YD

中华人民共和国通信行业标准

YD/T 1035—2000

基于IP网络的事务处理业务技术规范

IP Network – Based Technology Standards for Transaction Process

2000-01-07 发布　　2000-04-01 实施

中华人民共和国信息产业部　发布

目　　次

前　　言

本标准主要根据 RFC959、RFC2068、RFC1825 等草案和 ITU-T X.509 等相关标准制定。

国内 Internet（IP 网络）的发展日趋成熟，网上开展的各种业务越来越多，从广义上来看，其中很多业务都可以归入事务处理业务范畴。为保证 Internet 网上事务处理业务的顺利开展，根据我国的实际情况制定本标准。

本标准所规定的事务处理业务是基于我国 IP 网络的电子商务业务的一部分，即电子商务业务中的非支付型业务和不直接涉及银行支付的支付型业务。有关电子商务的内容另行规定。

本标准主要着眼于制定基于我国 IP 网络的事务处理业务的基础框架结构，内容包括事务处理业务所涉及到的安全平台和支付平台（不直接涉及银行）；全文规范了事务处理业务的应用范围，制定事务处理业务的基本实现流程；规范事务处理业务中可能用到的不直接涉及银行的支付技术；规范事务处理业务的身份认证技术、数据传输的安全技术；规范事务处理业务中涉及到的证书使用和证书认证中心的建立与管理；并以预付卡、在线订购、在线股票查询及交易、公文传送等几种典型业务为例，对事务处理业务的具体实施模式进行了介绍，供业务实施部门参考。

本标准所定义的事务处理业务适用于联入中国 Internet 网的用于各种事务处理的服务器、用户终端和其他设备。用户终端可以采用能够联入 Internet 网进行事务处理的各类设备，包括微型计算机、网络计算机、Web TV、工作站以及各种专用终端等。

鉴于基于 Internet 网的事务处理业务涉及的技术范围十分广泛，Internet 技术的发展又非常迅速，因此本标准还需随着技术和应用的发展不断补充和完善。

附录 A~附录 E 是提示的附录。

本标准由信息产业部电信研究院提出并归口。

本标准起草单位：信息产业部电信研究院新业务开发研究中心
广东省邮电科学研究院
信息产业部数据通信科学技术研究所
原邮电部电信科学技术研究院多媒体中心
湖南省信息产业局

起草人：刘辛越　刘　进　杨涛海　蒋林涛　任伟权　孙登峰　陈方煜

中华人民共和国通信行业标准

基于 IP 网络的事务处理业务技术规范

YD/T 1035—2000

IP Network-Based Technology Standards for Transaction Process

1 范围

本标准基于我国 Internet 网（IP 网络）制定了事务处理业务的应用范围、事务处理业务的实现流程；规范了事务处理业务中涉及到的支付技术、事务处理业务的身份认证技术、数据传输的安全技术；规范了事务处理业务中涉及到的证书认证中心的建立与管理；并以预付卡、在线订购、在线股票查询及交易、公文传送等几种典型业务为例，对事务处理业务的具体实施模式进行了规范。

本标准适用于在中国 Internet 网上开展事务处理应用，是我国 Internet 网上事务处理业务的组织、规划、工程设计和业务实施的技术依据。

2 引用标准

下列标准所包含的条文，通过在本标准中的引用而构成为本标准的条文。在本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

ITU-T X.509 (1993.11) 关于认证框架的介绍 Information technology-open systems Interconnection the directory: authentication framework

3 缩略语

CA	Certificate Authority	认证中心
CCTV	Closed-Circuit Television	闭路电视
CRL	Certificate Revocation List	证书作废表
E-Mail	Electronic Mail	电子邮件
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
ID	Identifier	个人标识符
IP	Internet Protocol	网际协议
ITU	International Telecommunication Union	国际电联
MIME	Multipurpose Internet Mail Extension	多用途的网际邮件扩充协议
MPTP	Micro Payment Transfer Protocol	小额支付传输协议
MTBF	Mean Time Between Failures	平均故障间隔时间
MTTR	Mean Time To Repair	平均修复时间

中华人民共和国信息产业部 2000-01-07 发布　　2000-04-01 实施

SET	Secure Electronic Transaction	安全电子交易
SMTP	Simple Message Transfer Protocol	简单邮件传输协议
SSL	Secure Socket Layer	安全套接层
TCP	Transfer Control Protocol	传输控制协议
UPS	Uninterrupt Power System	不间断电源
WWW	World Wide Web	万维网
CL	Client	客户
WS	Web Server	Web 服务器
AS	Access Server	接入服务器

4 定义及应用领域

4.1 定义

4.1.1 事务处理(Transaction Process)

事务处理是一种双向业务，它是指终端和其他设备进行的一次数据交换，它允许事务处理发起者发送一个特定的请求，去激发事务处理响应者的某一动作予以响应。

本规范所涉及的事务处理业务是指基于 Internet 网，面向在 Internet 网上提供和接受服务的政府、企业、商家及个人用户，采用相关的 Internet/Intranet 技术，提供在线服务的业务。

本规范中的事务处理业务是基于 Internet 网的电子商务业务的一部分，包括电子商务业务中的非支付型业务和不直接涉及银行的支付型业务。有关电子商务的内容另行规定。

4.1.2 事务处理请求(Transaction Process Request)

事务处理请求是指事务处理流程中一次主动的消息发送，它用来向对方申请某种服务，或只简单地通知对方。一个完整的事务处理应由一个或多个事务处理请求及相应的事务处理响应组成。

4.1.3 事务处理响应(Transaction Process Response)

事务处理响应是相对于事务处理请求而言的，对于申请服务的请求，它按要求提供所需的服务；对于通知而言，它只是在接收到请求后做相应的处理，不一定要求回复。

4.1.4 事务处理发起者(Transaction Process Requester)

事务处理发起者是指发送事务处理请求消息的一方。

4.1.5 事务处理响应者(Transaction Process Responsor)

事务处理响应者是指接收事务处理请求消息的一方。

4.1.6 身份认证(Identity Authenticate)

身份认证是指对事务处理参与方的身份进行鉴别，以防止非合法用户的参与以及假冒他人参与事务处理的行为。

4.1.7 信息认证(Information Authenticate)

信息认证是指对信息的真实性进行鉴别，确保信息的发送者与信息中所声称的发送者是一致的。信息认证用以防止欺诈行为。

4.1.8 安全通道(Security Channel)

安全通道是指能安全分发密钥的方式，包括各种各样的人工方式，如密钥使用者亲自领取密钥等，还包括各种各样的在线方式，如安全邮件等。

4.1.9 公钥数据库(Public Key Database)

公钥数据库是一种分发公钥的方式。把公钥放在安全的数据库中，数据库的访问是需要授权的。

4.1.10 数字证书(Digital Certificate)

数字证书是一种分发公钥的方式。数字证书中包含了用户的公钥和一些用户信息及签发数字证书的 CA 的签名数字证书。用户的数字证书要向 CA 中心申请，CA 中心确认用户的身份后为用户签发证书。只有信任 CA 中心才可以信任该中心签发的数字证书。

4.1.11 CA 认证中心(CA Center)

签发数字证书和管理数字证书的机构。该机构应该是权威机构，应该得到公众的信任。

4.1.12 保密模块(Cryptographic Module)

保密模块是保证用户的密钥安全的软件、硬件设备或软件和硬件的结合产品。用户访问密钥前，应先被保密模块认证其身份，确认身份后才能访问密钥。

4.1.13 单向散列函数(Hash)

把不同长度的数据块经过一系列的计算生成固定长度的信息，两个不同的数据块生成相同的信息在计算上是不可行的，并且函数是不可逆的。

4.1.14 实体(Entity)

实体是指参与事务处理的具体实物，可以是应用程序、个人、服务程序等。

4.1.15 请求认证者(Authenticate Requester)

参与认证过程的，需要被认证身份的实体。

4.1.16 认证者(Authenticator)

参与认证过程的，对请求认证者的身份进行认证的实体。

4.1.17 认证发起者(Authenticate Initiator)

参与双方实体认证过程的，发起认证的实体。

4.1.18 认证响应者(Authenticate Responsor)

参与双方实体认证过程的，对认证发起者的认证请求进行响应的实体。

4.1.19 认证挑战(Authenticate Challenge)

在使用公开密钥签名算法的认证中，由认证者产生的，发给请求认证者的一段信息。请求认证者需要使用自己的私钥对其签名，以响应认证者的挑战。认证者发出的认证挑战是不可以重复的。认证挑战一般是一个随机数。

4.1.20 认证响应(Authenticate Response)

在使用公开密钥签名算法的认证中，请求认证者对认证者发来的认证挑战使用自己的私钥签名后得到认证响应，因为私钥是只有请求认证者才有的，因此认证者通过验证认证响应可以确认请求认证者的身份。

4.1.21 认证挑战及响应(Authenticate Challenge and Response)

认证挑战及响应是在使用公开密钥签名算法的双向实体认证中，认证发起者对认证响应者发来的认证挑战生成认证响应后，再生成对认证响应者的认证挑战。把该认证响应和认证挑战合在一起称为认证挑战及响应。

4.1.22 数字货币(Digital Money)

数字货币是由货币发行方发行，经货币发行方数字签名的一串串随机数，并且这些随机数与现实生活中的货币一一对应。

4.2 应用领域

基于中国 Internet 网络的事务处理业务包括以下应用领域：

1) 企业、商家之间的事务处理应用。如：企业、商家之间及其各自之间的订购业务，原材料及商品批发业务，房地产买卖业务等；

2) 企业和商家对个人用户的事务处理应用。如：在线娱乐服务、在线订购和购物（参见附录 A、B 和 C）、在线金融交易服务（参见附录 D）、在线教育和培训等；

3) 政府部门与企业、商家和个人用户之间的事务处理应用。这类业务涉及政府部门向其他各类用户提供的服务，如企业、商家、个人的报税、纳税，政府对企业和商家的财务报表审核，为各类用户提供各类在线申请业务，政府在线项目招标等；

4) 政府部门之间的事务处理应用。如政府各级部门之间的公文传递，政府所需的各种统计资料及其他数据资料的传递等（参见附录E）。

5 业务分类

对事务处理业务可以从很多角度进行分类，如可以从事务处理业务所涉及到的实体是两方、三方还是多方来分；可以从业务是交易型业务还是非交易型业务来分；可以从不同的事务处理业务对安全级别的不同要求来分等。本章从身份认证流程对事务处理业务进行分类。

身份认证模式一般分为对参与实体的身份认证（即实体认证）和对信息自身的身份认证（即信息认证）。实体认证是对各参与实体的身份进行认证，它又分为单方认证、双方认证和多方认证。因此，根据认证模式和对安全的要求，将事务处理业务分为如下5类。

5.1 不需要身份认证的事务处理业务

不需要身份认证的事务处理业务是指在整个事务处理过程中，对参与事务处理各方的身份没有特殊要求，不需要对其身份进行认证，也不需要对信息本身进行认证。

此类事务处理主要针对那些对安全没有特别要求的、一般性的或公益性的业务，如网上广告、网上保健查询、网上大赛、免费的网上教学以及普通的电子邮件等。

5.2 需要信息认证的事务处理业务

需要信息认证的事务处理业务是指在事务处理过程中，对参与事务处理的实体的身份没有特殊要求，在进行事务处理前无需对他们的身份进行认证，但在接收到信息后必须对信息的真实性和可靠性进行认证。其认证方式往往是在信息中包含相应的认证信息，只有认证成功的信息才被接受。

此类事务处理主要针对不需要对参与方的身份进行认证、只需要保证信息的正确性和可靠性的情况，如数字货币等。

5.3 需要单方身份认证的事务处理业务

需要单方身份认证的事务处理业务是指在整个事务处理过程中，对参与事务处理各方中某一方的身份有特殊要求，在进行事务处理前需要对该参与方的身份进行认证。只有认证成功，该参与方才能参与此类事务处理。

此类事务处理主要包括对安全有一定的要求、需要对参与方中的某一方的身份进行认证的业务，如邮件跟踪、基于SSL协议的网上购物、报税、股票交易等。

5.4 需要双方身份认证的事务处理业务

需要双方身份认证的事务处理业务是指在整个事务处理过程中，对参与事务处理双方的身份有特殊要求，在进行事务处理前需要对参与双方的身份进行认证。只有认证成功的实体才能参与此类事务处理。

此类事务主要包括那些对安全有较高的要求、需要对参与双方都要进行身份认证的业务，如为政府高层领导服务的具有保密要求的信息服务、企业间的机密信息传递等。

5.5 需要多方身份认证的事务处理业务

需要多方身份认证的事务处理业务是指在整个事务处理过程中，参与事务处理的实体多于两个，而且至少对其中三方的身份有特殊要求，在进行事务处理前需要对他们的身份进行认证。只有认证成功的实体才能参与此类事务处理。

此类事务处理主要包括那些参与方较多、对安全有较高的要求、需要对参与各方都要进行身份认证的业务，如基于SET协议的电子交易、需要多个政府部门审批的报关等。

6 事务处理基本流程

本事务处理流程所基于的传输协议应为 HTTP、SMTP、MIME 及其他基于 TCP/IP 的传输协议。

6.1 不需要身份认证的事务处理基本流程

6.1.1 基本流程

在本事务处理基本流程中，事务处理发起者可以根据需要确定是否需要等待事务处理的响应消息。如果需要，事务处理响应者在事务处理完毕后必须向事务处理发起者回送相应的响应消息。否则，事务处理发起者在发起事务请求后即认为该事务处理结束，事务处理响应者可以自行决定是否执行该事务处理。基本流程如图 1 所示。

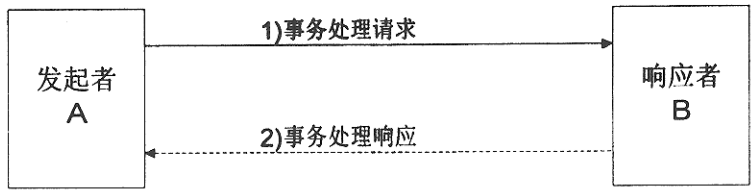


图 1 不需身份认证的事务处理流程

1) 事务处理发起者 A 选择事务处理的另一方（即响应者 B），并向 B 发送事务处理请求。

2) 事务处理的响应者 B 决定继续或终止事务处理。

a) 如果它决定继续事务处理，则应按照事务处理请求处理相应的事务，也可选用地在事务处理完毕后向发起者 A 回送相应的响应信息。

b) 如果它决定终止该事务处理，则应抛弃该事务处理请求，也可选用地向发起者 A 发送相应的终止事务处理的响应消息，应包含终止该事务处理的理由。

6.1.2 附加规定

1) 对于一般的事务处理均应包含事务处理响应消息，但对某些事务处理，如通过电子邮件散发广告等，也可以忽略事务处理响应消息。

2) 对该类各种具体的事务处理业务，其处理流程应由上述流程组合而成。而且，在一个完整的事务处理业务流程中，事务处理的发起者和响应者的地位允许改变，具体情况应随各具体业务需要而定。

6.2 需要对信息进行认证的事务处理基本流程

6.2.1 基本流程

在此类事务处理基本流程中，没有独立的认证流程，认证与事务处理是同时进行的。在需要认证的事务处理请求包中包含数据信息本身及用来对数据信息进行认证的认证信息。接收方在接收到此类信息后，首先根据其中的认证信息检查数据信息的合法性，然后根据检查结果决定采用或拒绝该信息。在处理完该事务后，根据需要，决定是否返回响应消息。基本流程如图 2 所示。

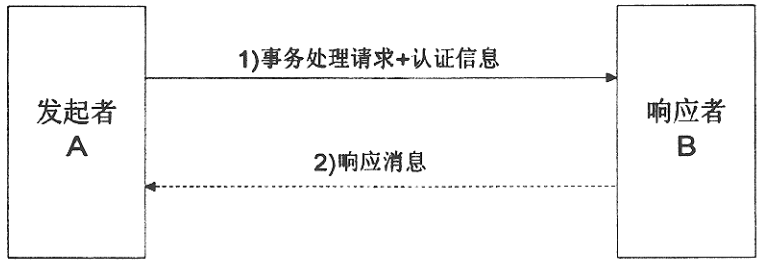


图 2 需要对信息进行认证的事务处理流程

1) 事务处理发起者 A 选择事务处理的另一方（即响应者 B），并向 B 发送事务处理请求。

a) 事务处理发起者 A 准备事务处理请求数据。

b) 事务处理发起者 A 根据需要认证的数据部分准备认证信息。

c) 事务处理发起者 A 将事务处理请求数据和认证信息联结起来作为一个完整的事务处理请求包发送给事务处理的响应者 B。

2) 事务处理的响应者 B 决定是继续还是终止事务处理。如果它决定继续事务处理，则进行以下操作：

a) 根据请求包中的数据及认证信息对事务处理请求的有效性进行检查。

b) 如果认证成功，则按事务处理请求处理相应的事务。

c) 也可选用地在处理完相应的事务后向事务处理发起者 A 发送相应的响应消息。

6.2.2 附加规定

1) 对于一般的事务处理均应包含事务处理响应消息，如果某些事务处理有特殊需要，也可以忽略事务处理响应消息。

2) 认证信息的生成可以使用数字签名或其他技术，如电子现金需要使用数字签名，具体的认证技术和加密技术参见第 8 章。

3) 如果事务处理需要保密，则对发送的消息应采用对称密钥加密算法进行加密。对称加密密钥的传递可采用数字信封或其他方法，具体情况参见第 8 章。

6.3 需要单方身份认证的事务处理基本流程

需要单方身份认证的事务处理基本流程包含两种认证模式：对事务处理发起者的身份认证和对事务处理响应者的身份认证。

在本事务处理基本流程中，事务处理发起者可以根据需要确定是否需要等待事务处理的响应消息。如果需要，事务处理响应者在事务处理完毕后必须向事务处理发起者回送相应的响应消息；否则，事务处理发起者在发起事务请求后即认为该事务处理结束，事务处理响应者可以自行决定是否执行该事务处理。

6.3.1 需要对事务处理响应者身份进行认证的事务处理基本流程

6.3.1.1 基本流程

需要对事务处理响应者身份进行认证的事务处理是指在事务处理请求中包含敏感信息，只能发给特定的响应者。因此，在发送事务处理请求前，要首先对响应者的身份进行认证，认证成功后才发送事务处理请求。基本流程如图 3 所示。

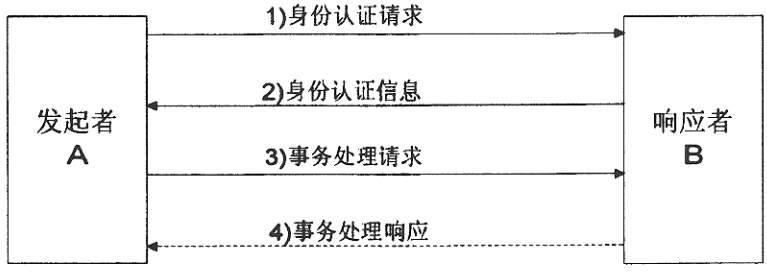


图 3 需要对事务处理响应者身份进行认证的事务处理流程

1) 事务处理发起者 A 选择事务处理的另一方（即响应者 B），向它发送身份认证请求。

2) 事务处理响应者 B 决定继续或终止身份认证信息交换。如果它决定继续认证过程，则向发起者 A 传送身份认证信息。

3) 事务处理发起者 A 在对事务处理响应者的身份进行认证后决定继续或终止进一步的事务处理。如果认证成功，而且决定继续事务处理过程，则向事务处理响应者 B 发送事务处理请求。

4) 事务处理的响应者 B 决定继续或终止事务处理。

a) 如果它决定继续事务处理，则应按事务处理请求处理相应的事务，也可选用地在事务处理完毕后向发起者 A 回送相应的响应信息。响应消息中应包含事务处理的执行结果。

b) 如果它决定终止该事务处理，则应抛弃该事务处理请求，也可选用地向发起者 A 回送相应的响应信息。响应消息中应包含终止该事务处理的原因。

6.3.1.2 附加规定

1) 对于一般的事务处理均应包含事务处理响应消息，如果某些事务处理有特殊需要，也可以忽略事务处理响应消息。

2) 认证方式可以根据业务要求使用数字签名或其他技术，如：基于 SSL 协议的网上购物、报税、股票交易等应至少使用口令字加密。具体认证技术参见第 8 章。

3) 对此类事务处理，最好对发送的消息采用对称加密算法进行加密，对称加密密钥的传递可采用数字信封或其他方法。如果需要防抵赖，还需使用数字签名。对基于 SSL 协议的网上购物、报税、股票交易等，如有可能，都应使用数字签名。具体加密技术参见第 8 章。

由上述事务处理的基本流程可派生出两种该类事务处理流程。一种是在一次身份认证后只能进行一次事务处理，其处理流程如图 4 所示。另一种是在一次身份认证后能进行多次事务处理，其处理流程如图 5 所示。各种事务处理业务应根据业务要求，选择相应的处理流程。

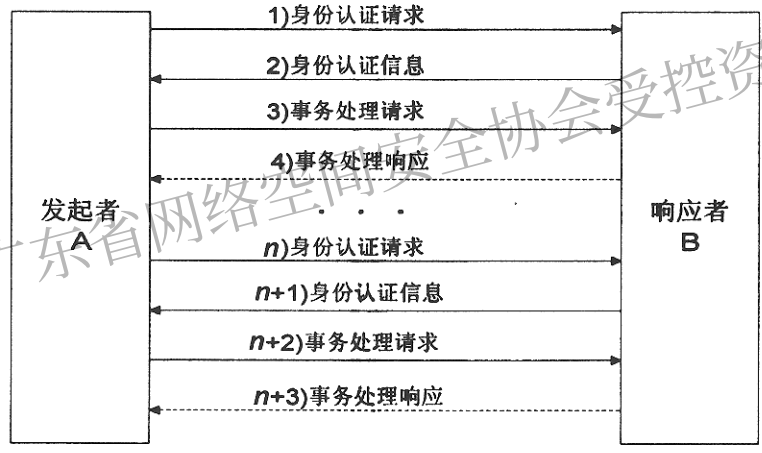


图 4 一次身份认证后只能进行一次事务处理的流程

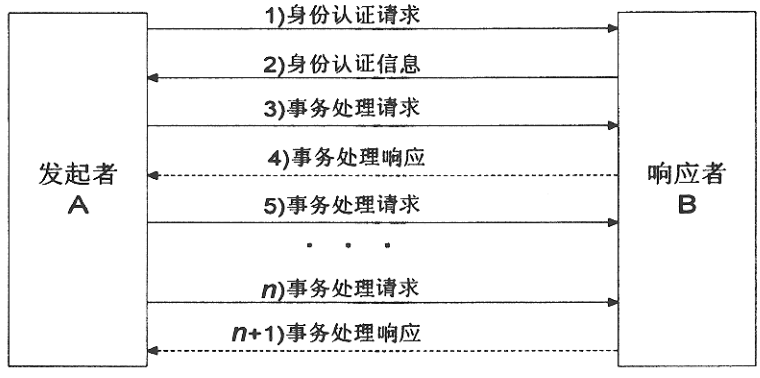


图 5 一次身份认证后能进行多次事务处理的流程

6.3.2 需要对事务处理发起者身份进行认证的事务处理基本流程

6.3.2.1 基本流程

需要对事务处理发起者身份进行认证的事务处理是指某些事务处理只为特定的用户服务，响应者在接收到事务处理请求后，要首先对事务处理发起者的身份进行认证，检查其是否是合法的用户。只有通过认证的用户，其事务处理请求才被接受。基本流程如图 6 所示。

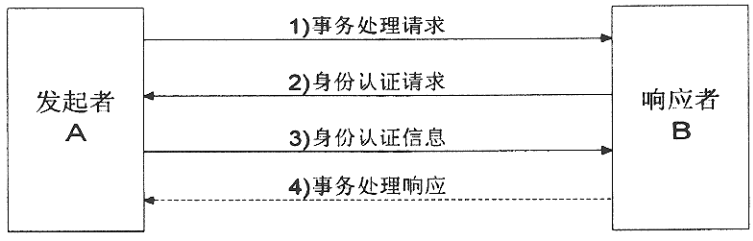


图 6　需要对事务处理发起者身份进行认证的事务处理流程

1) 事务处理发起者 A 选择事务处理的另一方（即响应者 B），向它发送事务处理请求。

2) 事务处理响应者 B 向事务处理发起者 A 发送身份认证请求。

3) 事务处理发起者 A 向事务处理响应者 B 发送身份认证信息。

4) 事务处理响应者 B 在接收到事务处理发起者 A 的身份认证信息后可进行以下操作：

a) 对事务处理发起者 A 的身份进行认证。

b) 如果对事务处理发起者 A 的身份认证成功，则按事务处理请求处理相应的事务。

c) 也可选用地处理完该事务后向事务处理发起者 A 发送相应的响应消息，表明该事务处理的执行结果。

6.3.2.2　附加规定

1) 对于一般的事务处理均应包含事务处理响应消息，如果某些事务处理有特殊需要，也可以忽略事务处理响应消息。

2) 认证方式可以使用数字签名或其他技术，如：邮件跟踪只需使用口令认证即可。具体认证技术参见第 8 章。

3) 对此类事务处理，最好对发送的消息采用对称加密算法进行加密。对称加密密钥的传递可采用数字信封或其他方法。如果需要防抵赖，还需使用数字签名。具体加密技术参见第 8 章。

由上述本类事务处理的基本流程可派生出两种该类事务处理流程。一种是在一次身份认证后只能进行一次事务处理，其处理流程如图 7 所示。另一种是在一次身份认证后能进行多次事务处理，其处理流程如图 8 所示。各种事务处理业务应根据业务要求，选择相应的处理流程。

