第3章

PKI/PMI技术及应用

随着公钥密钥技术在网络安全领域的应用，以提供身份认证、数据完整性和消息保密性等安全服务为核心的公钥基础设施(Public Key Infrastructure，PKI)已成为在开放网络环境中为各类应用系统提供安全支撑的重要技术，而基于角色的访问控制(Role Based Access Control，RBAC)技术是在PKI的基础上发展起来的授权管理基础设施(Privilege Management Infrastructure，PMI)，为网络环境中的各类应用提供了统一的授权管理和访问控制策略与机制。概括地讲，PKI证明用户是谁，而PMI证明这个用户有什么权限，能做什么，而且PMI需要PKI为其提供身份认证。本章在第2章的基础上，将系统介绍PKI和PMI的基本概念、功能和应用特点，使读者更加深入地掌握系统安全的相关技术和方法。

3.1 PKI概述


视频讲解

PKI是在公开密钥的理论和技术基础上发展起来的安全技术，它是一个为用户提供数据加密、数字签名等安全应用中所需要的密钥和证书的综合基础平台，是信息安全基础设施的一个重要组成部分。

3.1.1 PKI的概念

公钥基础设施(PKI)是利用密码学中的公钥概念和加密技术为网上通信提供的符合标准的一整套安全基础平台。PKI能为各种不同安全需求的用户提供各种不同的网上安全服务所需要的密钥和证书，这些安全服务主要包括身份识别与鉴别(认证)、数据保密性、数据完整性、不可否认性及时间戳服务等，从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的。利用PKI可以方便地建立和维护一个可信的网络应用环境，从而使得人们在这个无法直接相互面对的环境里，能够确认彼此的身份和所交换的信息，能够安全地从事各种活动。

PKI 的技术基础之一是公开密钥机制。因为在公开密钥机制中加密密钥和解密密钥各不相同，信息的发送者利用接收者的公开密钥对信息进行加密，接收者再利用自己的私有密钥进行解密。这种方式既保证了信息的机密性，又能保证信息的不可抵赖性。

PKI 的技术基础之二是加密机制。在 PKI 中，所有在网络中传输的信息都是经过加密处理的。为此，加密算法的可靠性决定了 PKI 系统的可靠性，加密系统的效率决定了 PKI 系统的效率。

因此，从技术上讲，PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础，从技术上解决网上身份认证、信息完整性和不可抵赖等安全问题，为网络应用提供可靠的安全保障。然而，PKI 绝不只涉及技术层面的问题，还涉及电子政务、电子商务以及国家信息化的基础设施，是相关技术、应用、组织、规范和法律的总和，是一个综合各方面因素的宏观体系。

3.1.2 PKI 与网络安全

随着以计算机网络为基础的现代信息技术的发展，电子政务、电子商务等网上电子业务已被人们所接受，并得到不断普及。在网上电子业务的活动中，一方面需要确认双方的合法身份，防止出现虚假身份；另一方面必须保证业务信息的安全性，防止信息被窃取。同时，一旦发生纠纷，必须能够提供充足的证据以供仲裁。所以，要推动电子业务活动的正常运行，就必须从技术上实现身份认证和安全传输，保证服务的权威性、不可否认性和数据的完整性。

在网上电子业务活动中需要确定可依赖的身份，因为仅拥有一对公钥和私钥是不足以确立一个可依赖的身份认证的。如果要在计算机网络中创建一个与传统纸上交易等效的环境，还需要一套公钥基础设施的支持，具体要求如下。

(1) 安全策略，以规定加密系统在何种规则下运行。

(2) 产生、存储、管理密钥的产品。

(3) 如何产生、分发、使用密钥和证书的一整套过程。

PKI 提供了一个安全框架，使各类构件、应用、策略组合起来为网络环境中的相关活动提供以下安全功能。

(1) 保密性。保证信息的私有性。

(2) 完整性。保证信息没有被篡改。

(3) 真实性。证明一个人或一个应用的身份。

(4) 不可否认性。保证信息不能被否认。

在实现方式上，PKI 支持 SSL、IP over VPN、S/MIME 等协议，这使得 PKI 可以支持 Web 加密、VPN、安全邮件等应用。而且，PKI 支持不同认证机构间的交叉认证，并能实现证书、密钥对的自动更换。一个完整的 PKI 产品除主要功能外，还包括交叉认证、支持轻型目录访问协议(Lightweight Directory Access Protocol，LDAP)、支持用于认证的智能卡等功能。基于 PKI 技术的 IPSec 协议现在已经成为架构 VPN 的基础，可以为路由器之间、防火墙之间或路由器和防火墙之间提供经过加密和认证的通信。另外，安全电子邮件协议(S/MIME)也采用了 PKI 数字签名技术并支持消息和附件的加密，收发双方无须共享相同

密钥。同时,在网络资源的安全访问、身份认证等系统中,PKI 提供了所需的安全支撑。

PKI 机制的主要思想是通过公钥证书对某些行为进行授权,其目标是可以根据管理者的安全策略建立起一个分布式的安全体系。PKI 的核心是要解决网络环境中的信任问题,确定网络环境中行为主体(包括个人和组织)身份的唯一性、真实性和合法性,保护行为主体合法的安全利益。

作为提供信息安全服务的公共基础设施,PKI 已成为世界各国共同采用的最佳的安全体系。在我国,已在金融、政府、电信等部门建立了大量的 PKI 认证服务中心,在此基础上正在加强系统之间、部门之间以及国家之间 PKI 体系的互联互通,提供更广泛、更权威的网络安全认证服务。

3.1.3 PKI 的组成

一个典型的 PKI 组成如图 3-1 所示,其中包括 PKI 安全策略、软硬件系统、认证机构(Certificate Authority,CA)、注册机构(Registration Authority,RA)、证书发布系统和 PKI 应用等。

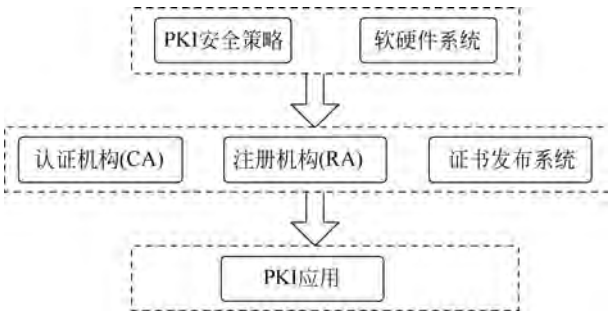

图 3-1 PKI 的组成示意图

1. PKI 安全策略

PKI 安全策略创建并定义了一个用于实施信息安全的策略,同时也定义了密码系统的使用方法和原则。一般情况下,在 PKI 中有两种类型的策略:一是证书策略,用于管理证书的使用,如确认某一 CA 是在 Internet 上的公有 CA 还是某一企业内部的私有 CA;另一种是认证操作管理规范(Certificate Practice Statement,CPS)。一些由商业证书发放机构或可信任的第三方管理的 PKI 系统需要 CPS。PKI 安全策略包括:

(1) CA 的创建和运作方式;

(2) 证书的申请、发行、接收和废除方式;

(3) 密钥的产生、申请、存储和使用方式。

2. 认证机构

认证机构(CA)也称为“认证中心”,它是 PKI 的信任基础,它管理公钥的整个生命周期,其作用包括发放证书、规定证书的有效期和通过发布证书废除列表(Certificate Revocation List,CRL)确保必要时可以废除证书。CA 必须是各行业、各部门及公众共同信任的、认可的、权威的、不参与交易的第三方网上身份认证机构。CA 制定了一些规则,这些

规则可以使申请和使用证书的用户确信该 CA 是可以依赖的。描述 CA 在各方面受约束的情况及运作方式的规则都被定义在 CPS 这一文件中，CPS 最初是由美国律师协会在其数字签名指南(Digital Signature Guidelines)中提出来的。管理证书的 CA 必须将其认证操作管理规范在用户申请证书时以方便用户查阅的方式提供给用户，由用户确定是否需要在该 CA 申请数字证书。如果一个 CA 没有 CPS，那么人们就很可能怀疑该 CA 的真实性，并降低对该 CA 所颁发的数字证书的信任程度。本章随后将对 CA 进行详细介绍。

3. 注册机构

注册机构(RA)提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。RA 主要完成收集用户信息和确认用户身份的功能。这里的用户，是指向 CA 申请数字证书的客户，可以是个人、组织或政府机构等。注册管理一般由一个独立的 RA 承担。它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 向其签发数字证书。

需要说明的是，RA 并不向用户签发证书，而只是对用户进行资格审查。因此，RA 可以设置在直接面对客户的业务部门，如银行的营业部、机构认证部门等。当然，对于一个规模较小的 PKI 应用系统，注册管理的职能可以由认证中心 CA 来完成，而不设立独立运行的 RA。但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。PKI 国际标准推荐由一个独立的 RA 完成注册管理的任务，以增强应用系统的安全性。

4. 证书发布系统

证书发布系统负责证书的发放。目前一般要求证书发布系统以 Web 方式与 Internet 用户交互，用于处理在线证书业务，方便用户对证书进行申请、下载、查询、注销、恢复等操作。

5. PKI 应用

PKI 的应用非常广泛，包括在 Web 服务器和浏览器之间的通信、电子邮件、电子数据交换(Electronic Data Interchange，EDI)、在 Internet 上的信用卡交易和虚拟私有网(VPN)等。同时，随着以 Internet 为主的计算机网络的发展，新的 PKI 的应用也在不断出现和发展。

另外，为了为应用程序提供 PKI 服务，在 PKI 系统的组成中还应有“PKI 应用接口”。PKI 应用接口是通过 PKI 的协议标准规范 PKI 系统各部分之间相互通信的格式和步骤。而应用程序接口(API)则定义了如何使用这些协议，并为上层应用提供 PKI 服务。当应用程序需要使用 PKI 服务，如获取某一用户的公钥、请求证书撤销信息或请求证书时，将会用到 API。目前 API 没有统一的国际标准，大部分都是操作系统或某一公司产品的扩展，并在其产品应用的框架内提供 PKI 服务。

一个简单的 PKI 系统包括 CA、RA 和相应的 PKI 存储库。CA 用于签发并管理证书；RA 可作为 CA 的一部分，也可以独立，其功能包括个人身份审核、CRL 管理、密钥产生和密钥对备份等；PKI 存储库包括 LDAP 目录服务器和普通数据库，用于对用户申请信息、证书、密钥、CRL 和日志等信息进行存储和管理，并提供一定的查询功能。

3.2 认证机构

PKI 系统的关键是如何实现对密钥的安全管理。公开密钥机制涉及公钥和私钥，私钥由用户自己保存，而公钥在一定范围内是公开的，需要通过网络传输。所以，公开密钥机制

的密钥管理主要是对公钥的管理，目前较好的解决方法是采用大家共同信任的认证机构(CA)。

3.2.1 CA的概念

认证机构(CA)是整个网上电子交易等安全活动的关键环节，主要负责产生、分配并管理所有参与网上安全活动的实体所需的数字证书。在公开密钥体制中，数字证书是一种存储和管理密钥的文件。它是一种采用特定格式的具有权威性的电子文档，其主要作用是证明证书中列出的用户名称与证书中列出的公开密钥相对应，并且所有信息都是合法的。如果要验证其合法性，就必须要有一个可信任的主体对用户的证书进行公证，证明主体的身份以及与公钥之间的对应关系，CA便是这样一个能够管理和提供相关证明的机构。

CA是一个具有权威性、可信赖性和公正性的第三方信任机构，专门解决公开密钥机制中公钥的合法性问题。CA是整个PKI系统的核心，负责发放和管理数字证书，其功能类似于办理居民身份证、护照等证件的发证机关。在PKI系统中，CA采用公开密钥机制，专门提供网络身份认证服务，负责签发和管理数字证书。同时，在证书发布后CA还负责对证书的撤销、更新、归档等管理。

由此可见，CA是保证电子商务、电子政务、网上银行、网上证券等安全交易的权威的、可信任的和公正的第三方机构，是PKI系统的核心。

从证书管理的角度来看，每一个CA的功能是有限的，需要按照上级策略认证机构制定的策略，负责具体的用户公钥证书的签发、生成和发布，以及CRL的生成和发布等职能。CA的主要职能如下。

