基于证书角色管理的电子文档安全探讨

曾 韬[1] 吴宝昌[2] 余永权[1]
(广东工业大学 广州 510000)[1] (广东金融学院 广州 510520)[2]

摘 要 本文通过对电子公文的安全性分析,针对电子文档的特点,详细讲述了将其应用于电子文档的安全管理。其中包括PKI/CA体系,证书在角色管理中的运用。提出一个利用证书扩展属性给予对应的角色作必要的控制。

关键词 电子公文,电子文档,PKI/CA,证书,角色

Discussion of Electronic Document Security Based on Certificate Role Management

ZENG Tao[1] WU Bao-Chang[2] YU Yong-Quan[1]
(Guangdong University of Technology, Guangzhou 510000)[1] (Guangdong University of Finance, Guangzhou 510520)[2]

Abstract This paper analyzes the security issues of electronic archives, comprehensively discusses security management towards electronic documents according to the characteristics of electronic document, including the application of PKI/CA system, certificate in role management. Using certificate extendibility for essential control to corresponding role is proposed in this paper.

Keywords Electronic official document, Electronic document, PKI/CA, Certificate, Role

1 引言

电子政务是政府管理方式的一次革命。电子政务环境下产生的电子文件涉及各级党委、政府和国防的核心政务以及个人隐私,它关系到党政部门、各大系统乃至整个国家的利益,有的甚至涉及国家安全。因此,维护电子政务环境下电子文件信息安全具有重要意义。在公文应用日益流行的同时,与之俱来的是文件信息安全性需求的出现。保证电子公文的真实性、可靠性、完整性、可用性,以及保证电子公文的机密性、可控制性是十分必要的。在此本文在了解PKI体系基础下,假定每个公务员申请拥有个人CA证书,探讨如何利用证书进行分配角色、如何进行利用证书对文档访问的管理。

2 电子政务PKI/CA体系

PKI是当今国际上使用的较为成熟的解决开放式互联网络信息安全需求的一套体系,而且尚在发展之中。它是利用公共密钥理论的基础上建立的提供安全服务的基础设施,使用公开密钥技术和数字证书来确保系统信息安全,并负责验证数字证书持有者身份,通过第三方可信任机构认证中心CA把用户公钥和相关标识信息捆绑在一起,从而实现用户身份验证、密钥管理等安全功能,继而可构建一个完整的授权服务体系,并为用户建立和维护一个安全可信的网络运行环境,使其可以在多种应用环境下方便地使用加密和数字签名技术验证用户身份,从而保证数据信息的在网络传输时的真实性、完整性、机密性和不可抵赖性,保障电子政务应用的安全。PKI是信息安全技术的核心,也是有效开展电子政务的关键基础。

2.1 CA认证机构

CA认证机构,也称作认证中心,在整个PKI构架中的地位至关重要,是组成电子政务安全体系的核心环节。它不仅为客户提供签发公钥证书,认证证书和管理证书的服务,还为生命周期内的密钥提供管理服务,它将用户的公钥与用户的名称及其他属性关联起来,并制定政策和具体的步骤来验证、识别用户身份,再对用户证书进行签名,以确保证书持有者的身份和公钥的拥有权,对用户之间的电子身份进行认证。一个CA机构由证书审批机构RA和证书操作部门CP组成,RA是PKI和终端实体的接口,负责证书申请者得信息录入审核等并对发放的证书完成相应的管理功能,它所获得的用户标识的准确性是CA签发证书的基础;CP负责为已授权的申请者制作发放和管理证书,并承担因操作运营错误所产生的一切后果,包括失密和为没有获得授权者发放证书等功能。作为确保信任度的公正可信第三方权威实体,CA涉及交易方的身份信息标示及验证,保证用于签名证书的密钥的安全和质量,它允许撤销已发放的数字证书,能根据用户请求或其他相关信息撤销用户证书同时管理证书序列号等证书信息并完成数据库的备份工作等,同时管理公钥的整个生命周期。

