基于 WPKI 的安全移动支付系统的设计与实现

石俊萍[1],李必云[2]

(1.吉首大学 物理科学与信息工程学院,湖南 吉首 416000;
2.吉首大学 数学与计算机科学学院,湖南 吉首 416000)

摘 要:安全移动支付是移动电子商务最关键的环节。针对移动支付这一核心功能,参照各种移动支付模型,引入 WPKI,利用多种安全技术进行设计,从而实现移动支付数据的机密性、完整性、可认证性和不可抵赖性。

关键词:移动电子商务;无线公开密钥基础设施;移动支付系统

中图分类号:TP393 **文献标识码**:A

Design and implementation of secure mobile payment system based on WPKI

SHI Jun-Ping[1], LI Bi-Yun[2]

(1.College of Physics Science & Information Engineering, Jishou University, Jishou 416000, China;
2.College of Mathematics and Computer Science, Jishou University, Jishou 416000, China)

Abstract: Secure mobile payment is the most critical aspect of mobile ecommerce. Mobile payment was designed at the core functionality of mobile payments, reference to a variety of mobile payment models, the introduction of WKPI, and used a variety of security technologies, Mobile payment was achieved at data confidentiality, integrity, authentication and non-repudiation.

Key words: electronic commerce; wireless public key infrastructure; mobile payment system

移动电子商务是有线电子商务的延伸和发展。企业现有的环境、系统和模式都可以技术性地移植到电子商务中,避免重复投资和资源浪费。但是加入移动电子商务的系统,其复杂性也带来一系列的安全问题。由于移动电子商务的特殊性,移动电子商务的安全问题尤其重要。安全性是影响移动电子商务发展的关键问题。

1 移动电子商务和移动支付

1.1 基于 WPKI 的移动电子商务

WPKI[1]以无线应用协议 WAP(Wireless Application Protocol)的安全机制为基础[2],从传统的公钥基础设施 PKI(Public Key Infrastructure)中发展而来。WPKI 与 PKI 都是通过管理密钥和证书来执行移动电子商务策略。WPKI 主要解决管理移动电子商务的策略问题,并为无线应用环境提供安全服务。WPKI 的优化主要包括对证书格式的简化,以减少存储容量。另外 WPKI 采用了先进的 ECC 公钥算法,而非传统的 RSA 算法,这就可以大大提高运算效率,并在相同的安全强度下减少密钥的长度。由于 WPKI 证书格式是 PKIX (Public Key Infrastructure on X.509)证书的子集,所以可以在标准 PKI 中保持互操作性[3]。

1.2 WPKI 移动电子商务安全框架

鉴于目前大部分手机计算能力的低下,下面提供一种适合移动电子商务的 WPKI 移动交易安全框架,即引入验证服务器 VA(Validation Authority)的 WPKI 移动交易安全框架[4],如图 1 所示。

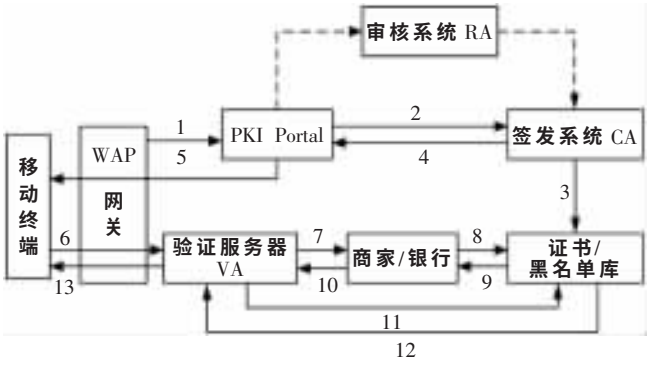

图 1 采用 VA 的 WPKI 移动电子商务安全框架

VA 作为所有无线终端的代理，完成各种复杂的证书验证和加密/解密操作(如多级证书链的验证)。此时，手机只需要处理单级证书验证，即只需对验证服务器回送的结果进行验证。

