第 3 章　数字签名与身份认证技术

本章学习目标

本章主要讲解数字签名技术、CA 身份认证技术、数字证书的基本概念、数字证书的标准和使用、电子商务认证中心等内容。通过对本章的学习，读者应该掌握以下主要内容:

- 数字签名技术的基本原理与应用
- CA 认证中心的定义与作用
- 数字证书的标准和数字证书的使用
- 电子商务认证中心的作用

3.1　数字签名技术

在日常的社会生活和经济往来中，签名盖章和识别签名是一个重要的环节，例如银行业务、挂号邮件、合同、契约和协议的签订等，都离不开签名。在当今的计算机网络通信时代，用密码学的方法实现数字签名显然具有非常重要的实际意义。

3.1.1　数字签名技术

数字签名技术是公开密钥加密技术和报文分解函数相结合的产物。与加密不同，数字签名的目的是为了保证信息的完整性和真实性。数字签名必须保证以下三点：

- 接受者能够核实发送者对消息的签名。
- 发送者事后不能抵赖对消息的签名。
- 接受者不能伪造对消息的签名。

数字签名技术在原理上，首先用报文分解函数，把要签署的文件内容提炼为一个很长的数字，称为报文分解函数值。签字人用公开密钥和解密系统中的私有密钥加密这个报文，分解函数值，生成所谓的“数字签名”。收件人在收到数字签名的文件后，对此数字签名进行鉴定。用签字人的公开密钥来解开“数字签名”，获得报文分解函数值，然后重新计算文件的报文分解函数值，比较其结果。如果完全相符，则文件内容的完整性、正确性和签字的真实性都得到了保障。因为如果文件被改动，或者有人在没有私有密钥的情况下冒充签字，都将使数字签名的鉴定过程失败。

假定 A 发送一个签了名的信息 M 给 B，则 A 的数字签名应该满足下述条件：

- B 能够证实 A 对信息 M 的签名。
- 任何人，包括 B 在内，都不能伪造 A 的签名。
- 如果 A 否认对信息 M 的签名，可以通过仲裁解决 A 和 B 之间的争议。

可见，数字签名具有通常签名的特点。

Diffie 和 Hellman 的公钥密码系统的思想，对实现数字签名提供了一种简单的实现方法。

如果加密和解密变换满足性质：

E (D (M)) = M 时，

变换 E 和 D 就可以用于数字签名。这是因为，解密变换 D_A 是 A 私人拥有的，其他人无从知晓，因此 D_A 可以作为 A 的签名。任何人，包括 B 在内，由于不知道 D_A，所以不可能伪造 A 的签名。D_A 的逆变换 E_A 是公开的，因此接收者 B 能够有效地鉴定 A 的签名，同时仲裁者也可以很容易地解决 A 与 B 之间的争端。总之，只要加密和解密算法互为逆变换，公钥密码系统就可以很容易地实现数字签名。假定 A 向 B 发送一条消息 M，则其过程如下；

（1）A 计算出 $C=D_A(M)$，对 M 签名。

（2）B 通过检查 $E_A(C)$是否恢复 M，验证 A 的签名。

（3）如果 A 和 B 之间发生争端，仲裁者可以用（2）中的方法鉴定 A 的签名。

对于传统的密码系统，例如 DES，因为 A 和 B 所用的密钥相同，所以不能用上述方法直接实现数字签名。例如，B 可以伪造 A 的数字签名，而且仲裁者无法解决 A 与 B 之间的争议。

R.C.Merkle 建议，如果有一个可以信赖的第三方 TTP（Trusted Third Party），用下面的方法可以用传统的密码系统实现数字签名。A 将自己的一对可逆的秘密变换 E_A 和 D_A 告诉 TTP，当 A 传送签名的消息 M 给 B 时，A 计算出 $C=D_A(M)$，然后将 C 发送给 B。为了验证 C 并得到 M，B 将 C 传送给 TTP。TTP 计算出 $E_A(C)=M$，然后通过 B 的秘密变换将 M 传送给 B。

用传统的密码系统实现数字签名还有许多其他方法，这里就不再介绍了。

3.1.2　带加密的数字签名

如果像银行转账的例子那样，在公钥数字签名系统中还要求保密性，必须对上述方案进行如下修改。

发送者 A 先将要传送的消息 M 用自己的秘密变换 D_A 签名。

$M_A=D_A(M)$

再用接收者 B 的公开变换 E_B 进行加密。

$C=E_B(M_A)=E_B(D_A(M))$

最后，将签名后的加密消息 C 发送给 B。B 收到 C 后，先用自己的秘密变换 D_B 解密 C。

$D_B(C)=D_B(E_B(M_A))=M_A$

然后用 A 的公开变换 E_A 恢复 M。

$E_A(M_A)=E_A(D_A(M))=M$

使用公开密钥算法的带加密的数字签名的基本过程如图 3-1 所示。

（1）设用户 A 向 B 发送附有 A 签名的信息 P，A 首先利用自己的解密密钥 sa 对 P 进行一次解密变换，即：

$D_{sa}(P)=S_P$

S_P 称为签名文本。

（2）用户 A 再利用 B 的公开密钥 kb 对 S_P 进行加密，得到密文 C。

$E_{kb}(S_P)=C$

（3）C 再从不保密信道传送给 B。

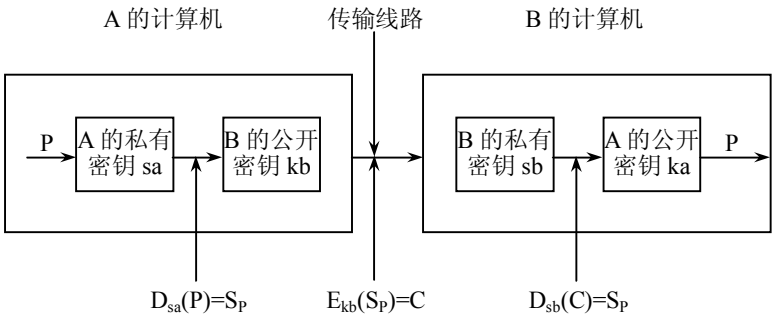

图 3-1 带加密的数字签名过程

（4）B 再用自己的解密密钥 sb 对 C 进行解密变换。

$E_{sb}(C)=S_P$

得到签名文本 S_P。

（5）B 再利用 A 的加密公钥 ka 对 S_P 进行一次加密变换，即可恢复明文 P。即：

$E_{ka}(S_P)=P$

此时收方 B 保存了发方 A 送来的明文和签名文本对（P，S_P）；现在假设第三方想冒充 A，向 B 发送信息 m，因为第三方不知 A 的密钥 sa，所以他也就无法做出 A 的签名 S_m。所以第三方也就无法冒充 A 向 B 发送信息 m，这也就达到了对发方 A 的证实。再假设 B 想将 P 篡改或伪造成信息 m，B 因为不知 sa，所以无法造出 S_m，因而无法进行伪造和篡改，这就达到了对收方 B 的证实。

