

基于 Web 服务的企业统一认证与授权系统

呼 和,张 钦,陈国青,杨 旻

(中海油研究总院,北京 100027)

(h.huh02@gmail.com)

摘 要:企业为了实现统一调度和统一管理应用系统的目标,统一认证和统一授权的工作越来越重要且趋于复杂化。首先通过分析统一认证和授权系统的背景和系统目标,进一步通过分析比较统一认证、授权方面的知识点和 Web 服务技术,提出了结合 Web 服务技术来完成企业在认证和授权方面的统一方式,从而方便应用系统的管理人员来分级管理具体的应用系统,真正做到完全统一的认证与授权,并通过实际的项目来提出具体的服务规范(或接口)设计和实现。

关键词:Web 服务;统一认证;统一授权;统一调度;统一管理;服务规范;接口

中图分类号: TP334 **文献标志码:** A

Enterprise unified authentication and authorization system based on Web services

HU He, ZHANG Qin, CHEN Guo-qing, YANG Yang

(Research Institute, China National Offshore Oil Corporation, Beijing 100027, China)

Abstract: In order to achieve the goal of unified scheduling and unified management in application system, unified authentication and authorization has become more and more important and sophisticated. The background and the goal of unified authentication and unified authorization system were analyzed firstly, then the unified authentication, authorization and Web services were analyzed and compared, and a unified method of authentication and authorization in enterprise combining the Web services was proposed; therefore, it was more convenient to administer the concrete application system for administrator, which truly reconstructed completely unified authentication and authorization, and the design and implementation of the concrete service specification (or interface) by the practical project were given.

Key words: Web service; unified authentication; unified authorization; unified schedule; unified administration; services specification; interface

0 引言

随着企业信息化进程的进一步加快,各个应用系统不断地上线运行,系统之间的异构性逐渐加大,企业应用系统之间的联系逐渐淡化,系统的数量直线上升,系统的重复工作量和维护成本在不断增加,管理人员有时候身兼数职,不断地在各个应用系统之间穿梭,如何规范化并减轻这些系统管理人员的工作量,如何在企业层面上提出统一的认证和统一的授权呢?本文通过分析统一认证、授权知识点和 Web 服务技术,并结合 Web 服务技术来完成企业在认证和授权方面的统一,从而让应用系统的管理人员从繁重的工作中解脱出来;并通过实际项目来分析具体的接口设计和实现,实现企业内应用系统认证与授权的统一调度和统一管理;最后,总结出目前这种解决方案的不足和下一步的改进措施。

1 系统概述

伴随着企业的发展壮大,企业中的应用系统逐渐增多,统一认证和统一授权方面的工作越来越复杂多样,下面从系统的目标和系统的定位方面来说明统一认证和授权系统建设的目标。

1.1 系统目标

系统的目标是为了统一各个系统用户、口令,实现单点登录(安全),提供公共认证服务和授权接口,并能够提供统一的授权列表完成用户权限的统一调度和管理。系统的目标具体描述如下。

1) 对于用户来说,所有应用系统必须能安全统一口径,实现统一的用一套用户来认证,做到单点登录(Single Sign On, SSO)。

2) 对于开发人员来说,为了减少今后系统在统一认证和授权方面的开发工作量,需开发必要的服务和定义标准接口规范,以达到尽可能地复用,同时为下一目标的实现做准备。

3) 对于管理人员来说,需要体现授权方面的统一调度和统一管理,从而建立公司信息系统大融合的工作平台。

1.2 系统定位

公司的人力资源服务系统负责将公司大部分员工的机构、岗位和人员信息定期地推送到统一认证系统中,而统一认证系统中还可能其他人员要访问一些专业系统,这就要求统一认证系统中提供一些接口让这些外来人员访问授权后的应用系统,比如分公司人员要访问动态库系统,就直接在统一认证系统中加入相应的虚拟机构、岗位和人员就可以访问相应授权的

