第 章 即付型网络支付方式

教学目标

通过本章学习,了解即付型 网络支付方式的特点,掌握并区分各类即付型网络支付方式的内容,熟悉使用银行卡和电子支票完成网络支付的方法,了解电子汇兑系统。

教学要求

知识要点	能力要求	相关知识
即付型网络支付 方式的特点	特点的列举和阐述	(1) 计算机网络安全基础 (2) 一般的电子商务模式 (3) 电子支付相关法规和标准
基于转账的网络支付方式	(1) 电子转账支付系统概述 (2) 即付转账清偿支付 (3) 账户划转的支付方式	(1) 各类存款账户银行卡账户 (2) ATM 和 POS 机的应用 (3) 网络银行的概念
基于银行卡的网络支付方式	(1) 基于 SSL 协议机制的银行卡网络支付方式 (2) 基于 SET 协议机制的银行卡网络支付方式 (3) 借助第三方代理机构的银行卡支付方式 (4) 银行卡网络支付实例	(1) 相关网络安全与保密技术 (2) 支付网关的作用 (3) 第三方代理
电子支票网络支付方式	(1) 同行电子支票网络支付方式(2) 异行电子支票网络支付方式(3) 电子支票支付的安全性要求(4) 电子支票网络支付的特点(5) 电子支票支付系统实例	(1) 传统支票支付模式 (2) 数字签名等网络安全技术
电子汇兑系统	(1) 电子汇兑系统简介 (2) 电子汇兑系统的特点和类型 (3) 电子汇兑系统的运作模式 (4) 电子汇兑系统的实例	(1) 汇出行与汇入行(解汇行)(2) 通信系统(3) 风险管理的概念

即付型网络支付方式 第 4 章



中国移动的网上充值缴费

2007 年 11 月 13 日,中国移动广东公司开通了网上充值缴费功能。该功能是中国移动广东公司与广州银联网络支付公司合作的一项便民服务,旨在为广大客户提供更为便捷、24 小时在线的电子充值服务。广东省全球通、动感地带和神州行用户均可使用已具备网络支付功能的银行卡为自己的手机或亲友的手机进行话费的充值。充值缴费后,话费将马上到账,安全、快捷,足不出户也可以缴纳手机话费。

目前,支持网站充值缴费的银行有中国工商银行、中国建设银行、招商银行、中国银行、广东发展银行、中国邮政储蓄银行、广州市商业银行、广州农村信用合作社、顺德农村信用合作社、南海市农村信用合作社联合社、中国民生银行、中国农业银行、兴业银行、中国光大银行。

这种便捷的充值方式吸引了大量的用户通过网站进行手机充值。

具体的操作步骤如下: ①输入充值手机号码; ②选择充值金额; ③选择支付方式; ④跳转到广东银联网站(网付通)进行支付; ③跳转到相应的银行页面进行支付的相关操作, 最终完成手机话费的充值。

资料来源: 广东移动网站. http://www.gd.chinamobile.com.

问题:

- 1. 导入案例可以看出即付型网络支付方式的哪些特点?
- 2. 通过导入案例思考账户划转和银行卡网络支付的区别和联系。

在导入案例的支付过程中,充值的金额从用户的银行卡账户上即时转账到商家的账户上,因此这种支付方式也叫即付型网络支付方式。具体来说,是指购买商品或者服务时客户的支付金额从银行账户即时转账到商家完成支付。通过对分析案例问题的思考,相信读者对"即付型"的支付方式有了直观的认识。结合网络支付的特点和方式,本章将详细介绍即付型网络支付方式的特点和内容。

4.1 即付型网络支付方式的特点

即付型网络支付方式是指购买商品或者服务时客户的支付金额从银行账户即时转账商家完成支付。其有如下几个特点。

- (1) 网络安全要求高。网络安全问题无疑是人们进行网上交易最为关注的事情。在即付型网络支付方式中,银行账户起到关键的作用。消费者的个人信息存储在银行,如果银行的网络遭到攻击,私人信息可能会泄露,若补救不及时,很可能给消费者造成巨大损失。
- (2) 交易过程中银行的参与。银行的参与部分解决了交易双方的信任问题,同时有效规避了网络支付中税收和洗钱的问题。但是对于网上 B2C 型的商品购买,由于其支付属于小额支付的范畴,利润空间不大,但支付过程和操作复杂,银行投入大,却无利可图。
- (3) 用户接受性强。即付型的支付方式,符合传统的支付结算习惯,使用户容易适应, 从而不会产生抵制。但同时又明显有别于传统的面对面支付,所以还是需要在观念和实践 上加强引导。

- (4) 有效减少在途资金。站在银行的立场考虑,这种在途资金的减少,会使从事网络支付的开户行的存款资金的金额直接受影响。
- (5) 适应各种市场和各种额度的支付。即付型网络支付较好地支持了企业与企业之间、 企业与政府部门之间、企业与消费者之间的电子商务支付。
- (6) 公平性强。在预付型网络支付中,消费者承担了一定的风险,如电子现金或智能卡金额过期、作废等,同时商家等钱到账后再发货,就没有便捷的时间优势,容易失掉信誉。在后付型网络支付中,如果有银行作为信用担保的话,则其资金有可能因为客户的失信而遭受损失的风险;如果没有信用担保机构参与,则商家承担了大部分的收不到钱的风险,因为商家很难知道购买者的身份信息,是否存在欺诈;而即付型网络支付可以有效避免上述问题,实现在商品交易过程中对交易参与方的公平性。
- (7) 支付的完成与否与客户的开户账户里的资金有关。从某种角度上来说,即付型网络支付方式都与客户在其开户行的银行账号紧密相关,其完成电子商务的支付金额都会立即从其银行账户里转出,如果其账户里没有钱或者账户里的钱少于需要支付的金额,此次支付即告失败。因此可以说即付型网络支付方式实质上是依赖于客户的账户,是基于转账的网络支付方式。

4.2 基于转账的网络支付方式

4.2.1 电子转账支付系统概述

电子转账支付系统是通过对账户的处理来完成支付的,包括存款人主动发出付款指令,将款项从自己的账户转到收款人的账户中的付款人启动支付和收款人主动发出请求付款的指令,经付款人确认后将款项从付款人账户转到自己的账户中的收款人启动支付两种类型。 其实质是存款在账户间的移动。常见的电子转账支付系统有如下几种。

1. 储蓄卡支付系统

消费者持储蓄卡可在 ATM 上自动存取现金,也可在 POS 上直接支付货款。其实际上是通过消费者自行发出的电子化转账指令,将储蓄上对应存款账户的存款提现或转入商家的存款账户中了。这是一种付款人启动支付的模式。

2. 网络银行提供的电子转账服务系统

将传统的银行业务搬上 Internet,即实现银行业务的电子化和网络化,网络银行就诞生了。网络银行利用 Internet 把业务终端伸入千家万户的家中,赢得了更为广泛的客户,同时人们也享用到了更为便捷多样的服务。网络银行提供的电子转账服务采用的也是顾客在 Internet 上直接对银行发出转账指令,然后使存款移动到指定账户中的结算方法,也是一种付款人启动支付的模式。

3. 电子支票支付系统

电子支票支付系统提供发出支票、处理支票的网上服务,是纸质支票的电子化延伸。

即付型网络支付方式 第 4 章

付款人向收款人发出电子支票以支付货款,收款人用此电子支票向银行背书以启动支付, 经认证的合法电子支票在支付过程中就作为将存款从付款人账户转入收款人账户的确认依据。这是一种付款人启动支付的模式。

大量的电子支票还可以经票据交换所进行清偿,即通过票据交换组织,互相抵消各自 应收应付的票据金额,然后只进行最终相差金额的转账。由于整个过程的自动化程度很高, 即使交易额很少,这种方式也是经济划算的。

4.2.2 即付转账清偿债务

例如,参与主体为销售商品的商家和购买商品的消费者,他们所选择的市场行为是销售和购买型的商务活动,如果市场环境为商场,而采用的支付活动方式为 POS 转账,则支付的特点就是即时清偿债权债务的转账支付活动方式,如图 4.1 所示。

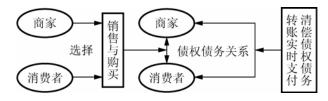
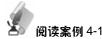


图 4.1 转账支付清偿债务示意图

在淘宝上为完成 B2C、 C2C 交易所使用的支付宝,作为一种第三方支付工具,起到了帮助商家和消费者之间完成即付转账的作用。



安全快速的支付宝

支付宝(中国)网络技术有限公司是国内领先的独立第三方支付平台,由阿里巴巴集团创办。支付宝提出的建立信任、化繁为简、以技术的创新带动信用体系完善的理念,深得人心。2009 年 7 月,支付宝用户数突破 2 亿大关,跃居全球第一位。支付宝已经进入全球几十个国家,日交易数达 400 多万笔,可以使用 12 种货币进行结算,日交易额逼近 8 亿元人民币。目前除淘宝网和阿里巴巴外,支持使用支付宝交易服务的商家已经超过 33 万家,涵盖了虚拟游戏、数码通信、商业服务、机票等行业。这些商家在享受支付宝服务的同时,更是拥有了一个极具潜力的消费市场。

目前国内工商银行、农业银行、建设银行、招商银行、上海浦发银行等各大商业银行以及中国邮政、 VISA 国际组织等各大机构均和支付宝建立了深入的战略合作,不断根据客户需求推出创新产品,成为金 融机构在电子支付领域最为信任的合作伙伴。

支付宝交易是互联网发展过程的中一个创举,也是电子商务发展的一个里程碑。支付宝的付款方式: 买家需要注册一个支付宝账户;利用开通的网络银行给支付宝账户充值;然后用支付宝账户在网站上购物 并使用网络支付;货款会先付款给支付宝;支付宝公司在收到支付的信息后给买家发货;买家收到商品后 在支付宝确认;支付宝公司收到买家确认收货并满意的信息后;最终给卖家付款。

资料来源: 网络 http://www.jjsdb.com/Top300/company.

问题:

支付宝实现的即付转账功能对电子商务发展起到怎样的作用?

支付宝是一个网络转账工具,也是一种网上的支付平台,用户可以通过它给其他有支付宝的人汇款,也可以把它作为第三方的机构,在特定的环境下(淘宝网)进行网上购物,这是一种可以同时保护买卖双方不被欺诈的第三方平台。

4.2.3 账户划转的支付方式

由于社会上出现银行类的金融机构,任何一个经济主体和社会人都能在银行开设有自己的账户,而银行是社会信用的产物,具有很高的社会信用,银行发行的票据和银行账户就具有与现金同等的信誉,社会相信它,因此它也可作为支付中的一个工具所使用。

A 向 B 支付以结清债务,可以采用将自己账户上等值数额的金额划拨到 B 账户上的方式来进行,如图 4.2 所示。

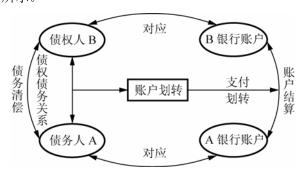


图 4.2 账户划转支付方式

这种支付方式减少了现金在社会中的流通量,并且支付的环节更简单。社会上债权债务关系的清偿,通过银行这个中间环节,变成了银行间账户划拨的结算关系。这种支付方式成为现代信用社会中常用的普遍通行的一种支付和结算方式。

4.3 基于银行卡的网络支付方式

银行卡按性质不同分为信用卡和借记卡,在即付型网络支付中,银行卡主要指不具备 透支功能的借记卡。银行卡网络支付与其他形式的网络支付方式相比,具有发行广泛,使 用简单等优势。

在我国,银行卡种类多,满足了不同用户的需求;另外,在银联的作用下,各类银行 卡具有一定的标准;这些都为银行卡网络支付的发展和普及做了积极的铺垫。



阅读案例 4-2

丰富的银联卡

中国银联是经国务院同意,中国人民银行批准设立的中国银行卡联合组织,成立于 2002 年 3 月,总部设于上海。目前已拥有 240 多家境内外成员机构。

作为中国的银行卡联合组织,中国银联处于我国银行卡产业的核心和枢纽地位,对我国银行卡产业发

130

即付型网络支付方式 第 4 章

展发挥着基础性作用,各银行通过银联跨行交易清算系统,实现了系统间的互联互通,进而使银行卡得以跨银行、跨地区和跨境使用。在建设和运营银联跨行交易清算系统、实现银行卡联网通用的基础上,中国银联积极联合商业银行等产业各方推广统一的银联卡标准规范,创建银行卡自主品牌;推动银行卡的发展和应用;维护银行卡受理市场秩序,防范银行卡风险。

在中国银联与各家商业银行共同努力下,我国银行卡的联网通用不断深化,银联网络不仅在东部地区和大中城市日益普及,更进一步加速向中西部地区、中小城市和广大农村地区延伸。截至 2009 年 6 月底,境内联网商户达 135 万户,联网 POS 具达 211 万合,联网 ATM 达 18 万合,分别是银联成立前 2001 年的 9 倍、9.7 倍和 4.7 倍,一个规模化的银行卡受理网络在我国已形成。随着联网通用的不断深化和国内银行卡受理环境的不断改善,银行卡交易额呈现快速增长趋势。2008 年全国银行卡跨行交易金额达到 4.6 万亿元,是银联成立前 2001 年的 50 倍。银行卡消费额在社会消费品零售总额中的比重由 2001 年的 2.7%上升到 2008 年的 24.2%。

为满足中国人日益增长的境外商务、旅游、学习的用卡需要,以及把境内商业银行的服务通过银联网络延伸到境外,中国银联积极展开国际受理网络建设。截至目前,银联卡已在境外 61 个国家和地区实现受理;与此同时,中国银联还积极推动境外发行银联标准卡,为境外人士到中国工作、旅游、学习提供支付便利,目前已有 8 个国家和地区的近 50 家金融机构正式在境外发行了当地货币的银联标准卡。银联卡不仅得到了中国持卡人的认可,而且得到了越来越多国家和地区持卡人的认可。

为满足人民群众日益多元化的用卡需求,中国银联大力推进各类基于银行卡的创新支付业务。人民群众不仅可以在 ATM 自动取款机、商户 POS 刷卡终端等使用银行卡,还可以通过互联网、手机、固定电话、自助终端、数字电视机等各类新兴渠道实现公用事业缴费、机票和酒店预订、信用卡还款、自助转账等多种支付。围绕着满足国人多元化用卡需求,在中国银联和商业银行等相关机构的共同努力下,一个范围更广、领域更多、渠道更丰富的银行卡受理环境正在逐步形成。

资料来源:中国银联主页.http://corporate.chinaunionpay.com/infoComIntro/huoban/file_2607598.html. 问题:

为实现银行卡网络支付的普及,现有的银行卡、银行卡管理和银联需要做哪些改进或者创新?

