无安全、不移动，
如何构筑移动营销平台的安全基石

HUAWEI

1 移动营销在中国银行业已渐露峥嵘，从理念走向落地

随着 3G/4G 网络及无线局域网的大规模建设普及，移动终端设备为各行各业带来了前所未有的改变和新的市场机会。很多行业都开始不同程度地采用移动终端来提高工作效率和客户体验，而金融产品因其无实体、复杂度高等因素非常适合移动端销售。商业银行通过打造移动营销平台，可将业务系统的信息化内容与手持终端的移动化优势结合起来，完成对销售流程和客户信息传递的电子化改造，最终帮助银行实现效率及业务收入的大幅提升。该平台具备如下三大特点：

- 终端展示功能强大，能够提供文字、图片、视屏等多媒体展示手段，可更好的宣传介绍金融产品，降低客户对金融产品的理解难度；
- 计算能力和通讯功能强大，通过加载各种应用程序，并利用无线宽带网络和银行后台业务系统相连，可实现现场在线业务办理；
- 轻便灵活，高效整合各类柜面终端，业务人员可随身携带，突破业务办理地域限制。

其使用者涵盖大堂经理、理财经理、客户经理（对公、私银）、信用卡经理、管理者等多个角色。通过该平台，银行可完成从“坐商”到“走商”的转型，并将服务渠道延伸至社区、企业、商圈、专业市场和高端客户所在地等价值区域。

在刚刚过去的智能移动终端浪潮中，大量移动应用的面世丰富了终端的功能，不断强化和丰富了移动营销概念，一些金融行业的先行者已经体验到了移动营销所带来的好处。包括民生银行、招商银行、中信银行、北京银行等大批创新性较强的银行已开始着手移动化战略布局，但每家银行策略则不尽相同。如民生银行一开始即着眼全行移动化平台建设，然后辐射移动办公、户外移动营销、小微商圈签约等多个业务领域。据统计，其全行移动平台有效支持社区、商圈的签约、发卡、申贷、理财等业务，该平台在实施上线该系统后 1 个月，日开户量达 9500 户并呈高速发展趋势，单设备日最高签约量达 50 户，可谓战果显著。而如南京银行、中信银行、杭州银行、北京银行等则针对具体的业务办理如厅堂展示、信贷审批、信用卡申请等优先级较高的业务进行试点，待业务成熟后再进行全面推广。但无论采用哪种策略，殊途同归，最终各家银行都将完成全行移动化改造。

2 移动营销在零售银行的典型应用场景及发展趋势

理论上讲，银行大部分不涉及现金的业务都可以在移动终端上办理，这样不仅可以打破物理网点受理业务的限制，拓展客户资源，也改进了服务方式，提升了客户体验。如工商银行早期开展的移动终端业务，即采用 3G 网络方式接入主机系统，经授权认证后的临时性终端，在限定场所为特定客户办理制定的业务。虽然该模式只限于办理规定的非现金业务，处于摸索试探阶段，但任然在市场上为工行赢得了不少赞誉。移动营销发展到今日，延伸出的业务领域已经五花八门，但就成熟度来看，最适合移动化的业务主要还是展示类（厅堂展示）、采集类（信用卡申请）、面签类（个人消费贷款）三类业务。下面我们来看看这些典型场景下的移动营销：

厅堂展示

传统厅堂作业模式下，客户识别和业务推荐都直接依赖于大堂经理的个人经验，理财产品的推荐和商机线索的发掘也缺乏工具支持，使用纸质产品说明书和电子显示屏展示产品，信息更新不及时演示也不方便，纸笔作业及办公电脑模式也不便于交互和共享。同时客户经理外出拜访客户和户外办公时，对客户和商机线索的管理也不方便，不能及时的拿到全面的营销资料和业务培训材料，而采用移动终端在厅堂做产品展示、线索搜集则更具有灵活性、实时性。