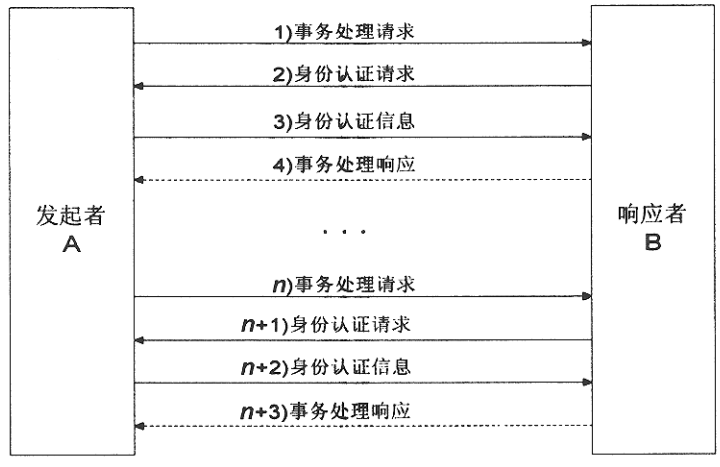


图 7　一次身份认证后只能进行一次事务处理的流程

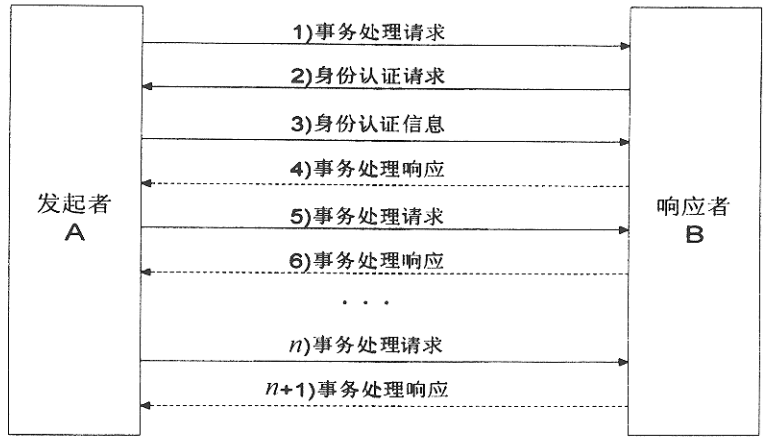


图 8　一次身份认证后能进行多次事务处理的流程

6.4　需要双方身份认证的事务处理基本流程

6.4.1　基本流程

需要双方身份认证的事务处理业务在进行事务处理前需要对参与双方的身份进行认证。只有认证成功的实体才能参与此类事务处理。基本流程如图 9 所示。

图 9　需要双方身份认证的事务处理流程

1) 事务处理发起者 A 选择事务处理的另一方（即响应者 B），向它发送身份认证请求。

2) 事务处理响应者 B 向事务处理发起者 A 发送身份认证信息。

3) 事务处理发起者 A 对事务处理响应者 B 的身份进行认证。也可选用地向事务处理响应者 B 传送认证结果。

4) 如果事务处理响应者 B 的身份认证成功，则事务处理发起者 A 向事务处理响应者 B 发送事务处理请求。

5) 事务处理响应者 B 向事务处理发起者 A 发送身份认证请求。

6) 事务处理发起者 A 向事务处理响应者 B 发送身份认证信息。

7) 事务处理响应者 B 对事务处理发起者 A 的身份进行认证。也可选用地向事务处理发起者 A 返回认证结果。

8) 如果事务处理发起者 A 的身份认证成功，事务处理响应者 B 执行相应的事务处理。也可选用地在事务处理完毕后返回相应的响应信息。

6.4.2 附加规定

1) 认证结果的返回，可以根据需要将其与下一个消息合为一个消息。如可以将 3)和 4)过程合为一个消息，7)和 8)过程合为一个消息。

2) 一般的事务处理最好包含响应消息，如果某些事务处理有特殊需要，也可以忽略事务处理响应消息。

3) 认证方式可以使用数字签名或其他技术，如：为政府高层领导服务的具有保密要求的信息服务、企业间秘密文件传递等均应采用数字签名技术。具体认证技术参见第 8 章。

4) 对此类事务处理，需对发送的消息采用对称加密算法进行加密。对称加密密钥的传递可采用数字信封或其他方法。如果需要防抵赖，还需使用数字签名。具体加密技术参见第 8 章。

6.5 需要三方/多方身份认证的事务处理流程

需要三方/多方身份认证的事务处理流程是前面几种事务处理基本流程的组合。因此，其处理流程不再赘述。对于该事务处理，首先分解为前面的基本事务处理，然后根据各事务处理基本流程采用相应的处理。

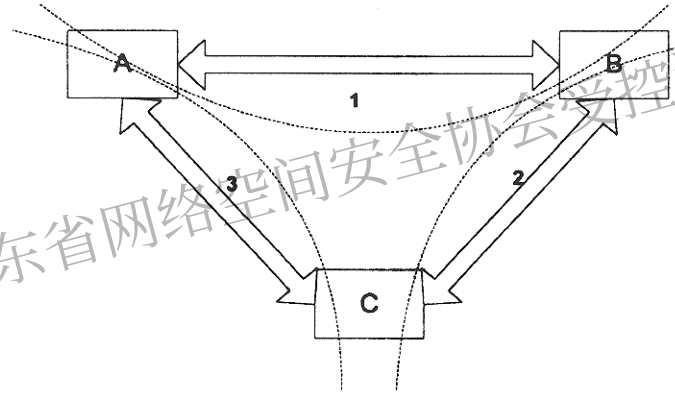


图 10 需要三方/多方身份进行认证的事务处理流程

例如：对于需要三方身份认证的事务处理系统（见图 10），参与方 A、B 和 C 在事务处理前要对各自的身份进行认证。可将此事务处理分解为 A-B，B-C 和 A-C 共 3 个基本事务处理，按各子流程执行。

对于各子流程的认证方式及加密手段，可以根据业务要求，在不同子流程中采用不同的认证方式及加密手段，也可在不同子流程中采用同一种认证方式及加密手段。如对于安全要求较高的需要多个部门审批的报关业务应采用数字签名进行认证，所传送的信息应使用对称密钥加密。而对于基于 SET 协议的电子交易，应采用数字签名进行认证，但只对传送信息中涉及金融秘密的数据部分采用数字信封加密。对于此类业务，在每个事务处理请求消息中都应使用数字签名对所发送的信息进行认证。具体认证技术及加密技术要求参见第 8 章。

7 支付模式

本章对基于 Internet 网络的事务处理业务的支付模式进行规范。在实际业务的实现中应根据具体业务的特性和需要选用相应的支付模式。

7.1 不涉及支付的在线事务处理业务

在这类事务处理业务中，事务处理业务的通信双方只需根据具体业务的安全需求进行单方、双方身份认证或根本不进行身份认证，以及根据业务的安全要求进行数据的加密传送和认证。身份认证技术

和实现方式及数据的安全加密技术实现方式分别参见第 6 章和第 8 章。

这种模式适用于如政府、企业、商家、个人间的公文传送；政府对企业、商家的财务报表审核等。

7.2 非在线支付的在线事务处理业务

这类事务处理业务从服务双方是否存在信任关系角度大致可分为两大类，一类是服务双方信誉度较高，服务双方相互信任；另一类是服务双方不存在信任关系。

7.2.1 服务双方互相信任

服务双方互相信任是指服务双方都有较高的信用度，这种情况下服务双方需要在进行服务之前进行较严格的身份认证，以确认对方身份。身份认证通过后，服务方为被服务方提供服务，付费可在以后当面结算或通过汇款、银行转账等方式完成。具体的认证过程、实现方式和数据加密技术参见第 6 章和第 8 章。

这种模式适用于如政府部门下采购清单、政府项目招标，企业、商家之间的原材料定购及商品批发业务、房地产买卖业务等。

7.2.2 服务双方不存在信任关系

服务双方不存在信任关系是指服务双方中的某一方或双方的信用度不够，这种情况下，服务提供者必须在得到被服务方的支付后才会为被服务方提供服务，因此服务方在得到被服务方的服务请求后对双方的在线身份认证和在线服务请求的认证以及数据传输安全级别要求不高，只提供简单的加密或不进行加密即可，而在提供服务时要当面进行确认、完成支付并提供服务（或在服务之前通过电话或 E-Mail 进行初步确认）。其流程如下：

1) 被服务方选择服务提供者提供的服务，在线发送服务请求；

2) 服务提供者接收服务请求，通过电话或 E-Mail 与被服务方进行请求确认；

3) 服务提供者得到被服务方的确认信息后，上门为被服务方提供服务，收取服务费用，开收据。

这种模式适用于如企业、商家为用户提供的各类在线购物服务等。

7.3 在线支付的在线事务处理业务

在这类事务处理业务中，服务提供者提供的在线服务基本可分为两大类：

1) 所提供服务的价格较高，交易成本只占服务价格的一小部分；

2) 所提供服务的价格本身比较低，交易的成本相对于服务价格而言则是不可忽视的一部分。

根据这两种服务类型，在线支付模式有两种：

1) 使用用户账号进行支付（参见附录 A）。对于上述前一类业务而言，使用用户账号进行支付，服务双方在线传输和认证的是用户的账号信息，类似于日常生活中的支票或信用卡交易；

2) 使用数字货币进行支付（参见附录 B）。对于上述后一类业务而言，使用数字货币这种小额支付模式进行支付，服务双方在线传输和认证的是数字货币，类似于现实生活中的现金交易。

7.3.1 使用用户账号进行支付

使用用户账号进行支付的事务处理是通过对用户账号进行认证，来确认用户的身份并实现支付。

用户账号是指能够确认用户身份并完成支付的识别信息。在实际操作中，用户账号可表现为以下几种具体形式（具体内容参见附录 A）：

1) 用户的会员身份号码，在某服务提供者处使用（具体内容参见附录 A1）；

2) 用户的逻辑卡号，在某些服务提供者范围内使用（具体内容参见附录 A2）；

3) 其他的实现模式。

无论是用户的会员卡或逻辑卡，实际都可以这样实现，即用户事先在某一个支付处理系统中开设一个账号，并在其中存入现金，以后当用户发出服务请求时，支付都可以通过这个账号来完成。

使用用户账号进行支付处理可以采用直接划账方式，也可以采用转移信用点方式等具体实现模式。

用户账号支付模式适用于服务价格本身比较高的情况，如在线购物（参见附录 C）、在线代缴费业务、家庭银行、在线金融服务（参见附录 D），企业、商家或个人向政府纳税，政府为各类用户提供的

在线申请业务，政府部门下采购清单，政府项目招标，企业、商家之间的原材料定购及商品批发业务，房地产买卖业务等。

7.3.1.1 用户账号支付系统的构成

1) 一般地，用户账号支付系统由三方构成：支付处理方、服务提供者和被服务方。

a) 支付处理方（支付结算服务器）作为第三方，负责在安全的环境中注册和管理用户及服务提供者的账号信息，处理用户和服务提供者的支付结算；

b) 服务提供者（服务提供者服务器，以下简称商家）是提供服务的个体，进行服务内容的发布，将用户的支付请求转发给支付处理方，并且要在支付处理方中建立一个现金账号以与用户结算；

c) 被服务方（用户终端，以下简称用户）是使用服务的个体，将服务请求和支付信息送给服务提供者，并且应在支付处理方（与服务提供者使用相同的支付处理方）建立一个现金账号并存入一定的金额用以支付，同时用户端需要一个软件（称为电子钱包）来保存与支付有关的账号、密钥等信息。

2) 在一些特别的业务（例如：股票交易系统、会员制服务系统等）中可简化为，服务提供者同时担负支付处理方的角色。用户在服务提供者处建立账号，在服务提供者的内部网络中实现支付结算。

7.3.1.2 业务流程

使用用户账号进行支付的业务流程图如图 11 所示。

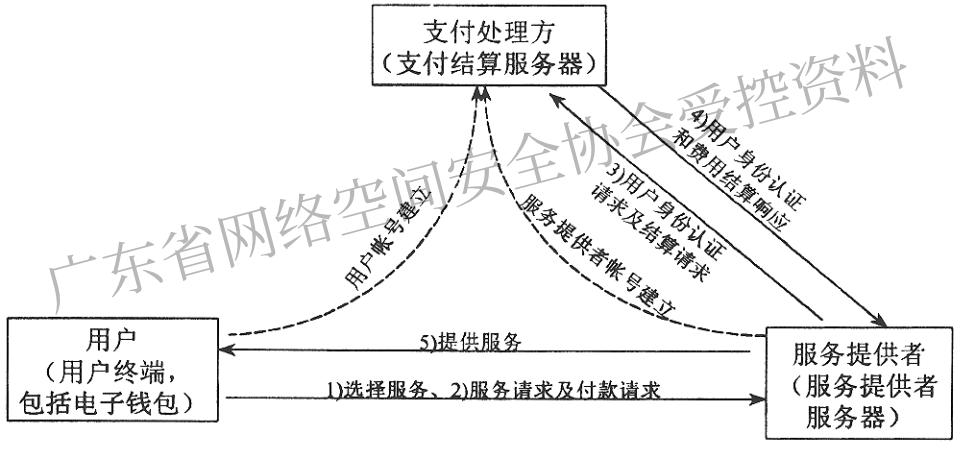


图 11 使用用户账号进行支付的流程

1) 用户使用各种方式（在线或非在线）选择服务；

2) 用户和服务提供者进行身份验证后，通过电子钱包把服务请求和支付信息加密发送给服务提供者以请求付款；

3) 服务提供者和支付处理方进行身份验证后，把自己的账号信息、用户要支付的金额等支付信息加密发送给支付处理方，请求支付处理方认证用户信息，并处理相应的付费请求；

4) 支付处理方接收服务提供者的信息，在其内部可靠的网络环境中对用户的支付信息进行认证，如果用户身份认证成功，则向服务提供者发回认证成功的响应，授权服务提供者为用户提供服务，并在用户和服务提供者之间进行结算；

5) 服务提供者接收到支付处理方的认证返回信息后，作相应的处理，并给用户发回响应，为用户提供服务。

以上只是这种模式的宏观流程，其中用户、服务提供者和支付处理方之间的数据传输和身份认证都要根据业务的实际内容选择不同的身份认证模式和数据加密方式，以满足业务对数据的保密性、完整性的要求以及对交易的防抵赖要求等。详细的身份认证方式及数据传输的安全技术分别参见第 6 章和第 8 章。

7.3.1.3 管理要求

1) 服务提供者的管理要求

a) 对用户使用服务和交易情况作日志，并在规定的时间内保留日志，以供查阅；

b) 对支付处理方的认证返回信息作日志，并在规定的时间内保留日志，以便查阅；

c) 对系统服务器的访问作出一定的限制，保证系统的重要信息（包括日志文件、用户的私人信息等）以及在服务器上停留的用户支付信息的安全；

d) 保证系统的硬件和环境的安全。

2) 支付处理方的管理要求

a) 对用户认证情况作日志，并在规定的时间内保留日志，以便查阅；

b) 对用户的支付情况作日志，并在规定的时间内保留日志，以便查阅；

c) 对系统服务器的访问作出一定的安全措施，保证系统的重要信息（包括日志文件、用户的私人信息等）的安全；

d) 需要的话，对服务提供者和用户的数字证书提供管理；

e) 保证系统的硬件和环境的安全；

f) 如果支付处理系统建立认证中心则应符合认证中心的安全及管理要求。

7.3.2 使用数字货币进行支付

在本节数字货币的实现模式中引用了小额支付传输协议（MPTP，Micro Payment Transfer Protocol）。

7.3.2.1 数字货币的原理

1) 数字货币（Digital Cash 或 e-Cash）是由支付处理方（货币发行方）发行的一串随机数；

2) 为保证发行出来的数字货币的合法性，数字货币中必须包含货币发行方的数字签名，并且这些数字签名中必须包含货币发行方的证书信息；

3) 经过支付处理方数字签名的数字货币必须与现实生活中的货币一一对应，具有货币的价值；

4) 为严格管理货币发行方，其发行数字货币所使用的数字证书必须由相关的证书认证机构统一发布。

7.3.2.2 数字货币的适用范围

数字货币适用于在线信息服务、在线数据库查询、在线目录服务、VOD、实时音乐播放、在线游戏、在线教育、软件下载、软件升级、产品的售后服务、在线订阅电子印刷品等服务价格较低的应用场合。

7.3.2.3 数字货币的分类

根据数字货币的流通范围，可分为通用数字货币和非通用数字货币。

1) 通用数字货币指数字货币统一由支付处理方发行，数字货币中包含支付处理方信息，此后这些货币在所有接收这种数字货币的在线商家都可使用，货币的最终验证和处理要由支付处理方来进行。

2) 非通用数字货币指数字货币由服务提供者本身发行，货币中包含服务提供者的信息，即不同的服务提供者发行各自的货币，各自即可进行用户所支付货币的认证，这种模式需要一个经纪人来管理被服务方和服务提供者账号以降低交易成本。

7.3.2.4 数字货币的应用

数字货币的应用主要包括两大部分：

1) 用户使用支付处理方账号在线购买数字货币，这个过程与前面描述的使用用户账号进行在线支付的过程类似；

2) 用户用购得的数字货币进行在线支付。

7.3.2.5 数字货币的实现及使用流程

数字货币的详细实现流程及使用数字货币进行支付的流程参见附录 B。

8 安全技术要求

本章主要规范在事务处理过程中网络上信息传输和身份认证相关的安全技术要求。

国家密码管理委员会对密码进出口有严格规定和限制，即："全国商用密码由国家密码管理委员会统一领导，国家密码管理委员会办公室具体管理。研制、生产和经营商用密码必须经国家密码主管部门批准。未经国家密码主管部门批准，任何单位和部门不得研制、生产和经销密码。需要使用密码技术手段加密保护信息安全的单位和部门，必须按照国家密码管理规定，使用国家密码管理委员会指定单位研制、生产的密码，不得使用自行研制的密码，也不得使用从国外引进的密码"。参照本技术规范建立的事务处理应用中涉及到的加密算法和加密位长均应符合国家法律和国家密码委员会的相应规定，并要保证加密算法的一致性以实现业务的互通。本技术规范不单独对这部分内容作另外规定。

本章涉及到公钥加密时需要使用证书认证技术。

8.1 加密

加密用来保护敏感信息的传输，保证信息的机密性。目前主要有两种加密方法：秘密密钥加密和公开密钥加密。

8.1.1 秘密密钥加密

秘密密钥加密也称为对称密钥加密，加密和解密使用同一个密钥。因此信息的发送方和接收方必须共享一个密钥。

8.1.2 公开密钥加密

公开密钥加密也称为非对称密钥加密。公开密钥加密使用两个不同的密钥，一个用来加密信息，称为加密密钥；另一个用来解密信息，称为解密密钥。用户把加密密钥公开，因此加密密钥也称为公开密钥，简称公钥。解密密钥是保密的，也称为私有密钥，简称私钥。这两个密钥是数学相关的，用某用户的加密密钥加密后所得的数据只能用该用户的解密密钥才能解密。因而要求用户的私钥不能透露给自己不信任的任何人。

用户的公钥需要由CA中心签发的数字证书来证明其有效性。有关CA证书的要求应符合本技术规范第9章的规定。

8.1.3 密钥的分发

密钥的安全分发是保证实现有效加密的重要环节。

8.1.3.1 秘密密钥的分发

实现秘密密钥加密必须保证信息发送方与信息接收方之间通过安全通道分发秘密密钥。因此秘密密钥加密不适合用在公共网络上许多事先互不认识的通信者之间的信息传送。

8.1.3.2 公开密钥加密中公钥的分发

适合于公共网络上事务处理业务中分发公钥的方法有两种，使用公钥数据库管理公钥和使用认证公钥的数字证书。

1) 使用公钥数据库管理公钥适合于参与通信的用户比较少的情况。每个用户必须建立一个公钥数据库储存与他通信的用户的公钥。该方式建立的数据库应满足以下条件：

a) 在该数据库中，每一个公钥唯一与一个用户对应；

b) 输入到数据库中的公钥必须被证实是对应用户的公钥，而该用户必须被数据库的使用者证实身份；

c) 该数据库的访问必须是安全的。

2) 使用数字证书是一种更易安全分发公钥的方式。

a) 基本的数字证书中包括证书持有人的个人信息、公钥以及证书签发者对这些信息的数字签名和证书签发者的数字证书；

b) 因为数字证书是由第三方签发的，所以确认数字证书持有人身份和从该证书获取证书持有人

的公钥，需要信任数字证书的签发者；

c) CA 认证中心是签发数字证书的机构，有关 CA 的体系结构及证书的内容应遵循 ITU－T 建议 X.509，具体要求应符合本规范第 9 章要求。

8.1.4 密钥的保护

密钥的安全是保证密钥有效的重要前提。秘密密钥与公开密钥加密方法中的私钥的密钥长度一般比较长，因此必须使用保密模块来保存这些密钥。用户使用这些密钥前必须被保密模块认证。保密模块可以是纯软件产品、纯硬件产品或软件和硬件结合产品等。

8.2 数字信封

8.2.1 数字信封原理

数字信封技术结合使用了秘密密钥加密技术和公开密钥加密技术，公开密钥的证书应符合本技术规范第 9 章的规定。

1) 在外层使用公开密钥加密技术来分发密钥，享受到公开密钥技术的灵活性；

2) 在内层使用对称密钥加密技术，由于内层的对称密钥长度通常较短，从而使得公开密钥加密的相对低效率被限制在最低限度，享受到秘密密钥技术的高效性；

3) 由于可以在每次传送中使用不同的对称密钥，系统有了额外的安全保证。

8.2.2 数字信封的实现

1) 当发信方需要发送信息时，首先生成一个对称密钥，用该对称密钥加密要发送的报文；

2) 发信方用收信方的公钥加密上述对称密钥；

3) 发信方将第一步和第二步的结果传给收信方；

4) 收信方使用自己的私钥解密被加密的对称密钥；

5) 收信方用得到的对称密钥解密被发信方加密的报文，得到真正的报文。

8.3 数字签名

数字签名用来保证信息传输过程中信息的完整和提供信息发送者的身份认证。使用公开密钥算法是实现数字签名的主要技术，其证书要求应符合本技术规范第 9 章的要求。

8.3.1 数字签名

使用公开密钥算法实现数字签名技术有两个密钥，一个是签名密钥，它必须保持秘密，因此称为私有密钥，简称私钥；另一个是验证密钥，它是公开的，因此称为公开密钥，简称公钥。实现数字签名的过程如下：

1) 信息发送者使用自己的私钥签名信息。该过程称为实现数字签名；

2) 信息发送者把信息本身和已签名的信息一起发送出去；

3) 任何接收者通过使用信息发送者的公钥来验证数字签名，以确认信息发送者的身份和信息是否被修改过。该过程称为验证数字签名。

8.3.2 使用信息摘要的数字签名

公开密钥算法的运算速度比较慢，因此可使用信息摘要技术以减小使用公开密钥算法的运算量。

信息摘要是通过使用一种单向散列函数而产生的。对不定长的信息使用信息摘要技术可以产生一固定长度的信息摘要，该信息摘要对于信息是唯一的。从信息摘要中不能得出生成信息摘要的信息，而且找出具有同一个信息摘要的两个不同的信息在计算上是不可行的。

使用信息摘要的数字签名的实现步骤如下：

1) 信息发送者使用一单向散列函数对信息生成信息摘要；

2) 信息发送者使用自己的私钥签名信息摘要；

3) 信息发送者把信息本身和已签名的信息摘要一起发送出去；

4) 任何接收者通过使用与信息发送者使用的同一个单向散列函数对接收的信息生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份和信息是否被修改过。

8.4 双重数字签名

双重签名是为了保证在事务处理过程中三方安全地传输信息的一种技术。

本节规定了双重数字签名的实现步骤，信息在传输中的加密不属本节内容。

双重数字签名的实现步骤如下：

1) 信息发送者对发给甲的信息 1 生成信息摘要 1；

2) 信息发送者对发给乙的信息 2 生成信息摘要 2；

3) 信息发送者把信息摘要 1 和信息摘要 2 合在一起，对其生成信息摘要 3，并使用自己的私钥签名信息摘要 3；

4) 信息发送者把信息 1、信息摘要 2 和信息摘要 3 的签名发给甲；

5) 信息发送者把信息 2、信息摘要 1 和信息摘要 3 的签名发给乙；

6) 甲接收信息后，对信息 1 生成信息摘要，把这信息摘要和收到的信息摘要 2 合在一起，并对其生成新的信息摘要，同时使用信息发送者的公钥对信息摘要 3 的签名进行验证，以确认信息发送者的身份和信息是否被修改过；

7) 乙接收信息后，对信息 2 生成信息摘要，把这信息摘要和收到的信息摘要 1 合在一起，并对其生成新的信息摘要，同时使用信息发送者的公钥对信息摘要 3 的签名进行验证，以确认信息发送者的身份和信息是否被修改过。

8.5 认证技术

事务处理业务的认证是保证事务处理安全的重要因素之一。基于 Internet 网络的事务处理业务的认证分为实体认证和信息认证。

8.5.1 实体认证

在公共网络上的实体认证方式有两种：一种是请求认证者的秘密信息（例如：口令）在网上传送的口令认证方式；另一种是使用公开密钥签名算法，而不需要在网上传送秘密信息的挑战响应(Challenge-Response)方式。

对于口令认证方式，根据业务需要，认证响应者可以允许同一时间内多个请求认证者使用同一用户身份认证，如网络接入等。但对使用公开密钥签名算法认证方式，认证响应者禁止同一时间内多个请求认证者使用同一用户身份认证。

