移动 OA 系统解决方案

1.1 项目概况

1.1.1 项目背景

随着办公自动化系统的普及，电子化、数据化的办公方式已进入越来越多的政府单位，信息化的办公系统在企事业内部编织起一套高效、畅通的信息互联体系，极大推动了企事业单位生产力的发展。

而移动信息化的出现，使得信息化摆脱了对固定办公环境，固定工作时间，固定电脑设备和网络的依赖，将信息化无缝延展到每个人手中，使得信息化从此可以随时随地的跟随着人走。它是对原有信息化的补充，也是对信息化本身的发展和跃变。

XX 公司不断发展，随之而来的工作越来越多、越来越繁重，为此，对基层移动信息化问题有必要作进一步的探讨，如何提高服务质量、如何提高内部办公效率已成为当务之急。

1.1.2 需求分析

XX 公司目前有一套自己的 IT 系统，可以满足自身在固定场景下的办公需求，比如说公文处理、领导简报、公告通知、电子邮件、通讯录查看等等，但是由于一些特殊情况，需要将这些功能同时支持移动场景下的应用：

- ★ 领导公务繁忙，经常在外，需要有一种方式可以实时了解和查询单位管理工作的情况；
- ★ 在出现紧急情况时，办事员需要将事情尽快呈报领导，需要有一种可以在瞬间进行多文件、多资料信息传递的沟通工具；
- ★ 领导在进行工作指示和计划落实时，经常涉及跨部门协作，需要有一种便捷的途径能通知到所有相关人员；
- ★ 对于重大问题，领导之间需要沟通磋商，需要确保领导在外出时也有方法可以参与多方集群会议，完成会议讨论和决策制定；
- ★ 领导在外时，需要有一种方式快速有效地处理重要公文和其他政务，避免由于环境、条件等问题贻误工作；
- ★ 政府工作人员经常外出办理事情，需要有一种手段可以即时将重要的文件资料传达给内部系统；

★ XX 公司对信息安全的要求很高，需要保证信息在各种应用场景下的安全问题。

通过对 XX 公司的需求进行分析，不难看出安全、高效的移动办公系统将将会大大提高 XX 公司的工作效率。

1.1.3 建设目标

1、安全性保障

保证该平台的安全性，包括数据的安全性，保密性，被访问网络的安全性,以及手机和原系统数据传输的安全性。

2、实时办公机制

充分利用综合一体化管理，改变传统的固定工作机制，形成统一领导、相关人员积极响应体制。通过这个平台可以在手机上完成待办公文的流转、审批和结束等工作。

3、信息主动机制

传统的待办公文等工作只能在电脑上完成，造成相关工作处理的滞后。现在要实现主动式处理方式，通过手机平台即可查看、处理相关信息。

1.1.4 建设意义

通过部署办公平台，可完成工单管理的信息化升迁，助推部门的一体化管理，可带来各方面的效果：

★ 手机平台更加智能化、安全化、快捷化

★ 领导层能精准的进行事务管理和信息调用，实现高效管理。

★ 部门科室通过手机可以随时随地进行信息查看处理。

★ 无处不在的移动化通信网络，可摆脱种种环境束缚，无论是在上下班堵车路上，还是在休假出差期间，均可以进行应急处理事务，办公效率更加出色。

★ 精准细严的信息获取、传达，为工作及时调整创造更好的效率。

1.2 平台建设

1.2.1 平台概述

手机工作平台是可一站式满足企事业信息化需求的综合开发平台。配套有业界领先的智能客户端解决方案、功能完备的核心服务器、丰富专业的二次集成开发工具、丰富的内置应用套件、维护管理工具及零门槛的客户培训教材等。完备的配套服务为企事业单位解决了开发建设成本高，技术门槛高，实施风险大，支撑和推广不利的一系列问题，降低了企事业单位的开发建设成本和技术门槛，解决了技术顾虑；降低了实施风险，有效的提高了支撑和推广力度。