其验证过程如下：

(1)手机用户使用生成密钥对和证书请求，向 PKI Portal 申请证书；

(2)PKI Portal 在完成审核后向 CA 签发系统申请签发证书；

(3)签发系统签发证书并通过证书库发布；

(4)签发系统将用户证书回送给 PKI Portal；

(5)PKI Portal 将证书回送给手机终端，存放在手机内的智能卡中。

1.3 移动支付

移动支付是指借助手机、掌上电脑、笔记本电脑等移动通信终端和设备，通过无线方式进行的银行转账、缴费和购物等商业交易活动。与传统支付方式相比较，移动支付的优点是真正实现了 3A(任何时间、任何地点以及任何方式)，也就是将无线通信技术的 3A 优势应用到金融业务之中[5]。它的优势从与以往支付方式(传统的支付方式与电子支付的方式)的比较中体现出来。但由于安全性和易用性问题尚未得到很好的解决，所以目前国内的移动支付主要是小额支付为主。

2 系统分析和设计

2.1 安全移动支付系统功能模块设计

安全移动支付系统组成如图 2 所示。该移动支付系统以 WPKI 为基础，依据移动支付业务需求设计[6]，各模块功能如下：

(1)RA 服务器提供 HTTP/HTTPS 服务，为用户提供申请证书的检查和审核，并提交给 CA 服务器进行证书签发；

(2)CA 服务器提供证书目录和证书签发、注销、更新等；

(3)商家服务器提供 HTTP 服务，为用户提供商品浏览和定购，并提供支付平台分布式接口；

(4)移动支付平台提供与银行的接口，提供用户手机号码与银行账号绑定的功能，提供与智能终端支付接口，提供与商家信息交互接口。

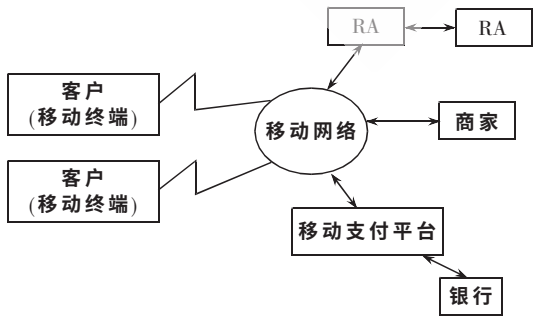

图 2 安全移动支付系统组成图

客户在申请移动支付服务业务时，首先到银行(或银行网站上)开户或使用已有的账户来绑定手持设备 ID(如手机号)，这里手机 ID 用客户的数字证书来表示。

2.2 系统安全解决方案

整个系统的实现由 4 部分组成，它们包括：商家安全支付软件 MSS、客户安全支付软件 CSS、商业银行安全支付软件 BSS 和交易中心安全支付软件 TSS。

2.2.1 安全功能设计

根据系统实体、交易流程及安全要求，4 个软件模块的主要安全功能设计如下：

(1)MSS：该软件构成了卖方交易平台。首先应提供商品订购过程中所需的安全功能：与客户之间的双向身份认证，验证客户对定单的数字签名，生成商家对账单和承诺的数字签名，加解密与客户之间传递的信息。其次提供支付过程所需的安全功能：与交易中心之间的双向身份认证，验证银行返回的支付结果的数字签名。另外还记录客户签名后的定单信息，记录支付信息以及保存自己签名后的送货信息等。

由上述功能可知，该软件模块应提供身份认证、数字签名、客户定购及支付信息的处理、密钥及证书管理等服务。

(2)CSS：该软件构成了买方交易平台。它首先提供产品订购过程中所需的安全功能：与商家之间的双向身份认证，产生客户对定单的数字签名，验证商家对账单和承诺的数字签名，加解密与商家之间传递的信息。其次提供支付过程所需的安全功能：与交易中心之间的双向身份认证，采用银行的公钥加密提交的转账信息，生成交易中心需保存的交易证据，产生对交易证据的数字签名。

该软件模块应提供身份认证、数字签名、交易与支付历史数据存储管理、支付交易查询、密钥与证书管理等服务。

(3)TSS：该软件构成了安全交易平台。它记录了交易过程中传输的各种重要信息、可供争议解决的证据。其安全功能是：与商家之间的双向身份认证、与客户之间的双向身份认证、与银行之间的双向身份认证、验证客户提交的交易证据的数字签名、验证银行响应的支付结果的数字签名，并在出现争议时验证争议各方提交证据的真伪。

该模块应提供身份认证、数字签名、与商业银行业务系统联系的公共接口、交易与支付历史数据存储管理、支付交易仲裁、密钥与证书管理等服务。

(4)BSS：该软件提供支付网关功能，其主要作用是完成银行网络与 Internet 及移动网络之间的通信、协议转换以及数据的加解密，以保护银行内部网络的安全。实现与 TTP 之间的双向身份识别，验证客户的数字签名，产生支付结果的数字签名，解密客户传来的转帐通知，

