIRM | 最小恢复数 | NUMERIC(2) | 非空 |  |

5.5.2 业务员数据模型设计

业务员ER业务员与终端证书、RA、互联信息及模板信息相关的E-R关系图如图5.22所示。

图5.22 业务员模块E-R图

根据数据模型，可以对业务员模块的相关数据表单进行如下设计：

1. RA信息表，主要存储对接的RA相关信息。其中主要属性包括ID、RA名称、证书序列号、证书主题、网络类型、网络地址、权限、联系地址、手机号码、创建日期、状态等。详细说明如表5.8所示。

表5.8 RA信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 |  |
| RANAME | RA名称 | VARCHAR(32) | 非空 | 名称和ocaName联合唯一 |
| OCANAME | 业务CA内部名 | VARCHAR(64) | 非空 |  |
| CERTSN | RA证书序列号 | VARCHAR(32) | 非空 | 16进制编码，与ocaName联合唯一 |
| SUBJECT | 证书主题 | VARCHAR(255) | 非空 |  |
| IPTYPE | 网络类型 | NUMERIC(1) | 非空 | 0：IPV4;1:IPV6 2:域名 |
| IP | 网络地址 | VARCHAR(256) | 非空 | 前期支持一个，后期支持多个IP地址 |
| PERMISSION | 权限 | VARCHAR(2048) |  | 针对OCA的业务模块授权，对终端设备证书的操作 |
| EMAIL | 邮件地址 | VARCHAR(128) |  |  |
| ADDRESS | 联系地址 | VARCHAR(128) |  |  |
| CELLPHONE | 手机号码 | VARCHAR(11) |  |  |
| TELPHONE | 座机号码 | VARCHAR(20) |  |  |
| ADDTIME | 创建日期 | NUMERIC(20) | 非空 |  |
| OPRSTATUS | 状态 | NUMERIC(1) | 非空 | 0无效 1有效 |

1. 互联信息表，主要存储和系统互联的其他系统的相关信息。其中主要属性包括ID、OCA内部名称、服务地址、系统身份证书信息、证书哈希、服务类型。详细说明如表5.9所示。

表5.9 互联信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 自增 |
| OCANAME | OCA内部名称 | VARCHAR(64) | 非空 |  |
| NAME | 名称 | VARCHAR(32) | 非空 | 与ocaname联合唯一 |
| URL | 服务地址 | VARCHAR(256) | 非空 |  |
| CERT | 系统身份证书信息 | VARCHAR(4000) | 非空 | 证书实体，Base64编码存储 |
| HSAHID | 证书哈希 | VARCHAR(64) | 非空 |  |
| TYPE | 服务类型 | NUMERIC(1) | 非空 |  |

（3）终端证书信息表，主要存储终端证书的相关信息。其中主要属性包括ID、证书主题、业务CA名称、证书类型、开始时间、结束时间、是否发布CRL、模板名称、公钥哈希、随机数、CRL版本号、撤销CA表示符、设备标识。详细说明如表5.10所示。

表5.10 终端证书信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 |  |
| SUBJECT | 证书主题 | VARCHAR(255) | 非空 | 最大32字节 |
| OCANAME | 业务CA名称 | VARCHAR(64) | 非空 | 业务CA的名称，与OCAINGO表中的OCANAME一致 |
| CERTTYPE | 证书类型 | VARCHAR(2) | 非空 |  |
| NOTBEFOR | 开始时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| NOTAFTER | 结束时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| TEMPLATENAME | 模板名称 | VARCHAR(32) | 非空 |  |
| ISCRL | 是否发布CRL | VARCHAR(1) | 非空 | F不发布，T发布，根据模板定 |
| PUBKEYHASH | 公钥哈希 | VARCHAR(64) | 非空 | 使用SM3对证书签名公钥进行hash后十六进制存储 |
| REFCODE | 随机数 | VARCHAR(8) | 可空 |  |
| CERTSTATUS | 状态 | NUMERIC(1) | 非空 | 默认2，2 正常 3 冻结 4 作废 |
| CRLSERIES | CRL版本号 | INT（16） | 非空 | 默认0，根据模板配置信息来存储 |
| CRACAID | 撤销CA表示符 | VARCHAR（6） | 非空 | 默认000000 16禁止存储 |
| UUID | 设备标识 | VARCHAR（128） | 可空 | 设备标识 |

（4）模板表，主要存储证书模板的相关信息。其中主要属性包括ID、名称、模板内容、是否被使用、是否可修改、模板类型、是否发布CRL、有效期。详细说明如表5.11所示。

表5.11 模板表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 自增 |
| NAME | 名称 | VARCHAR(32) | 非空 | 模板名，唯一，大写存储 |
| CONTENT | 模板内容 | VARCHAR(4000) | 非空 | 模板内容JSON格式存储，包含证书有效期，权限等扩展信息 |

续表5.11 模板表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ISUSED | 是否被使用 | VARCHAR(1) | 非空 | T：已使用,F：未使用，已被使用的模板不可在修改 |
| MODIF | 是否可修改 | VARCHAR(1) | 非空 | T：可修改,F：不可修改 |
| TYPE | 模板类型 | VARCHAR(2) | 非空 |  |
| CRL | 是否发布CRL | VARCHAR(1) | 非空 | T：发布,F：不发布 |
| VALIDITY | 有效期 | VARCHAR(32) | 非空 | 申请的证书不能超过此有效期，单位为年 |

（5）终端证书实体表，主要存储终端证书的实体数据。其中主要属性包括ID、证书主题、业务CA名称、证书类型、证书实体、证书实体哈希、加入时间、周期数据、周期种子值、LA身份信息。详细说明如表5.12所示。

表5.12 终端证书实体表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 对应certinfo表中id |
| SUBJECT | 证书主题 | VARCHAR(255) | 普通索引,非空 |  |
| OCANAME | 业务CA名称 | VARCHAR(64) | 非空 |  |
| CERTTYPE | 证书类型 | VARCHAR(2) | 非空 |  |
| CERT | 证书实体 | VARCHAR(2048) | 非空 |  |
| HASHID | 证书实体哈希值 | VARCHAR(64) | 非空 | 证书哈希的值16进制编码 |
| ADDTIME | 加入时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| IPERIOD | 周期数据 | NUMERIC(16) | 可空 | 自系统运行开始的第几周 |
| LSI | 周期种子值 | VARCHAR(32) | 可空 | 16进制存储 |
| LAID | LA身份信息 | VARCHAR(4) | 可空 | 16进制存储 |

