铁路计算机应用
RAILWAY COMPUTER APPLICATION

基于数字信封的铁路电子公文交换系统的研究与实现

张向阳，苏　飞，朱韦桥，王伟萌

Railway electronic document exchange system based on digital envelope

ZHANG Xiangyang, SU Fei, ZHU Weiqiao, and WANG Weimeng

引用本文:
张向阳, 苏飞, 朱韦桥, 等. 基于数字信封的铁路电子公文交换系统的研究与实现[J]. 铁路计算机应用, 2024, 33(7): 51–55.
ZHANG Xiangyang, SU Fei, ZHU Weiqiao, et al. Railway electronic document exchange system based on digital envelope[J]. Railway Computer Application, 2024, 33(7): 51-55.

在线阅读 View online: http://tljsjyy.xml-journal.net/2024/I7/51

文章编号：1005-8451（2024）07-0051-05

基于数字信封的铁路电子公文交换系统的研究与实现

张向阳，苏　飞，朱韦桥，王伟萌
（中国铁道科学研究院集团有限公司　电子计算技术研究所，北京　100081）

摘　要：随着铁路信息化的不断发展，铁路企业都建立了各自的电子公文系统，用于内部公文的批示和流转，但铁路企业间及上下级企业间仍然缺乏安全有效的公文交换方式和手段。文章基于数字信封加密传输技术，设计了铁路电子公文交换系统，阐述了其系统的架构、功能和关键技术。试用表明，该系统的应用可有效提高铁路企业间的公文交换效率，降低信息泄露风险，具有一定的推广价值。

关键词：数字信封；铁路企业；电子公文；数据交换；协同办公
中图分类号：U29 : U285 : TP39　**文献标识码：**A　**DOI：**10.3969/j.issn.1005-8451.2024.07.09

Railway electronic document exchange system based on digital envelope

ZHANG Xiangyang, SU Fei, ZHU Weiqiao, WANG Weimeng
(Institute of Computing Technologies, China Academy of Railway Science Corporation Limited, Beijing　100081, China)

Abstract: With the continuous development of railway informatization, railway enterprises have established their own electronic document systems for internal document approval and circulation. However, there is still a lack of secure and effective ways and means of document exchange between railway enterprises and between superior and subordinate enterprises. This paper designed a railway electronic document exchange system based on digital envelope encryption transmission technology, and elaborated on system architecture, system functions, and key technologies. The trial shows that the application of this system can effectively improve the efficiency of document exchange between railway enterprises, reduce the risk of information leakage, and has certain promotional value.

Keywords: digital envelope；railway enterprise；electronic document；data exchange；collaborative office

随着铁路信息化的不断发展，铁路企业都建立了各自的电子公文系统，用于内部公文的批示和流转。铁路电子公文交换是指通过信息化技术实现铁路企业之间的信息交流和公文传输。铁路企业具有纵向多层级、横向多单元、组织规模大、地域跨度广、工作事项多、业务复杂、人员覆盖面广等特点，不同铁路企业间建立安全、高效、便捷的电子公文交换系统显得尤为重要。目前，铁路企业间及上下级企业间仍然缺乏安全有效的公文交换方式和手段。

众多研究人员针对上述需求展开了相关研究，狄波等人[1]基于数字签名和 USB Key 身份验证等技术进行了电子公文交换研究，实现了中国铁路成都局集团有限公司内部公文交换和处理；杨光等人[2]基于数字信封技术，进行了电子公文交换过程中的机密性和完整性设计与研究，实现了电子公文的安全交换。但上述研究存在无法进行企业间电子公文交换等问题。

数字信封是一种对称加密和非对称加密相结合的安全通信加密技术[3]，具有安全性高、兼容性好等特点。本文基于数字信封设计了铁路电子公文交换系统（简称：本文系统），实现铁路企业间电子公文安全、便捷、实时交换，提高公文处理效率，降低信息泄露风险。

1　系统架构

本文系统主要由公文交换系统核心和公文交换模块组成。系统架构如图 1 所示。

收稿日期：2024-02-19
基金项目：北京经纬信息技术有限公司科研项目（DZYF23-22）；中国国家铁路集团有限公司科技研究开发计划（N2023W011）
作者简介：张向阳，助理研究员；苏　飞，助理研究员。

