

目 录

行业动态

- 1 中国人民银行高度关注美信用卡资料外泄波及中国持卡人事件 等

热点聚焦

- 5 解读《中国农业银行科技创新工程 2005—2007 年行动计划》

本刊编辑部

独家专访

- 8 中钞丰盛进军金融机具市场

庞瑞江 李 玮

金融业 IT 服务管理

- 11 集中用户管理在金融行业的应用

沈 鸥

管 理

- 15 试论工商银行的 IT 审计
18 基层银监局科技工作中存在的问题及对策
21 商业银行科技开发及创新机制的研究
25 会计集中核算系统安全运行的保障措施
28 数据仓库技术在工程建设项目管理中的应用
30 联行业务存在的风险因素与整改措施
32 银行业计算机安全问题与防范措施

孟军强 荆 东
王锁平 刘 江
徐占海 钱 斌
熊育彦
杨 莉 韩智勇
李毅恒
郑建明

技 术

- 35 国外核心银行软件包在内部控制方面的设计
38 商业银行资金信息管理系统的设计与分析
43 典型网络边界冗余设计实例分析
46 Unix 系统 root 用户管理的深入分析
48 银行业信息系统容灾技术初探
50 牡丹社保 IC 卡在 CITE 系统中的应用
52 中国银行授信决策核批系统
54 Translation-rule 命令在 VoIP 中的应用
57 企业信息集成技术在银行业中的应用
59 BP 神经网络在银行贷款分类中的应用

丁 磊
吴文忠
敦宏程
蒋志渊
施闻捷
庄伟雄 刘荣斌
杨向东
陈 磊
郑文峰
梁毅冬



中钞丰盛进军金融机具市场



“网上银行与信息安全”
高峰论坛摘要



2005年第7期(总第192期)

联合创办单位

中国人民银行 中国保险监督管理委员会
中国工商银行 中国农业银行
中国银行 中国建设银行
交通银行 中国人民保险公司
中国人寿保险公司 中国再保险公司
国家外汇管理局 信息产业部

编辑委员会

(以姓氏笔画为序)

顾问: 王新文 文四立 乔林 刘梅生
李仁杰 李早航 张建国 陈元
陈静 何如 吴建 吴小平
张琪 武青 郑之杰 洪崎
姚定一 唐建邦
主任: 张衡
副主任: 林晓轩
编委: 马鹏飞 王云生 文四立 冯菊平
成小平 刘安林 刘贵生 刘政权
朱宏玲 李坚 李政朝 陈皓
陈静 陈天晴 陈增圭 佟建民
张宏 张益民 林丽 单怀光
赵军 赵小凡 侯维栋 奚力铭
徐连峰 徐雅萍 顾冠群 贾振陆
黄巍 曹谷崖 程卫 覃孟征
韩玮玺 蒋国强 傅晓阳

社长: 林晓轩

副社长兼总编辑: 程卫

副总编辑: 张宏

总审: 董芳明

执行主编: 庞瑞江

市场部主任: 李勇

发行: 刘红秀

法律顾问: 王春艳

主办: 中国工商银行

编辑出版: 中国金融电脑杂志社

总机: 66109433 传真: 66109434

编辑部: 66109423

网址: <http://www.fcc.com.cn>电子邮件: pubsh@fcc.com.cnfcc@icbc.com.cnchinafcc@263.net

地址: 北京市海淀区翠微路15号(100036)

发行范围: 公开发行

发行日期: 每月15日出版

中国标准连续出版物号: ISSN 1001-0734

CN 11-2623/F

邮发代号: 82-368

广告许可证: 京海工商广字0171号

印刷单位: 北京国彩印刷有限公司

定价: 15.00元

目 录

自由论坛

- 63 “网上银行与信息安全”高峰论坛摘要 本刊编辑部
66 我国市政债券的发展研究 杨娟
71 综合柜员操作风险防范 柏燕
74 报账易产品的设计与实现 荣卫民 张继年
77 电子商务社群与产业门户 高明
79 学习力: 商业银行提升竞争力的根本 刘向东
82 新型网上支付工具及其支付流程 胡秋灵 王哲

IT 资讯

- 86 自组 VoIP: 河北中行评点华为 3Com 模式
——中国银行河北分行率先实现 VoIP 组网的决策分析
89 温州建行: 巧用 Windows 终端解决四大问题 陈跃等
91 基于数据仓库的客户关系管理
——NCR Teradata CRM 解决方案
93 SCO OpenServer 下的通用 USB 驱动软件包研发成功 等

编读互动

- 96 数据集中也要讲究集约化 李虎柱

广告要目

- | | |
|-------------------------|------------------|
| 封面: 江苏国光信息产业股份有限公司 | 彩插: 深圳市费能克科技有限公司 |
| 封二: 华为 3com 技术有限公司 | 中国财经界 |
| 封三: “金融业 IT 服务管理”专栏征稿启事 | 广州广电运通金融电子有限公司 |
| 封底: 山东弘业智能控制技术有限公司 | 南京富士通计算机设备有限公司 |
| 彩插: 迪堡中国 | CSB 电池 |
| 联想国际 | 首都金融文化节暨北京国际金融 |
| OKI 冲电气实业(深圳)有限公司 | 投资理财博览会预告 |
| 研祥智能科技股份有限公司 | 征订启事 |
| NCR Teradata 数据仓库事业部 | 北京鑫博恒力科技有限公司 |
| 深圳紫金支点技术股份有限公司 | 深圳市证通电子有限公司 |

CONTENTS

Financial News

- 1 The people's Bank of China paying highly attention to the affair of American credit card information betraying affecting China cardholders, etc.

News Focus

- 5 The outline of *The 2005-2007 Implementation Plan of Technology Innovation Project in ABC*

Exclusive Interview

- 8 CBPM-SMI entering the market of financial equipment

IT Service Management in FSS

- 11 Application of centralized user management in financial industry

Management

- 15 Discussion on IT audit of ICBC
18 Matter and countermeasure of technology work in basic branches of banking regulatory bureau
21 Research of technology development and innovation mechanism in commercial banks
25 Ensuring measure of security running of centralized accounting book system
28 Application of data warehouse in engineering item management
30 Risk factor and correction measure for inter-banking business
32 Computer Security and prevention measures in banking

Technology

- 35 Design of internal control for overseas core banking software package
38 Analysis and design of fund information management system in commercial banks
43 Case analysis of boundary redundancy design in representative network
46 Deep analysis of root user management in Unix system
48 Primary probe of IT system disaster backup in banking
50 Application of IC of peony social security in CITE system
52 Award credit decision authorization system in Bank of China
54 Application of Translation-rule command in VoIP
57 Application of EII in banking
59 Application of BP nerve network in loan Classification of banking

Free Forum

- 63 Summary of "online banking and information security" forum
66 Research of development of China city administration bond
71 Operation risk avoidance for integrated teller
74 Design and implementation of easy reimbursement product
77 E-business community body and industry port
79 Learning capability: fundament of advancing capacity of competition in commercial banks
82 New online payment tool and it's payment flow

IT Information

- 86 Hebei branch of Bank of China commenting Huawei-3Com mode
89 Using skillfully Windows terminal resolving four great matter in Wenzhou branch, CCB
91 Solution of NCR Teradata CRM
93 Universal USB driving software packet under SCO OpenServer developed successfully, etc.

