文章编号：1000-8608(2013)02-0298-08

基于预信任与公共服务域的柔性在线移动支付模式与协议

王红新*，杨德礼，王建军，马 慧

（大连理工大学 管理与经济学部，辽宁 大连 116024）

摘要：为动态适应电子商务不断创新以及客户对跨支付平台、跨支付方式的个性化需求，移动支付必须具备架构上的柔性与服务的柔性.为此，提出一种基于预信任与公共服务域的柔性在线移动支付模式，它支持支付系统架构的动态变化，支持跨平台支付服务，以线下信任与线上信任相结合以及依托公共服务域的办法解决支付系统的柔性问题，解决柔性与安全性之间的矛盾，并给出了该模式下的支付协议.通过对协议的分析，证明该模式与协议可以满足移动支付的柔性与安全性.

关键词：支付系统柔性；预信任；公共服务域；移动支付协议；支付安全

中图分类号：N945.2 **文献标志码：**A

0 引 言

支付服务最大的难点是安全问题[1].在不断创新的电子商务环境中，支付服务的另一难点是柔性问题.柔性是互联网环境下对E-服务的特别要求[2]，但同样是安全与信任问题，使支付服务成为开放性服务的雷区，成为互联网服务中几乎唯一缺乏柔性的服务领域.

柔性涉及两个方面.一是支付系统本身架构的柔性.随着电子商务的发展，会有更多新的服务模式或服务中介诞生，如果支付系统不具备架构的柔性，在新的中介服务增加或旧的服务中介撤离时就不能很好地适应，将面临大的系统修改甚至被淘汰.二是服务的柔性.电子商务的发展一定是朝着更便利客户，给客户最大选择自由度的方向发展.客户会在不同的交易场合（时间、地点、心情、交易对象），不同的账户状况（资金余额、积分折扣）下有意愿地选择不同的银行（或其他支付平台）与支付方式来进行结算，未来的系统必须能满足这种需求[3].这就需要系统与系统之间可以方便地柔性地转换.

传统支付系统以及现有的移动支付系统大都缺乏柔性，总是各建各的基础设施、银行网关、支付流程与协议，系统的骨干架构是固定的，支付流程与支付信息的传递路径也是固定的.这种刚性的、相对封闭的模式带来系统与系统之间难以通用、难以协调，资源难以共享，支付服务难以柔性适应日新月异的商务创新与发展等问题.

不少研究提出了支付系统的柔性问题，指出这是支付系统发展的方向与趋势[4-5].解决柔性的最好方法是模块化，分解系统并使各部分之间去耦，使之可以很好地柔性重组[6-7].一些研究曾在支付系统的柔性方面作出努力[7-10]，力图找到一种通用的支付模式，但它们大多局限于商户与客户的可扩展方面，多以一个通用的接口模块覆盖不同的终端（商户、客户），系统的骨干架构是不变的，支付信息的传递路径也是不变的；文献[11]指出过程虚拟化对认证需求较高时线下认证的必要性；文献[3、12]给出柔性的跨多个系统与多种支付方式的方案，但局限于多个MNO之间，且是客户单方在线的.目前还没有看到支付系统架构（或信息传递路径）柔性且交易双方在线的支付模式方面的研究.

支付系统架构的柔性牵涉信任与安全问题，这也许正是这种柔性迟迟未得到解决的重要原因.当架构是固定的，架构骨干间的信任关系容易

收稿日期：2011-12-08； **修回日期：**2013-01-24.
基金项目：国家自然科学基金资助项目（重大项目 70890080，70890083）.
作者简介：王红新*（1954-），女，博士生，高级工程师，E-mail：wanghongx@263.net；杨德礼（1939-），男，教授，博士生导师.

建立，而柔性架构就需要有新的认证方法与建立信任的方法.

文献[13]在对大量现有的互联网支付系统、移动支付系统以及中国国家现代化支付系统(CNAPS)研究的基础上，提出了一种基于预信任与公共服务域的柔性在线移动支付模式(flexible on-line mobile payment model based on pre-trust and p-pervice-domain system)，简称为 FMPTS.

