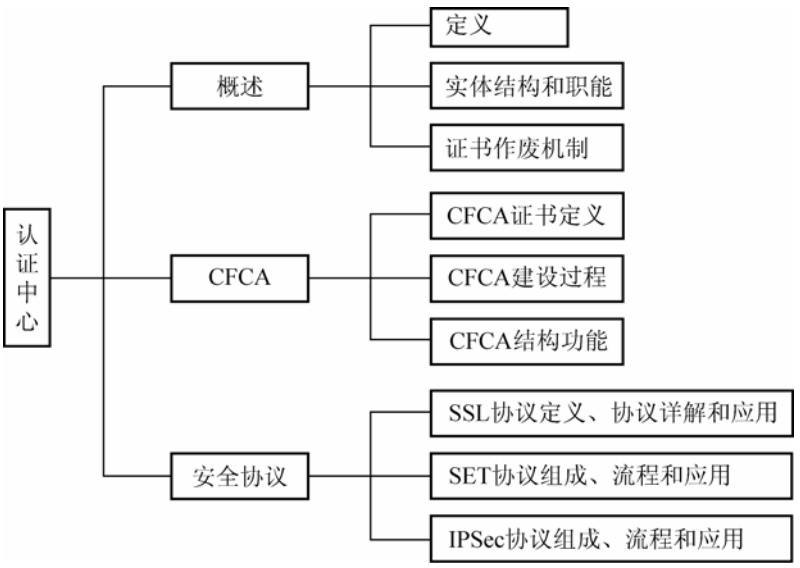
第10章 认证中心

教学目标与要求

- 掌握认证中心的定义、组成、职能;
- 了解中国金融认证中心的建设;
- 掌握 CFCA 的结构和功能;
- 掌握 PKI 证书及其优势;
- 掌握 SSL 安全协议;
- 了解 SET 安全协议、IPSec 协议。

知识架构



导入案例

互联网远程教育系统数字证书方案

互联网远程教育与通常的教育模式、教育手段有较大的不同。它可建立网络的虚拟课堂，能充分调动同学们互动的积极性。该教育特点是远程的，学生、教师、学校分布在不同地方，在不直接面对面的情况下进行。那么各类角色的身份的认证、数据安全的保障，是网络教育系统中必须要解决的问题。互联网远程教育随即引入了数字证书的解决方案。

网络教育是一种典型的 Internet 应用，它与电子政务、电子商务的应用非常类似。因此其 CA 体系下的数字证书技术也同样适用于网络教育应用。以下内容是应用于互联网远程教育系统的一个数字证书方案。该方案简述了基于 PKI 体系的安全网络教育系统功能模型(图 10.1)，提出了数字证书技术在网络教育中的几个应用方向，并描述了安全业务流程。

1. 基于 PKI 体系的安全网络教育系统功能模型

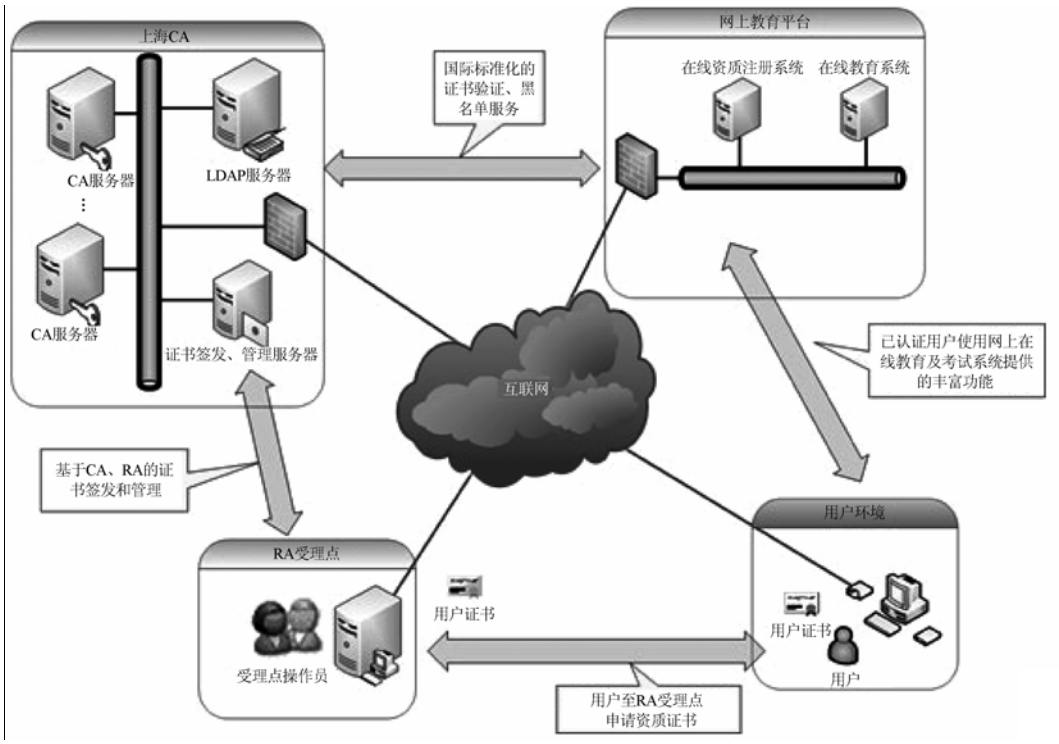


图 10.1　基于 PKI 体系的安全网络教育系统功能模型

2. 数字证书技术在网络教育中的应用

网络教育的安全应用包括多个方面，比如学生信息、教师认证信息、学生学籍成绩管理、学生网络缴费、在线答疑、在线考试、网络教育资源等。

1) 身份认证

在网络教育中，学生和教师都需要通过系统远程登录进行学习和工作。首要解决的就是身份认证和身份信息的管理。如图 10.1 所示的网络架构中，通过 PKI 的体系实现了各个角色的身份认证。同时保证了在身份的传递过程中信息的私密性。

在通过网络认证登录后，学生网上作业、网上考试，老师批改作业、批改试卷、成绩登记，可采用数字签名技术对老师和学生进行身份认证，可采用数字信封技术对考卷信息进行加密，防止冒名顶替、篡改分数情况的发生。在学生信息中，最敏感的是学校颁发的毕业证书/学位证书。在本方案中，学历/学位证书可以电子证书的方式在网上发布，在电子证书中包含授予证书的学校的数字签名，可保证电子证书不被篡改，保证其真实性。

2) 网上交费

网络教育中学生的远程分散特点使得集中缴纳学费比较困难。在电子商务中，有各类的支付工具，同理学费的缴纳同样可以建立这么一套支付模式。网上交费支付型业务是适用于网络教育的一种重要交费手段。利用基于数字证书技术的网上支付系统，与银行联网，提供安全的网上支付功能，从而实现网上交费。学生通过互联网即可完成各种费用的交纳，比如交纳学费、教材费、报名费等。网上交费也是安全网络教育的一个重要应用方向。

3. 安全业务流程示例

1) 在线考试

在线考试是网络教育中非常典型的应用场景，也是非常关键的应用。下面就在线考试的加密过程进行详细的描述。

在下面的业务环节中，考生使用客户端简称客户端，考试服务器简称服务器。

(1) 客户端向服务器发出考试请求，请求报文内容包括：考试课程 + 考生相关信息(姓名、学号等) + 考生的证书 + 数字签名。考试请求用考生本人的秘密密钥签名并以数字签名方式传送。

(2) 服务器接收考试请求，利用报文中考生的证书中的公钥验证数字签名，验证考生的身份，验证通过，继续以下流程；否则结束客户端请求。

(3) 通过验证后，服务器向考生发送考试响应。响应报文包括：考卷 + 服务器证书 + 数字签名 + 数字信封。数字信封包含一个对称密钥，考卷信息和服务器签名信息被该对称密钥加密后传送。

(4) 客户端利用私钥解开数字信封获得对称密钥，并使用该对称密钥解开加密的考卷、考试服务器证书及签名，最后通过服务器证书中的服务器公钥验证签名来验证服务器身份，该验证过程通过后，可在客户端答卷。

(5) 考试答卷完毕，提交答卷。提交的请求报文的内容为：答卷 + 考生证书 + 数字签名 + 数字信封。

(6) 服务器接收答卷提交请求。利用自己私钥解开数字信封中的对称密钥解开密文，验证考生数字签名，验证通过后，接受答卷存储，返回响应。响应报文信息以数字签名形式发送。

(7) 考生接收响应，验证数字签名，得到提交结果。

从以上流程可以看出，利用数字签名验证双方身份；敏感信息或需保密信息如考卷、答卷，利用数字信封进行加密传送，同时利用数字签名防止篡改或防抵赖。数字证书技术可以从数据保密性、完整性、身份认证、防抵赖几方面保证在线考试的安全。

2) 网络教育资源的版权保护

教师的重要课件、文件等学习资源，可利用数字信封技术、签名技术进行加密并签名，只有通过认证的具有合法身份的学生才能解密、阅读，同时对阅读的资料进行水印处理，实现版权保护。

资源下载中的安全处理流程如下。

(1) 学生向资源服务器发送资源请求，资源请求报文内容为：资源名称 + 学生信息 + 学生证书 + 数字签名。

(2) 资源服务器接收资源请求，利用学生证书验证数字签名是否正确，如果验证通过，则取得资源信息、学生信息，查询该生是否具有该资源的下载权限，如果有权限，则进行下一步；否则拒绝该请求，结束此流程。

(3) 资源服务器向学生客户端发送资源响应，资源响应报文内容为：资源 + 服务器证书 + 数字签名 + 数字信封。

(4) 学生客户端接收响应，利用自己私钥解开数字信封获得对称密钥，利用对称密钥解开密文，获得资源 + 服务器证书 + 数字签名，验证签名以验证服务器身份，保存资源。

从以上流程可以看出，利用数字签名可以验证学生身份，利用数字信封可以加密资源，防止资源被非法用户获取，实现数字版权保护。

总体来说，PKI 认证体系的建立，有效处理了远程教育系统中所涉及的安全问题，有效保障了网络教育信息化的安全性，从而拓展了远程教育的应用范围与应用场景，维护了远程网络教育体系的严肃性和公正性。

资料来源：http://www.sheca.com，上海数字证书认证中心。

10.1 认证中心概述

为解决互联网的安全问题，世界各国信息安全业者进行了多年的研究，形成了全方位、多层次的安全解决方案。其中，目前被广泛采用的 PKI 技术，在安全解决方案中占据了重要位置，它可以保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