注意：A 知道自己的私有解密密钥 D_A，还知道 B 的公开密钥 E_B，所以建立这条信息的工作应由 A 来做。

现在假设 A 后来否认曾经发送消息 P 给 B。当案子上了法庭，B 能够出示 S_P 和 $D_{sa}(P)$。法官只要使用一下 E_{ka}，就能轻易地证明 B 确实有一条用 D_{ka} 加密的有效信息。由于 B 不知道 A 的私有密钥，B 能得到用它加密的惟一途径就是 A 发送过来的。

下面举两个数字签名具体应用的例子。

【例 1】A 表示一个银行的电子转账系统的用户，B 代表 A 所在的银行。当 B 收到 A 要求提款 1 万元的消息后，必须鉴定这个信息的确是 A 签名后发出的。如果日后 A 否认这一笔提款，B 必须能够向仲裁方证实，这个提款单确实是由 A 签署的。

在上述例子中，由于银行和储户之间的业务往来是秘密进行的，所以这个数字签名系统除要求鉴定信息和信息发送者的真实性以外，还要求保密性。然而，并非所有的数字签名系统都要求保密性。G.J.Simmons 举了下面一个不能容忍保密性的数字签名的实际应用例子。

【例 2】假设美国和俄罗斯签订了一项禁止一切地下核试验的条约，那么如何对这个条约进行监督呢？在美国的 Sandia 试验室研制了一个监督系统，要求美、俄各自在对方的国土上设置若干个地震观测站，以便判断双方是否都遵守停止一切地下核试验的条款。各观察站将搜集到的全部数据送回位于设置该站的国家领土内的中心站进行分析和判断。对这个系统有下面三个要求：

（1）中心站必须确认它所收到的信息是从设置在对方国内的有关观测站发回的，而不是经对方篡改后的信息，因此，鉴定信息本身的真实性和信息发送者的真实性都是必要的。

（2）美俄双方都必须证实，设在本国国土上的对方的观测站不被用于其他任何目的。因此这个系统不能容忍保密性，亦即每个国家都必须能够读出从本国的观测站发往对方国内的任何消息。

（3）中心站和观测站的所在国都不能够伪造由观测站发出的消息。一旦美俄两国对信息的真实性发生争端，仲裁方（例如联合国或某个中立国）应当有办法予以评判。

在公钥数字签名系统中，令各观测站用自己的秘密变换 D（甚至观测站的所在国也不知道）将所有发往中心站的信息 M 签名，就可以满足上述所有的条件。中心站和观测站的所在国，以及作为第三方的仲裁机构都能够通过对应的公开变换 E，获悉所传输的信息 M。

以上就是数字签名的基本原理。它的现实意义在于彻底解决了收发双方就传送内容可能发生的争端，为在商业上广泛应用创造了条件。

现在被广泛应用的基于公钥密码体制的数字签名技术主要有：

- RSA 体制，它是基于求解一个大整数分解为两个大素数问题的困难性。
- E1Gamal 体制它是基于求解有限域上的乘法群的离散对数问题的困难性。

椭圆曲线密码体制是一种基于代数曲线的公钥密码机制，以其良好的安全性，曲线选取范围广，在同等长度的密钥下具有比 RSA 体制更快的加、解密速度及更高的密码强度而备受青睐。

此外，实现数字签名有很多方法，如基于 RSA Data Security 公司的公钥加密标准 PKCS（Public Key Cryptography Standard）、数字签名算法 DSA（Digital Signature Algorithm）、X.509、PGP（Pretty Good Privacy）。1994 年美国标准与技术协会公布了数字签名标准（DSS）而使公钥加密技术广泛应用。同时应用散列算法（hash）也是实现数字签名的一种方法。

3.1.3　RSA 公钥签名技术

数字签名可以利用秘密密钥，也可以用公开密钥。但采用秘密密钥是建立在有一个众人信任的中间机构的基础上，而采用公钥加密法进行数字签名则不受此限制，收发双方之间不需要任何可信赖机构。

2000 年 1 月举行的第六届国际密码学会议对应用于公钥密码系统的加密算法，推荐了两种：基于大整数因子分解难题的 RSA 算法和基于椭圆曲线上离散对数计算难题的 ECC 算法。所以基于 RSA 算法的数字签名还有一定的发展。

RSA 方法的加密和解密算法互为逆变换，所以可以用于数字签名系统。假定用户的公钥是（n_A，e_A），秘密钥是 d_A，加密和解密变换分别为 E_A 和 D_A，则 A 发送的签名后的消息是：

$$C \equiv D_A(A) \equiv M^{dA}（\bmod n_A）$$

收到 C 后的 B，可以用 A 的公开变换 E_A 恢复 M：

$$E_A(C) \equiv E_A(D_A(M)) \equiv M^{dA\ \ eA} \equiv M（\bmod n_A）$$

因为只有 A 知道 D_A，所以签名不可能伪造，并且 A 与 B 之间的任何争议都可以通过仲裁加以解决。

在要求 A 传送一条签名并加密的消息给 B 的情况下，A 必须发送：

$C=K_B(D_A(M))$

B 接收到密文 C 后，计算：

$$E_A(D_B(C)) = E_A(D_B(E_B(D_A(M)))) = E_A(D_A(M)) = M$$

注意：这里 n_A，n_B 必须满足一定的条件，本文不作详细讨论。

网络技术的发展使得电子商务正在广泛开展，电子邮件也被普遍使用，数字签名技术越来越重要。RSA 虽然有算法复杂、速度慢的缺点，但目前还是被广泛地应用于数字签名中。随着计算机技术的发展及对 RSA 的深入研究，目前 RSA 正在走向实用化、商业化。可以预见在网络安全中，基于 RSA 的网络安全系统的设计将会广泛使用。

3.1.4 数字签名的应用

1. 文件签名和时间标记

实际上数字签名包括时间标记。对日期和时间的签名附在消息中，并跟消息中的其他部分一起签名。银行将时间标记存储在数据库中。如果有一方想支取支票时，银行就要检查时间标记是否和数据库中的一样。若银行已经支付过这一时间标记的支票，有人再次支付时银行将会报警。

2. 电子商务中的应用

Internet 的迅猛发展使电子商务成为商务活动的新模式。电子商务包括管理信息系统 MIS、电子数据交换 EDI、电子订货系统 EOS、商业增值网 VAN 等。其中 EDI 成为电子商务的核心部分，是一项涉及多个环节的复杂的人机工程。网络的开放性与共享性也导致了网络的安全性受到严重影响。如何保证网上传输的数据的安全和交易对方的身份确认是电子商务能否得到推广的关键。可以说电子商务最关键的问题是安全问题，而数字签名又是电子商务安全性的重要部分。

