沈阳市优秀自然科学著作资助项目

关于跨域认证关键技术的研究

Research on Cross Domain Authentication and Key Technology

姚瑶 著

辽宁科学技术出版社
LIAONING SCIENCE AND TECHNOLOGY PUBLISHING HOUSE

关于跨域认证关键技术的研究

姚瑶 著

辽宁科学技术出版社
沈 阳

沈阳市优秀自然科学著作资助项目

图书在版编目（CIP）数据

关于跨域认证关键技术的研究 / 姚瑶著. —沈阳：辽宁科学技术出版社，2015.4
ISBN 978-7-5381-9168-4

Ⅰ. ①关… Ⅱ. ①姚… Ⅲ. ①计算机网络—身份认证—安全技术—研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2015）第061410号

出版发行：辽宁科学技术出版社
（地址：沈阳市和平区十一纬路29号　邮编：110003）
印 刷 者：沈阳旭日印刷有限公司
经 销 者：各地新华书店
幅面尺寸：185mm × 260mm
印　　张：6.75
字　　数：150千字
印　　数：1~1000
出版时间：2015年4月第1版
印刷时间：2015年4月第1次印刷
责任编辑：李伟民
特邀编辑：王奉安
封面设计：嵘　嵘
责任校对：尹　昭

书　　号：ISBN 978-7-5381-9168-4
定　　价：30.00元

联系电话：024-23284526
邮购电话：024-23284502
http://www.lnkj.com.cn

前 言

随着信息科技的发展，丰富、快捷的信息技术在给人们带来极大便利的同时，由于网络的互联、互通、弱安全性的特征，公共空间和私人空间的界限日渐模糊，对保护个人网络信息安全提出了更高的要求。

为了满足广大网络用户的安全需求，大量的网络安全技术得到了广泛的研究和应用，跨域认证模型及其相关技术成为其中的热点之一。本书围绕跨域认证模型和相关技术进行了研究，提出了3种适用于有线网络的跨域认证方案、3个适用于有线网络的跨域认证模型和1种适用于无线网络的跨域认证技术。

全书共分为8章。第1章主要介绍了互联网及其安全技术的发展，以及本书的研究内容和主要贡献。第2章提出了一种重量级的Web跨域认证与数据共享方案。该方案基于一致性哈希在认证服务器的环形空间上的虚拟节点之间建立了映射关系，允许以最小的代价增加或移除认证服务器，具有较强的负载均衡能力和较好的冗余机制。第3章提出了一种中量级的Web跨域认证与数据共享方案。该方案实现跨域认证、数据传输。第4章提出了一种轻量级的Web跨域认证与数据共享方案。该方案采用易用模型实现跨域认证。第5章提出了一种适用于大规模认证域的跨域认证模型。该模型基于超立方体的结构特征支持不同信任域间实体的双向认证，减少了认证服务器间注册的工作量，简化了认证服务器间共享密钥的分配和管理工作。第6章提出了一种适用于复杂认证域的支持双向认证的跨异构域认证模型。第7章提出了一种适用于资源有限环境的跨域认证模型。该模型能够以较少的计算资源、

存储资源和网络带宽实现跨域认证和密钥协商，提供保密性、鉴别机制、完整性和不可抵赖性等安全保证。第8章提出了一种适用于无线网络环境的跨域认证模型。分析了RC4算法的安全性，提出了一种提高RC4算法安全性的方法。

作 者

2014年5月5日

目 录

1 绪 论

1.1 跨域认证技术的研究背景

计算机网络是一个开放性的系统，由于其开放性导致了计算机网络中存在许多安全漏洞和安全威胁，网络中的各类资源容易被其他人非法访问，造成损失。因此，对于网络资源访问者的身份的合法性进行必要的认证非常重要。

网络认证是对网络实体身份有效性进行确定的过程，是网络安全的一道基本防线。应用系统正常运营时，用户需要同时访问多个应用系统。这些应用系统可能由多个同构或异构的信任域构成，每个域的信任都是独立自治的，拥有自己的认证机构，支持不同的认证机制和安全策略。用户在访问不同应用系统时均需要登录认证。当用户登录不同系统时，身份认证信息容易混杂或丢失；如果使用一套简单认证信息在多系统同时使用，则保密强度会降低。在系统管理方面，应用系统需要大量的IT技术管理人员，分别管理和维护不同系统。