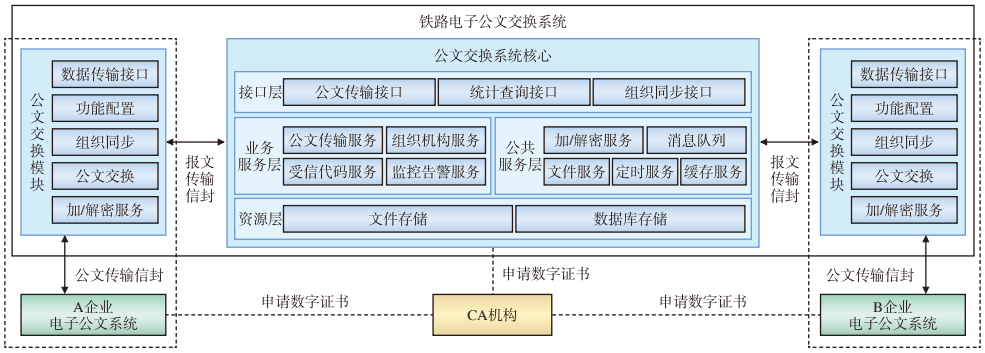

图1 铁路电子公文交换系统架构

1.1 公文交换系统核心

公文交换系统核心采用微服务架构，在对业务进行合理划分的基础上将整体系统拆分为独立的服务，提高开发效率，增强横向扩展能力和降低故障影响[4]，包括资源层、公共服务层、业务服务层和接口层。资源层实现文件存储和数据库存储；公共服务层提供通用的加/解密服务、消息队列服务、文件服务、定时服务及缓存服务；业务服务层提供公文传输、组织机构、受信代码、监控告警等服务；接口层提供公文传输接口、统计查询接口和组织同步接口，用于前端页面展示及接口调用。

1.2 公文交换模块

公文交换模块主要用于实现各铁路企业电子公文系统与公文交换系统核心通信的功能，提供数据传输接口、功能配置、组织同步、公文交换及加解密等服务。各铁路企业将该模块集成到本企业电子公文系统中，通过公文传输信封和报文传输信封进行数据封装、加密及签名保护后进行公文传输。

1.3 CA 机构

为增加数据交换双方的可信任性，本文系统引入第三方权威数字证书授权（CA，Certificate Authority）机构。各铁路企业电子公文系统集成公文交换模块进行数据交换前，需要先向 CA 机构申请国密数字证书，用于数据传输过程中的加/解密及签名保护。CA 机构无需与本文系统及各铁路企业的电子公文系统进行网络联通，仅需通过数字证书中的签名及签名有效期确保数据证书的合法性和有效性[5]。

2 系统功能

2.1 组织机构同步

本文系统依托铁路组织机构唯一编码，对铁路组织机构信息进行统一管理，当铁路企业组织机构有变动时，通过组织机构同步功能实时同步至铁路电子公文交换系统，确保接入的各企业电子公文系统进行数据交换时组织机构的唯一性和准确性。

在组织机构同步过程中，本文系统作好数据的校验工作，保证组织机构编码的唯一性，同时记录相关日志，包括同步时间、同步数据、同步结果等，以便及时发现和解决同步过程中的异常情况。各铁路企业需要保证本企业组织机构信息的准确性和完整性，及时更新和维护本单位组织机构数据。数据同步前要做好数据清洗和校验工作，初次全量数据采用手动同步方式，增量数据采用实时自动同步方式，并做好数据备份工作。

2.2 受信代码申请

受信代码申请功能对来自不同铁路企业的接口请求进行身份验证和权限控制，确保系统的安全性和可控性。

各企业在调用本文系统 WebService 接口前必须通过单位唯一标识 AppKey、AppSecret 向本文系统申请受信代码，作为后续功能接口调用凭证。受信代码由系统随机产生，由双方系统认可且不重复的字符串组成，用于双方身份确认。受信代码具有时效性，受信超时时间在申请受信代码时作为参数约定（但不可超过公文交换系统设置的最长时间），在受信代码有效期内，不必重复申请。在报文传输过程中，须将受信代码作为参数进行一并传输。

