汪 斌 （重庆万州重庆三峡学院经贸系 404000）

Realization and Improvement of On-line E-business Authentication System

电子商务中认证系统的实现与改进

摘要： 本文在介绍认证中心的基础上，分析了数字证书的原理、身份认证过程，讨论了智能卡身份认证系统方案，提出了认证中心的改进措施。

关键词： 数字证书 身份认证 智能卡CA

1 引言

在Internet开放式环境中身份认证是电子商务安全进行的前提和基础，如何保证网上身份的真实性，如何有效实施身份认证这是电子商务安全问题中的一个重要方面，这就引出了电子商务中一个非常重要的角色，即认证中心CA (Certificate Authority)，通过CA对网上交易参与者进行身份认证，确认身份真实后颁发网上身份证，即数字证书，CA保证认证范围内的用户身份是真实的，如果为假，CA来赔，CA不参加交易，以保证公正中立的角色，建立起第三方信任，因此，CA一般由能够承担赔偿责任的、权威的、社会公认的经济实体来担当，并承担相应的经济责任。我国一些地区已建立电子商务认证中心，开始网上认证系统的建设和运行，例如上海市电子商务安全证书管理中心有限公司。

CA有四大职能：证书发放、证书更新、证书撤消、证书验证。认证中心采用多层次的分级结构，如全国性总认证中心 (Root CA)，下属分支认证中心，再划分为个人、商业、网关等认证中心。在网上交易的参与方有：持卡人、商家、发卡行、收单行、认证中心、支付网关 (如图1)，各方根据SET协议来实现网上安全交易，由CA为这些交易参与方颁发相应的数字证书，如持卡人证书、商家证书、支付网关证书等，本文不讨论SET工作原理，重点分析认证系统是如何安全实现的。

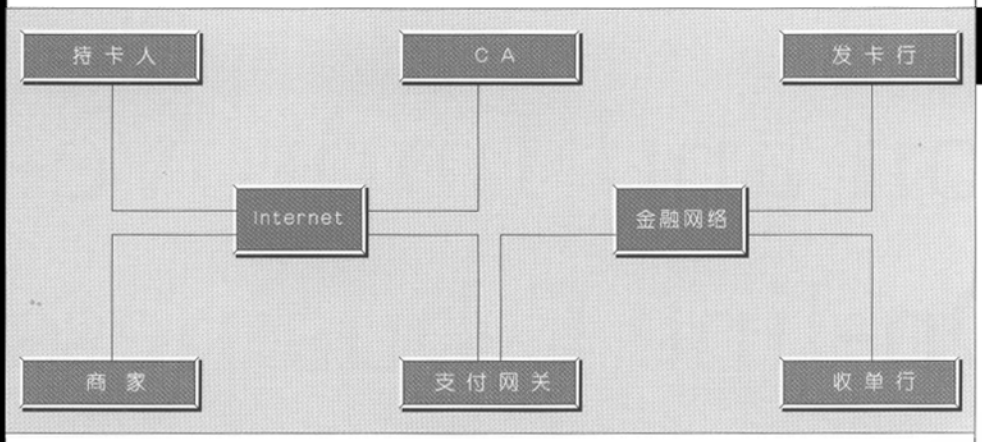

图 1　数字证书获取和密钥产生过程

2　数字证书及其工作原理

CA认证的主要工具是数字证书，数字证书是网上身份证、密钥和身份的绑定，通过数字证书和数字签名保证交易方身份的真实性，信息传输的保密性，访问权限的可控性，数据的不可篡改性，交易的不可抵赖性。数字证书是一个经CA数字签名的电子文件，证书的格式采用X.509V3国际标准，主要包括：拥有者姓名、拥有者的公钥、公钥有效期、颁发数字证书的单位及其数字签名、数字证书的序列号。

SET安全电子交易协议采用RSA公开密钥密码体系建立起一套严密的身份认证系统：将交易主体的公钥保存在数字证书中，将相应的私钥保存在个人PC机上。发送时，发送方用私钥进行数字签名；接收时，接收者用接收到的发送方证书中的公开密钥进行验证，从而实现对通信双方的认证，确保交易双方是合法主体。SET协议通过数字证书来保存公钥，并通过对数字证书的管理实现对公钥的管理。在交易过程中，交易双方使用数字证书来交换公钥，并提请CA来验证对方身份的合法性，并可以通过CA的上一级认证中心直至根认证中心来验证各级CA的合法性。