定义预信任为本次在线支付发生之前，交易各方预先建立的信任关系，主要指在现实世界中商户(产品或服务提供商)、商区(商业平台)及其他各中间服务商、支付服务商之间建立的信任关系(不包括客户与商户之间). 这个关系可以经实地考察、当面实物认证(证件、证书、印鉴、纸质合同等)、双方合作实践建立. 这个信任关系最终以电子证书的方式预存在这些相互认证与信任实体的服务器中. 而公共服务域指一国或一个区域的银行间支付清算系统加公共支付数据服务，在现实生活中，这个域已经或正在一些国家建立起来(如欧盟的 SEMOPS[14-15]，中国的 CNAPS、CUPN[13]，美国的 ACH[16]).

FMPTS 充分应用预信任以及分层认证模型来解决支付信息在广袤的互联网中跨平台传递问题，应用公共服务域解决用户对所有银行、多种支付方式的跨行服务需求及支付安全问题. 支付信息的传递路径不是固定的，而是可以按每次交易对支付的具体需求在商务信任关系中动态重建，即它是柔性的. 客户与商户可以根据自己的需求与信任选择不同的支付平台与支付服务商. 相应的 FMPTS 协议采用多种安全方案与技术，强调线上与线下认证的结合，在协议中体现交易的不可抵赖性，可追踪性，可满足支付服务灵活性与安全性需求.

1　基于预信任与公共服务域的柔性在线移动支付模式

1.1　模式的目标

模式的目标为使移动互联网环境下的在线支付活动具有最大的柔性，即通过移动设备

(1)任一客户可以与任一商户构成交易与支付关系；

(2)客户可以选择任何偏好的支付服务商(银行或某个第三方支付)，选择任何偏好的支付方式，即满足跨平台支付服务柔性；

(3)形成的支付信息可以通过不同的传递路径传递到不同的支付执行机构，即允许传递路径中随时加入新的传递者或减少某个传递者，也即可以满足支付架构的柔性；

(4)满足支付系统必需的 5 个安全标准，并有很好的全过程监督机制与争议解决机制.

1.2　FMPTS 基本架构

FMPTS 基本架构如图 1 所示. 其中：A 为手机客户(付款人)；B 为商户(收款人)，可以是任意产品或服务供应商；BCOM 为商区或社区，即 B 所在的商业平台；TPP 为有资质的非银行第三方支付平台：这里的有资质，是指经权威机构认证的具有良好信誉与所需能力的第三方支付服务机构，在中国即经央行批准的非银行支付机构；PDS 为支付数据服务中心，提供银行账户寻址服务，即可根据用户手机号、商户 ID(或名称)与各银行账号的绑定关系，将用户手机号及商户 ID 转换成真正的银行账户信息，如账号、账户名等；CBP 为跨行支付平台，可联通所有银行的银行间支付与清算平台；CAP 为证书与密钥发行平台，提供第三方可信的证书发行与基于身份密码方案的密钥发放；SMP 为争议管理平台，接受争议解决申请，调用在 TPP 与 PDS 存贮的交易证据送专门的仲裁机构；OIM 为其他中间代理，可以是一个或多个，它是可变化的，也是可包容各种电子商务创新服务的部分. 支付系统的柔性主要针对这一部分，当然也包括其他各部分的关联关系与关联方式的可变性.

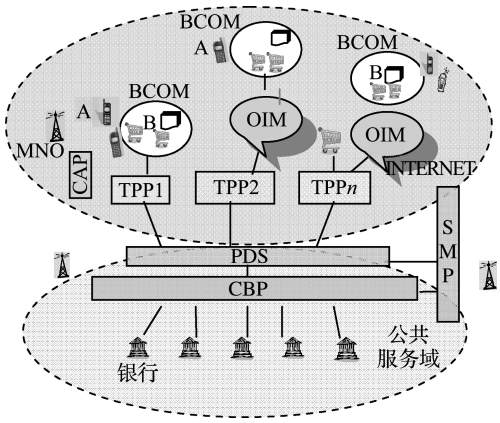

图 1　FMPTS 基本框架

Fig. 1　The basic structure of FMPTS

整个架构将移动支付分成互联网域与支付公共服务域PA.支付公共服务域由PDS、CBP及所有的银行组成,构成支付服务云.公共服务域参考了SEMOPS[14-15]的架构.只是不再要求客户与商户直接与自己的开户银行连接,而是可以通过各种中介去间接与之相联,为互联网上的商务创新与支付创新留下充分空间.

