国际电子商务的安全与应用

周大勇

当代信息技术和通讯技术的发展，网络技术的应用，特别是 Internet 的出现，正引起传统国际贸易领域的一场伟大变革。一种全新的国际贸易方式——国际电子商务正在向我们走来。什么是国际电子商务？国际电子商务的安全问题如何解决？国际电子商务的操作程序如何？是本文所要讨论的问题。

一、国际电子商务概述

国际电子商务是指买卖双方利用现代信息技术和通讯技术进行国际贸易活动的信息交换过程。

与传统的国际贸易相比，国际电子商务特点如下：(1) 国际电子商务是电子信息的传递，是计算机网络介质的信息交换；传统的国际贸易则依靠口头和书面介质进行信息交换。(2) 信息处理和传递的速度大大加快，处理成本大大降低，自动化程度大大提高。(3) 信息传播的范围扩大，地域上的概念在国际电子商务中不再那么重要。

由于国际电子商务是一种全新的贸易方式，其交易当事人的权利和义务与传统的国际贸易不尽相同。(1) 买方在国际电子商务中首要责任是付款，另外，收取货物，接受由第三方服务提供者提供的服务也是买方应尽的义务。(2) 卖方在国际电子商务中首要责任是交付货物，提供与合同相符的货物。另外，卖方必须按合同的规定安排由第三方服务提供者提供的服务。(3) 第三方服务提供者，包括承运人，保险公司等，在国际电子商务中按买方和卖方的要求提供服务。(4) 金融中介在国际电子商务中负责支付货款，担保买方的付款承诺，担保买方金融中介的付款责任。上述的买方、卖方、第三方服务提供者和金融中介必须对其发送给所有贸易当事人的电子报文的完整性、真实性、准确性负责。

二、国际电子商务的安全措施

Internet 是一个完全开放的系统，由于信息交换的传输机制使信息传输的途径不确定，信息在到达目的地以前可能周游世界各地，可能跨越任何机构的节点。正是这种开放性使电子商务在使用 Internet 过程中必须加以安全和保密措施。国际电子商务的安全保密基于密钥理论和技术以及由此衍生的数字签名、报文摘要、认证技术等。本文介绍密钥加密、数字签名、数字时间戳、认证 4 种技术。

1. 密钥加密　密码学需要有高深的数学理论支持，但加密的概念却十分简单：通信的数据和信息称为明文，发送时用一个加密算法即通过一个加密钥 K 将其转换成为不可辨识的形式，称为密文，使传输过程中的局外人无法懂得其含义，而当密文到达目的地后，收信人用一个解密算法即通过一个解密钥 H 将密文再转化为明文。有两种基本的加密算法：对称密钥算法和公开密钥算法。

(1) 对称密钥算法，又称传统密钥算法。这里加密钥和解密钥是同样的，即 H＝K，一把

钥匙开一把锁。对称加密算法的一个严重问题是它的密钥分发过程。如果密钥在分发过程中被截获,则密文可能在不知不觉中泄密。另外,密钥的数量在多方通讯时会随着通讯方的增加而爆炸性膨胀。再者,如果通讯对方是素不相识者,这就无法分发密钥也就无法秘密通信。为此,常常需要建立一个密钥分发中心为通信各方分发密钥,然而密钥分发中心本身的安全与保密又成为新的不安全因素。

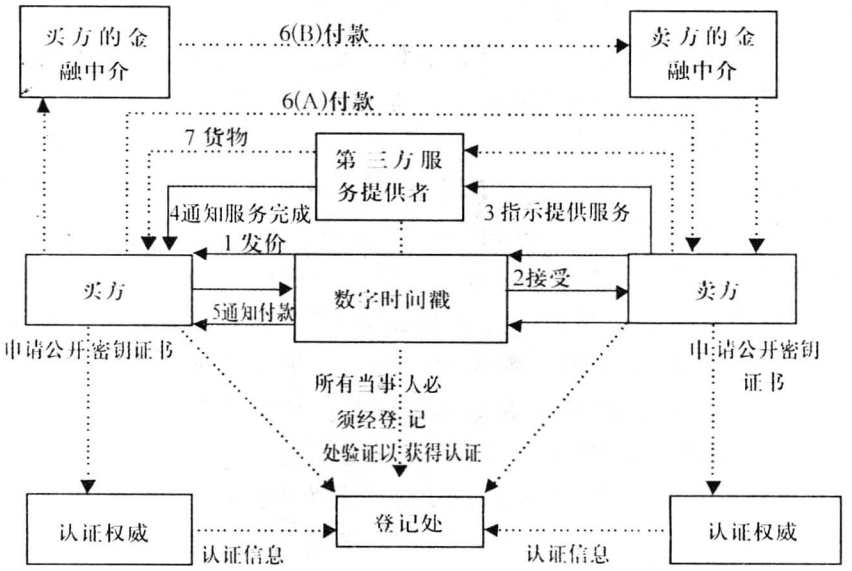
(2) 公开密钥算法。与传统加密方法不同,公开密钥技术使用两把不同的钥匙,即 H 与 K 不同,两把中的任何一把均可作为加密钥。通常每个人有两把钥匙,一把是公开钥匙,一把是秘密钥匙,前者用于加密,后者用于解密。所以,它也称非对称加密法。例如,甲公司发一封密信给乙公司,甲公司用乙公司的公开密钥加密此信,而乙公司则可以用只有它自己知道的秘密钥匙解密此信,因此,它是唯一能读此信的人。甲公司可以要求乙公司告诉其公开密钥,也可以查询公开密钥服务器(就象查电话号码簿一样),而得到乙公司的公开密钥。公开密钥加密技术解决了传统加密方法的根本问题,极大地简化了钥匙分发过程。Internet 上一种流行的公开密钥算法称为 RSA(RSADSI 公司开发)算法。

