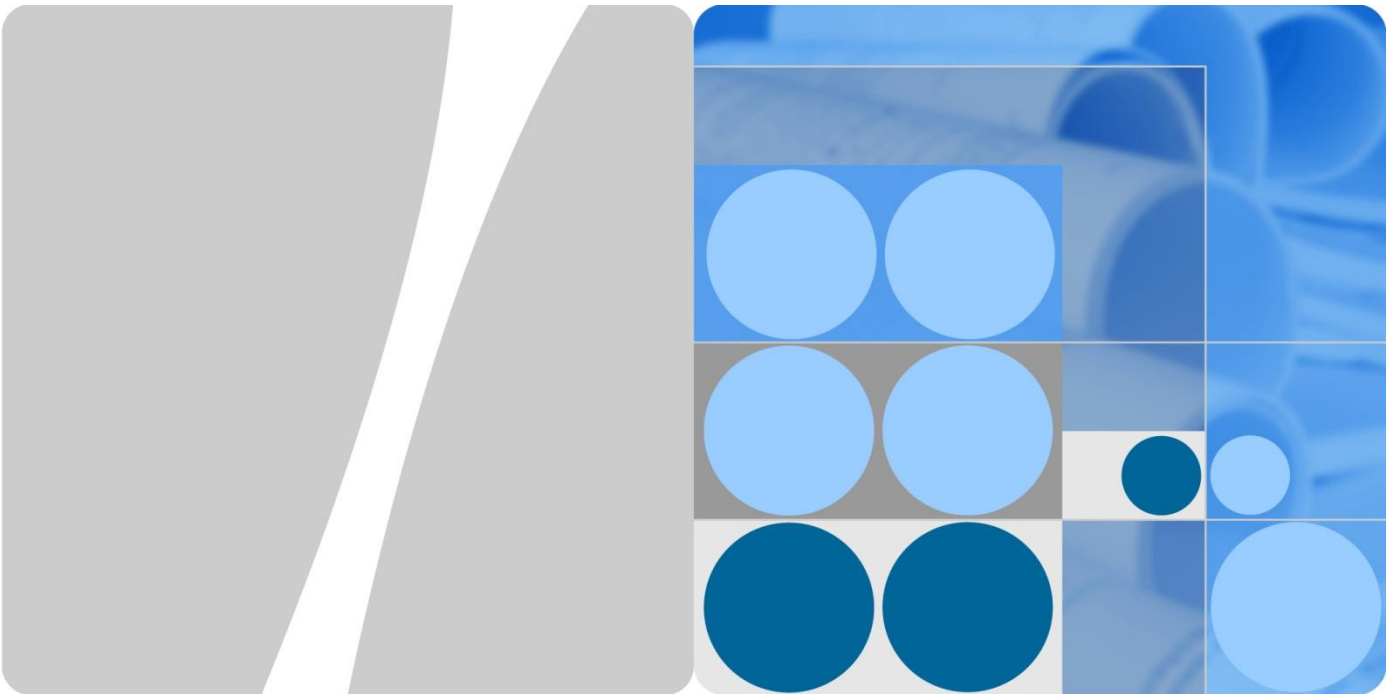


华为 AnyOffice 移动办公安全解决方案

FAQ

华为技术有限公司

目 录

缩略语清单List of abbreviations：

缩略语表

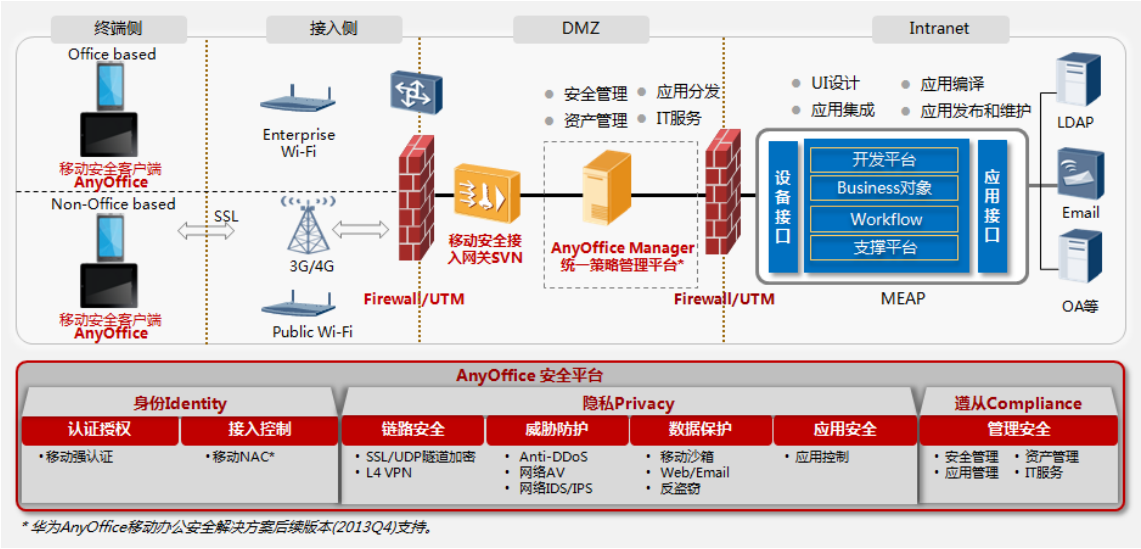
缩略语	英文全称	中文全称
AAA	Authentication, Authorization and Auditing	认证、授权和审计
ACL	Access Control Logic	访问控制逻辑
AD	Active Directory	活动目录
ARP	Address Resolution Protocol	地址解析协议
CF	Compact Flash	压缩闪存卡
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
FTP	File Transfer Protocol	文件传输协议
GE	Gigabit Ethernet	千兆以太网
HTTP	Hypertext Transfer Protocol	超大文本传输协议
IP	Internet Protocol	因特网协议
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
MTBF	Mean Time Between Failures	平均故障间隔时间
MTTR	Mean Time To Repair	平均修理时间
PCI	Peripheral Component Interconnect	周边器件插口
POP	Post Office Protocol	邮局协议
Radius	Remote Authentication Dial In User Service	远程认证用户拨入服务
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网管协议
SSL	Secure Socket Layer	安全套接层协议
