Design of Secure Internet Payment System Based on BtoB

Kai XIANG
School. of Computing, Hubei University of Economics, Wuhan, China
Email: xksuckx@gmail.com

Abstract: In this paper, I design a secure Internet payment system for the application based on BtoB e-commerce model, which can provide better security and reduce the cost of enterprise applications compared with the traditional Internet payment system, and fully protect the confidentiality, fairness and integrity of e-commerce payment. Thus, the system effectively provides enterprises with a higher efficiency of the transaction and has a certain value in application.

Keywords: BtoB; internet payment; security; SET

基于 BtoB 的安全网上支付系统的设计

项　慨
湖北经济学院计算机学院，武汉，中国，430205
Email: xksuckx@gmail.com

【摘要】 本文以 BtoB 电子商务模式为应用环境，设计了一种安全的网上支付系统，该系统与传统网上支付系统相比，可以提供更好的安全性并且降低企业应用的成本，同时可以充分保障电子商务支付的机密性、公平性和完整性，从而有效地为企业提供了更高的交易效率，具有一定的应用价值。

【关键词】 BtoB；网上支付；安全性；SET

1 引言

BtoB 的电子商务模式是指将发生在两个企业间的商务通过电子化的手段来实现，包括供求企业之间以及协作企业之间利用网络交换信息，传递各种票据，支付货款，从而使商务活动全过程实现电子化。传统上，企业之间的业务往来是通过传真、电话和设在各地的办事处完成，但这种模式效率低、成本高。BtoB 电子商务可以彻底改变旧的经营模式，为企业提供更低的成本、更高的效率和更多的商业机会。从协议方面来看，SET 协议虽安全性高，但协议比较复杂，费用昂贵，且不支持 BtoB 模式；SSL 协议虽然使用方便，但其安全性差。因此，本文主要以 BtoB 电子商务模式为背景，设计一个合理的、安全的电子支付系统。

2 网上支付系统概述

2.1 网上支付系统的交易原理

BtoB 安全网上支付系统主要包括 5 个实体：生产商、购买商、商业银行、认证中心、中国金融认证中心（China Finance Certificate Authority，简称 CFCA）和交易中心（即第三方信任实体，简称 TTP）。其中，生产商和购买商完成定单及账单的提交和生成；商业银行负责处理支付信息；CFCA 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和可供解决争议的证据。该系统原理图如下图 1 所示。

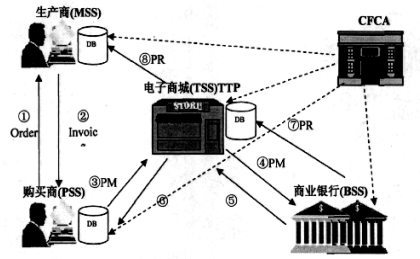

Figure1. schematic of secure online payment system
图 1. 安全网上支付系统原理图

2.2 网上支付系统的交易流程

根据网上交易过程的步骤分析，并参考了各种支

978-1-935068-12-9 © 2010 SciRes.

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）购买商向生产商下定单

购买商通过浏览器在生产商的 Web 服务器定购商品，购买商根据生产商的要求向生产商提交定单 Order，生产商根据定单形成相应的账单 Invoice，并将 Invoice 及生产商的说明及承诺 Statement 发到购买商浏览器。

2）购买商支付货款

购买商通过 TTP 的安全支付平台到银行支付货款，详细步骤如下：

①购买商将支付消息 PM（Pay message）提交到 TTP 的安全支付平台；

②TTP 安全支付平台将 PM 转发到银行；

③银行验证购买商对 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）告知 TTP 安全支付平台；

④TTP 安全支付平台将支付结果 PR 实时告知生产商。

3 网上支付系统的需求分析

为了确保上述整个系统的安全性，需要进行身份认证、数据加密和验证数字签名等手段。但验证签名和数据加密都要消耗系统资源，为了改善系统效率，有的信息可进行明文传递，而另一些敏感信息则要加密传输。下面详细分析该系统的安全需求：

