 二、CA认证系统 公共网络系统的安全性则依靠用户、商家的认证，数据的加密及交易请求的合法性验证等多方面措施来保证。 电子交易过程中必须确认用户、商家及所进行的交易本身是否合法可靠。一般要求建立专门的电子认证中心（CA）以核实用户和商家的真实身份以及交易请求的合法性。认证中心将给用户、商家、银行等进行网络商务活动的个人或集团发电子证书。 电子商务中，网上银行的建立，CA的建立是关键，只有建立一个较好的CA体系，才能较好地发展网上银行，才能实现网上支付，电子购物才真正实现。CA的机构如多方并进，各建各的，以后会出现各CA之间的矛盾，客户的多重认证等。应有一家公认的机构如银行或邮电或安全部来建立权威性认证机构（CA）。 1．SET的认证（CA） 在用户身份认证方面，SET引入了证书（Certificates）和证书管理机构（Certificates Authorities）机制。 （1）证书 证书就是一份文档，它记录了用户的公共密钥和其他身份信息。在SET中，最主要的证书是持卡人证书和商家证书。 持卡人实际上是支付卡的一种电子化表示。它是由金融机构以数字签名形式签发的，不能随意改变。持卡人证书并不包括帐号和终止日期信息，取而代之的是用单向哈希算法根据帐号、截止日期生成的一个编码，如果知道帐号、截止日期、密码值即可导出这个码值，反之不行。 商家证书：表示可接受何种卡来进行商业结算。它是由金融机构签发的，不能被第三方改变。在SET环境中，一个

商家至少应有一对证书。一个商家也可以有多对证书，表示它与多个银行有合作关系，可以接受多种付款方法。 除了持卡人证书和商家证书以外，还有支付网关证书、银行证书、发卡机构证书。 （2）证书管理机构 CA是受一个或多个用户信任，提供用户身份验证的第三方机构。证书一般包含拥有者的标识名称和公钥，并且由CA进行过数字签名。 CA的功能主要有：接收注册请求，处理、批准/拒绝请求，颁发证书。用户向CA提交自己的公共密钥 和代表自己身份的信息（如身份证号码或E-mail地址），CA验证了用户的有效身奠螅蛲没O浞⑭桓鬟A私有密钥签名的证书。 （3）证书的树形验证结构 在两方通信时，通过出示由某个CA签发的证书来证明自己的身份，如果对签发证书的CA本身不信任，则可验证CA的身份，依次类推，一直到公认的权威CA处。就可确信证书的有效性。SET证书正是通过信任层次来逐级验证的。通过SET的认证机制，用户不再需要验证并信任每一个想要交换信息的用户的公共密钥，而只需要验证并信任颁发证书的CA的公共密钥就可以了。 2．招商银行CA方案 我国的电子商务正在发展，各种规范要求还没有形成。目前招商银行、中国银行、中国建设银行、中国工商银行都再准备开发网上银行业务。这里以招商银行为例介绍其CA方案。 招商银行CA系统用于Web服务器的SSL公开密钥证书，也可以为浏览器客户发证，在SSL协议的秘密密钥交换过程中加密密钥参数。今后会开发其它的密码服务，并在国家有关部门规定下开展公开密钥认证服务。 CA系统处于非联机状态，运行CA的系统在私有网上，用户不能通过Internet访问。CA会在Web服务器上提供查询和客户证书申请接口，用户可以查询证书状态，提

交证书请求。Web服务器运行CA数据库的一个独立副本，与CA没有网络连接。 本方案采用层次认证结构，层次设置采用PEM规定的认证层次，设置以下目标类型： IPRA（Internet Policy Registration Authority）：IPRA负责管理认证策略，认证PCA，检查PCA运行与其策略的一致性。 PCA（Policy Certification Authority）：PCA负责根据业务需求指定认证策略，交IPRA审批，根据认证策略认证下一级CA，保证CA运行与策略的一致性。 CA（Certification Authority）：CA根据需要，选择相应的认证策略，提供用户公开密钥认证 用户：用户就是X.509中的最终实体。 RA（Registration Authority）：当用户与CA通信有困难时，CA就不可能对用户进行身份鉴别，就由RA代替CA，根据CA的业务要求进行用户身份鉴别。 CA管理提供CA密钥管理，认证策略管理和配置，以及服务级别的管理。CA管理的一个重要职能是CA密钥和策略管理。包括：生成新的密钥对、安装证书、撤消证书、备份CA的私有密钥、安装备份的CA私有密钥等。这些功能需要两个安全管理员同时注册才能完成。 目前，CA支持以下公开密钥算法：RSA/DH/DSA，并可提供上述密钥的证书，计划将增加对椭圆曲线加密算法的支持。此外，为了提高CA密钥的安全性，必须对CA密钥加密后保存，今后CA所有与密钥有关部门的操作将在IC卡中完成。 