2.3 电子公文数据交换

2.3.1 公文发送

公文发送是指各铁路企业通过调用本文系统的

接口，将成文后的电子公文发送给其他铁路企业。本文系统依托 CA 证书和数字信封加密等技术，确保公文发送过程中的数据完整性和保密性；支持公文的发送和补发功能，针对错发等问题，在公文未签收状态下提供公文收回功能，在公文已签收状态下提供“前文作废、以此为准”的公文重发功能，标记前序已签收的错发文件，确保公文信息准确送达。

2.3.2　公文接收

该功能包括公文的接收、消息回执反馈及消息跟踪等。公文接收企业接收到公文后的签收、拒收和退回等操作，通过公文短报文类型向发送方发送消息回执反馈，便于公文发送方及时了解公文的到达情况及后续处理情况。消息回执反馈和消息跟踪可实现公文发送方对公文传递过程的实时监控，全面了解公文的流转情况。

2.3.3　公文数据统计

该功能主要包括对公文的发送、签收、补发、错发纠正的统计，以及异常数据统计，方便运行维护（简称：运维）人员及时掌握铁路企业间的公文交换情况。同时，该功能提供可追溯的信息，主要记录公文交换处理过程及运维人员干预等特殊操作，从而加强整个公文交换过程的合规性和安全性，提高公文交换工作的透明度。

2.4　监控告警

该功能可帮助运维人员及时发现系统异常，保障系统的正常运行，主要包括 4 个方面的功能。

（1）性能监控：监控系统所在服务器的 CPU、内存、磁盘等硬件资源的使用情况，及时发现负载高、磁盘空间不足等异常情况，防止因资源不足导致的系统崩溃或性能下降。

（2）应用监控：监控系统的应用程序运行状态，及时发现程序出现异常或崩溃的情况，并自动进行告警和错误日志记录。

（3）中间件监控：监控消息队列和缓存集群的运行状态，以及消息队列中消息消费情况，记录消息消费异常信息，自动进行消息补偿消费等操作。

（4）网络通信监控：监控本文系统与其他接入系统的网络通信情况，及时发现网络故障或攻击情况，并进行日志记录。

3　关键技术

3.1　电子公文交换报文结构设计

电子公文交换报文分为报文传输信封和公文传输信封，其中，报文传输信封用于公文交换模块与公文交换系统核心间数据文件的传输；公文传输信封用于各企业电子公文系统与集成的公文交换模块之间数据文件的传输，具体结构如图 2 所示。

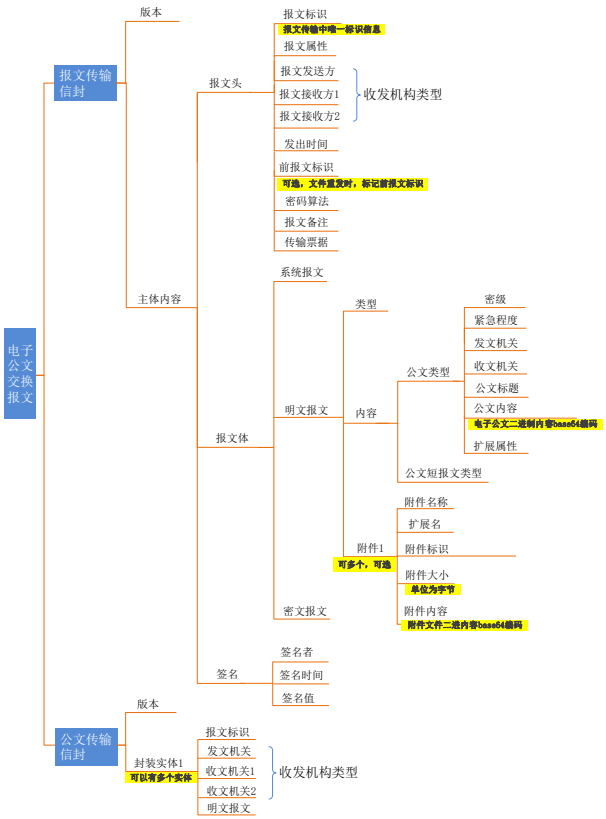

图2　电子公文交换报文结构

3.1.1　报文传输信封

报文传输信封主体内容包括报文头、报文体和签名。其中，报文头包含报文标识、报文属性、报文发送方、报文接收方、前报文标识、发出时间、密码算法等信息。报文体分为系统报文、明文报文和密文报文。系统报文用于发送系统通知类内容，可自定义包含信息；明文报文包含报文类型、报文内容和附件信息；密文报文指按照报文头中密码算法对明文报文进行加密后生成的报文。签名指对报文内容进行签名保护，记录整个报文信封的签名值