生成和验证数字签名的工具需要完善，只有用 SSL（安全套接层）建立安全链接的 Web 浏览器，才会频繁使用数字签名。公司要对其雇员在网络上的行为进行规范，就要建立广泛协作机制来支持数字签名。支持数字签名是 Web 发展的目标，确保数据保密性、数据完整性和不可否认性才能保证在线商业的安全交易。

和数字签名有关的复杂认证能力就像现在操作、应用环境中的口令保护一样为操作系统环境、应用、远程访问产品、信息传递系统及 Internet 防火墙所拥有，像 Netscape 支持 X.509 标准的 Communicator 4.0 Web 以上版本的客户机软件；Microsoft 支持 X.509 的 Internet Explorer 4.0 以上版本的客户机软件及支持对象签名检查的 Java 虚拟机等。

电子商务的应用前景非常广泛，安全问题是阻碍电子商务广泛应用的最大问题。改进数字签名在内的安全技术措施，确保身份认证的实施则是十分关键的问题。

3.2 电子商务安全交易的关键环节——身份认证

CA 是 Certificate Authority 的缩写，是认证中心的意思。在电子商务系统中，所有实体的证书都是由证书授权中心，即 CA 分发并签名的。一个完整、安全的电子商务系统必须建立起一个完整、合理的 CA 体系。CA 体系由证书审批部门和证书操作部门组成。

3.2.1 CA 的定义

为保证客户之间在网上传递信息的安全性、真实性、可靠性、完整性和不可抵赖性，不

仅需要对客户的身份真实性进行验证，也需要有一个具有权威性、公正性、惟一性的机构，负责向电子商务的各个主体颁发并管理符合国内、国际安全电子交易协议标准的安全证书。

CA 机构，又称为证书授权中心，作为电子商务交易中受信任和具有权威性的第三方，承担公钥体系中公钥的合法性检验的责任。CA 为每个使用公开密钥的客户发放数字证书，数字证书的作用是证明证书中列出的客户合法拥有证书中列出的公开密钥。CA 机构的数字签名使得第三者不能伪造和篡改证书。它负责产生、分配并管理所有参与网上信息交换各方所需的数字证书，因此是安全电子信息交换的核心。

电子商务的安全是通过使用加密手段来达到的。非对称密钥加密技术（公开密钥加密技术）是电子商务系统中主要的加密技术，主要用于对称加密密钥的分发（数字信封）和数字签名，以实现身份认证和信息的完整性检验，以预防交易的抵赖等。CA 体系为用户的公钥签发证书，以实现公钥的分发并证明其有效性。该证书证明了用户拥有证书中列出的公开密钥。证书是一个经证书授权中心签名的包含公开密钥拥有者信息以及公开密钥的文件。电子商务认证授权机构（CA），也称为电子商务认证中心，是负责发放和管理数字证书的权威。

CA 为电子商务服务的证书中心，是 PKI（Public Key Infrastructure）体系的核心。它为客户的公开密钥签发公钥证书、发放证书和管理证书，并提供一系列密钥生命周期内的管理服务。它将客户的公钥与客户的名称及其他属性关联起来，进行客户之间电子身份认证。证书中心是一个具有权威性、可信赖性和公正性的第三方机构，它是电子商务存在和发展的基础。

CA 中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书。在 SET 交易中，CA 不仅对持卡人、商户发放证书，还要对获款的银行、网关发放证书，并负责管理所有参与网上交易的个体所需的数字证书，因此 CA 是安全电子交易的核心环节。

CA 机构的数字签名使得攻击者不能伪造和篡改证书。证书的格式遵循 X.509 标准。

数字证书管理中心是保证电子商务安全的基础设施。它负责电子证书的申请、签发、制作、废止、认证和管理，提供网上客户身份认证、数字签名、电子公证、安全电子邮件等服务。

为了达到服务器和客户两端同时认证的目的，需要银行的网上交易服务器和访问该服务器的用户申请同一 CA 中心的 CA 证书，安装在交易服务器和用户的浏览器中。这样，当用户访问用户的交易服务器时，用户端接收到交易服务器的 CA 证书并送到 CA 中心验证，在用户端可以看到服务器 CA 证书的内容，知道所访问的服务器不是被冒充的，同时还要提交自己的 CA 证书，向服务器说明自己是合法用户。这样，就可以在双方的交易过程中，保证数据传输的加密和数据的一致性。

中国金融认证中心是国内第一个国家级认证中心。作为一个权威的、可信赖的、公正的第三方信任机构，为参与电子商务各方的各种认证需求提供证书服务，建立彼此的信任机制，为全国范围内的电子商务及网上银行等网上支付业务提供多种模式的认证服务。

CA 机构应包括两大部门：一是审核授权部门（Registry Authority，RA），作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。它负责对证书申请者进行资格审查，决定是否同意给该申请者发放证书，并承担因审核错误引起的、为不满足资格证书申请者发放证书所引起的一切后果，因此它应由能够承担这些责任的机构担任；另一个是证书操作部门（Certificate Processor，CP），负责为已授权的申请者制作、发放和管理证书，并承担因操作运营所产生的一切后果，包括失密和为没有获得授权者发放证书等。它可以由审核授

权部门自己担任，也可委托给第三方担任。

如图 3-2 所示，CA 体系具有一定的层次结构，它由根 CA、品牌 CA、地方 CA 以及持卡人 CA、商家 CA、支付网关 CA 等不同层次构成，上一级 CA 负责下一级 CA 数字证书的申请、签发及管理工作。通过一个完整的 CA 认证体系，可以有效地实现对数字证书的验证。每一份数字证书都与上一级的签名证书相关联，最终通过安全认证链追溯到一个已知的可信赖的机构。由此便可以对各级数字证书的有效性进行验证。根 CA 的密钥由一个自签证书分配，根证书的公开密钥对所有各方公开，它是 CA 体系中的最高层。

