文章编号：1005-8451（2006）01-0045-03

电子支付系统与安全

傅迎华[1]，张 勇[2]
（1.上海理工大学 计算机工程学院，上海 200093；2.上海铁路局 电子计算技术中心，上海 200071）

摘 要：电子支付系统的安全、可靠、快捷和方便是铁路电子商务被广泛接受并顺利完成的保证。介绍基于安全认证协议SSL/SET建立的电子支付系统模型及具体实现。

关键词：电子支付系统；电子商务；安全认证协议；实现
中图分类号：TP309 **文献标识码**：A

Electronic Payment System and security

FU Ying-hua[1], ZHANG Yong[2]
(1. School of Computer Engineering, Shanghai Institute of Technology, Shanghai 200093; 2. Electronic Computing Technical Centre of Shanghai Railway Administration, Shanghai 200071, China)

Abstract: Security, reliability, swiftness and convenience of electronics payment were guarantee for railway's e-Business to be accepted and completely implemented. It was analyzed and discussed two models based on SSL/SET and the methods of their implementation.

Key words: Electronic Payment System; e-Business; SSL/SET; implementation

铁路电子商务是铁路信息化的重要组成部分，是铁路客货运输进一步发展的新机遇。完整的铁路电子商务活动一般包括商务信息、资金支付和商品配送3个阶段，表现为信息流、物流和资金流3个方面。资金流是电子商务业务流程的重要环节，服务于资金流的电子支付系统已经成为商务各方关注的焦点。为了保证电子支付系统的安全性，必须有一套有效的安全技术作为保证，通常有加密技术、认证技术（数字签名、数字证书等）、安全认证协议（SSL、SET）等。

收稿日期：2005-08-16
作者简介：傅迎华，讲师；张 勇，工程师。

1 基于安全认证协议的电子支付系统模型

目前，电子商务中有两种安全认证协议被广泛使用，即安全套接层SSL协议和安全电子交易SET协议，下面将介绍基于这两种协议的电子支付系统模型。

1.1 基于SSL协议机制的电子支付系统模型

重要信息。

另外，自然语言中的词语存在多义词和同义词，这也给分词和准确聚类带来了困难。潜在语义索引是一种向量检索方法，用于文档检索有较好的效果，所以有人尝试把它引入邮件过滤来解决汉字多义词和同义词的问题。

3 结束语

垃圾邮件问题已经为人们广泛关注，反垃圾邮件技术已成为信息安全领域一个研究热点。如何准确过滤中文垃圾邮件是一个亟待解决的问题。在基于内容统计的邮件过滤器中，很多都把基于文本分类的模型用在反垃圾邮件领域，如贝叶斯模型，k—最近邻算法，SVM模型，等等，都取得了相当好的效果，但是还没有大量实验表明这些方法也能很好地运用在中文垃圾邮件的过滤上，因此有必要在这方面进一步研究。

参考文献：

[1] 李 洋. 基于数据挖掘的邮件分类识别研究[D]. 重庆：重庆大学，2004.
[2] 于 洪. Rough Set理论及其在数据挖掘中的应用研究[D]. 重庆：重庆大学，2003.
[3] 曹麒麟，张千里. 垃圾邮件与反垃圾邮件[M]. 北京：人民邮电出版社，2003.

基于SSL（Secure Socket Layer）协议机制的电子支付系统模型如图1。

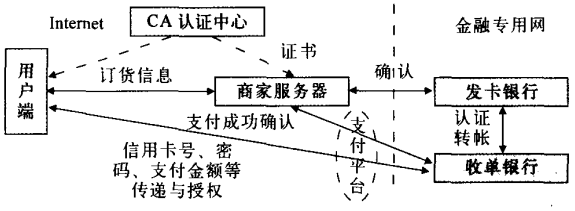

图1 基于SS协议的电子支付系统基本模型

（1）用户登陆商家电子商务网站，验证商家身份；

（2）用户选择相应服务，向商家发出购买请求；

（3）商家回复用户的购买请求，用户机浏览器弹出新窗口页面，提示即将建立与发卡银行端网络服务器的安全连接，SSL协议机制介入开始。用户端自动验证银行端网络服务器的数字证书身份后，SSL握手协议完成，双方建立起安全通道；