Interaction

- 96 Intensive management is also important in data centralization



Co-sponsors

The People's Bank of China
China Insurance Regulatory Commission
Industrial and Commercial Bank of China
Agricultural Bank of China
Bank of China
China Construction Bank
Bank of Communications
The People's Insurance Company of China
China Life Insurance Company
China Reinsurance Company
State Administration of Foreign Exchange
Ministry of Information Industry

Editorial Committee

Advisors:

Wang Xin Wen Sili Qiao Lin Liu Meisheng
Li Renjie Li Zaohang Zhang Jianguo Chen Yuan
Chen Jing He Ru Wu Jian Wu Xiaoping
Zhang Qi Wu Qing Zheng Zhijie Hong Qi
Yao Dingyi Tang Jianbang

Director: Zhang Qu

Vice Director: Lin Xiaoxuan

Members:

Ma Pengfei Wang Yunsheng Wen Sili Feng Juping
Cheng Xiaoping Liu Anlin Liu Guisheng
Liu Zhengquan Zhu Hongling Li Jian Li Zhengchao
Chen Hao Chen Jing Chen Tianqing Chen Zenggui
Tong Jianmin Zhang Hong Zhang Yimin Lin Li
Shan Huaiguang Zhao Jun Zhao Xiaofan
Hou Weidong Xi Liming Xu Lianfeng Xu Yaping
Gu Guanqun Jia Zhenlu Huang Wei Cao Guya
Cheng Wei Qin Mengzheng Han Weixi
Jiang Guoqiang Fu Xiaoyang

President: Lin Xiaoxuan

Vice President & Editor-in-chief: Cheng Wei

Deputy Editor-in-chief: Zhang Hong

Senior Editor: Dong Fangming

Executive Editor: Pang Ruijiang

Advertisement Director: Li Yong

Circulation: Liu Hongxiu

Legal Adviser: Wang Chunyan

Sponsor: Industrial and Commercial Bank of China

Layout & production: China Finance Computer Journal Press

Phone/Fax: (8610)66109433 (8610)66109434
(8610)66109423

Website: <http://www.fcc.com.cn>

E-mail: pubsh@fcc.com.cn

fcc@icbc.com.cn

chinafcc@263.net

Address: No.15, Cuiwei Road, Haidian District, Beijing, 100036, P.R.C.

中国人民银行高度关注美信用卡资料外泄波及中国持卡人事件

本刊讯 美国 MasterCard 国际组织 6 月 17 日宣布,卡系统公司 (CardSystems Solutions, Inc.) 的系统被黑客侵入,造成包括 MasterCard、VISA、American Express 和 Discover 在内的高达 4000 多万用户的数据资料被窃,其中 MasterCard 信用卡用户 1390 万, VISA 信用卡的用户 2200 万。

针对美国信用卡资料外泄波及中国持卡人事件,中国人民银行支付结算司负责人近日表示,中国人民银行高度关注美信用卡外泄波及中国持卡人事件,已要求相关的信用卡国际组织妥善处理中国持卡人信用卡信息泄露问题。

中国人民银行还要求国内的各发卡机构、银行卡清算组织以及提供银行卡数据处理的第三方服务机构要切实加强管理,采取有效措施,确保银行卡持卡人的信息安全。

建设银行启动应急程序 避免客户损失

本刊讯 美国 CardSystems 信用卡数据遭黑客侵入事件发生后,建设银行信用卡中心立即启动应急程序,与 VISA、MasterCard 国际组织保持密切联系,并要求相关国际组织立即提供有关持卡人名单。6 月 20 日,在得到了相关国际组织发来的曾经去过美国、使用过建行龙卡(双币种)贷记卡的持卡人名单后,建设银行迅速联系名单上的客户,并立即为其办理免费换卡手续:新卡通过特快专递寄出,将影响客户用卡的因素降到最低;对一时联系不到的客户,先行对客户卡片进行锁卡,并继续努力与客户联系、及时处理;一些客户表示目前正在境外并还正在使用银行卡,建设银行则通过交易监控关注持卡交易,和客户保持联系。

工商银行积极迅速采取措施 有力保护持卡人资金安全

本刊讯 根据有关国际信用卡组织的风险通报,美国发生的信用卡交易信息失窃事件使国内各发卡银行也不同程度地受到一些影响。在目前发行的牡丹国际卡当中,发生磁条信息泄漏的有几百个,但这些卡片暂未发现有资金损失的情况。

为避免欺诈损失发生,最大限度地保护持卡人的利益,工商银行牡丹卡中心在接到有关国际信用卡组织的通报后,立即采取果断措施,对此次发生信息泄露的卡片逐一确认,及时处理。一是通过手机、电话、信函等方式,在第一时间联系到持卡人,向其通报有关情况,并免费为其更换新卡;二是通过最近一期的对账单,就有关情况进行说明,提醒近期在美国用过卡的持卡人注意防范。三是积极与有关国际信用卡组织沟通情况,跟踪事态进展,随时准备采取进一步的应对措施。

据了解,针对卡片信息泄露问题,牡丹卡中心近年来已经建立起一套严密的风险防范体系和快速反应机制,从系统监控、管理制度和处理流程上,努力保障持卡人的用卡安全。今年以来,牡丹卡中心已多次收到 MasterCard、VISA 等国际组织发来的卡片信息失窃风险通报,均已及时通知持卡人并为其免费止付换卡,截至目前已止付约 1500 余张卡片。

中国银行启动应急程序 保护持卡人利益

本刊讯 6 月 23 日,中国银行新闻发言人王兆文表示,美国 CardSystems 信用卡数据遭黑客侵入事件发生后,中国银行已在第一时间从 VISA、MasterCard 国际组织获得可能受侵的中银信用卡和长城国际信用卡的卡号表单,并立即对之进行核实,目前还没有发现中行的信用卡客户遭受损失。

王兆文介绍说,中国银行本着最大限度保护持卡人利益的原则,根据从国际组织获得的可能受侵的中行信用卡客户名单,迅速联系客户、通报有关情况,为其免费更换新卡。对暂时联系不到的客户,先行对客户卡片进行冻结,并继续努力与客户联系、及时处理。同时,中国银行利用强大的欺诈侦测系统,加强对所有近期在美国地区使用过中行信用卡的客户的卡片交易进行监控,一旦发现可疑交易,立即与持卡人联系确认,避免欺诈损失的发生,保护持卡人的权益。

王兆文还表示,中国银行将继续关注该事件的进展,妥善做好后续跟进工作。

中国人民银行积极推动跨区域票据交换

本刊讯 近日,中国人民银行副行长苏宁在出席京、津、冀跨区域票据自动清分系统运行仪式时指出,要充分认识建立票据跨同城区域交换、扩大支票使用范围、促进支票使用和流通的重大意义;积极稳妥地做好支票截流试点工作,为扩大支票使用范围探索新的途径;要为扩大票据交换区域创造良好的法律环境和社会信用环境,推动我国非现金支付工具的使用。