因此，需要建立安全可靠的跨域认证系统来实现不同系统之间的交替访问，从而保证系统不受破坏和干扰。跨域认证是允许用户访问跨越多个信任域的服务器资源，而不必重新认证的一种技术。即用户只需要在某一个信任域内登录一次并通过认证，就可以访问这个信任域和其他信任域内的服务器资源。

此外，随着无线互联网发展迅速，越来越多的用户可以通过无线网络访问移动互联网，使用各种各样的服务。因此，移动互联网开始面临网络信息安全问题。虽然传统的安全技术可以应用到移动网络中，但是由于移动互联网的无线环境的自身特点，传统的安全技术并不能切实有效地完成工作，设计更加简单高效的安全技术才是移动互联网无线环境的最好选择。

1.2 跨域认证技术的研究现状

跨域认证的目的是允许用户访问跨多个域的多个服务器的资源，而不必重新认证。跨域认证从其系统物理结构角度出发，可以分为两种模型：支持网关型的跨域认证，支持分布式的跨域认证。网关型跨域认证系统和分布式跨域认证系统的组成和结构是不同的。

为了实现跨域认证，所有安全域之间需要建立信任关系。对跨域认证技术的研究包

含多个方面，例如，网格环境下基于身份的跨域认证、Web跨域认证构架研究与实现、基于PKI或Kerberos的跨域认证、移动IP网络跨域认证等。

1.2.1 基于身份的跨域认证技术

基于Cookie的单点登录是一种基于身份的跨域认证技术。用户使用代表其身份的字符串作为他的身份，因此，用户身份与公钥直接绑定在一起，而不需要证书来完成这项工作，避免了复杂的证书管理。此外，在PKI中，用户的公钥必须经过CA的签名，认证需要由CA来完成，而在此认证中无须第三方介入。

Cookie是用户在浏览网页页面时，服务器发送给浏览器的体积很小的纯文本信息，它保存在客户机的内存中，或作为文件保存在客户机的硬盘中。用户以后访问同一个Web服务器时浏览器会把它们原样发送给服务器，通过让服务器读取它原先保存到客户端的信息，网站能够为浏览者提供一系列的方便。目前，Cookie已广泛应用于Web应用中。

Cookie由变量名和值组成。其属性里既有标准的Cookie变量，也有用户自己创建的变量，属性中变量是用“变量=值”的形式来保存。

Cookie的基本格式如下：

NAME=VALUE；Expires=Date；Path=PATH；

Domain=DOMAIN_NAME；Secure。

首先是指定Cookie的名称，并为其赋值。接下来分别是Cookie的有效期、URL路径以及域名，在这几项中，除了第一项以外，其他部分均为可选项。

（1）NAME=VALUE是每一个Cookie均必须有的部分。NAME是该Cookie的名称，VALUE是该Cookie的值。在字符串“NAME=VALUE”中，不含分号、逗号和空格等字符。如NAME是role_cookie，其VALUE是manager。

（2）Expires=DATE：Expires变量是一个只写变量，它确定了Cookie有效终止日期。该变量可省，如果缺省时，则Cookie的属性值不会保存在用户的硬盘中，而仅仅保存在内存当中，Cookie文件将随着浏览器的关闭而自动消失。

（3）Path=PATH：Path定义了Web服务器上哪些路径下的页面可获取服务器设置的Cookie。该项设置同样是可选的，如果缺省时，则Path的属性值为Web服务器传给浏览器的资源的路径名。

（4）Domain=DOMAIN_NAME：Domain是Cookie在其内有效的主机或域名。Domain确定了哪些Internet域中的Web服务器可读取浏览器所存取的Cookie。即只有来自这个域的页面才可以使用Cookie中的信息。这项设置是可选的，缺省时，设置Cookie的属性值为该Web服务器的域名。

（5）Secure：在Cookie中标记该变量，表明只有当浏览器和Web Server之间的通信协议为加密认证协议时，浏览器才向服务器提交相应的Cookie。当前这种协议只有一种，即为HTTPS。

Cookie的使用。有两种方式使用Cookie，一是当用户用浏览器首次访问某Web站点时，服务器端先用Set Cookie Header来创建一个Cookie，再用Response命令将Cookie写入访问者的计算机，此过程称作创建Cookie；二是当用户用浏览器再访问Web站点时，用Request命令从访问者的计算机中以忽略路径的方式取回Cookie，此过程称作读取Cookie。

