# 基于SAML和PMI的授权管理模型

杨宏宇[1],孙宇超[2],姜德全[3]

(1.中国民航大学 计算机学院,天津 300300;2.中国民航大学 空中交通管理学院,天津 300300;3.中国国际航空股份有限公司 信息管理部,北京 100621)

**摘 要**:针对跨应用系统交互过程中存在的安全认证问题,提出了一种基于安全断言标记语言(SAML)和授权管理基础设施(PMI)的授权管理模型。该模型运用逻辑分离和应用结合的方法实现用户权限管理和授权访问。在PMI的基础上运用SAML断言、SAML协议和SAML绑定技术实现身份验证、属性获取和授权决策,通过属性权威机构(AA)和目录服务器(LDAP)实现对证书的管理。实验结果表明,该模型能有效实现对多角色用户的跨应用系统安全访问控制。

**关键词**:计算机应用;授权管理;身份验证;安全断言标记语言;授权管理基础设施

**中图分类号**:TP393.08;TP309.2 **文献标识码**:A **文章编号**:1671-5497(2009)05-1321-05

## Authorization management model based on SAML and PMI

YANG Hong-yu[1], SUN Yu-chao[2], JIANG De-quan[3]

(1. *School of Computer Science, Civil Aviation University of China, Tianjin* 300300, *China*; 2. *School of Air Traffic Management, Civil Aviation University of China, Tianjin* 300300, *China*; 3. *Department of Information Management, Air China Ltd., Beijing* 100621, *China*)

**Abstract**: During message exchange in across-application there is risk of security certificate. An authorization management model based on Security Assertion Markup Language (SAML) and Privilege Management Infrastructure (PMI) is presented in this paper. The model implements authority management and grants access through combination of logic separation and application. It uses SAML assertion, SAML protocol and SAML binding technologies to conduct identification, attribute acquisition and grant decision based on PMI. This model attains the ability of certificate management by the Attribute Authority (AA) and the Light-weight Directory Access Protocol (LDAP). Experiment results demonstrate that the model is competent for across-application security access control of multi-role users.

**Key words**: computer application; authorization management; identification; security assertion markup language(SAML); privilege management infrastructure(PMI)

目前,我国民航面向公众及全行业单位与部门间的数据交换共享及信息服务仍不适应民航事业的快速发展,主要体现在:目前民航网络结构比较复杂,应用系统比较多;不同的应用系统都采用

**收稿日期**:2007-12-25.

**基金项目**:国家自然科学基金项目(60776807);"863"国家高技术研究发展计划项目(2006AA12A106).

**作者简介**:杨宏宇(1969-),男,教授,博士.研究方向:网络与信息安全,民航信息系统分析与设计.

E-mail:yhyxlx@hotmail.com

不同的安全技术和安全策略;不同的用户对应不同的应用系统,原有应用系统和用户都是分散独立的。由于以上问题,在实现各应用系统之间数据交换共享时,对用户的授权管理和访问控制就显得非常复杂和凌乱。

解决这类问题的方案之一是采用一种标准的安全数据表示形式,无论应用程序的安全服务使用何种安全策略或技术,都可以识别安全数据。这就是结构化信息标准推进组织(OASIS)发布安全断言标记语言(SAML)规范所要达到的目标,SAML是一种规范,其核心是定义了表示身份验证、属性和授权信息的一种标准方法,它可以用作在应用程序之间传递安全上下文的通用解决方案的一部分,在分布式环境中,各种不同的应用程序都可以使用这些身份验证、属性和授权信息。所有遵守SAML规范的安全服务,都可以解释从一个安全服务发送到另一个安全服务的安全数据[1-2]。授权管理基础设施(PMI)建立在PKI基础上,它以向用户和应用程序提供权限管理和授权服务为目标,主要负责向业务应用系统提供与应用相关的授权服务管理,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管理无关的访问控制机制[3]。

