

文章编号: 1007-5321(2002) 02-0001-07

移动电子商务及 WPKI 技术

刘 杰, 王春萌, 范春晓

(北京邮电大学电子工程学院, 北京 100876)

摘要: 介绍了移动互联网的现状, 并对移动电子商务技术进行了分析. 根据作者的实践及研究成果, 介绍了安全移动电子商务系统及基于 WAP 的移动电子商务系统的解决方案.

关 键 词: 无线应用协议; WPKI; 无线公钥基础设施; 安全移动电子商务系统

中图分类号: TN 918. 8⁺ 2 **文献标识码:** A

Mobile E-commerce and WPKI Technology

LIU Jie, WANG Chun-meng, FAN Chun-xiao

(Electronic Engineering School, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: An overview of mobile e-commerce is given and the technology adopted by mobile e-commerce is analyzed. Based on our practice and research work, we introduce two models of secure mobile e-commerce system based on SMS and WAP in which the WPKI technologies are used.

Key words: WAP; WPKI; STK; Secure Mobile E-Commerce System

近年来移动通信技术发展迅速, 全球移动电话用户数量成级数增加. 20 世纪最后 10 年, 特别是 1995 年以来, 移动通信和互联网成为当今世界发展最快、市场潜力最大、前景最诱人的两大业务. 移动电子商务作为移动通信应用的一个主要发展方向, 日益受到人们的关注, 而移动交易系统的安全是推广移动电子商务必须解决的关键问题.

1 移动互联网及移动电子商务的现状

目前全世界移动终端的数量已经接近 10 亿, 而互联网用户可能已经超过 5 亿. 这 2 个用户数表明: 随着时代与技术的进步, 人类对移动性和信息的需求急剧上升. 越来越多的人希望在移动的过程中高速接入互联网, 获取急需的信息, 完成想做的事情. 移动与互联网相结合的趋势是历史的必然. 据国外预测, 到 2002 年, 在全球范围内将有 1 亿多移动电话接入互联网, 到 2003 年, 美国和欧洲的通信厂商将会向市场推出 5.25 亿台 WAP 设备. 亚太地区具有 WAP 功能的手机用户将达到 1 亿, 其中, 中国的用户将达到 1 400 万.

收稿日期: 2002-04-05

作者简介: (1961—), 男, 北京邮电大学电子工程学院院长, 教授.

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. <http://www.cnki.net>

1.1 WAP 与 I-Mode

WAP(wireless application protocol)^[1],即无线应用协议,是移动通信设备实现接入 Internet 的一组通信协议.它使移动用户可以不受网络种类、网络结构、运营商的承载业务以及终端设备的限制,充分利用自己的手机,随时随地接入互连网(internet)和企业内部网(intranet),为高速发展的移动通信领域和互连网领域带来巨大的活力和广阔的发展空间.

作为一种通用协议,WAP 可以支持目前使用的绝大多数无线设备;在传输网络上,WAP 也可以支持目前的各种移动网络,如 GSM、CDMA、PHS 等等,它也可以支持第三代移动通信系统.但相对于 Internet 的有线网络带宽,无线网络的带宽资源永远是有限的.WAP 充分借鉴了 Internet 的思想,并加以一定的修改和简化,应用程序和网络内容采用标准的数据格式表示,使用与在 PC 机上使用的浏览器软件相类似的微浏览器,应用标准的通信模式实现网上浏览.

WAP 协议栈采用分层设计,结构中的每层协议可以被上层的协议来访问.分层结构能够使得其他的服务和应用通过预先定义的接口访问 WAP 协议栈,扩展应用能够通过接口直接访问 WAP 协议的各层.

但是,从 WAP 推出以来,基于 WAP 的移动互联网发展一直很缓慢.其主要原因是:支持 WAP 的网络通信速率低(9.6 kbps);电路交换模式的采用;终端设备—手机与应用的严重失配.此外,由于 WAP 协议制定时间较短,其中有较多不完善的地方,各厂家的 WAP 产品兼容性较差.