（4）出现相应银行的支付网页，显示从商家发来的相应的订单及支付金额信息，用户填写支付信息，确认支付。支付成功后，用户确认离开安全SSL连接；

（5）银行在后台把相关资金转入商家帐号，发送付款成功消息给商家；

（6）商家收到银行发来的付款成功消息后，发送收款确认信息给用户，支付过程结束。

1.2 基于SET协议机制的电子支付模型

在SET协议环境下，客户需要在用户端下载一个用户端软件，商家需要在服务器端安装服务器端软件，支付网关需要安装对应的网关转换软件等，并要求参与各方为自己下载数字证书，借此获得自己的公私钥对，并且把公钥公开出去。基于SET协议的电子支付系统模型如图2。

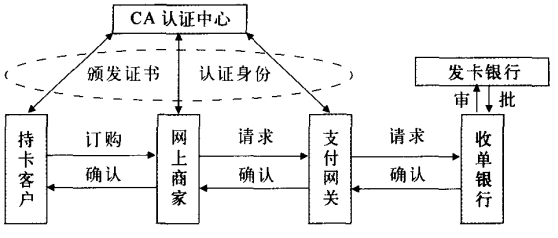

图2 基于SET协议的电子支付系统基本模型

（1）持卡人使用浏览器在商家Web主页上查看商品和服务的信息，选择要购买的商品和服务，填写定购单，提交购物请求并选择在线网络支付类型（如信用卡）；

（2）用户计算机自动激活装有电子钱包信息的用户端软件，输入软件用户名及其相关信息，取出里面的电子钱包进行支付，SET协议开始介入；

（3）用户端软件自动与商家服务器软件进行SET协议规定的信息交换与身份认证，然后自动提取电子钱包等信息，连同订货单等一起发送给商家；

（4）商家收到持卡客户发来的信息，验证通过后，回复持卡客户，同时进行结算请求，并将客户端信息一起发给支付网关；

（5）支付网关收到支付信息后，转入后台银行网络处理，通过验证审核后，支付网关收到银行端发来的支付确认信息，否则向商家回复支付不成功；

（6）持卡人收到商家发来的购货确认与支付信息后，表示这次购货与网络支付成功，客户端软件自动关闭，网络支付结束。

2 电子支付系统模型的具体实现

2.1 基于SSL协议的电子支付模型的具体实现

当一SSL客户和服务器开始通讯时，它们就协议版本、加密算法的选择、加密技术的应用等进行协商以产生共享的密钥，其过程如图3（其中*表示是可选的消息）。

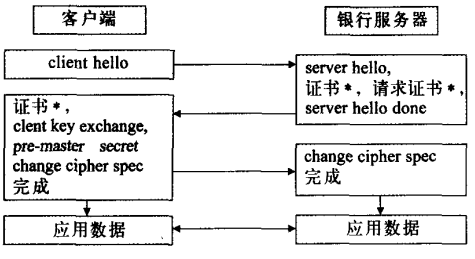

图3 SSL交互过程

（1）客户端首先发出客户问候消息（client hello message），服务器收到之后或者发出服务器问候消息（server hello message），或者发生一终止性的错误。问候消息产生了下列属性：协议版本号、加密套接字及压缩方法，并产生两个随机数且相互交换。

（2）在问候消息之后，服务器立即发出其证书，如果需要，它将向客户端请求证书（certificate request）；然后发出的服务器问候结束消息（server hello done message），等待客户端的回应。

（3）如果客户端收到certificate request消息，则发出其证书，或者一个no certificate报警；然后，发送客户端密钥交换消息（client key exchange

message）确定会话密钥。如果客户和服务器公钥算法是RSA算法，此时客户端产生预主密钥（pre-master secret），并用服务器的公钥PB对其进行加密，然后将加密的结果用消息发给服务器。大多数SSL公钥算法采用RSA算法。

（4）服务器端收到客户端消息后，使用其私钥PV解密得到预主密钥，并用协商后的算法、预主密钥产生真正的会话密钥（主密钥master secret）；客户端经过同样的步骤得到同一个会话密钥（主密钥master secret）。

