基于4A技术的统一身份管理在企业门户系统中的应用

单晓毅，王鑫彦
（北京医药集团有限责任公司，北京 100078）

摘 要:通过对企业门户、4A（帐号、认证、授权、审计）在功能和原理方面的阐述，介绍了以4A技术为基础的统一身份管理在企业门户系统中的实现方法及所起的重要作用，最后对目前两种技术融合的优缺点进行了比较和总结。

关键词：4A；企业门户；统一身份管理
中图分类号：TP393.07 文献标识码：A

Unified identity management application in enterprise portal systems based on 4A technology

SHAN Xiao Yi, WANG Xin Yan
(Beijing Pharmaceutical Group Co, Ltd., Beijing 100078, China)

Abstract:By the description of functions and principle to enterprise portal and 4A(account, authentication, authorization, audit), this article introduces the implementation method and important role of unified identity management in enterprise portal systems based on 4A technology, and at the end compares and summarizes the advantages and shortages to integration of the two technologies.

Key words: 4A; enterprise portal; unified identity management

经过多年来的信息技术建设，各企业单位IT自动化程度有了很大提高，已经建成了或者正在建设着多种应用系统。随着业务的增长，市场竞争的加剧，如何将各个业务系统相对独立的用户管理和分散的应用系统内容整合于同一页面管理下，以及提高低效的新业务系统接入能力，就成为IT部门急需解决的问题。

企业门户是企业信息化前进的必然战略性方向，据美林公司的调查显示，企业对门户的需求正日益增长，在接受调查的50家全球百强企业CIO中，有32%的人反映在开支优先权方面，2008年已让位于企业门户。Gartner发布的数据显示，2008年门户软件市场增长了59%，相比之下，同期企业软件投资的增长幅度仅为4.3%。Meta Group统计，2008年把门户作为核心系统的公司将从2007年的不足10%增加到35%左右。

概括地说，企业门户就是通过一个唯一入口，为企业员工、分销商、代理商、供应商、合作伙伴等同一价值链上的相关人员提供个性化的信息、知识、服务与应用。它是一种基于Web的，将不同应用、业务过程、后端系统、服务和信息、知识等内容集成到一个个性化窗口中的功能强大的软件系统平台[1]。

连接多种应用系统为不同角色的用户提供快捷服务的门户系统，其核心的基础就是用户身份的管控，包括用户身份管理、角色和权限管理、网络行为管控、统一用户信息管理这几个部分，即通常所说的4A：统一用户帐号（Account）管理、统一认证（Authentication）管理、统一授权（Authorization）管理和统一安全审计（Audit）四要素。

1 企业安全门户系统设计

企业安全门户系统的设计包含3个重要的步骤，即明确技术原理、定义功能和设定体系架构。

1.1 技术原理

门户技术原理结构图如图1所示。门户服务主要用来提供来自Web应用的内容，它允许用户可以在浏览器中查看一张或一套页面中显示的多种信息来源（通

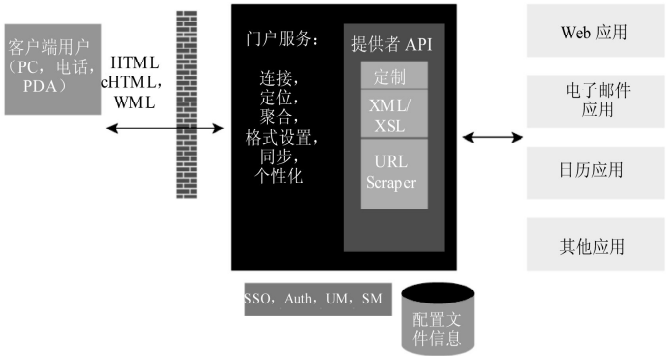

图 1 门户技术原理

常是 Web 应用）。包含内容的页面被称作桌面，在桌面的各个区域出现的各种内容来源被称作频道[2]。

在门户中，一个被称作提供者的部件负责将文件中的内容或 Web 应用的输出，转换成一种适合频道的格式。可以用内容提供者 API 为门户开发内容提供者，并且门户内应带有多种预置的专门提供者，向客户端设备提供内容的标记语言是超文本标记语言(HTML)、用于移动电话和 PDA 的 HTML (cHTML)、无线标记语言(WML)或可扩展标记语言(XML)等语言中的一种或多种。身份认证、授权、用户管理以及用户配置文件信息的存储，都是通过标识和策略 API 来完成的。这些 API 一般都实现于目录服务之上[2]。

门户聚合来自不同数据源的信息，这些来源可以是从企业内外或从垂直或专业门户聚合而来的，提供页面布局和创建可定制的图形化用户界面(GUI)所需的元素。负责为聚合转换和提供内容的组件被称作提供者。

1.2 定义功能

对于产生于各种来源的信息，门户提供一个访问点，为最终用户和他们使用的 Web 应用及服务带来了多种功能，这些功能包括聚合、展现、自定义和安全。

门户必须让企业内外的最终用户和应用都能进行安全访问。为了实现这个目标，它必须带来支持企业现有身份认证机制的灵活性，提供单点登录功能并且利用标识和策略组件，为其所有用户和应用提供单点登录、身份认证、授权、访问控制和会话管理。