（6）终端证书作废表，主要存储终端证书的作废信息。其中主要属性包括ID、证书主题、业务CA名称、证书类型、证书HashID、证书过期时间、作废时间、CRL版本号、撤销CA表示符、周期数据、周期种子值、LA身份信息。详细说明如表5.13所示。

表5.13 终端证书作废表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| ID | id | INT(16) | 主键 | 自增 |
| SUBJECT | 证书主题 | VARCHAR(255) | 普通索引，非空 |  |
| OCANAME | 业务CA名称 | VARCHAR(64) | 非空 |  |
| CERTTYPE | 证书类型 | VARCHAR(2) | 非空 |  |

续表5.13 终端证书作废表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段意义 | 数据类型 | 约束 | 说明 |
| HASHID | 证书HashID | VARCHAR(64) | 非空 | 证书哈希16进制编码 |
| NOTAFTER | 证书过期时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| REVOKETIME | 作废时间 | NUMERIC(20) | 非空 | 时间戳格式 |
| CRLSERIES | CRL版本号 | INT（16） |  | 默认0 |
| CRACAID | 撤销CA表示符 | VARCHAR（6） |  | 默认000000 16进制存储 |
| IPERIOD | 周期数据 | NUMERIC(16) | 可空 | 自系统运行开始的第几周 |
| LSI | 周期种子值 | VARCHAR(32) | 可空 | 16进制存储 |
| LAID | LA身份信息 | VARCHAR(4) | 可空 | 16进制存储 |

5.5.3 安全认证业务数据模型设计

业务ER安全认证业务中的各项信息相关的E-R关系图如图5.23所示。系统在进行安全认证业务时通过业务CA和证书模板的数据签发终端证书并存入数据表，再根据RA信息表里的记录对相应的对象提供下载许可。

图5.23 安全认证业务E-R图

安全认证业务相关的各项数据表单均在前文进行了详细设计，在此不再重复叙述。

5.6 本章小结

本章在论文前几章的基础上，对管理子系统的安全管理员、业务员这两大重要功能模块以及业务子系统核心的证书服务流程进行了详细设计，从动态与静态两个角度出发分析实现系统的运行逻辑，设计了消息格式、证书模板，并详细阐述了证书签发、更新、作废等业务执行过程。

第6章 系统实现与测试

6.1 系统的部署实现

在系统开发完成后，则需要将其部署到实际场景中并调试无误。系统部署到装有Linux操作系统的服务器上，部署过程如下：

1. 创建/opt/v2xca目录，解压程序压缩包至此处并使用sql文件创建数据库及各表单。而后进入数据库配置文件所在目录，执行命令修改hibernate.cfg.xml文件中的信息；
2. 执行命令进入v2x-ca-m目录，使用./start.sh命令启动管理子系统；执行命令进入v2x-ca-s目录，使用./startup.sh命令启动业务子系统；
3. 在本地hosts文件和服务器中/etc/hosts文件中配置域名。

部署完成后使用PC的Google Chrome浏览器即可通过域名访问管理页面，初次进入系统需要按指引完成激活操作，如图6.1所示。



图6.1 系统激活界面

点击按钮开始激活，进入如图6.2所示配置界面，依次配置数据库、加密机、门限方案等重要参数，完成系统的激活与初始化。



图6.2 系统配置界面

激活成功后刷新页面，即可进入如图6.3所示的登录界面，根据个人在管理规则中被分配的角色，选择使用证书登录或口令登录。



图6.3 系统登录界面

登录后，页面以简洁风格呈现，方便操作员快速进行工作。系统左侧显示可执行的功能，右侧显示操作详情界面。根据个人权限的不同，页面左侧的功能也不同，如业务操作员登录后即显示如图6.4所示的操作界面。



图6.4 业务操作界面

6.2 测试概要

6.2.1 测试概述

在系统部署完成后，需要对其进行各方面的测试，通过测试结果判断其是否满足了前期需求分析和系统设计的目标。同时，针对测试过程中发现的异常，还需要进行针对性的优化，解决相应的问题。

本文中根据前几个阶段所做的工作，将系统测试分为功能测试与性能测试两个部分。功能测试部分主要检测系统所包含的各项功能是否能够正常使用、有无逻辑问题，性能测试部分主要检测系统的响应速度、处理能力、安全性等方面是否符合现实使用的预期。由于系统规模较大，需要测试部门额外支持，同时受论文性质和组织内容的限制，本章将选取部分核心业务的测试用例，从整体上得出系统的测试结论。

6.2.2 测试环境

测试环境尽量模拟系统实际运行与日常使用的软硬件环境，与前期需求分析的结果应该相互映照。基于以上原则，系统测试所选取的硬件与软件环境配置如表6.1和表6.2所示。

测试的PC机搭载Windows 10操作系统，使用100M的局域网访问系统。系统部署在32G内存、800G容量的前后端服务器上，数据库版本为MySQL 5.7，服务器选择16G内存、300G硬盘。

表6.1 测试硬件环境表

|  |  |
| --- | --- |
| 硬件 | 配置 |
| 测试pc机 | CPU:core（TM） i5-1035 CPU@1.00GHz |
| 内存：8GB |
| 主机硬盘：1TB |
| 操作系统：windows 10 |
| 网络：100M局域网 |
| 前后端服务器 | 操作系统：Oracle Linux Server release 6.8  内存：32G  容量：800G  Cpu：8核 |
| 数据库服务器 | CPU：Intel(R) Xeon(R) CPU E7-8867 v4 @ 2.40GHz 2.39GHz  内存：16G，硬盘：300G  操作系统：64位Windows Server 2012 R2 Datacenter |
| 数据库服务器 | CPU：Intel(R) Xeon(R) CPU E7-8867 v4 @ 2.40GHz 2.39GHz  内存：16G，硬盘：300G  操作系统：64位Windows Server 2012 R2 Datacenter |

