



面向智能终端的移动办公系统

吕伯轩¹, 刘景文¹, 许玮¹, 王单¹, 聂雯莹¹, 何明²

(1. 普天信息技术有限公司, 北京 100080;

2. 中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 移动智能终端是互联网业务的关键入口, 将移动智能终端与办公平台结合成为一种全新的移动办公模式, 能够克服传统时空受限的办公模式的不足。为提高管理和办公效率、保障数据安全, 分析了移动办公业务的安全需求, 设计了一种安全可控的面向移动智能终端的办公系统, 着重介绍了系统结构、安全功能模块以及业务流程, 实现了移动办公系统的主要功能, 通过为移动设备提供统一管理, 能够实现基于许可授权和使用控制的数据安全保障机制。

关键词: 智能终端; 移动办公; 数据安全; 身份认证; 设备认证

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018100

Mobile office system oriented to intelligent terminal

LV Boxuan¹, LIU Jingwen¹, XU Wei¹, WANG Dan¹, NIE Wenying¹, HE Ming²

1. Potevio Information Technology Co., Ltd., Beijing 100080, China

2. Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: Mobile intelligent terminal is the key entry to the internet services. Combining mobile intelligent terminal with office platform becomes a new mode of mobile OA, which is able to overcome the space-time limitation of traditional office model. To improve the efficiency of management and work, and to ensure the security of data, the security requirements of mobile OA were analyzed, a secure and controllable office system for mobile intelligent terminal also could be designed. The system structure, security function module, and business process were introduced, as well as the main function of mobile OA system was realized. By providing the unified management for mobile devices, data security based on licensing and use-control could be achieved.

Key words: intelligent terminal, mobile OA, data security, identity authentication, device authentication

1 引言

移动智能终端已成为兼具新媒体、电子商务

与信息服务等诸多功能于一体的综合服务平台, 是互联网资源、移动网络资源与环境交互资源的重要枢纽^[1,2]。随着移动智能终端的日益普及和功

收稿日期: 2017-12-08; 修回日期: 2018-01-30

通信作者: 聂雯莹, neiwenying@potevio.com

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No. 2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No.2015AA017205)



能不断增强，其已成为人们日常生活不可或缺的用品^[3]。

在移动互联网、大数据、云计算技术深度发展以及“互联网+”对行业深度渗透的时代背景下，政府、企业以及个人对业务移动化的需求越来越强烈。这种需求促使移动智能终端与办公平台结合成为一种全新的办公模式，即移动办公，办公人员可在任何时间、任何地点处理与业务相关的任何事情^[4]。

移动办公是继电脑无纸化办公、互联网远程办公之后的一种新型办公模式，是企业和政府信息化建设的重要组成部分^[5]。这种办公模式利用移动智能终端的信息化软件，建立智能终端与办公管理平台一体的企业软件应用系统，借助移动智能终端通信的便利性，摆脱时间和场所局限，能够随时处理待办事宜、减少加班处理公文时间、避免因出差等原因不能及时审批等事宜，有利于提高管理效率，推动效益增长，对于突发性事件的处理、应急性事件的部署有极为重要的意义^[6]。

由于移动智能终端存储和处理大量的个人数据、商业数据，甚至机密数据，其重要信息可能流经政府或企业的内部网络、外部互联网、无线网络，甚至境外网络，面临着设备丢失、系统漏洞、程序缺陷、网络攻击等诸多安全风险^[7]。随着移动智能终端的广泛应用，安全形势不容乐观，如何安全地部署和应用，是移动办公系统需要考虑的首要问题^[8]。为保障移动办公系统安全，促进和规范移动办公系统行业应用，我国正在制定“移动终端安全管理平台技术要求”国家标准^[9]。

本文参考移动终端安全管理平台技术标准的要求，设计了面向移动智能终端的办公系统，增强移动终端的安全性、可控性和时效性，为智能手机、平板电脑等移动智能终端设备实现移动办公系统提供参考。本文主要以智能手机为例，分析了移动智能终端面临的安全威胁以及移动办公

系统的安全需求，提出了构建安全可控的移动办公系统方案，引入身份鉴别、访问控制、数据保密性、数据完整性、安全审计等安全技术，通过定制安全策略对移动智能终端设备、用户和应用等进行统一管理和安全接入控制。