一个完整的 PKI 系统是由认证机构、密钥管理中心(KMC)、注册机构、目录服务以及安全认证应用软件、证书应用服务等部分组成。其中，认证机构在 PKI 系统中居于核心地位。

认证中心(Certificate Authority，CA)为安全电子交易中的重要构件。它是一个公正、公开的代理组织，接受持卡人和特约商店的申请，会同发卡及收单银行核对其申请资料是否一致，并负责电子证书的发放、管理及取消等事宜。认证中心是在线交易的监督者和担保人，主要进行电子证书管理、电子贸易伙伴关系建立和确认、密钥管理、为支付系统中的各参与方提供身份认证等。CA 类似于现实生活中公证人的角色，具有权威性，是一个普遍可信的第三方。

目前在国内存在的 CA 基本上可以分为 3 类：第一类是行业性的 CA，如中国金融认证中心(CFCA)、海关 CA、商务部 CA(国富安 CA)等，这些 CA 是由相应行业的主管部门牵头建立的；第二类是地方性 CA，如北京 CA、上海 CA、浙江 CA 等，这些 CA 是由当地地方政府牵头建立的；第三类 CA 是商业性 CA，如天威诚信 CA，这类 CA 进行商业化经营，并不从属于任何行业或地域，但它们也必须具有良好的公信力，必须由国家主管部门审批通过才能投入运营，以确保其权威、公正性。

CA 中心的安全性、可信性、可靠性决定了安全电子交易的成功与否。本章从认证中心的定义入手，讨论认证中心实体结构的特点以及提供的各种基本职能，分析 CA 的作废证书列表的通用结构，比较并给出 CA 的各种作废证书机制的特点和适用范围。

10.1.1 认证中心的定义

在安全电子交易中，为了确保信息传输的过程中信息的机密性、真实性、完整性和不可否认性，通常采用公开密钥加密机制。而公钥机制所涉及的公钥是在互联网上公开传送的。因此，需要解决的一个重要问题就是公钥的信任问题。这就必然要求有一个可信任的机构对任何一个主体公钥进行公证，证明主体的身份以及它与公钥的匹配关系。CA 就是这

样的机构。为了确保 CA 的公信力，它必须具有高度的权威性、公正性和第三方性。

因此，CA(Certficate Authority)又称权威认证中心，是电子交易中信赖的基础，主要负责产生、分配并管理所有参与网上交易的实体所需的身份认证数字证书，通过自身的注册审核体系，核实进行证书申请的用户身份和各项相关信息，使网上交易用户属性的客观真实性与证书的真实性一致。

CA 中心解决了公钥体系中公钥的合法性问题。为每个使用公开密钥的用户发放数字证书，用以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。证书中，CA 中心的数字签名使得攻击者不能伪造和篡改数字证书。因此，在电子交易的各个环节，交易各方检验对方数字证书的有效性则可确定其身份的合法性，从而根本解决用户信任问题。

CA 中心为网上交易各方的信息安全提供有效的、可靠的保护机制。这些机制提供机密性、身份验证特性(使交易的每一方都可以确认其他各方的身份)、不可否认性(交易的各方不可否认它们的参与)。它的建立对开放网络上的电子商务安全保障具有非常重要的意义。

10.1.2 认证中心的结构

CA 认证体系的实体大致可分为以下几部分：接收用户证书申请的证书受理者(RS)，证书发放的审核部门(RA)，证书发放的操作部门(CP)，记录作废证书的证书作废表(CRL)，提供人工服务的业务受理点以及证书使用者，如图 10.2 所示。

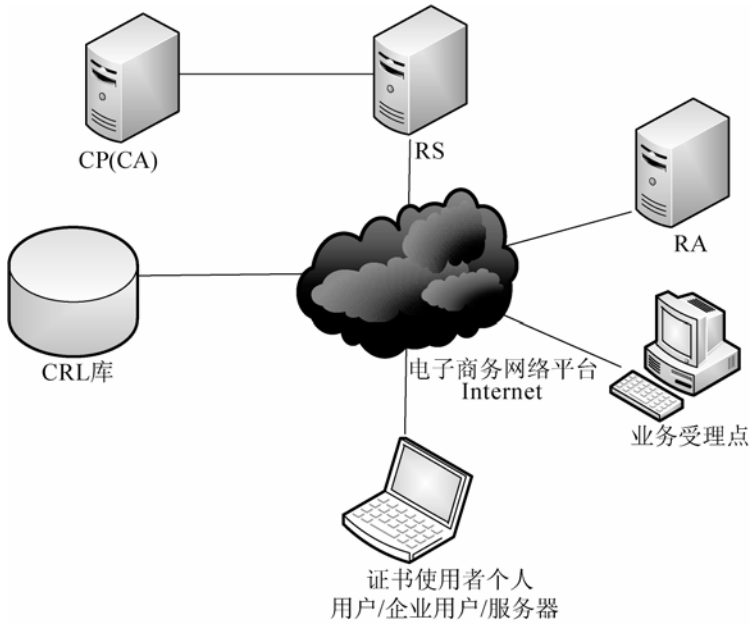


图 10.2 CA 中心的实体结构

RA 是证书发放的审核部门，负责对证书申请者进行资格审查。RA 也决定是否同意给该申请者发放证书，因此它应由能够承担这些责任的机构担任。

RS 是证书受理者，它用于接收用户的证书申请请求，转发给 CP 和 RA 进行相应的处

理。它也可以和 RA 合并在一起。

CP 是证书发放的操作部门，它负责为那些通过申请的人制作、发放和管理证书，它可以由审核授权部门自己担任，也可委托给第三方担任。

CRL 是证书作废表，又叫黑名单。其中记录的是一些已经有不良记录的用户。

业务受理点就是 CA 系统对外提供服务的一个窗口，由工作人员帮助用户录入、登记等。业务受理点可以作为用户证书发放的审核部门，当面审核用户提交的资料，从而决定是否为用户发放证书。

10.1.3 认证中心的职能

认证中心的基本职能是审批证书请求，发放证书，撤销证书，证书及 CRL 的存储、检索，密钥生存期管理以及 CA 自身的管理功能。其核心功能是发放和管理数字证书，具体描述如下。

1. 证书的审批

CA 通过自身的注册审核体系，以在线或离线的方式接收最终用户数字证书的申请，检查核实申请证书的用户身份和各项相关信息。根据相关法规确定是否接受最终用户数字证书的申请。

2. 证书的发布

CA 向申请者颁发证书的过程。即 CA 对包含用户公钥及其他相关信息的证书使用自己的私钥进行签名并最终颁发给用户。导致 CA 发布新证书的情况如下。

1) 初始化注册/认证

首次签发基于公钥密码体制的数字证书，并将证书返回给终端实体和公共资料库。

2) 证书更新

证书具有时效，当证书有效期满则需要重新发布证书。

3) 证书作废

当证书因某种原因作废时(如密钥对更新、私钥泄露等)，需要重新发布证书。

4) CA 密钥对更新

基于安全的考虑，CA 密钥对也会定期更新。

3. 证书的撤销

在网络环境中，如同日常生活中的各种证件，证书在 CA 为其签署的有效期以内也可能因多种原因需要作废。CA 撤销证书就是将有效的证书作废，并及时通知 PKI 系统的用户。通常的一种证书作废的方法是由 CA 周期性地发布 CRL(作废证书列表)数据结构。证书用户使用证书前不但要检查证书的签名和有效期，还需要通过访问一个最新发布的 CRL 来验证证书的有效性。

一般地，在下列非常事件发生时，必须进行证书的撤销处理。

(1) 持有者的私钥泄露。

(2) 持有者要求作废证书。

(3) 持有者的工作性质变化。

(4) 持有者消亡。

(5) 持有者身份标识错误。

如图 10.3 所示，在某种情况下证书所有者可申请证书撤销。这个请求可以向 CA 提出也可以向 RA 提出。环境允许时，经授权的管理者可以撤销终端实体的证书。

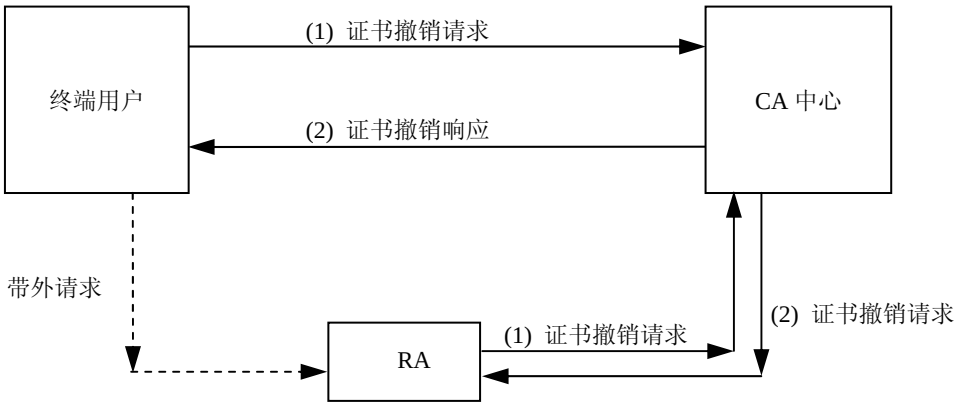


图 10.3 证书的撤销

4. 证书及 CRL 的分发、存储、检索

通常使用证书库来存储、检索证书及 CRL 的消息。所谓证书库，是指证书的集中存放地，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。

构造证书库的最佳方法是采用支持 LDAP 协议(Lightweight Directory Access Protocol)的目录系统。用户或相关的应用通过 LDAP 来访问证书库。使用目录系统来存放证书有很多好处：可透明地检索用户证书；支持大量用户；能快速、高效地响应检索证书要求；可满足企业分布式需要，实现证书分布式分发；具有良好的扩展性。其他的选择包括兼容 X.500 的目录、HTTP、FTP 和电子邮件。

5. 密钥生存周期管理

1) 密钥更新

证书、密钥对都有一定的生命期限，到期后需要更新；而当用户的私钥泄露时，则必须更换密钥对及证书；另外，随着计算速度的日益提高，密钥长度也必须相应地增长，这也提出了更换密钥对的需求。

