ELECTRONIC

# 电子商务实用全书

COMMERCE

3

姜旭平/主 编

印刷工业出版社

e 世纪

# 电子商务实用全书

## Practical Encylopedia of Electronic Commerce

姜旭平 主编



## 第三卷

印刷工业出版社

# 目录

第三卷

## 应用篇(续)

### 电子商务的应用状况

## 第11章 电子支付和结算体系

# 运行环境篇

## 电子商务的运行环境

## 第 12 章 供应链与物流配送系统

## 第 13 章 电子商务的法律和政策环境

# 营销篇

## 网络营销理论与实践

### 第 14 章　网络环境下的营销策略



### 第 15 章　基于网络环境的营销技术

## 第16章 市场营销资源

# 第 11 章

# 电子支付和结算体系

## ☞ 本章指南

**11.1 电子资金汇兑系统(FIT)**

本节主要向你介绍电子支付系统以及几种常见的电子支付工具及相关技术。

**11.2 金融结算和清算体系**

了解我国资金清算系统和银行间清分结算的电子化系统及其管理组织。

**11.3 招商银行、中国银行、建设银行的网络系统及电子货币系统**

Internet 的发展给金融业带来了便利。网上银行系统和电子货币也将给你个人带来更大的便利。

**重点解析**

本章重点:

1)了解电子资金支付系统和支付工具;

2)掌握银行间清分结算的电子化系统;

3)了解网上银行系统和电子货币。

# 11.1 电子资金汇兑系统(EFT)

## 11.1.1 Internet 电子支付系统

Internet 电子支付系统英文名即 EPS(Electronic Payment System)。

货币、现金支票、商品券等传统支付方法在计算机内部无法使用。为了能够在 Internet 上进行支付,特别是能够通过 WWW 进行支付,人们正在致力实现新的电子支付系统。

### 1.支付系统简介

无论是数字方式还是其他方式,支付系统都可分为两大类,即借方(Debit)和贷方(Credit)。借方指使现金,货方指进行信贷。在现金系统中,首先要把现金调拨进去,然后才可以从这里花钱。而在信贷系统中,可以先买东西然后再要求付款。例如使用黄金、纸币、旅行支票支付的便是现金系统。也有通过 ATM(自动提款机)使用现金卡进行支付的。而使用支票、赊账、信用卡等,则是信贷(信用)系统。

就像现金和信用卡在现代商业环境中并存一样,它们也将在数字世界中并存。所谓数字现金就是支票和无记名债券(由银行及其他机关发行)的数字版。用户从银行购入这些票据(银行把它们作为借方系统运用),然后可以把它们变换为实物。用户也可以把这些票据进行数字式复制,但银行只对票据的每一个编号兑换一次现金。

数字式信用和商业领域使用的信用系统类似。主要的差别在于采用数字时间戳和数字签名。通过这些,赋予系统以监督和责任的功能,以取代文件类的处理(这在数字世界中并不存在)。

支付人通过这样系统生成包含有交易的内容、支付人和收取人的名字、交易日期以及应付的金额等内容的凭证(表示交易的传票和证据等)的记录。支付人使用自己个人键码对这样凭证进行签署。凭证的收取人用公开的键码便可读这一记录,并对其进行签署,这样便可确认个人键码所有者所承担的支付义务。然而,收取人向清算系统提出该凭证,便可取得用以收款的法律根据。

### 2.电子支付系统的社会基础

现已存在电子支付系统的社会基础。主要信用卡公司(如 American Express, Master Card, Visa, Discover),ATM 网络以及 ACH(自动清算中心)便是这样基础。对信用卡业务来说,有三种处理系统。一是银行,它给顾客以信用卡并进行请求。二是第三方的处理公司,它向信用卡加盟店提供认证和收款业务。三是像 Visa 这样的国际网络,它把进行收款的处理业

者和银行联系在一起。这些系统虽很复杂但已完善,几乎可向所有场所普及。加盟店支付的手续费为交易总金额的2%～3%,另外每笔交易再加收20美分。

一些信用卡公司已向加盟店提供使用Internet的服务,信用卡系统已真正具有国际性,它已能应于用各种各样通货进行的交易。这些都能很好地纳入银行系统中。Internet的巨大优点已经表现在信用卡系统中。

所谓ACH是美国银行之间的一种机构,通过它,地方银行向数据库提出支付,第二天之前联邦贮备局便得以拨款。这是一种通过户头转拨的收费支付方式。ACH交易收费低廉(每笔不到15美分,而且能用计算机进行处理。ACH只能在美国银行户头间工作,但这种方法被广泛用于在线的支付清算业务。