此外，门户应提供以下可选功能：

(1)提供虚拟专用网(VPN)解决方案，以便在设备中除了 Web 浏览器外，不再需要装有任何专用客户端软件用户下访问企业内部网资源。

(2)带有一个重写 HTML 文档的反向代理，从而允许在不将企业内部网 Web 站点直接暴露给因特网的情况下，对所有这些站点进行访问。

1.3 体系架构

一般来说，企业门户主要分为 3 层，即 Web 服务平台、统一认证平台和聚集展现平台其体系架构图如图 2 所示。

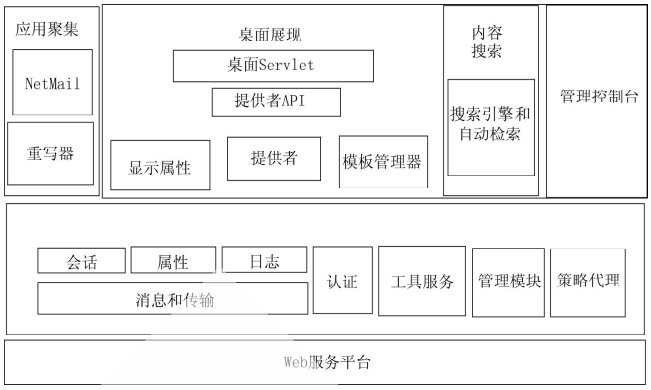

图 2 企业门户体系架构图

企业门户的 Web 服务平台是上层服务的容器，提供基于 Web 服务的容器和上层应用与模块的运行环境。

统一认证平台通过 4A 技术实现为用户提供跨系统访问的单一认证服务和管理功能。统一认证平台在系统设计中，与企业门户系统展现层的业务逻辑相对独立，其目的是为企业建立起完整的单点登录支撑平台。将用户认证功能与企业门户系统展现平台相分离，是充分考虑用户的使用习惯以及未来的系统扩展。用户在访问企业应用系统时，可以首先通过企业门户系统的认证授权功能，获取访问其他应用系统的权限，实现单点登录；同时，用户也可以通过直接访问特定应用系统，由统一认证平台对用户进行认证，授予用户跨系统访问的权限。

聚集展现平台主要处理用户访问企业门户系统的访问安全控制管理、策略管理及内容、应用聚集的功能，通常含有应用聚集、桌面展现和内容搜索三大功能。同时，企业门户系统展示层将负责支撑用户使用不同访问设备的内容格式提交，通过企业门户系统的渠道功能，将企业内部信息资源个极具性化地呈现给访问用户。

2 4A 原理和统一身份管理

门户系统中的 4A 技术，为整个系统的安全性提供了完善的平台保障。

最初的 4A 技术核心是单点登录（Single Sign-On），随着各企业不断开展电子商务和将内部资源不同程度地向客户、合作伙伴及员工开放，对于企业至关重要的信息财产安全越发显得重视，尤其是在信息访问越发便捷的背景下，这些资产也暴露在越来越多的威胁中。毫无疑问，信息保护的私密性、完整性、真实性和可靠性的需求日益突出，系统和安全管理人员需要对企业内部的用户和各种资源进行集中管理、集中权限分配、集中审计，从技术上保证支撑系统安全策略的实施，即，构建信息级的企业安全必须解决用户的帐号（Account）管理、认证（Authentication）管理、授权(Authorization)管理和安全审计(Audit)方面的问题，即 4A 解决方案[3]。

帐号管理即是将自然人与其拥有的所有系统帐号

的关联进行集中管理，包括按照密码策略自动更改密码、4 不同系统间的帐号同步等。一般帐号管理的实体部件通常采用目录服务器，基于“属性：值”对和层级树状逻辑组织的用户帐号数据，更加适合轻量目录访问协议（LDAP）的处理。

认证管理用以实现支撑系统对操作者身份的合法性检查。对信息系统中的各种服务和应用来说，身份认证是一个基本的安全考虑，只有通过系统预设规则的身份认证，才能够接触系统功能和应用系统的数据。

授权管理是指对用户使用支撑系统资源的具体情况进行合理分配的技术，实现不同用户对系统不同部分资源的访问按安全和数据敏感级别定义系统内部资源的访问权限。

审计管理是指收集、记录用户对支撑系统资源的使用情况，以便于统计用户对网络资源的访问情况，并且在出现安全事故时，可以追踪原因，追究相关人员的责任，以减少由于内部计算机用户滥用网络资源造成的安全危害。

3 企业门户系统中的统一身份管理应用

下面以基于 J2EE 体系的门户和统一身份管理服务为例加以说明。

统一身份管理流程如图 3 所示，统一身份管理平台与企业门户服务紧密集成，提供统一认证、统一授权、访问控制、单点登录和行为审计 5 大功能，完成访问者与门户之间的登录和资源列表返回、信息资源访问请求和用户身份传递等前后台的身份识别和信息访问过程。统一身份管理平台一般包含访问管理器和身份管理器两个逻辑部分。

