第 32 卷 第 5 期 计 算 机 工 程 2006 年 3 月
Vol.32 № 5 Computer Engineering March 2006
·安全技术· 文章编号：1000—3428(2006)05—0152—03 文献标识码：A 中图分类号：TP309

委托授权在 PMI 体系架构中的研究与应用

张志勇，普杰信
(河南科技大学电信学院，洛阳 471003)

摘 要： PMI 是构建在 PKI 基础上实施特权管理的服务体系，目前普遍采用基于角色的安全架构和基于属性证书的实现机制。该文提出了一种面向 PMI 环境基于角色和权限两级的开放分布式委托授权模型——DM for PMI(Delegation Model for PMI)，并在该模型的基础上引入委托证书，给出了一种扩展的 PMI 体系架构——EPMI(Extension PMI)。EPMI 增强了原有 PMI 中委托授权的语义和机制，解决了开放分布式环境下电子政务与电子商务实际应用中的特权委托问题。

关键词： 特权管理基础设施；开放分布式环境；DM for PMI；委托证书；EPMI

Research and Application of Delegation in PMI System

ZHANG Zhiyong, PU Jiexin
(School of Electronic and Information Engineering, HAUST, Luoyang 471003)

【Abstract】 PMI is a services system implementing authorization management in the basis of PKI, and it popularly adopts role-based security frame and realization mechanism with attribute certificate. The paper introduces a role and permission based delegation model with open and distributed property for PMI, as well as an extended PMI system based on delegation certificate EPMI (extension PMI). EPMI strengthens the semantic and mechanism of delegation, and solves delegation of e-government and e-commerce applications in distributed environment.

【Key words】 Privilege management infrastructure; Open distributed environment; Delegation model for PMI; Delegation certificate; Extended PMI

目前，特权管理基础设施(Privilege Management Infrastructure，PMI)的研究和应用主要集中在采用基于角色的访问控制(RBAC)策略构建集中式授权管理体系结构，以及使用属性证书实现特权的分发和回收等方面，这种传统的授权管理模式不能适应于分布式计算环境下电子政务与电子商务的实施。然而作为特权管理中的必要组成部分和能够实现分布式特性的关键技术——委托授权，又缺少全面深入的研究和具体的应用。PMI 的标准给出了委托的基本特征和一个简单应用模型，并没有较为系统地描述全面特性及其在 PMI 中的应用；文献[1～3]主要阐述了基于角色和属性证书的 PMI 体系框架，关于委托的实现仅限于集中式属性权威机构 AA 的委托授权，特权声称者 PA(Privilege Assertion)本身不具备委托能力，这将不适合于分布式 PMI 应用的创建；文献[4]给出了 RBAC 策略在 PMI 管理和实现中的形式化描述，但也未充分考虑委托特性及其约束规则从而给出它的形式化描述。

与 RBAC 策略相关的基本思想和实现机制已经趋于成熟[6]，基于角色的委托模型(Role-based Delegation Model)是在 RBAC 基础上提出的一种旨在解决分布式计算环境下访问授权管理复杂性问题的思想和安全机制。在 RBDM 研究中，目前具有代表意义的模型主要有 $RBDM_0$ 和 RBDM2000 等[6,7]。它们都不支持权限级粒度的委托授权，而是把角色作为委托授权的基本单位，即只能委托角色及其所具有的全部特权，这违背了 RBAC 策略中的“最小特权原则”，使得用户可能会获得超出自身所需的权限许可，从而造成信息安全的隐患。上述 RBDM 也未曾考虑委托的时效性问题，而这又是实现企业级安全访问控制策略所必需的。

本文将根据委托授权特性提出一种面向 PMI 的两级委托授权模型——DM for PMI，并在该模型的基础上引入委托证书 DC(Delegation Certificate)，阐述它在 EPMI 体系框架中的具体应用。

1 PMI 与委托授权

1.1 PMI

PMI 是建立在 PKI(Public Key Infrastructure)可信任身份鉴别基础上，提供授权访问服务的体系框架。它们二者相结合来完成信息资源的访问控制活动，有效地保障了信息安全的机密性、完整性、可控性和抗否认性，从而成为基于网络电子政务和电子商务应用的安全性基础设施平台。