采用Cookie技术解决SSO主要过程描述如下：

首先用户通过客户端浏览器，向应用服务器请求访问和使用受保护的资源，应用服务器分析请求，检查这个用户是否有已经创建好的有效的Cookie，其中包含有效的用户SSO票据。如果没有有效的Cookie，则应用服务器将用户的Web浏览器重定向到登录服务器。若验证成功，登录服务器产生一个有效的Cookie。其中包含有效的用户SSO票据。登录服务器将含有SSO票据的Cookie发送给用户的Web浏览器，并将用户的Web浏览器重定向到原先请求的资源，向应用服务器再次请求访问和使用已申请的资源。验证成功，则向用户提供所请求的资源；若验证不成功，则拒绝用户访问所请求的资源或提示用户重新登录（图1.1）。

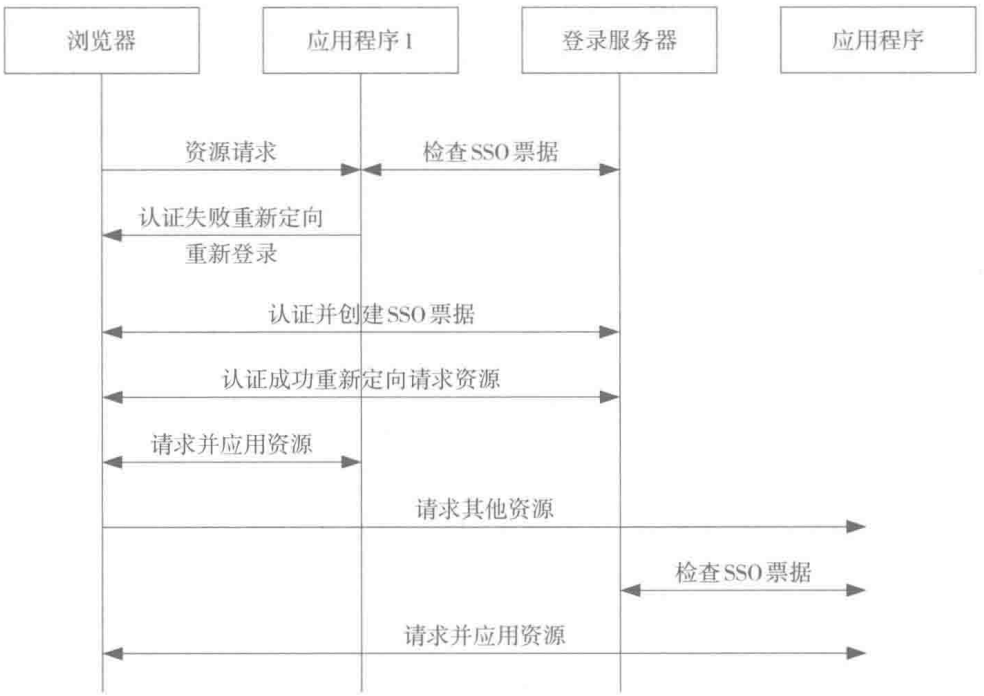

图1.1 基于Cookie的单点登录流程

Cookie的存取只对同一域下的主机有效，分布式应用系统往往不能保证所有的主机都在同一域下。当用户登录加入SSO认证体系里的一台服务器时，例如服务器A，客户机浏览器可以将获得的登录用户票据记录到本地Cookie中，当此客户机转而访问服务器B的时候，为了实现单点登录，服务器B必须要获得标识用户登录状态的票据作为凭证来进行验证，而此票据存储于先前访问服务器A时留下的Cookie，此Cookie只对来自服

务器A域里的访问有效，为获取访问其他域主机的Cookie，必须实现跨域共享Cookie。

假设处于不同域的服务器A和服务器B联合组成的网络应用需要统一的用户认证，客户机曾在服务器A进行了访问，并且在本地保存了服务器A的Cookie，图1.2显示了客户机在访问服务器B的时候共享服务器A的Cookie的过程。跨域共享Cookie实现单点登录涉及客户机、数据中心和登录认证中心（CA）3个角色之间的交互。采用Cookie技术解决跨域SSO主要过程描述如下：

