摘要： 本文介绍了安全移动电子商务的概念与应用，分析了实现安全移动商务的国际标准 WAP，构建安全无线商务环境WPKI的概念与安全机制，并且给出了两种基于WPKI认证环境的 模型与过程。

关键词： WAP WPKI PKI 移动电子商务 网络安全

Research of Secure Mobile E-commerce

安全移动电子商务研究

张浩军 （解放军信息工程大学 信息工程学院 450002）
李晓雪 （河南郑州 河南省农业银行科技处 450002）
祝跃飞 （解放军信息工程大学 信息工程学院 450002）

1 引言

无线通信设备（数字蜂窝手机、无线个人通信助理PAD）以其不受物理连接限制便携之优点 提供了比传统有线通信更广阔的应用。随着手机的功能及无线通讯性能的提升，移动商务的 应用将会越来越盛行，如移动定票、移动银行、移动政务、移动购物等等。权威机构估计20 02年整个全球移动上网的市值达两亿七千万美元，而在2004年时则可高达七亿五千万美元。

安全是电子商务（含移动商务）核心技术问题，各种应用有不同的安全要求，主要包括身份 验证、数据加密、数据完整性、不可抵赖性等，目前实现安全电子商务的最成熟和最有效的 方法是借助公共密钥基础设施PKI。

2 PKI

PKI（Public Key Infrastructure，公钥基础设施）是在局部或公共的环境中提供可信任并且有效率的密钥及认证管理，其功能包括了对数据加密所得的机密性，利用数字签名而产生 的不可否认性和资料数据一致性的验明，以及对认证用的密钥、密钥持有人、应用程序、认 证服务、与进入控制提供验证。换言之，PKI是利用一套完整的政策、人、过程；技术与服 务来大规模管理及运用公开密钥体制进行加解密与数字认证。简单来说，PKI机制的运行包 括了使用者、凭证管理系统、注册机构（RA）、认证机构（CA）与认证查验系统（Certific ate update/revocation）。利用PKI机制是目前实现Internet上安全电子商务最有效的办法 。

3 WAP

WPKI（Wireless PKI）的安全机制是建构在WAP的安全机制上，WAP是迄今移动通信上的唯一 国际标准协议。Motorola、Nokia等一些世界著名移动通信公司1997年成立了WAP论坛，旨在 共同设计和开发无线应用协议(Wireless Application Protocol, WAP)，通过定义一个开放 的全球无线应用框架和网络协议标准，将Internet上的应用和服务引入移动电话等无线终端 。

3.1 WAP 工作机理

图1给出了Internet环境、WAP对Internet扩展环境，以无线通信为基础的WAP与以有线IP网 络为基础的Web环境存在着一些主要的区别：与常规的Web客户端设备（PC）相比，无线端 设备有着较弱得到处理能力，如

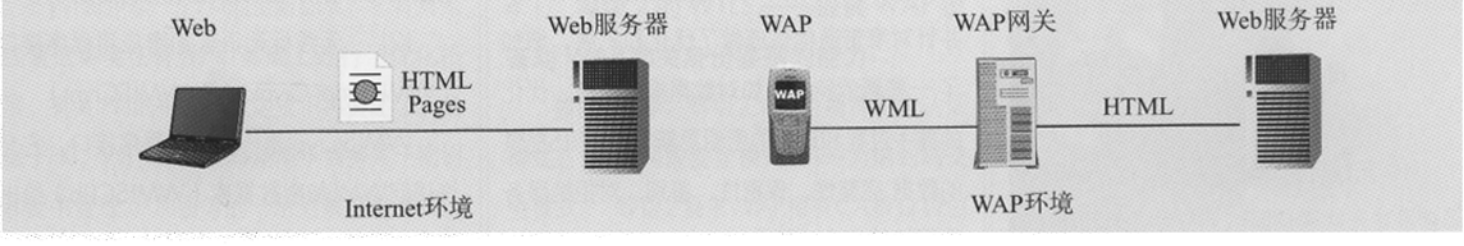

图 1 Internet 环境与 WAP 环境

处理能力较弱的CPU、较少的内存及数据和程序存储器、较 低的网络带宽和较小的显示屏；无线设备的有限处理能力要求WAP环境中服务与软件必须非 常有效，故WAP协议与Web协议存在不可互操作性；为了实现两种环境协议的互相转换，需要 设定WAP网关（WAP Gateway）。网关实现协议的转换，如WAP与网关采用WTLS安全协议连接 ，以WML标记语言传递内容；而网关与Web（内容）服务器以TSL/SSL安全协议连接，以HTML标记语言传递内容。