本文在SAML标准规范以及PMI基础设施的基础上,设计了一种基于SAML和PMI的应用系统授权管理模型,给出了相应的实现过程和实现方法。

## 1 安全断言标记语言和授权管理基础设施

### 1.1 安全断言标记语言(SAML)

SAML是一种基于XML的安全性标准,用于在Internet不同安全域中交换身份验证和授权凭证。SAML规范主要由SAML断言、SAML协议、SAML绑定组成。SAML断言描述的是域间传送的各实体的安全信息,包括身份验证断言、属性断言、授权断言。SAML协议定义了基于XML的请求/响应消息格式,用以在交互的多方之间传送SAML断言。SAML请求/响应协议可以与当前的多种标准的传输协议或消息交换协议绑定,这种绑定方法使SAML具有良好的开放性和可扩展性[1,4-5]。本文利用这些协议原有的安全机制实现了SAML协议传输的安全性。SAML协议在用户和安全机构之间的传输过程如图1所示。SAML提供了一种标准的格式对身份证明进行XML编码,具备了跨平台的交互能力[6]。

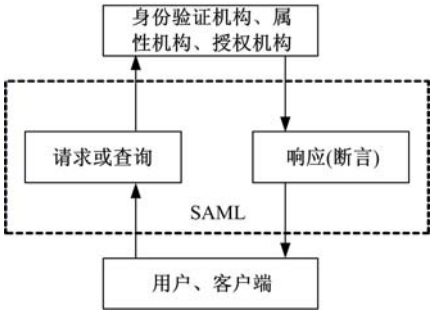


**图1 SAML断言与协议关系图**

**Fig. 1 Relationship of SAML assertion and protocol**

### 1.2 授权管理基础设施(PMI)

X.509(v4)定义的PMI模型能够与PKI和目录服务紧密地集成,对认可用户进行特定授权,对权限管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[3]。PMI主要由属性证书AC(Attribute certificate)、属性权威AA(Attribute authority)、属性证书库CR(Certificate repository)等部件组成,用于实现权限和证书的产生、管理、存储、分发和撤销等功能。AA是生成并签发AC的机构,它负责AC整个生命周期的管理。AC包含了一个实体的权限信息,实际上它是一个被数字签名的数据结构,由AA签发并管理,并包括一个展开机制和一系列证书扩展机制。

一个AA的基本组成如图2所示。主要包括AC签发、AA受理和管理,数据库服务器、LDAP目录服务器[3,7]。

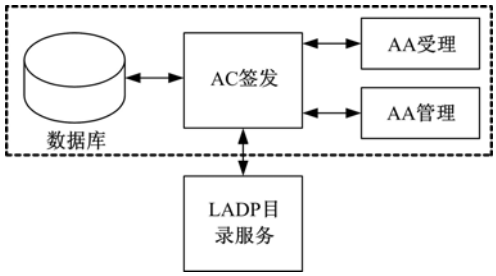


**图2 AA结构图**

**Fig. 2 Structure of AA**

AC签发服务是AA的主体,它是以PKI技术为基础、以授权服务为主要任务的服务模块,用于签发AC,该服务可以是独立的一台服务器提供,也可以是证书签发模块。

AA受理主要用于接受并验证对AC的请

求，以及对请求的处理，并提供基于 AC 的授权服务、基于 AC 的委托服务等。

数据库服务器主要是用于存储用户和资源的基本信息，也可以将这些信息直接放入 LDAP 目录服务器。LDAP 目录服务器主要用于发布供查询使用的 PMI 用户的 AC 以及 AC 撤消列表 ACRL（Attribute certificate revocation list）。该服务器可以直接存放用户和资源信息，不必用专门的数据库服务器存放上述信息，从而简化了操作。

## 2　授权管理模型的设计与实现

### 2.1　模型设计

本文提出的基于 SAML 和 PMI 的授权管理模型可以将权限管理和授权访问实现逻辑上的分离和应用上的结合。AC 的签发、维护和撤消完全由 AA 进行控制，并以 LDAP 目录服务器形式进行存储，系统的访问控制部分只需要跟 LDAP 进行交互就可以实现属性的读取，从而实现 SAML 与 PMI 的应用结合[8-9]。授权管理模型体系结构如图 3 所示。

