SMG 数字化网络新闻共享平台统一用户认证与授权的实现

李泽强 杨君蔚 陈子建 (上海文广新闻传媒集团技术运营中心信息技术部 200041)
吴德柱 谭晟中 (微软(中国)有限公司上海分公司 200030)

摘要:本文简要介绍了 SMG 数字化网络新闻共享平台统一用户认证与授权平台的设计思路和思想、结构、组成部分和总体框架,并对组成统一认证平台的三个核心部分用户身份管理框架、单点登录框架和统一应用授权框架的关键技术进行了详细描述,最后以 C/S 应用系统为例介绍了其接入统一认证平台的方法和流程实现。

关键词:用户身份管理 单点登录 统一应用授权 活动目录

1 概述

随着 SMG(上海文广新闻传媒集团)信息化建设的推进,目前集团的信息化环境中已经建设了众多的应用系统并投入日常的节目制作和办公使用,这些应用系统已经成为集团的重要组成部分。

由于系统比较多,这些系统又相对独立,大多数系统都有自成一体的用户管理、授权及认证系统,同一用户在进入不同的应用系统时都需要使用属于该系统的不同账号去访问不同的应用系统,这种操作方式对用户来说非常不方便,需要通过每个应用系统各自的入口来进入,重复登录不同的应用系统,不仅降低了工作效率,而且不利于系统安全;同时对管理员来说需要协助用户在多套应用系统中维护用户的登录信息,繁琐而且易出错。

结合集团新闻资源整合的应用需求,规划建立一套统一用户认证与授权平台。

2 统一认证平台结构、接口及组成部分

统一认证与授权平台基于 XML/SOAP/LDAP 技术,建立一套完整的用户身份管理、身份验证、用户授权机制,为集团新建的文稿、非线性编辑、媒资、办公管理等应用系统提供标准的身份认证服务和接口,使其它即将新建的系统也能够顺畅的无缝接入平台,实现单点登录和用户的集中管理。统一认证与授权平台结构如下图1所示。

(1) 用户在访问接入应用系统时,由统一认证与授权平台提供用户认证;

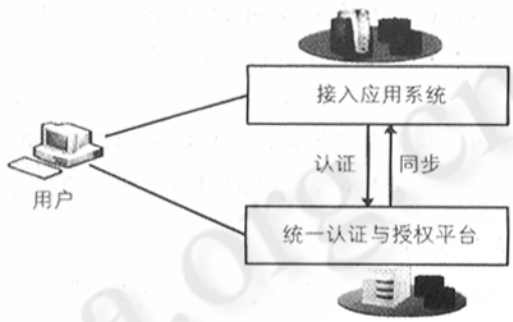

图 1 平台结构示意图

(2) 统一认证与授权平台的用户身份信息将同步到接入应用系统;

统一认证与授权平台组成及接口见图2。

3 SMG 统一认证平台系统总体架构和关键技术介绍

SMG 数字化网络新闻共享平台统一认证与授权平台采用了微软的活动目录和 MIIS2003 (Microsoft Identity Integration Server) 身份集成技术。其核心是单点登录和授权的实现。

