中国科学技术大学

专业硕士学位论文

(工程硕士）



作者姓名： 蔡澳

专业领域： 软件工程

校内导师： 杨威 副教授

企业导师： 赵万里 高级工程师

完成时间： 二〇二二 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 Safety Certification Management System for Internet of Vehicles**

Author：Cai Ao

Speciality：Software Engineering

Supervisor：Associate Professor. Yang Wei

Advisor：Senior Engineer. Zhao Wanli

Finished time: September 8, 2022

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**

伴随着信息与通信技术不断取得突破，车联网这一技术开始从理论变成了现实，有力地推动了道路交通的信息化、智能化。我国政府高度重视这一产业，智能网联汽车产业发展势头迅猛，产业规模不断扩大。在车辆可以与各式各样的对象进行信息交互之后，信息安全问题层出不穷，极大地威胁到了整个车联网系统的良性运作。而传统的安全认证管理系统主要的认证业务对象是以传统互联网为媒介的机构、设备、用户等实体，无法胜任车联网环境下高速运动的车辆、纷繁复杂的路边节点及其他智能设施之间安全认证管理的职责，也无法与车联网平台中其他系统进行信息交互。

为了解决上述问题，向智能网联汽车引入基于公钥基础设施(PKI)的安全证书管理系统。通过人工管控，根据自身规范遵循特定的方式向满足条件的通信参与者签发数字证书，证书中包含了该通信节点所提交的数字公钥，从而使现实世界中的用户与网络世界中的对象建立起对应关系。系统可以为相关人员提供系统管理功能，系统根据自身安全法规遵循国家密码算法向合格的通信参与者颁发数字证书，这些证书将成为车联网中设备进行信息交互的凭证。同时，还可以使得整个系统可以在监管之下有序、高效运行。

本文设计并开发了一个车联网安全认证管理系统，该系统以用户为导向，提供可视化界面与人机交互操作。具体进行的工作如下：（1）为系统的安全认证业务设计了专属的实现方式。本文根据我国车联网体系的安全需求设计了全新的安全证书格式、证书撤销列表及通信过程。（2）依据最新国家技术标准实现了系统的管理机构。本文设计了一套不仅可以为车联网中的汽车签发安全证书，还可以为路侧设备、服务提供商等其他通信实体进行安全认证的管理系统。（3）将系统部署到车联网平台中并完成实地车机测试。在系统完成后，将系统部署到实际工作环境中，并对其进行功能和性能上的调试。此外，为保证系统可以在车联网平台中正常履行职能，在实际的车联网试验区内完成了实际车机测试，保证安全认证业务的顺利完成。最后，本文还归纳出开发成果、指出执行过程中存在的不足之处，并对未来一个时期内系统的发展趋势与应用前景进行展望。

**关键词：**车联网 信息安全 身份认证 业务管理 系统设计

**ABSTRACT**

With the continuous breakthrough of information and communication technology, the technology of Internet of Vehicles began to turn from theory into reality, which effectively promoted the informatization and intellectualization of road traffic. The Chinese government attaches great importance to this industry. The development momentum of intelligent networked automobile industry is rapid and the industrial scale is expanding. After vehicles can interact with various objects, information security problems emerge one after another, which greatly threatens the benign operation of the whole vehicle networking system. The main authentication business objects of the traditional security authentication management system are institutions, equipment, users and other entities with the traditional Internet as the media. They are not competent for the responsibility of security authentication management between high-speed vehicles, complex road side units and other intelligent facilities in the Internet of Vehicles environment, nor can they interact with other systems in the Internet of Vehicles platform.

In order to solve the above problems, it is planned to introduce a security certificate management system based on Public Key Infrastructure (PKI) to intelligent networked vehicles. Through manual control, digital certificates are issued to qualified communication participants in a specific way according to their own specifications. The certificate contains the digital public key submitted by the communication node, so as to establish a corresponding relationship between users in the real world and objects in the network world. The system can provide system management function for relevant personnel. The system issues digital certificates to qualified communication participants according to its own security regulations and national password algorithm. These certificates will become the certificates for information exchange of devices in the Internet of Vehicles. At the same time, it can also make the whole system run orderly and efficiently under supervision.

This dissertation designs and develops a security certification management system for Internet of Vehicles, which is user-oriented and provides visual interface and human-computer interaction operation. The specific work is as follows: (1) A special implementation method is designed for the system's security authentication service. According to the security requirements of our country's Internet of vehicles system, this dissertation designs a new security certificate format, certificate revocation list and communication process. (2) According to the latest national technical standards to achieve the management of the system. This dissertation designs a management system that can not only issue safety certificates for cars in the Internet of vehicles, but also conduct safety certification for other communication entities such as roadside equipment and service providers. (3) Deploy the system to the Internet of vehicles platform and complete field vehicle testing. After the system is completed, the system is deployed to the actual working environment, and the function and performance of the debugging. In addition, in order to ensure that the system can normally perform functions in the Internet of vehicles platform, the actual vehicle and machine test is completed in the actual Internet of vehicles test area to ensure the smooth completion of safety certification business. Finally, this dissertation summarizes the development results, points out the shortcomings in the implementation process, and looks forward to the development trend and application prospect of the system in the future period.

**Key Words:** Internet of Vehicles Information Safety Identity Authentication Business Management System 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

人类生产力的发展和科学技术的进步使得当代社会的交通运输行业越来越繁荣。而伴随着信息与通信技术不断取得突破，车联网这一技术开始从理论走向了现实，有力地推动了道路交通的信息化、智能化[1]。2018年1月，《智能汽车创新发展战略》由国家发改委公布，文件提出，到2025年汽车要基本智能化，高级别智能汽车将完成规模化应用；2019年9月，国务院又颁布了《交通强国建设纲要》，纲要明确指出积极发展智能网联汽车产业，形成我国独立自主的完整产业链。以上官方文件表明了汽车智能网联化已经成为我国产业发展的战略大方向之一。2021年是十四五规划的开端之年，也是建设交通强国的关键节点，车联网技术作为车路协同发展的关键技术，成为了“新基建”的焦点。以上可看出，随着全球新一轮科技和产业革命的蓬勃发展，我国车联网产业发展势头迅猛，产业规模将不断扩大。

根据目前情况，智能汽车的功能正走向多样化和复杂化，整个系统的安全性和保密性是否满足现实社会环境需求[2]将在很大程度上影响车联网的实际发展与大规模应用。在并不遥远的未来，多种交互方式的使用、新技术的应用及基于场景化的设计将打造全新的智能汽车概念。和手机类似，随着用户需求的不断提升，汽车将拥有越来越多的新功能，它不再是单纯的交通工具，更将满足用户对娱乐、办公、通信、生活等方面的需求[3]。汽车智能化、网联化、电动化、共享化的趋势将深刻影响道路交通关系，人车信息交互也将成为智能网联汽车研究和进步的关键。同时，汽车作为车联网的一部分，将装载娱乐系统、语音系统、道路信息系统等[4]，这些系统在运作时都会产生大量的数据交互，并且基本都和个人隐私息息相关。以上种种都对整个车联网体系的信息安全提出了极高的要求。

车联网技术的发展让汽车从单一性走向了多元化，赋予了道路交通系统更大的信息量、更丰富的应用空间、更多元的技术结构，但同时也使得汽车的信息安全风险大大提高。在车辆可以通过移动通信网络接入到云端，与各式各样的智慧对象进行交互之后，数据丢失、信息篡改、身份伪造等问题层出不穷，极大地威胁到了整个车联网系统的良性运作，甚至可能会对车内人员的生命健康安全造成损害[5]。

