doi :10.3969/j.issn.1671-1122.2012.09.012

数字证书应用系统的设计与实现

韩水玲，马敏，王涛，康晓凤

（徐州工程学院信电工程学院，江苏徐州 2210000）

摘　要：为了使学习者更深入的了解数字证书的原理及应用，完善实验室数字证书应用教学系统，文章以 Java 为开发语言，以 Microsoft SQL Server 2008 为数据管理平台，开发了该数字证书系统，实现了数字证书申请、数字证书签发与销毁、数字证书挂失、数字证书加密及数字证书的数字签名等功能。该系统的应用不仅可以很好地解决网络应用中存在的信息泄露、窃听和用户抵赖等问题，同时还可以让使用者更快、更直接地了解数字证书技术。

关键字：数字证书；加密；签名；加密算法

中图分类号：TP393.08　文献标识码：A　文章编号：1671-1122（2012）09-0043-03

Design and Implemtntation of Digital Certificate Application System

HAN Shui-ling, MA Min ,WANG Tao, KANG Xiao-feng

(*Xuzhou Institute of Technology, Computing Science Department, Xuzhou Jiangsu,* 221000, *China*)

Abstract: We developed the system with the java and microsoft SQL server 2008. The purpose is to make the learners understanding the principle and application of digital certificate more deeply and improve lab digital the certificate system of laboratory. The system includes the function of application. issuing, destruction, reporting the loss, crypto, signature and so on. With the system not only can solution the network problem of information disclosure, tapping and user deny and so on but also can help the user understanding of certificate technology rapidly.

Key words: digital certificate; crypto; signature; crypto algorithms

0 引言

随着计算机技术和网络技术的飞速发展，网络攻击、黑客、病毒、抵赖、窃听、泄密等安全事件层出不穷，数字证书伪造事件时有发生，使一些网络用户遭受了大量的财产损失，数字证书技术渐渐的引起了人们的高度重视。为了使学习者更深入的了解数字证书的原理，应用并完善实验室数字证书应用教学系统，我们将数字证书的应用通过计算机模拟实现，然后应用到实际的学习或教学中，让学习者能很轻松的理解数字证书的应用原理并迅速掌握这些内容，以期有效的提高了学习者的学习效率和学习质量。

1 系统整体设计方案

本作品在充分研究了数字证书加密技术和签名技术原理的基础上，利用 RSA 加密算法，安全散列算法 SHA-1 和 MD5 签名算法[1-3]，以 Java 为开发语言，Eclipse 为开发环境，Microsoft SQL Server 2008 为数据管理平台[4-6]，实现了数字证书申请、数字证书签发与销毁、数字证书挂失、数字证书加密及数字证书的数字签名等功能[7]。

本系统有两种登录模式分为普通用户模式及管理员模式，并拥有五个模块，不同登录模式下可进入不同模块实现对证书的不同操作。普通用户模式下可进入的模块有：数字证书申请、证书加密、证书挂失、数字证书签名，管理员模式下可进入的模块为：证书签发与证书销毁。利用本系统普通用户可以实现数字证书的申请、导出、本地安装，然后利用申请到的数字证书进行数据加密和数字签名，管理员可以实现对用户申请的证书进行签发，对过期的或者违规使用的证书进行销毁和证书挂失等功能，其总体框架图如图 1 所示。

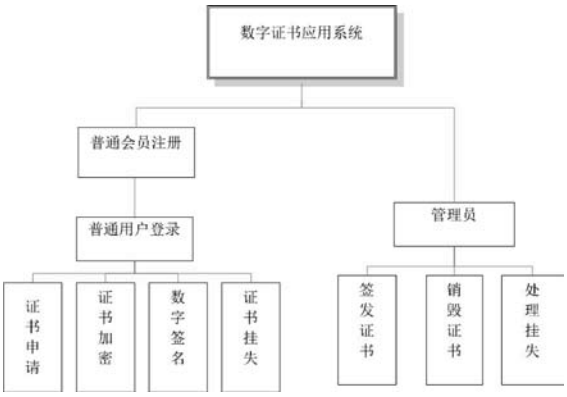

图1 系统总体框图

收稿时间：2012-07-28

作者简介：韩水玲（1991-），女，江苏，本科，主要研究方向：信息安全；马敏（1989-），女，江苏，本科，主要研究方向：信息安全；王涛（1989-），男，江苏，本科，主要研究方向：信息安全；康晓凤（1978-），女，江苏，讲师，主要研究方向：信息安全。

