基于融合通信的水利信息门户①

骆小龙, 虞开森, 金宣辰

(浙江省水利信息管理中心, 杭州 310009)

摘 要: 针对水利行业内信息资源多散乱、管理不便、操作繁琐等问题, 设计并开发一套综合的水利信息门户. 首先介绍门户的设计理念、系统结构, 然后对门户的具体功能详细阐述. 门户通过整合即时通信资源和业务应用资源, 实现资源和消息统一管理, 通过整合业务应用资源的用户体系, 实现身份认证和单点登录, 通过按部门、按岗位的资源推送, 实现资源按需定向发布服务. 实际使用情况表明, 门户较好地解决了资源的应用问题, 让资源的使用变得简单又方便, 让用户的工作变得愉悦又高效.

关键词: 信息门户; 单点登录; 即时通信; VPN; 应用资源

Water Resources Information Portal Based on Unified Communication

LUO Xiao-Long, YU Kai-Sen, JIN Xuan-Chen

(Information Management Center, Zhejiang Water Resources, Hangzhou 310009, China)

Abstract: In the light of too much dispersed information resources caused inconvenient management and complicated operation in water conservancy, we design and develop a compositive information portal. First, we introduce the design idea and the architecture of the systems. Then, we give a detailed exposition on various functional modules. Through the integration of instant communication resources, business application resources and user system of business application resource, the portal realizes the unified management of the resources, the message and the identity authentication and single sign on. Meanwhile, the portal realizes publishing service on-demand according to the department or position. The actual application results show that the portal can solve the problem of resource application, make use of resources more simple and convenient and make the work of the user more pleasant and efficient.

Key words: information portal; single sign on; instant messaging; VPN; application resources

近年来, 随着水利信息化建设不断深入, 浙江省水利厅建立了一大批水利业务应用系统. 这些系统为创新水行政管理模式, 提高水行政管理工作效率, 起到了积极推进作用[1]. 然而, 由于开发时间和开发厂商不同、采用的技术架构不同、运行的网络环境不同等多方面原因, 许多系统存在一定程度的独立性和封闭性, 致使用户在日常工作常有困扰, 典型表现为: (1)系统各自有独立的账户体系, 身份认证方式, 使用时涉及多地址、多账户、多密码记忆及多点登录, 记忆难, 操作不便; (2)部分系统应用环境仅局限于厅机关内部, 无法在机关之外的网络环境使用, 给外出人员工作带来不便; (3)单位用户之间的线上沟通交流平台缺乏, 需要借助 QQ 等社交软件, 难以与系统有机整合. 过多分散、孤立的业务应用系统和五花八门的即时沟通平台让用户在工作中千头万绪、疲于应付, 愉悦感大打折扣. 迫切需要建立一个综合性的统一信息门户, 整合各类资源, 解决用户长期以来的困扰.

1 信息门户简介

水利信息门户(以下简称“门户”)以身份认证平台为基础, 以融合通信技术为依托, 以整合电话、短信、即时消息等通信资源和政务、防汛、水资源等各类业务应用资源为主导, 以简化用户日常应用操作, 提升用户工作效率为目标. 它是访问各类信息和应用的个

① 收稿时间:2014-12-11;收到修改稿时间:2015-01-22

性化统一入口.

门户通过资源整合, 实现“八大统一”功能, 即统一的身份认证、单点登录、后台管理、资源管理、消息管理、访问控制、访问搜索和网络环境; 通过按部门、按岗位的资源推送, 实现应用资源“一站式”服务, 用户只需登录门户客户端, 便可访问与自己相关的应用资源, 实现同事之间的多渠道沟通, 最终达到“一切资源归门户, 使用资源靠门户”的目标. 门户较好地解决了目前水利行业系统多、数据散、查询不便, 账户密码难记等问题, 极大地提升用户体验感.

2 信息门户设计

2.1 总体架构

门户采用 C/S 架构模式, 分后台管理和前台客户端两个部分. 后台管理是门户的核心和主导, 建有身份库、资源库、权限库、日志库等 4 大数据库体, 支撑和保障门户的正常稳定运行, 实时监控各类注册资源信息和用户资源关系的权限信息, 详细记录人员调整、权限分配、平台登录、资源访问等各种操作日志. 前台客户端是门户与用户的人机交互界面, 按照框架结构模块化设计, 是资源信息的主要展示窗口. 门户总体结构分 4 层, 即基础设施层, 应用资源层, 应用服务层和表现层, 如图 1 所示.

