

学校编码: 10384

分类号\_\_\_\_\_密级\_\_\_\_\_

学 号: 200228030

UDC\_\_\_\_\_

厦 门 大 学  
硕 士 学 位 论 文

基于 Web Service 的 EDI 关键技术研究  
与原型系统设计

The Research of EDI Core Techniques and the Design of  
Prototype Based on Web Service

王 飞 龙

指导教师姓名: 李名世 副教授

专 业 名 称: 计算机应用技术

论文提交日期: 2005 年 5 月

论文答辩日期: 2005 年 6 月

学位授予日期: 2005 年 月

答辩委员会主席: \_\_\_\_\_

评 阅 人: \_\_\_\_\_

2005 年 5 月

## 厦门大学学位论文原创性声明

兹提交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文而产生的权利和责任。

声明人（签名）：

年 月 日

## 摘 要

EDI(电子数据交换)可以在不同部门的信息系统间实现结构化的事务数据交换,在电子商务、电子政务以至各个行业都有着迫切而广泛的需求。传统的 EDI 系统历经几十年的发展,至今仍然难以在实际应用中得到普及,究其原因,主要在于使用 EDIFACT 作为数据交换的标准,扩展性较差,不能适应各个行业复杂变化的数据格式要求;使用专用的软件和通信平台,开发和应用成本高昂,使用复杂,且不便同现有的 MIS 兼容,容易受到防火墙的阻隔,因而其应用范围受到很大的限制,尤其难以被中小型用户所接受。在这种情况下,探讨如何利用最新的软件和互联网技术,构建符合当今主流技术标准的低成本 EDI 平台,拓展 EDI 的应用范畴就是一项非常有意义的研究工作。

本文在剖析传统 EDI 系统关键技术(报文表示、报文交换和系统结构)的实现原理和存在缺陷的基础上,分析了 Web Service 松散耦合、面向组件和跨平台的技术优势,解析了其基础协议 XML、SOAP、WSDL 和 UDDI 的技术内涵,提出了构建新型 EDI 平台的总体技术方案,包括采用 XML 表示 EDI 报文,利用 SOAP 进行报文传输,运用 B/S 模式重构 EDI 体系等。

论文接着对新型 EDI 系统的安全框架进行了比较深入的研究。在分析各种典型加密算法之后,提出了适用于 EDI 的 XML 数据加密和数字签名机制;尤其在权限控制方面,设计了一种面向 Web 服务的 RBAC 模型(WS-RBAC),通过引入互斥角色的概念和参数级的控制,实现了更为安全的控制模型。

作者利用 J2EE 平台初步实现了一个新型 EDI 系统原型,最后对其实现技术进行了简要的描述,并对需要进一步研究的相关课题进行归纳和展望。

关键词: web 服务; 电子数据交换; web 服务安全

厦门大学博硕士学位论文摘要库

## Abstract

EDI (Electronic Data Interchange) can implement the structured transaction data interchange among the information systems within different departments. There is an impending demand of EDI for all kinds of industries such as e-business and e-government. Although traditional EDI techniques have been developed for several decades, they cannot be applied in practice. The vital reason lies in the weak extensibility of the EDIFACT data interchange standard. It cannot adapt to the complicate and changeable requirement of different data interchange situations. On the other hand, it is very expensive to use specific non-standardized software and communication platform to develop and deploy EDI. Furthermore, it is not compatible with existed MIS (Management Information System) and is more possible to be prevented by firewall using this EDI implementation. So this implementation mechanism has a big limitation and cannot be accepted by customers especial by small business customers. In this situation, analyzing latest related techniques, designing standard low-cost EDI platform as well as extending its application becomes a promising research issue.

In this thesis, after the analysis of the implementation and defects of core techniques (e.g. message representation, message exchange and system architecture) used in EDI, we explored the advances of Web Services Technique: loose-coupled, component-oriented and cross-platform and examined the related standard protocols such as XML, SOAP, WSDL and UDDI. Based on this knowledge, we proposed a solution to build up a new EDI platform. It includes using XML to represent EDI message, using SOAP in transmission, apply Browser/Server architecture refactoring EDI system and so on.

In the next step, we pursued our research in the security issues of the proposed EDI system. We proposed XML data encryption and digital signature

methods suitable for the EDI system based on the analysis of famous encryption algorithms. We design a new RBAC permission control model for web service called “WS-RBAC”. It utilizes the concept of mutex roles and parameter control to implement a safer control model. We have implemented a prototype of the proposed EDI system using J2EE. In the last part of this thesis, we briefly introduced the implementation of this prototype and draw a conclusion on the further research in the future work.