3.1 订购过程的安全要求

购买商向生产商订购商品的过程中，传递的重要消息有 Order、Invoice、Statement，其安全需求如下：

1）购买商和生产商之间进行双向身份认证。

2）Order、Invoice、Statement 作为商业机密应加密。

3）Order、Invoice、Statement 需做数字签名，提供防篡改及不可否认保护。

3.2 支付过程的安全要求

支付过程中的安全要求如下：

1）向 TTP 提供解决争议的证据，其安全要求包括：

①购买商与 TTP 之间的双向身份认证。

②对 PM 进行数字签名，以防止对 PM 的非授权修改和购买商否认发出 PM。

③PM 应包括解决争议的足够信息，包括发票号 IN，账单 INV0lCE，支付指令 Pl 等。

2）TTP 与银行之间的双向身份识别。

3）银行对 PR 进行数字签名。PR 包括的信息为:发票号 IN、交易标识 Random-T、转账金额 Amount、转账结果 R 等。其中转账金额为商业机密。

4）生产商、购买商与 TTP 之间的双向身份识别。

5）生产商、购买商都能验证银行的数字签名。

4 网上支付系统的设计

4.1 系统组成与功能

整个系统由四部分组成，它们是生产商安全支付软件 MSS、购买商安全支付软件 PSS、商业银行安全支付软件 BSS、交易中心安全支付软件 TSS，四个软件模块的主要安全功能如下：

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，即与购买商之间的双向身份认证，验证购买商对定单的数字签名，生成生产商对账单和承诺的数字签名，加解密与购买商之间传递的信息。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，还记录购买商签名后的定单信息，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）PSS：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:与生产商之间的双向身份认证，产生购买商对定单的数字签名，验证生产商对账单和承诺的数字签名，加解密与生产商之间传递的信息。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:与生产商之间的双向身份认证、与购买商之间的双向身份认证、与银

行之间的双向身份认证、验证购买商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:该软件起支付网关功能，其主要作用是完成银行网络与 Internet 两者之间的通信，协议转换和进行数据加解密，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，验证购买商的数字签名，产生支付结果的数字签名，解密购买商传来的转账通知，用生产商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。

4.2 数字证书的配置

模块 PSS、MSS、TSS、BSS 均为基于 PKI 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：

MSS：配置生产商服务器证书，用于与购买商 PSS 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。

PSS：:配置购买商服务器证书，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。

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

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。

5 网上支付系统的工作流程

针对前面所述系统交易流程，在购买商、生产商、交易中心和银行分别配置了 PSS、MSS、TSS、BSS 软件及相应的数字证书后，软件之间的工作流程详细过程在下面过程描述。

