用户统一管理在郑州轨道信息化建设中的研究与实现

夏景辉 秦义展 李昱见
(郑州地铁集团有限公司 河南 郑州 450046)

摘 要 提出一种用于地铁企业的用户统一管理方案,实现了企业信息管理过程中的用户身份库管理、用户授权管理和用户认证管理。通过对地铁企业用户的现状分析、关键需求整理和方案实施,给出用户统一管理的效果分析。实践证明,该方案有效提高了用户访问快捷性、用户管理科学性、用户授权安全性、用户审计准确性、用户同步及时性,还可以为地铁企业组织架构的频繁调整带来技术保障,同时也为用户信息统计及分析奠定了基础。

关键词 用户统一管理 用户认证管理 用户授权管理

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.06.020

RESEARCH AND IMPLEMENTATION OF USER UNIFIED MANAGEMENT IN ZHENGZHOU METRO INFORMATIZATION CONSTRUCTION

Xia Jinghui Qin Yizhan Li Yujian
(*Zhengzhou Metro Co., Ltd., Zhengzhou 450046, Henan, China*)

Abstract This paper presented a user unified management scheme for Metro enterprises, which realized user identity database management, user authorization management and user authentication management in the process of enterprise information management. Through the analysis of the current situation of users in Metro enterprises, the collection of key needs and the implementation of the scheme, the effect analysis of unified user management was given. Practice has proved that the scheme effectively improves the user access speed, user management scientificity, user authorization security, user audit accuracy and user synchronization timeliness. It also provides technical support for frequent adjustment of the organizational structure of Metro enterprises, and lays a foundation for user information statistics and analysis.

Keywords User unified management User authentication management User authorization management

0 引 言

郑州地铁集团有限公司(以下简称“公司”)是2008 年 2 月 22 日经郑州市人民政府批准成立的有限责任公司,负责郑州市轨道交通项目的工程投资、建设、运营、轨道交通的广告、通信、周边土地开发利用和特许经营权范围内的经营、融资等业务。

公司在信息化管理创新应用方面,结合轨道交通建设密集型、资产密集型和资金密集型的特点和管理风险,尤其是在地铁建设的大背景下,面对运营线路员工、企业供应商(咨询单位、施工单位和监理单位等)和企业合作客户(广告公司等)急剧增多,且实施系统种类繁多(如人力系统、财务系统、物资系统、费控系统及资金系统等),用户统一管理显得尤为重要。用户统一管理强调了系统用户的标准化和自动化管理,使用户管理、组织机构管理更加规范和统一[1],将各类用户单点登录到门户。

本文着重描述基于郑州地铁集团有限公司一体化管理信息平台的用户统一管理及其应用目标、需求分析、设计、实施、部署和应用等相关内容。

1 应用目标及关键功能需求分析

1.1 应用目标

实现企业基础库的用户管理和身份认证服务,用

收稿日期:2018-09-13。**夏景辉**,教授级高工,主研领域:土木工程,信息化。**秦义展**,高工。**李昱见**,高工。

户包括内部及外部用户;把这些服务以组件或服务的形式发布,并具备相应的使用规范、标准和指引。企业管理系统 ERP(Enterprise Resource Planning)、办公自动化 OA(Office Automation)、企业门户(Portal)和将来自主开发的系统等,都能使用这些组件或服务开发。用户统一管理使用户管理、组织机构管理更加规范和优化,形成各类用户单点登录到门户的核心基础。用户统一管理应实现组织机构维护、用户账号管理、用户凭证管理、组织/用户信息同步等功能。

通过统一的用户身份管理体系,解决信息化体系管理中诸多问题,如各自信息系统具有独立的登录认证系统[3],管理企业外部用户的访问,快速部署用户对大量资源的访问,控制对各种分散资源的访问,减少账户和密码管理的 IT 成本,防止非法用户的访问,同步各业务系统用户账户的管理,快速自动清理非授权用户等。用户统一管理是把所有的系统用户进行统一存放,形成一套全局用户库,作为企业内所有 IT 应用的用户源。以轻量级目录访问协议 LDAP(Lightweight Directory Access Protocol)信息库作为载体来实现企业用户信息库的构建和用户的统一管理。