日益强大的中国需要强大、自主的银行卡产业,强大、自主的银行卡产业需要中国银行卡产业界的共同努力。中国银联充分发挥卡组织职能,联合各商业银行牢牢掌握我国银行卡产业的话语权和主导权,维护国家经济、金融安全,为人民提供优质、安全、高效的银行卡服务。银联推出的各项创新内容,尤其是银行卡的电子标准化,将促使银联不仅服务于中国,而且服务于越来越多的国家和地区,成为具有全球影响力的中国自主支付品牌。

4.3.1 基于 SSL 协议机制的银行卡网络支付方式

1. 银行卡网络支付 SSL 模式简介

SSL 是设计用来保证互联网信息传递的保密性的,并不是专门用于电子支付的技术。通过 SSL,消费者在浏览商家页面信息的时候,其客户端的浏览器与商家服务器通过一个加密的安全通道进行信息交换,第三者无法通过窃听的方法把得到的加密数据还原成明文。同样,消费者的银行卡授权信息也将在安全的通道中传递。

SSL 协议在运行过程中可分为 6 个阶段。

- (1) 建立连接阶段:客户通过网络向服务商打招呼,服务商回应。
- (2) 交换密码阶段:客户与服务商之间交换双方认可的密码。

- (3) 会谈密码阶段:客户与服务商之间产生彼此交谈的会谈密码。
- (4) 检验阶段: 检验服务商取得的密码。
- (5) 客户认证阶段:验证客户的可信度。
- (6) 结束阶段:客户与服务商之间相互交换结束信息。

SSL 在信息传递上的安全性,刚好适应了电子支付的需要。又由于架构简单,处理的步骤少,速度快,所以虽然存在一定的安全性漏洞,但依然被广泛的应用在银行卡在线支付模式中。

2. 银行卡网络支付 SSL 模式工作流程

银行卡网络支付 SSL 模式的工作流程如图 4.3 所示。

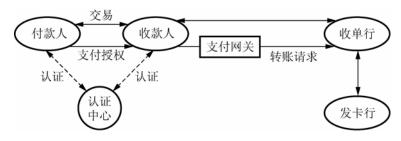


图 4.3 基于 SSL 的网络支付方式

- (1) 身份认证。SSL 模式的身份认证机制比较简单,只是付款人与收款人在建立"握手" 关系时交换数字证书。
- (2) 付款人建立和收款人之间的加密传输通道之后,将商品订单和银行卡转账授权传递给收款人。
 - (3) 收款人通过支付网关将转账授权传递给其收单行。
- (4) 收单行通过银行卡清算网络向发卡行验证授权信息,发卡行验证银行卡相关信息 无误后,通知收单行。
 - (5) 收单行通知收款人电子支付成功,收款人向收单行请款。
 - 3. 银行卡网络支付 SSL 模式的特点

分析银行卡网络支付 SSL 模式工作流程,可以总结出该支付方式的以下特点:①实现的是部分信息加密,以提高效率;②使用对称私有密钥和非对称公开密钥加密技术,各尽所长,相当安全;③客户端可选对商家身份验证数字证书,提高支付效率;④由于持卡客户端进行网络购物时只需一个银行卡号和密码,无须任何其他硬件设施,可以说比传统的银行卡支付投入还少,所以这种支付方式给支付客户带来极大的方便,支付处理速度也比较快。

另外,基于 SSL 协议机制的银行卡网络支付方式的业务流程中,由于需要一系列的加密、授权、认证及相关加密信息传送,需要有一定的交易成本,所以对微额支付而言不太适用。

4.3.2 基于 SET 协议机制的银行卡网络支付方式

1. 银行卡网络支付 SET 模式简介

银行卡网络支付 SET 模式,是电子支付中遵守 SET 协议的银行卡支付方式,以实现银行卡的即时、安全可靠的网络支付。在这种支付方式中,运用了一系列安全技术与身份认证手段,如对称加密、公开密钥加密、数字摘要、数字签名和双重签名、数字证书等。SET 协议的作用是达到网络的安全交易。安全电子交易的目的是提供信息的保密性,确保付款的完整性和能对商家及持卡人进行身份验证,而实施 SET 机制可以做到如下几点。

- (1) 对付款信息及订单信息能各自保密。
- (2) 能确保所有传送信息的完整性。
- (3) 能验证付款人是银行卡的合法使用者。
- (4) 能验证商家是该银行卡的合法特约商家。
- (5) 建立一个协议,该协议不是依赖传输的安全机制。
- (6) 能在不同平台上及不同网络系统上使用。

SET 协议为了能做到上述 6 点,必须要架构一个 PKI(Public Key Infrastructure,公钥基础设施)对参与的成员进行认证,同时利用密钥对传送信息进行加密。在 SET 协议中对认证的架构规定严谨,认证是采用层级式的架构,而无论是付款人、收款人或收单银行都需要经过认证才能参与交易。其中地区性认证中心并不一定存在,而品牌认证中心可能直接认证付款人、收款人及金融机构。当利用银行卡进行 SET 网络支付时,需要在客户端上安装一个特殊的客户端软件配合银行卡的运用才行。

2. 银行卡网络支付 SET 模式的工作流程

在 SET 协议环境下,应用银行卡进行电子支付,需要在客户端下载一个客户端软件(电子钱包软件),在商家服务端安装商家服务器端软件,在支付网关安装对应的网关转换软件等,并且各参与者还要各自下载一个证实自己真实身份的数字证书,借此获取自己的公开密钥和私人密钥对,且把公开密钥公开出去,手续稍显麻烦。具体的支付流程如图 4.4 所示。

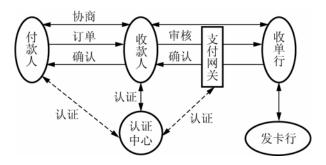


图 4.4 基于 SET 机制的网络支付流程

- (1) 付款人在发卡行柜台办理应用 SET 网络支付的银行卡; 收款人(商家)与收单行签订相关结算合同,得到商家服务器端的 SET 支持软件,并安装。
 - (2) 付款人从银行网站下载客户端软件,安装后设置应用此软件的用户名、密码等,

以防止被人非法运行。

- (3) 付款人访问认证中心网站,把银行卡相关信息,如卡类别、卡号、密码、有效期等资料填入客户端软件,并且申请一张数字证书。
- (4) 付款人在商家网站上选购商品,结账时选择 SET 银行卡结算方式。这时客户端软件被激活,付款人输入软件用户名和密码,取出里面的相应银行卡进行支付。
- (5) 客户端软件自动与商家服务器相应软件进行身份验证,双方验证成功后,将订单信息及银行卡信息一同发送到商家。
- (6) 商家服务器接收到付款人发来的相关信息,验证通过后,一边回复付款人一边产生支付结算请求,连同从客户端来的转发信息一并发给支付网关。
- (7) 支付网关收到相应支付信息后转入后台银行网络处理,通过各项验证审核后,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。
- (8) 支付网关向商家转发支付确认信息,商家收到后认可付款人的这次购物订货单, 并且给付款人发回相关购物确认与支付确认信息。
- (9) 付款人收到商家发来的购物确认与支付确认信息后,表示这次购物与网络支付成功,客户端软件关闭。电子支付完毕。
 - 3. 银行卡网络支付 SET 模式的特点

分析银行卡网络支付 SET 模式工作流程,可以总结出该支付方式的以下特点:①需要在持卡客户端安装客户端软件;②需要各方申请安装数字证书并且验证真实身份;③实现的是部分信息加密,以提高效率;④使用对称密钥加密法、非对称密钥加密法、数字摘要技术、数字签名、数字信封等多种技术,各尽所长;⑤充分发挥 CA 的作用以维护在 Internet 上的电子商务参与者所提供信息的真实性和保密性;⑥客户端软件功能多样,每次网上购物的相关信息都可集成在一个数据结构里,以后整体地自动提取应用,可以减少持卡客户每次购物的烦琐度和工作量。由于加密、认证多,支付处理速度相比于 SSL 机制,速度稍慢一些,各方开销大一些。

与 SSL 协议机制的银行卡网络支付方式一样,基于 SET 协议机制的银行卡网络支付方式对微额交易而言是不太适用的,成本相对较高。可在持卡客户端软件里装电子零钱应用,加密与认证次数就少多了,应用起来效果更佳。

- 4.3.3 借助第三方代理机构的银行卡支付方式
 - 1. 借助第三方代理机构的银行卡支付方式简介

在买方和卖方之间启用一个具有诚信的第三方代理机构支付的方式,这样可以在一定程度上降低支付的风险。

第三方代理人如果是发卡银行本身,那么发卡银行只需向持卡人分发一个代替银行卡账户的注册账号在网上传递,支付时由第三方核对确认并且经持卡人确认后进行资金的转移,其银行卡账号就没有暴露给广大的商家,这样只有发卡银行知晓持卡人的信息相对就安全得多。

如果第三方代理机构不是发卡银行本身,而是社会上具有良好信誉的金融机构或中介服务机构,这时第三方代理机构同样给持卡人分发一个代替信用卡账号的注册账号并在网

上传递,支付由第三方核对确认且经持卡人同意后由第三方代理机构与发卡银行、收单银行等进行专网连接,然后进行相应的资金转移。这样不但信用卡的账号没有暴露给广大的商家,而银行也不用直接与客户在 Internet 这样的非安全网络打交道,客户省去很多麻烦,支付事务都交给第三方来代理。

2. 借助第三方代理机构的银行卡支付流程

借助第三方代理机构的银行卡支付流程如下。

- (1) 持卡客户以在线或离线方式在第三方代理机构处登记银行卡号和注册一个相应的应用账号,由代理人持有买方的银行卡号和账号。
- (2) 持卡客户上网用该应用账号从网上商家处进行在线订货,且把应用账号传送给商家。
- (3) 商家将持卡客户传送来的应用账号、交易资金、支付条款等信息以离线或在线方式提供给第三方代理机构核实,第三方代理机构验证应用账号信息后,经与持卡客户协商,得到持卡客户确认,再返回给商家一个确认信息。
- (4) 商家在收到第三方代理机构的确认信息后,接收持卡客户的购货订单,然后给持 卡客户以及第三方发出交易确认通知。
 - (5) 第三方代理机构收到交易确认通知后,按支付条款要求办理资金转拨手续。 图 4.5 描述了借助第三方代理机构的银行卡支付的流程。

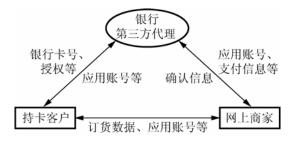


图 4.5 第三方代理机构的银行卡支付的流程

3. 借助第三方代理机构的银行卡支付方式的特点

使用这种方式是通过双方都信任的第三方代理机构协助完成的,由于真正的银行卡信息不在开放的网络上多次传送,因此持卡客户既没有信用卡信息被盗窃的风险,卖方也没有很高的受骗风险;这种方式对第三方代理机构的公正、信誉与操作规范有很高的要求,主要风险由第三方代理机构承担;该方式虽然提高了支付的安全性,但支付效率还是较低,成本也较高,其性能价格比在小额支付结算中并不高,它属于电子商务发展初期利用银行卡支付结算时的一种过渡方式。

在 B2B 类电子商务中,由于支付金额较大,有时商务各方出于安全、习惯等问题,反而愿意应用这种借助第三方代理机构担保的支付形式,因为这时支付成本、效率均是次要的了。

4.3.4 银行卡网络支付实例

实例:注册中国工商银行个人网络银行并利用银行卡进行支付。

- (1) 阅读《注册须知》,单击"注册个人网络银行"按钮。
- (2) 阅读《中国工商银行电子银行个人客户服务协议》,接受并单击"接受此协议"按钮,如图 4.6 所示。

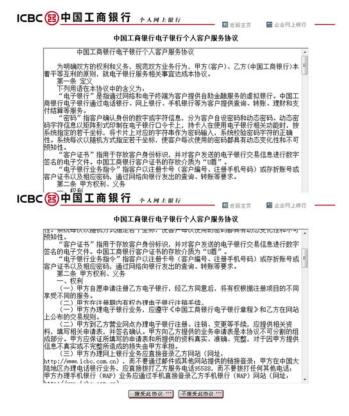


图 4.6 阅读并接受协议

(3) 输入注册卡卡号并单击"提交"按钮,如图 4.7 所示。



图 4.7 注册卡号

即付型网络支付方式

(4) 注册个人网络银行,填写相关信息(密码设置对安全很重要),并单击"提交"按钮,如图 4.8 所示。



图 4.8 填写信息

- (5) 确认注册为个人网络银行的卡号信息后,显示银行卡已经开通了网络银行。
- (6) 选择"我的财付通"选项卡,单击"充值"按钮,选中"中国工商银行"单选按钮,如图 4.9 所示。



图 4.9 "财付通"充值页面

(7) 单击"确定充值,去网银付款"按钮后,弹出新页面,进入工商银行支付系统。确认支付信息,包括金额和卡号,单击"提交"按钮,如图 4.10 所示。



图 4.10 进入工商银行支付系统

- (8) 对于预留信息进行校验, 若正确, 单击"金额付款"按钮。
- (9) 再次确认支付信息,输入口令卡密码,如图 4.11 所示。



图 4.11 预留信息校验

(10) 显示支付成功,同时原"财付通"页面也显示充值成功信息,如图 4.12 所示。



图 4.12 "财付通"充值成功

4.4 电子支票网络支付方式

4.4.1 电子支票网络支付方式概况

电子支票网络支付就是在互联网平台上利用电子支票完成商务活动中的资金支付与结算,包含了购买方、销售方以及金融机构 3 个主体。电子支票支付使用方式模拟传统纸质支票应用于在线支付,可说是传统支票支付在网络的延伸。电子支票的签发、背书、交换及账户清算流程均与纸质支票相同,用数字签名背书,用数字证书来验证相关参与者身份,安全工作也由公开密钥加密来完成。除此之外,电子支票的收票人在收到支票当时,即可查知开票人的账上余额及信用状况,避免了退票风险,这是电子支票超越传统支票的优点。

电子支票通过互联网传递,收款银行收到电子支票后,通过自动清算所(Automated Clearing House, ACH)网络来交换,这种银行体系和公众网络整合的做法,为银行及用户提供了类似实体支票处理机制的可行方案。电子支票支付方式按照参与银行的情况,可分为同行电子支票网络支付方式和异行电子支票网络支付方式两种。在同行电子支票网络支付模式中,金融机构有一家银行就行了;在异行电子支票网络支付方式中,则借助票据交易所,可由一独立的机构或现有的一个银行系统承担,其功能是在不同的银行之间处理票据和清算。

在第 2 章的案例中,曾经提到了旅游电子支票。旅行支票是由银行或专门的金融公司提供的一种非现金支付工具,它既可以直接用于消费,又可以和现钞混用。电子旅行支票则是一种替代纸张旅行支票的产品,它具备在 ATM 及 POS 上使用的功能,还可重复充值使用。通济隆和查打银行联手 VISA 在上海推出了国内首张电子旅行支票——"易世金",充分显示了银行、汇兑公司等金融机构抢占出境游市场的计划。

从阅读案例 4-2 可以看出,电子支票的形式和作用可以是多样化、个性化的。但作为 传统支票的衍生,所有的电子支票在实现网络支付时都要遵循一定的模式。

1. 同行电子支票网络支付模式

同行电子支票的应用由于只涉及同一个银行的资金结算问题,比较简单、方便与可靠。 因此,同行电子支票的支付流程示意图也比较简单,如图 4.13 所示。

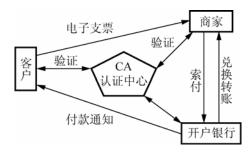


图 4.13 同行电子支票网络支付流程示意图

(1) 预备工作。客户与开户银行、商家与开户银行之间密切协作,通过严格的认证阶

- 段,如相关资料的认定、数字证书的申请与电子支票相关软件的安装应用、电子支票应用 的授权等,以准备利用电子支票进行网络支付。
 - (2) 客户和商家达成网上购销协议,并选择使用电子支票支付。
 - (3) 客户通过网络向商家发出电子支票。
- (4) 商家收到电子支票后,通过认证中心 CA 对客户提供的电子支票进行验证,验证无误后将电子支票送交银行索付。
- (5) 开户银行在商家索付时通过认证中心 CA 对客户提供的电子支票进行最后验证,如果有效即向商家兑付或转账。即从客户资金账号中转拨相应资金余额到商家资金账号。如果支票无效,如余额不够、客户非法等,即把电子支票返回商家,告知索付无效消息。
 - (6) 开户银行代理转账成功后,在网上向客户发出付款成功通知消息,方便客户查询。

2. 异行电子支票网络支付模式

异行的电子支票由于涉及两个或多个银行,以及中间的用于银行间资金清算的票据交易所(资金清算系统),所以流程较为复杂,但实施技术难度上与同行的电子支票应用并无多大的区别,需要银行间、银行与票据交易所间在电子支票的应用上达成协议。完整的异行电子支票网络支付业务的支付流程如图 4.14 所示。

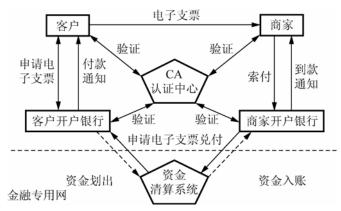


图 4.14 异行电子支票网络支付流程示意图

异行电子支票的支付流程,除包含与前面所述一样的电子支票应用预备工作阶段外, 一般可分为 3 个不同阶段,即客户的购买阶段、商家索付阶段和行间清算兑付阶段,每一 阶段又由若干个步骤构成。

- 1) 客户的购买阶段
- (1) 客户访问商家的服务器,商家的服务器向客户介绍其货物。
- (2) 客户挑选货物并向商家发出电子支票。
- (3) 商家通过认证中心和其开户银行对支付进行认证,并验证客户电子支票的有效性。
- (4) 如果支票是有效的,商家则接收客户的这宗业务。
- 2) 商家索付阶段

商家把电子支票发送给自己的开户行。商家可根据自己的需要,何时发送由其自行决 定,只要在电子支票使用期限内就行。

- 3) 行间清算兑换阶段
- (1) 商家的开户行把电子支票发送给票据交易所的资金清算系统,以兑换现金,进行清算。
 - (2) 票据交易所向客户的开户行兑换支票,并把现金发送给商家的开户银行。
- (3) 商家开户银行向商家发出到款通知,即资金入账,而客户的开户银行则向客户发出付款通知,即为客户下账。

异行电子支票网络支付模式实现了跨行存取款,提高了资金的周转率,在实际应用中, 其具体形式也是多种多样的。参见阅读案例 4-3。



阅读案例 4-3

小额支付系统银行本票业务

央行小额支付系统已在上海成功运行了国内第一单银行本票业务。这意味着今后银行客户可以在 24 家主要的中外资银行之间瞬时划转 50 万元以下资金,且其收费与传统的银行本票业务收费相同。央行上海总部指出,银行本票垫付资金及时回笼将大大提高资金周转效率。

小额支付系统银行本票业务,是指代理付款行与出票银行依托小额支付系统实现银行本票信息的实时 比对和资金清算的业务。采用小额模式处理银行本票后,银行本票出票信息全部转化为电子信息,录入出 票行行内系统;银行本票的兑付由代理付款行采集票据信息和密押后,通过小额支付系统转发出票行行内 系统进行自动比对兑付。

目前,共有24家中外资银行的共1000多家对公营业网点可以办理小额支付系统银行本票业务,且其收费与传统的银行本票业务收费相同。业内人士指出,此前股份制银行之间已经可以用"柜面通"实现跨行存取款,而小额支付系统的最大意义在于实现四大国有银行和股份制银行以及外资银行之间的跨行存取款。这使得后者可以集中精力于服务和产品,而不必与国有银行争开网点。

资料来源:证券时报.2008-05-09.