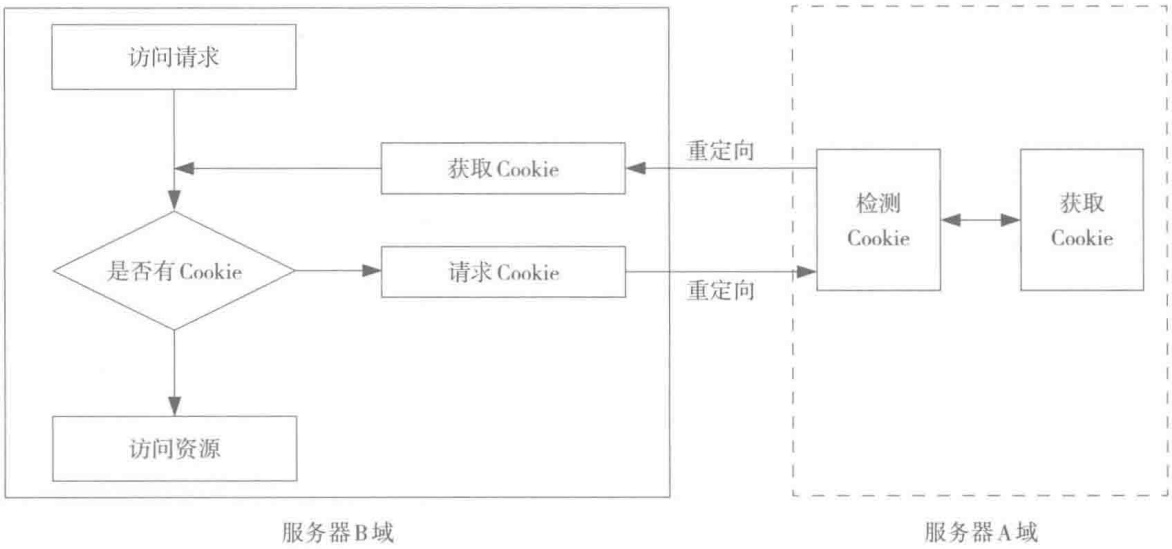

图1.2　跨域共享Cookie

（1）客户机访问某一数据中心网站的受保护资源，单点登录模块首先接管请求，查询客户机是否持有本数据中心的Cookie，并试图获取其中的访问票据。如果客户机可以提供，说明用户曾经以合法身份访问过此数据中心，并且尚未在本地注销，转向（4）；否则，要通过共享跨域的Cookie来确定是否进行全局登录，进行（2）。

（2）这个步骤的主要工作是跨域获取Cookie。客户机浏览器被重定向到登录认证中心，CA试图获取存储于客户机的Cookie，如果不存在，说明用户尚未全局登录，转向（3）；否则，从Cookie中获取票据。然后CA将客户机浏览器重定向回原先访问的数据中心，数据中心获取票据和返回地址，把票据写入客户端Cookie并跳转到返回地址，然后进行（1）。

（3）重定向客户机浏览器到CA上的登录页面，认证中心获取登录用户名和密码并将其与用户信息库信息核对，进行用户身份确认。如果没有这个用户或密码错误，直接返回登录失败；如果验证成功，随机生成标识此用户登录的唯一票据，并生成一个条目放入用户信息库中，并把票据存入客户机的Cookie中。然后，通过跨域Cookie共享机制，把此票据转入客户机所访问的数据中心，写到客户机的Cookie中，用户完成登录，转向（1）进行资源访问。

（4）客户机用票据来访问认证中心的用户状态查询服务，认证中心访问用户信息库确定该用户是否依然处于登录状态。如果处于登录状态则将用户名和用户的访问级别返

回数据中心，允许用户访问数据资源。否则转向（3），提示用户输入用户名和密码。

在本方案的整个流程中，除了最初输入的用户名和密码外，其他所传输的都是票据，最后客户机拿此票据获取登录用户的用户名，从而结束认证过程。

1.2.2 Web环境下跨域认证技术

Web跨域认证技术按照认证消息传递方式不同，通常有两种形式，即通过Web协议传递认证消息和通过独立于数据流的安全通信协议传递认证消息。

通过Web协议传递认证消息实现跨域认证中，认证消息流与数据流融合到一起，浏览器在页面请求中携带身份认证信息，Web服务器通过读取和分析Cookie、URI参数或隐藏字段中的认证信息来鉴别用户身份，这种方式通常实现基于Web请求代理的SSO。目前几种利用联盟身份实现跨域认证的XML标准，如安全声明标记语言、自由联盟计划和Web服务联盟语言均属于这种形式。这种形式实现简单灵活，不需要浏览器特殊支持，而且由于是以Web流通信，容易跨越防火墙和NAT网关，是较流行的一种形式。但是从实际情况来看，它更适用于安全级较低的应用环境中。