相对于 WAP 的缓慢发展,NTT DoCoMo 在日本推出的基于分组交换的 I-Mode 增值业务在商业上获得了巨大成功.归纳起来 I-mode 成功的原因有以下几点:(1)良好的商务模式,NTT DoCoMo 对所有加入其入口网站的内容服务供货商(ICP,ISP)并不收取费用,只借助于代收使用者信息服务费.借着开放的态度,让服务内容越趋多样化,而能吸引更多的用户使用;(2)I-Mode 采用分组交换系统进行通信,因而能够实现永远在线;(3)移动终端—手机良好的人机界面是专门为 I-Mode 服务设计的,能够充分体现移动数据服务和 I-Mode 信息服务的特色;(4)I-Mode 采用根据用户下载数据量及所提供服务内容为基础的灵活计费模式.但是,I-Mode 采用 cHTML 语言,与 WML 不兼容,缺乏国际标准的支持,因而通用性比较差;而且由于 I-Mode 手机仅能在有限范围使用,限制了 I-Mode 技术的进一步推广.

1.2 移动电子商务的现状

移动商务是电子商务的一个新的分支,但是从应用角度来看,它的发展是对有线电子商务的整合与发展,是电子商务发展的新形态.移动商务将传统的商务和已经发展起来的、但是分散的电子商务整合起来,将各种业务流程从有线向无线转移和完善,是一种新的突破.

随着移动互联网的快速发展,出现了通过移动终端进行的电子商务形式—移动电子商务.移动设备通常是隶属于个人,可以为其所有者随时随地提供信息,商家可以通过移动电子商务将市场目标定位到个人,而传统的基于有线连接的电子商务只能将市场细分到一个小群体,比如一个家庭.从这一点来说,移动电子商务是电子商务发展的最高形式.

与 Internet 上的在线交易相比,移动电子商务具有许多优点.首先,移动交易不受时间和地点的限制;其次,效率高,大大节省客户交易的时间;第三,移动终端的身份固定,能够向用户提供个性化移动交易服务;第四,可以提供与位置相关的交易服务.移动电子商务将用户和商家紧密联系起来,而且这种联系将不受 PC 或连接线的限制,使电子商务走向了个人.

移动电子商务被普遍认为将在未来几年内得到巨大的发展. 目前有不到 5% 的数据经过移动设备传输, 到 2005 年这一比例将上升到 25%. 预计移动电子商务到 2002 年将占整个电子商务市场的 10%. 爱立信对 2001 年后移动电子商务和电子商务预期发展速度的比较如图 1 所示.

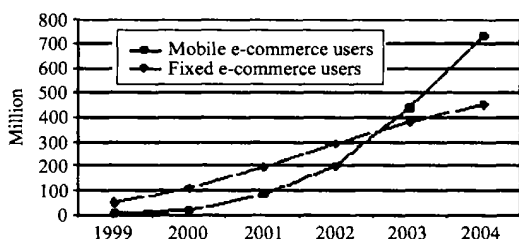


图 1 2001 年后移动电子商务和电子商务预期发展速度

2 WPKI 技术

2.1 移动电子商务的安全问题

在 2000 年初, 国内的移动运营商开始进军移动数据网络(移动 Internet)服务. 移动电子商务的发展经历了其第一个阶段, 即: 主要提供信息服务, 如天气和路况的预测、股市行情、新闻、E-mail 等. 这些服务的特点是用户在消费前必须和商家签订购买合同(如在商家的网站上购买消费点数等等), 属于预付费服务, 支付不在线上进行, 资金流动形式简单. 目前, 移动电子商务正经历着第二个发展阶段, 即提供具有在线支付能力的移动商务服务, 比如: 移动电子银行、移动贸易、移动购物、移动证券、移动缴费等. 这些服务的支付发起于用户操作移动终端进行所见即所得的购买. 由于涉及到移动环境下的资金流动, 安全问题就成为整个业务成功的焦点. 从移动电子商务的网络结构分析, 有可能遭受攻击的地方主要有: 移动终端与交换中心之间的空中接口、移动网关与应用服务提供商之间的传输网络.

一方面虽然 GSM 采用了比较先进的加密技术^[2], 可是由于移动通信的固有特点, 手机与基站之间的空中无线接口是开放的, 这给破译网络通讯密码提供了机会. 而且信息一旦离开移动运营商的网络就已失去了移动运营商的加密保护. 因此, 在整个通信过程中, 包括通信链路的建立、信息的传输(如用户身份信息、位置信息、用户输入的用户名和密码、语音及其它数据流)存在被第三方截获的可能, 从而给用户造成损失. 另一方面在移动通信系统中, 移动用户与网络之间不像固定电话那样存在固定的物理连接, 商家如何确认用户的合法身份, 如何防止用户否认已经发生的商务行为都是急需解决的安全问题.

