基于数字签名的身份认证模型的一种方案

徐小平，尹颖禹
（广东技术师范学院 电子信息工程系，广东 广州 510633）

摘 要：公开密钥基础设施(Public Key Infrastructure，PKI)是目前网络安全建设的基础与核心，是电子商务安全实施的基本保障。文中分析了PKI技术，提出了一种基于数字签名的身份认证模型的方案，给出了其模型结构，并详细地阐述了各部分的功能、实现的策略以及方法，解决了网络交易中对身份认证的要求，为保证网上交易安全提供了一种可行的身份认证模式。

关键词：公开密钥基础设施；数字签名；身份认证
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1005－3751(2006)02－0220－03

A Model Scheme for Identity Verification Based on Digital Signature

XU Xiao-ping, YIN Ying-yu
(Dept. of Electronic Info. Eng., Guangdong Polytechnic Normal Univ., Guangzhou 510633, China)

Abstract: PKI(public key infrastructure) is the infrastructure of electronic commerce security. It is the guarantee of electronic transaction security. Analyzes PKI, and presents a model scheme for identity verification based on digital signature. Gives the basic structure of model. Expounds its founction, strategy, and method in detail. Solves the problem of identity verification in electronic transaction, provides a model scheme of identity verification to ensure security in electronic transaction.

Key words: PKI; digital signature; identity verification

0 前 言

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并在不断普及。但由于各种原因，电子商务的安全性仍不能得到有效的保障。在通过网上进行电子商务交易时，由于交易双方并不现场交易，难以确认双方的合法身份，同时交易信息是交易双方的商业秘密，在网上传输时必须保证安全性，防止信息被窃取；双方的交易非现场交易，一旦发生纠纷，必须能够提供仲裁。由于数字证书认证技术采用了加密传输和数字签名，能够实现上述要求，因此在电子商务中得到了广泛的应用[1]。

1 公开密钥基础设施(PKI)

PKI(Public Key Infrastructure)是一个用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施。它遵循标准的公钥加密技术，为网上电子商务的开展，提供一整套安全的基础平台，为所有网络应用透明地提供采用加密和数字签名等密码服务所需要的密钥和证书管理[2]。

PKI采用证书进行公钥管理，通过第三方的可信任机构(认证中心，即CA)，把用户的公钥和用户的其他标识信息捆绑在一起，以在Internet网上验证用户的身份。通过把公钥密码和对称密码结合起来，实现密钥的自动管理，保证网上数据的安全传输。因此，所有提供公钥加密和数字签名服务的系统，都可归结为PKI系统的一部分。PKI组件如图1所示。

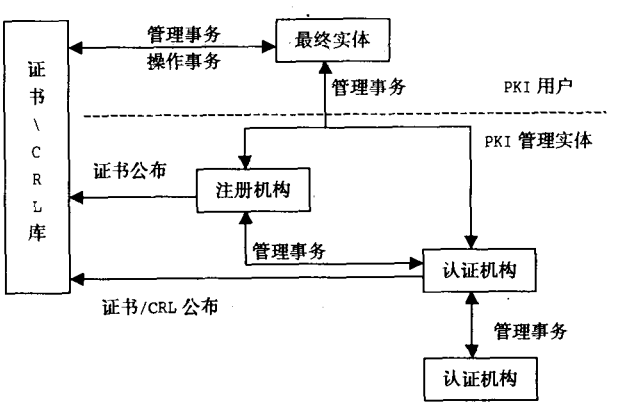

图1 PKI组件

2 认证模型的结构

文中设计了一个功能完善的CA系统，其组成结构如图2所示。

2.1 证书管理

证书管理处理在证书生命周期内应用于证书的操作

收稿日期：2005－05－25
基金项目：广东省教育厅高校自然科学研究项目(Z03061)
作者简介：徐小平(1965—)，女，重庆人，副教授，研究方向为软件工程、Internet环境及应用。

