

基于 XML 相关规范集的动态 Web Service 框架系统^{*}

魏兵海

(华中科技大学计算机科学与技术学院 武汉430074) (国家外存储专业实验室 武汉430074)
(信息存储系统教育部重点实验室 武汉430074)

摘要 介绍了 XML 相关规范集:XML-SIG、XML-Encryption、XKMS、SOAP、WSDL、UDDI,分析了各规范的技术特性和工作原理。基于 XML 相关规范技术,设计了一个可扩展动态 Web Service 框架系统 X-WebServS,包括构建于底层 PKI 公钥基础设施之上的 XKMS 安全模块组件和基于服务定向模型 SOA 的服务发布、查找和绑定的 Web Service 动态交互模块组件。通过 X-WebServS 的体系结构和工作流程剖析,探讨了基于 XML 相关规范的动态 Web Service 实现技术。

关键词 XML 相关规范,动态 Web Service,框架系统

Dynamic Web Service Framework System Based on XML-Related Specifications

WEI Bing-Hai

(School of Computer Sci. & Tech., Huazhong Univ. of Sci. & Tech., Wuhan 430074) (National Storage System Laboratory, Wuhan 430074)
(Key Laboratory of Data Storage System, Ministry of Education, Wuhan 430074)

Abstract XML-related Specifications; XML-SIG, XML-Encryption, XKMS, SOAP, WSDL, UDDI are introduced, which features and mechanisms are analyzed. Based on these XML-related Specifications, an extensible dynamical Web Service framework system X-WebServS is investigated and designed. The X-WebServS includes a XKMS security subsystem on PKI and a dynamical Web Service interactive subsystem on SOA model. Through anatomizing the architecture of X-WebServS and the working flow, the technologies on dynamical Web Service based on XML-related specifications are discussed.

Keywords XML-related specifications, Dynamical Web service, Framework

1. 引言

现代网络是一个多层次架构多异构组件的松耦合开放式系统。当今前沿 Web 技术已经从基于 HTML 的静态浏览 Web 技术经过基于 CGI/GUI 的交互式 Web 技术发展到目前基于 XML 相关规范集的动态 Web Service 技术。然而,在动态 Web Service 实践中,完善地实现异构互操作的数据交换,在存在着中介体的端到端场景中高效实现包含消息层和应用层的整体安全机制,相关问题尚未能得到很好地解决。异构互操作解决方案、整体安全解决方案是动态 Web Service 研究和应用人员重点考虑的二类典型问题。

基于 XML 规范集的相关技术为包含异构互操作机制和整体安全机制的动态 Web Service 解决方案提供了向导。W3C 工作组于1998年2月正式公开发布的可扩展标记语言 XML 1.0 规范^[1]及技术,初步实现了跨平台、跨语言异构互操作的数据交换,其后,XML 迅速渗透扩展到各应用层面,相继出现了一系列符合 XML 语法框架的标准规范集,包括基于 XML 的安全规范套件:XML 签名 XML-SIG (XML Signature)规范^[2]、XML 加密 XML-Encryption 规范^[3]、XML 密钥管理规范 XKMS (XML Key Management Specification) 草案^[4];应用 XML 语法的高效异构互操作 Web Service 协议栈:简单对象访问协议 SOAP (Simple Object Access

Protocol) 候选草案^[5],Web Service 描述语言 WSDL (Web Service Description Language) 草案^[6],统一描述、发现和集成 UDDI 规范^[7]。这些 XML 相关协议和技术的推出为动态 Web Service 的实现提供了应用基础。

本文首先介绍一系列与 XML 相关的规范集与技术,简要分析其特性和原理,之后,基于 XML 相关规范集,提出一个重点考虑异构互操作和整体安全的动态 Web Service 架构,即动态 Web 服务框架系统 X-WebServS (eXtensible Web Service System),通过 X-WebServS 的体系结构和工作流程剖析,探讨基于 XML 相关规范集的动态 Web Service 系统设计技术,包括基于 PKI/XKMS 的安全技术和基于 SOA 服务定向模型的 Web Service 动态交互技术。

