有自己的公钥和私钥，使用其私钥给用户（包含 CA 中心自己）签发数字证书，具体签发过程如下：

（1）将用户身份信息和用户公钥信息，按照特定格式组成数据 D。

（2）选择摘要算法对数据 D 进行计算得到摘要 H。

（3）使用 CA 私钥对摘要 H 进行加密得到数字签名 S。

（4）将用户身份信息、用户公钥信息和数字签名 S，按照特定格式就可组成数字证书。

2．CA 应对数字证书的全生命周期进行管理

CA 实际是一种特殊的公钥管理中心，为实现数字证书的安全性，应对数字证书的全生命周期进行管理，主要包括：

（1）数字证书的签发和更新。证书签发主要针对新用户；证书更新主要针对已有证书用户，更新时公钥可以改变，也可以不变。

（2）数字证书的作废（注销、撤销或吊销）。证书作废后将成无效证书，永远不能使用。

（3）数字证书的冻结（挂失）和解冻。证书冻结后将成无效证书，但可以通过解冻恢复成有效状态。

（4）数字证书的查询或下载。应提供公开服务方式，允许用户根据条件随时查询证书并下载。常用服务方式有 HTTP 和 LDAP。

（5）数字证书状态查询。应提供公开服务方式，允许用户随时查询证书状态，以便判断该证书是否处于有效状态。常用服务方式有 CRL 和 OCSP。

3．KMC 用于管理私钥

如果使用公钥（数字证书）对数据进行加密，则只有与公钥对应的私钥才能进行解密，从而可实现用户数据的保密性。当私钥丢失时，如果没有备份和恢复机制，将导致公钥加密的所有数据都无法解密，可能给用户带来损失。

为解决私钥的备份与恢复问题，PKI 引入了 KMC，用于对私钥的全生命周期进行管理。KMC 是 Key Management Center 的缩写。

用户公私钥对可由 KMC 产生，提交 CA 签发数字证书后，将私钥和数字证书同时安全移交给用户，而 KMC 将私钥留作备份，可按需要给用户恢复。用户公私钥对也可由用户自己产生（使用软件或密码设备），在向 CA 中心申请数字证书时，可将私钥安全提交 KMC 留作备份。

4．双证书机制

为防止用户身份被冒用，应保证用户私钥的唯一性，不允许备份恢复。为防止公钥加密后的数据无法解密，应提供用户私钥的备份恢复机制。

为解决这两种矛盾的应用需求，PKI 引入双证书机制：签名证书和加密证书。

签名证书及私钥只用于签名验签，不能用于加密解密；为保证签名私钥的唯一性，该公私钥对必须由用户自己产生，同时采用硬件技术（如只允许在硬件密码设备内产生公私钥对、私钥不允许导出等）保证无法复制，在证书签发过程中 CA 中心并不知道该私钥，只对其公钥进行操作。该私钥没有备份，因此永远不能恢复。

加密证书及私钥只用于加密解密，不能用于签名验签。为实现解密私钥的备份恢复机制，

该公私钥对必须由 KMC 产生，由 CA 签发完数字证书后安全移交给用户，用户应采用硬件技术保证该私钥的安全性。KMC 可根据需要恢复该私钥。

5．LDAP

CA 中心存储着所有数字证书，并通过公开服务形式供用户随时查询或下载。为解决数字证书查询或下载的性能问题，避免 CA 中心成为性能瓶颈，PKI 引入了 LDAP 技术，通过 LDAP 方式对外提供高速证书查询或下载服务。

