

Design and Implementation of Stamp-based Digital Signature System

Xin-gang ZHANG¹, Heng PAN²

¹School of Computer & Information Technology, Nanyang Normal University, Nanyang, China

²School of Computer, Zhongyuan University of Technology, Zhengzhou, China

Email: zxcg550@gmail.com, panhengpan@yahoo.com.cn

Abstract: The importance of digital signature in security problems of Internet transaction is expatiated, and the correlative technique of digital signature is introduced. Through the research of digital signature technology, the current domestic and foreign technology is analyzed, a digital signature system based on digital stamp is presented. This model is based on digital certificate and PKI, and it is feasible and simple; in the development of .NET, the approach is realized. Moreover, the running interface is shown.

Keywords: digital signature; stamp; e-commerce; digital certificate

基于图章的数字签名系统的设计与实现

张新刚¹, 潘 恒²

¹南阳师范学院计算机与信息技术学院, 南阳, 中国, 473061

²中原工学院计算机学院, 郑州, 中国, 450007

Email: zxcg550@gmail.com, panhengpan@yahoo.com.cn

摘 要: 本文首先阐述了网上交易安全问题中数字签名的重要性, 并介绍了数字签名的相关技术。通过对数字签名技术的研究, 在对目前国内外相关技术分析的基础上, 提出一种基于图章的数字签名系统模型, 该模型在前台完全类似于传统手写签名的过程, 后台实现采用基于数字证书和 PKI 的数字签名技术, 该方案简易可行, 具有重要的推广意义, 并在 .NET 环境下实现, 最后给出了运行界面。

关键词: 数字签名; 图章; 电子商务; 数字证书

1 引言

随着信息技术的不断发展, 电子商务对传统的商务活动带来了巨大的冲击, 其突出的标志就是增加贸易机会, 简化贸易流程, 提高贸易效率。电子商务极大地改变了商务模式, 带动了经济结构的变革。同时, 电子商务也是一个充满挑战的领域, 这种挑战在很大程度上来源于对可使用的安全技术的信赖。在开放的网络上处理交易, 如何保证传输数据的安全和交易对方的确认, 已成为电子商务能否更好普及的关键。数字签名作为一种特殊的安全机制, 成为电子商务安全性的重要部分, 特别是对从事国际间 B2B(企业对企业)电子商务的企业, 大大节省了交易时间, 降低了交易

成本。

在传统的商业系统中, 通常都是利用书面文件的亲笔签名或印章来规定契约性的责任; 而在电子商务中, 传送的文件是通过电子签名来证明当事人身份与数据的真实性。数据加密是保护数据的最基本方法, 它只能防止第三者获得真实数据, 数字签名则可以解决否认、伪造、篡改及冒充等问题。数字签名的应用范围十分广泛, 在保障电子数据交换(EDI)的安全性上是一个突破性的进展[1-4]。凡是需要对用户的身份进行判断的情况都可以使用数字签名, 如加密信件、商务信函、订货购买系统、远程金融交易、自动模式处理等。

如何保证网上传输数据的安全和交易对方的身份确认是电子商务是否得到推广的关键, 可以说电子商务最关键的问题是安全性问题。而数字签名(Digital Signatures)技术是保证信息传输的保密性、数据交换的

基金项目: 河南省重点科技攻关项目(No.102102210388); 河南省教育厅自然科学研究项目(No.2009B520023); 南阳市科技攻关项目(Nos.2008GG020; 2009GG035)

完整性、发送信息的不可否认性、交易者身份的确定性的一种有效的解决方案[5-8]，是保障电子商务安全性的重要部分。

电子商务中数据传输所面临的安全问题主要有：

(1) 数据的保密性：用于防止非法用户进入系统及合法用户对系统资源的非法使用。

(2) 数据的完整性：防止非法用户对进行交换的数据进行无意或恶意的修改、插入，防止交换的数据丢失等。

(3) 数据的不可否认性：对数据的来源进行验证，以确保数据由合法的用户发出；防止数据发送方在发出数据后又加以否认；同时防止接收方在收到数据后又否认曾收到过此数据及篡改数据。