手机工作平台将信息化典型应用抽象出来，形成了诸如短信、彩信、移动办公、移动行业应用等一系列丰富的业务功能。企事业单位可以使用终端通过短信、彩信等进行通知、点播、问答、抽奖等消息类业务；也可以通过终端收发移动邮件，将个人电子邮件主动推送用户的手机终端上，即时而准确；还可以用移动终端进行移动办公，很好的解决了企事业单位人员出差、休假、外出或其他特殊情况时不能及时处理重要办公事宜的问题，使得企事业单位人员能够随时随地、及时有效的进行移动化信息处理。

1.2.2 设计原则

1.2.2.1 安全性

移动 OA 平台能提供有效的安全保障，具备完善的身份认证、访问控制、数据加密等安全保密机制，保证网络系统、主机系统和应用系统的安全，为客户提供完整的安全保密，同时保证手机端和后台系统数据传输的安全性。

1.2.2.2 先进性

在保证方案可靠性和技术成熟性的基础上，采用先进的系统体系结构、先进的系统硬软件平台、先进的应用软件设计思想和实现技术，确保本系统起点高、技术领先，为平台的实现提供最佳的技术平台支持。

1.2.2.3 易操作性

平台应保证在功能和人机交互界面上贴近用户日常办公习惯，功能模块和功能按钮的说明应定义清晰、命名直观，达到简单易用、提高工作效率的目的。

1.2.2.4 可扩充性

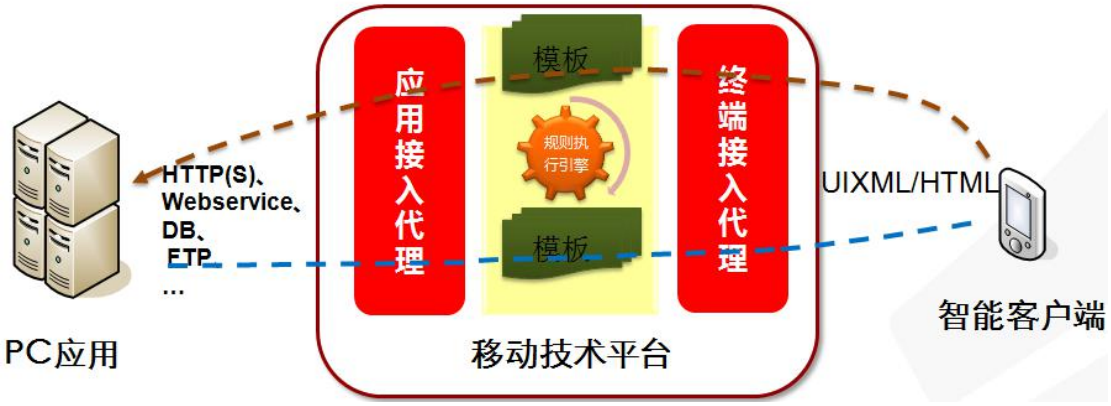
采用符合国际标准和适应国际发展潮流的移动化信息系统技术、可平滑扩展的系统硬件体系结构、开放式的系统软件平台、模块化的应用软件结构，确保系统在处理能力和业务功能方面可灵活扩充，并可与其它系统进行无缝集成。

1.2.3 解决思路

打破固定式、分散的办公管理，实现移动信息化，采用移动信息化应用技术实现，达到快速部署、节约、安全、接入、灵活调用、扩展、跨平台等能力。

1、从业务角度来看，是替代传统的、固定式办公，结合无线网络把 PC 办公发展到手机端应用，如下图所示：

2、从技术角度来看，是通过移动技术平台实现手机应用操作，并通过 http、webservice、DB、FTP 等接口接入应用实现 web 端和终端的交互，整个交互过程采用移动技术实现各种功能模型的规则配置、语义转换，最终通过 UIXML、HTML 语义识别展现到手机客户端。如下图所示：



3、江苏省移动办公平台支持多种数据交互接口方式，与 XX 公司办公系统的数据进行交互。可支持的接口方式有：

- ★ DP(DataParser)：展现层数据解析接入方式
- ★ WS(WebService)：标准 webservice 接入方式
- ★ DBV(DBVertical)：数据垂直读取接入方式
- ★ SP(StandardProtocols)：国际标准协议接入方式，如 ftp、socket 等协议