5.1 描述所涉及到符号的定义

P：购买商（Purchaser）；

M：:生产商（Manufacturer）；

TTP：:交易中心（第三方信认实体）；

B：商业银行（Bank）；

Num-card：购买商在银行的账号；

Brand-card：商业银行的品牌（商标）；

0I：订货指令（order-Instruction）；

PI：支付指令（Payment-Instruction）；

DateTime-Z：在 Z 处的时间戳，其中 Z∈{P，M，TTP，B}；

Random-T：随机数，表示一次交易；

Status-Z：:表示交易目前的状态，其中 Z∈{TTP，B，OK}；

IDZ：Z 的标识，在该系统中是唯一的，其中 Z∈{P，M，TTP，B，CA}；

SKZ：Z 的私密密钥，其中 Z∈{P，M，TTP，B}；

PKZ：Z 的公开密钥，其中 Z∈{P，M，TTP，B}；

KZ：Z 的对称密钥，其中 Z∈{P，M，TTP，B}；

CertZ：Z 的证书，其中 Z∈{P，M，TTP，B}；

EN_K（Msg）：用密钥 K 对 Msg 进行加密，其中 K∈{SKz，PKz，Kz}；

DE_K（Msg）：用密钥 K 对 Msg 进行解密，其中 K∈{SKz，PKz，Kz}；

H（Msg）：用 H 对 Msg 求摘要，H 为单向 Hash 函数；

SIGN_SKZ（Msg）：用私钥 SKZ 对 Msg 进行数字签名；

Verify（CertZ）：向认证机构核实证书 CertZ。

5.2 交易各阶段工作流程及信息结构

下面具体描述各阶段工作流程及信息结构。

（1）购买商提交订单

购买商提交订单交易步骤如图 2 所示：

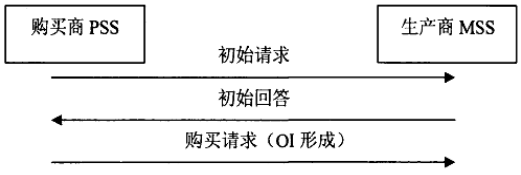

Figure 2. transaction steps of submitted order by buyers

图 2. 购买商提交订单交易步骤

①购买商在生产商的 WEB 服务器上选择好要订购的产品，并填写完其它必要信息后，点击页面上的提交接扭，此时激活 PSS 软件。PSS 软件发送一个初始请求（InitPM-Requ）给生产商的 MSS 软件，

978-1-935068-12-9 © 2010 SciRes.

InitPM-Requ 的数据结构见表 l 所示。

Table 1. data structure of InitPM-Requ
表 1. InitPM-Requ 的数据结构表

数据单元	描述
InitPM-Requ	{Message, IDP}
Message	购买商向生产商发出购买信息
IDP	购买商软件产生的本地 ID

②MSS 收到 InitPM-Requ 后，向 PSS 发送初始回答（InitPM-Resp）；InitPM-Resp 的数据结构见表 2 所示。

Table 2. data structure of InitPM-Resp
表 2. InitPM-Resp 的数据结构表

数据单元	描述
InitPM-Resp	{CertM，Resp-Msg，SIGN-SKM(H(Resp-Msg))}
CertM	生产商的数字证书
Resp-Msg	{Random-T，Message，IDM}
Random-T	标识这次交易
Message	说明已收到初始请求
IDM	生产商软件产生的本地 ID
H（Resp-Msg）	用 hash 函数对 Resp-Msg 求摘要
SIGN-SKM（）	生产商用签名私钥 SKM 对摘要签名

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

step1：Verify（CertM），若核实，则往下进行，否则终止；

step2：判断 DE-PKM（SIGN-SKM（H（Resp-Msg））是否等于 H（Resp-Msg），若相等则往下进行，否则终止。（DE-PKM 为 PSS 用生产商签名公钥验证其签名）；

step3：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（订货指令 Order-Instruction），OI 的数据结构见表 3 所示。

Table 3. data structure of OI
表 3. OI 数据结构表

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

step4：PSS 发送购买请求（Purchase-Requ）给 MSS，Purchase-Requ 的数据结构见表 4。

（2）生产商形成账单

生产商形成账单交易步骤如图 3 所示。

Table 4. data structure of Purchase-Requ
表 4. Purchase-Requ 的数据结构表

数据单元	描述
Purchase-Requ	{CertP，en-OI，OI-Envelope，SIGN-SKP（H（OI））}
CertP	购买商的数字证书
en-OI	{EN-KP（OI）}（PSS 软件随机生成对称密钥 KP，加密 OI）
OI-Envelop	{EN-PKM（KP）}（PSS 软件用生产商公开密钥加密 KP 形成数字信封）
OI	订货指令
H(OI)	用 hash 函数对 OI 求摘要
SIGN-SKP（）	购买商用签名私钥 SKP 对摘要签名

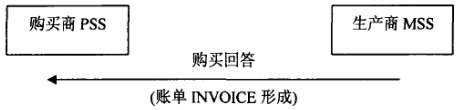

Figure 3. transaction steps of formation of billing by manufacturers
图 3. 生产商形成账单交易步骤

①MSS 收到 PSS 的购买请求（Purchase-Requ）后，做以下几步：

step1：Verify（CertP），若核实，则往下进行，否则终止；

step2：由 DE-SKP（OI-envelop）得到 KP，DE-KP（en-OI）得到 OI，再判断 DE-PKP（SIGN-SKP（H（OI））是否等于 H（OI），若相等，则往下进行，否则终止；

step3：MSS 验证签名成功后，将 OI 送到后台数据库订单处理系统，在本地取得 Datetime-M 用以标识生产商收到订货单的时间，根据货物、与交易中心通信时间等时间延迟 Delay，以及生产商的说明及承诺 Statement，形成账单 INVOICE，账单 INVOICE 的数据结构见表 5 所示。