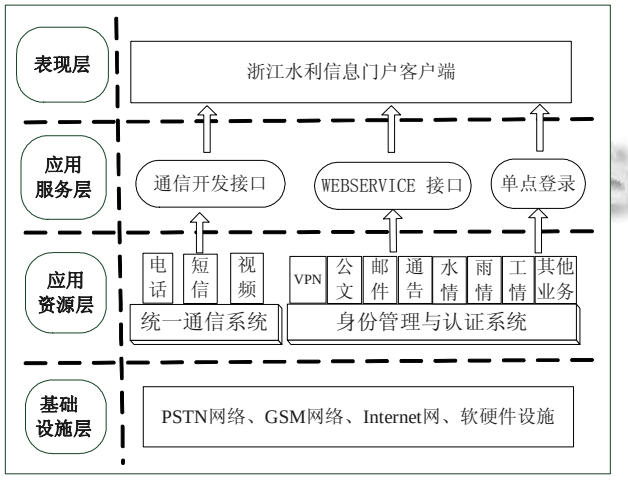

图 1 总体架构

(1) 基础设施层. 由 IP 网络、PSTN 网络、GSM 网络以及服务器、交换机等软硬件设施组成, 是各类应用的基础支撑环境, 为门户的应用资源奠定基石.

(2) 应用资源层. 是省水利厅现有各类公共资源和岗位资源的聚集地, 以身份认证平台为基础, 形成统一的身份管理与认证系统, 可为已建或新建的应用系统提供统一的用户管理、身份认证服务、访问控制、后台管理等; 通过统一通信系统, 融合电话、短信、音视频等多种通信手段. 通过该层, 各用户可登录认证, 表现层的各应用系统可进行数据交换和提取.

(3) 应用服务层. 以 Webservice 方式搭建各类通信接口、数据访问接口和单点登录接口, 通过接口发布为系统访问数据库服务器提供通道. 服务方式的引入有效地解决了系统直接调用数据库数据带来的连接不安全、访问速度慢、并发性不高等问题, 真正实现平台与服务器操作系统、数据库平台的无关性[2].

(4) 表现层. 类似于腾讯 QQ 的客户端软件, 按规则集成和展现各类公共资源和岗位资源, 实现身份认证、单点登录、消息提醒、通信融合等.

2.2 单点登录

单点登录(single sign on, sso)是一种方便用户访问多个系统的技术, 用户只需登录时一次注册, 就可在多个系统间自由穿梭, 不必重复输入用户名和密码来确定身份. 其根本原理是保持用户的会话状态, 经过一次认证就可建立单点登录会话, 每个单点登录会话对应于一个令牌, 用户访问应用系统时向应用系统传递单点登录令牌, 应用系统能够根据令牌识别用户的认证状态, 从而使一次认证能够被多个应用系统认可, 避免了重复认证. 其体系结构如图 2 所示.

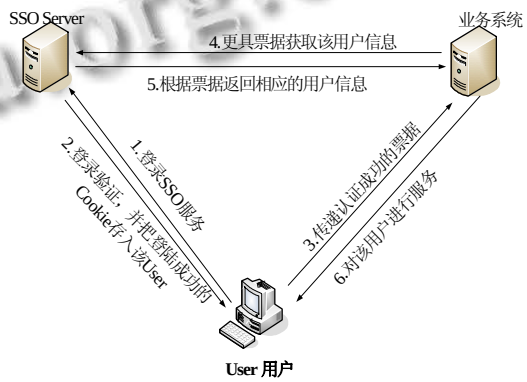

图 2 单点登录体系结构

门户以行业最权威的浙江省人力资源管理数据库为基础, 构建身份认证平台, 通过整合、改造各类业务应用资源的身份库和认证体系, 实现单点登录, 并内置三种单点登录方式, 即基于 WebService/ HTTP 接口的动态票据单点登录、基于 Agent 的单点登录和基于

HTTP 重定向技术表单方式的单点登录. 各应用系统根据各自的实际情况, 利用 webservice 形式的认证接口, 并选择任何一种登录方式即可完成整合. 通过单点登录, 门户汇聚了行业应用资源, 形成统一入口.

(1) 动态票据单点登录: SSO 生成一张带时间戳的动态票据, 加密后, 以 HTTP POST 方式推送给接入应用系统; 接入应用系统收到票据, 向 SSO 认证票据的有效性; 如票据有效, SSO 给接入应用系统返回用户名, 并请求登录接入应用系统.

(2) 基于 Agent 的单点登录: 通过在接入应用系统服务器上安装一个代理模块, 由该模块连接 SSO 负责认证和单点登录.