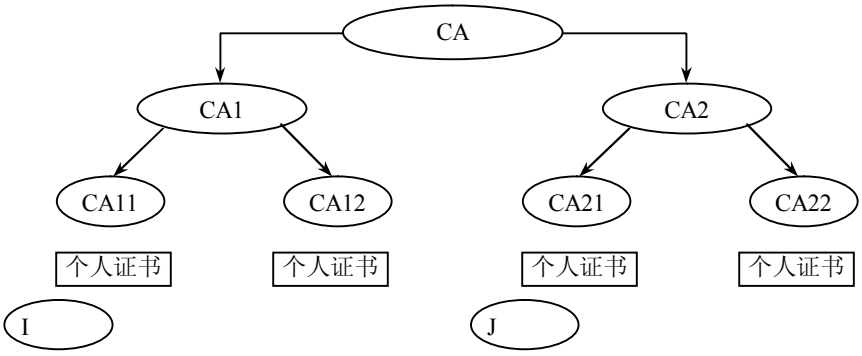

图 3-2　CA 证明链

3.2.2　CA 的作用

认证体系的安全对象根据其安全需求的不同大致可分为三类。一类是认证中心各个层次权威认证（CA）的私钥及其附属系统信息的安全，是重中之重。CA 是保障证书合法性，集权威与可信性于一身的实体，CA 私钥的不可信就意味着整个证书处理体系的不可信性。因此，CA 私钥的安全性具有很高的安全等级。另一类是注册审核体系系统的安全性，它提供了用户证书申请和证书审核的可靠途径，用户信息的真实与否由它来进行安全性保证。它提供一个可信的用户信息源，并由 CA 来对其签名及合法性进行公开确认。第三类是用户私钥及证书服务的安全性。

认证中心在密码管理方面的作用如下：

（1）自身密钥的产生、存储、备份/恢复、归档和销毁。从根 CA 开始到直接给客户发放证书的各层次 CA，都有其自身的密钥对。CA 中心的密钥对一般由硬件加密服务器在机器内直接产生，并存储于加密硬件内，或以一定的加密形式存放于密钥数据库内。加密备份于 IC 卡或其他存储介质中，并以高等级的物理安全措施保护起来。密钥的销毁要以安全为标准，彻底清除原有的密钥痕迹。特别是，根 CA 密钥的安全性至关重要，所以 CA 的密钥保护必须按照最高安全级的保护方式来进行设置和管理。

（2）提供密钥生成和分发服务。CA 中心可为客户提供密钥对的生成服务，它采用集中或分布式的方式进行。在集中的情形下，CA 中心可使用硬件加密服务器，为多个客户申请成批的生成密钥对，然后采用安全的信道分发给客户。也可以由多个注册机构（RA）分布生成客户密钥对并分发给客户。

（3）确定客户密钥生存周期，实施密钥吊销和更新管理。每一张客户公钥证书都会有有

效期，密钥对生命周期的长短由签发证书的 CA 中心来确定。各 CA 系统的证书有效期限有所不同，一般大约为 2～3 年。

（4）为安全加密通信提供安全密钥管理服务。在客户证书的生成与发放过程中，除了有 CA 中心外，还有注册机构、审核机构和发放机构（对于有外部介质的证书）的存在。行业使用范围内的证书，其证书的审批控制，可由独立于 CA 中心的行业审核机构来完成。CA 中心在与各机构进行安全通信时，可采用多种手段。对于使用证书机制的安全通信，各机构（通信端）的密钥产生、发放与管理维护，都可由 CA 中心来完成。

（5）提供密钥托管和密钥恢复服务。CA 中心可根据客户的要求提供密钥托管服务，备份和管理客户的加密密钥对。当客户需要时可以从密钥库中提出客户的加密密钥对，为客户恢复其加密密钥对，以解开先前加密的信息。密钥恢复时，采用相应的密钥恢复模块进行解密，以保证客户的私钥在恢复时没有任何风险和不安全因素。同时，CA 中心也应有一套备份库，避免密钥数据库的意外毁坏而无法恢复客户私钥。

（6）其他密钥生成和管理，密码运算功能。CA 中心在自身密钥和客户密钥管理方面的特殊地位和作用，决定了它具有主密钥、多级密钥、加密密钥等多种密钥的生成和管理功能。

对于为客户提供公钥信任、管理和维护整个电子商务密码体系的 CA 中心来讲，其密钥管理工作是一项十分复杂的任务，它涉及 CA 中心自身的各个安全区域和部件、注册审核机构以及客户端的安全和密码管理策略。

认证中心主要有以下功能：

- 每天 24 小时接受最终用户（如持卡人、商家、支付网关）的数字证书的申请，确定是否受理申请。
- 数字证书申请和审批，通过对客户在网上填写的内容进行验证，决定是否发放数字证书。
- 数字证书的生成、颁发和管理，对证书的管理包括更新、查询、撤销、归档及备份证书等功能。

以前，在网上交易中，大量的是采用安全套接协议层（Secure Sockets Layer，SSL），但由于该协议的缺陷，缺少认证能力，容易造成网上诈骗，因此维萨、万事达国际卡组织和多家科技机构共同制订了一个在 Internet 上进行在线交易的安全标准，这就是“安全电子交易”（Secure Electronic Transactions，SET）。SET 提供了消费者、商家和银行间的认证，确保了交易数据的安全性、完整可靠性和交易的不可否认性，特别是保证不将消费者信用卡号暴露给商家等优点，因此它成为了目前公认的信用卡/借记卡的网上交易的国际安全标准。

3.3　数字证书

3.3.1　什么是数字证书

1. 电子证书的用途

通过 Internet 进行通信或进行电子商务活动时，使用电子证书可以防止信息被第三方窃取，也能够在交易出现争执时防止抵赖的情况发生。电子证书是进行安全通信的必备工具，它保证信息传输的保密性、数据完整性、不可抵赖性、交易者身份的确定性。

使用电子证书，通过运用对称和非对称密码体制等密码技术建立起一套严密的身份认证系统，可以保证信息除发送方和接收方外不被其他人窃取，信息在传输过程中不被篡改，发送方能够通过电子证书来确认接收方的身份，发送方对于自己的信息不能抵赖。

例如，站点证书：

- 进行 SSL 安全连接，保证用户和服务器之间的数据安全传送。
- 通过客户证书使只有经过授权的人才能访问该站点。

账号认证：

- 访问需要客户验证的 Internet 站点。
- 用自己的数字证书对电子邮件进行加密和签名。

从技术上来说，数字证书的主要内容就是用户实体的公共密钥的数字签名，它是由公正的、被各方信赖的权威认证机构来颁发和管理的。

数字证书就是网络通信中标志通信各方身份的信息的一系列数据，提供了一种在 Internet 上验证身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。

2. 数字证书的内容

数字证书是由权威的、公正的认证机构来颁发和管理的。它在证书申请被权威性的证书管理机构即认证中心（CA）批准后，通过登录服务器将证书发放给申请者。

国际电信联盟 ITU-T 的 X.509 建议书是定义目录服务的 X.500 系列推荐书的一部分。从效果上看，目录是保存用户信息数据库的一个服务器或一组分布式服务器。信息包括用户名字、网络地址映射以及用户的其他属性。

电子证书是一段被 CA 签了名的数据信息，在网络通信中标志通信各方身份信息，作用类似于生活中的身份证，它是由权威机构——CA 中心发行的，包含公开密钥拥有者信息以及公开密钥的文件。人们可以在交往中用它来识别对方的身份。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、发证机关的名称、该证书的序列号等信息，证书的格式遵循 X.509 国际标准。

