PMI 技术白皮书

技术白皮书

总部：中国·长春前进大街 2266 号
：86-0431-5173333 ：86-0431-5172696

吉大正元信息技术股份

名目

产品相应技术

PMI 概览

运算机网络能有效地实现资源共享，但资源共享和信息安全是一对矛盾体。随着资源共享的进一步加强，随之而来的信息安全问题也日益突出，而身份认证，权限和访问操纵又是网络应用安全的两个重要内容，因此它们也成为了当前信息安全领域中的研究热点。许多应用系统都需要分别在这两个方面采取了相应的安全措施。

然而，对一些大型的组织机构来说，其网络结构比较复杂，应用系统比较多，假如分别对不同的应用系统采纳不同的安全策略，那么治理将变得越来越复杂，甚至难以操纵。不同的用户对应不同的应用系统，由于机构的网络结构比较复杂，应用系统和用户差不多上分散分布的，因此对用户的访问操纵和权限治理就显得专门的复杂和凌乱。而机构必须要能够操纵：有“谁”能够访问机构的信息，用户访问的是“什么信息”，哪个用户被授予什么样的“权限”。一旦机构确定了权限治理和公布的方式，访问操纵系统就能够依照机构发放的权限以及定义的安全策略操纵用户访问，爱护应用系统。然而，过去在权限生命周期治理，权限的表达和权限治理方式方面没有更成熟更有用的成果，权限治理方案进展相对滞后。

相反，访问操纵，或者说授权服务，差不多十分成熟，在过去的研究和应用中差不多获得了专门多的成果，建立了我们目前要紧使用的 DAC，ACL，MAC，RBAC 访问操纵模型，其中 ACL 和 MAC 得到了最普遍的应用。目前，RBAC 模型也差不多比较成熟，支持了最新的应用。

传统的应用系统通常是通过使用用户名和口令的方式来实现对用户的访问操纵的，而对权限的操纵是每个应用系统分别进行的，不同的应用系统分别针对爱护的资源进行权限的治理和操纵，这种方式存在一些缺点。同时，又因为不同系统的设计和实施策略不同，导致了同一机构内存在多种权限治理的现状。目前，缺乏有效的权限治理带来了以下问题：

- 权限治理纷乱

  对一个机构而言，数据和人力资源差不多上统一的。然而由于系统设计的缘故，可能同时对相同的人员采纳不同的治理方式，对机构内的共享数据采纳了不同的权限分配策略，这明显不合理，也不利于对机构资源的治理。

- 带来系统的不安全因素

  不同的权限治理策略产生的安全强度是不同的。这就可能造成机构信息安全治理的漏洞，因此入侵者就有可能瞄准那些权限治理相对不安全的系统进行集中攻击，这就给机构资源的安全性带来极大的危害。

- 权限治理依靠于访问操纵应用

  权限的给予和撤销往往差不多上在访问操纵应用中产生的，不同的访问操纵应用之间尽管有相同的用户和授权策略却往往不能互相使用对方产生的权限。每个应用都要爱护自己的用户信息和授权方法，权限无法在分布的应用中和远程应用中使用。

- 资源所有者没有权限

  应用系统负责权限的发放和使用，造成权限真正的拥有者不能有效，及时的更换，公布实时的权限信息。比如机构内一个人职务或业务的变化必须通知相关的不同应用中进行更新。而从本质上讲，权限的发放和权限的鉴别使用是完全不同的两个过程，完全能够分开，权限的拥有者发放权限，而由资源的爱护者验证权限。

- 增加了系统治理员的负担

  由于不同的系统采纳的是不同的权限治理策略，系统治理员不得不熟悉和操作不同的权限治理模式，这无疑增加了系统治理员的负担。另外，大多数老系统都采纳的是权限访问操纵列表的方式，然而关于大型复杂应用用这种方式来分配权限，给系统治理员带来庞大负担且易出错。

- 开发复杂费用高

  设计一个新的安全应用系统时，权限治理是一个极其重要的部分。在缺乏统一权限治理模型的情形下，设计人员要考虑选择权限治理模型、访问操纵授权方案，而且开发人员也要依照不同的应用花费较大代价来实现权限治理功能，为一个应用开发的治理往往无法在其它应用中重用，增大系统的费用。