1.3 实现目标的主要方法

支付处理分为支付的产生、确认,支付的发送,支付的清算与结算[16].以此作参照,要实现柔性支付模式也包括3个方面,即柔性需求的产生、确认;载有柔性需求的支付指令的柔性传递;载有柔性需求的支付指令的执行.

柔性需求的产生、确认可通过移动设备浏览器,通过交易双方协商过程标准化与协商结果标准化解决[3,12],如通过通用购物车软件或支付指令生成软件来记录并提取用户跨支付平台与支付方式的选择,形成标准格式支付信息(订单与支付指令)送到TPP或PA;而第三方面:执行,只要支付信息正确传递到相应的支付处理机构,就可由该支付机构完成;柔性问题最难实现的是第二方面:传递.跨平台服务必然带来支付指令传递终点的动态变化,采用不同中介服务将引起传递路径的变化,这时需采用新的机制来解决.

(1)以预信任与分层认证支持支付指令的柔性传递

预信任如引言中定义.支付指令生成后只在有预信任关系的节点中传递,这些节点之间有预先约定的共享会话密钥及对方的签名公钥甚至对方的IP地址.每步传递先由信息接收者认证信息来源,而后根据本次传递的最终方向来选择与自己有预信任关系的后一级节点进行传递.传递的路径与参与者是柔性的,如图2所示(图中虚线表示可能的选择.中间服务平台与第三方支付服务中的节点构成预信任集,IB表示付款行,AB代表收款行).

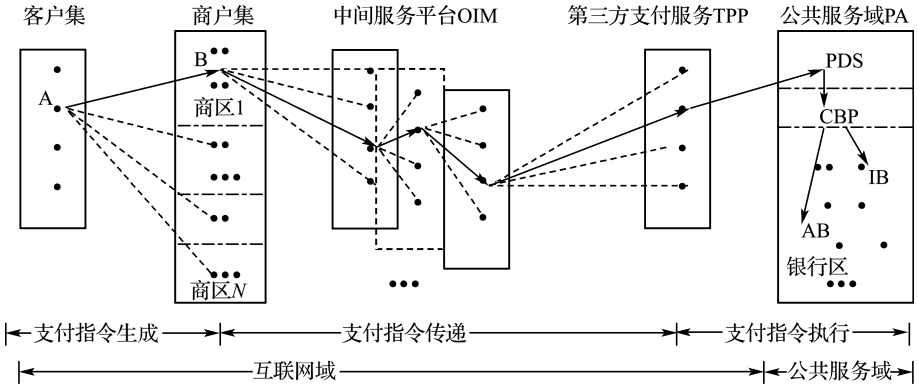

图2 支付信息传递路径

Fig. 2 The transfer path of payment information

这种柔性传递除满足传递路径的柔性(打破各支付系统封闭的传递框架)外,还可以结合实际存在的商务分层结构形成支付系统认证空间逐级缩小的结构,每个后一级节点只对信任圈中的前一级节点认证且搜索空间逐级缩小.如商区对所属商户进行认证,中介对所接入的商区认证,TPP对各种中介服务认证,最终使PA中的PDS只需对有资质的TPP进行认证(一百多个),大大减轻了PDS的接入压力与认证压力,达到安全可控的效果.

线下认证(预信任)使网络交易不再显得虚无缥缈,可以将真实空间与虚拟空间对应起来,用户一旦选择了商户,整个后续的搜索空间就变得有限与清晰.虽然支付链上(如图3)TPP_i之前各方的连接是在互联网虚拟空间,用户与商户之间又不存在预信任关系,但由于商户是处在一个有预信任关系的信任链条中,后续的各传递点也处在这个信任链条中,支付发生时容易相互识别,各方的行为也可受到信任链的相互制约,使网络交易安全有了保障.

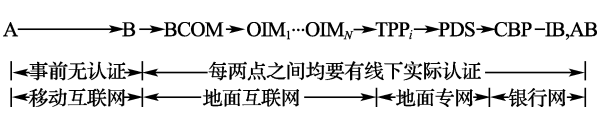

图3 FMPTS支付链举例

Fig. 3 The example of FMPTS payment chain

与没有预信任关系的线上认证相比，有预信任的线上认证有很大优势. 一是由于信任关系的预存省去了证书传递及追溯证书链的步骤，使线上认证得到简化；二是可更好地避免证书失效问题.