苏宁表示,京津冀跨区域票据自动清分系统的正式运行,是人民银行推动票据跨同城区域交换的又一重大探索,对扩大支票使用和支持区域经济发展具有十分重要的意义。

苏宁指出,票据作为重要的非现金支付工具,在我国经济生活中发挥着不可替代的重要作用。票据业务的发展对于减少现金流通、降低交易成本、培育信用观念、加强反洗钱和促进经济发展意义重大。其中,支票以其携带方便、支付便捷、费用较低、流通性强等优点,受到了企事业单位和个人的普遍欢迎,在支付结算业务中占有了相当大的比例。但是,长期以来,由于种种条件制约,我国的支票基本上只能在同城范围内使用,在社会主义市场经济发展的今天,这已远远不能适应经济社会发展和人们生产生活的需要。一个城市、一个地区的经济要发展,就必须积极参与专业化分工,融入全国统一的大市场,甚至加入全球化进程;就要推动物资和人员的跨城市、跨地区流动。物流和人流的增长,极大地促进一个城市、一个地区的经济发展。因此,打破支票在同城范围内使用的限制,逐步实现支票在全国范围内流通使用势在必行。

全国城市商业银行工作会议 暨城市商业银行发展论坛第六次会议在深圳召开

本刊讯 全国城市商业银行工作会议暨城市商业银行发展论坛第六次会议 6 月 22 日在深圳召开,会议总结了城市商业银行 10 年发展的经验教训,就城市商业银行下一步监管工作和发展重点作了部署,中国银监会副主席唐双宁参加会议并发表了讲话。银监会有关部门负责人、各银监局分管局长、城市商业银行监管处室负责人、113 家城市商业银行董事长和行长参加了会议。

自 1995 年国务院决定在大中城市组建地方股份制性质的城市商业银行以来,全国共有 100 多家城市商业银行相继开业。截至 2004 年末,全国共有城市商业银行 113 家,资产总额达 16 938 亿元,其中各项贷款 9045 亿元;负债总额达 16 361 亿元,其中各项存款 14 341 亿元;当年实现利润 82 亿元;所有者权益 577 亿元。

唐双宁对城市商业银行的 10 年发展给予了高度评价,他分析了城市商业银行当前面临的形势,并对今后的发展提出了具体的指导意见。唐双宁指出,城市商业银行十年间有效地控制和化解了数千家城市信用社积累的金融风险,并凭借灵活的机制和高效的决策进入市场,优化了银行业资源配置,为 100 多个中心城市经济发展和社会稳定做出重要贡献。目前,城市商业银行的市场信誉稳步提高,在支持地方经济发展中的作用越来越大,已经成为银行体系中最具生机和活力的群体之一,对于深化我国的金融体制改革,完善我国金融组织体系,支持中小企业,促进地方经济发展,特别是对防范和化解城市信用社的金融风险,具有重要历史意义。10 年来,城市商业银行为我国中小商业银行发展积累了丰富的经验,那就是,防范风险是生存基础,体制、机制转变是关键,明确市场定位是前提,地方政府的支持是防范和化解金融风险的重要条件,有效监管是稳健发展的保证。

交通银行在香港成功上市

本刊讯 6 月 23 日,市场追捧的“海外银行第一股”交通银行在香港联交所挂牌交易,代码为 3328。据香港联交所的消息,交通银行股票开市报 2.8 元,其后在 2.8~2.9 元之间徘徊,最终报收于 2.825 元,较招股价 2.5 元上涨 13%,全天共成交 51.6 亿元。

交通银行于 6 月 13 日在香港公开招股,6 月 18 日确定发行价为每股 2.5 港元,发行市盈率为 14.8 倍,预计将筹资约 146.6 亿港元,高盛和汇丰控股为其上市保荐人。

交行公开发售部分获得 205 倍超额认购,冻结资金近 1500 亿港元,国际配售部分获得 20 倍超额认购。

刘明康强调:监事会要围绕银行业案件治理 深入开展监督检查工作

本刊讯 日前,银监会召开国有重点银行业金融机构监事会案件治理工作会议,介绍当前银行业案件治理的形势、任务以及工作进展情况,重点传达国务院领导关于银行业案件治理工作的重要指示精神,对监事会围绕银行业案件治理开展监督检查进行了研究和部署。银监会主席、党委书记刘明康出席会议并讲话。

刘明康指出,银行业案件治理工作不仅关系到金融机构的改革和发展,也关系到国家金融安全和社会稳定。国务院领导同志对银行业案件治理工作高度重视,多次听取汇报并做出重要指示,各监事会要深入学习领会国务院领导同志指示精神,充分认识做好银行业案件治理工作的重要性;要紧紧围绕当前银行业案件治理工作,强化责任意识,加大专项检查和调研力度;要进一步明确工作目标、理清工作思路,充分发挥自身优势和独特作用,深入开展监督检查,坚决遏制银行业案件上升的势头。

刘明康强调,监事会和银监会监管部门要加强沟通协作,相互配合,充分发挥两支力量在银行业案件治理工作中的优势,形成监管合力。刘明康指出,监事会要认真研究深入开展监督检查工作的着力点和切入点,发挥优势,精心组织,部署安排好下半年的专项检查和调研工作。

国务院派驻国家开发银行等11家国有重点金融机构监事会主席和专职监事,中国银行、中国建设银行、交通银行的监事长和专职监事以及中央汇金公司主要负责同志等也参加了会议。

人民银行与教育部联合开展大学生征信与相关金融知识讲座

本刊讯 为普及金融知识,推动征信体系建设,2005年6月5~16日,中国人民银行与教育部联合在北京、西安、武汉、上海四地选择了九所高校,开展题为《珍爱信用记录,享受幸福人生》的大学生征信与相关金融知识讲座。

征信体系是现代金融体系运行的基石。有无健全的征信体系,是市场经济是否走向成熟的重要标志。就企业征信而言,银行信贷登记咨询系统已稳定运行6年多,对防范企业信用风险发挥了重要作用。为更好地满足商业银行信贷风险管理需要,目前人民银行正在对该系统进行升级改造。就个人征信而言,全国统一的个人信用信息基础数据库已于2004年12月中旬在北京等七个城市试运行,目前正逐步向全国推广,计划于2005年底实行全国联网运行。现阶段该数据库的数据主要来源于商业银行,采集的信息包括借款人和信用卡持卡人的基本信息和信贷信息,学生助学贷款的信息也包括在内,其偿还情况将反映在学生的信用报告中。

首场讲座于6月5日晚在中国人民大学举行,并受到了该校领导的高度重视和学生的热烈欢迎。中国人民大学党委副书记王新清说:“信用是要用制度来保证的,对大学生开展征信与相关金融知识教育非常及时”。

中国人寿 CBPS8 版综合业务处理系统在广西全辖成功上线

近日,经过中国人寿股份总、分公司相关部门的紧密配合、精心组织、反复测试、科学安排,在充分准备和保障安全的前提下,中国人寿广西区分公司在全辖同时上线 CBPS8 版综合业务处理系统获得成功,这在中国人寿后援系统建设的历史上是一次创新和突破。

CBPS8 是中国人寿核心运营系统(CCOS)的重要组成部分。它的成功上线,是中国人寿后援系统建设进程中一件具有里程碑意义的大事。中国人寿广西分公司作为中国人寿全国首家全辖同时上线的推广单位,为中国人寿下半年在全国进行系统推广坚定了信念、积累了经验、做出了贡献。

(中国人寿保险股份有限公司信息技术部 张琼之)

