DOI：10. 16516/j. gedi. issn2095-8676. 2015. S1. 052

企业级信息管理系统认证统一管理的设计与实现

郭威
（广东电网有限责任公司信息中心，广州 510000）

摘要：针对企业级信息管理系统中认证管理存在的数据访问安全与便捷性的矛盾，通过设计并实现了具有多重认证为统一认证中的增强型功能的 4A 子系统，实现用户权限的角色控制，通过构建企业身份、权限、认证、审计 4 大体系，使用户在登录系统的过程中只需进行一次登陆操作，后台自动进行多重、更深入的认证，解决了传统认证模式中所有业务系统、资源认证方式一刀切的弊端，转而根据资源的重要程度进行灵活的认证策略配置，保证了重要资源的认证强度，有效保证了数据访问安全并简化了登陆程序。

关键词：访问安全；角色控制；统一认证
中图分类号：TP311. 52　　**文献标志码**：A　　**文章编号**：2095-8676(2015)S1-0234-05

Design and Implementation of Authentication in Enterprise Information System

GUO Wei
(Information Center of Guangdong Power Grid Co. , Ltd. , Guangzhou 510000, China)

Abstract: This paper is aimed at the contradiction between the security and convenience of data access security and convenience in the enterprise information system. The 4A subsystem of the enhanced function with multiple authentication is designed and implemented in this paper for the role of user authority control. By the the construction of corporate identity, authority, certification, audit 4 system, the user in a log process only need one step and system automaticly carry on authentication operation. It uses smart strategy to autoconfigure the system, guarantee the authentication strengeh of resources, effectively ensure the data access security and simplify the loging procedure.

Key words: access security; role control; unified authentication

电网安全关系着国计民生的大事[1]，为了有效保障电网安全，提高企业运行效率，建成了企业级管理系统。随着企业级信息管理系统的建设推广，数据安全问题逐渐成为了亟须解决大问题，信息管理系统横纵联合，将各个不同子系统中的数据进行统一存储和管理，将重要数据定义成主数据，切实维护数据的同源性和唯一性。在不同的系统中，由于数据来源多样，数据呈现出多元异构的特点，视频、图像、音频、文本及日志等多种呈现方式，对数据管理提出了极大的挑战[2]。系统级的数据安全包括数据存储安全和数据访问安全[3]，系统在加强数据安全管理和建设的同时，必然影响系统的易用性。为了保证用户既能方便使用，又能有效保障企业级信息管理系统管理系统的数据安全，本文专门针对企业级信息管理系统的数据访问安全的易用性解决方案进行了研究。

企业级信息管理系统中打通了各个分子系统的数据，将各个子系统的数据放置在主数据平台，保证数据的同源性和唯一性，但在各个分子系统访问数据资源的时候，由于人员角色和认证策略的不同，对数据的访问权限也就不同。例如，在企业中门户系统和财务系统就存在着资源重要性的差别，门户中通常会发布一些大众的、分享性强的信息资源，而财务系统则较门户系统而言更具有私密性、受保护性。而在这种情况下，认证策略配置人员就可以在调查、研究后对财务系统进行多重认证策略设置，而对门户系统可采取较宽松、开放性的认证方式进行。这样既可保证单点登录进入门户系统的用户，不能毫无限制的直接进入财务系统阅读一些保密信息，而是按照多重认证的策略进行多重身份

收稿日期：2015-12-15
作者简介：郭威(1983)，男，工程师，硕士，研究方向为计算机应用，从事信息系统建设和管理工作(e-mail)81840895@qq. com。

认证，从而有效的限制了财务数据被非法浏览、使用的现象。

为了有效解决多重认证以及角色认证过程中存在的一刀切的问题，本文研究设计了以用户身份集中管理为核心，建立全局唯一的权威身份信息员，通过在一点集中管理用户身份和权限，从而降低管理成本，在在统一用户身份的基础上，实现各个应用的单点登录、统一认证、统一授权、审计等信息的集中统一管理，并能提供与本企业现有的应用系统及数字证书系统进行系统集成的解决方案，规划合理、高效的用户身份管理流程，集成开发规范和运行维护规范。

