房地产智能决策系统安全支撑平台①

郑卜之，段 斌

(湘潭大学 信息工程学院, 湘潭 410005)

摘 要：用简单对象访问协议(SOAP)消息签名加密的方案来解决房地产智能决策系统在跟其他异构系统数据交互时的通信安全的问题。参照国家对电子政务实施过程中信息安全的建议，综合考虑效率和安全性，通过对各种不同安全方案进行筛选和整合。并在 C#平台和 WSE3.0 开发环境下，实现安全支撑平台具有很好的安全性、可靠性、灵活性、可管理性和可扩充性。

关键词：智能决策；简单对象访问协议；电子政务；安全支撑平台

Security Support Platform for Intelligent Decision System of Real Estate

ZHENG Bu-Zhi, DUAN Bin

(College of Information Engineering, Xiangtan University, Xiangtan 410600, China)

Abstract: In this paper, a scheme of message signature and encryption based on Simple Object Access Protocol (SOAP) is designed for the intelligent decision-making system of real estate to solve communication security issues when interacting data with other heterogeneous systems. Referring to the national recommendations upon the information security area in the e-government implementing process and considering both efficiency and security of communication procedures between two endpoints, we screened and integrated various security methods, then implemented a security platform with C# and WSE3.0. The experiment shows its good safety, reliability, flexibility, manageability, and scalability.

Key words: intelligent decision; SOAP; e-government; security support platform

1 导语

随着科学技术的进步，智能系统越来越完善，在更多的地方发挥了重要的作用。房地产作为中国国民经济的支柱产业，不仅与国民经济有关，还涉及到建筑业、金融业、市政、交通、能源等重要部门，直接关系到中国经济的发展状况。结合我国政府行业的信息化建设现状，正处在从系统互联阶段到智能决策阶段转变这一现状[2]。房产智能决策系统将在一体化建设的基础上，充分利用现有资源优势，对数据、流程进行高度整合，对当前房地产市场建模，通过设定各种评价体系，提高对房地产市场现状分析的科学性和合理性。对房地产市场的研究需要通过对大量相关数据的整合，建立相关模型，对房地产交易量以及其他影响因素以及其合理性进行研究，并得出具有指导意义的成果[3-5]。房地产市场智能决策将建立专家系统，通过对整合建筑、金融、市政、交通等其他相关部门权威数据的学习和训练，来预测后期走势。

智能决策平台的专家系统需要大量细粒度的数据来进行全方位的学习，而传统房地产数据获取方式主要通过相关部门发布的信息播报或者通过网络、电话等方式联系相关部门来获取部分指定数据。这样的方式数据获取的数据难以达到细粒度的标准，而且具有一定的滞后性、高度整合性，以及因为计算方式不同而产生一定的误差。因此，为了更好的服务于智能决

① 收稿时间:2011-11-14;收到修改稿时间:2012-01-06

策系统，需要建立一个数据统一交换平台，能够从不同部门实时获取相关数据。然而各个部门在建设初期各种资源和技术的限制，采用的网络环境、操作系统和数据库都有所差异，传统的交换方式难以保证数据传输的安全性和可靠性。因此，如何在交换过程中实现数据提供方和数据访问方的可信，访问数据内容的可控，以及后期的可审查，都是目前难以实现不同异构系统间数据互通共用的难点。

本文基于电子政务对信息化安全性、可靠性、灵活性、可管理性和可扩充性[6]的需求，根据国家工信部发布的《基于互联网电子政务信息安全实施指南》的标准，设计并实现了一个异构系统间安全接入与安全互联的电子政务网络。主要实现了安全接入与安全互联，保证电子政务网络的安全性；较强的安全认证、授权管理与访问控制机制，确保电子政务系统的可控性和灵活性；采取分类分域控制措施，进行不同类别信息和系统的有效保护[6]来保障系统的可管理性；模块化设计保证了系统的可扩充性。

智能决策系统共分为基本设备和数据存储层、安全平台支撑层和智能系统决策层。安全支撑平台工作在基本设备和数据存储层与智能决策之间，用以支持用户的身份认证和信息的安全传输。