(3) 基于表单方式的单点登录: 在 SSO 记忆接入应用系统中的用户名和密码, 用户通过门户单点登录该应用系统时, SSO 自动取出记忆在 SSO 中对应的用户名和密码, 并帮助用户提交该认证请求, 最终完成单点登录全过程.

2.3 资源管理

门户资源分通信资源(邮箱、短信、电话、VPN 等)和业务应用资源(通知、公文等)2 大类, 均纳入门户后台统一管理. 资源管理分资源注册和分配两个环节, 前者决定门户拥有哪些可用资源, 后者决定资源授权给哪些用户使用.

(1) 资源注册. 记录每个资源的基本信息, 同步信息和认证信息. 通过注册, 门户后台形成完整注册信息的资源库. 资源基本信息包括资源的名称、图标、类型、显示方式、顺序、接入密码等, 记录资源的基本情况; 资源同步信息包括用户体系、数据交换模式、接口类型、同步加密类型、接口数据传输格式、版本号等, 记录资源本身用户体系与身份认证平台中用户体系之间的关系; 资源认证信息包括认证方式(commnetauth 认证、easyauth 认证、无认证)、认证 token(账户密码提交方式、票据统一认证方式)、重定向方式(post 方式、get 方式)等, 记录每个资源的认证信息. 通过资源注册, 确定了资源响应的操作方式和界面显示模式.

(2) 资源分配. 即资源授权, 参照现实工作中的权限体系, 门户划分了部门权限、岗位权限、特殊权限 3 种, 能满足复杂的权限控制需求, 可按用户、部门、用户组、角色、动态用户组等方式授权, 也可通过权限继承与过滤和分级授权等机制实现实际的授权需求. 授权管理能够基于角色进行访问控制策略, 对用户和角色进行灵活授权, 使同组用户具有相同的权限. 通过资源分配, 确定了资源被使用的范围.

2.4 消息管理

门户整合和集成各类应用资源的消息, 做到消息管理的即时化和规范化. 通过门户的消息管理, 用户和信息资源之间搭起了一座桥梁, 在统一的消息平台上获取多种信息服务, 实现与应用系统的无逢结合. 门户现整合的应用资源主要有: 通知、即时信息、短信、电话、邮件、待办公文等 6 大方面, 并有弹出提醒和主界面待办数量标记提醒两种方式.

(1) 弹出提醒消息; 适用于上述各类资源. 消息框风格一致, 固定于显示区右下角, 一般在信息到达后 60 秒内自动弹出, 框内包含信息的类别、来源、主题或内容等, 并可直接链接访问信息详细内容. 邮件和待办公文的消息在一次提醒 15 秒钟后自动消隐, 其他资源的消息框弹出后需用户手动关闭操作.

(2) 待办数量标记提醒消息; 适用于通知、邮件和待办公文 3 种资源; 在门户客户端主界面内集成, 待办数量一般在信息到达后 60 秒内自动刷新显示.

2.5 安全机制

门户包含的数据总类多, 信息量大, 数据的安全性显得很重要, 特别是用户信息, 直接决定用户对行业内其他应用资源的使用权.

(1) 数据加密, 确保数据存储和传输安全; 客户端与服务器端数据交互过程中, 全程通过 HTTPS 协议实现. HTTPS 协议是 SSL 记录协议在应用层的实现, 能够保证数据传输的机密性和完整性, 确保数据不被窃听、伪造和篡改, 并且始终对服务器进行认证[3]. 在协议层基础上, 实现对敏感数据进一步数据库存储数据加密, 确保用户信息的隐私. 即使发生数据丢失, 也能确保数据不被利用, 保证数据的安全性.

(2) 多方校验, 确保数据用户方合法性; 门户支持用户名口令、数字证书以及动态令牌三种认证方式. 接口认证增加接口参数认证和时间戳签名认证, 并且对调用方的数据源进行检测, 阻止个人通过其他手段获取身份认证系统的数据. 同时, 对数据获取进行流程规范, 防止个人随意获取数据. 在统一身份认证过程中, 使用 cookie 作为票据媒介, Cookie 首次产生时, 在 SSO 中记录用户 cookie 来源 IP 地址, 并在后续应用时进行 IP 地址匹配, 避免窃取者通过 cookie 访问信息

来身份认证.

(3) 虚拟化服务, 确保数据物理介质安全性; 在系统中, 实现 LDAP 服务器的主复制, 任何一个服务器数据的增加都会在另一个服务器中增加, 同样任何一个服务器数据的减少也都会引起另一个服务器数据的删减. LDAP 配合负载均衡, 可以既保证数据的完整性, 也能保证服务的连续性.

