一种基于 WAP 2.0 的移动安全支付协议架构

A WAP 2.0 based secure protocol for mobile payment

宋珊珊 （东华大学 旭日工商管理学院 上海 200051）

摘 要： 本文以 WAP 2.0 为技术标准，并以 SEMOPS 模型为业务流程基础，提出了一种新的移动电子商务安全支付协议架构。本文通过运用非对称密钥体制的加密算法、数字签名、数字证书、时间戳等技术保证交易数据的安全，对移动终端与服务器端之间的 TLS 握手协议进行了分析和优化，并首选椭圆曲线加密算法（ECC）作为数据加密算法。

关键词： WAP 2.0 安全支付 移动电子商务 移动支付

1 引言

移动电子商务是移动终端设备日渐普及、网络技术日益成熟的前提下诞生的新兴概念。近年来，手机、PDA（Personal Digital Assistant，个人数字助理）等移动终端日渐普及，引发了利用移动终端进行商务活动的热潮。然而，据调查显示，移动终端的用户中仍有很大一部分对于移动支付业务心存顾虑，不敢于过早尝试。他们的担忧不无道理，移动电子商务的支付安全问题尚未得到完全的解决：

（1）支付的业务模型百家争鸣，没有通用的业务标准。

当今的移动电子商务世界缺乏一个世界性的移动支付标准，使用较为广泛的业务模型有 Mobey[1]、PayCircle[2]，以及 SEMOPS[3]等。SEMOPS 模型与前两者相比，具有更多优势，理由如下：① SeMoPS 模型以用户为中心，所有的支付请求都由用户发起并且必须得到用户的授权与确认[4]。② SeMoPS 模型涵盖的交易种类广泛，具有更高的通用性。③ SeMoPS 模型的角色定义更合理，流程更细致，更侧重于交易发生的实际过程。

（2）无线网络的技术标准 WAP（Wireless Application Protocol，无线应用协议）协议虽已推陈出新，但相关支付协议却停留在过去的 WAP 1.x 版本，没有紧随 WAP 技术进步的脚步。

在 WAP 1.x 中，WAP 设备和 WAP 网关之间的安全数据传输采用的是 WTLS（无线传输层安全协议），而 WAP 网关和 Web 服务器之间的安全数据传输采用的是 SSL（安全套接字层协议）。从 WAP 设备发送至 WAP 网关的数据，必须首先解密成明文，再加密发送给 Web 服务器。上述传输方式造成了一定的安全隐患，即著名的 Security Gap（安全鸿沟）问题。新的 WAP 2.0 标准用 WAP 代理服务器取代了 WAP 网关，并且协议栈结构也更加向 Internet 标准靠拢，传输层的 WTLS 协议被 TLS（传输层安全协议）取代，解决了最初令人担忧的端到端安全问题。

国内也有关于移动电子商务安全支付的协议研究，最值得一提的是刘军、廖建新在 2006 年提出的“一种通用的移动支付协议模型”[4]。他们引入了认证中心和时间戳服务器这两个第三方组件，加强了模型中角色的认证，并用时间戳达到保证“不可抵赖性”的目的。此模型具有很高的研究价值，但没有详细描述数据加密算法的细节，对协议的效率缺乏有力的证明。

2 设计目标

2.1 技术规范性

移动支付模型必须遵循当前的移动电子商务技术标准和规范。本文基于 WAP 2.0 构建移动安全支付协议，模型中采用的非对称密钥体制、传输层安全协议、改进的握手协议均严格参照了 PKI 和 TLS 技术规范。