2. XML 相关规范与技术

XML 规范是 W3C 组织已经正式发布了的的一种跨语言、跨平台数据交换和表示的语言协议标准,已成为多种 Web Service 协议和安全协议的构建基石。XML 规范语言具有许多其它语言无可比拟的优越特性:XML 利用 DTD (Document Type Declaration) 或 XML Schema 模型定义文档的语法、语义和数据结构,具有严格结构化层次化的特点,利于数据结构或数据的映射和传输转换;XML 文档可包含自描述的元数据,用以标记文档相关信息,XML 的自描述特征增强了

^{*}华中科技大学博士后基金项目:基于 Globus/Web Service 的高性能 CFD 计算网格研究(AA183107)。魏兵海 博士后,主要研究方向:计算机体系结构、电子商务、分布式网络信息安全、机群与网格计算等。

数据交换过程中的定位、查找、检索功能,支持搜索的明确无二义性;XML 还可自定义标签表示特定的数据或属性,具有良好的可扩展性。应用 XML 语法框架的 XML 相关规范技术自然具备 XML 的多种优越特性。

XML 加密规范和 XML 签名规范基于 XML 协议采用 XML 结构封装信息元素,不同于仅仅只能提供文档整体加密功能的普通技术,XML-Encryption 能够提供部分加密功能,当同一文档中不同元素子集涉及不同用户时,能够方便地进行不同机密等级、不同访问权限的子集加密和个体签名,实现层次加密、等级授权的思想。

XML 密钥管理规范 XKMS 提供了一套标准的密钥/证书管理机制。XKMS 密钥管理规范技术的核心思想是由 XML 应用程序集成并简化已有的 PKI 技术^[8]和数字证书技术。通过将密钥的配置、注册等管理功能从原 PKI 用户端分离,委托给第三方的可信服务(Trust Server)中间层处理,XKMS 架构提高了安全系统的通用性、可扩展性和互操作性,并基于瘦客户机概念,减轻客户端负担^[9]。

SOAP 简单对象访问协议基于 XML 描述了一个在分布式环境中交换结构化类型信息的轻量简单技术规范。通过定义一个有标准组件的包模型和数据编码方法,SOAP 提供了表示应用程序语义的机制,从而 SOAP 适用于从消息传递如 HTTP 到 RPC 的各种类型系统。SOAP 主要包括:SOAP 信封:SOAP 信封以 XML 文档封装 SOAP 消息;SOAP 编码:SOAP 编码格式基于一个简单的类型系统概括多种类型系统的共同特性,定义了类型化对象的系列化规则;SOAP-HTTP: SOAP-HTTP 将 SOAP 绑定到 HTTP,兼备 SOAP 的形式化、灵活性和 HTTP 的各种丰富特性,如 SOAP 通信可遵循 HTTP 的 Request/Response 消息模型,即 SOAP 消息的 Request/Response 能够包含在 HTTP 消息的 Request/Response 中;SOAP-RPC: SOAP-RPC 利用 XML 的可扩展性和灵活性封装并交换 RPC,定义了远程过程调用的请求/应答的统一描述形式。在 Web Service 协议栈架构中,SOAP 层位于传输层(HTTP、FTP 等)的上一层。

Web Service 描述语言 WSDL 使用基于 XML-Schema 等类型系统的 WSDL 文档抽象描述 Web Service,定义了一套 Web Service 请求者、Web Service 注册管理者和 Web Service 提供者之间统一通用的 Web Service 描述机制。通过将一个 Web Service 描述为能交换消息的通信终端集,WSDL 提供了应用程序间自动通信的解决方案。在 Web Service 协议栈架构中,WSDL 层位于 SOAP 层的上一层。

UDDI 统一描述、发现和集成协议标准^[7]定义了一整套关于 Web Service 集中注册和 Web Service 发布/查找机制,通过基于 XML 的文档描述 Web Service 的提供者主体信息及被提供的 Web Service 本身的信息,即 UDDI 注册信息,包括:白页-提供者主体的地址、联系方式、标识信息;黄页-提供者主体的标准行业类别信息;绿页-所提供的 Web Service 的技术信息,如 Web Service 描述、调用方法、数据绑定等。UDDI 架构由作为 Web Service 注册入口的 UDDI-Schema 和作为描述注册入口检索用 SOAP 消息的 UDDI API 两层构成。在 Web Service 协议栈架构中,UDDI 层位于 WSDL 层的上一层。

