PKI 政策的研究及其应用

徐激* 高毓航 龚俭
（东南大学计算机系，210096 南京）

【摘要】本文分析了 PKI 政策的概念，提出了政策制定与实施的具体设计方案，给出 PKI 管理系统中的各具体政策类型及其相关政策集定义。文中阐述了政策应用在 PKI 管理系统中的重要性和优越性，并在最后通过具体的政策实例分析，介绍实际应用环境下的政策应用。

【关键词】PKI;RA;CA;CALock;政策

A Study of PKI Policy and its Application

Xu Ji, Gao Yuhang, Gong Jian
(Southeast University, Computer Science Dept., 210096 Nanjing, P.R.China)

【Abstract】In this paper, the design of PKI policy's establishment and enforcement is proposed basing on the describing the concept of policy. And the paper discussed the constitution of policy types in detail. Compared with traditional PKI management system, we present the importance and advantages of the policy controlled PKI management system. The last section of this paper gives practical application of PKI policy and its framework, including a list of policy instances in our realized PKI system.

【Key words】PKI;RA;CA;CALock;Policy

1. 引言

公开密钥管理框架（PKI）是面向大型开放互联网络应用环境的公开密钥管理机制，通过注册中心（RA）、认证中心（CA）、端实体（End Entity）、证书库（Repository）等实体间的操作来支持开放网络环境中的身份认证和数据安全功能。作为一种网络基础设施，提供从现实到电子世界的信任关系映射，PKI 系统必须遵循一定的安全策略约束。PKI 政策即是对这些安全策略的规范化描述，是证书信任实体（Relying Party）信任该证书的基础和依据。政策通过在管理系统中各政策实施点上的具体应用，体现 PKI 系统中的信任管理规则。

目前，IETF 的 PKIX 工作组正致力于网络安全领域的通用政策框架及其应用的研究，并已提出 PKI 证书政策（Certificate Policy）和认证实施声明（Certificate Practice Statement），用来规范政策框架。遵从该标准制定的较典型的证书政策有：美国银行联合会的信任证书政策（American Bankers Association Trust ID Certificate Policy）、用于电子服务访问证书（Access Certificate for Electronic Services）的证书政策、美国联邦政府的桥接认证结构（Federal Bridge CA）的证书政策，以及 VeriSign 等公司的证书政策等等。

本文将在概念分析的基础上，通过对政策制定和实施技术的讨论，介绍政策在整个证书管理过程中的具体应用实现。

2. 政策的定义

政策是 PKI 系统中固有的部分，但 X509 标准在开始提出时并没有涉及政策问题。随着 PKI 系统应用范围的迅速扩大，各种层次的信任关系变得越来越复杂，用户证书的管理也变得困难，因此引入规范化的证书管理政策变得十分重要。

IETF PKIX 工作组将证书政策（CP）定义为一系列规则，它们对具有共同认证需求的用户证书的适用性进行了描述。针对不同层次的认证需求，证书政策定义该安全级别

作者简介：徐激，助教，主要研究方向为网络安全；高毓航，硕士，毕业于东南大学计算机系，主要研究方向为网络安全；龚俭，工学博士，东南大学计算机系教授、博导，主要研究方向包括网络管理、网络安全、网络体系结构等。

定稿日期：2002-05-26

上的证书颁发策略和证书的认证适用范围，相当于“what”；认证实施声明（CPS）用来标明证书授权中心签发和管理证书时所遵循的具体实施制度，偏重于介绍所属 CA 的各种具体操作规程，相当于“how”。

本文所研究的政策应用主要是指依照标准政策内容，在证书管理实体中建立政策模块，为管理系统提供监督机制和指导依据，从而使部分管理操作在政策监督下自动完成、其它人工操作在政策约束下执行，实现基于政策控制的半自动化 PKI 证书管理系统。同时，政策应用对其它各实体也将产生影响，主要体现在对证书所有者的使用规范和对证书信任者提供政策说明（参见图 1）。

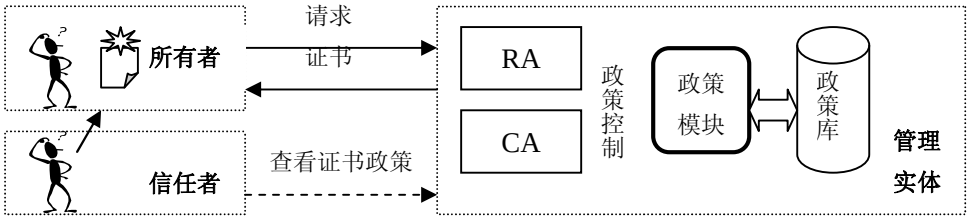

图 1. PKI 系统政策应用基本框架

3. 政策的制定和实施

IETF PKIX 工作组提出的证书政策和认证实施声明给出了基本的政策框架内容，但在实际应用中需要根据应用背景制定一个具体的 PKI 政策集，包括对各个实体的特性和操作流程的考虑。