2) 密钥存档

密钥或证书更新后，需要将更新前的密钥、证书归档，否则企业中那些用以前的密钥加密的历史数据就会变得无法读取，会造成历史记录的丢失，并使得责任无可追溯。

3) 密钥备份与恢复

用户常常忘记保护其私钥的口令或因各种原因而丢失密钥，系统可提供备份与恢复解密密钥的机制。值得强调的是，密钥备份与恢复只能针对解密密钥，签名私钥不能够作备份。

10.1.4 认证中心的证书作废机制

在使用证书时，除验证 CA 对该证书的签名外，还要确保该证书是可信、可用的。为实现这一点，PKI 必须提供作废证书的一系列机制。

CA 如何发布作废证书的机制是一个非常重要的问题。撤销信息更新和发布的频率将严重影响使用证书的交易系统的安全性。撤销证书的实现方法有多种：一种方法是利用周期性的发布机制，如证书撤销列表(CRL)；另一种方法是在线查询机制，如在线证书状态协议(Online Certificate Status Protocol，OCSP)。

1. CRL 结构

作废证书是通过将证书的唯一性序列号列入 CRL(废除证书列表)来完成的。通常，系统中由 CA 负责创建、签发并维护这些及时更新的 CRL，而由客户端应用程序代表用户在验证证书时负责检查该证书是否位列 CRL 之中。CRL 一般存放在目录系统中。

CRL 是一种包含撤销的证书列表的签名数据结构。它的完整性和可靠性由它本身的数字签名来保证。CRL 的签名者通常就是颁发证书的签名者。CRL 的一般结构如图 10.4 所示。

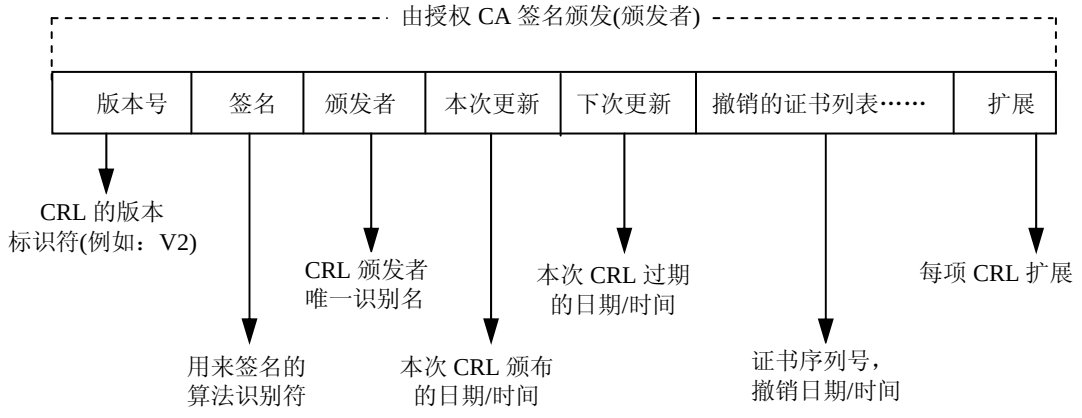


图 10.4 CRL 的结构

其中本次更新是指本 CRL 的发布时间，以 UTC Time 或 Generalized Time 的形式表示。下次更新是指下一 CRL 的发布时间。为验证证书的可信性，客户端程序可以在线或离线方式查询 CRL。撤销的证书列表包含的一系列被撤销的证书的序列号以及各证书不再有效的时间。每项 CRL 扩展使得在每个撤销里都可以携带该撤销证书的额外信息，如理由代码、证书颁发者、控制指示代码、无效日期等。

客户端程序可以通过缓存 CRL 来提高性能。CRL 的缓存使得既可以在线也可以离线验证证书。CRL 的缓存必须与相应的证书策略保持一致。

2. 周期发布机制

周期发布机制适用于 CRL 查询的离线操作，主要分为如下几种：完全 CRL、分段 CRL、增量 CRL、CA 撤销列表(Authority Revocation List，ARL)，它们全都基于同样的基本数据结构，即证书撤销列表 CRL。

1) 完全 CRL

完全 CRL 将所有的撤销信息都包括在一个 CRL 内，它仅对终端实体数目相对较少且证书撤销不频繁的 CA 域比较合适。原因如下。

(1) 颁发的规模性。因为撤销信息必须在已颁发证书的整个生命期内存在，这就有可能导致在某些 CA 域内完全 CRL 变得非常庞大。这就带来了另一个问题，即每次 CRL 分发会大量消耗网络带宽和客户机处理能力。并且，业务伙伴可能需要几天的时间才能收到有关撤销证书的通知，从而增加了破坏安全性的可能。

(2) 撤销信息的及时性。随着 CRL 的增加，CRL 的验证周期也将会变得很长。因为如果经常下载新的、很大的 CRL，将会对网络通信造成不可接受的性能下降。这就影响了查询到的撤销信息的及时性。

影响某个 CA 域中完全 CRL 大小的主要因素是终端实体的数目、撤销的概率、已颁发证书的验证周期和证书序列号的大小。在证书机构没有经常签发 CRL，或由于撤销证书的数量很大或用户基础很大的情况下，完全 CRL 通常会变得太大而难以使用。因此可以合理地得出完全 CRL 并不适用于许多环境这一结论。

2) 分段 CRL

分段 CRL 允许一个 CA 的撤销信息通过多个 CRL 发布出来。它和完全 CRL 相比有几个明显好处。首先，撤销信息可以被分成很多可控的片段以避免 CRL 过于庞大。其次，在证书中可以指出分段 CRL 的分布位置，这样用户就不需要提前知道关于特定证书的撤销信息的存放位置。与完全 CRL 相比，分段 CRL 提供了一种扩展性更强的替代方法。当它与缓存机制结合使用的时候，可以有效地解决性能问题。

3) 增量 CRL

增量 CRL 主要用于增强实时性。其基本原理是避免每撤销一个证书就产生一个完整的、潜在会变得越来越大的 CRL，而只产生新增加的证书撤销信息。当然，有了增量 CRL 并不意味着不需要完全 CRL 或分段 CRL。根据定义，增量 CRL 是以已颁发的撤销信息为基础的。已颁发的撤销信息称为基本 CRL。增量 CRL 可以比基本 CRL 的颁发频率高得多，从而可显著改善性能和实时性。

例如，考虑一个 CA 域的操作性能，限制完全 CRL 的发布仅为每周一次，而该 CA 域内的安全策略又规定当一个证书撤销后，撤销消息必须在 8h 内发布。显然，操作性能的问题和实时性的要求在撤销信息的发布上是彼此矛盾的。解决办法就是每周颁发一次基本 CRL，每 8 小时颁发一次增量 CRL。这样，每周只需下载一次庞大的 CRL，而相对小的增量 CRL 就可根据需要随时下载了。

3. 在线查询机制

在企业对企业(B2B)及企业对客户(B2C)电子商务中越来越多地使用数字证书来保证在线交易的安全性。这一行为引发了对另一种安全性的需要，即对这类证书的有效性进行在线查询，实时响应。

最普遍的在线查询机制是 IETF 颁布的用于检查数字证书在某一交易时间是否有效的标准——在线证书状态协议(OCSP)。OCSP 实时在线地向用户提供证书状态，避免了离线处理中令人头痛的逻辑问题和处理开销。它为电子商务提供了一种实时地检验数字证书有

效性的途径，比下载和处理证书撤销列表(CRL)的传统方式更快、更方便和更具独立性，从而节省了时间和资金。

OCSP 是一种相对简单的请求/响应协议，它提供了一种从名为 OCSP 应答器的可信第三方获取在线撤销信息的手段，如图 10.5 所示。

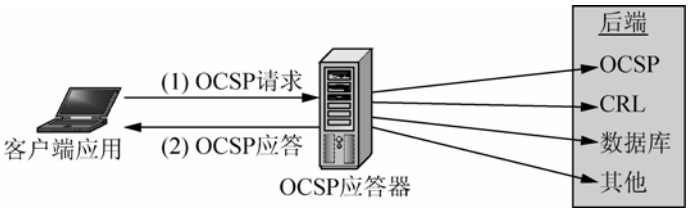


图 10.5　OCSP 在线查询机制

为实时地检查证书是否被撤销，用户的客户机必须形成请求，并将请求转发到一个 OCSP 应答器，即网络中保存最新撤销信息的服务器应用程序。(尽管 HTTP 是最通用的方式，但 OCSP 请求是独立于协议的。)

应答器收到请求后返回包括证书标识符，证书状态(“正常”、“撤销”、“未知”)的响应消息。如果一个证书的状态是“撤销”，就还要表明撤销的具体时间，也可能包括撤销的原因，这是可选的。

OCSP 的响应必须经过数字签名以保证响应是源于可信任方并且在传输过程中没有被改动。签名密钥可能属于颁发证书的 CA、一个可信任方，或是经过颁发证书的 CA 认可的实体。

OCSP 只是一个协议，具有一定的局限性。比如 OCSP 除了用来检查证书的撤销状态外，没有其他的功能。因此，它只能说明一个证书是否已被撤销，不验证该证书是否在有效期内，也无法验证是否被正确地使用。其次，它并没有明确用来收集撤销信息的后端的结构。如图 10.5 所示，它仍需要使用 CRL 或传统数据库或其他方式来收集撤销信息。对于使用 OCSP 应答器的用户来说，获得撤销信息的最佳途径是使证书机构将信息直接输入到应答器中。根据证书机构与 OCSP 应答器之间的关系，证书机构可以转发即时的通知或证书撤销信息，并且这些信息可以立即提供给用户。

总之，OCSP 的在线查询机制可以使各机构很容易地将多个应答器连接起来，方便企业对企业的交易。这意味着如果一家机构请求从应答器查询证书状态，若该应答器没有此证书信息，则应答器可以从其他应答器中获得这一信息。建立这种应答器网络，可以赋予贸易伙伴验证“国外”证书和在 Internet 共同开展业务的更多的灵活性。

10.1.5　认证中心的运作规范

从权威性、公正性出发，大部分 CA 都是作为独立的机构运营，为用户提供 PKI 数字证书认证服务，也有一些 CA 是作为本系统的 IT 单位之一，为系统内提供证书认证服务。

由于 CA 是 PKI 系统的核心，CA 的运作要求是很高的。如果 CA 出现故障停止对外服务，整个 PKI 系统就会瘫痪。因此，CA 自身的安全性显得无比重要。

CA 的安全是多方面的。从物理安全上讲，要求 CA 机房建筑必须防火、防水、防震、防电磁辐射、防物理破坏和外人侵入。防电磁辐射是防止入侵者企图通过仪器接收计算机

运算时发出的电磁波，来分析密码信息。为了达到这些目的，CA 机房墙面地板和天花板一般采用厚钢板六面体焊接，门也要采用电磁屏蔽门。此外，除了一般的人工把守的门禁外，还要安装双人双指纹检测的门禁系统以及磁卡门禁记录系统。CA 系统重要的操作必须有两人以上同时在场。