3.2 WAP协议栈

图2、图3给出了与Internet连接的WAP协议栈结构。

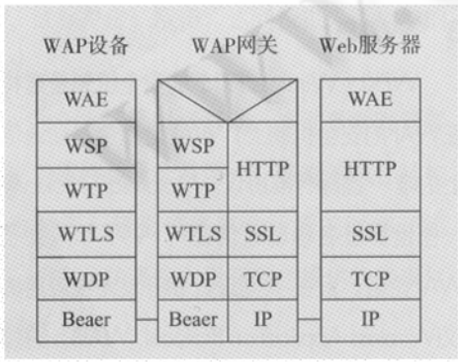

图 2 WAP 1.x 结构

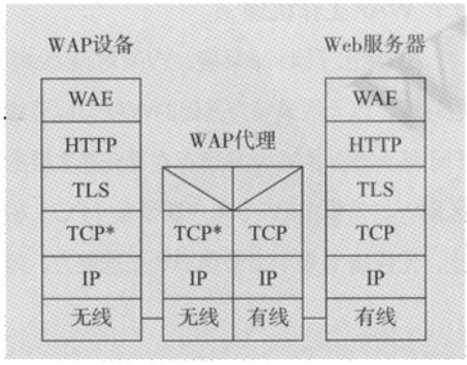

图 3 WAP 2.0 结构

(1) 无线应用环境（WAE）。WAE是为了满足在无线通信网络上开发应用和服务而制定的工业标准及规范，提供在各种不 同的无线平台上建立一个可互操作的通用应用环境，使网络经营者和服务提供者可在上面建立应用与服务。

(2) 无线会话协议（WSP）。WSP向WAP应用层提供两种会话服务的统一接口，还特别针对低带宽和高时延的承载网络进行了优化，这两种会话服务是：操作在事务处理层协议WTP之上的面向连接的服务、操作在数 据报协议WDP之上的无连接服务。目前，WSP协议主要包含适合于浏览器应用（WSP/B）的服 务，包括压缩编码下的HTTP/1.1的功能和语义、会话管理、“推”操作等。

(3) 无线事务协议（WTP）。WTP运行在数据报服务之上，提供适合于移动终端和无线网络的有效的基于交互式事务型应 用（请求/响应型）的运输服务。WTP针对移动终端受限的计算环境和无线网络受限的通信环 境做了优化，并且还特别兼顾了Web浏览等交互式事务型应用（具有非对称性、数据传输的 单向性、持续时间短、传输分组少和面向报文等特征）的通信需求。

WTP无显式的连接建立和拆除过程是面向报文的，定义了用于不可靠的“推”、可靠的“推”和基本请求/响应型应用三类报文传输服务。WTP通过唯一的事务标识符、确认和重传机制 以及重复删除等手段来保证事务的可靠性，还提供了可选的用户确认功能以及分段重组和选 择重传功能（用于提高协议的无线传输效率）。

(4) 无线运输层安全（WTLS）。WTLS是运行在无线事务层和无线数据报层之间的一个可选协议。WTLS基于工业标准运输层安全协议（TLS，其原称为安全套接层 SSL），并针对窄带通信信道做了优化和扩展，增加了 一些新的特性，如对数据报的支持、优化的握手过程和动态的密钥更新等。WTLS提供的数据 完整性、保密性、鉴别、对拒绝服务的保护的安全功能。

(5) 无线数据报协议（WDP）。WDP工作在由不同无线窄带网络类型所支持的数据承载服务之上，提供不可靠数据报服务， 向上层协议提供一致的服务和在可用载体服务上透明的通信功能。WDP能够独立于低层的承 载网络，由于短消息服务、交换式数据服务和分组数据服务等各种承载网络提供不同的服务 质量，包括带宽、吞吐量、误码率、时延等参数，WDP通过将运输层与低层载体的特殊性质 进行适配，能够补偿这些差异的影响，并通过协议优化提高服务质量。