本节规定了可用于事务处理业务中的实体认证的 3 种常用认证方式。

8.5.1.1 使用口令的单向实体认证

1) 使用口令的单向实体认证的前提

使用口令进行单向实体认证时，请求认证者必须具有一个 ID，该 ID 必须在认证者的用户数据库（该数据库必须包括 ID 和口令）中是唯一的。同时为了保证认证的有效性必须考虑到以下问题：

a) 请求认证者的口令必须是安全的。即满足口令只能允许相应 ID 的请求认证者知道，在认证者系统中必须保证口令的使用和存储是安全的。

b) 在认证的过程中，必须保证口令的传输是安全的。即在传输过程中，口令不能被窃看、替换。

c) 请求认证者在向认证者请求认证前，必须确认认证者的真实身份。否则会把口令发给冒充的认证者。

以上问题的解决尚需根据应用的需要和具体的环境，选择相应的安全技术实现，本节对此不作规定，本节主要规定使用口令的单向实体认证的流程。

2) 使用口令的单向实体认证流程

图 12 是使用口令的单向实体认证的流程图。

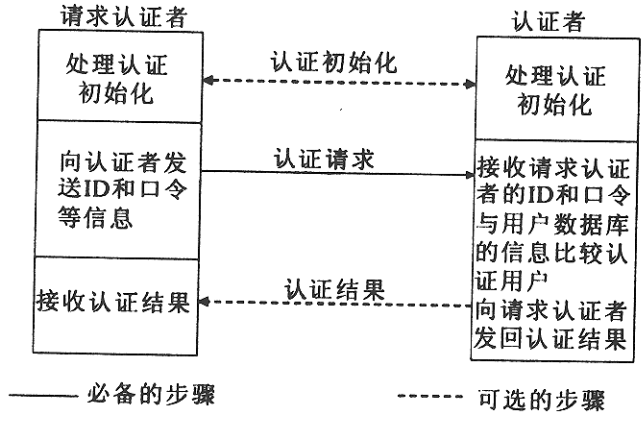


图 12　使用口令的单向实体认证流程

使用口令的单向实体认证过程如下：

a) 请求认证者和认证者之间作认证初始化，可在该过程中实现建立安全连接、确认认证者身份等。该步骤是可选的；

b) 请求认证者向认证者发送认证请求，认证请求中必须包括请求认证者的 ID 和口令；

c) 认证者接收 ID 和口令，在用户数据库中找出请求认证的 ID 和口令（若找不到相应的 ID，则跳过步骤 d 和 e）；

d) 认证者比较两口令是否相同（如果不同，则跳过步骤 e）；

e) 根据业务需求，可选用地检查数据库中该 ID 的状态。如果是正在使用，则拒绝认证；否则，接收认证，并将标志位置为正在使用（该标志位在用户退出时由认证响应者复位）。

f) 认证者向请求认证者发回认证结果，请求认证者接收认证结果。该步骤是可选的。

请求认证者的身份确认必须满足两个条件，即请求认证者的 ID 必须在认证者的用户数据库中；请求认证者发送的口令与数据库中的口令相同。

8.5.1.2　使用公开密钥签名算法的单向实体认证

使用公开密钥签名算法的认证方式，请求认证者的个人秘密信息（例如：口令）不用在网络上传送，减少了认证的风险。这种方式是通过请求认证者与认证者之间对一个随机数作数字签名与验证数字签名来实现的。作数字签名的公钥的数字证书应符合本技术规范第 9 章的规定。

1) 使用公开密钥签名算法的单向实体认证必须具备的前提如下：

a) 请求认证者必须具有使用私钥实现数字签名的功能；

b) 认证者必须具有使用公钥验证数字签名的功能；

c) 认证者必须具有产生随机数的功能，而且随机数的质量必须达到一定要求；

d) 用于实现数字签名和验证数字签名的密钥对必须与一个实体唯一对应。

2) 签名公钥的分发

用于数字签名的私钥的保密和用于验证数字签名的公钥的安全分发是保证认证有效的重要因素。公钥的分发可采用以下方式：

a) 对于在认证者处使用公钥数据库的方式，请求认证者 ID 必须包含在认证响应中（作为可选的需要作数字签名的附加信息）发送给认证者，认证者使用该 ID 从公钥数据库中获得请求认证者的公钥。

b) 对于使用证书认证中心签发数字证书的方式，认证者必须信任为请求认证者签发证书的证书认证中心，请求认证者的数字证书必须作为可选的不需要数字签名的附加信息发送给请求认证者，认证者检验请求认证者数字证书后，从数字证书中获取请求认证者的公钥。

其具体方式尚需根据不同的应用和管理需要来选择。

3) 使用公开密钥签名算法的单向实体认证流程

a) 请求认证者产生认证请求，向认证者发送认证请求。该步骤是可选的；

b) 认证者产生一个随机数作为认证挑战，并保存认证挑战，然后把认证挑战发送给请求认证者；

c) 接收认证挑战后，请求认证者生成认证响应（认证响应包括认证挑战和一些可选的需要数字签名的附加信息），请求认证者使用自己的私钥对认证响应作数字签名。请求认证者把认证响应、认证响应的数字签名和一些可选的不需要数字签名的附加信息发送给认证者；

d) 认证者接收认证响应后，比较认证响应中的认证挑战与在步骤(b)中保存的认证挑战是否相同；

e) 认证者根据不同的公钥分发机制使用不同方法获得请求认证者的被认证的公钥，认证者使用该公钥验证认证响应的数字签名；

f) 如果验证通过，检查数据库中该用户的状态。如果是正在使用，则拒绝认证；否则，接收认证，并将数据库中该用户的状态标志置为正在使用（该标志位在用户退出时由认证响应者复位）。

g) 认证者向请求认证者发回认证结果，请求认证者接收认证结果。该步骤是可选的。

图 13 是使用公开密钥签名算法的单向实体认证流程。

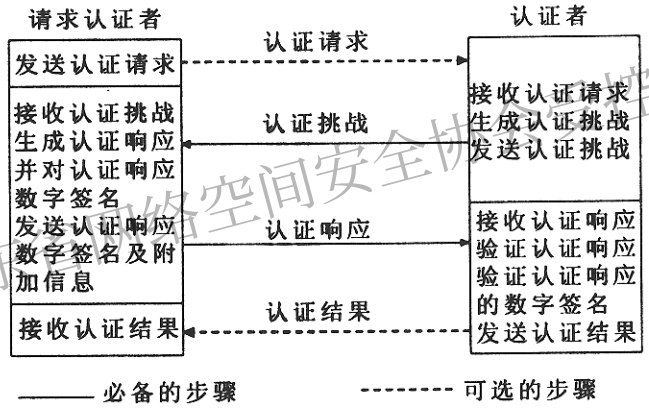


图 13 使用公开密钥签名算法的单向实体认证流程

4) 请求认证者身份确认的条件

a) 请求认证者发回的认证响应中的认证挑战与认证者保存的认证挑战必须相同；

b) 请求认证者对认证响应的数字签名必须被验证。

8.5.1.3 使用公开密钥签名算法的双向实体认证

在双向实体认证中，两个实体彼此要认证对方。先发出认证请求的实体称为认证发起者，响应认证的另一个实体称为认证响应者。

1) 使用公开密钥签名算法的双向实体认证必须具备的前提

a) 认证发起者、认证响应者必须具有使用私钥实现数字签名的功能；

b) 认证发起者、认证响应者必须具有使用公钥验证数字签名的功能；

c) 认证发起者、认证响应者必须具有产生随机数的功能，而且随机数的质量必须达到一定要求；

d) 用于实现数字签名和验证数字签名的密钥对必须与一个实体唯一对应。

2) 签名公钥的分发

用于数字签名的私钥的保密和用于验证数字签名的公钥的安全分发是保证认证有效的重要因素。

认证发起者和认证响应者可采用不同的方式获得公钥。认证发起者和认证响应者的公钥可由以下方式获得：

a) 对于使用公钥数据库的方式，认证发起者或认证响应者 ID 必须包含在认证响应及挑战或认证响应中（作为可选的需要数字签名的附加信息）发送给对方，认证发起者或认证响应者使用该 ID 从自己的公钥数据库中获得对应的公钥；

b) 对于使用证书认证中心签发数字证书的方式，认证发起者或认证响应者必须信任签发证书给对方的证书认证中心，认证发起者或认证响应者的数字证书必须作为可选的不需要数字签名的附加信息发送给对方，检验数字证书后，从数字证书获取对方的公钥。有关要求应符合本技术规范第 9 章的规定。

3) 使用公开密钥签名算法的双向实体认证流程

在这一节中，只描述双向实体认证的流程，公钥的分发方式可根据不同的应用和管理需要选择。图 14 是使用公开密钥签名算法的双向实体认证流程。

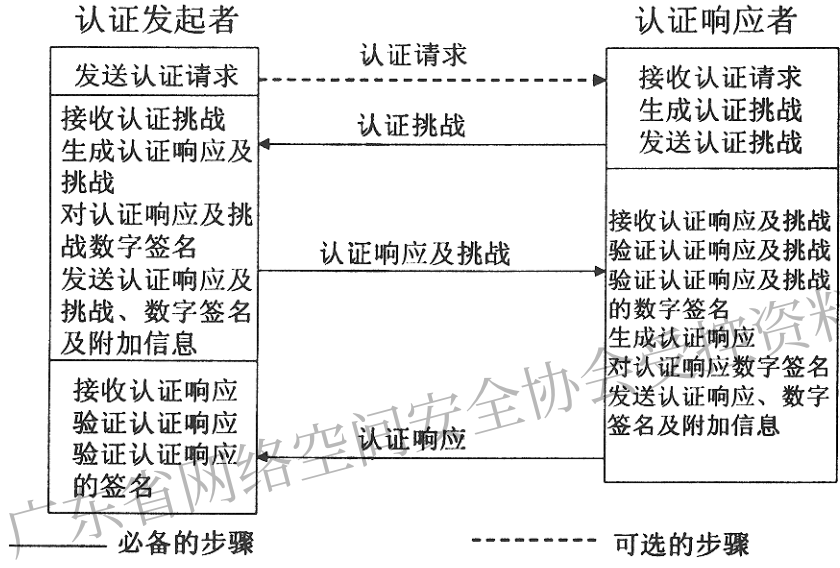


图 14　使用公开密钥签名算法的双向实体认证流程

使用公开密钥签名算法的双向实体认证的过程如下：

a) 认证发起者产生认证请求，向认证响应者发送认证请求。该步骤是可选的；

b) 认证响应者产生一个随机数 1 作为认证挑战 1，并保存认证挑战 1，然后把认证挑战 1 发送给认证发起者；

c) 接收认证挑战 1 后，认证发起者生成一个随机数 2 作为认证挑战 2，并保存认证挑战 2，同时把认证挑战 1、认证挑战 2 和一些可选的需要数字签名的附加信息合在一起作为认证响应及挑战，认证发起者使用自己的私钥对认证响应及挑战数字签名，然后把认证响应及挑战、认证响应及挑战的数字签名和一些可选的不需要数字签名的信息发送给认证响应者；

d) 认证响应者接收认证响应及挑战后，比较认证响应及挑战中的认证挑战 1 与在步骤 b)中保存的认证挑战 1 是否相同；

e) 认证响应者根据不同的公钥分发机制使用不同方法获得认证发起者被认证的公钥，并使用该公钥验证认证响应及挑战的数字签名；

f) 如果验证通过，检查数据库中该用户的状态。如果是正在使用，则拒绝认证；否则，接收认证，并将数据库中该用户的状态标志置为正在使用（该标志位在用户退出时由认证响应者复位）。

g) 认证响应者把认证响应及挑战和一些可选的需要数字签名的附加信息合在一起作为认证响应，并使用自己的私钥对认证响应作数字签名，然后把认证响应、认证响应的数字签名和一些可选的不需要数字签名的信息发送给认证发起者；

h) 认证发起者接收认证响应后，比较认证响应中的认证挑战 2 与在步骤 c)中保存的认证挑战 2 是否相同；

i) 认证发起者根据不同的公钥分发机制使用不同方法获得认证响应者被认证的公钥，并使用该公钥验证认证响应的数字签名。

4) 双方身份认证通过条件

双方身份的确认必须在一个认证过程中同时满足以下条件：

a) 认证发起者被确认身份必须满足：

- 认证发起者发回的认证挑战 1 与认证响应者保存的认证挑战 1 必须相同；
- 认证发起者对认证响应及挑战的数字签名必须被验证。

b) 认证响应者被确认身份必须满足：

- 认证响应者发回的认证挑战 2 与认证发起者保存的认证挑战 2 必须相同；
- 认证响应者对认证响应的数字签名必须被验证。

8.5.2 信息认证

信息认证是指对信息体进行认证，以决定该信息的合法性。信息认证发生在信息接收者接收到信息后，使用相关技术对信息进行认证，以确认信息的发送者是谁，信息在传输的过程中是否被修改、替换。

目前在网络上使用较多的信息认证方式是使用公开密钥签名算法对信息进行数字签名。

1) 签名公钥的分发

用于数字签名的私钥的保密和用于验证数字签名的公钥的安全分发是保证信息认证有效的重要因素。公钥的分发方式可根据不同的应用和管理需要选择。但必须保证一个公钥只对应于一个实体。公钥的分发可采用以下两种方式：

a) 对于在信息接收者处使用公钥数据库的方式，信息发送者的 ID 必须随信息的数字签名发送给信息接收者，信息接收者使用该 ID 从公钥数据库中获得信息发送者的公钥。

b) 对于使用证书认证中心签发数字证书的方式，信息接收者必须信任为信息发送者签发数字证书的证书认证中心，信息发送者的数字证书必须随信息的数字签名发送给信息接收者，信息接收者检验信息发送者数字证书后，从数字证书获取信息发送者的公钥。有关要求应符合本技术规范第 9 章的规定。

2) 信息认证流程

图 15 是使用公开密钥签名算法进行信息认证的流程图。

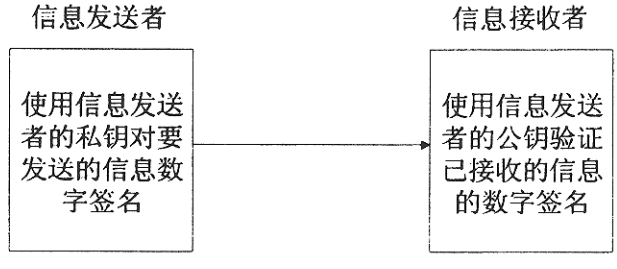


图 15 使用公开密钥签名算法的信息认证流程

使用公开密钥签名算法的信息认证过程如下：

a) 信息发送者生成要发送的信息，使用自己的私钥对要发送的信息数字签名。把信息、信息的数字签名和其他一些附加的不用签名的信息发送给信息接收者；

b) 信息接收者根据不同的公钥分发机制，使用不同方法获得信息发送者的被认证的公钥,信息接收者使用该公钥验证信息的数字签名。

3) 使用数字签名技术的信息认证通过的条件

信息的确认必须满足信息的数字签名必须被验证。

9 CA 体系的构建及管理要求

在 Internet 网上参与事务处理的实体通过出示证书来表明自己的身份。证书除了用来向其他实体证明自己的身份外，还同时起着公钥分发的作用，每份证书都携带着证书持有者的公钥，签名证书携带的是签名公钥，信息加密证书携带的是信息加密公钥。所有实体的证书都是直接由认证机构分发并签名的。

基于 Internet 网络的事务处理业务是电子商务业务的一部分（包括电子商务业务中的非支付型电子商务业务和不涉及银行的支付型电子商务业务），因此在事务处理业务中的 CA 认证中心应采用基于 Internet 网络的电子商务系统的 CA 认证中心。有关 CA 认证中心的相关要求另行规定。

附录 A
(提示的附录)
预付卡业务技术要求

本附录提供了在公共网络上如何实现使用预付卡进行支付的业务系统的流程，它是一个在公共网络上建立在线购物业务系统的参考。本附录引用了前文的第 6 章、第 7 章、第 8 章的相关规定。

A1 会员制方式

A1.1 会员制支付系统的构成

会员制支付方式的系统构成如图 A1 所示。

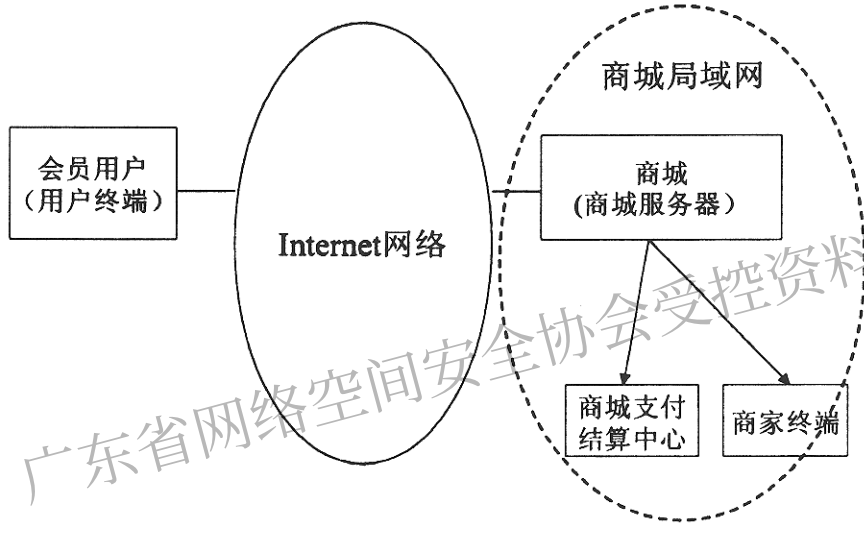


图 A1 会员制支付系统构成

1) 商城（商城服务器及支付结算中心）

a) 各商家联合起来组成一个虚拟商城；

b) 虚拟商城拥有自己的支付结算中心，发行只在本商城内使用的会员卡（该卡与信用卡的区别在于使用范围的不同）；

c) 支付结算中心负责管理加入到该商城的用户和商家的账号、保存用户预交的现金、在用户和商家之间进行转账。

2) 会员用户（用户终端）。想使用该商城会员卡进行购物的用户首先需要在该商城开设会员账号，并在账号中存入现金。加入该商城的用户即为该商城的会员。

3) 商家（商家终端）。加入该商城进行服务的商家也需要在该支付结算中心开设账号，用于在提供服务时与用户进行结算。加入到该商城的商家则称为该商城的商家会员。

A1.2 认证及数据加密技术要求

A1.2.1 身份认证

在会员制支付模式中，会员用户和商城之间在进行信息传送之前需要进行双向身份认证。由于商城同时承担提供服务和支付结算两个角色（在同一局域网内），因此在线的身份认证只在商城和用户之间进行，商城服务器和支付结算中心在同一局域网内，无需进行身份认证。具体的用户身份认证功能由支付结算中心承担。

身份认证可采用两种方式：

1) 使用口令方式认证用户。这种方式下用户首先要采用 SSL 单方认证技术认证与自己通信的商城的身份。此时商城需要有由 Internet 网 CA 中心签发的公钥证书（应符合第 9 章的相应规定），基本流程应符合 6.3 节中的规定；服务器对用户身份的认证流程应符合 8.5.1.1 条的相应规定。这时商城的支付结算中心需具有相应的数据库或文件来安全地保存每一个会员用户的会员号码和与之对应的口令；在认证时，用户 ID 和口令的传送应采用安全通道进行（如 SSL 协议，或自行开发的加密模块等）；

2) 采用数字签名方式进行身份认证。此时用户和商城都需要有签名公钥证书，其公钥证书应由 Internet 网 CA 中心签发，有关内容应符合第 9 章的规定。此时的基本流程应符合 6.4 节中的规定，认证流程应符合 8.3 节中的相应规定。本技术规范在这里不建议使用公钥数据库的方式分发公钥，原因是这种业务不同于附录 E 中的公文传送业务，这种业务中参与通信的用户较多。

A1.2.2 信息认证

为保证用户和商家之间通信时双方接收到的数据的完整性，应当使用数字签名技术，此时用户和商城都需要有签名公钥证书，它们的签名公钥证书应由 Internet 网 CA 中心统一签发，有关内容应符合第 9 章的规定。具体流程应符合 6.2 节中的相应规定，使用的技术应符合 8.3 节中的相应规定。

A1.2.3 数据加密

在这种模式中，用户的支付信息需要加密传送到商城服务器及商城支付结算中心。数据加密应符合 8.1.1 节中的对称密钥加密技术规定，有关对称密钥的分发应符合 8.2 节中数字信封技术的规定。此时用到的加密公钥的证书应由 Internet 网 CA 中心统一签发，有关内容应符合第 9 章的规定。

A1.2.4 私钥和公钥证书的保护

私钥和公钥证书的保护使用软件保密模块。由于私钥和公钥证书是系统安全的重点，系统某一端私钥和公钥证书的被窃和被替换将摧毁系统的安全性，并影响到其他端的安全。因此该保密模块的安全级别应根据具体业务的安全要求决定。同时整个系统的对称加密算法和非对称加密算法的加密强度也应由具体业务的安全要求决定。

A1.3 业务流程

业务流程如下，流程图如图 A2、A3 所示。

1) 会员用户访问商城的服务器，进行商品浏览，发出服务请求；

2) 商城与用户进行身份认证的方式有两种：

   a) 采用用户 ID 加口令的认证方式。

      - 用户通过 SSL 方式认证商城身份；
      - 用户将自己的会员卡号码及口令等通过安全通道安全传给商城；
      - 商城服务器接收用户请求，将用户的服务请求发给商家，将用户的会员卡号及口令传给商城支付结算中心要求认证用户身份；
      - 商城支付结算中心验证用户的会员卡和口令信息，将认证结果传给商城服务器；

   b) 采用数字签名认证方式。

      用户和商城支付结算中心采用认证挑战和响应的方式进行双方身份认证。认证挑战及响应信息由商城服务器转发（建议使用公钥数字证书的方式分发公钥，具体内容应符合 8.1.3.2 条中的相应规定，而有关数字证书的管理和分发应符合第 9 章中的相应规定）。

3) 认证通过后，商城的支付结算中心通知商城服务器或商家为用户提供服务。

   a) 用户购买硬件产品 —— 商家通知送货公司给用户送货；

   b) 用户购买软件产品 —— 商城服务器授权用户下载软件产品。

4) 用户接收服务；

5) 商家向商城支付结算中心发出转账（服务费）请求，与商城支付结算中心进行清算；

6) 商城支付结算中心定期向用户发送用户消费的账单信息。

在这种方式中，凡是加入该商城的商家均可以使用这种方式为持有该商城会员卡的用户提供在线服务。这种服务模式适用于在线信息服务、软件下载、在线定购、会员制在线购物等。

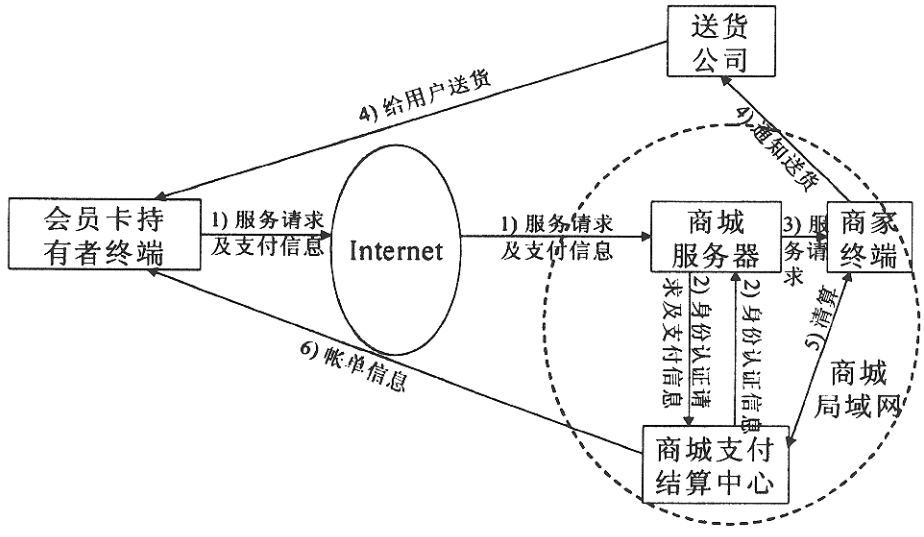


图 A2　会员制支付流程 —— 购买硬件产品

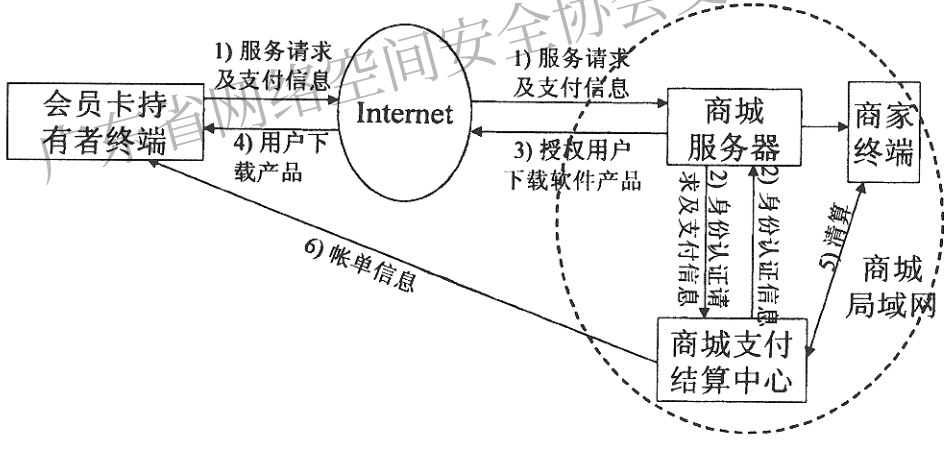


图 A3　会员制支付流程 —— 购买软件产品

A2　169 卡方式

A2.1　169 卡支付系统构成

在这种方式中，发行专门的适用于 Internet 网上各种付费业务的逻辑卡，这里暂且将其命名为 169 卡。169 卡由全网统一发行，可用于各种收费的信息服务、软件下载、在线定购、在线购物、在线缴费等业务领域。

在使用 169 卡支付模式的系统中，在线服务涉及到三方，即支付处理方（支付结算中心）、服务提供者（商家服务器）和用户（用户终端）。与前面会员制系统不同的是，它们之间（包括支付结算中心与商家之间）完全是通过 Internet 网进行通信。