随着密码技术的发展，数字安全证书技术在认证机制方面的优越性越来越明显[6]，它可以减少认证过程中密钥协商的复杂性，充分体现了用户的隐私自己掌

握的原则。在这样的背景下，为了保护车联网体系中的各种数据，维护信息安全，为智能网联汽车引入了基于公钥基础设施(PKI)的安全证书管理系统[7]。通过人工审核，根据自身规范遵循规范的方式向满足条件的通信参与者签发数字证书[8]，证书中包含了该通信节点所提交的数字公钥，从而使现实世界中的用户与网络世界中的对象建立起对应关系。

1.2 国内外研究现状

当前国内外关于车联网信息安全的相关研究早已起步，各国在发展和探索中逐渐形成了适合自身应用情况的安全认证体系。美、欧研究起步较早，中国正处在试点建设阶段。

1.2.1 国外应用现状与发展趋势

安全认证管理系统是否完备是决定车联网业务最终能否广泛商用的决定因素之一[9]。当前，欧盟与美国已经由官方机构牵头，研究建立了相当完善的安全认证管理系统，正在部分地区建立区域性的安全认证体系并对其安全性、稳定性进行测试。欧盟车联网网络安全认证体系由电信标准化协会（ETSI）牵头，主要目标是为车联万物（V2X）通信安全提供车载设备（OBU）、路侧设备（RSU）及公共基础设施的网络安全设计[10]、安全消息、安全传输[11]等相关验证和原型架构提供参考，为证书授权机构（CA）提供了从证书编码格式、证书吊销流程、CA 总体层级、证书匿名隐私保护等一系列相关标准。由于欧盟是多个成员国组成，不同成员国可能使用来自不同CA签发的证书，为此欧盟委员会成立了专门的监管机构依据欧洲电信标准化协会制定了系列标准来管理这些CA[12]。该监管机构的职责在于维护一张包含所有可信CA的证书可信列表，并通过在该可信列表中添加或移除CA的方式实现当前可信CA间的互认。通过存储该证书可信列表，当V2X设备收到其他CA签发的证书时，V2X设备只需确认该CA是否处于可信列表中，就可以进一步验证上述证书是否合法，以此实现CA间的互认，完成互相通信[13]。

美国车联网网络信任体系由交通运输部牵头，其安全认证管理体系使用一个根CA对所有证书进行管理[14]。官方联合行业专家委托车辆碰撞预防指标联盟（CAMP）设计了先进的安全证书管理系统，该系统基于电气和电子工程师协会（IEEE）制定的 1609 系列标准，旨在为参与者提供一个安全可信的通信环境[15]。该安全证书管理系统采用选举人机制认可或撤销当前签发证书的CA[16]，通常选举人可由政府部门或企业担任。由于安全证书管理系统中仅使用一个CA签发证书[17]，因此，并不存在CA间的互认问题。认证体系为建设智能交通V2X CA体系提供了完整的、可参考、可验证的、支持全面隐私保护的一整套公钥基础设施架构[18]。整个体系采用多级信任体系层级设计，可实现统一的Root CA，使用注册CA和假名CA的认证方式来实现隐私保护和匿名[19]。

欧美在车联网安全认证技术方面已经取得了较为完善的成果。目前，欧盟的相关体系架构已经完成，正在开展测试验证工作[20]；美国已完成体系架构和标准制定，在部分州建成区域性网络信任体系。下一步各国将进一步推动整个体系的发展完善，包括跨区域协调、证书格式兼容以及信任体系的统一化[21]，在试点建设取得成效后逐步推进至全国试行。

1.2.2 国内应用现状与发展趋势

我国的车联网安全认证管理体系建设较欧美稍为不足，目前正处于起步阶段[22]。中国的车联网CA相关标准体系建设涉及工业和信息化部以及汽标委、通标委、密标委等多个标准化委员会，目前各部委正积极参与相关标准体系建设工作，推动具体成果的落地，加快车联网CA应用。

全国汽车标准化委员会现主要立项《智能网联汽车车用数字证书应用技术要求》一项标准，制定V2X数字证书具体车端应用、数字证书技术要求，主要聚焦于车载端的具体实践应用[23]；工业和信息化部发布了《新能源汽车产业发展规划（2021-2025年）》及《车联网（智能网联汽车）产业发展行动计划》等相关文件，开展车联网电子认证与安全信任试点工作，推进行业统一的认证体系构建。

中国汽车技术研究中心作为国内唯一的汽车行业技术归口单位，为发展建设国内的车联网安全体系，近两年开展了车联网网络信任支撑平台建设工作，与相关企业、示范区、研究机构建立了广泛的联系，以行业安全根等方式为试点工作提供支撑和保障[24]。该项目作为行业CA服务平台，集成了安全认证系统、注册审批系统及云监测系统等重要安全性模块，并以车联网先导区为试点，对平台的运行能力进行实地部署与测试，卓有成效地推进了体系的构建。随着标准的逐步确立与完善，车联网安全认证管理体系将逐渐由理论走向实践，通过在先导区内部进行研究与测试，不断部署与测试各项技术，建立多个成熟有效的试点，逐步追赶上国际研究成果[25-26]。这也将是未来一段时间我国的发展趋势。

综上，目前国际的车联网安全认证体系并未统一，美国与欧洲采用了不同的信息安全策略，而国内的车联网安全认证体系仍处于起步阶段，未形成一体化的市场规范。这项安全工程需要既能符合中国目前的国情、满足安全认证业务的现阶段需求，又能符合国家提出的信息安全战略。因此，按照国家最新标准，设计一套适用于当前国内车联网平台的安全认证管理系统是必要的。

1.3 解决的主要问题

传统的安全认证管理系统主要的认证业务对象是组织机构、联网设备、网络用户等实体[27]，它们最大的特征是以传统的互联网为媒介，且地理位置、操作频率相对稳定，而车联网的情况则与之大不相同。智能网联汽车在整个网络中处于快速运动状态，使用广播向其他汽车和道路节点传递自身相关消息[28]。为了保护数据安全，每一次消息通知都需要做到保护实时位置隐私和快速传递。智能汽车的快速移动性[29]和部署环境的开放性[30]使得传统安全认证系统的认证业务无法满足车联网的信息安全需求。此外，传统的安全认证系统也无法实现与车联网体系中其他系统进行数据的兼容与交互。因此，设计并实现一套专用的车联网安全认证管理系统，对于整个车联网体系的信息安全保障是必要的。

车联网安全认证管理系统并不是一个孤立的系统，广义上来说它属于整个车联网体系的一部分，因此要求系统能够与环境中其他机构、设备进行通信与配合[31]，而车联网架构中机构复杂、设备繁多，开发系统时如何做到统一、兼容，是一大重点。业务子系统作为核心，基于PKI设计实现，PKI的逻辑结构十分明了，大致是“CA-RA-设备”的结构。而根据行业标准，业务子系统中只集成各CA，注册审批机构（RA）独立出作为注册审批系统负责V2X设备的申请核查。如何处理与RA之间的关系，使得公钥基础设施物理上分隔的情况下在逻辑上仍然可以作为一个整体有序运作[32]，是业务系统实现时需要着重考虑的。此外为了实现证书签发、存储等流程，必须设计出合理的数据结构，使得其既能够高效地进行存储、管理等操作，又能够满足证书签发时算法的需要，同时还要满足行业内制定的各项标准。整个系统作为车联网体系结构中的重要一员，需要做到完备可用，在代码编写方面要做到丰富充实、结构分明。

在安全认证系统投入实际应用后，可以在很大程度上保证智能网联汽车与设备、乘客进行交互时的信息安全，避免数据出错、隐私泄露甚至是交通事故的发生[33]。在整个车联网交通体系下，安全认证管理系统将与其他技术手段，如自动驾驶、车-云通信等互相保障、互相补充，促进整个智能交通平台的发展与进步，得到政府、社会组织及消费者的认可[34]，最终实现广泛而全面的应用。