(1) 制定并发布本地CA策略。但本地CA策略只能是对上级CA策略的补充，而不能违背。

(2) 对下属各成员进行身份认证和鉴别。

(3) 发布本地CA的证书，或代替上级CA发布证书。

(4) 产生和管理下属成员证书。

(5) 证实RA的证书申请，向RA返回证书制作的确认信息，或返回已制作好的证书。

(6) 接收和认证对它所签发的证书的撤销申请。

(7) 产生和发布它所签发的证书和CRL。

(8) 保存证书信息、CRL信息、审计信息和它所制定的策略。

3.2.2 CA的组成

一个典型CA系统包括安全服务器、CA服务器、注册机构(RA)、LDAP服务器和数据库服务器等，如图3-2所示。

1. 安全服务器

安全服务器是面向证书用户的提供安全策略管理的服务器，该服务器主要用于提供证书申请、浏览、证书撤销列表(CRL)以及证书下载等安全服务。作为CA系统的安全保障，用户与安全服务器之间的通信一般采取SSL加密方式，但不需要对用户进行身份认证。

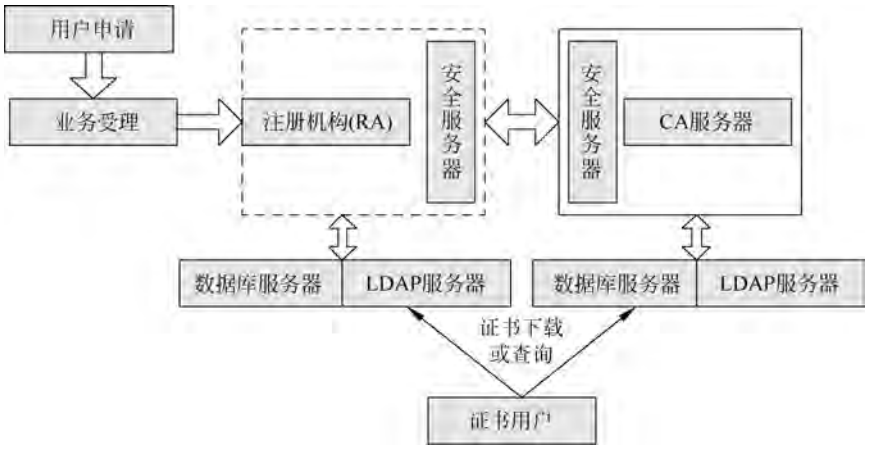

图 3-2 典型 CA 的组成

当 CA 颁发了证书后，该证书首先交给安全服务器。用户一般从安全服务器上获得证书，然后用户与各类服务器之间的所有通信，包括用户填写的申请信息以及浏览器生成的公钥均以安全服务器的密钥进行加密传输，只有安全服务器利用自己的私钥解密才能得到明文，这样可以防止其他人通过窃听得到明文，从而保证了证书申请和传输过程中信息的安全性。

2. CA 服务器

CA 服务器是整个认证机构的核心，负责证书的签发。CA 首先产生自身的私钥和公钥（密钥长度至少为 1024 位），然后生成数字证书，并且将数字证书传输给安全服务器。CA 还负责为操作员、安全服务器以及注册机构服务器生成数字证书。安全服务器的数字证书和私钥也需要通过安全方式传输给安全服务器。CA 服务器中存储有 CA 的私钥以及发行证书的脚本文件，出于安全的考虑，应将 CA 服务器与其他服务器隔离，确保认证机构的安全。

3. 注册机构

注册机构（RA）服务器面向注册机构的操作员，在 CA 体系结构中起着承上启下的作用：一方面向 CA 转发安全服务器传输过来的证书申请请求；另一方面向 LDAP 服务器和安全服务器转发 CA 颁发的数字证书和证书撤销列表。

4. LDAP 服务器

LDAP 服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入服务器。这样其他用户通过访问 LDAP 服务器就能够得到数字证书。

5. 数据库服务器

数据库服务器是认证机构中的关键组成部分，用于认证机构中数据（如密钥和用户信息等）、日志等统计信息的存储和管理。根据数据库技术和网络存储技术的发展，在实际应用中数据库系统应采取多种安全措施（如磁盘阵列、双机备份和分布式处理等），以维护数据库系统的安全性、稳定性、可伸缩性和高效性。

3.2.3 CA之间的信任关系

认证机构(CA)用于创建和发布证书,但一个CA一般仅为一个称为安全域(Security Domain)的有限群体发放证书。每个CA只覆盖一定的作用范围,不同的用户群体往往拥有各自不同的CA。在X.509规范中对于信任的定义是:如果实体A认为实体B会严格地按照A对它的期望那样行动,我们就说A信任B。信任关系是PKI系统中的重要组成部分,用来研究用户与CA的信任关系以及CA间的相互信任关系。

从实际应用来看,不同的组织或单位往往具有自己的PKI系统,而这些不同的PKI系统之间又需要建立彼此之间的联系。因此,解决单个PKI系统中用户与CA之间的信任问题,以及各个独立PKI系统间的交叉信任问题就显得尤为重要。

1. 单CA信任模型

如图3-3(a)所示,单CA信任模型是最基本的信任模型,也是目前许多组织或单位在Intranet中普遍使用的一种模型。在这种模型中,整个PKI系统只有一个CA,该CA为PKI中的所有终端用户签发和管理证书。PKI中的所有终端用户都信任这个CA。每个证书路径都起始于该CA的公钥,该CA的公钥成为PKI系统中唯一的用户信任节点。信任节点也称为"认证起点"或"信任锚"(Trust Anchor),它是整个PKI系统中CA的根。

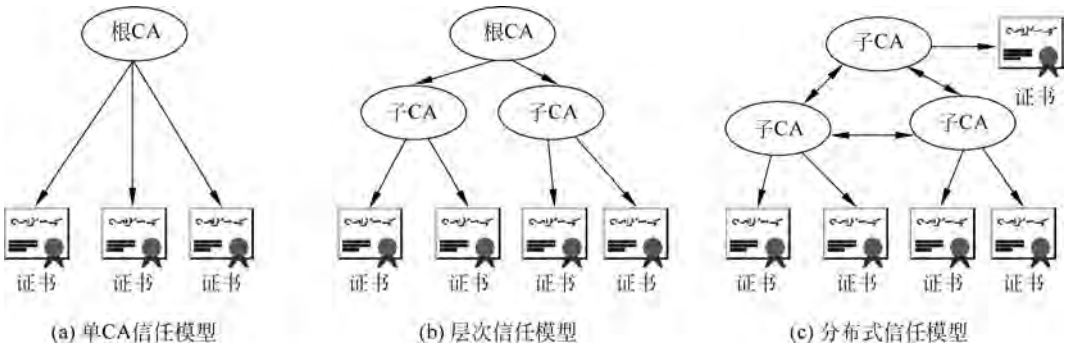

图3-3 单CA、层次和分布式信任模型

单CA信任模型的优点是容易实现,易于管理,只需要建立一个根CA,所有的用户都能实现相互认证;缺点是不易扩展,无法满足不同群体的用户需求。

2. 层次信任模型

层次信任模型也称为分级信任模型,它是一个以主从CA关系建立的分级PKI结构,具体结构如图3-3(b)所示。层次信任模型是典型的树状结构,树根为根CA,是整个PKI的信任锚,所有实体都信任它。树枝向下伸展,树叶在末端,代表申请和使用证书的终端用户。

作为信任锚,根CA通常不直接为终端用户颁发证书,而只为子CA颁发证书。在根CA下面可以存在多层子CA,子CA是所在实体集合的根。两个不同的终端用户进行交互时,双方都提供自己的证书和数字签名,通过根CA对证书进行有效性和真实性的认证。信任关系是单向的,即上级CA可以而且必须认证下级CA,而下级CA不能认证上级CA。

基于层次信任模型的PKI系统由于其简单的结构和单向的信任关系,具有以下优点。

(1) 增加新的子 CA 比较容易。新的子 CA 可以直接加到根 CA 下面,也可以加到某个子 CA 下面。这两种情况都很方便,容易实现。

(2) 证书路径由于其单向性,所以容易扩展,可生成从终端用户证书到信任锚的简单明确的路径。

(3) 证书短小、简单,因为用户可以根据 CA 在 PKI 中的位置来确定证书的用途。

层次信任模型也具有其缺点(整个 PKI 系统信任单个根 CA 是导致这些缺点的根源)。

(1) 单个 CA 的失败会影响整个 PKI 系统。与根 CA 的距离越短,则造成的影响越大。另外,由于所有的信任都集中在根 CA,一旦根 CA 出现故障,将导致整个 PKI 系统瘫痪。

(2) 创建一个所有国家、地区、组织或单位都信任的根 CA 存在很多困难。

3. 分布式信任模型

分布式信任模型也称为网状信任模型,在这种模型中 CA 间存在着交叉认证,如图 3-3(c)所示。如果任何两个 CA 间都存在着交叉认证,则这种模型就成为严格的网状信任模型。与在 PKI 系统中的所有实体都信任唯一根 CA 的层次信任模型相反,网状信任模型把信任分散到两个或更多个 CA 上。分布式信任模型的优点如下。

(1) 具有更好的灵活性。因为存在多个信任锚,所以单个 CA 安全性的削弱不会影响到整个 PKI 系统。

(2) 增加新的 CA 更为容易。当一个组织想要整合各个独立开发的 PKI 系统时,这种信任方式是很有效的。

(3) 系统的安全性较高。

分布式信任模型的主要缺点是路径发现比较困难。从终端用户证书到信任锚建立证书的路径是不确定的,因为存在多种选择,使得路径发现比较困难。

4. 桥 CA 信任模型

桥 CA 信任模型也称为中心辐射式信任模型,它用来克服层次信任模型和分布式信任模型的缺点,并连接不同的 PKI 系统,如图 3-4 所示。

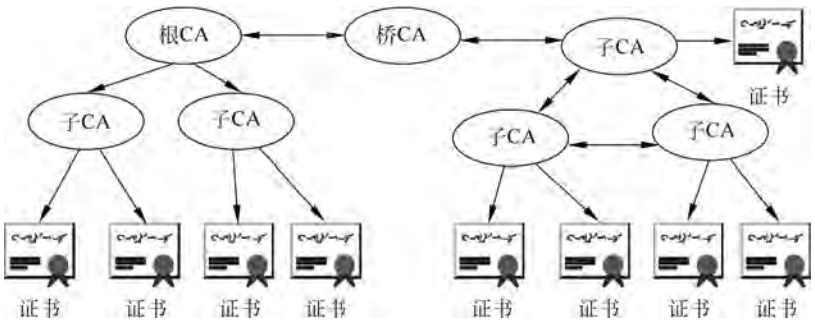

图 3-4 桥 CA 信任模型

不同于分布式信任模型中的 CA,桥 CA 与不同的信任域(子 CA)建立对等的信任关系,允许用户保持原有的信任锚。这些关系被结合起来形成信任桥,使得来自不同信任域的用户通过桥 CA 相互作用。其中,桥 CA 不是一个树状结构的 CA,也不像分布式信任模型中的 CA,它不直接向用户颁发证书。根 CA 是一个信任锚,而桥 CA 只是一个单独的 CA

而非信任锚。桥 CA 与不同的信任域之间建立对等的信任关系，允许用户保留自己的原始信任锚。

正如我们在网络中所使用的 Hub 一样，任何结构类型的 PKI 都可以通过桥 CA 连接在一起，实现彼此之间的信任，每一个单独的信任域都可以通过桥 CA 扩展到整个 PKI 系统中。桥 CA 信任模型的优点如下。