2. 数字签名 在许多情况下,信息是否真实有效取决于是否有授权人的亲笔签名。但在使用计算机进行信息处理时,手迹签名显然是行不通的,必须使用数字形式的签章来解决。一个可以替代手迹签名的系统必须满足以下三个条件:(1) 接收方可以通过文件签名来确认发送者的身份;(2) 发送者在发送信息之后不能否认发送过签名文件;(3) 接受方不能伪造发送方的签章。可以使用公开加密算法进行数字签名。使用公开密钥算法的数字签名,其加密算法和解密法除了要满足 $D(E(P))=P$ 外,还必须满足 $E(D(P))$ 这个假设是可能的,因为 RSA 算法具有此特性。当 A 想向 B 发送签名的报文 P 时,它向 B 发送 $E_B(D_A(P))$,由于 A 知道自己的私人密钥 D_A 和 B 的公开密钥 E_B,因而这是可能的;B 收到密文之后,先用私人密钥 D_B 解开密文,将 $D_A(P)$ 复制一份存放于安全的地方,然后用 A 的公开密钥 E_A 将 $D_A(P)$ 解开,取出 P。当 A 过后试图否认给 B 发过 P 时,B 可以出示 $D_A(P)$ 作为证据,因为 B 没有 A 的私人密钥 D_A,除非 A 确实发送过 $D_A(P)$,否则 B 是不会有这样一份密文的,只要用 A 的公开密钥 E_A 解开 $D_A(P)$,就可以知道 B 说的是真话。

3. 数字时间戳 数字时间戳是一个保证提供准确的时间、时区和报文日期的数字化时间认证证书。数字时间戳类似于邮戳,只不过是采用电子形式。由于在国际电子商务中也存在接受的期限以及愈期接受等问题,因此数字时间戳对于电子合同的成立以及贸易的顺利进行是十分必要的。

4. 认证 认证由认证权威完成。认证权威是一些不直接从电子交易中获利的受法律承认的权威机构。其负责发放和管理电子证书,使网上交易的各方能互相确认身份。电子证书的管理不仅要保证证书能有效地存取,而且要保证证书不被非法获取,这是一项非常复杂的工作,通常通过以下环节加以保证:发放证书遵循一定的标准;证书的存放管理应遵循 X.500 或其简化版本 LDAP 协议;管理密钥和证书的有效期限。

电子证书就是一个数字文件,通常由 4 个部分组成:第一是证书持有人的姓名、地址等关键的个人信息;第二是证书持有人的公开密钥;第三是证书的序号,证书的有效期等;第四是发证单位的电子签名。电子证书由认证权威发放,具有法律效力,是电子商务中个人或单位身份的有效证明,类似于现实世界中的身份证、护照等。通过以上 4 方面的安全措施,实现了信息的保密性、法律的有效性、信息的真实性和信息的时效性。



三、国际电子商务的操作程序

基于安全保护措施之上的国际电子商务的具体操作程序如上图所示：

(1) 卖方利用买方的公开密钥加密发价报文并且数字签名后交给买方，同时在报文上面加上数字时间戳。

(2) 买方利用其私人密钥破译报文并且证明卖方的数字签名有效。买方同时加密并数字签名一条接受发价的报文将其返还给发价人，于是达成一条电子合同。一个数字时间戳附在报文上面证明接受发价的日期和时间。

(3) 在一条电子合同中详细规定了卖方获得付款所必需的义务，这些义务包括第三方服务提供者(即货物转运人、承运人、保险代理、海关等)的义务。送交给第三方服务提供者的指示也必须加密、数字签名和所有数字时间戳。

(4) 第三方服务提供者完成义务后，发送一条加密、数字签名、盖有数字时间戳的报文给买方证明其义务已经履行。

(5) 根据电子合同所有的付款要求已经满足后，卖方给买方发送一条加密、数字签名并附有数字时间戳的报文证明合同条款已经履行并通知付款。

(6) 一旦确信所有的付款要求已经满足，买方可以通过电子支票和信用卡进行付款或通过金融中介付款。

(7) 根据付款或承兑，卖方发送数字签名、加密以及附有数字时间戳的报文给第三方服务提供者，指示其向买方转移货物所有权。随着代表货物所有权的电子单据转移给买方，买方可以收取货物。

(作者单位：上海对外贸易学院)