3. X-WebServS 框架系统设计

X-WebServS 系统的设计采用功能模块化架构,充分注重系统的通用性、可扩展性、灵活性、功能模块的可重用性以

及对原有系统组件的兼容性和安全性。主要的设计思想包括:

采用基于 XML 相关规范的标准技术,以跨操作平台、跨编程语言的优良特性提升系统的通用性。系统中所有功能性应用都封装成 Web Service,经由私有 UDDI 注册中心向外提供单一标准的 API 接口,可通过即时递增/递减的方式加以组合或集成,实现良好的可扩展性。

企业内部部门用户和外部企业用户既可通过 Web Service 注册中心发布/查找 WSDL 文档进行动态绑定和 Web Service 调用之外,也可基于特定的 Web Service 交互策略,对固定的部门业务通过两两之间静态绑定,由服务提供者绕过 Web Service 注册中心直接发布 WSDL 文档到服务请求者本地文件系统中,服务请求者查找本地文件系统中的 WSDL 文档选择需要的 Web Service^[10]。如此在提高效率的同时,增加系统的灵活性。

功能模块或其子功能模块如 XKMS 用户端模块设计强调可重用性。

企业原有应用软件或系统组件通过重新封装成 Web Service 发布,提供基于规范的标准 API 以供调用,不涉及原有内部应用源码的任何更改,实现对原有系统的兼容性。

安全策略实行等级解决方案,企业内部部门客户之间点到点交互可采用基本的传输层安全机制,对 XML 文档中重要敏感数据条目进行 XML-SIG 加密,与远程跨国协作子公司以及与外部伙伴企业客户的端到端交互采用 XKMS 密钥/证书解决方案,兼顾安全性与效率以及简易性。

3.1 X-WebServS 架构及主要功能模块

X-WebServS 系统的总体架构如图1所示,包括私有 UDDI 注册中心模块、企业应用服务器模块、作为 Web Service 请求者的企业内部部门和外部企业客户机1-N 模块(按照部门类别分:设计部客户机、财务部客户机、销售部客户机、仓储部客户机、生产计划管理部客户机、原材料供应商客户机等),作为 Web Service 提供者的企业内部部门和外部企业服务器1-N 模块(财务部服务器、销售部服务器、仓储部服务器、零配件供应商服务器、原材料供应商服务器,协作销售商服务器等),安全组件之可信服务模块,安全组件之 PKI 服务器模块。

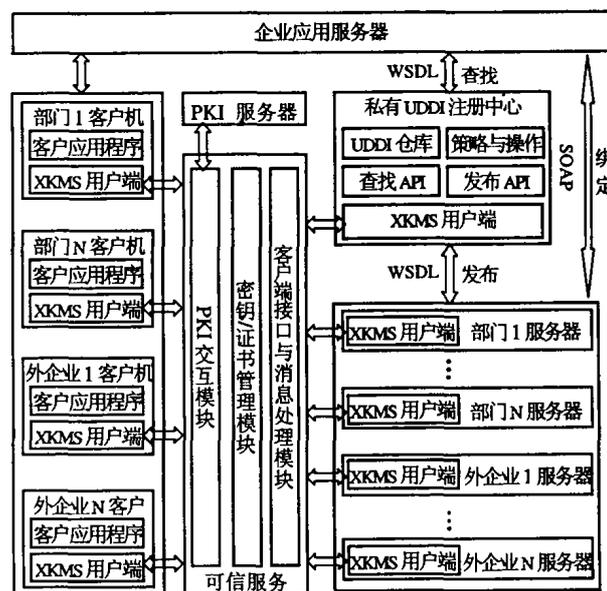


图1 X-WebServS 系统架构

XKMS 用户端模块如图2所示,属于 XKMS 密钥管理系

统中的功能模块,相关组件安装在用户端,实现加密/解密/身份认证等功能,根据文[4,9],主要子功能模块包括:

①安全功能子模块:实现 XML 编码/解析、XML 加密/解密、XML 签字、密钥/数字证书/认证/安全性令牌等功能,包括密钥/证书信息、认证信息的存储功能等。

②XKMS 消息模块:实现客户应用程序与 XKMS 密钥管理系统中可信服务模块交互的 XKMS 消息请求/应答功能,即提供客户应用程序访问可信服务模块并接受其返回的密钥/证书及认证信息的接口。