移动网关一般是实现信息格式的转换, 但也有的移动网关(如 WAP 网关)对信息进行加解密处理, 因而整个移动电子商务的安全链条就存在安全断点.

如何解决好移动支付的安全问题, 并且通过宣传培养用户通过移动终端进行消费的信心, 是决定移动电子商务下一步发展的关键.

2.2 WPKI

在无线世界里, 由于空中接口的开放, 人们对于进行商务活动的安全性的关注远超过有线环境. 仅当所有的用户确信, 通过无线方式所进行的交易不会发生欺诈或篡改, 进行的交易受到法律的承认和隐私信息被适当的保护, 移动电子商务才有可能成功和推广.

在有线通信中, 电子商务交易的一个重要安全保障是 PKI(公钥基础设施)^[3]. 在保证信息安全、身份证明、信息完整性和不可抵赖性等方面 PKI 得到了普遍的认同, 起着不可替代的作用. PKI 的系统概念、安全操作流程、密钥、证书等同样也适用于解决移动电子商务交易的安全问题, 但在应用 PKI 的同时要考虑到移动通信环境的特点, 并据此对 PKI 技术进行改进.

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

WPKI(wireless PKI)技术满足移动电子商务安全的要求: 即保密性、完整性、真实性、不

可抵赖性,消除了用户在交易中的风险. WPKI 技术主要包含以下几个方面:

(1) 认证机构(CA)

CA 系统是 PKI 的信任基础,负责分发和验证数字证书,规定证书的有效期,发布证书废除列表(CRL).

(2) 注册机构(RA)

RA 提供用户和 CA 之间的一个接口. 作为认证机构的校验者,在数字证书分发给请求者之前对证书进行验证. 它捕获并认证用户的身份,向 CA 提出证书请求. 认证的处理质量决定了证书中被设定的信任级别.

(3) 智能卡

智能卡^[4]将具有存储、加密及数据处理能力的集成电路芯片镶嵌于塑料基片中,具有体积小、难于破解等特点,在生产过程、访问控制方面有很强的安全保障. 很多种需要客户端认证的应用都可以使用智能卡来实现^[5]. GSM 移动运营商存放移动用户识别号(IMSI)和身份认证密钥(Ki)的 SIM 卡就采用了智能卡技术,同样智能卡也是存储移动电子商务密钥及相关数字证书的最佳选择,卡片载有持卡人的数字证书、私钥以及加密签名模块,从而实现移动电子商务中的身份识别和信息加密传输.

(4) 加密算法

加密算法越复杂,密钥越长则安全性越高,但执行运算所需的时间也越长(或需要计算能力更强的芯片). 所以,支持 RSA 算法的智能卡通常需要高性能的具有协处理器的芯片^[6]. 而椭圆曲线加密体制(ECC)使用较短的密钥就可以达到和 RSA 算法相同的加密强度. ECC^[7]于 1985 年由 Neal Koblitz 和 Vieter Miller 提出,它的数论基础是有限域上的椭圆曲线离散对数问题,现在还没有针对这个难题的亚指数时间算法,因而在当今公钥密码体制中,椭圆曲线密码体制(ECC)具有每比特最高的安全强度. 由于智能卡在 CPU 处理能力和 RAM 大小的限制,因而采用一种运算量小同时能提供高加密强度的公钥密码体制对在智能卡上实现数字签名应用是至关重要的. 椭圆曲线密码体制(ECC)在这方面具有很大的优势^[8]. RSA 算法与 ECC 算法的比较如表 1 所示. 因此,ECC 算法在智能卡领域具有广阔的应用前景^[9].