2 移动办公系统的安全需求与设计

2.1 总体设计

本系统在不影响现有办公系统运行的基础上，基于移动互联网与智能终端技术，实现同步办公、协同办公、交互办公的移动办公模式。

在逻辑结构上划分为内部网络服务、接入控制管理、移动用户 3 个部分，如图 1 所示。

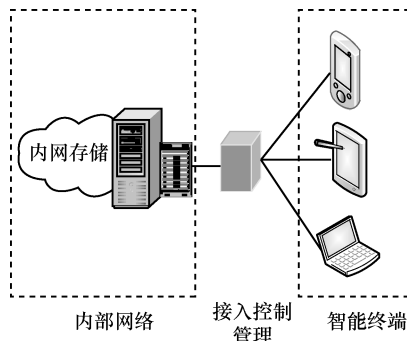


图 1 移动办公系统逻辑结构

在外网与内网之间设置接入控制管理服务器，实现内外网隔离，对设备与成员认证。移动智能终端用户通过认证之后，通过移动互联网访问内网服务，查阅通讯录与内部文档、接收或签发内部文件等。

为保障通信、数据存储、访问与操作的安全性，根据标准要求，移动办公系统应具有以下基本安全功能。

(1) 用户与智能端认证管理

只有合法的用户与终端才能接入系统，支持用户退出与权限变更。

(2) 通信安全

数据通信受到保护，防止被窃听、冒充、修改等。

(3) 存储安全

存储在智能终端的数据受到保护, 防止被恶意读取、修改和删除等。

(4) 操作安全

只有合法的用户或管理员才能对安全存储的数据进行修改、添加以及擦除等。

为实现上述安全功能, 移动办公系统的总体架构与安全模块如图2所示。

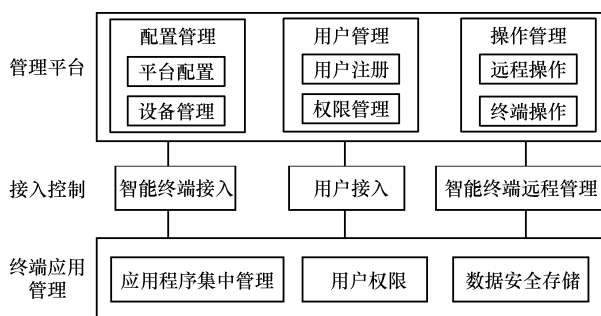


图2 移动办公系统的总体架构

内网管理平台负责设备注册、成员注册与权限、远程操作等管理, 智能终端应用程序的安装、用户权限变更、数据安全受网络管理平台的控制。

2.2 移动办公系统的管理平台

按功能划分, 内网管理平台包括管理员管理、智能终端设备管理、用户管理、终端应用程序管理以及终端操作管理, 另外包括用于权限管理的平台策略数据库与数据存储, 如图3所示。

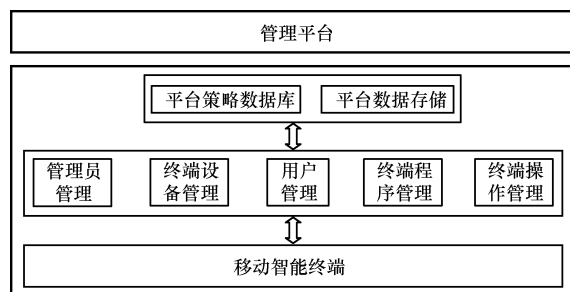


图3 移动办公系统的管理平台

系统管理员根据安全策略管理终端设备、用户注册、用户权限变更, 管理平台将可审计事件与相应管理员账户关联, 管理平台存储移动终端可加装的应用程序, 并可远程管理终端。

2.3 移动办公系统的智能终端

移动智能终端远程接入应用资源时, 应能够保证远程接入会话的保密性。智能终端的安全主要包括用户权限管理、应用管理、加密存储、异常报警等功能, 如图4所示。

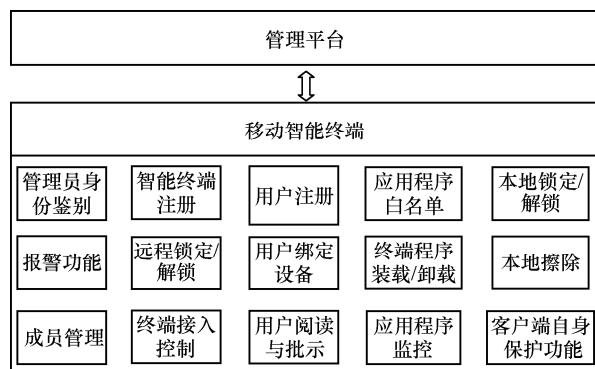


图4 移动办公系统的智能终端

系统管理员在执行与安全功能相关的操作之前应进行身份鉴别, 管理员能够修改远程接入控制相关策略、查阅和管理审计日志, 对成员进行管理。移动智能终端的办公系统保护机制能够识别异常接入、越狱或 root 操作, 并提供向管理平台报警功能, 禁止运行白名单以外的应用程序。

