技术方法

不动产登记跨网数据交换系统设计与实现

冯永玉[1]，关纯安[1]，王志强[1]，安雷刚[2]

（1.山东省国土空间数据和遥感技术中心，山东 济南　250002；2.山东发泰信息科技有限公司，山东 济南 250014）

摘要：结合山东省不动产登记“一网通办”便民服务平台建设实际，为解决不动产登记系统跨网数据交换技术问题，本文通过安全标记技术、多维动态标记和多机隔离技术等关键技术，使不动产登记跨网数据交换系统具有等级保护定制、跨级主客体访问控制和跨网应用实时监控三大系统特色，解决了数据传输安全的关键技术难题，保障了在不动产登记数据从电子政务外网交换到自然资源业务网过程中，数据从低密到高密的传输安全。

关键词：不动产登记；跨网数据交换；系统设计；自然资源

中图分类号：P208　　**文献标识码**：A　　doi：10.12128/j.issn.1672－6979.2020.11.012

引文格式：冯永玉，关纯安，王志强，等.不动产登记跨网数据交换系统设计与实现[J].山东国土资源，2020，36(11)：81－84. FENG Yongyu，GUAN Chun'an，WANG Zhiqiang，etc. Design and Implementation of Data Exchange System in Different Network of Real Estate Registration[J].Shandong Land and Resources，2020，36(11)：81－84.

0　引言

不动产登记涉及千家万户，关系企业、群众的重大财产安全，一直是社会关注热点[1-4]。根据《国务院办公厅关于压缩不动产登记办理时间的通知》（国办发〔2019〕8 号）《自然资源部办公厅关于完善信息平台网络运维环境推进不动产登记信息共享集成有关工作的通知》（自然资办函〔2019〕1041 号）、山东省自然资源厅办公室《关于做好全省不动产登记“一网通办”便民服务平台建设和对接工作的通知》（鲁自然资办字〔2020〕5 号）要求，参考《山东省电子政务和政务数据管理办法》的管理要求，为进一步做好信息互通共享和“互联网＋不动产登记”工作，将当前部署在自然资源业务网的不动产登记审核（权籍调查成果除外）、登薄、缮证环节业务和不动产登记数据库（不含图形空间数据），通过等级保护三级测评后迁移部署到电子政务外网，不动产权籍调查成果审核业务保留在自然资源业务网。通过省不动产登记“一网通办”便民服务平台，实现互联网申请、电子政务外网审核、自然资源业务网管理权籍信息三网并行模式[5-7]。

本文以不动产登记系统跨网迁移为例，通过对跨网数据交换系统的建设目标和总体建设思路的分析，给出了不动产登记系统跨网数据交换系统的建设思路、功能设计和技术实现。

1　系统建设目标和总体建设思路

1.1　系统建设目标

依托山东政务服务网，开发建设不动产登记“一网通办”便民服务平台，关联全省各市县不动产登记系统，整合全省不动产登记服务资源，开展信息共享集成，推进电子证照库建设和应用，打造全省不动产登记业务线上线下融合、多级联动，随时随地线上申请、网上查看、现场核验、随到随办的“一网通办”新模式。

不动产登记跨网数据交换系统设计遵循易用高效、整合共享、开放便民、保障安全的原则，结合不动产登记系统业务特点，利用安全数据导入、安全数据

收稿日期：2019－12－04；**修订日期**：2020－06－09；**编辑**：王敏

基金项目：国家自然科学基金（青年基金）项目“球面多尺度栅格 Voronoi 图生成及可靠性评价研究”（41801318）；国土资源公益性行业科研专项“国土资源‘一张图’与监管平台建设指南试验验证应用研究”（201311086－04）

作者简介：冯永玉（1979—），男，山东潍坊人，研究员，主要从事自然资源信息化和 GIS 等方面研究；E－mail：fengyongyu@shandong.cn

交换、安全数据隔离相关技术设计一个高效、安全、可靠的不动产登记跨网数据交换平台[8]。

1.2　系统总体建设思路

在开展不动产登记系统跨网迁移时，电子政务外网与自然资源业务网之间通过安全数据交换系统实现跨网络区的安全网络隔离，根据安全策略，对出入电子政务外网的数据分别进行协议剥离、格式检查和过滤，实现安全数据交换，保障自然资源业务网络区的安全。同时作好数据备份、信息同步、安全防护加固、等级保护三级测评和应急恢复预案等工作，保障不动产登记业务连续稳定[9-10]。