用商家的公钥加密支付结果。

该模块应提供:身份认证、数字签名、与交易中心业务系统联系的公共接口、支付历史数据存储管理、密钥与证书管理等服务。

2.2.2 数字证书的配置

模块 MSS、CSS、TSS、BSS 均为基于 WPKI 的安全应用软件,因此需配置相应的数字证书。具体配置情况如下:

(1)MSS:配置商家服务器证书,用于与客户 CSS 之间的身份识别、消息加密和生成数字签名;用于与交易中心 TSS 之间的身份识别、消息加密和生成数字签名;

(2)CSS:配置客户服务器证书,用于与 MSS 之间的身份识别、消息加密和生成数字签名;用于与 TSS 之间的身份识别、消息加密和生成数字签名;

(3)TSS:配置交易中心的服务器证书,用于与 MSS、CSS、BSS 之间的身份识别、消息加密和生成数字签名;

(4)BSS:配置商业银行的服务器证书,用于与 TSS 之间的身份识别、消息加密和生成数字签名。

3 系统的实现

3.1 系统原理和交易步骤

该系统包括 5 个实体:商家、客户、银行系统、认证中心 CFCA(China Finance Certificate Authority,中国金融认证中心)和交易中心 TTP(Trusted Third Party,第三方信任实体)。其中,商家和用户完成定单及账单的提交和生成;银行系统负责处理支付信息;CFCA 和 PKI Protal (RA)用作保证系统的安全性;TTP 记录了交易过程中传输的各种重要信息、可供解决争议的证据。系统原理如图 3 所示。

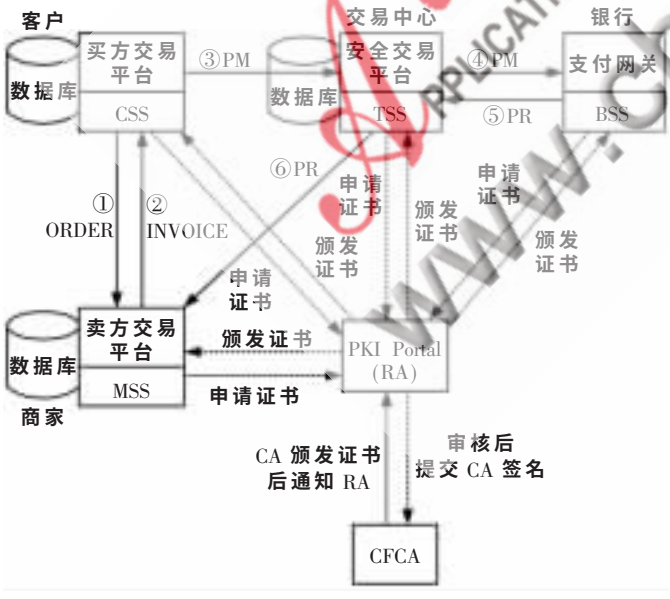

图 3 系统原理图

图中虚线代表 CA 分别向商家、客户、TTP 和商业银行颁发身份证书,实线代表系统的交易流程。根据网上交易过程的步骤分析,并参考了各种支付协议的数据流程,确定了该系统的信息流、数据流、资金流按下列步骤进行:

(1)客户向商家下定单

客户通过手机浏览器在商家的 Web 服务器定购商品。客户根据商家的要求向商家提交定单 Order,商家根据定单形成相应的账单 Invoice,并将 Invoice 及商家的说明及承诺 Statement 发到客户手机浏览器。

(2)客户通过手机支付货款

客户通过 TTP 的安全移动支付服务平台到银行支付货款。首先,客户将支付消息 PM(Pay Message)提交到 TTP 的安全移动支付服务平台;之后,TTP 安全移动支付服务平台将 PM 转发到银行;银行验证客户对 PM 的数字签名,取出支付指令 PI(Pay Instruction),根据 PI 进行转账;并将支付结果 PR(Pay Result)(包括支付金额、是否成功等信息)告知 TTP 安全支付平台;最后 TTP 安全移动支付平台将支付结果 PR 实时告知商家。