基于 X.509 属性证书的 PMI 主要是通过属性证书进行系统用户或其他实体的授权管理与访问控制过程。属性证书 AC(Attribute Certificate)不同于 PKI 中的公钥证书 PKC，它是由 AA(Attribute Authority)机构颁发的记录用户特权信息的载体，具有短期的时效性。在 X.509 属性证书的基础上，为提高系统授权管理的效率，增强特权之间的约束机制和灵活地实施面向应用的企业级自定义安全策略，引入了 RBAC 策略和机制。基于角色的 PMI 模型在用户(PA)和特权之间增加了角色实体，在实现时利用角色说明属性证书和角色分配属性证书完成授权管理。

1.2 基于角色的委托授权及其特性

在分布式应用环境下，传统的集中式授权管理加重了安全管理员的负担。这种繁重的授权工作已经不再适应新的环

基金项目： 教育部科技重点基金资助项目(20031016)；河南省自然科学基金资助项目(0311012600)；河南科技大学青年基金资助项目(2003 QN 06)

作者简介： 张志勇(1975—)，男，硕士、讲师，主研方向：信息安全，智能决策支持系统；普杰信，教授

收稿日期： 2005-02-24 **E-mail：** zhangzy@mail.haust.edu.cn

境，为此提出了委托的概念。委托(Delegation)的本质就是用户实体将自己所具有的权限或者角色转授给其他用户，使其可以代表自己的利益行使一定的职责，完成某些任务。例如，在政府、企事业组织中具有一定角色的职员可能因为某种原因暂时离开岗位，或者为了和其他职员协同工作，便可以将自身所具备的一些角色或者权限委托给其他职员，达到权利共享的目的。必要时，他还可以撤销该委托，收回所共享的特权。和委托相关的 3 个实体是：委托者(delegator)，委托的特权(delegated privilege)，受托者(delegatee)。

基于角色委托授权的基本思想是在分布式环境下，用户可以不经过安全管理人员，将自身所具有角色(显式角色)或所继承的角色(隐式角色)委托给其他用户，使他能够代表自己的职责(角色)行使一定的权限。这样便分散了授权管理，增加了分布式系统的灵活性，其中委托授权后所产生的安全性问题可由系统审计来处理。基于角色的委托具有以下主要特征：

(1) 整体角色委托或部分角色委托。前者是指用户可以将自身的角色整体委托给其他用户，从而使其获得该角色所具有的全部权限，而不能只委托该角色的部分权限。这种情况不能满足基本安全策略所要求的“最小特权原则”；部分角色委托可以允许用户将角色中的部分权限委托给另一用户，这样降低了可委托特权的粒度，遵循了最小特权原则，但是会产生大量逻辑意义上不完整的角色，从而又增加了特权管理的复杂性。

(2) 单步委托或多步委托。单步委托是受托者不可以进一步将委托角色或权限再次委托给其他用户；多步委托则允许受托者进一步实施委托，但撤销委托将是复杂和困难的。

委托的逆操作是撤销(Revoke)，它是收回被委托的角色或权限。撤销的主要方式有级联撤销、非级联撤销，独立于授权的撤销，非独立于授权的撤销，系统自动撤销和用户撤销等。

2 面向 PMI 环境的委托模型(DM for PMI)