(1)适应性原则。在保持内外网络有效隔离的基础上，实现两网间安全的、受控的数据交换。数据交换由电子政务外网以客户机身份与跨网数据交换系统连接，跨网数据交换系统再以客户机身份与自然资源业务网建立连接，实现数据交换。除了必须要开放的用于数据交换的特定应用通道外，跨网数据交换系统不提供任何对外的服务。跨网数据交换系统确保达到等级保护三级的防护效果，最多满足等级保护四级的防护要求。

(2)安全性原则。跨网数据交换系统采用经过精简加固的专用安全引擎，采用经过可信增强的操作系统免疫平台，为跨网数据交换系统提供全方位的保护[11]。

(3)驱动安全原则[12]。跨网数据交换系统数据迁移控制单元使用专用的私有协议与内外网进行通信，且其驱动程序模块也是独立编写的，在这种情况下，即使有人试图通过代码分析洞悉跨网数据交换系统一端机的接口，也无法通过控制单元攻击到另外一端机，也就无法攻击到另一端网络。

(4)专用硬件和专用通信协议加密安全原则。在跨网数据交换系统内部，采用专用高速数据处理部件，使系统具有极高的数据吞吐能力[13-18]。通过在专用操作系统内核中嵌入特有协议和认证机制，使得跨网数据交换系统安全隔离的能力进一步增强。对于并发的多数据流，跨网数据交换系统采用基于虚电路的并发处理机制，从而解决传统多进程处理的效率问题，大大提高现有硬件设备的数据吞吐能力。

2　系统功能设计与实现

遵照等级保护 2.0 与 GW0205－2014《国家电子政务外网跨网数据安全交换技术要求与实施指南》要求，信息系统经过定级、整改后有 4 个部分组成：安全计算环境、安全区域边界、安全通信网络和安全管理中心。安全区域边界负责保证定级系统与外部的信息交换中定级系统的可用性、完整性和保密性。定级系统与外部(其他定级系统)之间的信息交换称为定级系统互联。其中边界的数据交换通过单向光闸、网闸、内外交换服务器完成数据抽取、数据装载、设备认证、格式检查、内容过滤、安全审计等一系列安全功能。

不动产登记跨网数据交换系统由跨网管理中心、跨网交换前置、单向光闸及可信增强模块组成，如图 1 所示。

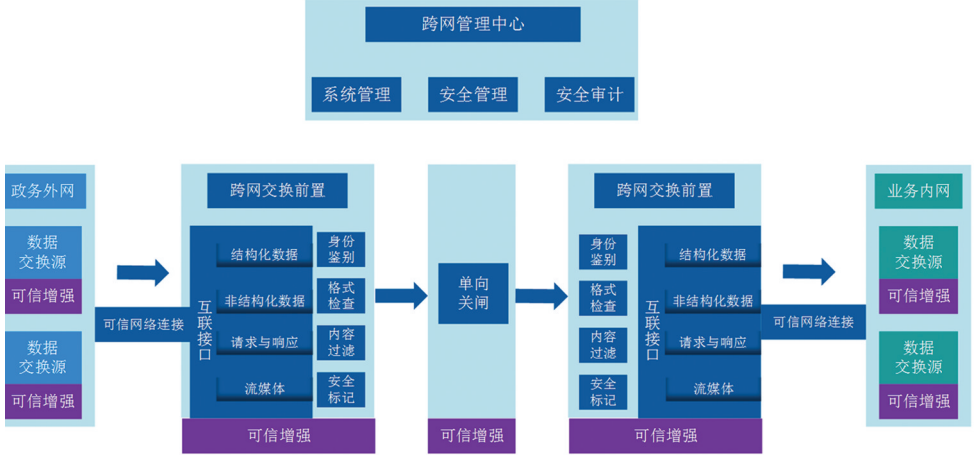

图 1　不动产登记跨网数据交换系统总体功能结构图

(1)跨网管理中心。跨网管理中心负责不动产登记跨网数据交换系统管理、安全管理、安全审计。其中安全管理主要负责策略的管理,可为跨网互联业务需求的定级系统安全管理中心提供策略接口,接收来自定级系统安全管理中心的策略信息,并生成跨级互联策略下发至单向光闸及跨网交换前置执行。