2.2 业务通用性

移动支付模型的业务流程必须具有通用性。本文

模型中的实体和业务流程均以 SEMOPS 模型为基础，尽管做了微小的调整和改进，但仍继承了 SEMOPS 模型的业务通用性。

据中心负责在消费者和商家各自的支付处理机构之间实现定位和信息传输的工作。

本文中的业务模型与支付协议的范围界定如下：

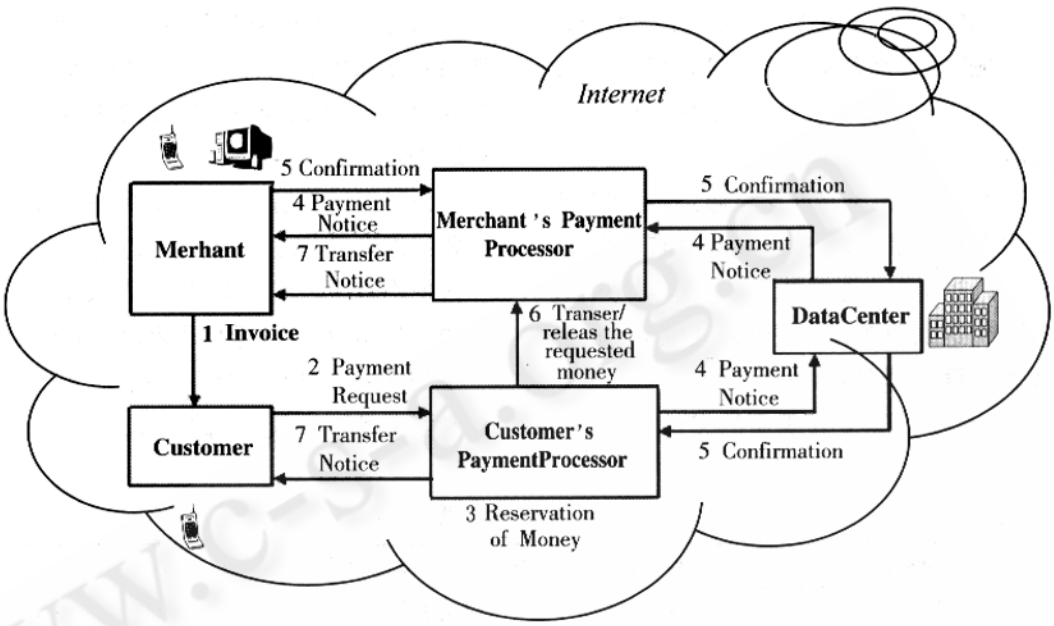

图 1　支付业务流程图

2.3 较高的安全级别和隐私保护

在移动支付过程中，交易双方的身份必须得到证明，同时，重要信息和隐私必须得到保护，避免被恶意第三方截取并篡改。本文采用非对称密钥体制、数字签名、时间戳和数字证书等技术保障交易数据的安全。

2.4 改善的效率

在移动电子商务中，安全和效率是两个既关键又矛盾的重要因素。本文在保证数据传输安全的基础上，首选运算速度高、安全性能好的椭圆曲线加密算法(ECC)作为非对称加密算法，并对移动终端与服务器端之间的 TLS 握手协议做简化，缩短消息长度，减少消息传递次数。

3 业务模型

本文在业务模型上借鉴了 SEMOPS 的结构，定义了以下 5 个支付实体：消费者、商家、消费者支付处理机构、商家支付处理机构，以及数据中心。其中消费者使用移动终端进行交易，商家可能使用移动终端，也可能使用计算机；支付处理机构由银行和网络运营及服务提供商组成，是消费者和商家充分信任的机构体；数

本模型的支付流程发生于消费者向商家确认了挑选的商品条目之后，以银行转帐操作完成后的通知消息为结束标记。银行内部转帐和处理的细节不属本文讨论的内容，故不作详细说明。

如图 1，本文将一次完整的交易业务流程划分为 7 步，分别为：询价、支付请求、资金冻结、支付通知、支付确认、转账/解冻，以及转账/解冻通知。下文将详细描述这 7 个步骤中数据的传输过程。

4 移动支付协议

4.1 支付流程描述

第一步：询价。商家根据用户的挑选记录，生成唯一的交易流水号和唯一能够标识自身身份的识别号，将详细的交易数据、价格、自身的帐户信息发送给消费者。此处商家的帐户信息是为了供银行等机构完成入帐而提供的，不包括敏感的信息，如帐户密码和商家身份。

第二步：支付请求。消费者验证商家的身份之后，确认交易数据和价格等信息的正确性，随即生成一条标准格式的支付请求消息至消费者支付处理机构。此

条消息包含消费者发送支付请求的时间标记。

第三步:资金冻结。消费者的支付处理机构接收到消费者的支付请求消息之后,根据消息中消费者的帐户信息冻结与价格相等金额的资金。

第四步:支付通知。消费者的支付处理机构通过数据中心,重构并签名消费者发出的支付通知,将其传送至商家的支付处理机构,商家支付处理机构随即将通知发送至商家。

第五步:支付确认。商家验证支付通知,生成对于消费者支付通知的确认消息,此消息参数具有两个值,分别是"同意"与"拒绝"。此消息通过商家支付处理机构、数据中心,传送到消费者的支付处理机构。此条消息包含商家发送确认消息的时间标记。