TCP/IP	Transmission Control Protocol/ Internet Protocol	传输控制协议/互联网协议
TLS	Transport Layer Security	传输层安全协议
UDP	User Datagram Protocol	用户数据报协议
URL	Uniform Resource Locator	统一资源定位器
USB	Universal Serial Bus	通用串行总线
VNC	Virtual Network Computing	虚拟网络计算
VLAN	Virtual Local Area Network	虚拟局域网

1 特性概述

华为BYOD移动办公安全解决方案是针对当前BYOD移动办公的需求、特点和挑战，在保障移动办公人员顺畅、安全访问企业的同时，提供高效和良好的用户体验，实现了“安全”、“效率”和“体验”的完美融合。

华为公司凭借在网络通信领域和网络安全的技术积累和优势，在方案中融合了AnyOffice移动办公客户端、移动安全接入网关SVN2000-M/SVN5000-M系列、兼具防火墙和UTM功能的USG2200/5100/5500设备、AnyOffice Manager统一策略管理平台*。

图1 华为 BYOD 移动办公安全解决方案



其中，AnyOffice作为移动办公客户端运行在移动智能终端上；USG作为防火墙和UTM设备部署在企业网络的出入口处，负责攻击防范、网络流量的过滤和监控，移动安全接入网关SVN可以单臂挂接在出入口防火墙或者交换机上，也可以双臂挂接在防火墙和交换机之间；而AnyOffice Manager统一策略管理平台*和MEAP服务器则一般部署在企业内网的数据中心。

不同于机型统一的企业配机，BYOD设备往往具有机型多样、操作系统多样、版本多样的特点，因此，这些设备在认证、VPN接入、数据加密、MDM安全管控等方面的支持程度、实现技术也存在不同程度的差异。华为公司充分考虑了移动办公的特点、BYOD设备在移动办公

