基于移动办公的铁路信息系统数据交换方案研究

李继勇[1] 孔祥瑞[1] 刘洋[1] 彭军[2] 周钰彬[2]
1. 中铁信安（北京）信息安全技术有限公司，中国·北京 100193
2. 中国铁路青藏集团有限公司，中国·青海 西宁 810007

摘 要：论文围绕铁路信息系统建设，提出了一种基于密码技术、安全隔离交换技术，满足铁路信息系统对于高效率跨网移动办公和信息安全性的需求。本方案首先进行了铁路信息系统需求分析，指出既有系统在网络通信安全、计算安全、数据安全、运维管理安全方面存在的挑战，提出的技术方案包括架构设计、技术选型、技术关键点等，特别强调了密码算法、敏感参数管理、随机比特生成技术、安全隔离等关键技术，并提供了一个特别设计的安全隔离和信息交换架构。为基于移动办公技术的铁路信息系统建设提供了具体的思路。

关键词：密码技术；隔离交换；铁路信息系统

Research on Data Exchange Scheme of Railway Information System Based on Mobile Office

Jiyong Li[1] Xiangrui Kong[1] Yang Liu[1] Jun Peng[2] Yubin Zhou[2]
1. China Railway Xin'an (Beijing) Information Security Technology Co., Ltd., Beijing, 100193, China
2. China Railway Qinghai Tibet Group Co., Ltd., Xining, Qinghai, 810007, China

Abstract: This paper focuses on the construction of railway information systems and proposes a method based on password technology and secure isolation exchange technology to meet the needs of railway information systems for efficient cross network mobile office and information security. This plan first conducted a requirement analysis of the railway information system, pointing out the challenges that existing systems face in terms of network communication security, computing security, data security, and operation and maintenance management security. The proposed technical solution includes architecture design, technology selection, technical key points, etc. It particularly emphasizes key technologies such as cryptographic algorithms, sensitive parameter management, random bit generation technology, and security isolation, and provides a specially designed security isolation and information exchange architecture. This provides specific ideas for the construction of railway information systems based on mobile office technology.

Keywords: password technology; isolated exchange; railway information system

0 前言

随着信息技术的飞速发展，铁路信息系统在提升运输效率、保障行车安全、提升服务质量等方面起到了至关重要的作用。特别是密码技术和安全隔离技术的成熟运用，为铁路信息化提供了新的思路，移动办公通过密码技术、链路加密、移动认证、安全隔离等措施，能实现资源的远程安全访问、集中管理、动态分配和优化利用，显示出其不受地域限制的便捷性优势。

目前铁路信息系统建设领域非常广泛，Q/CR 855—2021《铁路综合信息网内部服务网外部服务网数据安全交换技术要求》为铁路信息系统提供数据交换安全提供支撑，但目前还缺少综合性的移动办公建设指导，尤其是能满足当前青藏局多种业务场景需求的移动办公方案。论文在上述研究的基础上，综合最新的学术成果，结合国内现有的密码技术、隔离技术等保相关要求，提出一种基于密码技术、安全隔离技术的铁路信息系统移动办公建设方案，同时为后续的各类基于移动办公的铁路信息系统的建设给出了思路。

1 研究背景

2021 年 12 月国铁集团发布的《中国国家铁路集团有限公司互联网接入、终端使用和网站（应用）安全管理办法》明确支持“通过电信运营商移动互联网、无线局域网技术实现的互联网接入方式”。2022 年 1 月国铁集团发布的《“十四五”铁路网络安全和信息化规划》的重点推进示范项目中，“铁网护栏二期工程”要求“优化全路移动互联网安全接入及防护能力”“铁路移动互联网信息平台”要求“打造铁路移动信息化生态圈”。

铁路系统是推动中国经济发展和维护社会稳定的重要核心力量，随着信息技术的不断更新和发展，铁路办公信息化、自动化的应用爆炸式增长，办公业务的安全性和便捷性要求不断提升，传统办公模式已不能满足不断变化的网络管理需求。

2 关键技术

密码技术，通过使用中国自主知识产权的 SM2/SM3/

SM4 密码算法，为安全应用提供加解密、签名验签、杂凑算法、随机数生成、身份鉴别、数字证书管理等基础密码能力支撑。其核心技术包括：SM2 私钥分割、混淆技术；敏感安全参数管理；软件实现专用的随机比特生成器；除支持软件密码模块外，可灵活支持多种硬件密码设备以适应多种使用场景。

安全隔离技术，通过专用硬件设备，拦截 TCP/IP 数据流，过滤丢弃 TCP/IP 协议格式，还原上层应用数据，在访问控制和安全检查的基础上封装私有协议，以数据摆渡的方式实现不同敏感级别网络之间的跨网跨域安全的数据交换，形成逻辑强隔离的网络边界隔离防护机制，可有效的防止网络攻击、数据泄露等安全问题，保障信息安全，其主要特点：安全隔离；数据摆渡；安全审查。

