CA 认证系统的设计

吴庆敏[1]，韩义勇[1]，覃东海[1]，雷 霆[2]
（1. 广西玉柴机器股份有限公司，广西 玉林 537005；
2. 天津大学 计算机科学与技术学院，天津 300072）

摘 要：CA 认证是保证网上数据传输和网上身份认证的一种有效手段，PKI/CA 认证体系是目前比较流行的一种可靠的安全认证体系。本文给出一种方便有效的网上 CA 认证中心的搭建方式，重点讨论了 CA 认证中心证书的发布、认证、管理等问题，给出了一个包含 CA 认证中心和 RA 注册中心的完整 CA 认证系统的设计思想和具体实现方法。

关键词：CA 认证；网络安全；Web 平台；PKI
中图分类号：TP319 文献标识码：A 文章编号：1674-7720(2011)22-0001-03

Design on certificate authority system

Wu Qingmin[1], Han Yiyong[1], Qin Donghai[1], Lei Ting[2]
(1. Yuchai Machinery Co.,Ltd, Yulin 537005, China;
2. School of Computer Software, Tianjin University, Tianjin 300072, China)

Abstract: CA is an effective means to ensure that online data transmission and Internet certification authentication, PKI/CA authentication system is a more popular and reliable security authentication system. In this paper, a convenient and effective online CA structures is described. We focused on the CA certificate issued, authentication, and management. CA authentication system with CA and RA registration center integrity is designed and specific implementation is presented.

Key words: CA; Web security; Web network platform; PKI

为保障网上数字信息的传输安全，除了在通信传输中采用更强的加密算法等措施外，必须建立一种信任及信任验证机制，即参加电子商务的各方必须有一个可以被验证的标识，这就是 CA(Certificate Authority)认证[1-2]。

CA 认证是保证网上数据传输和网上身份认证的一种有效手段，PKI/CA 认证体系是目前比较流行的一种可靠的安全认证体系。CA 认证中心是公钥基础设施 PKI(Public Key Infrastructure)框架中负责发布和撤销证书的系统，它可以按照一定的信任模型来组织一个有效的信任系统[3,4]。CA 认证中心为每个 CA 用户发放一个数字证书，用来标识用户的身份，从而保证网上交易的安全性和不可抵赖性。

本系统的主要功能就是发放和管理数字证书，主要提供公钥加密和数字签名服务等功能，CA 认证系统是电子商务、电子政务等系统开展的基础，可以方便地为人们提供安全的通信方式，可以保护数据传输的安全性，从而建立一个安全的网上信任环境。

1 CA 认证技术

1.1 CA 认证

CA 认证的主要任务是受理数字证书的申请、签发数字证书及对数字证书进行管理。CA 作为可信任的第三方机构，把用户的密钥和其他的标示信息捆绑在一起，承担公钥体系中公钥的合法性检验的责任。CA 认证中心为每个客户发放数字证书，使第三者不能伪造和篡改证书，并负责产生、分配并管理所有参与网上信息交换各方所需的数字证书，是安全电子信息交换的核心[3]。CA 认证中心负责数字证书的申请、签发、制作、废止、认证和管理，提供网上客户身份认证、数字签名、电子公证、安全电子邮件等服务业务。

1.2 数字证书

数字证书是用来表示网上用户身份真实性的。数字证书就是网上表示用户身份的一系列数据，是由 CA 颁发的。目前使用较为广泛的数字证书的格式是X.509 v3 格式。X.509 v3 公钥证书的适用性非常广，采用 ASN.1

语法进行编码[5]。

1.3 RA

RA(Register Authority)是注册审核机构,RA 提供了用户与 CA 之间的接口,主要功能是用来收集用户信息和确认用户身份。一般来说,RA 接受用户的注册申请,并确认用户是否符合申请资格,最终决定 CA 是否给其签发数字证书,RA 还负责对发放的证书进行管理。发放的证书一般可以存在 IC 卡或 USB 设备中,RA 系统是整个 CA 系统不可缺少的部分。本系统的 RA 部分就是由基于 J2EE 的 Web 平台架构、MVC 设计模式实现,并采用 Oracle 来存储信息。