本文制定了一系列的政策类型集，将政策类型集实例化后得到政策实例集。政策类型与政策实例的关系类似于面向对象技术中的类与对象的关系：同一种政策类型对应相同的数据处理方法和流程，政策实例则是政策实际应用参数的设定。管理系统在政策决定点 PDP（Policy Decision Point）上会根据当前条件，判断是否需要和需要何种政策。如需要某种政策，则通过函数调用或数据通信实现与政策模块的链接，该应用点即为该政策实例的政策实施点 PEP(Policy Enforcement Point)。每一政策实例都是通过政策模块在对应政策实施点上的应用，指导和协调 PKI 管理系统的一致性运作（参见图 2）。从政策的可扩展性出发，本系统采用的是松耦合应用方式：各项政策被设计为独立的模块，具备通用数据接口，系统可以灵活的增加、删除、修改政策规则，因此政策的扩展将非常容易。

本文根据政策的应用方式和表现形式的不同，将 PKI 管理系统中的政策分为两方面描述：管理操作控制政策和证书扩展项政策。下面将分别给出具体的政策类型集的设计。

3.1 管理操作控制政策

管理操作控制政策包含多种政策类型，对应的政策实施点分布在整个系统之中。总的来说，这些政策是通过在政策库中预先设定的规则和参数，在到达某一个预定的政策实施点时，对系统的运行进行辅助决策和辅助处理。

举例来说，按传统方法对用户提交的申请进行处理时，需要管理人员人工检查各数据段的有效性。由于各用户群的证书内容要求不尽相同，管理人员很容易在判断时出现失误，导致不一致性和潜在的安全漏洞，并且处理效率低下。控制政策在前后两个实施点上对证书请求内容作约束：在用户申请时，链接请求表单政策模块，根据用户类型，动态生成用户申请表单，在客户端对申请格式和某些字段的内容作初始要求，例如字段长度、邮件地址格式等；用户申请提交之后，在定时批量处理用户请求时，链接请求核查政策模块，检查用户请求信息的有效性，例如预申请有效期是否合理、用户公钥是否完整等。通过政策检查的请求将被统一封装成 PKCS10 请求，存放在目录库中待下一步处理。其它无效申请将会自动滤除，政策会在自动发给用户的邮件中作出相应提示。