③传输模块:实现基于标准传输协议(如:HTTP、TCP/IP)以 SOAP 编码 XML 格式的消息传输接口功能。

可信服务模块如图1中所示,基于 XKMS 规范,属于 XKMS 密钥管理系统中的功能模块,实现密钥管理功能。主要子功能模块包括^[4,9]:

①接口与处理模块:可信服务模块面向用户端提供进行密钥/证书管理服务的 API 接口,并完成部分消息处理功能。

②密钥/证书管理模块:负责密钥/证书注册、密钥/证书认证 CA、密钥/证书库、密钥备份/恢复、密钥/证书撤销、策略管理等功能。

③PKI 交互模块:负责实现与底层 PKI 服务器进行交互的功能。基于 XKMS 规范,可同时实现对多个异构 PKI 服务器的交互。

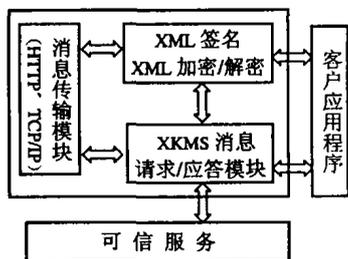


图2 XKMS 用户端模块架构

客户机中的客户应用程序模块包括一些实现部门业务功能的应用程序或应用程序集。考虑到部门业务变化的动态可能性,应用程序可独立增添/删减,无需更改系统的其他模块部分。部门服务器(组)模块提供集成业务处理的 Web Service,发布到受控的私有 UDDI 注册中心,通过 API 供特定的请求者调用。

私有 UDDI 注册中心是一个企业内部 Web Service 注册中心,面向企业内部各部门、内部职员以及已有协作关系的外部客户企业,提供可控制的 Web Service 描述元数据 UDDI 文档及相关映射/查询/发布操作,兼具 Web Service 登记注册和伙伴客户目录的作用^[11]。实现的主要功能包括:

①策略与操作模块:基于特定的访问策略控制 Web Service 的发布、查找和注册。实现 WSDL 文档元素与 UDDI 文档元素之间的映射转换操作。

② UDDI 仓库模块:提供 UDDI 文档以及其元素 businessEntity、businessService、bindingTemplate、tModel 的存储和目录服务等相关功能。

③ 查找 API 模块与发布 API 模块:实现基于 UDDI API 规范的 Web Service 发布/查找接口的各种操作^[12]。

3.2 Web Service 交互机制与 UDDI 对象模型

Web Service 的发布/查找/绑定交互机制如下:

Web Service 提供者使用 WSDL 描述文档对 Web Ser-

vice 进行抽象和封装,WSDL 描述文档主要包括 WSDL 服务接口文档和 WSDL 服务实现文档,通过文档中的元素与 UDDI 数据结构中元素的对应实现映射,将 Web Service 的抽象描述信息发布到 UDDI 注册中心,即在 UDDI 注册中心发布 UDDI tModel 或 UDDI businessService,例如使用发布接口函数 save_tModel 在 UDDI 注册中心增加一个 tModel 结构,通过 save_service 增加一个 businessService 结构。WSDL 到 UDDI 相关数据结构映射关系如图3。

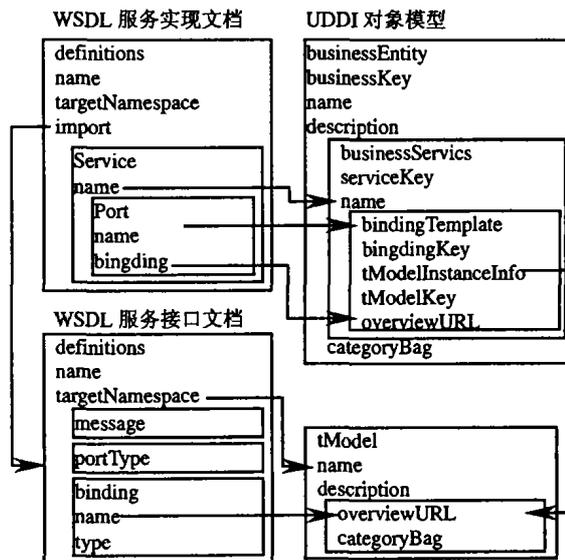


图3 WSDL 到 UDDI 映射

Web Service 请求者通过 UDDI API 在 UDDI 注册中心进行查找,例如:使用接口函数 find_tModel 查找标识 WSDL 服务接口描述的分类 tModel,通过接口函数 find_service 查找标识 WSDL 服务实现描述的分类 service,使用 find_binding 查找 businessService 中多个 bindingTemplate 的一个。