用户没有提供接口的情况下，移动办公平台可支持 HTTP 页面数据抓取方式来获得后台业务系统的请求、反馈数据，生成手机端的应用（注：通过页面抓取方式开发的客户端应用，高度依赖原系统架构，如原系统升级或发生改变，手机端应用均需进行二次开发）。

手机用户在使用移动办公客户端时，提交申请到移动办公服务器，服务器根据请求从数据库中提取相应数据后，原路返回，通过服务器端定义规则模版，直到反馈到用户的移动终端上。

后台应用系统根据业务逻辑处理来自手机的请求，并将响应数据返回给移动办公平台，服务器通过应用接入代理，将返回数据调用下行模板进行解析，再通过各种渲染引擎和接入代理

将数据传回手机智能客户端呈现。

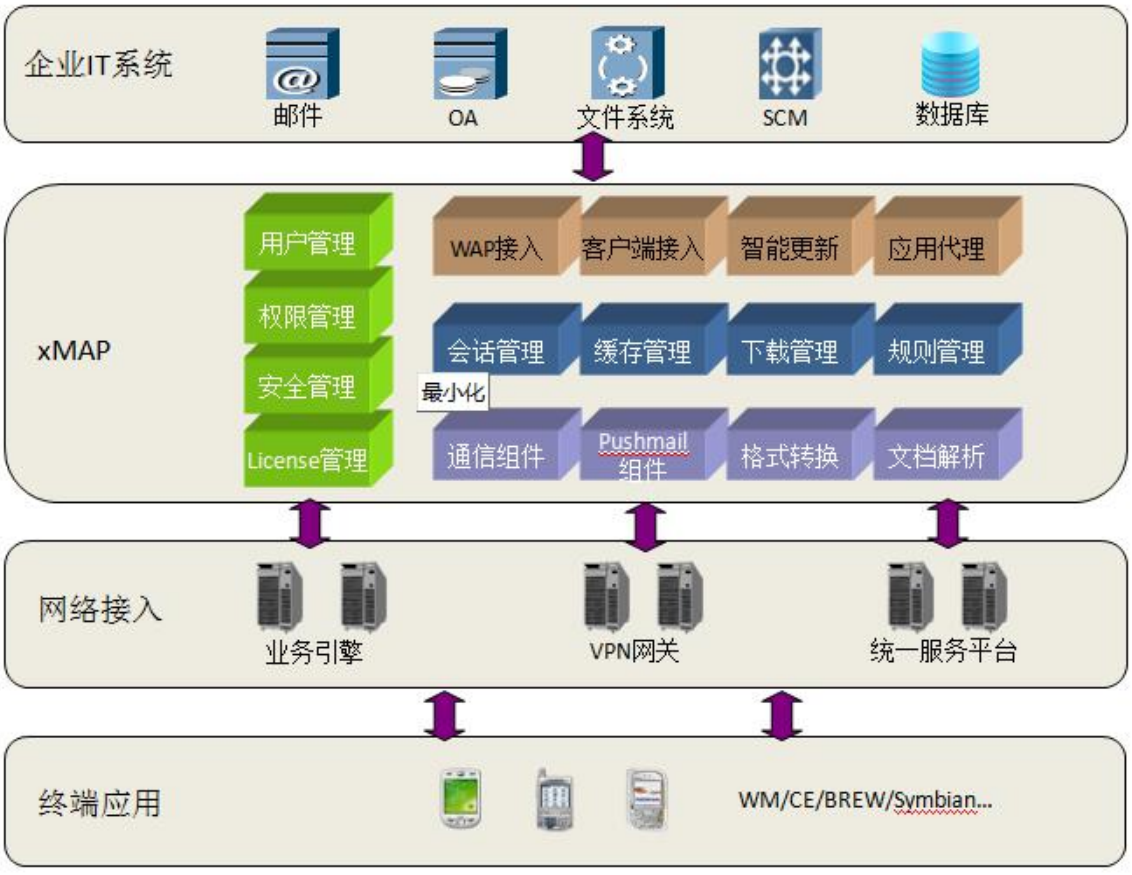
上述 B/S 适配过程无需对后台应用系统做任何变更，大大降低了移动化的成本，适用于大部分应用系统。对于部分使用了 ActiveX 等特殊控件的系统，可能需要原系统厂商提供接口技术配合，具体配合要求根据具体系统情况确定。