（1）实用性强。该模型非常符合目前证书管理机构的特点。

（2）证书路径较易发现，证书路径较短。桥 CA 架构的 PKI 比起具有相同数量 CA 分布式信任模型的 PKI 系统具有更短的可信任路径。

桥 CA 信任模型的缺点如下。

（1）证书路径的有效发现和确认仍然不很理想。因为基于桥 CA 模型的 PKI 系统可能包括部分的分布式信任模型。

（2）大型 PKI 目录的互操作仍不方便。

（3）证书复杂。在基于桥 CA 信任模型的 PKI 系统中，桥 CA 需要利用证书信息限制不同 PKI 的信任关系，这会导致证书的处理更为复杂。

（4）证书和证书状态信息不易获取。

5. Web 信任模型

Web 信任模型构建在 Web 浏览器的基础上，浏览器厂商在浏览器（如 Internet Explorer、Tencent Traveler、Mozilla Firefox、Opera 等）中内置了多个根 CA，每个根 CA 是相互平行的，浏览器用户同时信任多个根 CA 并把这些根 CA 作为自己的信任锚。以 Internet Explorer 为例，选择“工具→Internet 选项→内容→证书”，在打开的如图 3-5 所示的对话框中就会看到 Internet Explorer 的信任锚。

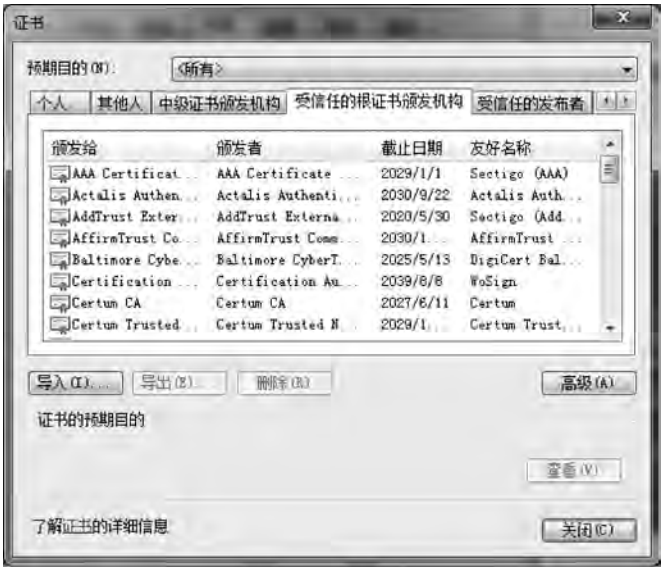

图 3-5　Internet Explorer 的信任锚

Web 信任模型表面上看起来与分布式信任模型非常相似，实际上它更接近层次信任模型。Web 信任模型通过与相关域进行互联而不是扩大现有的主体群来使用户实体成为在

浏览器中所给出的所有域的依托方，如图 3-6 所示。各个嵌入的根 CA（见图 3-5）直接内置在各个浏览器软件中，使用中这些根 CA 不会显示有关的信息。由于各个根 CA 是浏览器厂商内置的，浏览器厂商隐含认证了这些根 CA，这样浏览器厂商就成为事实上的隐含的根 CA。

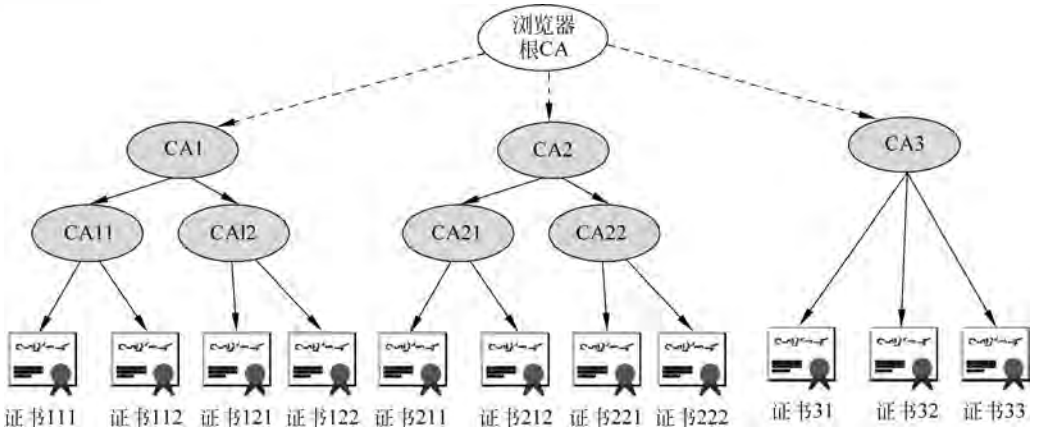

图 3-6　Web 信任模型

Web 信任模型的优点为：方便简单，操作性强，对终端用户的要求较低。用户只需要简单地信任嵌入的各个根 CA 即可，尤其适合目前在 Internet 和 Intranet 中的应用。

Web 信任模型的缺点如下。

（1）安全性较差。如果这些根 CA 中有一个存在安全问题，即使其他根 CA 仍然值得用户信赖，安全性也将被破坏。目前还没有有效可行的机制撤销嵌入浏览器中的根 CA（即密钥）。用户也难以查出到底哪一个根 CA 存在安全问题，这一切都依赖于浏览器厂商。

（2）根 CA 与终端用户信任关系模糊。终端用户与嵌入的根 CA 间交互十分困难。终端用户可在不同的站点得到不同的浏览器，用户很难知道某个浏览器中嵌入了哪些根 CA，并且用户一般不可能对证书颁发有足够的了解以至于与 CA 直接接触。同样，嵌入的根 CA 也无法知道和确定它的依托方是谁。

（3）根 CA 预先安装，难以扩展。

6. 以用户为中心的信任模型

在以用户为中心的信任模型中，每个用户都直接决定信赖哪个证书和拒绝哪个证书。没有可信的第三方作为 CA，终端用户就是自己的根 CA，如图 3-7 所示。

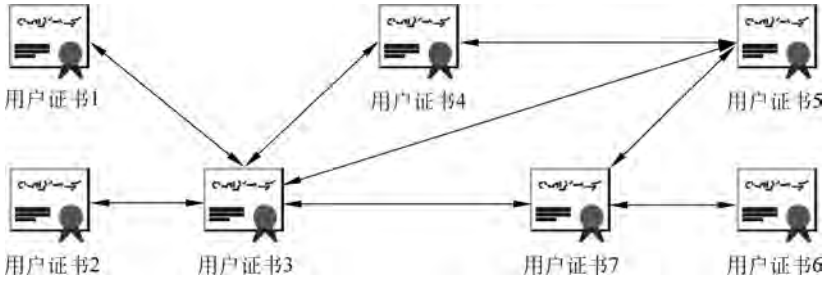

图 3-7　以用户为中心的信任模型

以用户为中心的信任模型的优点如下。

(1) 安全性很强。

(2) 用户可控性很强。用户可自己决定是否信赖某个证书。也就是说,每个用户可以直接和独立地决定信赖哪个证书和拒绝哪个证书。

以用户为中心的信任模型的缺点如下。

(1) 使用范围较窄。由于普通用户很少关心安全方面的问题,也缺乏相应的安全知识,将发放和管理证书的任务交给用户在许多应用中是不现实的。

(2) 这种信任模型在某些企业、金融机构或政府机关的网络环境中是不适用的。因为在这些群体中,往往需要以组织的方式控制一些公钥,而不希望完全由用户自己控制。

表 3-1 对前面介绍的各种 CA 信任模型的特点进行了描述。

表 3-1 各种 CA 信任模型的性能说明

信任模型	实用性	方便性	可扩展性	安全性	高效性	灵活性	互操作性	应用范围
单 CA	低	高	高	高	高	低	低	窄
层次	中	高	高	高	高	低	高	窄
分布式	中	低	低	高	低	高	高	广
桥 CA	高	低	高	高	低	高	高	广
Web	低	高	低	低	高	低	低	窄
以用户为中心	中	低	低	高	低	低	高	窄

3.2.4 密钥管理

密钥管理也是 PKI 系统(主要指 CA)中的一个核心问题。密钥管理主要是指密钥对的安全管理,包括密钥产生、密钥备份、密钥恢复和密钥更新等。

1. 密钥产生

密钥对的产生是证书申请过程中重要的一步,其中产生的私钥由用户保留,公钥和其他信息则交由 CA 中心进行签名,从而产生证书。根据证书类型和应用的不同,密钥对的产生也有不同的形式和方法。对于普通用户证书,一般由浏览器或固定的终端应用程序产生,这样产生的密钥强度较低,不适用于安全要求较高的领域。而对于比较重要的证书,如机构证书(CA 证书、RA 证书)等,密钥对一般由专用应用程序或 CA 中心直接产生,这样产生的密钥强度高,适合重要的应用场合。

另外,根据密钥对应用场合的不同,也可能有不同的产生方式。例如,签名密钥可能在客户端或 RA 中心产生,而加密密钥则需要在 CA 中心直接产生。

2. 密钥备份和恢复

在一个 PKI 系统中,对密钥对的安全管理非常重要,其中备份是最常用到的一种方式。如果没有安全保障,当密钥丢失后,将意味着使用该密钥加密的数据无法打开,对于一些重要数据,这将是灾难性的事故。所以,密钥的备份和恢复也是 PKI 系统中非常重要的一个

安全环节。在部署和使用 PKI 系统时，PKI 系统的提供者必须确保即使密钥丢失，受密钥加密保护的重要信息也必须能够恢复。

企业级的 PKI 系统至少应该提供对加密的安全密钥的存储、备份和恢复。密钥一般用口令进行保护，而口令丢失则是管理员最常见的安全疏漏之一。所以，PKI 系统应该能够备份密钥，即使口令丢失，它也能够让用户在一定条件下恢复该密钥，并设置新的口令。

另外，使用 PKI 系统的企业也应该考虑所使用密钥的生命周期，它包括密钥和证书的有效时间以及已撤销密钥和证书的归档等。

3. 密钥更新

每一个由 CA 颁发的证书都会存在有效期，密钥对生命周期的长短由签发证书的 CA 中心来确定，每一个 CA 系统所颁发的证书的有效期限有所不同，一般大约为 2～3 年。当用户的私钥被泄露或证书的有效期快到时，用户应该更新私钥。

3.3 证书及管理

PKI 采用证书管理公钥，通过第三方的可信任机构 CA 把用户的公钥和用户的其他标识信息捆绑在一起，在 Internet 或 Intranet 上验证用户的身份。数字证书的管理方式在 PKI 系统中起着关键作用。

3.3.1 证书的概念

数字证书也称为数字标识（Digital Certificate，或 Digital ID）。它提供了一种在 Internet 等公共网络中进行身份验证的方式，是用来标识和证明网络通信双方身份的数字信息文件，其功能与驾驶员的驾照或日常生活中的身份证相似。数字证书由一个权威的证书认证机构（CA）发行，在网络中可以通过从 CA 中获得的数字证书来识别对方的身份。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。例如，在进行网上银行的相关操作时，必须安装与银行账号相对应的数字证书，否则系统是无法完成相关操作的。目前，银行等单位为用户提供的数字证书文件既可以安装在用户的计算机中，也可以保存在 U 盘等存储介质中。例如，在现在的公安专网中，每一个民警都有一个用于标识自己身份的 U 盘，在该 U 盘中保存了民警自己的数字证书，每个民警访问网络的权限都集中在该数字证书中。通俗地讲，数字证书就是个人或单位在 Internet 等公共网络上的身份证。

比较专业的数字证书的定义是：数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下，证书中还包括密钥的有效时间、发证机关（证书授权中心）的名称、该证书的序列号等信息，证书的格式遵循相关国际标准。

通过数字证书就可以使信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性这四大网络安全要素得到保障。

3.3.2 数字证书的格式

在 TCP/IP 网络环境中，应用程序使用的证书都来自不同的厂商或组织，为了实现可交互性，要求证书能够被不同的系统识别，符合一定的格式，并实现标准化。目前有 X.509、无线安全传输层（Wireless Transport Layer Security，WTLS）和优良保密协议（Pretty Good Privacy，PGP）等多种数字证书，但应用最为广泛的是 X.509，X.509 为数字证书及其 CRL 格式提供了一个标准。其中，WTLS 是无线应用协议（Wireless Application Protocol，WAP）应用中提供数据安全传输的一种服务。PGP 是一系列采用公钥加密体制、用于消息加密与验证的应用程序。

需要说明的是，X.509 本身不是 Internet 标准，而是国际电信联盟（International Telecommunication Union，ITU）的标准，它定义了一个开放的框架，并在一定范围内可以进行扩展。为了提供公用网络用户目录信息服务，ITU 于 1988 年制定了 X.500 系列标准。其中 X.500 和 X.509 是安全认证系统的核心，X.500 定义了一种区别命名规则，以类似互联网中 DNS 命名树确保用户名称的唯一性；而 X.509 则为 X.500 用户名称提供了通信实体鉴别机制，并规定了实体鉴别过程中广泛适用的证书语法和数据接口，X.509 称之为证书。