无线控制报文协议（WCMP）规范了WDP数据报的错误报告机制，它模仿Internet控制报文协 议（ICMP），由WDP结点和无线数据网关报告处理数据报时出现的错误，也用于诊断和信息 报告。对于支持IP的承载服务，WDP必须是UDP，WCMP也必须是ICMP。

WAP2.0标准对1.0有较大改进，但兼容1.0标准。如标记语言可以使用WML/WML2或XHTML，安全层协议可以直接使用有线网络的TLS协议实现端到端的安全连接，可以直接使用IP、优化的TCP协议，总之与有线网络协议兼容性增强了，此时WAP网关由WAP代理所取代。

3.3 WAP安全机制

WAP安全机制包括了以下内容：

(1) WAP 身份模块（WAP Identity Module, WIM）

WIM是安装在WAP设备（手机、PAD等）中一个防篡改的计算机芯片，它可以存储诸如PKI根公 钥和用户私钥等密钥信息。目前WIM普遍使用智能卡实现，智能卡还可以包含内存和用于存 放数据和程序的外存。

(2) 无线标记语言加密应用程序接口（WML Script Crypto API, WMLSCrypt）

WMLSCrypt是一个应用程序接口，它允许访问WML加密数据库（WMLSCLib）给出的安全功能， 例如产生密钥对、数字签名，

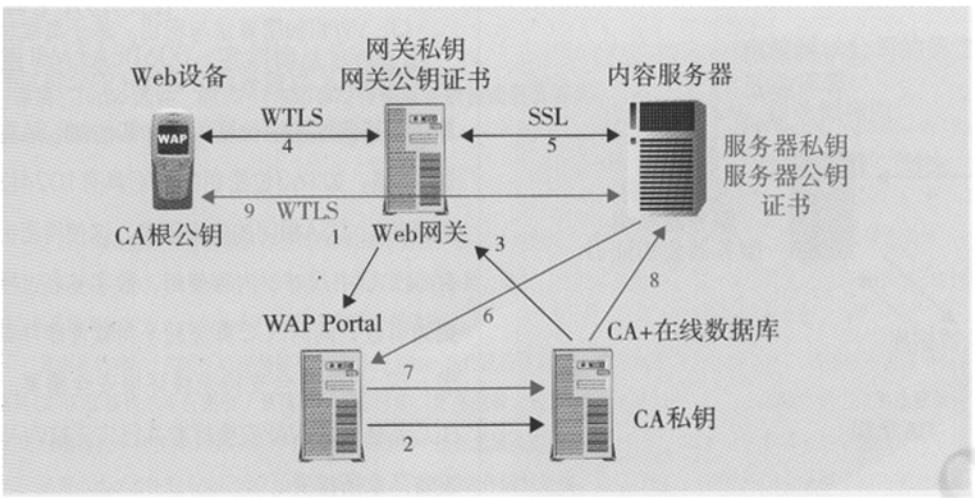

图 4 等级2WTLS认证过程

使用PKI中的处理如密钥与公钥证书等对象的一些常规功能。 基本的WMLSCrypt和WMLSCLib包括：密钥对产生、存储密钥和其他个人信息、对存储的密钥 及数据的访问控制、产生和验证数字签名、加密/解密数据。

(3) 无线传输层安全（the Wireless Transport Layer Security, WTLS）

WTLS作为以加密技术为基础实现PKI功能的协议提供四个方面安全服务：(1)鉴别：实现移动 终端与应用服务器之间的鉴别，它使用数字签名、公钥证书鉴别个人、服务方和节点。(2) 保密：保证在移动终端与应用服务器之间传送数据的隐私性，不能被接收到数据流的中间方 所理解。(3)完整性：保证所传输的交易信息不被中途篡改及通过重复发送进行虚假交易。W TLS采用一种散列加密方法实现数据签名防止数据篡改。(4)对拒绝服务的保护：WTLS能检测 并丢弃重播的或验证失败的数据。