独立于数据流的安全通信协议实现跨域认证中，由专门的认证系统完成，认证协议的执行独立于使用它的Web协议环境，认证消息在特定连接中传递，不再是通过捎带形式在Web流中传递，通信方式大都是C/S构架，主流操作系统通常会实现常见跨域认证系统的部分或全部，有些认证系统需要专用认证客户端。这种方式通常实现基于ticket凭证的SSO。

Web应用程序不直接参与认证协议交互，它通过访问跨域认证服务获取来访者身份信息。认证服务大都以认证API形式存在。根据认证发起方不同，可分为推模式和拉模式两种形式。推模式指用户访问Web服务器时，认证客户端主动完成凭证和鉴别码的提交。拉模式指认证客户端被动接收到Web服务器，出示凭证要求时才提交相应认证信息。实现推模式时，认证客户端需要监视用户访问情况，为此认证客户端或者实现Web访问代理，目前很多浏览器均支持Web代理方式；或者实现对访问的监听。但是这两个方法均要在认证客户端增加很多额外功能。拉模式由Web应用程序调用认证接口，然后Web服务器的认证组件向认证客户端索要鉴别信息，认证客户端只负责认证交互，相对容易实现，这是比较常见的一种形式。

1.2.3 基于PKI或Kerberos的跨域认证技术

1.2.3.1 PKI概述

公钥基础设施PKI（Public Key Infrastructure），是利用公钥理论和技术建立提供信息安全服务的基础设施。该系统在统一的安全认证标准和规范的基础上提供在线身份认证服务，包括CA（Certificate Authority）认证、数字证书、数字签名以及相关安全应用组件模块。PKI系统提供认证、机密性、完整性和不可否认性服务，可以有效解决网上身份认证、信息完整性和不可否认性等安全问题，为电子商务、电子政务和其他应用提

供可靠的安全平台。PKI关键组件包括数字证书认证中心CA、审核注册中心RA（Registration Authority）、密钥管理中心KM（Key Manager）。作为提供信息安全服务的公共基础设施，PKI是目前公认的保障网络社会安全的最佳体系。

PKI作为网络环境的一种基础设施，必须具有良好的性能。一般对PKI性能有如下要求：

（1）易用性。PKI应尽可能地向上层应用屏蔽密码服务的细节，屏蔽复杂的安全解决方案，使密码服务对用户而言简单易用，同时便于单位、企业完全控制其信息资源。

（2）可扩展性。证书库和证书撤销列表CRL（Certificate Revocation List）必须具有良好的可扩展性。

（3）互操作性。不同企业、单位的PKI实现方法可能是不同的，这就提出了互操作性要求。要保证PKI的互操作性，必须将PKI建立在标准之上，这些标准包括加密标准、数字签名标准、Hash标准、密钥管理标准、证书格式、目录标准、数字信封格式、安全会话格式、安全应用程序接口规范等。

（4）多应用支持。PKI应该面向广泛的网络应用，提供文件传送安全、文件存储安全、电子邮件安全、电子表单安全、WEB应用安全等保护。支持多平台。PKI应该支持目前广泛应用的操作系统平台。

基于PKI的身份认证是一种比较流行的身份认证解决方案，具有很强的安全性和可靠性。PKI以公钥技术为基础，采用证书来管理公钥，通过可信任的第三方CA认证中心，把用户的公钥和用户的身份标识捆绑在一起，能够为所有网络应用提供加密和数字签名等密码服务。基于PKI的身份认证是一种双向认证，不同实体间可以通过公钥证书来验证对方身份的真实性。验证方首先用CA的公钥解开证书上CA的数字签名，验证证书的可靠性，然后再查看证书是否过期，验证其有效性；最后用读取到的公钥解密证书持有者私钥加密的随机数，验证公私钥对的匹配性。

如果证书被认证是真实的，则用户通过身份认证。由此看来，基于PKI的身份认证技术相当于采用第二种方法来实现身份认证。一个完整的PKI系统主要有认证中心、注册中心、密钥备份及恢复系统、证书/证书作废数据库、终端实体等5个基本组成部分（图1.3）。

认证中心CA是PKI的核心组成部分，是严格按照策略机构制订的规则负责颁发公钥证书的机构。CA主要负责证书生命周期的管理，发布并维护证书撤销列表CRL，并对其他主体的公钥进行验证，证明主体的身份以及它与公钥的匹配关系是否真实。