表6.2 测试软件环境表

|  |  |
| --- | --- |
| 软件 | 配置 |
| 操作系统 | Windows 10 |
| 数据库 | Mysql 5.7 |
| 中间件 | nginx/1.9.15 |
| jdk | openjdk version "1.8.0\_252" |
| 客户端浏览器 | Chrome 84 |

6.3 系统功能测试

6.3.1 测试需求

本部分测试为车联网安全认证管理系统的功能测试，根据前期需求分析与系统设计的预期目标对车联网安全认证管理系统功能进行测试。同时，对测试结果进行统计分析，验证数据准确性、业务逻辑功能正确性，核实所有功能均已正常实现，描述系统能否满足功能要求。系统的功能测试范围及重点如表6.3所示。

表6.3 功能测试范围表

|  |  |  |
| --- | --- | --- |
| 模块 | 功能 | 测试重点 |
| 初始化 | 系统初始化 | 需对初始化的整个流程进行测试，判断配置数据库、加密机、管理证书的信息、安全管理员信息、密钥持有者信息等步骤数据是否正常。 |
| 登录 | 用户登录 | 对两种登录方式进行测试，验证两种登录方式的控制逻辑是否都正常，同时还需核验错误信息的处理和提示信息抛出 |
| 超级管理员 | 管理员管理 | 测试其添加管理员以及给其赋予管理员的权限这两个主要功能是否正常，以及对于非法数据如何处理、异常数据处理流考虑是否完善 |
| 安全管理员 | MCA管理 | 重点测试部分应倾向于MCA管理、业务CA管理及用户证书管理，另外其负责的系统激活、口令更新等模块也应当测试其逻辑正确性与成功情况 |
| 业务CA管理 |
| 用户证书管理 |
| 系统安全管理 |
| 业务管理员 | 业务员管理 | 测试其管理业务员基本信息以及给其赋予业务员的权限这两个主要功能是否正常，以及对于非法数据如何处理、异常数据处理流考虑是否完善 |
| 审计管理员 | 审计员管理 | 测试其管理审计员基本信息以及给其赋予审计员的权限这两个主要功能是否正常 |

续表6.3 功能测试范围表

|  |  |  |
| --- | --- | --- |
| 模块 | 功能 | 测试重点 |
| 业务员 | RA管理 | 测试其对互联信息、RA信息、证书模板及终端证书的管理功能是否正常，此外还要测试CRL的配置、证书归档策略配置的流程在逻辑上是否正确，对硬件参数的信息查询与返回是否可以顺利完成等 |
| 终端证书管理 |
| 证书模板管理 |
| 互联信息管理 |
| 系统业务 |
| 审计员 | 日志审计 | 测试审计员查看日志的返回结果是否完全，日志审计与日志归档在完成任务的情况下是否合规，以及日志下载功能是否可用，下载的日志信息是否有乱码 |
| 日志归档 |
| 日志下载 |
| 业务子系统 | 证书申请 | 验证业务流程符合设计原则且步骤正确，同时还要保证证书、报文等信息的正确性，以及无效申请的处理结果符合规范 |
| 证书更新 |
| 证书作废 |
| 证书验证 |

6.3.2 测试设计

功能测试的方式目标在于测试系统是否满足前期功能设计。本文在系统全部完成后的总体功能测试阶段，采用黑盒测试的方法，屏蔽掉系统内层的逻辑与各种细节，通过模拟用户日常的使用方式来测试系统的各项功能，合法的操作返回正确结果、非法操作抛出异常提示信息，最终判断系统的功能是否满足了前期的设计理念。

由于篇幅限制，本节以车联网安全认证管理系统中管理子系统的业务员模块为例来进行测试用例的设计。

表6.4即为业务员模块中RA管理功能的测试用例。在该页面中，已录入的全部RA信息作为页面主题展示给用户。用户可以根据自己的需要点击相关的按钮，通过输入必要条件之后点击确定，让系统按预定目标进行运作，成功后返回响应结果，失败后返回失败提示并告知相关原因。

表6.4 RA管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 用例名称 | 业务员-RA管理 |
| 用例类别 | 功能测试 |
| 测试目标 | 1. 验证业务员是否可以对RA信息进行管理 2. 验证业务员是否可以对已录入的RA进行授权操作 3. 验证业务员是否可以更改RA的当前状态 |

续表6.4 RA管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 前置条件 | 1. 用户已登录 2. 用户拥有业务员相关权限 |
| 测试流程 | 1. 测试员点击新增/查询/删除/修改按钮，弹出弹窗，在弹窗内输入关键信息，点击确定，等待系统返回结果 2. 测试员点击权限按钮，弹出弹窗，在弹窗内勾选/取消勾选各种权限，点击确定，等待系统返回结果 3. 测试员点击启用/停用按钮，等待系统弹出操作结果 |
| 预期结果 | 1. 用户可以通过点按按钮，对RA信息进行管理操作，包括添加、删除、修改及查询，且进行操作后会有成功或失败原因的弹窗提醒 2. 用户可以对数据库中目前已保存的RA进行权限授予/收回操作，进行操作后RA的权限会发生变化，限制对应实体在本系统的功能 3. 用户可以对数据库中目前已保存的RA进行状态切换，切换为启用状态后对应RA才能向本系统进行业务申请 |
| 实际结果 | 和预期结果相同 |
| 结论 | 功能正常，测试通过 |

表6.5即为业务员模块中终端证书管理功能的测试用例。在该页面中，已录入的相关终端证书信息作为页面主题展示给用户。用户可以根据自己的需要输入必要条件之后点击搜索，查看已保存的证书信息，或是选择要作废的证书，操作系统将其作废。

表6.5 终端证书管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 用例名称 | 业务员-终端证书管理 |
| 用例类别 | 功能测试 |
| 测试目标 | 1. 验证业务员是否可以对终端证书信息进行搜索与查看 2. 验证业务员是否可以作废选定的证书信息 |
| 前置条件 | 1. 用户已登录 2. 用户拥有业务员相关权限 |
| 测试流程 | 1. 测试员输入检索条件，点击检索，等待系统返回结果，而后点击重置 2. 测试员点击检索结果中的某一证书，等待弹出详情弹窗 3. 测试员点击某一证书作废按钮，弹出弹窗，点击确定，等待系统返回结果 |