应用中的特点，从身份（Identity)、隐私(Privacy)和遵从（Compliance）三个大方面提供了全面完善的端到端的解决方案。

在终端认证授权方面，本方案充分考虑了移动办公的特点，除传统的VPNDB本地认证、LDAP、Radius、SecurID、AD认证外，还可基于企业用户的不同角色、设备归属精细控制用户访问企业内网资源的不同权限。

在链路安全方面，本方案基于企业在不同场景下的接入需求，提供了L3VPN、L4VPN、Web代理及L2TP over IPSec这几种不同的接入方式，通过AnyOffice和移动安全接入网关SVN的配合，完美解决了移动办公人员的企业内网安全接入问题，通过加密的VPN隧道，既保障用户的顺畅接入，又避免企业数据在传输过程中被非法窃听和篡改，使得用户像内网办公一样顺畅地访问内网服务器或办公PC。

在威胁防护方面，除了提供业界领先的DDoS攻击防护，还融合入侵防御和反病毒技术，提供应用层的深度防护，充分确保进出企业的流量都是干净可信的。

在数据保护方面，采用“安全沙箱”技术，将终端上的企业数据采用高强度加密算法保存，密钥不在终端保存，而是在AnyOffice成功登录网关后向网关请求获取，并且加密密钥会周期性变更。另外，企业数据与个人数据是隔离的，从终端环节进一步遏制的企业数据泄密的可能性。

在应用安全和管理安全方面，方案支持各主流移动智能终端的各项通用MDM功能，包括应用管理、资产管理、安全管控、数据管理、设备管理等，同时，利用华为终端产品团队的优势，在华为手机、华为平板上提供更加强大和丰富的MDM控制能力。

2 常见问题答复

2.1 硬件&性能

2.1.1 移动办公安全解决方案涉及的SVN/USG等设备的硬件和性能参数？

答：请参考各产品规格清单。

2.2 数据加密

2.2.1 动态隧道功能和数据加解密功能，必须实现周期性的密钥更新

答：满足。

移动安全接入网关通过动态地建立SSL隧道来实现与客户端之间的通信，同时支持多种密码算法，包括加密算法：3DES/DES、RC4、AES，Hash算法：MD5、SHA-1，非对称密码算法：RSA，保障了数据传输的安全性、完整性。默认采用AES-256加密算法进行加密，默认密钥更新周期5分钟，可设置范围1-1440分钟。

2.2.2 支持SSL加速和HTTP压缩。

答：满足。

通过使用专用的 SSL 高速硬件加密芯片，使数据加密对系统运行速度的影响降至最低。支持 HTTP 压缩。

2.3 功能业务

2.3.1 使移动用户在发生漫游之后，仍然保持与原有网络的链接，并且不影响移动用户上层协议的运行，包括Email、www浏览、FTP、VOD等网络业务

答：满足。

主要用于实现移动用户对企业内网的访问，即使在发生漫游时，仍然能保持连接，不影响业务的运行。支持广泛的网络业务，包括WEB网页浏览、MS RDP、SSH、VNC、Lotus Notes、Email、FTP 、Oracle等各种应用。

2.3.2 支持SSL加速

答：满足。

移动安全接入网关SVN提供SSL加速功能，可以在Web服务器前部署SVN网关，用户通过HTTPS协议访问Web服务器时，HTTPS协议涉及的SSL加解密操作可以在SVN网关上完成，然后SVN网关通过HTTP协议与Web服务器交互。

通过将SSL加解密操作从原本Web上执行转移至SVN网关上执行 ,降低了对Web服务器上运算能力的要求，使得Web服务器可以更加关注Web业务，能够提供更高的用户访问能力。