169 卡系统构成如图 A4 所示。

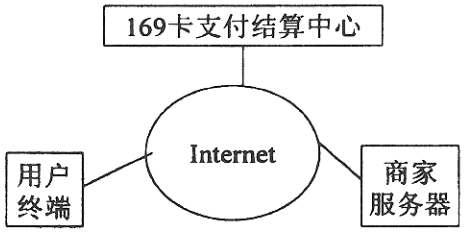


图 A4　169 卡支付系统构成图

1) 支付结算中心的功能如下：

a) Internet 网业务中心设置专门的支付结算中心，发行 169 卡，该卡仅用于在我国 Internet 网内获得服务时使用；

b) 该中心负责管理加入到该中心的用户和商家的账号，保存用户预交的现金，并在用户和商家之间进行转账。

2) 用户。想使用 169 卡享受服务的用户首先需要在 169 卡支付结算中心开设账号，并在账号中存入现金；

3) 商家。在 Internet 网上进行有偿服务的商家也需要在 169 卡支付结算中心开设账号，用于在提供服务时与用户进行结算。

A2.2　认证及数据加密技术要求

A2.2.1　身份认证

169 卡系统中，交易需经过三方的处理才能完成，因此需要对参与交易的三方身份进行认证。对三方的身份认证可分解为几部分，即用户和商家之间的身份认证；商家和支付结算中心之间的身份认证；支付结算中心和用户间的身份认证。此时的基本流程应符合 6.4 节和 6.5 节中的规定。通信的三方都需要有签名公钥，这些公钥必须由 Internet 网 CA 中心颁发的证书来保证，即它们的签名公钥证书应由 Internet 网 CA 中心统一签发，有关内容应符合第 9 章的规定。身份认证流程应符合 8.3 节（数字签名）和 8.4 节（双重数字签名）中的规定。

A2.2.2　信息认证

为保证用户、商家和支付结算中心之间通信时各方接收到的数据的完整性，应当使用数字签名技术，此时用户和商家都需要有签名公钥证书，它们的签名公钥证书应由 Internet 网 CA 中心统一签发，有关内容应符合第 9 章的规定。具体流程应符合 6.2 中的相应规定，使用的技术应符合 8.3 节和 8.4 节中的相应规定。

A2.2.3　数据加密

用户的服务请求和支付信息需要加密传送到商家及支付结算中心。数据加密应符合 8.1.1 节中的对称密钥加密技术规定。有关对称密钥的分发应符合 8.2 节中数字信封技术的规定。而此时用到的加密公钥的证书应由 Internet 网 CA 中心统一签发，有关内容应符合第 9 章的规定。

A2.2.4　私钥和公钥证书的保护

私钥和公钥证书的保护使用软件安全模块。因为私钥和公钥证书是系统安全的重点，系统某一端私钥和公钥证书的被窃和被替换将摧毁整个系统的安全性。因此该保密模块的安全级别应根据具体业务的安全要求决定。同时整个系统的对称加密算法和非对称加密算法的加密强度也应由具体业务的安全要求决定。

A2.3　业务流程

业务流程如图 A5 所示。

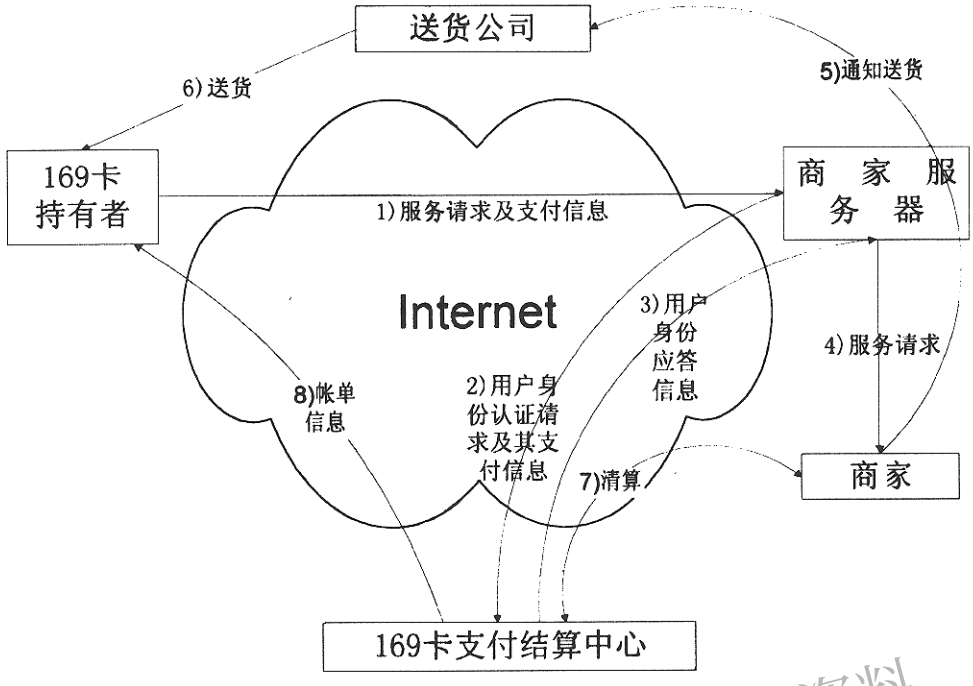


图 A5　使用 169 卡支付系统的业务流程

1) 169 卡用户访问商家服务器，进行商品浏览，向商家服务器发出服务请求及付款请求，使用 169 卡进行支付，支付信息中包含自己的 169 卡号信息，请求信息中包括自己的身份认证和信息认证信息（具体认证信息的内容应符合 8.4 节中的规定），其中对服务请求和支付信息的加密过程应分别符合 8.2 节的规定（分别使用商家和支付结算中心的加密公钥进行加密）；

2) 商家服务器接受用户加密后的服务请求、付款请求及相关的认证信息，保留用户的服务请求和相关的认证信息并解密该信息，进行验证；

3) 验证通过后，商家服务器将用户加密后的付款请求、商家自己的身份信息（使用 8.2 节中的方式加密）及相关的认证信息等发给 169 卡支付结算中心请求用户身份认证和转账，支付结算中心解密用户的支付请求和商家的身份信息（具体流程应符合 8.2 节的规定）；

4) 商家服务器和 169 卡支付结算中心与用户之间进行身份认证。

a) 商家服务器和 169 卡支付结算中心根据用户端发来的双重数字签名信息进行用户的身份认证和信息认证（符合 8.4 节规定）；

b) 用户根据商家服务器发给自己的响应信息中的数字签名及数字证书信息认证商家（符合 8.3 节的规定）；

c) 商家服务器和支付结算中心根据请求响应中各自的数字签名和数字证书进行身份认证（符合 8.3 节的规定）；

有关数字证书的管理和分发应符合第 9 章中的相应规定。

5) 认证通过后，169 卡支付结算中心授权商家服务器为用户提供服务。

a) 用户购买硬件产品 —— 商家服务器将用户的服务请求通知商家，商家通知送货公司给用户送货；

b) 用户购买软件产品 —— 商城服务器授权用户下载软件产品。

6) 用户接收服务；

7) 商家向 169 卡支付结算中心发出转账（服务费）请求，与 169 卡支付结算中心进行清算；

8) 169 卡支付结算中心定期向用户发送用户消费的账单信息。

A3 Internet 网事务处理业务支付结算系统的建立

在建设 Internet 网上涉及到支付的事务处理业务的支付系统时，可以选用上面的会员制支付系统或 169 卡支付结算中心的方式。当 169 卡支付结算中心建立完善后，网上的许多业务可以利用这个系统进行统一的支付和结算。

A3.1 会员制支付系统的建立

当具体的业务要求选用会员制支付系统时，视以下情况进行选择。

1) 当会员系统在本地时，可以参考 A1 中的模式来实施；

2) 当会员系统不仅限于本地，如一个大公司在各地的分公司提供会员制服务时，系统的组织可参见 A2，但支付结算中心由内部管理部门建立，而不是由 Internet 网络管理中心建立；

3) 无论会员制系统在本地还是异地，实施时都只涉及到本系统内部，操作比较简单，支付结算都在本系统内部进行，但支付结算中心的建立需经 Internet 网相关管理部门批准；

4) 由于采用公钥数字证书方式进行身份认证，所以还要经过 CA 认证中心的认证才能开展业务。

A3.2 169 卡支付结算中心的建立

网上的许多业务都可以利用 169 卡支付结算中心进行统一支付结算。其实施模式参见 A2。

1) 169 卡支付结算中心可以由国家级的相关主管部门或其指定的有关部门来建设和管理；

2) Internet 用户可向 169 卡支付结算中心（或下级支付结算中心）申请开设 169 卡账号；

3) 具体业务需要使用 169 卡进行支付时，需由提供服务的商家向支付结算中心提出申请，并开设结算账号后，用户才能使用 169 卡进行这种业务的支付；

4) 全国各省份事务处理业务涉及到的支付结算业务可以直接由 169 卡支付结算中心来承担，此时用户和商家的账号必须直接设在 169 卡支付结算中心；

5) 对于支付业务需求大的省份，可以在本省网络管理中心设置下级 Internet 网支付结算分中心；

6) 当设立省内支付结算中心（作为 169 卡支付结算中心的下级结算中心）时，对于省内的（本地）业务，用户认证和与商家的支付结算在省内结算分中心进行；

7) 对于跨省的（异地）业务，用户的支付请求需发给用户开户地进行用户的身份认证和与商家的支付结算，即通过 169 卡支付结算中心进行两级结算，流程图如图 A6 所示，流程如下：

(1) A 省用户向 B 省商家发出服务请求及支付请求；

(2) B 省商家接受用户的服务请求，将 A 省用户的支付请求发给 B 省支付结算中心请求身份认证及支付；

(3) B 省支付结算中心判断该用户不是本省用户，将用户的支付请求信息发给全国 169 卡支付结算中心；

(4) 全国 169 卡支付结算中心判断用户身份，将用户的支付请求信息发给用户的开户地 A 省支付结算中心；

(5) A 省支付结算中心对全国 169 卡支付结算中心发来的用户的支付信息进行认证，向全国 169 卡支付结算中心发回用户身份认证信息；

(6) 全国 169 卡支付结算中心把用户的身份认证结果传给 B 省支付结算中心；

(7) B 省支付结算中心接受到 B 省支付结算中心传来的 A 省用户的身份认证结果后，授权 B 省商家为 A 省用户提供服务；

(8) B 省商家为 A 省用户提供服务；

(9) 全国 Internet 网支付结算系统定期根据系统记录的漫游支付信息（即通过全国 169 卡支付结算中心转发的认证及支付请求）在全国各下级结算系统之间进行结算和转账；

(10) 系统定期与商家进行清算，并给用户和商家发送结算清单，以供用户和商家查阅。

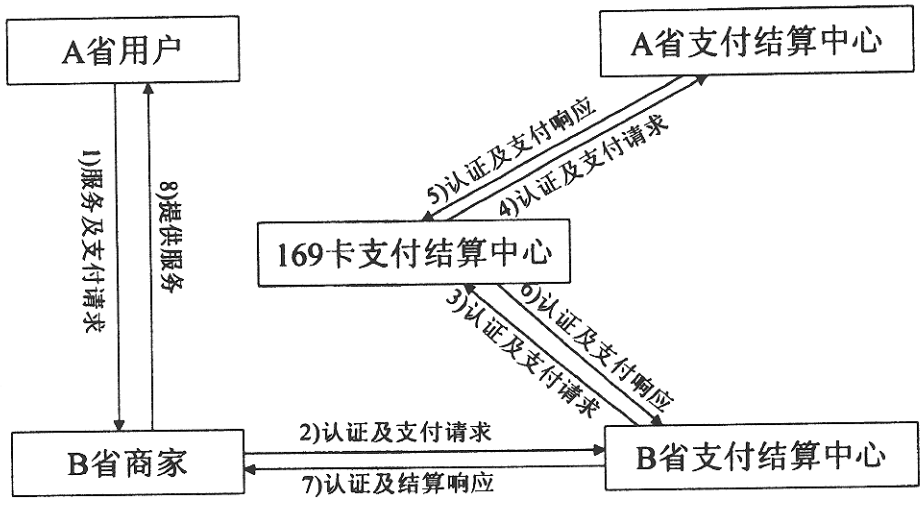


图 A6　169 卡异地支付结算流程

附录 B
(提示的附录)
使用数字货币进行支付的实现流程

本附录提供了在公共网络上如何实现使用数字货币进行支付的业务系统的流程，它是一个在公共网络上建立在线购物业务系统的参考。本附录引用了前文的第 6 章、第 7 章、第 8 章的相关规定。

B1 通用数字货币

B1.1 实现通用数字货币的系统构成

该系统通常由三方构成。

a) 支付处理方（货币发行服务器），这里指通用数字货币发行方，通常由货币发行服务器构成，其功能如下：

—— 注册和管理用户和商家的账号；

—— 可以发行和出售数字货币；

—— 验证用户支付给商家的货币的真实性；

—— 用一个大型数据库存储使用过而尚未过期的数字货币的序列号以验证数字货币是否被重复消费；

—— 将用户的数字货币转入用户的现金账号中，或将过期数字货币更新（对过期的数字货币赋予新的 ID 号）；

—— 将商家数字货币账号中的数字货币转入商家的现金账号中。

b) 服务提供者（服务提供者服务器），以下简称商家，其功能如下：

—— 需建立和管理自己的 Web 站点、制定服务价格、提供服务，将用户的支付信息发给货币发行服务器；

—— 在支付处理方开设现金账号以与用户结算。

c) 被服务方（用户终端，以下简称用户），用户端的软件可以看成是一个电子钱包，它与客户端浏览器配合，其功能如下：

—— 购买和存储经过数字货币发行服务器签名的数字货币；

—— 使用经过签名的数字货币进行支付；

—— 与支付服务器配合更新过期数字货币或将用户已购买的数字货币转换为现金；

—— 在支付处理方（与服务提供者使用相同的支付处理方）建立一个现金账号并存入一定的金额用以购买数字货币。

其结构如图 B1 所示。

B1.2 业务流程

B1.2.1 用户购买数字货币

用户可以根据自己的可能需求选择购买不同面值的数字货币，即用自己现金账号中的货币换取货币发行服务器发行的数字货币。

其流程如下：

a) 用户和货币发行服务器相互进行身份认证后（认证加密过程见第 6 和第 8 章），用户的电子钱包将自己的身份信息和要购买的数字货币数额及面额信息加密后传送至货币发行服务器；

b) 数字货币发行服务器将用户端传过来的信息解密，检查用户现金账号中的资金是否充足，若是，则按用户请求数字货币的数额和面额产生相应的数字货币，并对货币进行签名，同时从现金账号中扣除相应的数额，并将经过签名的数字货币加密后发回给用户的电子钱包；

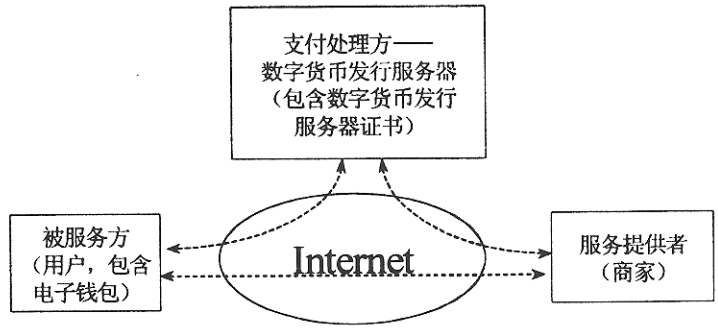


图 B1　实现通用数字货币的系统构成

c) 用户的电子钱包接收发回来的数据，解密后得到经过签名的数字货币，用数字货币发行服务器的公钥验证货币的真实性。

其流程如图 B2 所示。

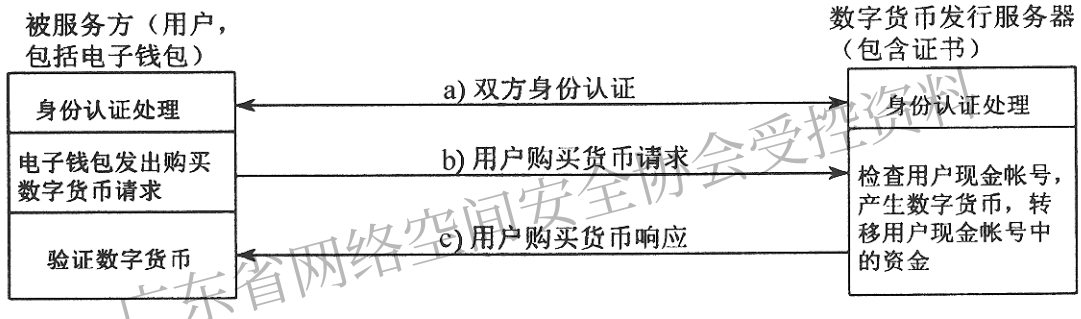


图 B2　购买数字货币处理流程

支付处理方货币发行服务器发行的数字货币中应包括以下内容：

a) 货币发行服务器的 IP 地址或主机名。

b) 过期时间 —— 指数字货币有效的截至时间。

c) 序列号 —— 货币发行服务器以此检查数字货币是否被重复消费。

d) 数字货币的面值。

B1.2.2　支付处理方和商家为用户提供服务

其流程如下：

a) 用户在商家站点选择需要的服务，点取支付按钮；

b) 支付按钮激活客户端的电子钱包，将应付的经过货币发行服务器签名的数字货币加密；

c) 电子钱包将用户的服务需求和经过加密的支付请求传送到商家服务器；

d) 商家服务器接收用户的服务请求，并在与支付处理方进行身份认证后将用户的加密支付信息连同自己的身份信息传送至货币发行服务器；

e) 货币发行服务器将用户的支付信息解密；

f) 货币发行服务器检查这些数字货币的有效时间看是否过期；

g) 货币发行服务器用自己的公钥验证数字货币中数字签名的真实性；

h) 验证通过后，货币发行服务器将这些数字货币的序列号与数据库中已有的货币序列号进行对比，以确认这些货币是否被重复使用；

i) 若未重复消费，则将这些货币的序列号及过期时间存入数据库中，并清除数据库中的过期货币；

j) 数字货币发行服务器通知商家给用户提供服务；

k) 商家为用户提供服务；

l) 货币发行服务器将用户支付的数字货币转入商家的现金账号中。

其流程如图 B3 所示。

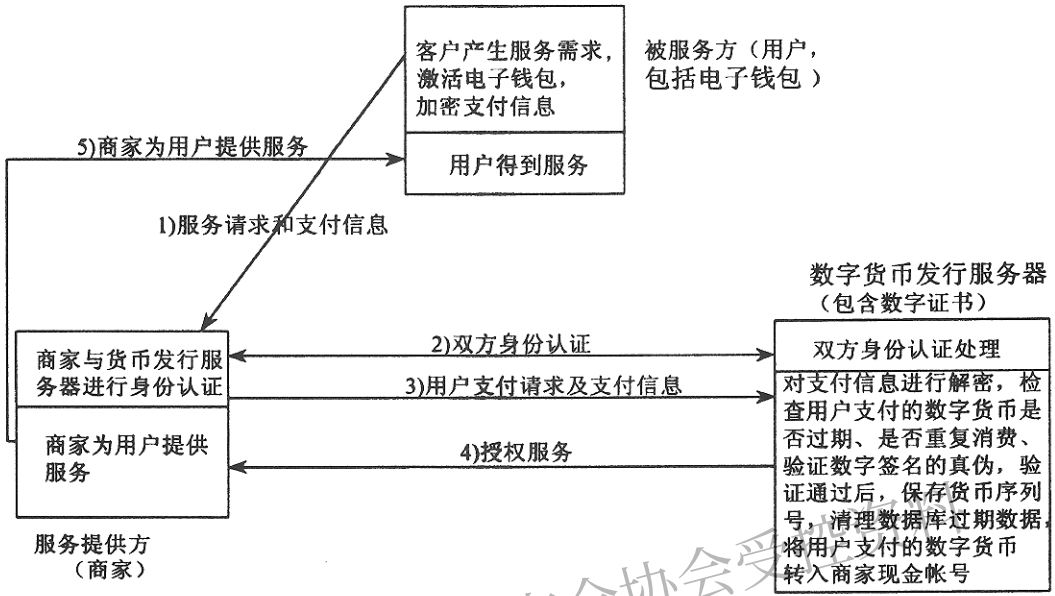


图 B3 使用通用数字货币为用户提供服务的流程

B1.3 系统管理

B1.3.1 数字货币的管理

1) 更新数字货币

为避免用户用数字货币进行重复消费，支付处理方需要一个大型的数据库来保存使用过的数字货币序列号，并要定期检查数据库中数字货币的有效时间，以清除过期货币序列号，降低数据库容量。这样，当用户更新数字货币时，数字货币发行服务器对过期的数字货币则应予以销毁，以防止恶意用户将使用过的数字货币在长时间后进行更新，而数字货币发行服务器系统又检测不出来，使得整个系统的完整性被破坏。

用户更新数字货币的需求包括：

—— 定期对自己电子钱包中的数字货币进行更新，以防超过过期时间而在消费或更新货币时被销毁；

—— 更换数字货币面值，以便在享受服务时方便支付。

用户用自己的电子钱包更新数字货币的流程如下：

a) 用户的电子钱包将需要更新的数字货币和要更换的数字货币的面额信息经加密后传送到货币发行服务器；

b) 货币发行服务器将用户数据解密，得到要更新的数字货币；

c) 货币发行服务器用自己的公钥验证数字货币中数字签名的真实性；

d) 货币发行服务器检查用户数字货币中的有效时间，看货币是否过期；

e) 货币发行服务器将这些数字货币的序列号与数据库中已有的货币序列号进行对比，以确认这些货币是否被使用过；若未重复消费，则将这些货币的序列号及过期时间存入数据库中；

f) 数字货币发行服务器根据用户申请的数额和面额信息产生新的数字货币，并对这些货币作数字签名，以证实数字货币的有效性；

g) 货币发行服务器将经过签名的新的数字货币加密后发回给用户的电子钱包；

h) 用户的电子钱包接收发回来的数据，解密后得到新的数字货币，用货币发行服务器的公钥验证新的数字货币的真实性。

其流程如图 B4 所示。

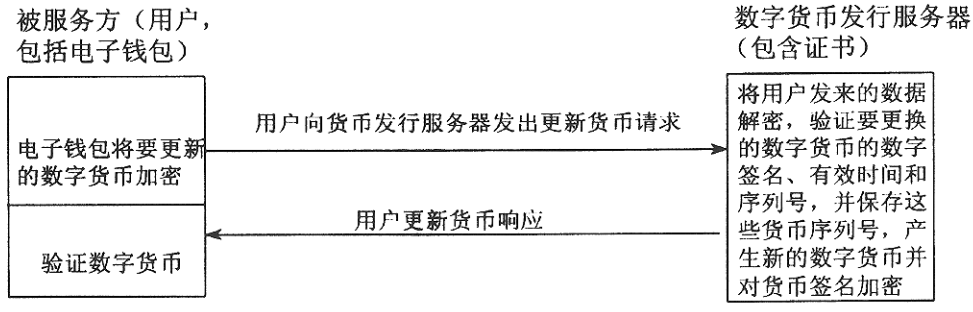


图 B4　数字货币的更新流程

2) 将用户电子钱包中的数字货币返回用户现金账号中

用户可以将自己电子钱包中的数字货币转入自己的现金账号中。流程如下：

a) 用户和货币发行服务器相互进行身份认证后（认证加密过程见第 6 和第 8 章），将经过货币发行服务器签名的要退还的数字货币连同自己的现金账号信息加密后传送到货币发行服务器；

b) 货币发行服务器将用户端加密过的信息解密；

c) 货币发行服务器用公钥验证数字货币中数字签名的真实性；

d) 货币发行服务器检查用户数字货币中的有效时间，若过期，则将用户提交的数字货币销毁；

e) 货币发行服务器将这些数字货币的序列号与数据库中已有的数字货币序列号进行对比，以确认这些货币是否被使用过；

f) 验证通过后，数字货币发行服务器将用户端传过来的数字货币的序列号存入数据库中，表明这些数字货币已被消费；

g) 货币发行服务器将这些数字货币的价值存入用户的现金账号中，给用户发回一条响应信息，交易完成。

其流程如图 B5 所示。

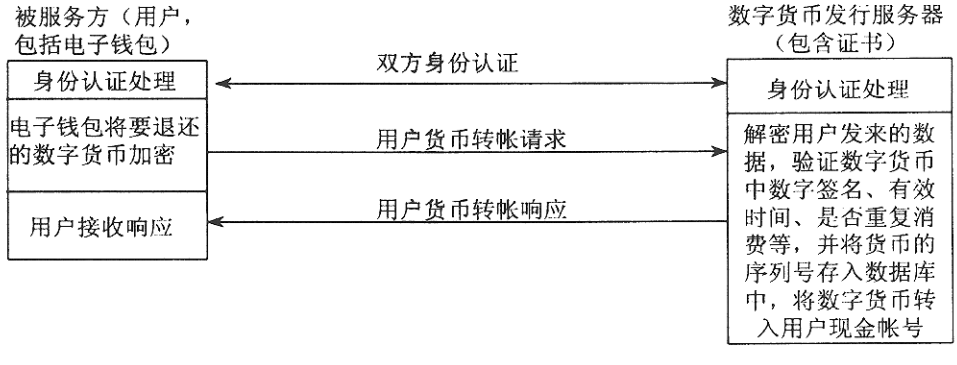


图 B5　数字货币的退还流程

3) 数字货币的“找零钱”问题

数字货币实质上是模拟现实生活中的现金交易模式来实施的，因此它也具有货币的一个重要特性，即也具有面值，因此也就有“找零钱”的问题。流程如下：

a) 当B1.2.2中支付处理方和商家为用户提供服务的步骤i)对用户支付的数字货币验证通过后，发现用户支付的数字货币多于服务价格，数字货币发行服务器产生一个新的数字货币以存储“应找回的”货币的价值，并对该货币进行数字签名，以证实数字货币的有效性；

b) 货币发行服务器将经过签名的数字货币加密发回给用户的电子钱包；

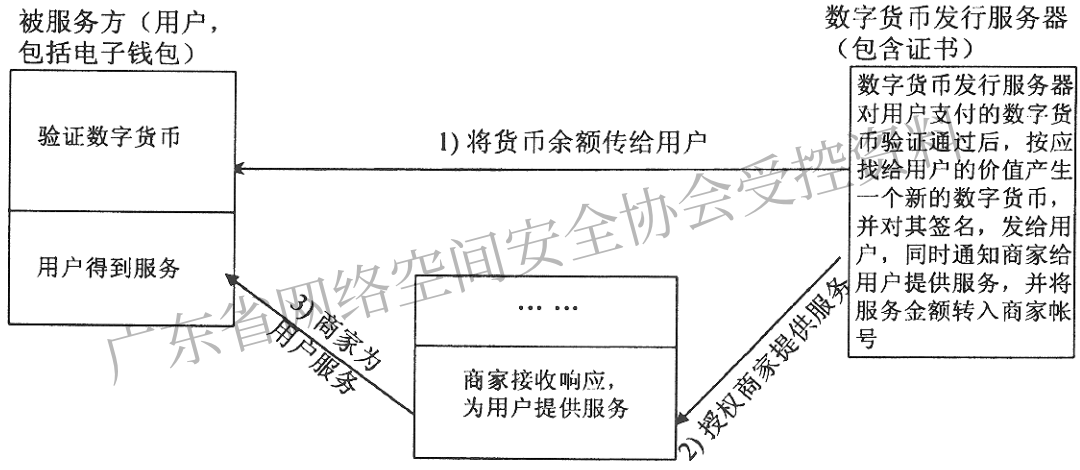
c) 用户的电子钱包接收发回来的数据，解密后得到“找回来的”数字货币，用货币发行服务器的公钥来检验货币中的数字签名以验证货币的真实性；

d) 数字货币发行服务器通知商家给用户提供服务；

e) 商家为用户提供服务；

f) 货币发行服务器将用户最初发来的数字货币总值减去“找给用户的零钱”后转入商家的现金账号中。

其流程如图B6所示。



图B6　数字货币的“找零钱”过程

B1.3.2　服务提供者的管理

A) 系统应当对支付处理方对支付请求的认证响应作日志，并在规定的时间内保留日志，以便查阅；

B) 对系统服务器的后台访问和管理要进行一定的限制和安全保护，保证系统的重要信息（包括系统日志文件、用户的私人信息等）以及在服务器上保存的用户支付信息的安全；

C) 保证系统的硬件和环境的安全。

B1.3.3　支付处理方的管理

A) 为保证数字货币发行服务器发行出来的货币的可靠性，数字货币发行服务器需要由政府来担保。具体可以通过使用数字签名来实现，即政府的证书授权机构给数字货币发行服务器的公钥发证并对证书进行数字签名，以确保所发行的数字货币与现实生活中的现金货币一样具有法律效应；