问题.

小额支付系统的作用和意义?

在《依托小额支付系统办理银行本票业务处理办法》中指出,依托小额支付系统办理银行本票业务是指代理付款行与出票行依托小额支付系统实现银行本票信息的实时比对和资金清算的业务。小额支付系统把本票信息实时比对的处理分为银行本票信息传输和银行本票业务回执的处理。与其他银行结算方式相比,银行本票结算具有如下的特点:①使用方便;②信誉度高,支付能力强。

在我国,为了有效利用现有网络资源实现电子支票的各项功能,可以采用行间直连模式和跨行连接模式两种,与上述模式相对应。

(1) 行间直连模式:采用行间直连模式,付款人银行、收款人银行、清算中心均需要有处理电子支票的设备。这种模式的具体流程如图 4.15 所示:①付款人用智能卡插入指定设备,生成一张电子支票,并通过 Internet 传送给收款人和付款人银行;②收款人在收到电子支票后,用自己的私钥对支票加盖电子签名,并发给收款人银行;③收款人银行可以利用存储在本地的收款人的证书,也可以从认证中心证书库中查询出的证书,对收到的支票进行认证处理,同时付款人银行也利用付款人的公钥证书对支票进行认证处理;④收款人

银行对支票进行处理,并把处理过的支票发往清算中心与付款人银行进行行间清算;⑤付款人银行通知付款人支票的处理情况;⑥收款人银行通知收款人支票的处理情况。

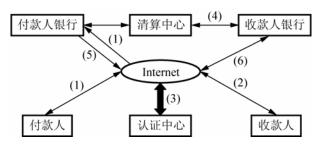


图 4.15 行间直连

(2) 跨行连接模式:采用跨行连接模式,只需支付网关配备电子支票处理设备即可,各银行的硬件设备无须改动,只需对现有的软件进行少许的修改。这种模式的具体运作流程如图 4.16 所示:①付款人用 IC 卡插入指定的设备,生成一张电子支票,通过 Internet 传给收款人;②收款人在收到的电子支票上用自己的私钥加盖电子签名,并发给支付网关;③支付网关对电子支票通过认证中心进行认证;④支付网关将认证后的支票(若认证成功)转换为银行原有的支票形式,并送给收款人银行;⑤收款人银行根据支票内容进行处理,并发往清算中心,与付款人银行进行行间结算;⑥支付网关将处理结果通知收款人和付款人。

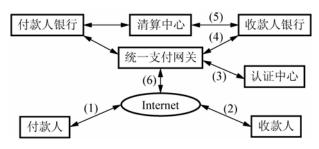


图 4.16 跨行连接

与行间直连模式相比,跨行连接模式具有很大的优越性。由于所有的电子支票交易均通过统一的支付网关进行,当需对硬、软件升级时,也只需对支付网关做相应的更改。同时,由于票据集中处理,提高了票据的处理速度。另外,统一支付网关作为独立的第三方机构,还可以对因交易引起的纠纷进行调节、仲裁、并协调各银行共同制定网络支付标准,确保支付安全、迅速地进行。

4.4.2 电子支票支付的安全性要求

1. 电子支票的认证

电子支票是客户用其私钥所签署的一个文件。接受者(商家或商家的开户行)使用支付者的公钥来解密客户的签字。这样将使接收者相信发送者的确签署过这一支票。电子支票是以纸质支票的电子替代品的形式存在,用来吸引不想使用现金,而宁可使用信用方式的个人客户和公司。电子支票支付仿真纸面支票,不过是用电子方式启动,使用电子签名作为背书,而且使用数字证书来验证付款者、付款银行和银行账号。电子支票的安全认证工

作是由公共密钥算法的电子签名来完成的。

2. 公钥的发送

发送者及其开户行必须向接收者提供自己的公钥。提供方法是将他们的 X.509 证书附加在电子支票上。

3. 私钥的存储

为了防止欺诈,可向客户提供一个 Smart 卡,以实现对私钥的安全存储。在电子支票体系结构下,要保证交易的真实性、保密性、完整性和不可否认性,最重要的一个环节就是确保私钥的安全性。现行的做法是客户使用智能卡来实现对私钥的保护。客户要通过电子支票进行支付,需要在计算机上安装读卡器和驱动程序。读卡器通过一根串行电缆与计算机的串行通信口相连。在安装驱动程序时,智能卡设备的加密驱动程序将被安装在机器上。Web 服务器首先验证客户端证书的有效性,在确认证书有效后,Web 服务器发送一串随机数给客户端浏览器(浏览器与智能卡通信时,要求输入智能卡的 PIN,增加了安全性),智能卡使用私钥对这串随机数进行数字签名,签名后的随机数串被回送给 Web 服务器,并由 Web 服务器验证签名,如果签名验证通过,Web 服务器和浏览器之间使用 SSL 协议规程,建立安全会话通道进行通信,两者之间发送和接收的信息经过加密,客户可以进行相关的操作。

4.4.3 电子支票网络支付的特点

电子支票是电子银行与新兴的网络银行服务中常用的一种电子与网络支付工具。与传统的纸质支票支付相比,电子支票的网络支付具有如下一些主要特点。

- (1) 节省时间。电子支票的发行不需要填写、邮寄或发送,而且电子支票的处理也很省时。在用纸质支票时,卖方必须收集所有的支票并存入其开户行。用电子支票,卖方可即时发送给银行,由银行为其入账。所以,使用电子支票可节省从客户写支票到为商家入账这一段时间。
- (2) 减少了支票被退回情况的发生。电子支票的设计方式使得商家在接收前,先得到客户开户行的确认。类似于银行本票。
- (3) 电子支票网络支付适合于各种市场,可以很容易地与 EDI 应用结合,推动 EDI 基础上的电子订货和支付。同时也较好地支持了企业与企业之间、企业与政府部门之间的电子商务市场。电子支票网络支付方式可在收到支票时验证出票者的签名、资金状况,避免收到传统支票时发生的无效或空头支票现象,减少风险。由于支票内容可以附在贸易双方的汇票资料上,所以电子支票容易和金融 EDI 应用的应收账款结合。金融 EDI 即是 FEDI,它是 EDI 的一种形式,是专门用来进行电子支付的系统。FEDI 通常建立在银行与它们的合作客户之间,银行可以通过 FEDI 收到付款人的付款授权,并向收款人付款,银行之间的资金转移一般通过银行自己的网络进行。因此电子支票网络支付非常适合 B2B 电子商务的中大额支付结算。
- (4) 通过应用数字证书、数字签名以及加解密技术,采用唯一电子支票号码检验技术, 提供了比使用印章和手写签名更加安全可靠的防欺诈手段。

- (5) 电子支票网络支付将整个处理过程自动化,帮助银行缓解了处理支票的压力,节省大量的人力和开支,极大地降低了处理成本。
- (6) 可以在任何时间、地点通过 Internet 进行电子支票的网络支付, 打破了地域的限制,最大限度地提高支票的收集速度, 从而为客户提供了更方便快捷的服务和减少了途中资金。

4.4.4 电子支票支付系统实例

目前基于 Internet 的电子支票系统在国际上日趋成熟,中国也将对这方面进行更加深入的研究。随着数字签名、数字证书和加密解密技术日趋完善,实际的大额网络支付应用需求已经出现,考虑到电子交易的飞速增长,B2B 交易将成为网上交易的主流,以及研发的前瞻性,我国开展电子支票研发的时机已经成熟。特别是对于银行来说,我国已加入 WTO,金融机构必将与国外的金融机构在提供现代化的金融服务方面展开激烈的竞争,因此研发我国自己的电子支票系统也就特别紧迫。

目前,电子支票支付主要遵循国际金融服务技术联盟(Financial Services Technology Consortium,FSTC)提的 BIP(Bank Internet Payment)标准(草案)。典型的电子支票系统有FSTC Electronic Check、The Mandate Electronic Cheque、NetCheque、Netchex,以及由美国匹兹堡 Carnegie Mellon 大学的 NetBill 等。

1. NetCheque

NetCheque 是由南加州大学信息科学研究院开发出来的一种基于 Kereros 应用的在线电子支票支付系统。NetCheque 支付系统中不仅有客户、商家与银行,还包括 Kereros 服务器。NetCheque 支付系统使用 Kereros 服务器提供客户签发支票的信用担保,允许被授权的持票者从 NetCheque 银行账户上提取资金,同时防止非法持有者存储不是发行给他的 NetCheque 支票。NetCheque 支付系统的运作流程如下。

- (1) 客户在签发支票时,首先生成支票的明文部分,包括支票数额、货币单位、日期、账户号码、收款人等信息。然后从 Kerberos 服务器获得一个标签 Tc(事先客户应通过 Kerberos 的信任验证),用以证明 Kerberos 服务器对这张纸票的信用授权。客户再用 Tc 向开户行证明身份,并获得开户行的加密证明文件 Ac,这是开户行对其所签支票的授信。支票明文部分再加 Tc 和护航的证明文件 Ac 就构成了一张完整的电子支票。
 - (2) 电子支票通过公共网络上的电子邮件或加密线路传送给商家服务器。
- (3) 商家收到支票后,根据 Tc 和 Ac 验证客户身份及信用,取出明文部分,再经过类似签发支票的方法对此支票进行背书,加上商家名称,背书时间等内容,形成背书后的支票。
- (4) 背书后的支票被传送给商家的开户行,如客户与商家是同一个开户行,则直接将客户银行账户上的资金划拨到商家账户上;如非同一家开户行,则支票需要在各银行间进行清算,最终将客户银行账户上的资金划拨到商家账户上。

2. FSTC 电子支票

FSTC(Financial Services Technology Consortium,美国金融服务技术联合会)成立于 1993 年,是由美国的银行、大学以及政府机构等 60 多个机构联合成立的非营利性组织,其目的在于提高全美金融服务业的竞争能力。其运作流程如下。

- (1) 付款人在签发支票时,使用由电信设备公司生产的,被称为"智能辅币机"的安全硬件设备来产生一张电子支票。该设备的功能就是安全地存储密钥和证书信息,并保持最近签发或背书过的支票记录。
 - (2) 生成的电子支票通过安全电子方式,或双方之间加密过的交互对话方式进行传送。
- (3) 收款人收到支票后,将利用票据交换所来清算支票。电子支票通过银行清算网络进行传送,相应地,资金从付款人银行账户转到收款人银行账户。

3. NetBill

NetBill 电子支票系统是美国卡耐基-梅隆大学开发的一种支付系统。该系统尽可能地改善了低价值信息产品的买卖。系统参与者包括客户、商家以及为他们保存账户的 NetBill 服务器。这些账户是信用卡预存资金账户,可与银行账户相连,客户可将银行账户上的资金划拨到 NetBill 账户,而商家则可以将 NetBill 账户中的资金存入其银行账户。客户在使用 NetBill 账户购买商品时,只需要选择自己所需要的商品,余下的处理过程将由 NetBill 自行完成。整个交易包括价格协商、商品传送以及支付 3 个阶段。NetBill 通过向客户与商家提供一种工具(在客户处称为"支票簿",商家处称为"收款机")来支持交易的实现。"支票薄"在客户端是一个使 NetBill 和客户的浏览器之间实现通信的程序,它能保存客户的 NetBill 账户资料,解密商家发来的信息,并显示客户的交易记录、期内平衡信息和账户平衡信息等,安全地处理交易、修改密码、检查交易状态;"收款机"在商家的服务器端是一个使 NetBill 和商家的服务器之间实现通信的软件,它实现对相关信息进行加密处理,保存客户的交易记录。与 NetCheque 支付系统相类似的是,在该支付系统中,也使用基于 Kereros 的保密密钥加密机制。具体交易流程如下。

- (1) 客户通过填写报价单与商家之间进行相关商品的价格磋商,磋商完毕,制定出具体价格后,商家将报价单返回给客户。
 - (2) 客户收到报价单后,如对价格满意,则通过支票簿向商家收款机发送购买请求。
- (3) 商家收到购买请求后,收款机使用对称加密算法对该信息产品进行加密,并将其 传送到客户的支票簿。
- (4) 客户支票簿在收到加密过的信息产品后,向商家收款机发送一份带有签名的电子支付订单。
 - (5) 商家收款机收到电子支付订单后对其进行背书,并将之发送到 NetBill 服务器。
- (6) NetBill 服务器验证电子支付订单后,将货款由客户的 NetBill 账户划拨到商家的 NetBill 中,并返回支付确认信息。
- (7) 商家收款机收到支付确认信息后,将对称密钥发送到客户支票簿。客户支票簿使 用对称密钥解密,得到信息产品。

由上述流程可以看出,NetBill 传送的货物非一般意义上的商品,而是能够在网络上进行传输的信息产品,因此,交易商品的种类受到了极大的限制,并且在整个交易中还必须涉及 NetBill 服务器。尽管在 NetBill 支付系统,参与各方的通信量已很低,但众所周知,信息产品的价值一般都比较低,相比而言 NetBill 通信成本还是比较高的,同时,系统的可扩展性也不强。

4.5 电子汇兑系统

所谓电子汇兑,即利用电子手段处理资金的汇兑业务,以提高汇兑效率,降低汇兑成本。广义的电子汇兑系统,泛指客户利用电子报文的手段传递客户的跨机构资金支付、银行同业间各种资金往来的资金调拨作业系统。具体来说,就是银行以自身的计算机网为依托,为客户提供汇兑、托收承付、委托收款、银行承兑汇票、银行汇票等支付结算服务方式。

任何一笔电子汇兑交易,均由汇出行发出,到汇入行收到为止。其间的数据通信转接过程的繁简,视汇出行与汇入行两者之间的关系而定。根据汇出行与汇入行间的不同关系,可把汇兑作业分成以下几种。

- (1) 联行往来汇兑业务。汇出行与汇人行隶属同一个银行的汇兑,属于银行内部账务 调拨,必须遵守联行往来约定,办理各项汇入和汇出事宜。
- (2) 通汇业务。资金调拨作业需要经过同业多重转手(多个银行参与)处理才能顺利完成的称为通汇业务。通汇业务是一种行际间的资金调拨业务,如本国通汇和国际通汇。跨行或跨国通汇,因涉及不同银行间的资金调拨,参与通汇的成员必须签署通汇协定,才能保证作业系统的正常运行。

电子汇兑系统的客户是单位,主要顾客是公司企业,其次是政府机构,社会大众很少使用。这种系统同前面介绍的各类电子货币网络支付系统相比有许多特点。前者额大量小,主要面对公司企业和政府部门;后者额小量大,主要面对社会公众。因此,国外把前者划归批发银行系统,把后者划归小额支付系统。

4.5.1 电子汇兑系统简介

银行与公司、企业单位、政府部门和其他金融机构的资金结算不同与面向大众的银行卡业务(可称为零售业务),是一种批量业务或批发业务。之所以称之为批量业务,是因为它们之间的交易金额大。据 Atlanta 的联邦储备银行统计,在商业银行处理的项目中,大于1000 美元的项目占总数的 5%,但是占总金额的 88%。因此,这种批量业务对银行来说是至关重要的,对整个社会的支付结算效率的影响也是非常重要的。

在银行实现电子化以前,同零售业务支付机制类似,批发业务支付机制也主要是基于支票等纸基凭证。对美国的企业调查表明,公司总收入的 80%是由支票收款的。这种基于纸基的手工支付机制,效率低,风险大,在途资金多,不能适应经济的快速发展要求,迫使企业和银行研制和发展用于批发业务的电子资金转账系统,即银行批量业务电子处理系统。