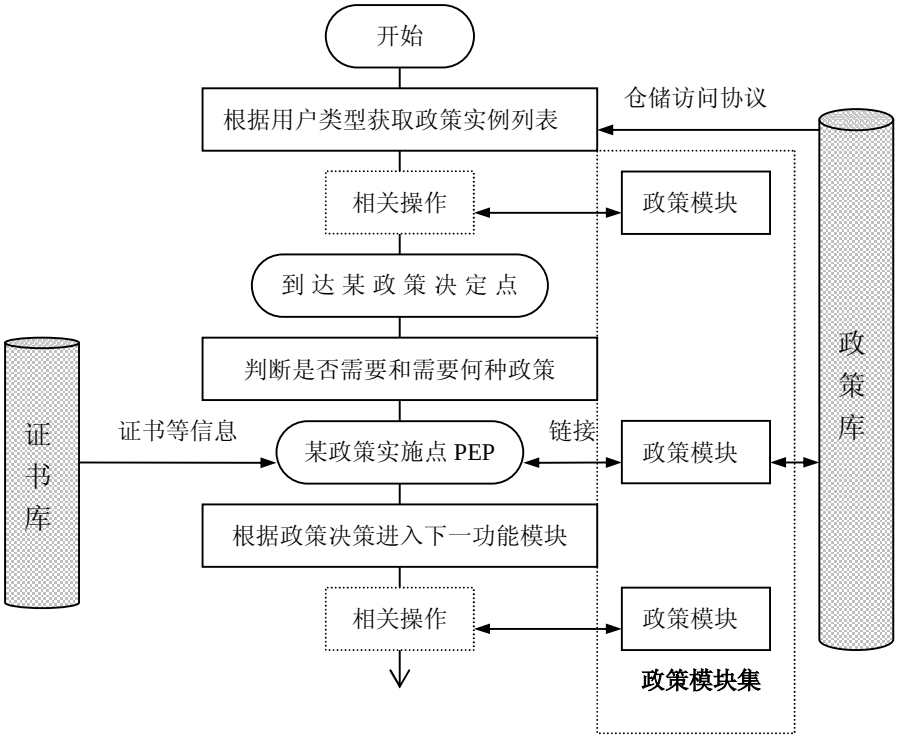

图 2. PKI 管理系统中的政策实施

PKI 系统的管理操作控制政策种类繁多，本文根据 IETF PKIX 组提出的证书政策和认证实施声明中所包含的身份认证和鉴别规则、操作规程、技术安全控制等方面内容，结合 PKI 系统的实际管理需求，制定了一系列控制政策。下面根据各管理实体的功能依次介绍这些控制政策。出于篇幅的考虑，不详细列出每个政策的实施点。

1）RA 实体：接收和处理用户请求，完成用户的注册工作。政策类型主要包括：请求表单属性限制政策（ReqFormConstraints）、签名算法限制政策（SigningAlgorithmConstraints）、公开密钥算法限制政策（PubKeyAlgorithmConstraints）、证书有效期限制政策（ValidityConstraints）和用户通知限制政策（NotificationConstraints）。

2）CA 实体：签发、撤销、挂起和恢复证书，负责管理和维护证书的工作。

a)与证书签发功能相关的政策类型：

证书主题唯一性限制政策（UniqueSubjectNameConstraints）、公开密钥算法限制政策（PubKeyAlgorithmConstraints）、签名算法限制政策（SigningAlgorithmConstraints）、子 CA 命名限制政策（SubCANamingConstraints）、证书主体命名限制（SubjectNamingConstraints）、证书有效期限制政策（ValidityConstraints）、CA 签发证书限制政策（CASignConstraints）、证书撤销限制政策（RevocationConstraints）、签名算法限制政策（SigningAlgorithmConstraints）、CRL 更新频率限制政策（RevocationFrequencyConstraints）。

b)与证书管理其它功能相关的政策类型：

发布点和发布方式政策（DistributionConstraints）、证书更新限制政策（RenewalConstraints）、证书挂起限制政策（CertHangConstraints）、证书恢复限制政策（CertHangConstraints）、用户通知限制政策（NotificationConstraints）。

3） 密钥备份实体：在支持密钥托管系统中负责用户密钥对的备份存贮管理。

密钥备份政策（KeyBackupConstraints）、签名算法限制政策（SigningAlgorithmConstraints）、密钥检索和访问限制政策（KeyRetrievalConstraints）。

4）任务调度管理实体：负责 PKI 系统中各项作业的调度工作。

RA 处理请求频率设置政策（JobScheduleConstraints）、CA 处理证书频率设置政策（JobScheduleConstraints）、CA 处理 CRL 频率设置政策（JobScheduleConstraints）。

5）授权管理实体：负责 PKI 系统资源访问授权管理工作。

角色判断政策（RoleAuthorizationConstraints）、页面授权政策（FuncCreditConstraints）。

3.2 证书扩展项政策

证书扩展项是证书结构的一部分，对扩展项内容的填写将直接体现在证书中。证书扩展项数据结构的制定是X509对v2版证书结构的改进，它的主要作用体现为：允许用户根据自己的实际应用需求定制一些证书属性传达信息；在证书的使用过程中，向验证方提供更多的政策信息和所属 CA 信息，加大认证力度，使多层次的认证应用成为可能；明确证书的使用范围，强化对用户证书的使用限制。

通过扩展项政策的应用，系统可自动根据预先设定的内容填写证书扩展项。这样，管理员如果需要在用户的证书扩展项中加入新的信息，可以通过基于 Web 的政策管理进行修改。由于证书扩展项将作为证书结构的一部分进行封装，因此证书扩展项政策的实施点要位于 X509 证书主体数据结构的构造之后、证书签署之前，由政策模块生成并添加扩展项到证书结构中去。

ITU-T X509 v3 版（RFC 2459）对证书的扩展项作了标准定义，并允许各证书管理系统根据需要选择扩展项内容封装到所签发的证书中。本文根据实际应用需求选择了基本的证书扩展项内容，省略了一些暂时没有应用需求的扩展项，例如证书主题的另一可选名称等。同时，针对 Netscape 浏览器的使用，增加了 Netscape 证书政策和 Netscape 密钥用途政策分别设置 Netscape 浏览器所能识别的说明信息以及它定义的单字节密钥用途标记。