本文将从统一认证和统一授权管理方面对数据访问控制进行设计，综合考虑系统的集成方式，从设计应用安全、数据安全、主机安全、网络安全、终端安全、边界安全和物理安全等方面进行系统验证，并通过系统的安全扫描和安全测试。

1　系统设计

本研究采用以用户身份集中管理的思路，建立全局唯一的权威身份信息源，使其通过集中管理用户身份和权限的方式，与其他企业级信息系统对接，降低管理成本。在统一用户身份的基础上，实现各个应用的单点登录、统一认证、统一授权、审计等信息的集中统一管理(4A 统一认证管理)，并能提供与本企业现有的应用系统及数字证书系统进行系统集成的解决方案，规划合理高效的用户身份管理流程，集成开发规范和运行维护规范等。

为了达到该目的，系统设计建设采用灵活的面向服务架构构建而成，开发过程中采用组件化开发思想，业务组件和业务组件之间的交互采用基于 SOAP[4] 的 Web 服务作为接口模式，实现组件时间的松偶合，降低组件之间的关联关系，能够有效地满足企业个性化定制和调整需求，消除系统升级的风险。技术选择上，采用 J2EE 技术架构，从而保障了系统具有良好的扩展性和稳定性[5]。

系统应用架构如图 1 所示。平台分为五个子系统，分别为身份管理系统，权限管理系统、访问控制系统、审计系统和目录服务系统，通过多种类型的标准数据源连接器实现多业务/应用系统的用户身份数据整合，并通过部署在用户客户端的统一认证接口，为用户提供多应用系统的安全的统一认证、统一授权和单点登录服务。

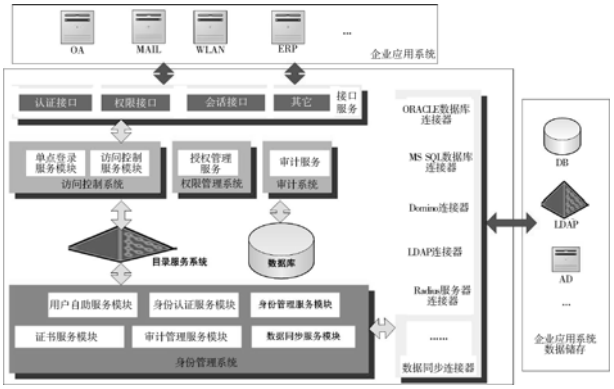

图 1　系统架构图

Fig. 1　Architecture

2　系统功能实现

2.1　身份管理模块

身份管理系统由用户自主服务模块、身份认证服务模块、身份认证服务模块和数据同步服务模块构成，主要负责用户的身份管理。

2.1.1　用户自助服务模块

用户自助服务模块使用户不需要管理员帮助和参与，就能够对自己的基本信息进行管理；能够在用户忘记帐号口令时重设口令。用户自助服务将用户信息的管理工作分散到个人，能显著减轻系统管理人员的维护负担，使得系统的安全策略得以贯彻。提供用户的自主性，用于在 SSO 环境中，实现帐号的集中管理。

模块提供用户自助更新信息更新、密码管理(包括密码修改、密码重置以及密码找回)、账号管理以及及行为日志记录查询等功能，用户可通过图形界面自助完成相关管理操作。

2.1.2　身份认证服务模块

身份认证服务模块提供全局唯一的用户登录认证，可以为应用系统提供统一的身份认证，通过安全的认证机制保证企业大门不被非法人员进入，服务便捷、高效、安全，应用系统接入改造小，具有灵活的扩展性、高可用性。

身份认证服务功能以统一的用户管理、统一的授权管理为基础，为应用系统提供身份认证的功能，做到只有通过统一认证系统验证的用户才可以访问后台的应用系统。

平台支持丰富的认证策略，并根据用户分类实现对应的策略控制，在登录企业门户时，若认证不通过，返回相关的错误提示信息，比如用户不存在、密码错误、用户被禁用等类似信息。同时，根据平台定义的用户认证策略，进行对应的策略控制。如提供多次尝试登录认证(比如3次)不通过之后，统一身份管理平台能够自动锁住该用户账号。