专业的关系型数据库管理系统（如 Oracle、DB2 等）专门对结构化数据进行管理，应用系统只需通过 SQL 语句（报文协议）发送各种数据管理指令，而具体管理工作完全由数据库管理系统负责。尽管这种数据管理方式大大简化了应用系统的复杂度，但由于其读写功能相对均衡，很难满足高性能的查询服务。为获得高性能的查询服务，需要对数据管理的读取功能进行特殊优化，于是出现了目录服务技术（DAP，Directory Access Protocol）。目录服务技术对查询功能进行优化，比修改操作快 10 倍以上，适合快速响应和大容量查询服务。DAP 技术通过目录树方式对数据进行管理，应用系统只需通过 X.500 协议就能对数据进行快速查询。

由于 X.500 协议过于复杂，实现成本很高，于是国际组织对 X.500 进行了简化，形成 LDAP 标准，而且 LDAP 支持 TCP/IP 协议，更适合于互联网领域使用。LDAP 为轻量目录访问协议，是 Light-weight Directory Access Protocol 的缩写。

由于数字证书是可以公开的，CA 中心也可以将其签发的数字证书存储到其他地方，供用户查询或下载。

6．CRL 和 OCSP

当用户私钥泄露后，CA 中心有责任将该用户的证书标记为失效。但用户如何获得对方证书是否失效的状态呢？为方便用户获得证书状态，PKI 引入了 CRL 和 OCSP 技术。

（1）CRL（Certificate Revocation List）

CRL 为证书作废列表，是 Certificate Revocation List 的缩写，也称作证书黑名单，是一种特殊的文件格式，包含所有失效的证书清单、下次 CRL 生成时间和 CA 中心私钥的签名。

CA 中心定期生成 CRL，并将下次生成时间写入 CRL 中，方便用户按时定期下载 CRL。跟数字证书类似，CRL 也是通过 CA 中心私钥的签名来保证 CRL 无法被篡改的。用户只需定期获取 CRL 后，就可在本地脱机验证证书是否失效，在下次 CRL 生成时间之前无需联系 CA 中心。

由于 CRL 是可以公开的，CA 中心也可以将其签发的 CRL 存储到其他地方，供用户查询或下载。CRL 也可以发布到 LDAP 中，提供高速下载服务。

（2）OCSP（Online Certificate Status Protocol）

当 CA 中心将私钥已泄露的用户证书标记为失效后，如果还未到下次 CRL 生成时间，此时其他用户通过最新 CRL 并不知道该用户证书已经失效，依然将该用户当作有效用户继续进行各种保密通信和合法交易，因此可能会造成一定的损失。

为解决 CRL 滞后的缺陷，避免给高实时性或高风险交易造成重大损失，PKI 引入了 OCSP，对用户提供实时的证书状态查询服务。

OCSP 为在线证书状态协议，是 Online Certificate Status Protocol 的缩写。当用户需要实时查询对方证书是否有效时，可通过 OCSP 协议实时访问 CA 中心获得对方证书的当前状态。

7. RA

在保证 CA 系统安全性的前提下，为方便证书业务远程办理、方便证书管理流程与应用系统结合，PKI 引入了 RA，专门用于对用户提供面对面的证书业务服务，负责用户证书办理/作废申请、用户身份审核、制作证书并移交用户等功能，而涉及证书签发时则提交 CA 系统集中处理。RA 是 Registry Authority 的缩写，又称作 RA 中心、注册中心。有时候，证书管理流程会与应用业务流程结合，并不单独体现出来，如对于网上银行，证书管理流程就会融合到网银业务流程中。

