文章编号:1000 - 582X(2003)12 - 0095 - 03

PKI/CA 系统互操作技术实现模型分析*

黄 勤[1], 谷振宇[1], 刘易良[2]
(1. 重庆大学 自动化学院,重庆 400044;2. 重庆工学院 信息安全研究所,重庆 400050)

摘 要:公钥基础设施和数字认证(PKI/CA ,Public Key Infrastructure and Certification Authorities)体系的应用已覆盖了电子商务、电子政务和电子事务等诸多领域,它是一个广泛应用的保障电子信息安全的解决方案。目前技术实现和安全策略的差异所造成的 CA 之间的互操作问题反过来制约了数字认证技术的应用。笔者在对互操作技术及国内外互操作技术实现模型作全面讨论基础上,论述了互操作研究的紧迫性及其广阔的应用前景,探讨了实施互操作需要解决的几个关键问题,并提出了解决方案的建议。

关键词:公钥基础设施;认证机构;互操作;模型
中图分类号:TP309 **文献标识码**:A

当今社会,电子商务、电子政务和电子事务等诸多领域迫切需要解决网上交易的安全问题。要保障网上的安全交易,涉及到信息的安全性、身份的合法性和行为的抗抵赖性等问题。其中对用户身份的确认是电子交易的关键。用户身份合法性的确认是通过从可信的第三方——CA (认证机构,Certification Authorities)获取对方公钥证书来实现的。在实际中存在以下两个方面的问题:一方面若要求任意通信的双方均拥有同一认证机构的公钥证书是不现实的;另一方面若要建立被所有证书使用者信任并能承担巨大风险的认证机构也是不实际的。那么,拥有不同 CA 证书的公钥用户如何确认对方身份从而进行安全通信呢? 唯一可行的途径是通过 CA 之间互签证书来确认信任关系,从而进行身份验证,即 CA 之间的互操作。

目前 PKI (公钥基础设施,Public Key Infrastructure)的应用发展非常迅速,已覆盖了安全电子邮件、VPN(虚拟专用网络, Virtual private networks)、Web 交互安全、电子数据交换、Internet 上的信用卡交易等业务,形成了年营业额达数亿美元的大产业。但由于没有统一的 PKI 互操作标准,不同种类产品或者实施不同安全策略的 CA 之间很难兼容和互操作,使得数字认证技术的广泛应用受到了制约,同时也成为制约电子商务发展以及电子政务战略实施的瓶颈。因此,开展 CA 互操作研究,尽快制定沟通各 CA 的有效方案和技术要求,切实解决目前各 CA 互不相通的现状对促进我国经济发展、保障国家利益具有重大意义。笔者对实施互操作中的几个关键问题略作分析讨论。

1 互操作技术及其要素

1.1 互操作的含义

所谓互操作是指不同 CA 之间的交叉认证,是引用 IETF (Internet 工程任务组, Internet Engineering Task Force)的 PKIX (Public Key Infrastructure on X.509)工作小组提出的概念,即由一个认证机构对另一个认证机构签发包含了 CA 的签名密钥的认证证书[1]。

在理论上,解决不同 CA 用户之间的身份认证问题的唯一可行方法是,公钥用户能够找到并使用另一证书——即由这个认证机构(公钥用户已经安全地拥有了该认证机构的公钥)所发放的包含了那个特定认证机构公钥的证书,如图 1 所示。

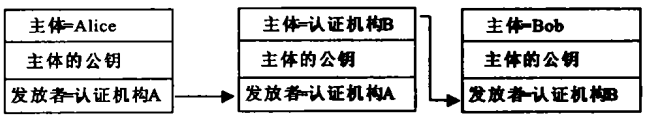

图 1 由交叉证书确立信任关系

Alice 想与 Bob 通信,则可通过认证机构 A 对认证机构 B 签发的证书获取 Bob 公钥。而这种 A 与 B 之间如何互签证书,以满足不同公钥用户之间进行身份验证就是互操作问题[1-2]。

* 收稿日期:2003 - 09 - 18
基金项目:重庆大学骨干教师资助基金资助项目
作者简介:黄勤(1960 -),女,重庆人,重庆大学副教授,主要从事计算机控制及网络安全方面的研究。

