

文章编号:1001-9081(2006)12-2910-03

基于可信第三方的安全支付协议的设计与分析

孙玲芳,许金波,朱 芸

(江苏科技大学 经济管理学院, 江苏 镇江 212003)

(slf0308@163.com)

摘 要:设计了一种同时支持数字商品和实物商品在线支付的安全支付协议 SETTP。构建了具有交易冲突仲裁和数据备份功能的可信第三方,提出了在银行支付中设置支付时间期限 PTE 的方法,以确保双方的交易公平。最后分析了 SETTP 的安全性、原子性和交易公平性。

关键词:SETTP;实物商品;可信第三方;支付时间期限;公平性

中图分类号:TP393.08 **文献标识码:**A

Design and analysis of secure payment protocol based on trusted third party

SUN Ling-fang, XU Jin-bo, ZU Yun

(School of Economic and Management, Jiangsu University of Science and Technology, Zhenjiang Jiangsu 212003, China)

Abstract: A payment protocol named Secure Electronic Transaction based on Trusted Third Party (SETTP) was proposed, in which both electronic and physical goods could be paid on line. A trusted third party which has the functions of confliction-arbitrate and data backup was constructed. A method of setting Payment Time Expire (PTE) during the process of bank payment was put forward to make sure the fairness to both parties of the transaction. Finally the characteristics of the SETTP protocol such as security, atomicity and fairness were analyzed.

Key words: SETTP; physical goods; TTP; PTE; fairness

安全协议是电子商务在线支付的关键。虽然目前电子商务安全协议很多,但这些协议在安全性、原子性以及适用性等方面存在着一些问题,特别是缺乏同时支持数字商品和实物商品的在线支付协议^[1,2]。基于此,本文在研究电子商务协议理论的基础上^[3~5],结合实际情况,提出一种新的安全支付协议——基于可信第三方的安全电子交易协议(Secure Electronic Transaction based on Trusted Third Party, SETTP),该协议不但能满足电子商务协议的安全性、原子性和公平交易的原则,而且也同时支持数字商品和实物商品的在线支付。

1 SETTP 协议模型的建模方法

1.1 SETTP 协议的有关说明

SETTP 协议的参与者由持卡者 C(Cardholder)、商家 M(Merchant)、可信第三方 TTP(Trusted Third Party)和银行 B(Bank)组成。其中可信第三方由支付网关 P(Payment gateway)、存储数据库 D(Databank)和仲裁机构 A(Arbitration)组成。在 TTP 中,支付网关负责证书的发放、身份认证和支付授权工作;存储数据库对交易的重要数据进行备份,为交易纠纷的处理提供证据;仲裁机构只有在出现交易纠纷的情况下才发挥作用。SETTP 协议是基于以下的安全性假设:1)TTP 被认为是可信的;2)C、M 的证书由 P 发放;3)只有 P 才可以完成资金划拨功能。SETTP 协议采用的加密技术有对称加密算法、非对称加密算法、数字信封、数字签名、消息摘要等技术。为了便于描述协议,对于协议中的 Hash 函数、数字签名检验过程全部略去。在实际过程中,数字签名仍然是不可缺少的部分。在协议描述中所使用的相关符号说明如下:

{ } 中表示为需要发送的消息;
[] 中表示为发送方所需要做的计算;
→ 表示信息发送;
|| 表示报文合并;
 $D_i()$ 表示用 i 进行解密;
 $E_i()$ 表示用 i 进行加密;
 $CK()$ 表示对证书进行合法性检验;
 No 表示商品编号;
 OI 表示持卡人 C 的订单;
 pkc 表示持卡人 C 的公钥;
 skc 表示持卡人 C 的私钥;
 pkm 表示商家 M 的公钥;
 skm 表示商家 M 的私钥;
 pkp 表示支付网关 P 的公钥;
 skp 表示支付网关 P 的私钥;
 Cer_C 表示持卡人 C 的数字证书;
 Cer_M 表示商家 M 的数字证书;
 Cer_P 表示支付网关 P 的数字证书;
 PTE 表示支付时间期限;
 TID 表示商家为持卡人生成的交易号,该号码是唯一的;
 PI 表示持卡人 C 的支付指令(信用卡密码);
 PAN 表示持卡人 C 的支付信息(姓名、信用卡号等);
 Pay 表示商家 M 的付款要求(付款金额、商家银行账号等);
 $Req()$ 表示持卡人 C 发出的请求(buy/pause/end——购买/暂停/结束);
 $Res()$ 表示 TTP 的仲裁机构的协调结果(success/