3 建设需求

基于移动接入的铁路信息系统建设需求可从以下维度进行考虑：

①数据中心和网络基础设施：对数据中心的安全性、稳定性和扩展性有很高的要求，需要满足多站点、多地域的覆盖；需要具备高性能的网络连接，保证数据传输的低延迟和高带宽，尤其在铁路运行关键应用中。

②安全性和合规性：铁路系统的数据敏感性决定了需为移动接入部署强化安全措施，需要满足国家关于铁路信息安全的法规要求以及行业标准，如采用安全传输通道保障技术，对办公应用业务数据进行加密传输保护，保证数据机密性和完整性；通过技术手段，实现身份认证和访问控制功能；建设满足等级保护相关要求。

③增效减耗：移动接入构建了一套高度可用的数据交换架构，很大程度上提高了集团公司终端办公效率，由传统 PC 办公模式变为不受地域限制的便捷办公，可在任意地点登录个人账户，使用和查看个人资料，完成自己未完成的任务，显著提升了用户办公效率。

4 技术方案

4.1 系统组成

本方案中提出的移动接入系统组成，如图 1 所示。

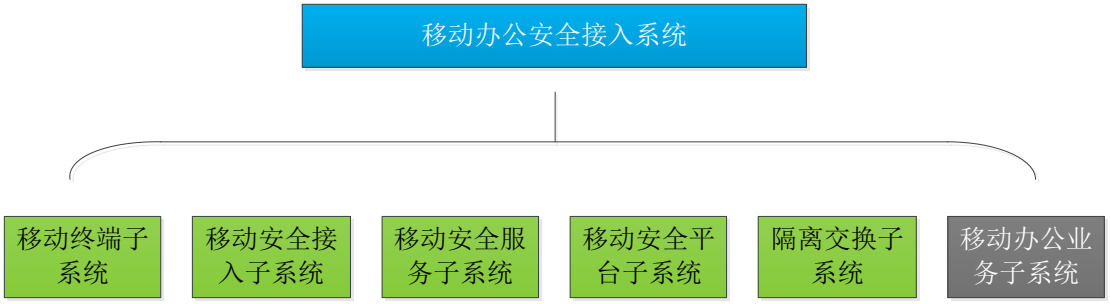

图 1 系统架构图

各层功能如下：

移动终端子系统：在本项目中用户个人移动终端设备需支持 4G/5G/WiFi 无线通信。移动终端上需安装客户端 APP（由第三方公司开发）。该 APP 包含所有铁路局移动办公应用，提供办公应用的统一入口，同时其内部集成 VPN SDK 和软件密码模块（二级），能够实现身份认证、SSL VPN 数据传输加密等功能。

移动安全接入子系统：在本项目中指 SSL VPN 安全网关，支持商密数字证书身份认证、SSL VPN 数据传输加密、访问控制等功能，实现铁路局移动办公业务应用系统接入，保障互联网上数据传输的机密性、完整性和不可否认性。

移动安全服务子系统：在本项目中指移动办公安全接入平台和软件密码模块系统。移动办公安全接入平台支持数字证书的在线申请、下发、管理等功能。软件密码模块系统支持二级密码模块的生产和密码协同计算。

移动安全平台子系统：在本项目中指安全平台，实现用户管理和身份认证。安全平台具备用户管理和身份统一认证能力，可以实现对移动办公用户信息进行管理以及完成用户身份统一认证。

隔离交换子系统：在本项目中指双向网闸，实现互联网接入区与内部网络之间的逻辑隔离，用于解决 CA 与移动办公安全接入平台之间数字证书信息的受控转发。

移动办公业务子系统：在本项目指用户自建政务移动办公应用系统，包含常规的“办文、办事、办会”等通用的办公业务应用，以及涵盖铁路局专用移动作业应用，客户端安装到 APP 内部。

本方案给出的移动办公安全接入系统，典型移动接入部署如图 2 所示。

总体划分为四个部分：移动终端系统，移动安全接入系统，移动安全服务系统，安全隔离与交换系统。通过构筑“加密传输、身份认证与访问控制、隔离交换”纵深防御体系，基于商用密码技术为移动数据提供统一支撑服务，保障用户通过远程接入安全、稳定、高效地访问业务数据和信息资源。

由于本项目涉及铁路信息系统建设，故需遵循相关技术与管理标准，“外网计算机不能访问内网，内网计算机不能上外网”等，保证数据传输过程中的可靠性、连续性及合规性。因此，本方案在铁路外部服务网和内部服务网之间的

部署了安全隔离交换平台，该区域内部署安全隔离交换链路，在移动终端和内网之间，形成逻辑强隔离防护机制。隔离链路为“2+1”结构，“2”表示连接铁路外服网的前置代理服务器、连接铁路内服网的后置代理服务器（以下简称“前 / 后置”），“1”表示前 / 后置之间负责隔离交换的双向网闸。