(2) 以公共服务域支持跨银行支付指令的传递与执行并保证支付安全

公共服务域的设立为跨银行服务提供了最大的便利. 只要将载有选择不同银行、不同支付方式的支付指令送到 PA，则无论选择了哪一个银行、哪一种支付方式都可以得到有效的传递与执行. PDS 的设立既可使互联网域中不必传递银行账号等敏感信息(利于保密，便于用户操作)，又使每个商户的收款账户处于可监控状态(只有经银行或 PDS 现场认证的商户才可在 PDS 注册，只有注册的商户才能得到银行系统的支付服务，且每次支付都会在 PDS 留下记录)，配合相应的措施，以有效防范商业诈骗.

建立国家级的公共服务域还因其公信力带来系统的可信性与可接受性[9,17]，使支付协议与流程的设计得到最大程度的简化. 统一的支付数据服务可以保证数据的一致性，资源共享性，可监测性.

(3) 采用多种安全模式与技术

如盲签名[18]、基于身份的密码方案[19]、订单与支付指令分别打包并捆绑、不可信前提下的传递机制[20-21]、支付授权与支付指令分路分时、在传递中生成与保留支付证据[22-23]等方法保证模式满足支付系统必需的 5 个安全标准，即可认证性、授权性、完整性、保密性、不可否认性[9,24].

2　支付流程与协议

以手机网络购物为例说明支付流程与协议.

2.1　基本符号表示

本文结合采用文献[21,25]等协议的形式化描述和分析方法，即

X：主体 X.

M：主体间发送的消息.

K_X：主体 X 的公钥.

K_X^{-1}：与 K_X 对应的私钥.

$[M]_K$：用密钥 K 对 M 进行非对称加密后的密文.

$sign_X(M)$：用 X 的私钥对消息 M 进行数字签名. 这表示完成下述过程：X 用自己的私钥对 M 的摘要(哈希函数 $H(M)$)进行加密.

$verify_X(sign_X(M))$：用 X 的公钥对 X 的签名验证，是签名的反过程. 这表示完成下述过程：用 X 的公钥解密 $sign_X(M)$，得到 M 的哈希值 $H(M)$；再对原始信息 M 取哈希值得到 $H'(M)$，如果 $H(M)$ 与 $H'(M)$ 相等，则说明数据传输正确并且信息确实是由 X 发来的.

$evid(M)$：将 M 作为证据，等于 $[F,M]_{KA}$. 其中 $F=[sign_B(M)]_{KA^{-1}}$，是 A 与 B 的双签名. 用 KA 加密 F 与 M，使之被封装起来，传递与存贮中不能被任一方打开，只有争议时在 A 的参与下才可以打开.

$K_X[M]$：用 X 的公钥对 M 解密.

$store[X]_Y$：在 Y 节点存储信息 X.

PPO：初始支付指令，$PPO=\{NO;ANM;BID;PID;SUM\}$.

其中 NO 为交易编号；ANM 为付款人 A 的手机号；BID 是收款人-商户的唯一标识；PID 为用户 A 所选择的，要完成付款任务的支付服务机构 ID；SUM 为支付金额.

PX：客户订单(本文也指其他商务合约)，$PX=\{NO;CNAME;CINF;CP;CNUM;ANM;BID\}$.

其中 $CNAME$ 为商品名称；$CINF$ 为商品信息，如外观、型号、品牌等；CP 为商品单价；$CNUM$ 为商品数量；NO、ANM、BID 含义同上. 商品可以是多种.

PPI：银行可执行支付指令，$PPI=\{IN;RN;SUM\}$.

其中 IN = 付款人银行账号；RN = 收款人银行账号；SUM 同上.

以上 PPO 与 PX 中的 NO 相同，保证两者的关联性. NO 为 PPO 生成时刻的函数.

