 [摘 要] 移动支付是将移动网络作为实现移动支付的工具和手段，为用户提供货币支付等金融服务，文章介绍了移动支付在电子商务环境下的技术实现及各支付环节所要关注的安全要求，并介绍了目前应用较广泛的安全标准WPKI。 [关键词] 电子商务 移动支付 安全认证 WPKI 电子商务环境下的移动支付是指单位或个人通过移动设备，直接或间接向银行业金融机构发出支付指令，实现货币支付与资金转移的行为移动支付所使用的移动设备可以是手机、PDA、移动PC等。从移动支付的实质上讲，移动支付就是将移动网络与金融系统结合，把移动网络作为实现移动支付的工具和手段，为用户提供货币支付、缴费等金融服务的业务。移动支付通常有以下几种实现方式:(1)短信（SMS）支付，终端用户通过发送短消息的形式请求服务内容，从用户的话费中扣除费用，通常只适合于小额支付。(2)WAP（Wireless Application Protocol），终端用户通过访问WAP站点，进行简单的金融业务。（3）USSD(Unstructured Supplementary Service Data，非结构化补充数据业务)，是一种基于GSM网络的新型交互式数据业务，如证券交易、移动银行业务。（4)NFC（(Near Field Communication），是一种短距离的无线连接技术，支付和票务业务是应用最早的NFC业务。 一、移动支付中的安全问题 在整个移动支付的过程中涉及到的支付参与者包括：消费用户、商户用户、移动运营商、第三方服务提供商、银行。消

费用户和商户用户是系统的服务对象，移动运营商提供网络支持，银行方提供银行相关服务，第三方服务提供商提供支付平台服务，通过各方的结合以实现业务。移动支付需要考虑以下安全问题：（1)移动终端接入支付平台的安全，包括用户注册时，签约信息的安全传递，以及用户通过移动终端登录系统，其间传递的数据如签约用户名、签约密码等的安全性。(2)支付平台内部数据传输的安全，即支付平台内部各模块之间数据传输的安全性。(3)支付平台数据存储的安全，涉及到签约用户的机密性的银行卡账户、密码、签约用户名、签约密码等的安全性。 二、移动支付的安全认证技术 当前，移动设备的大量普及为移动支付的实现提供了必要的条件，但也存在许多问题制约着移动支付的实施，如移动终端的计算环境和通信环境都非常有限，这就需要对相应的安全认证做一些特殊要求。 1.WPKI 安全标准概况 WPKI (Wireless PKI）是有线PKI的一种扩展，它将互联网电子商务中PKI的安全机制引入到移动电子商务中。WPKI采用公钥基础设施、证书管理策略、软件和硬件等技术，有效地建立了安全和值得信赖的无线网络通信环境。WPKI以WAP的安全机制为基础，通过管理实体间关系、密钥和证书来增强电子商务安全。WAP安全机制包括WIM（WAP Identity Module，无线应用协议识别模块）、WMLSCrypt（WML Script Crypto API，WML脚本加密接口）、WTLS（Wireless Transport Layer Security，无线传输安全层）和WPKI四个部分。以上各部分对实现无线网络应用的安全分别起着不同的作用。WPKI作为安全基础设施平台，一切基于身份验证的应用都需要WPKI技术的支持，它可与WTLS、TCP/IP相结合，实现身份认证、私钥

签名等功能。WPKI的主要组件包括：终端实体应用程序（EE）、PKI门户（PKI Portal)、认证中心（CA）、目录服务(PKI Directory)、WAP网关，在应用模型中还涉及数据提供服务器等设备，WPKI的基本结构和数据流向如图所示。 在WPKI中，代替RA（Registration Authority）的功能组件是PKI 门户（PKI Portal ），它是一个网络服务器，负责把WAP客户的需求转发给PKI中的RA和CA（Certification Authority）。CA主要负责生成证书、颁发证书和刷新证书等。WAP Gateway负责处理客户与源服务器之间的协议转换工作。WTLS 是经传统网络的TLS协议改进和优化而得来的，主要保证传输层的安全，WPKI也是对IETF PKIX标准的优化，使之更适合无线环境。 2.WPKI的加密算法和密钥 WPKI是通过管理实体间关系、密钥和证书来增强电子商务安全的，与WAP安全标准相比，WPKI所采用的ECC（Elliptic Curve Cryptography，椭圆曲线密码）密码系统更适合在无线设备中使用。同样强度的密钥，ECC的密钥长度（163bit）只是其他方案的六分之一(1024bit），但163bit的密钥长度对穷举密钥攻击几乎是绝对安全的，因为穷举163bit的密钥个数有1.156×1049个，按每秒钟测试1亿个密钥计算，也要3.6×1032年！来源于百考试题 三、 结论 支付手段的电子化和移动化已经成为了不可避免的发展趋势，而移动支付系统的安全性问题又是移动电子商务安全的核心问题。从技术角度上看，需要将无线通信的安全与其他的安全机制相结合才能满足移动电子商务安全的需要。 参考文献： [1] 关振胜:公钥基础设施PKI及其应用[M].北京:电子工业出版社 [2]WAP Forum.Public Key Infrastructure Definition. WAP Forum,Http://www.wapforum.org. 2001 F8F8" 100Test 下载频道