收稿日期:2010-07-01;修回日期:2010-10-18。

作者简介:呼和(1978-),男,内蒙古鄂尔多斯人,工程师,硕士研究生,主要研究方向:信息系统; 张钦(1965-),男,四川成都人,主要研究方向:数据库; 陈国青(1965-),男,江苏宁波人,主要研究方向:信息系统安全; 杨旻(1985-),男,广东湛江人,工程师,主要研究方向:信息系统。

应用系统。同时,统一认证系统最主要的工作是为了服务于其他应用系统,比如给其他系统提供一些用户信息、用户映射信息和岗位机构信息等,最终实现通过统一认证系统来统一地管理和调度所有的应用系统的具体人员权限信息。



图1 统一认证系统的定位

2 设计思想与系统架构

设计思想与系统架构将通过分析各种认证方式、授权思想,并简要介绍目前流行的 Web 服务技术,最终提出统一认证与授权系统的架构。

统一认证和授权系统主要包括认证和授权两方面的工作。该系统的提出希望做到统一地认证和统一地授权。最终的目标用户主要是各个应用系统的开发者和一般需要认证的用户,希望帮助他们减轻在认证和授权的工作量,并且规范化认证和授权功能。该系统的类型是各个应用系统的公共部分的浓缩,是一个公共模块,所以需要采用标准的接口和协议来完成设计和开发,尽量采用目前流行的、比较通用的基于 SOA 架构理念的一些标准协议和技术来完成设计和开发。主要目的是为了取代目前现有的统一认证的实现方式,以方便以后更多应用系统的集成,提供一种更加简洁、可靠和安全的方式来完成认证和授权,达到统一的认证、管理和调度。

2.1 统一认证

1) 传统的实现方式。

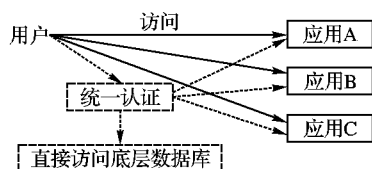


图2 传统的认证实现方式

优点:比较直接和直观,容易实现,以统一认证为中心;

缺点:直接操作底层数据库,不符合基于 SOA 的架构理念。

2) 传统方式的改造。

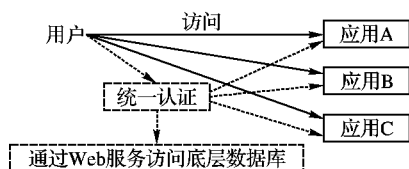


图3 传统认证方式的改造

优点:以统一认证为中心,实现模式比较固定,容易实现,采用标准 Web 服务更加符合基于服务的架构;

缺点:要求各个应用系统中的所有用户密码采用相同密码,或者不需要密码(直接使用登录名获取访问令牌)。

3) 以应用为主的实现方式。

优点:以各个应用系统为主,统一认证系统主要做的是后台服务性的工作,采用标准的 Web 服务提供用户的统一验证。

缺点:要求各个应用系统能够基于 Web 服务标准进行开

发,各个应用系统自己开发独立的登录页面,实现比较麻烦。

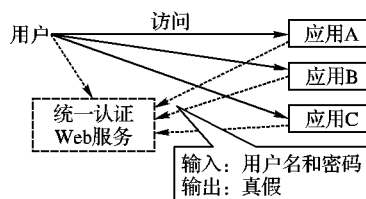


图4 以应用为主的认证方式

4) 用户独立的实现方式。

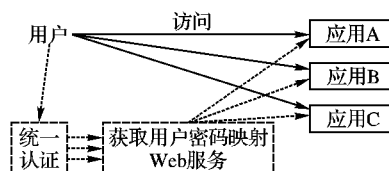


图5 用户独立的认证方式

优点:以统一认证为主,实现了单点登录和用户映射,这种方式分工比较明确,思路比较清晰,为以后给各个应用系统的简单授权提供了方便。

缺点:维护比较困难,涉及到由谁来维护这些信息的问题;同时,数据量相对来说也比较大。

目前已有的大部分系统基本上都有自己独立的认证,也是发展趋势,目前是为了信息的安全考虑。账号关联用于记录已有应用系统的用户账号与统一认证系统用户账号的对应关系。具体的比例是统一认证用户账号比一个具体的应用系统账号 = $N:1 (N \geq 1)$,即统一认证中的一个用户对于特定的一个应用系统来说必须映射为唯一的一个用户,但一个特定的应用系统的用户可以对应于多个统一认证用户账号,甚至是岗位或机构。

