基于 PKI 的电子签章系统的实现

郭正荣　周　城

（南京陆军指挥学院作战实验中心　南京 210045）（重庆通信学院计算机教研室　重庆 400035）

摘　要　首先介绍 PKI 公钥基础设施和数字签名的原理；然后阐述了基于 PKI 的电子签章各个功能模块的设计与实现，其中着重说明了签名与验证模块的实现原理及方法；最后，对电子签章的安全性进行了分析，表明所实现的电子签章能够保证网络信息的完整性、可认证性和不可抵赖性。

关键词　PKI，数字签名，电子签章，CryptoAPI

Implementation of Electronic Seal System Based on PKI

GUO Zheng-Rong　ZHOU Cheng

(Operations Research Center of Nanjing Army Command College, Nanjing 210045)

(Chongqing Comminucation College, Chongqing 400035)

Abstract　Firstly, the concept of PKI and the principle of digital signature are introduced. Then, describes the design and implementation of electronic seal's function modules, and the principle, method of how to realize the module of signature and verification are also emphasized. Lastly, analyzes the security of electronic seal and proves that it can ensure the data on network is integrality, availability, and no-denying.

Keywords　PKI, Digital signature, Electronic seal, CryptoAPI

基于 PKI(Public Key Infrastructure，公开密钥基础设施)的数字签名技术是当前解决信息完整性和不可否认性问题的主要技术手段之一。本文所实现的基于 PKI 技术的电子签章能够将数字签名与印章图像相结合，有效解决网络信息的完整性、可认证性和不可否认性等信息安全问题。

1　PKI 公钥基础设施

PKI 的概念是由美国学者于 20 世纪 80 年代提出的，它是一种遵循标准的、利用公钥密码理论和技术建立的提供安全服务的基础设施，是一种在开放的网络环境中提供安全服务的统一技术框架[1]。

PKI 主要由权威认证机构 CA 中心、证书库、密钥备份与恢复系统、证书作废系统和客户端应用接口系统等基本部分组成[2]。其中，CA 中心是 PKI 体系的核心，是数字证书的签发机构。它通过对实体身份信息和相应公钥数据的数字签名，来捆绑该实体的公钥和身份，以证明各实体在网上身份的真实性。数字证书，用于标识网络用户的身份，是由 CA 中心签发的，包含公开密钥拥有者相关信息、颁发者(CA 中心)相关信息以及公开密钥相关信息等的一种电子文件[3]。

2　数字签名

数字签名是指电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据[4]。它实际上是一个加密的信息摘要，即用签名者的私钥加密哈希值就构成了一个数字签名，可用来保证网络信息在传输过程中的完整性、信息发送者的身份可认证性和不可抵赖性，是保证网络中传输的数据没有被非法篡改的主要手段，可以解决否认、伪造、篡改及冒充等问题。其原理如图 1 所示：

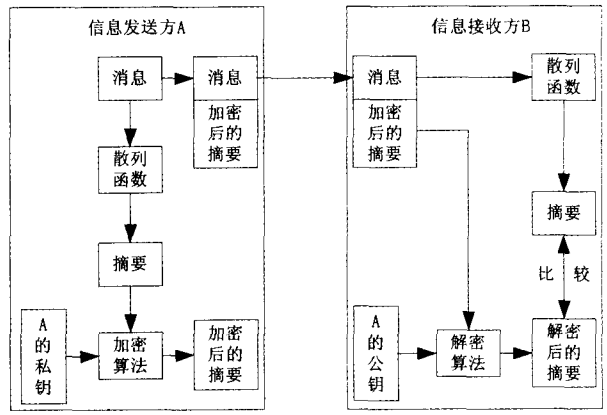


图 1　数字签名与验证

3　基于 PKI 的电子签章的设计与实现

我们通过 Microsoft Visual C++ 6.0 和 Microsoft Visual Basic 6.0 开发工具，采用 COM 组件技术实现了电子签章与 WORD 应用程序的无缝链接，利用 CryptoAPI 函数库实现的数字签名技术与数字图像处理技术有机地结合在一起，实现对 WORD 文档内容的电子签名与验证，并且将验证的结果通过印章图像直观地显示出来。