(4) 无线应用公钥基础设施（Wireless Application Protocol PKI, WPKI）

WPKI并非一个PKI的全新标准，它针对无线通信环境在有线PKI基础上进行了优化拓展。有关 PKI的相关知识这里不再赘述了。类似于PKI，WPKI是实现移动电子商务关于密钥和证书管理 、加密等的一系列策略与过程。WPKI关心的是使用这些策略，在无线通信环境通过使用WTLS 和WMLSCrypt实现电子商务和安全服务。在有线网络环境中一般采用IETF的PKI标准，而在无 线网络环境中一般使用WAP论坛的WPKI标准。

4 WPKI

WPKI主要组成内容与PKI一致，包括四个部分：终端实体应用程序EE、注册中心RA、认证中 心CA、目录服务，WPKI中的EE是为适应在WAP设备中运行而设计的优化软件，它依赖WMLSCry pt API实现密钥服务和加密操作，当然它也具有PKI常规功能：产生、存储并允许访问用户 公钥/密钥对；首次证书申请；证书更新请求；证书撤消请求；查询、恢复和撤消证书信息 ；验证证书和读取证书内容；产生和验证数字签名。

WPKI注册机构（PKI Portal）是一个网络服务器（有时集成在WAP网关），其逻辑上行使RA 功能，并负责将WAP客户产生的请求在PKI中的RA与CA之间传递，实现与无线网络中的WAP设 备和有线网络中的CA互相操作。

4.1 等级 2 的 WTLS——提供 WAP 设备对 WAP 网关身份鉴别的能力

如图4所示，等级2又分为两种安全认证模式，1-5为两段安全模式，1-9为端到端安全模式。 等级2要求WAP持有CA根公钥信息，操作过程如下。

(1) WAP网关生成密钥对（公钥/私钥），并向WPKI Portal发送证书请求；

(2) WPKI Portal验证ID并将请求转发给CA；

(3) CA将网关公钥证书发给WAP网关，并将WAP网关证书添加到在线数据库中；

(4) 在WAP设备与WAP网关之间建立WTLS会话连接；

(5) 在WAP网关与内容服务器之间建立SSL/TLS会话连接。

以下操作仅对端到端安全模式：

(6) 内容服务器向PKI Portal发证书申请请求；

(7) Portal验证ID将请求转发给CA；

(8) CA向内容服务器发放证书；

(9) 在WAP端设备与内容服务器之间以WAP网关（对网关不透明）为路由建立WTLS会话连接 。

4.2 等级3的WTLS——数字签名的安全交易实现

通过数字签名实现端到端的安全交易，这种情况需要WAP端设备与服务器事先都拥有CA根公 钥。采用singText机制使用WMLScript生成数字签名。数字签名过程（如图5所示）如下：

(1) WAP端设备通过WPKI portal申请证书；

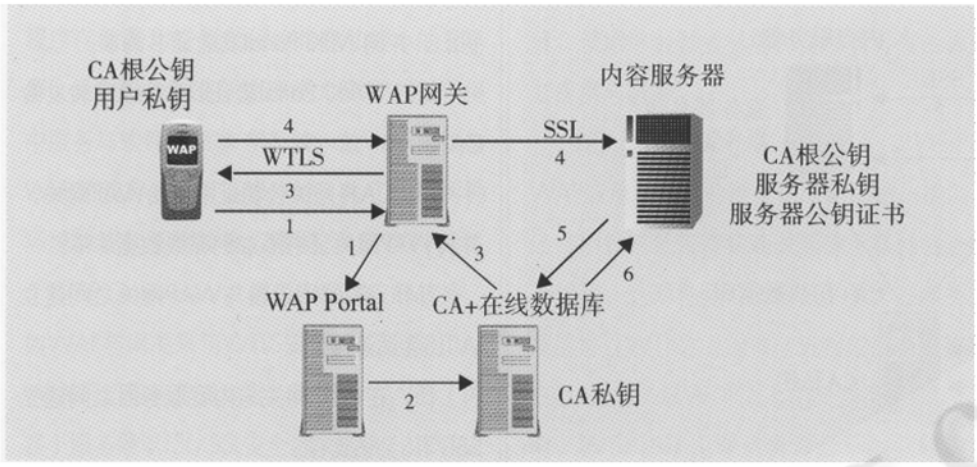

图 5 等级 3WTLS 认证过程

(2) WPKI Portal确认用户ID并将请求传递给CA;