3 门户客户端功能

门户是一个装载资源、整合应用的平台, 其各项功能产生于后台, 体现于客户端. 除通讯录和即时信息功能紧密集成于客户端本身外, 其他功能都以资源形式通过系统管理员后台授权配置推送至用户获得.

3.1 通讯录

通讯录分用户公用的企业通讯录和用户自主定制独享的个人通讯录. 企业通讯录由系统管理员统一维护, 包括组织结构调整、人员内容更新等, 一般用户无权操作, 且只能在被授权的组织结构范围内按姓名、手机号、短号、分机号、办公室号等信息的模糊检索、查找通讯录的人员信息. 企业通讯录支持人员在线、离线等状态感知; 支持从通讯录发起电话、即时消息、文件传输、短信等; 支持常用联系人、群组、最近联系人等信息分类. 个人通讯录由用户自主维护, 实现个人联系人资料管理, 可对人员进行分组, 发短信, 拨打电话, 支持电话簿的导入导出.

3.2 即时信息

门户具有类似于腾讯通 RTX[4]的实时通信功能, 支持用户之间随时点对点进行沟通. 除方便快捷地进行文字沟通外, 门户还支持在线和离线多文件拖拉式传输, 断点续传, 支持截屏、闪屏等功能. 为方便联系, 在即时信息界面中, 详细展示对方用户的电话、分机、手机、网内短号、办公室室号、邮箱地址等联系方式, 并支持直接触发电话拨打和邮件发送功能.

3.3 电话

门户整合中国电信协同通信 ECP [5], 以单位固话号码作为 ECP 资源号, 利用 ECP 后端的云通信平台, 实现 IP 网络、GSM 网和 PSTN 网络的融合通信, 并实现固话、小灵通、手机、PC、PDA 以及未来其他终端设备在业务层面的统一通信[6], 即一号通.

门户支持从通讯录中直接拨打电话, 支持手机号跨区自动判别、呼叫转移和来电续接; 用户拨打/接听电话时, 可通过门户灵活选择通信终端(手机、固话、小灵通、PC 等)作为拨打/接听时的终端, 做到来电不漏接, 号码随身带. 电话拨打流程如图 3 所示.

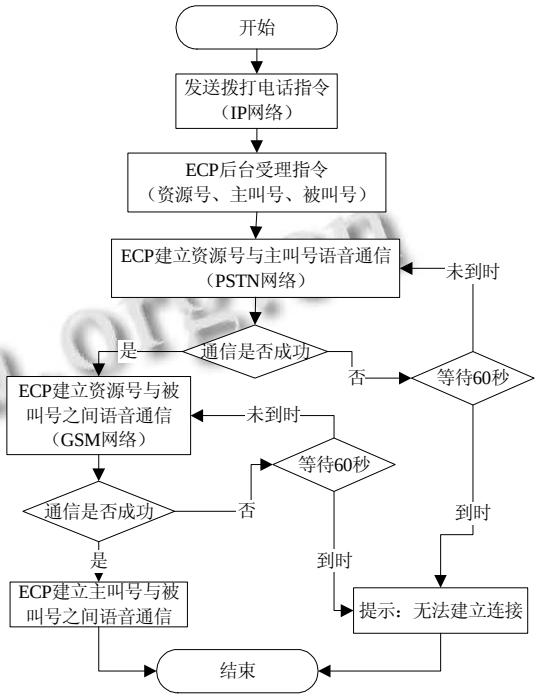

图 3 电话拨打流程

3.4 短信

门户对接移动企业短信机, 并为每位授权用户分配唯一短信号(由 12 位短信机号和 4 位内部顺序号组成), 设定每位用户的日短信发送量及是否允许发送定时短信的功能限制. 门户客户端支持短信即时发送、定时发送和任务发送等功能, 支持批量用户短信群发和指定手机号码短信单发功能, 支持移动用户回复短信的接收. 同时, 门户客户端对发送和接收短信日志的具有详细日志记录, 提供短信统计报表.

3.5 VPN

VPN 技术是综合运用密码、安全协议、访问控制等信息安全技术, 集加密、认证、访问控制、网络审计等多种安全机制为一体的一种较为全面的网络安全技术[7]. VPN 作为门户的特殊通信资源, 与后台 SSO 用户体系联动, 可实现统一认证. VPN 是厅机关局域网外用户通过互联网访问网内业务应用的唯一通道, 也是内部业务应用被外部用户安全使用的有效屏障.

门户客户端登录进程中, 会自动判断当前所处网络环境和当前用户的 VPN 资源被授权情况, 在有权使

用 VPN 且处于外部环境时，门户会自动开启 VPN 功能，建立用户与厅机关内部网络之间的专用网络隧道，为用户访问内部业务应用资源提供通道. 上述整个过程自动完成，无需用户干预. VPN 验证流程如图 4 所示.