收稿日期:2006-06-26;修订日期:2006-08-29 基金项目:国家自然科学基金资助项目(70472005);江苏省高校自然科学基金计划资助项目(03KJD630011);镇江市科技局项目(2005QT008J)

作者简介:孙玲芳(1963-),男,江苏镇江人,副教授,博士,主要研究方向:管理信息系统、电子商务;许金波(1980-),男,江苏盐城人,硕士研究生,主要研究方向:管理信息系统、电子商务安全;朱芸(1982-),女,江苏扬州人,硕士研究生,主要研究方向:企业协同集成。

failure——成功/失败);

$Msg()$ 表示支付状态信息 (agree/pause/end/success/failure——支付确认/暂停/终止/成功/失败)。

1.2 SETTP 协议的流程描述

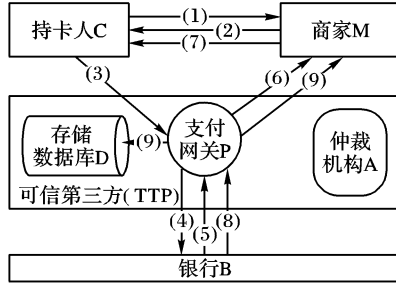


图1 SETTP 协议流程

图1是一个顺利交易的 SETTP 协议流程图,其步骤如下:

1) $C \rightarrow M: \{Req(buy)\}[]$

持卡人浏览商家网站,选定商品(该商品可以是数字商品,也可以是实物商品)后放入购物车并按确认,协议开始启动,把持卡人想要购买的商品发送给商家。

2) $M \rightarrow C: \{OI'\} [OI' = E_{skm}(Cer_M \parallel OI), OI = TID \parallel No \parallel PTE \parallel Pay]$

商家生成订单并把自己的证书和订单经数字签名后发送给持卡人。订单包括交易号、商品编号、支付时间期限和支付要求。

3) $C \rightarrow P: \{PI' \parallel OI'\}$

$[(Cer_M \parallel OI) = D_{plm}(E_{skm}(Cer_M \parallel OI)), CK(Cer_M)]$

$PI' = E_{pkp}(Cer_C \parallel PI \parallel PAN)$

持卡人用商家的公钥解密后确认商家的身份,在确认订单后,持卡人将自己的证书、支付指令、支付信息加密后连同 OI' 发送给 TTP 中的支付网关。

4) $P \rightarrow B: \{PAN \parallel PI \parallel Pay \parallel PTE\}; P \rightarrow D: \{OI \parallel Cer_C \parallel Cer_M \parallel PAN \parallel Pay\}$

$[(Cer_M \parallel OI) = D_{plm}(OI'), (Cer_C \parallel PI \parallel PAN) = D_{skp}(PI'), CK(Cer_C), CK(Cer_M)]$

支付网关验证交易双方的证书,确认双方的合法身份。之后支付网关将持卡人的支付信息、支付指令、商家的付款要求以及支付期限发送给银行。同时将持卡人的订单、交易双方的证书、商家的付款要求以及持卡人的支付信息发送给存储数据库。