用户统一管理的应用将成为企业管理信息系统日常维护的重要组成部分。通过标准化、即时化、规范化和自动化的信息化手段固化企业用户管理流程,为公司的一体化信息管理平台提供有效的服务管理支持,同时也降低服务管理维护的成本。

1.2 关键功能需求分析

1.2.1 构建统一用户身份库

依托一体化管理信息平台的建设思路,建立集中的用户信息库,统一管理应用系统用户,并制定用户信息库标准,包含人员信息、部门信息、组织结构及用户密码规则等,最终使用接口同步,实现用户信息库与其他应用系统用户体系的同步和映射。

1.2.2 用户全生命周期管理

基于角色的用户账户管理策略,企业内部或外部人员在一体化管理信息平台以用户的方式访问系统,同时根据用户自身角色申请相应的权限。基于统一的用户身份库,形成用户的产生、变更、销户、挂起等全生命周期,这其中也包含临时用户的建立(如外部供应商)。全生命周期管理不仅是用户的管理,还有用户的自助服务,如自助修改密码、账号申请的审批或系统权限申请等[5]。

用户全生命周期管理实现了用户账户的全面管理,包含创建、修改、删除和检查等,同时建立用户和组织架构的紧密关系,为频繁的组织架构调整打下基础。

1.2.3 构建用户账号和供应管理平台

在用户同步过程中利用 OIM(Oracle Identity Management)并通过 Connector 组件获取需要被统一管理的用户,获取到之后,在统一用户管理平台进行用户的创建,然后 OIM 向各个应用系统进行推送,在应用系统中进行各自的账户创建,与此同时统一用户信息被保存到统一身份管理目录。当增加一个应用系统时,只需要增加该应用系统账号(从账号)与用户唯一账号(主账号)的一个关联信息即可,不会影响其他应用系统。同时通过安全通道来保证单点登录过程中数据传输的安全[2]。

统一用户管理平台可通过配置标准化的用户来源,对公司现有的用户创建用户统一账号,并通过自动化的用户同步,实现各个应用系统与现有的身份管理目录的身份同步。通过统一化、自动化、标准化的人员接入模式,减少用户管理过程中的管理员操作,提高管理效率。

1.2.4 构建集中访问认证和单点登录

基于地铁企业的实际业务需求,可以结合地铁行业的多系统多业务管理经验,搭建高内聚低耦合的一体化管理信息平台。用户可以通过统一的系统入口访问企业门户信息。访问系统的过程中,需要构建一套集中访问认证和单点登录的访问策略,完成用户身份和用户授权检查。用户根据自身授权情况,进入授权系统完成实际业务。进入其他授权系统模块的权限,需要遵循各业务系统的授权体系和规则。

1.2.5 用户监控与审计

用户统一管理包括用户登录系统的监控和系统操作的审计。在系统应用层端,可以监控到用户的登录 IP 及访问时间信息,在数据库端,可以监控到用户操作功能及数据的跟踪信息,能对发生的所有访问和修改进行审计。还有事后触发功能,实现特定内容的审计。通过数据库审计功能,可实现对异常用户的检测及未授权访问,如统计用户在什么时间点访问了哪些应用系统等。

1.2.6 系统稳定性、扩展性和安全性

为保证服务不间断,整套用户统一管理体系需要集群环境。基于 UNIX 类或 LINUX 操作系统平台和高可用性软件,确保系统安全、稳定、可靠的运行。系统的扩展性也需要同步考虑,以保证与已有系统及未来建设系统进行集成。

用户统一管理的审计功能要能够覆盖到集中身份管理、身份认证、授权与应用系统访问等多个环节。确保安全基础设施的安全性,包括:物理环境安全、网络安全、系统安全、数据安全等。

2　统一用户安全管理平台架构设计

统一用户安全管理平台作为一个优秀用户管理工具,通过标准的管理用户生命周期,更加高效标准地对现有用户进行管理。如图 1 所示,该平台的管理应用功能主要依托访问管理 OAM(Oracle Access Manager),身份管理 OIM 和互联网管理 OID(Oracle Internet Directory)的服务实现。