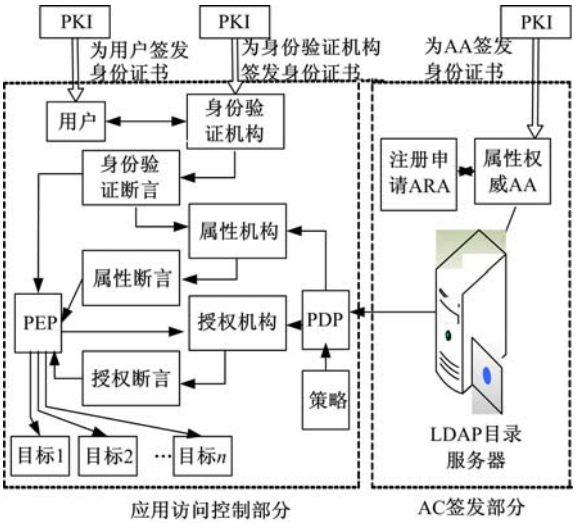


**图 3　基于 SAML 和 PMI 的授权管理模型体系结构**

**Fig. 3　Architecture of authorization management model based on SAML and PMI**

该模型主要由访问控制和 AC 签发两部分组成。其中，访问控制部分使用策略实施点 PEP（Policy enforcement point）和策略决策点 PDP（Policy decision point）进行交互。PEP 的主要作用是向授权机构申请授权，并根据授权决策的结果实施决策，即对目标执行访问或者拒绝访问。PDP 的主要作用是当接收到一个授权请求时，根据授权策略、访问者的安全属性断言以及当前条件进行决策。

交互过程中用户的身份验证、属性的获取和授权决策的执行都使用了 SAML 断言、SAML 协议和 SAML 绑定等技术。AC 签发部分主要包括 AA、ARA（属性注册权威，Attribute registration authority）和 LDAP 服务器，AA 负责签发 AC、ARA 为 AC 的注册申请提供服务，LDAP 是用来存储签发的 AC 和 ACRL。模型的两个部分通过 PDP 与 LDAP 目录服务器的交互实现应用上的结合，LDAP 目录服务器为 PDP 提供了授权所需要的一切必要信息，包括用户、资源和权限信息。

需要特别说明的是，在部署 AA 时，要根据系统内用户的数量、管理的模式定义 AA、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，确保 PMI 服务能力具有延续性和良好的业务量适应能力。

### 2.2　授权管理实现

基于 SAML 的 PMI 授权管理模型中各个模块的开发相互独立，只要遵循 SAML 标准，各个模块可以单独替换，而不会影响到其他模块和整个系统的正常运行。本授权管理模型采用 SUN JDK 1.5、VeriSign Trust Services Integration Kit 实现访问控制，使用 SUN Directory Server 5.2 实现 LDAP 目录服务，通过 PERMIS Attribute Certificate Manage 实现 AC 签发。其主要功能包括：基本访问控制逻辑；用户信息、角色信息和策略信息提取；用户与身份验证服务器双向验证身份；访问决策。授权管理系统的实现架构如图 4 所示。

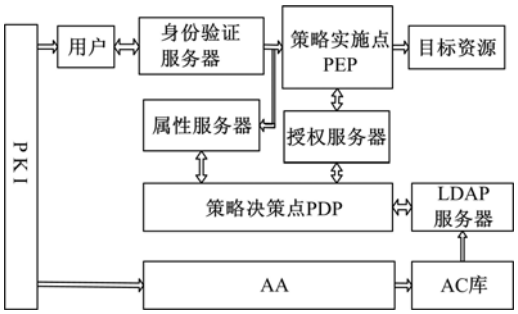


**图 4　授权管理系统架构**

**Fig. 4　Framework of authorization management system**

为了实现权限管理的控制，制定了 XML 格式的策略文件 mypolicy.xml，其部分内容如下：

＜X.509_PMI_RBAC_Policy OID＝“1.2.826.0.1.3344810.6.0.0.3”＞

XML 策略都包含在＜X.509_PMI_RBAC_

Policy/>体中,策略 OID 用来标识策略的唯一性。

```
<SubjectPolicy>
<SubjectDomainSpec
ID="SubjectDomain0">
<Include
LDAPDN="OU=caac,O=pmi,C=GB"/>
</SubjectDomainSpec>
</SubjectPolicy>
```

主体策略<SubjectPolicy/>定义的是主体域,规定访问主体必须来自这样的 3 个主体域。这里规定的主体域分别是 OU=caac,O=pmi,C=GB; OU=atm, O=pmi, C=GB 和 OU=airline,O=pmi,C=GB。

```
<RoleHierarchyPolicy>
<RoleSpec OID="1.2.826.0.1.3344810.1.1.14" Type="permisRole">
<SupRole Value="official"/>
<SupRole Value="personnel"/>
<SupRole Value="public"/>
</RoleSpec>
</RoleHierarchyPolicy>
```