存储数据库收到支付网关发送的消息后,将产生交易记录 Note, 记录: Data, TID, No, Cer_C , Cer_M , C_{acct} , M_{acct} , Value, PTE, Token。其中 Date 表示交易日期, TID 表示交易号, No 表示商品编号, C_{acct} 、 M_{acct} 表示交易双方的银行账户, Value 表示交易的金额, PTE 表示支付时间期限, Token 表示支付特征位(初始值为 0), 如果支付成功则 Token 置为 1, 否则 Token 置为 0。

5) $B \rightarrow P: \{Msg(agree)\}$

银行收到支付网关的信息后冻结持卡人交易所需的贷款金额。持卡人的贷款被冻结后,持卡人在无法将贷款取出或转账,只有被银行解冻后,持卡人才能取走贷款。

6) $P \rightarrow M: \{Msg'(agree)\} [Msg'(agree) = E_{plm}(Msg(agree) \parallel Cer_p)]$

支付网关将支付确认的信息发送给商家,通知商家准备发货给持卡人。

7) $M \rightarrow C: \{Msg''(agree)\}$

$[Msg(agree) \parallel Cer_p] = D_{skm}(Msg'(agree)), CK(Cer_p)$

$Msg''(agree) = E_{plm}(Msg(agree) \parallel Cer_m)]$

商家确认支付网关身份后,将支付确认的信息发送给持卡人并发货,如果是数字商品,则对数字商品加密后发送给持卡人;如果是实物商品,则通过物流系统发送给持卡人,并索要持卡人的商品签收单。

8) $B \rightarrow P: \{Msg(success)\}$

如持卡人满意,并在交易安全期内无任何信息反馈给支付网关,则银行在 PTE 结束时将货款转移到商家帐户,至此支付完成。银行将支付成功的消息发送给支付网关

9) $P \rightarrow M: \{Msg'(success)\} [Msg'(success) = E_{plm}(Msg(success) \parallel Cer_p)]$

$P \rightarrow D: \{Msg(success)\}$

支付网关将支付成功的消息发送给商家和存储数据库,存储数据库将 Token 位置为 1, 此时交易结束。

1.3 交易中遇到问题的处理

在实际交易过程中,并不是每次交易都是很顺利的。当交易过程出现纠纷时, TTP 的仲裁机构和存储数据库便发挥了重要的作用。实际交易过程遇到的问题主要有以下几种:

1) 若持卡人帐号的金额不足、帐户过期或密码不正确,则如图 2 所示。

$B \rightarrow P: \{Msg(failure)\}; P \rightarrow M: \{Msg(failure)\}; M \rightarrow C: \{Msg(failure)\}$

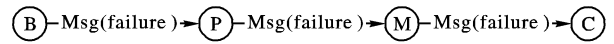


图2 第一种交易问题的 SETTP 流程

银行向支付网关发送支付失败,支付网关通知商家,商家通知持卡人并停止向持卡人发货。至此交易结束。

2) 当持卡人收到商品后发现商家所送的商品与客户购买的商品不符,或持卡人不同意所购商品,此时, SETTP 协议处理流程如图 3 所示,其步骤如下:

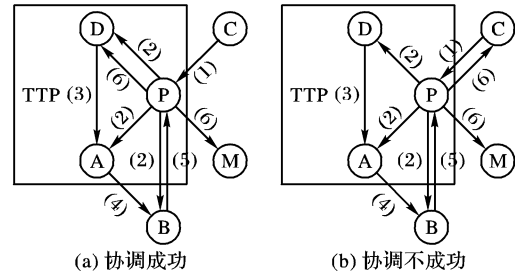


图3 第二种交易问题的 SETTP 流程

(1) $C \rightarrow P: \{Req'(pause)\} [Req'(pause) = E_{pkp}(Cer_C Req(pause) \parallel TID)]$

持卡人将自己的证书、暂停交易请求和交易号发送给支付网关,申请暂停交易。

(2) $P \rightarrow A: \{Req(pause)\}; P \rightarrow D: \{TID\}; P \rightarrow B: \{Req(pause)\}$