2 智能决策系统安全支撑平台体系设计

2.1 智能决策系统的体系结构、功能划分与组成。

本文综合考虑电子政务系统集成服务所要求的灵活性、层次性、可管理性和易维护性，设计出了由基本设备和数据存储层、安全平台支撑层和智能决策系统层构成的房地产智能决策系统体系结构。

智能决策系统中的基本设备和数据存储层主要包含数据库服务器、身份认证服务器、应用系统等，为智能决策平台提供基础数据来源。然而这些数据存储在不同部门的系统中，由于开发时没有也不可能进行统一规划，因此数据具有较大的异构性。安全支撑平台为了解决异构数据的安全传输问题，通过将数据映射到统一的 XML 文件的方式，解决了数据异构的问题，为智能决策层提供统一的数据格式，在此基础上实现了安全的数据传输功能；智能决策层根据安全支撑平台层提供的信息，对信息进行整合，做科学的分析，通过人工智能对数据进行预测与提取，得到最后最终的一个预测结果。房地产智能决策系统体系结构如图 1 所示。

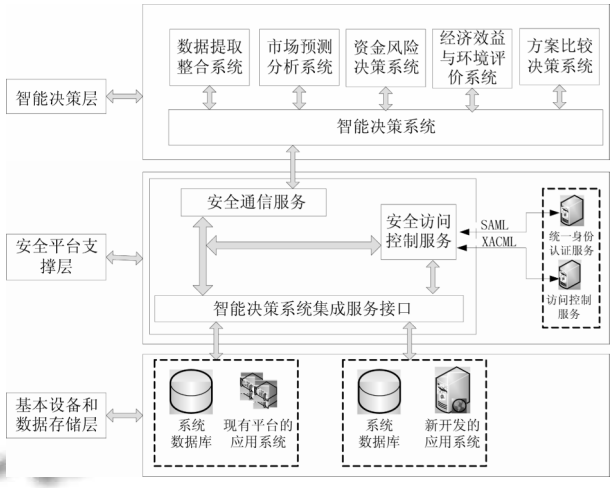

图 1 智能决策系统体系结构

2.2 安全支撑平台的体系结构

安全支撑平台主要包括两大模块：(1)安全通信服务模块，(2)安全访问控制服务模块

2.2.1 安全通信服务模块

安全支撑平台与访问实体之间的信息传输既要考虑效率，又要考虑安全性。本文尝试过以下两种方案来保证通信服务的安全性。

方案 1：直接在应用层传输报文，安全工作交给底层去做，最初方案是通过程序生成交互的报文，报文交给底层安全协议 SSL 传输，这样传输层的信息传输效率相对较高，但通过查看登录后的 SOAP 报文可知，该方案应用层的安全得不到保证。

```
- <soap:Envelope xmlns:soap="http://www.w3.org/2011/05/soap-envelope" xmlns:wsu="h
  - <soap:Header>
    - <wsu:Security>
      - <wsu:Timestamp wsu:Id="Timestamp-3365059e-9f17-4435-82d7-c438009734d1">
          <wsu:Created>2011-08-21T12:19:01Z</wsu:Created>
          <wsu:Expires>2011-08-21T12:19:26Z</wsu:Expires>
        </wsu:Timestamp>
      </wsu:Security>
    </soap:Header>
  - <soap:Body>
    - <HelloWorld5Request xmlns="http://tempuri.org/">
        <UserName>AloneWind</UserName>
        <Password>AloneWind</Password>
      </HelloWorld5Request>
    </soap:Body>
  </soap:Envelope>
```

图 2 采用方案一后登录信息的 SOAP 报文

方案 2：结合 XML、SOAP、WS-security 标准，建立了 Web 服务安全通信系统的有效功能模型，可有效满足公共服务安全中的统一身份鉴别、统一授权管理；访问控制的要求。