2.3.3 支持虚拟桌面功能

答：满足。

移动安全接入网关SVN支持虚拟桌面，用户可以从接入移动终端上登录SVN设备，进行用户认证授权后，即可在接入终端上经SVN设备访问位于内网的固定PC。接入终端通过远程桌面协议可以远程访问固定PC，用户通过这种方式远程控制固定PC，可以运行固定PC上的各种软件，进行远程办公。SVN产品为用户远程访问固定PC的数据流量在互联网范围内提供加密保护。

虚拟桌面功能特别适用于智能终端上的移动办公应用。通过使用远程桌面协议，不需要智能终端上安装各种办公软件，可以降低智能终端和内网服务器之间的数据流量，减少对智能终端上运算能力的需求。

2.3.4 支持Anti-DDOS功能

答：满足。

移动办公安全解决方案通过USG支持丰富的Anti-DDOS功能，包括以下内容

- 防范多种 DoS 和 DDoS 攻击：SYN Flood、ICMP Flood、UDP Flood、Get Flood、WinNuke、ICMP 重定向和不可达报文、Land、Smurf、Fraggle、IP Spoofing 等；
- 防范扫描窥探：包括地址扫描、端口扫描、IP 源站选路选项、IP 路由记录选项、时间戳、刺探路由；
- 畸形报文攻击：畸形 IP 分片报文、畸形 TCP 报文、超大 ICMP 报文、TearDrop、Ping Of Death；

2.3.5 SDK安全组件是否能和具体应用集成，具有良好的终端平台兼容性？

答：满足。

通过华为公司的Dopra抽象层和各个具体的操作系统适配对接（目前，支持的操作系统包括iOS、Android、Windows、Symbian、BlackBerry），屏蔽底层操作系统的差异，向上提供统一的本地加解密接口、数据加密传输接口，方便各类自研及第三方的应用集成，使之具备数据加密传输、本地数据加密等能力。

2.3.6 移动终端办公业务有哪些关键组件，支持在哪些平台上运行？

答：移动办公业务关键组件有AnyOffice移动办公平台、安全PushMail、安全浏览器及企业发布应用。支持移动平台有Android4.0、Android4.1、iOS 5.0及以上。

2.3.7 移动办公AnyOffice客户端平台与安全PushMail、安全浏览器之间相互关系是怎样的？

答 :AnyOffice客户端是移动办公重要安全组件 ,提供移动终端办公业务入口。 AnyOffice软件包预装安全浏览器、安全PushMail，并为安全浏览器、安全PushMail及其他企业应用，提供L4VPN隧道及本地数据加解密。

2.3.8 移动办公AnyOffice平台除预置应用外还有哪些功能？

答：AnyOffice办公平台除预置应用外，还支持从企业应用商店下载软件包，添加本地应用；支持用户自行添加或通过SVN网关下发以桌面图标方式添加内网URL链接到办公平台桌面；与SVN网关建立L4VPN隧道，并提供接口供上层应用调用。

2.3.9 移动办公AnyOffice平台支持哪几种工作模式？不同模式下加密密钥是否相同？

答：AnyOffice平台有两种工作模式，在线模式和离线模式。在线模式，AnyOffice需要输入用户名密码通过集成的L4VPN登录到SVN网关，并从网关获取动态密钥，通过密钥对本地应用数据加密。 离线模式，当用户配置了离线权限时，AnyOffice工作中不与网关进行交互，加解密文件时使用本地密钥，本地密钥通过用户登录口令进行保护。

2.3.10 L3VPN与L4VPN在移动终端数据传输模式有何差异？L4VPN相对L3VPN有何优势？

答：采用L3VPN登录模式时，移动终端上所有软件（包括病毒、木马）都可以通过L3VPN隧道访问企业内网；采用L4VPN登录模式时，只有集成SDK的安全应用才可以通过L4VPN隧道访问企业内网。L4VPN只对集成SDK的安全应用，向内网传输业务数据，同时数据到达网络层之前就已经经过加密，能够有效防止病毒、木马进行侦听和嗅探。

