SSO（Single Sign On）_百度百科

当用户第一次访问应用系统1的时候，因为还没有登录，会被引导到认证系统中进行登录；根据用户提供的登录信息，认证系统进行身份校验，如果通过校验，应该返回给用户一个认证的凭据 - - ticket；用户再访问别的应用的时候就会将这个ticket带上，作为自己认证的凭据，应用系统接受到请求之后会把ticket送到认证系统进行校验，检查ticket的合法性。如果通过校验，用户就可以在不用再次登录的情况下访问应用系统2和应用系统3了。
要实现SSO，需要以下主要的功能：

系统共享

统一的认证系统是SSO的前提之一。认证系统的主要功能是将用户的登录信息和用户信息库相比较，对用户进行登录认证；认证成功后，认证系统应该生成统一的认证标志（ticket），返还给用户。另外，认证系统还应该对ticket进行校验，判断其有效性。

信息识别

要实现SSO的功能，让用户只登录一次，就必须让应用系统能够识别已经登录过的用户。应用系统应该能对ticket进行识别和提取，通过与认证系统的通讯，能自动判断当前用户是否登录过，从而完成单点登录的功能。
另外：
1、单一的用户信息数据库并不是必须的，有许多系统不能将所有的用户信息都集中存储，应该允许用户信息放置在不同的存储中，事实上，只要统一认证系统，统一ticket的产生和校验，无论用户信息存储在什么地方，都能实现单点登录。
2、统一的认证系统并不是说只有单个的认证服务器
当用户在访问应用系统1时，由第一个认证服务器进行认证后，得到由此服务器产生的ticket。当他访问应用系统2的时候，认证服务器2能够识别此ticket是由第一个服务器产生的，通过认证服务器之间标准的通讯协议（例如SAML）来交换认证信息，仍然能够完成SSO的功能。
用户在访问页面1的时候进行了登录，但是客户端的每个请求都是单独的连接，当客户再次访问页面2的时候，如何才能告诉Web服务器，客户刚才已经登录过了呢？浏览器和服务器之间有约定：通过使用cookie技术来维护应用的状态。Cookie是可以被Web服务器设置的字符串，并且可以保存在浏览器中。当浏览器访问了页面1时，web服务器设置了一个cookie，并将这个cookie和页面1一起返回给浏览器，浏览器接到cookie之后，就会保存起来，在它访问页面2的时候会把这个cookie也带上，Web服务器接到请求时也能读出cookie的值，根据cookie值的内容就可以判断和恢复一些用户的信息状态。Web-SSO完全可以利用Cookie技

术来完成用户登录信息的保存，将浏览器中的Cookie和上文中的Ticket结合起来，完成SSO的功能。

为了完成一个简单的SSO的功能，需要两个部分的合作：

1、统一的身份认证服务。

2、修改Web应用，使得每个应用都通过这个统一的认证服务来进行身份校验。

很多的网站都有用到SSO技术，

新浪的用户登录也是用到的SSO技术.

实现SSO的技术主要有：

(1）基于cookies实现，需要注意如下几点：如果是基于两个域名之间传递sessionid的方法可能在windows中成立，在unix&linux中可能会出现问题;可以基于数据库实现；在安全性方面可能会作更多的考虑。另外，关于跨域问题，虽然cookies本身不跨域，但可以利用它实现跨域的SSO。

(2) Broker-based（基于经纪人），例如Kerberos等；这种技术的特点就是，有一个集中的认证和用户帐号管理的服务器。经纪人给被用于进一步请求的电子的身份存取。中央数据库的使用减少了管理的代价，并为认证提供一个公共和独立的"第三方"。例如Kerberos,Sesame,IBM KryptoKnight（凭证库思想)等。Kerberos是由麻省理工大学发明的安全认证服务，当前版本V5，已经被UNIX和Windows作为默认的安全认证服务集成进操作系统。