在过去的五年中，权限治理作为安全的一个领域得到快速进展，也提出了几种权限治理方案，如 Kerberos，基于策略服务器方案，但目前应用和研究的热点集中于基于 PKI 的 PMI 研究。在 PKI 得到较大规模应用以后，人们差不多认识到需要超越当前 PKI 提供的身份验证和隐秘性，步入授权领域，提供信息环境的权限治理将成为下一个要紧目标。PMI 实际提出了一个新的信息爱护基础设施，能够系统地建立起对认可用户的授权。建立在 PKI 基础上的 PMI，对权限治理进行了系统的定义和描述，差不多将权限治理研究推到了应用前沿。

关于权限治理和访问操纵差不多有了专门多相关的标准。

1995 年，公布了访问操纵的标准框架〔ISO/IEC 10181-3|ITU-T Rec. X.812〕，它要紧定义了访问操纵的差不多概念，定义了通用的访问控降服务和机制，定义了访问控降服务和机制的协议功能需求，定义了访问操纵的治理需求，阐明了访问控降服务和机制与其他安全服务和机制的相互作用关系。

在 1997 年 X.509〔V3〕中定义了差不多的属性证书语法〔属性证书第 1 版本〕，在 2000 年公布的 X.509〔V4〕中定义了 PMI 的框架结构，其中定义了扩展属性证书的语法〔第 2 版〕，定义了 PMI 模型，规定了托付路径处理，定义了标准 PMI 扩展集，并增加了名目服务对象定义。

2000 年 OpenGroup 提出了授权 API〔AZNAPI〕，定义了标准应用编程接口，用来实现访问操纵体系结构符合 ISO/IEC 10181-3|ITU-T Rec. X.812 规定的系统。

2000 年 NIST〔National Institute of Standards and Technology〕公布了基于角色的访问操纵建议标准，定义了 RBAC〔Role—Based Access Control〕的参考模型。

关于 PMI 的标准正在制定当中，IETF 正在进行的 PERMIS〔PrivilEge and Role Management Infrastructure Standards Validation，权限和角色治理基础设施标准验证〕项目将在 2002 年 9 月 31 日终止，并打算推出 PERMISAPI 的标准和相关的 RFC。RSA 已提出了 IETF 草案« An Internet Attribute Certificate Profile for Authorization»〔draft-ietf-pkix-ac509prof〕

国外差不多有了 PMI 相关的产品，如

- Entrust: Secure Control
- Baltimore Technology: Attribute Certificate ServerIBM: Secureway
- DASCOM (now IBM): aznAPI code 国内对 PMI 的研究差不多开始，也差不多有类似的产品显现，然而还没有应用实例。

从总体上看，PMI 的理论是完全成熟的，目前在相关应用支撑技术方面差不多具备，专门快将有相应的标准公布，产品应用差不多提到日程上来。

权限治理基础设施

PMI 的定义

ITU〔International Telecomunications Union〕& IETF〔Internet Engineering Task Force〕使用属性证书实现了 PMI。

Privilege Management Infrastructure (PMI) 即权限治理基础设施或授权治理基础设施，是属性证书、属性权威、属性证书库等部件的集合体，用来实现权限和证书的产生、治理、储备、分发和撤销等功能。

Attribute Authority (AA) 即属性权威，用来生成并签发属性证书〔Attribute Certificate，即 AC〕的机构。它负责治理属性证书的整个生命周期。

Attribute Certificate (AC) 即属性证书，关于一个实体的权限的绑定是由一个被数字签名了的数据结构来提供的，这种数据结构称为属性证书, 由属性权威签发并治理，它包括一个展开机制和一系列专门的证书扩展机制。下面我们称身份证书为 PKC〔Public Key Certificate〕。

X.509 定义的属性证书框架提供了一个构建权限治理基础设施〔PMI〕的基础，这些结构支持访问操纵等应用。属性证书的使用〔由 AA 签发的〕提供一个灵活的权限治理基础设施〔PMI〕。

关于一个实体的权限约束由属性证书权威〔已被数字签名的数据结构〕或者由公钥证书权威〔包含已明确定义权限约束扩展的〕提供。

PMI 实际提出了一个新的信息爱护基础设施，能够与 PKI 和名目服务紧密地集成，并系统地建立起对认可用户的特定授权，对权限治理进行了系统的定义和描述，完整地提供了授权服务所需过程。

建立在 PKI 基础上的 PMI，以向用户和应用程序提供权限治理和授权服务为目标，要紧负责向业务应用系统提供与应用相关的授权服务治理,提供用户身份到应用授权的映射功能，实现与实际应用处理模式相对应的、与具体应用系统开发和治理无关的访问操纵机制，极大地简化应用中访问操纵和权限治理系统的开发与爱护，并减少治理成本和复杂性。