注册中心是用户和CA的接口，是一个可选的部分。它的功能主要包括：代理终端用户注册、生成代理用户的密钥资料、授权执行一定的证书生命周期管理功能等，以此增强系统的可扩展性和安全性，并且降低运营成本。

密钥备份及恢复系统对用户的解密密钥和签名公钥进行备份，当丢失时进行恢复，而签名私钥不能备份和恢复，否则将会约束PKI系统提供的不可否认性的能力。

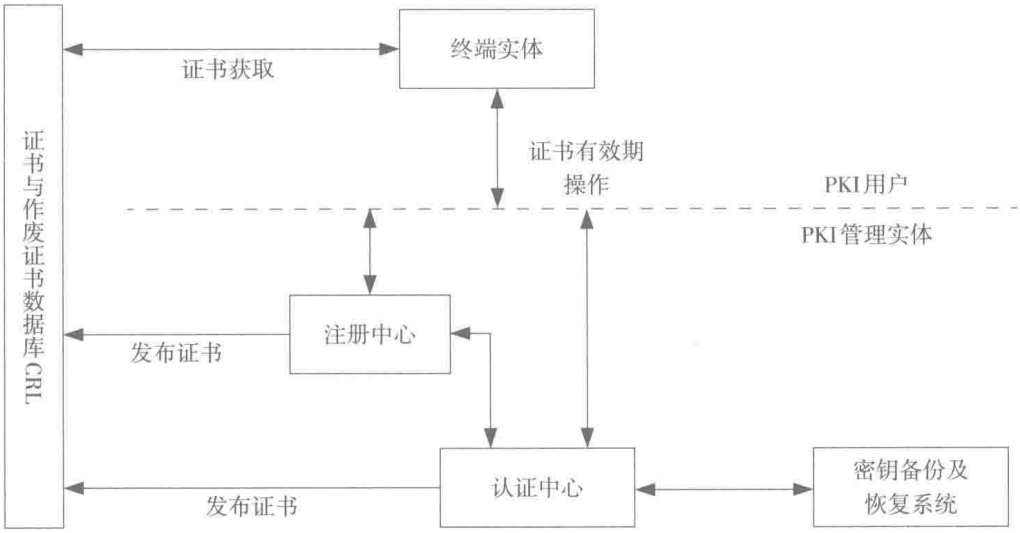

图1.3 PKI系统组成

数字证书库是集中存放CA颁发证书和撤销证书的数据库，用户可由此获得所需的证书及公钥。

证书作废系统通过CA签发的证书将用户身份和公钥绑定在一起，如果当用户的身份改变或密钥遭到破坏时，就必须存在一种机制来撤销这种认可。一般CA通过发布证书废除列表CRL来发布作废信息。CRL是由CA签名的一组电子文档，包括了被废除证书的唯一标识即证书序列号。

终端实体指最终使用数字证书的实体，不仅包括使用数字证书的人，也包括需要证书进行安全传输的其他实体，如主机等。

基于PKI的分布式认证模型主要有5类，包括层次结构模型、网状结构模型、桥形结构模型、混合结构模型、信任链结构模型。上述分布式认证模型的结构如下。

层次结构模型即一个倒置的树，根在顶部，树枝向下伸展，树叶在下面。根CA可以给直接链接在它下面的CA颁发证书，每个下层CA也都可以给直接链接在它下面的CA或终端实体颁发证书。根CA是层次结构中唯一的信任锚，所有实体都信任它。

网状结构模型没有唯一信任的根CA，各个CA之间都是平等的，每个CA都可以为其信任的用户颁发证书，各个CA之间也可以互相颁发证书来扩展信任关系，这样整个CA体系就形成一种类似网状的体系结构。网状结构中，各CA负载均衡。

桥形结构模型弥补了层次结构和网状结构的缺点，建立一个作为信任的桥梁，它不直接向用户颁发证书，而是使不同信任域建立对等的信任关系，用户可以保持原有的信任锚，实现了一个集中的分布式认证中心。