和相关信息，其中，签名值是将报文传输信封整个文件的二进制内容经过计算生成摘要信息后再进行数字签名，进行签名和验证签名时，需要将签名节点内容置空后再进行运算。

3.1.2 公文传输信封

公文传输信封主体包括版本及封装实体。封装实体包含报文标识、发文机关、收文机关及明文报文等信息。其中，明文报文内容同报文传输信封中的明文报文内容一致，因公文交换模块与各单位电子公文系统集成在一起，因此，使用公文传输信封封装的数据无须进行加密传输。

3.2 数字信封加密传输技术

3.2.1 数字信封原理

对称加密指加密和解密使用同一个密钥，优点是计算量小、加解密速度快、效率高。但由于加密和解密采用相同密钥，密钥的管理和分发较困难，不够安全。使用对称加密数据传输前，需要发送方和接收方商定好密钥，一旦一方的密钥泄露，则无法保障加密信息的安全。

非对称加密指加密和解密使用不同的密钥，公钥用来加密信息，私钥用来解密信息，公钥可以公开，私钥由解密一方保管。非对称加密安全性更高，但是加密效率没有对称加密快。

数字信封的原理是采用对称加密方法对大批量数据进行加密，再采用非对称加密方法对对称密钥进行加密。解密过程中，先用非对称密码算法解密获取对称算法密钥，后使用对称算法密钥解密数据，从而获取数据明文[6-7]。

3.2.2 数字信封封装流程

本文系统中的报文传输信封加密策略采用数字信封方式，使用CA证书对传输数据进行数字签名，确保电子公文数据在传输过程中的真实性和完整性[3,6-7]，具体封装流程如图3所示。

（1）利用数字信封技术，使用对称算法加密明文数据，密钥随机生成；

（2）使用接收方的公钥加密随机生成的对称算法密钥，将加密后的密文和对称密钥根据报文结构分别封装进报文头和报文体；

（3）报文头和报文体通过SM3算法生成消息摘要，再使用发送方的私钥生成签名信息；

（4）将报文头、报文体及签名信息统一封装成报文传输信封。

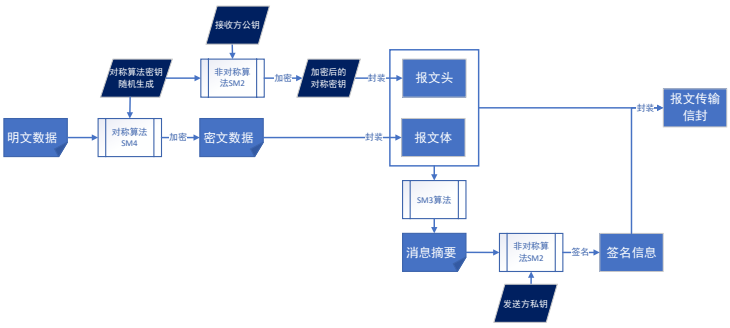

图3 基于数字信封的报文传输信封封装流程

3.3 数据交换时序

A铁路企业向B、C铁路企业发送电子公文，需要调用集成的公文交换模块数据接口，将公文发送给铁路电子公文交换系统，再由该系统发送给B和C企业，具体的数据交换时序如图4所示。