由于 CA 要与互联网相连，所以 CA 在网络安全防护上也要采取严密的措施以防止病毒、非授权访问和恶意攻击。为了确保 7×24 小时的不中断服务，系统必须采取高冗余度的配置，要求部署灾难备份中心。

CA 在人事管理上也是很严格的，在 CA 工作的员工必须安全可靠，要签署保密协议。按照信息产业部《电子认证服务管理办法》的规定，CA 的密码方案必须经过国家密码管理局的审批认证，CA 信息系统必须通过国家信息安全产品的评测认证，取得国家认可的资质，才能投入运营。

CA 的运作必须符合《认证运作规范(CPS)》。认证运作规范(Certification Practice Statement，CPS)是关于认证机构在全部数字证书服务生命周期中的业务实践(如签发、吊销、更新)所遵循规范的详细描述和声明。在 CPS 中，提供了相关业务、法律和技术方面的细节。它涉及 CA 的运营范围、遵循标准、证书生命周期管理、CA 的运作管理、安全管理、CRL 管理等全部范围。

根据 IETF RFC3647(公钥基础设施证书策略和证书运行框架)以及国家信息产业部《电子认证服务管理办法》、《电子认证业务规则规范》等规定，中国的 CPS 由 9 部分组成，分别如下。

(1) 概述性描述。
(2) 信息发布与信息管理。
(3) 身份识别与鉴别。
(4) 证书生命周期操作要求。
(5) 认证机构设施管理和操作控制。
(6) 认证系统技术安全控制。
(7) 证书、证书吊销列表和在线证书状态协议。
(8) 认证机构的审计。
(9) 法律责任。

这 9 部分内容详细地阐述了一个 CA 从诞生、运营，到生命终止的方方面面的规定，是 CA 的纲领性的文件。不但 CA 的运营者必须严格遵守 CPS 中的规定，CA 的 CPS 还必须在网站上公布，以接受证书持有者和依赖方的查询和监督。

10.2 中国金融认证中心

中国金融认证中心(China Financial Certification Authority，CFCA)于 2000 年 6 月 29 日挂牌成立，是经中国人民银行和国家信息安全管理机构批准成立的国家级权威的安全认证机构，是重要的国家金融信息安全基础设施之一，也是《中华人民共和国电子签名法》颁

布后，国内首批获得电子认证服务许可的 CA 之一。

CFCA 作为权威、公正的第三方安全认证机构，采用国际主流的 PKI(Public Key Infrastructure，公钥基础设施)技术，通过发放数字证书确保网上信息传递双方身份的真实性、信息的保密性和完整性，以及网上交易的不可否认性。为网上金融、电子商务、电子政务等行业提供安全认证服务。

现在各家银行为开展网上业务也都成立了各自 CA 认证机构，专门负责签发和管理数字证书，并进行网上身份审核，实现了权威的、公正的、可信赖的第三方的作用。这样，交易的双方在参加交易之前，就已经过了网络银行在互联网上的身份验证和确认。保证了买卖双方的真实身份，为安全的交易奠定了信任的基础。

10.2.1 CFCA 的建设

为解决电子商务网上支付的安全问题，在 1998 年 9 月的首都电子商务工程领导小组第二次会议上，由中国人民银行牵头组织中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、招商银行、中信实业银行、华夏银行、广东发展银行、深圳发展银行、光大银行、民生银行 12 家商业银行联合共建中国金融认证中心(CFCA)。在 1999 年 2 月 18 日，第 8 次金融信息化领导小组批准建设金融 CA 工程。该工程于 2000 年 6 月 29 日完成，中国金融认证中心(CFCA)挂牌成立，认证系统开通运行。

中国金融认证中心(China Finance Certificate Authority，CFCA)作为一个权威的、可信赖的、公正的第三方信任机构，专门负责为金融业的各种认证需求提供证书服务，包括电子商务、网上银行、支付系统等。在电子交易的各个环节，交易的各方都需验证对方数字证书的有效性，从而解决相互间的信任问题。中国金融认证中心通过数字证书为各类实体(包括个人/持卡人、企业/商户、银行/网关等)提供在网上进行信息交流及商务活动的身份证明，为网上交易提供安全的基础，建立彼此信任的机制。CFCA 不但满足电子商务的金融交易的服务认证需求，而且在中国电子商务发展中组织并参与有关网上交易规则的制定，确立相应的技术标准，提供跨行网上支付的相互认证。

金融认证采用 PKI 技术，能向各种用户颁发不同种类的数字证书来支持各成员行有关电子商务的应用开发。中国金融 CA 以金融行业的可信赖性及权威性支持中国电子商务的应用、网上银行业务的应用及其他安全管理业务的应用。其所适应的业务应用模式，包括网上银行、网上购物等 B2C、B2B 以及 B2G 的模式。

在系统建设初期，金融 CA 规模不大，预计每年发放 15 万张 Non-SET 证书(其中企业证书 3 万张，其余为 Web、SSL 证书等)；SET 证书 10 万张，企业 2 万张，个人 8 万张，SET 证书支持 SET 1.0 扩充版功能，既支持信用卡，又支持借记卡及 PIN 的处理。当 CA 完善后，扩大其应用范围，可发放 S/MIME、VPN 及特制 X.509 证书、支持无线 WAP 协议的证书。到 2006 年 7 月，CFCA 数字证书发放突破 100 万张。

中国金融认证中心的建立是我国金融系统建立金融最高认证权威的第一步，金融认证中心的建立对我国广泛开展电子商务活动以及建立网上银行、网上支付等现代金融、贸易活动起着巨大的推动作用，极大地提高网上支付的安全性。该项目的完成对我国金融市场的发展以及社会主义市场经济的完善都具有重大的现实意义和深远的历史意义。

10.2.2 CFCA 的组成部分

如图 10.6 所示，CFCA 主要由以下部分组成。

(1) CA 服务器：这是 CA 的核心，是数字证书生成、发放的运行实体，同时提供发放证书的管理、证书撤销列表(CRL)的生成和处理等服务。

(2) 证书下载中心：该中心连接在互联网上，用户通过登录 CA 网站访问证书下载中心，CA 服务器生成的证书通过证书下载中心供用户下载。

(3) 目录服务器：又称为 LDAP，它的功能是提供数字证书的存储，以及数字证书和证书撤销列表(CRL)的查询。该目录服务的技术标准遵循 LDAP (轻量级目录访问协议)。

(4) OCSP 服务器：该服务器向用户提供证书在线状态的查询。

(5) 密钥管理中心(KMC)：根据国家密码管理规定，加密用私钥必须由权威、可靠的机构进行备份和保管。CFCA 被授权建立 KMC，以备份和保管用户的加密密钥。

(6) 证书注册机构(Registration Authority，RA)：它负责受理证书的申请和审核，其主要功能是接受客户证书申请并进行审核。 RA 主要是远程的，CFCA 的 RA 部署在各家用户银行、税务机关或企业所在地。这样一方面便于进行客户资料的审查，另一方面也便于银行将证书与客户的账号进行绑定，以实现认证。但即使 RA 部署在远程所在地，这些 RA 也仍然是 CA 的组成部分。

此外，CFCA 还在其所在地部署了直属 CA，对一些比较零散的、不适合或者不必要建立 RA 的用户提供注册服务。

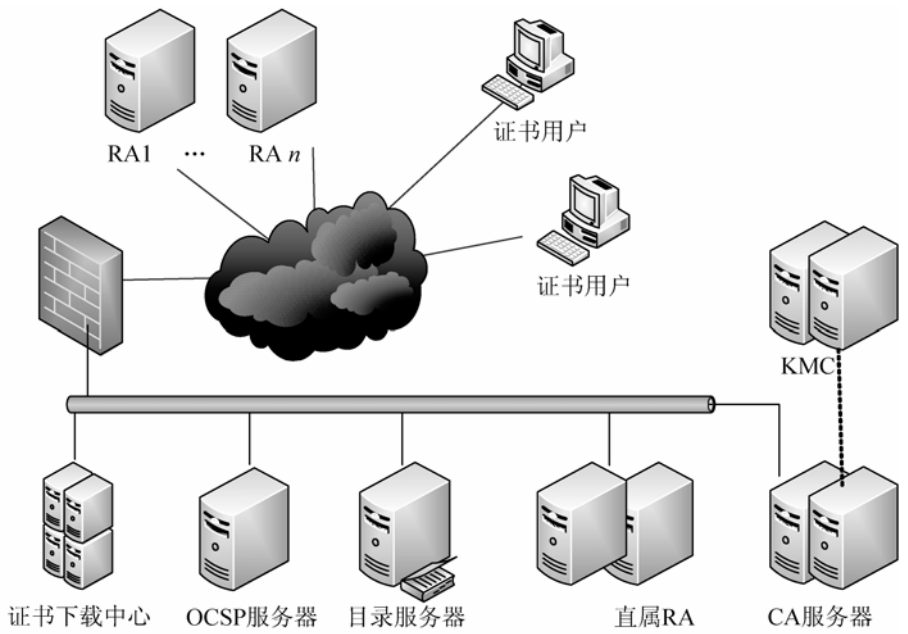


图 10.6 CA 的组成结构

10.2.3 CFCA 的结构

金融认证中心为了满足金融业在电子商务方面的多种需求，采用 PKI 技术，建立了 SET

和 Non-SET 两套系统，提供多种证书来支持各成员行及各应用单位对电子商务的开发以及应用。SET CA 由 IBM 承建，Non-SET CA 由 Entrust/SUN/德达承建。在业务模式上，CFCA 全面支持电子商务的两种主要业务模式(即 B2B 和 B2C)。SET CA 主要用于电子商务中的 B2C 业务模式的身份认证；而 Non-SET CA 则可同时支持 B2B 和 B2C 两种业务模式的身份认证。

1. Non-SET 系统

Non-SET 系统的逻辑结构对于业务应用的范围没有严格的定义。它结合电子商务具体的、实际的应用，根据每个应用的风险程度不同，把证书分为低风险值和高风险值两类证书，即个人/普通证书和高级/企业级证书。