1.2.4 系统结构

XX 公司移动办公平台基于中国移动移动化应用平台实现。以手机终端上的智能客户端为载体，使用运营商通信网络与服务器系统进行连接，可以将 XX 公司的业务系统和 OA 系统扩展延伸到移动终端，搭建成可移动化应用的综合办公平台。

XX 公司移动办公平台采用开放式设计，具备良好的应用无关性，可以连接原有系统，实现移动化建设。以手机终端上的智能客户端为载体，使用移动数据通信网络与服务器系统进行连接。手机终端上安装的智能客户端软件完全屏蔽终端底层的复杂性，终端用户可以享受到近乎完全一致的用户体验。

XX 公司移动办公平台将高强度存储加密体系和策略安全体系两者结合，完美保护了手机终端到移动办公平台，移动办公平台到后台应用系统间的信息安全，结构层次如下图所示：



1.3 安全保障

1.3.1 组网架构

为 XX 公司提供一整套基于 APN 专线网络的移动办公解决方案，确保端到端的安全应用。

网络结构图及**工作原理**如下：

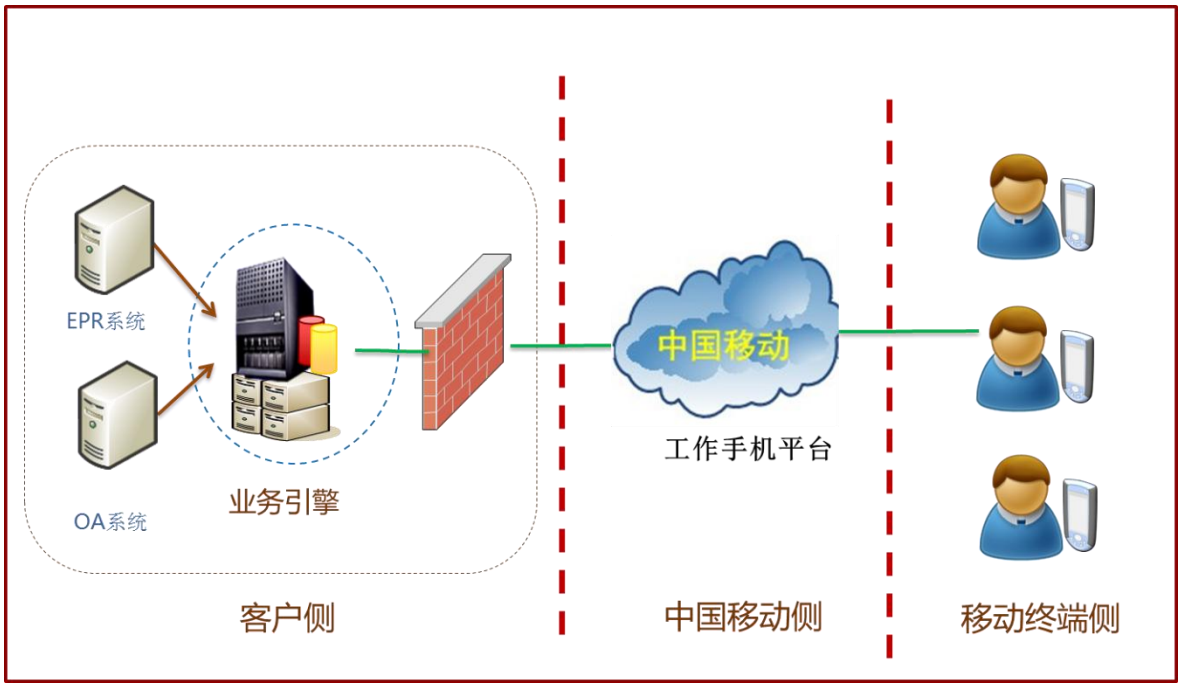
（1） 移动终端**设置 APN 接入点（XX 公司专用 APN 接入点）**接入移动工作手机平台，发送请求；