(3) CA生成用户证书并将证书URL(或完整证书)发送给WAP设备,并将证书添加到数据库 中;

(4) 用户在WAP设备上对交易签名,并将交易信息、数字签名及证书URL(或证书)发送给 内容服务器;

(5) 内容服务器依据用户提供的证书URL从数据库中恢复用户的证书;

(6) CA数据库将用户证书发送给内容服务器;

(7) 内容服务器使用用户证书鉴别WAP设备发来的交易信息。

4.3 优化的 WPKI

正如WML是HTML的优化,WTLS是TLS的优化,WPKI是针对无线环境对IETF的PKIX标准的优化, 主要体现在WPKI协议、证书格式、和加密算法与密钥几个方面。

(1) WPKI协议。有线PKI环境使用ASN.1基本编码规则(Basic Encoding Rules, BER)和增强编码规则(Dis tinguished Encoding Rules, BER),而BER/DER对处理资源的要求超出了WAP设备能够有效 处理的能力。WPKI协议通过使用WML和WMLSCrypt,如数位签名(SignText)功能,在编码和 提交PKI服务请求时性能有显著提高。

(2) WPKI证书格式。WPKI为了减小公钥证书存储空间,一种机制是定义新的证书格式——WTLS证书格式,比X.50 9证书格式尺寸(大小约2K,对于仅有8k容量大小的SIM卡来而言,仍属负担)明显减小。另 一种机制在证书格式上使用能储存大于100 bytes椭圆曲线密码机制(Elliptic Curve Cryp tography, ECC),并且密码机制演算也需符合ECC及能用占较小内存的密钥。由于ECC相对 其他加密机制有较小的密钥,使得证书总尺寸的缩小。同时WPKI对IETF PKIX证书格式中的 一些字段尺寸做了限制,由于WPKI是PKIX的子集,保证了这些PKI标准的互操作的可能性。

(3) WPKI加密算法与密钥。基于离散对数难题的ECC目前被认为最优化的公钥加密算法,其典型密钥长度可以比其他如R SA算法小6倍,如163位密钥的ECC具有1024位密钥RSA、DSA相同的安全强度,这使得密钥存 储、证书尺寸、内存使用、数字签名过程更为有效,同时ECC算法易于用软件硬件实现,因 此最适合支持无线环境安全需要。ECC完全支持WAP安全标准并已广泛被WAP设备厂家所接受 。

5 结束语

随着GPRS、3G无线通信技术的发展与应用,无线通信性能、带宽有显著提高,且用户费用越 来越低,使得其在电子商务领域领域中应用更加广泛。有线网络(Internet)中使用IETF P KI实现安全的电子商务,无线环境中使用W P K I实现安全的移动商务(m-commerce)。WPKI是 有线环境PKI的扩展,当然包括PKI的主要技术与内容,像WAP环境中的其它安全与应用服务 一样,WPKI必须使用优化的更为有效的加密与数据传输技术,确保资源有限的个人无线设备 在有限的通信带宽下工作,以实现安全的移动商务。目前WPKI技术的互操作性及相关国际立 法是架构移动商务的需要不断完善的问题。

参 考 文 献

1 Chan Yeob Yeun and Tim Farnham. Secure M-Commerce with WPKI [EB/OL]。 http://www.iris.re.kr/iwap01/program/download/g07_paper.pdf. 2002-11-2。

2 WAP Forum: Wireless Transport Layer Security [EB/OL], http://www.wapforum.or g/. 2002-10-5。

3 WAP Forum: Wireless Application Protocol Public Key Infrastructure [EB/OL], http://www.wapforum.org/. 2002-10-5。

4 [美] Bruce Schneier. Applied Cryptography Protocol, algorithms, and source c ode of C, 机械工业出版社 [M]。