X.509 目前有 4 个版本：X.509 v1、v2、v3 和 v4。其中，X.509 v1 提供了基于 X.509 公钥证书的目录访问认证协议；1993 年，ITU 公布了 X.509 v2，其中增强了对目录访问控制和鉴别的支持。证书由用户公开密钥和用户标识符组成，此外还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称、证书有效期等信息，还定义了包含扩展信息的数字证书，该版数字证书提供了一个扩展信息字段，用来提供更多的灵活性及特殊应用环境下所需的信息传送；1997 年，国际标准化组织/国际电工委员会（International Organization for Standardization/International Electrotechnical Commission，ISO/IEC）[①]和 ANSI X9 开发了 X.509 v3，它是基于公开密钥证书的目录鉴别协议。v3 定义的公开密钥证书协议比 v2 证书协议增加了 14 项预留扩展域，如发证者或证书用户的身份标识、密钥标识、用户或公钥属性、策略（Policy）扩展等，同时 v3 对 CRL 结构也进行了扩展；X.509 v4（X.509-2000）于 2000 年推出，v4 在扩展了 v3 的同时，利用属性证书定义了特权管理基础设施（PMI）模型，即如何利用 PKI-CA 对用户访问进行授权管理。X.509 证书的通用格式如图 3-8 所示，每一个组成域的功能描述如下。

证书版本号(Version)
证书序列号(Serial Number)
签名算法标识符(Signature)
颁发机构名(Issuer)
有效期(Validity)
实体名称(Subject)
证书持有者的公开密钥信息(Subject Public Key Info)
颁发者唯一标识符(Issuer Unique Identifier)
证书持有者唯一标识符(Subject Unique Identifier)
签名值(Issuer's Signature)

图 3-8 X.509 数字证书的基本格式

（1）证书版本号（Version）。版本号指明 X.509 证书的格式版本。0 表示 X.509 v1 标准，1 表示 X.509 v2 标准，以此类推。目前最新的版本为 X.509 v4。

① 1947 年，当 ISO 成立后，IEC 曾并入 ISO。从 1976 年开始，ISO 和 IEC 成为法律上独立的两个组织，其中 IEC 负责有关电工、电子领域的国际标准化工作，其他领域由 ISO 负责。

(2) 证书序列号(Serial Number)。序列号指定由 CA 分配给证书的唯一数字型标识符。当证书被取消时,实际上是将此证书的序列号放入由 CA 签发的 CRL 中,这也是序列号唯一的原因。

(3) 签名算法标识符(Signature)。签名算法标识用来指定由 CA 签发证书时所使用的签名算法。算法标识符用来指定 CA 签发证书时所使用的公开密钥算法和 Hash 算法,须向国际知名标准组织(如 ISO)注册。

(4) 颁发机构名(Issuer)。此域用来标识签发证书的 CA 的 X.500 DN(Distinguished Name)名字,包括国家、省市、地区、组织机构、单位部门和通用名。其中,DN 是类似于 DNS 的名称服务方式,在 LDAP 中目录记录的标识名称为 DN,用来读取某个条目。

(5) 有效期(Validity)。指定证书的有效期,包括证书开始生效的日期和时间,以及失效的日期和时间。每次使用证书时,需要检查证书是否在有效期内。

(6) 实体名称(Subject)。指定证书持有者的 X.500 唯一名字,包括国家、省市、地区、组织机构、单位部门和通用名,还可包含 E-mail 地址等个人信息。

(7) 证书持有者的公开密钥信息(Subject Public Key Info)。证书持有者公开密钥信息域包含两个重要信息:证书持有者的公开密钥的值和公开密钥使用的算法标识符。此标识符包含公开密钥算法和 Hash 算法。

(8) 颁发者唯一标识符(Issuer Unique Identifier)。颁发者唯一标识符在 v2 中开始加入。此域用在当同一个 X.500 名字用于多个认证机构时,用 1b 字符唯一标识颁发者的 X.500 名字。该域为一个可选项。

(9) 证书持有者唯一标识符(Subject Unique Identifier)。证书持有者唯一标识符在 v2 中开始加入。此域用在当同一个 X.500 名字用于多个证书持有者时,用 1b 字符唯一标识证书持有者的 X.500 名字。该域为一个可选项。

(10) 签名值(Issuer's Signature)。证书颁发机构对证书上述内容的签名值。

3.3.3 证书申请和发放

证书的申请一般有两种方式:在线申请和离线申请。其中,在线申请就是用户登录认证机构的相关网站下载申请表格,然后按要求填写内容;或通过浏览器、电子邮件等在线方式申请证书,这种方式一般用于申请普通用户证书。离线方式一般通过人工的方式直接到认证机构证书受理点办理证书申请手续,通过审核后获取证书,这种方式一般用于比较重要的场合,如网上银行的在线支付证书等。下面主要以在线申请方式为例进行介绍,申请的步骤如下。

(1) 用户申请。用户使用浏览器通过 Internet 或 Intranet 访问安全服务器,下载 CA 的数字证书,该证书称为根证书。然后在证书的申请过程中使用 SSL 安全方式与服务器建立连接,用户填写个人信息,浏览器生成私钥和公钥对,将私钥保存在客户端的特定文件中,并且要求用口令保护私钥,同时将公钥和个人信息提交给安全服务器。安全服务器将用户的申请信息传送给注册机构服务器。

(2) 注册机构(RA)审核。用户与注册机构人员联系,证明自己身份的真实性,或者请求代理人与注册机构联系。注册机构操作员利用自己的浏览器与注册机构服务器建立 SSL 安全通信,该服务器需要对操作员进行严格的身份认证,包括操作员的数字证书、IP 地址

等。操作员首先查看目前系统中的申请人员，从列表中找出相应的用户，单击用户名，核对用户信息，并且可以进行适当的修改。如果操作人员同意用户的申请证书请求，必须对证书申请信息进行数字签名。操作员也有权利拒绝用户的申请。操作员与服务器之间的所有通信都采用加密和签名方式，具有安全性、抗抵赖性，保证了系统的安全性和有效性。

(3) CA 发放证书。注册机构(RA)向 CA 传输用户的证书申请与操作员的数字签名，CA 操作员查看用户的详细信息，并且验证操作员的数字签名，如果签名验证通过，则同意用户的证书请求，发放该证书。然后 CA 将证书输出。如果 CA 操作员发现签名不正确，则拒绝证书申请。CA 发放的数字证书中包含的内容如图 3-8 所示。

(4) 注册机构证书转发。注册机构(RA)操作员从 CA 服务器得到新的证书，首先将证书输出到 LDAP 服务器以提供目录浏览服务，最后操作员向用户发送一封电子邮件，通知用户证书已经发布成功，并且把用户的证书序列号告诉用户，要求用户到指定的站点下载自己的数字证书。同时，在电子邮件中会告诉用户如何使用安全服务器上的 LDAP 配置、修改浏览器的客户端配置文件以便访问 LDAP 服务器、获得他人的数字证书等。

(5) 用户获取证书。一般情况下，利用在线方式申请证书后，用户需要使用申请证书时的计算机上的浏览器到指定的站点下载由注册机构转发的证书。需要输入用户的证书序列号。服务器要求用户必须使用申请证书时的浏览器，因为浏览器需要用该证书相应的私钥去验证数字证书。只有保存了相应私钥的浏览器才能成功下载用户的数字证书。

这时用户打开浏览器的安全属性(见图 3-5)，就可以发现自己已经拥有了 CA 颁发的数字证书。然后，可以利用该数字证书与其他人或拥有相同 CA 颁发证书的应用系统使用加密、数字签名方式进行安全通信。

3.3.4 证书撤销

在证书的有效期内，由于私钥丢失或证书持有者解除了与某一组织或单位的关系，该用户所使用的数字证书需要撤销。证书的撤销操作由 CA 完成，当 CA 接收到用户撤销证书的申请时，立即执行证书撤销操作，同时通知用户证书的撤销情况。其实，出于安全考虑，在证书的正常使用中，当用户每次使用证书时系统都要检查用户的证书是否合法和有效。

证书的撤销一般通过两种方式实现：一种是利用周期性发布机制，主要有证书撤销列表(CRL)；另一种是利用在线查询机制，如在线证书状态协议(Online Certificate Status Protocol，OCSP)。下面分别进行介绍。

1. 利用 CRL 撤销证书

证书撤销列表(CRL，又称证书黑名单)为应用程序和其他系统提供了一种检验证书有效性的方式。任何一个证书撤销以后，认证机构 CA 会通过发布 CRL 的方式来通知各个相关方。X.509 中 CRL 所包含的主要内容格式如下，结构如图 3-9 所示。

(1) 证书版本号。CRL 的版本号，0 表示 X.509 v1 标准，1 表示 X.509 v2 标准，以此类推。目前最新的版本为 X.509 v4。

(2) 签名算法。包含算法标识和算法参数，用于指定证书签发机构用来对 CRL 内容进行签名的算法。

图 3-9 证书撤销列表

(3) 证书签发机构名。签发机构的 DN 名,由国家、省市、地区、组织机构、单位部门和通用名等组成。

(4) 本次签发时间。本次 CRL 签发时间,遵循 ITU-T X.509 v2 标准,CA 在 2049 年之前把这个域编码为 UTCTime 类型,在 2050 或 2050 年之后把这个域编码为 GeneralizedTime 类型。

(5) 下次签发时间。下次 CRL 签发时间,遵循 ITU-T X.509 v2 标准,CA 在 2049 年之前把这个域编码为 UTCTime 类型,在 2050 年或 2050 年之后把这个域编码为 GeneralizedTime 类型。

(6) 用户公钥信息。其中包括撤销的证书序列号和证书撤销时间。撤销的证书序列号是指要撤销的由同一个 CA 签发的证书的唯一标识号,同一机构签发的证书不会有相同的序列号。

(7) 签名算法。对 CRL 内容进行签名的签名算法。

(8) 签名值。证书签发机构对 CRL 内容的签名值。

另外,CRL 中还包含扩展域和条目扩展域。CRL 扩展域用于提供与 CRL 有关的额外信息,允许团体和组织定义私有的 CRL 扩展域传送他们独有的信息;CRL 条目扩展域则提供与 CRL 条目有关的额外信息,允许团体和组织定义私有的 CRL 条目扩展域传送他们独有的信息。

基于 CRL 的周期发布证书状态信息机制主要有以下优点。

(1) 证书撤销列表的安全性是通过 CA 中心(或 CA 授权的机构)签名保证的,所以证书存储的地址并没有受到严格的控制,这样就可以根据需要在适当的地方存储需要的 CRL。

(2) 在 CRL 中,包含一个本列表的颁发日期,以及下一次 CRL 的颁发时间。这两个属性可以帮助管理 CRL 缓冲区。如果证书的撤销频率不是很高,CRL 将会是一个有效的、有较好伸缩性的证书状态信息分发机制。

(3) 使用增量 CRL 机制,仅发布那些自某个基本 CRL 颁发以来新撤销的证书,这样减少了单个签名的信息量,同时增加了 CRL 的实时性并且提高了证书状态响应器(服务器)的应答时间。

在 PKI 系统中,CRL 是自动完成的,而且对用户是透明的。CRL 中并不存放撤销证书的全部内容,只存放证书的序列号,以便提高检索速率。CRL 产生的主要步骤如下。

(1) RA 建立与 CA 的连接,提出撤销申请。该申请中包括撤销证书的序列号和撤销理由。

(2) CA 将撤销证书的序列号签发到 CRL 中。

(3) 系统通过数据库或 LDAP 目录等方式发放新的 CRL,并且提供用户在线查询。

2. 利用 OCSP 撤销证书

尽管利用 CRL 撤销证书具有许多优点,但该方式本身固有的 CRL 存储位置分散、CRL 的更新无法准确统计、客户端程序比较复杂等缺点,致使基于 CRL 的证书撤销机制在实际应用中存在不足。