续表6.5 终端证书管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 测试流程 | 1. 测试员输入检索条件，点击检索，等待系统返回结果，而后点击重置 2. 测试员点击检索结果中的某一证书，等待弹出详情弹窗 3. 测试员点击某一证书作废按钮，弹出弹窗，点击确定，等待系统返回结果 |
| 预期结果 | 1. 用户可以通过输入查询条件并检索，查看到所有符合条件的证书信息，重置条件后检索列表又恢复到默认状态 2. 点击结果列表中的查询按钮，可以查看这份证书的详细信息，但不可进行更改 3. 点击证书的作废按钮后，系统会二次确认是否执行操作，确定后执行 |
| 实际结果 | 和预期结果相同 |
| 结论 | 功能正常，测试通过 |

表6.6即为业务员模块中证书模板管理功能的测试用例。在该页面中，已设置的相关证书模板信息作为页面主体展示给用户。用户可以根据自己的需要点击相应按钮，对模板进行添加、修改、作废操作。输入各项必填信息后，相关模板会自动更新其在数据库内的存储内容。此外，还可以输入必要条件之后点击搜索，查看已保存的模板信息，符合检索条件的模板相关创建信息详细内容信息都将被展示。

表6.6 证书模板管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 用例名称 | 业务员-证书模板管理 |
| 用例类别 | 功能测试 |
| 测试目标 | 1. 验证业务员是否可以对证书模板信息进行管理操作 |
| 前置条件 | 1. 用户已登录 2. 用户拥有业务员相关权限 |
| 测试流程 | 1. 测试员输入检索条件，点击检索，等待系统返回结果，而后点击重置 2. 测试员点击检索结果中的某一模板，等待弹出详情弹窗 3. 测试员点击新增按钮，弹出弹窗，在弹窗内输入关键信息，点击确定，等待系统返回结果 4. 测试员点击某一模板的删除按钮，弹出弹窗，点击确定，等系统返回结果 5. 测试员点击某一模板的修改按钮，弹出弹窗，在弹窗内输入关键信息，点击确定，等待系统返回结果 |

续表6.6 证书模板管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 预期结果 | 1. 用户可以通过输入查询条件并检索，查看到所有符合条件的模板信息，重置条件后检索列表又恢复到默认状态 2. 用户可以通过点按按钮，对证书模板信息进行添加、修改操作，且进行操作后会有成功或失败原因的弹窗提醒 3. 点击模板的作废按钮后，系统会二次确认是否执行操作，确定后执行 |
| 实际结果 | 和预期结果相同 |
| 结论 | 功能正常，测试通过 |

表6.7即为业务员模块中互联信息管理功能的测试用例。拥有权限的用户进入此页面后，可以根据自己的需要对车联网平台中与本系统有信息交互的系统的相关互联信息进行管理，点击相关的按钮对其进行增删改及详情查看操作。

表6.7 互联信息管理功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 用例名称 | 业务员-互联信息管理 |
| 用例类别 | 功能测试 |
| 测试目标 | 1. 验证业务员是否可以对互联信息进行管理操作 |
| 前置条件 | 1. 用户已登录 2. 用户拥有业务员相关权限 |
| 测试流程 | 1. 测试员输入检索条件，点击检索，等待系统返回结果，而后点击重置 2. 测试员点击检索结果中的某一模板，等待弹出详情弹窗 3. 测试员点击新增按钮，弹出弹窗，在弹窗内输入关键信息，点击确定，等待系统返回结果 4. 测试员点击互联信息的删除按钮，弹出弹窗，点击确定，等待系统返回结果 5. 测试员点击互联信息的修改按钮，弹出弹窗，在弹窗内输入关键信息，点击确定，等待系统返回结果 |
| 预期结果 | 1. 用户可以通过输入查询条件并检索，查看到所有符合条件的互联信息，重置条件后检索列表又恢复到默认状态 2. 用户可以通过点按按钮，对系统间互联信息进行添加、修改操作，且进行操作后会有成功或失败原因的弹窗提醒 3. 点击信息的作废按钮后，系统会二次确认是否执行操作，确定后执行 |
| 实际结果 | 和预期结果相同 |
| 结论 | 功能正常，测试通过 |

表6.8即为业务员模块中其他业务功能的测试用例。用户在本模块，可以对CRL和证书归档策略进行配置，如果完成则提示操作成功，如果失败则提示失败相关信息。此外，用户点进对应页面时，还可以在这一模块查看到系统自动获取并绘制的终端证书统计图、管理员信息列表以及硬件目前的状态汇总。

表6.8 其他业务功能测试用例

|  |  |
| --- | --- |
| 用例条目 | 内容 |
| 用例名称 | 业务员-其他业务功能 |
| 用例类别 | 功能测试 |
| 测试目标 | 1. 验证业务员是否可以进行CRL的配置 2. 验证业务员是否可以进行证书归档策略的配置 3. 验证业务员是否可以查看终端证书的统计工作 4. 验证业务员是否可以进行管理员信息列表的查询 5. 验证业务员是否可以进行硬件信息的查询 |
| 前置条件 | 1. 用户已登录 2. 用户拥有业务员相关权限 |
| 测试流程 | 1. 测试员进入CRL配置界面，输入CRL发布间隔与文件名称，点击确定等待响应 2. 测试员进入证书归档策略配置界面，输入过期证书归档与时间配置，点击确定等待响应 3. 测试员点击菜单，进入终端证书统计界面，等待系统获取并绘制图表 4. 测试员点击菜单，进入管理员信息列表界面，等待系统获取并返回结果 5. 测试员点击菜单，进入硬件信息显示界面，等待系统获取并返回结果 |
| 预期结果 | 1. 用户进入CRL配置页面，输入想要配置的值，点击确定，如果成功则显示操作成功信息，如果失败则提示失败相关信息 2. 用户进入证书归档配置页面，输入想要归档的门槛，点击确定，如果成功则显示操作成功信息，如果失败则提示失败相关信息 3. 用户进入终端证书统计界面后，系统会自动读取终端证书的种类、数量并以统计图的形式展示出来 4. 用户进入管理员信息列表界面后，系统会自动读取管理员信息并以列表的形式展示出来 5. 用户进入硬件信息界面后，系统会获取内存、硬盘、CPU的状态并以饼状图的形式展示出来 |
| 实际结果 | 和预期结果相同 |
| 结论 | 功能正常，测试通过 |