移动发卡

传统的办卡流程上，信用卡销售流程不够严格、申办周期过长，填表即完成任务，因而信息准确性低、申请效率低，并且办卡时间长、活卡率较低，客户信息保密性等方面也比较受影响。特别是分期业务请款慢，非常容易丢失客户。而移动发卡即通过移动终端办理信用卡业务已屡见不鲜，早已被各家银行实践证明是提升信用卡销售额的利器。

面签类业务

目前的一些面签类业务由于其较高的人员和安全性要求，均需客户到网点现场办理，银行一般采用双柜员授权认证的模式，比如借记卡开卡、个人消费贷款、理财托管签约、网上银行签约、手机银行签约和银信通签约等。客户体验不好，导致价值客户的流失。但采用移动终端进行双柜员上门服务或者通过后台集中实时授权认证的形式，则可突破网点限制，走到客户身边批量办理业务，非常有利于这类业务的主动拓展。

未来通过打通银行前后台业务流程，并与后台CRM、产品支持系统、金融资讯系统、交易流程系统之间进行对接，可完成整个柜面移动化改造。现在柜台办理的非现金业务 90% 以上都可分流到移动柜台办理。

3 无安全、不移动，银行 CIO 们应该关注业务移动化后带来的哪些风险？

移动营销带来的好处显而易见，但随着业务多样化，规模不断扩大，其中蕴含的安全风险也渐渐暴露出来。在信息时代，每一次信息安全事故给金融企业带来的损失都是不可估量的。金融行业的网络结构复杂，而移动化使传统的网络边界变的模糊，承载业务和数据的终端移动到哪里，网络的边界就扩展到哪里，传统的安全防护手段很难再提供可靠的保障，银行的 CIO 们不得不重新考虑如何在高效与安全之间找到一个平衡点。但有一点是业内公认的，即一个完整的移动营销方案需要覆盖智能终端设备，网络管道，后台管理以及移动应用等多个部分，但每个部分所面临的安全挑战却各有不同：

首先 终端是所有业务应用展现的窗口，不管是金融企业内部的 OA 应用还是面向客户的服务应用，往往需要不同的应用客户端来完成不同的工作，比如基础 OA 需要有邮件客户端，访问内部 Web 应用需要有一个安全可靠的浏览器，为保证安全连接到银行内网还需要建立 VPN 链接的客户端，对于针对性的业务应用又有单独的客户端，甚至对与移动设备的管理还需再安装一个客户端。面对如此多的应用，一个统一的平台则可以避免在众多的应用中搜寻目标应用，并且反复切换登录。同时终端侧的员工个人数据会和银行的数据混合，存在很大的信息安全风险，目前针对“混合”带来的麻烦，通常采用 “隔离”技术来解决。而现在业内最先进、最成熟的数据隔离技术就是沙箱容器化技术，该技术可为应用和数据提供一个加密保护的安全沙箱环境，从而解决公私数据、应用混合带来的信息安全风险。

其次 接入和传输管道上的威胁如何防范呢？管道侧的安全问题层出不穷，金融行业因其巨大的可获利性一直都是传统网络攻击的主战场，在移动互联时代这个状况依然没有任何改变，反而带来了更多的入侵结点。园区附近伪装的恶意 Wi-Fi 链接，数据在传输管道中被窃听或篡改，终端则沦为对内网进行大规模攻击的跳板，这些威胁手段最大的特点就是新入侵点配合传统攻击方式，对这类威胁的防护除了需要提供包括 VPN 加密，统一威胁防护，Anti-DDoS 等很强的传统网络威胁防护能力，同时更需要针对终端接入有周全的考虑。

再者 各类金融移动应用往往是被攻击的发起点，而在对移动应用的保护上，不管是前面终端上统一安全的平台，还是网络管道的威胁防护，都只是保障了移动应用使用环境的安全，对应用本身的安全防护同样需要重点考虑。而随着业务的发展，金融移动应用的体量将非常庞大，为避免众多应用单独开发安全模块而造成的重复浪费、应用发布周期长等问题，银行应统一考虑应用的安全性问题，挑选可提供开放接口的安全厂商，以便各类应用可快速集成发布。