本文在 C#平台和 WSE3.0 开发环境下，对电子政务系统安全服务器与客户端间传输的 SOAP 消息进行

签名加密，这样就有效地保证了客户端与智能决策系统安全服务器之间的通信安全。方案 2 登录后的 SOAP 报文如图所示。

图 3　采用方案二后登录信息的 SOAP 报文

通过对上述两种方案登录后的 SOAP 报文的比较可知，方案 2 报文对用户名、登陆口令等信息经过了加密，安全性较好，故本文采用方案 2 实现安全通信模块。

2.2.2 安全访问控制服务模块

因为决策涉及众多部门的数据，并不是所有的数据智能决策系统都需要，因为私密性的需求，也不是所有的数据都可以被访问。因此，需要制定一套灵活的访问控制方案。根据公共服务安全中对统一身份鉴别和授权管理的要求，本系统采用证书和口令相结合的身份鉴别方式，解决该问题通常有两种方案：

方案 1：将子系统密码和安全平台密码作映射，再进行加密，这也是最常用的方案，实现简单，可用数据库直接完成，但安全性较差。

方案 2：从一个身份认证服务器获得 SAML 令牌，并以它为凭证访问多个子系统，方式灵活，但相对比较繁琐，且一个服务器进行控制的这种方式过于集中，容易受安全威胁，受攻击后影响更严重。

由于上述二种方案的欠缺性，本文按照 SAML 和 WS-Security 安全体系结构，将方案 1 和方案 2 结合起来，改进了统一身份认证鉴别和授权管理模块，该模块体系结构模型如图 5 所示，即安全支撑平台通过密码映射加密的方式登录身份认证服务器，然后通过 SAML 安全令牌登录子系统。

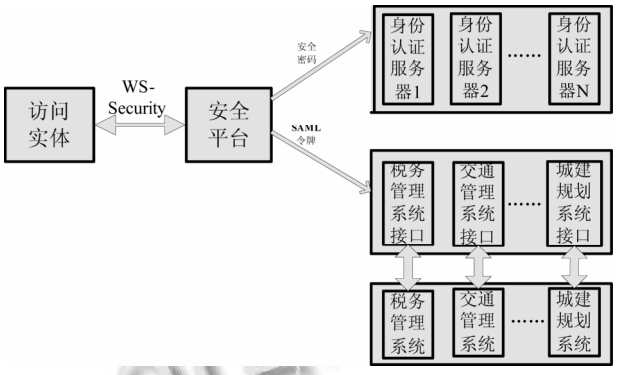

图 4　统一身份认证体系结构

传统的访问控制有自由访问控制(DAC)和强制访问控制(MAC)，DAC 将访问决定权交给产生消息的主体，MAC 要求所有用户遵循管理员建立的规则，两者的灵活性和在控制粒度上不及基于角色的访问控制(RBAC)。XACML 是一种基于角色的访问控制方式，它不仅提供了一系列逻辑算法对整个授权过程进行控制，而且提供了支持定义新功能、数据结构、合成算法等的标准可扩展点。本作品采用基于角色访问控制技术和 XACML 标准在智能决策系统中提供灵活和细粒度的控制，该实现方法的核心是实现策略文件的制定和上下文处理器对请求报文的评估。

3　安全平台支撑层的具体实现

安全支撑层通过集成服务接口与安全访问服务器和其他电子政务系统进行安全通信。安全支撑平台屏蔽原有各系统身份认证的差异性，为各部门的各种应用系统提供统一的基于 SAML 的身份认证、XACML 的访问控制等安全基础服务。通过把上述功能模块发布为服务，为需要进行用户身份认证的系统提供认证服务，访问控制决策与授权服务等。房地产智能决策系统安全支撑平台通过与原有数据库、应用系统协商，负责与其安全模块交互，为用户和需要交互的系统提供一个统一的安全访问接口。同时本平台不仅是一个安全信息转换接口，还可作为一个完整安全访问与通信模块，当新系统加入时，不必再单独设计安全模块。

3.1 安全通信服务

基于 WSE3.0 平台实现通信双方进行三次握手，从而防止了通信过程受潜在欺骗攻击，重放攻击。Web

服务安全通信机制的实现是通过逻辑节点协作完成，要实现 SOAP 消息的安全传输机密性、完整性、不可否认性，具有 SOAP 消息签名/验证、SOAP 消息加密/解密、认证信息处理、安全属性处理等功能。