B) 由于数字货币中不包含用户信息，所以满足用户的匿名要求，但为系统跟踪恶意用户的行为带来一定的困难。支付处理方应当对用户的支付请求和认证响应作日志，这样当系统经常受到干扰或收到用户的抱怨、产生纠纷时，可根据系统日志检测恶意用户的请求以跟踪检测恶意用户；

C) 对系统服务器的后台访问和管理要进行一定的限制和安全保护，保证系统的重要信息（包括系统日志文件、用户的私人信息、数字证书及相关的公钥等）以及在服务器上保存的用户支付信息的安全；

D) 保证系统的硬件和环境的安全；

E) 如果支付处理系统建立认证中心，则应符合认证中心的安全及管理要求。

支付处理方的收入来源不是对用户使用数字货币的每一笔交易收取手续费，而是在现金账号和数字货币相互转换时根据转换的总数按比例收取手续费。例如在用户购买数字货币时，或将现有电子钱包中的数字货币转入现金账号中时，商家将收到的数字货币转入现金账号中时均按比例缴纳费用。

B2 专用数字货币的实现模式

B2.1 实现专用数字货币的系统构成

该系统通常由三方构成。

a) 经纪人方（货币发行服务器），其功能如下：

—— 负责注册、管理用户和商家账号；

—— 发行经纪人数字货币；

—— 向用户出售经纪人数字货币；

—— 发行商家货币；

—— 向用户出售商家货币；

—— 建立一个大型数据库存储使用过而尚未过期的经纪人数字货币的序列号以验证数字货币是否被重复消费；

—— 提供经纪人数字货币与各商家数字货币、以及各商家数字货币之间的转换；

—— 将用户的数字货币转入用户的现金账号中；

—— 将数字货币更新（对过期的数字货币赋予新的 ID 号）。

b) 服务提供者（商家服务器），以下简称商家，其功能如下：

—— 建立和管理自己的 WEB 站点、制定服务价格、提供服务；

—— 发行商家自己的货币；

—— 建立一个大型数据库存储使用过而尚未过期的商家自己的数字货币的序列号以验证数字货币是否被重复消费；

—— 验证用户支付的数字货币是否真实；

—— 在经纪人处开设现金账号用以与经纪人结算，并授权支付处理方发行自己的数字货币。

c) 被服务方（用户终端，以下简称用户），用户端的软件可以看成是一个电子钱包，它与浏览器配合，其功能如下：

—— 购买和存储经纪人及商家数字货币；

—— 在经纪人数字货币和商家数字货币之间进行转换；

—— 与服务器配合将用户已购买的数字货币转入现金账号中；

—— 用商家数字货币购买在线服务；

—— 在经纪人处开设现金账号，并存入一定的金额用以购买经纪人或服务提供者的数字货币。

其结构如图 B7 所示。

B2.2 业务流程

B2.2.1 服务双方建立账号

服务双方在利用数字货币进行交易之前，首先要在经纪人处开设账号。用户在经纪人处开设现金账号，并往账号中存入现金；商家同样在支付处理方开设现金账号，并授权支付处理方生产自己的数字货币。

在这种模式中，用户的数字货币账号在用户购买一个新的数字货币时由服务提供者分配，即购买经纪人数字货币时由经纪人分配一个用户账号，保存在经纪人数字货币的用户 ID 中；购买商家数字货币时由商家分配一个用户账号，保存在商家数字货币的用户 ID 中。

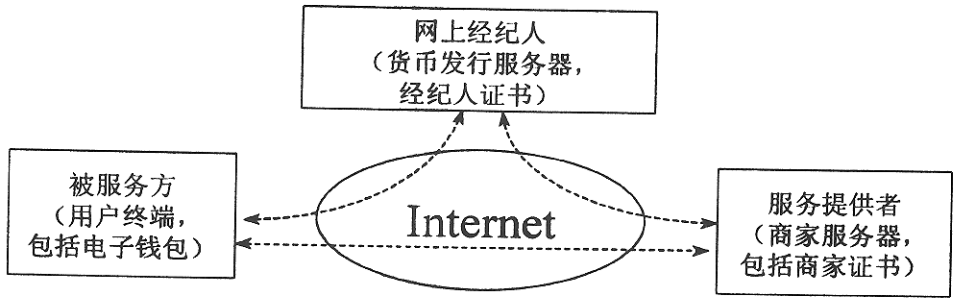


图 B7　实现专用数字货币的系统构成

B2.2.2　业务流程

经纪人和商家都要发行数字货币。

数字货币中应包括以下内容：

A) 服务提供者身份；

B) 货币面值；

C) 货币 ID 号；

D) 用户 ID 号（用来产生双方传输用的对称密钥）；

E) 过期时间；

F) 证书（指数字签名，防止假冒、篡改）。

经纪人除发行自身货币外，还被所代理的商家授权发行商家数字货币。商家授权经纪人发行自己的数字货币时，需要将数字货币中的货币 ID 号和用户 ID 号规定好送给经纪人。这种方式要求经纪人和商家要有良好的信任关系。

B2.2.2.1　用户和商家在同一经纪人处开设账号

这种情况下使用专用数字货币的服务流程大致可分为以下几步：

a) 用户用现金账号中的钱购买经纪人数字货币；

b) 经纪人将货币连同相关的对称密钥返回给用户；

c) 用户用已购的经纪人数字货币向经纪人申请购买某一商家货币；

d) 经纪人将商家货币连同相关的对称密钥返回给用户，并将多余的货币仍以经纪人货币返回给用户；

e) 用户用该商家货币享受该商家的服务；

f) 商家将多余的货币用商家自己的数字货币找给用户。

经纪人与商家要定期进行结算。结算方式是经纪人按商家收到的数字货币总额付给商家费用，转入商家的现金账号。经纪人从这笔总额中抽取一定的比例作为自己的服务费。

其流程如图 B8 所示。

其中详细流程如下面各节的描述。

1) 用户购买经纪人货币的流程如下：

a) 用户端软件（即电子钱包）向经纪人发出购买经纪人数字货币的请求，双方进行身份认证，认证加密过程见第 6 章和第 8 章；

b) 双方身份认证通过后，用户将自己的身份信息和购买货币的数额信息加密传送至经纪人服务器；

c) 经纪人解密传过来的数据，检查用户现金账号中的资金是否充足，若是，则产生数字货币，其中含经纪人身份信息、货币面值、货币 ID 号、用户 ID 号、过期时间以及经纪人的签名信息；

d) 经纪人根据分配给该用户的唯一的用户 ID 号产生一个密钥，该密钥作为对称密钥用来对今后双

方传输的数据进行加密；

e) 经纪人对该数字货币进行签名；

f) 经纪人将产生的数字货币连同密钥和数字签名一起加密传给用户的电子钱包；

g) 电子钱包将发来的数字货币解密，并根据经纪人的数字签名验证货币的真伪。

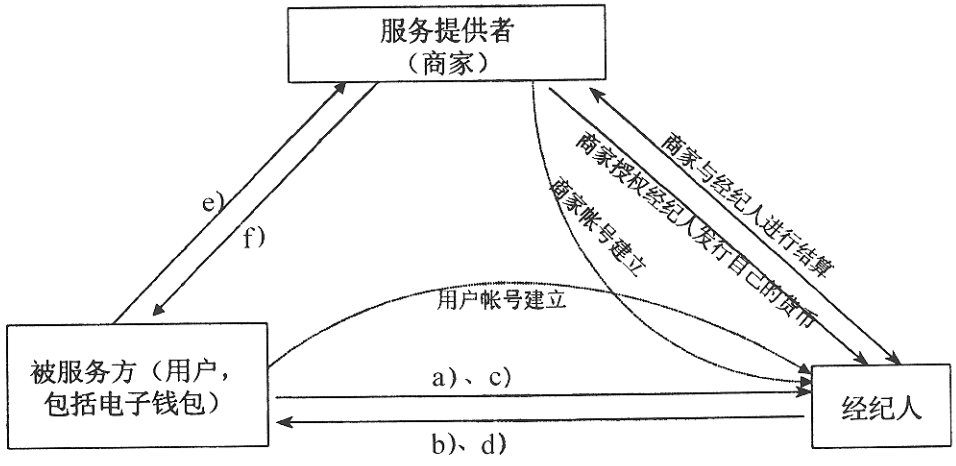


图 B8　专用数字货币的实现模式一（单个经纪人）

以上过程应当建立在传统的安全加密协议之上，以确保用户账号信息、传回来的数字货币和对称密钥的安全。其流程如图 B9 所示。

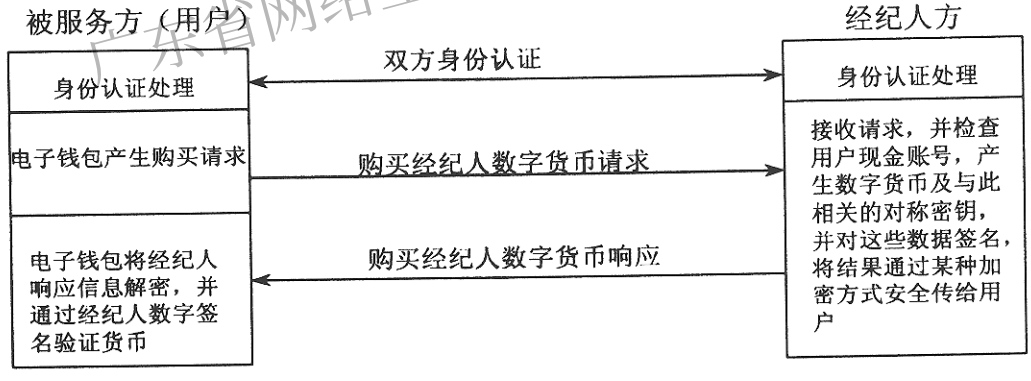


图 B9　用户购买经纪人数字货币实现流程

2) 用户购买商家货币

用户在网上浏览期间，发现某一商家提供的服务符合自己的要求，而电子钱包中没有该商家的数字货币，这时购买商家数字货币的流程如下：

a) 电子钱包将用户将要购买某商家数字货币的请求、已购得的经纪人数字货币，以及用户的对称密钥（在购买经纪人数字货币时得到的）一起作散列运算，将结果连同用户的请求、经纪人数字货币发给经纪人服务器；

b) 经纪人服务器收到用户的请求后，根据发来的数字货币中的用户 ID 号运算得到用户的对称密钥，再将该对称密钥连同用户发来的请求和数字货币一起作散列运算，以验证货币的真实性；

c) 经纪人服务器检查用户发来的数字货币是否过期；

d) 经纪人服务器根据货币的序列号查询经纪人数字货币数据库，以核实该数字货币是否被重复消

费，若证实没有重复消费，则将该货币的序列号记录入数据库中；

e) 验证通过后，经纪人将用户要购买的根据商家的授权产生的数字货币、与该数字货币中用户 ID 号对应的对称密钥用用户现有的经纪人数字货币的对称密钥加密，将运算结果与找给用户的余额（以经纪人数字货币支付，货币序列号改变，用户 ID 号不变）连同经纪人的数字签名一起发给用户的电子钱包；

f) 用户电子钱包用经纪人数字货币的对称密钥将发来的数据进行解密，得到商家的数字货币和与此对应的对称密钥，并根据数字签名验证发来的数据的真伪。

其流程如图 B10 所示。

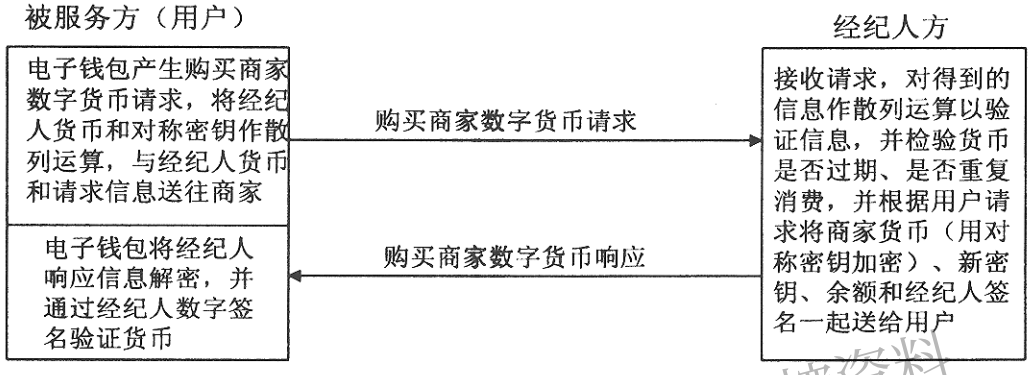


图 B10　用户购买商家数字货币实现流程

3) 商家为用户提供服务

a) 用户在商家站点发现自己需要的服务，发出服务请求和支付请求，激活用户的电子钱包，电子钱包检查自己是否有该商家的数字货币，若没有，则需用经纪人电子货币去购买商家电子货币（见前述）后继续交易；

b) 电子钱包将用户的请求、支付信息、与商家数字货币对应的对称密钥一起作散列运算，然后将结果和用户的请求及支付信息一起传给商家服务器；

c) 商家服务器根据用户发来的货币中的用户 ID 号得到用户的对称密钥，再将用户的对称密钥、用户请求、支付信息一起作散列运算，验证信息的真伪；

d) 商家服务器根据数字货币中的有效时间检查用户支付的数字货币是否过期；

e) 商家服务器根据数字货币中的序列号检索商家自己的数据库，以核实用户支付的数字货币是否被消费过，若未重复消费，则将该货币的序列号存入商家数据库中；

f) 验证通过后，将用户请求的服务，连同找给用户的余额（以商家数字货币支付，货币序列号改变，用户 ID 号不变）和商家的数字签名一起发给用户；

g) 用户通过数字签名验证商家发来的服务的真伪，享受服务。

其流程如图 B11 所示。

B2.2.2.2　用户和商家的账号不属于同一经纪人

当网上有多个经纪人时，用户申请服务的商家经纪人很有可能不同于自己开户的经纪人。此时的服务流程如下：

a) 用户向自己的经纪人申请购买商家的数字货币；

b) 用户经纪人向商家询问商家经纪人的身份；

c) 商家为用户经纪人提供商家经纪人的身份；

d) 用户经纪人向商家经纪人购买商家经纪人的数字货币；

e) 用户经纪人将商家经纪人的数字货币返回给用户；

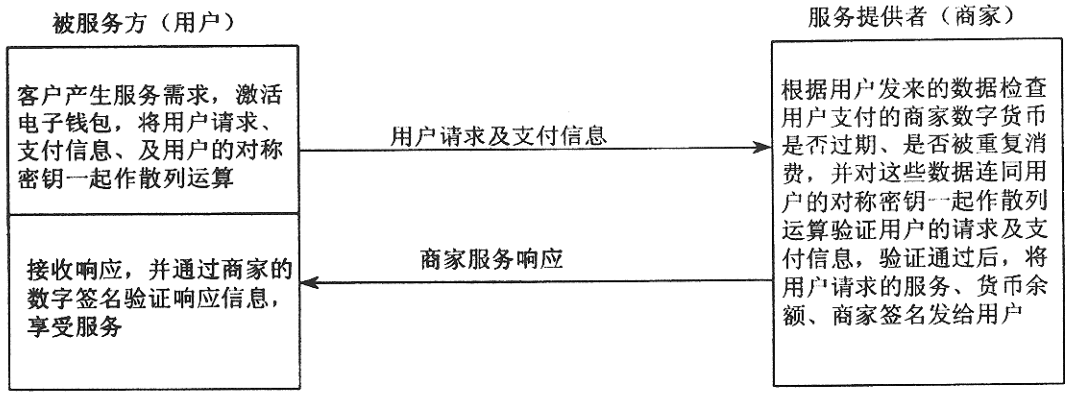


图 B11　用户使用商家数字货币享受服务的实现流程

f) 用户用商家经纪人的数字货币向商家经纪人购买商家数字货币；

g) 用户用商家数字货币享受商家的服务。

其流程如图 B12 所示。

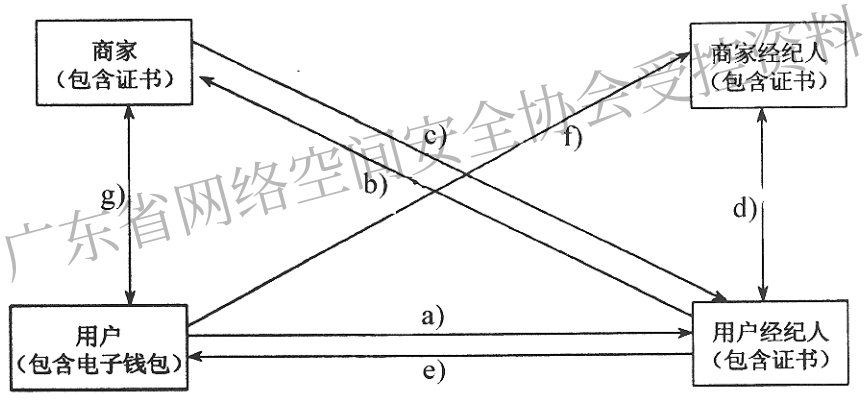


图 B12　专用数字货币的实现模式二（多个经纪人）

B2.3　系统管理

B2.3.1　数字货币的管理

1) 更新数字货币

a) 更新商家货币；

b) 更新经纪人货币。

2) 兑换数字货币

a) 把一个商家货币转换为另一个商家货币；

b) 把商家货币换成经纪人货币；

c) 把商家货币转入现金账号；

d) 把经纪人货币转入现金账号。

B2.3.2　服务提供者的管理

a) 系统应当对支付处理方对支付请求的认证响应作日志，并在规定的时间内保留日志，以便查阅；

b) 对系统服务器的后台访问和管理要进行一定的限制和安全保护，保证系统的重要信息（包括

系统日志文件、用户的私人信息、数字证书及相关的公钥等）以及在服务器上保存的用户支付信息的安全；

c) 为防止重复消费，服务提供者要建立大型数据库存储用户消费过的数字货币的序列号，并且要对数据库中过期的数字货币序列号定时清除，以防数据库过大；

d) 保证系统的硬件和环境的安全。

B2.3.3 支付处理方的管理

a) 支付处理方应当对用户的支付请求和认证响应作日志，这样当系统经常受到干扰或收到用户的抱怨，或产生纠纷时，可根据系统日志检测恶意用户的请求以跟踪检测恶意用户；

b) 对系统服务器的后台访问和管理要进行一定的限制和安全保护，保证系统的重要信息（包括系统日志文件、用户的私人信息、数字证书及相关的公钥等）以及在服务器上保存的用户支付信息的安全；

c) 为防止重复消费，服务提供者要建立大型数据库存储用户消费过的数字货币的序列号，并且要对数据库中过期的数字货币序列号定时清除，以防数据库过大；

d) 保证系统的硬件和环境的安全；

e) 如果支付处理系统建立认证中心，则应符合认证中心的安全及管理要求。

经纪人从商家购买数字货币时是对货币面值打折后购买的，而将这些数字货币卖给用户时是按照面值来卖以获得收入。

附录 C
(提示的附录)
在线订购业务技术要求

本附录提供了在公共网络上如何实现安全订购系统的流程，它是一个在公共网络上建立在线订购系统的参考。本附录引用了前文的第 6、7、8、9 章的相关规定以及附录 A 和附录 B 的相关内容。

属于 Internet 网络的事务处理的订购类业务从支付方式分类，可以分为预定方式、小额付费方式、预付卡支付方式等 3 类。

其基本过程是由用户通过网上浏览获取相关信息并确定自己所要购买的物件以后，向商家提出订购申请并进行身份认证，然后通过身份认证的用户向商家提交订购申请单，商家应答是否有能力提供该商品或服务，用户对是否接收服务进行最后确认。

此后牵涉到支付，可以分成以下 3 种：

a) 预定，即不在线进行支付，而是在商家提供服务以后直接面对面进行现金支付。

b) 小额付费，参见附录 A。

c) 预付卡支付，参见附录 B。

具体实现方式详细描述如下。

C1 预定方式

用户以非在线方式到认证中心登记，取得一个用户名、密码和密钥等。

用户在线向商家提出订购请求，并在商家提供了相应服务以后以非在线方式支付服务费用。此方式适用于网上订购机票、车票、船票，订宾馆客房、订花、订书等。

其具体流程如下面各节所述。

C1.1 用户浏览并决定是否订购

此处与一般的对于 Web 页的浏览并无区别，用户直接登录到商家所设立的站点进行查询。

C1.2 用户向商家提出请求

在商家的 Web 页上有一个按键，当用户激活这个按键时，激活一个进程，将有关消息传送到商家服务器。其数据格式如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 1；

长度占两个字节，为后面具体数据内容的长度，此处为 0；

具体数据暂时设置为空。

C1.3 商家要求用户进行身份认证

商家服务器的处理程序接收到用户的请求后，检查用户是否具有有效电子身份证，没有的情况下要求用户进行身份认证。依据用户的开户地点在商家还是在认证中心可以分为两种类型，即以弹出 Web 页的方式要求用户到认证中心进行身份认证和商家直接进行认证。

C1.3.1 到认证中心进行身份认证

以弹出 Web 页的方式要求用户到认证中心进行身份认证。用户向认证中心提供能确认身份的个人相关信息，个人信息中至少包括用户名、密码等，加密后发送给认证中心。

具体过程如下：

1) 用户看到来自商家的 Web 页后登录到认证中心，填写认证单 —— 至少应该包括用户的用户名和密码。

2) 用户点选在认证中心 Web 页的按键激活一个进程，该进程负责将用户加密后的有关信息传送到

认证中心。

其数据格式如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

类型 1 为一字节整数，此处设置为 2；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为经过用户随机产生的对称加密密钥加密的字符串。

类型 2 为一字节整数，此处设置为 3；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以认证中心的公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_auth(char *str1,int len1,char *str2,int len2,…);

其中 str 为所得的字符串，str1 为用户名，len1 为其长度，str2 为密码，len2 为其长度。

b) 将随机产生的对称加密密钥以认证中心的公开加密密钥加密：

char * str=encrypt_auth1(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

3) 认证中心对用户进行身份认证，并为通过认证的用户签发电子身份证，具体过程如下：

a) 认证中心服务器在接到用户传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以认证中心的私有加密密钥对该数据字段进行解密：

char *str=decrypt_auth1(char *str1,int len1);

其中 str 为解密后得到的由用户随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密用户身份信息：

char *str=decrypt_auth(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为用户认证信息加密后的字符串，len1 为 str1 长度。

c) 用认证中心数据库中数据检验用户身份。

d) 对未通过身份认证的用户，直接以 Web 页方式通知无权继续进行事物处理过程。

e) 对通过身份认证的用户发放电子身份证，至少包含以下内容：身份证版本号，认证中心域名或 IP，有效期，有效级别，用户名，用户 IP。例如：

01:10.0.0.1:1998-07-01-00-00-00:1:user:10.10.10.10

即表示由主机 IP 地址为 10.0.0.1 的认证中心所发放的电子身份证，版本号为 01，到 1998 年 7 月 1 日 0 点 0 分 0 秒前有效，有效级别为 1 级(级别区别由认证中心决定)，其用户名为 user，用户 IP 地址是 10.10.10.10。