(2)跨网交换前置。在未部署管理中心的定级系统中,可通过跨网交换前置,对需要跨网访问业务进行安全标记,同时负责提供跨网访问互联服务接口并提供应用代理。

(3)单向光闸及可信增强模块[19-21]。单向光闸是定级系统间互联访问接口,并按照管理中心下发的互联策略对定级系统的跨网互联业务进行仲裁,同时提供应用信息流控制、身份认证、访问控制、日志审计等功能,确保只有策略允许的互联业务可以通过。

单向光闸由 3 个部分组成:发送子系统、UPET(单向专用交换通道和接收子系统)。其中发送子系统与接受子系统是两台独立的主机系统。发送子系统与接收子系统之间存在唯一的连接接口,即 UPET(单向专用交换通道),如图 2 所示。

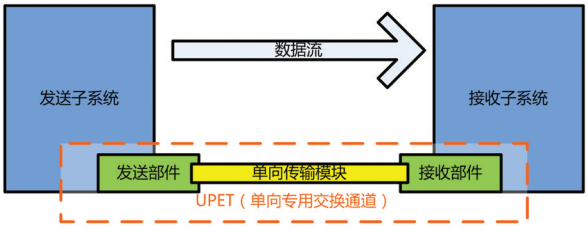

图 2　单向光闸数据单向传输功能结构图

UPET(单向专用交换通道)包含了发送子系统中的发送部件、接收子系统中的接收部件以及连接发送部件和接收部件的单向传输模块。发送与接收部件为两块专用数据交换卡,分别通过 PCI－E 接口与发送/接收子系统相连。发送/接收部件采用专用的信号传输模块,模块之间由单根光纤和单向传输模块连接组成。发送子系统的发送部件只具有信号发射模块,接收子系统的接受部件只具有信号接受模块,由此保证信号从政务外网到自然资源业务网的绝对单向传输。

3　关键技术及特色

3.1　系统关键技术

不动产登记跨网数据交换系统主要应用了以下关键技术:

(1)安全标记技术。目前,大量的定级系统内,未部署安全管理中心,同时,未对系统内进行主客体标记。因此,在跨网互联业务中,难以对其身份或行为进行鉴别。不动产登记跨网数据交换系统通过安全标记技术,针对未进行安全标记的跨定级系统互联业务进行安全标记,为数据交换提供仲裁依据。

(2)多维动态标记。不同于传统的标记,不动产登记跨网数据交换系统可以根据主客体信息、访问控制权限、应用协议等构建多维标记,从而实现对标记的立体化。此外,多维标记还可以根据时限要求进行自动更换,实现动态标记。多维动态标记技术可以有效地保护主客体对标记的使用安全,避免标记冒用的问题,提高标记的复杂性和安全性。

(3)多机隔离技术。不动产登记跨网数据交换系统中的单向光闸采用多系统隔离技术,即通过多主机之间的专用通信硬件及专用通信协议交换方式,对跨网互联业务进行协议剥离与转换,实现不同定级系统之间安全隔离前提下高效受控的数据交换。

3.2　系统特色

(1)等级保护定制。不动产登记跨网数据交换系统的设计,参考 GB/T25070,综合了安全隔离、身份认证、访问控制等多种成熟技术应用的优点,解决了等级保护整改过程中,跨网安全互联问题,为国家网络安全等级保护制度的落地提供了有力的技术支持。

(2)跨级主客体访问控制。通过“跨网管理中心”,可以对不动产登记跨网数据交换系统中所有的组件和主客体的访问控制策略进行集中管控配置,通过“单向光闸和交换前置”,对既定的跨网主客体访问进行标记控制。

(3)跨网应用实时监控。通过不动产登记跨网数据交换系统可以实现对跨网的应用进行实时监控,一旦业务出现中断,可以采用多种方式及时通知到管理人员,从而保证跨网访问的有效性。

4　结语

随着山东省不动产登记“一网通办”平台建设工作的开展,不动产登记跨网数据交换系统承载了所有电子政务外网与自然资源业务网之间的数据交换

工作。物理链路上单向的数据推送结合应用层的安全过滤，充分利用标记技术保障了在不动产登记数据从电子政务外网交换到自然资源业务网过程中，数据从低密到高密的传输安全。不动产登记数据从自然资源业务网交换到电子政务外网过程中，为保证高密到低密的安全性，根据国家保密相关政策，只能通过人工拷贝的方式将数据导入电子政务外网。针对实时访问的不动产登记类业务，单向传输＋人工离线拷贝的数据交换模式还不能满足不动产登记数据实时交互的需要，如何在保证安全的前提下，解决自然资源业务网到电子政务外网数据交换的时效性，是我们下一步继续探索和研究的方向。

参考文献：

[1] 李军，丁雷龙，王芳.不动产登记分析数据库建设研究[J].信息技术与信息化，2018，47(7)：152－154.

