



移动办公在发电企业中的研究和应用

刘 铮¹, 王 静²

(1. 中国电能成套设备有限公司 北京 100080; 2. 中国电力投资集团公司 北京 100140)

摘 要: 随着移动互联网和云计算技术的飞速发展, 企业移动办公需求应运而生。以中国电力投资集团公司移动办公系统建设项目为案例, 深入地研究了现存的各条技术路线, 提出了将成熟的页面适配技术与 VPN、身份认证体系及移动设备管理系统相结合以构建移动办公平台架构的方法, 并严格对照信息系统安全等级保护二级标准建设安全保障体系, 实现了在保障信息安全前提下, 交付最佳用户体验的移动办公产品的目标。

关键词: 移动办公; 企业应用; iOS; Android 系统; 发电企业

doi: 10.3969/j.issn.1000-0801.2013.11.020

Research and Application of Mobile OA Technology in Power Generation Enterprise

Liu Zheng, Wang Jing

(1. China Power Complete Equipment Co., Ltd., Beijing 100080, China;

2. China Power Investment Corporation, Beijing 100140, China)

Abstract: As the rapid development of mobile Internet and cloud computing technology, enterprise mobile OA needs bred. Using the CPI group mobile OA system construction project as a case, the existing various technical routes were researched in-depth. Combining the mature page adaptation techniques with VPN, authentication system and mobile device management system, a method to build mobile OA platform architecture was proposed and strictly controlled class 2 of information system level protection to building the security system, and the mobile OA system can deliver the best user experience under the premise of information security.

Key words: mobile OA, enterprise application, iOS, Android system, power generation enterprise

1 引言

随着科技发展的日新月异, 平板电脑全球出货量已经超越传统 PC 机, iOS 与 Android 系统飞速发展, 成为移动互联网主流操作系统。革命性的人机交互界面、Wi-Fi/3G 等无线网络的迅速普及、云计算技术的发展和大规模应用以及终端能力不断提升, 推动着移动互联网超越了传统, 成为主流的信息交互模式。

在这样的时代背景下, 企业移动办公需求应运而生。企业领导及管理层由于工作需要, 经常出差参加公务活动, 工

作地点并不固定。智能手机、平板电脑等时尚信息设备已逐渐得到企业高层用户的认可, 成为工作、生活的重要工具。使领导和员工方便地使用移动终端设备、便捷地处理企业内部的日常工作是亟待解决的一个重点问题, 对信息资源整合的需要越来越迫切, 需要更好地面向不同层次用户、不同终端设备发挥更加精细、全面、准确的信息化支撑作用。

2 技术方案研究

2.1 技术路线选择

构建企业级移动办公系统, 目前存在两条主流技术路



线,一条是采用页面适配技术,利用移动设备终端客户端展现目标应用系统经裁剪后的界面。另一条技术路线是采用虚拟化技术,将PC版目标应用系统映射到移动设备屏幕。在对多方电力行业业主单位及实施单位进行大量的调查和研究后,得出如下基本结论。

(1) 页面适配路线

将PC版应用系统的界面进行裁剪重组,突出重点内容,调整版式,使其适合移动终端浏览,将调整后的页面以XML格式在移动业务平台中发布。页面适配路线的客户端程序不存储系统数据信息,退出时可以清空缓存,对带宽要求较小,网络条件不好的地区亦可正常使用。系统风格样式可以定制,操作简单,运行流畅,体验效果较好。网络上可以支持3G、GPRS、Wi-Fi等移动网络,支持SSL VPN。系统上支持iOS、Android等主流操作系统,系统可自适应终端屏幕尺寸。经过开发可支持基于硬/软证书的身份认证。

(2) 虚拟化路线

搭建虚拟化应用服务器,移动终端用户通过登录客户端获得虚拟应用服务。如在B/S架构的应用中,系统会将IE浏览器推到用户屏幕,显示内容和效果与在PC机侧相同。用户可操作此浏览器进行移动办公。理论上绝大多数PC应用都可不经改造在移动终端使用。缺点是在智能手机类屏幕尺寸较小的终端上,显示效果不佳,无法滑动,只能依靠滚动条,打开附件时用户体验较差,网络较差地区使用延迟感较强。另外,根据终端屏幕大小可能还需对应用系统进行简单改造。