1.2 互操作——交叉认证涉及的几个要素[3-6]

从技术要求上看，实现互操作主要考虑以下几个问题。

1）证书策略（CP，Certificate Policies）分析、确定互操作标准和相关的技术实现方案。证书策略分析是控制CA之间的风险继承、保证信任路径扩展、实现互操作的前提和基础。CA要实现（某类证书的）交叉认证，相关的CA要有等价的（某类证书的）CP，这就产生了两个问题：①多个CA的CP要等价，与谁的等价；②如果CP要修改，参照谁的修改。而对于一个CA而言，CP的修改不是一件简单的事情，因为这可能涉及到改变CA的整个认证业务。

2）协议及认证路径的研究。PKI协议是一个大的协议族，要仔细研究，对其进行完善和修改，以便更好地支持交叉认证。通过对现有CA系统、PKI应用做出较大改变或增加复杂的额外技术手段来获取最优的证书可信路径是很难接受的。

3）目录体系的建立。要有效地实现互操作，要有统一的目录体系建设方案和指导规范，使CA的目录系统满足互操作的要求：即每个CA的目录系统能够加入到统一的、全局目录系统中，并且CA的目录系统应存放交叉认证所需的信息。

4）应用支持。互操作在技术上存在的最大问题是应用对互操作的支持。如何让互操作满足应用支持是一项艰巨的任务。

2 互操作结构模型

从整体看互操作技术还处于论证研究阶段，目前，解决不同信任域之间的互操作性问题，实现CA互信互通的方式主要有以下几种。

2.1 基于对等方式的网状交叉认证结构[2-3]

CA之间互相签发包含对方公钥的交叉认证证书，保证每个CA的用户通过交叉认证证书来信任另外一个CA的用户，从而实现信任的扩展和互通。如图2所示，A和B互签证书，则A的用户可以信任B，进而与B的用户相互认证。反之亦然。这种结构在两个CA之间创建了一个直接的信任通道，使得信任的路径相对简捷有效。但该模型存在以下两方面的困难：

1）对于用户端应用程序而言，当用户所在CA没有一个直接的交叉认证链接时，很难在用户之间确定一个证书链。

2）在交叉证书结构中，每两个CA之间都需要互相签发证书。证书的签发和分派在数量上是非常大的。如果要通过这种方式来实现交叉认证，那么整个交叉认证关系需要大量的管理和维护，因此不具有实际的操作意义。此外如何安全地保存和分派这些证书也是一个难题。因此，单纯的交叉证书模式不能适应于CA数目很多的场合。

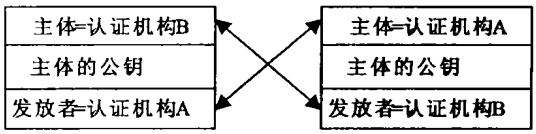

图2 对等交叉认证示意图

2.2 基于根CA的树状信任结构[2]

这种树状结构根CA是所有最终用户的公共信任锚，所有信任关系都起源于它。其结构如图3所示，E_1信任CA_1，E_3信任CA_2，由于CA_1与CA_2共同信任根CA，则他们也相互信任，这样E1就可以与E3实现认证。这是一种构造良好的、模块化的、组织上易于扩展的信任模型，而且信任关系的查找更加快捷，信任关系很容易建立。这种模式在一定规模的社区里可以运行良好，如果扩展到全社区范围，不同组织的安全策略差异将使信任路径扩展与风险控制之间的冲突难以协调。