2.1.3 身份认证服务模块

用户身份管理是4A平台统一认证、单点登录以及统一授权等统一控制的实现基础，实现用户身份及多账号信息的统一管理支撑功能，是实现集中化的用户信息管理、有效提升企业管理效率的必要手段。其主要功能是在企业内部建立统一的用户视图，完成各应用系统的用户信息整合，实现用户生命周期的集中统一管理，并建立平台与各应用系统的用户身份信息同步机制，简化用户及其账号的管理复杂度，降低系统用户管理的安全风险。

2.1.4 数据同步服务模块

实现统一身份管理平台与数据连接器，统一身份管理平台与单点登录代理组件以及统一平台内部各服务模块之间中用户信息与业务信息的数据交换、同步以及处理功能，是统一身份管理平台各功能模块以及其与企业应用系统交互，完成业务功能的必要通信服务组件。

2.2 访问控制模块

访问控制模块包括访问控制服务和授权管理服务模块，主要负责用户登录的访问控制。

2.2.1 访问控制服务模块

访问控制服务功能是4A平台的核心服务功能之一。平台可以将接入的应用系统作为资源进行管理，提供添加、修改和删除等功能，并通过建立资源与用户、角色之间的关联关系，实现系统级的访问控制。同时，平台能支持基于角色的授权模型，支持对用户进行分角色管理，可以建立多种角色，并针对不同角色设定访问权限。针对权限设定提供对用户访问权限的控制功能，根据授权管理服务模块的动态授权控制，灵活的实现用户的访问控制功能。

2.2.2 授权管理服务模块

在用户账户、用户组、角色信息创建完毕后，就可以进行授权操作。授权操作可分为两种授权方式：单用户授权和批量用户组。

授权管理服务模块提供对用户角色、用户权限的管理支撑功能，可动态生成访问控制列表，灵活的实现用户的访问控制服务支撑功能。模块提供系统权限管理及访问控制功能，对用户使用信息系统资源的具体情况进行合理分配，实现不同用户对系统不同部分资源的访问控制。需要说明的是，此处强调的“集中”为逻辑意义上的集中。即在各网络设备、主机系统、应用系统中可拥有各自的权限管理功能，并提供统一的授权系统，通过该系统，管理员可以对各管理对象进行授权，而不需要进入每一个被管理对象。访问授权管理包括以下两个阶段。

1)权限分配阶段

这个阶段通常是指在创建用户账号时，给账号赋予相应的访问权限，包括能够以什么样的方式访问哪些系统、哪些资源。这个阶段是一个相对静态的授权过程。

2)访问授权阶段

这个阶段通常也称访问控制。这个阶段是在用户提出对具体资源的访问请求时，根据前一阶段的权限分配结果，决定用户是否有权按照所请求的方式，对所请求的资源进行访问。这个阶段是一个相对动态的控制过程。

授权管理系统具体功能包括以下几个方面：

1)应用系统级权限管理

考虑在南方电网现有应用系统中，有部分不能改造的系统，4A平台针对不可改造应用系统提供入门级的访问控制，授权粒度控制到应用系统级。

2)菜单级权限管理

对于可改造应用系统，通过对系统权限功能的细化与分类，并提出授权规范，对用户设置授权级别，对应用系统中进行定制开发，按授权规范进行修改。对新系统和可以改造的旧系统提供菜单级别的集中授权管理。

2.3 权限管理模块

权限管理是由系统管理员发起，对业务系统访问权和业务系统内部菜单或者按钮等权限员进行管理的模块。

2.4 审计模块

审计管理服务模块能够实现全面、集中的用户行为审计管理。系统能收集、记录、管理用户对应用系统的登录认证、数据访问等关键操作行为，并

提供查询服务支持，同时也可以实现对平台管理员的操作行为进行审计。

审计管理服务模块可以实现平台内部的集中安全审计，提供全面、集中的安全审计功能，包括安全审计自动响应、安全审计数据生成及安全审计浏览三个方面。能及时发现非法登录和非法操作，并对非法登录和非法操作快速分析、定位和响应。在出现安全事故时用于责任追踪。同时，对人员的登录过程、关键操作行为等进行审计和处理。

