工程公司统一身份认证平台的规划与建设

宫　成　王鸿捷　吴靖寰　傅贺平

中国石油工程建设有限公司西南分公司，　四川　成都　610041

摘　要：在 PC 机时代，工程公司拥有不同种类、不同范围、不同领域的计算机软件或应用系统，这些系统购置途径不同、生产厂商不同，有着独立的账户密码，同一用户在不同系统的使用过程中，必须记忆不同的账号和密码，造成降低工效的困扰。随着互联网技术的进步，在应用软件与物理硬件之间出现的数据平台层（PAAS 层），为实现统一身份认证、调用授权使用的应用系统提供了可能。针对工程公司常见应用系统的 IT 架构进行了分析，提出一种规划与建设的方法，适用于工程公司 PAAS 层承载不同应用系统的统一身份认证，实现用户在这些系统中一次登录可使用多个系统。统一身份认证平台充分考虑了功能和安全方面的要求，对工程公司的统一身份认证平台建设有一定的积极意义。

关键词：工程公司；统一身份认证；IT 架构；平台层；业务系统

DOI：10. 3969 /j. issn. 1006 - 5539. 2018. 03. 022

The Planning and Construction of Unified Identity Platform for Engineering Company

Gong Cheng, Wang Hongjie, Wu Jinghuan, Fu Heping

China Petroleum Engineering & Construction Corp. Southwest Company, Chengdu, Sichuan, 610041, China

Abstract: In the era of PC, engineering companies have different types and areas of computer software or application systems, which are purchased in different ways and manufacturers. They have their own separate account password. User, while in the use of different systems, must remember different account and password, which results in a lower working efficiency. With the advancement of Internet technology, the data platform layer(PAAS layer), which appears between application software and physical hardware, provides the possibility of application system in implementing unified authentication and calling authorization. The IT architecture of the common application system of the engineering company is analyzed, and a method of planning and construction is put forward. It is applicable to the unified authentication of different application systems carried by the PAAS layer of the engineering company, to achieve the use of multiple systems after login-in by user. The platform fully considers the requirement of function and safety, which has positive significance to the construction of the unified authentication platform of the engineering company.

Keywords: Engineering company; Unified identity authentication; IT architecture; Platform layer; Business system

收稿日期：2017 - 10 - 31

基金项目：中国石油集团工程设计有限责任公司项目“统一身份认证及公共数据库研发”（JCF - 2014 - 36）

作者简介：宫　成（1982 - ），男，辽宁丹东人，工程师，硕士，主要从事信息化建设工作。

0　前言

信息技术的发展及互联网的普及,使企业应用系统已呈快速增长态势。应用系统在企业业务生产及管理等方面发挥着越来越重要的作用,并为各种业态下的企业生产经营模式的改变、企业精细化管理的实现提供基础[1],有效地提高了企业的经营管理水平。

工程公司由于业务和管理的需要,应用系统的建设也在不断增长,由于历史原因,不同时期建立的应用系统所采用的技术不同,当时为解决对应用系统的权限及数据安全的管控,每个应用系统分别部署独立登陆账号和密码[2-4]。但由于应用系统数量的不断增长,导致了众多的问题:

1)用户体验差:用户必须记住不同应用系统的用户名和密码,登录每个应用系统使用时不断重复登录操作。

2)运维管理复杂:业务部门需要对各业务系统的多套用户名及密码进行管理,运维工作量巨大,难以管控。

3)安全隐患严重:用户为记住登录名和密码,采用了简单的密码,造成保密级别降低,为业务数据安全带来极大的隐患。

4)信息不一致:各系统之间的账号不统一,形成信息孤岛现象[5]。

这种分散式的认证方式已经成为企业实现信息系统集成化、一体化所必须解决的问题。本文根据工程公司的实际应用情况提出了一种新的统一身份认证建设思路,能够较好地解决以上问题。

1　规划目标

统一身份认证平台建设应在工程公司自身的信息化建设总体规划下进行,以遵循“统一规划,分步实施”的策略[6],根据工程公司自身的实际需求,明确项目建设目标。统一身份认证平台规划目标应从两方面考虑:

1)所谓统一身份认证就是用户只需通过一个账号密码,就可访问具有合法权限内的所有资源,是统一身份认证平台实现的最基本目标。

2)从整体信息化架构角度考虑,构建一个完整统一、高效稳定、规范安全的集中式身份管理。

2　规划范围

范围决定需求,需求决定架构[7],如果范围不能正确地定义将会导致一系列的不良连锁反应,最终造成系统的严重缺陷。正确、合理的定义范围是保证成功实施的重要工作之一。

笔者认为范围的定义通俗来讲就是为达成目标所必须要做的事情。统一身份认证平台建设范围的确定应以前文提出的规划目标为基础,并根据信息化整体 IT 架构及应用使用情况进行分析、细化的一个过程。工程公司规划统一身份认证平台建设范围可从三方面考虑:

1)制定身份认证标准,建设一个没有重复、冲突的统一身份认证信息架构[8]。

2)兼容企业整体 IT 基础架构和运行环境要求,笔者所在工程公司提出了需兼容企业内部的私有云架构模式。

3)满足已存在的各种异构应用系统的接入及改造,实现各应用系统之间身份认证信息的整合。

3　技术路线选择

如何将工程公司不同的业务应用系统进行有效整合,做到统一认证,统一管理[9-11],是实现统一身份认证平台核心关键。

3.1　统一身份认证标准的建立

统一身份认证标准的建立,应建立在能够满足工程公司各种异构应用架构的基础上,与应用系统本身的开发语言、平台无关,无论是 B /S 结构、C /S 结构以及移动 APP 应用(原生、混合、Web)结构。

统一身份认证标准的建立要充分利用 SOA(面向服务体系)架构松耦合的特点[12-13],采用国际标准的网络协议和规定的一些标准数据格式,包括登录方式、交互流程、认证协议等。

3.2　集中安全管控

统一身份认证平台的集中安全管控必须从全局角度考虑:

1)授权管理:对接入到统一身份认证平台的应用进行授权,为应用系统的接入提供安全、高效、可用的安全机制。

2)审计管理:对应用系统的使用情况、用户对应用系统的访问行为进行审计,可为后续发生事故时提供一个可追查的机制[14]。

3.3　统一身份认证平台与用户信息的关系

统一身份认证平台本身并不对用户信息进行管理,这取决于企业本身对信息管理的划分。从工程公司信息化整体管理角度而言,用户信息一般是由公司人力资源管理部门进行管理[15]。该部分内容的确定,对统一身份认证平台的整体架构设计起着重要的作用。

笔者所在工程公司,采用了基于活动目录进行用户身份验证的解决方案。活动目录中的用户及组织机构信息与“人力资源公共数据管理平台”实现无缝集成,不需要对活动目录中的用户信息单独维护。统一身份认证平台中的用户身份认证直接使用活动目录中的用户信息进行验证。

3.4 统一身份认证与已有应用系统的关系

工程公司必然会对已存在的应用系统进行改造，以适应统一身份认证方式。因此，如何实现让已有应用系统与统一身份认证进行无缝集成是需要解决的另一个问题。建议遵循如下原则和方法解决：

1）统一身份认证平台为各应用系统提供身份认证服务，其他业务系统只需根据其规则调用此服务即可。

2）已有应用系统的身份认证一般与权限控制紧密相连，权限控制是用户通过身份认证后，为用户授权其在应用系统中的角色和使用资源。当前在一个比较完整、规范的企业信息化建设体系中，应由一个统一身份认证供各应用系统使用，权限控制由各应用系统自行管理。

3）针对应用系统改造较多的工程公司，可能存在技术复杂（不同平台）、项目干系人众多（各应用系统的开发商、业务部门、技术人员）等问题。因此，可根据应用系统的使用范围、人数、改造难易程度等进行优先级排序，并在项目实施过程中制定合理的统一规划。

4）明确统一身份认证登录账号与已有应用系统用户信息的共同点，可从用户名、员工编号、邮箱名称等信息进行关联。

在已有应用系统的改造过程中，必然会存在无法改造的应用系统，但针对自研及定制开发类型的软件完全可避免。笔者所在工程公司对自研及定制研发类软件在开发过程中就进行管控，包含对成果文件（需求报告、设计报告、数据字典等）、代码进行审查（编写规范、注释、编译、封装等），以避免此问题发生。