1.4 本文主要工作

（1）为系统的安全认证业务设计了专属的实现方式。

根据车联网平台通信的特点以及我国车联网体系的安全需求，本文设计了全新的安全证书格式、证书撤销列表及通信过程。证书格式简单，适配中国自主设计的国密系列算法，满足相关技术标准，可以为车联网消息提供有效的完成性和抗攻击性保护，拥有较高的安全性和各类信息的适配性。该证书格式比x.509格式或ITS格式更适合车联网的复杂需求，信息传递效率也更高。同时，在系统间的HTTPS通信过程中本文以国密SSL协议替换掉传统的SSL协议，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，比传统的HTTPS协议更加安全。此外，本文还完成了证书签发、更新等安全认证业务过程，在RA系统向业务端提出安全认证业务的申请之后，系统可以即时响应，读取并处理信息之后进行业务执行，完成后向RA系统提供业务成果。

（2）依据最新国家技术标准实现了系统的管理机构。

本文在设计的车联网安全认证管理系统实现了2021年工信部颁布的最新国家标准，立足于现阶段车联网平台中通信安全的实体关系，完成了整个体系中负责授权证书机构的实现。设计了一套不仅可以为车联网中的汽车签发安全证书，还可以为路侧设备、服务提供商等其他通信实体进行安全认证的管理系统。本文实现了标准所要求的各项基本功能，在设计中需要算法的相关部分使用了中国自主设计的国密SM系列算法，对比国际通用的同类型算法在性能与效率方面同样优秀。

（3）将系统部署到车联网平台中并完成实地车机测试。

本文所设计的系统并非孤立的，它需要同平台中其他系统协同工作，共同构建车联网体系。所以在系统完成后，将系统部署到实际工作环境中，并对其进行功能和性能上的调试，保证系统可以在车联网平台中正常使用。此外，为确保系统的可用性，还需在实际的车联网试验区内完成实际车机测试，保证安全认证业务的顺利完成。

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。本章将介绍促进本文进行设计开发的社会背景，探讨国内外车联网信安体系研究的状况，同时介绍本次设计主要进行了哪些工作、解决了什么现实问题。

第二章是相关技术及理论。本章将重点阐述本文的设计与实现阶段采用了哪些技术与理论，通过剖析与对比说明为何选择这些技术、它们对比同类技术的优势以及可以实现的目的。

第三章是需求分析。本章将从目前车联网安全业务相关人员的关键需求入手，根据调研结果通过系统化的方法详细分析系统中的各种用户角色，同时利用不同类型的用户对系统的具体需求构建出清晰的需求分析模型。

第四章是系统概要设计。本章将介绍本次设计的车联网安全认证管理系统，将课题所设计的系统从总体层面展示出来。利用图文结合的形式描述系统的总体结构，从动静两方面剖析管理和业务两个子系统。同时，本章还将介绍系统存储数据的数据库相关设计。

第五章是系统详细设计。本章将对系统中本人开发的各功能模块具体实现进行详细描述，通过使用UML模型、关键代码分析等手法来设计系统，例如模块的关键代码细节、重要数据结构等。其中包括系统框架的搭建、用户角色的分配、管理端的具体构造以及服务端安全认证业务的实现机制等。

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 相关技术及理论

2.1 通信协议与数据格式

2.1.1 超文本传输安全协议

本系统服务端接口采用超文本传输安全协议（HTTPS），理由如下：

传统的HTTP协议以明文方式传递信息，而且不提供任何数据加密的方式，如果攻击者截取了两个通信对象之间的传输报文，就可以直接分析破解其中包含的关键信息[35]，因此，HTTP协议不能胜任一些敏感数据的传递，尤其是本文中所涉及的安全认证与数字证书信息。

与之相比，HTTPS是一种利用计算机网络进行安全通信的传输协议。HTTPS协议虽然比较消耗服务器资源，且通信效率比HTTP要差，但是通过SSL/TLS以加密的方式传输数据包，用协商的对称加密算法和密钥进行加密，保证数据机密与安全；用协商的哈希算法进行数据完整性保护，保证数据不被篡改。此外，HTTPS是目前保护网络安全最安全的解决方案，经过SSL层加密后，解密工程变得较为复杂，很大程度上避免了网络的中间人攻击[36]。本文中为适配国密算法，SSL协议采用国密SSL技术规范。

2.1.2 JS对象简谱

本系统管理端报文的数据格式采用JS对象简谱（JSON），理由如下：

JSON是一种语法，可以被用于数据的存储与交换中。在JSON中，文本均以JavaScript对象标记法进行书写。由于它本质上将数据作为文本来处理，故其具有很强的易用性与跨语言特性。JSON库和JSON解析器支持许多不同的编程语言，目前主流的编程语言都可以处理JSON。与可扩展标记语言（XML）相比，XML文件庞大，文件格式复杂，传输占带宽；服务器端和客户端都需要消耗大量资源与时间来解析XML，这将使得服务器端和客户端[代码](http://www.fly63.com/tag/%E4%BB%A3%E7%A0%81)变得较为复杂且难以维护。而且，必须重复编写很多[代码](http://www.fly63.com/tag/%E4%BB%A3%E7%A0%81)来解决不同[浏览器](http://www.fly63.com/tag/%E6%B5%8F%E8%A7%88%E5%99%A8)之间解析XML的方式不一致的问题。

JSON具有和XML相同的可扩展性、同样丰富的解析方式，而与之相比却具有更快的传递速度、更小的数据体积，这也带来了更小的编码与解析难度。故而，在车联网体系中采用JSON的数据格式符合车联网快速性和移动性的特点[37]。

2.1.3 抽象语法标记

本系统服务端报文的数据格式采用抽象语法标记（ASN.1），理由如下：

ASN.1以一种独立于计算机架构和编程语言的方式来描述数据结构。其编码规则不管计算机、应用程序或编程方式中如何表示等因素，单纯描述了如何对ASN.1中定义的信息进行编码，且可以快捷地被映射为C或Java等语言的数据结构，并可以得到运行平台程序库的支持，被应用程序代码使用。此外，ASN.1的编码技术比许多相似功能的标记方式更高效，它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[38]，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。

2.2 体系结构与框架

2.2.1 B/S三层架构

本文设计的系统采用B/S三层架构，理由如下：

传统的C/S架构虽然响应速度快、安全性强且技术性成熟，但是它大大限制了系统的使用场景与使用形式，其正式运行后的管理与维护十分不便，未来要对其进行变更也较为困难。而B/S架构则基于日渐成熟的浏览器技术，用户界面完全通过浏览器实现，具有易开发性、易维护性以及强分布性，为使用者提供了更广泛的使用场景，比之C/S架构更加适合本文的开发目标。

图2.1即为B/S架构示意图。

bs

图2.1 B/S三层架构图

2.2.2 开发框架

本文采用SSM开发框架（Spring+SpringMVC+MyBatis），理由如下：

SSM框架是已经被应用于系统开发设计多年的框架，其安全性与稳定性已经得到了时间和各厂商的检验。对于本文要开发的安全认证系统，最重要的就是系统的安全性与稳定性[39]，因此更倾向于使用成熟的而非新颖的框架。作为典型的三层结构，它在开发和维护的阶段可以极大地减少开发的复杂性和构建时间[40]，而在修改和扩展阶段又可以提供灵活的耦合与解耦[41]，大大提升了可插入性与重构成功率。此外，SSM框架各部分的优点也很突出：

（1）Spring是已被广泛使用的轻量级开源框架。使用Spring可以方便解耦，简化开发流程，在工程中，可以将创建对象与依赖关系都交给Spring进行管理。此外，它还可以简单方便地与其他框架进行组合使用，大大提高了工程设计与开发过程中的灵活性。

（2）SpringMVC。SpringMVC是Spring提供的基于MVC设计模式的框架，它内部的各个模块职责清晰、分工明确，可以与Spring进行完美的对接。由于采用了低耦合度、可组合的组件结构，与其他MVC框架相比，它更加具有灵活性。它采用工作者模式，客户端向Web容器发命令，由前端控制器进行拦截，将业务需求发给应用控制器，二者又分别在视图层与模型层进行交互操作，最终将结果返回。