混合结构模型是层次结构与网状结构的混合体，存在多个根CA，任意两个根CA之间都要通过相互颁发交叉证书，进行分布式认证。

在混合结构模型中，每个层次结构都在根CA有一个单一的交叉证书通向另一个层次结构，也可以有选择性地在非根CA之间直接进行分布式认证。如果各个根的分布式

认证不复杂，可以较容易地构建简单且单一的认证路径；如果层次结构中两个低层节点要高频地链接，可以在它们之间直接颁发交叉证书，以简化认证路径的构建。

信任链结构模型：类似于层次结构，只是它同时拥有多个根CA，这些可信的根CA被预先提供给客户端系统，为了成功地被验证，证书一定要直接或间接地与这些可信根CA链接，目前所用浏览器中的证书就是应用这种结构。该结构存在许多安全隐患，例如，由于浏览器的用户自动地信任预安装的所有公钥，如果这些根CA中有一个是坏的，安全性将被完全破坏。另外一个潜在的安全隐患是没有实用的机制来撤销与更新嵌入到浏览器中的根密钥。如果发现一个根密钥是坏的或者与根的公钥相对应的私钥被泄密了，要使全世界数百万个浏览器都自动地废止该密钥的使用也是不可能的。

以上5种分布式认证模型适应于不同的CA构建结构，它们的特点如表1.1所示。

表1.1　分布式认证模型的比较

分布式认证模型	优点	缺点
层次结构	信任路径比较容易建立，只需依次查询颁发者的证书，一直到达根CA证书即可。有较好的扩展性，易于管理，适用于相同组织结构的团体	需要一个单一的信任点，这样的信任点很难实现，单个CA的失败会影响整个PKI体系，而且目前还没有直接恢复的技术
网状结构	CA之间没有上下级关系，信任域的扩展性好，灵活性强，适合动态变化的组织结构	随着CA数量的增加，认证路径的构建也变得比较困难，它需要对CA发布的证书进行反复的比较，可能会出现多条认证路径和死循环的现象，使证书验证难于实现
桥形结构	各CA相对独立，风险相对分散，能够方便地在不同结构的CA之间建立信任关系，证书路径比较容易构建，但是比层次结构的路径要稍微困难一些	要有一个大家都信任的第三方来充当桥CA，而这样的CA在现实中很难实现
混合结构	结合了层次结构与网状结构的特点，能够较容易地构建证书路径	当进行域间扩展时，每加入一个域，域间的交叉证书的个数就会以平方的数量级增长，不利于进行大规模扩展
信任链结构	不需要信赖目录服务器，具有方便性和简单易操作性	存在安全隐患

1.2.3.2　Kerberos概述

Kerberos是基于Needham、Schroeder的可信第三方协议。Kerberos协议是基于对称密码体系实现身份认证的协议。

Kerberos协议采用对称密码体制来实现通过可信第三方KDC（Key Distribution Center）的认证服务，实现通信双方相互的身份认证机制。并且它不依赖于主机的操作系统和地址，可以有效解决分布式网络环境下用户访问系统资源的安全性问题。

Kerberos身份认证协议是目前应用广泛，也相对较为成熟的一种身份认证机制。

Kerberos认证的实现不依赖于主机操作系统，不依赖对主机操作系统的信任，不要求网络中全部主机的物理安全性，并且是基于这样的假设：沿网络传送的数据包可能被增、删、改。Kerberos使用传统密码技术，即对称密钥加密技术，来提供可信任的第三方认证服务。主体必须向所期望的任何服务证明自己的身份，身份的证明是通过票据（Ticket）、会话密钥（Session Key）等来完成的。Kerberos的实现包括运行在物理安全主机上的一个或多个认证服务器。认证服务器保存主体及其密钥的数据库。代码库提供加密并实现Kerberos协议。典型的网络应用调用Kerberos库来获得认证。Kerberos认证技术中涉及的几个关键的概念如下：

（1）主体（Principal）。是参与网络通信中客户或服务器使用的唯一名称。使用Kerberos认证的主体既可以是一个用户也可以是一个网络服务器，从客户/服务器基于WPKI的Kerberos身份认证的应用研究的意义上讲，因为它们都使用Kerberos服务，故均可被称为客户。用主体表示这样的一个Kerberos的客户。Kerberos主体无论是用户还是服务，都是由以下3部分来定义：①主体名（Primary name）；②实例（Instance）；③域（Realm）。

所以，Kerberos主体可以表示为：Primary name/Instance@Realm，一个在SY.EDU.CN域内的用户名为yy，实例为管理员admin的主体名可以表示为：yy/admin@SY.EDU.CN。