$[Cer_C \parallel Req(pause) \parallel TID = D_{skp}(Req'(pause)), CK(Cer_C)]$

支付网关确认持卡人身份后通知仲裁机构卷入协调,通知存储数据库提取这次交易的数据,通知银行将交易期延长直至协调结束。

(3) $D \rightarrow A: \{Note\}$

存储数据库根据交易号 TID 提取这次交易的交易记录 Note, 并发送给仲裁机构,为交易纠纷的处理提供证据。仲裁机构对交易纠纷进行协调。

(a) 若协调成功,持卡人同意购买该商品,则:

(4) $A \rightarrow B: \{Res(success)\}$

(5) $B \rightarrow P: \{Msg(success)\}$

(6) $P \rightarrow M: \{Msg'(success)\} [Msg'(success) = E_{pkm}(Msg(success) \parallel Cer_p)]$
 $P \rightarrow D: \{Msg(success)\}$

仲裁机构向银行发送协调成功信息。银行收到协调成功信息后,将持卡人货款支付给商家;并通知支付网关。支付网关将支付成功的消息通知商家,并通知存储数据库将 Token 位置为 1,交易结束。

(b) 若协调不成功,持卡人不同意购买该商品并退还商品给商家(退还商品时,需向商家索要退货签收单):

(4) $A \rightarrow B: \{Res(failure)\}$

(5) $B \rightarrow P: \{Msg(end)\}$

(6) $P \rightarrow M: \{Msg'(end)\} [Msg'(end) = E_{pkm}(Msg(end) \parallel Cer_p)]$

$P \rightarrow C: \{Msg''(end)\} [Msg''(end) = E_{pkc}(Msg(end) \parallel Cer_p)]$

仲裁机构向银行发送协调失败信息。银行收到协调失败的信息后,将终止向商家支付持卡人的货款,并将持卡人的货款金额解冻,同时将支付终止的消息通知支付网关。支付网关将支付终止的消息发送给商家和持卡人。至此交易结束。

3) 商家收到支付网关的支付确认信息后,没有发货给持卡人,此时,SETTP 协议处理流程如图 4 所示,其步骤如下:

(1) $C \rightarrow P: \{Req'(end)\} [Req'(end) = E_{pkp}(Cer_c \parallel Req(end))]$

(2) $P \rightarrow A: \{Req(end)\}; P \rightarrow B: \{Req(end)\}$

$[Cer_c \parallel Req(end) = D_{skp}(Req'(end)), CK(Cer_c)]$

(3) $A \rightarrow B: \{Res(failure)\}$

(4) $B \rightarrow P: \{Msg(end)\}$

(5) $P \rightarrow M: \{Msg'(end)\} [Msg'(end) = E_{pkm}(Msg(end) \parallel Cer_p)]$

$P \rightarrow C: \{Msg''(end)\} [Msg''(end) = E_{pkc}(Msg(end) \parallel Cer_p)]$

持卡人将自己的证书和结束交易请求加密后发送给支付网关,申请结束交易。支付网关确认持卡人身份后通知仲裁机构进行仲裁,并通知银行将 PTE 延长至仲裁结束。如果商家确实没有发货,商家就不能向仲裁机构提供持卡人的签收单凭证,则仲裁机构向银行发送协调失败信息。银行收到协调失败的信息后,将终止向商家支付持卡人的货款,并将持卡人的货款金额冻结,同时将支付终止的消息通知支付网关。支付网关将支付终止的消息发送给商家和持卡人。至此交易结束。