第六步:帐户转帐/解冻。消费者的支付处理机构收到支付确认消息,如果商家的消息是"同意",则执行常规的银行帐户转帐操作,将消费者帐户冻结的金额传送至商家的帐户上,如果商家"拒绝",则将消费者帐户上冻结的金额解冻。

第七步:转帐/解冻通知。帐户处理完成之后,消费者和商家的支付处理机构分别通知消费者和商家,告知他们支付确认和账户处理的结果。

4.2 支付协议

为了保证交易匿名性,避免将隐私数据透露给不必要的接受者,在上文描述的每个步骤中,传递的消息和数据均有所不同。本文用 M 表示各个实体之间发送的消息,M 后面的数字表示此消息所处的步骤,若同一个步骤中出现的消息有区别,则用"-"来分隔。本文模型中各种消息参数的意义见表 1。

表 1　主要参数说明表

参数	TransactionID	MerchantID	MerchantAccountInfo	CustomerAccountInfo
说明	交易流水号	商家标识号	商家帐户信息	消费者帐户信息
参数	TransactionData	Price	T-Request	T-Confirmation
说明	交易数据	价格	支付请求的时间标记	支付确认的时间标记

协议中,KA 表示实体 A 的公钥,H 表示 Hash 散列函数,KA-1 表示实体 A 的私钥,C、CPP、DC、MPP、M 分别代表消费者、消费者支付处理机构、数据中心、商家支付处理机构和商家。本文中的协议基于非对称密钥体制,首选椭圆曲线加密算法(ECC)。对于一次完整的支付过程,其支付协议描述如下所示:第一步、询价-Invoice:

(1) $M \rightarrow C$: $K_C\{M1,[H(M1)]K_M^{-1}\}$

M1: TransactionID、MerchantID、TransactionData、Price、MerchantAccountInfo

第二步、支付请求-Payment Request:

(2) $C \rightarrow CPP$: $K_{CPP}\{M2,[H(M2)]Kc^{-1}\}$

M2: TransactionID、Price、CustomerAccountInfo、MerchantAcountInfo、T-Request

第三步、资金冻结-Reservation of Money:

银行内部操作,略。

第四步、支付通知-Payment Notice:

(1) $CPP \rightarrow DC$: $K_{DC}\{M4-1,[H(M4-1)]K_{CPP}^{-1}\}$

M4-1: TransactionID、MerchantAccountInfo、T-Request

(2) $DC \rightarrow MPP$: $K_{MPP}\{M4-1,[H(M4-1)]K_{DC}^{-1}\}$

(3) $MPP \rightarrow M$: $K_M\{M4-2,[H(M4-2)]K_{MPP}^{-1}\}$

M4-2: TransactionID、T-Request

第五步、支付确认-Confirmation:

(1) $M \rightarrow MPP$: $K_{MPP}\{M5,[H(M5)]K_M^{-1}\}$

M5: TransactionID、T-Request、Approval/Reject、T-Confirmation

(2) $MPP \rightarrow DC$: $K_{DC}\{M5,[H(M5)]K_{MPP}^{-1}\}$

(3) $DC \rightarrow CPP$: $K_{CPP}\{M5,[H(M5)]K_{DC}^{-1}\}$

第六步、帐户转帐/解冻-Transfer/Release the Requested Money:

银行内部操作,略。

第七步、转帐/解冻通知-Transfer Notice:

(1) $K_C\{M7,[H(M7)]K_{CPP}^{-1}\}$

M7: TransactionID、T-Request、T-Confirmation、Price、Approval/Reject、Success/Denied

(2) $K_M\{M7,[H(M7)]K_{MPP}^{-1}\}$

4.3 简化的 TLS 握手协议

在 WAP 2.0 中，客户端和服务器端之间的通信采取 TLS 安全隧道，WAP 1.x 中的 WAP 网关被 WAP 代理服务器取代。在本文的模型中，消费者与消费者支付处理机构之间（上文中的步骤 2）的通信协议栈遵循图 3 的描述。如果商家也使用移动设备，则商家与商家支付处理机构之间（上文中的步骤 5.1）的通信协议栈也符合图 2 描述。

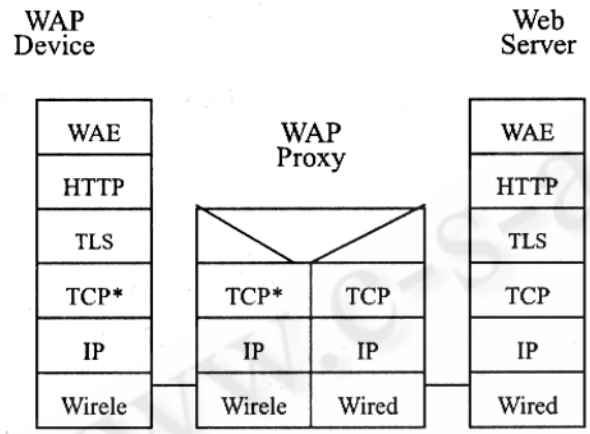

图 2　WAP2.0 协议栈[5]