2 系统的实现及应用原理

2.1 注册界面模块

系统的注册界面模块保证了后续申请证书时，一个用户只能对应一个证书。在注册新用户的界面下，需要输入的信息包括 :证件类型、证件号码、用户名、密码、确认密码、联系方式。在输入信息的过程中，当证件类型选择身份证时，在证件号码中必须填写合法的身份证号（身份证号必须为 18 位），身份证号码必须唯一，密码和确认密码必须保持一致，否则系统将会根据错误原因提示错误信息，并要求重新输入。信息填写成功后，系统会自动将新申请用户的信息加载到数据库。

2.2 登录界面模块

在登录界面下共有两种身份的登录模式，分别为“ 普通用户 ” 登录模式和“ 管理员 ” 登录模式。在进入所需登录的模式后，在用户名和密码栏中填写信息，提取数据库中的信息与填写的信息与进行比较，在对数据库的信息进行提取时采用 DBConnect 下的 update(String sql) 方法参数为所进行的正确的 SQL 语句，经比较后若一致则成功进入系统，否则提示“ 用户名或密码错误 ” 并要求重新输入。

2.3 申请证书界面模块

申请证书模块拥有让已登录的普通用户输入申请数字证书所需的信息的权限。在此系统中能够申请数字证书并且最终完成证书的导出安装以及后续的加密签名。这个申请的证书就类似于我们生活中办理的身份证一样，在本模块下采用 Keytool 工具下的 genkey 命令将数字证书和密钥对储存到密钥仓中，同时采用自定义类 DBConnect() 下的 update() 函数将证书加载到数据库中进行管理，其申请证书界面如图 2 所示。

当申请证书步骤完成后，等待管理员审核通过，当管理员签发了该数字证书，普通用户有权将证书导出。同样是再次进入到申请证书界面，在界面的最右下角，普通用户输入自己的用户名后，点击导出证书按钮。导出证书时，系统会根据普通用户的别名（alias）在密钥仓库中找到之前用户申请时所填写的信息，通过 X.509 的标准，将这些信息以证书的形式完整的保存。然后，普通用户可以选择的保存路径来保存该数字证书，证书文件名是用户保存时填写的，文件类型为 .cer。最后，用户就可以对此证书进行本地安装导入以及后续的加密签名等工作，图 3 为导出后的证书信息。

图2 申请证书模块

图3 证书信息

2.4 证书加密解密界面模块

网络中在传送数据时，存在被窃听的可能，所以加密技术是最常用的保密安全手段，它利用证书的公钥把重要的信息变成乱码进行加密，得到密文，然后利用该证书的私钥对密文进行解密，得到明文。通过对比待加密的信息与解密后得到的明文，可验证证书公钥加密和私钥解密的有效性。

经管理员签发后的数字证书可以进行加密解密，在该界面，用户输入自己的数字证书的别名（alias）和密码后可以在“ 请输入待加密的消息 ” 中填写你需要在该数字证书中所要进行加密的消息，然后点击“ 利用公钥对消息进行加密 ” 系统便会对此消息进行加密，“ 利用私钥对密文进行解密 ” 便会进行逆时针解密操作。系统利用算法进行的具体加密和解密过程如图 4 和图 5 所示。该模块下使用的核心加密算法是 RSA 加密算法。

图4 证书加密界面

图5 证书解密界面

2.5 数字签名界面模块

加密技术解决了信息传送的保密问题，而确定发送者身份和防止他人对传输文件进行破坏的问题还需要数字签名这一手段，例如在电子商务中，完善的数字签名具备签字方不能抵赖、他人不能伪造、在公证人面前能够验证真伪的能力。本系统模拟了这种技术，如图 6 所示。首先对原始文件进行摘要，得到摘要文件 digest.dat，然后利用证书的私钥对摘要文件 digest.dat 进行签名，得到签名文件 Sign.dat，然后利用证书的公钥对签名文件 Sign.dat 进行验证。若验证成功，则显示“签名正确”；否则，显示“签名不匹配”。