通过现金卡网络,既可用ATM从自己的户头上取出现金,又可作为支付拨到别的银行去。银行要求这种业务每笔支付50美分。银行在进行支付前既要求有实物的卡又要求有密码(也叫PIN)。现在安全性上还存在问题,解决了以后便可利用网络进行直接的在线支付。

个人和民营企业将保持自己的顾客户头,不妨碍从这些户头进行支付。几乎所有的在线服务都可用这种方法向提供服务内容的公司进行支付。如果这些在线服务机构提供对使用者户头的服务器,这种系统也许就能承担重要的银行业务。

### 3.电子支付系统的种类

(1)电子信用卡。

电子信用卡包括具备信用循环业务的信用卡(如Visa和Master)及不具备信用循环业务的美国运通卡和花旗卡两种,统称为信用卡。

以信用卡为基础的电子支付系统,一般消费者在网页上购物时只需将信用卡资料通过因特网传送至特约商店,商店再将数据集成传至信用卡取款银行,就可依原有的信用卡结算系统完成付款。付款机制仍以SET协议为主,是全球电子商务的共同付款机制。采用SET协议的付款方式,可防止数据在网络传输中被劫取、窃听、篡改;可确认交易人的身份,防止日后否认交易;还可保护卡内资料不为商家所知,这一点比在传统商店使用信用卡安全。

(2)电子货币。

目前电子货币仍停留在专有系统(Proprietary System)阶段,还没有一个共同遵循的公开机制。

在电子货币(又称数字化货币)的基本模式中,消费者首先把标准的货币(例如钞票)交给他的电子银行,兑换成等值的电子化货币。这些电子化货币是以二进制文件的方式返回给消费者的,其内容代表了货币的数量。当消费者要向销售商付款时,他把相应数量的这些"钞票"传递给销售商;然后销售商把这些"钞票"传递给电子银行,兑换成真正的货币。

后来开发的隐秘的钞票模型(Blinded Token Model)的目的就是要保护付款者的匿名权。它不是由电子银行发行电子钞票交用户使用,而是由付款者拥有一个软件,这个软件可以创建数字化钞票。每个数字化钞票有一个序列号,在使用前必须传送到电子银行,以获得授权。在

提交给电子银行前,付款者的软件把序列号隐藏起来,它把序列号乘以一个随机数。因此,电子银行可以为数字化货币进行授权,加上银行的数字签名,但却不知道提交钞票者是谁。在付款者使用这个数字化钞票前,该软件再删除用于隐藏序列号的随机数,收款者及其银行可以看到原来的序列号,当这样一个电子钞票用于支付时,收款者及其银行可以验证钞票上的数字签名是否的确是由一家有权的电子银行发出的。

电子货币的另一问题是如何保证消费者对一个电子钞票只使用一次。消费者的身份标识在交易时与银行授权同时在联机系统中出现,可以防范对数字化钞票的复制或非法多次使用。

电子货币的主要优势在于在 Internet 上的小额付款市场,以小额电子货币支付网上小额的消费。如购买 Internet 上的一篇文章,一首音乐或图片等。据 Jupiter Communications 的估计,基于访问的服务,如即时新闻、软件租用、网上游戏,甚至 Internet 电话的使用等小额付款市场到 2000 年,规模可达几亿美元。

(3)电子支票。

在 1994 年,美国支票的清算量是 570 亿张,而信用卡交易的数量只达到 92 亿次,从习惯上人们仍通过开立支票来清偿债务,这样使用电子资金转账(ETT)的系统开始出现。

电子支票与一般支票的不同是以 Internet 作支票的传递,与电子货币一样属专有系统,没有统一公开的付款机制可循。一般,收、发支票双方都需在银行开有账户,让支票交换后的票款能直接在账户间转移,而付款系统则提供身份认证、数字签名等,以弥补无法面对面的交换。

电子支票的特点主要在于介入企业与企业间的电子商务市场。在线的电子支票可在收到支票时即验证发票者的签名、资金状况,避免了收到传统手签支票时发生的无效或空头支票的现象。电子支票的遗失也可办理挂失止付。

(4)智能卡。

智能卡应用较广,一般分为存贮智能卡和金融智能卡两种,可具有身份证、保健卡、金融卡、会员卡等集于一身的多种功能。Internet 电子商务所推动的电子钱包,则属于金融智能卡范畴。目前智能卡应用仍以金融支付所占的比例较大。