建设银行首家推出网上银行动态口令刮刮卡

本刊讯 近日,建设银行在全面分析现有网上银行安全手段、充分考虑客户使用习惯的基础上,在国内首家试点推出了动态口令刮刮卡。该业务已在辽宁、浙江、宁波三个分行试点,待条件成熟时将向全国推广。

动态口令是一种动态密码技术,简单地讲,就是客户使用不同的一次性密码进行身份认证和交易确认。建设银行此次推出的网上银行动态口令刮刮卡是一种大小、形状与银行卡类似的卡片,每张刮刮卡上覆盖有45个不同的密码。客户在使用网上银行过程中,需要输入交易密码时,只需按顺序输入刮刮卡上的密码,每个密码只可以使用一次。据了解,此次建设银行率先在国内试点推出的刮刮卡,是专门针对网上银行个人客户的需要设计开发的。

工商银行五月份 ATM 交易量再创新高

本刊讯 随着全辖ATM布放的不调整,工商银行ATM布局日趋合理、更加方便使用。五月份,工行全辖ATM各项运营指标显著提升,ATM单机日均交易量达237笔,单机日均交易金额达到7.6万元,再创历史新高;存取款一体机和存款机受理存款交易量也不断上升,达到259万笔,存款交易金额达37.5亿元。

国家外汇管理局召开外汇反洗钱工作情况银行通报会

本刊讯 近日,国家外汇管理局召开外汇反洗钱工作情况银行通报会,16家中资外汇指定银行代表参加了此次会议。

国家外汇管理局副局长邓先宏出席会议并讲话。他通报了两年来外汇反洗钱工作情况及今后的工作安排和设想,希望并要求银行今后继续支持配合外汇领域反洗钱工作。

会议还分别就银行外汇反洗钱数据报送及信息利用情况和外汇反洗钱信息系统开发推广情况进行了介绍。

本刊讯 日前,伴随着个人负债及相关系统数据已上收的最后一家分行河北分行的上线成功,中国农业银行2005年全国数据集中工程四大目标之一的“六行一部”(北京、天津、河北、吉林、海南、青海和总行营业部)新一代综合业务系统版本升级工作宣告完成。

据悉,在实施全国数据集中工程的初期,由于一定的原因造成了农总行运行中心有两套应用系统并行的情况,一套“六行一部”使用,另一套广东和大连分行使用。因此,为了给全国数据集中工程建设创造更好的上收环境,首先就必须实现总行运行中心应用系统版本的统一,将并行的两套应用系统合并,即将已经上收的“六行一部”的新一代综合业务系统统一升级到最新版的系统——广东和大连分行已经使用的版本上来。因此,在年初制定的全国数据集中工程建设目标时,该项工作被确定为2005年全国数据集中工程建设的目标之一。

农行实现全国数据集中工程阶段目标

建设银行与美洲银行在北京隆重签署战略投资与合作协议

本刊讯 6月17日,建设银行和美洲银行于北京共同宣布,双方签署了关于战略投资与合作的最终协议。根据协议,美洲银行将分阶段对建设银行进行投资,最终持有股权可达到19.9%。首期投资25亿美元购买中央汇金投资有限公司持有的建设银行股份,第二阶段将在建设银行计划的海外首次公开发行时认购5亿美元的股份,未来数年内美洲银行还可增持建设银行股份至19.9%。这项交易是迄今为止外国公司对中国公司的最大的单笔投资。

作为整个交易的一部分,建设银行和美洲银行还签署了战略合作协议,美洲银行将在众多领域向建设银行提供战略性协助。这些领域包括公司治理、风险管理、信息技术、财务管理、人力资源管理、个人银行业务(包括信用卡)以及全球资金服务等。根据协议,美洲银行将在建设银行董事会中拥有席位,同时还向建设银行派遣大约50名人员在以上领域提供咨询服务。

编者按:一直以来,中国农业银行的科技发展和信息化建设是行业内关注的重点。然而,正如农业银行科技部某位负责人所言,长期以来农业银行并不善于宣传自己,这也为农业银行的信息化建设,尤其是总行层面的信息化战略规划蒙上了一层神秘的面纱。2004年底《中国农业银行科技创新工程2005~2007年行动计划》正式出台,为未来三年农业银行的科技工作提供了指导性文件。本刊将通过系列报道的形式解读中国农业银行未来一段时间内信息化建设的总体构想和具体措施,帮助关心农业银行信息化建设和股份制改造的读者了解相关的信息。

解读《中国农业银行科技创新工程 2005~2007年行动计划》

本刊编辑部

特殊背景下出台的行动计划

中国农业银行的电子化建设“十五”发展规划将于2005年结束,随后即将启动信息化建设“十一五”发展规划,因此2005~2007年正处于两个五年规划之间的过渡时期。正是基于这种情况,2004年初农业银行领导提出科技创新工程不能局限于“十五”规划的内容,而是应该集中精力,紧紧围绕今后一段时期全行工作的中心任务,充分发挥科技作为第一生产力的先导作用,重点解决制约农业银行改革和发展的突出问题。与此同时,农业银行将科技创新工程列为全行四项基础性战略工程之一,并做出了动员全行力量,集中优势资源加速推进,利用三年时间力争赶上国外同业信息化建设先进水平,全面提升农业银行综合竞争实力的重大战略决策。

据介绍,科技创新工程涉及农业银行全行上上下下、方方面面,是一个庞杂的系统工程,也是农业银行今后一个时期的重点工作之一。为此,农业银行主管科技工作的唐建邦副行长于2004年4月底组织召开了由研究室、科技部、人事部、财务会计部和软件开发中心负责人及相关人员参加的会议,就如何启动科技创新工程进行了专题研究,确定了课题研究的组织、原则和思路。

在随后的四个月时间里,课题组制定了工作方案,迅速启动了课题研究。根据《中国农业银行2005~2007

年改革规划》对科技发展的需求,课题组在收集和研究国内外同业相关资料,深入调查并召开多层面的座谈会,认真分析农业银行科技创新环境现状的基础上,形成了《中国农业银行科技创新工程课题研究报告》。

课题组经过认真分析研究,把提高农业银行科技创新能力作为科技创新工程的主要目的,即通过实施科技创新工程,使农业银行科技发展战略的规划和实施能力、金融产品的快速开发和部署能力、信息资源的快速获取和综合应用能力、客户关系管理能力以及生产运营管理能力等都得到极大提升,农业银行内部的管理决策人员和一般用户,外部的客户、合作伙伴以至监管当局,都将从中受益。

科技创新工程的具体受益方包括:内部各级管理决策人员将可以看到及时、准确、完整的经营管理信息,据以进行分析并做出决策,支持企业目标的实现;分布于各个部门的各类工作人员,将借助于科技手段提高企业的工作效率,形成相互关联的流程,在整个价值链上把企业贯穿起来,实现管理水平的整体提高;外部客户受益于农业银行的综合服务和客户关系管理,获得多渠道、分层次、个性化的金融服务;合作伙伴将分享农业银行网点优势和网络优势相结合的巨大竞争优势,与农业银行共同成长;农业银行日益提高的盈利能力、风险管理能力和信息披露透明度,有助于监管当局加快推进国有商业银行金融体制改革步伐。