2 系统功能需求

2.1 系统功能需求模型

一个完善的 CA 认证系统应具备的主要功能如图 1 所示。

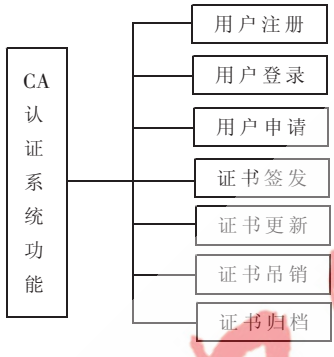

图 1 系统功能需求图

系统具有三种使用角色:用户、RA 管理员、CA 管理员。下面将对他们进行详细的用例分析。

(1) 用户的用例图如图 2 所示。

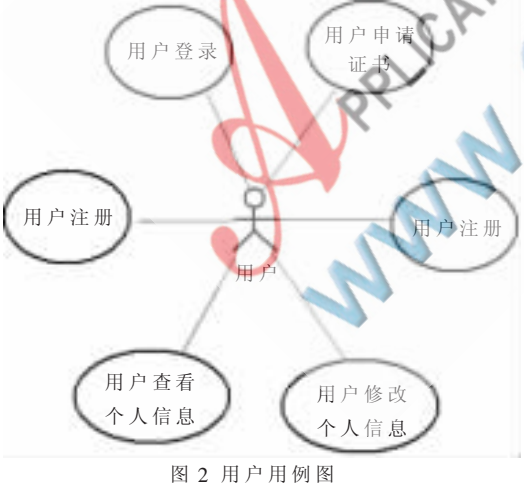

图 2 用户用例图

(2) RA 管理员用例图如图 3 所示。

(3) CA 管理员用例图如图 4 所示。

2.2 详细功能需求

(1) 用户注册。为了方便系统和用户管理,系统必须要有注册功能,用户注册之后将会拥有更多的权限,能够使用更多的功能。

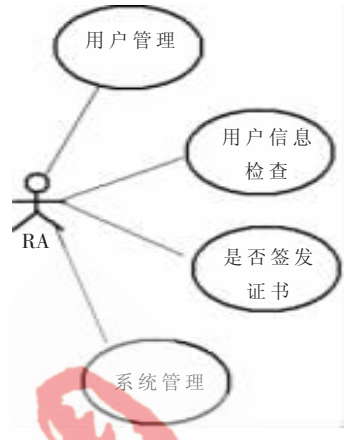

图 3 RA 管理员用例图

图 4 CA 管理员用例图

(2) 用户登录。注册之后的用户可以登录系统,使用系统的更多功能。

(3) 证书申请。采用在线申请方式和离线申请方式。在线申请:申请人登录到 RA 注册网站,通过网页提交申请信息,完成申请;离线申请:申请人到专门的 RA 申请机构,填写由申请机构提供的申请表,并提供相关的证件,完成申请。在证书申请阶段,申请人需要提供能够标示自己身份的公钥信息。申请信息提交到 RA 之后,证书申请过程即可完成。

(4) 申请人信息审核。RA 系统在接收到用户提交的申请之后,必须对证书进行审核,确认申请者是否具备申请条件,是否能够为该用户颁发数字证书。审核的范围一般包含两个方面:申请人提供的申请信息是否真实可信和申请证书的用途是否正确合法。

(5) 证书签发。申请人的申请通过审核之后,CA 中心就需要为合法用户签发数字证书,证书签发后,必须通过一定的渠道进行发布并储存,才能被用户使用。证书的发放有两种形式,一是在线发送,签发完毕后直接发送到用户邮箱中;二是离线发放,CA 将证书存入介质,一般为 IC 卡或 USB 设备,再由用户携带有效证件到 CA 处领取。证书的存放一般不需要加密存储,因为证书中存在 CA 的数字签名,证书中的任何改动都可以被发现,从而保证证书信息的完整性。