两种技术路线的测试比较如下。

针对两条技术路线,前期分别与相关单位合作进行了测试。测试结果表明,页面适配路线在操作体验效果上有较明显优势;虚拟化路线部署应用虽然快捷,但用户体验较差。

根据企业实际需求,办公系统对清晰的界面和简洁流畅的操作有较高的要求,经多方论证,一致认为更适合采用页面适配技术路线进行建设。并结合信息安全方面的防护需求,形成了以SSL VPN为数据通道,页面适配技术为移动业务平台核心,证书身份认证为安全保障基础的总体技术路线。

2.2 移动办公平台技术模型

(1) 智能客户端

为保证最佳用户体验及更小网络带宽要求,智能客

端采用C/S架构部署。智能客户端在底层智能客户端内核(SCC)的基础上封装了一层系统抽象层,屏蔽了各种平台、各种终端之间的差异。客户端的核心模块包括AM(应用管理)、RE(渲染引擎)、SUA(智能升级代理)、LA(本地能力代理)、标准语言支持能力(JS/CSS/HTML)、LD(本地数据库能力)等。此外,智能客户端支持原生态的JS/CSS/HTML语言,可方便系统二次开发的快速部署。

通过智能客户端可调用移动终端丰富的本地能力,如拍照、GPS、录音、录像、蓝牙、拨打电话、发送短信等,实现移动业务中各种本地能力调用需求,并集成原生的特效于终端应用,提高用户的原生体验。当使用者业务到达所在节点后,智能客户端以推送消息的方式,提醒使用者对其业务进行处理;第一时间告知使用者新业务到达,避免使用者未及时打开移动门户应用而耽误业务处理最佳时间。Android操作系统采用非TCP的面向连接协议进行消息比对,对服务器资源占用更少,移动终端耗电量更低,网络流量更少。iOS采用APNS方式进行消息推送。

(2) 服务端平台

移动业务平台技术模型如图1所示。

服务端平台为移动办公平台技术模型的核心环节。移动应用系统数据来源采用页面适配方式将原业务系统数据对接至移动应用系统,移动应用系统服务端主动以HTTP/HTTPS方式请求原业务系统页面,以智能抓取的方式获取页面数据,在服务端将数据信息重新格式化之后展现在移动终端,对于需要提交的数据信息,同样以HTTP/HTTPS方式模拟请求队列数据进行数据提交。

服务端平台提供了极为强大的扩展能力,通过移动应用平台的四大接口可以和几乎所有的IT系统进行对接,满足各式各样的简单或复杂的系统,4种方式为:展现层数据解析(data parser)接入方式、标准Web Services接入方式、数据垂直(DB vertical)读取接入方式、国际标准协议(standard protocol)接入方式。

(3) 技术安全体系

移动办公应用平台从技术层面上对信息安全提供了有力保障。客户端与服务端采用基于SSL的传输通道进行数据交互,保证数据传输的私密性。设计了四重绑定认证机制,对用户的IMSI、ESN/IMEI、手机号码、用户姓名进行绑定,保证一部手机、一张卡、一个手机号、一个用户名只能由该户主使用,任何一项出现偏差,系统都拒绝访问,有效保证了用户重要数据的安全性。同时,引入