（3）MyBatis。MyBatis是一款支持定制化数据存储过程的持久层框架。它不会对工程系统或数据库产生任何影响，通过将SQL语句写进XML文件里解除了数据库查询语句与代码的交杂，分离业务逻辑与数据访问，大大降低了耦合度。图2.2为SSM框架的业务调用过程图。

业务调用

图2.2 业务调用过程图

2.3 国家商用密码算法

本文的目标是设计出一套可以应用于车联网体系的安全认证管理系统，其核心功能在于相关信息的管理以及安全认证业务，而安全认证业务中加密算法是必不可缺的。本文在设计与开发中选择国家密码管理局颁发的国家商用密码算法（简称国密算法），原因如下：

1. 常见的密码算法，如RSA算法，属于国际通用密码，虽历经几十年的研究与发展已经足够完备成熟，但其也一直是信息安全攻击与破解的重要对象，受到较大威胁。
2. 国密算法虽发布时间较晚，但是其投入实际应用后已被证明具有不逊于国际通用算法的性能。以非对称加密算法为例，国际通用的RSA算法一般来说密钥长度达到2048位已经满足据大部分加密场景，而基于椭圆加密算法的256位的国密SM2算法在密码强度与安全性方面接近一致。而SM2算法凭借其较短的密钥长度获得更高的效率的同时消耗的资源却更少，满足了车联网中快速通信的要求。
3. 国密算法为我国独立研究，拥有自主知识产权的算法。国家相关机构近年来大力推动国密算法在关键领域的应用，掌握核心技术、维护国家信息安全，逐步摆脱对国外的技术依赖。本次要开发的是车联网体系中安全认证相关的系统，使用我国自研的密码算法恰如其分。

2.3.1 SM2非对称加密算法

本文中所有安全业务的签名验签以及需要进行非对称加密运算的场景都使用SM2非对称加密算法实现。SM2算法主要分为三个部分，分别是数字签名算法、公钥加密算法以及密钥交换协议。数字签名算法的输入值为待签名的消息及签名方的身份标识ID，输出两个32位的签名值；公钥加密算法输入值为待运算的明文、公钥以及它们的长度，输出加密后的密文；密钥交换协议则定义了两个用户间协商密钥交互的过程[42]。SM2算法基于椭圆曲线上点群离散对数的复杂性，综合性能与国际通用的RSA算法不相上下。

2.3.2 SM3密码杂凑算法

本文中所有安全业务的哈希值计算以及SM2中的摘要计算都使用SM3密码杂凑算法实现。SM3算法中，输入值为待运算的数据及其长度，经过消息填充、消息扩展和迭代压缩这三步之后，输出哈希计算结果。SM3算法输出结果为256位，好于国际通用的SHA-1算法[43]。图2.3为SM3算法的总体过程。

SM3

图2.3 SM3总体过程图

2.3.3 SM4分组加密算法

本文中所有对外接口报文处理中需要使用对称加密算法的部分都使用SM4分组加密算法。SM4加密算法中，输入值为待运算的明文、密钥以及它们的长度，经过消息填充、消息扩展和迭代压缩这三步之后，输出加密后的密文；解密算法与之相反，输入值为待运算的密文、密钥，输出解密后的明文[44]。由于SM4算法中密钥长度为128位，因此其安全性高于常见的DES算法。图2.4为SM4加密算法的总体方式。

SM4

图2.4 SM4总体过程图

2.4 技术标准

安全认证业务是围绕着安全通信证书展开的。安全通信证书是一种数字证书，由证书机构签发给车联网中各种智能通信设备，它是设备在车联网中进行各式通信的安全凭证。因此，对安全证书的格式，要进行符合车联网通信要求的设计[45]。

传统的互联网安全通信中，证书一般采用X.509格式。证书内容覆盖了安全认证过程中的所有必要信息，可以很好地表征证书的持有者。但是它并不适合用于车联网体系中，因为其编码后数据较长，而且验证过程是证书链的形式。这两者导致了使用X.509证书进行通信将需要较大的通信带宽与较长的计算时延，这些都是车联网通信不可接受的。

交通部于2019年发布了ITS证书标准，目前已得到国内很多智能运输系统的采用。但是，ITS标准过于宽泛，只从整体上定义了运输系统中应当遵循的证书规范，并没有专门针对车联网体系提出证书的格式、通信的要求、系统间进行互联的基础等关键问题，因而不能作为车联网安全认证管理系统完美的解决方案加以采用。

随着车联网体系建设的日益成熟，设计专用的安全认证系统势必要采用更加完善的行业标准。工业和信息化部于2021年发布了《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》，这一标准是专门面向车联网安全认证业务颁发的，具有极强的关联性、针对性，将成为往后车联网行业遵循的规范。本文的系统将全部采用此标准。

2.5 本章小结

本章主要介绍了课题项目开发中所用到的重要技术理论，主要分为通信协议、系统框架及密码算法三个部分。通过与其他相似技术的分析与对比，剖析了选中技术的优势，说明了选择这些技术的理由。

第3章 需求分析

3.1 系统概述

为了解决车联网平台中智能网联设备的通信与安全问题，本文设计提出车联网安全认证管理系统。系统能够针对不同业务人员的不同需求进行全面化、专业化、层次化的管理，并致力包括根证书机构、注册证书架构、假名证书、应用和身份等证书认证的实现以及和假名注册机构和应用注册机构系统实现。系统应提供专用登录操作对每一位用户进行身份认证和区分；提供一些机制控制用户对文件和数据库表单等对象的访问；提供覆盖到每个用户的安全审计功能，对相关操作日志进行审计。

此外，还要充分考虑安全认证业务在未来一段时期内的发展需求，具有一定的前瞻性，充分考虑系统在未来移植、更新、扩充的可行性，并针对本系统平台未来会涉及权限复杂、设备繁多、数据量大的特点，充分考虑业务处理的响应逻辑以及业务操作的速度和精度等方面的潜在需求。

3.2 需求导出

本次课题设计的车联网安全认证管理系统面向的对象是车联网平台中安全认证业务相关的专业人员，因此需要从认证业务和系统管理的角度来考虑系统各方面的需求。为了得出明确有效的系统需求，在课题设计的前期阶段通过市场现有产品考察、推送调研问卷、与合作车企举办洽谈会，收集系统相关的各方管理人员、业务人员和业务对象对系统的详细需求，并进行专业化梳理与汇总，对系统需求进行初步说明。

高效便捷地对车联网安全业务相关信息进行管理是使用者对本系统最基本的期望之一。由于车联网平台较为庞大复杂，从业人员较多，根据自身职责和管理级别的不同对系统有不同的使用需求。除了通用需求之外，还应考虑安全认证业务中各角色的功能特点。

3.2.1 通用需求导出

通用需求，指的是不分使用对象、所有系统操作员都会用到的一般功能需求。这方面需求主要集中在系统的初始化和登录方面，重点在于相关操作的稳定性与安全性。

（1）初始化：主要需求在于进行数据库、加密机等软硬件的参数配置并初始化整个系统。操作人员第一次使用前系统必须先执行初始化，初始化成功后才能对外服务，管理服务。

（2）登录：需根据使用者在系统中角色的不同提供常规登录入口或安全管理员登录入口。常规登录入口为用户提供采用管理员证书对密码本id签名的方式登录，密码本用一次后删除，登录后显示所有业务CA，及每个业务CA的信息，以及当前管理员在每个CA下的角色权限，供管理员选择一个有效的CA进入，管理其事物；特殊登录入口中，CA管理端提供给安全管理员登录，使用用户名+口令的方式登录CA系统，此操作无签名，口令采用密码本加密，一次一密。

3.2.2 管理员需求导出

系统管理员依据现行制度大致可分为超级管理员、审计管理员、业务管理员及安全管理员。前三类管理员都是针对系统角色的信息和权限进行管理，而安全管理员负责的是系统安全和业务相关的操作，属于系统中的核心角色。