持卡人数字证书获取和密钥产生过程如下(见图1)：

(1) 持卡人提出申请，登记。

(2) CA接收申请，发送自己的证书和应答。

(3) 持卡人收到应答，验证证书后，填写信用卡信息并请求登记。

(4) 认证中心通过发卡行验证信用卡后处理登记表信息并发回登记表。

(5) 持卡人接收登记表，填写个人信息同时产生密钥对，将公钥和登记表发送给CA，请求颁发数字证书。

(6) CA处理证书请求，创建证书并生成CA对该证书的数字签名，发回给持卡人。

(7) 持卡人接收证书并保存在自己的PC机上。

密钥对即是公钥和私钥，是基于RSA算法的，公钥保存在数字证书上，私钥保存在自己的PC机上，根据RSA算法原理，私钥必须是保密的，确保私钥及数字证书的安全显得极其重要。而个人PC机在物理安全、病毒破坏、盗窃私钥、网络攻击等方面存在潜在的威胁，相比起来使用智能卡保存数字证书和私钥会更加安全。

3　使用智能卡的认证系统方案

使用数字证书实现网上交易的一种方法是将数字证书和私钥保存在自己的PC机上，另一种方法是保存在智能卡上。智能卡(Smart Card)是一种镶嵌有大规模集成电路芯片的塑料卡片，包括CPU、RAM、ROM、EEPROM、COS，与IC卡不同的是它既能存储、读写数据，还有数据处理能力，可以进行数据加密、解密和数字签名。其优点有：

(1) 由于磁卡不具备数据处理能力，持卡人不能验证系统真伪，只能系统验证持卡人的身份，而智能卡具有数据处理能力，可实现与系统的相互认证。

(2) 智能卡中的数据处理可在卡中完成，避免了在卡与读写设备之间频繁传输数据，从而大大提高了信息的安全保密性。

(3) 智能卡可以设置口令，以便对使用者进行身份鉴别，确认用户的合法性。

(4) 可以实现异地网上购物，而将数字证书和私钥保存在PC机上就只能在该机上进行交易，显得不方便。同时PC机连在开放的Internet上，存在着潜在的安全威胁。

使用智能卡系统进行认证的流程如下：

(1) 客户机请求连接。

(2) 认证服务器生成随机数X，并计算出X的数字摘要M，并用私钥SK进行数字签名，得S，将X+S传送给客户机。

(3) 客户机将X+S传给智能卡。

(4) 智能卡用CA数字证书中的公钥对S解密得到数字摘要M，并用同样算法计算出X的数字摘要M1，比较M与M1，若一致则认证服务器为真，如图2。

(5) 智能卡用自己的私钥对X进行数字签名，得X1，并用CA数字证书中的公钥对数字签名X1加密，得X2，将X2传给客户机。

(6) 客户机将X2传给认证服务器。

(7) 认证服务器用自己的私钥解密X2，得X1，用智能卡数字证书中的公钥对数字签名X1进行验证，得X，如果验证正确，则该卡可以进行交易。

在以上流程中安全实现了智能卡和认证服务器之间的双向认证，既保证智能卡接收到的数据是从认证服务器传过来的，又保证智能卡

确实是这个持卡人的，身份得以确认。其身份认证是基于RSA公开密钥密码系统和数字签名技术，这些技术均符合智能卡具备的基本功能，SET协议又为支持智能卡作了相关规定，解决了智能卡与网上交易的结合，因此使用智能卡比使用磁卡和固定PC机更安全、更方便，更适应电子商务的发展需要。