协议假定：对移动用户 A 的认证采用基于身份 ID 的密码算法[19]，即各商户可以根据用户的手机号及标识生成用户 A 的公钥；用户 SIM 卡存有用户自己的私钥(而不必存贮任何客户账号与银行证书等敏感信息)；用户与 SIM 卡绑定，与手机号绑定(不是与手机设备绑定)；手机制造商或运营商有技术措施保证 SIM 卡的唯一性、不可复

制性，保证 SIM 卡中的密钥不可非法读出.

2.2 流程

(1) 客户 A 在手机上与商户 B 的网页交互，形成订单. 决定支付时，在选择支付机构与账户(用别名) 后，按下支付确定键.

(2) 商户网页接收支付确认，生成 PX 与 PPO，分别签名后送 A. 同时向 A 送出 TPP 的公钥(非银行支付下 TPP 由用户选择，否则由 B 选择).

(3) A 解密、验证并核对(PX 与 PPO 将在移动设备上显示出来)，确认则对 PX 进行 $evid$ 操作，加密 PPO'($PPO' = [sign_A(PPO), sign_B(PPO), PPO]$) 构成加密信封，再与 PX 证据一起用 TPP 公钥加密构成二级加密信封，签名后送 B；否则不签名，选择修改，交易再开始回到第(1) 步.

手机存贮 PPO，可用于以后对银行支付通知的自动核对.

(4) B 验证是 A 所发，将信封盲签名后转发商区 BCOM. B 同时向 BCOM 发送 ID_{TPP}，对后续整个传递链提示传递目标；发送自己的标识 BID，便于支付机构对盲传递信息的验证(防止手机端对收款人的更改).

(5) BCOM 验证 B，将 B 的信息盲签名后转发到自己信任的，且可以有路径到达 TPP 的节点 OIM_1.

(6) OIM_1 验证 BCOM，而后将信息盲签名传递到自己信任的下一个有路径到达 TPP 的 OIM_2，依此类推，每一次传递都是后一节点验证前一节点，然后签名后向再后一级传递，依此类推.

(7) 最后一个中介 OIM_N 将信息传递到 TPP. TPP 验证 OIM_N，存储 $evid$(PX) 作为交易的证据，以备后用. 当 Y = TPP 则转入支付程序并保存 PPO'，验证 BID，否则进入下一步.

(8) 进入银行支付，加编支付指令序号 PN，以备信息反馈.

(9) PDS 验证 PPO 中的 BID 是否与传送来的 BID 相同(不同则中止支付)；根据 NO 进行重放检验；需要时(大额交易或特别交易) 将商户信息送 CAP 审核；将 PPO 转换为正式支付指令 PPI；将 BID(在付款行提示用户 A 授权时用) 与 PPI、PN 送 CBP；PPO' 备份留存 PDS.

(10)…

整个流程及协议的信息流如图 4 所示.

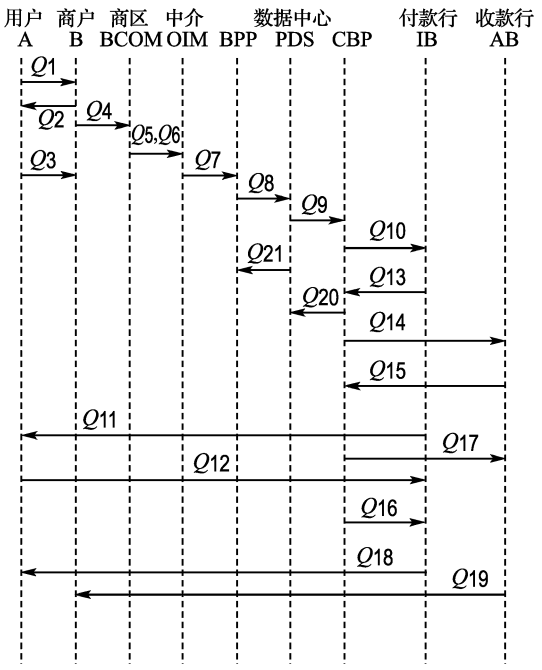

图 4 协议信息流图

Fig. 4 The flow graph of protocol information

从第 10 步开始是 CBP 及银行之间的支付处理过程(即支付指令的执行阶段，充分利用原来 CNAPS 中的功能，如图 4 中的 Q10、Q13 ～ Q17 所示) 以及银行与客户、商户之间的交互过程(Q11、Q12、Q18 ～ Q21). 其中两点很重要：

一是付款行 IB 在执行付款指令前必须向付款人 A 要求授权(要求密码及支付确认，Q11、Q12)；这个过程通过用户与开户机构直接的安全通道(如短信、微信或 WAP)，而不是原来的支付指令传递路径.

