基于路径发现的 PKI 扩展方法
An Expansion method of PKI with Path Discovery

龚俭　刘建航
Jian GONG　Jianhang LIU

东南大学计算机系
Department of Computer Science and Technology, Southeast University

摘要：PKI 的可扩展性集中表现为当证书服务用户的规模超出原有系统的容量后，能够通过增加 PKI 管理实体的数量和层次来满足需求，并同时保证原有系统能够平滑地过渡到新的规模。本文探讨了 PKI 管理域之内和之间所可能的向下，平级，和向上三种扩展方式，提出使用"路径发现"过程来减少 PKI 扩展时对端实体的影响，从而提高 PKI 服务范围的可扩展性。

Abstract: The expansibility of PKI is expected to have the features that when the amount of user exceeds the system capacity, the users' requirement can still be met by simply expanding the number of PKI entities and management levels, and this expansion can achieved smoothly from the original system. The upward, downward, and horizontal expansions of PKI have been discussed in this paper. A path discovery method has been suggested to reduce the effect of PKI expansion to the end-entities, so as to enhance the expansibility of PKI services.

关键词：网络安全、密钥证书、CA、PKI、路径发现。

Key words: Network Security, Key Certificate, CA, PKI, Path Discovery.

1. 引言

全局性 PKI（Public Key Infrastructure）的形成是一个自发的过程，从 PEM 到 SET，都不能一开始就拥有一个覆盖所有用户的树状 CA 体系，需要不断将各自相对独立的 PKI"粘贴"起来构建更大的体系。因此要求 PKI 有良好的可扩展性，使得当证书服务用户的规模超出原有系统的容量后，能够通过增加 PKI 管理实体的数量和层次来满足用户需求，并同时保证原有系统能够平滑地过渡到新的规模以保证应用系统的正常工作。

对端实体而言，CA 证书有两类：CA 自签名证书和 CA 间证书。前者仅用于承载 CA 公钥，后者则是一个 CA 对另一个 CA 信任关系的体现。当涉及不同管理域时，CA 间需要通过签发 CA 间证书建立信任关系，并需要让相关的端实体得知这个新建立的域间信任，以形成访问不同管理域对象时使用的证书链。

目前的 PKI 框架中，端实体对证书的处理是相同的，即都作为个人安全环境 PSE 静态配置的一部分，在初始化时由端实体加载。这种做法使 PKI 的扩展对端实体不透明，即当域间信任发生变化时，端实体需要静态地改变配置，以指出 CA 间新的关系。本文探讨了 PKI 管理域之内和之间的向下、平级、和向上三种扩展方式，提出了 CA 服务的一种实现机制，称为“路径发现” 。这个机制的基本思路是对以上两类 CA 证书作不同的处理：对 CA 自签名证书，仍作为 PSE 的关键部分由端实体静态配置；对 CA 间证书，则除初始时的静态配置外，端系统还可通过路径发现算法动态地获得跨越 PKI 管理域所需要的 CA 间证书，从而可自动扩展 PKI 的覆盖范围，减少 PKI 扩展时对端实体的影响，改

进系统了的可扩展性。

2. PKI 的扩展问题

PKI 的扩展原则上可分为三类情况：向下扩展，平行扩展和向上扩展。向下扩展发生在单个 PKI 管理域之内，当原有 CA 的处理能力不足以满足系统内用户需求时，要求增设下级 CA 来分担证书的管理任务。

PKI 的向下扩展是直观的，对端用户完全透明，其步骤可归纳为：

(1) 根 CA 通过签发 CA 间证书来授权下级 CA 的建立。

(2) 子 CA 向直接申请 CA 证书的新用户提供证书链。

(3) 属于新 CA 命名空间内的老用户在向根 CA 作证书更新时将收到证书链，从此由新 CA 接管这些用户的证书管理工作。

PKI 的平行扩展是两个管理域进行交叉验证的需要，图 1 给出了一个例子。NorthSchool 的研究生希望能够查阅 EastSchool 图书馆的资料，为此，EastSchool 签发了以 EastSchool 根 CA 为 Subject 的 CA 证书，并在图书馆 Server 的 ACL 中允许所有 ou=Graduate,o=NorthSchool,c=CN 的用户访问。