智能卡以半导体技术来保存用户资料,具有安全的存贮功能、便于携带、不限于在 PC 上使用等优点。但智能卡需配备读卡机,以目前 PC 为主要的上网设备而言,读卡机尚需一段时间才能成为标准外设配备,但从长期看基于非 PC 的上网设备(能读卡的 NC、顶置盒、WebTV 等)仍有很大增长空间(市场占有率至 2001 年约 34%),智能卡仍是极具潜力的付款工具。

**4.采用客户/服务器方式**

在线的支付处理通常同三方面有关。顾客进行支付,加盟店接受支付,银行进行会计处理并确认从顾客那里把款拨到加盟店户头上。在对等通信系统中,用户起到顾客和加盟店两方面的作用。支付服务系统虽然从法律上说不能视为和银行一样,但它可起银行那样的作用。

顾客将运行客户机软件。有的是像 Mosaic 那样的 WWW 浏览器,有的是带有 Netscape 和 S-HTTP(安全超文本传输协议)的 Mosaic 那样的有密码化功能的浏览器。也许还有使用

专门的支付客户机。

加盟店为了支付请求和处理,要在服务器上运行加盟店软件。在许多情况下,加盟店软件同 WWW 服务器相结合。支付服务器在网络上是银行 POP(存在点)。在进行实时交易时,加盟店把信息送到支付服务器,在这里对支付进行认证然后往加盟店户头进行拨款。

**5.安全性和私人秘密保护是必须解决的问题**

安全性在所有数字支付机构中都是非常重要的问题。用以证明确是用户本身最一般的方法是要求密码。由于消息在 Internet 上传送时很容易被读走,所以几乎在商用服务中在发送密码前都进行了加密。采用新一代 WWW 浏览器进行这种加密。作为这种浏览器有使用 SSL(安全插接层)加密协议的 Netscape 和 Mosaic 派生品(使用 S-HTTP)的。

问题在于加密的密码重复使用两次以上也不安全。最后,也许用户只能使用硬件标志的方法。这就是在普通信用卡的大小上,作成唯一一次的密码,并使其加密以保持安全。

为了确保安全,金融消息的内容(支付、信用卡号码或数字署名)都要保密,此外还要使消息不被篡改。在现在正在使用的几乎所有系统上,都保持有用以检查监督交易的某种凭证文件。为了发展在线支付系统,必须有能和这种文件相匹敌的功能。能进行加密的现有机构,能提供这种功能。

保守私人秘密也是同安全性有关的问题。在当今庞大数据库时代,许多人都在想这一问题,大家都同意在数字金融交易中应和现金交易中一样,采取匿名原则。任何人在使用现金时,无关的人都不应该知道。使用现有的数字加密技术便可达到这一目标,但已经使用这一技术的只有一部分电子支付系统。

## 11.1.2 电子支付工具

它是现代商品经济高度发展要求资金快速通信的产物,利用现代科学技术特别是计算机技术而实现。电子支付工具用计算机系统记录和处理,它使得各种票据和贵金属在整个货币供应量中的比重愈来愈小。这种通过银行的电子存款系统和各种电子清算系统记录和转换资金,比动用各种贵金属和凭证货币来完成大规模的交换,更节约、方便、安全。目前,电子支付工具和人们的生活密切相关,银行的存款、贷款、汇款等柜台服务大都借助于计算机系统实现。代发工资、代收费、储藏通存通兑、银行卡、电子支票、电话银行等多种银行业务就是电子支付工具的各种表现形式。

电子支付工具作为现代金融业务和现代科技相结合的产物,它具有下列特征:

(1)以往货币的存在方式是单一的物质材料,而电子支付工具因不同的处理媒体而不断变化着存在方式,在计算机存储设备上是磁介质,在计算机网络中传播是是电磁波或光波,在 CPU 处理器中是电脉冲等。

(2)电子支付工具的流通以相关的设备正常运行为前提,新的技术和设备也引发了电子支

付工具新的业务形式的出现。

(3)电子支付工具比其他类型的货币在流通中具有更高的安全性和可靠性,它的安全性是通过用户密码、软硬件加解密系统以及路由器等网络设备的安全保护功能来实现的。

电子支付工具改变了银行传统的手工记账、手工算账、邮寄凭证等操作方式,各种银行卡和 IC 卡的发展,给百姓生活带来很多便利。人们在购物、饮食、旅游和娱乐时用各种卡代替支票和现金来支付,只要将卡插入终端设备,再输入一定的密码和信息,就可实现付费。电子支付工具的广泛应用要借助于以下设备和计算机系统:

(1)自动柜员机(ATM)。客户可在银行营业网点、大商场、宾馆等场所的 ATM 上进行存款、取款、转账、查询,ATM 不受银行工作日的限制,客户可得到一周 7 天、每天 24 小时的 ATM 服务。

(2)售货点终端(POS)。银行在饭店、商场等消费场所设置 POS 机,客户在消费时凭银行卡在 POS 机上进行支付。

(3)电话和客户终端。客户通过电话银行、客户终端同银行进行金融交易,如查询账户信息,办理部分转账、证券买卖等。

(4)网上银行。客户通过接入因特网(Internet)的计算机,利用银行提供的网上银行服务进行查询和转账支付。

(5)电子支付工具的广泛应用离不开银行支付清算系统,目前我国几个大的国有商业银行的电子联行系统已经基本建成,而作为中央银行的人民银行与几大商业银行之间的支付清算系统正在建设之中。

银行采用计算机等技术进行电子支付的方式可分为如下 5 种,分别代表着电子支付工具发展的不同阶段。

第一阶段是银行利用计算机处理银行之间的货币汇划业务,办理汇划结算;

第二阶段是银行计算机与其他机构计算机之间资金的汇划,如代发工资等业务;

第三阶段是利用网络终端向客户提供各项银行服务,如客户在自动柜员机(ATM)上进行取、存款操作等;

第四阶段是利用银行销售点终端(POS)向客户提供自动的扣款服务,这是现在阶段电子支付工具的主要方式;

第五阶段是最新发展阶段,电子货币可随时随地通过公共网络(如 Internet)进行直接转账结算,形成电子商务环境。这是正在发展的形式,也将是下一世纪的主要金融支付方式。

如今各种新兴电子支付工具不断出现,以下介绍几种比较成熟的网上支付工具:

### 1.电子支票(E-check)

FSTC(金融服务技术联盟)由美国各大银行和技术公司构成,致力于评估和演示电子支票的可行性。

电子支票针对银行一般的活期账号而提出,它们被设计成相当于 10 美元支付能力或更

多。在很多方面,一张电子支票就像一张真的纸钞票,但其优越性在于电子支票将使用现存的SET协议,与现存的支票清算,结算以及记录保存设施有机结合。

电子支票系统抛开了纸面支票,最大限度地利用了当前银行系统的自动化潜力。例如,通过银行专用网络系统进行一定范围内普通费用的支付;通过跨省市的电子汇兑、清算,实现全国范围的资金传输;世界各地银行之间的资金传输。

电子支票方式的付款可以脱离现金和纸张进行。电子支票传输系统目前一般是专用网络系统,国际金融机构通过自己的专用网络、设备、软件及一套完整的用户识别、标准报文、数据验证等规范化协议完成数据传输,从而控制安全性。这种方式已经较为完善,现在发展的主要问题是扩充到IP网络Web方式操作。今后将逐步过渡到因特网络上进行传输。

**2.电子现金(E-cash)**

E-cash基于预付存储金,作用相当于用户对保存于发卡行的基金的支取凭证。可以经过因特网传递和交换,可以设计成美分和10美元的面额。每笔E-cash的交易由发卡行和使用者签名。它与普通现金有很多相同的特征;交易可以是私下的,有丢失金额的可能性,任何场合均可被接受,交易为个人到个人。E-cash成为现实的首先条件是必须建立一个全新的基础设施去支持币值的管理、确证、清算和记录保管。

电子现金是以数字化形式存在的现金货币,其发行方式包括存储性质的预付卡(电子钱包)和纯电子系统形式的用户号码数据文件等形式。电子现金的主要优点是它可以提高效率,方便用户使用。电子现金具有不可跟踪性,不需要连接银行网络就可以使用。从技术上讲,各个商家都可以发行电子现金,如果不加以控制,电子商务将不可能正常发展,甚至由此带来相当严重的经济金融问题。电子现金的安全使用也是一个重要的问题,包括限于合法人使用、避免重复使用等。对于无国家界限的电子商务应用来说,电子现金还存在税收和法律、外汇汇率的不稳定性、货币供应的干扰和金融危机可能性等潜在问题。有必要制定严格的经济金融管理制度,保证电子货币的正常运作。