采用双向网闸传输：利用双向网闸解决两网之间的信息交换，切断协议连接，剥离协议封装，还原应用层数据，实现边界的安全隔离和数据的安全交换，确保比防火墙更加安全的边界逻辑强隔离。

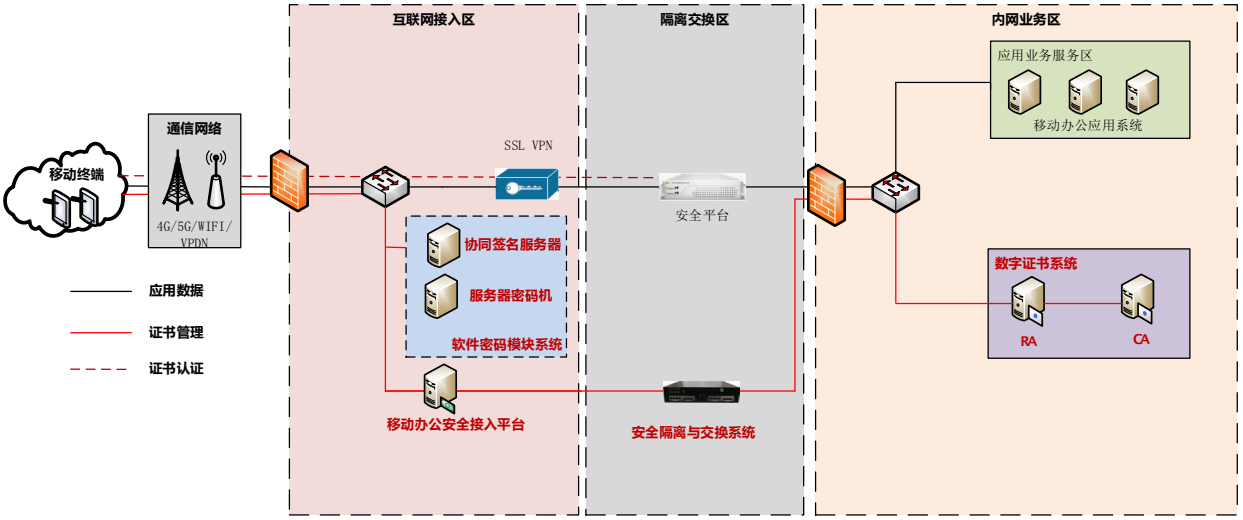

图 2 移动接入部署图

4.2 技术实现

本方案需实现以下技术：

①密码技术：支持中国自主知识产权的 SM2/SM3/SM4 密码算法，为安全应用提供加解密、签名验签、杂凑算法、随机数生成、身份鉴别、数字证书管理等基础密码能力支撑。

②安全隔离与信息交换技术。安全性是铁路信息系统建设的重中之重，本方案在外部服务网和内部服务网之间的部署了安全隔离交换平台，该区域内部署安全隔离交换链路，在移动终端和内网之间，形成逻辑强隔离防护机制。利用双向网闸解决两网之间的信息交换，切断协议连接，剥离协议封装，还原应用层数据，实现边界的安全隔离和数据的安全交换，确保比防火墙更加安全的边界逻辑强隔离；采用双机热备，确保链路的高可用性。

4.3 技术关键

①服务器、终端等推荐使用国产化硬件。

②密码技术，支持中国自主知识产权的 SM2/SM3/SM4 密码算法，包括 SM2 私钥分割、混淆技术、敏感安全参数管理、随机比特生成器、兼容适用。

③隔离交换技术，通过专用隔离部件，拦截内网外协议连接，通过私有协议摆渡受控数据。

④标准防护：依据 GB/T22239—2019《信息安全技术网络安全等级保护基本要求》中“一个中心三重防护”的原则建设。

5 产品选型推荐

本方案介绍的铁路信息系统建设方案需要实际的产品选型方可具体实施，依据铁路信息系统国产化替代的要求，结合等级保护相关安全需求，产品选型优选国产化软硬件平台作为首选。

6 结论

通过深入分析和论证，本研究成功地提出并验证了一种基于密码技术、安全隔离技术支撑的移动办公系统建设方案。该方案展现了移动办公在青藏局铁路信息系统建设中的可行性与高效性，通过构筑“加密传输、身份认证与访问控制、隔离交换”纵深防御体系，基于商用密码技术为移动数据提供系统支撑服务，保障移动终端通过远程接入安全、稳定、高效地访问业务数据和信息资源，为铁路信息系统便捷办公提供更为优质的体验和服务。

参考文献：

[1] 金文龙,翁成斌,胡顺之,等.铁路综合协同业务领域信息技术应用研究[J].中国信息化,2024(9):85-86.

[2] 王伟萌,刘承亮,朱韦桥,等.铁路办公系统异构数据库双活架构构建及数据同步关键技术研究[J].数据通信,2024(4):6-10+26.

[3] 李清欣,吴艳华,周雯,等.面向数据安全流通的铁路隐私计算方案研究[J].铁路计算机应用,2024,33(10):78-82.