3.1 用户身份管理框架

该框架集成了各种核心身份管理功能,使企业能够更轻松地定义和维护用户身份统一管理和各个系统

的信息同步。基于 MIIS2003 架构的用户身份管理框架逻辑设计如图 3 所示。

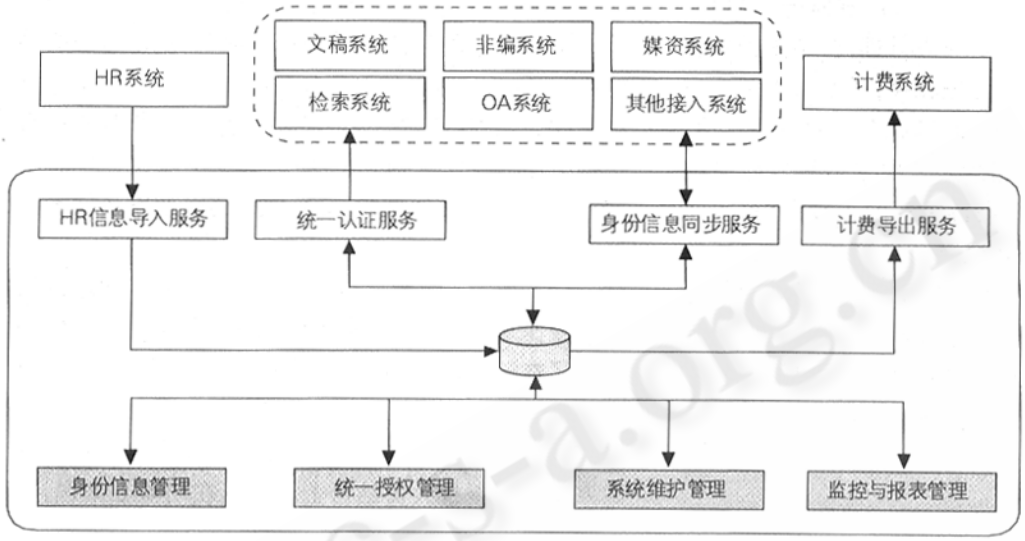

图 2　系统定义及接口示意图

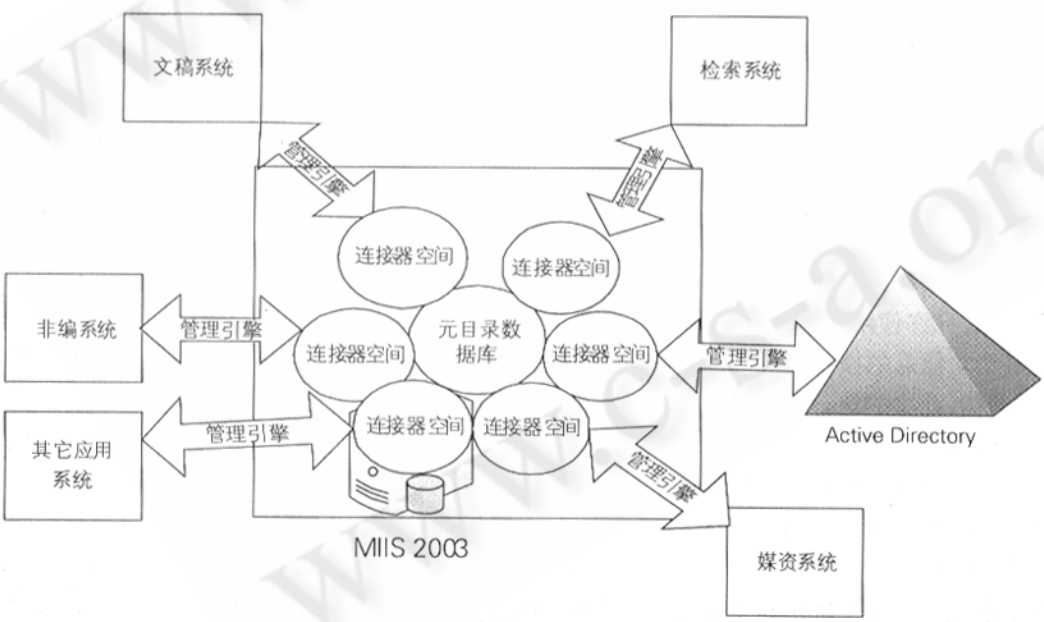

图 3　基于 MIIS2003 架构的用户身份管理框架逻辑设计图

MIIS 2003 的架构体系的功能：

(1) 存放集中的来自各个应用系统的身份信息，形成一个全局的整合的所有对象的视图。

(2) 可以从各种授权来源抽取用户信息，如人力资源和新闻系统、电子邮件目录以及 Web 服务器注册数据库。

(3) 可以进行元目录数据库向其他身份信息数据库进行双向的同步或者单向的同步。

(4) 提供了整合的用户管理工具，例如可以查看用户身份信息同步历史信息。

(5) 可以非常灵活地设置属性映射规则等，并且还有对整体身份密码修改管理的管理平台实现密码重置、同步等。

3.2 用户单点登录框架

单点登录是一个集成的机制使得用户通过一次登录即可访问多个不同的应用。一旦用户在统一认证平台中认证成功，无需额外的认证过程就可访问平台上所集成的其他应用系统或者后端系统资源。

单点登录技术的本质在于面向企业内部用户提供局域网内部及跨网络边界的用户凭据 (Credential) 存储，映射，检索，传输及相关的管理和配置服务。

实现企业单点登录的技术有许多不同的方式。从技术架构上来说，有统一用户凭据登录和用户应用凭据自动登录等；从认证方式上来说，有基于目录服务认证和基于数据库认证等方式。SMG 统一认证平台选用了统一用户凭据登录和基于目录服务的认证方式。