Non-SET CA 系统逻辑分为 3 层结构，第一层为根 CA(Root CA)，第二层为政策 CA(Policy CA)，第三层为运营 CA(Operation CA)，如图 10.7 所示。针对运营的业务的不同，在运营 CA 层中分别有普通证书、高级证书、设备相关的证书。Non-SET CA 签发的各种证书，其主要目标是支持广泛的电子商务应用模式、网上安全银行应用模式、网上证券以及电子政务等广泛的应用。

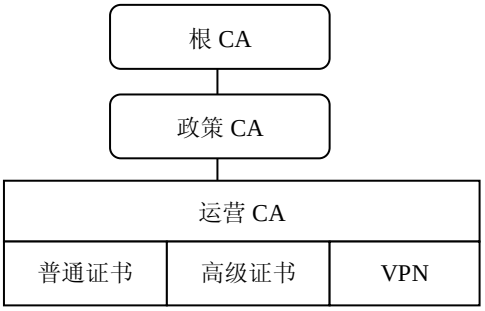


图 10.7 Non-SET 体系

1) RCA

系统结构的第一层为根 CA，即 Root CA(简称 RCA)。RCA 的职责是：负责制定和审批 CA 的总政策；为自己“自签”根证书，并以此为根据为二级 CA 签发并管理证书；与其他 PKI 域的 CA 进行交叉认证。

2) PCA

系统结构的第二层为政策性 CA，即 Policy CA，简称 PCA。PCA 的职责是：根据根 CA 的各种规定和总政策，制定具体政策、管理制度和运行规范；安装根 CA 为其签发的证书；为第三级 CA 签发证书；管理证书及证书撤销列表(CRL)。

3) OCA

系统结构的第三层为终端用户 CA，也称运营 CA(Operation CA)，简称 OCA。OCA 的职责是：安装政策 CA 签发的证书；根据根证书及二级 CA 证书，直接为最终用户颁发终端实体证书，即支持电子商务各种应用的数字证书；管理所发证书及证书撤销列表(CRL)。

当初设计这种结构的初衷是，CFCA 做成全国性的金融 CA，向公众提供服务，这样根 CA 的作用主要是负责制定和审批 CA 的总策略，向政策 CA 发放证书，以及与国际其他

PKI 域的 CA 进行交叉认证；3 个政策 CA 则分别负责制定和审批银行、证券、保险领域 CA 的策略，向运营 CA 发放证书；运营 CA 则负责颁发最终用户的证书。

由于 3 层结构 CA 的证书链较长，认证速度效率较低，而且认证业务并没有按原来所设想的方向发展，政策 CA 实际上只建了 1 个，原来的初衷未能实现。因此，CFCA 后来新建的 CA 系统全部采用 RCA—OCA 两层的扁平结构(图 10.8)，省去了政策 CA 这层。

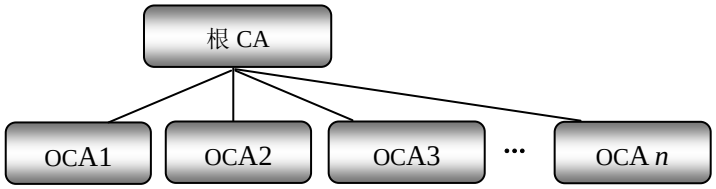


图 10.8　扁平结构 CA 系统

CFCA 的 Non-SET CA 系统是引入加拿大 Entrust 公司的产品。Entrust 公司是目前世界仅存的 3 家实力雄厚的 CA 公司(Entrust、Verisign、Baltimore)之一，CFCA 采用的 Entrust 公司的高级/企业级证书是目前世界领先的工具。

2. SET 系统

SET 协议使用 PKI 加密技术能提供信息的机密性，保证支付的完整性，验证支付网关、商家和持卡人的真实身份。SET CA 对其所签发的持卡人、商家和支付网关 3 种证书具有完善的证书管理功能。PKI SET CA 系统一般为层次结构。SET CA 总体上也分为 3 层总体结构。PKI SET CA 的总体结构如图 10.9 所示。

第一层 RCA(Root CA)，即根 CA；第二层 BCA(Brand CA)，即品牌 CA；第三层 ECA(End User CA)，即终端用户 CA。

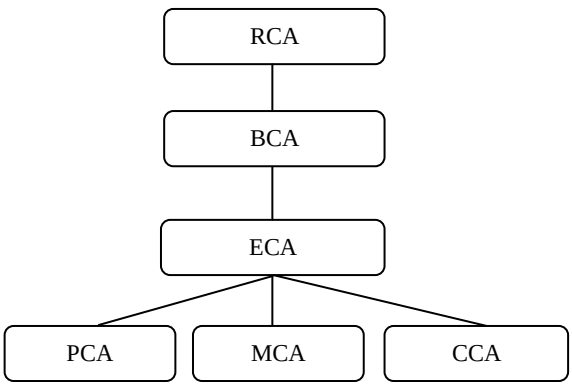


图 10.9　PKI SET 体系

1) RCA

系统结构的第一层为根 CA，简称 RCA。RCA 的职责是：负责制定和审批 CA 的总政策；签发并管理第二层 CA 证书；与其他根 CA 进行交叉认证。

2) BCA

BCA 为各个商业银行所发放的不同信用卡品牌发放证书。它的职责是：根据 RCA 的

规定，制定具体政策、管理制度及运行规范；签发第三层证书并进行证书管理。

3) ECA

系统结构的第三层 CA 为终端用户 CA(End User CA)，简称 ECA。ECA 为参与 SET 电子商务各实体颁发证书，即为支付网关(Payment Gateway)、商家(Merchant)及持卡人(Cardholder)签发证书。签发这 3 种证书的对应 CA 为 PCA、MCA 及 CCA。签发证书的目标是面向持卡人、发卡行、商家、收单行和支付网关。

SET 协议使用 PKI 加密技术能提供信息的机密性，保证支付的完整性，验证、支付网关、商家和持卡人的真实身份。SET CA 对其所签发的持卡人、商家和支付网关 3 种证书具有完善的证书管理功能。

10.2.4 CFCA 的证书

CFCA 作为国内重要的认证体系，提供适用于企业、个人 Web 站点、VPN、电子邮件、手机应用等在内的 10 多种数字证书服务。CFCA 采用 PKI 技术为基础的数字证书技术，有效地解决了电子商务中交易安全问题。我国于 2005 年 4 月 1 日正式颁布实施《电子签名法》，从法律上确认了电子签名的法律效力。因此，由 CFCA 颁发的 CA 证书，必要的时候可作为具有法律效力的证据。

目前 CFCA 在各个行业领域有广泛的使用，下面就其应用进行介绍。

1. CFCA 个人证书

CFCA 个人证书符合 X.509 协议，它面向个人用户，在网上信息传递过程中提供身份验证、信息加密和数字签名等功能。CFCA 个人证书通常又可分为个人高级证书和个人普通证书。其中，个人高级证书适用于个人作金额较大的网上交易，安全级别较高，可用于数字签名和信息加密。个人普通证书适用于个人用户用于 SSL、S/MIME，以及建立在 SSL 之上的应用，它的安全级别较低，常用于小额的网上银行和网上购物。

根据 X.509 协议，CFCA 个人证书中包含了用户身份信息(如身份证号码)、公钥信息、证书有效期等。CFCA 个人证书支持多种存储方式，比如 U 盘、硬盘文件等。

个人证书的使用需要结合到具体的应用平台中。比如，在银行申请网上转账服务，需要在指定行先申请个人证书；网上银行的服务器端安装服务器证书，用户端安装一张个人证书；进行网上转账时，网银系统会对证书有效性进行检查，只有双方证书都有效，才能建立安全传输通道。

CFCA 为保证安全性，为个人证书设置了有效期，一般为两年；个人证书到期时，需重新进行申请。CFCA 也支持网上证书自动展期功能。

个人证书需要结合到具体的应用平台中，如在个人网银系统中。

2. CFCA 企业证书

CFCA 企业证书面向企业用户，在网上信息传递过程中提供身份验证、信息加密和数字签名等功能。CFCA 企业证书通常又可分为企业高级证书和企业普通证书。其中，企业高级证书适用于企业作金额较大的 B2B 网上交易，安全级别较高，可用于数字签名和信息加密。企业普通证书适用于企业用户用于 SSL、S/MIME 以及建立在 SSL 之上的应用，它

的安全级别较低，常用于金额较小的网上交易。

CFCA 企业证书存储方式与个人证书一样，具有多种存储方式。与个人证书不同的是，企业证书中除了公钥信息、证书有效期外，还包含了企业的一些重要的信息，比如企业身份信息(如企业营业执照号)、企业法人、企业注册资金等。企业间的交易涉及大额的资金交割，为确保证书的安全，建议企业证书存放在 USB Key 里。相对于个人证书而言，CFCA 企业证书提供更高的安全性和更完善的支持服务。

企业证书的使用和验证方式同个人证书一样，都需要通过 CFCA 构建的验证体系，进行严格的认证过程。系统会对证书有效性进行检查。只有双方的证书都有效，才能建立安全传输通道。在安全传输通道中，使用企业证书中的密钥对交易数据进行加密传输，确保数据的完整性；对交易的关键数据进行数字签名，确保交易的不可否认。

为保证安全性，企业证书设置了有效期，一般为两年；企业证书到期时，需重新进行申请。CFCA 也支持网上证书自动展期功能。

3. CFCA Web 服务器证书

CFCA Web 服务器证书是为网站的 Web 服务器而设立，其目的是保证网站的 Web 服务器不被假冒，可在站点服务器提供金额较小的 B2C 网上交易时使用。若一个网站要提供 B2B 交易时，应申请 Direct Server 证书，并配合 Direct Server 软件来保证它的安全性。Direct Server 证书主要用于数字签名和信息加密。

服务器证书(以下称 Web Server 证书)是 Web Server 与浏览器用户建立安全连接时所必须具备的证书。Web Server 证书的密钥对由相应的 Web Server 自己产生和管理，申请证书时只需将 Web Server 产生的证书申请数据包提交给 CFCA 证书下载中心即可，密钥位长为 512 位(或 1 024 位)。按照 CFCA 证书申请和下载的流程，CFCA 下载中心将返回证书应答，即可将证书装载到 Web Server 中。

目前，CFCA 能够签发 Netscape Web Server，Microsoft IIS Server，Apache Web Server 等 WWW 服务器的证书。

Web 服务器证书与个人证书和企业证书的使用目的和功能不同，因此其证书中涉及的信息也不相同。Web 服务器证书中包含了网站的服务器域名信息、公钥信息、证书有效期等。通过服务证书，用户客户端能够通过该证书对网站的真实性进行检查。同时，利用服务器证书的加密机制将用户浏览器和服务器之间传输的信息进行加密。加密后的信息只有对应的服务器才能解密。