（1）A企业通过唯一标识向本文系统申请受信代码，受信代码随机产生，在受信代码有效期内可重复使用；

（2）A企业向本文系统请求铁路唯一组织机构信息；

（3）A企业通过数字信封方式进行数据加密，并封装报文；

（4）A企业向本文系统发送封装后的报文；

（5）本文系统获取报文信息，验证数字签名（简称：验签），通过后解密报文信息，并存储报文数据。

（6）本文系统将报文接收企业信息放置分发消息队列中，同时将解密后的报文数据按步骤（3）再

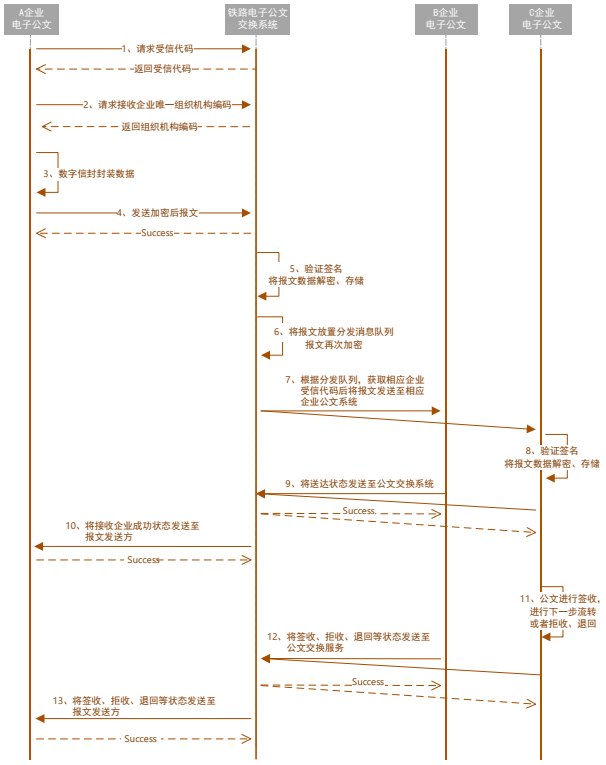

图4　数据交换时序

次进行数据加密并封装报文；

（7）铁路电子公文交换系统根据分发消息队列，分发至 B 企业和 C 企业；

（8）B 企业和 C 企业接收到报文数据后，按照步骤（5）对报文进行验签和解密操作，获取电子公文报文信息；

（9）B 企业和 C 企业将公文的送达状态反馈至本文系统；

（10）本文系统将公文的送达状态反馈至 A 企业公文发送方；

（11）B 企业和 C 企业进行签收操作，进行下一步流转，或进行拒收/退回操作。

（12）B 企业和 C 企业将“签收”“拒收”或“退回”等回执状态返回本文系统。

（13）本文系统将回执状态返回公文发送方。

4　系统应用情况

本文系统已在多个铁路企业部署并进行上线试用。试用期间，本文系统依托 CA 证书、数字信封及受信代码等可靠的加密技术和访问控制机制，有效地确保了公文信息的机密性、完整性和可靠性；通过铁路唯一组织机构编码及消息队列等技术，确保公文能够及时、准确地传递和处理，并实现了交换结果的及时通知，以便发文企业跟进后续工作；本文系统提供的电子公文交换记录查询和统计功能，方便用户随时了解公文交换的进度和状态。

综上，本文系统在试应期间取得了良好的效果，也积累了大量的试用数据和优化经验，为本文系统的推广应用提供了良好的数据支撑。

5　结束语

本文通过设计铁路电子公文交换系统，为铁路企业提供了更加便捷、高效、安全、可靠的电子公文交换服务，可有效提高铁路企业的公文处理效率，降低信息泄露风险。后续将进一步完善和优化该系统功能，增强其稳定性和安全性，改善用户体验、提升易用性，为铁路企业提供更加专业、及时、高效的电子公文交换服务。

参考文献

[1] 狄　波. 成都铁路局电子公文交换系统的研究与实现 [D]. 成都：西南交通大学，2014.

[2] 杨　光. 基于数字信封的电子公文安全交换系统设计与实现 [J]. 莆田学院学报，2013，20（5）：74-78.

[3] 赵延博，张学杰，姜永玲. 基于数字信封的高强度文件加密的应用研究 [J]. 计算机工程与设计，2007，28（18）：4357-4359.

[4] 张向阳，朱建生，朱韦桥. 基于微服务的铁路企业协同办公系统研究与实现 [J]. 铁路计算机应用，2021，30（3）：50-54.

[5] 洪　琳，李　展. 数字签名、数字信封和数字证书 [J]. 计算机应用，2000，20（2）：41-42.

[6] 范永清. 密码学及其在现代通讯中的应用 [J]. 信息网络安全，2009（3）：35-39.

[7] 赵文清，王德文，宋　雨. 基于 PKI 的数字签名和数字信封的实现 [J]. 华北电力大学学报，2003，30（6）：71-74.

责任编辑　李依诺