政企移动终端管理方案研究

陈长怡[1]，杨广龙[2]
(中国电信股份有限公司广东研究院,广州中山大道西109号,510630)

摘要：随着政企移动信息化的发展以及越来越多的员工携带自有移动终端使用企业内部应用，企业需要保护企业自身的数据信息安全以及对员工移动终端进行管理。本文提出的政企移动终端管理方案实现了设备管理、应用管理、数据管理及安全管理等移动终端管理功能，解决了政企客户保护企业内部数据信息的安全性需求与对员工移动终端的可管理性需求，将在政企移动信息化进程中发挥重要作用。

关键词：移动信息化，移动终端管理，安全管理，数据管理

1 引言

随着移动通信技术的发展，3G 和 4G 时代相继来临，智能移动终端包括智能手机与平板电脑不断丰富，企业信息系统移动化应用发展迅速，很多企业通过移动应用来提高工作效率和客户服务质量。随着移动应用的推广，企业员工携带自有移动终端使用企业内部应用的情况日益增多，而智能移动终端型号与操作系统的多样性特点使得这些设备很难进行统一、有效的管理。一旦发生移动终端丢失、被盗或感染病毒，可能会导致企业内部数据泄露，以及被非法访问的危险[1]。同时，多平台操作系统和不断增长的移动终端应用程序整合工作，大大提高了企业移动终端应用程序的管理成本。

鉴于以上安全性和可管理性等方面的因素，政企移动终端管理方案为政企客户的移动终端、应用及数据提供安全防护和管理功能,主要包括设备管理，应用管理，配置管理和安全管理等功能，帮助企业在提高工作效率、提升客户服务质量的同时，保护移动终端、应用和数据安全。

2 政企移动终端管理方案

2.1 政企客户对移动终端管理的需求

2.1.1 安全性需求

随着政企移动信息化的广泛应用，尤其是 Android 和 iOS 智能终端的大规模使用，大量移动终端正处在一个欠缺安全保障的环境中，面临诸多安全漏洞的隐患及较高的侵入风险。因此，企业需要对使用企业内部应用的员工移动终端和涉及到的企业内部数据信息进行加强管理和保护，并规范企业终端用户的使用行为。而对于企业移动终端设备的管理而言，并不是传统意义上对企业设备资产的管理，需要区分企业、个人所拥有的设备和数据问题[2]，充分考虑保障员工隐私，进行有效的安全管理。

2.1.2 可管理性需求

企业员工使用各类移动终端访问公司资源的工作方式已成趋势。对企业而言，管理这些移动终端的需求主要包括为企业各级管理人员、一线工作人员提供方便的管理服务，如提供移动邮件、WiFi、VPN 等远程、批量自动配置，对摄像头、蓝牙、SD 卡、WiFi 进行远程禁用与过滤，对企业应用进行远程推送、批量部署等。

2.2 政企移动终端管理方案组网图

政企移动终端管理系统主要由企业客户侧的后端平台与终端侧客户端组成，组网图如下图所示：

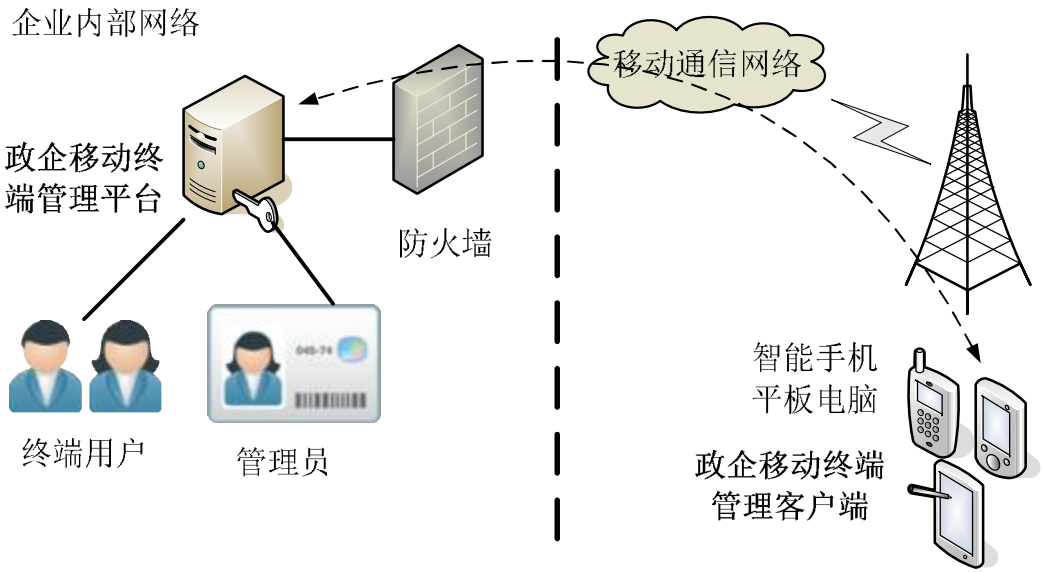

图 1 政企移动终端管理系统组网图

- 移动终端管理平台部署在企业侧。企业管理员能够通过后台管理界面登录到移动终端管理平台对移动终端进行管控。
- 移动终端管理客户端是指安装在智能手机、平板电脑等移动设备上的客户端软件。后端平台管理客户端、传送客户端更新以及从客户端收集数据。用户可以通过 PC 机登录移动终端管理用户自服务系统对自己的终端实现部分管控功能。

