

一种OMS系统门户集成方案的设计与实现

为满足南方电网OS2一体化电网运行智能系统建设要求，实现OMS系统与外部系统的横向互联，通过分析对比各种常见SSO实现方案的优缺点，结合实际应用需要，设计一套面向OMS系统的门户集成方案。该方案对旧系统的改造量小，运维便捷，能够方便地与新建系统对接集成，同时能保证系统的安全性和可靠性，给电网系统用户的日常工作带来极大便利，实际应用效果良好。

罗黎明¹ 葛艺晓¹ 陈章国¹ 苏扬² 邓大为² 温柏坚^{2/1} 1.南京南瑞集团公司 2.广东电网有限责任公司电力调度控制中心

0 引言

OMS系统，又称电网运行管理系统，旨在提高电网公司调度控制中心的工作效率，减轻调度运行人员的工作负担，减小电网运行的不确定性风险。为了满足南方电网OS2一体化电网运行智能系统建设要求，OMS系统需要与其他系统（OCS、6+1系统）横向互联，各系统之间需要跨域单点登录。

单点登录（Single Sign-On），简称SSO，即用户在访问多种受限资源时，只需进行一次身份校验和登录，即可在一定时期内多次免登录访问资源，从而提高工作效率和安全性。OMS系统中单点登录多应用在业务流程中，出于电网运行安全考虑，提供的资源访问权限只限定于与触发请求工作流相关的特定页面，OMS系统在一次单点登录访问过程中，应避免免登期内对全流程的访问权限。本文主要研究在符合电网安全运行前提下，OMS系统如何实现与其他系统的跨域单点登录。

1 一般SSO的实现

实现单点登录关键在于统一的身份校验方法以及身份信息的跨域流转。评价SSO系统主要考虑其可实施性、可管理性、可扩展性和安全性。可实施性指SSO系统的复杂性以及现有系统如何有效的集成SSO功能；可管理性指系统运行过程中，对SSO运行状态的监测以及出现异常行为后的消缺；可扩展性指针对新建系统的单点登录要求能否快速适应；安全性指估量系统在运行中是否易受攻击。

表1列出各种方案，各有优缺点，但都是比较粗略的指导思想，没有给出可行的实施方案，而且结合南方电网OS2一体化电网运行智能系统建设要求，这些方案也无法适应OMS系统的实际运行环境，因此单独运用某一种方案无法设计出一个适用于OMS系统的可行的SSO方案。

2 OMS系统环境下的SSO设计方案

为OMS系统（电网运行管理系统）设计了单点登录系统，按照南方电网OS2一体化电网运行智能系统建设要求，集成与OMS横向互联的几个外部系统，包括电网运行控制系统（OCS）、安全生产管理系统（PMS）、通信管控系统等，用户从浏览器登录一次即可以同样的身份登录其他系统，允许权限范围内的OMS用户通过单点登录进入对接系统指定页面，同时允许权限范围内的对接系统用户通过单点登录进入OMS系统指定页面，查阅指定的数据范围。



罗黎明/高级工程师

关键词/Keywords

单点登录 ·
OMS系统 ·
身份认证 ·
OSB总线 ·
OS2架构 ·

表1 对比几种主要SSO实现方案的特点

一般SSO	可实施性	可管理性	可扩展性	安全性
Broker-based	改造旧系统的工作量大	集中式的管理是主要优点	认证服务器的故障将影响所有用户	依赖于实施的过程
Agent-based	移植容易，但需设计和实现与原有应用程序交互的接口	增加了管理难度	取决于被代理服务器的使用便捷性	使用密码技术的实现的代理程序的通信安全
Token-based	需要增加新的组件	增加了管理的负担	需要额外的硬件和软件	增加了系统的安全性
Agent&Broker-based	比Broker-based方案对旧系统的改造工作量小	比Broker-based方案更易于管理	认证服务器的故障将影响所有用户	代理软件需要增加安全和本地验证的功能
Gateway-based	安装和设置网关很方便	比Broker-based方案更易于管理。但多个网关时，多个用户数据库的同步比较难实现	网关的状态会影响到整个系统的服务运行	易被攻击，应用分开的防火墙保护网关

2.1 方案目标与技术前提

实现OMS系统与对接系统之间双向单点登录方案，关键数据采用MD5加密，技术上遵循OSB总线技术规范。对接系统联调前需确保开通双方服务器对应端口的访问权限。

对接系统双方用户数据共享是实现单点登录的前提，南方电网主数据资源平台中的人力资源数据可作为统一的用户数据源。

2.2 功能设计

单点集成方案业务流程图如图1所示。

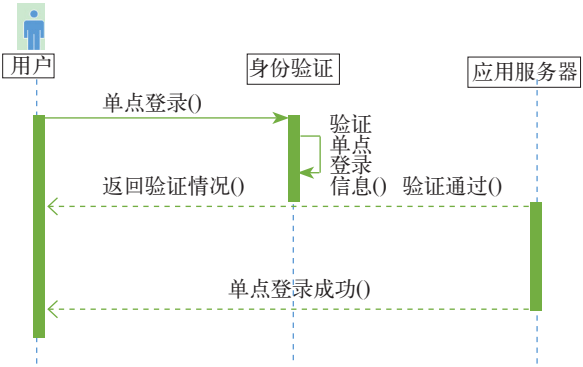


图1 单点集成方案业务流程图

2.3 设计思想

用户通过点击集成系统的单点集成菜单项，将访问请求转发到“本地单点集成服务”，“本地单点集成服务”根据约定规则，封装“单点集成认证信息”，对附带认证信息的单点登录地址发起登