集合。在完成注册过程之后,CA必须对证书负责。证书管理包括以下过程:证书注册、证书更新、证书撤销。

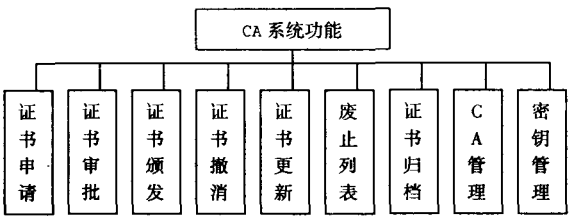

图2　CA模型功能结构

2.1.1　证书注册

(1)初始化。

初始化要求包括:RA名称/地址、CA证书、RA证书、可信锚列表、库名称、本地密钥产生、最终实体名称。

必须告知最终实体,可能需要配置的注册使用的RA或者CA的网络名字和地址或者与适当服务相应的URL。而在任何传输发生之前,PKI中的服务需要认证,必须在最终实体中安装秘密共享的某中适当形式,文中方案是将服务器证书的散列值传送给最终实体,并且调用CA或者RA操作,确认散列值与将要发送的某个值相匹配。分配信任锚给最终实体,为许多实现所接受的、不存在日期问题的一种机制是信任其友好Web浏览器发布的根CA集合。在注册请求中将使用的最终实体的名字必须是以某种方式配置或已知的,并且要求确定最终实体或者配置证书属性需要的其他信息。

(2)初始信任。

注册过程的下一个问题,即如何验证那将要证明的最终实体的身份。

对于数字签名来说,可以分配给新签署者一个用户ID和一个一次性口令。这可以通过一个带外机制如电子邮件来提供。当用户注册时,用户ID和口令可以用来验证用户身份。这并不要求处理验证的数据入口和透明问题,只要求极少的数据输入来初始化这个过程。

(3)注册要求。

在注册过程期间利用的信息应该不在CA最终颁发的证书中发布。诸如个人电话号码或者地址是显而易见的问题,并且为公众分发证书时有直接的隐私问题。然而,证书内依然有许多其他字段有暴露不同等级的敏感信息的潜在可能,如用户的唯一识别名。

在CA使用关于用户源信息的后台数据库以减少需要的数据条目数量的情况下,可能存在生效的关联,即证书中包含的最终信息透露出了比签署者乐意显示的信息更多的信息。因此,模型要求用户在证书发布给公开库之前提供关于证书内容的肯定确认。这允许用户验证在发行过程中CA增加或者修改的任何信息。

(4)拥有的证据。

对注册请求而言,要确认申请者真正拥有与正在注册的公开密钥相应的私钥。然而,私钥是存储在一个安全存储设备中或者受保护存储单元中。模型要求在证书发行之前证明申请者是私钥持有者,即要在注册时确定身份和私钥之间的联系。

(5)关于证书申请表格。

采用PKCS#10标准规定的电子证书申请的内容与格式,它分为两大部分,其一是申请书的基本信息,包括申请人名称、申请人公钥、申请人其他信息如:国家、省份、城市、单位、分支机构、电子邮件地址以及身份证号码;其二是申请人签名及签名算法。

2.1.2　最终实体证书更新

证书更新是假定你已经通过确定身份的过程和之前的所有其他约束。倘若密钥还没有因为某种原因而泄露,这就为更新证书时奠定了一个基础。

发行新证书有几个原因:与证书相关的密钥可能已经到达它有效生命的终点;证书可能已经过期;证书中已经证明的一些属性可能已经改变,并且对于这些新属性值必须重新证明。

不过,只要证书没有撤销,先前的密钥和证书就能够用来完成认证过程。如:当用户注册一个新密钥时,使用旧密钥和证书签名请求是允许的。

2.1.3　证书的获取

在验证信息的数字签名时,用户必须事先获取信息发送者的公钥证书,以对信息进行解密验证,同时还需要CA对发送者所发的证书进行验证,以确定发送者身份的有效性。

利用数字签名,可以方便地进行证书的分发。因为检验数字签名的通信方可能在本地已经拥有了必需的证书,因此,附加证书一般由签名者来决定。发送数字签名的证书的同时,可以发布证书链。这时,接收者拥有证书链上的每一个证书,从而可以验证发送者的证书。