CFCA Web 服务器证书支持的 Web 服务器包括：IIS、iPlanet、Apache、IBM HTTP Server、BEA Weblogic、IBM WebSphere、Tomcat 等 WWW 服务器。

为保证安全性，Web 服务器证书设置了有效期，一般为两年；Web 服务器证书到期时，需重新进行申请。

4. CFCA 手机证书

随着 3G 网络的部署，互联网快速延伸到无线用户群体。现有 Web 资源的随时随地地接入，实现移动银行、移动证券、移动购物等各种形式的移动商务及服务。但无线模拟与数字信号传输仍是不安全的，无线数据通道可能受到攻击，需要解决其安全问题。

CFCA 手机证书支持无线 PKI 机制，提供基于 WAP 和短信息等方式的手机证书。由于手机终端采用的平台和技术具有较大的差异等原因，CFCA 手机证书支持多种应用模式，提出针对性解决方案。例如针对短信息模式的应用中，移动用户以短信息的形式将请求及指令发往移动运营商，移动运营商将信息转换，使用 TCP/IP 协议发往移动商务平台，由该平台转发对应的应用服务提供商，采用证书机制能够验证移动用户、移动设备的身份、认证经加密发往各服务器的信息。

5. CFCA 安全电子邮件证书

在互联网的应用中，电子邮件已经成为一个普遍而重要的通信工具。正是其广泛的应用，随之而来的种种安全隐患也日渐暴露。电子邮件在互联网上传递，其安全问题显而易见。首先，端到端的传输过程是明文，没有任何安全措施；其次，电子邮件系统具有开放性，用户邮件中的保密信息、个人隐私很容易被木马程序或者黑客所窥视及修改。再次，邮件的所有投递都要经过邮件服务器，邮件服务器的安全性更是值得关注的焦点。

针对电子邮件的安全性要求，CFCA 安全电子邮件证书为邮件体系中的各个环节建立了安全、认证和防护能力。CFCA 专门为邮件用户发放数字证书，邮件用户使用数字证书发送加密和签名邮件，来保证用户邮件系统的安全。邮件用户使用数字证书对电子邮件进行数字签名并加密传输，以证明邮件发送者身份的真实性，保障邮件传输过程中不被他人阅读及篡改，并由邮件接收者进行验证，确保电子邮件内容的完整性。

CFCA 安全电子邮件证书遵循国际数字证书 X.509 V3 标准，采用对称密钥长度为 128 位，非对称密钥长度为 1 024 位的密码机制，确保证书在进行邮件加密时的高安全性。

使用时，需要在 Outlook、Outlook Express、Foxmail 等邮件客户端软件上安装并设置申请号的 CFCA 电子邮件证书。

6. VPN 设备证书

VPN 是 Virtual Private Network，即虚拟专用网的缩写。VPN 应用于多种不同的应用场景。

(1) 远程接入：可以让远程用户在需要时接入企业网络资源。

(2) 分支机构办公：在远距离的办公室间建立持久的 VPN 连接。

(3) 广域网：在互联网上，让业务伙伴可以接入共同的资源。

VPN 模式与传统专线和电话网拨号连接模式相比，具有更高的经济性、灵活性、开放性。VPN 的接入需要专业的 VPN 设备，CFCA 对于 VPN 设备提供了设备证书。设备证书保证数据的安全合法，包括保证 VPN 设备的真实性，保证接入端的合法登录，保证信息传递的私密性。

CFCA VPN 设备证书增强了 VPN 机制的安全性。CFCA VPN 设备证书为 VPN 机制提供身份认证机制和数据加密能力。

10.2.5 CFCA 的功能

CFCA 是按国际通用标准开发建设的，它具有对用户证书的申请、审核、批准、签发证书及证书下载、证书注销、证书更新等证书管理功能。证书符合 ITU 的 X.509 国际标准，

提供具有世界先进水平的 CA 认证中心的全部需求。CA 的核心功能就是发放和管理数字证书，归纳起来有以下几个方面。

1. 证书的申请

CFCA 授权的证书的注册审核机构(Registration Authority，RA)(各商业银行、证券公司等机构)面向最终用户，负责接受各自的持卡人和商户的证书申请并进行资格审核，具体的证书审批方式和流程由各授权审核机构规定。

申请方式包括离线申请方式和在线申请方式。离线方式即面对面申请，用户方(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，同时提供有关的证件，申请信息是手工录入的。申请银行支付网关证书，只能到 CFCA 的 RA 申请，不能面对面申请。在线申请方式即用户在互联网上，通过自己浏览器，连接到银行主服务器上，下载标准表格，按内容提示进行表申请，也可以通过电子邮件和电话呼叫中心传递申请表格的有关信息，以便进行审核。

2. 证书的审批

当 CFCA 接到用户(包括下级 CA 和最终用户)的证书申请，首先将申请的内容存入数据库，并根据申请的内容验证用户的合法性，确定是否接受最终用户数字证书的申请。审批方式包括离线审核方式和在线审核方式。

经审批后，RA 将审核通过的证书申请信息发送给 CFCA，由 CFCA 签发证书。在 Non-SET 系统中，CFCA 将同时产生的两个码(参考号、授权码)发送到 RA 系统。为安全起见，RA 采用两种途径将以上两个码交到证书申请者手中：RA 管理员将授权码打印在密码信封里当面交给证书申请者；将参考号发送到证书申请者的电子邮箱里。在 SET 系统中，由持卡人/商户到 RA 各网点直接领取专用密码信封。

3. 证书的发放

在 CFCA 的所有功能中，最为重要的是证书的发放。CA 签发的证书格式符合 X.509 V3 标准。CA 对其签发的数字证书全部内容，包括证书用户姓名标识、公钥信息、颁发者标识、证书有效期、签名算法标识等信息，进行数字签名，从而权威地证明了证书持有者和公钥的唯一匹配关系。

证书在本地生成，证书由 CFCA 颁发，用户私钥由客户自己保管。证书发放方式包括离线方式发放和在线方式发放。在线方式中，在明确给用户颁发何种类型的证书(个人证书、企业证书、服务器证书或其他证书)后，CFCA 用自己的私钥对证书进行签名，然后将证书数据写入数据库。为保证消息的完整性，返回给用户的所有应答信息都要使用 CFCA 的私钥进行签名。

具体的证书发放方式各个 RA 的规定有所不同。可以登录 CFCA 网站 http://www.cfca.com.cn 联机下载证书或者到银行领取。

4. 证书的归档

当证书过了有效期之后就将撤销，但是撤销的证书不能简单地丢弃，因为如果有时需要验证以前的某个通信过程中产生的数字签名，就需要查询撤销的证书。基于此种考虑，

CFCA 具备管理撤销证书和撤销私钥的功能，用于密钥和证书的恢复。

5. 证书的撤销

证书的撤销有两种情况：第一种情况是证书的有效期已到，CFCA 自动将过期的证书撤销；第二种情况是由于用户的私钥泄密、丢失或是忘记保护私钥的口令等原因，造成用户证书的撤销。这时用户需要向 CFCA 提出证书撤销的请求，CFCA 根据用户的请求确定是否将该证书撤销。CFCA 通过定期发布证书撤销列表(CRL) 接收最终用户数字证书的撤销请求。

6. 证书的更新

为提高系统的安全性，CFCA 可定期更新所有用户的证书，或者根据用户的请求来更新证书。这时 CFCA 重新生成新的密钥对并颁发新的证书，妥善处理作废的密钥和证书。其中，包括人工密钥更新和自动密钥更新。

7. 证书撤销列表的管理功能

产生和发布证书撤销列表(CRL)。其管理功能包括证书撤销原因的记录、CRL 的产生及其发布、企业证书及 CRL 的在线服务功能。

8. CA 的管理

规定根证书、个人证书、企业证书、服务器证书的密钥长度、有效期、是否备份等策略。

9. CA 自身密钥的管理

CA 自身密钥的管理，必须确保其具备高度的机密性，防止其被伪造而颠覆 CA 的权威性。在 CFCA，根密钥被存放在安全的屏蔽机房，其访问受到了严格的管理。CA 的密钥由通过国家认证的加密机产生，私钥一经产生则不能通过明文方式离开加密机。这些措施保证了 CFCA 根密钥的安全与 CFCA 的权威性。

10.2.6 CFCA 的发展

中国的 PKI 市场起步较晚，CFCA 作为国内较早的运营 CA，在 2000 年正式对公众提供服务。由于当时国内并没有成熟的 CA 软件提供商，经过严格的国际招标流程，CFCA 选择采用 Entrust 公司提供的 CA 系统软件产品进行认证服务。在 CFCA 运营之初，Entrust CA 软件由于其严谨的设计、强大丰富的功能，对 CFCA 业务发展起到了积极的推动作用。但随着客户的增加，其弊端也不断地暴露出来。由于其本土化能力有限，产品支持是一个难题，困扰着 CFCA 的业务拓展。同时其高昂的收费策略也影响了 CFCA 的持续发展。

随着国内 CA 产品系统的日渐成熟，以及国家对于 CA 业务的重视程度不断提高，2002 年，在科技部和人民银行的大力支持下，CFCA 国产化改造被列入国家 863 计划，得到了中国人民银行、国家科技部、国家密码管理局和中国银联的高度重视和支持。经过各方努力，2004 年年底，CFCA 国产化 CA 项目宣告完成，正式对外提供服务。2005 年 5 月，该系统正式通过科技部 863 项目验收，并开始大规模应用。专家评价，CFCA 国产化 PKI/CA

系统是我国银行业信息安全基础设施的一项重大技术成果，完全可以满足未来我国金融行业大容量用户和快速发展的业务需求，对于提升我国金融信息安全保障能力具有重要意义。截至 2007 年 9 月，CFCA 国产化系统共发放证书 50 万余张。同时，CFCA 开发人员经过多年的开发和经验积累，不断向客户提供具有自主知识产权的丰富多彩的证书应用软件。国产 PKI 系统正成为 CFCA 的骄傲，推动着中国的信息安全事业更好地向前发展。