具体流程如下：

① 系统将用户信息封装到 SOAP 请求报文中，放在 SOAP 的 Body 元素中。然后对 SOAP 请求报文进行签名：先用单项 Hash 函数计算摘要，然后生成一对非对称密钥，用此私钥进行对摘要值进行加密得到签名值，接着构造一个<Signature>元素，里面包含<DigestMethod>(摘要计算方法)、<DigestValue>(摘要值)、<Signature Value>(签名值)等元素，最后把<Signature>元素封装到 SOAP Header <Security>元素中。

② 对签名后的 SOAP 消息进行非对称加密：使用 X509 证书进行加密，构造<EncryptedData>元素，里面包含<EncryptedMethod>(加密方法)、<X509Certificate>(X509 证书信息)、<EncryptedKey>(加密密钥)、<CipherData>(加密后的值)等元素。再把<EncryptedData>元素替换原信息。

③ 将 SOAP 消息发送到服务器端，服务器接收后进行解密：先从<EncryptedKey>中提取出加密私钥，然后用加密者的私钥对此 SOAP 报文进行解密。

④ 对解密后的消息进行验证：签名与验证双方先要对签名密钥进行协商，使用同一对非对称密钥。

3.2 安全访问控制服务

按照 SAML 和 WS-Security 安全体系结构，构建由访问实体(即客户端)、身份认证服务器和目标应用系统三部分组成的模型。本模块主要生成 SAML 令牌，并将对验证 SAML 令牌为合法用户提供权限范围内的服务。身份认证控制时序如图 5 所示。

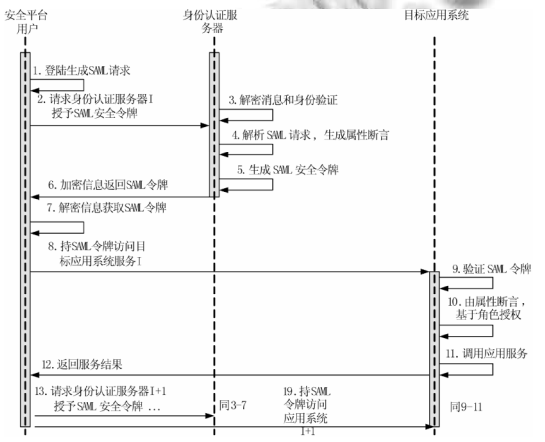

图 5 身份认证控制时序图

XACML 不仅提供了一系列逻辑算法对整个授权过程进行控制，而且提供了支持定义新功能、数据结构、合成逻辑算法等的标准可扩展点，还定义了基于 PAP(策略管理点)、PIP(策略信息点)、PEP(策略执行点)、PDP(策略决策点)等构建的体系结构，能够在分布式的环境中根据主体、资源、环境的属性以及所采取的行为进行控制——允许还是拒绝。返回的结果有四种：允许(Permit)、拒绝(Deny)、无法决定(Indeterminate)和不适用(Not Applicable)。

XACML 控制流程图如图 6 所示：

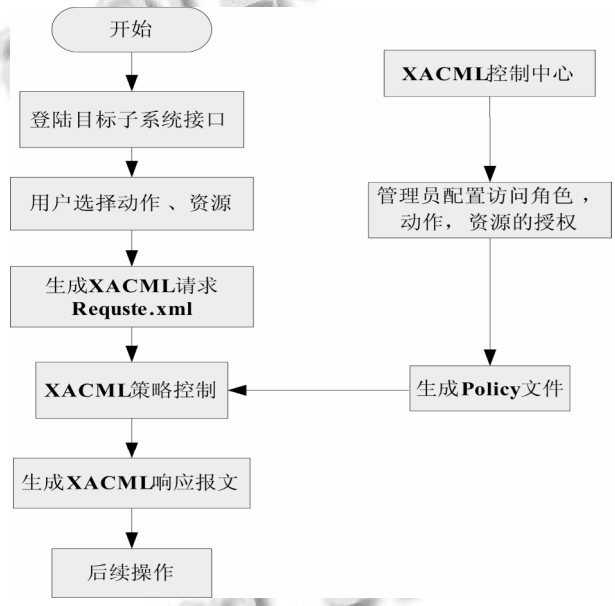

图 6 XACML 控制流程图

3.3 平台子系统的可扩充性

本文以 Microsoft Visual Studio 2008 C#为环境，利用 Web Service Enhancement3.0 平台实现安全通信，分别基于 ComponetSpace.SAML2 和 XACML.Core 组件实现安全通信服务模块和安全访问控制服务模块。由访问实体、安全平台和服务器端三者构成的智能决策系统集成服务安全支撑平台体系结构。