（1）超级管理员在CA系统中主要负责对业务管理员的管理，其核心业务需求主要集中在对系统中管理员信息的操作以及权限分配，超级管理员可以对权限内的所有管理员信息进行新增，查看业务管理员详情，停用、启用业务管理员。同时超级管理员可对其他角色的身份信息进行修改。超级管理员还可以对已经确定分管业务的业务管理员进行授权操作，在系统上授予其在安全认证管理系统中的管理及操作权限，以便其开展相关工作；同理，当其他管理员工作发生变动时，可以利用此功能撤销对此管理员的权限授予。

（2）审计管理员在CA系统中主要负责对审计员的管理，其核心业务需求主要集中在对系统中审计员信息的操作以及权限分配，审计管理员可以对权限内的所有审计员信息进行新增，查看审计员详情。每个用户在CA系统中最多拥有一个角色，审计员可以选择一个类型为已登录的用户与当前系统进行关联，设置其角色为新审计员，同时审计管理员可对其身份信息进行修改。审计管理员还可以对已经确定岗位职责的审计员进行授权操作，在系统上授予其在系统日志审计业务中的特定权限；同理，当审计员工作发生变动时，可以利用此功能撤销对此员工的审计权限授予。

（3）业务管理员在CA系统中主要负责对业务员的管理，其核心业务需求主要集中在对系统中业务员信息的操作以及权限分配。业务管理员可以对权限内的所有业务员信息进行新增，查看业务员详情，更新、删除、停用、启用业务员。每个用户在CA系统中最多拥有一个角色，业务员可以选择一个类型为已登录的用户与一个业务CA进行关联，默认设置其角色为新业务员，权限默认为空，状态默认启用。同时业务管理员可对其身份信息进行修改。业务管理员可以对已经确定岗位职责的业务员进行授权操作，在系统上授予其在安全认证业务中的特定权限；同理，当业务员工作发生变动时，可以利用此功能撤销对此业务员的权限授予。

（4）安全管理员是整个安全认证业务的关键角色之一，管理用户证书等安全相关数据，同时还可以进行系统级重要操作。安全管理员是唯一一个可以在系统未激活情况下进行登录的操作员，在密钥持有者的配合下可以进行系统的激活操作。安全管理员可以对管理CA（MCA）信息和MCA身份证书信息进行相关操作，但不可以对算法进行修改。安全管理员可以对用户证书进行操作。还可通过系统对业务CA进行签发、导入、查询及其他基础操作。此外，在得到旧持有者的确认下，安全管理员可以对密钥持有者进行更新。

3.2.3 业务人员需求导出

业务人员主要分为审计员和业务员。其中业务员负责关键的认证业务及相关信息管理，属于系统的核心角色。

（1）审计员在CA系统中对日志信息进行管理。在管理员进行管理操作和业务模块处理业务请求的时候，都会产生相应的日志审计员可以查看系统中生成的各项日志。日志中包含的各项信息，如操作者、操作类型等对审计员应当都是公开的，以便审计员可以确认日志状态。审计员需要对系统生成的大量日志进行审理，判断系统记录是否出错以及相关人员操作是否合规。对于审计通过的日志则可进行归档操作。根据所选的时间段进行归档，被归档的日志需要从日志表和审计表中删除，日志信息和审计信息全部转移到归档表中，作为历史日志留存。对于需要另作用途的或是需要保存到磁盘的日志，审计员可以利用系统将相关文件下载到计算机里，以便在离线状态进行查看和分享。

（2）业务员是整个安全认证业务的关键角色之一，和安全管理员一样需要承担整个安全认证系统中最核心的工作内容。业务员RA管理的基本操作包括对RA的增删改查，此外，业务员可以对RA进行权限授予与收回，还能启用/停用任一RA。业务员可以对终端证书进行查询与作废操作。终端证书由安全管理员进行签发，业务员可查询其相关信息，在终端证书出现问题的情况下可将其作废。根据实际需求，业务员可对系统中的模板进行管理操作，以便业务的顺利推进。业务员还承担了车联网平台中系统间互联信息的管理工作。业务员应当能够对相关互联信息进行增加、删除、修改和查找等操作。此外，业务员还可通过系统配置业务CA的CRL、对业务CA的证书归档策略进行选择与配置等。

3.2.4 业务对象需求导出

本系统的业务对象指的是需要得到系统认证并进行业务执行的各类实体，如注册审批机构、异常行为机构等。业务对象不能直接操作并使用系统，但是它们是系统核心业务的服务对象，故而其需求应当成为系统开发时着重考虑的因素。当前业务对象对车联网安全认证管理系统的核心需求如下：

1. 证书种类：根据车联网信息安全的制度，本系统需要为业务对象提供注册证书、假名证书、身份证书和应用证书这四类数字证书，从而满足智能设备在车联网体系中安全通信和数据交互的需求；
2. 证书服务：对上文提到的四种证书，系统应提供签发、申请下载、更新下载、违规作废以及详细资料查询的相关服务接口，同时还应对签发后的证书做资料留存，以便必要时进行安全核验。

3.3 功能性需求

根据上一部分对系统的需求进行初步分析与导出，整个车联网安全认证管理系统的核心业务在于管理员对系统的管理、业务员对系统主要功能的日常操作以及系统向外部业务对象提供安全认证业务。本节围绕着安全认证管理的核心业务描述系统的功能性需求。

首先可得出核心需求描述列表如表3.1所示。

表3.1 核心需求描述

| 需求编号 | 名称 | 参与者 | 说明 |
| --- | --- | --- | --- |
| R1 | MCA管理 | 安全管理员 | 对MCA的信息进行管理 |
| R2 | 用户证书管理 | 安全管理员 | 对用户证书主题、内容等进行管理 |
| R3 | 业务CA管理 | 安全管理员 | 对业务CA进行签发、导入等操作 |
| R4 | 其他管理功能 | 安全管理员 | 口令更新、系统激活等其他安全相关的业务 |
| R5 | RA管理 | 业务员 | 对RA信息进行业务处理 |
| R6 | 终端证书管理 | 业务员 | 管理已有的终端证书 |
| R7 | 证书模板管理 | 业务员 | 管理系统现有证书模板 |
| R8 | 互联信息管理 | 业务员 | 管理车联网各系统间互联信息 |

续表3.1 核心需求描述

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 参与者 | 说明 |
| R9 | 其他功能 | 业务员 | CRL配置、硬件信息等其他业务功能 |
| R10 | 证书申请下载 | 业务对象 | 申请签发相关证书并下载保存 |
| R11 | 证书更新下载 | 业务对象 | 下载更新后的注册证书 |
| R12 | 证书作废 | 业务对象 | 作废过期或不合法的证书 |
| R13 | 证书查询 | 业务对象 | 业务对象查询证书相关信息 |

3.3.1 安全管理员核心用例

安全管理员是整个安全认证业务的关键角色之一，通过指定的特殊登录入口登入系统，管理用户证书等安全相关数据，同时还可以进行口令更改、系统激活等重要操作。经过前期的调研，其主要需求可罗列如下：

（1）MCA管理：安全管理员可以对MCA信息进行更新操作，同时可更新一些基本信息，如是否对响应签名，以及可选更新根证书、更新有效期、可选更新更证书密钥，但不可以对算法进行修改。此外，还可以更新MCA身份证书信息，可进行身份证书有效期更新、密钥更新，算法不可更新。新的身份证书采用 MCA 根证书签发，且需校验根证书有效性。

（2）用户证书管理：安全管理员可以对用户证书进行增删改查的基础操作。新增时用户证书使用MCA根证书签发，用户证书有效期不能大于根证书，且证书类型分为系统证书和登录证书，系统证书为RA使用，登录证书为管理员使用；查询时可对用户证书信息以列表方式进行结果查询；修改时除证书主题、用途外，可对任一信息进行更改；删除时删除用户证书信息后删除其作为登录证书赋予的角色，同时删除作为系统证书关联的RA。