Table 5. data structure of INVOICE
表 5. INVOICE 数据结构表

数据单元	描述
INVOICE	{message， IN， Datetime-M， Delay， Statement，Status-TTP}
Message	生产商向购买商说明订货单已收到，包含金额等敏感信息
IN	为该次交易订单的编号
Datetime-M	标识生产商收到订货单的时间
Delay	生产商根据货物与交易中心通信时间等情况设置时间延迟
Statement	生产商的承诺
Status-TTP	说明目前交易的状态是等待交易中心回答

MSS 将 INVOICE 存在本地，以备购买商收不到货物时查询（提供 IN 进行查询）。

step4：然后向 PSS 发送购买回答（Purcha-se-Resp），Purchase-ResP 的数据结构见表 6 所示。

Table 6. data structure of Purchase-Resp
表 6. Purchase-Resp 数据结构表

数据单元	描述
Purchase-Resp	{CertM， en-INVOICE， INVOICE-envelop，SIGN-SKM（H（INVOICE））}
CertM	生产商的数字证书
en-INVOICE	{EN-KM（INVOICE）}（MSS 软件随机生成对称密钥）KM 加密 INVOICE}
IN-VOICE-envelop	{EN-PKP（KM）}（MSS 软件用购买商公开密钥加密 KM 形成数字信封）
H（INVOICE）	用 hash 函数对 INVOICE 求摘要
SIGN-SKM（）	生产商用签名私钥 SKM 对摘要签名

②PSS 收到 MSS 购买回答（Purchase-Resp）后，做以下几步：

step1：Verify（CertM），若核实，则往下进行，否则终止；

step2：由 DE-SKM（INVOICE-envelop）得到 KM，从 DE-KM（en-INVOICE）得到 INVOICE，并判断签名 DE-PKM（SIGN-SKM（H（INVOICE））是否等于 H（INVOICE），若相等则往下进行，否则终止。然后把 INVOICE 连同其数字签名保存起来。

（3）购买商转账

购买商转账交易步骤如图 4 所示：

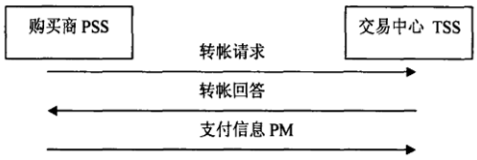

Figure 4. transaction steps of transfer by buyers
图 4. 购买商转账交易步骤

①购买商填写转账支付指令 PI，PI 的数据结构见表 7 所示。

Table 7. data structure of PI
表 7. PI 的数据结构表

数据单元	描述
PI	{Brand_card， Num_card， IDM， Amount，Random-T}
Brand_card	购买商所用支付卡品牌号
Num_card	购买商支付卡号码
IDM	从 InitPM-Resp 得到
Amount	支付金额
Random-T	从 InitPM-Resp 得到

②PSS 生成一个初始化请求 InitPT-Requ 发给 TSS，InitPT-Requ 的数据结构见表 8 所示。

Table 8. data structure of InitPT-Requ
表 8. InitPT-Requ 的数据结构表

数据单元	描述
InitPT-Requ	{Message，IDP，Random-T}
Message	向 TTP 说明购买转账支付初始请求
IDP	从 InitPM-Requ 得到
Random-T	从 InitPM-Resp 得到

③TSS 收到 InitPT-Requ 后，取出 Random-T，向 PSS 发送初始回答 InitPT-Resp，InitPT-Resp 的数据结构见表 9 所示。

Table 9. data structure of InitPT-Resp
表 9. InitPT-Resp 数据结构表

数据单元	描述
InitPT-Resp	{CertTTP， Resp-Msg， SIGN-SKTTP（H（Resp-Msg））}
CertTTP	交易中心的数字证书
Resp-Msg	{Random-T，message，IDTTP}
Random-T	从 InitPT-Requ 得到
message	说明已收到初始请求
IDTTP	TTP 产生的本地 ID
H（Resp-Msg）	用 hash 函数对 Resp-Msg 求摘要
SIGN-SKTTP（）	交易中心用签名私钥 SKM，对摘要签名