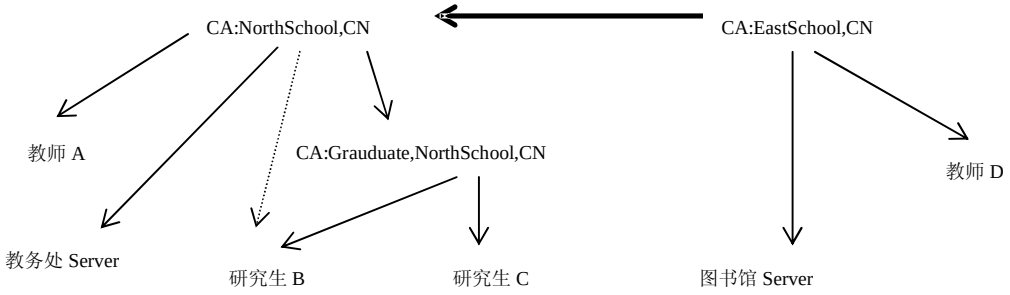

图 1　　PKI 平行扩展的例子

然而如果 NorthSchool 的用户象访问本校服务器一样对 EastSchool 图书馆服务器出示了源于 NorthSchool 根 CA 的证书链，而对方使用 EastSchool 根 CA 的公钥作验证时会导致失败。因此，NorthSchool 的用户必须下载 EastSchool 根 CA 向 NorthSchool 根 CA 签发的 CA 证书，并在访问 EastSchool 图书馆服务器时将它置于证书链的最左端。在这种方式下，CA 间信任关系的变化需要端实体的参与，假如又有 WestSchool，SouthSchool 提供服务，则端实体就要对所有的变化下载新的证书。因为 PKI 的水平扩展是不透明的，这在较大规模的网络中会对端实体产生很大影响，所以有必要在实现过程中引入优化的方法，使 PKI 的平行扩展对端系统透明。

3. 路径发现方法

端实体所拥有的各类证书信息构成的证书环境(Certificate Environment)由三个证书集，一个默认证书链，和一个映射关系表组成。三个证书集为 SelfCACerts，CrossCACerts，和 EndEntityCerts，分别对应 CA 自签名证书集合，CA 间证书集合以及端实体证书集合。默认证书链为端实体鉴别过程中缺省出示的证书链；映射关系表记录目标地址与应出示证书链的对应关系。

路径发现方法的基本思路是在每个 PKI 管理域中设立 CA 间证书的存储代理，称为路

径发现服务提供者，它收集所有其它域 CA 签发的，以本域 CA 为 Subject 的 CA 间证书。引入路径发现过程后，不同 PKI 管理域之间的端实体 A 访问 B 的证书链确认过程为：

(1) A 检查是否访问过 B，若是则出示映射关系表中对应的证书链；否则出示自己的默认证书链。

(2) B 检查自己的 SelfCACerts 集，试图找到某个自签名 CA 证书，以它为起点可以校验 A 所出示的证书链。若找到，则证书链确认完成；否则，向 A 返回鉴别失败信息以及 B 所支持的根 CA 名（即 SelfCACerts 中的所有 CA）。

(3) A 发起路径发现过程：A 向自己 PKI 域内的路径发现提供者提交 B 所支持的根 CA 列表，查询是否存在 B 所在管理域对本域的信任关系。

(4)若不存在，返回空，表明 B 所在的 PKI 管理域无法确认 A 的真实性；若存在，路径发现提供者将返回一个或多个 CA 间证书，这些证书由 B 所支持的某个根 CA 签发，以 A 所在域 CA 为 Subject。

(5)A 选择一个返回的 CA 间证书置于最前面，与默认证书链一起构成新的证书链重新发起请求。B 将重复(2)中的工作。

(6)若失败，A 将终止鉴别过程，丢弃路径发现过程中得到的那些 CA 间证书；若鉴别成功，A 将目标地址和完整的证书链写入映射关系表以备下次使用；将该 CA 间证书写入 CrossCACerts 集合。