（2） 工作手机平台进行**身份认证**后，处理请求；

（3） 工作手机平台将通过**移动数据传输专线（该专线为 XX 公司专用）**将改请求发送至客户服务器，客户服务器响应数据后，返回至工作手机平台；

（4） 工作手机平台针对数据进行相应处理后通过移动终端显示。

以上所有操作的安全性请参考下一章节 1.3.2。



1.3.2 安全设计思路

XX 公司移动办公平台安全方案分解为网络安全、传输安全、应用安全、存储安全、身份认证五大部分，将采取多种安全机制来保证移动办公平台的安全性。

1、为了保证移动终端用户安全接入 XX 公司移动办公平台，推荐使用无线 APN 的方式接入；

2、通过身份识别机制，确保登陆 XX 公司移动办公平台用户的合法性；

3、在移动办公平台前设置入侵检测机制，屏蔽违规、危险的操作；

4、传输加密：移动办公平台在数据传输过程中，为保证数据的安全，使用了 SSL 的加密机制（SSL 加密为 2048 位），确保不会有明文在网络上传输。

1.3.3 互联网接入

关于互联网接入安全是指防火墙安全访问控制。已经建设有信息系统的企业一般都会在网络的边界部署有防火墙，利用防火墙灵活的安全访问控制可以有效隔离内外网之间的通信，只有规则允许的访问才能通过防火墙。

通过防火墙的 NAT 功能将移动应用中间件服务器的内网地址静态映射成可与运营商通信的外网地址。

通过边界防火墙可以有效地限制运营商通信网络侧只能访问移动应用中间件服务器的相应端口和服务。

通过防火墙的安全策略可拒绝和阻断来自广域网、专线和企业内网的非授权访问和攻击

通过企业网内现有的入侵检测系统、漏洞扫描系统和网络防病毒系统对移动应用中间件服务器制定其安全访问、安全保护的策略和规则。

1.3.4 专线接入

移动应用中间件支持使用专线网络接入方式。使用运营商网络以及移动应用中间件时，可通过物理专线来构建专用的安全网络通道。

专线网络是完全不同于互联网的一种网络，是完全的运营商用于安全传输的内部网络，与互联网完全隔绝，确保了信息传输的安全和保密。

申请专线接入后，即可获得直达运营商网络的物理连接和对应的 IP 地址，移动应用中间件服务器通过这条专用通道与运营商网络侧内部网络相连。

专线接入具有可靠、简单、高效、安全、时延小的特点。

能提供高性能的点到点通信，通信保密性强，特别适合政府、金融等保密性要求的客户需要；

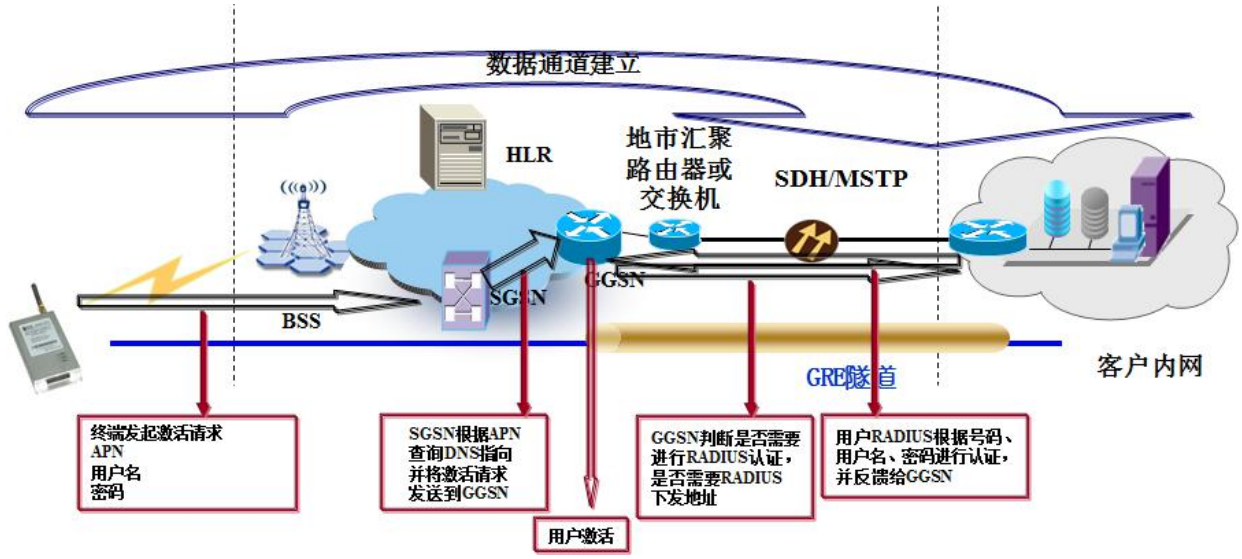
传输质量高，网络时延小，信道固定分配，充分保证了通信的可靠性，保证用户的带宽不会受其他用户的影响。