④PSS 收到初始回答（InitPT-Resp）后，做以下几步：

step1：Verify（CertTTP），若核实，则往下进行，否则终止；

step1：PSS 用 INVOICE 和 PI 生成支付信息 PM，并发给 TTP 转账请求 TransPT-Requ，PM 的数据结构见表 10 所示。

Table 10. data structure of PM
表 10. PM 数据结构表

数据单元	描述
PM	{Random-T， Brand_card， EN-PKB（IN，INVOICE，PI）}
Random-T	从 InitPT-Resp 得到
Brand_card	从 PI 得到
EN-PKB（）	购买商用其支付卡银行的加密公钥对 IN，INVOICE 和 PI 加密

TransPT-Requ 的数据结构见表 11 所示。

Table 11. data structure of TransPT-Requ
表 11. TransPT-Requ 的数据结构表

数据单元	描述
TransPT-Requ	{CertP，En-PM，PM-envelop，SIGN-SKP（H（PM））}
CertP	购买商的数字证书
En-PM	{EN-KP（PM）}（PSS 软件随机生成对称密钥 KP 加密 PM）
PM-envelop	{EN-PKTTP（KP）}（PSS 软件用交易中心公开密钥加密 KP 形成数字信封）
H（PM）	用 hash 函数对 PM 求摘要
SIGN-SKP（）	购买商对 PM 数字签名

978-1-935068-12-9 © 2010 SciRes.

（4）交易中心转发转账通知

交易中心转发转账通知步骤如图 5 所示：①TSS 收到 PSS 的转账请求 TransPT-Requ 后，做以下几步：

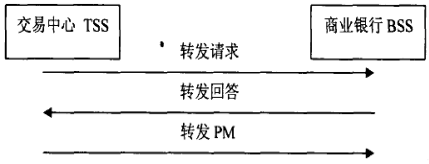

Figure 5. steps of forward transfer notification by trading center
图 5. 交易中心转发转账通知步骤

step1：Verify（CertP），若核实，则往下进行，否则终止；

step2：由 DE-SKTTP（PM-envelop）得到 KP，DE-KP（en-PM）得到 PM，再验证签名 DE-PKP（SIGN-SKP（H（PM））是否等于 H（PM），若相等，则往下进行，否则终止；TSS 将 PM 及其签名 SIGN-SKP（H（PM））作为交易证据保存在数据库中。

step3：TSS 根据 Brand-card 信息，向 BSS 发送初始请求（InitTB-Requ），InitTB-Requ 的数据结构见表 12 所示。

Table 12. data structure of InitTB-Requ
表 12. InitTB-Requ 的数据结构表

数据单元	描述
InitPT-Requ	{IDTTP，Random-T}
IDTTP	TSS 产生的本地 ID
Random-T	从 TransPT-Requ 得到

step4：BSS 收到 InitTB-Requ 后，向 TSS 发送初始回答（InitTB-Resp），InitTB-Resp 的据结构见表 13 所示。

Table 13. data structure of InitTB-Resp
表 13. InitTB-Resp 的数据结构表

数据单元	描述
InitTB-Resp	{CertB，Resp-Msg，SIGN-SKB（H（Resp-Msg））}
CertB	商业银行的数字证书
Resp-Msg	{message，IDB，Random-T}
Message	说明已收到初始请求
IDB	BBS 产生的本地 ID
Random-T	从 InitTB-Requ 得到
H（Resp-Msg）	用 hash 函数对 Resp-Msg 求摘要
SIGN-SKB（）	商业银行对 Resp-Msg 数字签名

②TSS 收到 InitTB-Resp 后，做以下几步：

step1：Verify（CertB），若核实，则往下进行，否则终止；

step2：:验证签名，EN-PKB（SIGN-SKB（H（Resp-Msg））是否等于 H（Resp-Msg），如正确，继续进行，否则中止；

step3：TSS 将转账请求 TransTB-Requ 发送给 BSS，TransTB-Requ 的数据结构见表 14 所示。

Table 14. data structure of TransTB-Requ
表 14. TransTB-Requ 的数据结构表

数据单元	描述
TransTB-Requ	{CertTTP，CertP，PM，SIGN-SKP（H（PM））}
CertTTP	交易中心的数字证书
CertP	购买商的数字证书
PM	从 TransPT-Requ 得到
SIGN-SKP（H（PM））	从 TransPT-Requ 得到