2.5　目录服务系统

LDAP 目录服务[6]系统是 4A 管理平台的重要组成部分。要求遵循标准的 LDAP 协议规范(支持 LDAP V2、LDAP V3 版本)，具有高可扩展性(支持 LDAP Schema 灵活扩展，支持自定义 Schema 模式的导入和导出，并提供基于 Java 和 C 的 LDAP API 接口，具备良好的二次开发能力和整合能力)，具备为企业应用提供集中化管理和数据存储的标准化访问的能力。

LDAP 目录服务在 4A 平台中主要实现用户数据、证书数据、应用系统数据的集中存储和集中对外查询服务功能，并支持与各应用系统数据源的双向数据同步。主要用来管理用户信息和 CRL 信息等。为平台提供了分布式管理和快速查询的功能。

2.6　系统集成

由于系统涉及身份、权限、认证、审计 4 大析的集中管控和应用，所涉及的集成内容有平台类系统集成和普通业务应用的集成。

2.6.1　平台类系统的集成

平台类系统集成关系如图 2 所示。平台类业务组件的功能权限和数据权限通过 4A 平台的用户认证和授权签权完成，业务应用的功能点同样通过 4A 平台的用户认证和授权签权完成授权。

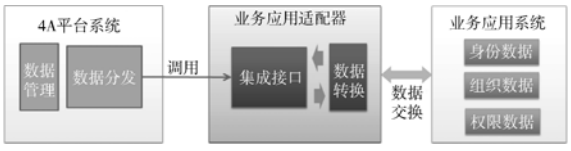

图 2　平台类系统集成图

Fig. 2　Figure of platform integrated

4A 平台与平台类系统的认证步骤如下：

1)平台类系统登录时，由 4A 系统的认证服务以及访问网关自动完成用户登陆。

2)平台类系统将组织机构、角色、功能资源、数据资源注册到 4A 平台中，平台类系统不保存这些数据。

3)用户访问平台类的资源时，平台类调用 4A 平台提供的接口服务，对用户请求的资源进行权限校验。

2.6.2　普通应用业务的集成

针对本企业已建设业务应用系统，与 4A 平台集成的内容主要包括统一认证服务的集成以及权限数据的集成、以及审计日志数据集成，对数据集成系统采用基于“业务应用适配器”的方式，其业务集成关系图见图 3，数据同步集成方式主要基于“业务应用适配器”与业务应用系统进行数据同步集成，数据的同步方向为单向，以 4A 平台数据为数据源，对各集成业务应用系统进行数据同步。

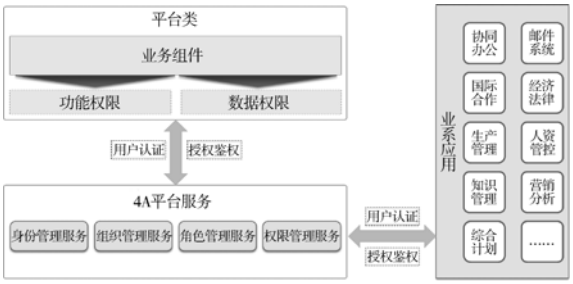

图 3　业务集成图

Fig. 3　Figure of process integrated

3　系统测试

3.1　测试方法

为了测试测试系统设计和实施的有效性，保证系统性能，我们根据业界标准测试准则[7]及《广东电网公司信息化评测实验室交付测试操作指南 V2.0》、《南方电网公司 4A 统一管理平台系统需求规格说明书 V1.0》与《南方电网公司 4A 统一管理平台系统用户操作手册 V1.2》，在测试环境中对“南方电网公司 4A 统一管理平台 V1.2”进行了交付(性能)测试，开展了登陆、获取菜单列表接口、登陆接口、票据验证接口、退出接口的多用户模拟仿真测试。

