电子商务概论知识辅导：CA系统功能 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/170/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_170709.htm 一、证书的申请证书的申请也称注册。CA电子证书的申请，分为个人普通证书的申请、Web证书的申请、企业高级证书的申请及SET证书的申请。1、CA证书申请的前提条件（1）证书申请者必须在某商业银行开有账户。（2）证书申请必须具有唯一的身份证号码或工商营业执照号码，或全国机构代码。（3）证书申请必须具有电子邮件地址。（4）各商业银行总行应具有PKI管理能力，设管理官员；各商业银行总行应拥有一个证书申请注册机构RA(Registiatlign，Authority)及多个分支机构的证书申请受理点LRA(Local Registration Authority)。（5）各个PKI实体之间可以进行基于TCP／IP的通信。2、CA证书的申请方式（1）离线申请方式所谓离线申请方式即面对面申请方式，用户(包括个人用户及商户)到商业银行的受理点LRA及证书注册审批机构RA进行书面申请，填写按一定标准制定的表格并同时提供有关的证件。（2）在线申请方式用户连接上Internet网，通过自己的浏览器，到银行的主页服务器上下载标准表格，按内容提示进行填表申请；也可以通过电子邮件和电话呼叫中心(Call center)传递申请表格的有关信息，但有些信息仍需要人工录入，以便进行审核。（3）CA PKI Web证书的申请Web证书，即个人证书，申请方式可通过在线或离线方式：在线申请方式即客户通过因特网使用浏览器连接到商业银行网站并下载一个浏览器专用的客户端软件，做好填写申请信息的准备。离线方式即客户持有效证件(身份证、信用卡等)，填

写申请表格中的有关信息，面对面的进行申请。（4）企业高级证书的申请企业高级证书的申请只能以面对面的方式进行，企业负责人到他们所在的商业银行开户行所设置的注册申请机构RA进行申请。企业高级证书申请者需提供一张证明企业法人身份的证明、营业执照及电子邮件地址等。（5）SET证书的申请SET证书的申请者主要是持卡人，一般为离线申请。即持卡人事先必须在某商业银行开设信用卡账户，然后持本人的身份证明，到银行营业网点办理证书申请手续，填写有关登记表格。版本号申请人名称申请人公钥申请人其他信息国家省份城市单位机构电子邮件地址身份证号码 证书申请基本信息签名算法申请人签名证书签名信息图9.5 电子证书申请表经审查无误后，营业网点（即LRA）将申请信息录入RA，并得到一次性口令（Onetime pass code）和参考号（Reference number）。用户在自己的浏览器上申请下载证书。（6）关于证书申请表格对于上述各种证书，无论是通过哪种申请方式，都要填写证书申请表。该表的主要内容如图9.5所示。电子证书申请的内容与格式是由两大部分组成，其一是申请书的基本信息，包括申请人名称、申请人公钥、申请人其他信息如：国家、省份、城市、单位、分支机构、电子邮件地址以及身份证号码；其二是申请人签名及签名算法。二、证书的审批用户提交的证书申请表需经RA或LRA中的审查人员进行核查。核查的方法有如下两种：1、在线审核方式即将人工录入的用户申请信息与银行原有的客户信息数据库系统进行自动审查核对，RA的审核系统与银行的客户信息系统在线连接起来，使用一个专用的应用程序对申请证书的客户资信程序进行审查，确定接受签发或拒绝签发证书。2、离

线审核方式即对手工录入的用户申请信息进行人工审查，审批人员调用客户在银行的有关信息，进行资格和信用度的审核，并有权决定同意或拒绝客户的证书申请。如果同意客户的审请，LRA和RA使用专用的应用程序在PKI系统中注册用户。这个应用首先对LRA及RA的身份进行验证，然后在RA的申请数据库中创建新用户的信息。三、证书的颁发(下载)证书的发放分为两种方式：一是离线方式发放，即面对面发放，特别是企业高级证书，通常是面对面的离线方式发放；二是在线方式发放，即通过Internet网在目录服务器上下载证书。1、离线方式发放的步骤（1）一个企业级用户证书的申请被批准注册以后，RA端的应用程序初始化申请者信息，并在LDAP目录服务器中添加企业证书申请人的有关信息。（2）RA在初始化(enable)申请者信息后，传给CA。CA为申请者产生一个参照号(Ref. number)和一个认证码(Auth.code)，在PKI中有时也称做user ID及Password。参照号是一次性密码。RA将Ref.number和Auth.code通过电子邮件或打印在保密信封中，通过可靠途径将保密信封传递给企业高级证书的申请人。企业高级证书的申请人输人参照号及认证码，在RA面对面领取证书。证书介质可存人软盘或者存放于IC卡中。2、在线方式发放的步骤（1）在个人证书申请者的信息写入CA的申请人信息数据库中后，RA端即可接收到从CA中心发放的参照号和认证码，并将在屏幕上的显示的参照号和认证码打印出来，当面提交给证书申请人。（2）证书申请人回到自己的微机上，登录到银行的网站，首先通过浏览器安装Root CA的证书。（3）接着申请人在银行的网页上，按提示填人参照号和授权码，自助式地下载自己的证书。四、证书的归档及

撤消CA所发证书要定期归档，以备查询。除用于用户的签名密钥外，对证书所有数据信息，都要进行归档处理。CA使用目录服务器系统存储证书和证书的撤消列表。目录和数据库备份，可以根据组织机构的安全策略执行归档，最长时间可达7年保存期。数据库还保存审计和安全记录。对于用户密钥对，CA是通过专用程序自动存储和管理密钥历史及密钥备份。在证书的有效期内，由于私钥丢失泄密等原因，必须废除证书。此时证书持有者要提出证书废除申请。注册管理中心一旦收到证书撤消请求，就可以立即执行证书撤消，并同时通知用户，使之知道特定证书已被撤消。PKI CA提供了一套成熟、易用和基于标准的证书撤消系统。从安全角度来说，每次使用证书时，系统都要检查证书是否已被撤消。为了保证执行这种检查，证书撤消是自动进行的，而且对用户是透明的。这种自动透明的检查是针对企业证书进行的，而个人证书则要人工查询。五、证书的更新用户证书过期后，可以申请更新。更新方式有两种：一种是执行人工密钥更新；一种是实现自动密钥更新。1、执行人工密钥更新用户证书过期时，可到受理点向注册中心提出更新，注册中心可以通过提供新的参考号和授权码，来更新用户的证书。与初始申请和下载证书的过程相同，用户可以使用共享式密码进入注册站点，填写更新表格，然后回答对话框中提出的问题。浏览器将产生新密钥对和证书申请，用户与浏览器中的专用软件进行交互，实现证书更新的注册过程。CA签发新证书送到受理点，用户到受理点取回证书。