银行批量业务电子处理系统主要包括面向单位客户的银行电子化服务系统(如电子银行及 EFT、网络银行、电子支票等)和面向银行同业资金往来的电子汇兑系统。而面向单位客户的银行电子化服务系统要为其客户提供电子资金转账 EFT 服务,必须通过电子汇兑系统才能完成。

4.5.2 电子汇兑系统的特点

电子汇兑系统的特点如下。

- (1) 交易额大、风险性大。
- (2) 对系统的安全性要求高于时效性要求。客户汇款时最关心的是安全,其次才是及时送到。为了系统的安全,在设计电子汇兑系统时,信息的传输方式几乎都是先存后送,确保信息在传输过程中所通过的每个站点都有确切的记录,万一汇兑业务出现问题,也能迅速找出出事点。
- (3) 跨行和跨国交易所占的比重很大。因此,设计电子汇兑系统时,应适应国际上通 行的各种标准、规格和要求,才能顺利进行国际汇兑业务。

4.5.3 电子汇兑系统的类型

为适应国际贸易快速发展的需要,国际上建立了许多著名的电子汇兑系统。这些系统 所提供的功能不尽相同,按照依其作业性质的不同,可把电子汇兑系统分成三大类:通信 系统、资金调拨系统和清算系统。

- (1) 通信系统(Communication System)。主要提供通信服务,专为其金融机构成员传送同汇兑有关的各种信息。成员行接收到这种信息后,若同意处理,则将其转送到相应的资金调拨系统或清算系统内,再由后者进行各种必要的资金转账处理。这种系统的典型实例是国际环球同业财务电信系统(SWIFT),它把原本互不往来的金融机构全部串联起来。
- (2) 资金调拨系统(Payment System)。是典型的汇兑作业系统,负责具体支付。这类系统有的只提供资金调拨处理,有的还具有清算功能,属于这类系统的代表性系统有:在美国的 CHIPS、FEDWIRE,日本的全银系统,我国各商业银行的电子汇兑系统,中国人民银行的全国电子联行系统等。
- (3) 清算系统(Clearing System)。主要提供清算处理。如果汇入行与汇出行之间又无直接清算能力,则需委托另一个适当的清算系统进行处理。以美国为例,CHIPS 除可作资金调拨外,还可兼做清算,但对象仅限纽约地区的银行。纽约以外的银行清算则要交由具有清算能力的 FEDWIRE 进行处理。我国的异地跨行转汇,必须经过中国人民银行的全国电子联行系统,才能最终得以清算。

4.5.4 电子汇兑系统运作模式

电子汇兑系统运作是一个复杂的模式,如图 4.17 所示。尽管电子汇兑系统的种类很多,功能也不尽相同,但是汇出行和解汇行的基本作业流程及账务处理逻辑是很相似的。以一笔电子汇兑交易为例,由汇出行启动至解汇行收到为止,不论是点对点传送,还是通过交换中心传送,汇出行与解汇行都要经过以下基本作业处理流程。

- (1) 数据输入(Input Source)。
- (2) 电文的接收(Message Receipt)。
- (3) 电文数据控制(Data Control)。
- (4) 处理与传送(Process & Transfer)。
- (5) 数据输出(Out Destination)。

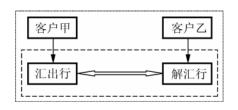


图 4.17 电子汇兑系统运作模式

4.5.5 国际网络支付系统

在第 2 章里面介绍的 CNFN 和 CNAPS 都属于电子汇兑系统,本小节与下两小节再分别以国际网络支付系统(SWIFT)、纽约清算所银行同业支付系统(CHIPS)、美国联邦储备通信系统(FEDWIRE)来为例。

1. SWIFT 的产生

SWIFT 全称是 Society for Worldwide Interbank Financial Telecommunication,中文名是环球同业银行金融电信协会。为适应国际贸易发展的需要,20世纪70年代初期,欧洲和北美的一些大银行,开始对通用的国际金融电文交换处理程序进行可行性研究。研究结果表明,应该建立一个国际化的金融处理系统,该系统要能正确、安全、低成本和快速地传递标准的国际资金调拨信息。于是,美国、加拿大和欧洲的一些大银行于1973年5月正式成立 SWIFT 组织,负责设计、建立和管理 SWIFT 国际网络,以便在该组织成员间进行国际金融信息的传输和确定路由。1977年夏,完成了环球同业金融电信网络(SWIFT 网络)系统的各项建设和开发工作,并正式投入运营。

2. SWIFT 管理结构

SWIFT 由 25 名董事长领导下的执行董事会为最高权力机构,监督由 CEO 领导的执行部门的工作。董事会包括 6 个委员会,分别是财务委员会,负责会计、财务报告与财务管理等;偿付委员会评估公司绩效,决定董事会成员和其他主要主管的薪酬管理,雇员薪酬管理,薪贴计划;两个商务委员会负责银行与支付和证券;两个技术委员会分别负责标准及技术和产品。具体管理结构如图 4.18 所示。

3. SWIFT 会员分类

SWIFT 的成员分为持股者和非持股者。

持股者(会员)Shareholder(Member)包括银行、符合资格的证券经销商以及符合规定的投资管理机构,都可以持有SWIFT SCRL的股份。会员行有董事选举权,当股份达到一定份额后,有董事的被选举权。

非持股者(Non-shareholders)主要分为非参股成员、附属成员及参与者 3 类。

非参股成员是那些符合成为参股人资格但是并未选择或不愿选择成为参股人的机构。

附属会员是持股会员对该机构组织拥有 50%的直接控制权或 100%的间接控制权。此外,该机构组织还需满足附属会员条例中第 8 款第 1 节的要求。即必须和会员所参与的业务相同。但必须完全由参股人控制管理。

即付型网络支付方式 第4章

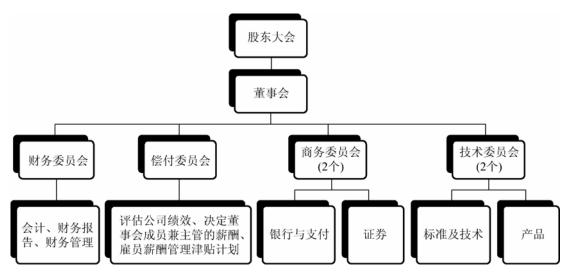


图 4.18 SWIFT 的管理结构

参与者是主要来自于证券业的各个机构,如证券经纪人和经销商,投资经理,基金管理者,货币市场经纪人等。只能获得与其业务相关的一系列特定服务,并且需满足公司大会中为其设定的标准。参与者不能持股。需要特别指出的是,根据参与者的类型不同,能够享有的 SWIFT 服务与产品会有所不同。

4. SWIFT 提供的服务

SWIFT 扮演着国际间银行业中枢神经系统的角色,担负着全球银行之间信息交流、资金流通的重任。SWIFT 提供的服务分为 4 大类:接入服务、金融信息传递服务、交易处理服务、分析服务与分析工具。

1) 接入服务

SWIFT 的接入服务通过 SWIFTAlliance 的系列产品完成,包括以下部分。

- (1) SWIFTAlliance Access and Entry: 传送 FIN 信息的接口软件。
- (2) SWIFTAlliance Gateway: 接入 SWIFTNet 的窗口软件。
- (3) SWIFTAlliance Webstation:接入 SWIFTNet 的桌面接入软件。
- (4) File Transfer Interface: 文件传输接口软件, 通过 SWIFTNet FileAct 使用户方便地访问其后台办公系统。

SWIFTNET Link 软件内嵌在 SWIFTAlliance Gateway 和 SWIFTAlliance Webstation 中,提供传输、标准化、安全和管理服务。连接后,它确保用户可以用同一窗口多次访问 SWIFTNet,获得不同服务。

2) 金融信息传送服务

SWIFTNet 启用以后,传统的 FIN 服务转而在新的网络 SWIFTNet FIN(已于 2002 年 8 月开通)上提供。SWIFT 把传统的 FIN 服务与新开发的、交互性的服务进行了整合,开发出 SWIFTNet 信息传送服务以满足现代金融机构不断发展的需要。包括以下 4 种服务。

(1) 在金融信息传送方面,SWIFT 的核心服务是 FIN。它通过 SWIFT 网络接收、存储转发各种金融业务处理中的数据。内置的冗余、分布式处理系统确保 FIN 服务安全、灵活、

可靠。其增值处理服务包括:按 SWIFT 标准进行信息格式化,信息的保存与恢复,信息管理及优先级控制。SWIFT 为支持大额支付及与证券相关交易中的清算、结算、净额结算提供了 FIN Copy 服务。在交易指令传达给接收方之前,指令要备份并通过第三方(如中央银行)的认证。FIN 服务使 SWIFT 称为世界上使用最广泛的支付服务系统,各国银行的国际业务都依赖于它,其信息种类、格式和技术架构已成为全球支付系统中的典范。如图 4.19 所示,近年来 SWIFT 处理的信息量一直保持在较高的水平。

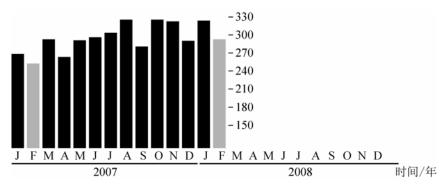


图 4.19 SWIFTNet FIN 每月信息发送量(横轴:时间,单位:年;纵轴:信息量,单位:百万)

- (2) SWIFTNet InterAct: 提供交互(实时)和存储与转发两种信息传送方式,适合要求实时应答的金融业务。InterAct 有 3 种不同的工作模式,分别是存储转发、实时报文、实时查询及响应模式。无论收报行联机与否,使用存储转发模式,当收报人准备好后,报文会被立即分发出去。对于交易时处于联机状态的收报行,实时报文模式比存储转发模式更快捷有效。实时查询及响应模式是一个典型的基于联机查询或报告的交互式服务系统,该模式通常和 SWIFTNet Browse 配合使用。
- (3) SWIFT FileAct: 提供交互和存储与转发两种文件自动传输方式,适合大批量数据的传输。通过 SWIFTNet 浏览器,用户可以方便地使用这两种服务。FileAct 支持任何类型的字符集、任何内容的结构,可使用 SWIFT 格式、集团内部格式或私有格式,最大可传输250MB 大小的文件,适合大批量数据的传输。利用 FileAct,所有的 SWIFT 成员紧密地连接在一起,快速地收发文件。无论是集中支付处理、支票影像交易、有价证券的附加信息还是给央行的报告、内部机构报告都可利用 FileAct 完成,欧美多数的金融机构都已经从安全、可靠、低廉的文件传输交换中获得了利益。
- (4) SWIFTNeBrowse: 以浏览器为基础,使用标准的 Internet 浏览器(如 IE)和 SWIFT Alliance Web Station 访问 Browse 服务,其安全由 SSL 和 SIPN 保证。

SWIFT 的访问过程如图 4.20 所示。

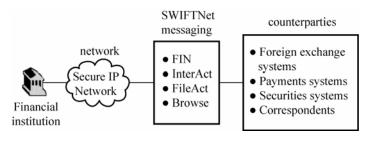


图 4.20 SWIFT 的访问示意图

3) 交易处理服务

交易处理服务(transaction processing)也是通过 SWIFTNet 向外汇交易所、货币市场和金融衍生工具认证机构提供交易处理服务,具体包括:①交易处理匹配服务;②实时报告的双边净额清算服务;③支持 B2B 的商务中的端对端网络支付。

4) 分析服务与分析工具

SWIFT 也向金融机构提供一些辅助性的服务,即分析服务与分析工具(Analytical Services/Tools)。

- (1) BIC Online 和 BIC Directory Update broadcast: 向金融机构提供最新的、世界范围内的金融机构的代码(BIC)。
 - (2) Traffic Watch: 可以监视 SWIFT 当前传送信息的数量。
- (3) Transaction Watch: 可以监视信息从发出到接收所经历的过程,获得各种参数,为提高证券系统和支付系统的效率提供分析数据。
- (4) STP Review: 金融机构为提高自身竞争力,直达处理(Straight Through Processing, STP)能力变得愈加重要。SWIFT 可以向用户提供独立、客观的 STP 评估。

5. SWIFT 的系统结构

目前的 SWIFT 系统结构是 4 层,如图 4.21 所示。

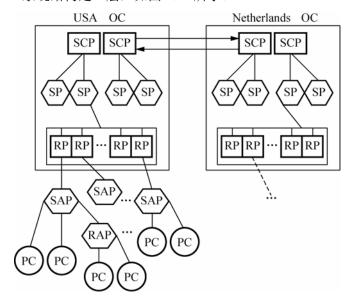


图 4.21 SWIFT 系统层次结构图

其中网络控制由设置在系统控制中心 OC 的系统控制处理机 SCP 完成,它控制和监测 网络片的片处理机,片处理机 SP 通过区域处理机 RP 进行发送和存储事务,区域处理机 RP 经过 SWIFT 访问点 SAP 连接到用户终端 PC 上。

SWIFT 的传输网络分为网络管理中心、核心网络、校验网络和界面网络 4 个层次,操作中心备有双重后备发电机、继电器设施电信网络及 24 小时的查询服务。网络和系统管理设置在美国和荷兰操作中心,遇故障时,另一个中心网络智能工作台可以照顾整个 SWIFT

网,网络的设置及更改由比利时网络操作中心统一运筹管理。银行本地线路、校验站由当地处理站处理。银行用户可用电话、电传等方式查询网络状况。

SWIFT 系统利用高度尖端的通信系统组成国际性的银行专用通信网,且在会员间传递信息、账单和同业间头寸划拨,即为全世界各个成员银行提供及时良好的通信服务和银行资金清算等金融服务。SWIFT 的使用,为银行的结算提供了更为安全、可靠、快捷、标准化、自动化的通信业务,从而大大提高了银行的结算速度。

1) 操作中心(Operating Centers, OC)

目前,整个 SWIFT 网络的业务处理集中在美国和荷兰两个操作中心。 SWIFT 通过这两个 OC 把发报行和收报行连接起来,OC 之间通过全双工链路连接,必要时可以互相备援。如果一个 OC 出现故障,该 OC 的通信工作转由另外一个 OC 处理。 SWIFT 网络的所有处理机都集中在这两个操作中心,它主要执行下述 6 种主要功能。

- (1) 注册(Login)。成员行的 SWIFT 接口设备 SID 经过注册才能进入系统。SID 的使用者必须输入经确认的密码,OC 才允许其注册和进入系统。
- (2) 电文接收(Message Reception)。当发报行将电文发到系统后,SWIFT 系统要对电文的内容进行验证。验证合格,则向发报行回发一条信息,说明已经收到电文,同时准备转发电文。
- (3) 电文处理 (Message Processing)。电文发出前,系统要对电文进行若干处理,主要包括记录追踪轨迹,检查是否符合系统规定的标准,编定输出参考码(Output Reference Number)及系统参考码 (System Reference Number)。其中,输出参考码包括收报行终端机代码及系统编定的输出电文序号 OSN;系统参考码包括发报行终端机代码及发报行编定的输入电文序号 ISN。上述参考码都是追踪电文在网络中运行的重要数据。
- (4) 电文提交(Message Delivery)。发报的准备工作,主要检查到目的地的路由是否畅通。若畅通,则将收到的电文转发到收报的 SID。除了系统电文(System Message)和紧急电文(Urgent Message)可享受发送优先权外,一般正常的交易电文采用先到先发的原则。通常,电文收到 10 分钟内就可发出。
- (5) 检索功能(Retrieval Function)。向成员行提供查询系统数据文件功能。但是严禁查询与自身无关的其他数据。
- (6) 网络控制 (Network Control)。SWIFT 系统中的每个 OC 都有一部主机负责与另一个 OC 及各 RP 之间的线路连接。该主机自动检测每条线路的负荷,若发现某条线路有超载现象,则自动使电文绕道转送。若检测到某线路故障或 RP 故障,亦将自动执行侦测功能,判断问题的原因,做出必要的恢复处理。
 - 2) 系统控制处理机(System Control Processor, SCP)

SCP 负责整个 SWIFT 网络的正常运行,不断监测、控制网络中的各种设备、线路和用户访问。在美国、荷兰的操作中心,各有两台 SCP,在任何时刻,只有一台 SCP 处于激活状态,控制整个网络,其余 3 台 SCP 处于热备份状态。在处于激活状态的 SCP 出现故障时,备份 SCP 被激活,保证网络的安全可靠性。