录请求。

被集成系统接受到单点登录请求后，按照约定规则，解析并校验获取的认证信息，如果校验通过，证明是有效登录方式，向集成系统提供访问权限，如图2所示。

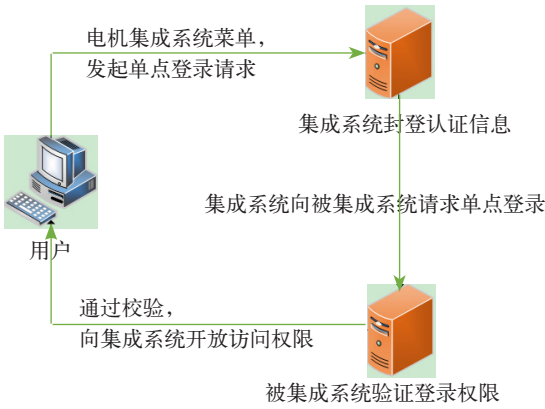


图2 单点登录单向交互实例

2.4 身份验证

以OMS系统作集成系统为例。

在OMS系统中单点登录外部系统，在相关位置配置单点登录菜单项，点击菜单项发起单点登录请求，菜单地址应分别包含集成系统与被集成系统的处理单点登录请求的“单点集成服务地址”，菜单地址如下：

“SSOClientServlet?url=SSOServerServlet”

1) 【SSOClientServlet】：集成系统“单点集

成服务地址”（客户端）。

2) 【SSOServerServlet】：被集成系统“单点集成服务地址”（服务端）。

其中，“SSOClientServlet”和“SSOServerServlet”的地址应包含IP、端口号等，格式如：“http://ip:port/context/”。

OMS系统本地“单点集成服务”接收到服务请求后，系统封装目标单点登录请求URL，发起访问，目标单点登录地址如下：

“SSOServerServlet? ack=MD5密文&userid=人资唯一标识&logintime=登录时间& syscodeID=对接系统编码&businessURL=业务参数”

(1) URL参数说明

单点登录请求URL参数说明如表2所示。

表2 单点登录请求URL参数说明

参数名	参数涵义
ack	MD5加密验证串
userid	人资唯一标识
logintime	登录时间
syscodeID	对接系统编码
businessURL	业务参数

【ack】：由“人资唯一标识”、“登录时间”和“单点集成口令”用冒号【：】组合而成，经过MD5加密，形成加密串：

1) “人资唯一标识”：系统根据获取的发起单点登录请求的用户名称，在南方电网主数据资源平台中的人力资源数据中查找相应的人资台账唯一标识。

2) “登录时间”：系统自动获取从“1970-01-01 00: 00: 00”到当前的毫秒数。

3) “单点集成口令”：此参数为对接系统双方事先约定，命名规则为交互双方系统名称首拼，以“广东中调OMS与通信管控系统”交互为例，单点集成口令为：GDZHOMSTXGK。

【userid】：人资唯一标识，取自“南方电网主数据资源平台”。

【logintime】：登录时间（“1970-01-01 00:

00: 00”到当前的毫秒数）。

【syscodeID】：对接系统编码，此参数为交互双方事先约定，命名规则为“集成系统名称首拼+集成系统所在局编码”，以“广东中调OMS”为例，系统编码为“GDZHOMS_0300”。

【businessURL】：业务参数，为了满足实际业务需要和对接系统的结构性差异，或有多个参数，每个参数用“|”分隔，参数格式为“=”分隔的键值对，模板如下：

“businessURL=参数1=参数值|参数2=参数值|参数3=参数值”

(2) 验证过程

OMS系统本地“单点集成服务”用Servlet实现，在接收到服务请求后，系统自动获取用户认证信息：人资唯一标识、登录时间、单点集成口令，并用冒号将三者拼接成字符串，通过MD5加密算法，形成密文，作为单点登录参数之一【ack】，同时将“人资唯一标识【userid】”、“登录时间【logintime】”、“对接系统编码【syscodeID】”、“业务参数【businessURL】”和【ack】一并封装进目标单点登录请求URL，请求访问。