表 1 RSA 算法与 ECC 算法的比较

破解时间 (M IPS years)	RSA/DSA 密钥长度	ECC 密钥长度	RSA/ECC 密钥长度对比
10 ⁴	512	106	5 1
10 ⁸	768	132	6 1
10 ¹¹	1 024	160	7 1
10 ²⁰	2 048	210	10 1
10 ⁷⁸	21 000	600	35 1

从上面可以看出,在 WPKI 机制下,数字证书非常重要,但是由于无线信道和移动终端的限制,如何安全、便捷地交换用户的数字证书,是 WPKI 所必须解决的问题. 笔者认为有以下 2 种解决办法:

WTLS 证书的功能与 X.509 证书相同,但更小、更简化,以利于在资源受限的手持终端中处理。但所有证书必须含有与密钥交换算法相一致的密钥。除非特别指定,签名算法必须与证书中密钥的算法相同。但是,由于 WTLS 证书是一种新的证书类型,所以必须对 CA 系统进行升级,才能支持该类证书。

④移动证书标识

将标准的一个 X.509 证书与移动证书标识唯一对应,并且在移动终端中嵌入移动证书标识,用户每次只需要将自己的移动证书标识与签名数据一起提交给对方,对方再根据移动证书标识检索相应的数字证书即可。移动证书标识一般只有几个字节,远小于 WTLS 证书,并且不需要对标准的 X.509 证书做任何改动。

3 移动电子商务系统

3.1 基于 SMS 的移动电子商务系统——安全移动电子商务系统

安全移动电子商务系统的构成如图 2 所示。

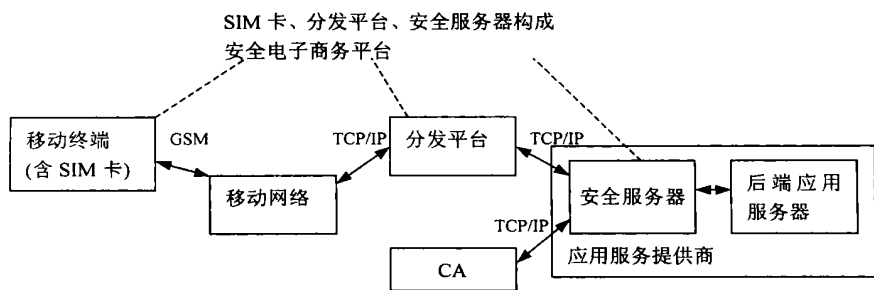


图2 安全移动电子商务平台

如图所示,整个系统由移动终端、移动网络、安全移动电子商务平台、应用服务提供商、认证中心(CA),共5部分构成。而安全移动电子商务平台由SIM卡、分发平台和安全服务器3个部分构成。其中SIM卡作为客户端组件,提供数据加密与签名功能;分发平台和安全服务器作为服务器端组件,提供数据分发、数据加密及签名验证功能。除了移动终端与移动网络是通过GSM通信外,其余部分均通过传输控制协议/因特网协议(TCP/IP)数据专线通信。安全移动电子商务平台与认证中心(CA)相连以保证交易的安全和身份的确认。

实现安全移动电子商务的步骤如下:

- (1) 根据用户从移动终端上输入到应用服务提供商所需数据,利用SIM卡对数据进行加密、签名,并以短消息的格式发出加密并签名的数据;
- (2) 将加密并签名的短消息通过移动网络转发至安全移动电子商务平台的分发平台;
- (3) 分发平台将短消息重组为数据包,并转发至相应的应用服务提供商;
- (4) 位于应用服务提供商的安全服务器对加密并签名的数据进行解密及验证,如验证通过,则提交后端应用服务器,如果验证未通过,则提示用户验证失败;
- (5) 后端应用服务器处理后的结果由安全服务器进行加密处理,并转发至分发平台;分发平台将数据拆分为短消息,通过移动网络发送给移动终端;
- (6) 移动终端接收到短消息后重组数据包,并对加密数据进行解密,最终将结果显示给用

户.

安全移动电子商务平台是开放的安全移动电子商务平台,它可支持多形式的访问服务,使不同的用户可以通过不同的设备(STK 手机、WAP 手机、微机)访问服务提供商.

分发平台是消息分发中心,它将双向的访问请求,经过消息的队列处理,分发到目的端,分发的形式有2种:

(1) “拉”请求

由移动终端发起“拉”(pull)请求.在需要进行浏览时,移动终端通过安全移动电子商务平台的分发平台向服务提供商发送“拉”请求.