正确认识成果与差距

在《中国农业银行科技创新工程课题研究报告》中,农业银行的管理人员、研究人员和科技人员重点分析了农业银行在基础技术平台建设方面取得的主要成果。在“十五”以前,农业银行电子化建设经历了微机、县域网、城市综合业务网络等阶段,整体上未形成全行性的基础技术平台,科技竞争所形成的优势仅限于局部地区和个别应用。2001年农业银行党委提出了建设全国数据中心的“十五”规划目标,这是农业银行建设全行性基础技术平台的开始。经过三年多的努力,到2004年第一步目标已经顺利实现。这主要体现在以下几个方面。

(1)全行网络结构得到了统一和简化。农业银行全国36个省域数据中心全部建成。原来分散在二级分行、县级支行和营业网点的核心业务数据集中到了36个省域数据中心,形成了一个以36个省域数据中心为节点、以总行为交换中心的相对稳定的全国性网络。

(2)核心业务系统得到了整合和统一。原来独立发展起来的对公、储蓄、信用卡、国际业务等各类业务系统统一到了新一代综合业务系统和国际业务系统;柜台终端、自助设备、网上银行、电话银行、客户服务中心等服务渠道统一集成到综合应用前置平台进行管理;以综合业务系统和综合前置系统为核心的金融服务系统基础技术平台已经基本成型。

(3)产品渠道应用支撑环境初具规模。以综合应用前置系统为主体,中间业务平台已在大部分分行投入使用,渠道整合平台正在江苏分行进行试点,更新一代的中间业务产品开发和运行支撑环境即将在广东上线。这些软件系统的研发推广,为完善产品渠道应用支撑环境奠定了基础。

(4)集中式信贷管理系统顺利推广应用。集中式信贷管理系统的全面推广,为农业银行在开发和应用大型管理信息系统方面积累了宝贵的实践经验。综合办公系统在部分分行的一定范围内先后得到应用,启动了 workflow 应用的进程。部分分行发挥省域集中的数据优势,在数据仓库和经营分析方面开展了积极的试点。

(5)全国数据集中工程正在稳步推进。总行数据中心已先后逻辑上收了青海、天津、海南、北京、大连、吉林

分行和总行营业部的数据,且运行良好。原型试点工程对优化和改造综合应用系统、加速全国数据集中工程发挥了积极作用。适应全国数据集中的新一代综合业务系统正在抓紧改造和优化。

以36个省域数据中心全面建成为标志,农业银行全行性的基础技术平台初步形成,技术环境得到较大改善,生产运行安全性、稳定性有了很大提高,明显缩短了全行性金融产品的研发和部署周期,初步缓解了经营管理信息不对称的局面,增强了全行一体化营销和服务的能力,把农业银行的综合竞争力提升到了一个新的水平,带动了全行业务的发展和经营管理水平的提高。

但是,农业银行的科技工作者也认识到,缺乏一个统筹业务需求的部门,没能形成一个清晰、完整的业务架构和应用架构,导致技术架构不完整,信息系统基础架构较为薄弱,基础技术平台难以适应业务发展创新的需要。这种差距主要体现在:全国数据集中的基础技术平台尚未形成;全国计算机网络的灵活性、开放性不足;全行性应用的集成度偏低;不能支持以客户为中心的营销和服务;经营管理信息系统的基础设施薄弱等。

四个转变与五大目标

在《中国农业银行科技创新工程2005~2007年行动计划》中确定了科技创新工程的总体思路:必须适应当前农业银行改革与发展的要求,以全国数据集中工程建设为主线,以市场为导向、以客户为中心、以效益为出发点,利用三年时间,整合和完善信息基础技术平台,建立健全科技创新工作体系,基本完成科技体制的改革,基本建立起新型的运作机制,实施信息化人才发展战略,使科技创新能力成为农业银行在国内外金融市场取得竞争优势的主要源泉,成为推进农业银行向科技先导型现代商业银行发展的不竭动力。通过科技创新行动计划的实施,充分发挥农业银行的两大优势,即由全国集中联网后网络优势形成的全新含义的网点优势,以及全国数据集中后数据优势形成的统筹管理的信息优势。

此外,农业银行提出通过科技创新工程行动计划的实施实现四个方面的转变。

(1)网络建设要本着“对内搞活,对外开放”的原则,在保证安全的前提下,满足整合各类应用系统的需

要,拓宽和延伸全行信息“高速公路”,张大网络,形成“全国一网、一网打尽”,实现网络模式从封闭型向开放型转变;

(2) 产品研发要立足于数据集中形成的信息优势,贴近市场,研发具有相对优势的产品,建成统分结合的产品研发、部署和应用体系,满足对市场的快速响应,实现从业务主导型向市场主导型的转变;

(3) 营销和服务要依托客户信息的统一视图和企业知识库,引导全行柜员、客户经理和理财专家与客户协同互动,针对客户多样化、个性化的需求,实现从产品中心型向客户中心型的转变;

(4) 管理决策要充分利用基础数据平台和统一分析平台,把数据转化为信息,把信息转化为知识,用知识来指导银行管理决策,实现从经验型向知识型的转变,全面提升市场竞争的综合实力。

根据农业银行的改革和发展规划,考虑到国内外金融信息化发展的趋势,在 2005~2007 年三年间,科技创新工程要全面实现五大主要目标:

(1) 全面完成全国数据集中工程,建成适应全国集约化经营管理的信息系统基础架构;

(2) 建立统分结合的应用体系架构,形成产品、渠道、决策支持、工作流等各类应用的快速创新平台;

(3) 整合和完善适应数据大集中的科技创新工作流程,建立健全产品创新、信息资源管理、生产运营工作体系;

(4) 基本完成科技体制改革,建立有利于科技创新的组织架构;

(5) 建立人才的发展战略和市场化的激励机制,初步形成一支符合数据大集中需要的信息化队伍。

层次清晰的基本目标模型

实现农业银行全国数据大集中是《中国农业银行电子化建设“十五”发展规划》确定的总目标,也是实施科技创新工程行动计划的基础。把农业银行建设成科技先导型的现代商业银行,是农业银行今后一个时期的重点工作之一,也是农业银行今后信息化建设的主攻方向。《中国农业银行科技创新工程 2005~2007 年行动计划》确立的科技创新工程基本模型见图 1。



图 1 中国农业银行科技创新工程基本目标模型

从模型可以看出,科技创新工程在内容上可分为六个层面、四个部分:第一部分(对应着图中由下至上的第一层和第二层)是对基础技术平台在科技创新工程中的地位和关系的描述;第二部分(对应着图中第三层)是对产品创新、信息资源管理和生产运营等三大工作体系在科技创新工程中的地位和关系的描述;第三部分(对应着图中第四层),是对科技体制改革在科技创新工程中的地位和关系的描述;第四部分(对应着图中第五层和第六层),是对实现科技创新工程行动计划效果的描述。