一个标准的 X.509 电子证书包含以下内容：

- 证书的版本信息。
- 证书的序列号，每个证书都有一个惟一的证书序列号。
- 证书所使用的签名算法。
- 证书的发行机构名称，命名规则一般采用 X.500 格式。
- 证书的有效期，现在通用的证书一般采用 UTC 时间格式，它的计时范围为 1950～2049。
- 证书所有人的名称，命名规则一般采用 X.500 格式。
- 证书所有人的公开密钥。
- 证书发行者对证书的签名。

3.3.2 数字证书的标准

数字证书是一个经证书授权中心数字签名的包含公钥拥有者信息及公开密钥的文件。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

ITUT　X.509 国际标准。

X.509 定义了一个由 X.509 目录向它的用户公开提供的鉴别服务框架。目录可以作为公开密钥证书知识库。每个证书包含用户的公开密钥和可信证书权威机构私人密钥的签名。X.509 定义了基于使用公开密钥证书的可选鉴别协议。

X.509 是一个重要的标准，在 X.509 中定义的证书结构和鉴别协议已有广泛的应用，已成功应用于 S/MIME、IP 安全以及 SSL/TLS 和 SET。

X.509 基于公开密钥加密和数字签名。这个标准没有专门指定使用的加密算法，但推荐使用 RSA。数字签名则假定要求使用散列函数。

X.509 方案的核心是与每个用户联系的公开密钥证书。这些用户证书由某些可信证书权威机构（CA）创建，由 CA 或用户放在目录中。目录服务器本身不负责公开密钥的生成或证书函数，它仅提供一个易于访问的位置以便用户获得证书。

一个标准的 X.509 数字证书包含如图 3-3 所示的一些内容。

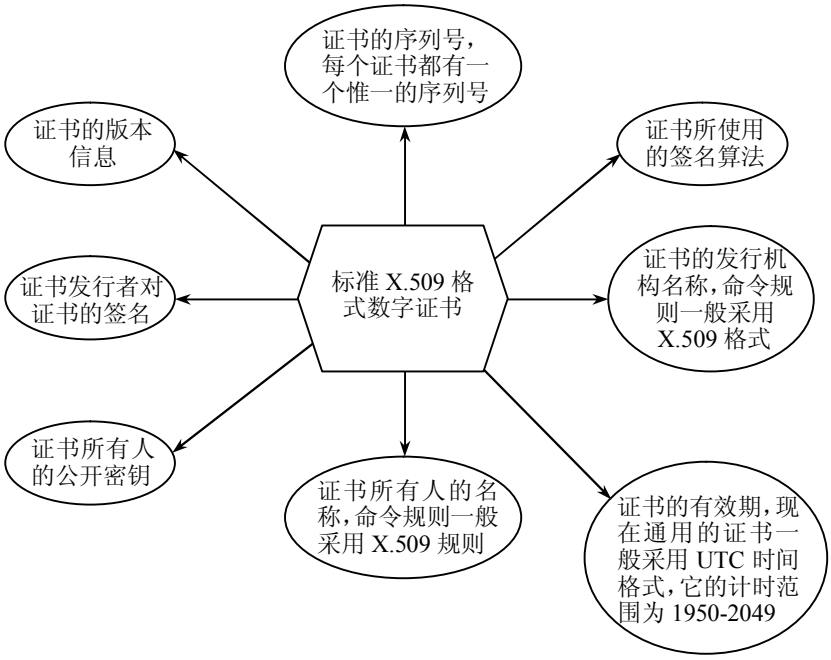

图 3-3　标准格式数字证书

【例】NETCA 数字证书是网证通 CA 中心采用国家密码委员会通过的算法，结合国际先进安全标准，独立开发、享有独立版权的数字证书。该证书系列支持 1024 bit 的非对称加密算法和 128 bit SSL 加密协议。在安装了高强度加密包的 IE 中可以正常使用，建立 128 bit SSL 加密通道。

NETCA 证书系列包括 5 种证书。

（1）个人证书。用户使用此证书来向对方表明个人身份，同时应用系统也可以通过证书获得用户的其他信息。

（2）单位证书。颁发给独立的单位、组织，在互联网上证明该单位、组织的身份。单位数字证书根据各个单位的不同需要，可以分为单位证书和单位员工证书。

（3）服务器证书。主要颁发给 Web 站点或其他需要安全鉴别的服务器，证明服务器的身份信息。服务器数字证书支持目前主流的 Web Server，包括但不限于：IIS、Lotus Domino、Apache、iPlant 等 Web 服务器。可存放于服务器硬盘或加密硬件设备上。

（4）安全邮件证书。结合使用数字证书和 S/MIME 技术，对普通电子邮件做加密和数字签名处理，确保电子邮件内容的安全性、机密性、发件人身份确认性和不可抵赖性。

（5）代码签名证书。为软件开发商提供对软件代码做数字签名的技术，可以有效地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。

3.3.3 数字证书的使用

1. 获得一个用户证书

由 CA 产生的用户证书有以下特点：

- 任何有 CA 公开密钥的用户都可以恢复被证明的用户公开密钥。
- 仅有证书权威机构能够更改证书，其他任何一方更改证书都将被察觉。

因为证书是不可伪造的，因此它们可以放在一个目录内，而无须提供特殊的保护措施。

如果所有用户都预定了相同的证书，那么这是对那个 CA 的共同信任，所有用户的证书能被放在所有用户都能访问的目录内。此外，用户可以直接将他或她的证书传递给其他用户。一旦 B 拥有 A 的证书，B 将确信用 A 的公钥加密的报文可以安全地防止窃听者，而用户 A 的私人密钥签名的报文将不会被篡改。

如果用户的数目巨大，让所有的用户向同一个 CA 预订则是不现实的。当用户很多时，设立多个 CA 机构，每个 CA 机构可以安全地向一小部分用户提供它的公开密钥，这样安全性更高。

获得电子证书的步骤如下：

（1）下载根证书。用户把 CA 中心生成的根证书下载并安装到自己的浏览器中，用来对账号证书进行验证。用户申请账号证书后，在下载安装账号电子证书之前应该首先把 CA 中心的根证书安装到自己的浏览器中。也可以首先下载安装根证书，然后再申请账号证书。

IE 用户，单击下载根证书后将弹出一个窗口，询问是在当前位置打开还是保存到磁盘上。请选择在当前位置打开，然后单击安装证书按钮，接下来单击“下一步”，根据证书类型选择存储区，再单击“完成”按钮和“是”按钮，就安装上根证书了。