上述需求对应于防火墙、加密、数字签名、身份认证等技术，但其关键还是在于数字签名技术。而基于图章的数字签名系统就是在数字签名技术上更深入的去解决上述问题。

本文将从什么是数字签名和数字签名的理论基础来更深入的研究基于图章的数字签名系统。基于图章的数字签名系统是在 Microsoft Visual Studio 平台上开发出来的一种基于 .net 架构的新型数字签名系统。该系统的数字签名技术在电子商务中应用最多的 web 应用程序和文件传输过程中嵌入电子图章来实现数字签名的可视化。这种可视化既继承了传统的纸质签名的特点，增强了用户的安全感；又可以在不改变密钥的基础上修改图章，展现用户的个性。本文将以在基于 web 应用程序开发的在线购书系统来实现和调试该课题的研究。

2 数字签名

数字签名是非对称密钥技术的一种应用模式，用于保证报文的完整性，不可否认性，以及提供身份认证。在数字化文档上的数字签名类似于纸张上的手写签名，是不可伪造的。接收者能够验证文档确实来自签名者，并且签名后文档没有被修改过，从而保证信息的真实性和完整性[9-11]。完善的签名应满足以下三个条件：

- (1) 签名者事后不能抵赖自己的签名；
- (2) 任何其它人不能伪造签名；
- (3) 如果当事人双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。

2.1 数字签名的原理

数字签名的原理如图 1 所示。发送者在发送报文之前，先选用某种摘要算法为报文生成一个摘要值，并使用自己的私钥对摘要值加密，然后将加密后的摘要值附在报文后面，一同发送给报文的接收者。接收者收到报文后，从中分离出原始报文和加密后的报文摘要，使用与发送者相同的摘要算法计算原始报文的摘要值 D ，并使用发送者的公共密钥将加密后的报文摘要解密得到摘要值 D' ，检查 D 与 D' 是否匹配。如果匹配，那么由于密钥对的唯一性，便可以确定报文发送者的身份，根据数据摘要算法的特点，还可以确定原始报文在传输过程中是否被篡改。

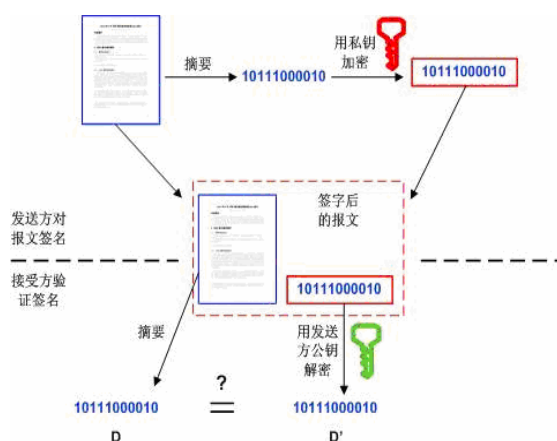


Figure 1. the principle of digital signature

图 1 数字签名的原理

2.2 数字签名的验证及文件传输过程

数字签名的验证及文件的传输过程如图 2 所示。

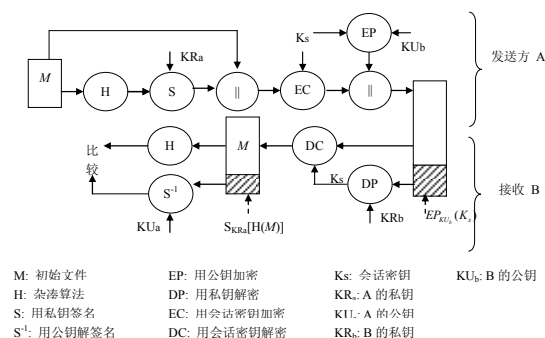


Figure 2. Digital Signature Authentication and the transmission of files

图 2 数字签名的验证及文件的传输过程

在网络传输过程，发送方和接收方的加密解密处理过程如下：

(1) 发送方将要发送的信息原文用 SHA 函数编码, 产生一段固定长度的数字摘要;

(2) 发送方用自己的私钥密钥对摘要加密, 形成了数字签名, 并附在要发送的信息原文后面;

(3) 发送方产生一个通信密钥, 并用它对带有数字签名的信息原文进行加密后, 传送到接收方;

(4) 发送方用接收方的公开密钥对自己的通信密钥进行加密后, 传到接收方;

(5) 接收方收到发送方加密后的通信密钥后, 用自己的私钥对其解密, 得到发送方的通信密钥;

(6) 接收方用发送方的通信密钥对收到的经加密的签名原文解密, 得到数字签名和信息原文;

(7) 接收方用发送方的公共密钥对数字签名进行解密, 得到摘要; 同时将收到的原文用 SHA 函数编码, 产生另一个摘要;