《中国农业银行科技创新工程 2005~2007 年行动计划》是一份非常具体的行动计划,总篇幅超过 100 页。该计划由四个部分组成。第一篇科技创新工程——行动计划的总体思路、总体目标和基本模型,提出了农业银行今后三年科技创新的发展方向;第二篇科技创新工程——基础技术平台建设行动计划,在分析农业银行基础技术平台建设现状和问题的基础上,提出了基础技术平台建设的基本思路、目标架构、主要任务和实施步骤,明确了 2005~2007 年三年的年度工作目标和具体任务;第三篇科技创新工程——科技创新工作体系建设行动计划,在分别对农业银行的金融产品创新工作体系、信息资源管理工作体系、生产运营工作体系现状和问题分析的基础上,以理顺关系、提高效率为基点,提出了科技创新三大工作体系建设的基本思路、工作流程和部门的基本职责,并就三大体系建设提出了具体实施步骤;第四篇科技创新工程——科技体制改革行动计划,通过对农业银行科技体制现状的分析,借鉴国内外同业科技体制建设的基本经验,提出了科技体制改革的基本思路、目标组织架构设计的基本原则和启动科技体制改革工作的基本要求。FCC

编者按:假币问题无疑是现代金融体系中的一颗“毒瘤”。在各类金融机具迅猛发展的今天,提高金融机具的验钞、识假能力无疑是至关重要的。然而,长期以来我国金融机具市场一直由国外厂商占据主流,而国外厂商在人民币验钞环节的技术还有待加强。为提高我国金融机具的识假和鉴别能力,推动机具行业健康发展,中国印钞造币总公司决定大力发展金融机具产业,并在组建中钞长城金融设备控股公司的基础上,与香港丰盛科技有限公司合作成立中钞丰盛现金处理技术(北京)有限公司(以下简称中钞丰盛),致力于银行自助设备的研发和生产。是什么原因促使中国印钞造币总公司下大力气开拓金融机具市场?又是什么原因促成中国印钞造币总公司与香港丰盛科技有限公司之间的合作?带着这些问题,记者走访了中国印钞造币总公司银行机具部主任杜旭东(兼中钞丰盛董事长)和中钞丰盛总经理林憬怡。



中钞丰盛进军金融机具市场

本刊记者 庞瑞江 李玮

记者:是什么原因促成中国印钞造币总公司和香港丰盛科技有限公司成立合资公司?中国印钞造币总公司选择香港丰盛科技有限公司作为合作伙伴出于哪些方面的考虑?双方又能够在哪些方面实现优势互补?

杜旭东:根据人民币流通和行业可持续发展的需要,中国印钞造币总公司制定了发展金融机具的规划,采取强强联合、优势互补、做大做强、共同发展的战略,并已全面启动了金融机具研发、生产、销售和服务的各项工作。

中国印钞造币总公司和香港丰盛科技有限公司在成立合资公司之前已经有四年多的合作历史。在此期间香港丰盛科技有限公司担任了中国印钞造币总公司银行机具方面的技术和商务顾问,在引进国际技术和商务合作方面给予了积极的帮助。双方在金融机具发展方向也有共同的想法。在多年合作的基础上,双方

于2004年开始合资合作的洽谈,经过一年多的反复论证和商讨后签订了合资合作协议。

双方合资合作的优势表现在,中国印钞造币总公司拥有雄厚的资金实力、良好的行业信誉和品牌效应,掌握着人民币印制技术及人民币核心机读防伪识别技术;香港丰盛科技有限公司具有多年金融机具销售和服务管理的经验,对金融机具行业有着深刻的理解,能够正确把握国际金融机具的发展趋势,在国内金融机具市场上建立了完善的营销体系及售后服务网络,具有良好的客户资源和渠道,在国际上与多家国际专业机构有着多年的合作基础和经验。中国印钞造币总公司和香港丰盛科技有限公司合资合作成立中钞丰盛,可取长补短,发挥各自优势,共同发展和不断推进金融机具事业。

中钞丰盛公司已经获得了国内多家商业银行的自助设备采购合同和技术支持服务合同。目前,在国内

超过 60 个城市内已经安装有中钞丰盛的银行自助设备。作为中国印钞造币总公司体系内第一家中外合资的金融机具企业，中钞丰盛公司以诚信为宗旨，采用完全市场化的运作机制，博采国内外同行各家之长，坚持把引导和满足客户需求作为主导企业经营的根本，坚持产品和技术创新，为客户创造价值，不断完善组织架构和管理体系，力争将中钞丰盛打造成为业内最优秀的企业之一，为国家、股东、员工创造财富，也为国家现金处理技术和服务的提升做出应有的贡献。

记者：针对目前国内银行自助设备领域中验钞技术产品现状，中国印钞造币总公司将如何凭借其优势发挥积极作用？

杜旭东：在银行自助设备中，验钞技术产品是关系到现金处理的核心部分，也是所占设备价值比重最大的部分。在国内金融机具行业中，虽然生产厂商众多，但主要都还是从事中、低端产品的生产，无法向市场前景广阔、技术附加值高的领域迈进。



杜旭东：中国印钞造币总公司已全面启动了金融机具研发、生产、销售和工作的各项工作

中国印钞造币总公司涉足金融机具行业，将凭借其优势不断促进国内银行自助设备及防伪技术水平的全面提升。中国印钞造币总公司作为国家法定货币生产企业，在相关技术领域中，我们不断吸收国际先进的印制工艺、防伪技术和检测手段的同时，结合自身

印钞造币特点，在纸张寿命、防伪油墨、制版工艺、生产流程、质量控制、常规防伪技术等方面上不断提高票币防伪技术的一致性、安全性、可靠性、机读性及保密性。在做好防伪的同时，将鉴伪与防伪有机地结合起来，大力开发机读防伪识别技术，并根据不同的应用方向开发相应的金融机具产品。

记者：中钞丰盛公司的成立对金融机具，尤其是包含现金处理技术的银行自助设备产业将会有何影响？

杜旭东：中国印钞造币总公司大力拓展金融机具业务，就是为了提高人民币机读防伪、打击假币、促进货币正常流通以及改善货币使用环境方面发挥积极作用，从而更全面、更好地为人民银行履行职责服务。当然，这也是印制行业实施可持续发展战略、建设现代化企业集团、培育新的经济增长点和实施结构调整、优化资源配置、参与市场竞争的需要。近几年来，我国金融机具市场需求旺盛，而国内金融机具产业正处于成长期，相对于欧美企业，我们还存在很大的差距，尤其在自动存取款机、现金循环机、纸币清分机、票据清分处理系统等自助设备方面差距更大。在国内，这些产品和服务几乎全部依赖进口。这种情况也直接导致金融行业用户所选择的机具品种太少、功能单一，无法全面满足用户对金融机具产品的要求。我们着眼于金融机具行业的发展，成立中钞丰盛公司，就是要把握核心技术，吸收国内外先进经验，研发具有自主知识产权的现金处理技术产品和银行自助设备，将公司逐步建设成为国内领先、国际知名的专业化公司，在发展民族产业、塑造民族品牌和规范银行自助设备市场方面发挥积极作用。

记者：作为强强联合的产物，中钞丰盛将凭借哪些优势来拓展市场？

林懋怡：根据市场需要，中钞丰盛注重开发趋势性、个性化的新产品。的确，目前市场上的自助设备国外产品居多。它们的不足是本地化工作欠缺。我们的战略是在合作中寻找差异化，在产品中增加增值功能。比如，我们在本地化方面会开发本地银行能接受的软件，并使之可与银行主机相连，同时凭借中国印钞造币总公司掌握的核心技术优势，我们会使产品具