2.3.11 安全浏览器与常见浏览器如UC、Firefox、Chrome、Safari有何区别？

答：安全浏览器是华为自研浏览器，支持Android 4.0以上、iOS 5.0移动平台。

- 提供安全沙箱，支持Office、文本、图片、压缩文件等办公所需文档格式的在线或离

线安全浏览，实现公司数据与个人数据的隔离；

- 提供数据加解密保护，支持离线资源、密码、下载的文件、访问历史、Cookies和临时文件的在线加解密能力；在退出浏览器时，可按照策略自动清理缓存和配置
- 支持访问行为管控，基于URL黑白名单的管控，并根据策略限制文件上传、下载和保存等行为；

安全浏览器用来从外网访问企业内网（Intranet），数据报文采用密文，而普通浏览器一般用来访问互联网（Internet），数据报文采用明文。

2.3.12 安全浏览器的安全沙箱技术是否安全，能否真正实现数据隔离？

答：安全沙箱在应用与系统中间构建一个虚拟的隔离区域，可疑程序和应用被转移到真实系统之前，我们可在这个隔离区域中对它们进行下载，解压和测试等操作，从而达到拦截恶意程序的目的。目前主流厂商都在使用沙盒技术防范各种安全风险，如谷歌、卡巴斯基、苹果。

2.3.13 安全PushMail邮件与普通邮件软件如Outlook、Foxmail等有什么区别？

答：PushMail客户端是支持DirectPush技术的邮件客户端。PushMail的主要用途是为用户提供安全受控的即时邮件推送服务。

- 邮件加密，传输加密方式支持全系列的SSL/TLS协议，支持客户端/SVN间传输加密；支持客户端/邮件服务器间传输加密
- 邮件在线浏览，支持Office和文本文件浏览；支持压缩文件浏览；支持图片文件浏览；
- 邮件控制策略，支持邮件附件的访问、转发策略控制；支持邮件内容转发策略控制；支持离线登录邮箱的权限策略控制。

- 本地数据加密：支持对PushMail本地数据库加密、本地配置文件加密、本地目录以及文件名加密、本地邮件正文加密、本地邮件附件加密
- 本地数据隔离：通过PushMail添加和下载附件时，策略控制是否允许可以从非工作目录获得或存放

2.3.14 通过安全PushMail从邮件服务器获取的邮件（正文、附件）在移动终端本地加密是如何实现的？

答：PushMail客户端会调用AnyOffice平台提供的低层数据加密接口，对本地数据进行透明加解密。也就是说PushMail客户端能够在在线模式和离线模式下查看安全邮件，移动终端上其他应用无法访问和打开PushMail客户端下载的邮件。

2.3.15 安全PushMail有哪些邮件控制策略？

答：PushMail能够对邮件发送权限进行控制，能够对邮件附件进行控制，包括附件上传、下载、转发、在线浏览控制策略，第三方浏览控制策略及邮件本地保存时间。

2.3.16 通过安全PushMail与移动办公AnyOffice平台能否实现单点登录？

答：当PushMail邮件登录用户、密码与移动办公AnyOffice平台一致时，可以实现单点登录，即登录AnyOffice平台后，无需再次输入密码，直接登录PushMail邮件系统。

2.3.17 为什么要检查终端是否越狱？如何探测员工Pad Jail Break（越狱或Root），技术如何实现？

答：在不越狱的移动智能终端上系统权限低，不能删掉系统自带应用、不能对系统文件和

设置进行修改、不能安装第三方输入法以及其它未经苹果App Store认可的应用程序等等；越狱后将获得更高的用户权限后，可以修改系统文件、可以安装更多拥有高系统权限的应用程序，从而实现更多高级功能。同样，未经审核安装的程序中隐藏的病毒、木马也将获取到更多的用户隐私信息和更高的权限。

移动安全接入网关SVN通过向移动智能终端下发指令，使其执行系统权限命令、访问系统文件来进行检测，判断越狱情况。越狱的基础是获取了超级权限，从而对系统拥有了超级权限，检测也是从这个方面入手。