（3）业务CA管理：安全管理员可通过系统对业务CA进行签发、导入、查询及其他基础操作。签发业务CA时，证书模板类型需要与所选的CA类型对应，模板需要初始化之后，后台预置到数据库中，且需要配置好其超级管理员和审计管理员；导入证书时，导入的证书需要与该 CA 匹配，主题名相同，类型相同，该CA的私钥签名，导入的证书的公钥能验签；查询证书时可对CA证书信息以列表方式进行结果查询；此外，还能对证书进行更新、作废等基础操作。

（4）系统安全功能需求：在得到旧持有者的确认下，CA管理端安全管理员可以对密钥持有者进行更新；安全管理员还可以更新安全口令来确保系统的安全；此外，安全管理员是唯一一个可以在系统未激活情况下进行登录的操作员，在密钥持有者的配合下可以进行系统的激活操作。

根据上文内容，绘出安全管理员核心用例图如图3.1所示。

安全管理员用例图 新

图3.1 安全管理员用例图

接下来以业务CA管理为例进行此角色的用例说明，安全管理员的需求进行用例描述如表3.2所示。

表3.2 业务CA管理用例描述

|  |  |
| --- | --- |
| 用例名称 | 业务CA管理 |
| 用例描述 | 安全管理员管理业务CA |
| 主执行者 | 安全管理员 |
| 优先级 | 高 |
| 触发条件 | 管理员点击管理界面相应按钮 |
| 后置条件 | 进入业务CA界面 |
| 基本事件流 | （1）管理员选择要操作的业务CA  （2）点击要执行的功能  （3）填写必要字段补足信息  （4）点击确认 |
| 异常事件流 | 目标CA异常，无法执行业务 |

3.3.2 业务员核心用例

业务员是整个安全认证业务的关键角色之一，可以在CA系统中对RA，终端证书，证书模板，互联系统及其他事务进行管理。业务员和安全管理员一样需要承担整个安全认证系统中最核心的工作内容。业务员的核心功能需求在下面列出：

（1）RA 管理：RA管理的基本操作包括对RA的增删改查。新增RA时，为其配置一张安全管理员新增的用户证书中可选类型的身份证书；删除RA时，可清空RA的全部信息，但不删除该用户证书信息；修改RA时，RA名称，证书主题，证书序列号等关键信息不可修改；查询RA时，检查结果以列表形式呈现。此外，业务员可以对RA进行权限授予与收回，还能启用/停用任一RA。

（2）终端证书管理：业务员可以对终端证书进行查询与作废操作。终端证书由安全管理员进行签发，业务员可查询其相关信息，在终端证书出现问题的情况下可将其作废。

（3）证书模板管理：证书的签发时，新证书是根据模板进行生成的，故而业务员需要对证书模板进行管理。根据实际需求，业务员可对系统中的模板进行添加、查询、修改和删除操作，以便业务的顺利推进。

（4）互联信息管理：CA系统应当能和车联网中其他系统进行互联互认。因此，业务员还承担了车联网平台中系统间互联信息的管理工作。业务员应当能够对相关互联信息进行增加、删除、修改和查找等操作。

（5）系统业务功能需求：业务员可通过系统配置业务CA的CRL；可以对业务CA的证书归档策略进行选择与配置；可以查询终端证书的数量统计图、实现饼图等统计结果；还可以查询到本业务中的管理员和其他业务员信息。

接下来以RA信息的管理为例对业务员的需求进行用例描述如表3.3所示。

表3.3 RA管理用例描述

|  |  |
| --- | --- |
| 用例名称 | RA管理 |
| 用例描述 | 业务员管理RA相关信息 |
| 主执行者 | 业务员 |
| 优先级 | 高 |
| 触发条件 | 业务员登录认证管理系统 |
| 后置条件 | 默认进入RA管理界面 |
| 基本事件流 | （1）点击要执行的功能  （2）填写必要字段补足信息  （3）点击确认 |
| 异常事件流 | （1）服务器异常，无法执行操作  （2）操作不合规，无法获取结果 |

根据上文内容，绘出业务员核心用例图如图3.2所示。

业务员用例图

图3.2 业务员用例图

3.3.3 业务对象核心用例

业务对象是整个车联网安全认证业务的服务目标，它的实体不一，可能是智能网联汽车，也可能是路侧设备等其他被认可的车联网构成要素，所共同的地方在于它们的业务请求要通过注册审批机构的审核后由其代向CA申请。业务对象的核心功能需求在下面列出：

（1）证书的申请下载：RA代业务对象向系统提出证书申请请求，系统首先校验参数是否合法、申请方的身份证书是否过期，核查通过之后再检查注册CA的状态以及有效的证书实体信息以及是否不存在此种申请。当这些检查都通过后则进入签发阶段，检查数据库保存的证书公钥是否唯一、处理有效期与模板信息是否合法，一切正常则生成注册证书并返回成功结果。

（2）证书的更新下载：RA代业务对象向系统提出证书更新请求，当收到证书申请请求后，系统首先会校验参数是否合法、申请方的身份证书是否过期，核查通过之后再检查注册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、处理有效期与模板信息是否合法，一切正常则生成注册证书并返回成功结果。

（3）证书的作废：在系统收到RA提出的证书作废申请后，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则将作废信息写入数据库，并生成响应数据反馈给RA。业务中任意环节审查不通过则返回失败结果。

（4）证书的验证：系统收到验证证书的申请后，校验请求是否来自认证的RA，确认无误后根据其查询的对象反馈给其相关验证结果，即此证书是否为本系统所颁发与相关细节。

根据上文内容，绘出业务对象核心用例图如图3.3所示。

业务对象用例 新

图3.3 业务对象用例图

接下来以证书申请下载为例进行角色的用例说明，业务对象的需求进行用例描述如表3.4所示。

表3.4 证书申请下载用例描述

|  |  |
| --- | --- |
| 用例名称 | 证书申请下载 |
| 用例描述 | 业务对象申请下载证书 |
| 主执行者 | 业务对象 |
| 优先级 | 高 |
| 触发条件 | RA认可此对象并向系统发出申请 |
| 后置条件 | 系统接收到RA的申请 |
| 基本事件流 | （1）点击要执行的功能  （2）填写必要字段补足信息  （3）点击确认 |
| 异常事件流 | （1）申请未成功传到系统  （2）参数有问题，申请失败  （3）申请方证书过期，业务不合规 |

3.4 非功能性需求

3.4.1 性能需求

系统整体性能要求如下：

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。

3.4.2 可扩展性与可维护性

设计阶段应充分调研安全认证业务在3至5年内的发展前景，充分考虑系统升级、扩展、修改和维护的可操作性，需要在对未来的系统建设方面给出合理的解决方案。系统的总体体系架构应该在未来5年内保持相对稳定，同时必须能够满足可扩展的要求，主要表现在对于业务需求和数据变化要能够适应。

系统的可维护性主要体现在系统的可管理性、持续的系统调优能力两个方面。要提供成熟的系统管理项，满足对系统各方面维护的要求，实现日常运行过程中系统的审核、监查、管控，维护时间可控制在5小时以内，保证系统的运行随着维护时间的增加可以逐渐趋于稳定和最优化。

3.4.3 易用性与可执行性

在系统的设计与实现阶段，应该尽量选择成熟的技术和规范，采用国际主流、成熟的体系架构来构建，实现合理的应用。此外，需要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，对整个设计过程进行严格的管理和控制。

系统的目标用户包括非计算机、软件专业人员，故而要求整个系统是便于使用的，使用者通过阅读使用手册即可理解系统功能，故而要求系统具有易用性。因此，需要做到人机交互界面明了，符合日常办公习惯；尽可能提高系统更新升级的方便易用性，提供针对性功能，满足不同角色用户工作使用惯例。