3.1　电子签章的功能模块设计

整个电子签章系统划分为 WORD 嵌入模块、公章图像模块、数字签名及验证模块和证书信息模块四个模块，各个模块设计方法及功能如下：

1. WORD 嵌入模块　采用了 COM 控件的形式，直接调用 WORD 的函数库。此模块主要负责整个签章与 WORD 的信息交换，是签章和 WORD 之间的桥梁，数字签名的数据以

及验证时候的数据都由此模块负责提供，并且它还有一个重要的作用，就是载入公章图像模块。实现该模块的 COM 组件为 WordCert. dll，其中，对外接口 IWordCert 是实现整个电子签章模块与 WORD 交互的接口。在运行程序后，WordCert. dll 就已经嵌入 WORD 中，进行签章、验证和其他操作的时候，其他模块即可调用 IWordCert 的方法和属性和 WORD 实现交互。

2. 公章图像模块　是整个签章的可见部分，主要负责浮透显示印章图象，以及提供功能菜单，可以看作是整个签章模块的中枢。它负责调用各个功能模块的应用，同时也是与用户交互的模块。此模块采用了 OCX 控件技术，无对外接口，保证了数据的安全性以及系统的稳定性。

3. 签名与验证模块　完成 WORD 文档内容的数字签名以及需要时候的验证。既保证了电子文档在网络传输当中的完整性，同时也保证了签名的不可抵赖性。实现该模块的 COM 组件为 CertSignVerify. dll，它调用 CryptoAPI 函数库进行开发，采用的算法为 SHA-1 摘要算法和 RSA 签名算法。主要的两个接口分别为 ICertSign 接口（实现数字签名）和 ICertVerify 接口（实现验证）。这两个接口都由公章图像模块的弹出式菜单的菜单项调用。

4. 证书信息模块　主要是实现让用户可以查看签章使用的数字证书。GetCertificate. dll 就是此模块的 COM 实现组件，通过调用 IGetCert 接口，从电子令牌里面获取签章所用的数字证书，查看相应信息。

各个模块之间是相互作用的，首先安装电子签章系统，WORD 嵌入模块 WordCert. dll 被嵌入到 WORD 当中。其次，实现电子签章，用户通过签章按钮将图像模块插入到 WORD 文档，图像模块通过 WordCert. dll 的 IWordCert 接口的方法和属性与 WORD 交互，然后再将获取的信息提交给电子签名模块实现电子签名，最后将签名数据保存到图像模块中以便以后验证。它们之间的关系如图 2 所示：