证书扩展项的政策类型主要包括：CP 和 CPS 发布点政策（PolicyExtensions）、CRL 发布点政策（CRLDistributionPointExtensions）、Netscape 证书政策（NSExtensions）；基本限制政策（BasicConstraintsExtensions）、密钥用途限制政策（KeyUsageExtensions）、扩展密钥用途限制政策（ExtKeyUsageExtensions）、Netscape 密钥用途政策（NSKeyUsageExtensions）；政策映射政策（PolicyMappingExtensions）、政策限制政策（PolicyConstraintsExtensions）。

扩展项政策的内容在 X509 v3 证书“data”中的“X509v3 extensions”一项中依次排列。

4. 政策应用实例分析

CALock 是由 CERNET 华东（北）地区网络中心提出、设计、开发、建立和运行的 PKI 管理系统，面向教育网用户提供基于 X509 数字证书的安全认证服务，首先支持的应用是用户流量使用情况的查询服务。在第一代原型系统中加入 PKI 管理的政策应用，升级为目前的 CALock2。

在 CALock2 认证系统中，我们提供了基于 Web 的可视化政策管理，特权用户可以通过修改政策实例的内容而调整系统的安全策略，也可以按照 CALock2 的政策编写规范自行编写政策应用模块，并在系统中注册该政策类型，使系统可以找到并识别它。同时，在主页上向所有用户发布遵从标准 CP 与 CPS 框架（RFC 2527）的政策文档。

CALock2 中所实现的政策控制采用本文所讨论的松耦合应用方式，政策类型中的管理操作控制政策和证书扩展项政策分别以“Constraints”和“Extensions”结尾命名。针对不同的用户群，将政策实例以线性列表的形式存放在目录库中作为政策库。政策实例应用列表的第一栏为政策类型名，第二栏为政策实例名，第三栏为政策实例内容。同一种政策类型采用相同的数据处理方法，因此一种政策类型对应一种政策模块。某一政策模块在被链接时激活，根据用户类型选择政策实例名，读入应用列表中政策实例的参数设定内容，进行处理和返回决策结果（参见图 3）。

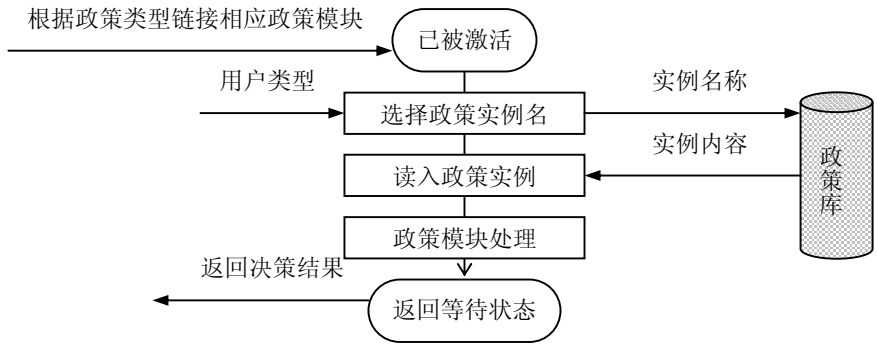

图 3. 某一政策模块的工作流程

本文将通过给出一套具体政策实例应用列表，说明政策类型实例化的应用。在流量查询服务中，为保证安全和方便，需要用户在登录时提供证书，以控制用户的权限。本例正是针对该需求所列出的用于流量查询证书的政策实例应用列表，对应的用户群是 CERNET 华东（北）地区的教育网用户。在政策库中，该应用列表的政策谓词为“certType =user_account”，政策实例名以“_u_a”结尾。出于篇幅考虑，以下给出的列表（表 1）均已简化，仅以证书申请和签发过程为例。