(6) 证书更新。CA 证书申请时都有有效期,一般为 1 年或 3 年,最长一般也不超过 5 年,这也是由实际因

素和理论因素所决定的,实际因素:CA 主体(包括单位和个人)的信息不是一成不变,一旦这些信息发生了变化,CA 证书的有效性和真实性就难以得到保证。另外,理论上的因素主要有:目前的电子计算机的运算速度发展很快,新的加密算法和破解算法也层出不穷,一个加密算法很难保证一直不会被破解,因此长期使用一种加密算法的做法并不可取,CA 证书需要在一定时间后及时更新。这就是证书的更新功能。每一个证书在申请时都有一个有效期,证书有效期期满后就需要更换新证书。

(7) 证书吊销。用户申请的证书也可能丢失或被盗窃,一旦发生了这些意外情况,就需要证书的吊销功能,证书的吊销就是用户在证书的有效期结束之前,要求停止使用证书,并作废证书。证书的吊销一般有两种情况:

① 必须是上级 CA 对下级证书的吊销,而不能反向执行,出现这种情况一般是上级 CA 不能信赖下级 CA。这时上级 CA 就可以吊销下级 CA 的证书。

② 下级证书主动申请证书的撤消。出现这种情况一般是下级 CA 或用户的自证书或密钥丢失或被盗窃,为了避免更大的损失而申请吊销证书。

(8) 证书归档。证书到了有效期,而用户却没有申请继续延长使用,这时就必须使用证书的归档功能。当用户更新证书之后,原来的旧证书也是要进行归档操作的。另外用户撤销的证书不能随意丢弃,也需要归档操作。

3 系统设计

3.1 系统功能设计

RA 注册中心主要负责普通用户浏览系统、注册用户、申请证书以及 RA 管理员管理用户、申请信息和管理系统。

RA 系统设计为三种用户权限,即一般游客、普通用户和管理员。三种用户应具备不同的权限,所看到的系统页面也应该有所不同。一般游客功能比较少。很多功能只有在注册成为普通用户后才能使用。

(1) 普通用户的活动图如图 5 所示。

(2) RA 管理员的活动图如图 6 所示。

RA 系统在接收到用户提交的申请之后,必须对证书进行审核,确认申请者是否具备申请条件,是否能够为该用户颁发数字证书。审核的范围一般包含:申请人提供的申请信息是否真实可信;申请证书的用途是否正确合法。

(3) CA 管理员的活动图如图 7 所示。

申请人的申请通过审核之后,CA 中心就需要为合法用户签发数字证书,证书签发后,CA 认证中心应包括证书签发、证书更新、发布证书信息、证书归档、证书管理与维护等功能。

3.2 系统数据库设计

系统的核心数据主要包括用户的信息、认证中心管理用户证书的相关数据。这些数据全部存在一个数据库里。用户的注册信息、申请信息、有效证书信息、作废或过期证书的信息将分别储存在不同的表中。为了保证系统有良好的移植性和扩展性,本系统的数据库采用 Oracle9i 数据库。用户证书申请表用于用户申请证书,其中存储的主要是用户的申请信息;用户证书表存储的主要是用户证书的相关信息;用户申请撤销表用于储存用户