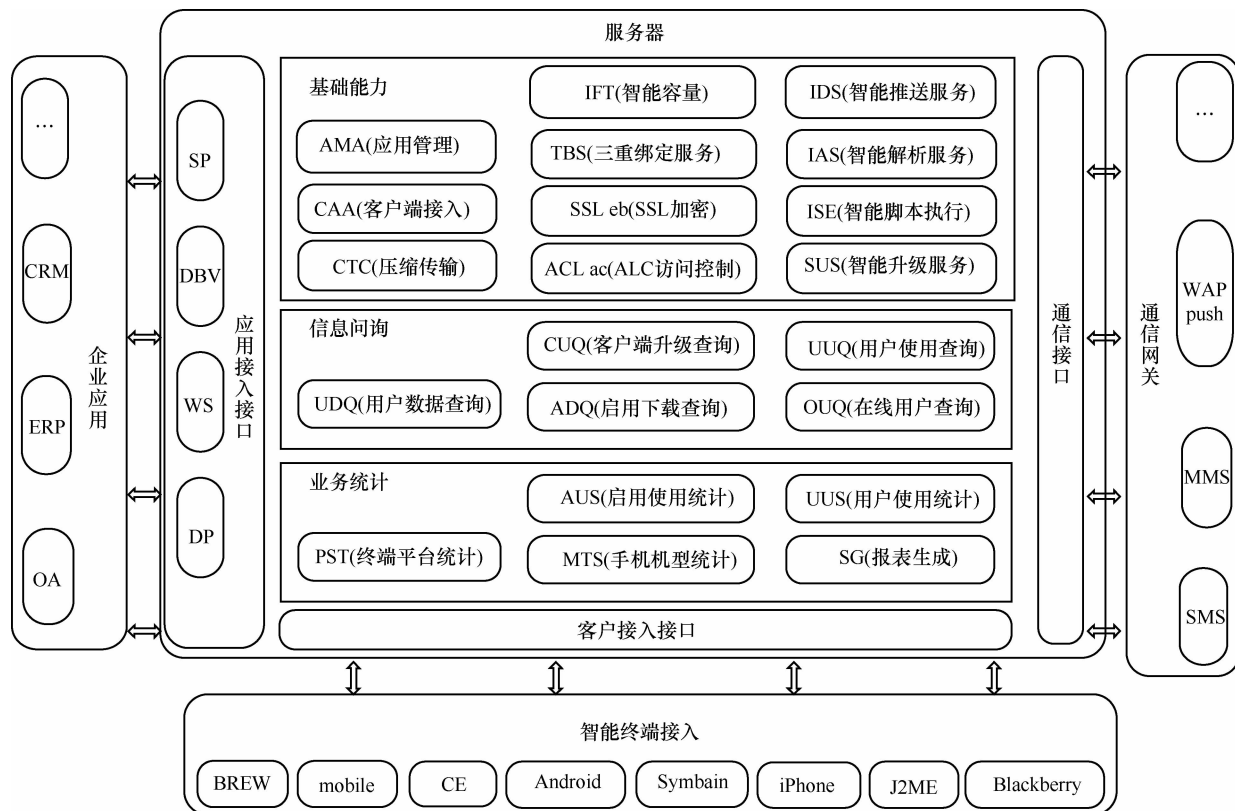


图 1 移动业务平台技术模型

了移动设备管理系统,对移动终端的系统安全及接入安全提供有力技术保障。

2.3 移动终端的选择

目前,市场上主流移动终端操作系统分为 iOS 和 Android 系统两种,两种系统均拥有完善的系统功能和庞大的市场占有率。iOS 为苹果公司开发的移动操作系统,终端包括 iPhone、iPad,用户体验优秀,系统稳定,知名度高。但由于系统封闭,程序开发难度较大,使用限制较多,终端价格较贵。Android 系统是由谷歌公司研发的开源操作系统,终端相对较丰富,遍布三星、HTC、华为技术等大型国内外移动终端制造商,选配更为灵活,但缺乏 iPhone 级别的明星产品。

由于两种系统内核结构不同,无法实现能够同时兼容两种系统的应用程序,因此移动办公终端选型格外重要。经过深入研究,最终形成了同时支持 iOS 和 Android 系统手机及平板电脑的统一方案:根据 iOS 和 Android 系统架构分别开发用户客户端,采用软证书安全认证机制,并部署移动终端管理系统,加强多系统、多终端的可管理性。

3 移动办公系统在发电集团的应用

在中国电力投资集团公司(以下简称中电投集团)移

动办公系统建设中,用户移动终端设备通过 3G、Wi-Fi 等网络介质拨入集团 SSL VPN,登录公司内网,向移动业务平台发出请求,移动业务平台将用户请求转换,与内网应用系统交互后,将返回结果传回用户客户端,完成一次移动办公的交互过程。SSL VPN、移动办公平台和内网应用系统的登录由数字证书管理与身份认证支撑平台统一管理。移动办公系统建设架构如图 2 所示。

3.1 建设范围

中电投集团建设了企业门户和公文流转移移动办公系统。企业门户系统包括重要新闻及指标数据的展示,实现对公文流转系统的单点登录及待办显示等。公文流转系统实现收文、发文等主要公文业务的审批处理。用户包括中电投集团总部全体员工,支持平板电脑及智能手机等手持设备。