通过查找到的 UDDI 条目关联到 WSDL 元素得到端口等绑定信息后,即完成 Web Service 请求者同 Web Service 提供者的绑定,并可通过 SOAP 机制进行调用交互。

在发布/查找/绑定之后,即进行如下节所述的业务应用操作。

3.3 WebServS 典型应用流程

一个完整的 WebServS 应用流程可能是动态交互的复杂多 Web Service 调用链。考虑重用性并不失典型性,本节以部门客户机 C1(采购部)的应用程序调用部门服务器 S1(采购部)提供的 Web Service(采购部采购清单 Web Service)和部门客户服务器 S2(财务部)提供的 Web Service(财务部资金转账 Web Service)以完成一个 Web Service(资金转账)的应用流程为例,说明 WebServS 系统中客户部门两两之间进行 Web Service 交互的工作流程以及整个系统的架构和相关典型模块的功能。

在进行上述的一个 Web Service(资金转账)之前,C1(采购部)在不同时间内多次调用其它相关部门的 Web Service(如:生产管理部服务器的采购指令 Web Service),将一定周期内不同时间发布的不同类别零配件或原材料的品名、数量等相关信息存储到部门服务器(采购部)的 DB2 数据库。据此,C1(采购部)与外部企业客户服务器(供应商)交互,按照采购策略(价格、质量、交货期等)协商决定采购品类型、采购品价格、采购品数量等,存储相信息到部门服务器(采购部)DB2 数据库。

在上述基础上,基于文[10],进行本 Web Service 应用(资金转账),工作流程描述如下:

首先,部门客户机 C1(采购部)应用程序 Input PartsBuy.jsp 通过应用服务器 PartsListServlet,调用部门服务器 S1 中基于 DADX 的 Web Service(采购清单 Web Service),并以 SOAP 编码 XML 文档返回查询结果-采购清单(类型、数量、价格)。

基于 DADX 的 Web Service(采购清单 Web Service)包括对 DB2 数据库进行 XML 格式的查询/存储的文档访问定义扩展(Document Access Definition Extension)功能,即通过 DB2 XML Extender 中的 DADX 定义关系表或 SQL 语句与 DTD 文件之间的映射,以从 DB2 数据生成 XML 文档或从 XML 文档转换成 DB2 数据,实现具有本地 DB2 数据库查询检索功能的 Web Service。

其次,PayRequest Servlet 将返回的采购清单提交到部门服务器 S2(财务部),调用 S2 中基于 EJB 的 Web Service(资金转账 Web Service),将支票及清单划拨到部门客户机 C1(采购部),PayRequest Servlet 集成并交换 XML 数据和信息。

基于 EJB 的 Web Service(资金转账)使用一个会话 EJB 进行 DB2 数据库 SQL 查询后返回 XML 数据,经过可扩展样式表语言 XSL(Extensible Stylesheet Language)转换成公共的 XML 格式,这一转换模块可选。

整个动态 Web Service 应用架构和工作流程如图4所示。

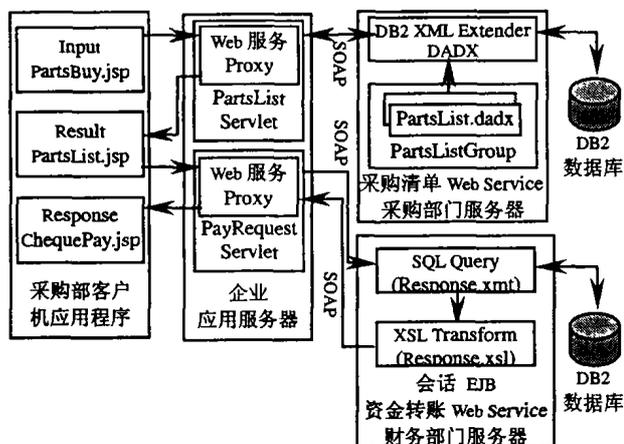


图4 Web应用(资金转账)操作架构和工作流程

4. WebServS 性能特点

基于 XML 相关规范技术的 X-WebServS 动态 Web Service 系统通过 WSDL 封装使复杂异构的应用程序可以跨异构的操作平台或编程语言互相进行交互调用,为跨国企业内部和外部各部门复杂应用系统的对接、升级、维护和定制提供了较传统 EAI 架构更简易高效的全新解决方案。