系统管理员依据安全策略能够远程锁定/解锁智能终端设备, 能够允许/阻止智能终端和用户接入。

用户与智能终端设备绑定, 每次登录时移动办公系统管理平台对设备与用户认证。

管理平台对移动智能终端的位置信息、运行程序等信息进行监测, 对应用程序集中管理, 管理平台对移动智能终端的应用程序拥有强制卸载的权限。

智能终端能够远程备份/擦除本地文档, 支持敏感数据加密存储, 基于安全策略对终端敏感数据访问操作行为进行监控。

表1统计了移动办公系统的主要功能模块与功能。



表 1 主要功能模块与功能

功能模块	功能
管理员管理	管理员注册、管理员身份鉴别、管理员权更改、异常报警
终端设备管理	智能终端注册、智能终端接入、设备丢失锁定、更换 SIM 卡锁定、更换 SD 卡锁定、远程数据擦除、外设接入监控、智能设备定位
用户管理	用户注册、用户登录、用户信息修改、用户与终端设备绑定、用户注销、用户阅读与批示
终端程序管理	越狱/root 检测、应用程序白名单、应用程序装载/卸载、应用程序监控
终端操作管理	数据加密传输、数据加密存储、本地锁定/解锁、本地数据擦除、账户安全监控

3 移动办公系统的功能模块与业务逻辑

移动办公系统将传统纸质的、固定台式机的处理模式扩展到移动智能终端，融入了新的业务流程，其显著特点是通信即时与交互性，用户不再是单纯地接收文档，还能发布、更新或修改文档，如图 5 所示。

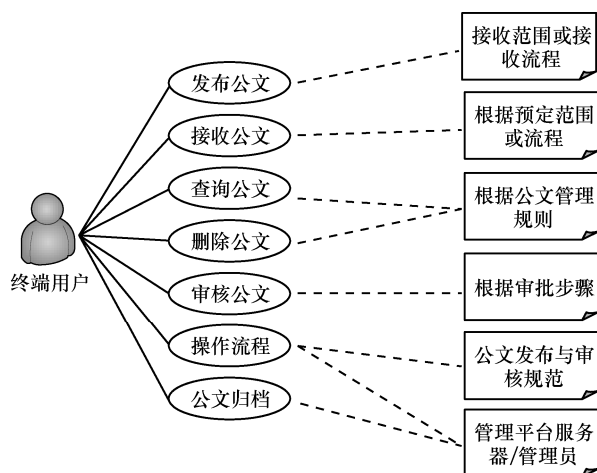


图 5 公文管理功能示例

操作流程由系统建立时预定义，系统管理员也可根据内部业务流程的公文更改发布、接收、审核等公文操作流程。

(1) 设备注册

设备注册在安全环境下完成，在智能终端装载移动办公系统客户端，客户端向管理平台服务器发送设备注册信息，包括硬件型号、设备序列号、系统软件版本，管理平台服务器记录相应注册信息、注册日期以及所属部门等，如图 6 所示。