3.2 SSL VPN 部署

中电投集团远程办公须通过 SSL VPN,VPN 支持移动终端设备接入,支持在 iOS、Android 系统等主流操作系统中访问。

SSL VPN 需具备支持 100 个用户并发数以上的系统性能,部署在内外网边界,同时配置内外网两个 IP 地址,通过核心交换机控制连接移动业务平台。移动终端通过访

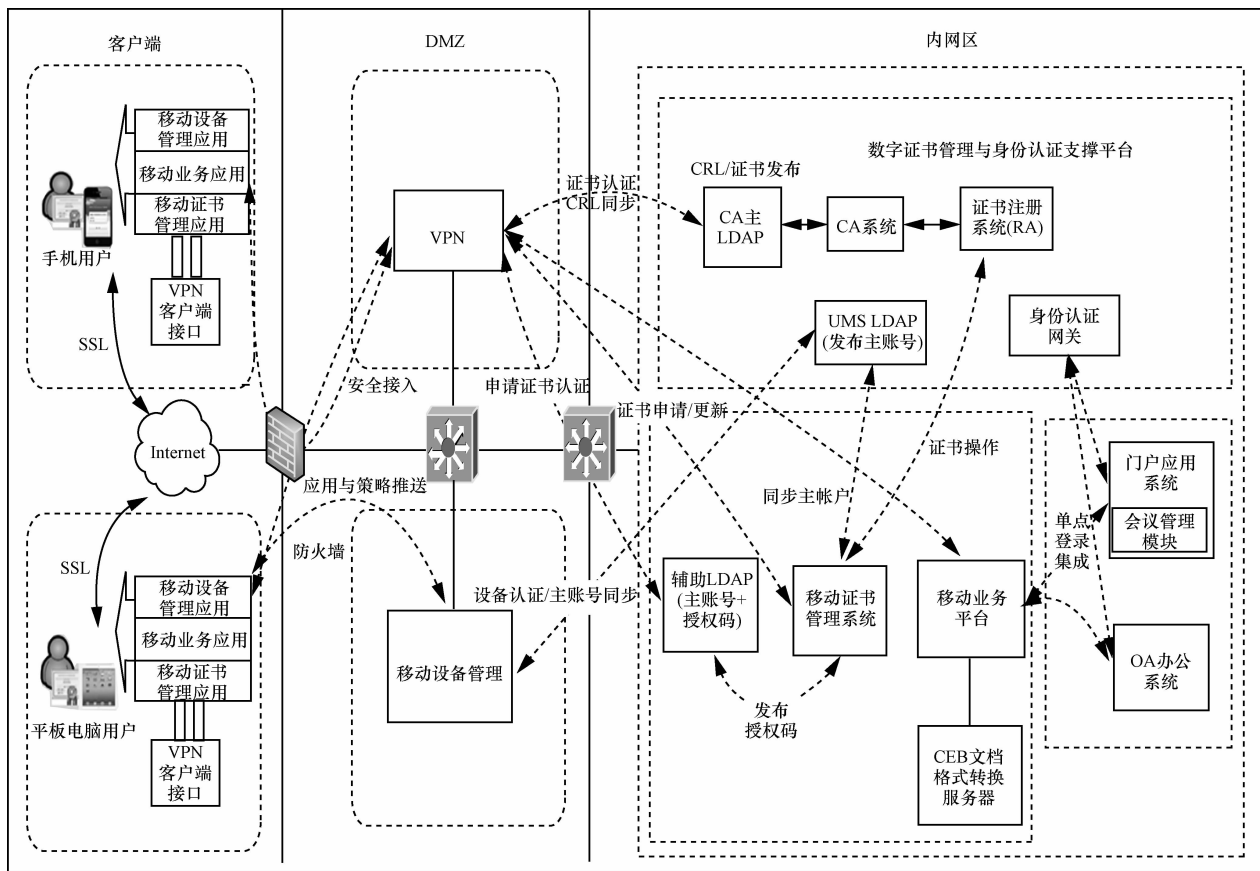


图2 移动办公系统建设架构

问其外网IP连接到VPN,VPN负责建立加密数据隧道,作为移动终端与移动业务平台交互数据的通道,加固网络传输的安全。

3.3 移动业务平台部署

移动业务平台是实现移动办公系统部署、系统访问交互的核心模块。架构上支持分布式部署,可适用虚拟化服务器,技术上遵循J2EE标准,数据存储上可通用各种关系型数据库。

移动数据平台实现各移动办公应用系统的集中发布部署与独立存储及权限管理。开发层面上,利用模板定制化快速搭建目标应用系统界面的各映射页,以XML格式存储。与目标应用系统做数据传输调用接口,以交互用户请求。