2.1 DM for PMI 构建与形式化描述

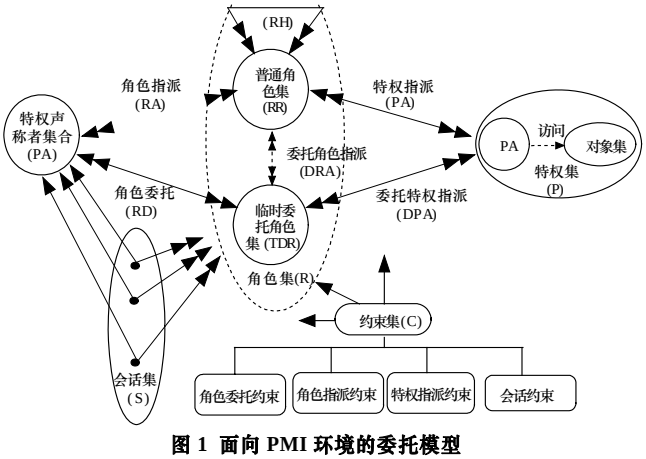

图 1 面向 PMI 环境的委托模型

DM for PMI 在 RBAC 模型的基础上增加了临时委托角色 TDR(Temporary Delegated Role)。系统为特权声称者 PA 的委托授权自动创建 TDR 后，PA 便可以将需要委托的普通角色和权限指派给 TDR，然后将其委托给其他用户实体 PA，从而完成一次委托授权过程。由于 TDR 具有时效性，因此在 DM for PMI 中描述了“TDR 生命周期”，进而丰富了它的语义。DM for PMI 主要由特权声称者、普通角色、委托角色、特权、约束规则和会话等六部分构成，如图 1 所示。

用集合论和谓词逻辑形式化描述该模型如下：

定义特权声称者集合 PA，角色集 R，普通角色集 RR，临时委托角色集 TDR 及其状态集 S，特权集 P，约束集 C，角色委托约束集 DC，会话集 S。

定义 1(临时委托角色) TDR 是普通角色和权限的并集，$TDR=\{r_1,r_2,\ldots r_m,p_1,p_2\ldots p_n \mid r\in RR,p\in P\}$，即 $TDR=RR\cup P$。

定义 2(委托授权) 委托授权关系是一个五元组(PA_1, PA_2,TDR,TL,DC)，其中 PA_1 为委托者，PA_2 为受托者，TL(Limit of Time)为委托时限，DC 是委托约束。该五元组的语义解释为用户实体 PA_1 在满足 DC 的前提下可以将 TDR 委托授权给 PA_2，使得 PA_2 在 TL 内享有 TDR 所有的显式或隐式特权。

定义 3(状态集) TDR 的状态集 S={init,invoke, sleep, expire}，其中 init 为初始态，invoke 为激活态，sleep 为睡眠态，expire 为终止态。

定义 4(委托时限) TDR 具有时效性，委托时限 $TL=\{x \mid x=[\tau_{bi},\tau_{ei}](i=1,2,\ldots,n)\}$，其中 τ_{bi} 为该时段的起始时间，τ_{ei} 为终止时间。

定义 5(状态迁移) TDR 在其生命周期内会发生以下状态转换：假定 ST 为系统时间，$\forall i(i\in N)\ ST\notin [\tau_{bi},\tau_{ei}]\wedge ST<\tau_{b1}\rightarrow S=init$；$\ni i\ (i\in N)ST\in [\tau_{bi},\tau_{ei}]\rightarrow S=invoke$；$\forall i(i\in N)ST\notin [\tau_{bi},\tau_{ei}]\wedge (ST>\tau_{b1})\wedge (ST<\tau_{en})\rightarrow S=sleep$；$\forall i(i\in N)ST\notin [\tau_{bi},\tau_{ei}]\wedge ST>\tau_{en}\rightarrow S=expire$。

2.2 DM for PMI 委托约束规则及相关性质

普通基于角色 PMI 授权的实施者为 AA 机构，授权管理相对集中；而在分布式环境下委托授权的实施者可以是系统中所有的 PA，委托操作比较分散。因此实施委托约束有利于加强委托管理，以防止某些 PA 有意或无意地进行非法授权。委托约束规则主要包括非委托角色和权限、委托冲突角色和权限、委托步和委托基数约束等。它们将构成实际电子政务与电子商务活动中具体的委托授权策略。

定义 6(非委托角色和权限集) 非委托角色和权限集 $NDRP=\{r_1,r_2,\ldots,r_i,p_1,p_2,\ldots,p_j\}$。

约束规则 1 非委托角色和权限集中的元素不能进行委托。

$\forall x(x\in NDRP)\rightarrow(x\notin TDR)$

定义 7(委托冲突) 如果角色 r_i 和 r_j 不能同时委托给其他 PA，则称二者为委托冲突角色，记为 $collr(r_i, r_j)$；如果许可 p_m 和 p_n 不能同时委托给其他 PA，则称二者为委托冲突权限，记为 $collp(p_m, p_n)$。