6.3.3 测试结果

根据设计内容，使用用例多次对整个系统进行功能测试，最终汇总得到测试结果如表6.9所示。

表6.9 功能测试结果表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 所属系统 | 模块/业务 | 用例总数 | 通过 | 失败 | 通过率 |
| 管理子系统 | 登录 | 50 | 50 | 0 | 100% |
| 管理子系统 | 初始化 | 20 | 20 | 0 | 100% |
| 管理子系统 | 超级管理员 | 50 | 50 | 0 | 100% |
| 管理子系统 | 安全管理员 | 100 | 100 | 0 | 100% |
| 管理子系统 | 业务管理员 | 50 | 50 | 0 | 100% |
| 管理子系统 | 审计管理员 | 50 | 50 | 0 | 100% |
| 管理子系统 | 业务员 | 100 | 100 | 0 | 100% |
| 管理子系统 | 审计员 | 50 | 50 | 0 | 100% |
| 业务子系统 | 注册CA | 50 | 50 | 0 | 100% |
| 业务子系统 | 假名CA | 50 | 50 | 0 | 100% |
| 业务子系统 | 应用CA | 100 | 100 | 0 | 100% |

根据表格内容可以看出，依据功能的丰富程度及重要性，对不同的模块进行了不同数量的用例测试。对于掌握核心业务的安全管理员、业务操作员等都进行了两倍于其他模块的测试，确保功能都可以正常使用，不会触发bug。应用CA由于肩负两种证书的业务，故而测试量也比假名CA和注册CA要多。整个车联网安全认证管理系统的各模块功能均可正常使用，能够完成对安全信息的管理以及安全认证业务的执行。功能测试中所有测试用例的通过表明了前期开发阶段进行的各项测试发现的逻辑错误、bug等问题都得到了解决。对系统的功能性，可做出如下总结：

（1）系统登录功能可用，初始化流程可正常执行；

（2）各级管理员所需求的功能全部实现，易用性高；

（3）业务员和审计员的日常任务可以顺利完成，无系统错误；

（4）业务子系统实现了安全认证业务所要求的证书签发、更新、作废与查询，包含着处理结果的响应报文可正常发送给RA系统。

6.3.4 优化策略

通过测试结果可以看到，系统的整体完成度高，可以正常运行，功能完善，易用性良好。但是，也依然还存在着一些问题有待优化，可以进一步提升用户体验、适应多种使用场景。

例如，业务员查询RA信息时，当数据量过大时会出现一定的响应延迟，此问题虽不影响其功能性，但建议对其进行优化，使用户获得更好的使用体验。此外，系统的UI布局在1920\*1080分辨率的情况下最美观，在低于此分辨率的屏幕中布局较为紧凑、在高于此分辨率的情况下界面又过于稀疏，也未针对手机等小尺寸设备做适配。考虑到日后大规模应用后的设备多样性，也可考虑针对这一情况做优化。

6.4 系统非功能测试

6.4.1 测试需求

本系统并非独立运行的系统，而是需要部署到车联网平台中和其他系统进行协同工作并完成车联网体系的安全保障。本次非功能性测试主要检测车联网安全认证管理系统的日常运行能力，通过测试，达到在现有软硬件环境下，验证系统是否满足指标要求、满足上线标准，并针对性地提出优化建议的目的。

根据前期设计，系统应当满足以下表6.10中描述的各项非功能性指标。

表6.10 非功能性指标表

|  |  |  |
| --- | --- | --- |
| 指标 | 指标要求 | 测试重点 |
| 可扩展性与可维护性 | 扩展能力 | 系统在保持架构相对稳定的前提下对于业务需求和数据变化能够适应 |
| 维护难度 | 提供成熟的系统管理项，满足对系统各方面维护的要求 |
| 易用性与可执行性 | 使用体验 | 人机交互界面明了，符合日常办公习惯，满足不同角色用户工作使用习惯 |
| 技术规范 | 系统采用现行标准的通信、网络等协议，严格遵循软件工程规范化的设计原则 |
| 安全性 | 应用安全 | 系统提供专用登录管理功能，并由授权方配置访问控制策略，严格限制每个账户的访问权限，审计功能覆盖到每个使用人员的操作。 |
| 网络安全 | 主要网络设备的运作水平具备冗余性能，把网络中各节点运行状态记录进系统日志中实时监视系统各部分运作情况，即时锁定危险事件并进行有效拦截。 |
| 数据安全 | 能够检测重要业务信息的数据完整性，采用一定手段实现存储数据的保密性，对数据有完整备份并能及时恢复受损的数据。 |

此外，性能指标作为非功能性需求中最重要的一项内容，关乎系统能否满足车联网当前体量，故而本次非功能性测试应当重点围绕性能测试进行，在性能测试的同时验证其他非功能性指标。安全认证管理系统的性能应当满足如下需求，否则视为测试不通过：

1. 满足不少于每年50万张车证书管理使用需求，支持从小容量向大容量的平滑扩容，扩容过程中业务不中断；
2. 并行处理能力：假名证书生成效率不低于2000张/秒；注册证书、应用证书及身份证书生成效率不低于500张/秒；
3. 响应要求：请求的平均响应时间小于500ms；
4. 阈值要求：内存占用<80%，物理机<80%，虚机/容器<75%；
5. 系统稳定性：可承受日常使用负载量，系统运行稳定无问题。

6.4.2 测试设计

此次非功能性测试主要对象是业务子系统的性能，系统包含4类CA接口，相关的测试在实际车联网试验区内进行实际车机验证，以确保面对真实而复杂的道路交通通信环境，本系统依然可以保持稳定运行并完成安全认证业务。

测试选取4类CA中使用频率最高、耗时最长、负载压力最大的证书申请下载功能对各接口进行指标验证。如果系统满足此类测试下的性能指标，则认可系统的总体性能满足要求。由于生产环境和测试环境没有差异，本次的测试结果数据以当前压测环境配置和项目版本为主。