4 建设方案比选

统一身份认证平台建设一般有“产品 + 服务”模式和“定制化开发”模式两种。不管选择哪种开发模式，都需要以正确的、量体裁衣式的解决方案为基础。

4.1 “产品 + 服务”模式

根据调研，“产品 + 服务”模式是当前企业选择较多的一种模式[16-18]。这种模式是软件供应商将产品功能基本固化，再根据个性化需求进行二次开发，这种模式因有一个原型产品的存在，能够快速地满足一个较大应用群体的共性化需求，以及后期的运维服务等。笔者建议，工程公司选择这种商业产品时要注意：前期一定要对产品有充分了解，确切是否能够满足所有需求，包括二次开发是否能够满足工程公司自身的个性需求，因为商业产品在设计架构上基本是固化的，很难改变。

4.2 “定制化开发”模式

“定制化开发”模式是企业建设目标需要什么，软件开发商就生产什么，是一种由无到有的一种模式。这种开发模式与商业化产品对比，具有较强灵活性及适应性，可更好地实现企业建设目标。但同时也带来了不小的挑战，因此需要以工程公司信息化建设部门为主导，掌控整个平台的架构设计，对整体规划及技术有较高的要求。

4.3 两种模式的对比分析

统一身份认证平台建设具体选择哪一种模式，不能一概而论，没有最完美的，只有最适合的。表 1 是针对两种模式的比较，建议工程公司根据自身需求情况并结合表 1 的分析结果，来选择最适当的建设模式。

表 1 “产品 + 服务”与“定制化开发”模式对比分析

建设模式	周期	成本	兼容性	运维 /响应	个性化	技术要求
产品 + 服务	短	较低	一般	慢	一般	较低
定制化开发	长	高	高	快	满足	高

5 实践与应用

笔者所在工程公司按照上述提出的建设思路、方法进行了规划实施，统一身份认证平台建设选用了“定制化开发”模式。

统一身份认证平台自建成后，已无故障运行 28 个月，并有 18 个应用系统接入到统一身份认证平台，其中包括 13 个 B /S 架构应用系统、2 个 C /S 架构应用系统、3 个移动 APP 模式应用系统，用户登录访问总计 869 308 次。该平台的建设有效提升了公司信息化整体管理水平及用户自身的工作效率。

6 结论

本文提出了一种适用于多应用架构模式的统一身份认证建设思路，满足当前所有不同应用架构系统的统一身份认证问题，保证了各业务集成系统的松散耦合。

在工程公司的实际使用也展现了良好的应用效果。用户只需要记住一套用户名 /密码就可以访问所有不同平台、不同语言所开发的应用系统，提升了用户体验和 IT 的运维管理工作。笔者建议，在统一身份认证平台建设过程中，一定采用科学的项目实施方法论为指导，才能较好实现建设目标。

参考文献：

[1] 郭成华. 工程公司企业信息化建设的规划[J]. 天然气与石油，2016，34(2)：78 - 81.
Guo Chenghua. Planning for Engineering Company's Informatization Construction [J]. Natural Gas and Oil, 2016, 34 (2): 78 - 81.

[2] 严 骏. 单点登录和统一用户认证设计与实现[J]. 信息与电脑，2016，(12)：59 - 60.

Yan Jun. Design and Implementation of Single Sign-On and Unified User Authentication [J]. China Computer & Communication, 2016, (12): 59 - 60.

[3] 曹敏年,张　玮,宋雪君. 统一身份认证平台的数据交换机制与实现[J]. 上海理工大学学报,2006,28(3):293 - 298.
Cao Minnian, Zhang Wei, Song Xuejun. Mechanism and Realization of Data Exchanging in the Unified Identity Authentication Platform [J]. Journal of University of Shanghai for Science and Technology, 2006, 28 (3): 293 - 298.

[4] 王鸿捷. 一种创新的工程公司云平台建设理论与实践[J]. 天然气与石油,2017,35(4):120 - 123.
Wang Hongjie. An Innovative Construction Theory and Practice for Cloud Platform Based on Engineering Company [J]. Natural Gas and Oil, 2017, 35 (4): 120 - 123.

[5] 郑东曦. 基于 Web 服务的统一身份认证服务的设计实现[J]. 计算机工程与设计,2006,27(6):921 - 923.
Zheng Dongxi. Design and Implementation of Single Sign-on Web Service [J]. Computer Engineering and Design, 2006, 27 (6): 921 - 923.