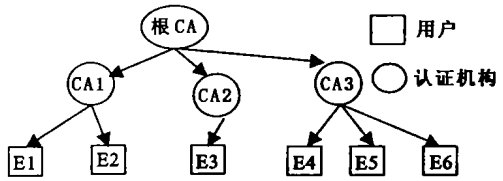

图3 严格的树状层次信任模型

2.3 基于交叉认证信任中介点的桥接结构[2]。

简单地说，桥CA是CA_i（$i=1,2,3,\cdots,n$）之间信任关系的介绍者。通过建立一个桥认证机构，由它来与各个不同的CA信任域进行交叉认证，并且作为与其它的PKI/CA建立信任关系的桥梁。借助这样的认证体系，不同的信任结构（如网状、树型等）就可以通过桥认证机构来实现交叉认证，而不是相互之间进行认证。如图4，桥CA分别与CA_1，CA_2，CA_3建立了信任关系，这样信任CA_6的E_1就可与信任CA_4的E_5进行认证。任何两个通过桥进行交叉认证的通信方都可以建立可信的路径，该模型大大减轻了建立信任关系时的开销。但该模式在实际确定互操作最小标准以控制风险的难度很大，同时限制了PKI/CA的完整应用，如授权，访问控制等。

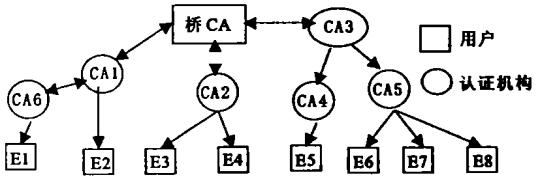

图4 桥CA连接不同的PKI

2.4 “交叉承认”模型

交叉承认是APEC（亚太经济合作组织，Asia-Pacific Economic Cooperation）组织的TEL（Telecommuni-

cation，电讯）工作组提出的。它基于这样一个概念：独立的 CA 之间可以被它们均信任的权威机构许可和审计。该模型的缺点如下：

1）目前，相关方如何获取判断证书是否可信的所需信息的机制尚不清楚。

2）该模型中被共同信任的权威机构的负担过重。

3）该模型未讨论对独立多层信任链的适应性问题。

2.5 证书信任链（Certificate Trust Lists）

这是一个签名的 PKCS#7 数据结构，该数据结构中存放了一个信任 CA 链。从域间互操作观点来看，CTL 与网状交叉认证结构有很多相似的地方，因此，它同样具有网状交叉认证结构的优缺点。

2.6 信任证书（Accreditation Certificate）模型[1]

澳大利亚政府提出的这个模型形式上与树状结构模型相似，但二者却存在着本质的区别：①每个被澳大利亚政府信任的 CA 可以拥有自己的 CP 和 CPS（Certification Practice Statement 认证过程描述）；②每个 CA 可以有自签发的公钥，而在严格分层的模型下，这是不允许的。从这一点看，信任证书模型中，信任 CA 是被相同的权威信任的自治实体。

2.7 委派路径发现和验证模型（Delegated Path Discovery and Validation）

该模型中客户端软件从信任的第 3 方服务器上查询是否可以信任来自非本地域的证书。该模型可以通过在线证书状态协议和路径委派和验证协议查询证书的有效性。与前几种相似，该模型的前端体系结构比较复杂，但由于它大大减轻了 CA 互联中的传输和处理过程，因此有一定的应用前景。但在应用中需要考虑带宽的压力，以及如何捕获应答信息。

3 互操作实验模型方案

一个可行的互操作方案应该不仅要在技术理论上是可行的，还要符合中国 CA 的实际发展情况，应做到在对现有 PKI 做最小改动、产生最小影响的情况下，实现 CA 之间的交叉认证，并保证原有系统的安全性和可扩展性，减少改造 CA 的代价。根据对各种互操作模型可行性和适应性的分析，针对中国目前的实际情况，提出下述实验模型方案。

1）从国际上目前对互操作模型的研究发展来看，比较普遍认可的、相对成熟、可行性比较大的有三种模型：①以加拿大政府公开密钥基础设施体系（GOCPKI）为代表的树状层次模型。②以美国政府的联邦桥为代表的桥接 CA 模式。③基于对等方式的的网状交叉认证结构。从美国进行 PKI 互连以及加拿大与新加坡互连的经验来看，利用任命的管理机构来进行认证是推动电子化进程较为合适的方式。树状模型、桥 CA 和网状交叉认证结构是特定 CA 间互通较合适的方式。采用与这三种相关联的互操作模型结构，能够推动形成国际互操作标准，实现世界各国 PKI/CA 体系的互连互通。