[2] 黄宝华.烟台市不动产数据整合建库关键技术研究[J].山东国土资源，2018，34(8)：85－90.

[3] 汪修勇，卢威志，吴非，等.莒县不动产统一登记信息数据整合与平台建设研究[J].山东国土资源，2018，34(4)：78－83.

[4] 靳婷.不动产统一登记存量数据整合中房屋空间关联技术与实现[J].北京测绘，2017(S2)：41－44＋57.

[5] 平宗玮.山东省基础地理信息数据库管理系统升级技术分析及关键点研究[J].山东国土资源，2019，35(8)：53－58.

[6] 侯一俊，陈卉，杨征，等.“互联网＋政务服务”的发展趋势及对自然资源部门门户网站的启示[J].山东国土资源，2019，35(7)：78－81.

[7] 徐秋晓，孙斌，李常锁，等.济南城市四维动态地质信息系统构建研究[J].山东国土资源，2018，34(10)：115－119.

[8] 江娜.山东省地理国情信息综合统计分析技术与实现[J].山东国土资源，2018，34(6)：65－70.

[9] 史卫杰，颜敏.不动产历史数据整理及入库方案探讨[J].山东国土资源，2018，34(1)：65－71.

[10] 周建宁，季君，彭璇.公安内外网数据交换平台的设计研究[J].中国公共安全(学术版)，2017(2)：73－77.

[11] 王永连，李树虎，贺佃鹏.物理隔离网间数据单向传输策略的设计[J].网络空间安全，2018(6)：70－73.

[12] 梁晓兵，刘书勇，李涛永.面向对象的用电信息系统安全通信协议设计[J].电测与仪表，2019(4)：80－87.

[13] 巫钟兴，阿辽沙·叶，郑安刚.基于面向对象互操作技术的用电信息采集系统通信协议设计[J].电测与仪表，2016(24)：69－74.

[14] 杨伟，何杰，万亚东.物联网通信协议的安全研究综述[J].计算机科学，2018(12)：32－41.

[15] 陈雅琳，张京伦，马永红.基于国密算法的主动配电网安全通信协议研究[J].电力信息与通信技术，2018(12)：14－21.

[16] 胡倩.基于可信计算的物联网物品信息传输协议研究[J].无线互联科技，2018(20)：21－23.

[17] 沈昌祥.可信计算构筑主动防御的安全体系[J].信息安全与通信保密，2016(6)：34.

[18] 冯登国，秦宇，汪丹.可信计算技术研究[J].计算机研究与发展，2011(8)：1332－1349.

[19] 黄强，常乐，张德华.基于可信计算基的主机可信安全体系结构研究[J].信息网络安全，2016(7)：78－84.

[20] 谈剑峰.可信计算技术研究与应用[J].信息安全与通讯保密，2014(3)：116－119.

[21] 袁学旺，杨金涛，赵倩，等.智慧潍坊时空大数据与云平台建设及应用[J].山东国土资源，2019，35(10)：71－75.

Design and Implementation of Data Exchange System in Different Network of Real Estate Registration

FENG Yongyu[1]，GUAN Chun'an[1]，WANG Zhiqiang[1]，AN Leigang[2]

(1.Shandong Geographical Institute of Land Spatial Data and Remote Sensing Technology Center，Shandong Ji'nan 250002，China；2. Shandong Fatai Information Technology Limited Corporation，Shandong Ji'nan 250014，China)

Abstract：Combining with the construction of convenient service platform of "all in one network" of real estate registration in Shandong province，in order to solve cross network data exchange technology，based on the security technology，multidimensional dynamic marking and machine key technology，custom level protection，across different level subject to access control and real－time monitoring of cross network data exchange system of real estate registration can be realized. It has solved the key technology of data transmission security，ensured the transmission security of data from low density to high density in the process of real estate registration data exchange from e－government extranet to natural resources business network.

Key words：Real estate registration；data exchange in different network；system design；natural resources