验证过程如下:

通过检查发送者证书的发放机构CA,从CA中的目录服务器取得该CA证书,并重复这个步骤,直追溯到一个已拥有可信任公钥证书的CA机构为止。

2.1.4　证书格式

采用ITU的X.509定义的、被人们普遍接受且使用得最为广泛的标准公钥证书格式[3]。

2.1.5　证书验证

证书用户需要验证收到的证书。要验证一个证书则需要:

* 验证该证书的签名者的有效数字签名,以此确定证书内容没有被修改。

* 检查证书的有效期,确保该证书仍然有效。

* 证书可以包含一些字段,它们可被标记为关键的或者非关键的。如果证书被认为是有效的,则所有被标记为关键的字段必须能够被证书验证者的证书所理解。

* 检查该证书的预期用途是否符合CA在该证书中指定的所有策略限制。

* 确认该证书没有被CA撤销。

验证证书的过程是迭代寻找证书链中下一个证书和它相应的上级 CA 的证书。在使用每一个证书前,必须检查相应的 CRL(对用户来说,这种在线的检查是透明的)。用户检查证书的路径,是从最后一个证书(即用户已确认可以信任的 CA 证书)所签发的证书有效性开始,检验每一个证书,一旦验证后,就提取该证书中的公钥,用于检验下一个证书,直到验证完毕发送者的签名证书,并将该证书中包括的公钥用于验证签名。

2.1.6 证书撤销

公钥证书具有有限的有效生命期,该生命期用一个起始和终止日期时间来表示,存放在证书的有效期字段内。有效期的长短视发放证书的认证机构的政策而定,一般可以从几个月到几年不等。

在发放证书时,人们总希望在整个有效期内都能使用证书。然而在某些情况下,用户必须在证书期满前停止对证书的信任。当已知或怀疑相应的私钥被泄露,名称变更或主体与认证机构的关系发生变化时,就会发生这种情况。这时,认证机构可以撤销证书。由于证书可能被撤销,所以证书的运作期可能比原定的有效期要短[4]。

2.2 CA 的系统结构

为了使用某个异地通信方的公钥,证书用户(使用方)必须找到一条有效的完整的认证路径,将公钥从一个或多个认证机构传送到可信任的根认证机构——证书用户持有该 CA 的公钥并信任该 CA。在这过程中,一个主要的问题就是如何使寻找有效认证路径的过程变得简单、方便和高效,这在很大程度上要依赖于构造 CA 间结构关系的规则或协定,因为借助 CA 间的结构关系,才能使得一些认证机构能够验证其他认证机构的身份。

2.2.1 认证机构的组织结构

在证书格式确定后,需要确定结构模型来满足所有应用环境下的应用。模式的结构在于要解决两个核心问题:一是如何找到合适的认证路径,二是找到认证路径以后,如何使它生效。在每一个证书使用系统中都要有这两个功能,要把它们当作两个分开的任务来看待;而且它们的实现过程也是相对独立的,因为寻找认证路径的过程不是在实现安全性功能,而使认证路径有效则是在实现安全性功能。

这里采用网状模型结构。在该模型中,为建立一组信任关系,允许对等交叉认证关系中的每个参与者与其他对等方进行交叉认证。通过允许证书路径经过多个 CA 而创立一种建立长证书链的通用机制。采用这种机制,通过只允许从上级 CA 到下级 CA 的单向验证,可以建立一个下属层次结构。如果允许双边信任关系,沿路径上的每个 CA 已经相互交叉认证了对方。

2.2.2 路径构造

沿层次结构的路径算法在交叉认证的互联网络层次结构中比较容易实现。因此为了确定一条路径,路径构造过程沿"正向"从最终实体证书起始,到信任锚结束。它执行一个迭代过程,依次处理每个证书,把前一证书的颁发者名字作为后一证书的主体名字。由于每个证书都被处理,因此对证书的颁发者是否可信和 CA 都做了验证。为了验证待处理的证书颁发者,可以从 X.500 目录属性中获得接续的证书。如果遇到死终端和路由回绕,那么可以原路返回然后从一个已知点开始继续构造路径。