Netscape 用户依次单击 next 即可完成安装。

（2）申请账号认证。通过 Internet 进行通信或进行电子商务活动时，使用电子证书可以防止信息被第三方窃取，也能够在交易出现争执时防止抵赖的情况发生，电子证书是进行安全通信的必备工具。用户通过 Internet 进入电子证书中心后，可利用此功能填写个人证书申请表，如果用户填写合格，通过 E-mail 发给用户一个个人标识字（PIN），用户可凭此 PIN 以及申请时所填写的口令查询和修改申请书。

用户通过表单将其填写的 E-mail 地址、姓名、单位、部门、国家代码、省份、城市、密码和用这些信息产生的申请书提交给电子证书中心。

（3）下载安装证书。当用户申请完证书后就会收到电子证书中心的第一封信，通知用户 PIN，用户可凭此 PIN 以及申请时所填写的口令查询和修改申请书。当用户的证书通过审核后会收到第二封信，当证书被签发后就会收到内含证书序列号的第三封信。用户可利用证书序列

号，下载并安装 CA 签发的电子证书。安装完成后，系统提示用户安装已经完成，并指导用户如何使用电子证书。

2. 获得通信过程中验证签名和公钥的过程

现在假定 A 已经从证书权威机构 X_1 处获得一证书，B 从证书权威机构 X_2 获得一证书。如果 A 无法安全地获得 X_2 的公开密钥，那么由 X_2 颁发给 B 的证书对 A 是没有用的。A 可以阅读 B 的证书但不能验证签名。然而，如果两个 CA 能够安全地交换各自的公开密钥，下面的过程可以使得 A 获得 B 的公开密钥。

步骤 1：A 从目录获得由 X_1 签名的 X_2 的证书。因为 A 能安全地知道 X_1 的公开密钥，A 从它的证书中能获得 X_2 的公开密钥，并通过证书中 X_1 的签名来证实它。

步骤 2：然后 A 能回到目录中得到由 X_2 签名的 B 的证书。因为现在 A 已经拥有一个可信的 X_2 的公开密钥备份，因此 A 能验证这个签名并安全地获得 B 的公开密钥。

在这个过程中，A 使用了一个证书链获得了 B 的公开密钥；用同样的方式，B 使用相反的链可获得 A 的公开密钥。

3. 证书的撤销

前面已定义过每个证书都包含一个有效期，就像信用卡。典型的做法是在老证书即将过期之前颁发一个新的证书。此外，有时基于以下某个原因要在证书过期之前撤销它：

- 认为用户的密钥已泄露。
- 用户不再由这个 CA 颁发证书。
- 认为 CA 证书已泄露。

每个 CA 必须保持一个所有已撤销的但还没有过期的证书表，这些证书可能由这个 CA、用户和其他 CA 颁发证书。这些表也应该被粘贴到目录中。

4. 证书的鉴别过程

X.509 也包括三个可选的鉴别过程供不同的用户使用。所有这些过程都使用公开密钥签名。它假定双方都知道对方的公开密钥，或者通过从目录获得对方的证书，或者证书被包含在双方的初始报文中。

（1）单向鉴别。单向鉴别涉及信息从一个用户（A）传送到另一个用户（B），它建立如下要素：

- A 的身份标识和由 A 产生的报文。
- 打算传递给 B 的报文。
- 报文的完整性和新颖性（还没有发送过多次）。

注意：在这个过程仅验证发起实体的身份标识，而不验证响应实体的标识。

报文至少要包括一个时间戳 t4、一个现时 A 和 B 的身份标识，均用 A 的私用密钥签名。时间戳由一个可选的产生时间和过期时间组成，这将防止报文的延迟传送。现时用于检测重放攻击。现时值在报文的有效时间内必须是惟一的，这样 B 能存储这个现时直到它过期并拒绝有相同现时的报文。

对单纯的鉴别，报文简单用作向 B 提交证书。该报文可能也包括要传递的信息，这个信息（sgnData）也包含在签名范围内，保证它的可信性和完整性。报文也可用作向 B 传递一个会话密钥，密钥用 B 的公开密钥加密。

（2）双向鉴别。除了上面列举的三个要素，双向鉴别还建立如下要素：

- B 的身份标识和 B 产生的回答报文。
- 打算传递给 A 的报文。
- 回答报文的完整性和新颖性。

因而，双向鉴别允许通信双方验证对方的身份。

为了验证回答报文，回答报文包括 A 的现时，它还包括由 B 产生的一个时间戳和一个现时。和前面一样，报文可能包括签名的附加信息和用 A 的公开密钥加密的会话密钥。

（3）三向鉴别。在三向鉴别中，包括一个最后从 A 到 B 的报文，它含有一个现时 B 的签名备份。这样设计的目的是无须检查时间戳，因为两个现时均由另一端返回，每一端可以检查返回的现时来探测重放攻击。当没有同步时钟时，需要使用这种方法。

图 3-4 显示了 X .509 的强鉴别过程。

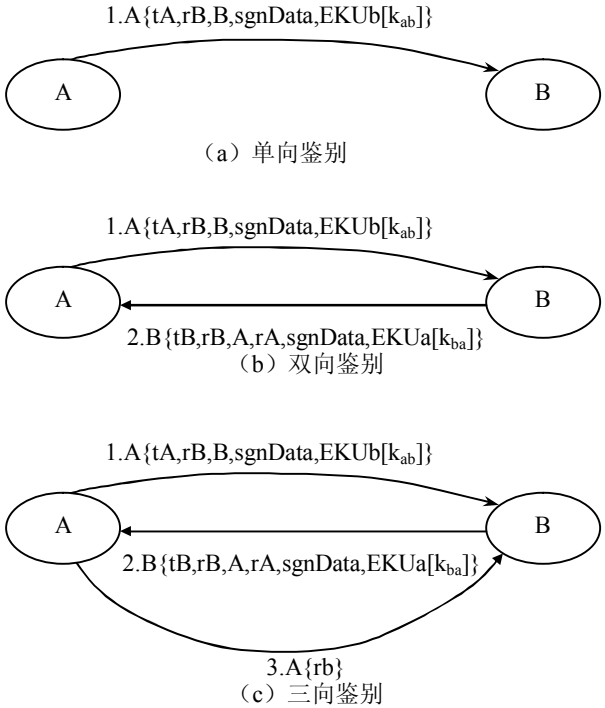

图 3-4　X.509 的强鉴别过程

3.4　电子商务认证中心安全方案

认证中心是电子商务体系中的核心环节，是电子交易中信赖的基础。它通过自身的注册审核体系，检查核实进行证书申请的用户身份和各项相关信息，并将相关内容列入发放的证书域内，使用户属性的客观真实性与证书的真实性一致。认证中心以其公正、权威、可信赖的地位，获得证书使用者对它的信赖，并使用户通过对其发放的证书的信赖，实现对交易中持有证书的各方的信赖。安全可信性是认证中心在电子商务体系中存在的基石。