在线证书状态协议(OCSP)是 IETF 工作组颁布的用于检查数字证书在当前时刻是否有效的标准协议。该协议提供给用户一条便捷的证书状态查询通道,使 PKI 体系能够更有

效、更安全地应用于各个领域。OCSP 可以作为周期性 CRL 的一种替代机制或补充机制，它对于获得一个证书撤销状态的及时信息是必要的。与 CRL 相比，OCSP 对获得证书撤销信息的及时性更强，所以 OCSP 一般用于网上银行、网上证券、电子政务中的某些关键部门。

OCSP 协议是用于 OCSP 请求者(客户端)和 OCSP 响应器(服务器)之间的一个请求/响应协议。客户端生成一个 OCSP 请求，它包含一个或多个待查询证书的标识符，客户端可以选择性地对该请求进行数字签名。然后，客户端将请求发送给服务器。OCSP 响应器对收到的请求返回一个响应(出错信息或是确定的回复)。OCSP 响应器返回出错信息时，该响应不用签名。出错信息包括请求编码格式不正确、内部错误、稍后再试、请求需要签名、未授权等内容。OCSP 响应器返回确定的回复时，该响应必须进行数字签名。

OCSP 是一种相对简单的请求/响应协议，它使得客户端应用程序可以测定需要验证的证书状态。协议对 OCSP 请求者和 OCSP 响应器之间需要交换的数据进行了描述。一个 OCSP 请求包含以下数据：协议版本、服务请求、目标证书标识和可选的扩展项等。一个确定的响应由以下信息组成：版本号、响应器名称、对每一张被请求证书的回复、可选扩展项、签名算法、对象标识和签名等组成。

OCSP 机制的主要优点如下。

(1) 从 OCSP 响应器得到的信息总是能够反映该证书的真实状态。

(2) 与 CRL 相比，每一次证书查询需要处理的信息量要小得多，因为用户只关心当前查询的证书状态，而且客户端应用程序需要处理的返回信息也要少一些。

尽管 OCSP 有许多优点，但基于证书响应状态协议的机制也存在一些问题与不确定性。

(1) 证书状态响应器应该是一个可信的在线服务器，并为每一个请求提供及时的响应。而且，证书状态响应器不能完全替代 CRL 存储库，一定条件下仍然需要访问 CRL 存储库去查找证书。

(2) 证书状态响应器难以实现镜像，也难以备份，从而可能成为通信中的瓶颈。而且，在线响应系统的访问流量可能非常不均匀，从而使得服务器系统经常处于一种不稳定的状态，这样很容易受到拒绝服务(DoS)等攻击。

(3) 证书状态响应器必须生成大量的签名，以保证每次响应的真实性和有效性，同时也可能需要验证大量的签名，这些过程将降低服务器的性能，甚至可能出现由于请求等待时间过长而丢失请求信息的现象。

3.3.5 证书更新

在 PKI 系统中，每一份数字证书被颁发以后都有其生命周期。当证书超出了其有效期就被作废而要求更新。进行证书更新的主要原因如下：一是与证书相关的密钥可能达到它有效的生命终点；二是证书即将到期；三是证书中的一些属性发生了改变，而且必须进行改变。在这些情况下，必须颁发一个新的证书，称为证书更新或重新证明。根据证书应用对象的不同，证书更新分为普通用户证书更新和机构证书更新两种类型。

1. 普通用户证书更新

普通用户证书一般是指由普通用户根据个人(包括组织或单位)需要所申请和使用的数字证书。普通用户证书更新一般有以下两种方式。

(1) 人工更新。用户向注册机构(RA)提出更新证书的申请,RA 根据用户申请信息更新用户的证书。

(2) 自动密钥更新。PKI 系统采用对管理员和用户透明的方式,对快要过期的证书进行自动更新,生成新的密钥对。

2. 机构证书更新

机构证书也是一种证书,只是这种证书专门用来证实机构(如 CA、RA)的真实性、合法性、可靠性以及可信任性。机构证书与普通用户证书一样,如果在有效期快到期时,就要进行更新并将更新消息告知所有的相关用户及机构。因此,这就需要一套完整的机制保证机构证书的顺利更新,从而保证整个系统的有效性和安全性。在一个 PKI 系统中,机构的类型分为各级 CA 机构及 RA 机构,因而机构证书的类型也相应地分为 RA 机构证书和 CA 机构证书。

当机构证书快到期时,就需要对它进行更新操作,以保证整个系统的安全性、稳定性和连续性。作为用户证书申请和签发的机构,其证书稳定性、连续性和安全性至关重要,它的更新操作与一般普通用户证书有很大的差别。普通用户证书在更新时,只需要向签发机构发出申请,由签发机构撤销旧的证书,并重新产生新的公私密钥对和颁发新的证书,用户证书就更新结束。相比之下,机构证书的更新就复杂得多,它分为根 CA 的更新和下级 CA 的更新。

为了保证系统的连续性,在机构证书更新期间,根 CA 就有多个证书存在。如下所示,根 CA 在更新期间,共有 3 类证书存在(其中 old 表示旧证书,new 表示新证书)。

(1) oldwithnew:表示用新证书签发的旧证书。

(2) newwithold:表示用旧证书签发的新证书。

(3) newwithnew:表示根 CA 自签发的新证书。

其中,oldwithnew 和 newwithold 证书是为了在证书更新期间保持证书认证的连续性,它们在根 CA 证书更新结束时要被全部撤销。oldwithnew 用于旧的用户证书的认证以及新旧用户证书的相互认证;newwithold 用于新旧证书的相互认证;newwithnew 用于新证书的认证和颁发新的下级证书。在根 CA 更新的同时,也需要用 newwithnew 对证书撤销列表进行操作,并生成新的证书链文件。

下级机构证书的撤销相对根 CA 而言就要简单些。下级机构证书快到期时,由下级机构向上级 CA 申请证书更新,上级 CA 通过为下级机构颁发新的证书并同时撤销旧的证书来达到下级机构证书的更新目的。但是,下级机构证书更新后,如果是 CA 机构,则要同时重签证书撤销列表并发布到证书目录服务器上,以供用户使用及认证使用。

需要说明的是,由于证书的不断更新,一段时间后同一个用户(或机构)可能存在多个“旧”证书,这一系列的“旧”证书形成了证书的历史档案,需要对其进行归档,并集中管理,以备需要时使用。

3.3.6 数字证书类型

随着电子商务、电子政务、网上银行等应用的快速发展，数字证书所提供的保密性、完整性、不可否认性等认证功能得到了发挥，数字证书无论从载体还是应用环境上都在发生着变化。

1. 数字证书的应用类型

目前，在互联网应用中使用的数字证书，根据应用功能和环境的不同主要分为以下 5 种类型，如图 3-10 所示。

图 3-10 常见的数字证书

1）机构证书

机构证书是符合 X.509 标准的数字证书，证书中包含使用者(单位)信息和使用者的公钥，用于标识证书持有者的身份，可以用于机构在网上银行系统、电子政务、电子商务等业务中。

2）机构员工证书

颁发给独立的机构员工，在网上证明机构中个人的身份，机构员工证书对外代表单位中具体的某一位员工，进行合法的电子签名。

3）个人证书

个人证书是符合 X.509 标准的数字证书，证书中包含个人身份信息和个人的公钥，用于标识证书持有人的个人身份，可以签名，也可以加密，用于个人在网上进行网银交易、个人安全电子邮件、合同签订、支付等活动中表明身份。

4）代码签名证书

代码签名证书为软件开发商提供的针对软件代码进行数字签名的证书，可以有效防止软件代码被篡改，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发商的版权利益。为了规范应用软件的管理，防止软件被篡改后重新封装上传，手机 App 应用软件在上

传到平台供用户下载之前一般都要利用数字证书进行签名。

5) SSL 服务器证书

SSL 服务器证书是遵守 SSL 协议的一种数字证书,由全球信任的证书颁发机构(CA)验证服务器身份后颁发。将 SSL 证书安装在网站服务器上,可实现网站身份验证和数据加密传输功能。它的主要应用功能如下。

(1) 实现加密传输。用户通过超文本传输协议(Hyper Text Transfer Protocol,HTTP)访问网站时,浏览器和服务器之间是明文传输,这就意味着用户填写的密码、账号、交易记录等机密信息都是明文,随时可能被泄露、窃取、篡改,被攻击者获取并利用。安装 SSL 证书后,使用超文本传输安全协议(Hyper Text Transfer Protocol over Secure Socket Layer,HTTPS)访问网站,可建立客户端浏览器到网站服务器之间的 SSL 加密通道(SSL 协议),实现加密传输,防止传输数据被泄露或篡改,确保信息在网上传输的安全。

(2) 认证网站真实身份。随着互联网的广泛运用,互联网上存在着许多假冒、钓鱼网站,让用户无法分辨真伪。网站部署全球信任的 SSL 证书后,浏览器内置安全机制,实时查验证书状态,通过浏览器向用户展示网站认证信息,让用户轻松识别网站真实身份,防止钓鱼网站仿冒。

2. 数字证书的应用示例

以电子邮件为例,数字证书在电子邮件中体现的主要作用如下。

(1) 保密性。通过使用收件人的数字证书对电子邮件加密,只有收件人才能阅读加密的邮件,这样保证在 Internet 上传递的电子邮件信息不会被他人窃取,即使发错邮件,收件人由于无法解密而不能看到邮件内容。

(2) 完整性。利用发件人数字证书在传送前对电子邮件进行数字签名不仅可以确定发件人身份,而且可以判断发送的信息在传递的过程中是否被篡改过。

(3) 身份认证。在 Internet 上传递电子邮件的双方互相不能见面,所以必须有办法确定对方的身份。利用发件人数字证书在传送前对电子邮件进行数字签名即可确定发件人身份,而不是他人冒充的。

(4) 不可否认性。发件人的数字证书只有发件人唯一拥有,故发件人利用其数字证书在传送前对电子邮件进行数字签名后,就无法否认发送过此电子邮件。


视频讲解

3.4 PMI 技术

授权管理基础设施(PMI)是国家信息安全基础设施的一个重要组成部分,目标是向用户和应用程序提供授权管理服务,提供用户身份到应用授权的映射功能,提供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授权和访问控制机制,简化具体应用系统的开发和维护。

3.4.1 PMI 的概念

PMI 是在 PKI 发展过程中为了将用户权限的管理与其公钥的管理分离,由 IETF 提出的一种标准。PKI 以公钥证书为基础,实现用户身份的统一管理,而 PMI 以 2000 年推出的

X.509 v4 标准中提出的属性证书为基础，实现用户权限的统一管理。

在过去的几年里，PKI 已成为电子商务、电子政务等网络应用中不可或缺的安全支撑系统。PKI 通过方便灵活的密钥和证书管理方式，提供了在线身份认证的有效手段，为访问控制、抗抵赖、保密性等安全机制在系统中的实施奠定了基础。随着网络应用的扩展和深入，仅仅能确定“他是谁”已经不能满足需要，安全系统要求提供一种手段，能够进一步确定“他能做什么”。为了解决这个问题，PMI 应运而生。就像现实生活中一样，网络世界中的每个用户也有各种属性，属性决定了用户的权限。PMI 的最终目标就是提供一种有效的体系结构来管理用户的属性。这包括两个方面的含义：首先，PMI 系统保证用户获取他们有权获取的信息、在他们的权限范围内进行相关操作；其次，PMI 应能提供跨应用、跨系统、跨企业、跨安全域的用户属性的管理和交互手段。

概括地讲，PMI 以资源管理为核心，对资源的访问控制权统一交由授权机构统一处理。与 PKI 相比，主要区别在于 PKI 证明用户是谁，而 PMI 证明这个用户有什么权限、能干什么。PMI 需要 PKI 为其提供身份认证。PMI 实际提出了一个新的信息保护基础设施，能够与 PKI 紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行系统的定义和描述，完整地提供授权服务所需过程。

3.4.2 PMI 的组成

PMI 与 PKI 不同，PKI 主要进行身份鉴别，证明用户身份。而 PMI 主要进行授权管理，证明用户有什么权限。PMI 主要由属性权威（Attribute Authority，AA）、属性证书（Attribute Certification，AC）和属性证书库 3 部分组成。