(8) 接收方将两个摘要进行比较, 如果两者一致, 则说明发送的信息原文在传送过程中信息没有被破坏或篡改过, 从而得到准确的原文。

3 基于图章的数字签名系统的设计与分析

3.1 系统设计与实现

基于图章的数字签名, 其核心技术是数字签名技术。由于数字签名是一组难以理解的数字串, 这对于使用者来说太抽象, 而电子图章是数字签名的可视化表现形式。我们设计的基于图章的数字签名系统结构如图 3 所示。

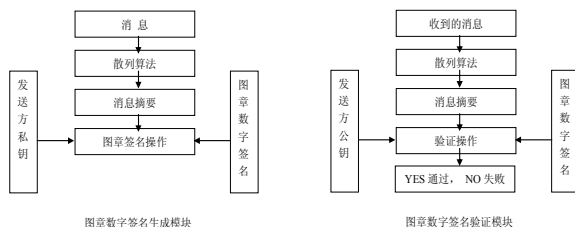


Figure 3. the system structure of stamp-based digital signature system

图 3 基于图章的数字签名系统结构图

系统的功能实现分析如下:

(1) 获取数字证书。在数字签名的实现及验证流程中, 为了证实签名的公钥确实来自声称的签名方, 可以通过数字证书来绑定签名者的身份。数字证书可以通过向任何合法的 CA 中心提交申请而获得。本文使用 CAPICOM 提供的 Certificates 类的 Certificates.Find 方法来加载符合搜索条件的数字证书并加载到某个 Certificate 对象上。

(2) 生成摘要的实现。CAPICOM 中的 HashedData 类提供使用 hash 函数生成指定字符串摘要的功能。该类的 HashedData.Hash(p) 使用 Algorithm 属性中指定的算法标识产生 p 字符串的摘要, 并将结果存放于 Value 属性中。

(3) 数字签名的实现。CAPICOM 提供的 SignedData 类封装了实现数字签名的 SignedData.Sign 方法。该方法的第一个参数为一个 Signer 对象, 该 Signer 对象能够获得其 Signer.Certificate 属性指定的数字证书对应的密钥, SignedData.Sign 方法将会使用该密钥对 SignedData.Content 属性中指定的内容进行数字签名, 然后返回经过加密后的数字签名。

(4) 签名验证的实现。签名验证使用 CAPICOM 中的 SignedData 对象的 SignedData.Verify 方法实现。该方法首先验证由第一个参数指定的数字签名是否有效, 如果有效, 则调出签名者的公钥对数字签名进行解密, 获得报文摘要, 然后再使用签名者的 Hash 值对 SignedData.Content 属性中指定的值计算生成摘要, 最后比较两个摘要, 如果相同, 则返回验证成功值。反之, 则验证失败。

3.2 系统运行测试

我们对系统进行运行测试, 其具体运行过程如下。首先打开主界面, 如图 4 所示:

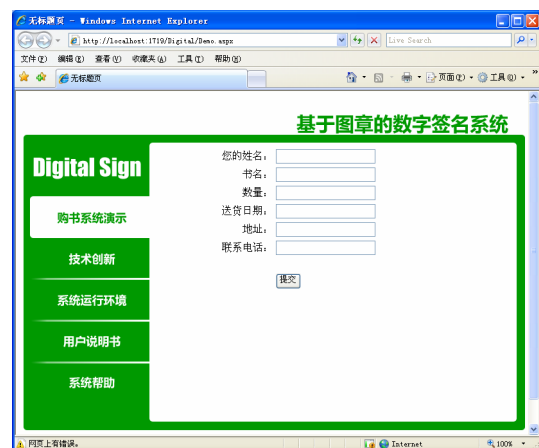


Figure 4. the main interface of the system

图 4 系统运行的主界面

在上图表单中填写需要被签名的数据, 点击“提交”将会出现对刚才所填信息的核对, 再点击底端的“数字签名”, 将出现以下窗口: 在图 4 中的“选择证书”窗口中选择计算机中已安装的证书, 或者点击“从磁盘打开”然后选择自己的证书, 证书格式一般为

pfx 或 der, 选择了错误的文件会出现错误的界面, 如果选择的证书需要输入密码, 则在弹出的窗口中输入正确的密码, 将会出现另一个窗口, 在该窗口中可以设置使用证书的安全级别, 比如可以在使用证书之前输入密码进行确认。默认级别点击“OK”即可。选择好证书后出现的界面如图 5 所示:



Figure 5. Effect Picture of digital signature

图 5 数字签名完成后的效果图

以上是选择证书的过程, 相当于传统签章中准备印章, 然后就会出现用户已经设定好的印章图片, 印章将会跟随鼠标移动, 将印章移到要签名的位置后点击左键, 即可完成签名过程。查看证书签名的效果如图 6 所示。

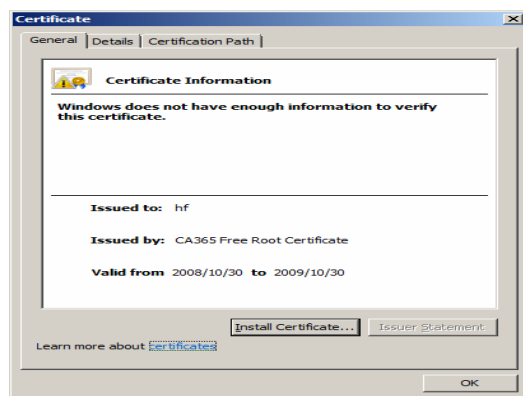


Figure 6. the main interface of signature verification

图 6 验证签名的界面图

3.3 过程分析

当用户触发签名事件时, 新建 Store 对象, 调用 open() 方法打开已安装到计算机的证书, 用 Certificates() 方法读出所有查找到的证书供用户选择, 如果用户不选择证书而是从磁盘加载, 则创建 Certificate 对象, 用 Load() 方法加载磁盘的证书, 然后

创建 Signer 对象, 让 Signer 对象的 Certificate 属性为上一步中用户在证书列表或磁盘中选择的证书, 当用户确认签名时创建 HashedData 对象, 对 Algorithm 属性赋值以选择不同的 Hash 算法, 调用 Hash() 方法后, 结果将保存到 value 属性中, 然后创建 SignedData 对象, Content 属性中存入需要签名的 Hash 值 value, 并调用 Sign(Signer) 方法, 返回值即为已签名的数据, 此时完成了签名的整个过程, 可以调用 SignedData 中 Certificates() 方法返回的 Certificate 对象的 Display() 方法显示证书, 或 SignedData 对象的 Verify() 方法验证签名。

4 结束语

基于图章的数字签名技术不仅可以在网络上进行身份识别和消息认证, 还可以代替一切的签名、盖章、证件等。在电子商务中, 数字签名可以保障交易的安全, 也可以用作数字货币。基于图章的数字签名技术通过图章或图片签名来直观表现出来, 用户只需对图章或签名进行验证就可以达到目的。这样既节省了验证所需的时间, 同时也提高了软件的使用效率。

本文通过对数字签名技术的研究, 在分析目前国内外对电子商务中数据传输的保密性、完整性和不可否认性以及交易对方的身份确认所采用的技术后, 提出一种基于图章的数字签名方案。基于图章的数字签名系统采用 B/S 模式, 提供 .Net 控件和代码插件, 可广泛应用于 .Net 和 J2EE 两大 Web 平台, 通过控件直接调用基于图章的数字签名的功能, 方便用户使用。

References (参考文献)

- [1] Y.Q.ZHANG and G.Z. XIAO, Software Developing for Digital Signature Scheme[J]. Journal of xi'an highway university, 1999, vol. 23, no.4, p55-58.
- [2] Xingang Zhang. Analysis of Campus Network Security Emergency Response Linkage System. Proceedings of 2010 International Conference on Information Technology and Industrial Engineering. June 2010, p1016-1020.
- [3] He Xuechen, Chen Linling, Zhao Yan. The information confrontation and network safety. Beijing: Tsinghua University Press. 2006.
- [4] Long Dongyang, Wang Changji, Wu Dan. Application coding and Computer. Beijing: Tsinghua University Press. 2006.
- [5] Poulakis, Dimitrios, A variant of Digital Signature Algorithm Designs, Codes, and Cryptography, 2009, v51, n1, p99-104.
- [6] Gauravaram, Praveen and nudsén, Lars R. On randomizing hash functions to strengthen the security of digital signatures. Lecture Notes in Computer Science, 2009, p88-105.
- [7] Levi, Albert; Güder, Can Berk. Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach. Computers and Security, 2009, v28, n3-4, p105-120.
- [8] Xin-gang Zhang. Control Strategy Based on Worms Spread in Complex Network, 2009 Third International Symposium on In-