电子现金支付有其特殊性,目前已经有三种实用系统开始使用。例如:

(1)DigiCash(http://www.digicash.com):无条件匿名电子现金支付系统。主要特点是通过数字记录现金,集中控制和管理现金,是一种足够安全的电子交易系统。

(2)Netcash(http://www.isi.edu):可记录的匿名电子现金支付系统。主要特点是设置分级货币服务器来验证和管理电子现金,其中电子交易的安全性得到保证。

(3)Modex(http://www.modex.com):欧洲使用的、以智能卡为电子钱包的电子现金系统。可以应用于多种用途,具有信息存储、电子钱包、安全密码锁等功能,可保证安全可靠。

**3.电子借记卡(E-debit)**

E-debit的作用相当于银行常规活期账户,经常账号的支取凭证。资金可用性的在线验证,包括使用PIN(个人身份识别号码),就像基于ATM的交易一样。E-debit使用类似SET

的基础设施和交易流。E－debit 可以用于从 1 美元到 50 美元小额交易。

4. **微额账单**(Micro－billing)

假如你想进行一笔几分钱的在线交易：比如浏览在线杂志，进行在线研究、投资等，一般付费标准为一页几分。Micro－billing 就是专为此而设计的。Micro－billing 的在线处理需要商户的介入，由 ISP 或者电话公司进行支持以进行账单数据的收集与发放。

## 11.1.3 几个典型的电子支付协议

### 1. SET 协议

安全电子交易(SET)协议是由两大信用卡商 Visa 和 MasterCard 联合制定的实现网上信用卡交易的模型和规范。从概念上，它是通用信用卡的自然延拓。保留了信用卡交易的一切特点，同时针对网上交易，制定了确保安全的一系列规范和协议。SET 得到了美国 IT 企业的支持，如 GTE，IBM，Microsoft，Netscape，RSA，SAIC，Terias 和 VeriSign。

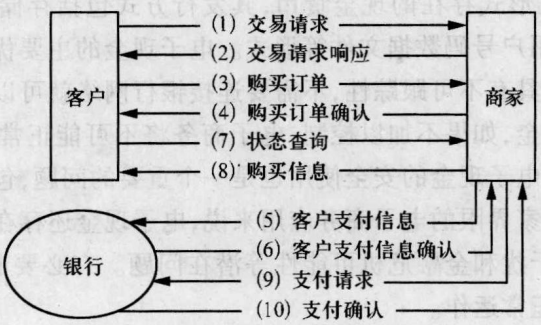


**图 11.1.1 SET 协议流程**

图 11.1.1 中，消息 1，消息 2 是交易初始设置，客户与商家相互交换身份证书，建立一个交易 ID 号。在消息 3 的客户购买消息中，包含商品或服务名，客户签名，加密的客户信用卡信息。消息 4 是商家对用户购买订单的确认。消息 5，6 是商家对客户支付信息合法性的验证，在商家与银行(或其代理)间进行。消息 7，8 使用户对交易内容、状态有查询的能力。消息 9，10 是商家与银行间的兑现和平账过程。

SET 中的信任关系为分层树状结构，低层的证书都包含高一级证书中心的签名。同所有的 CA 一样，SET 证书层次中存在一个最高层的认证中心(根)，对它的信任是无条件的。

### 2. NetBill 协议

NetBill 协议是由卡耐基－梅隆大学开发的一个网络支付协议。NetBill 支付协议包括八个主要步骤，如图 11.1.2 所示。在此之前，客户与商家相互交换公钥证书彼此验证身份，随即建立一个对称密钥用于以下的交易步骤。