该模块就是通过 MD5 算法使原文件形成摘要，再利用自己的私钥对此摘要进行加密形成数字签名，这份数字签名不但能够确认用户的真实身份具有认证性和不可否认性，同时还可以保证信息传递过程中的完整性。简而言之，如果 A 向 B 发送消息，A 先从报文文本中生成一个报文摘要，然后用自己的私钥对这个摘要进行加密作为自己的数字签名，而接收方 B 接收到报文后，先计算出该摘要，然后用发送方 A 的公钥对该数字签名进行解密，如果两个一样，那么 B 就能确认是 A 发送的。

图6 数字签名界面模块

2.6 挂失申请界面模块

当数字证书丢失，或者用户认为其的证书密钥可能泄露而导致不安全时，可以选择向管理员申请挂失数字证书，类似于身份证丢失，向公安机关申请挂失一样。当然在管理员更新数据的 16 秒内，用户也具有取消挂失的权利。

2.7 管理员界面模块

管理员界面模块中包括签发证书、销毁证书、处理挂失请求等功能。

本系统的签发证书模块是用来对已经申请的证书进行审核签发的操作，就好像公安机关签发身份证一样，只有签发后的证书才可以进行安装，加密与数字签名等一些应用。在该系统中，普通用户申请后的证书已经将其所有的信息以 flag 值为 0 的形式保存在数据库中，管理员以管理员的身份通过登入界面登入后。在该界面中，管理员可以看到所有普通用户申请的数字证书（即在数据库中 flag 值为 0 的证书），管理员选择一个普通用户的数字证书点击签发证书按钮对证书进行签发。签发后，该用户保存在数据库中的证书的 flag 值便会由 0 变为 1，也就是将已签发的证书的 flag 值标识为 1。

管理员签发后的数字证书，如果超过有效期或者存在违规操作的情况，管理员有权销毁证书，销毁证书的功能也是通过数据库得以实现的。管理员点击选择销毁证书按钮，下拉菜单中会向管理员展示所有已经签发了的数字证书，即在数据库中 flag 值为 1 的证书，管理员选定一个证书点击销毁证书按钮，弹出”销毁成功！”即该证书已为无效的证书，不能进行其他操作了。销毁后，该数字证书在数据库中的 flag 值变会由 1 变成 2。

管理员签发后的数字证书，如果有用户因某些原因申请挂失的情况，管理员有权处理用户的挂失请求，处理挂失功能是通过数据库得以实现的。管理员管理的系统界面中列出申请挂失的所有证书（即在数据库中 flag 值为 4 的证书），管理员选定确定挂失按钮，弹出“挂失成功！”对话框后，该数字证书在数据库中的 flag 值变会由 4 变成 5，在此期间，管理员更新数据 16 秒内，用户可以取消挂失，但超过 16 秒，该证书将处于销毁阶段。

3 结束语

本系统具有界面清晰、操作简单、灵活性强的特点，摆脱了商业或者企业数字签名系统的冗余与复杂，通过模拟实现证书申请和管理，实现了相关理论，对传输的数据进行了加密和鉴别，保证了信息传输的机密性、真实性、完整性和不可否认性，大大降低了探索数字证书系统的成本。同时，其简易性缩短了试验时间，为学习者进一步研究数字证书系统奠定了良好的基础，这样让使用者能够快速地了解数字证书技术的原理和数字证书系统的使用方法，能很好地满足业内人士实验和学习的需求，是教学中的好帮手，是安全人员的好工具。（责编 程斌）

参考文献：

[1] 周立兵，周大伟 . 基于数字证书的访问控制研究 [J]. 计算机与数字工程，2001，(01)：114-116
[2] 关振胜 . 公钥基础设施 PKI 及其应用 [M]. 北京：电子工业出版社，2008.
[3] 林东岱，曹天杰 . 应用密码学 [M]. 北京：科学出版社，2009.
[4] 马臣云，王彦 . 精通 PKI 网络安全认证技术与编程实现 [M]. 北京：人民邮电出版社，2008.
[5] 赵满来 . 可视化 Java GUI 程序设计 - - 基于 Eclipse VE 开发环境 [M]. 北京：清华大学出版社，2010.
[6] 霍尔泽 . Eclipse 集成开发工具 [M]. 南京：东南大学出版社，2005.
[7] 关振胜 . 公钥基础设施 PKI 及其应用 [M]. 北京：电子工业出版社，2008.