1. 属性权威

属性权威（AA）也称为“授权管理中心”或“属性权威机构”，是整个 PMI 系统的核心，它为不同的用户和机构进行属性证书（AC）创建、存储、签发和撤销，负责管理 AC 的整个生命周期。表面上，PMI 中的 AA 有一些类似于 PKI 中的 CA，但两者在逻辑上是完全独立的。PKI 中的 CA 主要用来管理用户的身份，而 PMI 中的 AA 主要管理用户的权限。另外，有可能在 PMI 建立之前 PKI 就已经存在。

图 3-11 所示的是 AA 的层次结构。其中，在该树状结构最顶端（树根）的是权威源（Source of Authority，SOA）。SOA 是授权管理的中心业务服务节点，所有的实体（包括 AA、终端用户等）都信任由 SOA 授予的部分或所有权利。在不存在授权委托的情况下，SOA 是 AC 的初始签发者，它将授权分配给授权持有者（如终端用户）。然而，如果存在着授权委托，SOA 可以授权给 AA，使得 AA 可以作为代理点，委托授权给其他实体。SOA 也可以对 AA 的权限委托施加一些限制（如限制路径长度等）。

在 AA 层次结构中，下一层 AA 的产生有两种情况：一种是上一层 AA 需要将某些相对独立的证书创建、颁发工作委托给一个子 AA；另外一种情况是某个已经存在的 AA 主动申请加入 PMI 系统中，并成为某一个 AA 的子节点。一般情况下，上一层 AA 充分了解自己的子节点 AA 和自己直接管理的终端用户的情况，而不一定充分了解子节点 AA 所负责管理的终端用户的情况。一般情况下，应用功能相近的终端用户可以在同一个 AA 下。

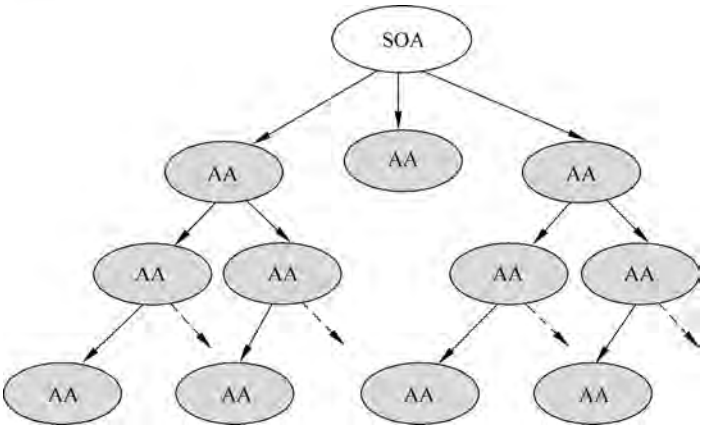

图 3-11　AA 的层次结构

2. 属性证书

属性证书(AC)是由 PMI 的权威机构(即属性权威,AA)签发的将实体与其享有的权限属性捆绑在一起的数据结构,权威机构的数字签名保证了绑定的有效性和合法性。AC 主要用于授权管理。

AC 建立在基于 PKI 公钥证书的身份认证基础上。PKI 中的公钥证书保证实体及其公钥的对应性,为数据完整性、实体认证、保密性、授权等安全机制提供身份服务。那么,为什么不直接用公钥证书加密属性而使用独立的 AC 呢? 首先,身份和属性的有效时间有很大差异。身份往往相对稳定,变化较少;而属性(如职务、职位、部门等)的变化较快。因此,属性证书的生命周期往往远低于用于标识身份的公钥证书。举例来说,公钥证书类似于居民身份证,而属性证书类似于工作证。居民身份证代表了一个人的身份,签发时间一般都比较长;而工作证的有效期一般要视具体的工作单位和性质而定,时间相对比较短。

其次,公钥证书和属性证书的管理颁发部门有可能不同。仍以居民身份证和工作证为例进行说明。居民身份证实行一人一证,并由唯一的国家机关签发;而工作证可能存在一人多证,并分别由不同的单位签发。与此相似,公钥证书由身份管理系统进行控制,而属性证书的管理则与应用紧密相关。目前,许多高校都建立了数字化校园平台,在该平台上集成了教务管理、学生管理、财务管理、资产管理等应用系统。对于学校的教工,每人都需要一个进入数字化校园的唯一账号,该账号用于确定用户的身份;但是,不同的人员在进入数字化校园后,可能根据工作性质的不同,对不同的系统具有不同的权限。例如,普通教师只可以访问教务系统,财务人员只可以访问财务管理系统,而学校领导则可以同时访问所有的系统。

版本
主体名称
签发者
签发者唯一标识符
签名算法
序列号
有效期
属性
扩展项

图 3-12　属性证书的格式

所以,在一个系统中每个用户只有一张合法的公钥证书,而属性证书的签发则比较灵活。多个应用可使用同一属性证书,但也可为同一应用的不同操作颁发不同的属性证书。属性证书的格式如图 3-12 所示。

(1) 版本说明 PMI 中 AC 的版本号,具体含义与 PKI 中的

数字证书相同。

(2) 主体名称用于说明该授权证书的持有者。

(3) 签发者为签发该 AC 的 AA 名称。

(4) 签发者唯一标识符为签发该 AC 的 AA 的唯一标识符,以比特串形式表示。

(5) 签名算法为签发证书时所使用的算法。

(6) 序列号为该证书的有效序列号,在 PMI 系统中该序列号是唯一的。

(7) 有效期为该证书的有效使用期限。

(8) 属性为拥有者所具有的权限属性。

(9) 扩展项用于功能的扩展。

PMI 中的属性证书的撤销与 PKI 中的公钥证书相似,也是通过证书撤销列表(CRL)的方式实现的,在 PMI 系统中,需要维护属性证书撤销列表(Attribute Certificate Revocation List, ACRL)进行证书的撤销操作。

3. 属性证书库

属性证书库用于存储属性证书,一般情况下采用 LDAP 服务器。在属性证书库中采用 LDAP 服务器主要出于以下几点考虑:一是由于 LDAP 服务器能够处理大量的用户并发,这样便于属性证书的检索,并具有更快的响应速度;二是 LDAP 服务器具有完善的安全机制,可以通过访问控制列表(ACL)设置对目录数据的读和写的权限,通过支持基于 SSL 的安全机制完成对明文的加密,可以为属性证书的管理提供安全保障;三是 LDAP 服务可以跨平台操作,支持 Windows、UNIX、Linux、NetWare 等几乎所有的主流操作系统;四是同步复制功能,如分布在不同地理位置的两台 LDAP 服务器可以通过使用"推""拉"技术使服务器保持数据的同步和一致;五是 LDAP 服务器的数据的组织方式采用树状层次结构,便于扩展。

3.4.3 基于角色的访问控制

随着现代信息技术的迅速发展,在网络中传输和处理的信息和数据越来越多。对于一个资源可控的网络来说,在资源数量迅速扩大的同时需要加强对资源的控制和管理。

在分布式网络环境下,对于安全性要求较高的信息资源,既要求能够由信息资源的管理部门统一进行管理,确保信息资源受控、合法、安全地使用,又需要授权管理和访问控制的复杂度不能因为资源和用户数量的增长而迅速增加,以确保授权和访问控制的可管理性,实现统一、高效、灵活的访问控制。传统的访问控制机制主要有自主访问控制(Discretionary Access Control,DAC)和强制访问控制(Mandatory Access Control,MAC)。

自主访问控制(DAC)又称为基于身份的访问控制,其主要思想是系统的主体可以自主地将其拥有的对客体的访问权限授予其他主体,且这种授予具有可传递性。特点是灵活性高,但授权管理复杂,安全性低。而强制访问控制(MAC)又称为基于规则的访问控制,其主要思想是将主体与客体分级,根据主体和客体的级别标识来决定访问控制,特点是便于管理,但灵活性差,完整性方面控制不够。

随着网络应用的不断发展,传统的 DAC 和 MAC 两种访问控制方式已远远不能满足访问控制的上述要求。20 世纪 90 年代以来发展起来的基于角色的访问控制(RBAC)技术可

以降低授权管理的复杂度和管理开销，提高访问控制的安全性，而且能够实现基于策略的授权管理和访问控制。

以资源分配管理为主的 PMI 系统，其授权管理是基于角色的。角色是给用户分配权限的一种间接手段，是对用户拥有的职能和权限的一种抽象。通过定义角色，为每个角色分配一定的权限。RBAC 的基本思想是：根据用户在组织内的职称、职务及所属的业务部门等信息来定义用户拥有的角色。而授权给用户的访问权限，由用户在组织中担当的角色来确定。

鉴于基于角色的访问控制技术的优势，需要在 PMI 中采用基于角色的访问控制技术进行授权管理和访问控制。具体以角色为中介，建立以对象与操作、权限、角色、组织结构、系统结构为核心的层次化的资源结构和关系的描述、定义和管理框架，充分反映信息系统资源配置和部署的现状以及未来资源结构动态变化和业务发展的需求，为授权管理和访问控制提供基础信息，并通过角色的分配实现对用户的授权，提高授权的可管理性和安全性，降低授权管理的复杂度，降低资源管理和授权管理的成本，提高管理的效率。

与传统的访问控制机制相比，在 PMI 系统中的基于角色的授权管理模式主要有以下 3 个方面的优势。

(1) 授权管理的灵活性。基于角色的授权管理模式可以通过属性证书(AC)的有效期以及委托授权机构来灵活地进行授权管理，从而实现了传统的访问控制技术领域中的强制访问控制(MAC)模式与自主访问控制(DAC)模式的有机结合，其灵活性要优于传统的授权管理模式。

(2) 授权操作与业务操作相分离。基于角色的授权管理模式将业务管理工作与授权管理工作完全分离，更加明确了业务管理员和安全管理员之间的职责分工，可以有效地避免由于业务管理人员参与到授权管理活动中而可能带来的一些问题。

(3) 多授权模型的灵活支持。基于角色的授权管理模式将整个授权管理体系从应用系统中分离出来，授权管理模块自身的维护和更新操作将与具体的应用系统无关。因此，可以在不影响原有应用系统正常运行的前提下，实现对多授权模型的支持。

3.4.4 PMI 系统框架

授权管理基础设施(PMI)在体系上可以分为 3 级，分别是权威源(SOA)、属性权威(AA)和 AA 代理点。在实际应用中，这种分级体系可以根据需要进行灵活配置，可以是三级、二级或一级。PMI 系统的基本框架如图 3-13 所示。

1. 权威源

权威源(SOA)是整个授权管理体系的中心业务节点，也是整个授权管理基础设施(PMI)的最终信任源和最高管理机构。SOA 的职责主要包括授权管理策略的管理、应用授权受理、AA 的设立审核及管理和授权管理体系业务的规范化等。

2. 属性权威

属性权威(AA)是授权管理基础设施(PMI)的核心服务节点，是对应于具体应用系统的授权管理分系统，由具有设立 AA 业务需求的各应用单位负责建设，并与 SOA 中心通过业