(2) “推”请求

“推”(push)请求是由固定设备(如微机)而不是移动终端发起的.应用服务提供商通过安全移动电子商务平台的分发平台将请求“推”给移动终端.

认证中心(CA)为国家认可的认证中心,该中心为用户发放的数字证书格式遵守 X.509 V3 标准,安全移动电子商务系统中采用前面所述的简化证书——移动证书标识来完成用户身份的验证.

该系统不针对特定服务和市场,而是对所有服务开放,移动用户和各种应用服务提供商都可以通过该系统进行端对端的安全交易.该系统的主要特点有:

基于 STK 卡和短消息服务(SMS)^[10],在 32K SIM 卡内嵌入 3DES 和 RSA 插件,用以数据加密和数字签名.另外卡内还嵌有 SIM 卡浏览器,可通过标准接口访问 WML 格式的数据.

采用空中下载(OTA)技术,移动用户可以通过 OTA 下载功能更新菜单.这样就避免了智能卡空间不足的问题.OTA 技术的采用使安全移动电子商务系统的应用接入更具灵活性和扩展性,应用及内容服务商不受系统的局限,可以不断创新,开发出更个性化的满足用户需求的服务.

采用无线-公钥基础设施(W-PKI)技术,通过移动证书标识和签名算法实现身份验证和交易的不可抵赖性.

安全移动电子商务系统是将无线标记语言(WML)作为系统的会话语言,WML 是一种扩展标记语言(XML)的应用简化,选用它能便于今后系统的更新和升级.将 WML 作为系统的会话语言,容易过渡到下一代既支持 STK 又支持 WAP 的产品.

安全移动电子商务系统的技术方案与现有的成熟技术做了很好的整合,系统的稳定性和实用性得到了充分的保障.

安全移动电子商务系统的目标是可支持多形式的访问服务,使不同的用户可以使用不同的设备(STK 手机、WAP 手机、微机)访问服务提供商的应用,成为开放的移动商务系统.

3.2 基于 WAP 的移动商务系统

为保证端到端的安全性和交易的不可否认性,基于 WAP 的移动电子商务应采用 WIM (WAP 用户识别模块)+智能卡技术,即利用智能卡实现 WIM 的功能,并将加密库集成于智能卡中,形成一张 WIM 卡.用户的私钥存放于 WIM 卡内,WIM 卡可完成加密、解密、数字签名,WIM 在 WTLS 层上对 WAP 客户端提供认证和会话管理.基于 WAP 的移动商务模型如图 3 所示.

为了保证加密的安全,可以考虑将 WIM 模块和加密库集成于 SIM 卡中,形成一张 WIM 卡.利用 WIM 卡从信息的发起端进行加密、签名,并将此结果以 WML 的格式发送出去.

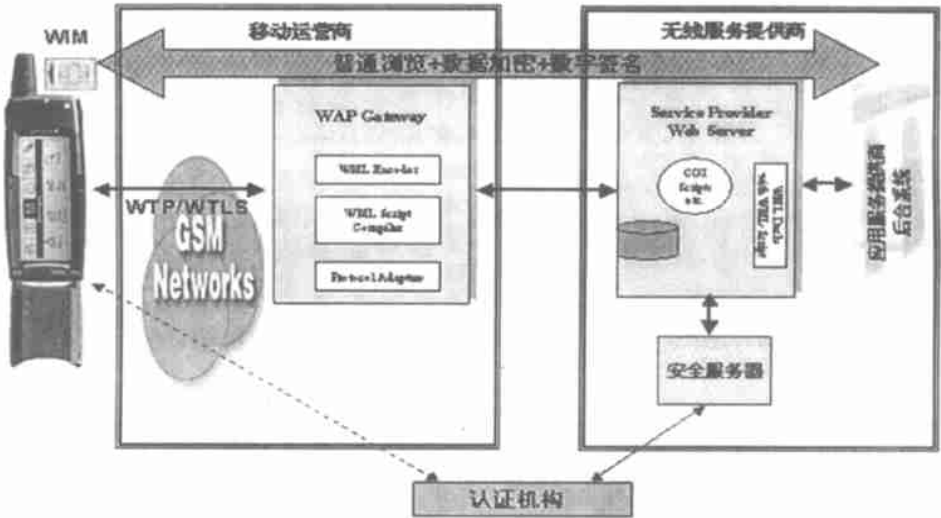


图 3 基于 WAP 的移动商务模型

WAP 网关只完成数据的格式转换,并不对数据进行解密处理. 只有当数据到达应用提供商一方才解密并验证签名. 在整个处理过程中,攻击者所能得到的只是密文和数字签名,因而保证了移动商务的安全性.