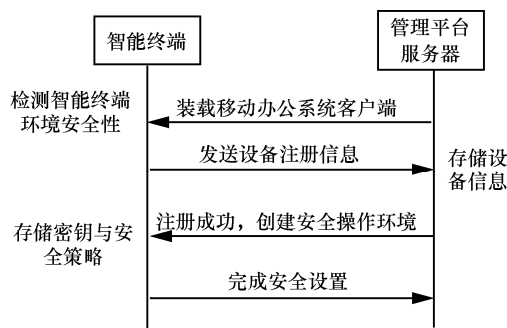


图 6 设备注册流程

(2) 用户注册

智能终端用户在移动办公系统完成注册、创建账户与登录密码/数字指纹，管理平台将移动智能终端与用户绑定，并根据安全策略授予用户相应的操作权限，如图 7 所示。

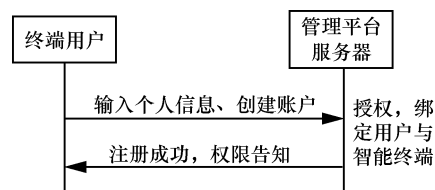


图 7 用户注册流程

用户在本阶段获得个人数字证书，用于解密和签发文档。

(3) 应用程序管理

应用程序的管理启用白名单机制，由管理平台集中管理、用户下载安装，无法安装白名单以外的应用程序，管理平台能够根据安全策略删除运行在智能终端上的应用程序。

(4) 文档阅读与批示

移动办公系统支持用户能够随时随地阅读、

批示、发布文件，如图8所示。

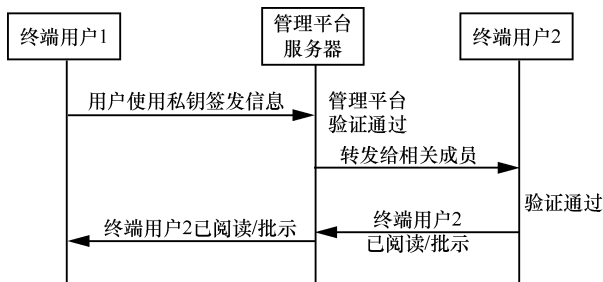


图8 文档阅读与批示流程

步骤1 当用户1需要发布信息时，系统调用数字签名系统，使用私钥签发文档，对敏感信息加密，选择接收范围，客户端将签发后的文档上传到管理平台服务器。

步骤2 管理平台服务器验证真实性后存档，并根据接收范围转发给相关用户。

步骤3 用户2阅读后，客户端自动返回该用户已阅读的信息，管理平台服务器将已阅读信息归档，并将该信息通知用户。

步骤4 如果用户签发的信息需要用户2批示，则用户2通过客户端的公钥系统对该文档执行签名批示并返回，管理平台服务器归档，并将该批示信息返回用户1。

这样，用户使用该移动办公系统，能够随时随地发布、阅读、批示文件。

(5) 加密传输

客户端、管理平台服务器分别存储对方的公钥证书，并安全存储各自的私钥。基于公钥系统客户端与管理平台服务器可以建立共享安全信道。

(6) 远程锁定/擦除

如果需要防止某智能终端内的文档被阅读或处理，由该智能终端持有者申请或由管理员直接通过管理平台服务器对智能终端远程锁定。

移动办公系统对存储在智能终端的敏感数据执行生命周期管理，这类数据在预定有效期后将由系统客户端删除，并向管理平台服务器回报。

另外，根据安全策略，管理员能够远程强制擦除存储在移动终端的敏感数据。

4 移动办公系统的流程与功能实现

(1) 用户注册

在使用移动办公系统前，需要在管理员处注册登记个人信息，包括真实姓名、工作证编号、部门、职务等信息，见表2。

表2 个人信息登记

字段名	数据类型	说明
id	字符串	用户登录编号
name	字符串	真实姓名
department	字符串	部门
position	字符串	职务
phone number	字符串	联系电话
permission	字符串	用户权限
description	字符串	其他描述

用户的登录账号为个人的工作证编号，初始密码为身份证号码后6位，用户登录后客户端后可更改密码，用户登录界面如图9所示。



图9 用户登录界面

(2) 设备注册

在用户完成注册的同时，在移动智能终端装载客户端。客户端向用户请求获取设备信息，在用户授权的情况下，客户端向管理平台服务器发送设备注册信息，存储在服务器数据库中的“设备信息表”中，见表3。



表 3 智能终端信息登记

字段名	数据类型	说明
hardware_model	字符串	用户的硬件型号
serial_no	字符串	用户设备序列号
version_num	字符串	系统软件版本
register_date	日期	注册日期
department	字符串	所属部门