统一的用户凭据进行登录的流程如下图 4 所示。

3.3 统一应用授权框架

统一授权管理是一个支撑平台，它以统一用户、组织机构部门和组等数据信息为基础，面向多种类型应用系统提供统一的权限管理和授权管理，为各个应用系统提供授权服务。同时为了更有效的实现管理，还需要设置有效的授权管理。它要求能够做到系统的集中授权，能够对系统进行统一的管理；而且为了能够减轻管理工作的工作强度和提高用户的工作的效率，要求本系统能够采用把权限下放，以方便与专人管专事；为了提高本系统的精确性和灵活性；而且具有更高的可伸缩性、灵活性更大并且更易于实现。可以定义角色以及这些角色可以执行的任务、操作。可以嵌套角色以继承其他角色的特征，并且可以定义应用程序组。

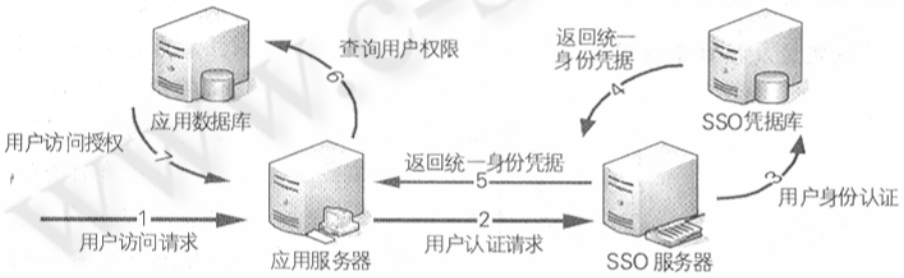

图 4　统一的用户凭据进行登录的流程图

在项目实施的本阶段，统一授权管理的目标是实现用户对各个应用系统是否允许使用的控制，不需要完成对每个应用系统，每个功能点的授权管理。但是考虑到平台未来的发展趋势，此次的统一授权管理应该支持平滑升级到对每个应用功能的授权管理。

因此，从可扩展性的角度考虑，在使用 Windows 2003 中的 Authorization Manager 进行开发时，仍然要合理使用一些正确的设计理念。

(1) 应用程序。授权系统中为每个应用建立了自己的一套数据结构，它包括有多项属性数据：名称(是具体应用系统的名称)、描述(具体引用在通用授权系统中的具体信息描述)、版本、允许权限委派及安全权限管理。在应用程序中，用户可以创建自己所需要的操作、任务、角色。

(2) 角色。角色是通用授权信息中的中间层，它从属于应用程序。它是系统中功能的集合，它与功能之间的对应关系可以随意调整(在自授权允许的情况下)；它也是系统中授权对象(人员、机构部门、组)的集合，在其中的对象享有该角色所对应的功能。用户可以更具自己的需要来调整角色数量、角色与功能的对应关系、角色人员的对应关系。

(3) 规则。Authorization Manager 任务对象具有根据附加的与任务相关的 脚本来动态限定在任务中授予的权限的附加功能，这可以使访问控制决策考虑运行时数据。

(4) 操作。预留此概念，但本阶段不对其进行处理。操作是授权系统中最基础的数据信息。它具体的体现了在一个应用(或栏目或单独授权的文件)中有哪些具体的细节功能项。这些功能是和具体的应用的程序绑定在一起的，它通过与角色的结合才能更好的与系统中的授权人员结合上。所以在功能上来说，要求是越细越好。

(5) 任务。预留此概念，但本阶段不对其进行处理。任务是从属于应用程序的，这里的任务包括了两部分操作的集合以及任务的嵌套。同时在任务这个级别可以定义授权脚本，执行动态授权检测。这样对于静态授权不能满足需要的情况，应用程序可以用变量和对象引用的形式向 API 接口提供额外的上下文。这使脚本编写者可以使用 JScript 或 VBScript 添加业务逻辑，而无需更改和重新编译应用程序。

(6) 关系。应用——操作——任务——角色——人员。

(7) 通用授权系统以 AD 中机构人员信息数据和应用授权系统数据为基础，向应用层提供应用系统中各种不同的授权管理查询信息数据。

(8) 提供的方式可以采用多种。XmlHttp 获取、WebService 提供服务、基本访问接口程序和高级编程接口。

4 统一认证平台认证授权的实现及流程描述

统一认证平台主要为集团已有或即将建设应用系

统提供一个基础平台，通过该平台来实现用户的集中管理和授权管理，方便用户操作，避免以前各应用系统相对独立，用户访问任一应用系统都要输入一次用户名和密码的现象，统一认证平台实施后，用户用自己的帐号在任意一台能访问集团内部网络的计算机上登录以后，就具有了访问属于自己应用系统的权限，这就是本文所说的单点登录。