1.3.5 移动 APN 技术

为 XX 公司开通 APN 网关通道，为授权用户分配专用的 APN，普通用户不能访问该 APN。

3G 终端通过 PPP 拨号方式由 APN 无线网关接入，移动 APN 认证服务器提供接入认证，通过验证后，APN 将与 XX 公司的路由器之间建立起安全专用隧道（APN 内网），并分配内网 IP 地址。

通过 APN 网关通道访问 XX 公司的移动办公平台，能实现业务数据的互联互通，从而搭建在外的人员访问内部业务流程处理的通道。通过 APN 网关接入，客户端本身具有移动内网固定 IP，减少中间环节，稳定性增强；所有数据都在移动的 APN 内网传输，无需经过公网，安全性增强。



APN 接入网络拓扑图

用户业务安全性保障点：

1、移动侧对 SIM 卡是否合法进行判定；

2、移动侧对 SIM 于卡使用的 APN 是否合法进行判定

3、用户 RADIUS（远程接入拨入用户服务）对于用户号码是否合法进行判定；

4、用户 RADIUS（远程接入拨入用户服务）对于用户名、密码是否合法进行判定

5、可以在无线侧到用户核心侧叠加加密算法

采用公司 APN 专线接入 XX 公司内部网络，不需要 XX 公司提供专用设备，但需要 XX 公司在内网与外网之间的防火前开放 APN 所需要的端口，并指定可访问的 IP 地址。

APN 接入手机操作方法如下：APN 接入点设置方式（设置前保证移动网络正常打开）：进入设置＊选择设定菜单＊移动网络＊选择接入点名称＊打开 CMWPA＊设置代理服务器地址和端口号＊完成。

1.3.6 网络传输层安全措施

移动应用中间件支持使用专线网络接入方式。使用运营商网络以及移动应用中间件时，可通过物理专线来构建专用的安全网络通道。

专线网络是完全不同于互联网的一种网络，是完全的运营商用于安全传输的内部网络，与互联网完全隔绝，确保了信息传输的安全和保密。

申请专线接入后，即可获得直达运营商网络的物理连接和对应的 IP 地址，移动应用中间件服务器通过这条专用通道与运营商网络侧内部网络相连。

专线接入具有可靠、简单、高效、安全、时延小的特点。

＊ 能提供高性能的点到点通信，通信保密性强，特别适合政府、金融等保密性要求的客户需要；

＊ 传输质量高，网络时延小，信道固定分配，充分保证了通信的可靠性，保证用户的带宽不会受其他用户的影响。

1.3.7 网络侧安全防火墙

防火墙技术是目前用来实现网络安全措施的一种主要手段，主要是用来拒绝非法用户的访问，阻止非法用户存取敏感数据，同时允许合法用户顺利访问网络资源。依据系统内事先设定的过滤逻辑，检查数据流中每个数据包后，根据数据包的源地址、目的地址、TCP/UDP 源端口号、TCP/UDP 目的端口号及数据包头中的各种标志位等因素来确定是否允许数据包通过，其核心是安全策略即过滤算法的设计。用户网络可以选用适合于本单位的防火墙产品来保证自己网络数据的安全。

防火墙作为网络安全体系的基础设备，其作用是切断受控网络的通信主干线，对通过受控干线的任何通信进行安全处理。

其特点是：

1、防火墙能够强化安全策略

因为网络上每天都有上百万人在收集信息、交换信息，不可避免地会出现个别品德不良，或违反规则的人，防火墙就是为了防止不良现象发生的“交通警察”，它执行站点的安全策略，仅仅容许“认可的”和符合规则的请求通过。