什么缘故不是 PKI

既然 PMI 建立在 PKI 的基础之上，什么缘故不直截了当基于 PKI 进行权限治理和访问操纵呢？

Public Key Infrastructure〔PKI〕，即公布密钥基础设施，按照 X.509 标准中定义，"是一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和证书的产生、治理、储备、分发和撤销等功能。"

应用 PKI 的目的是治理密钥并通过公钥算法实现用户身份验证。但在实际访问操纵应用中，存在一些问题: 如，用户数目专门大时，通过身份验证仅能够确定用户身份，但却不能区分出每个人的用户权限。这确实是 PKI 新扩展产生的一个缘故。

另外，访问操纵和授权专门复杂。比如说，在一个机构相关范畴内，往往包含多种角色，每个角色担负不同的职责和业务，每个人员又能够承担多个角色〔企业内，领导，技术人员，治理人员，销售，伙伴，客户〕；要爱护的内容也是不同的，如数据库，网页，文件…；治

理规定可能多种多样，如分支机构定义的规那么不能违反高一级机构的规那么；访问操纵

策略也是及其复杂的，同样的一个角色，在不同的系统中具有的权限往往是不同的，部门内的策略不能和机构的策略冲突；安全应用系统的环境也千差万别，等等。

而且，权限信息相关于身份信息来说容易改变，爱护授权信息代价相对爱护身份信息要高的多。

在 PKI 得到较大规模应用以后，人们差不多认识到需要超越当前 PKI 提供的身份验证和隐秘性，步入授权验证的领域，提供信息环境的权限治理将成为下一个要紧目标。因此，ITU 和 IETF 进行了 PKI 的扩展,承诺该基础设施支持和处理授权。

PKI 和 PMI 的关系

PKI 和 PMI 之间的要紧区别在于：PMI 要紧进行授权治理，证明那个用户有什么权限，能干什么，即〝你能做什么〞；PKI 要紧进行身份鉴别，证明用户身份，即〝你是谁〞。它们之间的关系类似于护照和签证的关系。护照是身份证明，唯独标识个人信息，只有持有护照才能证明你是一个合法的人。签证具有属性类别，持有哪一类别的签证才能在该国家进行哪一类的活动。

由于 X.509 中定义，关于一个实体的权限约束由属性证书权威〔已被数字签名的数据结构〕或者由公钥证书权威〔包含已明确定义权限约束扩展的〕提供。授权信息能够放在身份证书扩展项中〔subjectDirectoryAttribute〕或者属性证书中，然而将授权信息放在身份证书中是专门不方便的。第一，授权信息和公钥实体的生存期往往不同，授权信息放在身份证书扩展项中导致的结果是缩短了身份证书的生存期,而身份证书的申请审核签发是代价较高的;其次，对授权信息来说，身份证书的签发者通常不具有权威性，这就导致身份证书的签发者必须使用额外的步骤从权威源获得授权信息。另外，由于授权公布要比身份公布频繁的多，关于同一个实体可由不同的属性权威来颁发一属性证书，给予不同的权限。因此，一样使用属性证书来容纳授权信息，PMI 可由 PKI 建筑出来同时可独立的执行治理操作。然而两者之间还存在着联系，即 PKI 可用于认证属性证书中的实体和所有者身份，并鉴别属性证书签发权威 AA 的身份。

Concept	*PKI Entity*	*PMI Entity*
Certificate	*Public Key Certificate*	*Attribute ertificate*
Certificate issuer	*Certification Authority*	*Attribute Authority*
Certificate user	*Subject*	*Holder*
Certificate binding	*Subject's name to public key*	*Holder's name to privilege attribute(s)*
Revocation	*Certificate revocation list (CRL)*	*Attribute certificate revocation list(ACRL)*
Root of trust	*Root certification authority or trust anchor*	*Source of authority(SOA)*
Subordinate authority	*Subordinate certification authority*	*Attribute authority*

PMI 和 PKI 有专门多相似的概念。如属性证书〔Attribute Certificate ，AC〕与公钥证书〔PKC〕，属性权威〔Attribute Authority ，AA〕与认证权威〔CA〕。

公钥证书是对用户名称和他/她的公钥进行绑定，而属性证书是将用户名称与一个或更多的权限属性进行绑定。在那个方面，公钥证书可被看为专门的属性证书。

数字签名公钥证书的实体被称为 CA，签名属性证书的实体被称为 AA。

PKI 信任源有时被称为根 CA，而 PMI 信任源被称为 SOA。

CA 能够有它们信任的次级 CA，次级 CA 能够代理鉴别和认证，SOA 能够将它们的权益授给次级 AA。

假如用户需要废止他/她的签字密钥，那么 CA 将签发证书撤销列表。与之类似，假如用户需要废止授权承诺〔Authorization Permissions〕，AA 将签发一个属性证书撤消列表〔ACRL〕。