管理上,可基于应用系统实现用户管理、机构管理、权限管理、日志管理和业务管理。系统安全上,做到移动设备访问控制、停用锁止、防穷举攻击、安全审计及服务器存储的安全防护。

3.4 身份认证系统部署

根据移动终端选型确定身份证书类型。登录时,通过

数字证书管理与身份认证支撑平台验证用户数字证书身份,统一管理分配用户身份。该平台已开发完成,需要移动办公系统与其建立交互接口。数字证书存储方式分为利用电子密钥存储(硬证书)和常规存储(软证书)两种,电子密钥能够通过加密芯片对证书加密且具有PIN口令保护,因此安全性更高。数字证书应用在移动设备时,通常使用TF卡(类似手机中的SD卡)作为电子密钥。

为了实现终端身份证书的统一管理,采用软证书部署方式,并配套部署终端设备管理系统,对应用的安装使用和系统安全进行统一管理。

3.5 移动设备管理系统部署

移动设备管理(MDM)系统可支持iOS、Android系统等主流操作系统,由服务器端和客户端组成。服务器端部署在移动业务平台,提供基于Web的设备管理界面。客户端部署在移动终端设备,正确安装配置后加入中电投集团移动设备管理体系。

MDM系统可按照用户分组推算新增的企业移动应用客户端与已有移动应用的更新提醒,可推送企业内部Wi-Fi等网络配置文件,实现统一管理,简化用户使用。

MDM 系统可对用户及设备的注册和分组进行管理,辅助设备与证书的绑定,并可远程擦除挂失设备的移动应用及数据,加固系统安全。

3.6 客户端整合

系统涉及数字证书驱动、SSL VPN 客户端程序和移动办公系统客户端程序,都需要将其安装到移动终端中。经过多方的研讨和协调,形成了将 3 部分程序整合为一个移动办公客户端的整体方案,自动完成数字证书识别和 SSL VPN 的连接动作,减少用户操作复杂度,增加系统实用性,大大增强了用户体验。

3.7 安全防护

为确保移动办公业务安全可靠、内部信息安全可控、信息安全事件可追溯,按照信息系统安全等级保护基本要求(GB/T 22239-2008)第二级系统安全标准设计中电投集团的移动办公业务安全保障方案,从移动终端安全接入、移动业务平台安全开发、移动业务平台安全部署以及移动办公安全审计 4 个层面,开展移动办公业务安全保障建设,同时采取有效的移动终端遗失应急处理措施,加强移动办公业务的整体安全性,实现身份防盗用、数据防窃取、系统防入侵、遗失有准备、事件可追溯、隐私有保护六大安全目标。移动办公业务安全保障架构如图 3 所示。

移动办公业务系统第二级安全措施对照(对照标准:信息系统安全等级保护基本要求(GB/T 22239-2008))见表 1。

3.8 功能实现

实现了中电投集团企业门户和公文流转移动办公系统的基本功能,具体如下。

(1) 企业门户移动办公系统

- 新闻发布类内容:包括头条回顾、通知公告、部门简报等重要已有板块。
- 数据展示类内容:包括发电量情况、煤铝产量情况、安全监察数据及日历进度等重点数据报表展现。
- 企业通讯录:整合企业员工通讯录,方便员工查找,支持应用内直接拨打,提高办公效率。
- 电子邮件系统:集成集团公司电子邮件系统,方便员工浏览与发送邮件。
- 内容管理模块:发布公司内刊及会议资料等内容。

(2) 公文流转移动办公系统

- 公文流转审批:移植公文流转系统中主要流程的审批处理,可整合包括发文、收文、报销、合同等审批流程。
- 正文和附件查阅:可阅览多种格式的公文及附件,包括 Word 文档、WPS 文档、Excel 表单、PDF、CEB 版式文件等常见文件格式。
- 即时推送:实现基于配置推送新待办、通知或消息信息到用户终端,提高办公效率。