RA 可以部署多个，既可以单独部署，也可以与应用系统集成。

CA 主要模块组成如图 2-3 所示。

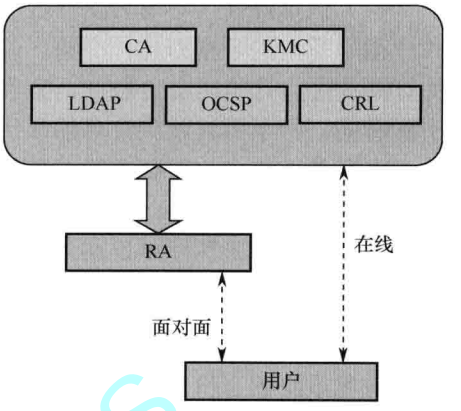

图 2-3　CA 主要模块组成

2.4　PKI/应用

1. 基于数字证书可实现四种基本安全功能

（1）身份认证。

网上交易的双方很可能素昧平生，相隔千里。要使交易成功进行，首先要能确认对方的身份，对商家要考虑客户不能是骗子，而客户也会担心网上的商店是不是一个玩弄欺诈的黑店，因此能方便而可靠地确认对方身份是交易成功的前提。对于为顾客或用户开展服务的银行、信用卡公司和销售商店，为了做到安全、保密、可靠地开展服务活动，都要进行身份认证的工作。对销售商店来说，他们对顾客刷卡消费所用的信用卡的真伪是不知道的，商店只能把信用卡的身份确认工作完全交给银行来完成。

数字证书可作为网络身份证，在网络世界中进行交互时，证书持有人（持证人）只需出示数字证书，对方通过判断该证书是否伪造、持证人是否拥有对应的私钥、该证书是否被作废或冻结等内容即可验证该持证人的身份是否合法，从而很方便地实现高强度的身份认证功能。

（2）保密性。

交易中的商务信息均有保密的要求。如信用卡的账号和用户名被人知悉，就可能被盗用，订货和付款的信息被竞争对手获悉，就可能丧失商机。

使用数字证书中的公钥对静态数据（如文档）或动态数据（如交易报文）进行加密，只有持证人才能使用对应的私钥进行解密，从而实现各种敏感数据的保密性。

（3）完整性。

为保障交易的严肃和公正，交易的文件不应被修改，如合同或订单。卖方收到订单后，如发现商品大幅涨价，若能私自改动合同，将商品价格或订购数量修改，就可大幅受益，那么买方可能就会蒙受损失。

使用私钥对静态数据（如文档）或动态数据（如交易报文）进行签名，使用对应的数字证书中的公钥就能验证该数据是否被篡改，从而实现各种敏感数据和交易记录的完整性。

（4）抗抵赖性（不可否认性）。

由于商情的千变万化，交易一旦达成是不能被否认的，否则必然会损害一方的利益。例如订购黄金，订货时金价较低，但收到订单后，金价上涨了，如果销售方能否认收到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。

在交易过程中，可要求对方使用其私钥对交易数据进行签名，交易完成后可将交易数据及对方签名存储起来，一旦发生交易纠纷，就可调出所存储的交易数据和对方签名，使用对方数字证书中的公钥即可证明该交易是对方进行的，从而实现交易过程的抗抵赖性。

2．数字证书如何与应用系统结合

基于证书接口中间件（模块或组件），应用系统可以很方便地使用数字证书技术，从而提高应用系统的身份认证强度、保证应用系统中各种敏感数据的保密性、保证应用系统中各种敏感数据和交易记录的完整性、用户各种操作或交易的不可否认性。

PKI 技术经过 30 多年的发展历程，已经形成比较完善的标准规范体系，几乎覆盖应用系统的各个方面，目前很多软件都已经支持数字证书技术，如操作系统、数据库系统、Web 服务器、应用服务器等。由于受应用环境多样性和应用技术复杂性的影响或限制，在不同的应用环境和应用技术下，数字证书技术应用的方式可能差异很大。

当前主流的数字证书应用技术主要包括：Windows 域登录、操作系统登录、电子文件加密、安全电子邮件、电子印章、代码签名、时间戳、WTLS 应用、SSL/TLS 应用（如 Web 网站安全、SSL VPN）、IP Sec 应用（如 IPSec VPN）等。

3．数字证书典型应用

（1）网上报税。

随着 IT 技术的迅速发展及其在税收领域的广泛应用，网上税收已成为不可逆转的发展趋势，其主要存在两类安全隐患或问题：一是网络安全问题。重点是身份认证，目前采用的用户名/口令机制容易被他人假冒身份；二是纸质报表的事后报表问题。只有加盖企业公章的纸质报表才能作为法律凭证。