2.2 证书

PKI体系通过颁发证书来实现身份认证、完整性、机密性和不可否认性等安全服务。证书是一个经证书认证机构(CA)数字签名的包含用户身份信息以及公开密钥信息的电子文件,证书是把一个密钥对绑定到一个身份上的被签署的数据结构,通过认证中心CA对证书的签名保障其合法性和有效性。证书包含的持有者公钥和相关信息的真实性和完整性也是通过CA签名来保障的,证书公钥可用于加密数据或验证对应私钥的签名。证书还有一个扩展属性,利用这个域可以标识不同用户的角色及其对文档的权限。

3 基于PKI证书角色分配解决方案

3.1 基于角色的访问控制(RBAC)文档安全访问控制技术

曾 韬 博士,研究方向:控制理论与控制工程。吴宝昌 硕士研究生。余永权 教授,博士生导师。

RBAC是近年来研究和发展得比较成熟的一种授权机制，它引入了角色的概念，所谓角色就是对资源进行操作的一组权限集，对用户的授权就是授予相应的角色，而不是将权限逐一地授予用户，因而减少了授权管理量，如图1所示。

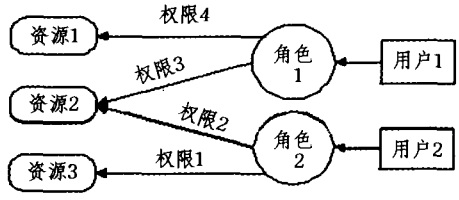

图1 基于角色的访问控制

对政府而言就是将政府组织视图中不同的职能岗位划分成不同的岗位角色，岗位角色就是在一个信息系统上具有相同操作权限的用户组，不同的岗位角色只能享有由系统管理员或子系统管理员分配的操作权限，它将整个系统的操作权限根据系统的菜单项划分成不同的功能元权限。功能元权限就是指不可再分的对系统的操作权限，而所有这些元权限构成一个功能元权限集合。分配给岗位角色的权限就是同工作岗位的职能相对应的功能元权限集合的子集，各个子集彼此不相等，对所有子集进行集合并运算得到的集合为元权限集合。每个用户根据需要可对应一个或几个岗位角色，同时在授予用户岗位角色时必须满足基本安全原则，即：

1)最小特权原则。指用户拥有的权限不能超出应完成工作所需的权限。

2)职责分离原则。指用户不能同时拥有这样两个岗位的角色。它们在工作中的职能是互相监督与制约的用户-岗位角色。

采用基于角色的访问控制在政府信息集成平台的电子文档安全管理中相当重要，就整个政府信息集成平台的电子文档安全管理而言，安全管理不仅仅是防止敏感信息的泄露，同时更要保证平台的可用性。所以，必须对电子文档的创建、查询、修改、删除等操作进行严格的管理，防止各类蓄意或无意的操作而导致平台中产生大量冗余而无用的垃圾信息或有效信息丢失，使得信息平台的使用效率降低。系统采用基于角色的访问控制，就是将系统的各项操作功能按不同的角色给予分配。而不同的用户又分配不同的角色，使每个用户都在规定的范围内对信息平台进行操作，保证信息平台高效安全地工作。