根据性能需求，系统应满足不少于每年50万张车证书的管理使用，即进行测试时数据库的数据规模应至少维持在50万条。为达到此条件，在进行其他方面的性能测试前先利用试验场内的智能网联汽车进行业务申请，将数据库中数据量提升至如表6.11所示的规模。

表6.11 数据测试规模表

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 库名 | 表名 | 测试数据量 |
| Mysql | v2x\_eca | certentity | 159689 |
| Mysql | v2x\_aca | certentity | 185894 |
| Mysql | v2x\_ica | certentity | 165660 |
| Mysql | v2x\_pca | certentity | 190390 |

在系统的非功能性测试中，应当让系统处于日常的环境中。如图6.5所示，实验区域为真实的道路交通区域，存在着大量移动通信设备及路侧智能节点，智能网联汽车循环转移于1、2、3区域内，系统即在此种条件下受理各项申请。由于车联网体系仍处于建设阶段，应用量不高，故当前阶段并发量控制在500左右。对系统的性能测试使用压力检测工具，通过它来检测车联网实际运行环境下系统运作的效率、响应时间以及出错率等性能指标。



图6.5 性能测试道路图

在测试结束之后，从结果一栏中获取整场测试中的各项重要指标，如平均响应时间、错误率、中位数等，并将这些参数汇总制表，得出测试结果。

6.4.3 测试结果

根据上文设计，在标准环境中对系统进行测试，使用软件记录相关指标，得到结果分别如图6.6、6.7、6.8、6.9所示。



图6.6 EC测试结果



图6.7 AC测试结果



图6.8 IC测试结果



图6.9 PC测试结果

根据测试结果，同时结合运行时测得的CPU及MEM利用率，汇总得测试结果总表如表6.12所示：

表6.12 性能测试结果表

| 用例  编号 | 用例名称 | 并发  数量 | 结果统计 | | | | CA服务器 | | DB服务器 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 实际  TPS | 平均响应时间/ms | 99%响应时间/ms | 成功率  （%） | CPU  （%） | MEM  （%） | 数据量 |
| C01 | requestAndDownEc | 513 | 502.8 | 79 | 265 | 96.34 | 44.66 | 48.52 | 159689 |
| C02 | requestAndDownAc | 495 | 565.9 | 37 | 153 | 99.71 | 49.15 | 45.64 | 185894 |
| C03 | requestAndDownIc | 524 | 552.7 | 45 | 247 | 90.99 | 44.31 | 45.70 | 165660 |
| C04 | requestAndDownPc | 544\*20 | 579.2 | 29 | 124 | 99.7 | 46.17 | 27.52 | 190390 |

通过上面汇总的测试结果可以看到，系统的综合性能情况如下：

1. 数据库的总数据量合计701633条，高于50万张证书的要求，测试通过；
2. 证书生成效率：实际通过CA下载EC证书每秒502.8张，AC证书每秒565.9张，IC证书每秒552.7张，PC证书579.2\*20张，测试通过；
3. 响应时间：实际通过CA下载EC证书响应时间154ms，AC证书响应时间85ms，IC证书响应时间96ms，PC证书响应时间55ms，测试通过；
4. 系统阈值：内存占用<80%，没有内存溢出，物理机<80%，虚机/容器<75%，测试通过；
5. 系统稳定性：压力测试未出现死锁、崩溃、无响应等现象，测试通过。

本次非功能性测试除了汇总出性能指标外，可扩展性、安全性等各项非功能性指标都得到了验证，系统的设计符合规范，在日常的运行中具有合格的稳定性与安全性。

6.4.4 优化策略

通过测试结果不难发现，完成后的系统基本满足了非功能性需求。但是EC证书的每秒签发张数十分接近最低标准，而且其下载证书的响应时间也最长。为了进一步提升系统效率、满足未来越来越大的应用量，需要优化注册证书的签发模块，增加接口并发量，提升申请下载证书的效率与工作量。

6.5 本章小结

本章主要内容是为验证系统是否满足设计要求而进行的功能、性能两方面的测试。通过编写测试用例并输入系统来验证其功能性是否完善，通过测试工具模拟用户并发数来测试其性能是否满足基本要求，并指出尚存的一些问题和优化方向。

**第7章 结 论**

7.1 工作总结

随着车联网在现实交通体系中的部署与推进，车联网相关的信息安全性问题也日益突出，因此，本文为其设计一套专用的安全认证管理系统，用以车联网中各节点及设备的身份认证与安全信息管理。本文主要内容为车联网安全认证管理系统的设计与实现，还包括了对系统的部署及测试结果。工作总结如下：

（1）设计了专属的证书格式、撤销列表格式与通信方式。车联网系统的安全性和保密性是否满足现实社会环境需求将在很大程度上影响车联网的实际发展与大规模应用。与传统的X.509格式或ITS格式不同，本系统设计的LTE-V2X格式的证书及撤销列表专门为当前的车联网通信技术所设计，具有更强的针对性，更适合正式应用于车联网体系。同时，为了系统既能够适配自身的功能，又可以高效便捷地与平台中其他机构进行通信，结合HTTP协议与国密SSL协议设计了新的通信方式。

（2）使用国家自主产权的技术完成系统架构的设计。当前传统的安全认证管理系统无法满足车联网的信息安全与数据管理需求。考虑到车联网平台的特殊性和国家安全战略，本系统所用到的核心技术需要尽量具有我国独立自主的知识产权。故而在开发系统时采用了最新国家标准，建立独立的安全认证体系，通过管理系统控制整个车联网中的安全认证业务。在具体的证书业务中，采用国家密码算法实现证书的签名与验签，完成了证书的签发、更新、验证及作废。

（3）在系统实现之后，完成系统的配置激活及实际道路测试。将完成后的系统部署到了实际操作环境中，并完成了其相关的配置与激活。此外，由于本系统并非独立的系统，而是车联网平台的重要组成部分，为验证成果，测试阶段还将其部署到环境中并对其功能和性能等方面进行了模拟实际日常应用场景的测试，保证满足现阶段使用需求。