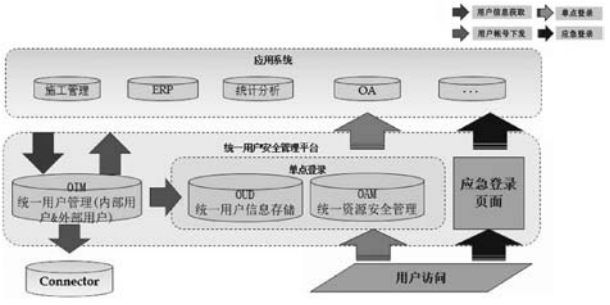

图 1　用户管理生命周期

统一用户安全管理平台的 OIM 模块通过标准 Connector 连接人力系统,进行员工基础信息的获取,获取到基础信息后自动根据一定规则创建员工账户,并实时触发数据分发事件,通过标准 Webservice Connector 或 EBS Connector 连接下游系统进行用户数据分发。OIM 模块创建用户账户数据后会同步至 OID 模块中进行统一用户信息存储。OAM 模块在用户访问时,进行单点资源授权,与 OID 模块中的用户信息进行统一认证,认证通过且在 OAM 模块中该资源已授权,则允许用户访问。

统一用户安全管理平台,前期通过 Connector 对用户进行统一收集,中期使用 OIM 对这些用户进行统一的管理,后期通过 OAM 使得用户登录安全等得到实现,在用户安全管理的生命周期中都起到了使用户管理得到安全化,统一化的作用。只有依赖目前既定的用户管理标准,通过既定的流程使得零散的用户管理得到整合,化零为整,使得企业用户的安全、高效管理得到保障。

在设计实现关键功能的过程中,需要从三个阶段来完成服务的标准化管控和高效的集成:

1)在用户管理之初,需要 OIM 通过 Connector 中获取到需要进行管理的用户,通过标准化的用户整合服务。在统一收集完之后,可基于标准的 OIM 的账号源将该账号同步至各个需求系统。通过统一化的用户管理可以避免用户信息孤岛、用户重复管理、手工创建用户操作繁杂、由于系统过多用户账户密码也需要管理多个[6]等用户管理痛点。在用户信息录入管理过程中,存在同一批次用户权限分配不同的情况,人工对权限进行管理难免出现纰漏,同时由于企业人员变动较为频繁,会大大增加用户管理成本。通过使用统一化的用户管理可以避免以上的问题发生,进而提高用户管理的效率。由于是标准化,自动化的用户同步过程,在管理实施过程中,运维人员不需要进行频繁 的操作,只需直接对用户来源变更即可。

2)在将用户统一之后要对统一化的用户进行管理。在这个过程中,以往的管理模式中存在诸多用户身份管理问题,如手动创建用户账户、对应用授权等耗时费力;ERP 系统内的职责划分难以完成;许多被弃用账户难以被检测和删除;失效用户和权限时人工操作过于繁琐等。统一用户安全管理平台可有效解决以上问题,且用户管理的安全也可以得到保障。通过端到端的访问管理,对登录风险进行分析、欺诈检测和应用细粒度授权管理等。[7]

3)用户统一管理为用户提供了统一的接入服务[4],通过多系统单点登录,将分开的登录进行集中,简化用户操作,提高了用户使用便捷程度。用户初次访问应用程序时,由于本地没有登录凭证,因此浏览器会重新定向到统一身份认证页面[5],在 OAM 内部单点实现过程中将输入用户密码与统一用户信息库进行比对,比对成功后并且确认用户权限无误后实现目标系统的跳转[8]。

统一的用户管理平台实现了以上三个阶段的步骤,能够提高在用户的统一收集、统一管理、统一登录等方面的用户管理效率,并使得用户安全的管理得到保障[9],步骤流程参见图 2。