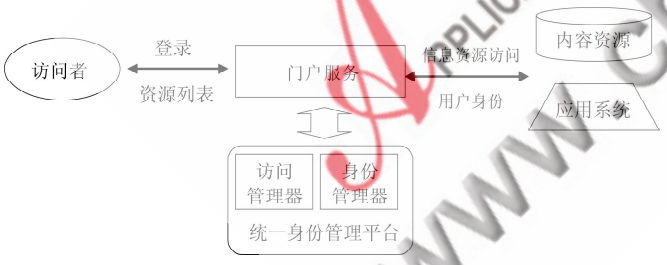

图 3 统一身份管理流程

(1) 访问管理器和身份管理器

访问管理器为门户服务提供了针对 Web 服务器、J2EE 应用服务器、Web 代理服务器以及典型企业应用的多个策略代理 (Policy Agent)；另外，它还提供了访问管理器 SDK，用以集成企业的 Java 或 C/C++ 应用，实现集中认证、授权和单点登录[4]。

用户管理与信息同步系统由身份管理器实现，对各应用或子网络系统用户帐号的集中管理，包括用户帐号在其相对应的应用系统里的自动创建及创建的规则，帐号生成的审批流程管理，帐号的禁用和销毁，帐号在各个应用系统之间的对应关系及同步，口令的管理，提供统一的管理界面和分级授权管理，帐号的审计和风险分析等。身份管理器也是一个标准的 J2EE 应用系统，它通过部署于其本身服务器端（而不是要管理的应用系统一端）的资源适配器创建和管理在各个应用系统上的用户帐号。

(2) 统一认证

访问管理器提供了公共的认证服务架构，具有灵活的认证方式和多种认证服务接口。因此，基于统一的认证服务的应用系统间可以实现单点登录。

访问管理器提供的认证服务基于 JAAS（Java 认证与授权服务）框架，提供 Java 和 XML/HTTP 两种应用认证接口。

(3) 认证方式定制化接口

不同的认证方式具有不同的安全性、易用性和部署成本。因此，针对企业门户中不同的用户群与不同的应用范围，需要对认证方式进行定制化。在访问管理器中，可以根据角色、用户、服务指定不同的认证方式，也可以在认证时直接指定认证模块。对于不同组织、角色和服务，可以配置个性化的认证选项。

访问管理器为应用程序提供两种类型的认证编程接口。对基于 Java 的应用系统（包括基于 JSP 的 WEB 应用系统和基于 Java 的应用程序）可以使用 Java 编程接口；对于非 Java 的应用系统，可以使用 XML/HTTP 编程接口或 C/C++编程接口。

(4) 单点登录支持

单点登录的根本原理是保持用户的会话（session）状态。访问管理器对单点登录提供的 SDK 级别的支持，其中包括单点登录令牌的创建与验证。以 Web 应用的单点登录为例：用户通过访问管理器的认证页面进行认证，认证通过之后，平台为该用户创建一个单点登录令牌，并将该令牌的 ID 通过 cookie 返回至用户浏览器；当用户访问 Web 应用系统时，单点登录令牌 ID 自动通过 cookie 传递至 Web 应用系统，Web 应用系统可以通过单点登录令牌 ID 还原单点登录令牌，并向 Access Manager 验证单点登录令牌是否有效。如果有效，则应用系统可以从单点登录令牌获取用户身份信息，而不再需要用户进行再次认证。对于 C/S 结构的应用，单点登录过程类似，只是单点登录令牌 ID 的传递方式不同。

综上，基于 4A 技术的统一身份管理为企业门户服务带来较为全面的安全保障，从人员、访问、授权和审计等角度保护企业内部应用的数据的合法使用，具有如下优点：

(1)统一认证、授权和审计，管理维护工作复杂度大幅度降低，减少维护操作带来的故障隐患；

(2)统一监管，企业系统安全状况随时被自动监管；

(3)免去用户在各系统间切换时需要再次输入用户名和口令的繁琐操作，减少帐号密码泄露机会；

(4)对各个系统进行统一的访问审计，利于综合分

析，及时发现入侵行为。

但从技术实现方式和用户使用效果上看，基于4A的统一身份管理也存在着一定的不足，具体表现为：

(1)技术实现方式限制较多，例如基于策略代理的SSO，对门户系统产品提出固定要求，对特定产品的版本、未提供开放接口的系统缺乏灵活的处理方法。

(2)合规审计能力一般不强，多数产品只提供以日志为主的审计能力，以及基于日志的数据传输接口由第三方模块完成审计报告。

相信，随着企业门户对安全管控需求的不断细化，随着各厂家产品和技术的发展，4A技术对企业门户安全的贡献将越来越突出。

参考文献

[1] 邓宇,宋成林.企业门户技术及在企业管理信息系统中的应用[C].2004全国电力行业信息化年会,2004.

[2] Sun Microsystems Inc. Sun ONE Architecture Guide- Delivering Services on Demand, 2003.

[3] CMCC. 中国移动业务支撑网运营管理系统规范v2.0, 2008.

[4] Sun Microsystems Inc. Web services security. Identity Management and Liberty, 2008.

(收稿日期：2009-03-29)