C1.3.2 直接与商家进行身份认证

用户向商家提供能确认身份的个人相关信息，个人信息中至少包括用户名、密码等，加密后发送给商家。

具体过程如下：

1) 用户看到来自商家的 Web 页后，填写认证单 —— 至少应该包括用户的用户名和密码。

2) 用户点选 Web 页的按键激活一个进程，该进程负责将用户加密后的有关信息传送到商家。

其数据格式如下：

类型	长度	具体数据

类型为一字节整数，此处设置为 2；

长度为两字节整数，内容是后面具体数据内容的长度；

具体数据是经过商家公开加密密钥加密后的用户身份信息。

char * str=encrypt_auth2(char *str1,int len1,char *str2,int len2,…);

其中 str 为所得的字符串，str1 为用户名，len1 为其长度，str2 为密码，len2 为其长度。

3) 商家对用户进行身份认证，并给通过认证的用户发电子身份证。

具体过程如下：

a) 商家服务器在接到用户传来的信息后，以商家的私有加密密钥对该数据字段进行解密：

char *str=decrypt_auth2(char *str1,int len1);

其中 str 为解密后得到的信息，str1 为用户传来的加密串，len1 为 str1 长度。

b) 以商家数据库中数据检验用户身份。

c) 对未通过身份认证的用户，直接以 Web 页方式通知其无权继续进行事物处理过程。

d) 对通过身份认证的用户发放电子身份证，至少包含以下内容：身份证版本号，商家域名或 IP，有效期，有效级别，用户名，用户 IP。例如：

01:10.0.0.3:1998-07-01-00-00-00:1:user:10.10.10.10

即表示由主机 IP 地址为 10.0.0.3 的商家所发放的电子身份证，版本号为 01，到 1998 年 7 月 1 日 0 点 0 分 0 秒前有效，有效级别为 1 级(级别区别由商家决定)，其用户名为 user，用户 IP 地址是 10.10.10.10。

C1.4 用户再次向商家提出申请

具体过程如下：

1) 商家服务器验证电子身份证后要求用户填写订购物品申请表。

2) 用户按项目填表，并激活一个进程，将用户相关数据传输到商家服务器，此处要采用完整性处理（原文＋原文的数字签名字符串）。

例如填写一张关于订飞机票的申请如下：

姓名：	身份证号：
航班：	种类：
时间：	数量：

其数据格式如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 3；

长度为两字节整数，内容为后面具体数据内容的长度；

具体数据的结构如下：

代码	长度	数据……
代码	长度	数据……
代码	长度	数据……
……		
加密字符串		

代码域为一字节整数，表示项目名：

=1：姓名；

=2：身份证号；

=3：航班号；

=4：日期；

=5：票种；

=6：张数；

……。

长度为相应项目内容的长度；

数据是用户所填写的内容；

数字签名字符串是以用户的私有密钥对以上数据的 Hash 运算结果签名后所得的字符串：

char *str=encypt_request(char *str1,int len1)；

其中 str 为所得字符串，str1 为原始输入字符串，len1 为其长度。

C1.5 商家获得用户购买信息

具体过程如下：

1) 商家服务器在接到用户传来的信息后，首先取出签名字符串部分。

2) 商家服务器以用户的公开密钥解密签名字符串：

char *str=decrypt_request(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为签名字符串，len1 为 str1 长度。

3) 对接收到的原文进行 Hash 运算，将运算结果与解密得到的字符串相比较，如果相同则继续处理，否则以 Web 页方式要求用户重新申请。

C1.6 商家通知用户能否提供服务

确认申请无误后，商家服务器根据用户申请查询库存信息，确定能否为用户提供服务。如果可以，用 Web 页方式要求用户确认是否接受服务，否则，以 Web 页方式通知用户不能提供服务。

C1.7 用户进行服务确认

用户作出是否接受服务的确认(或取消)；

用户确认(或取消)时将激活一个进程，传送加密后的确认信息给商家服务器。其数据格式如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 4；

长度为两字节整数，内容为后面具体数据内容的长度；

具体内容是使用商家的公开加密密钥加密后的确认字符串。

char *str=encrypt_sign(char *str1,int len1);

其中 str1 为确认(或取消)信息，len1 为其长度。

C1.8 商家提供服务并收取费用(非在线)

1) 商家接到用户的确认(或取消)信息，以商家的私有加密密钥解密：

char *str=decrypt_sign(char *str1,int len1);

其中 str 为所得字符串，str1 为源串，len1 为其长度。

2) 如果是确认信息，则保存用户的购买清单以及确认信息，提供非在线服务，并非在线收取费用，否则不做处理。

具体流程根据认证方式的不同分别如图 C1 和图 C2。

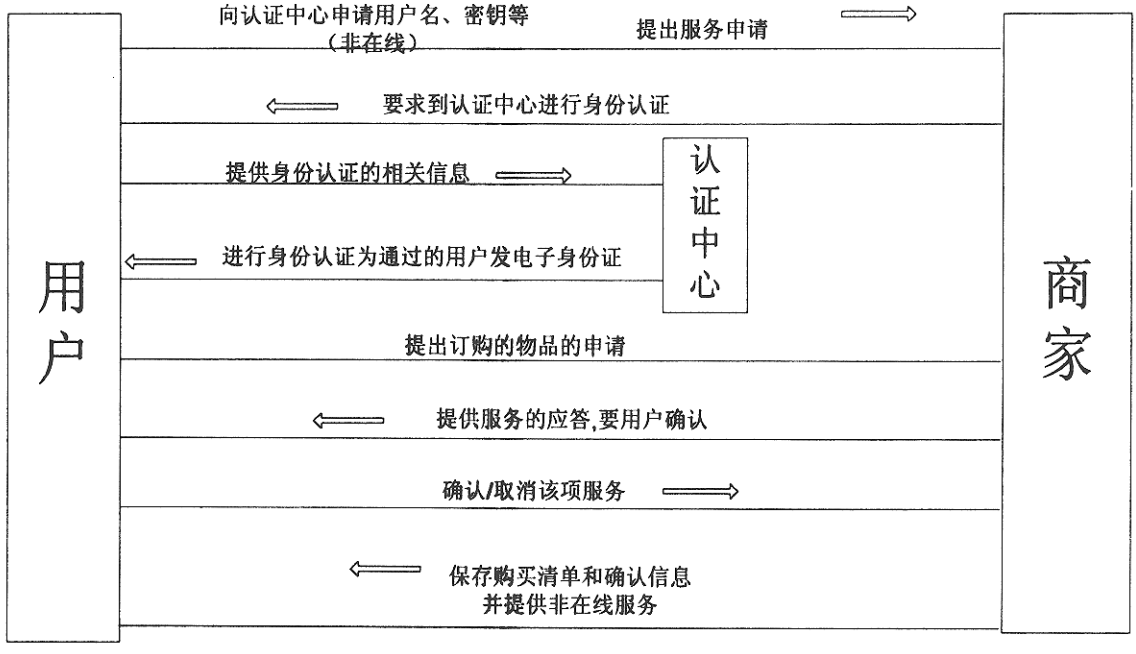


图 C1　基于到认证中心认证的预定方式的流程

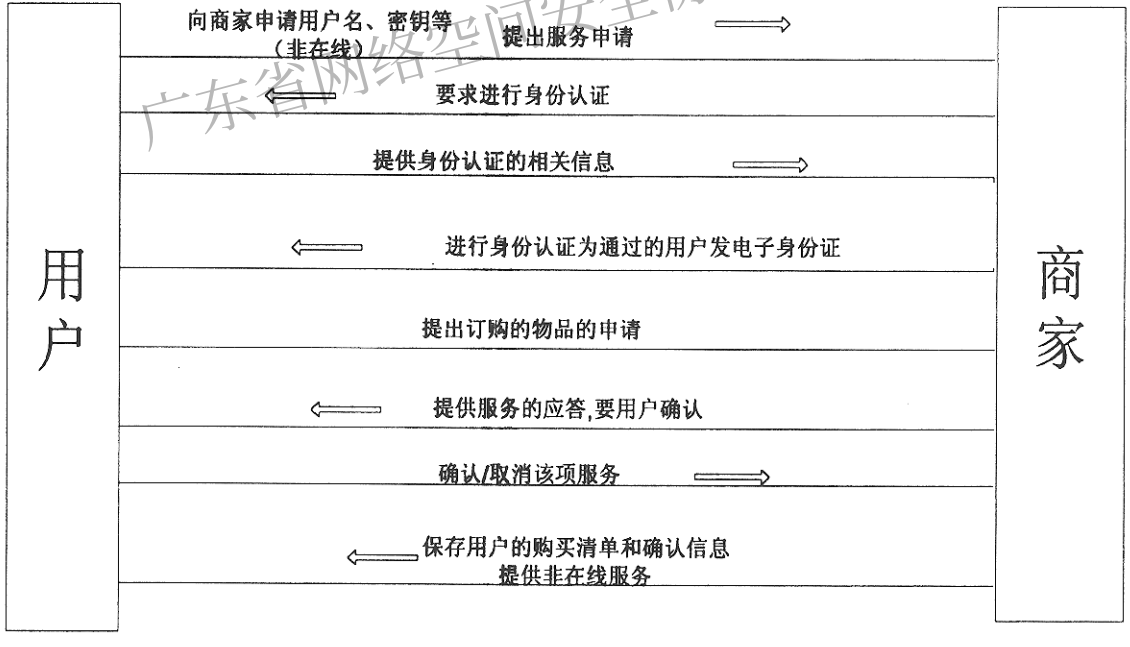


图 C2　基于到商家认证的预定方式的流程

C2　预付卡支付方式

用户首先以非在线方式向结算中心登记注册，申请一个可以存入和划账的账号并存入资金，同时得到密码和密钥。

用户向商家提出购物申请，得到相应服务，并由商家直接到结算中心从用户的账号或服务卡上划账。

此方式适用于商场购物等。

C2.1 用户浏览并确认是否订购

用户浏览商家的 Web 页并决定是否要定购。

C2.2 用户向商家提出请求

用户向商家发出购买申请，提出购买物品的请求，此处进行完整性处理（原文＋原文的数字签名）。

具体的过程与 C1.4 相同。

C2.3 商家获取用户的购买信息

具体过程与 C1.5 相同。

C2.4 商家通知用户能否提供服务

商家服务器检查自己的库存信息，确认自己能否为用户提供服务，然后要求用户传送自己的相关信息，即账号以及密码等。具体过程如下。

1) 用户填写有关信息，加密后传送给商家。

加密信息只有结算中心可以解密，商家得到的是一个加密字符串，而无法获得实际内容。

其数据格式如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 5；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为经过用户随机产生的对称加密密钥加密的字符串。

类型 2 为一字节整数，此处设置为 6；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以结算中心公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_account1(char *str1,int len1,char *str2,int len2,…);

其中 str 为所得的字符串，str1 为账号，len1 为其长度，str2 为密码，len2 为其长度。

b) 将随机产生的对称加密密钥以结算中心的公开加密密钥加密。

char * str=encrypt_account2(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

2) 商家服务器在接到用户传来的信息以后，首先将该信息与用户的购买清单一起保存，并向结算中心服务器发出检查用户账号的申请：传送自己的身份认证信息和未解密的用户信息以及用户购物所需资金到结算中心服务器；

其数据格式如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 7；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为以下数据经过商家服务器随机产生的对称加密密钥加密的字符串：

代码	长度	数据
代码	长度	数据
……		

代码为一字节整数表示后面内容的项目

1：服务器名；

2：商家密码；

3：未解密的用户信息；

4：所查金额；

……

长度为后面具体数据长度；

类型 2 为一字节整数，此处设置为 8；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以结算中心公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_account3(char *str1,int len1);

其中 str 为所得的字符串，str1 为原始数据，len1 为其长度。

b) 将随机产生的对称加密密钥以结算中心的公开加密密钥加密。

char * str=encrypt_account4(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

3) 结算中心对商家传送的信息进行解密，得到商家以及用户信息，具体过程如下：

a) 结算中心服务器在接到商家传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以结算中心的私有加密密钥对该数据字段进行解密：

char *str=decrypt_account4(char *str1,int len1);

其中 str 为解密后得到的由商家服务器随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密商家传送过来的信息。

char *str=decrypt_account3(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为商家传送过来的信息，len1 为 str1 长度。

c) 根据代码取出商家身份信息，用结算中心数据库中的数据检验商家身份。

d) 如果确认商家身份无效，拒绝继续进行事物处理；如果有效，则根据代码取出加密的用户账号信息。

e) 用结算中心的私有加密密钥对该数据字段进行解密：

char *str=decrypt_account2(char *str1,int len1);

其中 str 为解密后得到的由用户随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

f) 根据解得的对称加密密钥解密用户的账号信息。

char *str=decrypt_account1(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为用户的账号信息，len1 为 str1 长度。

g) 根据代码取出检验的资金额，用结算中心数据库的数据检验用户身份和资金。

4) 结算中心服务器对用户账号进行检查，并发反馈信息给商家服务器；

其数据格式如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 9；

长度为两字节整数，内容为后面具体数据内容的长度；

具体内容为用户账号资金情况：

0：资金不够；

1：资金正好；

2：资金充裕。

商家服务器接到用户资金足够的信息后反馈 Web 页要求用户确认服务，否则反馈 Web 页拒绝服务。

C2.5 用户进行服务确认

用户作出是否接受该服务的确认(或取消)，此处与 C1.7 相同。

C2.6 商家获取用户确认信息

具体过程如下：

1) 商家接到用户的确认信息，以商家的私有加密密钥将之解密：

char *str=decrypt_sign(char *str1,int len1);

其中 str 为所得字符串，str1 为源串，len1 为其长度。

2) 如果得到用户的确认信息，则保存用户确认信息，否则不做处理。

C2.7 商家通过结算中心服务器从用户的账号或服务卡中划账

具体过程如下：

1) 商家服务器在接到用户确认后向结算中心服务器要求划账。

传送自己身份认证信息到结算中心服务器。其数据格式如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 10；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为经过商家服务器随机产生的对称加密密钥加密的字符串。

类型 2 为一字节整数，此处设置为 11；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以结算中心的公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_paycheck1(char *str1,int len1,char *str2,int len2,...);

其中 str 为所得的字符串，str1 为商家注册名，len1 为其长度，str2 为密码，len2 为其长度。

b) 将随机产生的对称加密密钥以结算中心的公开加密密钥加密：

char * str=encrypt_paycheck2(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

2) 结算中心在接到商家请求后首先对应解密。

a) 结算中心服务器在接到商家传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以结算中心的私有加密密钥对该数据字段进行解密：

char *str=decrypt_paycheck2(char *str1,int len1);

其中 str 为解密后得到的由商家随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密商家身份信息。

char *str=decrypt_paycheck1(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为商家认证信息加密后的字符串，len1 为 str1 长度。

3) 检验商家真伪，并在证实商家身份后将自己的身份认证信息传送到商家服务器。

其数据格式如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 12；

长度为两字节整数，内容为后面具体数据内容的长度；

具体数据为将自己身份认证信息经商家的公开加密密钥加密后的字符串：

char *str=encrypt_payback(char *str1,int len1,char *str2,int len2);

其中 str 为加密后的字符串，str1 为结算中心名，str2 为结算中心密码，len1 为 str1 长度，len2 为 str2 长度；

4) 商家服务器在接到结算中心服务器请求后首先以商家的私有加密密钥对应解密：

char *str=decrypt_payback(char *str1,int len1);

其中 str 为解密所得字串，str1 为源串 len1 为其长度。

5) 通过双方身份认证后商家服务器传送自己的身份信息和用户账号以及所划资金信息到结算中心服务器；

其数据格式如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 13；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为以下数据经过商家服务器随机产生的对称加密密钥加密的字符串：

代码	长度	数据
代码	长度	数据
代码	长度	数据
……		

代码为一字节整数，表示后面内容的项目名：

1：商家名；

2：商家密码；

3：商家服务器保存的未解密的用户信息；

4：所划金额。

长度为后面具体数据长度；

类型 2 为一字节整数，此处设置为 14；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以结算中心公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_payment1(char *str1,int len1);

其中 str 为所得的字符串，str1 为原始数据，len1 为其长度。

b) 将随机产生的对称加密密钥以结算中心的公开加密密钥加密：

char * str=encrypt_payment2(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

6) 结算中心对商家传送的信息进行解密，得到商家信息、用户信息以及划账信息，具体过程如下：

a) 结算中心服务器在接到商家传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以结算中心的私有加密密钥对该数据字段进行解密：

char *str=decrypt_payment2(char *str1,int len1);

其中 str 为解密后得到的由商家服务器随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密商家传送过来的信息：

char *str=decrypt_payment1(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为商家传送过来的信息，len1 为 str1 长度。

c) 根据代码取出商家身份信息，用结算中心数据库中的信息检验商家身份。

d) 如果确认商家身份无效，则拒绝继续进行事物处理过程；如果有效，则根据代码取出加密的用户账号信息。

e) 用结算中心的私有加密密钥对该数据字段进行解密：

char *str=decrypt_account2(char *str1,int len1);

其中 str 为解密后得到的由用户随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

f) 根据解得的对称加密密钥解密用户的账号信息。

char *str=decrypt_account1(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为用户的账号信息，len1 为 str1 长度。

7) 结算中心服务器从用户账号划账，并发反馈信息给商家服务器；

其数据格式如下。

类型	长度	具体数据

其中类型为一字节整数，此处设置为 15；

长度为两字节整数，内容为后面具体数据内容的长度；

具体内容为用户账号转账情况：

1：成功

0：失败

8) 商家服务器在接到转账成功信息后，反馈确认信息给结算中心服务器，结束一次转账。

其数据格式如下。

类型	长度	具体数据

其中类型为一字节整数，此处设置为 16；

长度为两字节整数，此处值为 0；

具体数据暂时定为空。

C2.8 商家提供服务

具体流程如图 C3 所示。

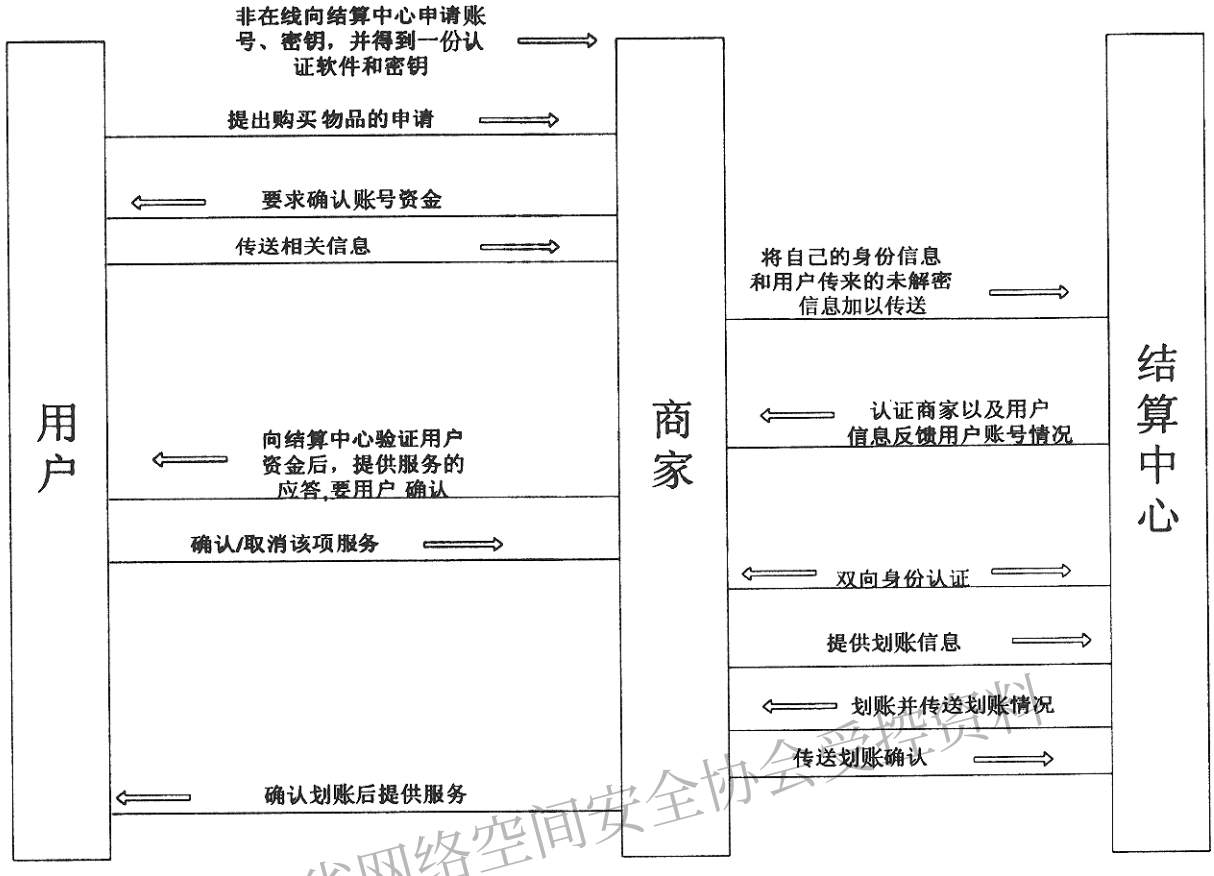


图 C3　预付卡方式的流程

C3　小额支付方式

用户首先以非在线方式向货币发行方登记注册，得到一个可以存入和划账的账号并存入资金，并得到密码和密钥。

用户从自己账号上提出一部分资金在线购买数字货币。

用户向商家提出购物申请，得到相应服务，并由用户以小额付费方式支付。此方式适用于商场购物等。

C3.1　用户在线购买数字货币

简单流程如下。

1) 用户的电子钱包向货币发行服务器要求购买数字货币，激活一个进程，将以下信息传送给货币发行服务器。

其数据格式如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 17；

长度为两字节整数，此处为 0；

具体数据暂定为空；

2) 货币发行服务器接到用户请求后要求用户进行身份认证。

3) 用户的电子钱包将自己的身份认证信息发送给货币发行服务器。

数据结构如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 18；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为经过用户的电子钱包随机产生的对称加密密钥加密的字符串。

类型 2 为一字节整数，此处设置为 19；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以货币发行服务器公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_userrequest1(char *str1,int len1,char *str2,int len2,…);

其中 str 为所得的字符串，str1 为账号，len1 为其长度，str2 为密码，len2 为其长度。

b) 将随机产生的对称加密密钥以货币发行服务器的公开加密密钥加密。

char * str=encrypt_userrequest2(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

4) 货币发行服务器对用户进行身份认证，具体过程如下：

a) 货币发行服务器在接到用户传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以货币发行服务器的私有加密密钥对该数据字段进行解密：

char *str=decrypt_userrequest2(char *str1,int len1);

其中 str 为解密后得到的由用户电子钱包随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密用户身份信息。

char *str=decrypt_userrequest1(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为用户认证信息加密后的字符串，len1 为 str1 长度。

c) 货币发行服务器根据其数据库中数据检验用户身份。

5) 货币发行服务器在验证了用户身份后，将自己的身份信息发送给用户的电子钱包，数据结构如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 20；

长度为两字节整数，内容为后面具体数据内容的长度；

具体数据为货币发行服务器身份信息经由用户的公开加密密钥加密后的字符串：

char *str=encrypt_dcrequest(char *str1,int len1);

其中 str 是加密所得字符串，str1 是源串，len1 为其长度。

6) 用户的电子钱包用自己的私有加密密钥解密，并检验货币发行服务器是否合法。

char *str=decrypt_dcrequest(char *str1,int len1);

其中 str 是加密所得字符串，str1 是源串，len1 为其长度。

7) 通过双方身份认证后，用户的电子钱包将自己的身份信息和要购买的数字货币数额及面额信息加密后传送至货币发行服务器。

数据结构如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 21；

长度 1 为两字节整数，内容为后面具体数据内容的长度；

具体数据 1 为以下数据经由用户的电子钱包随机产生的对称加密密钥加密后的字符串。

代码	长度	数据
代码	长度	数据
代码	长度	数据
……		

代码为后面所表示的具体内容的项目名：

1：用户名；

2：用户密钥；

3：所需的数字货币种类；

4：所需的数字货币数额；

注：3 与 4 两项可以重复，但要一一对应

类型 2 为一字节整数，此处设置为 22；

长度 2 为两字节整数，内容为后面具体数据内容的长度；

具体数据 2 是以货币发行服务器公开加密密钥对对称加密密钥封装后的字符串；

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_dcrequest1(char *str1,int len1);

其中 str 为所得的字符串，str1 为原始数据，len1 为其长度。

b) 将随机产生的对称加密密钥以货币发行服务器的公开加密密钥加密：

char * str=encrypt_dcrequest2(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

8) 货币发行服务器在接到用户请求后首先对应解密。

a) 货币发行服务器在接到用户传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以货币发行服务器的私有加密密钥对该数据字段进行解密：

char *str=decrypt_dcrequest2(char *str1,int len1);

其中 str 为解密后得到的由用户随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密用户身份以及购买信息。

char *str=decrypt_dcrequest1(char *str1,int len1);

其中 str 为所得解密后字符串，str1 为用户身份以及购买信息加密后的字符串，len1 为 str1 长度。

9) 检查用户现金账号中的资金是否充足，若是，则按用户请求数字货币的数额和面额产生相应的数字货币，并使用签名密钥对货币进行签名，同时从现金账号中扣除相应的数额，再将经过签名的数字货币加密后发回给用户的电子钱包。支付处理方货币发行服务器发行的数字货币中应包括以下内容：

a) 货币发行服务器的 IP 地址或主机名；

b) 过期时间 —— 指数字货币有效的截止时间；

c) 序列号 —— 货币发行服务器以此检查数字货币是否被重复消费；

d) 数字货币的面值。

例如：10.0.0.2:1998-07-01-00-00-00:1:100 即表示由主机 IP 地址为 10.0.0.2 发行的到 1998 年 7 月 1 日 0 点 0 分 0 秒有效的序列号为 1 的 100 元数字货币。