(3) Agent-based（基于代理人）在这种解决方案中，有一个自动地为不同的应用程序认证用户身份的代理程序。这个代理程序需要设计有不同的功能。比如，它可以使用口令表或加密密钥来自动地将认证的负担从用户移开。代理人被放在服务器上面，在服务器的认证系统和客户端认证方法之间充当一个"翻译"。例如SSH等。

(4) Token-based，例如SecurID,WebID，现在被广泛使用的口令认证，比如FTP,邮件服务器的登录认证，这是一种简单易用的方式，实现一个口令在多种应用当中使用。

(5) 基于网关Agent and Broker-based，这里不作介绍。

(6) 基于安全断言标记语言（SAML）实现，SAML(Security Assertion Markup Language，安全断言标记语言）的出现大大简化了SSO，并被OASIS批准为SSO的执行标准。开源组织OpenSAML 实现了 SAML 规范。

CAS由耶鲁大学开发的单点登录系统（SSO,single sign-on），应用广泛，具有独立于平台的，易于理解，支持代理功能。

SSO Sun-synchronous orbit太阳同步轨道的英文缩写

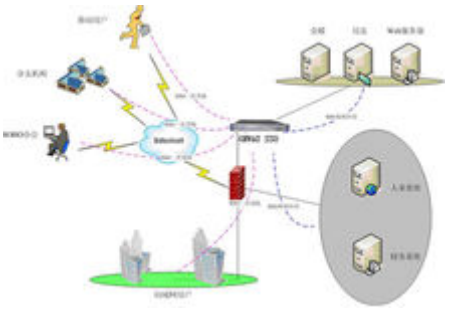
SSO Ship Security Officer船舶保安员的英文缩写

SSO Schedule of System Operation 系统运作时间表（常用于机电工程的前期规划设计）

技术实现

以金万维单点登录为例：如图所示：统一的身份认证系统主要功能是将用户的登录信息和用户信息库相比较，判断其有效性。整个系统可以存在两个以上的认证服务器，这些服务器甚至可以是不同的产品。认证服务器之间要通过标准的通讯协议，互相交换认证信息，就能完成更高级别的单点登录。

应用优势



单点登录：用户只需登录一次，即可通过单点登录系统（eTrueSSO）访问后台的多个 应用系统，二次登陆时无需重新输入用户名和密码

C/S单点登录解决方案：无需修改任何现有的应用系统服务端和客户端即可实现C/S单点登录系统

即装即用：通过简单的配置，无须用户修改任何现有B/S、C/S应用系统即可使用

应用灵活性：内嵌金万维动态域名解析系统（gnHost），可独立实施，也可结合金万维异速联/天联产品使用

基于角色访问控制：根据用户的角色和URL实现访问控制功能

全面的日志审计：精确地记录用户的日志，可按日期、地址、用户、资源等信息对日志进行查询、统计和分析

集群：通过集群功能，实现多台服务器之间的动态负载均衡

传输加密：支持多种对称和非对称加密算法，保证用户信息在传输过程中不被窃取和篡改

可扩展性：对后续的业务系统扩充和扩展有良好的兼容性[1]

应用缺点

1）不利于重构

因为涉及到的系统很多，要重构必须要兼容所有的系统，可能很耗时

2）无人看守桌面

因为只需要登录一次，所有的授权的应用系统都可以访问，可能导致一些很重要的信息泄露。[2]

存在问题

某某集团公司坐落于兰州，在西藏、北京、上海等地拥有多个分子公司，并在全国各大城市

设有办事处，随着业务的快速发展与壮大，集团公司已经意识到信息化是实现企业终极目标的重要手段，自2000年开始，公司先后实施了ERP、BPM、HR、EIP、企业邮局、腾讯通平台、OA、财务等[3] 多套管理系统，实现公司各项业务流程及管理流程的信息化、自动化。然而，随着业务数量的不断增加，各系统之间互不兼容造成的信息共享性差、需要记忆多套密码、客户端维护成本高等问题日益凸显，一些花巨资购买并实施数月的系统运用效果远不如预期理想。