Keywords: Web Service; EDI(Electronic Data Interchange); Web Service Security

## 目 录

<b>第一章 绪论 .....</b>	<b>1</b>
1.1 研究背景.....	1
1.2 本文主要研究内容 .....	4
<b>第二章 Web Service 技术剖析.....</b>	<b>5</b>
2.1 服务体系结构 .....	5
2.1.1 Web 服务的定义 .....	5
2.1.2 Web 服务模型 .....	5
2.1.3 Web 服务协议栈 .....	7
2.2 Web 服务的关键技术.....	9
2.2.1 XML.....	9
2.2.2 SOAP .....	10
2.1.3 WSDL .....	11
2.2.4 UDDI.....	11
2.3 Web 服务的安全.....	12
2.3.1 Web 服务的安全需求 .....	12
2.3.2 Web 服务安全的技术 .....	13
<b>第三章 EDI 关键技术的改进 .....</b>	<b>15</b>
3.1 EDI 报文的 XML 表示 .....	15
3.1.1 EDIFACT 报文格式 .....	15
3.1.2 XML 表示 EDI 数据 .....	18
3.2 XML 的数据格式转换 .....	20
3.2.1 XSL 介绍 .....	20
3.2.2 XML 数据格式转换实现.....	21

<b>3.3 报文交换系统的改进 .....</b>	<b>22</b>
3.3.1 传统 EDI 的报文传输系统.....	22
3.3.2 Web Service 结构下的传输系统 .....	23
<b>3.4 EDI 系统结构的更新 .....</b>	<b>24</b>
3.4.1 传统 EDI 系统结构.....	24
3.4.2 Web Service EDI 系统结构.....	25
<b>第四章 新型 EDI 系统的安全机制研究.....</b>	<b>29</b>
<b>4.1 EDI 系统的安全需求 .....</b>	<b>29</b>
<b>4.2 XML 加密 .....</b>	<b>29</b>
4.2.1 XML 加密概述.....	29
4.2.2 加密算法分析.....	31
4.2.3 XML 加密机制设计.....	34
<b>4.3 XML 签名 .....</b>	<b>36</b>
4.3.1 XML 签名概述.....	36
4.3.2 数字签名机制分析.....	37
4.3.3 XML 签名机制设计.....	39
<b>4.4 权限控制.....</b>	<b>42</b>
4.4.1 Web Service EDI 的权限控制需求.....	42
4.4.2 访问控制策略分析.....	42
4.4.3 Web Service EDI 权限控制设计.....	45
<b>第五章 J2EE 平台上的新型 EDI 系统原型设计 .....</b>	<b>49</b>
<b>5.1 系统的技术选择方案 .....</b>	<b>49</b>
5.1.1 SunJ2EE 介绍.....	49
5.1.2 Microsoft .NET 介绍 .....	50
5.1.3 系统所选用的 Web Service 平台 .....	51
<b>5.2 电子数据交换模块 .....</b>	<b>52</b>

5.2.1 模块功能具体实现.....	52
5.2.2 主要工作流程.....	54
<b>5.3 数据安全模块 .....</b>	<b>54</b>
5.3.1 功能模块具体实现.....	54
5.3.2 主要工作流程.....	59
<b>5.4 访问控制模块 .....</b>	<b>60</b>
5.4.1 主要实现类及功能.....	61
5.4.2 主要工作流程.....	62
<b>第六章 结论 .....</b>	<b>65</b>
6.1 全文总结.....	65
6.2 后期工作.....	66
<b>参考文献 .....</b>	<b>67</b>
<b>发表论著 .....</b>	<b>69</b>
<b>致谢 .....</b>	<b>71</b>

厦门大学博硕士学位论文摘要库

## 第一章 绪论

### 1.1 研究背景

随着世界经济的发展和科技的进步，全球经济一体化已经成为 21 世纪的大趋势，电子商务就是这一趋势的产物。Internet 的发展，使得数据不但要在企业内部实现共享，也要在 Internet 上实现共享，才能满足电子商务不断发展的需要。EDI 就是这样一项为满足在各个系统间进行数据交换的技术。

传统 EDI 技术出现在 20 世纪 60 年代末，它采用专用的增值网(VAN Value Added Network)来传输信息，而其信息格式已经专门针对减少传输带宽的要求而进行了优化、压缩和编码，主要使用 EDIFACT<sup>[1]</sup>协议和 ANSI X.12<sup>[2]</sup>协议，具有安全、保密、高效等特点。就技术而言，EDI 报文采用结构化的数据，它是按 EDI 单证标准进行格式化的，而 EDI 用户的应用系统使用的则是各种内部数据库的专用数据格式，因此，EDI 用户在报文提交网络前，须将其译成标准的 EDI 报文格式。在实际应用中，用户系统从数据库中取出符合内部格式的源数据，要先通过一个映射程序 (Mapper) 转化为平面文件 (Flat-file，一种无格式的数据文件)，然后由翻译软件 (Translator) 将无格式的数据添到 EDI 报文的相应字段中完成翻译。同样，接收系统对收到的 EDI 报文需经过“EDI 报文→翻译软件→平面文件→映射程序→系统内部数据格式”的转换才能使用<sup>[3]</sup>。EDI 架构对信息的安全保密提出了很高的要求 (遵循 X.800 安全管理框架)，一般用户系统通过专用的 EDI 增值网 VAN 相连，并由 EDI 服务中心控制数据的传递。EDI 将新的电子信息技术与商业活动较好的结合起来，尤其对于那些信息吞吐量大，复杂度高，安全性、可靠性、完整性、及时性要求很强的高端 B2B