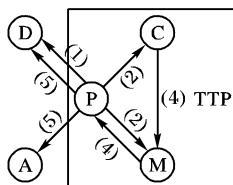


图 4 第三种交易问题的 SETTP 流程

2 SETTP 协议的分析

2.1 协议的安全性分析

(1) 持卡人、商家和支付网关之间的通信采用对称加密算法和非对称加密算法来保证数据传输的安全。

(2) 在 SETTP 协议中,持卡人和商家的证书是由支付网关发放的,在交易过程中,支付网关对持卡人和商家进行身份认证,从而确保交易双方身份的合法性。

(3) 由于支付信息由持卡人直接发送给支付网关,不经过商家,因此持卡人银行账号和密码不会被商家知道。

(4) 在 SETTP 协议中,一个数字签名是采用发送者私有密钥加密的 Hash 值,如果交易信息被修改,则 Hash 值也不同。从而保证了消息内数据的完整性。

2.2 协议的公平交易分析

在 SETTP 协议中,TTP 为交易双方的公平交易提供了强有力的保证。持卡人购买商品后,货款立即被银行冻结,在 PTE 内,货款既不能被持卡人取走,也没有支付给商家。

如果在 PTE 内,持卡人对商品有异议,则向 TTP 申请协调。TTP 的仲裁机构卷入协调。只有在持卡人对商品无异议并同意购买时,银行才向商家支付货款。否则,银行终止向商家支付货款,并将持卡人货款解冻,货款又发归还给了商家。如果在 PTE 内,持卡人对自己所购商品无异议,则银行在 PTE 结束时,将货款转移到商家账户,至此支付完成。由此可以看出,持卡人和商家之间的交易是公平的。

2.3 协议的原子性分析

(1) 钱原子性:从协议的执行过程可知,钱在交易过程是守恒的。持卡人只能得到与所付货款等值的商品,而商家也不能从持卡人那里得到多余的金额。

(2) 商品原子性:从协议的执行过程可知,只有持卡人得到正确的商品后,银行才将货款支付给商家,所以持卡人付了款后就一定会得到正确的商品;如果持卡人不付款,商家就不会给持卡人发货,所以持卡人得到商品就一定给商家付了款。

(3) 确认发送原子性:从协议的执行过程可知,如果持卡人得到的商品不是他所定购的商品,那么商家是不会从银行那里得到货款的。因此,如果交易成功,那么持卡人得到的商品就一定是他所定购的商品,商家也发送了持卡人所定购的商品。

3 结语

本文提出了一种基于可信第三方的电子商务安全协议——SETTP 协议,该协议满足电子商务交易的安全性、原子性、和公平交易的原则^[6],同时也支持数字商品和实物商品的交易。SETTP 协议在支付授权时引入了支付时间期限 PTE 的概念,在支付期限内,货款暂时由银行保管(银行冻结货款)。只有在 PTE 内,持卡人收到自己购买的商品,并对该商品无异议的情况下,银行才可以在 PTE 结束时将货款支付给商家。如果在 PTE 内,持卡人没有收到商品,或对商品不满,可向 TTP 的仲裁机构提出协调申请;如果协调不成功(持卡人想终止交易),则在持卡人退还商品后,银行将货款归还给持卡人(银行解冻货款)。而 TTP 的存储数据库对交易数据进行备份,为交易纠纷的解决提供了重要的证据。

参考文献:

- [1] 祁明. 电子商务安全与保密[M]. 北京: 高等教育出版社, 2001.
- [2] 梁晋, 施仁, 王育民, 等. 电子商务关键技术[M]. 北京: 经济科学出版社, 2002.
- [3] 甘元驹. 基于多银行的匿名的电子商务协议[J]. 计算机工程与应用, 2003, 39(29): 161-163.
- [4] 卿斯汉. 电子商务协议中的可信第三方角色[J]. 软件学报, 2003, 14(11): 1936-1943.
- [5] 彭勋, 董荣胜, 郭云川, 等. 安全支付协议与验证研究[J]. 计算机工程与应用, 2005, 41(6): 139-143.
- [6] TYGAR JD. Atomicity in Electronic Commerce[A]. Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing[C]. 1996. 8-26.