①单一标准的 Web Service 接口屏蔽了 Web Service 应用程序内部包括操作系统、数据库结构、编程语言、对象模型等各种实现细节的异构性,Web Service 抽象描述文档基于 XML 格式,简洁高效,实现了 Web Service 应用功能模块之间的松散耦合,任意一个 Web Service 应用程序功能模块的故障或变更不影响整个系统其他部分的运行,系统具有容错性和易维护性。

②WebServS 系统具有良好的可扩展性、通用性和功能模块的可重用性。

③基于 PKI 和 XKMS 的密钥管理系统组件提供强大的密钥/证书自动管理功能,即:密钥/证书的自动申请、生成、发放、更新、备份/恢复、托管、撤销。

④基于 PKI 和 XKMS 的密钥管理系统组件提供无缝透明的签名/加密/身份验证等一体化集成功能服务,为 Web 用户提供立体多层次端到端的安全 Web 应用运行环境。

⑤WebServS 系统具有良好的灵活性:动态绑定与静态绑定相结合;实行多级安全解决方案;功能模块化架构可独立增添/删减模块组件或应用程序。

结束语 动态 Web Service 是传统 Web 应用的一次革新,实现了人与程序静态交互到程序与程序动态交互的飞跃。基于 XML 相关规范技术的动态 Web Service 是未来电子商务等网络应用的重要发展方向,动态 Web Service 技术本身正处于不断的发展之中。部分 XML 相关规范候选草案仍在由 W3C 研讨,包含许多细节的规范版本有可能进一步被提升和改进。本文基于现有 XML 相关规范技术对动态 Web Service 系统框架作了初步尝试和探索,今后,随着应用业务需求的变化和相关技术的发展,将逐步递进地进行改进和扩展升级。

参考文献

- 1 Bray T, et al. Extensible Markup Language (XML) 1.0 (Second Edition). W3C Recommendation. October 2000. <http://www.w3.org/TR/2000/REC-xml-200001006>
- 2 Eastlake D, Reagle J, et al. XML-Signature Syntax and Processing. W3C Recommendation. Feb. 2002. <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>
- 3 Eastlake D, Reagle J, Imamura T, et al. XML Encryption Syntax and Processing. W3C Recommendation. Dec. 2002. <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>
- 4 Hallam-Baker P. XML Key Management Specification (XKMS 2.0). W3C Working Draft. March 2002. <http://www.w3.org/TR/2002/WD-xkms2-20020318/>
- 5 Box D, Ehnebuske D, Kakivaya G, et al. Simple Object Access Protocol (SOAP) 1.1 W3C Candidate Recommendation. May 2000. <http://www.w3.org/TR/SOAP/>
- 6 Moreau J J, Schlimmer J. Web Services Description Language (WSDL) Version 1.2: Bindings W3C Working Draft. Jan. 2003. <http://www.w3.org/TR/2003/WD-wsdl-1.2-bindings-20030124>
- 7 Bellwood T, et al. UDDI Version 3.0, Published Specification, July 2002. <http://uddi.org/pubs/uddi-v3.00-published-20020719.htm>
- 8 OMG, Public Key Infrastructure Specification Version 1.0[s] <http://www.omg.org/technology/documents/formal/publickey.htm>. 2002
- 9 Zhang Jiangqing, Liu Xudong, Huai Jinpeng. Research and Implementation of XML-Based Management. Journal of Computer Research and Development, 2003, 40(1)
- 10 Li Jin [Canada]. Web Service in Dynamic e-Commerce. Tsinghua University Press, 2002
- 11 Graham S. The role of private UDDI nodes in Web service Part 1: Six species of UDDI, Part 2: Private nodes and operator nodes. <http://www-106.ibm.com/developerworks/webservices/library> May 2001
- 12 Bellwood T, Bryan D, Draluk V, et al. UDDI Version 2.04 API Specification http://uddi.org/pubs/programmers_API-V2.04-Published-20020719.html Jul. 2002