林憬怡：我国在识别、验钞和整钞处理技术方面还有待提高和完善，相关标准也有待制定

备高质量的人民币防伪识别能力。事实上，这种高效、准确的识别能力对于银行机具越来越重要。在与外商合作中，我们会选择不同的先进技术，将它们应用到我们的产品中，加上我们自主开发的检测识别技术，我们相信，中钞丰盛的产品将会具有很强的竞争力。

记者：国际上银行业自助设备、现金处理技术的发展趋势如何，我国在有关技术上还有哪些需要改进的地方？

林憬怡：在现金处理方面，日本的自助设备应用最为广泛。据了解，日本 90% 以上的银行自助设备产品都具有现金循环功能。这主要是因为日元的特殊性、日本人的用钞习惯以及现金识别的问题得到了妥善解决。欧洲一些国家生产的自助设备也非常先进。自欧元发行后，欧洲央行针对自助设备处理鉴定出台了第 6 条款，要求存取款机必须具备对假币的保留功能。在国外，银行业一致认为自助设备是柜台的延伸，应该严格按柜台要求来做。

国外的银行现金处理技术研发比较早，像德国捷德（G&D）公司和英国的德拉鲁（Delarue）本身就是造币企业，同时大力研究和发展金融机具。在日本，主要涉及现金识别的金融机具大企业也都是在日本央行支持下，并与央行保持密切的合作关系。它们都拥

有针对纸币和硬币防伪处理的核心技术。

我国金融机具在未来发展中还面临一些问题。仅就技术而言，我认为在识别、验钞和整钞处理技术方面还有待提高和完善，相关标准也有待制定。

记者：国内银行业现金处理设备的应用状况如何？还存在哪些不足？

林憬怡：目前，我国银行所使用的 ATM 品种单一、功能简单，主要的布放方式是在行式。而在国外离行应用则超过 50%。在我国，绝大多数银行的离行应用只有 10%~20%。其中最主要的原因在于现金管理具有一定难度。如果银行的离行 ATM 数量较多，则现金管理问题难以解决，大部分银行还难以把握现金安全问题。

国外的现金处理技术比较成熟，主要是基于多年发展的经验积累和完善的法律法规，而且外包服务也相当发达。外包服务公司可以对银行 ATM 进行现金管理和维护，既帮助银行降低成本，又可以实现管理的专业化。值得一提的是，因为要涉及大额现金的清分和处理，这些外包公司基本上都是印钞行业的衍生物。

记者：中钞丰盛的未来发展规划是什么？

杜旭东：在知识经济和经济全球化的背景下，中钞丰盛将致力于现金处理和银行自助设备产品现代化、信息化和产业化发展，全力提升产品档次和水平，积聚企业独特的核心技术，逐步成为国内领先、国际知名的现代化企业。中钞丰盛在未来的发展中，将重点做好先进识别技术的研发工作，加强与国内外相关单位及印钞造币行业开展技术交流与合作，大力开发更可靠、更稳定、科技含量更高的机读防伪识别技术及自助设备。积极培养和引进高技术专业人才，加大研究和开发投入力度。加强经营管理，巩固并扩展市场营销网络，扩充并完善技术服务网点，努力打造“中钞丰盛”品牌。FCC

集中用户管理在金融行业的应用

沈 鸥

一、集中用户管理的需求分析

谈到企业 IT 系统的安全,很多人都会想起防病毒、防火墙或者入侵检测系统,从安全保护角度而言,这些都称之为外部的保护,或者称之为系统边缘保护。外部的保护有了,那么,内部的保护呢?

什么是系统的内部保护?也许很多人觉得很困惑。

其实,在一个企业中,最为核心的就是企业的员工。同样,在一个系统中,最为关键的就是系统的用户。员工在企业中会有流动,相应地,用户在系统中也会随着其企业中的流动而有不同的使用权限和访问范围,这两者是相互一致的。举一个大家都熟悉的例子:在欧美的一些电影中,往往有这样的情节,一个员工从公司离职了,从他离开的那一刻起,他将无法访问原有的系统,包括他原先使用的电脑系统、门禁系统以及电话系统等,高度的安全保障保证了公司的信息资源免遭损失。很多企业的管理人员看后都很羡慕这样的一套“神奇”系统,其实这就是企业集中用户管理系统在发挥它的作用。

而在国内,很多企业 IT 系统的用户管理仍然停留在手工操作的阶段。要么所有的人都是用一个账号访问系统,如在 Unix 上大家都用 root 账户,“真是太方便了!”,大家都这样认为。但对于系统的安全呢?当重要的系统配置文件被删时,不知谁干的,因为谁都有 root

用户账号的口令;要么账户管理没有动态实时性,一个新的员工上班两天了,邮件账号也许还没有创建。如果说这样仅仅是影响工作效率的话,那么,当员工离开,他的工作账号没有及时注销,仍然有效,该员工就可能以“非法身份”去访问系统,从而造成系统不可预计的影响。这些都是由于没有一种可以对用户账户及账户属性、权限进行集中管理的系统而造成的。

对于中国的金融机构,集中用户管理显得尤为重要。国内银行的所有业务交易系统都已经是基于 IT 系统的自动化处理。如何保证系统用户的安全性是金融机构安全内部保护的重要一环,而这就需要集中的用户身份管理。

对于一个企业而言,集中用户身份管理有以下三个主要的作用:

(1) 及时添加或者解除用户在系统中的账号,从而提升整个系统的安全性,减少由于用户账号问题而带来的安全隐患。据统计,一个员工在企业内平均有 12 个账号,如 E-mail 账号、内部网络账户、特定应用系统账号等。当企业员工数量越来越多,应用越来越多时,管理员不可能再靠手工对每个离职员工的所有账户进行手工清除。只要存在一个没有被删除的账号,就会给系统留下后门。

(2) 减少用户账户和密码管理的工作量,据 META Group 的统计,一个企业的帮助台会消耗 48% 的时间用于账户和密码重置的工作。

(3) 控制用户账户的获得过程,并且监督账户的变动情况,从而发现管理员对于用户属性的改变动作,从企业策略的角度控制系统用户和用户属性非法变动的发生。

二、集中用户管理系统

集中用户管理有一个专业术语,称为“用户身份生命周期管理”,或者称为“用户供应管理”。

用户身份生命周期管理代表的意义是指集中用户管理针对的是用户在一个企业中全部过程,这是一个动态变化的过程,即从用户加入企业,在企业中的身份变动,如从一个一般的员工进行职位升迁、岗位调动,一直到离开企业的全部用户账户变动情况,都应该在集中用户管理系统中实现。如图 1 所示。