2.3.18 华为方案在iOS和Android分别实现的MDM安全特性上有何差异？

答复：iOS系统封闭，成熟，所有MDM厂商在iOS上能力基本一致，苹果公司提供了丰富的接口，但是不能完全满足客户的定制化的需求；Android系统开放，MDM功能都是需要新开发，对硬件的控制范围可以更大。

2.3.19 移动用户权限管理特性，技术如何实现？

答：用户权限体现在各个方面：

1) 用户通过AnyOffice客户端登陆移动安全接入网关SVN时，SVN会根据用户所属角色下发各种终端策略，包括限制（密码限制，设备控制）和能力（Wi-Fi，Email等）；移动终端MDM组件通过执行策略，实现设备权限控制

2) 用户登录AnyOffice后，通过安全浏览器或其他移动应用访问内网时，SVN会根据其所属角色对应的访问策略，允许或拒绝其网络访问行为。

3) 用户通过AnyOffice访问企业应用商店时，会根据管理员为角色制定的应用权限策略，授权其访问到对应的应用，进行下载和安装

2.3.20 方案中MDM平台和安全网关是否可以不同厂商供应？

答：不能，华为移动安全接入网关SVN除提供MDM功能外，还能为安全Pushmail，安全浏览器及集成安全SDK的企业应用，提供应用级加密传输隧道（L4VPN），本地文件在线加解密、安全沙箱等能力；MDM能够与这些安全应用进行联动，提供终端准入策略检查，只有通过检查的终端才允许访问安全应用，这些通过第三方安全网关无法实现。

2.3.21 PushMail在线浏览功能如何实现，如果集成文档Viewer升级（比如Office文档由2003版本升级到2007版本），如何解决？

答复： AnyOffice自带工具浏览时,会判断文件类型，调用相应的方法打开；集成文档Viewer升级可通过升级AnyOffice客户端实现。目前AnyOffice支持Office、文本、图片、压缩文件等办公所需文档格式的在线或离线安全浏览，实现公司数据与个人数据的隔离。

2.3.22 华为安全Pushmail是否可实现微软的Exchange和IBM的Lotus Notes，如何实现？

答复：安全Pushmail兼容微软的Exchange 2007、2010服务器，支持IBM Lotus Notes 8.0、8.5邮件服务器。通过IMAP协议实现接收邮件，SMTP协议实现发送邮件，其中Exchang邮件系统的日历、联系人同步通过EWS协议实现，Notes邮件系统的日历、联系人同步通过EAS协议实现。

2.3.23 华为移动办公Push Mail邮件功能需实现日历、联络人功能，是否需要每次登录更新？

答复：目前Pushmail每次登录时会同步一次日历和联络人（只同步个人联络人），之后

日历会实时更新。日历功能允许用户通过电子邮件的方式发送“会议请求”或“任务”。收信人使用支持日历功能的邮件客户端时，可以将“会议请求”或“任务”同步到日程安排中，并可按照日历设置进行会议或任务提醒。

2.3.24 部署华为移动办公方案需要哪些涉及的软件和设备列表，软件部分需包括iOS和Android ？

1) 硬件部分：

必选：移动安全接入网关SVN

可选：防火墙、MDM数据服务器

2) 软件部分：

AnyOffice客户端iOS版本或AnyOffice客户端Android版本

必选组件：无

可选组件：MDM组件、安全Pushmail、安全SDK、安全浏览器、虚拟桌面及统一通信(由UC&C产品线销售)

2.3.25 如何实现资产注册和资产注销（如果是员工自己PAD）？

答：

AnyOffice客户端获取：管理员通过短信或邮件方式发布一个URL，员工可以通过认证账号登陆下载安装AnyOffice客户端程序 ;或直接通过访问官方应用商店(如APP Store、Google Play）下载AnyOffice客户端程序进行安装。