7.2 课题展望

7.2.1 不足之处

本次课题基本上完成了纸面设计阶段的系统各项要求，实现了调研后汇总分析出的功能性需求与非功能性需求。但是，由于个人工程能力以及现实物质基础的限制，仍存在着以下一些问题有待改进。

首先，系统采用集中式的部署方式，部署在内部机房中。这样保证了系统的安全性，也利于日常的管理与维护，但是在扩展性和处理能力方面则有一定欠缺。下一步可以考虑建设多个安全机房，同时细化可信人员名单，在保证安全性的前提下实现分布式部署，提升系统的可用性。

其次，系统可以兼容采用相同数据格式的安全证书，可以与采用相同通信协议的系统进行互联通信，但对于不采用国密算法、不遵循工信部CCSA标准的相关通信实体则不能进行认证与交互。在未来更广泛的应用场合，本系统所服务的车联网平台不可避免地要与其他平台进行互联互通，而且移动设备持本平台签发的证书也无法实现跨平台通信。这使得目前只能做到本地车联网平台内各系统的兼容与交互，对于平台间的信息传输则需要日后开发相应的接口。

最后，本系统是基于本地车联网实验区和各联合单位的实际应用体量而开发设计的，其功能与性能满足当前一个时期车联网平台的信息安全需求。但是随着车联网技术的发展成熟，未来到达广泛应用时期后，本系统将无法胜任更高的需求，届时需要再次进行调研分析，对现行的系统进行扩充与改进。

7.2.2 课题展望

目前车联网安全认证体系主要的发展趋势与移动通信技术的研究进步息息相关，在5G普及之后，车联网安全技术将由当前主流的LTE-V2X技术发展为5G-V2X技术。5G时代，车联网将会和自动驾驶、分布式、移动边缘计算等技术更加紧密地结合起来。新技术带来的安全挑战将具体表现在更大的数据量、更快的传输速度以及更高的响应要求。

此外，考虑到车联网平台在我国国内将逐渐建立统一认证机制，并将与国际车联网安全认证体系接轨，为了确保信息互通与跨平台安全认证，未来将使用国际和国密标准双证书的认证形式。智能设备不仅获得一张国密标准的数字证书，还将获得一张基于国际技术标准签发的数字证书，两张证书都具有同等安全效力，使用其进行数据传输都能获得通信对象的认证，确保智能网联汽车等移动设备在跨平台的情况下依然可以正常地进行安全通信。

为了解决这些问题，进一步推进车联网信息安全防护，安全认证系统需要搭建更大的数据平台、设立更细致的管理等级制度、采用更高效的消息格式，此外伴随着国内加解密算法研究取得新的突破，也可考虑采用更新的国密算法。随着车联网技术逐渐地发展，未来一定会逐渐形成成熟的应用体系，进而走出试验区，真正普及到社会交通中去。

**参 考 文 献**

[1]SHANZHI C, JINLING H, YAN S, et al. A Vision of C-V2X:Technologies,Field Testing, and Challenges With Chinese Development[J].IEEE Internet of Things Journal,2020,7(5):3872-3881.

[2]刘楠.智能车联网信息安全中身份认证机制的设计与原型开发[D].北京:北京邮电大学,2020.

[3]TARIK T, ABDERRAHIM B. Design Guidelines for a Network Architecture Integrating VANET with 3G &amp; Beyond Networks[C]. //2010 IEEE Global Telecommunications Conference. [v.4].:IEEE, 2010:2975-2979.

[4]张宏涛.车载信息娱乐系统安全研究[D].河南:战略支援部队信息工程大学,2021.

[5]AMRITA G,MAURO C. Security issues and challenges in V2X: A Survey[J]. Computer Networks,2020,169(C): 1070-1093.

[6]BABAGHAYOU M, LABRAOUI N A, ADO A A, et al. Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey[J].Journal of information security and applications,2020,55:102618.1-102618.17.

[7]SHIM K A. CPAS : An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.

[8]LONG Y , TANG Z , XU L . Application-oriented cross-CA certificate trust[C] // 2010 IEEE International Conference on Information Theory and Information Security. [v.1].:IEEE, 2010:354-357.

[9]MARIO F,PASQUALE P,GIANLUCA A, et al. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges.[J]. IEEE Internet of Things Journal,2018,5(4):2483-2495.

[10] KAYHAN Z G, MOHSEN G, LINGHE K, et al. Enabling Efficient Coexistence of DSRC and C-V2X in Vehicular Networks[J]. 2020,27(2):134-140.

[11] SYED S H, ANDREAS K, ATHUL P, et al. Ultra-secure transmissions for 5G-V2X communications[J]. IEEE Communications Standards Magazine,2019,3(2):46-52.

[12] MARKOPOULOU, DIMITRA, PAPAKONSTANTINOU, VAGELIS, DE HERT, PAUL. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation[J]. Computer Law & Security Review: the international journal of technology law and practice,2019,35(6):105336.1-105336.11.

[13] PANKAJ K, SARU K, VISHNU S, et al. Secure CLS and CL-AS schemes designed for VANETs[J]. Journal of supercomputing,2019,75(6):3076-3098.

[14] WANG L , JING W . A Frame Collision Reduction Method for Safety Message Broadcasting in IEEE1609.4/IEEE802.11p based VANETs[J]. KSII Transactions on Internet and Information Systems, 2018, 12(3):1031-1046.

[15] REKIK M , MEDDEB-MAKHLOUF A , ZARAI F , et al. Improved Dual Authentication and Key Management Techniques in Vehicular Ad Hoc Networks[C]// IEEE/ACS International Conference on Computer Systems & Applications. IEEE, 2017:1133-1140.

[16] ALSHAREEDA M A.,ANBAR M,MANICKAM S,HASBULLAH I H. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Secure Communication in a Vehicular Ad Hoc Network[J]. Symmetry,2020,12(10):2681-2691.

[17] WILLIAM W, ANDRE W, VIRENDRA K, et al. A security credential management system for V2V communications[C]. //2013 IEEE Vehicular Networking Conference: 2013 IEEE Vehicular Networking Conference (VNC), 16-18 December 2013, Boston, MA, USA.: Institute of Electrical and Electronics Engineers, 2013:1-8.

