基于 SSO 的统一用户管理服务平台的设计与实现

马同宽

（河北新天绿色能源股份有限公司，河北　石家庄　050000）

摘要：由于企业各应用服务平台都拥有独立的用户认证、权限管理体制，用户在来回切换登录不同平台时浪费大量时间，亟需设计并实现基于 SSO 的统一用户管理服务平台。该平台是四层、可扩展的 B/S 框架结构，引入 SSO 设计统一身份认证模块，基于智能合约设计统一访问控制模块，采用时钟同步方式设计数据同步模块。最后通过对平台的全面测试，验证了本文设计统一用户管理服务平台的可行性与可靠性。

关键词：SSO；统一用户管理；服务平台；平台设计

中图分类号：TP39　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2023.08.031

随着信息技术的迅猛发展，我国各企业根据自身业务需要逐步建设出各种各样的应用服务平台，然而每一个平台均有着相对独立的用户管理体制，缺乏统一的用户管理标准。当管理员进行企业所有平台的全生命周期管理工作时，则需要分别使用相应的账号、密码登录各个平台，不仅容易造成账号滞留、账号混乱等问题，而且难以确保企业数据资源的一致性，对企业信息管理效率与安全有着非常不利的影响。因此，在企业运营发展进程中，如何将分散的应用服务平台进行集中、统一的管理，消除各平台之间的用户信息孤岛，对提升企业账号的信息化管理水平至关重要。时至今日，用户管理的统一化已经成为我国企业信息化管理研究中的一项热点课题，在企业的可持续发展以及网络化建设中发挥着越来越重要的作用。

1 统一用户管理服务平台的架构设计

平台的架构设计是统一用户管理服务平台开发的核心内容，本文基于 B/S 架构设计一个多层、可扩展的平台框架结构[1]。

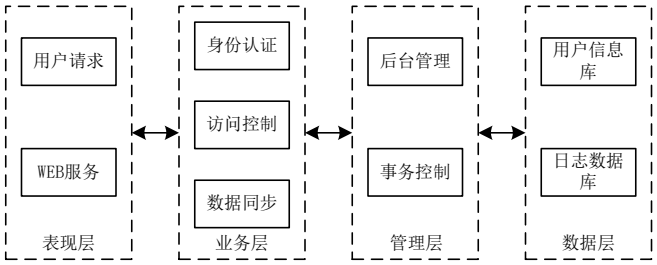

图 1　统一用户管理服务平台架构图

本文所设计的统一用户管理服务平台主要包括四层体系结构。其中表现层是该平台关键的对外服务层，所有想访问平台的用户都必须通过表现层发出访问、登录请求，执行登录操作；业务层主要负责为整个平台提供业务逻辑，当用户通过表现层进入统一用户管理服务平台后，经过身份认证即可获得平台列表权限，进而实现各平台的单点登录以及数据同步等功能；管理层主要负责对平台最底层数据进行处理，不仅可以对用户进行添加、删除、修改等操作，而且可以维护各独立平台的逻辑修改、删除等；数据层是该平台的最底层，主要负责存储平台的一些核心数据，如用户信息、操作日志数据等，而且数据层可以为整个平台提供数据服务[2]。

2 统一用户管理服务平台的功能实现

2.1 统一身份认证模块

身份认证也可以称为用户身份鉴别，就是当用户访问统一用户管理服务平台时，需要向平台提供自身身份证明，只有平台确认身份真实后，才能让用户登录平台[3]。一般情况下，我国各平台与系统主要使用用户名和密码的认证方式，但是每次用户使用这种认证方式登录平台时，需要多次输入口令与密码，不仅不利于企业多平台的管理效率，而这种各平台都拥有单独的资源库，会导致资源浪费。所以，本文引入单点登录技术（SSO）来设计统一身份认证模块。SSO 就是用户在服务平台中只需进行一次身份认证，即可实现各授权子平台的统一登录，不仅可以提升企业平台管理效率，而且可以避免资源浪费。本文结合统一用户管理服务平台的实际使用环境，设计如下图所示的基于经纪人的单点登录模型。