3.4.4 安全性需求

本系统的安全性需求主要包含应用安全、网络安全以及数据安全。

本系统需从如下方面考虑应用安全：

（1）身份鉴定：提供专用登录管理功能对操作用户进行身份鉴别和区分；提供账号身份标识唯一性检查。

（2）访问控制：提供访问控制功能，控制使用者对文件和数据库表单等对象的访问；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；对重要信息资源设置标记，严格控制对具有敏感标记资源的操作。

（3）安全审计：覆盖到每个使用人员的操作审计功能，对重要操作步骤进行审计；保证无法单独中断审计进程、无法篡改和隐藏相关记录；提供对审计结果的统计、归档、核算以及其他操作。

本系统的网络安全需求集中在以下几个方面。

（1）结构安全：主要网络设备的运作水平具备冗余性能，满足超负荷工作情况需求；网络各大带宽至少500Mbps，满足高峰期传输需求；有详细的网络拓扑结构图，根据各部分工作责任，对信息的重要性等按情况分出网段；避免关键网段直连外部其他系统而且部署在网络边界处；按认证业务的优先级确定分配带宽的不同级别。

（2）安全审计：把网络中各节点运行状态、用户操作等记录进系统日志中；日志的内容包括发生的时间、用户、操作类型等数据；生成审核后的报表，保护日志审计结果以避免人为篡改隐瞒等违规行为。

（3）威胁防范：实时监视端口、服务器、数据库等各部分运作情况，防止遭受木马攻击、后门攻击、蠕虫病毒散播等。对内网中的系统操作员和智能车联网设备未通过批准私自连接外部网络等危险行为，进行即时锁定并进行有效拦截。

整个系统对信息数据的安全需求主要体现在数据完整性、数据保密性、可备份与恢复性。

（1）数据完整性：能够检测到身份信息和重要业务信息在传输过程中是否破坏了完整性，以及系统管理资料、用户身份信息和重要业务信息在保存过程中是否破坏了完整性。

（2）数据保密性：采用加密及其他有效方法实现系统中各项数据存储的保密性；尤其是用户隐私信息和重要业务数据的存储保密性。

（3）备份和恢复：对核心信息进行备份以便恢复；异地数据备份，利用通信网络将核心数据定时传送到备用储存设备；提供本地数据的备份和恢复、按照每日1次进行数据的备份；采用冗余的手段设计系统的拓扑网络，避免单点故障导致的系统崩溃。备份硬盘至少2块，大小至少在1000GB以上。

3.5 本章小结

本章最开始对整个系统进行概要阐述，描绘其大致实现的功能目标。然后对相关使用人员的具体需求进行初步导出，形成原始的系统需求。接下来运用专业化手段建立需求模型，明确系统的功能性需求以及非功能性需求，形成完备的系统需求，满足用户的要求。

第4章 系统概要设计

4.1 系统设计目标和原则

车联网安全认证管理系统的主要功能是为车联网体系中的相关工作人员提供一个可进行管理、审计、安全认证的操作平台，同时实现为智能网联汽车签发数字证书，保护信息安全。整个系统的有序运作取决于各个子系统之间能否按照需求分析的结果进行互相配合与制约，为此需要设计出一个合理、完善的系统结构，实现预定的功能。为实现这些目标，在概要设计中应满足以下原则：

（1）系统结构的选取与构建。

系统的构建使用B/S三层架构，用户界面完全通过浏览器实现，为使用者提供更广泛的使用场景，三层架构技术将二层架构中直接耦合在一起的客户端与数据库服务器独立开来，让二者分别与中间层进行耦合。

（2）系统功能设计与实现。

对各方面需求进行分析，得出系统应当在功能上满足安全证书及相关业务人员的管理与操作，同时还应保障系统的信息安全、运作稳定、操作高效。根据需求分析的结果选取合适的开发技术、结合软件工程的分析方法。本文使用Spring+SpringMVC+MyBatis的技术框架对车联网安全认证管理系统进行架构、功能方面的具体设计与实现。根据业务需求，将系统总体分为两个子系统，分别负责信息管理业务与安全认证业务。

（3）系统的数据存储。

系统开发过程中和开发完成后通过专业测试软件对系统各模块、各功能、性能以及完成度进行测试，判断其是否满足前期的需求分析与设计思路，同时核验完成后的系统是否满足实际使用的需要。本次对整个系统采用划分模块的方式进行设计，最后将各模块耦合在一起完成最终的产品，设计将秉承先进行、标准化、可扩展与安全性四大原则。下面从各个角度来阐述系统的概要设计思路。

4.2 系统静态结构设计

4.2.1 拓扑结构设计

首先对系统的整体框架进行规划。

系统拓扑架构如图4.1所示。作为车联网体系的组成部分，它并非独立工作的，而是与身份认证系统、通用组件及证书注册审批机构（RA）等其他软硬件有着数据交互。根据前期调研与需求分析得出的结果，整个系统根据其功能和面向对象的不同可以分为管理子系统和业务子系统。

在车联网安全认证管理系统中，两个子系统属于并行关系，但由于系统是为用户服务的，且业务系统主要对外发证，不设计人机交互界面，故而管理系统中的特定模块（如业务员）可以对业务系统进行操作和控制。系统可以和整个车联网体系中的其他机构进行通信和数据交互，如证书注册机构RA，它向业务系统的CA申请签发各式证书，交给车联网中智能设备。

系统拓扑

图4.1 系统拓扑图

4.2.2 管理子系统设计

接下来进行管理子系统的总体设计。

根据需求分析得到的结论，目前将管理子系统分为八个功能模块，分别是初始化、登录、安全管理员、超级管理员、业务管理员、审计员、业务员以及审计员模块。各模块根据其具体执行任务又可进一步细分为具体的功能。系统根据车联网安全认证管理的实际需求，结合对数据库的相关操作提供专业服务，如：证书模板管理、互联信息管理以及硬件信息查询等。具体的模块如图4.2所示。

1. 初始板块中主要包含了登录与初始化这两个模块。登录模块分为两类：一是用户名+口令+密码本+验证码的登录模式，二是智能密码钥匙+数字证书+口令模式+数字签名的登录模式。不同管理员采用不同的登录模式，以保护系统登录安全。初始化模块，负责初始化CA，如配置数据库、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。
2. 管理员板块中包含安全管理员、超级管理员、业务管理员及审计管理员四个模块。安全管理员模块主要负责用户证书的管理，管理CA的更新，身份证书的更新、密钥持有者的更新和业务CA管理。超级管理员可以添加管理员并自动给其赋予管理员的相关权限。业务管理员可以添加业务操作员并给其赋予业务操作员的权限。审计管理员可以添加审计员，并授予审计员的权限。
3. 操作员板块分为业务员与审计员这两个功能模块。业务操作员可以进行证书管理，证书模板管理、互联配置管理、系统配置管理。审计员可以进行操作日志查询、审计、归档，只有审计过后的日志才会被归档。

模块图

图4.2 管理子系统模块图

4.2.3 业务子系统设计

接下来进行业务子系统逻辑上的设计。

业务子系统的各模块是基于公钥基础设施实现的，如图4.3所示。系统架构中主要包括根证书机构（根CA）、中间证书机构（中间CA）、假名证书认证机构（假名CA）、注册证书认证机构（注册CA）及应用证书认证机构（应用CA），同时为假名注册审核机构、应用注册审核机构等安全认证注册机构提供服务。

根CA是证书管理系统的本源，负责系统根证书的管理与维护并对二级证书机构进行注册审批。在确认证书机构的合法性之后，根证书机构为其颁发管理机构的数字证书，认可其成为系统内的有效对象。PCA、ECA等负责管理V2X安全通信应用相关数字证书，负责审核证书申请主体的合法性，签发、撤销证书申请主体的数字证书。