二是支付完成后由消费者 A 的开户行 IB 向 A 及时反馈支付情况(Q18、短信等)，商户 B 的开户行 AB 向 B 及时反馈收款情况(Q19、短信等). 同时由 CBP 向 PDS，再由 PDS 向 TPP 反馈支付完成情况以备后用(Q20、Q21).

2.3 协议描述

(1) A → B：Q1. A 确定好购物车内容，决定支付.

(2) B → A：$Q2 = [sign_B(PX), sign_B(PPO), KB, KC, PX, PPO, KTPP]_{KA}$. // 银行支付时

$KC = KPDS$，非银行支付时 $KC = 0$

(3)A → B：$Q3 = [sign_A(Q3'), Q3']_{KB}$，其中 $Q3' = [evid(PX), Y, [PPO']_{KY}]_{KTPP}$. // 当银行支付时，Y = PDS；当非银行支付时，Y = TPP

(4)B → BCOM：$Q4 = [sign_B(Q3'), Q3', BID, ID_{TPP}]_{KBCOM}$

(5)BCOM → OIM_1：$Q5 = [sign_{BCOM}(Q3'), Q3', BID, ID_{TPP}]_{KOIM1}$

(6)OIM_1 → OIM_2：$Q6 = [sign_{OIM1}(Q3'), Q3', BID, ID_{TPP}]_{KOIM2}$，…

(7)OIM_N → TPP：$Q7 = [sign_{OIMN}(Q3'), Q3', BID]_{KTPP}$. $store[evid(PX)]_{TPP}$

(8)TPP→PDS：$Q8=[sign_{KTPP}([PPO']_{KY}), [PPO']_{KY}, BID, PN]_{KPDS}$，$store[PPO']_{PDS}$. // 此时 $KY = KPDS$

(9)PDS → CBP：$Q9 = (PPI, BID, PN)$

(10)…

协议中，PDS 与 CBP 及银行间的认证采用 CNAPS 的认证方法.

当交易双方有异议，可向 SMP 平台申请争议解决.

在以上流程中，客户 A 的各银行付款账户以及商户 B 的收款账户均需预先在 PDS 柜台或银行柜台进行认证与注册. 商户可通过 MNO 所提供的通用服务获取手机号.

3　性能分析

主要从 2.1 中的柔性目标与安全性目标角度进行分析.

3.1　满足柔性目标

(1)支付信息传递路径与传递终点是可变的、柔性的，可以满足客户对不同支付平台的跨平台服务需求.

(2)支付信息传递过程中可以随时加入新的中介与代理，可以满足支付系统架构的柔性，可适应电子商务创新的需求.

(3)可满足支付方式选择的柔性. 模式使互联网域的所有支付活动只是支付信息的生成与传递，只要生成的支付信息足够丰富(设不同支付方式标志)，就可以使支付信息到达执行区(TPP 或 PA)后实现足够丰富的支付方式.

3.2　满足安全性目标

以一个购买飞机票的案例对协议进行检验、模拟，证明协议可以实现安全性目标.

(1)保密性：商户只能看到客户的手机号，看不到账号，更看不到也接收不到客户密码(密码与支付信息分时分路传递)；订单只有客户商户可见，银行看不到；银行账号只有 PA 域可见；其他中间传递机构无论对订单还是支付指令都既看不到也不可能修改.

(2)完整性：信息的整个传递过程采用了数字签名，而对数字签名验证本身就保证了信息的完整性. 因为有 $verify_X(sign_X(M))$ 成立当且仅当 $KX[sign_X(M)] = H(X)$，若信息传递中完整性出了问题(篡改或丢失)，签名的验证也一定不成功.

(3)可认证性：线下信任关系与分层认证机制以及线上的逐级签名认证保证了商户、各中间服务商、TPP 与银行之间的可认证性. 对客户的认证通过手机与账户的绑定关系以及支付时的授权(口令)认证.