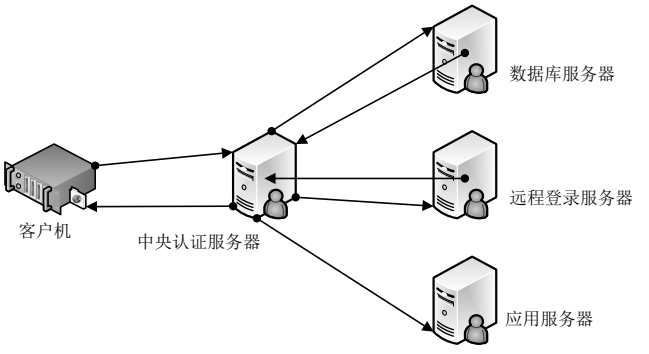

图 2　统一用户管理服务平台 SSO 模型图

如图所示，在本文所设计的 SSO 模型中，经纪人会为平台用户提供一个电子凭证，且拥有一个统一的数据库，在用户登录平台时，会将数据统一存储至数据库中。那么，用户通过 SSO 登录平台的具体流程如下：首先用户通过远程登录服务器进行单点登录，此时应用服务器会对用户凭据进行检查；如果数据库中存在用户凭据，那么直接于单点登录数据库中进行检索，检索成功后向用户呈现子平台。反之，如果数据库中不存在用户凭据，服务器会重新定向至相应的登录表单，并要求用户提供子平台凭据，检查无误后，存储至单点登录数据库中，再向用户呈现子平台。在单点登录模块实施过程中，平台于数据库中检索登录凭据的环节，相对于用户是透明的。

2.2 统一访问控制模块

访问控制模块是确保统一用户管理服务平台数据安全的关键[4]。在该平台中，由于每个子平台均是独立的个体，且每一个平台的访问权限与其属性之间存在一定关联，所以本文针对统一用户管理服务平台的实际情况，设计一种基于智能合约的统一访问控制模型，主要由 PEP、AA、PAP、PDP 以及 PIP 这几个重要部分构成。详细来说，就是当 PEP 收到用户的访问请求之后，平台会调用 PIP 对相关属性信息进行查询，并建立一个描述了主体、属性等内容的访问请求。此时，PEP 就会将该请求封装成请求事务，验证其合法性之后，分别调用 PDP、PAP 与 PIP 来获取属性信息，对访问请求进行判定，最后将判定结果返回至 PEP。至此，实现统一用户的访问控制。那么在本文所设计的统一访问控制模块中，主要采用智能合约作为代理，在智能合约提供属性服务期间，因为企业子平台节点数量较多，严重影响智能合约的使用效率，所以本文通过布隆过滤器配合智能合约，为平台提供查询与判定服务。假设存在一个集合 $X=\{x_1,x_2,\cdots,x_n\}$，且 i 位二进制向量为 $E=\{e_0,e_1,\cdots,e_{i-1}\}$，此时将 E 中所有位的初始值归零后，让 X 中的 x_m 满足下式则可得到布隆过滤器：

$$E\left[h_j\left(x_m\right)\right]=1 \tag{1}$$

式中，h_j 表示相互独立的哈希函数 $H=\{h_1,h_2,\cdots,h_j\}$ 中元素。由于在统一用户管理服务平台中需要进行访问控制的子平台数量是不断增加的，所以本文通过布隆过滤器配合智能合约的模式，来提升平台属性资源的查询效率，保障统一访问控制模块的稳定运行。

2.3 数据同步模块

在本文所设计的统一用户管理服务平台中，数据同步模块担负着整理子平台数据并同步至平台数据库中的重任，由于本文设计平台是点对点的组网方式，因此采用时钟同步模式来设计数据同步模块。针对平台时间的精密同步要求，本文引入了精密时钟协议来解决平台数据同步的实时性问题[5]。在精密时钟协议中，每一个子平台节点以标记时间戳的形式进行高精度的数据同步。由于本文设计统一用户管理服务平台使用的通信网络传输速率较快，为避免交换机为数据同步带来一定的延时，在进行数据同步时，需要综合考虑不同时钟之间的偏差 μ，以及报文传输延时 τ。那么，基于时钟同步模式的数据同步过程图 3。

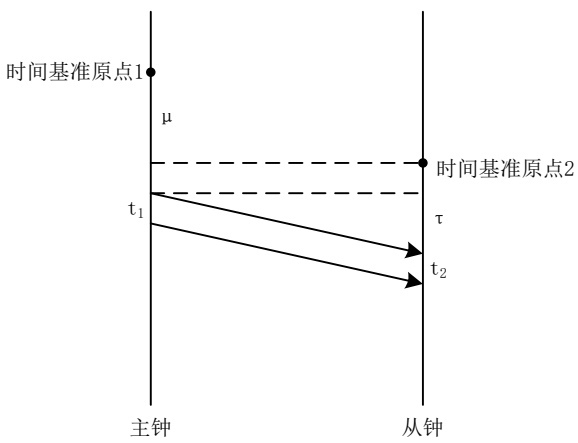

图 3　数据同步过程

在统一用户管理服务平台数据同步过程中，考虑到时钟的对应关系，存在：

$$t_1-\mu=t_2-\tau \tag{2}$$

式中，t_1、t_2 分别表示报文传输时间。在数据同步过程中，时钟偏差 μ 需要根据实际情况进行测算，而报文传输时延可以根据下式所示的乒乓算法来获得：

$$\tau=\frac{t_1+t_2}{2} \tag{3}$$

由此可知，在本文所设计统一用户管理服务平台的数据同步模块上，主要基于精密时钟协议来实现报文的同步传输，最后将响应数据同步到平台数据库内。

3 平台测试

测试就是在平台运行过程中，检验其功能与性能是否满足设计需求。本章主要针对统一用户管理服务平台的各个功能点是否实现、平台 Bug 数量与缺陷率是否在可控范围内这两个层面进行测试，首先将平台与数据库分别部署在两台操作系统一致的服务器上，其硬件配置如表 1。