账号的映射工作完成后,用户在进行统一身份认证服务之后,用户访问具体的应用系统时自动使用相应的映射账号和密码来获取令牌,并通过该令牌来访问该应用系统,不过这对于任何用户来说,都是透明的。

通过上面的分析可以看出,每一种认证方式都有优缺点,统一认证与授权系统采用用户独立的实现方式,因为其比较规范、标准,能够满足项目最初提出的目标,同时各个应用系统又可以独立地运行。

2.2 统一授权

严格来说,只有统一的认证,没有统一的授权^[2],因为各个应用系统关注的角度、侧面和业务领域不同,很难做出一个比较全面的授权模式。但可以通过标准的规范来完善在授权工作方面的具体实现方式,逐渐达到统一,实现授权模式的最大化重用,至于底层数据库如何实现不需要关心,最终希望通过统一调度和管理来完成授权工作。经过分析目前已有的 20 多个系统的授权功能,总结为几种授权方式^[3-5],如表 1 所示。总共有 $3 \times 4 = 12$ 种授权方式,具体业务系统经常是几种授权模式的组合,如用户的功能点授权和角色的数据范围授权综合使用。比如地震库系统中有相同测线浏览权限,但有的人只能看湛江分公司,有的人可以看其他分公司,在具体分公司下面有人可以下载导航数据,有人可以下载处理成果数据等,这些相当于有相同功能点,但有不同的数据范围,也有不同的数据范围操作权限。如果系统能够明确地将用户分组,或者使用系统的组织有明确的岗位等行政级别分类,一般使用用户组的方式;否则就采用用户的方式,至于角色是带有权限描述信息的一种分类,可以认为是一种特殊的用户组,但已经含有权限的

具体描述。比如系统管理员,不过具体权限还需要与具体功能、及数据范围及操作关联;至于系统的功能点和功能操作就是为了实现系统而提出的功能分类,目的是为了整体设计系统的需要,同时方便用户使用,也为了授权的需要;而数据范围和操作就是与具体的业务系统有关系,各个业务系统的数据范围几乎不同,甚至交叉,所以数据范围及操作是与具体的业务系统紧密相关,授权也是一样的,但授权的类型应该是一样的。表 1 就是各种授权类型的汇总。

表 1 授权类型的汇总

具体授权点	被授权主体对象		
	用户	用户组	角色
功能点	√	√	√
功能操作	√	√	√
数据范围(资源)	√	√	√
数据范围操作(资源操作)	√	√	√

由于在不同的应用系统中具体含义有些区别,本文提出如下解决统一授权方面的解决方案。

1) 认证。由于授权和具体的认证实现方式紧密相关,该系统的认证方式采用用户独立的实现方式。

2) 授权。对于已有的系统,首先按照接口规范来提供相应的数据信息,主要是授权信息和使用 Web 服务实现标准的接口规范;然后按照接口规范提供可编辑的授权功能实现,具体也是按照标准的接口实现具体的授权操作,实现统一调度和统一管理的目标。

3) 授权。对于新开发的系统,希望后台直接按照标准的规范来设计结构,这样接口规范实现就比较统一了,几乎不需要重新开发。

4) 相关信息。统一认证与授权系统中存放的是应用的相关信息,统一认证用户在具体应用中的映射名和加密密码信息,其他的比如授权信息、角色信息来自于各个应用系统。

总结上面几点,各个应用系统具体的授权工作还是由各个应用系统来独立完成,但要求按照规范来设计和实现,目的是为了实现在授权的统一调度和统一管理,以后具体应用系统可以通过统一认证与授权系统进行权限管理,也可以通过自己的授权模块进行管理,但二者必须统一。