属性权威

Attribute Authority (AA) 即属性权威，用来生成并签发属性证书〔Attribute Certificate，即 AC〕的机构。它负责治理属性证书的整个生命周期。

AA 和 CA 在逻辑上是完全独立的。〝身份〞的创建和爱护能〔应该〕与 PMI 分离开来。因此完整的 PKI，包括 CA，可能在 PMI 建立之前存在同时可选用。尽管 CA 是域身份权威的源，然而它不是自动的权限权威源。因此，CA 本身并不必是 AA。

在实际应用 PMI 系统构建安全应用时，属性权威 AA 能力和应用方式能够依照具体的建设要求和成本灵活的决定。

例如在一个较小的应用中，系统的使用人员和资源较少，能够采纳嵌入式的属性权威 AA 签发和治理属性证书，减少建设成本和治理开销。而在一个由多个应用组成的较大的系统中，存在着大量的用户和资源，并对系统有整体的安全需求，这时能够考虑建立属性权威中心，简称 AA 中心，将所有的应用纳入到同一个安全域下，由 PMI 的整体安全策略和授权策略实现整个系统范畴内的所有应用的整体安全访问。如此，一方面能够减少属性权威 AA 的重复性投来资操纵成本，另外一方面能够通过较为集中的治理模式减少治理复杂性和开销，并带来更好的全局安全性。

一个属性权威 AA 的差不多组成如以下图所示：

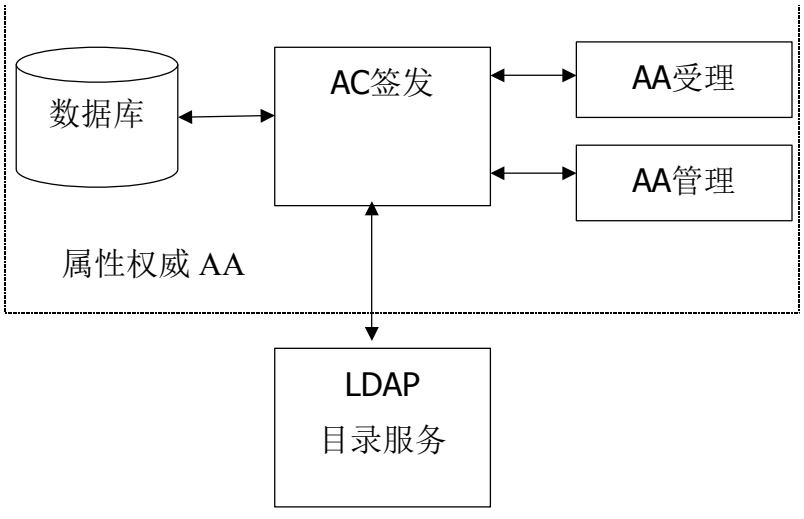

图　　属性权威 AA 的结构图示

要紧包括 AC 签发，受理和治理，数据库服务器、名目

服务器，其中数据库服务器不是必须的。

1）AC 签发服务

AC 签发服务是属性权威 AA 的主体，是以 PKI 技术为基础，以授权服务为要紧任务的服务模块，用于签发属性证书，该服务能够是独立的一台服务器提供，也能够是证书签发模块。

2）AA 受理

要紧用于同意并验证对属性证书的要求，处理该要求，并提供基于属性证书的授权服务、基于属性证书的托付服务等。

3）AA 治理

用于治理属性权威 AA

4）数据库

要紧是用于储备用户和资源的差不多信息，也能够将这些信息直截了当放入 LDAP 名目服务器。

5）LDAP 名目服务器

要紧用于公布 PMI 用户的属性证书以及属性证书的撤消列表 ACRL〔Attribute Certificate Revocation List〕，以供查询使用。该服务器能够直截了当存放用户和资源信息，如此能够不使用数据库存放这些信息。

需要专门说明的是，各业务应用系统在建设属性权威 AA 时，要依照系统内用户的数量，治理的模式确定 AA 属性权威、LDAP 服务器的服务能力，并相应地确定与现状相适应的服务能力冗余备份和性能扩展方案，以确保整个 PMI 服务能力具有连续性和良好的业务量适应能力。