在添加新的子系统时，只需要子系统遵循核心控制文件的数据标准，通过 XACML 的策略决策点的 policy.xml 文件对外来访问进行权限控制。真正做到即插即用。

4 结语

本文从电子政务系统应用集成的实际需要出发，

提供了一个完整、可靠的面向 Web 服务的安全支撑平台。本文以《基于互联网电子政务信息安全实施指南》为指导，结合 WS-Security、SAML、XACML 等一系列国际、国内的标准，在 C#平台和 WSE3.0 开发环境下，设计了安全支撑平台用来实现系统的安全性、可靠性、灵活性、可管理性和可扩充性的安全需求。

服务器与客户端间的传安全采用采用 SOAP 协议对消息进行签名加密，增强了客户端与其他电子政务系统安全服务器之间的安全性；在统一身份认证模型的基础上，实现了支持不同协议的绑定的单点登录的统一子接口，增强了系统的可控性和不可抵赖性；在子系统接口上建立 XACML 的策略决策点来控制用户的访问权限，将单点登录与访问控制相结合的来保证了智能决策系统的可管理性。

参考文献

1 中华人民共和国质量监督检疫总局.中国国家标准化管理委员会,GB/Z24294-2009,信息安全技术 基于互联网电子政务信息安全实施指南,2010,2.1.

2 杨梅云.关于电子政务系统整合及应用支撑平台建设的思考.电子政务,2009,8.

3 曾力勇,裘亚峥.房地产开发项目三阶段投资决策的实物期权模型研究,长沙理工大学学报(社会科学版),2005,2.

4 杨培培,邓长荣,马永开.我国商品房市场量价关系的实证分析,当代经济管理,2009,7.

5 鞠方,欧阳立鹏.我国房地产价格的影响因素及其合理性研究.财经理论与实践,2008,4.

6 胡勇.广州电子政务中信息交换系统的设计.世界电信,2003,7.

7 XML signature syntax and processing. [2007-10-13] http://www.w3.org/ R/xmldsig-core/.

8 XML encryption syntax and processing.[2007-10-13]. http://www.w3.org/TR/xmlenc-core/.

(上接第 34 页)

基于深圳“图文一体”数字房产系统架构的设计研究，本次选择了典型片区进行了深圳市“图文一体”数字房产系统的开发试验，实现了图文一体化，做到了以图管房，大大提升了深圳房产管理的准确性、直观性、科学性和透明度。如图 5 是该应用系统的一个客户界面。

4 结语

随着城市建设的日新月异和房产交易的市场化发展，房产信息的计算机化管理变得尤为重要。作为数字城市的重要组成部分，数字房产的研究和应用越来越受到广泛重视。数字房产是 GIS 以及房产综合业务管理相结合的产物，是一个庞大的系统工程，是房地产业发展和社会信息化的必然趋势，具有良好的市场应用前景[4]。

深圳市数字房产综合查询系统是一个二维和三维集成的综合性查询系统。通过对政策性住房管理、房产交易、房产产权登记和物业等业务数据的整合，并与建筑物空间数据库、3D 数据库建立关联，实现了一套共同的基本楼盘表，最终给公众提供强大的房产信息综合查询服务，让公众可以更加便捷、直观的了解房屋的详细情况，对数字房产系统建设具有一定示范意义。

参考文献

1 姜小奇.数字房产的一体化设计.福建电脑,2007,4:172–173.

2 宋亚超,张宏,温永宁,蒋文明.南京“数字房产”WebGIS 共享平台研究.计算机工程,2004,30(15):161–163.

3 石伟伟,钟耳顺,蔡阳军.“数字房产”时空数据模型的建立与应用.地球信息科学,2006,8(3):12–16.

4 毛迎丹.GIS 技术在房产管理信息系统中的应用.软件导刊,2008,7(2):113–114.