[18] KAYHAN Z G, MOHSEN G, LINGHE K, et al. Enabling Efficient Coexistence of DSRC and C-V2X in Vehicular Networks[J]. Mathematical research letters: MRL,2020,27(2):134-140.

[19] CONTRERAS J ,ZEADALLY S ,GUERRERO-IBANEZ J A .Internet of Vehicles: Architecture, Protocols, and Security[J]. IEEE Internet of Things Journal, 2017:1-1.

[20] LONC B, CINCILLA P. Cooperative ITS security framework: Standards and implementations progress in Europe[C]// 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE, 2016:1-6.

[21] AZEES M , VIJAYAKUMAR P , DEBOARH L J . EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, PP(9):1-10.

[22] ZHANG J, ZHENG K, ZHANG D, et al. AATMS: An Anti-Attack Trust Management Scheme in VANET[J]. IEEE Access,2020, 8: 21077-21090.

[23] 张瑾瑜. 基于车载云的安全认证和隐私保护机制研究[D].北京:北京交通大学,2018.

[24] 姚知含. 基于C-V2X系统的智能网联汽车安全系统研究与实现[D].北京:北京邮电大学,2020.

[25] 李月笛.车联网中安全认证和隐私保护技术研究[D].四川:电子科技大学,2021.

[26] 许先云.车联网中的位置隐私保护方法研究[D].浙江:浙江大学,2021.

[27] LU Z, QU G , LIU Z, A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20: 760-776.

[28] BOUALOUACHE A , SENOUCI S M , MOUSSAOUI S . Towards an Efficient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks[C]// IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016:1-7.

[29] SHIM,K.A. CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.

[30] FALLGREN M , DILLINGER M , J ALONSO-ZARAT, et al. Fifth-Generation Technologies for the Connected Car: Capable Systems for Vehicle-to-Anything Communications[J]. Vehicular Technology Magazine IEEE, 2018, 13(3):28-38.

[31] ABDELWAHAB B, SIDI-MOHAMMED S, SAMIRA M. PRIVANET: An Efficient Pseudonym Changing and Management Framework for Vehicular Ad-Hoc Networks[J]. 2020,21(8):3209-3218.

[32] JINHUA G, JOHN P. BAUGH, SHENGQUAN W. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework[C]. //2007 Mobile Networking for Vehicular Environments Workshop (MOVE 2007). 2007:103-108.

[33] SAMPIGETHAYA K , LI M , HUANG L , et al. AMOEBA: Robust Location Privacy Scheme for VANET[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(8):1569-1589.

[34] CORSER G P , FU H , BANIHANI A . Evaluating Location Privacy in Vehicular Communications and Applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(9):1-10.

[35] XUEMEI Z, XINGSHU C GUOLIN S, et al. DTA-HOC :Online HTTPS Traffic Service Identification Using DNS in Large-Scale Networks[J].Tsinghua Science and Technology,2020,25(02):239-254.

[36] HERNANTES J , GALLARDO G , Serrano N . IT Infrastructure-Monitoring Tools[J]. IEEE Software, 2015, 32(4):88-93.

[37] QIU H , QIU M , LU R . Secure V2X Communication Network based on Intelligent PKI and Edge Computing[J]. IEEE Network, 2020, 34(2):172-178.

[38] DUA A , KUMAR N , BAWA S . A systematic review on routing protocols for Vehicular Ad Hoc Networks[J]. Vehicular Communications, 2014, 1(1):33-52.

[39] HANAZUMI S, DE M, ANA C. V. A Formal Approach to implement java exceptions in cooperative systems[J].The Journal of Systems and Software,2017,475-490.

[40] WANG S , HOU P , YUN L , et al. Design and Research of dissertation Management System Based on SSM Architecture[J]. Journal of Physics Conference, 2018, 1069:15-21

[41] LU D , Y QIU, QIAN C , et al. Design of Campus Resource Sharing Platform based on SSM Framework[C]. IOP Conference Series Materials Science and Engineering, 2018:1-6.

[42] 信息安全技术SM2椭圆曲线公钥密码算法第1部分:总则[S].中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会,2016.

[43] 信息安全技术SM3密码杂凑算法[S].中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会,2016.

[44] 信息安全技术SM4分组密码算法[S].中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会,2016.

[45] 基于 LTE 的车联网无线通信技术安全证书管理系统技术要求[S].中华人民共和国工业和信息化部,2021.

**致 谢**

行文至此，我深深感到作为一名学生，能够在中国科学技术大学度过硕士研究生阶段的学习生涯是我最大的荣幸。

本次论文的完成首先最需要感谢的就是我的校内导师杨威副教授和企业导师赵万里高级工程师。在论文的撰写阶段，杨老师准确地发现了我在学术方面存在的不足，为我提供了悉心的指导与详细的意见。在杨老师的引导下，我明白了课题前期的开题与设计阶段一定要完善翔实，这样才能保证后续的开发实现阶段可以完成既定目标。此外，论文的行文一定要规范整洁，条理分明。杨老师严谨、认真且又一丝不苟的治学风格深深地影响了我。在公司中，赵老师既是我工作上的领导又是我学术上的导师，既在系统的开发设计中引领着我熟悉各方面的工作内容，让我能够很快地适应岗位；又在相关技术上为我指明了研究的方向，引导我掌握车联网信息安全相关的知识。在两位导师的教导之下，我逐渐熟悉并掌握了相关专业技术，最后成功设计并实现了课题的相关内容，并完成了论文的撰写。在毕业论文的撰写阶段能得到两位老师的指导，是我过去这段时间里最大的荣幸。在论文的结束之际，我对杨老师和赵老师致以最诚挚的敬意与最衷心的感谢！

同时我还要感谢我的同学与领导。在过去的时间里，我与同学们经常进行开发技术上的交流，大家在交流研讨之中加深了对以往所学技术的理解，也互相解决了彼此关心的一些问题。设计系统并完成论文使用了大量的时间，感谢实习公司的领导对于我的支持与理解。

最后，作为一名中国科学技术大学的研究生，真诚祝愿科大的未来更加精彩与辉煌！

2022年9月

1. [↑](#footnote-ref-0)
2. [↑](#footnote-ref-1)