最后 一个完整的安全体系永远都需要一个强大的安全管理后台，而对于移动营销平台来说，运维管理可分三个层面：移动设备的管理、安全策略的管理以及移动应用的管理。在新移动互联时代，最大挑战是存在多种异构平台的移动设备都会接入网络，而传统的 PC 管理手段很难移植到移动设备上。金融机构必须建立针对移动设备的管理方法，对所有被允许接入内部网络的设备进行全生命周期的管理；策略的管理同样如此，不仅需将传统的安全策略重新定义到移动设备上，更重要的是如何能够实现移动安全策略与传统策略的统一管理与下发，确保任何设备上的策略一致性；对移动应用的管理也是必不可缺的环节，统计显示有近三成的恶意应用活跃在各种移动应用市场上，在应用审查机制足够完善之前，金融机构自有的应用管理是非常关键的，应自行建立一个可信的内部应用商店，确保接入内部的应用都是可信可控的。

4 具备终端，网络，安全及应用能力的厂商最适合实现银行的移动化战略

商业银行的移动化部署需要多个技术领域协同配合才能够做到最优，所以在选择合作伙伴上，需要其拥有网络、安全、统一通信与协作、无线、终端等丰富的产品，并有能力解决部署中面临的策略、安全、管理和应用等多个方面的问题。这样的公司需具备＂一站式的解决方案＂和＂定制化的服务能力＂，它可以为银行的移动化提供咨询、并提供基础设施选型和工程实施服务，全面解决移动战略实施过程中所遇到的各类问题。华为公司以其宽广的产品线以及在移动领域的大量积累，尤其是在整体安全防护方面的传统优势，在国内移动市场上获得不少赞誉，其移动营销解决方案提供的产品和系统覆盖终端、网络、安全、应用和管理等多个方面，如下图所示：

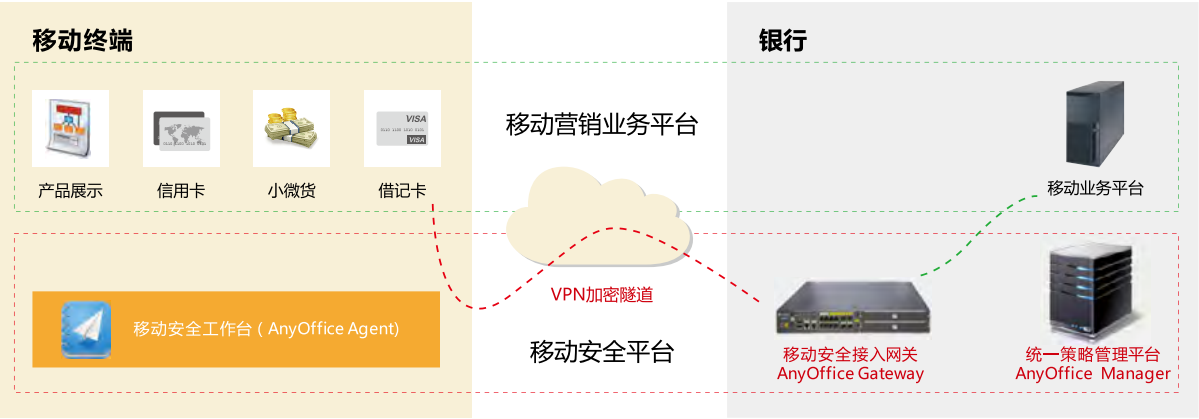

图 1 移动营销解决方案架构图

该方案包括移动终端、移动安全平台两个重要部分，分别如下：

移动终端及外设

移动终端采用华为 10 寸 mediapad 外加一体化背夹，背夹上集成了公安部授权认证的二代证读取模块，能够实时收集并验证二代身份证真伪，客户经理在诸如办卡、开户等场景时能轻易识别虚假证件，防止恶意套现等金融犯罪的发生。同时该终端支持蓝牙 2.0 技术，与蓝牙打印机、指纹识别仪等设备良好整合，可支撑丰富的业务办理场景。