约束规则 2 临时委托角色集中任意两个角色或权限都不能存在委托冲突。

$\forall r_i,\ r_j,\ p_m,p_n(r_i\in TDR,\ r_j\in TDR,p_m\in TDR,p_n\in TDR)$ $collr(r_i, r_j)\vee collp(p_m, p_n)=F$

定义 8(委托步和委托基数) 委托步 d 为自然数，表示角色 r_i 或权限 p_j 可以级联委托的次数。当 d=1 时，称为单步委托；当 d>1 时，称为多步委托。委托基数 n 为自然数，表示角色 r_i 或权限 p_j 可以委托的用户数。

约束规则 3 TDR 的委托步和委托基数取决于 TDR 集中所有角色和权限的委托步或委托基数的最小值。

$\forall r_i, p_m (r_i\in TDR, p_m\in TDR)\ d_{TDR}<d_{ri}\wedge d_{TDR}<d_{pm}$

$\forall r_i, p_m (r_i\in TDR, p_m\in TDR)\ n_{TDR}<n_{ri}\wedge n_{TDR}<n_{pm}$

性质 1(委托授权前提) 具有委托授权关系的 PA 之间应同属于某一个上层 AA 机构。

性质 2(多步委托) PA 间 TDR 的多步委托关系是一种偏序关系，满足自反性、反对称性和传递性。

性质 3(级联委托撤销) 当原始 PA 强制收回委托授权或 TL 结束时，经 PA 多步委托出去的 TDR 被级联收回。

性质 4(依赖委托撤销) 只有原始委托者可以撤销委托授权，具有相同角色的其他 PA 都无权收回委托。

最小特权原则、责任分离原则和数据抽象原则是实现企业级访问控制的基本安全策略，也是提供安全服务的首要原则。约束规则 1 增强了应用系统中对委托授权的控制，满足了“最小特权原则”；约束规则 2 解决了企业级委托授权的冲突问题，实现了“责任分离原则”。特权集中的任意权限既可以为普通读、写、执行等，也可以是企业级抽象的许可权限，如现金出纳、账目审计等，从而达到“数据抽象原则”。

3.DM for PMI 在 PMI 中的应用

3.1 扩展的 PMI 体系架构(EPMI)

传统 PMI 体系中的委托授权者是 SOA 或各级 AA，SOA 具有最高和最广泛的权限，各级 AA 只具备由上一级 AA 授予的局部权限，它们可以将所属的特权或特权子集委托给实体 PA。这种委托过程属于集中式特权管理，PA 不具有委托能力。因此在大型分布式应用环境下，由于大量实体的存在，委托授权只能集中在 AA 机构，将给其带来繁重的管理工作，并且在委托验证时需要 AA 逐级向上回溯至 SOA，这又增加了委托验证的时间复杂度。