在接下来 4 节中我们将按照如下方式讨论 PMI 权限治理和访问操纵系统框架。第一，讨论基于属性证书的权限治理，了解权限的生命周期是如何通过属性证书来治理的；其次，介绍访问操纵框架，了解访问操纵的抽象模型和证书在其中的作用；接着，介绍策略在不同应用中的作用和组成；最后，讨论如何基于 PMI 构建安全应用系统。

权限治理

PMI 使用属性证书表示和容纳权限信息，对权限生命周期的治理是通过治理证书的生命周期实现的。属性证书的申请，签发，注销，验证流程对应着权限的申请，发放，撤消，使用验证的过程。而且，使用属性证书进行权限治理方式使得权限的治理不必依靠某个具体的应用，而且利于权限的分布式应用。

属性证书的特点

PKC 将一个标识和公钥绑定，AC 将一个标识和一个角色，权限，或者属性绑定〔通过数字签名〕；和 PKC 一样，AC 能被分发和储备或缓存在非安全的分布式环境中；不可伪造，防窜改。同时，属性证书具有以下特点

- 分立的发行机构

由于把属性信息从身份信息中分离出来，同时彼此又分别放置在各自证书中，如此发放过程变的合理而且有针对性。通过一个法定的集中权威机构，来发放身份证书；另外通过一个局域的、熟知用户属性的组织来发放属性证书。一个人能够拥有好几个属性证书，但每一个都会与唯独的身份证书关联，几个属性证书能够来自不同的机构。

■ 储备介质

属性证书能够分发给用户，由用户储备在磁盘上或者 USBKEY 上，或者托付给系统进行统一储备和治理而不必分发给用户。在用户持有属性证书的情形下，为了应用属性证书进行访问操纵，必须建立相应的协议来使用属性证书，同时要求用户选择与具体应用对应的属性证书，当用户权限改变时更新自己的属性证书。由系统托管属性证书时，应用系统依照用户的身份直截了当从属性库中获得用户相应的属性证书，不需要建立相应的协议，属性证书的使用和变更对用户是透亮的。由于权限的生存期通常比较短，相对来说属性证书的更新是频繁的。例如，在用户治理属性证书的情形下，当用户的权限增加时，假如用户没有及时更新证书，系统就会拒绝访问，尽管用户确实具有该权限。而在托付治理模式下，用户的权限增加赶忙就会得到认可。因此，由用户自己治理属性证书往往不如由系统托管方便。

■ 本地发放，

在一个本地发放属性证书的系统中，用于治理证书的架构能够专门简单。当证书发放者和应用系统同处在一个环境中，安全措施和证书发放手续能够极大简化。另外，本地发放的属性证书，能够被系统外安全应用系统使用，不管该持有属性证书的用户是处于本地依旧远程。

■ 基于属性，而不是基于身份进行访问操纵

应用属性证书的最大好处是，在存取操纵方面不再基于用户身份，取而代之的是基于其拥有属性来决定其对某一资源或服务是否拥有访问权。这带来各方面的好处：

应用程序中访问操纵规那么能够简单地被定义成按属性的有效期来决定访问权。这专门简单、容易明白得，同时更易爱护。

同时，这是一个可伸缩的方案，能够支持大量的用户，但又不用对应用程序作任何改变〔假定所有用户都能够被定义成同样的一套属性集合〕。

假如使用传统的基于用户访问操纵机制，每增加一个新用户，都要求在每个应用程序的 ACLs(Access Control List)中。此举导致的必定结果是要么 ACLs 在各处分布，要么产生一个集中式的大型 ACLs，所有应用程序必须联机访问。从治理角度来说两者差不多上十分困难的。假如迁移到基于角色的访问操纵，能够幸免以上操作带来的实施和治理复杂性。

■ 短时效

属性证书能够设置成短时效的，假如属性证书被设定成短时效的。发放必须是一个轻载过程。也确实是说，属性证书的发放必须简单，甚至自动化，因为那个过程须经常重复。而且本地操作要好于远程、集中的治理。

撤回证书变得毫无必要，因为有效期过短，被暴露的属性证书专门快会失效。

■ 属性证书与身份证书的相互关联

属性证书不能单独使用，而且必须支持某种形式的身份认证过程。这种身份证书与属性证书的关联检查是至关重要的，因为那个过程建立起一种信任传递，能够防止一个人的属性被另外的人假冒使用。

PMI 模型

绝大多数的访问操纵应用都能抽象成一样的权限治理模型，包括 3 个实体：对象，权限声称者〔privilege asserter〕和权限验证者(privilege verifier)。

■ 对象能够是被爱护的资源，例如在一个访问操纵应用中，受爱护资源确实是对象。

■