表 1　统一用户管理服务平台测试环境

配置	平台服务器	数据库服务器
用途	统一用户管理服务平台	Oracle数据库
操作系统	Win10	Win10
参数	CPU：i7、内存：16G	CPU：i5、内存：8G

在此基础上，通过 IE 浏览器访问本文设计的统一用户管理

服务平台，按照表 2 所示的测试用例对平台功能进行进一步测试。

表 2　统一用户管理服务平台测试用例表

序号	测试用例描述	测试过程	预期结果	确认结果（YES/NO）
1	用户管理	选择用户	显示用户列表	YES
		分别点击账号添加、修改、删除按钮	显示添加/修改/删除账号页面	YES
		填写表单信息并保存	提示“保存成功”	YES
		输入用户信息查询	显示该用户信息/显示“该用户不存在”	YES
2	流程管理	点击进入流程管理页面	显示流程表单页面	YES
		设置“添加步骤”信息，包括步骤ID、名称、操作人员等	显示“添加”后的界面	YES
		输入配置后的流程信息进行查询	显示该流程信息	YES
3	权限管理	进入权限管理界面，选择权限分配选项	显示权限管理菜单页面	YES
		选择菜单资源，点击添加/删除角色	显示添加后/删除后的页面	YES
		选择角色名称，进行角色分配	返回角色列表	YES

在本次测试过程中，为确保平台测试结果具有可信性，本文针对每个功能模块分别进行了多次重复测试。如表中结果所示，本文设计的统一用户管理服务平台的各个功能模块具有完整性与联通性，可以满足企业实际业务需求。然后本文将在虚拟机中搭建一个模拟测试环境，采用 LoadRunner 工具来测试统一用户管理服务平台运行性能，测试结果如图 4。

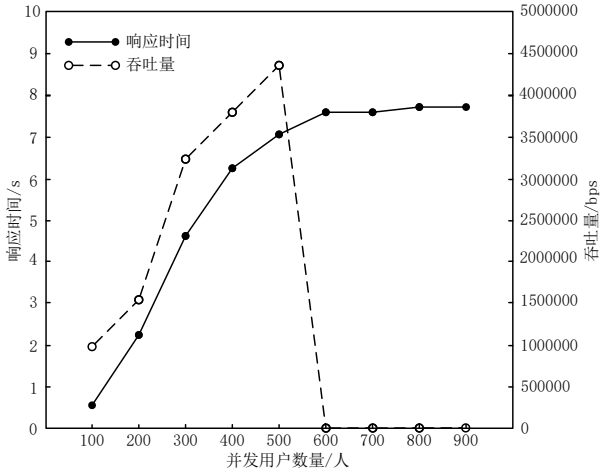

图 4　统一用户管理服务平台性能测试结果

从图中测试结果可以看出，随着平台并发用户数量的不断增加，平台响应时间缩短，每秒吞吐量也相应提升，但是当 600 个用户同时在线操作时，平台响应时间开始呈现较为稳定的状态，且吞吐量骤降至零点，且持续保持吞吐为 0 的状态，说明此时平台处理事务的错误率不再增加。由此可以说明，本文设计的统一用户管理服务平台整体性能表现良好，可以在多用户、多并发的情况下稳定运行，满足预期设计需求。

4 结语

综上所述，本文设计并实现了基于 SSO 的统一用户管理服务平台，在 B/S 架构的基础上，完成统一身份认证模块、统一访问控制模块以及数据同步模块的研发，并通过测试结果，验证了该平台在功能上与性能上基本可以满足设计需求。统一用户管理服务平台可以将企业不同应用服务平台的账号资源数据进行整合与同步，从而解决企业账号分散的难题。该平台操作页面简单易懂，不仅便于管理员对企业各用户信息进行运维管理，而且可以有效提升账号信息全生命周期的管理效率。

参考文献：

[1]李姝熹，李潼，王建祥.论智慧城市框架下的档案管理服务平台建设[J].档案管理，2021，(01)：53-54.

[2]吴君楠，欧洋，李琰.基于 LAMP 的高性能计算用户组织架构管理系统设计与实现[J].计算机工程与科学，2021，43(02)：235-241.

[3]李睿智，刘念，延肖何.基于势博弈的综合能源系统用户能量管理优化方法[J].电力科学与技术学报，2021，36(01)：21-31.

[4]邹容容，杨晨.Launcher 管理发布系统设计[J].电视技术，2022，46(01)：126-128，135.

[5]王羿.基于大数据的监管平台统一运维管理系统设计[J].电视技术，2022，46(02)：97-100.

作者简介：马同宽（1993-），男，河北石家庄人，硕士研究生，中级工程师，主要从事软件设计研究。