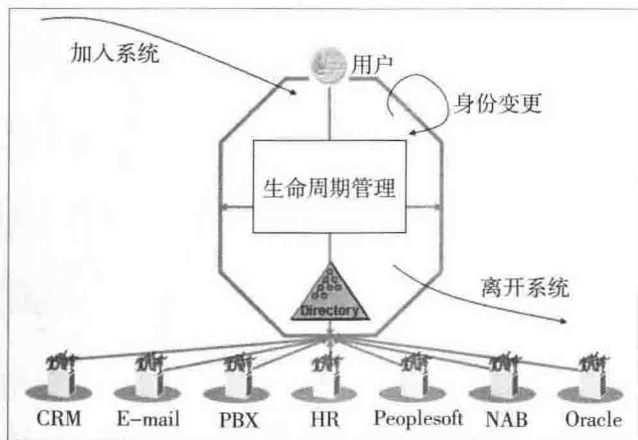


图 1 用户身份生命周期管理

而账户管理的对象则从最为基本的邮件系统、应用系统一直延伸到网络系统乃至电话系统,只要企业中有用户账户的系统,都可以纳入用户身份生命周期管理系统中。

身份管理一般分成两个方面,分别针对企业内部用户和管理企业外部,即合作伙伴、供应商等。自员工加入企业,或者合作伙伴和公司签约后,身份管理系统就开始追踪和管理所有的关系。随着身份的变更,身份管理系统可以根据工作角色自动实现所要求的访问变更,并且启动所有的工作流程和

批准流程。对于一个内部用户而言,这一切是从人力资源系统开始的,所以人力资源系统往往是身份管理系统的数据源和原始驱动源。而用户角色则是一切变动的基础,用户角色直接决定了用户在系统中应该拥有哪些账户资源,正如“干什么活,应该有什么权利”。角色一变,其拥有的账户资源和账户属性也随之变化,这也是用户账户主动供应管理的核心思想。

这种角色变动是否不受任何限制呢?答案是否定的,因为这没有安全性。一个成熟的集中用户管理系统必然要求具有完善的管理范围设置和审批流程。一个用户需要一个新的账号,则意味着该用户具有访问该系统的权利,这种权利的指派正是用户管理系统中审批流程负责处理的过程。如图 2 所示,一个用户需要获得一个资源(系统上的账户资源),需要经过一个完整的处理和审批流程(通常称之为授权过程)。

作为一个面向所有企业员工的系统,集中用户管理系统为每个员工提供了可以自己管理自己信息的窗口,以发挥每个员工的主观能动性来减少后台支持人员的工作量。在这个个人工作窗口下,企业员工可以完成诸如修改自己联系方式、申请新的资源访问权限的工作,而领导层更可以进行审批、查看、统计的工作。自助服务已经日渐成为提升管理能动性的一个重要手段。

集中用户管理正在成为新一代信息服务不可缺少的核心环节之一,并且正在从其传统的应用方式(用户身份信息的集中管理)向支持跨越信息安全域边界的信息共享发展,通过基于业界标准的 SAML、WS-Security 等安全访问标准,企业之间可以对用户进行相互管理和对资源的信任授权,从而加强企业用户在相互信任

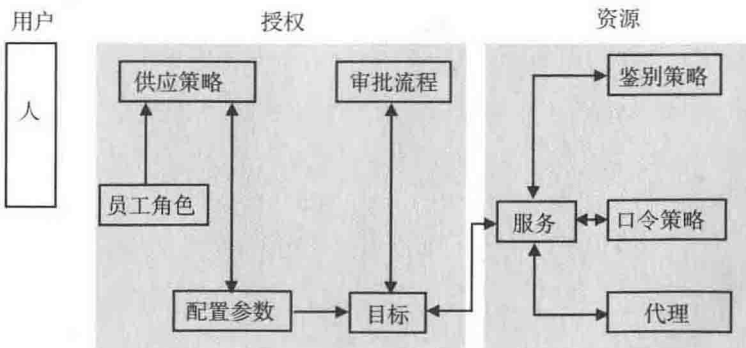


图 2 授权过程

的基础上对应用及数据进行快速、安全、有效访问。

三、集中用户管理系统的实现

企业在实现集中用户管理系统时,一般需要考虑如下几个方面的要素。

1. 如何管理用户身份

企业首先需要知道如何管理自己系统的用户身份。比如可以按用户的业务职能来确定不同的用户组:员工、客户、供应商、合作伙伴等,也可以按照用户的所在部门地域进行分组。

相比而言,一个用户只有一个身份要比有多个身份管理起来容易许多。企业可以按用户的需求来管理他们的身份,并借此不断提高客户满意度。在企业内部,用户身份管理系统一般由 IT 部门部署和掌握,并与人力资源应用程序集成。具体的用户角色都有预定义的资源访问定义和访问属性(权限)定义。

在企业外部,当它吸引了一个客户、供应商或合作伙伴时,它一定要确保用户身份的自助管理过程是直接、顺畅和安全的,这一点至关重要。为了让用户有被重视的感觉,一定要让他们相信,他们所提交的信息将成为高度机密,并且不会出现安全问题。

2. 用户目录基础架构

建立基于 LDAP 技术的目录服务,这是因为身份管理系统需要一个以稳定且可扩展的目录为基础的强大的基础性骨干架构。目录服务器的选择一般需要满足以下几个要求:

- (1) 基于 LDAP V3 的标准,并且得到 Open Group 的认证。
- (2) 支持 LDAP over SSL 的加密传输机制和最新的 AES 加密算法。
- (3) 具有高度伸缩性,支持并发和上亿的用户数量级。
- (4) 高可靠性,支持多种复制模式和实现技术。
- (5) 高安全性,支持用户目录的角色访问和高细粒度控制。

而元目录系统也是很多企业需要考虑的一个技术点,通过元目录产品的目录整合技术可以将分散的、不规范的用户目录进行整合、统一或者同步,以配合集中

用户管理系统的部署。

3. 基于角色的用户身份供应管理

用户身份管理系统的建立与如下信息密切相关:

- (1) 需管理的用户的类型。
- (2) 用户需要访问的系统、应用程序和其他公司资源。
- (3) 资源的访问属性和不同用户的访问级别。
- (4) 创建、更新和删除用户账号的实现机理。
- (5) 和行政手段相吻合的管理流程。
- (6) 事后监督机制和监督流程。

用户身份集中管理可以帮助企业以最低的成本将恰当的资源提供给用户。它的管理覆盖用户的整个生命周期,包括在不同系统上创建账号、访问权设置,以及临时暂停访问权限或永久废除账号。有效的用户身份管理能够降低诸如密码保密性能不足之类的安全风险,并最大可能地消除影响用户生产力的障碍。另外,用户身份管理还可通过基于角色的账户创建和访问权限指派,来实现集中的管理功能和自动化功能。

4. 用户验证技术

现在业界开始采用生物识别、智能卡和数字证书等方式来验证用户的身份,它们是可信交易的基础。所以用户身份管理也需要和这些验证技术有相应的数据交互和共享,如在用户管理中增加特定的控制属性和验证信息属性。

5. 自助式的用户身份管理服务

提供哪些自助式的用户身份管理服务是很多企业都认真考虑的问题,因为这种服务最能带来管理效益,增进用户使用感受。自助式注册和自助式管理通过将相应的管理权交给用户,从而降低了后台服务的成本,缩短了用户获得资源访问的时间。例如,用户通过 Web 提交了访问请求,直接进入用户身份审批流程,在不需要后台技术人员干预的情况下获得所需的资源,直接减少 IT 部门的工作量。

6. 跨域的账户变动

现代企业的组织结构变化迅速,人员流动速度也相应加快,身份集中管理的一个关键战略就是要确保用户账户的移动性。员工在企业内部频繁地移动,而许多用户也因工作的关系需要经常出差。身份集中管理系统将确保用户跨部门、跨地区移动时,其身份随之移动和变