移动互联网安全加密技术

深圳天创移动网络技术有限公司　谢胜落 张佩辰

摘　要　本文分析了建立移动互联网安全交易环境所面临的特殊问题，并以WAP协议WPKI规范为参照，阐述了移动互联网数据加密、身份认证和数字签名的具体实现方法。受限于移动终端的有限计算能力和移动网络的低带宽、高时沿特性，传统Internet的安全解决方案必须经过一定的修改才能适用于移动网络。

关键词　无线公钥体系（WPKI），无线传输层安全（WTLS），椭圆曲线算法（ECC），无线标记语言脚本（WML Script），无线用户标志（WIM）

1 引言

“无所不在的计算”是21世纪网络信息技术发展的趋势，移动互联是这一领域中最具影响力的技术，它把信息网络无限延伸到任意时间的任意角落。据权威机构预测，到2005年，移动互联网用户数量将超过固定互联网。移动电子商务是移动互联网最具市场潜力的应用领域，如何保证信息传递和交易在安全的网络环境中进行是移动电子商务面临的关键问题。

移动互联网服务的最终物理载体是传统Internet服务器和其他已有的专网（如证券交易网络、银行支付网络等），这些最终载体提供的服务必须结合移动互联网用户终端和承载网络的特性，才能真正体现移动互联网的价值，形成正反馈价值链。

移动终端有限的计算能力和显示屏幕要求服务提供商以尽量简洁的方式提供信息和交易流程，要求数据加/解密算法、身份认证、数字签名等安全机制占用尽量少的系统资源和时间。多种承载网络并存的现状（如SMS、CSD、GPRS等）要求服务端具有很强的数据融合能力，不仅支持多种移动接入方式，还能根据服务类别主动选择服务提供方式。

移动网络相对规范的用户申请和注册体系（如手机用户入网注册流程）便利了服务提供商提供个性化服务和服务收费。移动互联网的多种服务端主动推送机制（如SMS、WAP PUSH PROXY等）也彻底改变了传统Internet服务必须由用户发起的限制，使得服务提供商可以开发出许多传统Internet无法提供的特色服务。

2 移动互联网安全体系WPKI

WPKI（WAP Public Key Infrastructure）借鉴PKI标准的主要思想，并针对WAP安全规范和移动互联网的特别环境做了必要的改动。WAP安全规范包括：

(1) WAP传输层安全规范

即WAP WTLS（Wireless Transport Layer Security Specification），提供与传统Internet TLS1.0相对应的安全机制，WTLS充分考虑了移动网络低带宽和高时延的限制，支持数据报、优化握手以及动态密钥刷新等特征。

(2) WAP应用层安全规范

即WML Script Crypto Library，为移动终端提供WML脚本函数Crpto.sign Text实现用户对文本串的数字签名。调用该函数时，弹出将被签名的文本并请求用户确认。签名完成后，签名连同数据一起被发送到网络

作者简介：谢胜落，男，1973年11月生，1994年获西安交通大学学士学位，1997年获中科院自动化研究所硕士学位，现任深圳天创移动网络技术有限公司产品总监，863课题“无线互联网安全加密技术”成员。张佩辰，清华大学在读在职博士，现任深圳天创移动网络技术有限公司产品总经理，863课题“无线互联网安全加密技术”组长。

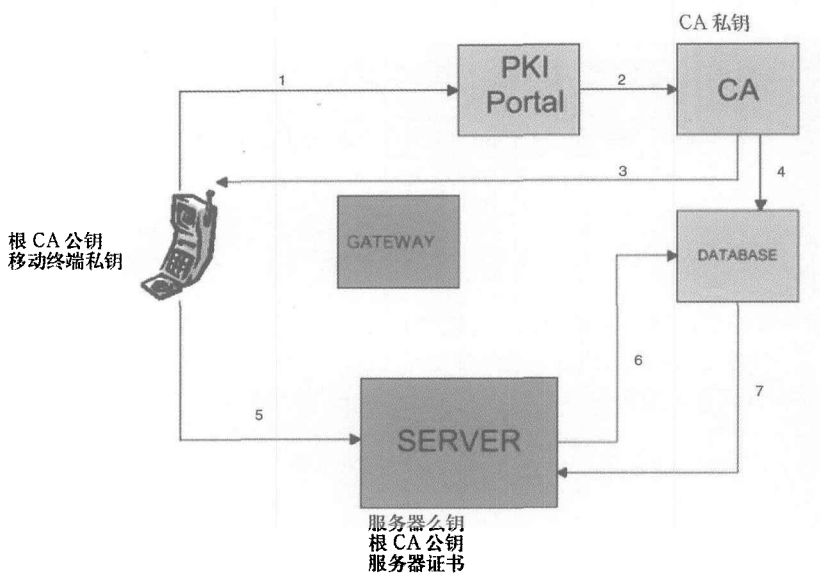

图 1 移动互联网安全体系 WPKI

上传输。

(3) WIM 规范

即 WPA Identity Module，为移动终端传输层和应用层安全机制提供证书及私钥存储和加 / 解密算法调用，WIM 的典型载体是智能卡。

(4) WAP 证书管理规范

即 WAP Certificate and CRL Profiles，提供证书时效校验、移动终端证书管理等机制。

建立一个完备的移动互联网安全体系需要过程如下（参看图 1）:

(1) 移动终端向 CA 入口申请证书;

(2) CA 入口确认申请后将其传送到认证中心;