（5）商业银行处理转账通知

①BSS 收到转账请求 TransTB-Requ 后，做以下几步：

step1：Verify（CertTTP），Verify（CertP），若核实，则往下进行，否则终止；

step2：:验证购买商的数字签名，DE-PKP（SIGN-SKP（H（PM））是否等于 H（PM），则往下进行，否则终止；

step3：给 TSS 发送转账受理通知 Notes，Notes 的数据结构见表 15 所示。

Table 15. data structure of Notes
表 15. Notes 的数据结构表

数据单元	描述
Notes	{Message，Random-T，Status-B}
Message	对 PM 的有效性进行说明
Random-T	从 TransTB-Requ 得到
Status-B	表明目前交易的状态是：银行授权支付

②TSS 收到 Notes 后，向 PSS 发送此消息。

③BSS 从 PM 中用自己的私钥取出转账支付指令 PI，并将 PI 送到银行后台系统进行处理，后台系统处理完后，将支付结果 R 告知 BSS。BSS 形成支付结果信息 PR，PR 的数据结构见表 16 所示。

Table 16. data structure of PR
表 16. PR 数据结构表

数据单元	描述
PR	{Random-T，Status-B，EN-PKM（IN，Amount，R，Datetime-B）}
Random-T	从 TransTB-Requ 得到
Status-B	表明目前的状态是：银行授权支付
IN	该次交易订单的编号
Amount	表示转账金额
R	表示转账结果
Datetime-B	银行交易时间
EN-PKM（）	用生产商的公开密钥加密

④BSS 将向交易中心发送转账回答 TransTB-Resp，TransTB-Resp 的数据结构见表 17 所示。

⑤TSS 收到转账回答 TransTB-Resp 后，做以下几步：

Table 17. data structure of TransTB-Resp
表 17. TransTB-Resp 数据结构表

数据单元	描述
TransTB-Resp	{CertB，PR，SIGN-SKB（H（PR））}
CertB	商业银行的数字证书
PR	支付结果信息
H（PR）	用 hash 函数对 PR 求摘要
SIGN-SKB（）	商业银行对 PR 数字签名

step1：Verify（CertB），若核实则往下进行，否则终止；

step2：：验证银行数字签名，DE-PKB（SIGN-SKB（H（PR））是否等于 H（PR），如正确，继续进行，否则中止；

step3：TSS 将（PR，SIGN-SKB（H（PR））保存在本地，以便争议时提供证据。

⑥TSS 向生产商转发转账回答 TransTM-Resp，TransTM-Resp 的数据结构见表 18 所示。

Table 18. data structure of TransTM-Resp
表 18. TransTM-Resp 的数据结构表

数据单元	描述
TransTM-Resp	{CertTTP，Datetime-TTP，Random-T，PR，SIGN-SKB（H（PR））}
CertTTP	交易中心的数字证书
Datetime-TTP	标识交易中心对该次交易后记载的时间
Random-T	从 TransTB-Resp 得到
PR	从 TransTB-Resp 得到
SIGN-SKB（H（PR））	从 TransTB-Resp 得到

⑦MSS 收到 TransTM-Resp 后，做以下几步：

step1：Verify（CertTTP），若核实，则往下进行，否则终止；

step2：：验证商业银行对 PR 的签名 DE-PKB（SIGN-SKB（H（PR））是否等于 H（PR），若核实，则往下进行，否则终止；

step3：生产商用自己的加密私钥从 PR 中解密得到转账结果及金额，并将其送到后台处理系统；

step4：计算 Datetime-TTP 减 Datetime-M 是否大于 Delay，若大于，则向顾客发送延迟通知，说明延迟原因并表示立刻发货，将（Datetime-B，Datetime-M，IDB，IDTTP。）保存，用 status-OK 代替 status-B。

6 网上支付系统的特点

该支付系统与基于其它协议的支付系统相比较的优点如下：

1）认证体系上：SET 证书要求各实体具有信用卡，而且与证书绑定；本系统采用的 CFCA 颁发的证书只是对各实体的身份认证，与其金融信息分开。这样，在验证证书时要比验证 SET 证书耗时少。