2、防火墙能有效地记录网络上的活动

因为所有进出信息都必须通过防火墙，所以防火墙非常适用于收集关于系统和网络使用和误用的信息。作为访问的唯一点，防火墙能在被保护的网络和外部网络之间进行记录。

3、防火墙限制暴露用户点

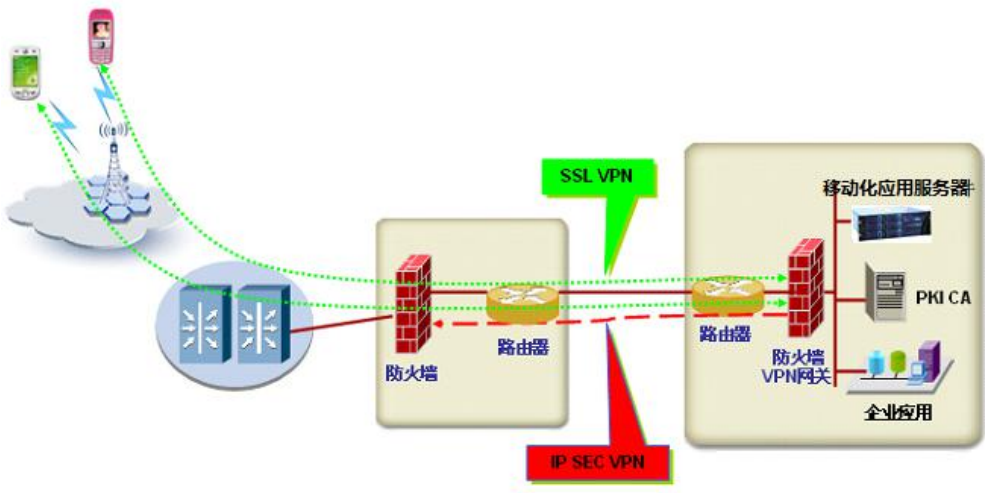
防火墙能够用来隔开网络中的两个网段，这样就能够防止影响一个网段的信息通过整个网络进行传播。

4、防火墙是一个安全策略的检查站

所有进出的信息都必须通过防火墙，防火墙便成为安全问题的检查点，使可疑的访问被拒绝于门外。

1.3.8 传输通道加密

XX 公司移动办公平台支持 SSL（或者在用户侧部署专门的 SSL VPN 网关）传输通道加密，可以在手机客户端与服务端、PC 与服务端之间搭建基于 SSL 的传输通道，保证数据传输的私密性。



1.3.9 应用层的安全性

应用层本身可以通过专用的安全协议进行数据加密和传输，进一步提高安全性。

强制密码验证

系统不保存用户登录密码，强制要求使用者在登录移动办公平台应用时必须输入密码进行验证，保证他人无法随意使用安装了移动办公平台客户端的手机终端登录系统。

多重身份验证

系统支持用户名绑定，对于内部工作人员，使用一个固定用户名进行安全认证，没有进行登记的用户无法登陆内部使用的移动办公平台工作站，更无法得到信息。

数据传输加密

系统支持对手机客户端与服务器之间传输的数据进行加密，无线传输过程中的信息和数据加密后传输防止移动数据传输中被窃听。

存储安全

XX 公司移动办公手机客户端上保存的离线数据支持 128 位高强度 AES 加密存储，确保数据的保密性和完整性，防止数据被非法获取或篡改。

1.4 手机功能介绍

任何系统都需要进行逐步的使用、建设和完善，本章节对 XX 公司“移动办公平台”的功能进行描述，将一些已经具备条件延伸到手机使用的功能。以下功能效果仅供参考，具体方案待与贵处讨论后决定。

1.4.1 首页效果

通过手机客户端登录移动办公平台，在首页将常用的功能以快捷图标的方式列出，用户可直接点击功能按钮快速进行相关业务模块进行工作。以南京市旅游管理委员会界面为例，首页包含办公公告、公文待办、邮件系统、通讯录功能。参考如下：