10) 用户的电子钱包接收发回来的数据，解密后得到经过签名的数字货币，用数字货币发行服务器的公钥验证货币的真实性。

C3.2 用户浏览并确定是否订购

C3.3 用户向商家提出请求

用户向商家发出购买申请，提出购买物品的请求,此处进行完整性处理（原文＋原文的数字签名）。

此处的过程与 C1.4 相同。

C3.4 商家获取用户的购买信息

具体过程与 C1.5 相同。

C3.5 商家作出能否提供服务的应答

具体过程与 C1.6 相同。

C3.6 用户作出是否接受该服务的确认(或取消)

具体过程与 C1.7 相同。

C3.7 用户以小额方式付费

具体过程如下。

1) 商家服务器接收用户的服务请求后，与货币发行服务器进行身份认证，其过程与用户购买数字货币时的双方身份认证相同。

2) 通过双方身份认证后，商家服务器将用户支付的数字货币连同自己的身份信息传送至货币发行服务器。

数据结构如下：

类型 1	长度 1	具体数据 1	类型 2	长度 2	具体数据 2

其中类型 1 为一字节整数，此处设置为 23；

长度 1 为两字节整数，内容为后面具体数据内容的长度。

具体数据 1 为以下数据经由商家服务器随机产生的对称加密密钥加密后的字符串：

代码	长度	数据
代码	长度	数据
代码	长度	数据
……		

代码为后面所表示的具体内容的项目名：

1：商家名；

2：商家密码；

3：用户名；

4：转账的数字货币种类；

5：转账的数字货币。

注：4 与 5 两项可以重复，但要一一对应。

其中类型 2 为一字节整数，此处设置为 24。

长度 2 为两字节整数，内容为后面具体数据内容的长度。

具体数据 2 是以货币发行服务器公开加密密钥对对称加密密钥封装后的字符串。

具体加密过程如下：

a) 调用一个函数，随机产生一个对称加密密钥，并用它对原始数据进行加密：

char * str=encrypt_dcpay1(char *str1,int len1);

其中 str 为所得的字符串，str1 为原始数据，len1 为其长度。

b) 将随机产生的对称加密密钥以货币发行服务器的公开加密密钥加密：

char * str=encrypt_dcpay2(char *str1,int len1);

其中 str 为所得的字符串，str1 为随机产生的对称加密密钥，len1 为其长度。

c) 过程 a)产生的字符串即为具体数据 1，过程 b)产生的字符串即为具体数据 2。

3) 货币发行服务器在接到商家传送的信息后首先对应解密。

a) 货币发行服务器在接到商家传来的信息后，根据类型以及长度字段取得封装后的对称加密密钥，以货币发行服务器的私有加密密钥对该数据字段进行解密：

char *str=decrypt_dcpay2(char *str1,int len1);

其中 str 为解密后得到的由商家服务器随机产生的对称加密密钥，str1 为封装后的对称加密密钥，len1 为 str1 长度。

b) 根据解得的对称加密密钥解密商家信息以及划账的数字货币信息：

char *str=decrypt_dcpay1(char *str1,int len1);

其中 str 为所得解密后的字符串，str1 为加密字符串，len1 为 str1 长度。

4) 货币发行服务器检查这些数字货币的有效时间看是否过期，如果货币过期，则反馈如下信息给商家服务器。

类型	长度	具体数据

其中类型为一字节整数，此处设置为 25；

长度为两字节整数，此处为 0；

具体数据暂定为空。

5) 货币发行服务器用自己的公开签名密钥验证数字货币中数字签名的真实性，此处使用一个函数处理：

int i=check_dcoin(char * str,int len)；

str 为源串，len 为长度，i 为检验结果：

i=0：真

i=1：伪

发现数字货币是伪币时，发送以下信息给商家服务器：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 26；

长度为两字节整数，此处为 0；

具体数据暂定为空。

6) 验证通过后，货币发行服务器将这些数字货币的序列号与数据库中已有的货币序列号进行对比，以确认这些货币是否被重复使用；

7) 若未重复消费，则将这些货币的序列号及过期时间存入数据库中，并清除数据库中的过期货币；

8) 数字货币发行服务器将相应数字货币值转入商家账号，并通知商家给用户提供服务；

其数据类型如下：

类型	长度	具体数据

其中类型为一字节整数，此处设置为 27；

长度为两字节整数，此处为 0；

具体数据暂定为空。

9) 商家服务器在接到类型为 25 或 26 的通知时都主动与货币发行服务器中断通信，并通知用户拒绝服务。在接到类型为 27 的通知后，反馈以下信息给货币发行服务器：

类型	长度	具体数据

其中类型为一字节整数，此处为 28；

长度为两字节整数，此处为 0；

具体数据暂定为空。

双方结束支付流程。

C3.8 商家提供该项服务

具体流程如图 C4。

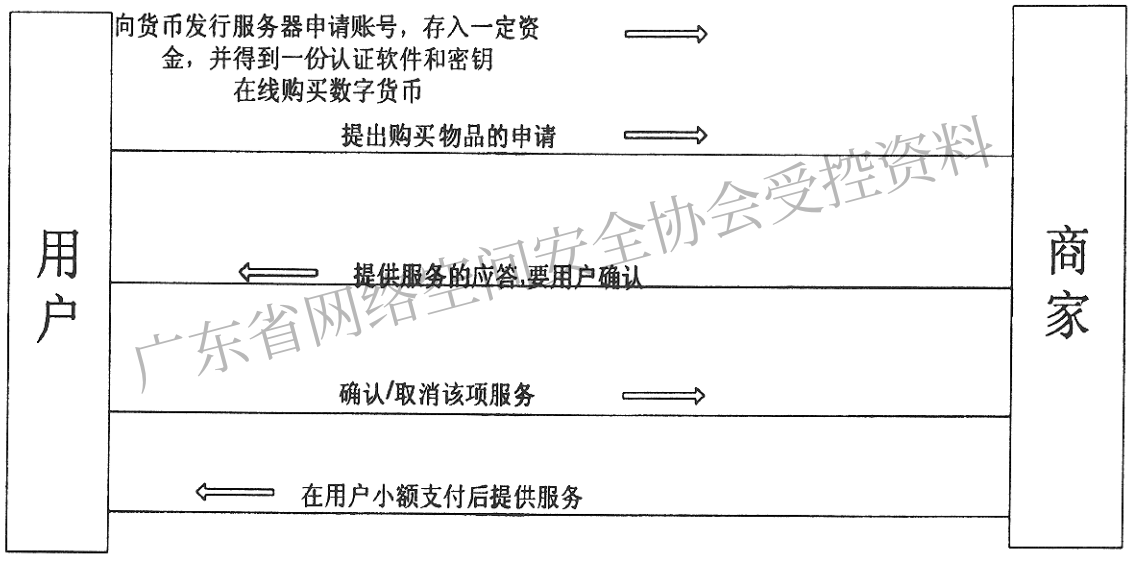


图 C4 小额支付方式的流程

注：

1 小额支付涉及到许多难以解决的问题，使得它在使用时十分不便，例如：

a) 关于找零的问题：由于支付过程中数字货币是由商家服务器转送货币发行服务器，所以找零也必须通过商家服务器，这就使用户很难确认数字货币的真伪，而如果让用户接到数字货币后再到货币发行服务器去验证货币，又将是十分麻烦而用户不愿采用的。

b) 关于什么情况使用小额支付：如果是需要不停支付的情况，例如浏览收费信息，将会大大减慢浏览速度，而如果是一次性支付，则考虑小额支付的限度又是多少？而且在同样需要到固定地点开账号(货币发行服务器或者结算中心)的前提下，小额支付多了一道购买数字货币的过程，是否相应麻烦了许多？

由于以上问题的存在，所以我们虽然在此处提出了小额支付的方法，但不建议在 Internet 网上的事物处理中采用这种方法。

2 由于涉及到保密性问题，许多具体的加密解密办法不能详述，只采用函数方式说明，函数名仅供参考。

附录 D
(提示的附录)
在线股票查询及交易系统

本附录提供了在公共网络上安全地进行股票交易的实现。它是一个在公共网络上建立股票交易系统的参考，适用于券商建立和设计网上股票应用系统，同时也适用于指导软件开发商做相关系统的开发。本附录引用了前文的第 6 章和第 8 章的相关规定。

D1 综述

D1.1 名词定义

D1.1.1 股民

在电子股票交易系统中，股民使用计算机或专用终端通过公网进行股票交易。股民必须已经通过证券登记中心申请到股东代码卡。他可以通过本系统申请在券商的交易系统上开户，或者利用已经存在的资金账户通过电子股票交易系统买卖股票。

股民要使用电子股票交易系统至少要有一个证书，用于加密和签名；也可以使用两个证书，分别用于加密和签名。

D1.1.2 股票交易所

股票交易所是为股票的买卖所提供的一个公开的场所。它同时为参与买卖的人提供现在或以前的股票信息。通过证券登记中心它为有意参与股票买卖的人提供一个特定的代码，规定买卖的范围和性质。

D1.1.3 券商

券商接收股民的买卖请求，利用他与股票交易所的关系帮助股民完成买卖业务，同时也为股民提供证券信息。开通电子股票交易系统的券商应该通过公网向股民提供信息，接收股民通过公网提交的请求。券商在电子股票交易系统中应有两个证书，分别用于加密和签名。

D1.2 总体原则

本附录的总体原则如下：

a) 尊重和保留现存的股民、券商、交易所、证券登记公司的关系；

b) 加速在线股票交易系统市场的发育。

D1.3 交易安全

保障交易系统安全的目标如下：

a) 提供股民、券商之间的相互验证；

b) 提供交易数据的保密；

c) 确保交易数据的完整性；

d) 定义安全机制的算法和协议。

D1.4 互操作性

互操作性的目的如下：

a) 尽可能地建立在已有的标准之上；

b) 与标准机构的政策兼容，获得标准机构的认可；

c) 容许在不同的软件、硬件平台之上实现，如 PowerPC, Intel, Sparc, UNIX, MS-DOS, OS/2, Windows 和 Macintosh。

D1.5 市场可接受性

市场可接收性的目的如下：

a) 通过协议的简单和易于实现，同时又不对或尽量少对券商及股民的现有系统带来任何影响，以此

来获得普遍的认可；

b) 尽量不对现有股民、券商、交易所和证券登记公司间的关系带来影响；

c) 尽量不对券商、交易所和证券登记公司的现有系统带来影响；

d) 允许在已有的客户应用系统内添加电子交易协议。

D2 系统安全策略

a) 提供交易数据的保密保护，使用的技术参见本标准 8.1.1 节中的对称密钥加密技术规定；

b) 保证所有传输数据的完整，流程应符合本标准 6.2 节的相应规定，使用的技术应符合 8.5.2 节中的相应规定；

c) 验证参与交易的股民是某个股东代码卡的合法使用人，流程应符合本标准 6.4 节的相应规定，使用的技术应符合 8.5.1.3 节中的相应规定，此时股民需要有签名公钥证书，其签名公钥证书应由 Internet 网 CA 中心统一签发，有关内容应符合本标准第 9 章的规定；

d) 验证参与交易的券商，保证可以通过他在交易所交易股票，流程应符合本标准 6.4 节的相应规定，使用的技术应符合 8.5.1.3 节中的相应规定，此时券商需要有签名公钥证书，其签名公钥证书应由 Internet 网 CA 中心统一签发，有关内容应符合本标准第 9 章的规定；

e) 保证采用最好的安全手段和系统设计来保护参与交易的各方利益；

f) 保证本协议不依赖于传输机制的安全性，不妨碍采用安全的传输机制。

D3 系统功能

系统的用户有 3 类：

- 总公司系统管理员；
- 营业部系统管理员；
- 投资者。

相应地系统功能可分为 3 类：

- 总公司处管理功能；
- 营业部处管理功能；
- 证券操作功能。

D3.1 证券操作功能

D3.1.1 实时行情显示

因为如果广域网的交易系统比较普及，黑客完全有可能对行情进行恶意修改，导致投资者作出错误的判断，造成重大损失，故需对于行情进行签名。

a) 个股集中显示

对选择的个股类别，在一屏中同时显示多只个股，并且可用多种方法排序。

b) 概貌显示

在实时行情显示和实时行情分析时，此概貌显示永远存在，有一组或多组概貌。每组概貌确定如下内容：交易所、指数、涨跌、涨跌平个股数、成交量、委比。

D3.1.2 实时行情分析

a) 分时分析

个股分时分析包括分时价量走势图、委托区域（价量图示和买卖情况）、概况区域、回报区域（成交回报、成交内外盘、成交价量图和大盘分时价格走势图）。

b) 日动态分析

个股日动态分析包括日线分析图、委托区域（买卖情况）、概况区域、回报区域（成交回报、成交价量图和个股分时价格走势图）。

c) 定义

1) 分时价量走势图：横轴为时间，单位为 min；纵轴为价格，图为曲线图。包括价格均线图，纵轴为成交量，图为柱形图。

2) 日线分析图：横轴为时间，单位为日、1 h、30 min、15 min、5 min，A 类图纵轴为指标刻度，如价格等；B 类图纵轴为成交量，图为柱形图，纵轴为指标刻度。

3) 委托区域：价量图示（买价量 1、买价量 2、买价量 3、卖价量 1、卖价量 2、卖价量 3、成交价 1、成交量 1），买卖情况（委比、委差、买价量 1、买价量 2、买价量 3、卖价量 1、卖价量 2、卖价量 3）。

4) 概况区域：成交价、升跌、幅度、总手、现手、外盘、均价、今开、最高、最低、金额、内盘。

5) 回报区域：成交回报：时间、成交价、成交量。

- 成交内外盘：有序成交价、内盘、外盘；
- 成交价量图：有序成交价、成交量；
- 大盘分时价格走势图：纵轴价格、横轴时间；
- 个股分时价格走势图：纵轴价格、横轴时间。

6) 技术分析 A 类：移动平均线、股票通道、保历加、多空指标、价量线、K 线、Town 线、Close 线、SAR 线、柱线图、新价线、天地线、四度空间。

7) 技术分析 B 类：乖离率、VR 指标、主力进出、强弱势、逆势操作、金额图、AR、BR 线、ALF 线、ACD 线、3-6BIAS 线、6-12BIAS 线、CCI 线、CHO 线、DMI 指数、HLC 线、KDJ 随机指标、FAST_KD 线、MACD 平滑异同移动平均线、VMACD 线、MTM 线、MFI 线、NVI 线、OSC 线、OX 线、PVI 线、PSY 线、ROC 线、RSI 线、QRSI 线、SWI 线、TAPI 线、VPT 线、买卖气 UBS。

D3.1.3 历史数据分析

WEB 服务器端按每日、每周、每月、每年将行情数据转为历史数据，分别形成 5 min、15 min、30 min、1 h、日、周、月、年的关于个股和指数的数据（开盘、收盘、最高、最低、成交量、成交金额）。

a) 历史数据分析图

横轴为时间，单位为 5 min、15 min、30 min、1 h、日、周、月、年 A 类图纵轴为指标刻度，如价格等；价量叠加、除权除息修正（仅一次或多次）；B 类图为柱形图，纵轴为成交量。

b) 个股数据

列示个股以日或某段日期为周期的日期、开盘、收盘、最高、最低、成交量、成交金额、涨幅、换手率、市盈率等情况。

c) 阶段行情

列示多个个股某日或某段日期的代码、名称、前收盘、开盘、收盘、最高、最低、成交量、成交金额、涨幅、换手率、市盈率等情况。

d) 分类评估

列示某日或某段日期个股分类中类名称、总市值、总金额、涨幅、换手率、市盈、领涨股列示某日或某段日期个股分类中类下的个股名称、市值、金额、涨幅、换手率、市盈率等。

D3.1.4 委托和股民个人资料查询

系统可进行实时证券交易。系统在投资者和投资者所开户的营业部之间建立连接。如果投资者在多个营业部开户，则系统列出投资者所有开户的营业部，由投资者选择在哪个营业部进行交易。

系统对股民的委托和查询以及券商的应答进行加密和签名，以保证信息的秘密、完整和真实。

D3.1.5 委托、委托查询和成交查询

a) 买入委托

选择或输入要买入的个股，列示买入个股的成交回报和买卖情况，符合涨跌停板制度和买入单位的有效委托。

b) 卖出委托

选择或输入要卖出的个股，列示卖出个股的成交回报和买卖情况，符合涨跌停板度和卖出单位的有效委托。

c) 撤单委托

列示当天所有买入、卖出委托，选择委托撤单。

d) 委托查询

列示当天所有买入、卖出、撤单委托。

e) 成交回报查询

列示当天成功买入的股票、成功卖出的股票及成功撤单。

D3.1.6 个人资料查询

a) 查询总账

总资金、提现资金、所持股票市值、持股名称、数量、平均单价、原值、市值、增值。

b) 查询明细

买入、卖出个股明细。

c) 更改口令

改变入网口令，私有密钥不能自己更改，需到证券营业部申请。

D3.2 管理功能

D3.2.1 信息服务

券商制作的关于本公司的信息；上市公司的信息；国家有关政策、法规、法律；引导投资者买卖证券的建议。

a) 个股基本情况

公司名称、地址、主营业务、兼营业务、公司历史、公司重大事项（投资、法律纠纷、资产重组等）。

b) 个股财务报表

公司历年财务报表，财务报表说明。

c) 个股股本结构

公司历年股本结构，公司前十大股东，现金红利、送股、转配股、法人股转配等。

d) 个股报道

以时间为序，分不同的媒体对公司的报道摘要。

e) 荐股跟踪

以时间为序，分不同的机构或个人推荐摘要。

f) 基本面消息

以时间为序，国内国际政治、经济等报道。

D3.2.2 管理员管理

管理员分为普通管理员和超级管理员两类。普通管理员的权限包括对营业部和投资者的管理。超级管理员除了具有普通管理员的权限外，还具有对普通管理员进行管理的权力，以及多个管理员共同对私钥进行管理的权力。

对管理员进行增加、删除、修改和查询等操作，对管理员身份进行认证，对管理员操作进行审计。

D3.2.3 投资者管理

对投资者进行增加、删除、修改和查询等操作，对投资者身份进行认证，对投资者操作进行审计。在投资者和所属营业部之间建立连接。

股东代码和认证密钥以密文形式存放。

D3.2.4 营业部管理

对营业部进行增加、删除、修改和查询等操作。

D3.3 安全功能

投资者委托及个人资料的查询都以密文的形式传输。详细内容应符合本标准第 6 章和第 8 章的技术要求。

D4 系统结构和运行环境

系统采用 Internet/Intranet 结构，从这个意义上划分，可分为 3 个子系统：Client（CL）系统，Web 服务器（WS）子系统和接入服务器（AS）子系统。由于 Client 分为 3 类：面向投资者的、面向总公司管理员的和面向营业部管理员的，所以对应于 3 类用户，CL 系统有 3 个：CL1，CL2 和 CL3。

D4.1 系统连接

D4.1.1 硬件连接

CL1 可分布于世界各地，通过 Internet 或其他 IP 网和 WS 相连；CL2 放置在证券公司，通过 IP 局域网和 WS 相连；WS 放置在证券公司，通过数据网或 Internet 上的安全通道和营业部的局域网相连；CL3 放置在营业部，通过 IP 局域网和 AS 相连；AS 放置在营业部，使用 VPN 技术，通过 Internet 网和总公司连接。网络总体如图 D1 所示。

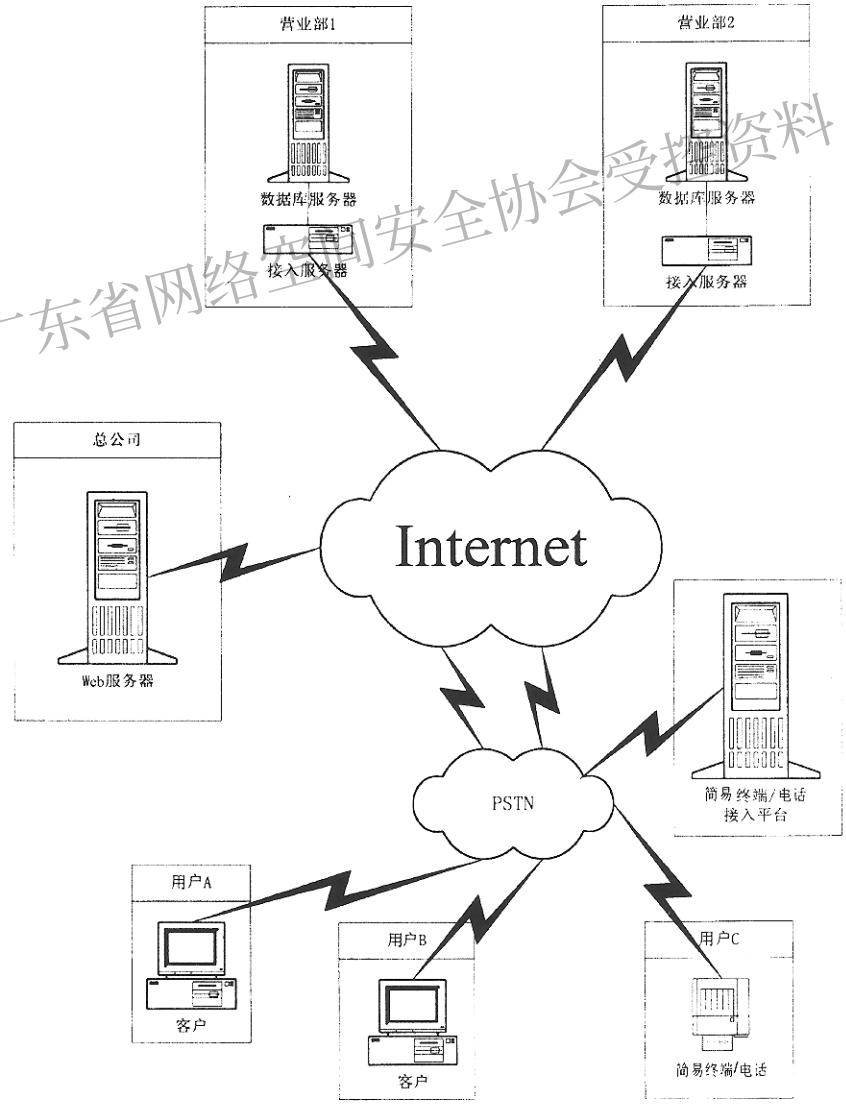


图 D1 系统构成

D4.1.2 软件连接

CL1 和 WS 通过 HTTP 相连；CL2 和 WS 通过 HTTP 相连；CL3 和 AS 通过 HTTP 相连；AS 和券商原交易系统通过自定义接口相连；WS 和 AS 通过 HTTP 相连，模块之间以及和数据块之间的连接如图 D2 所示。

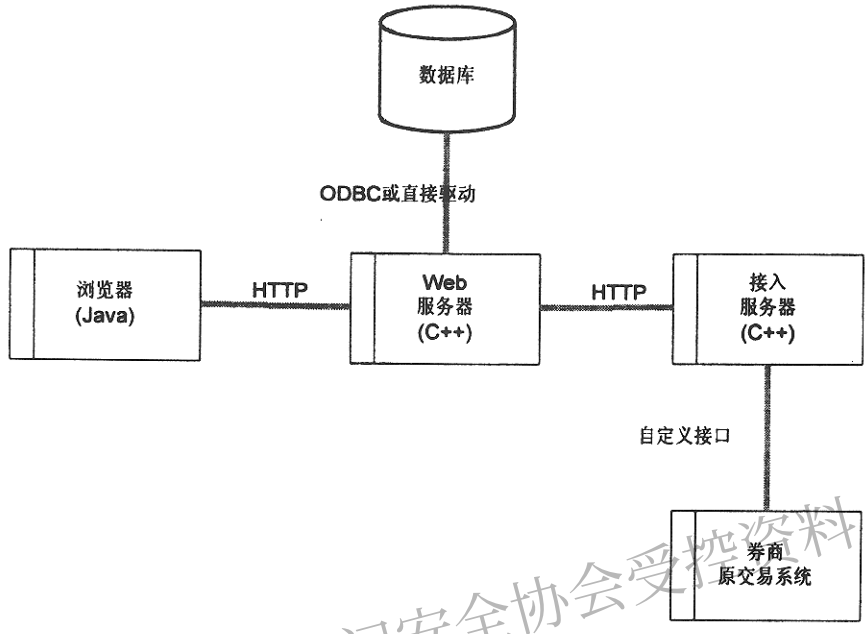


图 D2 模块之间以及和数据库之间的连接

D4.2 投资者 Client(CL1)系统

D4.2.1 功能

1) 投资者和系统间的人机界面

投资者直接通过 PC 机输入指令，或通过专用终端，根据语音或其他提示信息提示输入指令。系统软件对投资者的输入进行初步检查和过滤，接受投资者的以下输入请求并输出系统处理结果。

a) 查阅股市信息，包括以下内容：
- 实时行情；
- 历史资料；
- 各种技术指标；
- 基本面；
- 个股资料；
- 股坛评论；

b) 申请证书。

c) 登录。

d) 查询投资者资料，包括以下内容：
- 投资者资金账户；
- 投资者证券账户；
- 成交回报；
- 其他个人资料。

e) 委托，包括以下委托：
- 买入委托；

- 卖出委托；
- 撤单；
- 委托查询。

2) 安全功能

a) 当投资者输入账号、口令、密钥时，防止其他程序截取键盘输入。

b) 配合 Web 服务器对投资者进行认证。

c) 对投资者资料查询、委托和更改网上交易口令的请求进行加密，传给 Web 服务器。

d) 对从 Web 服务器传来的投资者资料查询、委托的结果进行解密。

e) 对投资者的委托请求制作数字签名。

3) 下载历史数据和各种信息资料。

D4.2.2 开发工具和实现方法

使用纯 Java，提供 Applet 和 Application 两种版本。

D4.3 总公司管理员（CL2）系统

D4.3.1 功能

对总公司管理员的输入进行初步检查和过滤。接受总公司管理员输入请求并输出系统处理结果。这些请求和结果如下：

a) 申请证书。

b) 查询投资者资料。

c) 查询、增加、删除、修改管理员资料。

d) 查询、增加、删除、更改营业部资料。

e) 查询、增加、删除、更改股坛评论等信息。

f) 数据库备份和修复。

D4.3.2 开发工具和实现方法

使用纯 Java，程序以 Applet 为主体。

D4.4 营业部管理员（CL3）系统

D4.4.1 功能

对营业部管理员的输入进行初步检查和过滤。接受营业部管理员输入请求并输出系统处理结果。这些请求和结果如下：

a) 查询、增加、删除、修改投资者网上交易开户资料。

b) 查询本营业部投资者资料。

c) 查询、增加、删除、修改本营业部管理员资料。

d) 查询、增加、删除、更改本营业部资料。

e) 查询、增加、删除、更改股坛评论等信息。

D4.4.2 开发工具和实现方法

使用纯 Java，程序以 Applet 为主体，必要时使用 JavaBeans。

D4.5 Web 服务器（WS）系统

D4.5.1 功能

WS 主要功能分为两类：一类是在投资者和 AS 之间担当网关，另一类是在本地处理用户（投资者和管理员）的输入，并承担系统管理。WS 接受 CLI1、CLI2 和 CLI3 的输入，处理这些输入，并将结果输出。