由于统一认证平台是为其它应用系统提供的一个基础平台，而目前企业中的应用系统主要分为 C/S 和 B/S 模式两大类，所以根据不同模式的接入应用系统，统一认证与授权平台的认证授权流程可以分为：C/S 模式认证授权和 B/S 模式认证授权，这两种模式的授权实现方式基本上相同，而 B/S 模式应用在企业中越来越多，所以本文以 B/S 模式的授权为例，简要介绍其授权的实现及流程。

4.1 技术实现

统一认证与授权平台通过使用 UserToken 和 ApplicationToken 实现单点登录的功能。UserToken 和 ApplicationToken 均为临时的身份凭证。其中，UserToken 由统一认证与授权平台生成并颁发给用户，作为统一认证与授权平台赋予用户的临时身份凭证，其中包含了用户的详细登录信息；ApplicationToken 由接入应用系统根据统一认证与授权平台提供的信息生成并颁发给用户，作为接入应用系统赋予用户的临时身份凭证，其中包含了用户的登录信息和在该接入应用系统上的授权信息。

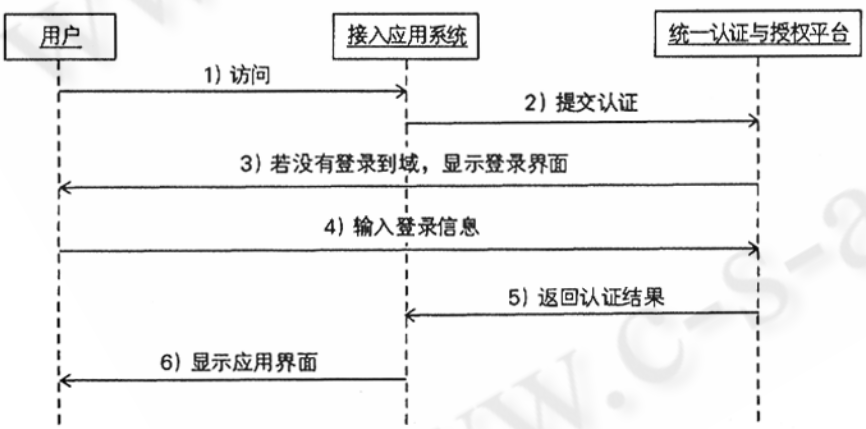

图 5 首次认证流程示意图

当用户登录到统一认证与授权平台的网站后，统一认证与授权平台根据用户信息生成并颁发 UserToken。当用户访问某个接入应用系统时，该接入应用系统如果不能辨别用户的身份，则通过重定向技术向统一认证与授权平台提交身份验证请求，统一认证与授权平台判断用户拥有合法的 UserToken，则将相关信息返回给接入应用系统，接入应用系统生成并向用户颁发 ApplicationToken。当用户再次访问该接入应用系统时，接入应用系统通过判断用户是否拥有 ApplicationToken，即可自行决定用户是否有权限使用此应用。

4.2 认证的有效期

ApplicationToken 是一个临时的身份凭证，具有有效期属性，超过指定的时间后，ApplicationToken 不再有效。此时接入应用系统需要在用户下一次访问其系统时再次向统一认证与授权平台发出认证请求并根据认证结果生成新的 ApplicationToken。

同样，UserToken 也是一个临时的身份凭证，具有有效期属性，当超过指定的时间后，UserToken 不再有效。统一认证与授权平台需要再次验证用户的身份，以生成并颁发新的 UserToken。

5 总结

因此，在新闻共享平台上建立统一认证与授权体系，可以很好地实现：

统一身份信息、统一身份认证、统一应用授权及统一开发接口规范。

参考文献

1 Windows2003Server 网络管理手册，李劲编，中国青年出版社。

2 怎样用微软 IIS 实现身份认证管理详解，Jeffrey Juday 2005－8－7，出处：赛迪网。

3 Should Microsoft Identity Integration Server Be Part of Your Security Plan，作者 Deb Shinder 2005 11－12 出处：微软网站 。

4 组建微软 MIIS 身份认证的模拟网络环境，2005－9－16 出处：赛迪网。

5 基于身份和访问平台的应用开发，2005－9－15，出处：download. microsoft. com.