为了确保业务的高效运行与管理的高效执行，企业急需优化信息化方案：

第一， 如何实现公司各种业务流程及信息资源的全面整合？

第二， 如何简化各种信息系统的使用方式，降低使用成本？

第三， 如何降低信息系统维护与管理成本？

解决方案

实现资源整合：

为了解决第一个问题，即实现各信息系统之间的全面整合，集团公司引进了企业信息门户(EIP)，即将各种应用系统(诸如ERP、BPM、HR、OA、企业邮局等)、数据资源和互联网资源统一集到企业信息门户之下,根据每个用户使用特点和角色的不同,形成个性化的应用界面，并通过对事件和消息的处理、传输把用户有机地联系在一起。

简化系统应用：

在实施EIP的过程中，集团公司使用单点登录eTureSSO解决用户需要记录多个系统账号的问题，用户只需要在第一次访问信息系统时，输入用户名与密码，以后再访问同一个系统资源时，无需再次输入，由单点登录系统自动登录。

降低信息维护成本：

(E-SoonLink)实现C/S分布式软件的集中式部署，将管理系统服务器端与客户端统一部署在客户服务器中心，任何授权客户机都能够以WEB形式访问，并更新数据，轻松实现了系统在广域网中的局域网应用。集团在实施异速联系统之后，无需在每个用户客户机安装每套信息系统的客户端软件，因此对客户机硬件配置要求降低，另外，无需对每个客户机进行安装配置和维护，大大减少了安装维护的工作量，降低了用户数量日益增长所产生的信息化成本。[4]

在交换设备中表示基于状态的切换与不停顿转发一起使用(NSF/SSO)[5] ，它具有如下特点：

1. Active/Standby主控板运行在同步模式
2. 冗余的MSFC处于hot-standby模式
3. 交换机处理器同步二层端口的状态信息
4. PFCs同步L2/L3的FIB转发信息库，Netflow和ACL访问控制表

Learn how to enable nonstop forwarding with stateful switchover (NSF/SSO).Config SSO

first

Router> enable

Router# configure terminal

Router(config)# redundancy

Router(config-red)# mode sso

Router(config-red)# end

Router# show redundancy states

Multicast MLS on by default

enable in routing process

router(config)#router ospf 120

router(config-router)nsf

e.g.:NSF/SSO: MPLS VPN[3]

Cisco Catalyst 4500 E-Series High Availability[4]

NSF/SSO: L2VPN Pseudowire Redundancy[6]

简单说，你可以设置一个HA备份节点，在主SSO失效时接管SSO功能。这种方式需要占用更多服务器资源，但需要的基础设施资源已经很便宜，特别是虚拟化之后。VMware演示了如何使用免费的Apache软件创建基本的SSO服务器负载平衡组。要搭建一套带负载平衡的SSO基础设施，需要对证书和负载平衡技术有足够的了解。

假定正在使用虚拟化基础架构，任何承载SSO服务器站点虚拟机的物理主机出现故障，SSO站点虚拟机都会通过HA机制从备份节点重新启动，从而接管SSO功能。当然，这并不能修复配置错误。如果要应对配置错误的情形，快照非常有用，即使你因为配置失误而把SSO弄丢了，你也可以很容易回滚快照进行恢复。只要你能决定，这种投入肯定是值得的。但可惜，即使是一些我曾经工作过的大型组织都没有采用这类措施。如果有正常运行的HA系统，确实没有必要。

如果需要运行多个站点并期望实现单一管理体系，方法会略有区别。多站点安装过程需要在SSO安装选项下拉，选择多站点。从本质上说，使用多站点模式意味着在多主控模式下为每个站点设置了自己单独的主节点。区别是，当您设置多站点模式时，你需要一个SSO服务器将这些站点链接到一起。

这种安装模式的一个潜在问题是，不同站点彼此之间将不会复制数据库。在实际案例中，对于大多数站点，数据库复制并不重要。数据库偶尔会需要复制，但是只要你选择外部独立的身份验证系统进行身份验证，如OpenLDAP或微软AD，就几乎不会有这种复制需要。[7]

参考资料