应用有着独特的优势。

不过，经过几十年的发展，EDI 虽然在技术上日趋成熟，但始终无法得到广泛的商业应用，这说明其本身存有较大的局限性，具体而言有如下几点：

- 费用高昂，需租用专用的 VAN，定制一对一转换系统，增加了企业信息处理成本；
- 覆盖面低，采用封闭的专用增值网络，只能与有限的贸易伙伴连接；
- EDI 标准的结构灵活性差，不能随着与其对应的业务环境的变化同步；
- EDI 报文传输有较多限制，只能使用指定的网络协议和安全保密协议；
- 现行单证、报文、EDIFACT/X.12 等标准无法满足实际需求时，无计可施；
- EDI 标准基于传统商业事务规则，由于社会的发展，规则的进步，有许多商务应用已无法用早期的 EDI 标准去规范化表示。

传统的 EDI 已经不能满足不断增长的需求，因此在新一代的 EDI 系统中，必须要满足以下要求：

- 减少商务活动的开支
- 减少进入电子商务的成本
- 提供更加简便的用户操作工具
- 提高数据的完整性和可访问性
- 适当的安全和控制
- 提供可扩展和可控制技术
- 与现有的应用系统相集成
- 利用开放标准
- 提供 X12/EDIFACT 的替换升级及与 X12/EDIFACT 进行互操作的

## XML 语法

- 全球可部署以及全球可维护

Web Service 是一项新兴的技术，Web Service 的目标是要实现语言的独立性、平台独立性并且能够在任何地方使用任何的方式进行访问。这些特性都是 DCOM、COBRA、RMI 等分布式组件不能比拟的。因此，Web Service 概念一提出就倍受推崇，各大技术提供商和传统商业企业都投入到 Web Service 标准的制定和应用的架构中去，基于 Web Service 的公共技术标准 SOAP/WSDL/UDDI /WSFL 等都已经成为了事实行业标准。作为 Web 服务的体系架构的领导者 IBM 和 Microsoft 也已经在全球推广 Web 服务技术。各大技术提供商都已经推出了 Web 服务的开发工具：Microsoft 的 .NET<sup>[4]</sup>，IBM 的 WebSphere<sup>[5]</sup>，Sun 的 SunONE<sup>[6]</sup>等。有理由相信，Web Service 将成为未来动态商务 Web 的主流技术。根据 W3C 的定义，Web Service 是由 URI 定义的一种软件应用程序，其接口和绑定都能被定义，以 XML 方式进行自我描述和可以被发现，并且支持以基于 XML 的消息通过 Internet 协议的方式和其他的应用软件进行直接的互操作<sup>[7]</sup>。Web Service 向外界提供一个能够通过 Web 进行调用的接口，使客户能够很方便地使用提供的服务，不需要增加额外的开支；通过 WS-Security 和数据加密、数据签名技术，保证了数据的完整性，提供适当的安全性；同时 Web Service 与平台无关性，可以比较方便地同现有的系统相集成；Web Service 用于传输数据的格式采用 XML，XML 是基于开放的标准；Web Service 部署在 Internet 上。根据对 Web Service 的分析，我们可以看到 Web Service 满足了新一代 EDI 系统的需求，不失为 EDI 的一种好的解决方法。本文提出了一种采用 Web Service 构建 EDI 系统的新方法，对 EDI 系统的关键技术进行了分析，提出了采用 Web Service 的相关技术实现 EDI 系统中的数据表示格式、通信模式和安全需求，并设计出了一个系统原型。

## 1.2 本文主要研究内容

本文的主要研究对象是电子数据交换系统，研究的目的是探索一种新型的安全的基于 Web Service 的 EDI 系统。本文阐述了对 EDI 系统的核心技术进行深入研究和采用 Web Service 技术对其进行改进的研究工作，尤其是在实现系统安全做了深入地研究，并给出了系统原型的具体实现。

本文共分六章。各章节的内容概述如下：

第一章为绪论。介绍了本文的研究背景，简单介绍了传统 EDI 技术面临的主要问题，提出了采用 Web Service 技术来解决电子数据交换的方案。

第二章剖析了 Web Service 的体系结构及适合 EDI 系统的相关技术。

第三章结合 Web Service 中的技术对 EDI 关键的模块进行了改进，包括报文表示、报文交换和系统结构。

第四章为新型 EDI 系统的安全机制研究，首先分析了 EDI 对安全机制的要求，然后通过相关技术实现了 EDI 的安全机制，包括 XML 数据加密，XML 数据签名，RBAC 权限控制策略。