扩展库允许根据密钥用法、有效期和主体密钥标识(该标识必须和路径中前一证书的颁发者密钥标识一致)来规定证书选择原则。

2.2.3 路径验证

* 证书必须包含有效的密码签名,证明证书内容没有被他人更改过。

* 必须使用颁发者公钥来验证证书签名。

* 当前时间必须在由起始日期和终止日期说明的有效期内。

* 后继证书中的主体名字和颁发者名字必须匹配。

* 证书中不能含验证者不理解但在解释证书时又标记为关键的字段。

* 证书只能用于最初生成证书时想使用的场合。

* 主体名字必须符合所有的指定名称限制。

* 最终实体证书以外的其他证书必须明确标记为 CA 证书。

* 带有路径长度限制的所有 CA 证书,其后跟着的证书数目必须满足限制。

* 其他说明证书使用条件的策略限制也必须被遵守。

最后,证书必须未被撤销。即使证书内部所有信息都表明证书有效,也必须检查是否发生了一些导致要求作废证书的外部异常事件。因此必须使用证书撤销列表或者某种形式的在线验证进行撤销检查。

2.2.4 认证策略

当一个认证机构签发了一份证书后,它同时也向证书的使用者提供了一份声明,表明了一个特定的公钥只适用于一个特定的实体(证书的实体)。但是鉴别一个人的身份和他的其他特征以及检查公司的法人资格是否可信是认证机构的重要任务,所以,证书要按照不同的实际和程序来签发,并且要适应不同的需要。

一个认证机构一般会公布一份声明,叫作认证操作规范说明(CPS),规定了在认证过程中要遵循的操作程序。认证操作说明的内容包括证书的复杂性及长度说明等,但主要的是公开说明认证机构是如何运作的,认证策略的内容是由认证机构认为必须包含的内容组成,这些内容主要以来满足证书用户对特定认证的接受需要。根据 IETF 在 RFC2527 里给出的建议,认证策略中包含的主题包括:介绍;一般性规定;识别与认证策略;操作需求;物理上、程序上以及个人安全的控制;技术安全控制;证书及证书撤销表文件;管理规范。

(下转第 225 页)