3) 片处理机(Slice Processor, SP)

SP 负责电报的存储转发和控制电报的路由选择。目前两个操作中心各有两台 SP 处于激活状态,同时每个激活的 SP 都有一台同型号的 SP 进行热备份。为了适应发报量不断增

第 **4** 章 即付型网络支付方式 ********

长的需要,还要陆续增加 SP。目前 SWIFT 采用的是 CNISYS 公司的 A 系列主机作为 SCP 和 SP。

4) 地区处理机(Reginal Processor, RP)

RP 是连接 SWIFT 网络终端(Computer Based Terminal, CBT)与 SWIFT 系统的安全有效的逻辑通道,运行在 RP 上的软件与运行在 CBT 上的接口软件通信。所有用户发出的电报都由 RP 对其格式、地址代码等进行审核。合格后才能发往 SP,在电报即将出网进入CBT 前,也暂时存放在 RP 上,等待送达接收用户。

每台 RP 基本上承担一个国家的电报处理,所以称为地区处理机,所有的 RP 都在美国和荷兰的两大操作中心内。OC 通过全双工国际数据通信链路与 RP 连接,各成员行则通过国内数据通信链路与 RP 连接。RP 担任的工作类似于网络集线器,成员行的所有进出电文,全部通过 RP 送入或发出。

为进一步提高系统的运行可靠性,在各 RP 之间还设有备用链路。如果主链路出故障,该 RP 通过另一个 RP 连接到某个 OC 上。

5) SWIFT 访问点(SWIFT Access Point, SAP)和远程访问点(Remote SWIFT Access Point, RAP)

SAP 是连接 SWIFT 骨干网 SWIFT Transport Network, STN)的分组交换结点机,它们把 SWIFT 系统的各种处理机(SCP, SP, RP)和遍布世界的 SWIFT 用户连接到 STN 网上。目前,SAP 采用北方电信公司的 DPN1OO 交换机,整个 SWIFT 骨干网有 150 台左右 DPN1OO 交换机(包括备份)。根据入网用户数量和发报量的大小,SAP 的配置不尽相同。除了少数用户数和发报量很大的国家和地区外,多数国家采用远程 SAP 方式(即 RAP),采用一个统计时分多路器,将几个用户连到一个多路器上,通过一条专线连到邻近国家或地区的 SAP 上,这个多路器称为远程 SWIFT 访问点 RAP。

1995 年以前,中国地区的远程 SWIFT 访问点在北京中国银行大楼内,几家商业银行通过一个统计时分多路器,复用一条 9600bps 的卫星线路连接到香港的 SAP 上。20 世纪 90 年代以后,中国 SWIFT 用户和发报量增长很快,原来的 RAP 不能满足需要。1995 年,RAP 升级为中国 SAP,并迁入北京电报大楼内,同时在上海电信局内也设立了同样型号的 DPN100。北京的 SAP 通过卫星线路连接到新加坡的 SAP,上海的 SAP 连接到中国香港的 SAP。北京和上海的 SAP 用 9600bps 的光缆互联公共数据网 CHINAPAC 使用 19200bps 连接北京的 SAP,使国内 SWIFT 用户使用 SWIFT 更加安全可靠。

6) 用户与 SAP 的连接

根据发报量的大小、SAP的位置以及对费用的权衡,用户与 SAP 有 3 种连接方式,即 专线连接、通过公共电话线的拨号连接和通过公共数据网连接。为了增加安全性,避免由 于设在本国的 SAP 出现故障时引起用户通信中断备份线路直接连接某个境外的 SAP。用户 访问 SWIFT 系统需要有一套计算机系统与 SWIFT 系统连接,目前有多家计算机公司开发 运行在多种平台上的 SWIFT 接口软件。

6. SWIFT 的网络结构发展

早期的 SWIFT 电报采用 X.25 协议进行传输,主要提供 FIN、GPA 业务,共有 240 种以上的电文标准供成员使用。FIN 的用户与 SWIFT 或其他用户间交换着标准的格式化报文;

GPA 是普通目标的应用,通过 GPA 可在逻辑终端和 FIN 系统间建立和控制通信,同时也能起始和中断 FIN 会话, GPA 主要处理系统报文,不处理用户间的报文。

面对不断增加的 SWIFT 连接和迅速成长的 FIN 类的报文流量,1997 年 SWIFT 宣布计划开发基于 IP 技术的产品和服务。

2000 年 SWIFT 宣布在信托及支付两方面进军 B2B 领域。在开发新的 XML 标准时,SWIFT 推出了安全 IP 网(Secure IP Network, SIPN)、SWIFTNet Link(一种通过安全 IP 网访问 SWIFTNet 报文服务的软件产品)、SWIFTNet PKI(提供数字签名及支持认证服务的公钥密码技术)、SWIFTNet InterAct、SWIFTNet FileAct。

2002 年,SWIFT 开始对其网络技术进行升级。SWIFTNet 完成了 X.25 到 SIPN 的迁移,它处于公网和 Internet 之外,仅对 SWIFT 会员开放。SWIFTNet 二期也在实施之中,该阶段的主要任务和目的是使用工业标准的(IPublic Key Infrastructure,PK)公钥基础设施技术建立一个单一的安全模式来访问所有的 SWIFTNet 服务,同时引入一种全新的RMA(Relationship Management Ap-plication,关系管理应用)使 SWIFT 的各成员能够更有效地管理他们的客户关系。

2003 年 6 月,SIPN 启用了多供应商模式,即用户可以使用不同的网络供应商提供的网络系统与 SWIFT 系统相连。这些网络系统一端通过主干网访问节点与 SIPN 主干网相连,一端通过 M-CPE 与用户相连,这样用户就可以访问 SWIFTNet,获得相关服务,服务流程如图 4.22 所示。

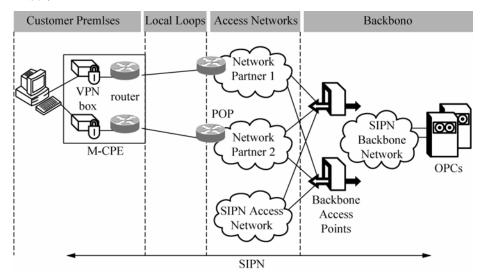


图 4.22 服务流程图

M-CPE 是由 SWIFT 管理的安装在客户端的网络设备,由一个或多个 VPN 盒及一个或多个网络路由器组成。在客户端既可选用适宜高速专网的 M-CPE 与 SWIFT 网络伙伴(Point Of Presence, POP),连接,亦可选用适宜低速用户拨号 Modem 与 SWIFT 网络伙伴的连接。SWIFT 谨慎地选择了一定的网络伙伴供客户连接到 SWIFT,避免了单个网络供应商可能导致的垄断,客户可在多个网络供应商间引入竞争机制,连接使用一个或多个网络供应商的网络。

即付型网络支付方式 第 4 章

新一代 SWIFT 系统是开放的、基于 IP 网络连接方式的 SWIFTNet 系统。其基础架构可分为 4 层,自底向上分别为: SWIFTNet 网络连接层、报文平台层、交易服务专用接口层和业务应用层。SWIFT 更详细的系统架构如图 4.23 所示。

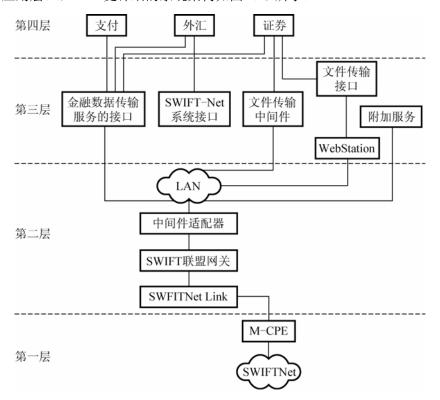


图 4.23 SWIFT 的详细系统架构图

7. SWIFT 的特点

从 1973 年 SWIFT 组织成立至今,该组织已经过了 30 多年的成长,作为国际间结算的平台,SWIFT 系统兼具成熟与可靠的特点。30 多年的实践成就了 SWIFT 的成熟,而其详尽的安全架构使得它非常可靠。

详细地说,SWIFT 有下列几个特点。

1) 格式标准化

具体地说,SWIFT 的标准格式分为两种,一种是基于 FIN 的标准 MTs,另一种是基于 XML 的新标准 MXs。目前,两种标准处于暂时的共存状态。

(1) MTs(Message Type ,MTs 通用表达式为 MTnXX),n(0~9)表示报文类型,XX 表示在n 类型中的分类: Category n-Common Group Messages; Category 1-Customer Payments & Cheques 客户的汇款与支票; Category 2-Financial Institution Transfers 银行头寸调拨; Category 3-Treasury Markets - Foreign Exchange,Money Markets & Derivatives 外汇、货币市场与衍生物; Category 4-Collection & Cash Letters; Category 5-Securities Markets 证券买卖; Category 6-Treasury Markets-Precious Metals; Category 6-Treasury Markets-Syndications; Category 7-Documentary Credits & Guarantees 信用证业务和保函; Category 8-Travellers

Cheques; Category 9–Cash Management & Customer Status 银行账单及报表。上述 10 类信息中应用较多的是第 1、2、3、5、7、9 类型。

(2) MXs: 在 1999 年,SWIFT 组织选择了 XML 编码作为新一代标准,同时决定最终应用新一代以 XML 为基础的标准(MXs),这将是一个漫长的过程,因为它在实现难易程度及需求上都有一定挑战,以至于暂时无法立即替代现有的 FIN 为基础制定的 MTs。这使得MTs、MXs 将有一段意义重大的共存期,这同工业上正在采用的其他共存方法并无差别。

新型的 MXs 标准由 12 类组成,账户管理: acmt.xxx.xxx.xx; 管理: admi.xxx.xxx.xx; 现金管理: camt.xxx.xxx.xx; 支付清分与结算: pacs.xxx.xxx.xx; 支付起始: pain.xxx.xxx.xx; 证券: seev.xxx.xxx.xx; 交易服务管理: tsmt.xxx.xxx.xx; 债券管理: trea.xxx.xxx.xx; 证券交易: setr.xxx.xxx.xx; 证券结算: sese.xxx.xxx.xx; 证券管理: semt.xxx.xxx.xx; 参考日期: reda.xxx.xxx.xx。

(3) MTs 与 MXs 的共存及解决方式:目前,一个两步的方法正在用来评估特定环境下的商业交易以及鉴定究竟如何才能够解决共存现象。

步骤 1: 确保语义的完全。

第一步用来评估现存的标准是否能够提供令人满意的端对端商业交易的支持。这个分析会考虑到账户服务的水平,并由一些特点诸如日期的丰富性、质量及时间等代表。也许这会揭露出漏洞或者矛盾,比如丢失信息或者重复信息。被鉴定出的问题会通过标准的发展解决。自由格式信息、自由文本领域或者独立信息等用来发送丢失信息的工作区会被抑制,因为它们不能够保证兼容 STP,也就是说,在长期来看它们对于用户会意味着更大的成本。

步骤 2: 决定使用的语法(MT 或者是 MX)。

第二步会评估将被商业交易所采用的语法。假如以后的信息一直采用不同的语法,那么互用性及 STP 的弊端带来的风险将日益明显,所以最终的目标就是在每个商业交易领域有唯一的语法。标准发展将会默认采纳执行 XML,除非商业交易只对 MTs 有好感,或者是并没有意愿迁移到 XML。

2) 传送量大、费用低

SWIFT 每日信息传送量很大,为国际间结算提供强有力的支持。SWIFTNet FIN 客户数量统计中,活跃状态国家有 208 个,活跃状态会员为 2264 个,活跃状态附属会员 3224 家,活跃状态参与者 2897 家,总计活跃状态用户数量 8385。

SWIFT 通信费是基于路由和通信量定价的,对通信量多的用户可打折扣,最高可折让50%,对发展中国家则减半收费。SWIFT 每年底还根据经营情况向成员行返还部分(如 20%)收费,并根据其业绩向成员行发放红利。

3) 提高了金融通信和金融机构业务处理的效率

对于金融机构业务处理来说,SWIFT 提供了详细的业务处理记录节省金融机构结算、查账和控制的时间; Transaction Watch 服务为金融机构监视信息传递过程,方便对系统效率的分析; STP Review 向用户提供 STP 评估,提高服务质量。

4) 提供了有效的安全措施和风险管理机制

SWIFT 采取的安全措施主要有:储备系统中心备份,建立了两套独立、完整的设备和线路。日常的系统检测,在访问应用流程方面采取认证、入侵检查、信息流量的控制等。

156

在支付风险管理方面,SWIFT 并不向金融机构提供直接的帮助,但是 SWIFT 向其提供间接的帮助:大额支付和证券交易的清算、结算;净额结算提供 FIN Copy:在交易指令传达给接收方之前,指令要备份并通过第三方(中央银行)的认证。

5) 多元化的服务

SWIFT 的服务对象范围在不断扩大。早期,SWIFT 的会员主要是银行、证券机构等。现在,SWIFT 向大量的金融服务机构提供信息传送和接入服务。而且,SWIFT 正在逐渐地把企业吸收到协会中来,这项措施对企业和会员银行都有利,一方面提高了企业信息传输的效率和安全性;另一方面,会员银行将吸引更多的客户,这会增加信息传输量,从而降低每笔业务的费用,而且可以提供更多种类、更为优质的服务。

SWIFT 从 4 个角度服务金融市场——证券、贸易服务、财政及派生物、支付及资金管理。具体产品及服务包括以下几个方面。

- (1) SWIFT 解决方案: 包括如 SWIFTNet Accord 、SWIFTNet Affirmations 、SWIFTNet Bulk Payments 、SWIFTNet Cash Reporting 、SWIFTNet CLS Third Party Service 等服务。
 - (2) 市场基层设施: 具体分为证券市场及银行市场两方面。
- (3) 信息传递服务:包括 SWIFTNet FIN 、SWIFTNet FileAct、SWIFTNet InterAct、SWIFTNet Browse 等。
 - (4) 接入服务:包括 SPIN、SWIFTNet Link 在内的各种直接与间接接入服务。
- (5) 交互式服务: SWIFTAlliance 系列产品,信息传送方面拥有 SWIFTAlliance Access、SWIFTAlliance Entry;信息交流方面拥有 SWIFTAlliance Gateway、SWIFTAlliance Starter Set; 在桌面操作则有 SWIFTAlliance WebStation、SWIFTAlliance Messenger。
 - (6) 信息产品: 其中包括了 BIC 查询服务等内容。
 - 8. SWIFT 的风险防范

SWIFT 安全威胁来自两个方面:一是支付风险;二是系统风险。

在支付风险方面,SWIFT 并不向金融机构提供直接的帮助。利用 SWIFT 所提供的服务,金融机构可以有效控制支付风险。例如,SWIFT 为支持大额支付及与证券相关交易中的清算、结算、净额结算,提供了 FIN Copy 服务。在交易指令传达给接收方之前,指令要备份并通过第三方(如中央银行)的认证。

1) SWIFT 的安全体系

SWIFT 系统的安全主要遭受这几个方面的威胁:假冒;报文被截取(读取或复制)、修改、重播;报文丢失;报文发送方或接收方否认等。针对这些安全威胁,SWIFT 系统从3个方面设计其安全体系,即进入系统的操作管理场所的物理安全(Physical Security)、系统访问安全(Security of System Access)、报文安全(Message Security)。

(1) 物理安全。SWIFT 使用电子仪器探测系统,保证只有合法的授权人,才可进入系统的"敏感区"。对于远程无人操作地点,在两个系统控制中心(SCC)都有检测器进行监视,对于任何闯入企图,检测器将立即报警。凡要进入访问节点(SAP)的用户,必须通过支持中心(Support Centre)或 SWIFT 技术代理(SWIFT Technical Representatives)向系统申请,并要获得 CIO(Chief Inspector's Office)的同意,才可进入。