CFCA 国产化系统，采用国际主流的 PKI 技术，提供适用于企业、个人、Web 站点、VPN、安全 E-mail、手机应用等在内的 10 多种证书和各种信息安全服务，确保网上银行、网上证券、网上保险、网上税务、电子商务、电子政务、企业集团等的信息安全。为确保业务的可持续性，满足国家法律法规、国际认证要求，CFCA 建立了高水准的异地灾难备份系统。同时，中国金融认证中心本身是严格按照现代企业制度建立起来的，采用国际标准管理体制的市场化运作企业，并于 2004 年 12 月通过了 ISO 9000 质量管理体系认证。它拥有稳定可靠的系统，先进成熟的技术，严密、规范的内部运作流程，完善的三级支持服务体系。自成立以来，CFCA 已建立了覆盖全国的认证服务体系。目前，CFCA 的认证领域已经覆盖了绝大部分已经开办网上银行业务的商业银行(包括外资银行)，十几家证券公司、二十几家基金管理公司、五十几家企业集团、网上公积金、物流、煤炭领域，以及中国人民银行和中国银联若干应用系统、中央国债登记公司等，对我国广泛开展的电子商务特别是网上支付起着巨大的推动作用。

10.3 安 全 协 议

安全协议是认证中心的基础。安全协议保障了 PKI 体系中各类信息交互的数据保密性、完整性、一致性和不可抵赖性。下面主要介绍 SSL、SET 和 IPSec 这 3 种安全协议。

10.3.1 SSL 安全协议

SSL(Secure Sockets Layer，安全套接层)协议是由网景公司 1994 年底研究制定的基于 Web 应用的安全协议。该协议以及后续的作为 Internet 标准的传输层安全(Transport Layer Security，TLS)是安全访问 Web 服务器的最重要的标准。

该协议向基于 TCP/IP 的客户/服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息机密性等安全措施。通过在应用程序进行数据交换前交换初始握手信息来实现有关安全特性的审查。在 SSL 握手信息中采用了 DES、MD5 等加密技术来保护信息传输的机密性和完整性，并采用 X.509 的数字证书实现鉴别。主要适用于点对点之间的信息传输，常用于 Web Server 方式。

1. SSL 的结构

SSL 安全协议提供的基本服务主要包括以下几方面。

(1) 认证和鉴别用户和服务器的身份，使得通信双方能够确信数据将被发送到正确的客户机和服务器上。

(2) 加密数据以隐藏被传送的数据。

(3) 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 协议建立在传输层和应用层之间，包括两个子协议：SSL 记录协议和 SSL 握手协议，其中记录协议在握手协议下层，如图 10.10 所示。

<table>
<tr><td>SSL 握手协议</td><td>SSL 改变密码格式协议</td><td>SSL 警告协议</td><td>HTTP,FTP,…</td></tr>
<tr><td colspan="4">SSL 记录协议</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

图 10.10 SSL 记录协议和 SSL 握手协议

在 SSL 的体系结构中包含两个协议子层，其中底层是 SSL 记录协议层(SSL Record Protocol Layer)。

2. SSL 的握手协议

SSL 中的握手协议是在客户机和服务器之间交换消息强化和保障安全的协议，主要有以下 4 个阶段。

第 1 阶段：建立安全能力。客户通过网络向服务商打招呼，服务商响应。该阶段用来初始化逻辑连接，并建立与之相关的安全能力。在该阶段中，初始化了的交换的安全属性包括：协议版本，会话 ID，密文族，压缩方法，同时生成并交换用于防止重放攻击的随机数。同时，密文族参数包括密钥交换方法(Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换和另一种实现在 Fortezza chip 上的密钥交换)、加密算法(DES、RC4、RC2、3DES 等)、MAC 算法(MD5 或 SHA-1)、加密类型(流或分组)等内容。

第 2 阶段：服务器身份验证和密钥交换。服务器向客户发送 X.509 证书开始与客户协商双方认可的密钥。一般选用 RSA 密码算法，也有的选用 Diffie-Hellman 和 Fortezza-KEA 密码算法。有的还需要验证客户的可信度。

第 3 阶段：客户机验证和密钥交换。客户机验证服务器证书完成与服务器间的密钥协商。客户与服务商间产生彼此交谈的会谈密钥。

第 4 阶段：结束。该阶段客户与服务商之间相互交换结束信息，完成安全连接的建立。

当上述动作完成后，双方就可以使用协商产生的会谈密钥。即使盗窃者在网络上取得加密信息，由于没有掌握产生密文的加密算法也不能获得可用信息。

3. SSL 的记录协议

SSL 记录协议为 SSL 连接提供两种服务：机密性和报文完整性。使用 SSL 可保证信息的真实性、完整性和保密性。

SSL 记录协议定义了要传输数据的格式，它位于 TCP 可靠的传输协议之上，用于高层协议的封装，记录协议主要完成分组和组合，压缩和解压缩，以及消息认证和加密等功能。其步骤如下。

(1) 分段。每个上层应用数据被分成 2^{14}B 或更小的数据块。记录中包含类型、版本号、长度和数据字段。

(2) 压缩。压缩是可选的，并且是无损压缩，压缩后内容长度的增加不能超过 1 024B。

(3) 在压缩数据上计算消息认证 MAC。

(4) 对压缩数据及 MAC 进行加密。

(5) 增加 SSL 记录头。

在 SSL 协议传输过程中，所有的传输数据都被封装在记录中，记录的具体格式如图 10.11 所示。

内容类型	主要版本	次要版本	压缩长度
明文(压缩可选)			
MAC(0，16 或 20 位)			

图 10.11　SSL 记录协议字段

内容类型(8 位)：封装的高层协议。

主要版本(8 位)：使用的 SSL 主要版本。对于 SSL v3.0，值为 3。

次要版本(8 位)：使用的 SSL 次要版本。对于 SSL v3.0，值为 0。

压缩长度(16 位)：明文数据(如果选用压缩则是压缩数据)以 B 为单位的长度。

4. SSL 协议采用的加密算法和认证算法

SSL 协议 v2.0 和 v3.0 版本支持的加密算法包括 RC2(块加密)、RC4(流加密)、IDEA 和 DES，消息散列主要使用 MD5 算法生成。

在认证算法中，采用电子证书标准 X.509，通过 RSA 算法进行数字签名。其中，认证包括服务器的认证和客户端的认证。

服务器方与客户方分别拥有一对 RSA 的密钥对，在服务器进行认证时，只有正确的服务器写密钥加密的消息形成的数字签名才能被客户端解密，从而验证服务器的身份。同样，只有客户端的写密钥加密的内容才能被服务器读密钥正确地解开。在认证的过程中，所有的证书数据都需要通过 MD5 进行签名，保证数据的正确性和完整性。

5. SSL 协议的应用

SSL 安全协议是国际上最早应用于电子商务的一种网络安全协议，至今仍然有许多网上商店在使用。在点对点的网上银行业务中也经常使用。该协议已成为事实上的工业标准，并被广泛应用于 Internet 和 Intranet 的服务器产品和客户端产品中，如网景公司、微软公司、IBM 公司等领导的 Internet/Intranet 网络产品的公司已在使用该协议。结合 SSL 协议和数字证书，PKI 技术可以保证 Web 交易多方面的安全需求，使 Web 上的交易和面对面的交易一样安全。

10.3.2 SET 安全协议

SET(Secure Electronic Transaction)协议是为了在 Internet 上进行在线交易时保证信用卡支付的安全而设立的一个开放的规范。它是由 VISA 国际组织和万事达组织共同制定的一个能保证通过开放网络(包括 Internet)进行安全资金支付的技术标准。SET 协议 1.0 主要由 SET 业务描述、SET 程序设计规范和 SET 协议描述 3 部分组成。SET 1.0 版已经公布并可应用于任何银行支付服务。

SET 协议规定了交易各方进行安全交易的具体流程。在 SET 协议中，使用 DES 对称密钥算法、RSA 非对称密钥算法等提供数据加密、数字签名、数字信封等功能，给信息在网络中的传输提供了安全性保证。SET 协议通过 DES 算法和 RSA 算法的结合使用，保证了数据的一致性和完整性，并可实现交易以预防抵赖；通过数字信封、双重签章，确保用户信息的隐私性和关联性。

SET 协议本身比较复杂，设计比较严格，安全性高。它是 PKI 体系下的一个典型实现，同时也在不断升级和完善，如 SET 2.0 将支持借记卡电子交易。

1. SET 安全协议目标

(1) 提供支付和订购信息的机密性：防止数据被黑客或内部人员窃取。

(2) 保证电子商务参与者信息的相互隔离：客户的资料加密或打包后通过商家到达银行，但是商家不能看到客户的账户和密码信息。

(3) 解决多方认证问题：不仅对消费者的信用卡认证，而且对商家的信誉度认证，以及消费者、在线商店与银行间的相互认证。

(4) 保证网上交易的实时性：使所有在线支付过程实时、高效。

(5) 互操作性：规范协议和消息格式，促使不同厂商开发的软件具有兼容性和互操作功能，并可运行在不同的硬件和操作系统平台上。

2. SET 安全协议中的角色

(1) 消费者。包括个人消费者和团体消费者，按照在线商店的要求填写订货单，通过由发卡银行发行的信用卡进行付款。

(2) 在线商店。提供商品或服务，具备相应电子货币使用的条件。

(3) 收单银行。通过支付网关处理消费者和在线商店之间的交易付款问题。

(4) 电子货币(如智能卡、电子现金、电子钱包)发行公司，以及某些兼有电子货币发行的银行。负责处理智能卡的审核和支付工作。

(5) 认证中心(CA)。负责对交易对方的身份确认，对厂商的信誉度和消费者的支付手段进行认证。

3. SET 协议定义的工作流程

(1) 用户向商家发送购货单和一份经过签名、加密的信托书。信托书中的信用卡号是经过加密的，商家无从得知。

(2) 商家把信托书传送到收单银行，收单银行可以解密信用卡号，并通过认证验证签名。

(3) 收单银行向发卡银行查问，确认用户信用卡是否属实。
(4) 发卡银行认可并签证该笔交易。
(5) 收单银行认可商家并签证此交易。
(6) 商家向用户传送货物和收据。
(7) 交易成功，商家向收单银行索款。
(8) 收单银行按合同将货款划给商家。
(9) 发卡银行向用户定期寄去信用卡消费账单。

4. SET 的认证

在用户身份认证方面，SET 引入了数字证书和证书管理机构机制。

在 SET 中，证书记录用户的公共密钥和其他身份信息。其中最主要的证书是持卡人证书和商家证书。持卡人证书实际上是支付卡的一种电子化表示，由金融机构以数字签名形式签发，不能随意更改。持卡人证书使用单向哈希算法，根据账号、截止日期生成密钥。 商家证书用来表示可接受何种卡来进行商业结算，也由金融机构签发，不能随意更改。