$(p_1) \rightarrow roles(p_2))$

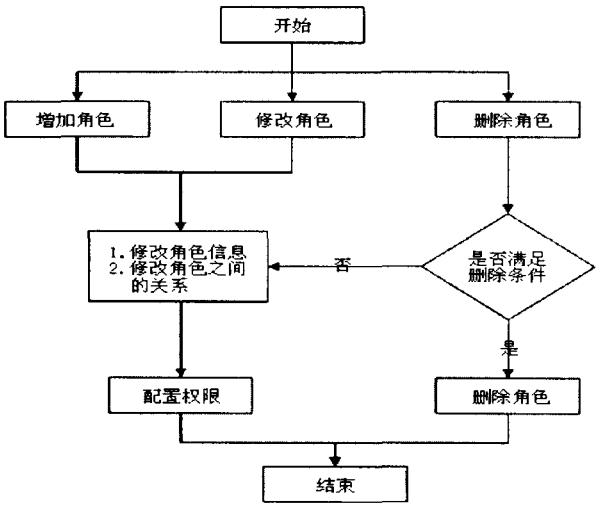

图 3　角色定义子模块流程图

2.3　数据库设计

根据需求分析和功能设计,系统的用户权限管理模块的数据库表结构设计如图 4 所示。

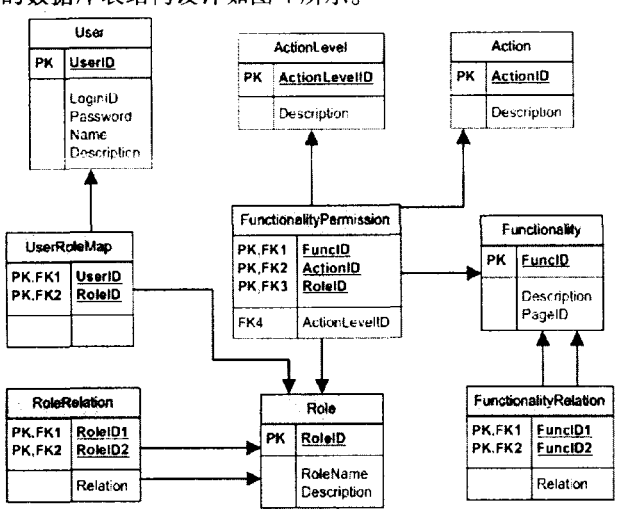

图 4　用户权限管理模块数据库表结构设计图

用户表(User)保存的是用户的登录信息,主要包括用户的登录名和密码等信息。角色关系表(RoleRelation)和功能关系表(FunctionalityRelation)分别保存的是角色间的关系信息和功能间的关系信息。角色表(Role)和用户表(User)通过 UserRoleMap 表关联,一个用户可以有多个角色,一个角色也可以分配给多个用户。为了满足最小权限原则,特别将权限的组成细分为:功能、功能上定义的操作和操作的级别,分别对应于 Functionality 表、Action 表和 ActionLevel 表。角色表(Role)通过 FunctionalityPermission 表和权限关联。FunctionalityPermission 表描述了某个角色在某个功能的某项操作上所具有的操作级别。一个角色可以有多项权限,一个权限也可以赋予多个角色。

3　结束语

以上所述实现基于角色的动态授权机制的实现方法已经成功应用于"黄陵县人事管理信息系统"。通过实践进一步证实了使用基于 RBAC 的动态授权机制开发的用户权限管理模块可以增强系统的灵活性,提高系统的安全性,增加模块的可重用性。

参考文献:

[1] 乔　颖,须　德,戴国忠. 一种基于角色访问控制(RBAC)的新模型及其实现机制[J]. 计算机研究与发展,2000(1):37－44.

[2] Ferraiolo D, Kuhn D R, Chandramouli R. Role based Access Control[M]. [s.l.]: Artech House, 2003.

[3] 李孟轲,余祥宣. 基于角色的访问控制技术及应用[J]. 计算机应用 2000(10):44－47.

[4] 黄益民,杨子江,平玲娣,等. 安全管理系统中基于角色访问控制的实施方法[J]. 浙江大学学报,2004(4):408－413.

[5] 蒋　韬,李信满,刘积仁. 信息安全模型研究[J]. 小型微型计算机系统,2000(10):1076－1081.

[6] Chang－Joo Moon, Dae－Ha Park, Soung－Jin Park, et al. Symmetric RBAC model that takes the separation of duty and role hierarchies into consideration[J]. Computers & Security, 2004(23):126－136.

[7] Joshi D J, Bertino E, Ghafoor A. Temporal Hierarchy and Inheritance Semantics for GTRBAC[A]. Proc. of the Seventh ACM Symposium on Access Control Models and Methodologies[C]. Monterey, CA, USA: [s.n.], 2002.

(上接第 222 页)

3　结束语

电子商务是 21 世纪最重要的商务模式,它势必会渗透到生活、生产及社会的各个方面中去。文中分析了 PKI 技术,并在此基础上提出了一种基于数字签名的身份认证模型的方案,基本能够解决在网络中交易对身份认证的要求,为实现网上交易提供了一种可行的模式,保证了交易的安全。

在设计开发的过程中,严格按 CMM 的要求进行,力争提供一个实用的商业版本[5]。目前模型还在设计阶段,对于具体的实现细节,还有许多需要进一步改进的地方。

参考文献:

[1] Nash A, Duane W. 公钥基础设施(PKI)实现和管理电子安全[M]. 张玉清,陈建奇,等译. 北京:清华大学出版社,2002.

[2] 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.

[3] Ford W, Baum M S. 安全电子商务——为数字签名和加密构造基础设施(第 2 版)[M]. 劳帼龄,等译 . 北京:人民邮电出版社,2002.

[4] 李明柱. PKI 技术及应用开发指南[EB/OL]. http://www.javaresearch.org, 2002－06－24

[5] 徐小平. CMM 中的需求管理[J]. 微机发展,2004,14(6):79－81.