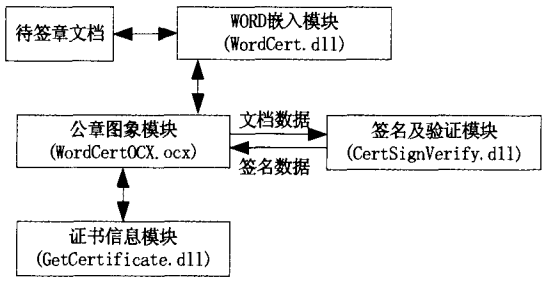


图 2　电子签章各功能模块之间的关系

3.2　电子签章中签名与验证模块的实现

前面我们已对签章各个模块的功能设计进行了简述，下面我们主要阐述电子签章中签名与验证模块的实现原理及方法。

1. 签名与验证模块实现的原理

(1)数据的签名

在实际应用中，签名的实现主要是通过签名证书来完成的。图 3 给出了利用签名证书实现数据签名的主要过程，其主要步骤如下：

①获取要签名的数据；

②打开包含签名者证书的证书库；

③获取与证书公钥相对应的签名私钥，并从证书属性中判断所使用的哈希算法；

④利用哈希函数对数据进行散列，产生数据的摘要(哈希值)；

⑤利用从签名证书属性中获取的私钥加密摘要，产生数字签名。

所以，在一个数字签名中，要包含如下信息：要签名的数据、哈希算法、签名、签名标识(证书发布者和序列号)和签名者证书(可选，包括签名者公钥)等。

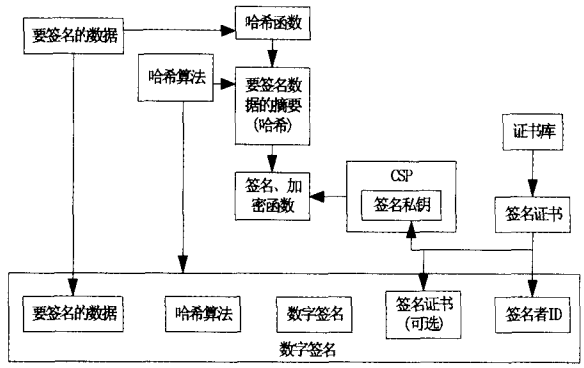


图 3　基于证书的数字签名

(2)签名的验证

签名的验证刚好相反，图 4 给出了利用证书实现一个数字签名的验证过程。

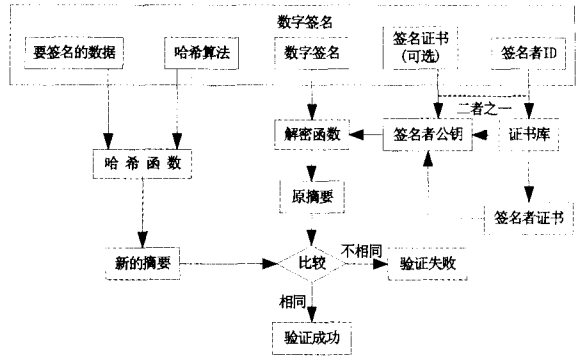


图 4　基于证书的数字签名的验证

2. 程序实现

签名与验证模块 CertSignVerify. dll 的两个主要接口分别为 ICertSign 接口(签名接口)和 ICertVerify 接口(验证接口)，其方法分别为：

STDMETHODIMP CCertSign::SignData(BSTR signeddata, BSTR pk, BSTR * signature)该方法实现数据的签名，其参数的定义为：

Signeddata：电子签名的原始数据；pk：签名数字证书的公钥；signature：电子签名结果；

STDMETHODIMP CCertVerify :: VerifySign (BSTR signeddata, BSTR signature, BSTR * signer)，该方法实现签名的验证，其参数的定义为：

Signeddata：电子签名的原始数据；signature：电子签名的结果；signer：验证结果。

这两个方法主要是通过调用 Microsoft CryptoAPI 函数库来实现[5]。其涉及到的 CryptoAPI 函数主要有：

CryptAcquireContext(获得 CSP 的句柄)

CertOpenStore(取得本地系统证书库句柄)

CertFindCertificateInStore(在本地证书库中查找签名者的证书)

(下转第 88 页)

总结和未来的工作 本文介绍了 NetData-Workbench，即一个语义网环境的网上数据工作台。设计和开发这个平台的目的是为了帮助领域专家更加方面快捷地在线加入领域研究和相关工程。文内介绍了工作台的体系和工作台使用的本体。并且利用这个平台建立了中医药领域的应用。本体是平台的核心部分，没有本体，工作台就不能成为一个整体。

当然，还有很多的工作需要继续完成。语义支持是很重要的部分，也是平台可以不断发展的部分，进一步的开发要不断地加强这一模块的功能。另一方面，在下一步的开发中打算使用 OWL 替代 RDFS，作为本体的描述语言来得到更强的语义表达。同时，我们对于数据的表达形式要做到可配置，使得领域专家在处理数据时可以更加方便有效。

所以，接下去最需要改进平台的两个部分：一个是语义支持，另一个就是数据的表现形式和数据的输入方式需要可以对应于本体概念进行配置。

参 考 文 献

1 Chen Huajun, Wu Zhaohui, Huang Chang, et al. TCM-Grid: Weaving a Medical Grid for Traditional Chinese Medicine. In: International Conference on Computational Science, 2003. 1143～1152
2 Wu Zhaohui, Chen Huajun, Xu Jiefeng. Knowledge Base Grid: A Generic Grid Architecture for Semantic Web. J Comput Sci & Technol, 2003, 18(4): 462～473
3 Wu Zhaohui, Chen Huajun, Deng Shuiguang, et al. DartGrid: RDF-Mediated Database Integration and Process Coordination Using Grid as the Platform. In: APWeb 2005. 351～363
4 Dingli A, Ciravegna F, Wilks Y. Automatic semantic annotation using unsupervised information extraction and integration. In: Proceedings of SemAnnot 2003 Workshop, 2003
5 Decker S, Melnik S, van Harmelen Frank, et al. The Semantic Web: The Roles of XML and RDF. IEEE Internet Computing, 2000, 4(5): 63～74
6 Kiryakov A, Popov B, Ognyanoff D, et al. Semantic Annotation, Indexing, and Retrieval. International Semantic Web Conference (ISWC), 2003