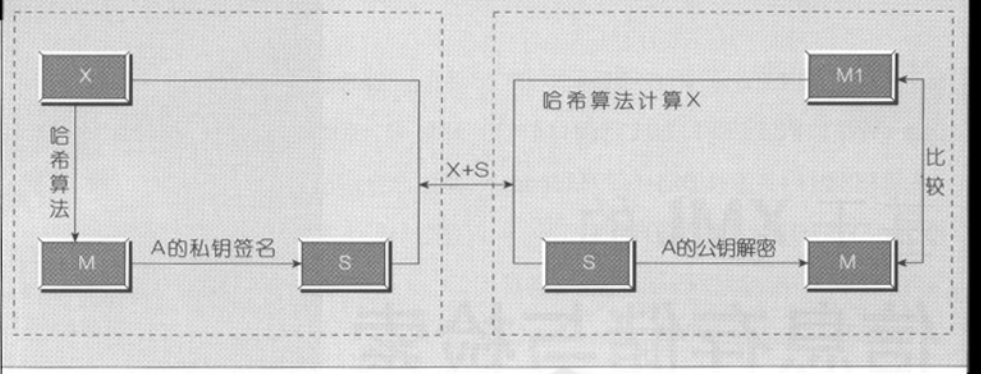

图 2　数字摘要的算法及服务器认证

4　认证中心的改进措施

以上讨论的认证中心确认了交易双方身份的有效性，CA具有证书发放、更新、撤消、验证的功能，但对于交易中、交易后依然存在以下问题：交易事务处理后，如何安全地保存或销毁数据，是保存在个人PC机上，还是在商家服务器和收单行计算机里？商家提供的货物不符合质量标准，消费者提出异议，怎么办？如何进行仲裁？因此还需要进一步确认电子交易的有效性。若增设一个电子交易认证中心ECA，或者由传统的认证中心充当，增强认证中心功能，则可以解决这些问题。

当网上交易发生后，要使双方不得否认此交易的有效性，可采取如下措施：电子交易认证中心对有效性交易加盖时间戳，并在一定时间内加以保存，作为交易有效性的法律依据。在交易中双方发生争执时，电子交易认证中心有权进行仲裁，决定此交易是否应当取消或者应当生效。此笔交易记录及时间戳放在电子交易认证中心，可以避免将电子交易记录放在个人PC机、商家服务器、收单行计算机上而受到各种恶意攻击。

当网上交易中消费者提出异议时，可以按照SET协议交易的流程并采用如下的改进措施，来实现网上公平、安全交易。交易参与方关系见图1所示。

(1) 消费者已确定定单，签发付款指令，发卡行核实消费者有能力付款后，将此笔款项存入一冻结帐户暂存七天，并通知商家的收单行可以交货。

(2) 收单行得到发卡行的通知后，通过支付网关通知商家可以交货。

(3) 商家收到收单行通知后，向消费者发货或提供服务。

(4) 如果七天内，消费者无异议，则在第八天电子交易认证中心自动通知发卡行将冻结帐户资金划入收单行，收单行再通知商家款已到位，如果第八天款没有到位，商家可向电子交易认证中心询问，进行仲裁。

(5) 如果七天内，消费者有异议，则向电子交易认证中心和商家同时发消息，要求退货或取消此笔交易，电子交易认证中心通知发卡行将冻结帐户再推迟七天，等待商家答复。

(6) 若商家同意退货，则电子交易认证中心要求商家和消费者共同签名，并将签名发给发卡行，发卡行将冻结帐户划回给消费者。

(7) 若商家不同意退货，则电子交易认证中心派人调查，进行仲裁。仲裁结果为货物有质量等问题，则执行(6)步，仲裁结果为货物符合质量等要求，则执行(4)步。以上步骤都要加盖时间戳。若商家不予答复，则电子交易认证中心每隔七天通知发卡行冻结推迟七天，直到商家答复为止。

通过采用以上措施，可以加强认证中心的功能，既可避免商家提供的货物不符合质量标准，又可避免消费者故意不付款，在电子交易认证中心的监督下，同时保证商家和消费者的利益。使认证中心的功能得以扩充，不但能进行身份有效性认证，而且能进行交易有效性认证，使之成为电子商务系统的安全核心。

5　结束语

CA认证是互连网络、电子商务中的关键环节，它为交易方颁发数字证书，为网上交易加盖时间戳，确定交易的有效性，为交易争端进行仲裁。离开CA认证系统，电子商务的安全就没有保障，认证系统的安全实现至关重要。因此，我们在构建电子商务系统时应重视智能卡在认证系统的软硬件应用，加强认证系统的建设，改进原有系统的漏洞，使认证系统更完善、更安全，有了这样的基础条件，我国的电子商务就会健康、快速发展，在进入WTO和全球经济一体化环境下有更强的竞争能力。

参 考 文 献

1 陈凡等，SET协议的分析与改进措施 [J]，计算机系统应用，2000.7。

2 詹江平，SET电子商务中更安全的密钥和证书保护方案 [J]，武汉大学学报 (自然科学版)，2000.3。

3 钱名海，B2B企业电子商务的安全保障，中国B2B电子商务上海论坛，2000.6。