业务子系统简图

图4.3 管理子系统模块图

根CA，负责向中间CA模块签发中间证书（ICA）、注册证书（ECA）、根证书（RCA）、假名证书（PCA）等相关证书。根证书机构Root CA是LTE-V2X证书管理系统的信任根，负责系统根证书的管理与维护并对LTE-V2X证书机构进行注册审批。在确认LTE-V2X证书机构的合法性之后，根证书机构为其签发管理机构的数字证书，使其成为系统内的有效实体。

中间CA，负责向注册CA、假名CA、应用CA三个模块签发中间证书、注册证书、根证书、假名证书等相关证书。中间CA和根CA功能相似，是根据PKI部署的实际需要，在根证书机构与LTE-V2X证书机构之间部署的证书机构，以支持多级CA部署方式。

注册CA，承担申请下载注册证书、更新下载注册证书、查阅注册证书和作废注册证书的业务。注册CA负责向OBU和RSU等车联网设备签发注册证书。为了加入目标的车联网应用，OBU和RSU等智能设备在通过注册机构的审批后拿到注册证书，而后利用注册证书向应用授权机构（假名CA、应用CA等）申请实际用于生成V2X安全消息的V2X通信证书。在同一个车联网 PKI系统中，可以根据不同的应用业务和管理区间设置不同的注册 CA，管理对应业务领域的设备接纳。

假名CA，承担申请下载假名证书、查阅假名证书和作废假名证书的业务。假名CA负责向 OBU 签发假名证书。OBU可使用假名证书对自身发出的主动安全消息（Basic Safety Message，BSM）进行数字签名。为避免泄露车辆行驶路径，PCA 要向 OBU 签发多个相同有效期假名证书；OBU依据假名证书的使用规则，定期替换掉被用于消息签名的证书。

应用CA，承担申请下载、更新下载、查阅和作废应用证书和身份证书的业务。应用证书的签发对象为RSU等车联网设备，身份证书的签发对象主要是OBU。

4.3 系统动态结构设计

上一节从静态角度对系统进行了总体上的设计，本部分将描述系统使用中的动态结构。根据静态架构和系统逻辑的不同，分别使用系统活动图和数据流图来描述车联网安全认证管理系统的管理子系统和业务子系统。

4.3.1 管理子系统动态结构

由于系统较为庞大，从总体层面上绘制管理子系统的系统活动图如图4.4所示。所有的用户在使用系统前都必须进行登录操作，验证通过后才能进入系统。用户在首次登录或系统调整后可以对自己的账号进行初始化配置，先设定个人信息，而后依次连接数据库与加密机等关键设施。配置完成后可以进行安全管理业务相关的操作，不同用户的权限不同，其可进行系统活动是根据岗位职级进行区分的。

管理子系统活动图图4.4 管理子系统活动图

在超级管理员的操作下，系统可以进行对管理员的管理活动，包括对权限内的所有业务管理员信息进行新增，查看业务管理员详情，更新、删除、停用、启用业务管理员。此外，超级管理员可以使用系统对已经确定分管业务的业务管理员进行授权操作，系统授予其在安全认证管理系统中的管理及操作权限，以便其开展相关工作。

在安全管理员的操作下，系统可以对MCA信息进行更新操作，可以对用户证书进行增删改查的基础活动，以及对业务CA进行签发、导入、查询及其他基础活动。此外，还可进行如口令更新、系统激活等重要安全活动。

业务管理员在职级上属于超级管理员的下属，使用系统对业务员的相关信息进行管理。和超级管理员一样，系统可以进行对业务员的管理活动，包括对权限内的所有业务员信息进行新增，查看业务员详情，更新、删除、停用、启用业务员，也可为其进行授权。

在业务员的操作下，系统可以对RA，终端证书，证书模板，互联系统及其他事务进行管理活动。业务员和安全管理员的工作是整个管理子系统中最核心的系统活动。

审计管理员和业务管理员职责类似，在职级上均属于超级管理员的下属，使用系统对审计员的相关信息进行管理。包括对权限内的所有审计员信息进行新增，查看审计员详情，更新、删除、停用、启用审计员，也可为其进行授权。

在审计员的操作下，系统可以进行日志审计相关活动，如查看或下载生成的各项日志、对系统生成的大量日志进行审理、判断系统记录是否出错以及相关人员操作是否合规，对于审计通过的日志则可进行归档操作，将日志信息和审计信息全部转移到归档表中，作为历史日志留存。

4.3.2 业务子系统动态结构

业务子系统主要的日常业务是接收业务对象的相关申请（一般由注册审批机构RA代申请），而后根据其申请内容进行业务相关的处理并返回结果，故而采用数据流图描述其动态结构。

业务子系统的数据输入来自注册审批机构，最终其输出对象也是注册审批机构。在系统内部，接收的来自RA的申请报文经过数据预处理、状态检查、业务办理和结果返回四步之后，将响应报文发回RA。

经过以上四步再根据UML知识进一步细分，预处理部分分为接收申请与数据处理、状态检查分为证书检查与CA状态检查，就可得到如图4.5所示的业务子系统的二级数据流图。该图展示了业务子系统在执行安全认证业务时主要的数据流向。

服务子系统数据流图图4.5 业务子系统数据流图

当RA发出请求后，业务子系统通过接口收到申请报文，通过特定转换方式将其格式转化为业务子系统可进行处理的业务参数，接下来从数据库中读取对应的证书状态信息以及CA状态信息，检查是否具有进行业务处理的必要条件。接下来从模板库中调出对应模板，并根据请求参数进行签发/更新/作废等相关操作，并将生成的结果存入证书信息表中。最后，将业务成果封装为响应报文，并传达给RA系统，形成一条完整的数据流。

4.4 本章小结

本章在需求分析的基础上，对系统的主要模块及模块间连接进行了概要设计，站在总体视角，以静态和动态两个方面介绍了系统的模块构成、逻辑架构以及逻辑架构等内容，对系统的总体框架做了概要性说明。

第5章 系统详细设计

5.1 详细设计目标

在概要设计完成对系统总体架构及各模块间联系的描述之后，应对系统所有子系统的各模块进行详细设计。但是，由于本文所设计开发的车联网安全认证管理系统较为庞大，受论文篇幅及学术性质的限制，无法将整个系统的所有设计细节及各式解决方案表述完全。

本章选择车联网安全认证管理系统中管理子系统中功能最复杂、职责最重要的安全管理员模块与业务员模块，结合UML类图与时序图进行重点开发说明，同时结合系统活动图、证书模板等图表对业务子系统的核心业务逻辑进行详细设计。此外，还将对系统的数据库在上一章概要设计的基础上进一步明确各表单中的内容。

5.2 业务子系统设计

本文中，面向车联网智能设备的安全认证业务是系统核心的功能之一，主要由业务子系统负责完成。智能设备通过注册审批机构的代理，向系统发出业务申请，系统接收到申请之后进行处理，将结果以报文形式返回给RA。

5.2.1 安全认证逻辑设计

车联网环境中，主要的智能设备有两类，一类是车载设备（OBU），一类是路侧设备（RSU）。OBU由于搭载在智能网联汽车上，故而时刻处于高速运动的状态下；而RSU作为支持车联网正常运作的关键节点，具有种类繁多、情况复杂的特点。为了能够成功为他们提供安全认证及管理，将系统实现安全认证过程的逻辑结构详细设计如下。

车联网平台中，由于智能设备数量较多、实时情况纷繁复杂，尤其是可能存在着伪装成业务申请的网络攻击，如果由本系统直接接收并处理所有消息报文，将会大大影响安全认证业务的效率，甚至威胁到系统安全。为解决这一问题，车联网中智能设备申请各种业务并不由它们直接向安全认证管理系统发送报文，安全认证管理系统下发证书也并不直接发送给智能设备，二者通过注册审批系统间接实现安全认证业务。注册审批系统和本文设计的系统一样，是车联网平台的重

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