2.3 政企移动终端管理系统架构图及功能介绍

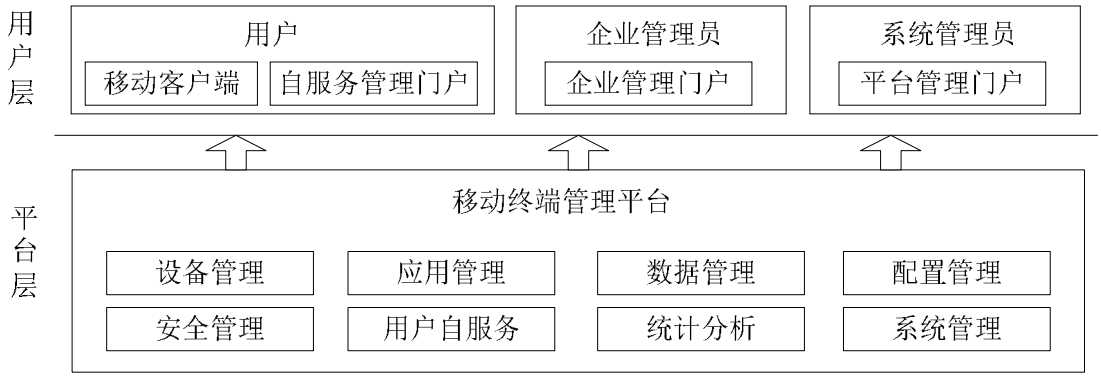

图 2 政企移动终端管理系统架构图

- 用户层：系统管理员利用平台管理门户实现对移动终端管理平台的系统管理；企业管理员利用企业管理门户实现对企业移动终端管理功能的管理；用户利用自服务门户和移动终端管理客户端软件实现对自身移动终端的管理；
- 平台层：提供包括设备管理、应用管理、数据管理及安全管理等移动终端管理的业务功能，以及平台本身的管理功能。

政企移动终端管理系统主要功能如下：

1) 设备管理：

管理企业移动终端，包括对企业移动终端的注册、分组、注销等进行管理。对移动终端的基本信息和运行情况进行管理，包括获取移动终端的软硬件信息，比如内存信息、运营商信息、已安装移动应用信息等。

2) 应用管理：

实现企业内外部移动应用的发布、远程推送与分发、批量部署等。对政企应用和个人应用安装、更新、卸载及使用情况进行监视与限制，对应用的合规性进行检查等。

3) 数据管理：

对企业数据进行安全保护管理，包括数据备份与恢复、数据擦除、数据加密、数据防泄露等。

4) 配置管理：

对所有的移动终端进行配置管理，比如提供移动邮件、WIFI、VPN 等远程、批量统一配置，提供摄像头、蓝牙、SD 卡、WIFI 的远程禁用与过滤。

5) 安全管理：

对企业内移动终端进行安全管理和防护，监控企业内移动终端的总体安全状况，并进行安全策略管理，包括终端安全参数采集、安全事件采集与分析、终端安全策略配置与实施等，以确保企业内移动终端及其应用与数据的安全。

6) 自服务管理：

提供企业移动终端用户自服务管理功能及门户，每个注册用户都可以登陆用户自服务门户，来管理自己名下所有的移动终端设备，并完成有限的功能操作，包括寻找手机，擦除手机，锁定手机，修改密码，查看手机上应用情况等。

7) 统计分析：

提供对企业移动终端的设备、应用与数据的各类安全管理信息进行统计分析功能。

8) 系统管理：

系统管理员利用平台管理功能及门户实现对移动终端管理平台自身的系统管理，包括平台的系统配置、网络配置、系统备份与恢复以及对企业管理员的管理等功能；企业管理员利用企业管理功能及

门户实现对企业移动终端用户及设备的管理，包括企业内部门户的管理、移动终端用户及其名下移动终端的管理、系统备份与恢复、日志管理、统计分析等功能。

3 结束语

政企移动终端管理方案实现了设备管理、应用管理、数据管理、配置管理、安全管理、用户自服务、统计分析、系统管理等功能，使员工移动终端可纳入安全保障范围，一旦发生移动终端丢失、被盗或感染病毒，企业即可通过此移动终端管理系统作出相应安全措施。政企移动终端管理方案在帮助企业在提高工作效率、提升客户服务质量的同时，解决了企业对自身数据信息的安全性需求以及对员工移动终端的可管理性需求，对政企移动信息化的进一步发展具有重要意义。

[参考文献]

1. 王卫东,企业移动设备安全管理方法与实践[J],计算机安全,2011 年,第 11 期:44-47。
2. 钱煜明,董振江,吕达等,BYOD 企业移动设备管理技术[J],中兴通讯技术,2013 年,第 19 卷第 6 期:33-39。

作者简介：

陈长怡（第一作者），硕士。现任职于中国电信股份有限公司广东研究院政企客户产品开发部，从事行业移动信息化平台和应用的需求分析、测试工作。

杨广龙，硕士。现任职于中国电信股份有限公司广州研究院政企客户产品开发部，从事行业移动信息化平台和应用、以及移动互联网领域的产品规划、设计及研发工作。