**[信息系统开发平台OpenExpressApp － 用户权限模块设计](http://www.cnblogs.com/zhoujg/archive/2009/12/12/1622331.html)**

       管理型软件不同于工具型软件，它涉及到多人协同操作，所以用户权限管理是必备的功能之一。本篇讲介绍一下OpenExpressApp的用户权限模块的大体应用思路，后续将会实现为框架的内置提供模块。

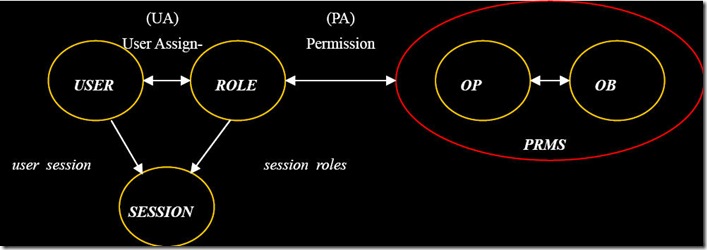
     现在很多系统都是采用RBAC（Role-based\_access\_control）来作为权限系统的设计参考，OpenExpressApp也准备参考它来设计权限子系统，所以下面我先简单介绍一下RBAC的内容，如果熟悉的可以略过这一小节。

[**Core RBAC**](http://en.wikipedia.org/wiki/Role-based_access_control)

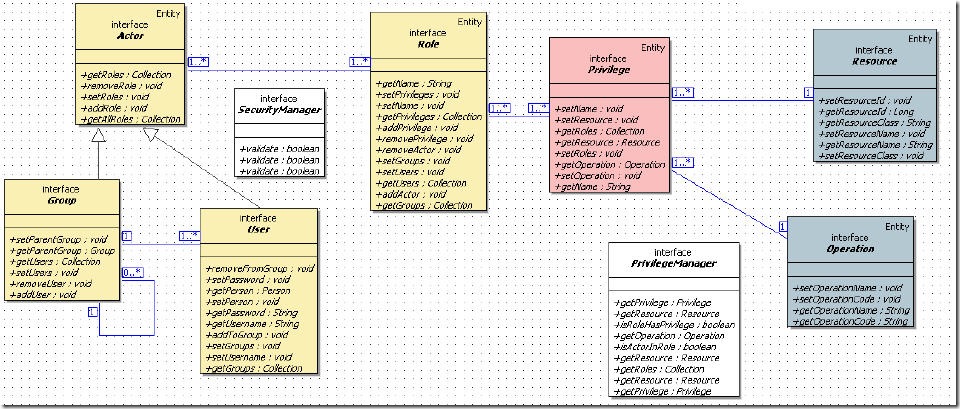
     IT业界在2000年基于Ravi Sandhu等人提出Role-based抽象模型基础上形成了RBAC模型标准草案，这个草案实质是建立一套基于角色授权的模型标准

。RBAC标准包括两部分：RBAC参考模型和RBAC功能描述。RBAC参考模型定义了RBAC的基本语义和基本元素集合，并通过集合论给出了一套RBAC数学模型，RBAC功能描述定义了RBAC系统必须的特性。

     下面为RBAC的核心参考模型示意图：对象主体（OBS）和操作主体（OPS）的许可权限（Permission）直接赋予角色（Role），用户（User）通过与Role的关系实现权限的授予，具体介绍可以参考[an\_introduction\_to\_rbac](http://u.download.csdn.net/source/947614)。

[](http://images.cnblogs.com/cnblogs_com/zhoujg/WindowsLiveWriter/OpenExpressApp_EFCF/Core%20RBAC_2.jpg)

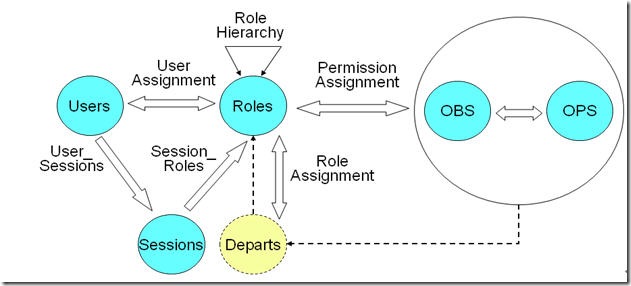
**RBAC实现参考**

[](http://images.cnblogs.com/cnblogs_com/zhoujg/WindowsLiveWriter/OpenExpressApp_EFCF/RBAC%E5%AE%9E%E7%8E%B0.jpg)

参见[an\_introduction\_to\_rbac](http://u.download.csdn.net/source/947614)

**组织机构相关的RBAC模型的变体**

      在企业级应用时除了角色外，组织机构仍然是一个十分重要的维度，如何将角色与组织机构连接起来，是我们着重考虑的问题。因此结合组织机构和RBAC模型，衍生了与组织机构相关的RBAC模型的变体，如下图所示：**部门＋岗位＝角色**：岗位不能直接授权，只有与部门挂接后才能形成角色

[](http://images.cnblogs.com/cnblogs_com/zhoujg/WindowsLiveWriter/OpenExpressApp_EFCF/Core%20RBAC%202_2.jpg)

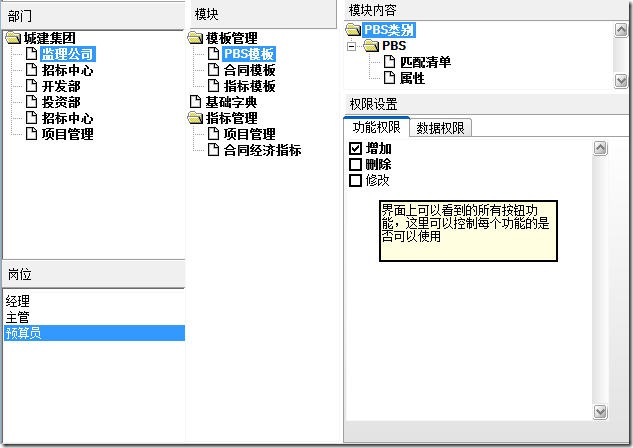
**模块设计**

**部门管理（组织机构）**

[](http://images.cnblogs.com/cnblogs_com/zhoujg/WindowsLiveWriter/OpenExpressApp_EFCF/%E9%83%A8%E9%97%A8%E7%AE%A1%E7%90%86.jpg)

       组织机构是企业的管理体系，企业的所有经营行为都要通过组织机构发挥作用。岗位只有处于特定的组织下才能发挥作用，此时形成角色。组织机构中节点成为部门，部门下挂接岗位，岗位与具体人员相关。

**权限设置**

[](http://images.cnblogs.com/cnblogs_com/zhoujg/WindowsLiveWriter/OpenExpressApp_EFCF/%E6%9D%83%E9%99%90%E8%AE%BE%E7%BD%AE.jpg)

      该模块只有系统管理员（包括部门级系统管理员）可以操作，设置部门＋岗位下的各个模块的**功能权限**和**数据权限**

**功能权限**：显示模块类别下的所有[Command](http://www.cnblogs.com/zhoujg/archive/2009/11/16/1603826.html)，控制到所有界面可以看到的工具条按钮和右键菜单

**数据权限**：数据权限包含整个模块是否允许查看（模块打开功能）、单条记录是否允许访问（记录查看权限）和记录属性可见（字段级别权限）。这块还没有想得很清楚，目前先控制数据记录级别的权限，指定可以查看到哪些记录。

注：目前不考虑上下级隶属关系、权限下发等等复杂组织机构功能

更多内容：[***开源信息系统开发平台之OpenExpressApp框架.pdf***](http://www.docin.com/p-44561376.html)