(4)授权：虽然为了简化客户操作，每次支付发起时并不要求客户注册，但每笔支付实现的最后时刻，支付机构必然通过直接安全通道要求客户授权，要求密码，保证了支付安全.

(5)不可否认性：由于支付信息产生、传递的每一步都有数字签名，所有参与主体的行为都可追溯，都能区分责任. 另外，SMP 的设置、订单证据 $evid(PX)$ 在 TPP 的保留、支付发起证据 PPO' 及支付结果数据在支付机构的保留可保证争议发生时的可追溯性. 例如：当 B 否认错发了货品(质量、数量与订单不符)，客户 A 可向 SMP 申请调出在 TPP 的订单证据，即：

$[[sign_B(PX)]_{KA-1}, PX]_{KA}$ → arbitrator

仲裁者在 A 的配合下解密，而后验证 $KA[[sign_B(PX)]_{KA-1}] = [H(PX)]_{KB}$ 是否成立，如果成立，仲裁者可以将得到的订单 PX 与 A 收到的货单进行核对，证明 A 的申述是否正确.

4　结论与展望

本文提出了新的柔性移动支付模式——FMPTS，通过采用预信任下的分层认证模型及公共服务域使模式有较好的柔性，可以支持移动支付架构的变化及用户跨平台服务需求. 对支付系统资源共享、统一测控、标准化与开放性也做出有

益探索.

与现有的其他移动支付模式研究相比,本文的主要特点如下:

(1)提出了支付系统架构的柔性问题.给出预信任定义,并以线上线下信任相结合的方案解决移动支付指令的柔性传递问题.

(2)提出公共支付服务域 PA 的思路与方案,以解决跨银行支付问题及支付资源共享问题.

(3)综合运用各种安全技术解决支付指令传递中的认证(包括跨平台认证)与安全问题,并使认证程序得到简化.

模式还存在一些局限性,如手机资源的局限性要求手机认证程序与签名加密算法足够安全且简单高效,但现在还未进行多种方案严谨比较以得到最佳方案.另外,在跨行、跨平台柔性系统方案的基础上,对于支付资源共享的各方合作关系及利益分配机制也将是进一步研究的方向.

参考文献:

[1] Dahlberg T, Mallat N, Ondrus J, *et al*. Past, present and future of mobile payments research: a literature review [J]. **Electronic Commerce Research and Applications**, 2008, **7**(2): 165-181.

[2] Kim D J, Agrawal M, Jayaraman B, *et al*. A comparison of B2B e-service solutions [J]. **Communications of the ACM**, 2003, **46**(12): 317-324.

[3] Huitema G, Kühne R, Meyer U, *et al*. Compensation: Architecture for supporting dynamicity and negotiation in accounting, charging and billing [J]. **Computer Communications**, 2010, **33**(15): 1823-1833.

[4] Kreyer N, Pousttchi K, Turowski K. Mobile payment procedures: scope and characteristics [J]. **E-Service Journal**, 2003, **2**(3): 7-22.

[5] Karnouskos S, Kauffman R J, Lawrence E P. Key guest editorial: research advances for the mobile payments arena [J]. **Electronic Commerce Research and Applications**, 2008, **7**(2): 137-140.

[6] Peffers K, Tuunanen T. Planning for IS applications: a practical, information theoretical method and case study in mobile financial services [J]. **Information and Management**, 2005, **42**(3): 483-501.

[7] Fischer M, Gall H, Manfred H. TUV-1841-2002-53 towards a generalized payment model for Internet services technical [R]. Vienna: Technical University of Vienna, 2002.

[8] Chong C, Chua H N, Lee C S. Towards flexible mobile payment via mediator-based service model [C] // **Proceedings of the 8th International Conference on Electronic Commerce**. New York: ACM, 2006: 295-301.

[9] Kousaridas A, Parissis G, Apostolopoulos T. An open financial services architecture based on the use of intelligent mobile devices [J]. **Electronic Commerce Research and Applications**, 2008, **7**(2): 232-246.

[10] Peiro J, Asokan N, Steiner M, *et al*. Designing a generic payment service [J]. **IBM Systems Journal**, 1998, **37**(1): 72-88.