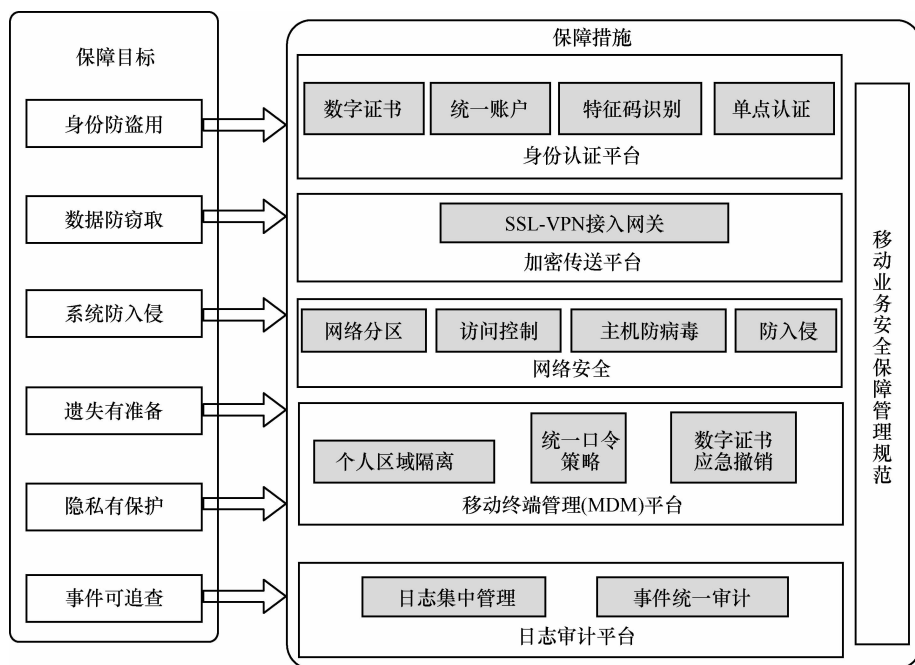


图 3 移动办公业务安全保障架构



表 1 移动办公业务系统第二级安全措施对照

等级保护二级基本要求		中电投集团移动办公安全保障措施
物理安全	物理位置选择	沿用中电投集团现有的机房保护措施
	物理访问控制	
	防盗窃和防破坏	
	防雷击	
	防火	
	防水和防潮	
	防静电	
	温湿度控制	
	电力供应	
	电磁防护	
网络安全	结构安全	单独划分移动办公网络区域
	访问控制	移动办公区与内网服务器区之间部署防火墙
	安全审计	通过 VPN 设备审计用户接入移动办公网络情况
	边界完整性检查	不适用
	入侵防范	沿用集团互联网边界的入侵防御系统为移动业务平台提供入侵防护能力
主机安全	网络设备防护	沿用集团网络系统现有防护措施
	身份鉴别	配置移动业务平台服务器的 Windows 口令策略,使用 8 位数字+字母+特殊字符口令,更改管理员账户默认用户名,关闭远程管理功能
	访问控制	关闭操作系统默认账户
	安全审计	开启操作系统日志功能
	入侵防范	安装集团终端安全管理系统,执行统一补丁管理、软件白名单管理策略
应用安全	恶意代码防护	安装集团 McAfee 防病毒系统
	资源控制	关闭操作系统远程登录
	身份鉴别	使用用户数字证书+移动设备特征码进行双重鉴别,限定证书 PIN 码尝试次数不大于 5 次,超过 5 次锁定证书
	访问控制	按照通用的系统授权模型开发移动业务平台授权功能
	安全审计	开发移动业务平台安全审计功能,审计登录用户信息、登录时间、操作内容、结果
	通信完整性	利用校验码技术保护移动业务交互数据的完整性,即防篡改
	通信保密性	利用 SSL 技术加密通过无线信道传输的信息;开发移动设备缓存区清除功能,实现移动设备不存储企业信息
数据安全及备份恢复	软件容错	开发输入信息有效性检验功能
	资源控制	开发会话自动中断功能,10 min 移动终端未响应服务器自动终端连接。限制移动办公业务平台最大并发数为 100;单用户多重会话数为 1
	数据完整性检测	利用校验码技术检测数据完整性
	数据保密性	利用 PKI 数字证书技术、SSL 技术保护鉴别信息和企业信息
	备份和恢复	不适用