认证中心的安全结构包括物理与环境安全、网络安全、应用业务系统与数据安全、人员

安全与日常操作管理、系统连续性管理这几大环节。

1. 物理与环境安全

物理与环境安全建设的尺度，取决于认证中心系统服务功能的规模、信息与网络系统的安全敏感度。它的建设，既要考虑到资金的承受能力，也要考虑到未来系统发展的可适应性。

2. 网络安全

网络安全的目标是通过对各种网络服务、网络框架的有效保护，达到对证书处理系统架构及数据信息的安全防护目的。各种网络服务的接口、远程用户（包括远程注册审核系统及一般证书用户）的身份认证机制、用户对信息服务的访问控制，是实现这一目标的三道关隘。

3. 应用业务系统与数据安全

应用业务系统与数据安全的目标是保障业务系统敏感数据（如私钥、用户敏感信息等）的私密性、完整性。它的安全实现与操作系统、数据库、业务应用软件的安全是密不可分的。对于安全要求较高的系统，可以考虑采用高安全级的 OS 或加固操作系统，按照最小特权的原则进行权限划分和用户管理。数据库和应用系统的登录应实施强用户身份认证。同时，可以充分利用证书本身的安全可信特性，定义证书安全特征域，借助证书实现可靠的身份鉴别。

4. 人员安全与日常操作管理

安全方案的实现离不开管理。管理的有效性可以解决许多技术层次解决不了的安全性问题。人员是管理的核心，其人员安全要求应与一般机构有所不同。除了技术层次的要求，还应有安全性要求。日常的交互与操作安全管理，涉及系统运作时的方方面面，它的基本原则是：要求发生在系统内的所有行为都是有定义行为，并且符合程序控制的要求，所有行为的发生都有审计记录。

5. 系统连续性管理

系统备份、恢复策略的存在，是为了满足系统业务连续不间断的要求，避免由于自然灾难、事故、设备的损坏和恶意的破坏行为带来的系统不停顿服务功能的丧失。由于认证中心提供 24 小时不间断服务，它的停机可能造成证书不能及时获取、证书服务不能实时提供、电子交易无法进行等多种严重的负面影响。因此，保障认证中心服务的连续性是十分重要的。实现系统连续性管理的安全策略有：冗余设计、数据备份、异地冗余中心的建立等。

安全方案的设计与实现，要经过风险评估、弱点分析、框架构建、方案实施等若干步骤。需要说明的是，安全的实现不是一成不变的。策略的定义要随着系统的发展不断进行适应性调整，这是一个周期性控制过程。只有万变的系统，没有不变的安全，这是所有从事安全技术领域的工作人员都应牢记的。

【例】个人数字证书申请。

目前，有些认证中心向用户提供免费的试用型数字证书，其申请过程即时在网上完成，并可以立即投入使用。本节以网证通 NETCA 电子认证系统（试用型）为例，说明试用型个人数字证书的申请过程。具体步骤如下：

首先登录网证通 NETCA 电子认证系统（试用型）http://testca.netca.net，单击“证书申请”链接，选择“试用型个人数字证书申请”链接，如图 3-5 所示。

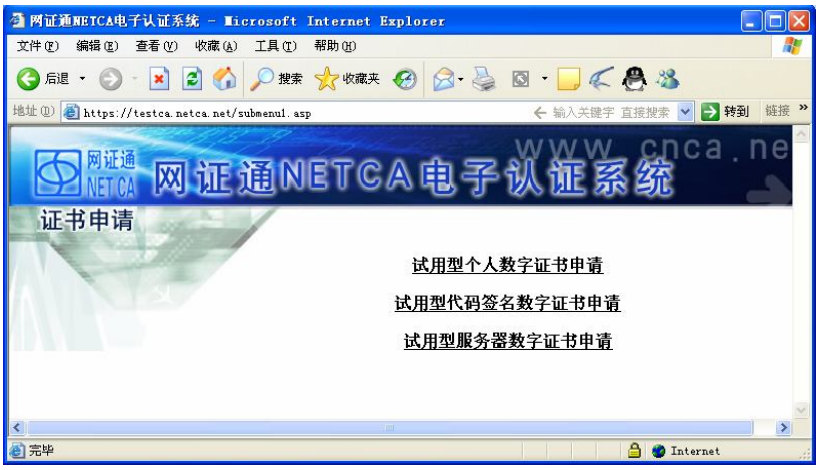

图 3-5 网证通 NETCA 电子认证系统

网证通 NETCA 电子认证系统的建设维护与技术支持单位是广东省电子商务认证中心，用户如果要使用网证通的数字证书，可以登录到 http://www.cnca.net，选择“网证通数字证书”→“个人证书”→“购买流程”，如图 3-6 所示，进入后先查阅购买流程，再单击“立即购买”按钮，按照界面提示完成个人数字证书的申请。

图 3-6 广东省电子商务认证中心主页

需要特别强调的是，只有安装了证书链的计算机，才能完成后面的申请步骤并正常使用申请的数字证书，所以需要先安装证书链。按照系统提示，单击“安装证书链”按钮，如图 3-7 所示。