电子签名法赋予数字签名法律效力后，数字证书技术就可有效解决上述两个问题，使得企业网上报税成为现实，同时提高了企业和税务部门的工作效率。

事实上，国内大部分省份上千万家企业已经通过数字证书进行网上报税。

（2）网上银行。

网上银行是商业银行基于互联网为客户提供安全、实时的银行业务服务。作为一种全新的银行客户服务渠道，客户可以不必亲自去银行办理业务，只要能够上网，无论在家里、办公室，还是在旅途中，都能够每天 24 小时安全便捷地管理自己的资产，或者办理查询、转账、缴费等银行业务。

网上银行以 Internet 等开放式网络环境传输交易数据，而且涉及用户资金转移等敏感信息，所以在用户的身份认证、资金的秘密传输以及数据的完整性方面，存在许多安全问题。网上银行服务提供者首先需要确定自己的系统不会受到网络黑客的入侵，造成秘密信息泄露、业务损失或服务中断。对用户而言，必须确认在网络上输入的秘密信息不会被盗用、输入的交易资料不会被篡改并且能正确迅速地传送到接收端系统。

基于数字证书技术，网上银行能有效解决用户身份认证、敏感数据保密性、交易数据完

整性和交易操作不可抵赖性问题，极大地方便了银行企业客户和个人客户。

数字证书（俗称 U 盾）已经成为国内网上银行的标准配置。如果没有数字证书，企业用户将不允许使用网上银行。上亿个人用户已经通过数字证书访问网上银行实现转账或汇款等资金操作。

2.5　PKI/运营

《电子签名法》规定："电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。"显然，电子签名法不仅赋予了电子签名的法律效力，而且明确了电子认证服务提供者的法律地位。电子认证服务提供者又称作电子认证服务机构或 CA 中心。

1．电子认证服务机构需满足政策法规的各项要求

《电子签名法》（2004 年版）规定：提供电子认证服务，应当具备下列条件：

（1）具有与提供电子认证服务相适应的专业技术人员和管理人员。

（2）具有与提供电子认证服务相适应的资金和经营场所。

（3）具有符合国家安全标准的技术和设备。

（4）具有国家密码管理机构同意使用密码的证明文件。

（5）法律、行政法规规定的其他条件。

《电子认证服务管理办法》（2009 年版）规定：电子认证服务机构应当具备下列条件：

（1）具有独立的企业法人资格。

（2）具有与提供电子认证服务相适应的人员。从事电子认证服务的专业技术人员、运营管理人员、安全管理人员和客户服务人员不少于三十名，并且应当符合相应岗位技能要求。

（3）注册资本不低于人民币三千万元。

（4）具有固定的经营场所和满足电子认证服务要求的物理环境。

（5）具有符合国家有关安全标准的技术和设备。

（6）具有国家密码管理机构同意使用密码的证明文件。

（7）法律、行政法规规定的其他条件。

《电子政务电子认证服务管理办法》（2009 年版）规定：电子认证服务机构应当具备以下条件：

（1）事业法人或者取得电子认证服务许可的国有控股企业法人。

（2）具有经国家密码管理局批准的电子政务电子认证基础设施。

（3）具有与从事认证服务相适应的专业技术人员、运行维护人员、安全管理人员和服务人员。

（4）具有与认证服务相适应的运行服务、应用支持和安全保障等机制。

（5）法律法规规定的其他条件。

《卫生系统电子认证服务管理办法》（2009 年版）规定：电子认证服务机构面向卫生系统提供电子认证服务应当具备以下必要条件：

（1）取得工业和信息化部颁发的《电子认证服务许可证》。

（2）符合《电子政务电子认证体系建设总体规划》（国密局联字〔2007〕2 号）中关于电