移动终端资产注册（支持两种方式）：

1) 使用AnyOffice登陆时，可以进行自助注册，管理员审批后，即可进行移动办公；

2) 管理员对移动终端进行批量资产注册，注册后用户即可使用移动终端通过AnyOffice客户端直接登录访问。

移动终端资产注销（支持两种方式）：

1) 管理员通过MDM服务器控制台，解除终端资产绑定；被解除绑定移动终端，配置文件、AnyOffice客户端及企业应用程序被卸载，应用数据被清除；

2) 通过自助网站，员工可以解绑定自己的设备，员工设备绑定解除后，被解除绑定移动终端，配置文件、AnyOffice客户端及企业应用程序被卸载，应用数据被清除。

2.4 协议与规范

2.4.1 支持SSL通信协议SSL3.0和TLS1.0

答：满足。

SSL加密传输支持的SSL协议版本有SSL2.0、SSL3.0和TLS1.0。

2.4.2 安全浏览器支持哪些页面类型及通讯协议？

答：安全浏览器支持HTML/SHTML/XHTML/DHTML页面访问，支持HTTP（1.0，1.1）HTTPS（TLS1.0，SSL2.0，SSL3.0）协议

2.4.3 安全PushMail邮件支持哪些邮件协议？

答：支持SMTP、IMAP4 、EWS、ActiveSync等邮件协议；支持通过SSL/TLS协议对客户端/网关，客户端/邮件服务器间邮件传输进行加密。

2.4.4 SDK有哪些成功应用集成案例？

1) AnyOffice

AnyOffice就是一个集成了安全SDK的典型应用，AnyOffice内置的“安全浏览器”和“安全邮件”两大功能模块共用了安全SDK提供的“数据加密传输接口”进行VPN隧道的建立、WEB业务数据和邮件数据的加密传输，共用安全SDK提供的“文件加解密接口”进行了邮件正文、邮件附件、浏览器下载文件等的本地加密存储。

2) UC

UC是华为推出的一款IM软件，它具有即时消息、文件传输、音频及多方会议、语音通话等丰富的功能，目前，它已推出了移动客户端，支持iOS4.0及以上版本（iPhone 3GS/iPhone 4G），Android 2.1及以上版本（如HTC G12/Huawei U8800等）。目前，eSpace的移动客户端也已集成了安全SDK，具备了加密数据传输能力。

2.4.5 对移动应用实现安全加固有两种方法：一通过App Wrapper工具处理；二通过SDK二次开发集成。两者有哪些优劣势？使用App Wrapper安全打包工具是否就可以不用找移动应用的软件开发商了？

答： App打包方式无法支持从苹果AppStore下载的标准应用，需要向软件供应商的研发部门提供特殊版本，才可支持，优劣势对比表如下：

移动应用安全加固方法	App Wrapper工具处理	SDK二次开发
处理方式	每次版本升级时，都需要向软件供应商研发部门申请特定的未签名包或	第一次需让软件供应商集成SDK，并发布标准安装包。然后通过企业版发布证

	ADHoc方式签名的iOS安装包，然后通过工具进行安全加固处理和企业版发布证书签名后发布	书签名。后续不需要单独申请版本，只需获取标准安装包，进行企业版发布证书签名即可。
沟通频率	针对iOS，每次版本发布均需要联系原厂处理	第一次集成工作量大，后续每次只需做发布签名
灵活性	无法针对子特性进行是否走隧道或沙箱的控制	可以灵活控制各种子功能是否需要安全能力，不过度使用
限制条件	无法对Apple AppStore应用进行集成	无限制
兼容性	每次版本更新都需要对二进制进行类似反编译和改写，误修改可能导致软件不稳定，必须自行充分验证才能发布	首次集成和每次版本更新时，都会由软件开发方进行充分验证，质量易保证。

总结

华为的安全SDK具备跨平台、易集成的特点，各类应用的开发者只需要少量的适配工作即可让业务应用具备典型的安全特性。目前安全SDK提供了数据加密传输（包括自动建立和SVN网关之间的VPN隧道）、文件加密、本地数据加密接口，后续的版本将根据移动办公安全需求而集成更多的安全特性，譬如，数据隔离、行为监控等。

商标声明

 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118