1.4.2 办公公告

通过手机客户端以列表形式展示客户原 OA 系统的所有办公公告，支持阅读及附件查看。界面风格参考如下：

1.4.3 公文待办（含公文扭转）

通过手机客户端展示客户系统中所有的待办公文（点击进行公文办理）、并支持待办公文、在办公文、已办公文、检索等功能。界面风格参考如下：

1.4.4 邮件系统

支持写邮件，收件箱、发件箱和草稿箱的展示和回复。界面风格参考如下：

1.4.5 通讯录

支持原系统中所有通讯录联系人的个人信息和电话，并支持拨号。界面风格参考如下：

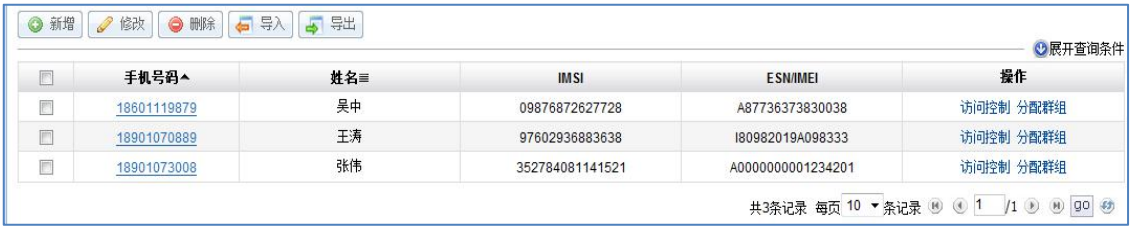
1.5 平台优势

1.5.1 不影响原有系统

手机平台就如同一台电脑，如有新员工上班，传统做法是先给员工买台电脑用，现在就是用手机来代替电脑先工作。对于现有的原系统，移动办公平台与原系统进行访问时，和电脑一样，不需要企业原有系统做些改动，不改变企业原有组网方式。

1.5.2 多重安全保障

专线或者 APN 接入；基于 SSL 的传输通道，保证数据传输的私密性；三重绑定认证机制，对用户的 IMSI、ESN 及帐号进行绑定，保证一部手机、一张卡、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。



1.5.3 用户体验良好

在不改变用户电脑 Web 页面的操作习惯下，并切合用户在手机终端的操作方式，功能界面给用户良好的体验。

在一些公文处理页面中，把流程的主要信息，一目了然的呈现给客户，其他的明细内容可

以收缩展现，使整个手机页面显得不那么臃肿，按钮始终位于屏幕下方，不随着页面滚动，便于客户流程提交。

效果展示图如下：

在企业的组织架构图中，我们采用异步请求的机制，实时刷新部门的人员结构，避免组织架构庞大所等待的加载时间过长。此外，对于组织架构中的人员选择，放在页面的顶部，便与勾选；查看人员的中的电话信息时，可以直接拨打电话、发送短信，避免需要退出客户端在重新拨打的多次操作。

企业常用的数据图表，柱状图、饼状图等，在手机上完美展现业务系统的数据分析图表，给应用增添色彩。

1.5.4 文档的多方式浏览

对常用的应用分析平台文档格式（word、excel、ppt、pdf）有很好的浏览支持。在浏览文档的过程中，采用的边请求边浏览的方式，提高附件的预览速度和文档的流量控制。

1.5.5 应用能力可扩充

移动办公平台具有可扩充性，在企业新增模块功能和其他应用系统的移动化需求时，客户端不在需要重新定制，完全考虑到这个业务的扩充性，直接在移动平台上添加应用，客户端更新即可。

1.5.6 多终端覆盖

支持以下平台： Android、ios（ IOS 认证需 XX 公司申请，方法如下）、Windows Phone 等。并且分别对每个平台做了特别的优化，以此达到最优的效果，为用户提供最好的 UI 和 UE 体验。

1.6 终端支持

具备出色的全终端覆盖能力，可广泛适用于市场上各类常见的手机系统，且保证了用户体验的一致性。支持的主流手机系统包括 Android、ios 等。支持的主流手机品牌包括苹果、摩托罗拉、三星、LG、华为、中兴、等等。