- (2) 系统访问安全。进入 SWIFT 系统的 CBT(Computer Based Training),必须经过 LOGIN 操作;进入 FIN 应用环境,要经过 SELECT 操作;凡不能正确完成 LOGIN 和 SELECT 操作的都无法进入系统,而这两个操作都需要口令,只有有权进入该服务系统的人员,才能提供正确的口令。SWIFT 系统的每个 CBT 都有一套自己唯一的口令。
- (3) 报文安全。发送报文的安全。所有 GPA(General Purpose Application)和 FIN(Financial Application)报文,SWIFT 系统都要对其加密,经过加密算法得到的结果 CHK 放在报尾 (Checksum Trailer),每个报文都有唯一的 CHK。网络的输入输出节点还要重新计算 CHK,来验证报文在传送过程中是否有损坏,如果有损坏系统将要求重发报文。
- ① 报文验证。在报文进入片处理器(SP)以前,需要经过地区处理器(RP)的验证,只有符合 SWIFT 标准和语义的报文方可进入系统。
- ② 传递报文安全。接收端收到报文后对其 CHK 重新计算,确认报文是否安全送达,只有正确收到报文后,接收端才向 SWIFT 系统发出正确接收信息 UAK, 否则发出 UNK。如果系统收到 UNK,还需重新传递报文,最多 11 次,如果还是收到 UNK,系统将自动终止传递,并通知发报方报文未被安全送达。
- ③ 用户密押。FIN 用户报文都要用到用户密押对报文加密,只有用户双方知道密押值。 发报方用密押按照公开算法对报文进行加密计算,得到 MAC(Message Authentication Code) 放在 MAC 报尾后,收报方用密押按照相同的算法重新计算,如果算得的 MAC 与报文的 MAC 相同,就可以确认报文在发送途中未被篡改,报文的数据是真实的。SWIFT 系统向 用户提供了密押交换服务 BKE,用户可按照自己的要求互换密押。
 - 2) SWIFT 系统安全策略

针对系统的安全威胁, SWIFT 系统提供了安全策略, 用以维护系统安全。

- (1) 安全登录和选择服务。用户通过 LOGIN/SELECT 功能连接 SWIFT 系统,LOGIN/SELECT 的作用是鉴别和审核 SWIFT 的逻辑终端。这一功能是通过交换一次性的 SESSION KEY 得以完成的。SESSION KEY 原来是通过使用印制在 LOGIN/SELECT 表中的 LOGIN/SELECT 序号和密钥产生,以打印形式传递,需要进行手工处理。读卡器从 IC 中获得密码产生访问代码,这些密码只有 IC 卡和 SWIFT 安全系统知道,在 IC 卡中密码被 固化在内存中,只有 IC 卡自身才可以读出。智能卡技术的使用,使系统连接控制简单化。
- (2) 防止第三方冒充。即通过报文验证代码(MAC)鉴别报文发送方的真实身份,从而准确地鉴别报文的来源,或通过产生一次性的会话密钥确保用户与 SWIFT 系统正常连接。
- (3) 防止第三方截取报文。即防止报文内容被未经授权的人阅读或复制,通过对报文进行加密从而达到内容保密,既使第三方截获报文也难以理解报文内容。
 - (4) 使第三方无法修改、替换报文内容,或者可以发现报文在传输的过程中被修改。
- (5) 防止报文的重播和丢失。通过重复报文报尾 PEMtrailer、传送时限来防止报文重播和丢失。
- (6) 在系统内进行交换的报文被复制存储,与报文交换有关的各种活动及其发生的时间均被记录。
- (7) 相关安全责任的分离,即一人不能负责多项安全事务,即使是系统管理员也不能 一人拥有所有的权限,而是由多个系统管理员分别管理各项功能。

即付型网络支付方式**,**

9. SWIFT 与中国

中国银行作为中国银行业中的第一个 SWIFT 组织成员,于 1983 年 2 月率先加入了 SWIFT 组织,并于 1985 年 5 月 13 日正式开通了 SWIFT,是 SWIFT 组织的第 1034 家成员行,成为我国与国际金融标准接轨的重要里程碑。随后,中国工商银行、中国农业银行、中国建设银行、交通银行、中信实业银行等也相继加入 SWIFT,并利用 SWIFT 系统开展国际金融业务。例如,中国建设银行的快速电子清算系统就是利用 SWIFT Alliance Access 的电子服务系统,通过 SWIFT 组织开发的 PC-Connect 软件与主机相连,为客户间的国际结算提供服务。中国银行的环球收付清算系统以 SWIFT 通信网络为运行环境,与国外代理行计算机系统对接,集收付指令处理及资金清算为一体,把遍布 22 个国家和地区的 554 个海外分支机构连成有机整体,形成一条快捷、安全、高效的资金传递"高速公路"。

2007 年 6 月 7 日,中国银行正式注册加入由 SWIFT 开发的贸易服务设施系统(Trade Services Utilities, TSU)。作为中国银行业中的第一个 SWIFT 组织成员,中国银行的业务专家在包括开发推广"TSU"系统等工作过程中发挥了建设性作用。下一步,中国银行将积极应用"TSU"系统开展供应链管理和融资业务的实践和创新,为广大贸易企业提供优质高效的产品和服务。

SWIFT的优势在于批量支付银行可以将原本需要多次发送的同类报文和文件打包进行一次性的处理,直接进行与清算中心、银行间和企业用户间的直连从而降低运营费用。这对我国金融行业的发展具有借鉴作用。

10. SWIFT 的未来发展

1) SWIFTNet Phase 2 简介

当 SWIFT 协会决定将 FIN 服务从 X.25 迁移到 IP 技术时,二期的设想已经完成。迁移到 SWIFTNet 平台是为了应对 FIN 接入服务,在第二阶段,更加强调安全方面,并推出一种单一安全模型来接入到 SWIFTNet 的各项服务中,为 SWIFT 的严格安全规格而制定的工业标准 PKI(Public Key Infrastructure)技术将保证 Phase 2 的安全性。

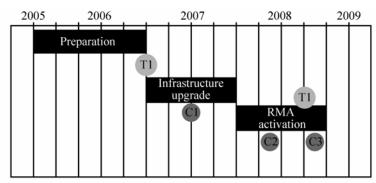
根据 Phase 2 的规划,分为 3 个里程碑阶段: 里程碑 C1 阶段(The Milestone C1)所有用户必须完成基础设备升级 (The Infrastructure Upgrade); 里程碑 C2 阶段(The Milestone C2), 所用于户必须保证愿意接受并使用 RMA 并使其投入运行; 里程碑 C3 阶段(The Milestone C3), 所有用户必须强制使用 RMA (Relationship Management Application)。

在 2008 年 9 月末,客户不再能够使用 BKE (Bilateral Key Exchange)。这也将接近 Phase 2 的完成期。其具体进程如图 4.24 所示。

2) SWIFTNet Phase 2 的特点及优势

相对于现有的 SWIFTNet, Phase 2 的特点如下。

现行的接入 FIN 服务代码(Access code)将会被数字签名(Digital Signatures)所取代。数字签名亦将作为用户对用户的信息认证的基础而被使用,从而替代了现行的通过 Bilaterally Exchanged Keys 产生并认证的 MAC(The Message Authentication Codes)。将会使用新的抗干扰硬件设备,即 Hardware Security Modules,以取代今日所使用的安全读卡器(Secure Card Reader)以及 ICCs。SWFITNet Phase 2 的 FIN 安全网络如图 4.25 所示。



- C1:Customer infrastructure upgrade completed T1:SWIFTNet Release 6 availabilty
- C2:Customer demonstrates live RMA ceadiness T2:End of BKE
- C3:Customer cut-over to RMA completed

图 4.24 SWIFTNet Phase 2 的进程规划

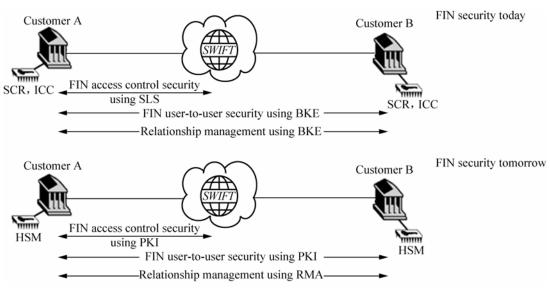


图 4.25 SWIFTNet Phase 2 的 FIN 安全网络

Phase 2 的优势有 5 点。

- (1) 简单化: SWIFTNet PKI 比 BKE 的过程更简便,而且也不再有交换密钥及更新密 钥的必要。
 - (2) 商业驱动: 只有当商业关系发生改变时,通信授权才需要产生改变。
 - (3) 明晰: 商业关系可以比现在通过更详细的线索来界定。
- (4) 更广阔的应用:新的 RMA 可以被所有 SWIFTNet 为基础的用户使用,而不仅仅是 SWIFTNet FIN 用户。
- (5) 运作成本下降: 比 BKE 更加简便操作,新的安全模型将尤其使运转大量业务的客 户获益。

目前要访问 FIN 必须经过安全 LOGIN&SELECT(SLS)处理,所使用的安全设备是读卡 机(SCRs)和 IC 卡(ICCs)。这些设备和技术尽管是安全可靠的,但是在 SWIFTNet 二期完成

即付型网络支付方式 第 4 章

后,SWIFT 成员与 SWIFT 之间的安全依靠 PKI 架构、硬件安全模块 HSMs、IPSec-VPN 保证,成员与成员间,或者说银行始发报方,可以确保报文的完整性和发报方不可抵赖。

经过 SWIFTNet 二期的变化,SWIFT 把安全和客户关系管理提高到了一个新的层次。 RMA 具有如下优点。

- (1) RMA 规避了不必要的交往。通过 RMA,不必要的交往将会在发信者一段被阻止。 不必要的交往有潜在的消极影响,比如调查、旁听以及道德风险等。
- (2) RMA 比 BKE 更简单。RMA 草案比现行的 BKE 机制更加简单。通过 RMA,每 6 至 12 个月的更新授权不再被需要,这样就使得 RMA 的运营比现有需要更少的员工。
- (3) RMA 还可以在 SWIFTNet 上提供关系管理能力。RMA 的目的是给予成员对于自己的 SWIFT 对立方的必要控制,这也是它设计的初衷。RMA 将会与其他在通信交往中需要类似控制等级的 SWIFTNet 服务一同被 SWIFTNet FIN 所使用。
- (4) RMA 还给予通信双方关系更细化的控制。通过 RMA,不仅可以控制谁来接受交流,更可以控制让其接受到什么。对于 FIN,这将意味着可以随意地控制通信的水平,并将其提高到个人信息验证的高度。

PKI 主要用于 FIN 接入控制安全管理(FIN Access Control Security)及 FIN 用户对用户的 通信安全管理(FIN Use-To-User Security)。PKI 优势有如下几点。

- (1) PKI 使 SWIFTNet FIN 的安全水平得到提升。现行的 SWIFTNet FIN 安全机制依赖于 SCRs/BCRs 以及 ICCs,尽管这些读卡器及卡片依旧安全,但是他们正在接近寿命的极限。
- (2) PKI 相较以前的产品更加强大。SWIFT 将会通过引进抗干扰的设备,即HSM(Hardware Security Modules)来加强 PKI 的安全性,以保证 PKI 存储的机密。
- (3) PKI 实行了对于所有 SWIFTNet 服务用户的单一安全机制。SWIFTNet PKI 将替代现行的对于 FIN 的安全机制,因此,推进了面对所用 SWIFTNet 服务的单窗口服务,同时减少了维护两个截然不同的安全模型的操作成本。
- (4) PKI 使得密钥管理更加简便。通过 SWIFTNet PKI,用户只需要管理自己的密钥,也不会有任何与通信者交换密钥的必要(在当今的 BKE 世界中则有这种需要),因此同时减少了不必要的操作及可能的错误带来的风险。

标准格式作为 SWIFT 另一个重点,通过阅读案例 4-4 加以了解并掌握其最新的发展情况。



阅读案例 4-4

2008 年度 SWIFT 标准格式变动要点

2008 年 SWIFT 标准格式升级实施日: 2008 年 11 月 15 日 涉及变动的报文格式有:

MT101.103

MT202.203.205.210

MT300.305.320

MT499

MT535.537.540.541.542.543.544.545.546.547.548.549.564.565.566.567

MT707.734.750.760.767.768.769.799

MT910

MTn95

主要的变动内容如下。

(1) 报文的字符容量增大

例如 MT499.799.707.734.750 的字符数从 2000 个增加到 10000 个; MT734 中的 77J 栏位的行数及字符数由原来的 $40 \times 35x$ 增加到 $70 \times 55x$;

(2) 个别报文格式的 79 栏位允许重复使用

例如 MT499.707.799 的 79 栏位允许重复使用

(3) 个别代码字的变更

例如 MT760 增加了代码字 ISPR,删除了 URCG; 又如 MT734 中的 77B 增加了代码字 NOTIFY 和 PREVINST 等等。

总体而言,2008年的格式变动幅度不是很大。

资料来源: 汇天国际结算网. 2008.

问题:

为什么 SWIFT 的标准格式需要作出这样的变动?

正是由于 SWIFT 的格式具有标准化,目前信用证的格式主要都是用 SWIFT 电文。

4.5.6 纽约清算所银行同业支付系统

1. 简介

CHIPS 是 Clearing House Interbank Payment System 的缩写,是"纽约清算所银行同业支付系统"的简称。纽约是世界上最大的金融中心,国际贸易的支付活动多在此地完成。因此,CHIPS 也就成为世界性的资金调拨系统。现在,世界上 90%以上的外汇交易,是通过 CHIPS 完成的。可以说,CHIPS 是国际贸易资金清算的桥梁,也是欧洲美元供应者进行交易的通道。

20 世纪 60 年代末,鉴于纽约地区资金调拨交易量迅速增加,纽约清算所于 1966 年研究建立 CHIPS 系统,1970 年正式创立。当时,采用联机作业方式,通过清算所的交换中心,同 9 家银行的 42 台终端相连。1982 年时,成员行共有位于纽约地区的银行 100 家,包括纽约当地银行和美国其他地区及外国银行。到 20 世纪 90 年代初,CHIPS 发展为由 12 家核心货币银行组成,有 140 家金融机构加入的资金调拨系统。该系统采用 UnisysAl5 多处理机,有 23 台 CP2000 高性能通信处理机及 BNA 通信网,以处理电子资金转账和清算业务。

CHIPS 的参加银行,除了利用该系统本身调拨资金外,还可接受银行同业往来的付款指示,透过 CHIPS 将资金拨付给指定银行。这种层层代理的清算体制,构成了庞大复杂的国际资金调拨清算网。因此,它的交易量非常巨大,每个营业日终了,中央计算机系统对各参加银行当日的每笔交易进行统计,统计出各参加银行应借或应贷的净金额。中央计算机系统除了要给各参加银行传送当日交易的摘要报告外,并需于当日下午 4:30 后,通过

FEDWIRE 网,将各参加银行应借或应贷的净金额通知纽约区联邦储备银行。纽约区联邦储备银行利用其会员银行的存款准备金账户完成清算。清算完成后,通知 CHIPS,CHIPS 则于当日下午 5:30~6:30,用 1 小时的时间轧平账务。

从上述处理过程可看出,利用 CHIPS 进行国际间的资金转账是很方便的。因此,各国银行在纽约设有分行者,都想加入 CHIPS 系统。面对日益增多的参加银行,为了清算能快速完成,纽约清算所决定,由会员银行利用其在纽约区联邦储备银行的存款准备金账户,代理各参加银行清算。目前,参加清算的银行,除了纽约清算所 12 家会员银行外,另有Bank Of America 及 Continental Bank International 加入,总共 14 家。因此,在 CHIPS 清算体制下,非参加银行可由参加银行代理清算,参加银行又由会员银行代理清算,层层代理,构成了庞大复杂的国际清算网。

CHIPS 日处理交易 28.5 万笔,金额 1.5 万亿美元,平均每笔金额 500 万美元。全球 95% 的美元跨国支付由该系统完成。金融机构可通过 CHIPS 私有 IP 网络或 SWIFTNet 与 CHIPS 连接,支持 ANSI X.12 820、UNEDIFACT、XML 多种消息格式。

CHIPS 直接会员在 CHIPS 开设清算账户,同时在联储银行开设结算账户,CHIPS 自身也在联储银行开设结算账户。CHIPS 进行双边、多边连续轧差清算,日终通过 FEDWIRE 完成结算。

2. CHIPS 系统的参与者

CHIPS 的参加银行主要包括如下 3 类。

- (1) 纽约交换所的会员银行。这类银行在纽约联邦储备银行有存款准备金,具有清算能力,并且都有系统标识码,作为收益银行的清算账号。CHIPS 会员银行的系统标识码用以符号 CP 为开头的 ABA 3 位数字码来标识。
- (2) 纽约交换所非会员银行。这类银行称为参加银行,参加银行需要经过会员银行的协助才能清算。CHIPS 的参加银行,除了利用该系统本身调拨资金外,还可接收往来银行的付款指示,透过 CHIPS 将资金拨付给指定银行。
- (3) 美国其他地区的银行和外国银行。它主要包括美国其他地区设于纽约地区的分支机构,它们具有经营外汇业务的能力;外国银行设于纽约地区的分支机构或代理行,这些外国银行可以选择 CHIPS 会员银行为代理行,参加 CHIPS 同业清算。它们在代理行设定用户识别号 UID 号码,UID 号码以字母 CH 为开头,后面有 6 位数字。