第五章为具体 EDI 模型的实现，介绍系统实现的技术，包括开发平台的选择，各个功能模块的详细设计。

第六章为结束语，对目前的工作进行总结，并对日后的研究工作及前景进行展望。

## 第二章 Web Service 技术剖析

### 2.1 服务体系结构

#### 2.1.1 Web 服务的定义

Web 服务是描述一些操作(利用标准化的 XML 消息传递机制可以通过网络访问这些操作)的接口<sup>[8]</sup>。Web 服务是用标准的、规范的 XML 概念描述的,称为 Web 服务的描述。这一描述囊括了与服务交互需要的全部细节,包括消息格式(详细描述操作)、传输协议和位置。该接口隐藏了实现服务的细节,允许独立于实现服务基于的硬件或软件平台和编写服务所用的编程语言使用服务。这允许并支持基于 Web 服务的应用程序成为松散耦合、面向组件和跨技术实现。Web 服务履行一项特定的任务或一组任务。Web 服务可以单独或同其它 Web 服务一起用于实现复杂的聚集或商业交易。

#### 2.1.2 Web 服务模型

Web 服务体系结构<sup>[7][8]</sup>基于三种角色(服务提供者、服务注册中心和服务请求者)之间的交互。交互涉及发布、查找和绑定操作。这些角色和操作一起作用于 Web 服务构件: Web 服务软件模块及其描述。在典型情况下,服务提供者托管可通过网络访问的软件模块(Web 服务的一个实例),其定义了 Web 服务的描述并把它发布到服务请求者或服务注册中心;服务请求者使用查找操作来从本地或服务注册中心检索服务描述,然后使用服务描述与服务提供者进行绑定并调用 Web 服务实现或同它交互。服务提供者和服务请求者角色是逻辑结构,因而服务可以表现两种特性。图 2-1

显示了这些操作、提供这些操作的组件及它们之间的交互。

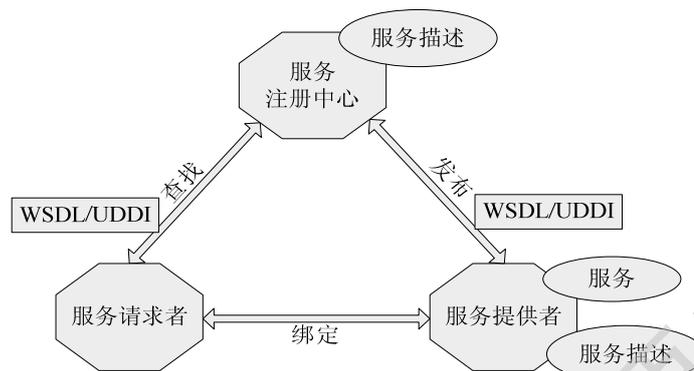


图 2-1 Web 服务角色、操作和构件

### 2.1.2.1 Web 服务体系结构中的角色

**服务提供者：**服务提供者是创建该 Web 服务的实体。从企业的角度看，这是服务的所有者。从体系结构的角度看，这是托管访问服务的平台。

**服务请求者：**任何使用服务提供者建立的 Web 服务的机构都叫做服务消费者。从企业的角度看，这是要求满足特定功能的企业。从体系结构的角度看，这是寻找并调用服务，或启动与服务的交互的应用程序。服务请求者角色可以由浏览器来担当，由人或无用户界面的程序来控制它。

**服务注册中心：**服务注册中心位于 Web 服务体系结构的中心位置，服务提供者在此发布他们的服务描述，服务消费者可以在那里搜索 Web 服务。对于静态绑定的服务请求者，服务注册中心是体系结构中的可选角色，因为服务提供者可以把描述直接发送给服务请求者。同样，服务请求者可以从服务注册中心以外的其它来源得到服务描述，例如本地文件、Web 站点、广告和服务发现（Advertisement and Discovery of Services, ADS）等。

### 2.1.2.2 Web 服务体系结构中的操作

要使 Web 服务起作用，必须有以下三个基本的操作：发布服务描述 (publish)、查询或查找服务描述 (find)、根据服务描述绑定或调用服务 (binding)。这些行为可以单次或反复出现。

Degree papers are in the "[Xiamen University Electronic Theses and Dissertations Database](#)". Full texts are available in the following ways:

1. If your library is a CALIS member libraries, please log on <http://etd.calis.edu.cn/> and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to [etd@xmu.edu.cn](mailto:etd@xmu.edu.cn) for delivery details.

厦门大学博硕士论文摘要库