3.2 安全移动支付系统工作流程及实现

以客户提交订单的过程为例说明安全移动支付系统的工作流程及系统实现。

(1)客户在商家的 Web 服务器上选择要订购的产品,并填写完其他必要信息(如送货时间、地点等)后,点击页面上的提交按钮,此时激活 CSS 软件。CSS 软件发送一个初始请求(InitPM-Requ)给商家的 MSS 软件,InitCM-Requ 的数据结构如表 1 所示。

表 1 InitCM-Requ 的数据结构

数据单元	描述
InitCM-Requ	{Message, IDC}
Message	客户向商家发出购买信息
IDC	客户软件产生的本地 ID

(2)MSS 收到 InitPM-Requ 后,向 CSS 发送初始回答(InitPM-Resp);InitCM-Resp 的数据结构如表 2 所示。

表 2 InitPM-Resp 的数据结构

数据单元	描述
InitCM-Resp	{CertM, Resp-Msg, SIGN-SKM(H(Resp-Msg))}
CertM	商家的数字证书
Resp-Msg	{Random-T, message, IDM}
Random-T	标志这次交易
message	说明已经收到初始请求
IDM	商家软件产生的本地 ID
H(Resp-Msg)	用 Hash 函数对 Resp-Msg 求摘要
SIGN-SKM	商家用签名私钥 SK_M 对摘要签名

(3)CSS 收到 MSS 的初始回答(InitCM-Resp)后,做以下几步:

①Verify(CertM),若核实,则往下进行,否则终止;

②判断 $DE-PK_M(SIGN-SK(H(Resp-Msg)))$ 是否等于 H(Resp-Msg),若相等,则往下进行,否则终止($DE-PK_M$ 为 CSS 用商家签名公钥验证其签名);

③从 Resp-Msg 中获得交易标识 Random-T，并根据页面上订购的产品，生成 OI（Order-Instruction，订货指令），OI 的数据结构如表 3 所示。

表 3 OI 的数据结构

数据单元	描述
OI	{Order，Random-T，Datetime-C}
Order	订单及其相关描述
Random-T	从 InitPM-Resp 得到
Datetime-C	标识定货时间

④CSS 发送购买请求（Purchase-Requ）给 MSS，Purchase-Requ 的数据结构如表 4 所示。

表 4 Purchase-Requ 的数据结构

数据单元	描述
Purchase-Requ	{CertC，en-OI，OI-Envelop，SING-SKC(H(OI))}
CertC	客户的数字证书
en-OI	{EN-KC(OI)} （CSS 软件随机生成对称密钥 KC 加密 OI）
OI-Envelop	{EN-$PK_M(K_C)$} （CSS 软件用商家公开密钥加密 KC 形成数字信封）
OI	订货指令
H(OI)	用 Hash 函数对 OI 请求摘要
SING-SKC	客户用签名私钥 SK_C 对摘要签名

该安全移动支付系统提供了通过 WAP/WTLS 无线环境与第三方支付机构建立联系的安全支付方式。各参与实体所使用的公钥由 CFCA 签发的证书来分配，可以充分保障移动电子商务支付的机密性、认证性、公平性和完整性。同时，完整性中的数字签名技术也提供了安全移动电子支付的不可否认性。实现了从传统网上购物及网上银行卡支付向手机 WAP 无线购物及在手机终端直接使用银行卡进行网上支付的延伸，扩充了网上购物和支付的渠道，为人们的日常生活提供更多的便利性。

参考文献

[1] 刘英群，王克宏.VMSDT——一个设备无关的移动电子商务开发平台[J].微型机与应用，2004，23(02)：58-60.

[2] Wireless application protocol.Public Key Infrastructure definition.http://www.forum.com.2001.

[3] 赵文，戴宗坤.WPKI 应用体系架构研究[J].四川大学学报(自然科学版)，2005，8(4)：725-730.

[4] SANDRA K M.Facing the challenge of wireless security.IEEE Computer Magazine，2001：16-18.

[5] ZHANG Wei Dong.Research on security in mobile commerce[J].Xidian University，2005(1)：42-43.

[6] SANG K K.Modeling of policy-based mobile payment[J].Advanced Communication Technology，The 6th International Conference，2004(2)：1009-1011.

（收稿日期：2009-10-20）

作者简介：

石俊萍，女，1974年生，硕士，讲师，主要研究方向：数据库技术、计算机网络。

李必云，男，1973年生，硕士，讲师，主要研究方向：计算机网络、嵌入式系统。