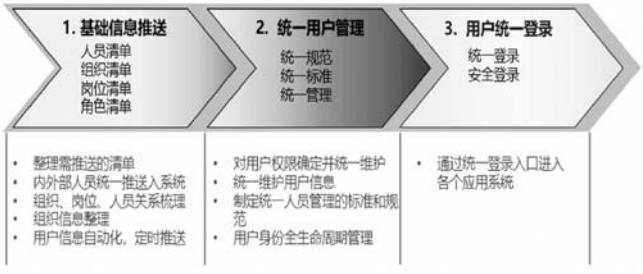

图 2　平台实现流程图

前期梳理员工数据,外部用户数据及组织,岗位相关数据,整理成具体清单后,将用户基础数据通过 Connector 或线下导入方式,同步至统一用户管理平台。由统一用户管理平台对用户访问权限进行维护确定,并维护统一用户信息,同步至各业务系统。当用户信息更新时,自动触发事件同步分发各业务系统,进行用户身份全生命周期管理,实现用户入职创建,离职失效的实时效果。用户通过单点登录平台,进行业务系统的访问,通过统一入口访问各应用系统,实现一次登录,全网漫游的高效体验。

(下转第 208 页)

2002, 62:1019 – 1043.
[5] Chan T F, Shen J. Non-texture inpainting by curvature-driven diffusions(CDD)[J]. Journal of Visual Communication and Image Representation, 2001,12(4): 436 – 449.
[6] Yeh R, Chen C, Lim T Y, et al. Semantic Image Inpainting with Perceptual and Contextual Losses[C]//The IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Los Alamitos, July 7 – 26, 2016.
[7] Pathak D, Krahenbuhl P, Donahue J, et al. Context Encoders: Feature Learning by Inpainting[C]//Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Los Alamitos. IEEE Computer Society Press, 2016: 2536 – 2544.
[8] Iizuka S, Simo-Serra E, Ishikawa H. Globally and locally consistent image completion [J]. ACM Transactions on Graphics, 2017, 36(4):1 – 14.
[9] Li Y J, Liu S F. Generative Face Completion[C]//Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Los Alamitos. IEEE Computer Society Press, 2017: 3911 – 3191.
[10] Yang C, Lu X, Lin Z,et al. High-Resolution Image Inpainting using Multi-Scale Neural Patch Synthesis[C]//Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Los Alamitos. IEEE Computer Society Press, 2017: 6721 – 6729.
[11] Ren S Q, He K M, Girshick R, et al. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks[C]//Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Los Alamitos. IEEE Computer Society Press,2015:1137 – 1149.

(上接第 103 页)

3 实现和部分应用效果分析

经细化设计和实施部署,实现了用户管理管控的标准化、自动化、实时化的新模式。用户管理搜索界面和用户统一登录界面如图 3 和图 4 所示。

图 3 用户管理搜索界面

图 4 用户统一登录界面

4 结 语

本文依托于郑州地铁集团有限公司所实施的用户统一管理进行分析,从用户管理的过程出发,将标准化的用户管理模式融合到传统的用户管理模型中。通过分析平台的关键功能需求,体现出该平台的功能优势,并从分析的结果中提炼出针对目前用户管理痛点的解决方案,以及提高服务管理效率的方案。根据平台实施的架构设计方案,对平台整体的使用过程进行了分析与阐述。

参 考 文 献

[1] 申海波,韩璞庚. 人工智能背景下的治理变迁及其路径选择[J]. 求索,2018(6):74 – 81.
[2] 李满玲. 基于单点登录的房地产税收一体化系统设计[J]. 中小企业管理与科技,2015,17(4):49 – 52.
[3] 戚利娜. 基于 Cookie 的同域单点登录的实现[J]. 创新科技与应用,2017,17(6):23 – 30.
[4] 陈丽群. 基于工作流平台的并联审批系统的设计[J]. 陕西科技大学学报(自然科学版),2011,6(5):15 – 16.
[5] 杨梦希. 数字化校园统一身份认证系统的研究[J]. 创新科技与应用,2016,28(9):15 – 16.
[6] 朱纹玉. 高职院校网络教学平台的应用探究[J]. 科技风,2017,7(3):36 – 40.
[7] 袁杰. 浅析提升企业信息化建设水平的策略. [J]. 科技创新与应用,2015,15(10):10 – 16.
[8] 周彬彬,张宏军,张睿,等. 军事语料实体标注系统的设计与实现[J]. 信息系统工程,2018(8):56 – 60,62.
[9] 眭建新,陈毅波,胡其辉. 大规模数据中心迁移关键技术研究[J]. 中国管理信息化,2018(19):142 – 144.