被集成系统“单点集成服务”利用Servlet实现，接收到OMS系统的单点登录访问请求后，解析出【ack】、【userid】、【logintime】、【syscodeID】和【businessURL】的参数值，其中“人资唯一标识”和“登录时间”与“单点集成口令”，按照客户端相同的方式，拼接后使用MD5处理成密文，对比解析出的【ack】中的值，如果完全匹配，则在“南方电网主数据资源平台”中验证【userid】有效性，验证通过则视此次单点登录成功，通过Ajax回调函数返回单点登录成功信息，如果验证不通过，通过Ajax回调函数返回“异常响应编码”。

单点登录身份流程如图3所示。

3 性能分析

评价SSO系统主要考虑其可实施性、可管理性、可扩展性和安全性。本方案基于J2EE架构，是一种轻量级的解决方案，统一了单点登录

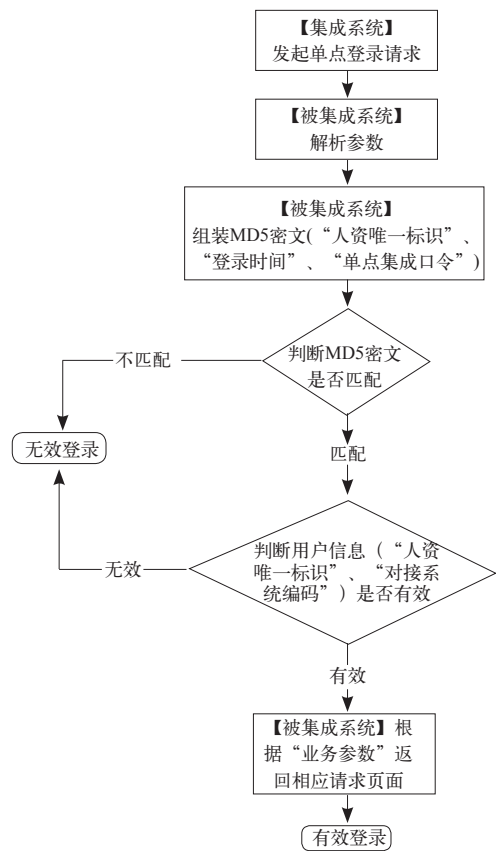


图3 单点登录身份验证流程

客户端到服务端的用户认证信息访问标准，统一了验证信息加密的传输和识别标准，为全网（电力系统III区网络）提供了统一的单点登录框架。主要优点如下：①服务端使用Servlet，适用于所有主流平台，方便集成；②设计了统一的“异常响应编码”，运行过程中的任何异常可快速定位并消缺；③设计了可扩展的“业务参数【businessURL】”，对新建系统的集成提供了可行性；④身份验证过程中关键参数使用MD5加密，保证了数据的完整性和安全性；⑤使用时间戳“登录时间【logintime】”与“单点集成口令”共同解决了重传攻击的问题；⑥网络传输中无用户密码信息，只包含对接系统共享的“南方电网主数据资源平台”人资数据的唯一标识，可以防止密码恶意捕获；⑦由于OMS系统和其他对接系统均运行在电力系统III区（生产管理区）网络，使用时间戳做安全时间服务是可行的，同时该网络环境也一定程度上遏制了重传攻击。

本方案在实际运用当中，还存在一些局限

性，如无法保证访问请求按照请求的顺序到达被集成系统服务端，但是由于实际情况下，单点登录的访问实际间隔时间较长且请求不频繁，保证了这种方法的可行性。本方案的不妥之处需要进一步完善。

4 结束语

随着门户集成的需要以及Web技术的不断发展，电网公司电网运行管理的信息化水平愈高，设计出一个面向OMS系统的单点登录方案有其现实意义和迫切需要。本方案实现了在电力系统III区（生产管理区）网络下OMS系统与外部互联系统的门户集成，保证了用户在多个系统之间流转操作的便捷性，同时保证了应用系统的安全性和稳定性，对提高用户的工作效率，提升用户操作满意度有着深远的意义。

参考文献

[1] 毛捍东. 一个基于Web服务的单点登录系统[J]. 计算机工程与应用, 2004(24).

[2] 林满山. 单点登录技术的现状及发展[J]. 计算机应用, 2004(增刊).

[3] 张挺, 耿继秀. Web环境下的SSO实现模式的研究[J]. 计算机仿真, 2005, 22(8): 129-131.

[4] 刘润达. 一种简单跨域单点登录系统的实现[J]. 计算机应用, 2007, 27(2).

[5] 陈东. 支持多模式应用的分布式SSO系统设计与实现[J]. 计算机应用研究, 2007, 24(4).

[6] Chamberlin N. A brief overview of single sign-on technology[EB/OL]. <http://www.gitec.org/assets/pdfs>, 2000.

[7] 李小平. 基于公开密钥基础设施的单点登录系统的设计[J]. 北京理工大学学报, 2002(2).

作者简介

罗黎明（1980-），男，高级工程师，主要从事电力调度自动化系统研究与开发工作。

陈章国（1979-），男，助理工程师，主要从事电力调度自动化系统研究与开发工作。

（收稿日期：2015-12-10） EA

（编辑：鞠佳）