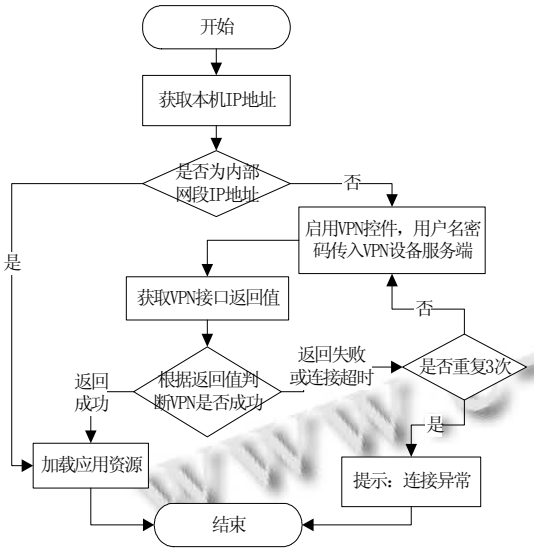

图 4　VPN 验证流程

3.6 邮件和公文

邮件和公文是门户中使用范围最广、使用频繁最高、与账户结合程度最紧密的两项业务应用. 门户分别进行深度资源整合，实现身份认证和单点登录，并在门户客户端主界面醒目位置提供快捷图标.

(1) 邮件系统. 采用网易公司提供的企业邮局平台构建. 门户通过邮件标准 POP3 协议，实时侦听、监测邮件系统中当前用户的未读邮件数量，并在邮件到达时通过消息框弹出和未读邮件具体数量两种方式即时提醒.

(2) 协同办公系统. 是机关用户处理日常公文的业务应用系统. 门户通过公文相关接口函数，实时监测系统中当前用户的待办公文数量，并做到代办文件到达时消息框和待办具体数量两种方式即时提醒.

3.7 其他应用

门户还集成其他水利业务应用系统，以“个性化图标+关键字”方式排列标注，如图 5 所示. 按照应用系统在门户中的认证方式不同，大致可分 3 类:

(1) 无认证应用: 此类应用集成于门户客户端仅为了资源管理和调用的方便，属开放式应用，与门户账户无关. 如: 浙江水利文献网、等等.

(2) 弱认证应用; 此类应用非完全开放式应用，面向一定范围的用户群公开，用户一旦有权使用此类系统，则对系统操作权限全部相同. 系统使用时须校验用户登录信息，故必须通过信息门户客户端调用访问. 如省防汛减灾 GIS 支撑平台、等等.

(3) 强认证应用; 系统有丰富的权限控制认证要求，与 SSO 用户体系对接，做到账户同步. 根据账户在系统中不同岗位或角色，实现不同权限体系下的系统操作使用. 如省计划项目管理系统、等等.

图 5　应用系统

4　结语

本文通过水利信息门户的建设实践，详细阐述了门户的构架、原理和功能需求，提出了门户“八统一”概念. 通过灵活多样的资源配置方式，安全可靠的数据传输通道，门户实现资源按岗位、按角色的定向推送服务，做到用户终端应用层面数据和资源的整合、共享. 门户自 2012 年在厅机关投入运行以来，覆盖范围不断扩大，已从厅机关内部处室逐步延伸到厅属直属单位和市县水利部门，它不仅是水利行业内职工即时沟通交流的通信平台，也是部署、推广水利行业内部业务应用资源的载体，更是保障系统安全可靠使用的通道，为我省水利行业职工日常工作带来极大便利，真正体现了“门户在手，应用全有”.

参考文献

1 李歆,米持平.基于统一身份认证的长江委信息门户设计及应用.水文,2008(增刊):136–138.

2 骆小龙,耿洛桑,余金铭等.水利工程实时图像资源切片与应用.水利信息化,2012(6):35–39.

3 卢士达.SSL 在构建安全智能电网中的研究与应用.计算机应用与软件,2012,29(6):282–284.

4 苗来柱.腾讯通(RTX)在企业办公系统中的应用.自动化与仪器仪表,2007(6):87–88.

5 沈毅纲,宋革联.智慧城市中基于云通信的协同通信系统研究.计算机光盘软件与应用,2013(15):21–22.

6 范兴发.统一通信在企业信息化中应用探讨.电脑知识与技术,2014,10(5):910–912.

7 曹利峰,杜学绘,陈性元.一种新的 IPsec VPN 的实现方式研究.计算机应用与软件,2008,25(7):66–67.