(3) 认证中心产生用户证书，并将存储用户证书的 URL 回送到移动终端（认证中心也可以将整个证书回送到移动终端，但这要求移动终端支持 WIM）;

(4) 认证中心向 CA 数据库发布移动终端公钥;

(5) 移动终端同服务器通过双向身份认证和握手建立安全通道，需要数字签名时，移动终端将原文、签名和证书 URL 一同传送到服务器;

(6) 服务器通过证书 URL 从数据库中取得用户证书，进行身份认证或签名校验;

(7) CA 数据库将用户证书传送到服务器数据库。

3 数据加密

移动终端和服务器初次通信时，它们通过WTLS握手协议商定一组会话状态的密码参数，包括协议版本号，选择密码算法，可选择的相互鉴别，使用公开密钥加密技术生成共享密钥。在应用数据阶段中，所生成的共享密钥(预主密钥)将首先被转换成主密钥，主密钥在被转换成加密密钥和MAC密钥，加密密钥为客户机和服务器所共有，使用它对传输数据进行对称加密，保证了机密性，并提高了加密速度。

移动终端的弱计算力将影响加密算法的选择和实现。由于移动终端 CPU 的处理能力有限，所以不宜采用计算复杂性高的加密算法。移动终端的存储空间也十分有限，所以在移动终端上只能实现为数不多的加密算法，而且要尽量选用小算法，尤其是对 RAM 的要求必须很低。

椭圆曲线算法（ECC）特别适用于移动互联网公钥体系，ECC 同 RSA 比较，具有如下特性:

(1) 抗攻击性强;

(2) 计算量小，处理速度快;

(3) 密钥尺寸和系统参数小;

(4) 带宽要求低。

表 1 160 比特 ECC 同 1024 比特 RSA 性能比较

性能	ECC-160	RSA--1024
密钥生成速度	50 对 / 秒	0.028 对 / 秒
加密速度	80 次 / 秒	148 次 / 秒
解密速度	80 次 / 秒	23 次 / 秒
签名速度	80 次 / 秒	23 次 / 秒
验证速度	80 次 / 秒	148 次 / 秒

4 身份认证

在进行安全握手时，服务器的证书会通过无线网络传到移动终端。对无线网络而言，定义一种缩微证书格式是很有必要的，这既能减轻传输负载，也会减轻移动终端的处理负载。WTLS 证书是X.509证书的缩微格式，适用于无线网络环境。

另外，电子商务应用需要一种证书取消机制，保证如果服务器出现问题，用户不会跟一个伪装的服务器进行所谓的安全交易。由于无线网络传输速率和移动终端处理能力的限制，在有线网络环境下使用的 CRL 或 OCSP 都不适用于无线网络环境。在无线网络环境下，可以采用短时效证书来实现证书取消。

对内容服务器或WAP网关依旧采用长时效信用验证，但同有线网络不同的是，在时效期间，不是自始至

表 2 WMLScript 数字签名函数

函数	SignedString = Crypto.signText(stringToSign, options, keyIdType, keyed)
ID 号	16
描述	该脚本函数要求用户对文本串进行数字签名，待签名文本串在签名前必须显示给用户确认。
参数	StringToSign 字符串类型 待签名文本串 option 整型 签名选项，由或运算组合 0x0001-INCLUDE_CONTENT，函数返回值包含待签名文本串 0x0002-INCLUDE_KEY_HASH，函数返回值包含用签名私钥对公钥进行 HASH 运算的值 0x0004-INCLUDE-CERTIFICATE，函数返回值包含用户证书或证书URL,如果无法取得证书，函数返回“error:noCert” keyIdType 整型 指明签名密钥的类型 0- NONE，不提供公钥标志 1- USER_KEY_HASH，提供用户公钥的 SHA_1 运算结果 2- TRUSTED_KEY_HASH，提供 CA 公钥的 SHA_1 运算结果 KeyId 字符串类型 由上个参数决定的签名密钥串
返回值	如果签名成功，返回签名后的字符串（base-64 编码）；如果失败，返回错误代码
错误	error:noCert 或 error:userCancel

终用一对密钥。证书颁发机构每天都向内容服务器或WAP网关颁发新的证书，如果证书颁发机构决定取消对服务器的信用，就不再颁发证书。

5 数字签名

在许多应用场合（如电子商务）都需要提供一种某人进行过某项事务的永久性证明，尽管WTLS提供了在一次会话中的短暂用户身份验证机制，但它不能提供在这次会话中可能进行过某些事务的永久性证明。实现这种永久性证明的一种机制就是对在事务处理过程中产生的数据（如订购单或其他财务文档）进行数字签名。

WAP为了支持这种需求，在浏览器端提供WML脚本函数 Crypto.sign Text 要求用户对文本串进行签名。

6 结论

移动互联网即将广泛应用于移动证券、移动银行、移动商务及移动办公等领域，这些应用都要求我国拥有自主知识产权的移动互联网安全产品，包括嵌入式微浏览器、安全网关、无线 CA 以及安全应用平台等。

(收稿日期：2001.3.26)

参考文献

[1] WAP Forum, WAP Public Key Infrastructure Definition Proposed Version, 2000
[2] WAP Forum, Wireless Transport Layer Security Specification, 1999
[3] WAP Forum, WAP Identity Module Specification, 1999
[4] WAP Forum, WMLScript Crypto API, 1999
[5] WAP Forum, WAP Certificate and CRL Profiles Specification, 2000
[6] MeT, MeT Core Specification