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。

1) 证书管理机构

SET 中的 CA 是提供身份验证的第三方机构，是一个或多个用户信任的组织实体。例如，持卡人要与商家通信。持卡人从公开媒体上获得商家的公开密钥，但无法确定商家的信誉。于是请求 CA 对商家认证，CA 对商家进行调查、验证和鉴别后，将包含商家公钥的证书传给持卡人。同样，商家也可对持卡人进行验证。

在实际中，CA 可由大家都信任的一方担当。例如，在客户、商家、银行三角关系中，客户用的是由某个银行发的卡，而商家又与此银行有业务关系。在此情况下，客户和商家都信任该银行，可由该银行担当 CA 角色，接收、处理付款卡、客户证书和商家证书的验证请求。又例如，对商家自己发行的购物卡，则可由商家自己担当 CA 角色。

2) 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。

5. SET 标准的应用

SET 协议规定了参加电子交易各方在交易中的行为规范和信息交换的过程和规则，有助于实现安全、可靠的电子商务，得到了 IBM、HP、Microsoft、Netscape、VeriFone、GTE、VeriSign 等一些著名网络和计算机公司的支持。但是，SET 协议实施起来很复杂，因而在短期内推广 SET 协议还存在一定的困难。

10.3.3 IPSec 协议

IPSec(Internet Protocol Security)是 IETF(Internet Engineer Task Force)制定的网络层安全标准，它把几种安全技术结合在一起形成一个较为完整的体系，通过对数据加密、认证、完整性检查，可保证 IP 和 IP 层以上数据传输的可靠性、私有性和保密性。

IPSec 提供了一种标准的、健壮的以及包容广泛的机制，可为 IP 及上层协议(如 UDP、TCP 和 ICMP)提供安全保证。它用于在 IPv4 或 IPv6 上提供互操作、高质量、基于密码学的服务。IPSec 可以支持各种应用，可以在 IP 层次上加密或验证所有的通信量。这样，所有的分布式应用，包括远程登录、客户机/服务器、电子邮件、文件传输、Web 访问等都可以保证安全。

IPSec 支持的安全体系通常同操作系统相结合，集成在操作系统的内核中，成为协议本身的可选部分。

1. IPSec 安全体系结构

IPSec 安全体系结构的建立为 IP 层数据的传输提供多种安全服务，包括访问控制、数据起源验证、无连接的完整性、数据的机密性、防重播保护以及受限通信流量的机密性。通过一整套的服务，可以有效地保护 IP 数据报的安全。

这些服务是依靠 IPSec 协议簇来实现的。IPSec 协议簇由两个传输安全协议和一个应用层级的密钥管理协议组成。它们分别如下。

(1) AH(Authentication Header)：IP 认证头协议，提供访问控制、无连接完整性、数据起源身份验证和可选用的防重播功能。

(2) ESP(Encapsulated Security Payload)：安全载荷封装协议，提供访问控制、数据机密性、有限的通信流量机密性以及可选用的防重播功能。

(3) IKE(Internet Key Exchange)：密钥管理协议，提供密钥的自动安全分发和更新。

其中 AH 协议和 ESP 协议可单独使用，也可结合使用。每种协议都支持两种模式：隧道模式和传输模式。在传输模式中，协议主要是对上层协议如 TCP 和 UDP 进行加密，而隧道模式是将进入隧道的 IP 数据包封装在安全的 IP 帧中。在隧道模式下，信息封装是为了保护端到端的安全性，即在这种模式下不会隐藏路由信息。隧道模式是最安全的，但会带来较大的系统开销。

2. IPSec 的优缺点

1) IPSec 的优势

(1) 当 IPSec 在路由器或是防火墙中实现，可应用于所有跨越网络边界的通信量的安全保证。内部通信量不会引起与安全处理相关的开销。

(2) IPSec 低于传输层(TCP,UDP)，可以对应用程序和最终用户透明。

(3) IPSec 用来在多个防火墙和服务器之间提供安全性。

2) IPSec 的缺点

(1) IPSec 在实际应用中，需要公钥来完成。密钥分配相对复杂。

(2) IPSec 需要已知范围的 IP 地址或固定范围的 IP 地址，因此在动态分配 IP 地址时不太适合于 IPSec。

(3) 除了 TCP/IP 协议外，IPSec 不支持其他协议。除了包过滤之外，它没有指定其他访问控制方法。

3. IPSec 协议的应用

IPSec 的特征使它最适合构建可信的 LAN 到 LAN 之间的虚拟专用网 VPN，即内部网虚拟专用网。现在基于 PKI 技术的 IPSec 协议已经成为架构 VPN 的基础，可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。虽然它的实现比较复杂，但其安全性比其他协议完善。

IPSec 也可用于连接其他层已存在的通信协议，如支持安全电子交易(Secure Electronic Transaction，SET)协议和 SSL(Secure Socket layer)协议。即使不用 SET 或 SSL，IPSec 也能提供认证和加密手段以保证信息的传输。

由于 IPSec 是 IP 层上的协议，因此很容易在全世界范围内形成一种规范，具有非常好的通用性。而且 IPSec 本身就支持面向未来的协议——IPv6。总之，IPSec 还是一个发展中的协议。随着成熟的公钥密码技术越来越多地嵌入到 IPSec 中，相信在未来几年内，该协议会在网络安全领域扮演越来越重要的角色。

本 章 小 结

认证中心是一套由各种不同角色，通过认证体系有机的组成在一起的体系，它有效地保障了网络交易的各个角色的安全。CFCA 作为中国金融领域唯一合法的第三方安全认证机构，采用国际标准管理体制的市场化运作企业，通过了 ISO 9000 质量管理体系认证。基于 PKI 体系，已经建立并完善了数字证书服务和安全电子印章、时间戳、动态口令、网上银行托管、安全评估、IT 审计、安全产品测评、安全集成开发等多种信息安全服务。目前它的认证业务已覆盖网上银行、证券、保险、税务、电子商务、电子政务、企业集团等多个领域。

本章在基于认证中心的体系架构上，对认证体系中重要的 SSL 安全协议和 SET 协议进行了重点的讲解。SSL 协议的两层结构：握手协议和记录协议，每层协议使用下层协议的服务，并为上层协议提供服务。随后，对 SET 协议的交易流程、程序设计规范和 SET 协议进行了完整描述。SET 支付系统为交易流程中持卡人、商家、发卡行、收单行、支付网关及认证机构 6 大角色，提供了加密、数据完整、身份验证、数据不可否认性等服务。

关键术语

认证中心；CFCA；SSL；SET；PKI；IPSec；CA

习　题

一、选择题

1．SET 协议通过(　　)算法和(　　)算法的结合使用，保证了数据的一致性和完整性，并可实现交易以预防抵赖。

A．DES　　B．RSA　　C．MD5　　D．RC2　　E．RC3

2．CFCA 体系中证书的发放包括(　　)和(　　)。

A．离线方式　B．在线方式 C．人工发放 D．银行发放 E．个人申请

3．IPSec 协议簇由两个传输安全协议和一个应用层级的密钥管理协议组成，它们分别是(　　)。

A．AH　　B．ESP　　C．RA　　D．RS　　E．IKE

4．(　　)是一种相对简单的请求/响应协议，它提供了一种基于应答器的可信第三方获取在线撤销信息的手段。

A．OCSP　　B．SSL　　C．SET　　D．CA 系统　E．IPSec

5．CA 认证体系的实体大致可分为以下几部分：接收用户证书申请的证书受理者(　　)，证书发放的审核部门(　　)，证书发放的操作部门(　　)，记录撤销证书的证书撤销表(　　)。

A．CA　　B．CP　　C．CRL　　D．RA　　E．RS

二、简答题

1．CA 认证中心的定义和组成是什么？

2．认证中心有哪些主要的职能？

3．在 CFCA 体系中，目前支持哪些类型的证书？

4．SET 协议包含哪 3 大部分？分别简述每个部分的主要内容。

5．简述中心证书的撤销流程。

三、讨论题

1．SSL 协议与 SET 协议有什么不同？它们各有什么样的特点？SSL 协议在应用时，可能会存在哪些缺陷？这些缺陷如何通过技术的手段进行避免？

2．根据证书的作废机制，讨论在 CFCA 体系中，一个用户证书作废的业务流程。在该业务流程中，需要做哪些安全处理措施，以保障整个流程的安全性？

3．使用某个银行的网上转账系统，体验一下转账交易的整个业务过程。分析在 CFCA 体系下，整个业务环节的安全保障措施。

案例分析

中国民生银行网上银行系统

中国民生银行于1996年1月12日在北京正式成立，是我国首家主要由非公有制企业入股的全国性股份制商业银行。中国民生银行自成立以来，业务不断拓展，规模不断扩大，效益逐年递增，并保持了良好的资产质量。截至2006年12月31日，中国民生银行总资产规模达7 004亿元，并在北京、上海、广州、深圳等地设立了23家分行，机构网点达到287家。

为顺应现代企业以及企业集团的发展与普遍需求，民生银行推出了优势卓越的企业网上银行服务。民生网通过Internet将客户的计算机与银行主机相连，架起客户与银行间的安全快速通道，使客户在任意时间和地点，足不出户就可以享受到民生银行安全、高效、快捷的金融服务。

为实现将银行服务直接送到广大客户家中，达到足不出户，轻松实现投资理财的需要，民生银行推出全新的金融服务工具——个人网银系统，并采用CFCA数字证书来保证网上银行的安全。

(1) 身份的可靠性：网银服务器端和用户端进行了双向的身份认证，确认双方身份的可靠。

(2) 信息的保密性和完整性：用户在提交转账支付等机密信息时，服务器端和用户端会建立一个安全通道，确保信息传递的真实完整。

(3) 交易的不可否认性：系统对于提交的重要交易信息或表单进行签名，并在服务器端进行保留，便于在发生纠纷时举证，防止交易抵赖。

为了快速地对证书和黑名单进行查询，民生银行在本地部署了目录服务，作为CFCA主目录服务的镜像。

截至2006年年底，民生行发放CFCA企业证书4万多张，个人证书近23万张，证书总量已突破34万，成为CFCA发证规模大的银行之一。

资料来源：中国金融认证中心网站(http://www.cfca.com.cn/fangan/anli-008.htm)。

问题：客户在使用民生银行的网上交易时需要办理什么业务才能使用？在使用网上银行时，这套系统提供了哪些安全保障措施？民生银行的金融认证，如何与第三方的银行、证券进行互联？它们是通过什么样的体系进行互信的？