[6] 严晓光,王小刚,陈卓宁,等. 软件质量保障平台中基于 RBAC 的统一身份认证应用研究[J]. 计算机工程与科学,2009,31(3):97 - 100.
Yan Xiaoguang, Wang Xiaogang, Chen Zhuoning, et al. Implementation of RBAC-Based Unified Identity Authentication for Software Quality Management and Support Systems [J]. Computer Engineering & Science, 2009, 31 (3): 97 - 100.

[7] 罗　婵,董丽丽,马宗方. 基于 SOAP 协议的统一身份认证服务设计与实现[J]. 计算机技术与发展,2006,16(10): 237 - 239.
Luo Chan, Dong Lili, Ma Zongfang. Design and Implementation of Unified Identity Authentication Service Based on SOAP [J]. Computer Technology and Development, 2006, 16 (10): 237 - 239.

[8] 周建友. 统一身份认证系统的研究与实现[D]. 西安:西安电子科技大学,2010.
Zhou Jianyou. Research and Implementation of Unified Identity Authentication System [D]. Xi'an: Xidian University, 2010.

[9] 万灿军,李长云. 开放网络环境中面向信任的单点登录[J]. 计算机工程,2010,36(3):148 - 151.
Wan Canjun, Li Changyun. Trust-Oriented Single Sign-On in Open Network Environment [J]. Computer Engineering, 2010, 36 (3): 148 - 151.

[10] 李福林,徐开勇,李立新. 基于 ESB 的统一身份认证系统设计与实现[J]. 计算机应用,2012,32(1):52 - 55.
Li Fulin, Xu Kaiyong, Li Lixin. Design and Implementation of Unified Identity Authenti-cation System Based on Enterprise Service Bus [J]. Journal of Computer Applications, 2012, 32 (1): 52 - 55.

[11] 叶晓彤,王　飞. 基于页面集成的统一身份认证 SSO 系统的实现[J]. 四川理工学院学报:自然科学版,2009,22(5):51 - 54.
Ye Xiaotong, Wang Fei. Realization of General Identity Authentication and SSO System Based on Integrate WEB Page [J]. Journal of Sichuan University of Science & Engineering: Natural Science Edition, 2009, 22 (5): 51 - 54.

[12] 孙韩林,刘建华. 公众网络统一身份认证服务及标准研究[J]. 电信科学,2013,29(2):84 - 88.
Sun Hanlin, Liu Jianhua. Study on Unified Identifier Authentication Service and Standards on Public Network [J]. Telecommunications Science, 2013, 29 (2): 84 - 88.

[13] 潜　昕,罗沙白,卢康权. 构建基于分布式 SOA 架构的统一身份认证体系[J]. 软件,2013,34(1):17 - 19.
Qian Xin, Luo Shabai, Lu Kangquan. Build Unified Authentication System Based on a Distributed SOA Architecture [J]. Software, 2013, 34 (1): 17 - 19.

[14] 孙　超. 异构集成环境下的统一身份认证系统[D]. 南京:东南大学,2006.
Sun Chao. Uniform Identity Authentication System in Heterogeneous Integrated Environment [D]. Nanjing: Southeast University, 2006.

[15] 汤晓勇. 对工程公司协同办公平台的认识与实践[J]. 天然气与石油,2016,34(4):75 - 78.
Tang Xiaoyong. Understanding and Practice of Collaborative Working Platform in Engineering Company [J]. Natural Gas and Oil, 2016, 34 (4): 75 - 78.

[16] 于　华,蔡海滨,刘良旭. 基于 LDAP 和 PKI 的 Intranet 统一身份认证系统研究[J]. 计算机工程与设计,2006,27(10):1863 - 1866.
Yu Hua, Cai Haibin, Liu Liangxu. Study of Intranet Single User Authentication System Based on LDAP and PKI Technology [J]. Computer Engineering and Design, 2006, 27 (10): 1863 - 1866.

[17] 林满山,郭荷清. 单点登录技术的现状及发展[J]. 计算机应用,2004,24(增刊 1):248 - 250.
Lin Manshan, Guo Heqing. The Current Situation and Development of Single Sign-On Technology [J]. Computer Applications, 2004, 24 (Suppl 1): 248 - 250.

[18] 马荣飞. 统一身份认证系统的研究与实现[J]. 计算机工程与科学,2009,31(2):145 - 149.
Ma Rongfei. Research and Implementation of SSO [J]. Computer Engineering & Science, 2009, 31 (2): 145 - 149.