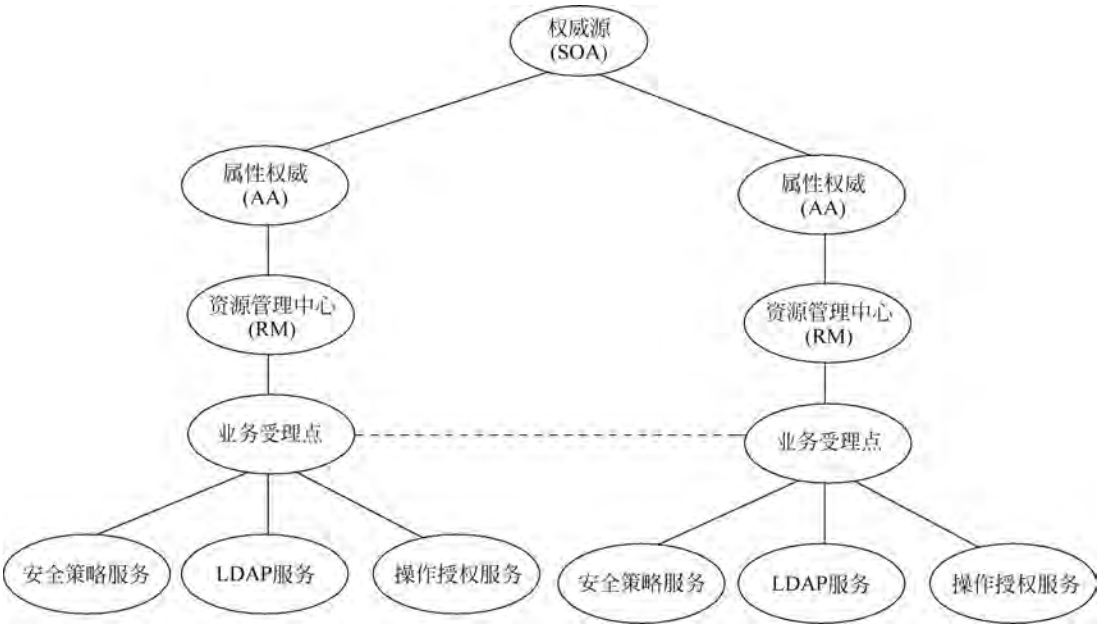

图 3-13 PMI 系统框架

务协议达成相互的信任关系。AA 的职责主要包括应用授权受理、属性证书(AC)的发放和管理以及 AA 代理点的设立审核和管理等。AA 需要为其所发放的所有 AC 维持一个历史记录和更新记录。

3. AA 代理点

AA 代理点是授权管理基础设施(PMI)的用户代理节点,也称为"资源管理中心",AA 代理点与具体应用直接联系,是对应 AA 的附属机构,接受 AA 的直接管理,由各 AA 负责建设,但必须经过 SOA 的同意,并签发相应的证书。AA 代理点的设立和数目由各 AA 根据自身的业务发展需求而定。AA 代理点的职责主要包括应用授权服务代理和应用授权审核代理等,负责对具体的用户应用资源进行授权审核,并将 AC 的操作请求提交到 AA 进行处理。

4. 访问控制执行者

访问控制执行者是指用户应用系统中具体对授权验证服务的调用模块。实际上访问控制执行者并不属于授权管理基础设施(PMI)的一部分,却是授权管理体系的重要组成部分。

访问控制执行者的主要职责是将最终用户针对特定的操作授权所提交的授权信息(AC)连同对应的身份验证信息(公钥证书)一起提交到 AA 代理点,并根据 AA 返回的授权结果,进行具体的应用授权处理。

3.4.5 PMI 与 PKI 之间的关系

在建设 PMI 设施时,必须拥有足够安全性的 PKI 设施。其中,PKI 负责公钥信息的管理,而 PMI 负责权限的管理。PMI 设施中的每一个 AA 实体和终端用户都是 PKI 设施的

用户，所以从应用角度来看，PMI 和 PKI 的发展是相辅相成并互为条件的。虽然 PMI 是在 PKI 的基础上提出的，但是 PMI 的应用和发展离不开 PKI 设施的支持。

可以将 PMI 和 PKI 绑定在一起，也可以将 PMI 与 PKI 在物理上分开。因为与 PMI 相比，PKI 相对比较稳定，其属性的变化较小。而 PMI 则会因为应用类型的变化（如增加或删除）而动态更新。所以 PMI 在逻辑上必然与 PKI 相联系，而在物理上可分离也可合并。

PMI 和 PKI 有很多相似的概念，如属性证书（AC）与公钥证书（Public Key Certificate，PKC），属性权威（AA）与认证机构（CA）。公钥证书是对用户名称和其公钥进行绑定，而属性证书是将用户名称与一个或更多的权限属性进行绑定。数字签名公钥证书的实体被称为 CA，签名属性证书（AC）的实体被称为 AA。PKI 和 PMI 之间的主要区别在于：PMI 主要进行授权管理，证明这个用户有什么权限，能干什么，即“你能做什么”；而 PKI 主要进行身份鉴别，证明用户身份，即“你是谁”。将 PKI 和 PMI 技术结合，实现可信的身份认证和可信授权管理是目前较为完善的安全保障措施。

*3.5 轻型目录访问协议

随着 Internet 和各类网络应用的快速发展和广泛应用，人们可以在世界范围内共享各种资源和信息。网络中的资源纷繁复杂，种类众多，因此，有效管理各种资源信息以利于检索查询至关重要。目录服务技术就是适应网络信息飞速发展而产生的，它是一种管理资源信息以方便查询的技术。由于轻型目录访问协议（LDAP）已经成为目录服务的事实上标准，本节主要介绍 LDAP 的相关概念和应用特点。

3.5.1 目录服务与 LDAP

目录（Directory）是用来存储用户账户、组、打印机、共享文件夹等对象（Object）的一个集合。像我们使用的电话号码簿，它包括了用户的姓名、性别、电话、地址、出生时间等基本信息，所以从应用功能来看，电话号码簿也是一种目录。另外，我们在计算机系统中使用的文件目录，它记录了文件的名称、大小、时间、存储位置等信息，文件目录是一种最常见的数字资源目录。因此，我们可以将目录理解为一个特定的管理单元，将存储目录中相关组成元素的数据库称为目录数据库（Directory Database）。

1. 目录服务的概念

目录服务（Directory Service，DS）是一个代表网络用户及资源的基于对象的数据库，主要用于存放用户的信息及网络配置数据，便于管理人员和应用程序对信息进行添加、修改和查询。目录服务的功能就是让用户很容易地在目录内方便、快速地查找到所需要的数据。

概括地讲，目录服务就是按照树状信息组织模式，实现信息管理和服务接口的一种方法。目录服务系统一般由两部分组成：第一部分是数据库，它是一种分布式的数据库，且拥有一个描述数据的规则；第二部分则是访问和处理数据库时使用的访问协议。虽然目录服务由于应用环境和具体实现的不同而呈现各种特点，但是其中具有以下 5 个方面的共同特点。

（1）目录服务专门为读信息而做了特殊优化。

(2) 目录服务实施分布存储模型。

(3) 目录服务应能扩展它所存储的信息的种类。

(4) 目录服务应具有高级检索功能。

(5) 目录信息在目录服务器之间可以松散地复制。

目前,应用最为广泛的目录服务主要有 Novell 公司的 Novell 目录服务(Novell Directory Services,NDS)、微软公司的活动目录(Active Directory,AD)、SUN 公司的 iPlanet 目录服务(iPlanet Directory Server,iDS)和 LDAP。

2. LDAP

LDAP 是一个新的目录访问协议,它是在继承了 X.500 标准的所有优点的基础上发展起来的一个基于 TCP/IP 体系的目录服务协议,也是目前在网络上应用最广泛的目录服务协议。

X.500 协议是最早的具有完备意义的目录服务协议,它由 CCITT 和 ISO 两大国际组织各自对目录服务的开发成果融合而产生,并于 1988 年被认可,1990 年初由 CCITT 发布,之后曾数次更新,目前仍在发展中。由于 X.500 协议是基于开放式系统互联(Open System Interconnection,OSI)体系结构的,所以早期设计人员过多地考虑了其通用性和可扩展性,致使 X.500 协议内容庞杂,开发和部署都极其复杂,同时性能不高。

随着 Internet 的发展,TCP/IP 成为事实上的网络标准。与 X.500 协议不同,LDAP 直接运行在更简单和更通用的 TCP/IP 或其他可靠的传输协议层上,避免了在 OSI 体系会话层和表示层的开销,使连接的建立和数据的传输更加简单、快捷,适应了以 Internet 为主的互联网和企业内部网络(Intranet)的应用需要。具体来说,LDAP 从以下几方面对 X.500 协议做了简化和发展。

(1) 功能方面。缩减了 X.500 中冗余的和使用频率较小的功能,以较低的开销完成了原来 X.500 协议中 90%的功能。

(2) 数据表示方面。统一采用文本字符串形式,避免数据解释时可能产生的二义性。

(3) 编码方面。仅采用 X.500 协议的一个子集(基本编码规则(Basic Encoding Rules,BER)),节约了空间,而且大大简化了其实现过程。

(4) 传输方面。直接运行于 TCP/IP 体系的传输层,对系统的开销较小,在提高了性能的同时,使目录服务的部署更加简单易行。

1993 年 7 月,第一个 LDAP 规范在 RFC 1487 文档中发布;同年,LDAP v2 发布,其功能在 RFC 1777 文档中进行了描述;1997 年,随着 LDAP v3 的发布(详见 RFC 2251 文档),LDAP 进入一个更加成熟的阶段。与 LDAP v2 相比,LDAP v3 提供了更多的功能,如使用 UNICODE 支持国际化,支持强度认证及使用 TLS(SSL)进行完整性和安全保护等。目前,LDAP v3 已成为 Internet 的标准。

3. LDAP 的目录结构

与 UNIX 的文件系统类似,在 LDAP 中目录按照树状结构组织,该树状结构称为目录信息树(Directory Information Tree,DIT)。LDAP 标准定义了目录中访问信息的协议,规定了信息的形式和特性、信息存放的索引和组织方式、分布式的操作模型,并且使 LDAP 协议本身和信息模型都是可以被扩展的。LDAP 目录中可以存放文本、图片、统一资源定位符

(Uniform Resource Locator,URL)、二进制数据、证书等不同类型的数据。

LDAP 树状信息中的基本数据单元称为条目(Entry),条目可以理解为关系数据库中表的记录;条目是具有标识名(DN)的属性(Attribute)集合,DN 可以理解为关系数据库表中的关键字(Primary Key);属性由类型(Type)和多个值(Values)组成。LDAP 中的属性可以理解为关系数据库中的域(Field),域由域名和数据类型组成,在 LDAP 中为了便于检索类型,一个类型可以同时拥有多个值(Value)。与关系数据一样,LDAP 服务器也是用来处理查询和更新的,但 LDAP 与关系数据库具有较大的不同,LDAP 不具有关系数据库完备的关系运算处理能力,也没有很强的数值计算能力。但是 LDAP 目录服务对读、浏览和搜索等操作进行了优化。

LDAP 中条目的设计一般按照地理位置或组织关系进行组织,应用中非常直观。LDAP 把数据存放在文件中,为提高效率可以使用基于索引的文件数据库,而不是关系数据库。LDAP 还规定了 DN 的命名方法、访问控制方法、搜索格式、复制方法、URL 格式、开发接口等功能。

LDAP 是一个类似于 DNS 的关于目录服务的网络协议。如图 3-14 所示,在 LDAP 的 DIT 结构中,最顶部被称为根,即"基准 DN",代表一个国家、组织或学校;下一层是组织单元(Organization Unit,OU),可以代表该国家、组织或学校中的一个内部机构;更低一层的 OU 可用来对上一层的 OU 进行更细的归类,如对某一机构内部的人员按照职务进行细分等。其中,DC 表示 Domain Component。

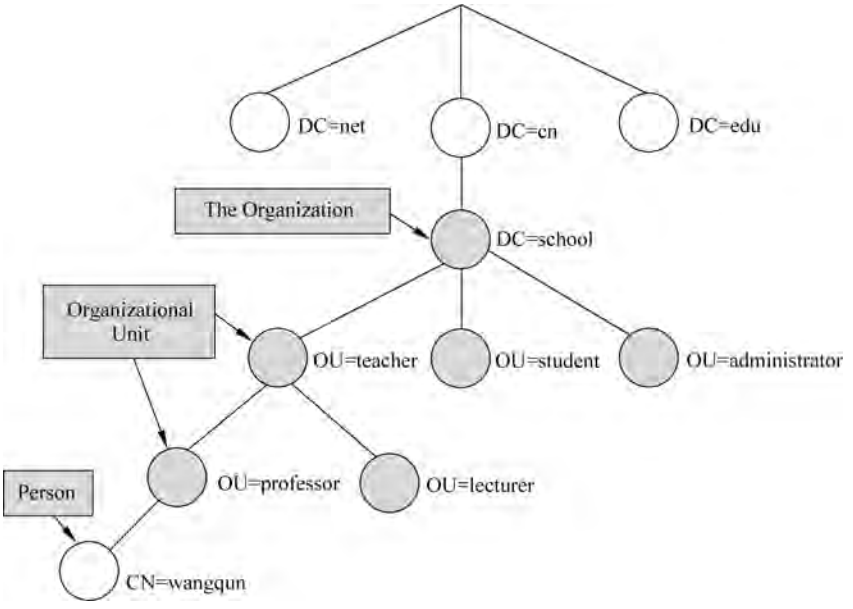

图 3-14 LDAP 目录的树状结构

3.5.2 LDAP 的模型

LDAP 通过定义 4 种基本模型描述其工作机制,具体说明什么样的数据可以存放在 LDAP 目录中以及如何操作这些数据。下面分别介绍这 4 种模型的功能。

1. 信息模型

LDAP的信息模型定义了目录中存储的数据的基本单位和数据的类型。其中，目录中数据的基本单位为条目(Entry)，即关于对象的信息集合，每一个条目为一个属性集合，每一个属性含有一个属性类型和一个(或几个)值。条目相当于现实世界中的一个对象(如一个部门、一台计算机等)，属性则从某一方面反映对象的特征(如部门的归属、计算机的型号等)。另外，目录模式(Directory Schema)规定了哪些属性是必须具有的，哪些只是允许存在的。