移动安全平台

移动安全平台包括移动安全工作台、移动安全接入网关、统一策略管理平台三个组件，各组件之间紧密配合完成终端管控、应用管理、数据安全保障等平台支撑功能。其中移动安全工作台作为移动终端上的应用统一接入平台，配合统一策略管理平台实现 MDM、MAM、MCM 等功能。而移动接入网关则在移动应用接入银行内网时触发统一策略平台联动检查，只有终端合规性检查通过的才允许接入访问内网资源，可有效避免应用接入与 MDM 检查分离导致的非法终端访问或违规处理不及时等问题。

• 移动安全工作台（AnyOffice Agent）组件

移动安全工作台（AnyOffice Agent）作为移动终端上的银行应用统一接入平台，兼容 IOS、Android 等主流操作系统，分层布局，界面简洁美观。支持单点登录功能，用户只需一次登录，所有应用通行，避免重复登录。在安全方面，AnyOffice 客户端提供安全沙箱、SSL VPN 等功能。其内置的安全 SDK 可供第三方应用快速集成，从而使应用具备数据加密传输、移动沙箱等安全能力，保障移动应用 3-7 天内快速。

- **移动应用安全接入网关 (AnyOffice Gateway) 组件**

移动应用安全接入网关 (AnyOffice Gateway) 部署方式灵活，支持 2 万规模并发 VPN。具备多种认证方式，如：口令、数字证书、短信、硬 Key 等。该设备支持国密算法，可实现移动应用的安全接入、数据的安全传输，建立安全加密的接入管道。

- **统一策略管理平台 (AnyOffice manager) 组件**

统一策略管理平台 (AnyOffice manager) 一般部署在银行内网的数据中心，实现移动终端的资产管理、安全管控、应用管理。通过 AnyOffice manager 管理平台可对所有终端进行全生命周期管理，在提供高效业务体验的同时保障终端数据安全。

整个平台从终端接入、公私数据隔离、链路传输加密、到后台抵御网络攻击进行了端到端的安全设计，保障业务办理安全无忧。同时高效整合终端外设，让终端更加便携易用。通过部署该方案，银行可打造一个安全高效的移动金融业务办理平台。华为银行移动营销解决方案具备如下亮点：

- **统一平台集中管理**

方案提供应用统一接入平台，自带应用商店功能，支持移动应用集中部署、集中管理。平台支持单点登录，客户经理只需一次登录，所有应用通行，避免重复登录。

- **全方位终端定制支持**

作为终端厂商，方案可支持终端深度定制，如 ROM、银行 LOGO、软件预装等。且终端配套一体化背夹，该背夹集成了二代证识别器，与蓝牙刷卡器、打印机、指纹仪等柜面设备完成预集成，便携性易用性更佳。

- **SDK 快速集成能力**

方案提供具备开放接口的安全 SDK，支持第三方移动应用 3-7 天内快速集成，集成后应用具备数据加密传输、移动沙箱等安全能力。

- **国密支持，CFCA 联动**

安全沙箱、SVN 的加密功能支持国密算法，安全性能更优。可与 CFCA 证书系统进行定制对接实现证书自动化管理，屏蔽人工操作，提高证书管理效率和改善用户体验。

我们应该看到，互联网对金融业的“侵袭”正在改变传统金融业生态格局，从观念、运营模式，到资金链的流转，传统金融行业已经迈出“移动”步伐，这也预示着金融业正全面进入移动互联时代。但我们也应该对安全问题有着清晰的认识，尤其是对安全要求比较高和敏感的金融行业来说，必须全面考虑新技术所带来的风险，在保障技术促进业务发展的同时优先解决掉安全这块短板。

商标声明

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司
深圳市龙岗区坂田华为基地
电话: (0755) 28780808
邮编: 518129

www.huawei.com