2.3 Web 服务技术分析

有了上述解决方案,就需要提供一种支持标准接口规范的协议来实现,采用 Web 服务技术。Web 服务是一套标准,它定义了应用程序如何在 Web 上实现互操作性。可以

用任何语言,在任何平台上写 Web 服务,可以通过 Web 服务标准对这些服务进行查询和访问。Web 服务是将 XML 文本在各个网站之间传送和接受,以达到信息交换的目的。在接受和传送时有一个协议,就是对象访问协议(Simple Object Access Protocol, SOAP),可以通过各种应用层协议来传送,比如 http、ftp 等。

支撑 Web 服务的有 3 大协议^[1]:

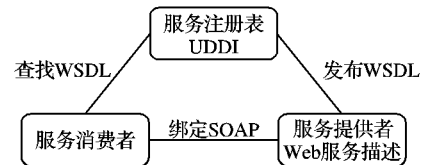


图 6 Web Service 架构

1) SOAP。SOAP 提供了标准的远程调用协助(Remote Procedure Call, RPC)方法来调用 Web 服务。SOAP 规范定义了 SOAP 消息的格式,以及怎样通过超文本传输协议(Hypertext Transfer Protocol, HTTP)协议来使用 SOAP,SOAP 也是基于可扩展标记语言(Extensive Markup Language, XML)和 XML 结构定义(XML Schemas Definition, XSD)的,XML 是 SOAP 的数据编码方式。

2) WSDL。Web 服务描述语言(Web Service Description Language, WSDL)是基于 XML 的描述语言,用于描述 Web 服务及其函数、参数和返回值。因为是基于 XML 的,WSDL 既是机器可阅读的,又是人可阅读的。一些最新的开发工具既能根据 Web 服务生成 WSDL 文档,又能导入 WSDL 文档,生成调用相应 Web 服务的代码。

3) UDDI。统一描述、发现和集成(Universal Description, Discovery, and Integration, UDDI),相当于 Web 服务的一个公共注册表,通俗点说它就是电子商务应用与服务的“网络黄页”,旨在以一种结构化的方式来保存有关各公司及其服务的信息。通过 UDDI,可以发布和发现有关某个公司及其 Web 服务的信息,然后就可以根据这些发布在 UDDI 的信息,通过统一的调用方法来享受这些服务。

2.4 服务接口规范

有了最基本的软件工程底层技术的支持,就需要定义一套规范或标准,这套规范和接口是系统交互的基础,如表 2 所示。下面是部分接口规范说明,目前与具体应用系统相关的有 9 个接口,2 个审计接口没列入表中。

表 2 部分接口规范说明

接口名称	输入参数	输出参数	接口说明
机构岗位和人员树信息	节点 ID	XML 格式的数据集	获取中心所有的机构岗位人员树信息
用户或角色在具体应用下的功能树	用户登录名或角色 ID, 节点 ID, 操作类型	XML 格式的数据集	获取用户在各个应用系统的有效功能树信息
具体应用下的功能树	用户登录名或角色 ID 或用户组 ID, 节点 ID, 操作类型	XML 格式的数据集	获取各个应用系统的功能树信息(包含用户或角色在各自功能点的权限信息)
具体应用下的功能点和数据范围权限的分配	用户名或角色 ID 或用户组 ID, 授权字符串, 操作类型	成功与否	完成对各个应用系统中具体功能或数据范围授权
具体应用下的角色(用户、用户组)树	用户名或角色 ID 或用户组 ID, 节点 ID, 操作类型	XML 格式的数据集	获取各个应用系统角色树信息(包含用户所属的角色信息或角色包含的用户信息)
具体应用下的用户树	节点 ID	XML 格式的数据集	获取各个应用系统账号树信息
具体应用下的用户的操作审计接口	用户名	XML 格式的数据集	获取各个应用系统下该用户的操作日志信息