3.2　测试环境搭建

本次测试使用了 3 台系统应用服务器、一台系统数据库服务器和 2 台测试客户端进行，各机器配置如下：

使用3台Intel(R) Xenon(R) CPU E7-4850 @ 2.00GHz的CPU，16G内存，160G硬盘的虚拟机作为系统应用服务器；

使用Intel(R)物 Xenon(R) CPU E7-4850 @ 2.00GHz的CPU，32G内存，160G硬盘的虚拟机作为系统数据库服务器；

使用2台联想台式机作为测试客户端，测试客户端采用Intel(R) Core(TM) i3-2350M CPU @ 2.30GHz ×2的CPU，4G内存，500G硬盘。

3.3 测试结果

在登陆测试中，我们以500个用户并发执行“登录-web500”测试案例，持续运行10 min。在500个并发用户情况下，“登录-web500”的事务平均响应时间为10.44 s，在事务成功率方面，“登录-web500”的事务成功率为99.92%。

在获取菜单列表接口中，以500个用户并发执行“获用户列表接口500”测试案例，持续运行10 min。在500个并发用户情况下，“获用户列表接口500”的事务平均响应时间为1.20 s。在事务成功率方面，“获用户列表接口500”的事务成功率为100.00%。

在登陆接口测试中，以1 500个用户并发执行“登录接口1 500”测试案例，持续运行10 min。在1 500个并发用户情况下，“登录接口1 500”的事务平均响应时间为12.11 s，在事务成功率方面，“登录接口1 500”的事务成功率为99.99%。

在票据验证接口测试中，以500个用户并发执行“票据验证接口500”测试案例，持续运行10 min。在500个并发用户情况下，“票据验证接口500”的事务平均响应时间为2.48 s，在事务成功率方面，“票据验证接口500”的事务成功率为99.99%。

在退出接口测试中，以500个用户并发执行“退出接口500”测试案例，持续运行10 min。在500个并发用户情况下，“退出接口500”的事务平均响应时间为3.87 s，在事务成功率方面，“退出接口500”的事务成功率为100%。

综上所述，此系统设计与实现的性能满足设计要求。

4 结论

在深入理解和实现统一身份认证和权限管理的基础上，通过权限控制限制非法用户的访问，梳理统一的用户身份认证，形成统一的账号管理，实现业务系统用户生命周期的集中统一管理，并实现一处登陆，可访问所有企业级业务系统；形成统一授权管理，为企业级应用及业务流程整合提供有效支撑；形成统一审计管理，对身份、权限、资源进行集中审计和分析，实现系统信息资源访问安全和预警能力。在实现统一认证和统一管理的环节实现了以下措施方便用户保障安全：

1)平台类系统登录时，由4A系统的认证服务以及访问网关自动完成用户登陆。

2)平台类系统将组织机构、角色、功能资源、数据资源注册到4A平台中，平台类系统不保存这些数据。

3)用户访问平台类的资源时，平台类调用4A平台提供的接口服务，对用户请求的资源进行权限校验。

参考文献：

[1] 文浩. 供电企业安全生产可视化管理模式应用研究[J]. 南方电网技术，2010，4(s1)：68-71.

[2] 刘义军. 基于云计算平台的个人信息融合系统的研究与实现[D]. 北京：北京邮电大学，2010.

[3] 张莉艳. 基于云计算的铁路信息共享平台及关键技术研究[D]. 北京：中国铁道科学研究院，2013.

[4] 华悦. 面向SOAP消息的Web服务安全交互机制研究[D]. 南京：南京航空航天大学，2012.

[5] 左国华. 基于J2EE架构的分布式企业级Web应用的研究[D]. 武汉：华中科技大学，2005.

[6] 蒋兴浩，杨树堂，李萍. LDAP目录服务在PKI/PMI中的应用[J]. 计算机工程，2004，9(18)：49-51.

[7] GB/T 25000.51—2010，软件工程软件产品质量要求与评价(SQuaRE)商业现货(COTS)软件产品的质量要求和测试细则[S].

(责任编辑 高春萌)