3.2 电子文档自主访问角色控制的实际应用

尽管RBAC提供了较好的安全管理机制，但由于政府内部是一个有机的整体，要提高政府竞争力必须保证各部门之间有机地协同合作，因此各类电子文档在不同部门，不同级别的岗位上流动，共享是不可避免的，而且部门间、部门内的合作关系也不是一成不变的。但是RBAC根据岗位来确定岗位角色，岗位角色被分配的权限是相对固定的，而且对应一组用户而不是单一用户，不可能根据某一用户权限需要的改变而改变分配给角色的权限，如果将电子文档权限的管理设计成为一种固定的模式则不能反映各部门之间、岗位之间合作的不确定性，因此，设计出一种能反映部门间、岗位间动态合作关系的电子文档动态授权模型并和RBAC相结合就显得十分必要。电子文档种类繁多，在此将各种电子文档统称为实体，对各种电子文档的授权称为实体授权，实体授权采用自主访问控制(DAC)是指文档创建者可以根据用户而不是角色来授予其文档的操作权限，而拥有对该文档操作权限的用户又可以将自身所拥有的操作权限授予其他不具有该操作权限的用户。对实体不可再分的各种操作权限称为实体元权限，这些元权限构成的集合称为实体元权限集合。每个主体、用户对某一实体的操作权限的集合都是实体原权限集合的子集。实体的创造者拥有对该实体的所有权限，并作为实体授权关系的起点。由于DAC是一种自主式授权，整个授权过程难以控制，如果不对授权者的授权行为进行监督，那么会使得授权行为具有相当大的随意性，可能造成政府敏感信息的泄露，因此加强授权行为的监督是必不可少的，最重要的是必须禁止重复授权，并且该授权关系必须记录在授权日志当中。当要削除某用户对某一实体的某项操作权限时必须由其上级授权用户来执行，削权信息也必须记录在日志内，在这种机制的管理下，如果一旦发生敏感信息泄露就可根据授权日志进行授权关系的追踪，从而达到掌控整个授权过程的目的，便于分析出由于人为因素造成的敏感信息的泄露的问题。尽管DAC机制提供了授权过程相当的灵活性，但同时也使授权关系变得十分复杂，如果不加以控制，用户间的授权关系将会十分混乱，不易管理，如图2所示。

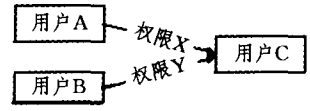

图2 授权关系一

图中用户A仅拥有权限x，而用户B仅拥有权限y，用户C不拥有权限x、y。但授权后，C却同时拥有权限x、y，反而比授权者A、B更高。当用户C拥有权限x、y后，又可能分别授予用户A对该实体的y权限，用户B对该实体的x权限，如图3所示。

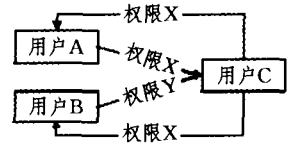

图3 授权关系二

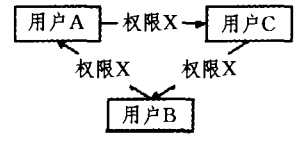

图4 授权关系三

除此之外，还会出现如图4一样的多个用户之间的循环授权。由于上述两种关系使得整个实体授权关系会形成一个网状结构，如果不对这个网状结构进行分解简化，会使得整个授权关系逻辑混乱、层次不清，大大降低管理效率。通过追踪某一具体实体元权限的授权关系可以发现，如果在这个网状结构上，将仅具有该权限的结点用户以及这些结点间的授权关系从整个实体授权关系中独立出来，会形成一个以实体创建者为根结点的树结构。那么假设实体元权限共有n个就会产生n棵授权关系树，一棵授权关系树就表示实体上一项权限的授权关系。树上的每一个结点表示对该实体具有该项操作权限的用户。如果n值不大，那么通过对这n棵树的管理就可以达到对整个实体授权的管理如图5所示。

(下转第111页)

表 2 试验结果

组别	节点数	平均查找步数
1	100	2.8809
2	1000	7.8433
3	2000	10.6713
4	3000	12.9757
5	4000	14.9045
6	5000	16.7572
7	6000	18.5037
8	7000	20.1106
9	8000	22.0903
10	9000	23.0067
11	10000	24.6342
12	12000	27.4529
13	15000	31.6142
14	20000	36.7902
15	25000	43.4994
16	30000	47.6794
17	40000	58.0572
18	50000	66.2148

我们将试验结果转换成平均查找步数与资源点数之间的关系图，如图 4 所示。

其中横坐标是资源点数，纵坐标是平均查找步数；黑色曲线(带点)是试验结果曲线，红色曲线是拟合函数曲线，拟合函数是 $y=x^{0.6}/10$。

结论 本文提出了一种描述网格计算资源的空间模型，在该模型下，不需建立全局的资源视图，系统不会随着资源数量的快速增加而变得不可用。另外由于资源的搜索总是朝着有利的方向发展，因此能够提高资源的搜索速度比较快。