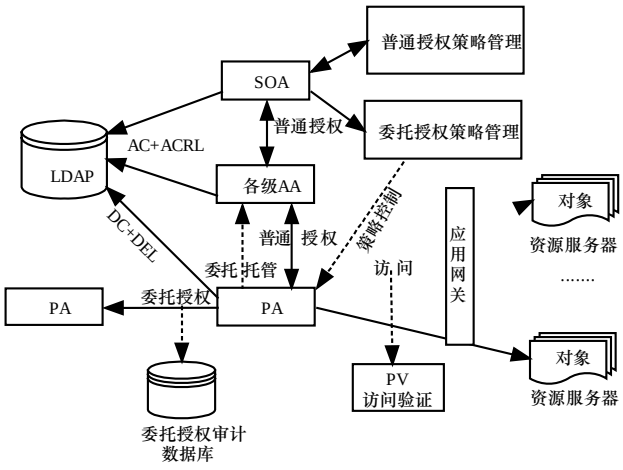

图 2 .EPMI 体系架构

DM for PMI 是面向 PMI 具有分布式特征的委托模型，在它的基础上扩展原有的 PMI 体系架构，引入委托证书、委托失效列表、委托审计等组件构成了 EPMI，使其具有分布式委托特性。鉴于委托授权的短期时效性，不将委托信息写入属性证书，而是构建 DC 发放给受托者。除了 SOA，AA 具有委托特权外，终端实体 PA 也具备委托能力。PA 可以在遵循 SOA 制定的委托策略前提下，通过终端系统生成的 DC 直接(或者间接由 AA 机构托管)将显式或隐式角色以及权限委托给受托者 PA。当 PA 需要撤销委托或委托时限到达时，PA(或系统)将在委托失效列表 DEL(Delegation Expire List)中添加 DC 的唯一标识，进而 DC 作废，同时多步委托特权也被具有依赖性的级联撤销。

鉴于分布式委托的分散性，为保证 PA 委托的安全和合法，在 EPMI 中引入委托审计机制。系统对 PA 每一次委托授权和撤销过程进行跟踪监视，将审计信息存储在审计数据库中，以便将来进行安全检测。EPMI 体系架构如图 2 所示。

3.2 EPMI 委托授权过程

完整的委托授权与撤销会话过程可分为以下 6 个步骤：

(1)PA 收到委托请求后，首先判断请求是否来自同一上层 AA 机构所属的 PA，如果不是，则拒绝委托请求；否则，接受委托请求，开始一次委托会话过程。此外，PA 也可以自愿委托所属特权；

(2)终端系统生成委托证书 DC，并自动产生对于整个访问域有效的唯一标识 DC_ID。PA 在 DC 上填写其他相关信息，如受托者唯一标识，名称，临时委托角色 TDR，DC 生效时间，DC 失效时间，DC 生命周期，是否可以多步委托等；

(3)PA 将填写好的 DC 经过数字签名后通过终端系统或者由 AA 代理发放给受托者，同时也将 DC 的一个副本提交给所属 AA 机构的 LDAP(Lightweight Directory Access Protocol)备份，以便 PV(Privilege Validate)进行访问控制；

(4)委托者可以随时终止委托权限，PA 直接在 DEL 中发布委托撤销证书的 DC_ID；否则，AA 将根据备份 DC 的失效时间自动将失效的 DC_ID 添加在 DEL 中；

(5)委托授权(包括多步)与撤销(包括级联)过程由 EPMI 委托审计系统跟踪监视，相关信息存储在审计数据库中；

(6)委托授权(撤销)会话过程结束。

4 结束语

本文根据委托特性所给出的 DM for PMI，既弥补了原有委托模型不支持权限级委托授权的缺陷，又保持了角色级委托授权管理中高效、灵活的特点，是一种在分布式应用环境下解决委托问题较为完备的模型。该模型在 PMI 体系架构中的应用，完善了 PMI 特权管理的功能，解决了分布式电子政务与电子商务实际应用中的安全性问题。DM for PMI 委托授权的上下文约束问题及其在 EPMI 中的应用，需要做进一步的研究工作。

参考文献

1 Linn J, Nystrom M. Attribute Certification: An Enabling Technology for Delegation and Role-based Controls in Distributed Environments[C]. RBAC 99’,VA, USA, 1999: 121-130.

2 Chadwick D W, Otenko O. The PERMIS X.509 Role Based Privilege Management Infrastructure[C]. ACMAT, Monterey, California, USA, 2002.

3 许长枫, 刘爱江, 何大可. 基于属性证书的 PMI 及其在电子政务安全建设中的应用[J]. 计算机应用研究, 2004,21(1): 119-122.

4 安晓江, 李大兴. PMI 系统中 RBAC 策略的实现与管理[J]. 计算机工程与应用, 2004,40(7): 115-117, 132.

5 张志勇. 基于角色的访问控制及其面向对象的建模[J]. 计算机工程与设计, 2004, 25(8): 1367-1369,1374.

6 Barka E, Sandhu R. A Role-based Delegation Model and Some Extensions[C]. The 16th Annual Computer, Sheraton, New Orleans, 2000.

7 Na SangYeob, Cheon SuhHyun. Role Delegation in Role-based Access Control[C]. ACM RBAC2000, 2000.