（5）客户端发送一个改变加密说明（change cipher spec）消息，通知应用数据（如支付消息）将会用会话密钥加密和解密，并发出结束消息。SSL握手过程结束，在发出结束消息之后便可发出加密过的应用数据。

2.2 基于SET协议的电子支付模型的具体实现

（1）持卡者发送支付初始化请求消息InReq给购票中心。

（2）购票中心收到持卡者的初始化请求消息后，产生响应消息InRes，同时附上购票中心的证书和支付网关的证书。

（3）持卡者接收InRes后，验证证书的有效性。生成订购信息OI（order information）和支付信息PI（payment information）。持卡者将OI、PI用HASH运算，分别得到摘要MDB和MDC；接着将MDB和MDC连接后再运算，得到MDBC；用A的私钥PVA对MDBC加密，形成双重数字签名DS。用密钥SKA1和SKA2对OI、PI加密，得密文EMB、EMC。再用B的公钥PBB对SKA1加密得到信封DEB，用C的公钥PBC对SKA2和持卡客户账号加密得到信封DEC。接着持卡人向购票中心发出购票请求消息PReq，包含持卡人的数字证书，OI和PI密文EMB、EMC、DS、DEB、DEC、MDB和MDC等。其中EMC，DS，DEC和MDB等由购票中心转发给支付网关。

（4）购票中心接收到PReq后，验证持卡人证书的有效性。先用PVB打开DEB取出SKA1，用SKA1解开EMB得到OI'，将OI'作摘要得MD'B，将MD'B MDC与连接后作摘要DS'，再用从证书中取出PBA解除签名中的DS，如果DS'= DS，则如果数据完整，处理订单信息产生将支付请求Rb，否则丢弃。购票中心对Rb做摘要得MDR，用PVB对其签名，同时用密钥SKB将Rb加密，然后，用PBC将SKB和签名加密成数字信封DE R。最后购票中心将Rb密文、DE R、支付信息（EMC，DS，DEC，MDB）及持卡人和购票中心的证书等一起传给支付网关。

（5）支付网关分别验证购票中心和持卡人的数据。首先，支付网关确认购票中心证书，用PVC打开DE R获得密钥SKB，打开得到用SKB，解开密文得到R'b，再用PBB（包含在购票中心的证书中）打开签名得到摘要MDR，同时用HASH算法对R'b摘要得MD'R，再判断MDR和MD'R是否相同，如果相同则数据完整，如果不同则丢弃。接着按相同的步骤检查持卡者的数据。通过审核后，支付网关向发卡银行提交授权请求。

（6）支付网关和收单银行、收单银行和发卡银行之间，通过金融专用网相连，SET不参与。当银行完成相关支付结算后，支付网关得到发卡行的授权确认，产生“支付应答”消息AuthRes，并对其进行数字签名、用SKC加密、将SKC装入数字信封。支付网关将数字证书、“支付应答”签名、装有密钥SKC的信封，“支付应答”密文一起发送给购票中心。

（7）购票中心接受到信息后，检查支付网关发来的“支付应答”。购票中心产生“购物应答”消息PRes。对“购物应答”产生摘要，签名，最后，将商家证书、购物应答、数字签名一起发往持卡客户。购票中心收到“支付应答”，表明交易成功。

（8）持卡客户收到“购物应答”后，验证购票中心的数据。如果完整，则成功，如果不完整，则丢弃。交易与支付流程结束。

3 结束语

安全并且快捷的电子支付系统是铁路电子商务安全、快速和大规模开展的保证，也是发挥其优越性的保证。当前，由于基于SSL协议的电子支付系统成本低、应用简单透明、相对简单且快捷而占据优势地位。而基于SET协议的电子支付系统实现了多方认证，采用公钥加密、信息摘要、数字签名和双重签名等技术，确保了信息的保密性、完整性和不可否认性，使整个支付过程更安全，在未来的铁路电子商务中它将会逐步占据主导地位。

参考文献：

[1] 柯新生. 网络支付与结算[M]. 北京：电子工业出版社，2004，8.

[2] Andrew Nash. 公钥基础设施（PKI）[M]. 北京：清华大学出版社，2002，12.