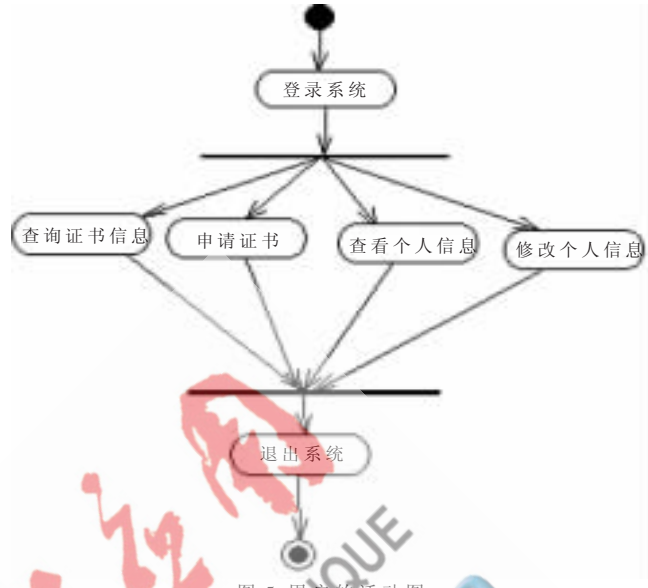

图 5 用户的活动图

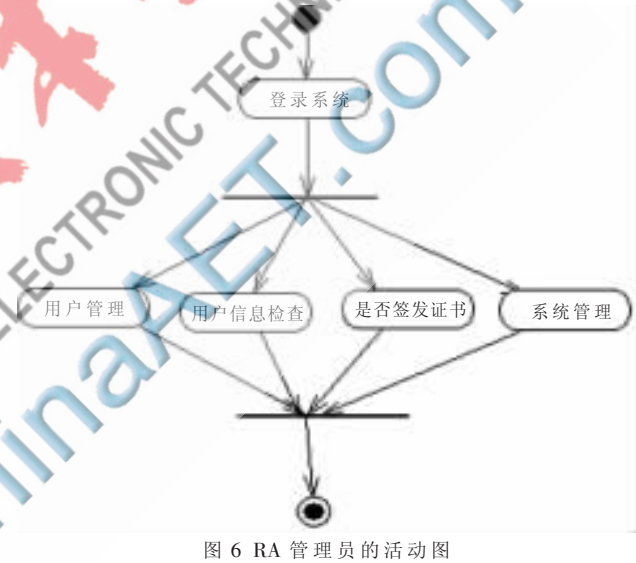

图 6 RA 管理员的活动图

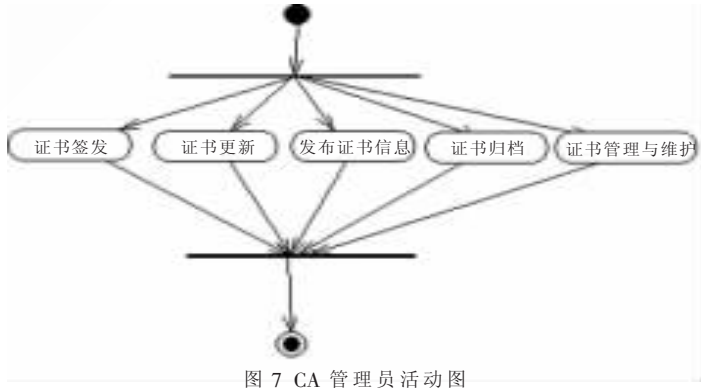

图 7 CA 管理员活动图

申请撤销证书的信息;用户撤销证书表记录被用户撤销的证书。

CA作为现代网络与信息系统的安全基础设施核心内容之一，在信息安全领域起到重要的作用，为电子商务、电子政务等网络应用提供了认证完整性、保密性和不可否认性等安全服务。本文就CA认证系统的体系结构和各个组成部分作出了详细的分析和设计，并给出了一种切实可行的系统实现方式,实现了CA系统的主要功能。

参考文献

[1] 卡哈特.Cryptography and network security[M].北京:清华大学出版社,2005.

[2] RESCORLA E. SSL与TSL[M].北京:中国电力出版社,2002.

[3] 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,2002.

[4] 宁宇鹏,陈昕. PKI技术[M]. 北京:机械工业出版社,2004.

[5] 迈瓦尔德.网络安全基础教程/Fundamentals of network security[M].北京:清华大学出版社,2005.

(收稿日期:2011-07-16)

作者简介:

吴庆敏,女,1981年生,本科,主要研究方向:信息技术及内燃机工程。

韩义勇,男,1979年生,硕士,主要研究方向:信息技术及内燃机工程。

覃东海,男,1975年生,本科,主要研究方向:信息技术及内燃机工程。