2. 命名模型

LDAP的命名模型定义了目录的组织和查询方式。LDAP中的条目都有自己的DN和相对标识名(Relative Distinguished Name，RDN)，其中DN为该条目在整个目录树中的唯一名称标识，而RDN是条目在父节点下的唯一名称标识。LDAP目录树的根(Root)是虚根，树的每一个节点都存储信息，每一个节点都有一个属性作为RDN。从其中一个节点回溯到根，经过的RDN依次连接后组成该节点的DN，DN在整个LDAP目录树中是唯一的。在LDAP目录中存储的记录内容都要有一个名字，这个名字通常存在于共同名(Common Name，CN)这个属性里，在LDAP中存储的对象都用其他的CN值作为RDN的基础。图3-15所示的是LDAP目录树中RDN和DN的组成。

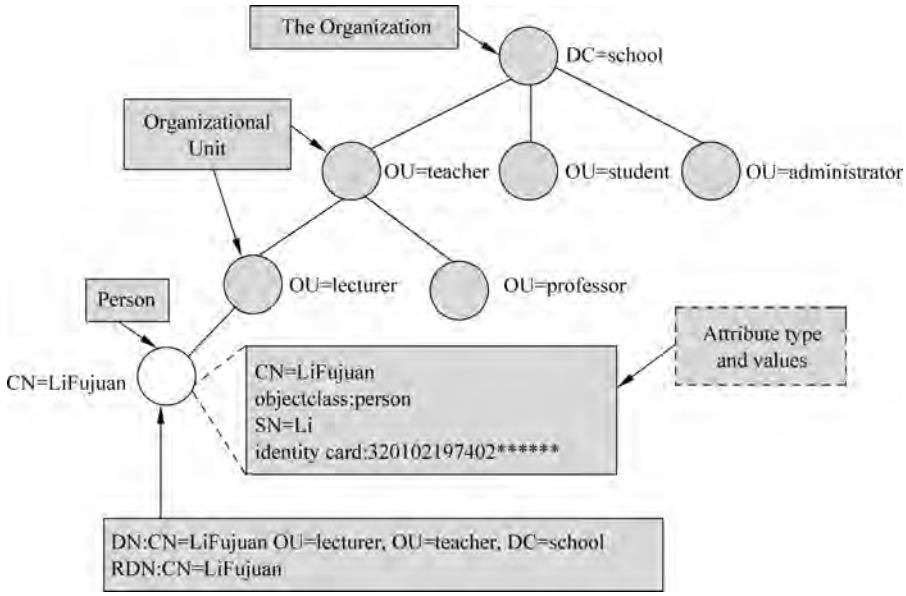

图3-15 LDAP目录中的DN和RDN

3. 功能模型

LDAP的功能模型也称为函数模型，具体定义了访问和更新目录的4类操作。

(1) 查询类操作。查询某个条目并返回结果，LDAP同时支持根据DN的查询和根据某一属性的检索，如检索、比较等。

(2) 更新类操作。进行条目或其属性的增加、删除及重命名。

(3) 认证类操作。对客户端进行认证,控制某些交互行为,如绑定、解绑定等。

(4) 其他类操作,如放弃、扩展操作等。

4. 安全模型

LDAP 安全模型定义了如何保护目录信息,防止未授权用户对目录信息的访问和修改。其中应用最广泛的主要有绑定操作,而且绑定操作的不同使得安全机制有所不同,主要有以下 3 种。

(1) 无认证。无认证是指 LDAP 客户端与服务器之间的通信不进行认证。这种方法只在没有数据安全问题且不涉及访问控制权限(如匿名访问)的时候才能使用。

(2) 基本认证。当使用基本认证方式时,客户进程通过网络向服务进程发送一个用于进行身份标识的 DN 和口令,服务进程检查客户进程发送的 DN 和口令,如果与目录数据库中存储的匹配,则通过认证,并进行访问授权; 否则,拒绝用户的访问。

(3) SASL 认证。简单认证与安全层(Simple Authentication and Security Layer,SASL)是一种为基于连接的网络应用协议(如 LDAP、IMAP、SMTP 等)增加认证支持的标准,主要在 RFC 2222 文档中进行了描述。SASL 支持多种认证机制,并且允许用户根据自己的需要进行扩充,目前已被多种网络协议所支持,具有十分广阔的应用前景。SASL 认证的基本过程由服务器的请求和客户端的应答组成,根据认证机制的要求,这个过程可以重复,直到服务器发送成功或失败消息为止。这个认证过程不仅可以执行必要的认证,而且还能传送安全层的标识信息和协商选项。如果协商成功了一个安全层,它将在认证过程完成后立即生效,为后续的协议通信提供一个安全的通道。目前常用的 SASL 认证机制主要有 Kerberos v4、GSS-APIS、Key 与 OTP、CRAM-MD5 和 EXTERNAL 等。

3.5.3 LDAP 的功能模块和工作过程

LDAP 认证过程的实现,由相应的认证功能模块组成。各功能模块之间协调操作,完成认证操作。

1. 功能模块

LDAP 的目录服务是建立在 TCP/IP 基础之上的应用层协议,客户端与服务器之间以 Client/Server 模式工作,所有的目录数据存储在 LDAP 服务器上。如图 3-16 所示,出于安全和分布式访问的需要,同一网络中一般需要两台或两台以上的 LDAP 服务器组成 LDAP 目录树,每一个 LDAP 服务器由目录服务模块、复制服务模块和管理模块 3 部分组成。

(1) 目录服务模块。目录服务模块主要由网络通信模块和目录数据库两部分组成,其中位于前端的网络通信模块主要负责 LDAP 服务器与 LDAP 客户端之间的通信; 目录数据库负责 LDAP 目录数据的管理。

(2) 复制服务模块。复制服务模块负责不同 LDAP 服务器之间的目录数据的复制,以保证目录服务的一致性。

(3) 管理模块。管理模块负责目录信息的管理,为用户提供所期望的反应时间、通信的管理性、数据传输的完整性和服务的一致性。

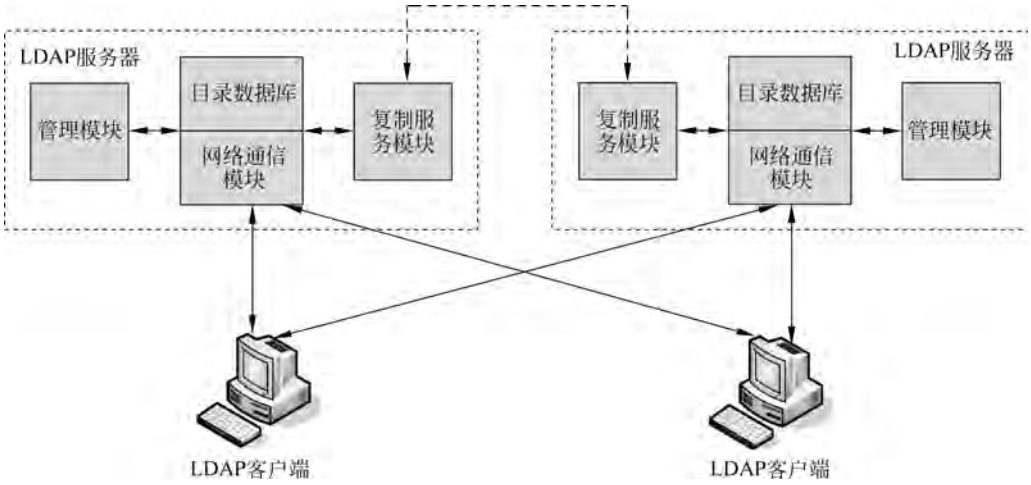

图 3-16 LDAP 目录服务功能模块组成

2. 工作过程

LDAP 是基于面向连接的 TCP 协议实现的，定义了 LDAP 客户端与 LDAP 服务器之间的通信过程和数据格式。LDAP 服务器在服务端口（默认 TCP 端口为 389）进行监听，当收到客户端的请求后，建立连接，开始会话。LDAP 的工作过程如下，如图 3-17 所示。

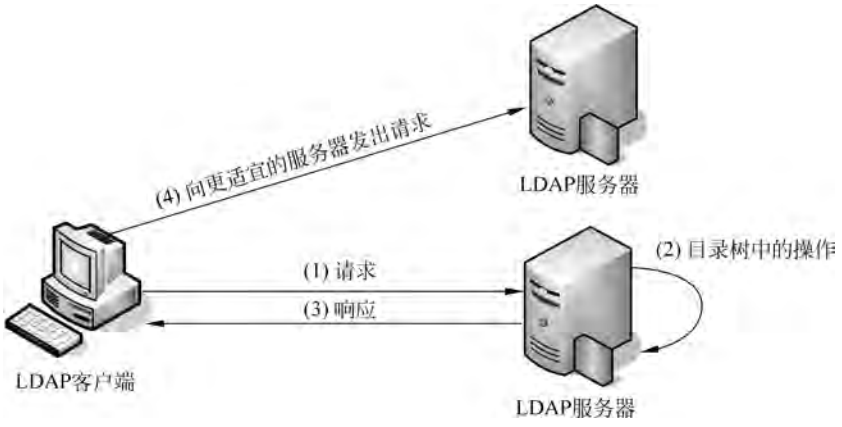

图 3-17 LDAP 的工作过程

（1）LDAP 客户端根据访问需求向 LDAP 服务器发送操作请求。

（2）LDAP 服务器负责对目录树中的条目进行必要的操作。

（3）LDAP 服务器向 LDAP 客户端返回一个应答（响应）。这个应答可能包含查询结果，或包含操作出错信息，或者是一个引用。引用（Referral）是一种重定向机制，表明客户所需要的目录服务不在本地服务器，并向客户端返回一个能够提供服务（或能够提供更好的服务）的服务器的 URL。

（4）如果步骤（3）在响应信息中包含的操作是引用，那么客户端则向该 URL 指定的 LDAP 服务器发送请求。

习题 3

3-1 什么是 PKI？PKI 与数据加密算法之间存在什么关系？PKI 主要解决网络安全中的什么问题？

3-2 从消息的保密性、完整性、真实性和不可否认性等方面，分析 PKI 与网络安全之间的关系。

3-3 从 PKI 策略、认证机构 CA、注册机构 RA、证书发布系统和 PKI 应用等方面，分析 PKI 系统的特点。

3-4 在 PKI 系统中，CA 的作用是什么？

3-5 结合实际应用，从安全服务器、注册机构 RA、CA 服务器、LDAP 服务器和数据库服务器等方面，分析 CA 各组成部分的功能特点。

3-6 联系实际，说明 CA 之间是如何建立信任关系的，并分析不同 CA 之间信任模型的特点。

3-7 什么是数字证书？在网络安全中数字证书的作用是什么？

3-8 详细分析数字证书的签发和撤销方式。

3-9 在 PKI 系统中为什么要进行数字证书的更新操作？如何实现？

3-10 联系 PKI 技术，介绍 PMI 的概念和应用特点。

3-11 什么是基于角色的访问控制方式？

3-12 联系实际应用，分析 PKI 与 PMI 之间的关系。

3-13 什么是目录服务？结合 Internet 应用系统，介绍目录服务的功能。

3-14 介绍 LDAP 的模型和功能组成。

3-15 通过实验，掌握数字证书的使用方法。