TLS 包括记录协议和握手协议，而记录协议使用的公钥加密算法和 Hash 函数的运算速度相对很高，对消息的发送不会有很大影响，握手协议采用公钥加密算法，计算量大，是影响 TLS 协议运行效率的重要因素[6]。因此本文将在保证数据安全的基础上对 TLS 握手协议作出一定简化。

本文中 TLS 握手协议的简化原则如下：(1)、采取增加服务器运算量的方法减轻移动终端负担。服务器既要验证客户端证书，也要将自身证书生成摘要，与客户端发送的服务器证书摘要对照，因此运算量有所增加。(2)、客户端储存经常与之通信的服务器证书，将其生成摘要发送。由于无需发送请求验证信息，这样做可以减少消息发送的次数；摘要信息较短，消息长度也得到了控制。(3)、服务器须验证客户端的证书，验证过程使用的时间戳（T－Request、T－Confirmation）作为交易证据。这个验证过程定义在消费者和商家分别与他们的支付处理机构建立安全通信时。验证证书的过程必须使用时间戳，验证的时间点与支付请求及支付确认的时间吻合，提供了不可抵赖证据。

图 3 描述了简化的 TLS 握手协议，在遵循了上述步骤之后，安全的 TLS 隧道就建立起来了，双方在安全隧道内传输交易数据。与 TLS 原先的握手协议相比，简化的握手协议省略了服务器方的三个消息：服务器证书（Certificate）、要求客户端证书（CertificateRequest）、服务器问候结束（ServerHelloDone），原先的四步握手过程也减少到了三步。

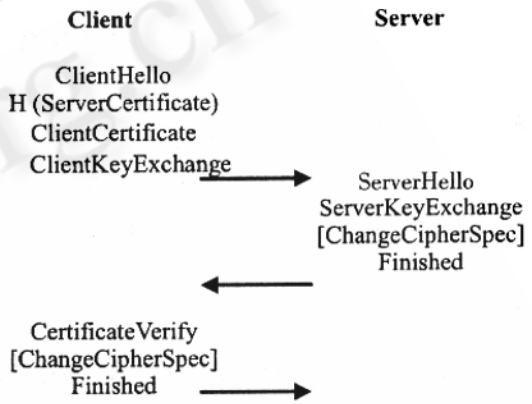

图 3　简化的 TLS 安全通道握手协议

5 结束语

本文提出的模型采用了非对称密钥体制的加密算法，运用数字签名、数字证书和时间戳等技术保证交易数据的传输安全。在保障安全性的基础上，模型首选安全系数高、运算速度快的椭圆曲线加密算法（ECC）作为加密算法，并对移动终端与服务器端之间的传输层安全协议（TLS）做了握手协议的优化，缩短了消息长度，减轻了移动终端的数据处理压力。

参考文献

1 Juha Risikko, Bishwajit Choudhary. Mobile Financial Serbices: Business Eecosystem Scenarios & Consequences [EB/OL]. http://www. mobeyforum. org. Mobey Forum. Mobile Financial Services Ltd.. 2006.

2 PayCircle consortium. PayCircle: User Scenarios [EB/OL]. http://www. paycircle. org. February 2002.

3 S. Karnouskos, A. Vilmos, A. Ramfos, B. Csik, P. Hoepner. SeMoPS: A Global Secure Mobile Payment

（下转第 23 页）

(上接第 27 页)

Service. In the book of Wen - Chen Hu, Chung - Wei Lee, and Weidong Kou (editors). Advances in Security and Payment Methods for Mobile Commerce. IDEA Group Inc.

4 刘军、廖建新，一种通用移动支付模型及其协议的研究[J]，高技术通讯，2006 (6)：560 - 565.

5 WAP Forum. WAP Architecture Version 12 - July - 2001. WAP - 210 - WAPArch - 20010712 - a [EB/OL]. http://www.openmobilealliance.org/tech/affliliates/wap/wapindex.html.

6 赵安军、郭雷、姚俊，一种快速 TLS 握手协议分析与实现[J]，计算机工程，2004 (2)：131 - 134.