角色层次策略<RoleHierarchyPolicy/>指定了策略中包含的角色类型 permisRole 及其顶级角色值。这里指定了行政管理人员(official)、信息员(personnel)和公众用户(public)3 个角色。

### 2.3 授权管理流程

授权管理模型的角色定义与权限分配流程如图 5 所示。授权管理模型的访问控制工作流程设计如下:

(1)用户与身份验证服务通过公钥证书 PKC(Public key certificate)双向验证对方身份。一旦用户通过身份验证,他就可以请求身份验证服务返回一个 SAML 断言,这个断言作为其身份验证的证明。

(2)用户请求到达目标资源前,身份验证服务将一个 SAML 身份验证断言送至 PEP,这个 SAML 身份断言就是前面从身份验证服务检索到的。

(3)PEP 收到这个断言以后,首先检查这个身份验证断言,判断其是否真实,以及它是否来自一个信任的机构,然后转向一个 SAML 属性服务,把这个身份验证断言传递给属性服务,请求一个 SAML 属性断言。

(4)属性服务根据 PEP 的请求,从 PDP 处获取属性信息,并把这个属性信息以 SAML 属性断言的形式返回给 PEP。

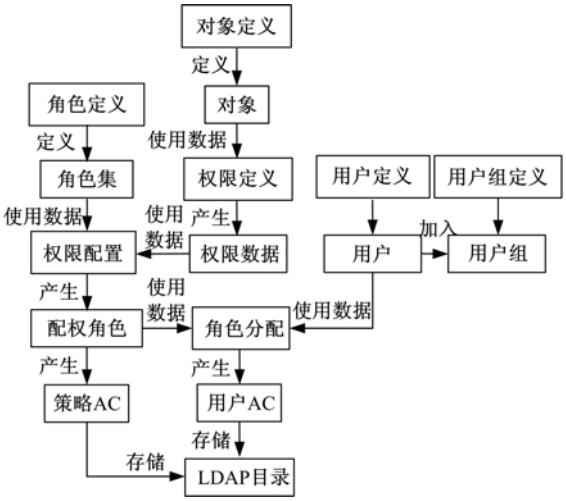


**图 5 角色定义与权限分配流程**

**Fig. 5 Flowchart of role definition and right distribution**

(5)PEP 向授权服务发送一个 SAML 授权请求和希望访问的指定资源,这个授权请求可以包含一个断言,这个断言可以有身份验证断言和属性断言或者只有一个属性断言。

(6)授权服务在收到请求以后,根据 PDP 及响应的策略作出一个访问决策,然后返回给 PEP 一个授权断言,这个授权断言包含了同意或者拒绝决策,最终 PEP 根据得到的授权断言实现用户对目标资源的访问控制。

## 3 实验与结果

为了验证本文提出的授权管理模型的有效性和可行性,在民航综合信息服务仿真平台上对该模型进行了测试。针对民航综合信息服务平台中参与数据交换的信息系统用户和信息资源的特点,并根据民航综合信息服务平台的用户性质,授权管理系统将用户划分为政府行政管理、空中交通管理和运输服务保障三类用户。根据用户职能的不同将用户划分为行政管理人员(official)、信息员(personnel)和公众用户(public)三类角色,将信息资源划分为航班信息(flight_information)和公众信息(public_inforamation)两类,将用户对资源的操作权限定义为查询操作和发布操作。

测试实验中的角色测试数据如表 1 所示。用户名为 User1,PKC 证书为 User1.cer,用户的角色为 public,用户请求的航班信息资源在 LDAP 服务器中的目录位置为 CN=flight_information,

OU＝resources，O＝pmi，C＝GB、公众信息资源在 LDAP 服务器中的目录位置为 CN＝public_information，OU＝resources，O＝pmi，C＝GB。

User1 通过授权管理模型对目标资源的预期访问结果如图 6 所示。授权管理模型的测试实验结果如表 2 所示。

**表 1　Public 角色测试表**

**Table 1　Public role test table**

| 用户 | 包含角色 | 目标资源 | 操作 |
|---|---|---|---|
| UID：User1<br>PKC：User1. cer | public | CN＝flight_information，<br>OU＝resources，O＝pmi，C＝GB | query |
| UID：User1<br>PKC：User1. cer | public | CN＝flight_information，<br>OU＝resources，O＝pmi，C＝GB | publish |
| UID：User1<br>PKC：User1. cer | public | CN＝public_information，<br>OU＝resources，O＝pmi，C＝GB | query |
| UID：User1<br>PKC：User1. cer | public | CN＝public_information，<br>OU＝resources，O＝pmi，C＝GB | publish |