(3) 客户端主界面

完成注册之后，用户登录客户端，即可进入客户端主界面，使用移动办公智能客户端的各项功能，客户端主界面如图 10 所示。



图 10 客户端主界面

在办公过程中，业务报批是最基本的功能之一，员工发布的公文若需要相关负责领导审批，则可以根据单位管理要求选择需要报批审核的领导。

(4) 业务审批

在审批人的客户端，将为审批人提示待审批的文档。

在负责人审批过程中，需要对员工申请的事项进行“批准”或“驳回”的操作，对需要修改和建议的地方可以备注，文件审批界面如图 11 所示。

(5) 文件管理

文件管理模块根据用户的身份信息和权限，显示当前身份可见的文件列表，并提示指定用户需要阅览的文档，文件管理界面如图 12 所示。



图 11 文件审批界面

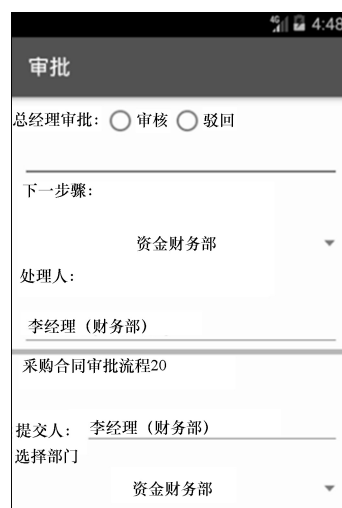


图 12 文件管理界面

5 结束语

移动办公系统融合了智能终端与移动互联网的应用，能够显著提高办公效率，有利于突发性事件的处理、应急性事件的部署，推动了政府和企业效益增长。本文分析了移动办公系统的安全需求，设计了面向移动智能终端的办公系统，提出安全解决方案，并实现了系统功能。采用统一管理和接入控制方式，通过设备监控、身份鉴别、访问控制、数据保密性、数据完整性等安全技术，增强移动办公系统的安全性、可控性和时效性。

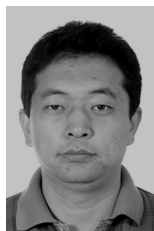
参考文献:

- [1] XIE X W, MAO H. Mobile intelligent terminal equipment learning software design and development[C]// International Conference on Intelligent Transportation, Big Data and Smart City, July 27-28, 2015, Shanghai, China. Piscataway: IEEE Press, 2016: 515-518.
- [2] 吴吉义, 李文娟, 黄剑平, 等. 移动互联网研究综述[J]. 中国科学: 信息科学, 2015, 45(1): 45-69.
WU J Y, LI W J, HUANG J P, et al. A review of mobile internet research[J]. Chinese Science: Information Science, 2015, 45(1): 45-69.
- [3] WU L. Research and development of mobile forestry GIS based on intelligent terminal[C]// International Conference on Remote Sensing, Environment and Transportation Engineering, June 24-26, 2011, Nanjing, China. Piscataway: IEEE Press, 2012: 1-4.
- [4] 汪峰. 基于移动互联网技术的办公 OA 系统设计与实现[D]. 南京: 东南大学, 2016.
WANG F. Design and implementation of office OA system based on mobile internet technology[D]. Nanjing: Southeast University, 2016.
- [5] 庞峰. 基于 Android 的##类公司移动办公自动化系统的设计与实现[D]. 长春: 吉林大学, 2017.
PANG F. Design and implementation of mobile office automation system based on Android ## company[D]. Changchun: Jilin University, 2017.
- [6] HUSSEIN E A A, IQBAL M T. Design of renewable energy system for a remote mobile office in Newfoundland[C]// Electrical Power and Energy Conference, January 18-19, 2016, Singapore, Singapore. Piscataway: IEEE Press, 2016: 1-6.
- [7] 许艳萍, 马兆丰, 王中华, 等. Android 智能终端安全综述[J]. 通信学报, 2016, 37(6): 169-184.
XU Y P, MA Z F, WANG Z H, et al. Survey of security for Android smart terminal[J]. Journal on Communications, 2016, 37(6): 169-184.
- [8] JIANG Y, LI G, HU A. Mobile office security technology for WLAN[M]. Piscataway: IEEE Computer Society, 2010.
- [9] 信息安全技术—移动终端安全管理平台技术要求(草稿)[S]. 2017.
Information security technology-technical requirements for mobile terminal security management platform (draft)[S]. 2017.

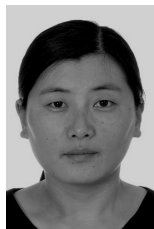
[作者简介]



吕伯轩(1979—), 男, 普天信息技术有限公司研发部总经理、高级工程师, 主要研究方向为基于行业的信息通信。



刘景文(1974—), 男, 博士, 普天信息技术有限公司技术总监、高级工程师, 主要研究方向为移动互联网技术、应用和安全。



许玮(1983—), 女, 普天信息技术有限公司解决方案经理、高级工程师, 主要研究方向为基于行业的信息通信。

王单(1977—), 女, 博士, 普天信息技术有限公司产品经理、高级工程师, 主要研究方向为无线通信专网、物联网关键技术。

聂雯莹(1983—), 女, 普天信息技术有限公司标准化工程师、助理研究员, 主要研究方向为基于行业的信息通信标准。

何明(1976—), 女, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为云计算安全、移动互联网安全、SDN/NFV 安全等。