政策类型名	政策实例名	主要实例应用参数说明
RA 实体		
ReqFormConstraints	ReqForm_u_a	CN:TEXT::您的姓名(CN):64 Email:TEXT:*@*.edu.cn:E-mail 地址:64 OU:TEXT::部门名称(OU):100 O:TEXT:*:H*:组织名称(O):100 C:TEXT:CN:国家代码(C):10 S:TEXT::省份名称(S,可选):30 L:TEXT::城市名称(L,可选):30
SubjectNamingConstraints	SubNam_u_a	CN=4:,Email=15:*@*.edu.cn,OU=,O=*:H*,C=CN
SigningAlgorithmConstraints	SignAl_u_a	MD5withRSA
CA 实体		
PubKeyAlgorithmConstraints	PkeyAl_u_a	RSA,1024
ValidityConstraints	V_u_a	<=365
SubjectNamingConstraints	SubNam_u_a	CN=4:,Email=15:*@*.edu.cn,OU=,O=*:H*,C=CN
UniqueSubjectNameConstraints	UniqSNam_u_a	True
CASignConstraints	CASign_u_a	Auto
BasicConstraintsExtensions	BC_u_a	User cert, pathlen=10
PolicyExtensions	Pol_u_a	PolOID=2.16.156.0.0.0.5 CPS=http://ca.njnet.edu.cn/
KeyUsageExtensions	KeyUsg_u_a	0X01F0=digitalSignature, nonRepudiation,keyAgreement, keyEncipherment,dataEncipherment
NSKeyUsageExtensions	NSKeyUsg_u_a	0X80＝SSL Client
NSExtensions	NS_u_a	NSComment＝Net Traffic Accounting Cert
SigningAlgorithmConstraints	CASignAl_u_a	MD5withRSA
DistributionConstraints	Distr_u_a	ldap://x.njnet.edu.cn:999
NotificationConstraints	Notify_u_a	Email:CAagent,User

表 1. user_account 类用户政策实例应用列表（简化）

分析：某用户单位工作人员 XuJi，申请一张流量查询证书。首先登录到申请页面，选择用户证书类型为 user_account，系统根据该类列表中的政策实例 ReqForm_u_a 自动生成证书请求表单。XuJi 填写个人信息并提交。RA 按照证书命名政策 SubNam_u_a 检查请求信息，如不正确则转到用户通知功能模块。SubNam_u_a 要求用户必须填写 CN、Email、OU、O、C 这四个字段，且 CN 和 Email 的长度不能分别短于 4 和 15 字节，Email 必须以“edu.cn”为后缀，O 字段中必须包含 H 开头的教育网用户编号，C 必须为“CN”。如果请求无误，RA 就按照 SignAl_u_a 指定的 MD5withRSA 算法对请求签名，并提交请求给 CA。

CA 对该请求的处理工作由任务调度实体按照政策要求定期触发。CA 根据该类型列表中的“PkeyAl_u_a、V_u_a、SubNam_u_a、UniqSNam_u_a”项，依次检查：请求中的公钥算法是否为 RSA、强度是否为 1024；请求的有效期，若无或大于 365 就设为 365 天；命名是否合法；是否具有唯一性。当所有检查通过后，CA 根据 CASign_u_a 中的“Auto”设置自动将该请求放入待签发队列，同时向管理员发出通知。如果管理员不进行任何人工干预，CA 将在设定的时间签发该请求。当然 CASign_u_a 亦可设为“manual”强制要求人工干预。

若签发该请求，CA 根据请求信息构造 X509 证书结构，并按照列表中的“BC_u_a、Pol_u_a、KeyUsg_u_a、NSKeyUsg_u_a、NS_u_a”扩展项要求，生成证书扩展项结构，并依次加入到证书中。表明这是一张用户证书，最大允许认证深度为 10；该证书遵循以 2.16.156.0.0.0.5 为 OID 标识的证书政策；签署该证书的 CA 及其管理机构所遵循的具体认证实施声明可从 http://ca.njnet.edu.cn 得到；该证书可用于数字签名、无否认、密钥交换、密钥和数据加密；该证书可用于 SSL 通信；该证书用于流量查询。最后，CA 按照 CASignAl_u_a 的要求对证书进行 MD5withRSA 签名，根据证书发布政策 Distr_u_a 将证书通过 LDAP 协议发布到位于主机 x.njnet.edu.cn、端口 999 的目录服务器上。完成后，根据用户通知政策 Notify_u_a 将签发的结果用 Email 方式通知 CA 管理员和用户。

5. 结束语

CALock2 作为教育网中 PKI 管理的示范系统，提出并实现了政策控制下的半自动化运行模式，将政策应用以政策集的形式制定和存放、以政策模块集的形式实现，从而将整个 PKI 系统的技术安全控制和运行规则集中到政策的管理上，该系统的使用对在 CERNET 中推广普及网络安全通信概念和 CA 技术起到了积极的作用。随着 Internet 的发展，复杂认证结构应运而生，各子认证系统之间的认证策略协商和比照将会成为建立相互信任关系中的重要工作。通过政策的应用，子认证系统间信任关系的建立将成为可能。