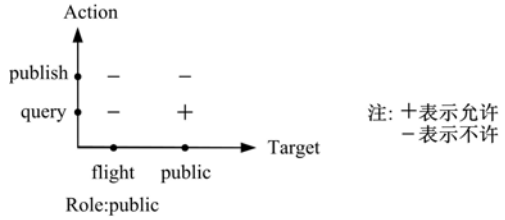


**图 6　Public 角色测试预期结果**

**Fig. 6　Anticipation of public role test**

**表 2　Public 角色测试结果**

**Table 2　Results of public role test**

| 用户 | 包含角色 | 目标资源 | 操作 | 结果 |
|---|---|---|---|---|
| User1 | public | flight_information | query | 1：the action is not |
| User1 | public | flight_information | publish | 1：the action is not |
| User1 | public | public_information | query | 0：action succeeded |
| User1 | public | public_information | publish | 1：the action is not |

从图 6 和表 2 的测试结果可以看出，通过授权管理模型的角色权限管理，拥有 public 角色的用户只可以对公众信息 public_information 进行查询操作，不具备对航班信息 flight_information 的查询操作权限，也无法发布 public_information 和 flight_information 信息，上述结果与实验预期目标一致。

## 4　结束语

目前，大多数应用系统主要使用基于 PKI 的授权管理机制，PKI 体系采用非对称公钥技术并利用数字证书作为媒介，可以有效地解决大型应用系统的身份认证、数据保密、抗抵赖等安全问题。但上述授权机制是以应用为中心，应用与应用之间相互独立，且各个应用系统自行实现其身份认证、控制措施，用户不能在不同的应用系统之间进行跨应用的访问，这样不利于不同应用系统之间的互联互通。本文提出的基于 SAML 和 PMI 的授权管理模型正是针对这一问题而设计的，该模型利用 AC 为应用系统提供了统一的授权管理机制，采用基于 XML 的 SAML 标准规范实现了对数据跨平台、跨应用系统传输的安全保护，简化了数据交换平台中访问控制和权限管理系统的开发与维护，降低了管理成本和复杂性。

**参考文献：**

[1] Hartman Bret，Flinn Donald J. 全面掌握 Web 服务安全性[M]. 杨硕，译. 北京：清华大学出版社，2004.

[2] Deitel Harvey M. Java Web 服务高级教程[M]. 邱仲潘，陈纯颖，陈凌峰，译. 北京：机械工业出版社，2003.

[3] 刘建伟，王育民. 网络安全-技术与实践[M]. 北京：清华大学出版社，2005.

[4] 钟迅科. 基于 SAML 实现 Web 服务的单点登录[J]. 现代计算机，2004，185(1)：32-36.
Zhong Xun-ke. SAML-based single sign-on model for Web services[J]. Modern Computer，2004，185(1)：32-36.

[5] Thomas Grob. Security analysis of the SAML single sign-on browser/artifact profile[R]. IBM Zurich Research Laboratory Zurich，Switzerland，2002.

[6] 胡九庆，张立，戴红权. 基于 SAML 单点登录安全服务体系的应用研究[J]. 微计算机信息，2006，22(12)：31-33.
Hu Jiu-qing，Zhang Li，Dai Hong-quan. Research on application of security service single sign on based on SAML[J]. Microcomputer Information，2006，22(12)：31-33.

[7] Chadwick David W. An X. 509 role-based privilege management infrastructure[J]. Future Generation Computer Systems，2003，19(2)：277-289.

[8] 罗昌行，欧阳晋，章卫国. 基于 SAML 标准的信任与授权服务平台设计[J]. 计算机工程，2005，31(13)：118-120.
Luo Chang-xing，Ouyang Jin，Zhang Wei-guo. Design of trust and authorization service platform based on SAML[J]. Computer Engineering，2005，31(13)：118-120.

[9] Sankar Krishna. Distributed services security using the SAML[C]// Key Presentation，Sixth Workshop On Distributed Objects and Components，MA，USA，2002.