该系统与 WAP2.0 协议中所提出的安全体系有所不同^[11],由于 WAP2.0 协议中的 WTLS 层对数据进行加解密及签名验证,导致整个安全链条在 WAP GATEWAY 形成断点,而上述系统将 WTLS 层的功能转移到安全服务器,从而提供了端到端的安全性. WIM 技术与 WPKI 技术相结合,为移动商务提供了更好的安全保障.

随着移动通信技术的发展,采用 WAP+ GRPS/WAP+ 3G 模式更有利于基于 WAP 的移动电子商务系统的推广.

4 结论

移动互联网和移动电子商务目前的发展非常迅速,基于 WPKI 的移动电子商务涉及多方面的技术,基于 SMS 的安全移动电子商务系统是目前阶段一个比较完善的解决方案,而基于 WAP 的移动电子商务系统的解决方案是以后的发展方向. 可以预见,在不久的将来移动终端将会成为人们生活中不可分离的个人信用终端 PTD(personnel-trusted-device).

参考文献:

[1] Wireless Application Protocol Version 2. 0. Copyright wireless application[EB/OL]. <http://www.wapforum.org>. 2001.

[2] Carlisle Adams, Steve Lloyd. 冯登国等译. 公开密钥基础设施- 概念、标准和实施[M]. 北京: 人民邮电出版社,2001.

[3] GSM 03. 48 version 7. 0. 1- 1998, ETSI[S].

[4] 杨千里,王育民. 电子商务技术与应用[M]. 北京: 电子工业出版社, 1999.

[5] Rankl W, E ng W. Smart ard handbook[M]. John Wiley & Sons:1997.

可以看出: 在轻负载参数配置下:

(1) 当负载处于 0.5~0.8 区间, EF 业务的时延缓慢的增长. 但是当负载超过 0.8 后, EF 业务的时延迅速增长. 整体的时延同 EF 时延类似, 说明大于 0.8 的负载已经超出了路由器参数配置的工作范围.

(2) 当负载处于 0.5~0.8 区间, AF 丢弃率缓慢的增长. 但是当负载超过 0.8 后, AF 丢弃率迅速增长.

5 结 论

本文给出了支持区分服务的高速路由器仿真模型的设计和在 OPNET 中的模型实现. 为 2.5 Gb/s 高速路由器确定了重要参数, 为高速路由器的工程设计提供了数据参考.

参考文献:

- [1] RFC2638- 1999. Nichols K, Jacobson V, Zhang L. A two-bit differential services architecture for the Internet[S].
- [2] RFC2475- 1998. Blake S, et al. An architecture for differentiated services[S].
- [3] RFC2698- 1999. Heinanen J, Telia Finland, Guerin R. A two rate three color marker[S].
- [4] Nick McKeown. iSLIP: A scheduling algorithm for input-queued switches[J]. IEEE Transactions on Networking, 1999, 7(2): 188- 201.
- [5] Distributed Weighted Random Early Detection[EB/OL]. <http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/wred.htm>, 1998- 2002.
- [6] Golestani S J. A self-clocked fair queueing scheme for broadband applications [A]. IEEE INFOCOMM '94[C]. 1994. 636-645.

(上接第 7 页)

- [6] 刘尊全. 刘氏高强度公开加密算法设计原理与装置[M]. 第二版. 北京: 清华大学出版社, 1998.
- [7] Koblitz N. A course in number theory and cryptography[M]. 2nd edition. Springer-Verlag: 1994.
- [8] Randall K. Nichols. ICSA guide to cryptography[M]. Computing McGraw-Hill, first edition, 1999.
- [9] Scott B. Guthery, Cronin Mary J. Mobile application development with SMS and the SIM toolkit[M]. McGraw-Hill Companies, Inc. 2002.
- [10] Wang Chunmeng, Liu Jie, Zou Junwei. WAP and ECC in wireless e-commerce[C]. ISTN'2000 proceedings, 2000. 255-258.