（2）票据（Ticket）。是客户用于向服务器认证它自己的一个记录。包含客户的ID（身份）、会话密钥、时间戳及其他信息，并使用服务器密钥进行加密。

（3）会话密钥（Session key）。是在两个主体之间使用的暂时的加密密钥，生存时间仅局限在一次通信会话过程中。

（4）证书（Credentials）。是在一次认证交换中为了成功使用票据所需的信息，它包含一张票据和一个会话密钥。

（5）认证符（Authenticator）。是用于仅为客户和服务器已知的会话密钥新近生成的信息记录。

Kerberos的密钥分发中心KDC（Kerberos Distribute Center）是一个所有客户和他们的秘密密钥的数据库。秘密密钥是一个加密的口令，需要鉴别的网络业务、需要运用这些业务的客户机都要用Kerberos注册其秘密密钥。由于Kerberos知道每个实体的秘密密钥，故而它能产生消息向一个实体证实另一个实体的身份。Kerberos还能产生会话密钥，只供一个客户机和一个服务器（或两个客户机）使用，会话密钥用来加密双方间的通信消息，通信完毕后，立即销毁会话密钥。

当客户试图访问一个网络服务时，即KDC首先会验证客户的身份是否合法以及所请求的服务是否合法，如果合法它会向客户分发一个含有时间戳的会话票据（Session Ticket）。应用服务器通过会话票据来确认用户的身份。

出于对用户实现和安全分析的考虑，KDC任务被分配到两个相对独立的服务器AS（Authentication Server，认证服务器，链接并维护一个存放用户口令等信息的中央数据

库）和TGS（Ticket Granting Server，票据分发服务器）。因此整个系统将由4部分组成：AS，TGS，Client，Server。Kerberos认证模型如图1.4。

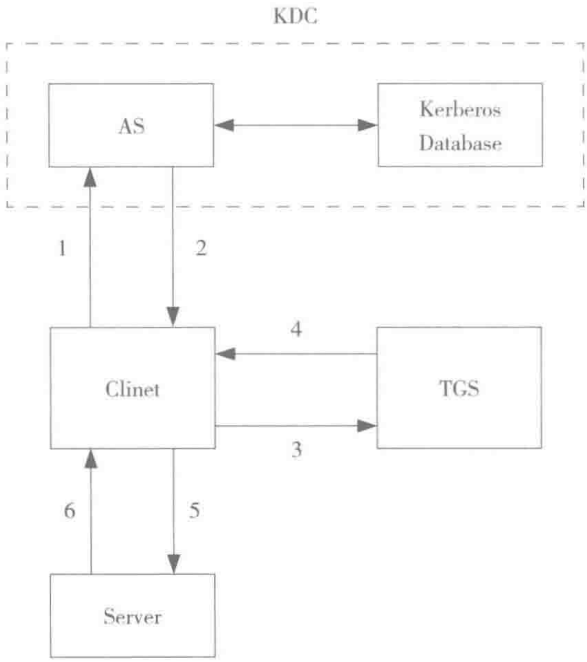

图1.4 Kerberos认证模型

Kerberos中有两种证书：票据（Ticket）和认证符（Authenticator），这两种证书都需要加密，但加密的密钥不同。

Ticket用来安全地传递用户的身份，同时保证使用Ticket的用户必须是Ticket中指定的用户。Ticket由以下内容组成：C/S标识符、Client的地址、时间戳、生存时间和会话密钥。Ticket一旦生成，在life指定时间内可以被Client多次使用，向申请同一个Server的服务。

Authenticator将提供信息与Ticket中的信息进行比较，一起保证发出Ticket的用户就是Ticket中指定的用户。认证符由Client的名字、Client的地址、记录当前时间的时间戳组成。认证符在一次服务请求中使用，每当Client向Server申请服务时，必须重新生成认证。

Kerberos认证过程包括3个阶段，即认证服务交换，票据许可服务交换和用户/服务器鉴别。需要分步完成。

第一阶段：认证服务交换（获得与票据许可服务器TGS通信的票据）。认证服务交换发生在客户和Kerberos认证服务器之间，通常是由一个未持有任何证书（Credentials）的客户发起的。这种交换典型地应用在初始登录会话阶段，以获得一个票据服务器的证书，把此阶段获得的证书里的票据称为TGT（Ticket Granting Ticket）。

用户将自己的名字输入系统，注册程序会自动发起该请求。用户的请求信息包括用户名和TGS服务器的名字，该请求以明文的形式发送过去。