2）SET 协议支付系统中，客户把定购和支付信息都推向商家，商家还要进行签名验证，处理完信息后，才向支付网关转发支付信息，如果在同一时间多个客户提交购买信息时，商家服务器将成为瓶颈，时间延迟较长，不利于交易的即时性；本支付系统中，利用购买者向交易中心转交支付信息，交易中心只须解密、验证签名并记录该信息，不必再作其它处理，直接打包转交银行，整个交易平稳，不会造成资源紧张而产生较多延迟。

3）SET 协议的支付系统没有记录功能，在起争议时提供的证据不充分；本系统充分考虑到 BtoB 买卖双方交易的金额较大，为了把风险降到最低限度，采用了交易中心作为中介而记录下了足以解决争议而需要的证据，解决了交易各方的后顾之优。

4）为了防止重放攻击，本系统用生产商随机数据生成 Random-T，它既可以表示一次交易，又可当作签名新鲜值，签名时必须使用时间域或新鲜值来防止重放攻击，本系统采用新鲜值 Random-T 在交易中心软件模块中设置条件，当第二次接到具有相同 Random-T 的支付信息时，拒绝处理该信息。

5）SSL 支付系统中，客户的信息先到商家，让商家阅读，这样，客户资料的安全性就得不到保证；本系统中，购买商购买商品的发票号、账单、支付指令是用银行的公开密钥 PK 加密后经交易中心转交给银行的，只有银行才能看到这些支付信息，交易中心仅起转交、记录的功能，这样，既维护了支付信息的保密性和完整性，又很好地保护了购买商的利益。

7 结束语

在已有的电子支付安全协议中，SET 协议虽安全性高，但协议比较复杂，费用昂贵，且不支持 BtoB 模式，SSL 协议虽然使用方便，但其安全性差。本文通过对各种电子支付安全协议和电子支付模型的分析

978-1-935068-12-9 © 2010 SciRes.

和研究，利用数据加密技术，设计了一个 BtoB 电子商务安全支付系统，该系统提供了通过 Internet 与第三方支付机构建立联系的安全支付方式，适用于全电子交易，各参与实体所使用的公钥是由中国金融认证中心（CFCA）签发的证，可以充分保障电子商务支付的机密性、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电子支付的不可否认性，而且，本系统对交易过程也做了状态描述，能使购买商和生产商对交易的状态能较好地把握。本系统在实际应用中可以支持中国借记卡、账户存折、电子支票等支付工具的应用，具有一定的应用推广性。

References (参考文献)

[1] LIN Song, LI Zhou-jun1, ZHANG Fan. Internet payment security architecture based on service-oriented architecture. Computer Integrated Manufacturing Systems, 2008, (12): 2468-2475.
林松，李舟军，张帆. 基于面向服务架构的网上支付安全体系研究与实现[J]. 计算机集成制造系统，2008，（12）：2468-2475.

[2] XUN Da-yong. Internet Payment System in Electronic Commerce Based on SSL and SET Protocols. Communications Technology, 2009, (04): 156-158.
寻大勇. 基于 SSL 与 SET 协议的电子商务支付系统[J].通信技术，2009，（4）：156-158.

[3] HUANG Jing-tao. Design and implementation of Internet Payment System for bank. University of Electronic Science and Technology, 2009.
黄敬涛.银行网上支付系统的设计与实现[D].电子科技大学，2009.

[4] ZHANG Ruo-yan, LIU Xiao-xia, ZHANG Hong. Formal model establishment and security analysis for SET protocol. Computer Applications and Software, 2009, (05): 81-84.
张若岩，刘晓霞，张宏. SET 协议形式化模型的建立和安全性分析[J].计算机应用与软件，2009，（05）：81-84.

[5] CHEN Qin-feng, BAI Shuo. Analysis of the problem and solution in SET protocol. Chinese Journal of Computers, 2005, (04): 202-209.
陈庆锋，白硕.SET 协议中问题的分析及解决方案[J].计算机学报，2005，（04）：202-209.

[6] YUAN Ling. Analysis of E-payment system. Application Research of Computers, 2004, (05): 56-66
袁凌.网上电子支付系统分析[J].计算机应用研究，2004，（05）：56-66.