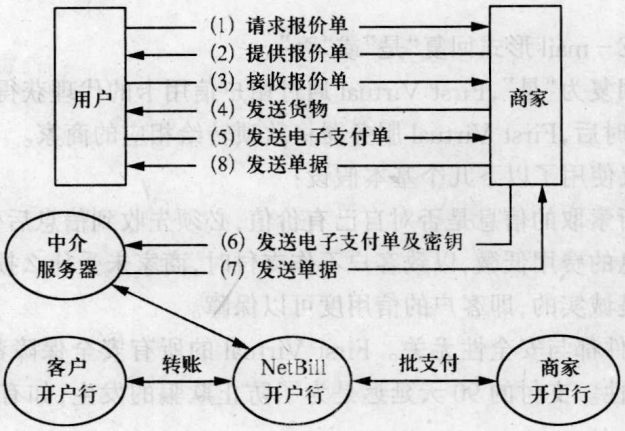


图 11.1.2 NetBill 协议流程

步骤(1)中的报价单申请基于用户身份信息，这样使商家可以根据不同的用户确定单价、折扣或预定服务等。如果报价单被客户接收((2),(3)步)，商家在步骤(4)中把客户需要的信息加密传送给客户，但其解密密钥并未同时发给客户。客户收到商家在步骤(4)的发送信息后，按规定格式生成电子支付单(EPO)，其中包括交易的描述、收到信息的校验值等。这个单据由用户私钥签押，在步骤(5)发送给商家。商家收到步骤(5)中的电子支付单后，依次作以下操作：①验证 EPO 的内容准确。②附加客户信息的解密密钥于 EPO 之后，对整个单据用数字签押。③发送签押的单据给 NetBill 服务器(步骤(6))。

NetBill 服务器在用户开户行验证客户账目及额度，若足够，合法交易，完成转账过程。从客户账目扣除交易金额，相应地增加在商家账户。随后在步骤(7)签押一份收据，包括客户所要信息的解密密钥。最后一步中，客户从商家得到信息的解密密钥，从而获得所购的信息，交易完成。

NetBill 协议的特点是：客户在收到货物后才付款，而同时商家可以保证客户有足够的款项用于支付，否则交易中止，客户得不到所需的解密密钥。

### 3. First Virtual 协议

First Virtual 协议是美国 First Virtual 公司提出的支付协议，它也是用于网上信息卡的安全交易协议。它与其他协议不同，采用了非密码学的方法来解决安全性问题。

客户先在 First Virtual 建立一个 ID 号,并把自己的信用卡号注册。当需要支付信息费用时,其支付过程如下:

(1)客户把在 First Virtual 的 ID 号发给商家。

(2)商家联结 First Virtual 服务器验证 ID 号的合法性。如果合法,商家把客户所需的信息直接发送给客户。

(3)First Virtual 服务器向客户以 E-mail 形式发送询问信息,征询客户是否愿意为其付费。

(4)客户同样以 E-mail 形式回复"是"或"否"。

(5)如果客户的回复为"是",First Virtual 通过用户信用卡的代理获得相应的款项。

(6)在 90 天的延时后,First Virtual 服务器将款项转给相应的商家。

First Virtual 协议使用了以下几个基本假设:

(1)客户不知道所索取的信息是否对自己有价值,必须先收到信息后作出支付判断。

(2)电子发送信息的费用低微,以致客户不作支付时,商家未受什么损失。

(3)多数的客户是诚实的,即客户的信用度可以保障。

可以看到这些条件都与安全性无关。First Virtual 的所有安全保障都基于 E-mail 通信体系的安全性和完整性。支付的 90 天延迟是为了防止欺骗的发生,如有这样的情况,客户的款项将被返还。

**4. iKP 协议**

iKP(i-Key-Protocol,i=1,2,3)是一族安全电子支付协议。该族协议与现有的商业模型和支付系统基础设施相匹配。协议中涉及到三个成员,即顾客(进行支付的人),商人(接收支付的人)和门关(充当电子世界和已有的支付基础设施之间的门关,并且用来认证使用已有的基础设施所进行的传输)。所有的 iKP 协议都基于公钥密码学,但它们随着拥有自己的公钥对的成员的数目而变化,分别称为 1KP 协议,2KP 协议和 3KP 协议,其安全性和复杂性递增。

1KP 协议是最简单的协议,它只要求门关拥有一对公私钥。顾客和商人只需拥有门关的认证了的公钥或经一个权威机构认证了的门关公钥(该机构通过签名证书来使门关的公钥合法化)。这就涉及到了 CA 基础设施。顾客通过他们的信用卡号和可能的相关的秘密 PIN 来认证。支付是通过交换用门关的公钥加了密的信用卡号和 PIN 以及限定的相关信息(诸如交易量,ID 号等)来认证的。1KP 协议不能对顾客和商人发送的消息提供非否认性,这就意味着不容易解决支付订购的争端。

2KP 协议要求门关和商人都拥有公钥对和公钥证书。协议对来自商人发送的消息能提供非否认性。该协议能使顾客无需和任何在线第三方联系就能通过检测他们的证书来验证他们正在和真实的商人进行交易。与 1KP 协议一样,支付订购是通过顾客的信用卡号和 PIN 来认证的(在传输之前要求加密)。