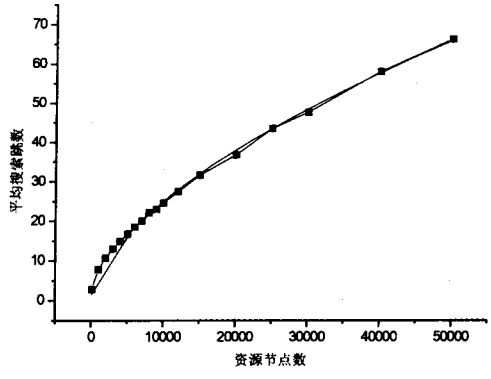

图 4

参 考 文 献

1 Foster I, Kesselman C, et al. The Grid : Blueprint for a New Computing Infrastructure. Morgan2Kaufmann, San Francisco, CA, 1998

2 徐传福，陈海涛，等. 基于 DHT 的层次式 P2P 资源定位模型. 计算机工程与应用，2004，18：156～158

3 李伟，徐志伟，等. 网格环境下一种有效的资源查找方法. 计算机学报，2003，26(11)：1546～1549

4 董方鹏，龚奕利，等. 网格环境中资源发现机制的研究. 计算机研究与发展，2003，40(12)：1749～1755

5 李伟，徐志伟. 一种网格资源空间模型及其应用. 计算机研究与发展，2003，40(12)：1756～1762

6 Rajkumar B. High Performance Cluster Computing. Beijing, Posts & Telecom Press, 2002

7 Foster I, Kesselman C. Globus: a meta- computing infrastructure toolkit[J]. International Journal of Supercomputer Applications, 1997, 11(2): 115～128

(上接第 102 页)

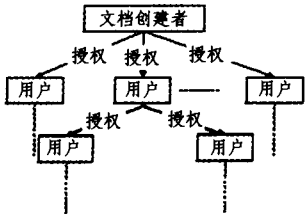

图 5 授权关系树

图 5 表示在一个有 n 个实体元权限的实体上，n 棵授权关系树中的一棵。其它的 $n-1$ 棵授权关系树都与此类似。假设这是实体权限为 x 的授权树，那么有且只有该树上的用户才具有对文档创建者所创建的文档享有 x 操作权限。由于电子文档的元权限只有有限的几种，因此采用这种方法使得授权关系在逻辑上更简明。当对某一用户授予对文档的一种操作权限时，就在该权限树上添加该用户作为授权用户的子结点。当对某一用户削除权限时，必须且只能由其上级结点进行并采用一种级联式削权，即在删除该结点的某项权限之前必须扫描子结点 找出具有该权限的子结点并删除该权限。通过这种递归式扫描一直到叶结点，这样以该结点为起点的子树将被删除，如图 6 所示。

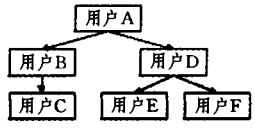

图 6 削权前的授权树

图 6 是从一个授权关系网中分离出来的关于权限 x 的一棵授权关系子树，用户 B,D 的 x 权限只能由用户 A 取消，并且在这棵树上用户 A 也仅能取消其子树的 x 权限(假设用户 B、C 还拥有其它权限)。当用户 A 取消 B 的 x 权限时，用户 C 的 x 权限也会被取消。同理，当用户 A 取消用户 D 的 x 权限时，用户 E 、用户 F 的 x 权限也会被取消 。结果如图 7 所示。

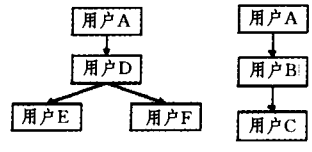

图 7 削权后的授权树

这样通过一个基于授权关系树的 DAC 模型就能灵活地根据政府运作的需要对相关文档进行授权管理跟踪，弥补了 RBAC 的不足。

通过以上对应政府角色的层层授权，结合 PKI 体系进行角色管理，政府信息集成平台中的电子文档可以达到综合安全而高效的管理。

参 考 文 献

1 盛小钢，王克，陈庆荣. 电子公文同样可信——基于 PKI 的电子印章系统的设计与实现. 计算机安全，2004(12)

2 朱靓，叶志坚. 基于 PKI 的交叉认证技术在电子政务中的研究与应用. 福建电脑，2005 (12)