CHIPS 对参与者的要求如下。

- (1) 在每天交易开始前储蓄一定数量的资金。
- (2) 在系统运行时间内,只有参与者当前的资金头寸足以完成借记 CHIPS 才释放支付指令,而且任何参与者当前的资金头寸都不得小于零。
- (3) 需要接受 CHIPCo 的信用评估。CHIPS 参与者需要向 CHIPCo 董事会提交财务情况方面的文件,接受董事会定期问讯。

3. CHIPS 的运作机制

CHIPS 的开通时间,在普通营业日为上午 6:40 至下午 4:40,假日后第一营业日为上午 4:40 至下午 5:00。维持 CHIPS 运作的机制主要有:付款机制、收款机制、风险控制机制、清算机制。

1) 付款机制

CHIPS 中的银行间支付是以代客户付款的银行(即付款行)主动向代客户收款的银行(即收款行)发送付款电信开始的。付款行通过 CHIPS 付款时分 3 个步骤:输入、储存、发报。付款行付款时首先需要把原始付款指示按 CHIPS 规定的付款格式输入专用电路终端,这样付款电流就传输到 CHIPS 中心电脑中,并在中心电脑的数据库储存起来。CHIPS 中心计算机收到付款行付款电信后会立即向付款行发回确认信息,以供付款行验证其输入正确与否。付款电信一般可以提前 4 个工作日储存在 CHIPS 中心计算机中,付款行在起息日当天发出发报指令,发报指令就是付款行对 CHIPS 中心计算机发出的支付款项指令。如果经 CHIPS中心电脑检验,付款金额是在其净借额和双边信用额度以内,CHIPS 中心电脑将把付款电信以付款通知形式传递到收款行,同时给付款行发回确认电。

2) 收款机制

CHIPS 中心计算机根据付款行的发报指令,自动将付款电信以付款通知的形式送到收款行。收款行收到付款通知后,要检验其合格性,并据此作出相应的处理。所谓合格付款是指付款行在其付款格式中的"收款行应贷记的账号的 UID 号、账号或 SWIFT 代码"项目中填入有关内容的付款,否则就认为是不合格付款。对合格付款,收款行可以不做任何加工,计算机自动将款项贷记付款电信指示的有关账户。对不合格付款,收款行根据不同情况,按下列原则处理:①付款行没有提供受益人账户或有关情况,以汇款人作为受益人;②付款摘要提供的应贷记账户的账号与付款电信其他部分提供的内容不一致,以付款摘要栏提供的应贷记账户的账号为准,收款行即可将款项贷记该账户;③如付款电信各部分提供的情况有差异,而收款行不能决定应该贷记的账户时,收款行应向付款行发出查询;④如收款行对不合格付款进行退款,无论金额大小均要使用 CHIPS 规定的退款 UID 号"200111"作成合格付款,并在付款电信中提供原付款电信的序号、付款行客户名称和退款原因等内容。

3) 风险控制机制

CHIPS 由于采用的是日终清算方式, 所以在 CHIPS 每日清算前, 成员银行之间的收付 并无实际货币资产的转移,完全是在信用基础上进行,即付款行向收款行付款实际上是收 款行向付款行提供了信用,也就是收款行在没有收到付款行的实际货币资产支付时就为付 款行垫付款项即向客户支付了款项。这时,就有可能出现信用风险,即清算成员银行可能 由于得到信用过多而在清算时没有足够的准备金偿付其净借额而造成清算失败的风险。对 于信用风险, CHIPS 主要运用事前控制和事后救助的措施, 具体讲: 事前控制就是在清算 前就对付款行得到的信用量加以限制。CHIPS具体采取两种措施,双边信用额度和净借额。 所谓双边信用额度是各成员银行根据对每一个成员银行资信的评定给予对方先付后收的额 度,超过这一额度后,收款行可以拒绝接受付款行的付款。收到拒绝的付款行只能要求对 方增加额度;或者等待对方对本方付款,减少本方付款时的先付后收差额;或者通过其他 清算途径付款。净借额则是指 CHIPS 对每一个成员银行规定的最高收付净欠差额。当成员 银行的收付差额超过该额时,CHIPS 则不再继续接受该成员银行的付款。净借额的计算方 法是成员银行作为付款行得到的其他成员银行当日调整后的双边信用额度总额乘以5%。当 付款行的一笔付款电信的发送会使付款行的实际净借额超过规定的净借额时,CHIPS 就会 拒绝接受发报指令。此时,该付款行只能等其他银行向它付款而将实际净借额降下来;或 者通过其他渠道付款了。所以双边信用额度和净借额分别控制了成员银行从个别银行和全

即付型网络支付方式 第 4 章

体成员银行那里得到的信用量,借此控制信用风险。而事后救助,则主要是指当清算确实出现某家银行清算困难时,所采取的挽救措施。CHIPS 在事后救助上采用了"清算终结"方案,即所有 CHIPS 成员银行签订一个共同分担损失的协议,当一个或数个成员银行不能清算其收寸净借差额时,其他各成员银行提供必要的资金以完成 CHIPS 清算。清算终结方案关于成员银行分担损失的计算公式如下。

ASOi=ND×Cdi/TCd

式中 ASOi—i 成员行对失败成员行收付净借额应承担份额;

ND——失败成员行收付净借额的美元金额;

Cdi——i 成员行给予清算失败成员行当日最高双边信用额度;

TCd——各成员行给予清算失败成员行当日最高双边信用额度。

ASOi 最高不超过各成员银行给予其他任何一家成员银行最大双边信用额度的 5%。为保证终结方案的实施,CHIPS 还要求每一成员银行存放一定数量的抵押品,其价位等于ASOi 的最大值,即最高双边信用额度的 5%。

4) 清算机制

CHIPS 的清算是在其清算成员银行之间进行的。CHIPS 通常以每日下午4:30 作为储存、发报的截止时间。从截止时间起,CHIPS 中心电脑计算各成员银行的收付款净借或净贷差额,并将该情况的报告发送给各成员银行核对,其中对清算成员银行的报告除列有该行本身的收付净额外,还列有该行代为清算的各成员银行收付净额和该行应清算的总收付净额。为清算需要,纽约清算所在纽约联邦储备行开立一个 CHIPS 账户,每日清算开始后账户开始活动,清算结束后账户终止活动。清算分 3 步进行:第一步,核对一致,清算成员行如果对清算净额议,净额为借方的清算成员行向 CHIPS 发送一个"同意付款美元×××"的电信,净额为贷方的清算成员行则向 CHIPS 发送一个"同意收款美元×××"的电信,净额为贷方的清算成员行则向 CHIPS 发送一个"同意收款美元×××"的电信,当清算成员行通过 FEDWIRE 向纽约联邦储备银行拨款,联邦储备银行借记银行账户、贷记 CHIPS 账户;第三步,付款,当清算净额为借方的清算成员银行全部完成拨款后,纽约联邦储备银行从 CHIPS 账户向清算净额为贷方的清算成员行进行付款,该讨款通过直接借记 CHIPS 账户和贷记有关清算成员行在纽约联邦储备银行的账户而完成。付款全部完成后,CHIPS 账户余额为零。如果纽约联邦储备银行对账户余额核对无误,CHIPS 中心电脑则向全体成员银行发送"CHIPS 清算结束"的电信,然后关闭 CHIPS 账户,完成整日的清算。

4. CHIPS 系统的运作流程

应用 CHIPS 系统的资金清算处理过程并不复杂,可把整个流程分为两部分,即第一部分是 CHIPS 电文的发送,第二部分是在实体银行间完成最终的资金清算。

例如,美国境外的某国银行甲(汇款银行)汇一笔美元到美国境外的另一家银行乙(收款银行),则利用 CHIPS 的国际资金调拨流程如图 4.26 所示。



图 4.26 利用 CHIPS 的国际资金调拨流程

- (1) 美国境外的某国银行甲经国际线路,如 SWIFT 网向其在纽约时区的参加 CHIPS 美元清算的成员银行 A 发送电子付款指示,要求 A 行于某日(即生效日)扣其往来账,并将此款拨付给在纽约银行 B 设有往来账号的他国乙银行。美国境外的某国甲行在纽约市区的银行 A 开设有用户识别号 UID 清算账号。
- (2) 纽约市区内的银行 A 收到电文后,核对电文的信息识别码 MAC 无误,即交与终端操作员处理。操作员根据电文,依据纽约清算所规定的标准格式,将有关数据(包括 A 行、B 行、甲行和乙行的编号,付款金额,生效日等)输入计算机终端。该文经 CHIPS 网络传送到 CHIPS 中央计算机系统中存储起来。该中央计算机系统必须接到 A 行稍后下达的"解付"命令后,才将此付款通知传送到开设在纽约市区的另一家 CHIPS 成员银行 B 的计算机终端上。
 - (3) 纽约市区内的 CHIPS 成员银行 B 行通知美国境外的银行乙接收汇款,完成汇款。
- (4) 接着进行日终结算。CHIPS 的成员银行 A,将每天收到的不同的境外委托银行的付款单交给在纽约市内的能够直接进行清算的银行,进行净差额借记清算。
 - (5) 直接进行清算的银行在日终与 FEDWIRE 进行清算。
 - (6) CHIPS 的成员银行 B 要与直接进行清算的银行进行净差额贷记清算。

总之,利用 CHIPS 系统的清算过程,凡是在纽约市内的 CHIPS 的成员银行之内开设了用户识别号 UID 号码的美国境外银行,都可以经过 CHIPS 的成员银行,将资金调拨指示经 CHIPS 美元清算系统支付给另一家接收银行。在进行日终结算时,在纽约市内的 CHIPS 的成员银行,要经过直接进行清算的银行与美国联邦储备局清算系统进行清算。与此同时,在纽约市内的 CHIPS 的成员银行,将代理委托在 CHIPS 成员银行开设了 UID 号码的美国境外银行,全部完成各个银行之间的美元支付,并且通过电子网络将支付结果通知被委托的银行,整个支付过程只需几秒钟。

5. CHIPS 的特点

1) 允许事先存入付款指示

参加银行除了可在当日调拨资金外,CHIPS 还允许参加银行事先将付款指示存入中央计算机系统,然后等到 Value Date(解付日)当日才将此付款通知传送到收款银行。任何资金调拨需经拨款银行下达"解付"命令后,CHIPS 的中央计算机系统才会于解付日将此付款通知传送给收款银行。未下达解付命令前,拨款银行有权取消该笔付款指示。

2) 完善的查询服务功能

由于中央计算机系统能即时将每笔资金调拨情况存入文件,因此各参加行的账务管理员,可随时查询自己银行的每笔提出或存入的金额,并及时调整自己的头寸。

3) 自动化程度高

CHIPS 设计了一个灵活的记录格式,以方便发报行和收报行能进行高效的计算机自动处理。这样,参与行的支付信息可在不同系统之间流动,而无须人工干预。例如,CHIPS 接受 SWIFT 的标识码,并可自动地与 CHIPS 的通用标识码相互参照。

166

4) 安全性好

CHIPS 将 4 台 Unisys Al5 大型计算机组成两套系统,实行两套系统互为备份,每套系统又是双机互为备份。两套系统分别安装在不同的地方,并用高速线路连接。为保证不间断的电源供应,由蓄电池储备,并以双内燃发电机系统保证。

6. 国际资金网络支付运作模式

国际贸易要通过国际电子汇兑系统完成国际资金网络支付。国际汇兑信息通常是通过 SWIFT 系统传输的,而国际资金结算通常是通过 CHIPS 系统来完成的。因此,SWIFT 和 CHIPS 是国际资金调拨的两个最重要的系统。

1) 国际资金网络支付机制

国际网络支付过程的复杂性,随源行(业务发生行)和目标行(业务结束行)之间的关系差别很大。一笔国际电子汇兑过程,往往要经过不同国家多个同业的转手才能完成。但主要应用"SWIFT+CHIPS"配合机制完成,即通信传递用SWIFT,到纽约进行CHIPS同城结算。

2) 国际大额资金网络支付的运作架构

国际大额资金网络支付的运作架构基本以美国目前的批发支付业务处理机制为架构,或类似其架构,如图 4.27 所示。

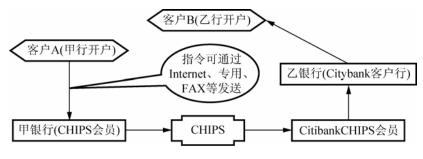


图 4.27 国际支付运作架构

客户通常是公司客户、银行和政府部门。汇兑过程的复杂性,随汇兑方和受益方两者 开户银行之间的相互关系而异,地区性和国内型的电子资金转账,通常只需一两个银行参 与独立完成;国际性的电子资金转账服务,有时需要同业多重转手。

4.5.7 美国联邦储备诵信系统

1. 简介

FEDWIRE(Federal Reserve Settlement System)也称为美国联邦储备通信系统(Federal Reserve Communication System)。FEDWIRE 是美国的第一个国家级电子支付与清算网络系统,也是美国境内最大的资金调拨网络系统。该系统接受和处理各种形式的数字现金、电子信用卡、电子支票,能实时处理客户间的资金转账及大额资金的划拨业务,并可以逐笔清算资金。该系统提供电子支付服务和各种其他支付网络的电子资金划拨服务,还提供大量金融信息服务,是美国可以实现最终清算的网络系统,目前已有1万多家银行参加联网。

FEDWIRE 系统是 1996 年开始酝酿, 1971 年开始建设,至 1976 年才全面应用。目前有 3 个处理中心,分别设在纽约、达拉斯和里斯满。资金传送在纽约处理中心运行,其他

业务在达拉斯和里斯满两地平均分配。3个处理中心之间用高速链路相接,以共享数据和实现互为备份。整个储备银行及其分行通过一个高速通信网连接在一起。每个储备银行都具有资金处理和证券业务处理功能,并都保存有各自的记录。每个地区联邦储备银行的网络将该地区的金融机构与上级银行连接在一起,即整个系统把国家联邦储备银行及其分支机构与国库、其他政府部门、全国1万多家商业银行及其他金融机构连接成一体。

2. FEDWIRE 的功能

FEDWIRE 的功能齐全,可为世界范围内提供资金调拨处理、清算等功能和大额资金支付功能,还具有跨国、跨地区、跨行进行转账、最终清算以及各种金融信息处理功能,也可以为电子商务中的大额资金支付与结算提供服务。

通过 FEDWIRE 系统可以完成多种功能,这主要体现在传送和处理的信息不同上,功能主要有如下 5 种。

- (1) 资金转账功能。即可以将储备账户的资金从一个金融机构划拨到另一个金融机构的户头上,通常这些资金几乎都是大额资金。
 - (2) 传送美国政府和联邦机构的各种证券交易信息。
 - (3) 传送联邦储备局的管理信息和调查研究信息。
 - (4) 完成自动清算业务。
 - (5) 进行批量数据传送。

利用 FEDWIRE 系统进行的资金转账过程,是通过联邦储备成员的联邦储备账户实现的。因此,资金转账的结果将直接影响各个成员行持有的联邦储备账户的储备余额水平。

3. FEDWIRE 的风险管理

FEDWIRE 是美国银行间清算及其他大额资金转移的主渠道。如何在提高支付效率的同时确保系统的安全可靠运行,一直是美联储最为关注的问题。经过几十年的实践和研究,FEDWIRE 不仅保证了系统安全高效地运作,而且还大大提高了服务的质量。以下简要对其风险管理策略及风险管理工具加以介绍。

- 1) 风险管理策略
- (1) 对大额清算系统日间透支的收费。日间透支是指一个金融机构在一个营业日中其储备账户余额为负。日间透支的存在,使美联储面临巨大的信用风险。为了控制金融机构在美联储账户上的当日透支,从 1994 年 4 月开始,美联储对金融机构平均每日透支进行收费。包括由 FEDWIRE 资金转移及记账证券转移两部分产生的合并透支额(在此以前,美联储对记账证券产生的透支不予管理)。其计算方法是对 FEDWIRE 营业时间内,每分钟的最后时间金融机构储备账户的负值加以总计(正值不予计算),再将总透支额除以当日FEDWIRE 运行的总分钟数得到金融机构每日平均透支额。美联储对每日平均透支额减去相当于银行资本的 10%后的部分征收费用。但美联储保留根据市场反映情况对征收标准进行修改的权力,美联储有权加速对金融机构当日透支征收费用的进行,也可以将费用征收标准加以改变。
- (2) 透支上限。透支上限的制定一般以信用度为基础,金融机构除必须每年对自己的财务状况和经营环境做出详细准确的评估外,金融机构本身还必须监督和控制其客户对日