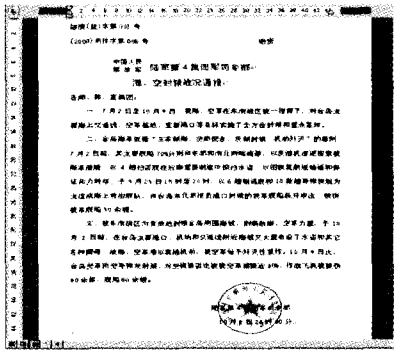
(上接第 84 页)

CryptSignMessage(签名原始数据)

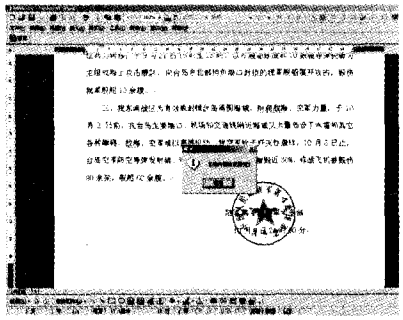
CryptVerifyMessageSignature(对签名进行验证)

3. 实现结果

为验证该电子签章的实际效果，笔者利用该电子签章对军用文书分别进行签章、验证和篡改后的验证，实验结果如图 5 所示。



(a) 文档的签名



(b) 文档内容无篡改的验证

(c) 文档内容篡改后的验证

图 5 WORD 文档的签名与验证

4 基于 PKI 的电子签章的安全性分析

基于 PKI 技术的电子签章的安全性主要表现在以下几个方面：

1. 数字证书和用户印章本身的安全。本电子签章中，用户证书和印章图像绑定在一起，采用 USB 接口的硬件设备－电子令牌作为存储介质。数字证书及其对应的私钥、用户印章图像都存储在电子令牌中，私钥由电子令牌内置 CPU 生成，不可导出数据，使得电子令牌无法被复制及仿冒；同时，电子令牌中数据由用户可以定期修改的 PIN 码提供保护，可有效地防止电子令牌丢失后被他人冒用。

2. 信息的完整性。由 Hash 函数(散列函数)的特性可知，若信息在传输过程中被篡改，完整性受到破坏，接收方重新计算出的摘要必然不同于用发送方的公钥解密出的摘要，则接收方得知其得到的信息并非发送方最初发送的信息。

3. 信源确认(信息可认证性)。因为公钥和私钥间存在对应关系，既然接收方能用发送方的公钥解开加密的摘要，并且其值与接收方重新计算出的摘要一致，则该信息必然是发送方发出的。

4. 信息的不可抵赖性。由于只有信息的发送方持有自己的私钥，其它人不能冒用其身份，故发送方无法否认他曾经发送过该信息。

结束语 本文设计并实现了一个基于 PKI 技术的电子签章系统，该系统将数字证书与印章图像绑定在一起，保证了签名的不可抵赖性；同时电子签章又确保了文档的完整性，使得对签章以后的文档的任何改动都会从签章上显示出来。在网络安全服务倍受关注的今天，该系统具有较高实用价值，有着广阔的应用前景。

参 考 文 献

1 关振胜. 公钥基础设施 PKI 与认证机构 CA [M]. 北京：电子工业出版社，2002
2 张世永. 网络安全原理与应用[M]. 北京：科学出版社，2003
3 雪涛. 基于 PKI 的安全电子邮件系统的设计与实现[D]. 四川：四川大学计算机系，2003
4 曹丽红. 浅议《电子签名法》[J]. 网络安全技术与应用，2004，46(10)：69～70
5 周城，郭正荣. 基于 Microsoft 密码体系的数字信封的实现[J]. 重庆大学学报，2005，28(6)：77～78