1) 投资者管理

a) 投资者登录，生成传输密钥，将密钥传给投资者。

b) 对投资者的查阅股市信息请求在本地处理，并将结果传给投资者。这些请求和结果如下：

- 实时行情；
- 历史资料；
- 各种技术指标；
- 基本面；
- 个股资料；
- 股坛评论。

c) 对投资者的查询个人信息请求解密，再加密，传给 AS，接收 AS 处理结果，解密，再加密，传给投资者。这些请求和结果如下：

- 投资者资金账户；
- 投资者证券账户；
- 成交回报；
- 其他个人资料。

d) 对投资者的委托请求解密，鉴别，检查完整性，再加密，传给 AS，接收 AS 处理结果，解密，再加密，传给投资者。这些请求和结果如下：

- 买入委托；
- 卖出委托；
- 撤单；
- 查询委托。

2) 总公司管理员管理

a) 总公司管理员资料的增加、删除、修改和查询；

b) 审计管理员操作。

3) 营业部管理

a) 营业部资料的增加、删除、修改和查询；

b) 营业部安装本系统后，总公司给它交易号，营业部用这个交易号从 Internet 网 CA 中心申请交易证书。得到证书后，交易号作废。

4) 系统维护

a) 自动备份数据库；

b) 提供管理员备份数据库界面；

c) 提供管理员修复数据库界面；

d) 搜集系统运行状态信息和危险告警信息，并显示。

5) 股市信息管理

a) 交易所信息的自动接收、转换、存储；

b) 总公司管理员对信息的查询、增加、删除、修改；

c) 投资者对信息的查阅。

D4.5.2 开发工具和实现方法

使用 C++编程。

D4.6 接入服务器（AS）系统

D4.6.1 功能

AS 主要是担当 WS 和券商原交易系统的网关，还是管理投资者网上交易账号开户。

1) 投资者管理

a) 接收 WS 有关投资者管理的输入，解密；处理，传给原交易系统；接受原交易系统的处理结果；加密，再将结果传给 WS。这些输入和输出如下：

- 投资者资金账户；

- 投资者证券账户；
- 成交回报；
- 其他个人资料；
- 委托。

b) 投资者网上交易开户，为投资者生成临时的网上账号和口令。投资者用账号和口令通过网络申请交易证书，得到证书后，账号和口令作废。

2) 信息管理

接受营业部管理员输入的与股市有关的信息，并传给 Web 服务器。

3) 营业部管理员管理

管理员资料查询、增加、删除、修改。

D4.6.2 开发工具和实现方法

使用 C++编程。

D4.7 安全系统

安全系统由访问控制系统、传输加密系统、数字签名系统组成。

D4.7.1 访问控制

访问控制系统的功能是阻止未授权用户访问受保护信息。本系统的受保护信息的访问控制对网外的限制有 2 个级别：可访问和不可访问，有网上交易证书的投资者有权访问，其余无权访问。对网内的限制有 3 个级别：超级管理员，普通管理员，非管理员。访问控制在两处实现：CL1 和 WS，重点在 WS。

a) CL1

只有拥有证书的投资者才能登录。

b) WS

WS 是实现访问控制最重要的地方，应使用硬件防火墙，对用户和管理员的权限进行严格控制，使用户和管理员都无法绕过网关（Web 服务器）直接进入营业部的交易网，或直接访问证券公司有关信息，并对管理员的操作进行审计。

D4.7.2 传输加密

下列信息在传输时需要用对称密钥加密：

a) 投资者资料

- 投资者资金账户；
- 投资者证券账户；
- 成交回报；
- 其他个人资料。

b) 委托

- 买入委托；
- 卖出委托；
- 撤单；
- 委托查询。

下列信息在传输时需要用非对称密钥加密：

a) 投资者和 WS 之间的传输密钥；

b) WS 和 AS 之间的传输密钥。

D4.8 签名和鉴别

对于证券交易，签名和鉴别比保密更重要。签名保证数据确实是发送方发出的而不是第三方伪造的，并且保证信息的完整性。鉴别保证数据的真实性和完整性，没有被第三方篡改或发生传输错误。

D5 证券交易流程

证券交易的所有参与者在执行下面的流程之前，必须先按本标准 9.3 节规定的流程获得电子身份证书。

D5.1 投资者

投资者凭借 CA 证书从营业部得到网上交易账号。投资者的交易系统从指定站点下载，一般是从证券交易商的站点处下载，或由证券交易商的营业部发放。

D5.2 营业部

营业部在本交易系统中装载营业部证书。

D5.3 公司总部

公司总部完成券商内部的账务功能。

D5.4 投资者登录流程

投资者在委托和查询个人资料前，必须登录。如仅查阅行情、技术指标等，则不必登录。在登录过程中，完成投资者和券商的相互认证，并生成对称密钥用于加密传送的信息。投资者登陆流程如图 D3 所示。

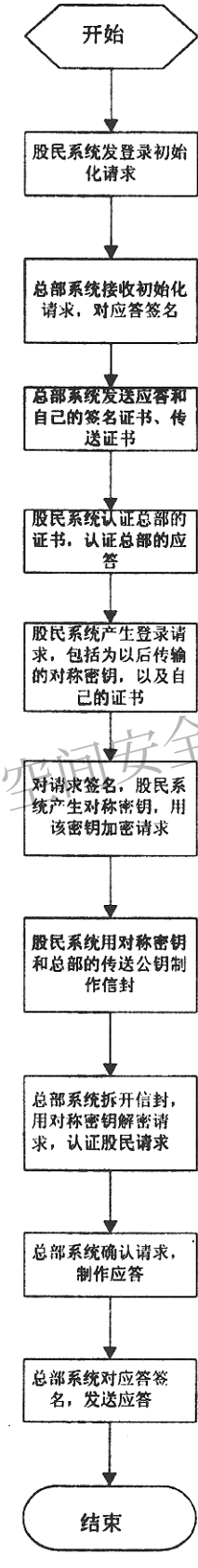


图 D3　投资者登录流程

D5.5　投资者委托处理流程

投资者的委托请求处理流程是投资者发送定单，公司总部接收定单，再将定单传给相应的营业部。投资者委托处理流程如图 D4 所示。

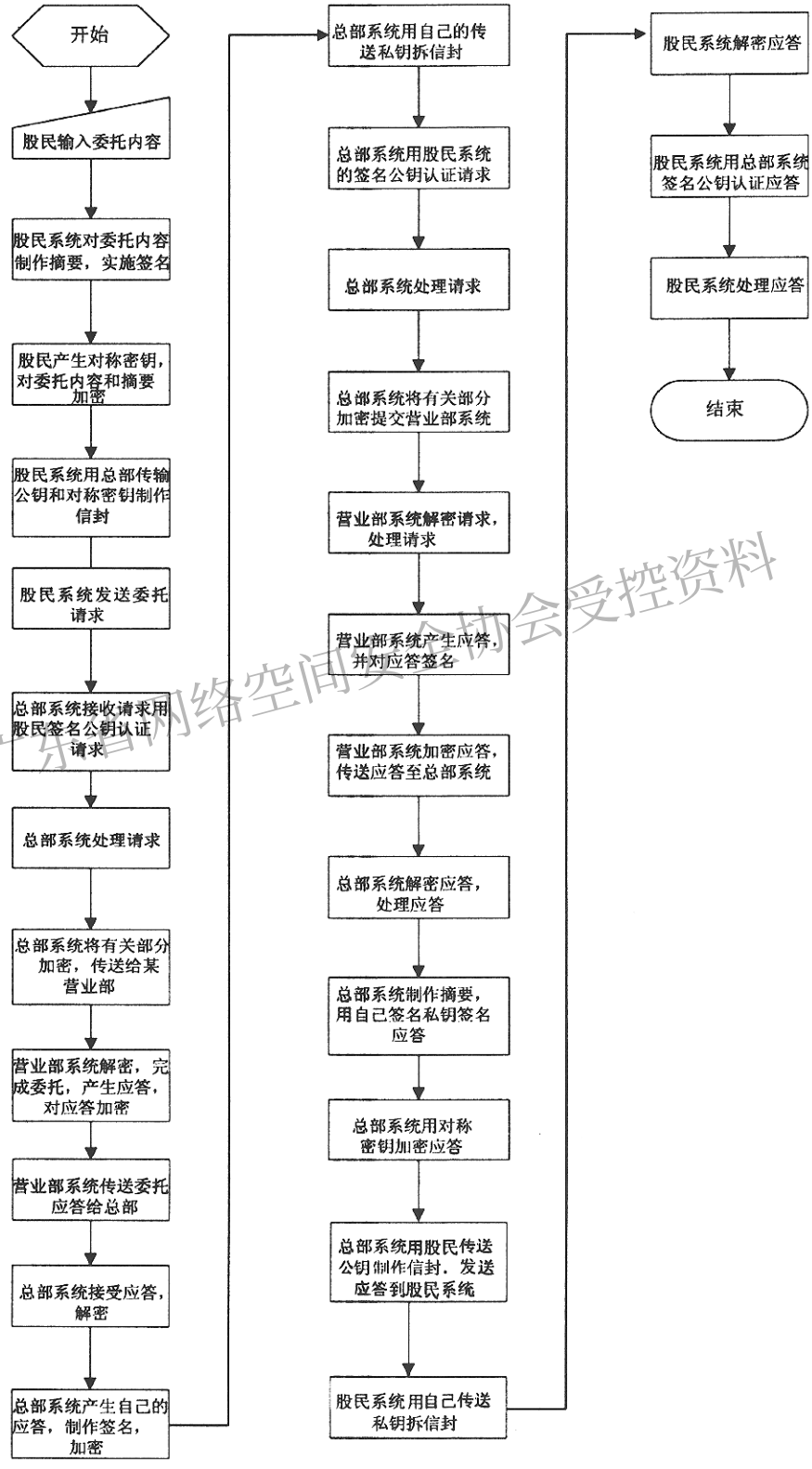


图 D4　股民委托处理流程

D5.6　投资者查询个人资料处理流程

有关投资者个人信息的查询过程，需要用密文传送。与电子购物不同的是，投资者的委托都通过公司总部的 Web 服务器，不是先选择一个营业部的页面。投资者个人资料查询处理流程如图 D5 所示。

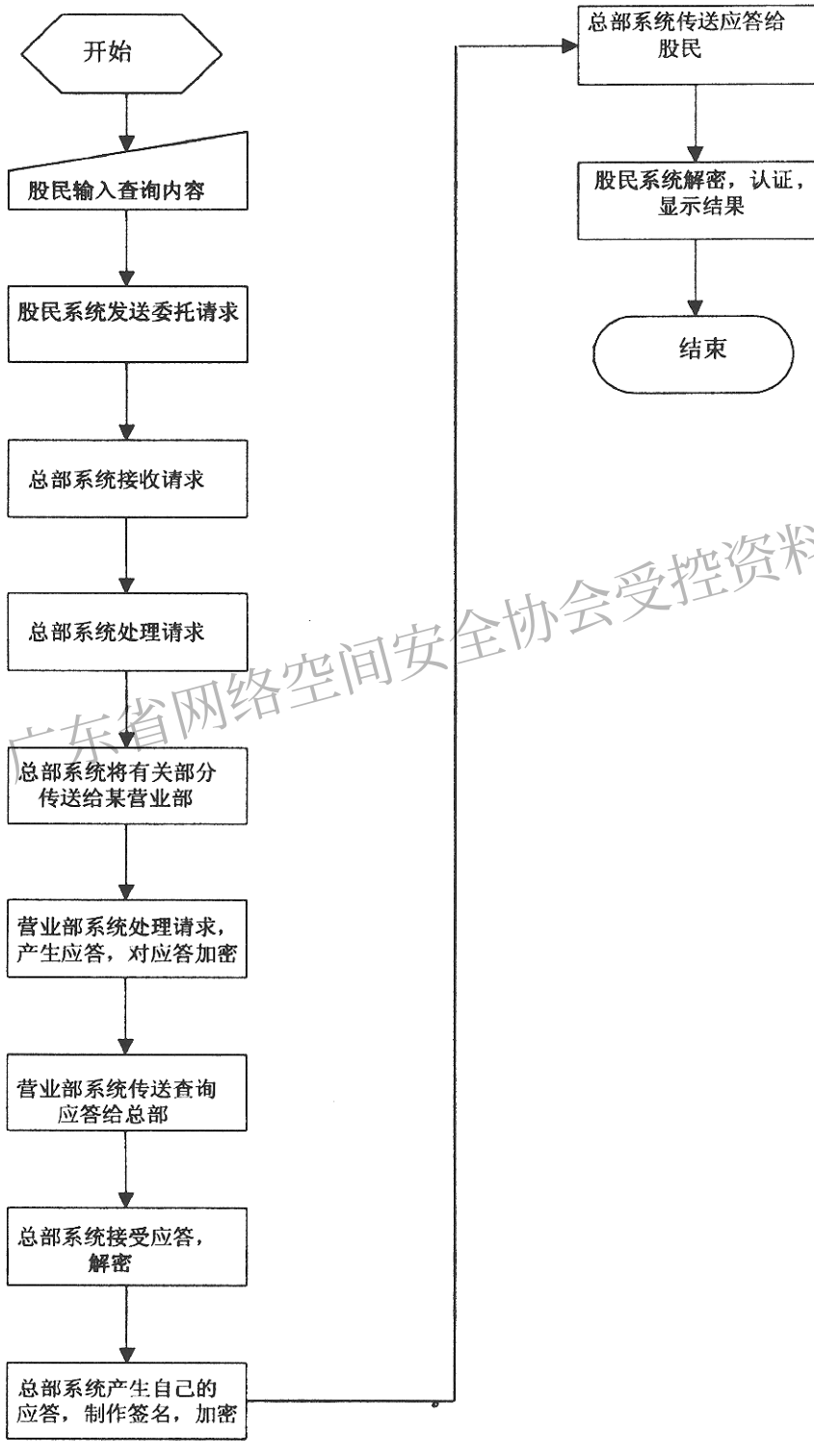


图 D5　股民查询个人资料处理流程

附录 E
(提示的附录)
公文传送业务技术要求

本附录提供了在公共网络上如何安全地实现公文传送业务的流程，它是一个在公共网络上建立公文传送业务系统的参考。本附录引用了前文的第 6 章、第 8 章、第 9 章的相关规定。

E1 公文传送业务的应用范围

本标准中的公文传送业务可应用于以下领域：

1) 各级政府机关的公文通过 Internet 网进行传送；
2) 各种企业单位通过 Internet 网传送商业信息；
3) 各种事业单位通过 Internet 网传送敏感信息；
4) 政府机关、企业、事业单位之间通过 Internet 网传送重要信息。

E2 公文传送系统的安全性要求

公文传送系统的安全性要求共有 4 个方面：

1) 公文传送的安全性 —— 如果公文在传送过程中被他人非法窃取，窃取者不能从所窃得的公文中获得有用信息；

2) 公文传送的完整性 —— 如果公文在传送的过程中被他人恶意篡改，公文传送系统能够发现这种篡改；如果公文的接收者恶意篡改他所收到的公文，公文传送系统也能够发现这种篡改；

3) 公文传送双方的身份认证 —— 任何人不能冒充他人发送或接收公文；

4) 公文传送的不可抵赖性 —— 公文发送者不能事后否认该公文是他所发送的。

E3 实现公文传送安全性的技术手段

实现公文安全传送的技术手段共有 3 个：

1) 加密 —— 通过对传送的公文进行加密可以提供传送公文的安全性，一旦传送的公文被非法窃取，能够使窃取者不能从所窃得的公文中获得有用信息；

2) 数字签名 —— 通过对传送的公文进行数字签名可以实现身份认证、不可抵赖并保障数据的完整性。一方面签名者不能否认他所发送的公文(因为公文上有他的签名)，另一方面如果公文被篡改，被篡改的公文会与其数字签名不一致，从而被公文传送系统所发现；

3) 认证 —— 使用认证技术能够确保公文发送者和公文接收者的合法身份，防止他人冒充公文发送者发送公文，防止他人冒充公文接收者接收公文。

具体实现见下面各节。

E3.1 加密证书与签名证书

我国 Internet 网设立证书管理中心。需要通过 Internet 网传送公文的单位必须首先向 Internet 网 CA 中心申请加密证书与签名证书。有关 CA 中心和证书的要求应符合本标准第 9 章的规定。

E3.2 公文加密技术

通过 Internet 网传送的公文必须进行加密。加密方法（符合本标准 8.1 节和 8.2 节的技术要求）如下：

1) 用经中央主管部门批准的密钥产生算法或密钥产生器产生加密密钥；

2) 用经中央主管部门批准的对称加密算法对公文进行加密；

3) 用经中央主管部门批准的公开密钥加密算法和公文接收者的公文传送公钥把加密密钥加密后附在所传送的公文的前面随公文一起传送给接收者；

4) 公文接收者收到公文后，首先用自己的公文传送私钥对附在公文前面的加了密的加密密钥进行解密以获得加密密钥，然后用它对加了密的公文进行解密从而获得明文公文。

E3.3 公文签名技术

通过 Internet 网传送的公文必须进行数字签名（符合本标准 8.3 节的技术要求），签名方法如下：

1) 用经中央主管部门批准的散列函数算法把要传送的公文散列为一个具有固定长度的信息摘要；

2) 用经中央主管部门批准的数字签名算法和公文签名密钥对上一步算出的信息摘要，进行数字签名，得到所传送的公文的公文数字签名；

3) 把上一步算出的公文数字签名和公文发送者的签名证书附在所传送的公文的后面随公文一起发送给公文接收者；

4) 公文接收者收到公文后，首先验证签名证书的正确性，然后再用签名证书中的公文签名验证密钥验证附在公文后面的公文数字签名的正确性。如果发现签名证书是伪造的则拒绝接收该公文，如果发现公文数字签名不正确则告知公文发送者该公文在发送途中被篡改，请求重发。

E3.4 认证技术

通过 Internet 网传送公文的用户在传送公文前必须对对方的身份进行认证（符合本标准 8.5 节的技术要求），方法如下：

1) 认证过程由公文发送方发起。公文发送方在传送公文前首先向公文接收方发送随机数甲，要求公文接收方对该随机数进行签名；

2) 公文接收方收到随机数甲后，首先生成随机数乙，把随机数甲、随机数乙和自己的签名证书连接起来，然后用自己的公文签名密钥对它进行签名，最后把下面的数据发送给公文发送方；

随机数甲	随机数乙	公文接收方的签名证书	公文接收方对前三项内容的数字签名

3) 公文发送方收到上述数据后，首先验证公文接收方的签名证书的正确性，若发现签名证书是假的就终止公文传送过程，否则再验证公文接收方所作的数字签名是否正确，若发现数字签名不正确则终止公文传送过程，否则进行下一步；

4) 公文发送方生成随机数丙，把随机数乙、随机数丙和自己的签名证书连接起来，然后用自己的公文签名密钥对它们进行签名，最后把下面的数据发送给公文接收方；

随机数乙	随机数丙	公文发送方的签名证书	公文发送方对前三项内容的数字签名

5) 公文接收方收到上述数据后，首先验证公文发送方的签名证书的正确性，若发现签名证书是假的就终止公文传送过程，否则再验证公文发送方所作的数字签名是否正确，若发现数字签名不正确则终止公文传送过程，否则进行下一步；

6) 公文接收方向公文发送方发送认证通过信息。

E4 公文传送流程

以下是公文传送的具体实现流程：

1) 公文发送方和公文接收方进行身份认证过程；

2) 认证过程结束后，公文接收方向公文发送方发送自己的加密证书；

3) 公文发送方验证公文接收方发来的加密证书是否合法，若是，进行下一步；否则终止公文传送过程；

4) 公文发送方产生一个随机数作为加密密钥，用它对要传送的公文进行加密得到公文密文，然后用公文接收方的公文传送公钥(从公文接收方的加密证书中获得)对加密密钥进行加密得到一个数字信封，里面装有加密密钥，最后公文发送方用自己的公文签名密钥对要发送的公文密文进行签名得到一个数字签名，而后把下面的数据发送给公文接收方；

公文密文	数字信封	数字签名	公文发送方的签名证书

5) 公文接收方收到公文发送方发来的上述数据之后，首先验证公文发送方的签名证书的真伪。若发现签名证书是伪造的就拒绝该公文，否则用签名证书中的公文签名验证密钥验证公文密文的数字签名是否正确，若发现数字签名不正确就向公文发送方报告公文在发送途中已被篡改的消息并要求重发，否则用自己的公文传送私钥对数字信封进行解密得到加密密钥，然后再用加密密钥对公文密文进行解密得到公文发送方所要发送的公文；

6) 公文接收方向公文发送方发送公文已收到的消息。

图 E1 是公文传送流程。

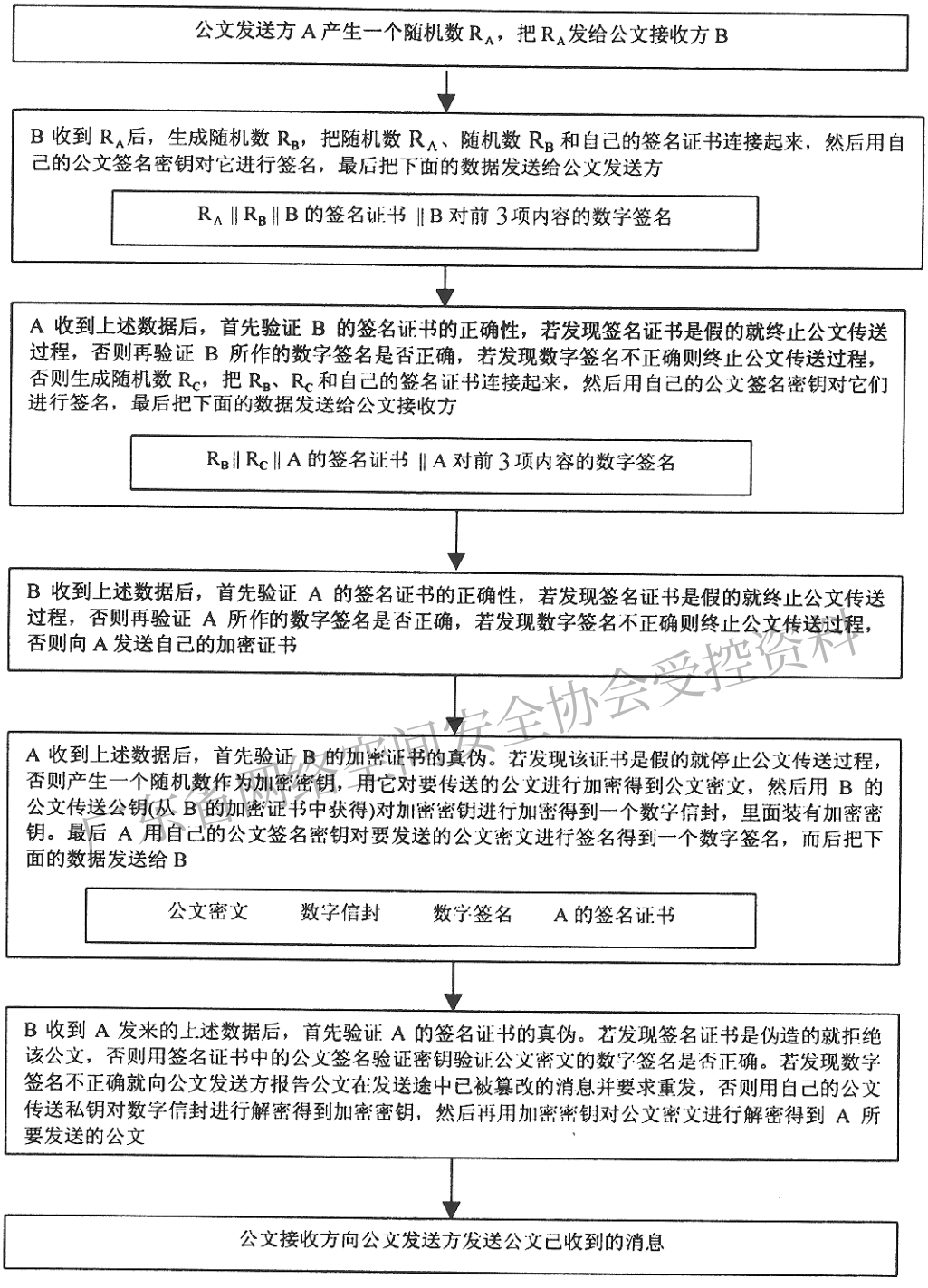


图 E1 公文传送业务流程

中华人民共和国
通信行业标准

基于IP网络的事务处理业务技术规范

YD/T 1035—2000

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号
邮政编码:100061
电话:67132792
北京鸿佳印刷厂印刷

*

开本:880×1230　1/16　　2000年7月第1版
印张:5　　2000年7月北京第1次印刷
字数:146千字　　印数:1-2000册

ISBN 7-115-416/00-36

定价:30.00元