以图 1 为例的路径发现交互过程如图 2 所示。端实体可以通过手工配置指定自己的路径发现服务提供者，但更好的办法是由它所信赖的根 CA 在证书中声明，这可以通过定义类似于 CRLDistributionPoint 的扩展项来实现。

由于 PKI 管理域中端实体的最终信任者是根 CA，因此路径发现服务提供者由根 CA 兼任是合理的。由于路径发现动作只是在端实体在向另一个陌生的端实体第一次进行访问时才发生，因此原则上不会对根 CA 的性能产生重大影响。路径发现过程无需特别的安全保护措施，因为端系统用户得到的 CA 间证书内容的有效性是靠数字签名来保证的，它没有必要也无法确认路径发现的返回结果是否正确。对路径发现的攻击，如篡改，只会导致鉴别失败而无法使进行身份认证的系统作出错误的授权。因此路径发现过程可以使用 HTTP，FTP 等通用传输协议。

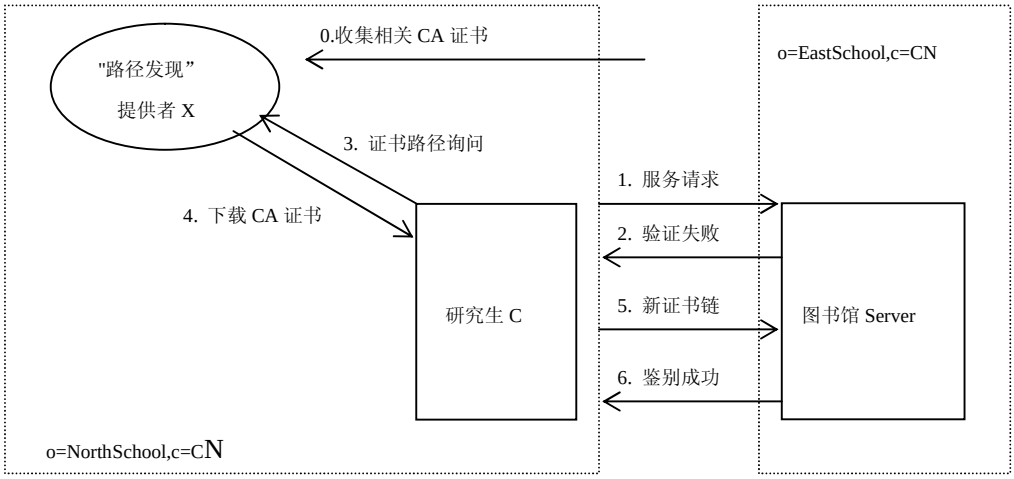

图 2 "路径发现"过程示例

4. PKI 向上扩展的路径发现

PKI 的平行扩展实现不同 PKI 管理域之间的沟通，但通过各根 CA 互授证书来维持域间信任在 PKI 管理域数量较多的情况下就显得低效，需要建立更高层次的 CA，进行 PKI 的向上扩展。在图 3 所示的例子中，管理 Education,CN 域的根 CA 建立以后，向上扩展了原有的 PKI 管理域，域中端实体可直接获取该根 CA 的公钥（自签名证书）和源于它的证书链。PKI 向上扩展之后，原来各管理子域中端实体原有的证书在子域内可不受影响地照常使用。然而当跨子域使用时，将会遇到与 PKI 平行扩展时相同的问题。这时需要新 PKI 管理域中的端实体下载 Education, CN 根 CA 公钥，即建立起新的最终信任者。这样将向上扩展问题转化成类似于向下扩展问题后，PKI 管理域中的端实体可使用路径发现服务向新体系平滑迁移，原有的服务仍然可保证正常提供。例如研究生 B 从未访问过 EastSchool 的图书馆 Server，此时他的 CE 为：

SelfCACerts : { (CA:NorthSchool,CN) }

CrossCACerts : { (CA:NorthSchool,CN EE: CA:Graduate,NorthSchool,CN) }

EndEntityCerts:

{ (CA:Graduate,NorthSchool,CN EE:B,Graduate,NorthSchool,CN) }

B 对 EastSchool 图书馆 Server 的首次访问将失败，这时他将得到对方支持的两个 CA 名: CA:Education,CN 和 CA:EastSchool,CN。B 于是发起"路径发现"过程，得到两个 CA 间证书:

(CA:EastSchool,CN EE: CA:NorthSchool,CN) 和

(CA:Education,CN EE: CA:NorthSchool,CN)

B 可以选择以上任一个，与其默认证书链：

(CA:NorthSchool,CN EE: CA:Graduate,NorthSchool,CN) ，

(CA:Graduate,NorthSchool,CN EE:B,Graduate,NorthSchool,CN) 。

一起构成完整的证书链重新发起访问。

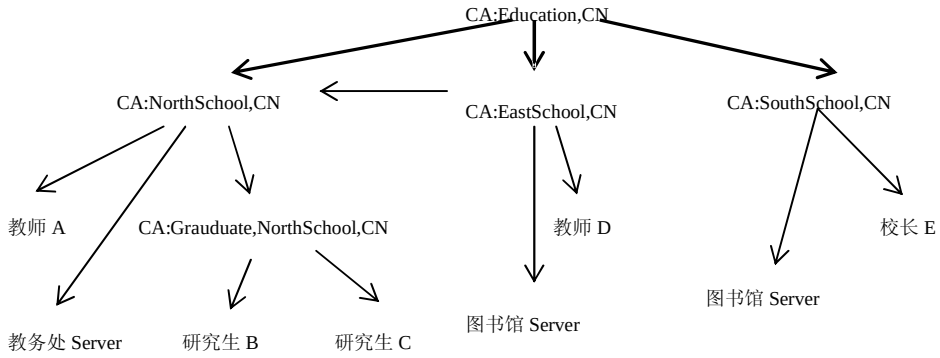

图 3 PKI 的向上扩展

5. 结论

完整的 CA 体系并非一朝一夕能够建立，虽然 X.509 标准定义了 PKI 管理域中 CA 和端实体的工作机制，但每个 PKI 域都是一个信息孤岛，因此增强 PKI 管理域之间的可扩展性十分重要。本文讨论了 PKI 的三种基本扩展方式，并提出一种支持 PKI 管理域扩展

的路径发现方法。路径发现方法是一种实现机制，它可以保证端系统获得正确的证书链，而证书的使用本身仍然由 PKI 的正常机制控制。路径服务的实现可以与 PKI 管理域中的根 CA 的实现联系起来，通过调整端实体的配置来引入 PSE；而路径发现服务器对其他管理域的 CA 间证书的获得过程则可由 CMP 协议控制，因此并不影响 PKI 的标准性和互操作性。

通过路径发现来进行 PKI 的扩展可实现 CA 间证书的动态获取，使域间信任关系的引入尽量对端实体透明，以提高 PKI 的可扩展性。通过路径发现过程，端实体可以在需要时动态查询 CA 间证书而不用事先下载，这就使域间信任关系的引入只涉及 CA 和路径发现服务提供者等少数实体，从而令 PKI 的平滑扩展成为可能。

参考文献

[1] 刘建航，基于 CA 的公开密钥管理框架[硕士学位论文]，南京：东南大学，1999.2

[2] IETF PKIX WG, "Internet X.509 Public Key Infrastructure Roadmap", draft-ietf-pkix-roadmap-00.txt, 1998.9

[3] IETF PKIX WG, " Internet X.509 Public Key Infrastructure Certificate and CRL Profile",draft-ietf-pkix-ipki-part1-08.txt, 1998.6

[4] IETF PKIX WG," Certificate Policy and Certification Practices Framework", draft-ietf-pkix-ipki-part4-03.txt, 1998.4

* 本文研究内容受国家 863 计划课题 863-317-01-04-99 资助

* 龚俭，1957 年 8 月出生，男，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、开放分布式处理等。

* 刘建航，工学硕士，东南大学计算机系研究生毕业，现在中国摩托罗拉软件中心工作。

第一作者联系地址：南京东南大学计算机系 邮编 210096

电话：025-3794341

电子邮件：jgong@njnet.edu.cn

1999 年 9 月 24 日投：计算机工程与科学（长沙）

1999 年 12 月 27 日返回要求修改。