间透支的使用。一般信用度越高,透支上限也就越高,信用度较差的金融机构一般不能得到日间透支。

为限制金融机构在储备账户上当日透支的总量,美联储为透支上限的计算制定了统一的标准。一个金融机构的最大透支额的计算等于该机构一定时间内的平均透支额乘以一个透支类别乘数。美联储为各金融机构设定了5个透支类别。

美联储在设定透支类别乘数时,制定了两种标准:一是两周平均乘数;一是单日平均乘数。美联储认为,由于金融机构的支付活动每天都可能发生波动,因此设定两周平均乘数为金融机构提供较大的灵活性。两周平均透支额的计算根据金融机构在两周内,每天在美储备账户产生的最大透支额加总后除以计算周期内美联储的实际营业天数。如果在计算周期中某天金融机构的储备账户头寸为贷记,则该天金融机构的透支额视同为零。金融机构在两周内的透支上限则等于两周平均透支额乘以透支类别乘数。类似的,单日透支上限等于单日平均透支额乘以透支类别乘数。单日类别乘数要高于两周平均乘数。制定单日透支上限主要是为了控制金融机构在某天中产生过大的透支,迫使金融机构完善内部控制手段,加强对每日信用量的管理。

美联储规定,如果一个金融机构在一个营业日中所产生的当日透支基本上不超过 1000 万美元或不超过该金融机构注册资本的 10%(两个数字中较小的一个),则认为该金融机构对美联储造成的风险较小,无须向美联储提交其自我评定的最大透支上限保证,从而减轻金融机构进行自我评定的负担。

(3) 记账证券交易抵押。美联储对金融机构当日透支的计算是将金融机构的资金转移透支和记账证券转移透支合并计算。对一些财务状况比较健全,但却由于记账证券转移造成超过最大透支额的金融机构,美联储要求它对所有的证券转移透支提供担保。对于抵押品的种类美联储没有特别的要求,但抵押品必须要能够被美联储接受。

风险管理策略一般不要求金融机构对所有的日间透支进行抵押担保。从 2001 年 5 月 30 日起,美联储允许金融机构由于某些原因通过抵押担保申请超过透支上限的透支服务。 另外,对于财务状况欠佳或面临危机的金融机构,美联储要求其必须提供抵押才能进行日间透支。

(4) 对金融机构支付活动的监测。美联储对金融机构支付活动的监测一般在事后进行。如果一个金融机构当日净借记头寸超过其最大透支额,美联储要把该金融机构的负责人召到联储局,与其讨论减少该金融机构当日透支额的措施。美联储有权单方面减少该机构的最大透支额,要求金融机构提供抵押或维持一定的清算余额。对于美联储认为经营不佳并在美联储产生超过正常透支额的金融机构,美联储对其头寸情况进行实时跟踪,如果该机构的账户余额超过美联储认为正常的水平,美联储可以拒绝或延迟对该机构支付命令的处理。

2) 风险管理工具

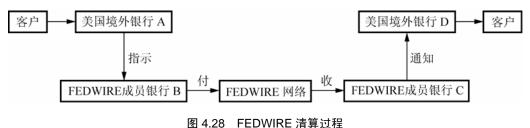
(1) 账户余额监控系统(ABMS)。美联储利用账户余额监控系统对指定机构的支付活动及目间账户余额进行实时监控。被监控的对象主要包括那些被认为会给联邦储备银行带来风险的机构,比如财务状况每况愈下,或存在超额透支历史的金融机构。如果某家金融机构在 ABMS 中被设置为拒绝模式,那么任何超出该机构可用资金的支付要求都会立即被拒绝。只有该机构账户余额满足支付数额时,系统才会进行相应的支付处理。实际上只有少数金融机构被列为拒绝模式,大多数金融机构都可获得超过该机构最大透支额的透支服务。

ABMS 还可以被金融机构用来查询日间账户余额,以及进行日间透支管理。ABMS 可以向金融机构提供日间实时账户信息。此外,ABMS 每天定时收集不通过 FEDWIRE 系统的支付信息,比如通过支票或清算所进行的支付活动。ABMS 系统还可以提供金融机构的期初差额、最大透支额、抵押资产等信息。

- (2) 目间透支报告和定价系统(DORPS)。美联储利用目间透支报告和定价系统,根据支付系统风险管理策略中的事后监督原则,对金融机构的透支活动进行监督,并对目间透支进行定价和费用计算。另外,DORPS 还提供多种事后报告,从而更好地对目间透支进行监督。比如超过透支上限的透支额、每分钟末的账户余额等。
- (3) 风险管理信息系统(RMIS)。风险管理信息系统是基于网络的应用系统。它结合了监督的、金融的,以及其他支持联邦储备局进行风险管理决策的所有的信息,通过 RMIS可以获得金融机构的事后监控信息,使风险管理规则自动化,并为信用和风险的管理决策提供科学先进的分析工具。FEDWIRE 的普通用户一般不能进入 RMIS。

4. FEDWIRE 的清算过程

FEDWIRE 运行时间以美国东部时间为准,每天早上8:30,截止时间跨区下午5:00,区内下午6:00。由于是逐笔清算,系统一般要求付款银行提前半小时提交业务。假设美国境外的某银行A(汇款银行)汇一笔美元到美国境外的另一家银行D(收款银行),FEDWIRE的清算过程如图4.28所示。



- (1) 汇款行 A 发电文指示给在美国境内属于 FEDWIRE 系统成员银行 B,境外银行 A 在美国的银行 B 开设有 FEDWIRE 系统银行的用户识别号(UID 清算账号),即银行 B 是银行 A 的境外美元账户银行。
- (2) 银行B收到美国境外的银行A汇一笔美元到美国境外的另一家银行D的支付指示(电文)后,通过FEDWIRE 美元清算网络系统,将汇款直接调拨给FEDWIRE 系统成员银行C,银行C必须是收款银行D在美国境内的美元账户银行和FEDWIRE 系统成员银行。
 - (3) 银行 C 收到汇款通知单后,立即通知美国境外的收款银行 D 进行接收,完成汇款。

本章小结

即付型网络支付方式是指购买商品或者服务时客户的支付金额从银行账户即时转账商家完成支付,公平性强、网络安全需求高、用户接受性强等是该支付方式的显著特点。

即付型网络支付方式 第4章

本章首先介绍了基于转账的网络支付方式,列举了常见的电子转账支付系统,对即付转账清偿债务、账户划转支付方式的流程进行了阐述。

基于银行卡的网络支付方式是本章的重点内容,比较和分析了基于 SSL 和 SET 协议机制的银行卡网络支付的流程和特点,并对借助第三方代理机构的银行卡支付方式进行介绍。

电子支票网络支付方式分为同行和异行电子支票网络支付两种模式,两者存在较大的差异。在电子支票中运用电子签名等技术保证其支付安全性是这一节的重要内容。

最后,本章介绍了电子汇兑系统,它可分为通信系统、资金调拨系统和清算系统 3 大类。FEDWIRE 是这一节的重点。



即付型网络支付 转账 银行卡支付 SSL SET 电子支票 电子汇兑系统

综合练习

-,	填空题	
	1. 从即付型网络支付方式的特点中,可以看出该支付方式有用户接受性强、_	
	、、、等优势。	
	2. 使用对称加密法、、数字摘要技术、、、等技术是	是银行卡
网络	各支付 SET 模式的特点。	
	3. 为满足电子支票的、、_	(
其中	中电子支票的认证工作是由来完成的。	
	4. 电子汇兑系统,就是以自身的计算机网为依托,为客户提供汇兑、	托收承
付、	、银行承兑汇款、等支付结算服务方式。	
	5. 电子汇兑系统的运作都要经过以下基本作业处理流程:、电文的接	美受、 电
文数	牧据控制、、。	
_,	判断题	
	1. 电子转账支付的实质是存款在账户间的移动。	()
	2. 在基于 SSL 协议机制的银行卡网络支付中各方需要下载安装证实身份的数字	字证书。
		()
	3. 借助第三方代理机构的银行卡支付中,当第三方代理机构不是发卡行本身,	则持卡
人自	的银行卡账号信息将会在网上传递。	()
	4. 电子支票通过互联网传递, 收款银行收到电子支票后, 通过自动清算所网络	来交换。
		()
	5. 电子汇兑系统的主要用户是社会大众。	()

三、选择题

1. 以下()网络支付方式具有最强的公平性。

A. 预付型

B. 即付型

C. 后付型

D. 移动

2. 在即付型网络支付方式中,使用的银行卡一般是()。

A. 借记卡

B. 贷记卡

C. 狭义的信用卡

D. 会员卡

3. 支付效率较低,成本较高,但具有一定支付安全性的银行卡支付模式是(

A. 无安全措施的支付模式

B. 借助第三方代理机构的支付模式

C. 基于 SSL 协议机制的支付模式 D. 借助 SET 协议机制的支付模式

4. 以下不属于电子支票网络支付特点的是()。

A. 节省时间

B. 有效减少在途资金

C. 降低处理成本

D. 相比传统支票安全性差

5. 以下不属于电子支票支付系统的是()。

A. NetCheque

B. NetBill

C. FEDWIRE

D. Netchex

四、简答题

1. 简述即付型网络支付方式的特点。

2. SSL 协议在运行过程中可以分为哪几个阶段?

3. 简述银行卡网络支付 SET 模式的工作流程。

4. 简述同行电子支票网络支付与异行电子支票网络支付方式的异同。

5. 简述电子汇兑系统的类型。

实际操作训练

熟悉国内常用的银行卡,并申请开通银行卡的网络银行功能。用该银行卡完成实际的 网络支付, 描述支付过程, 并谈谈你对该过程的体验感受, 支付过程是否有待完善的地方。

案例分析

- 1. 根据分析案例 1 所提供的资料, 试分析以下问题。
- (1) 银行卡由磁条卡向 IC 卡方向转变的前景。
- (2) 基于银行卡的网络支付方式存在哪些安全隐患。

即付型网络支付方式 第 4 章



磁条银行卡升级为IC卡,中央银行开始试点

近日,一种复制储户银行卡、冒领储户存款的新型犯罪形式开始在福州、杭州等地出现。不法分子通过在银行 ATM 机上安装自制窃密装置,窃取储户银行卡信息、密码后,"克隆"银行卡冒领储户银行存款。仅去年上半年,福州市发生"克隆"银行卡窃取卡内资金的案件达 33 起,涉案金额数十万元。

不少市民提出质疑: 既然目前的磁条银行卡那么容易就能被复制,有没有更先进的卡? 事实上,目前在欧美等发达国家,人们的银行卡大多是 IC 卡。相比磁条卡, IC 卡由于增加了读写保护和数据加密保护,在使用保护上采取个人密码、卡与读写器双向认证、芯片卡复制难度极高,具备很强的抗攻击能力,很难被复制和伪造。

目前国内银行卡向 IC 卡过渡进程较慢,主要是成本的原因:银行卡升级为 IC 卡,发卡系统、受理系统、终端系统都要投入巨额资金进行技术升级改造,目前最便宜的 IC 卡一张也要 10 多元成本,此外一旦升级为 IC 卡,还存在现有磁条卡与 IC 卡并行使用的过渡期问题,所以,磁条卡向 IC 卡转变不可能一蹴而就。目前,宁波正在推广的市民卡,就带有金融应用功能,除了日常支付功能的"电子钱包"外,还可以直接到 ATM 上取现,让市民卡具有金融功能,目前宁波是央行批准的唯一试点城市。

资料来源: 广州日报. 2009-03-02.

- 2. 根据分析案例 2 所提供的资料, 试分析以下问题。
- (1) 发展手机移动即时支付方式最大的挑战与困难是什么?
- (2) 中国现在发展移动即时支付的时机是否已成熟?
- (3) 除了手机与信用卡结合的模式外,能否提出新的可行模式?



移动商务手机:新技术带来即使支付功能

在韩国等市场,可支付手机已逐渐取代传统付费电话,被普遍应用于餐馆买单、家庭购物、购买地铁票或自动售货机中的饮料等交易活动中,成为了一种新的移动即时支付模式时尚。电信分析师 O-JOO KwOn 感叹道: "模式又一次发生了转变。过去我们曾预测现金将被信用卡所取代,而现在,从技术角度讲,蜂窝电话便可以实现即时支付功能。"

"手机支付"服务在韩国的推出是主要电信服务提供商与信用卡公司通力合作的结果。同时,由于韩国率先采用了 CDMA 移动电话技术,因而一跃成为了移动通信领域的领导者。

SKT 成功开发了支付终端,以支持移动商务功能。其公关部门表示,到目前为止全国已有 40 万个商家购买了具有该功能的终端,截止到 2004 年 4 月, SKT 已经向市场投放了 150 万部支持移动商务的手机,并计划在年底使 MONETA 手机供应量增加到 400 万。根据移动交易这一服务不断增长的趋势,SKT 预计今年其用户中将有 200 万人体验这种移动金融服务。

希望使用移动商务服务的韩国客户需要在发放 IC 芯片(处理信用卡功能)的信用卡公司进行注册,并购买一部采用 CDMA 芯片组支持移动商务的手机。然后,客户就可以将 IC 芯片自由插入或取出其移动商务手机。

Visa 韩国公司总裁 YC Kim 最近向媒体宣布: "随着信用卡业务的开展与 IT 行业的关系日益紧密,由当地创业公司开发的信用卡相关技术通过 Visa 进行了标准化处理,这种手机移动即时支付方式将广泛

应用于全球各地,对经济产生的影响也日益突出。"

资料来源:解放日报网,http://news.xinhuanet.com.

- 3. 根据分析案例 3 所提供的资料, 试分析以下问题。
- (1) 案例中的电子支付工具您用过哪几种,哪一个体验较好。
- (2) 第三方支付平台在即付型网络支付方式中的作用。
- (3) 电子支付市场是否饱和,若没有,其他独立的第三方支付平台如何走差异化路线来扩大自身市场份额。



电子支付网站影响力排行榜 Top10

网站		总分	品牌影响力	市场认可度	联系方式(供参考)
1	支付宝	98.9	54.6	44.3	0571-26885188
2	财付通	91.1	47.8	43.3	0755-86013388-84157
3	银联电子支付	88.6	45.5	43.1	021-52504528
4	快钱	83.0	47.1	35.9	021-58776399
5	网银在线	84.1	43.9	40.2	010-62698686
6	环迅支付	79.9	44.6	35.3	021-62263829-2004
7	易支付	85.1	40.3	44.8	010-82652626-6631
8	YeePay 易宝支付	75.1	39.9	35.2	010-59017500
9	云网支付	73.4	38.9	34.5	010-82888778-2
10	易达信动	68.3	35.6	32.7	010-51667407

市场认可度,包括两部分,一是用户对该支付产品的兴趣和认可程度,包括产品主观评价、访问量、访问频繁度;二是指市场占有率等,主要来源于用户问卷调查、市场公开数据(公司财报、市场份额研究报告、年交易额),总分55分;品牌影响力,品牌本身在市场上的影响力度,主要来源于品牌活动的投入及频繁度、品牌知名度,总分45分。

伴随着电子商务和银行增值业务的推动,中国的电子支付产业经历了一轮疯狂的野蛮生长,在市场的淘汰机制下,原来遍地开花的电子支付企业,到 2009 年已经相对集中。原来无序、野蛮的发展阶段,如今正在逐渐呈现一个成熟、份额集中的电子支付生态圈。

目前存在的电子支付公司基本上都是经历了一轮激烈的市场淘汰战之后存活下来的,可划分为两种不同的阵营:一是从总公司业务中衍生出来、得以发展壮大的,有支付宝、财付通、银联电子支付;二是独立的第三方支付平台如快钱等。支付宝、财付通、银联电子支付、快钱这4家公司基本上垄断了目前70%以上的电子支付市场份额。而其他的独立的第三方电子支付平台份额相对较小,都是试图拓展新的支付市场空间,走差异化路线来生存。

依附于淘宝网的高速成长和阿里巴巴的支撑,支付宝名列国内电子支付影响力榜首。但近年来支付宝已经不再满足于淘宝网的成长,正加强与其他电子商务网站的合作和扩展海外市场,其日益深化的信用体系也增强了在用户心目中的地位; 财付通依托于腾讯网络游戏业务和拍拍网的业务而高速增长; 而银联电子支付的优势在于有着中国银联的官方背景作为依托,用户基础比较大; 快钱作为独立的第三方支付平台提供了多样化的支付解决方案, 2009年2月份与贝宝(Paypal)达成战略合作,开始拓展海外市场。

资料来源: 互联网周刊, 2009-07-07.