[11] Overby E. Process virtualization theory and the impact of information technology [J]. **Organization Science**, 2008, **19**(2): 277-291.

[12] Bhushan B, Hall J, Kurtansky P, *et al*. OSS functions for flexible charging and billing of mobile services in a federated environment integrated network management [C]// **Proceedings of the 9th IFIP/IEEE International Symposium, IM 2005**. Berlin: IEEE, 2005: 717-730.

[13] 中国人民银行支付结算司. 中国支付系统发展报告[M]. 北京:中国金融出版社, 2007.
Department of Payment and Settlement, People's Bank of China. **China Payment System Development Report** [M]. Beijing: China Finance Publishing House, 2007. (in Chinese)

[14] Karnouskos S, Vilmos A, Hoepner P, *et al*. Secure mobile payment-architecture and business model of SEMOPS [C] // **European Institute for Research and Strategic Summit**. Heidelberg: Spinger, 2003: 1-8.

[15] Karnouskos S, Hondroudaki A, Vilmos A, *et al*. Security, trust and privacy in the secure mobile payment service [C]// **Proceedings of the 3rd International Conference on Mobile Business**. New York: ICMB, 2004: 1-8.

[16] 苏 宁. 支付系统比较研究[M]. 北京:中国金融出版社, 2005
SU Ning. **Payment System Comparison Research**

[M]. Beijing: China Finance Publishing House, 2005. (in Chinese)

[17] Changsu K, Wang T, Namchul S, *et al*. An empirical study of customers' perceptions of security and trust in e-payment systems [J]. **Electronic Commerce Research and Applications**, 2010, **9**(1): 84-95.

[18] Fan Chun-i, Liang Yu-kuang. Anonymous fair transaction protocols based on electronic cash [J]. **International Journal of Electronic Commerce**, 2008, **13**(1):131-151.

[19] LIN P, CHEN H Y, FANG Y, *et al*. A secure mobile electronic payment architecture platform for wireless mobile networks [J]. **IEEE Transactions on Wireless Communications**, 2008, **7**(7):2705-2713.

[20] Carbonell M, Sierra J M, Lope Z J. Secure multiparty payment with an intermediary entity [J]. **Computers and Security**, 2009, **28**(5):289-300.

[21] Kungpisdan S. Accountability in centralized payment environments [C] // **Proceedings of the 9th International Symposium on Communications and Information Technology**. Piscataway: IEEE, 2009: 1022-1027.

[22] Ou C M, Ou C R. SETNR/A: An agent-based secure payment protocol for mobile commerce [J]. **International Journal of Intelligent Information and Database Systems**, 2010, **4**(3):212-226.

[23] SUN Jin-yuan, ZHANG Chi, ZHANG Yan-chao, *et al*. SAT: A security architecture achieving anonymity and traceability in wireless mesh networks [J]. **IEEE Transactions on Dependable and Secure Computing**, 2011, **8**(2):295-307.

[24] Martinez P R, Rico N F J, Satizabal C. Study of mobile payment protocols and its performance evaluation on mobile devices [J]. **International Journal of Information Technology and Management**, 2010, **9**(3):337-356.

[25] Marko H, Konstantin H, Elena T. Utilizing national public-key infrastructure in mobile payment systems [J]. **Electronic Commerce Research and Applications**, 2008, **7**(2):214-231.

A flexible on-line mobile payment model and protocol based on pre-trust and p-service-domain

WANG Hong-xin*, YANG De-li, WANG Jian-jun, MA hui

(Faculty of Management and Economics, Dalian University of Technology, Dalian 116024, China)

Abstract: To adapt to electronic business innovation and customer's personalized demand of cross payment platform and cross payment mode dynamically, mobile payment must have the structure and service flexibility. So a model of flexible on-line payment is introduced based on pre-trust and public service domain (p-service-domain). The model supports the dynamic change of payment system framework and cross-platform payment service, and solves the flexibility problem by the combination of offline-trust, on-line-trust and p-service-domain. Meanwhile, the conflict of flexibility and security is also solved by the model. Furthermore, a payment protocol is given according to the proposed model. As the same time the flexibility and security of the model and protocol are also met by protocol analysis.

Key words: payment system flexibility; pre-trust; public service domain (p-service-domain); mobile payment protocol; payment security