2）在中国目前已建的 CA 中，绝大多数都是树状层次模型。为了减轻各 CA 的互联改造代价，使方案更加实际可行，可以考虑借鉴 GOCPKI 的结构。GOCPKI 之所以比较成功是由于加拿大政府前期规划好，而且准备充分，投入力度大。这种模型有很大的优点，但 GOCPKI 适用于 PKI 系统建立之初就比较规范的情况。由于中国目前已经成立了相当数量的 CA，他们分属于不同行业、不同区域，且技术各异，如进行重新规划再投资则数量巨大，且造成已有投资浪费。GOCPKI 结构需要统一的最高信任源和信任策略（包括管理制度），在已经建立的众多 CA 中，按照信任域扩展原则分类，建立局部 GOCPKI 结构是可行方案。重庆工学院信息安全研究所正在进行这种模型的实验研究。

3）对 CP 差异比较大的 CA 之间，由于无法找到他们之间互联的互操作最小标准，这时可考虑借鉴美国的桥接 CA 模式。

4 结束语

PKI 的互操作是非常复杂又具有突破意义的研究问题。实现互操作是一项复杂的系统工程，考虑到现有 PKI 互操作方面的经验有限，所以适宜采取实验研究和逐步改进的方法。就互操作模型而言，仅靠某一种模型无法满足不同需要，可以考虑先对某一种模型进行实验研究，分别找到相对较优的方案，最终采用组合结构来实现 CA 的互操作。

参考文献：

[1] FORD W，BAUM M S，劳帼龄 译. 安全电子商务 - - - 为数字签名和加密构造基础设施[M]. （第二版）. 北京：人民邮电出版社，2002.

[2] NASH A，张玉清 译. 公钥基础设施（PKI）[M]. 北京：清华大学出版社，2002.

[3] HOUSLEY R. Internet X.509 Public Key Infrastructure Certificate and CRL Profile，RFC 2459[EB/OL]. ftp://ftp.isi.edu/in - notes/rfc2459.txt，January 1999.

[4] CHOKHANI S，FORD W. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework，RFC2527[EB/OL]. ftp://ftp.isi.edu/in - notes/rfc2527.txt，March 1999.

[5] ADAMS C，FARRELL S. Internet X.509 Public Key Infrastructure Certificate Management Protocols，RFC2510[EB/OL]. ftp://ftp.isi.edu/in - notes/rfc2510.txt，March 1999.

[6] DAVIS C R，周永彬 译. IPSec VPN 的安全实施[M]. 北京：清华大学出版社，2002.

（下转第 102 页）

A MP3 Player Solution Based On Universal Microchip

LUO Jun, GUI Jie-chu

(Key Laboratory of Optoelectronic Technology and System under the State Ministry of Education, Chongqing University, Chongqing 400044, China)

Abstract: This paper introduces a MP3 player solution based on universal microchip, Intel 8 bit microchip. It downloads music by USB interface and stores files into compact flash card. This paper specifies the usb interface technology between microchip and computer, interface design between microchip and compact flash card, and the control method of STA013 , a mp3 decoding chip. The discrete audio signal is transformed into the continual audio signal by D/A transformer CS4334. Because of using a universal microchip, this system can also be embeded into other microcontrol system to achieve an apparatus with MP3 player.

Key words: microchip; MP3; USB; compact flash card

(编辑 吕赛英)

(上接第 97 页)

Analysis on PKI/CA System Interoperbility Model

HUANG Qin, GU Zhen-yu, LIU Yi-liang

(1. College of Automation , Chongqing University , Chongqing 400044, China;
2. Information security research institute, Chongqing Institute of Technology, Chongqing 400050, China)

Abstract: Public Key Infrastructure and Certification Authorities (PKI/CA) have been used to support secure unclassified transactions over open networks, thus it promotes e - commerce, e - government, and electronic transactions protection. But the problem of PKI interoperability caused by the difference of the realization of technique and certificate policy has restricted the application of PKI. This article introduces the technique of Cross - Certification and its realization models. The emergency of Cross - Certification research and application landscape are described also. Furthermore, this article discusses several key problems those should be solved when preparing to carry the Cross - Certification model into practice.

Key words: PKI; CA; Interoperbility; model

(编辑 吕赛英)