· 公文查询:实现按类型、时间、标题等查询公文信息。

(1) 安全性

4 结束语

在中电投集团移动办公系统调研及开发过程中,详细地研究了适合电力企业应用的移动办公系统架构,对其中形成的有益经验进行了总结,主要体现在以下几方面。

中电投集团移动办公系统将如何保障系统安全作为最重要的考量因素,首先明确了按照信息系统安全等级保护二级要求建设系统,涉密或等级保护三级以上的信息系统,移动办公暂不支持,确保信息系统与安全保护级别一致。在方案设计及建设过程中,采用了证书身份认证、移动终端特征码匹配、信息不落地、移动设备管理

软件、移动设备防病毒软件、主账号口令及移动办公使用管理制度等多重维度的手段加固系统安全,有效地保证了信息安全。

(2) 体验性

中电投集团移动办公系统以用户体验为中心进行设计,无论技术路线、产品选型或是实施方案,都以增强系统用户体验为最终目的。在设计及实施过程中摸索形成的集 VPN 连接、证书身份认证、主账号密码认证、特征码匹配认证、企业门户及公文流转系统单点登录等功能于一体的应用程序设计思路,最大程度上解决了用户体验与安全性之间的矛盾性,即在满足高安全性的前提下简化用户操作步骤,易于上手使用。在系统功能及 UI 设计上,也以用户使用方便、简洁明了及响应速度快为最优考虑因素,并全面支持了目前市场主流的手机及平板电脑,系统自正式运行起,便获得了用户的一致好评。

(3) 扩展性

中电投集团移动办公系统以扩展性为系统架构设计的核心要素,将来不仅可以在移动平台中部署其他应用系统,以满足用户更深层次的办公需求,而且系统本身也可以快速适应 iOS 及 Android 系统的新版本,自动适配尺寸更大、分辨率更高的新移动终端,且提出了应用接入规范,

制定了持续完善滚动更新的机制,确保了中电投集团移动办公系统在未来仍然可以拥有较好的兼容性和先进性。

参考文献

- 1 陈静.移动办公与管理.北京:对外经济贸易大学出版社,2012
- 2 冯登国. PKI 技术. 北京:科学出版社,2008
- 3 苹果公司. iPad 企业应用,2011

[作者简介]



刘铮,男,中国电能成套设备有限公司工程师、信息化主管,主要研究方向为信息化系统建设与管理。



王静,女,中国电力投资集团公司高级工程师、处长,主要研究方向为大型发电集团信息化管理与建设,包括总体规划、方案设计、应用系统开发和部署、基础设施建设、运维管理、安全体系建设等。

(收稿日期:2013-08-01)

(上接第 114 页)

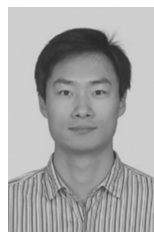
参考文献

- 1 Rhee I, Shin M, Hong S, *et al.* On the levy walk nature of human mobility. *Networking*, IEEE/ACM Transactions on, 2011(3)
- 2 Yang B, Duan W Q, Chen Z. New method to estimate scaling of power-law degree distribution and hierarchical networks. *Applied Mathematics and Mechanics*, 2006, 27(11):1475~1479
- 3 葛玉伟,周战,陈万田.洪泽地区配电网故障幂律分布特性.现代电子技术, 2011,34(6):172~174
- 4 Chris A. The Long Tail. CITIC Publishing House, 2005

[作者简介]



王冠男,女,现就职于北京国电通网络技术有限公司,主要从事大数据分析和挖掘工作。



邓春宇,男,北京国电通网络技术有限公司工程师、部门副总经理,主要从事大数据在电力行业中的应用与实践研究。



赵悦,女,现就职于北京国电通网络技术有限公司,主要从事大数据分析和挖掘工作。

郑亚芹,女,现就职于北京国电通网络技术有限公司,主要从事大数据分析和挖掘工作。

(收稿日期:2013-08-01)