出现如图 3-8 所示的提示框，单击“是”按钮。

出现如图 3-9 所示的提示框，单击“是”按钮。

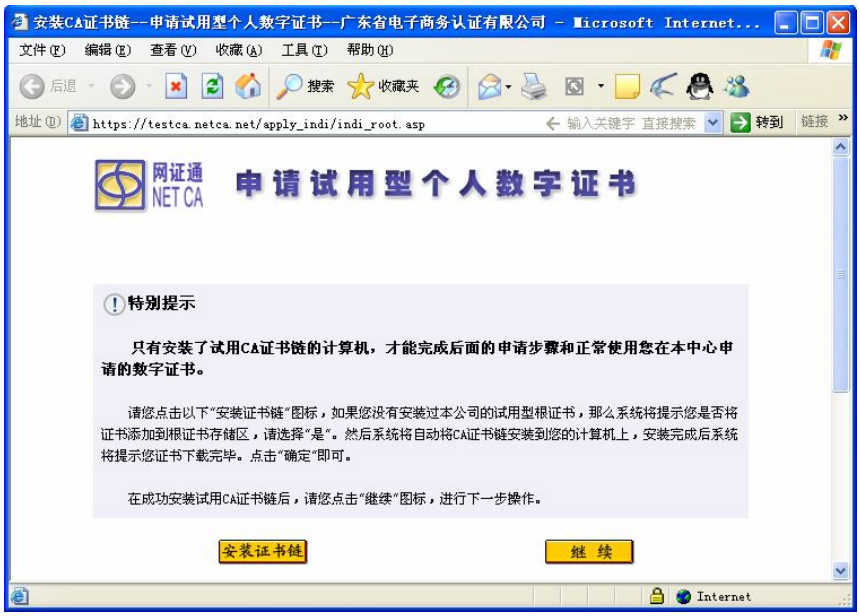

图 3-7　安装证书链

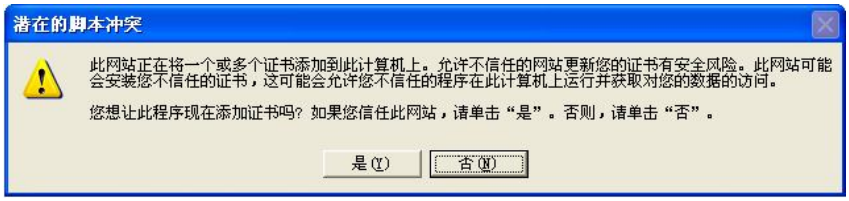

图 3-8　“潜在的脚本冲突”对话框

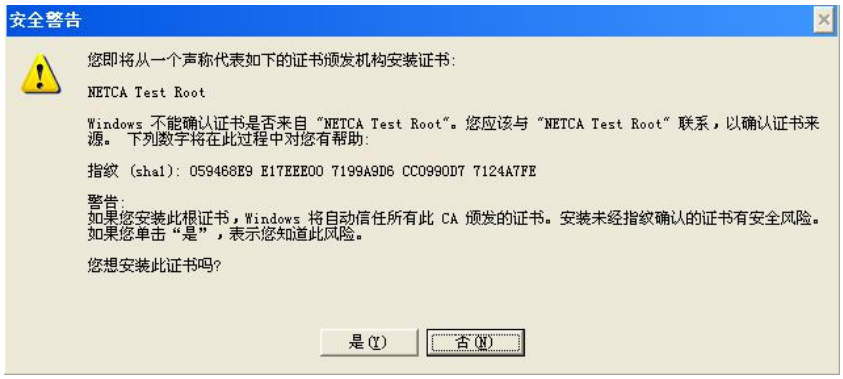

图 3-9　“安全警告”对话框

CA 证书链下载完毕，单击“确定”按钮，如图 3-10 所示。

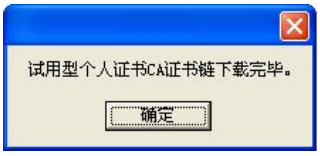

图 3-10　“试用型个人证书 CA 证书链下载完毕”对话框

接着进入填写基本信息页面，如图 3-11 所示。

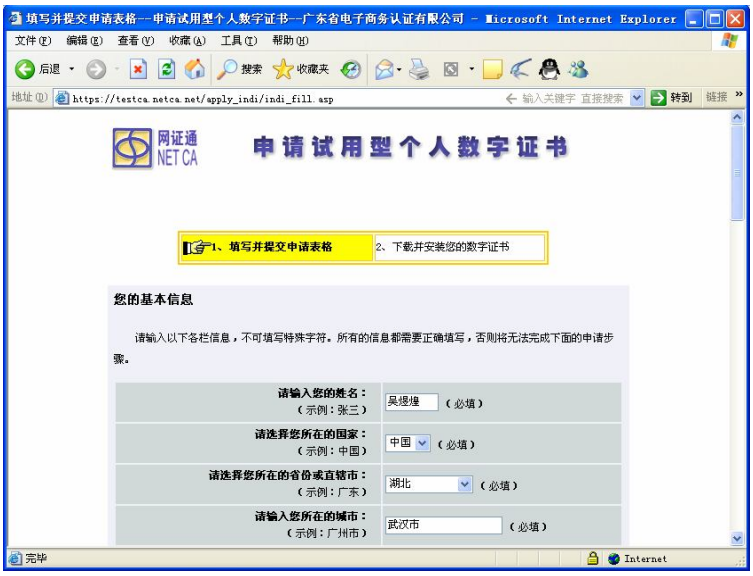

图 3-11　填写基本信息

填写完基本信息后，单击“继续”按钮，出现如图 3-12 所示的对话框，单击“是”按钮。

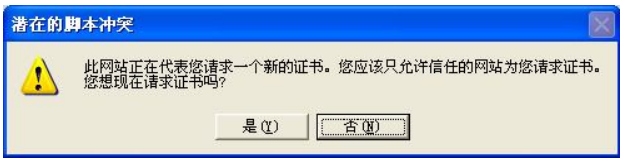

图 3-12　“潜在的脚本冲突”对话框

进入数字证书的下载安装页面，单击“安装证书”按钮，如图 3-13 所示。

图 3-13　下载并安装数字证书

进入数字证书身份校验页面，输入证书业务受理号和密码，单击“确定”按钮，如图 3-14 所示。

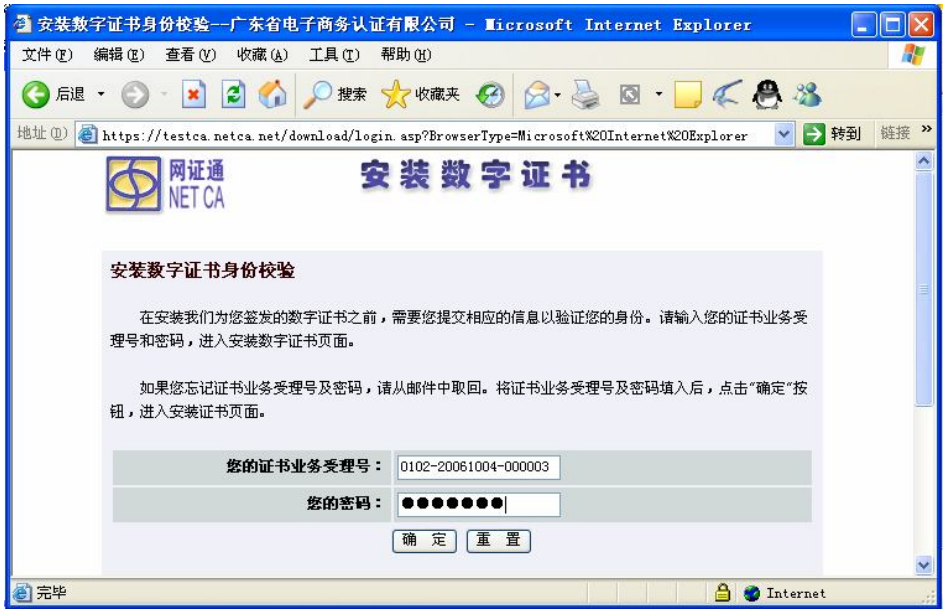

图 3-14　安装数字证书身份校验

系统提示已获得数字证书的基本信息，单击“安装证书”图标，如图 3-15 所示。

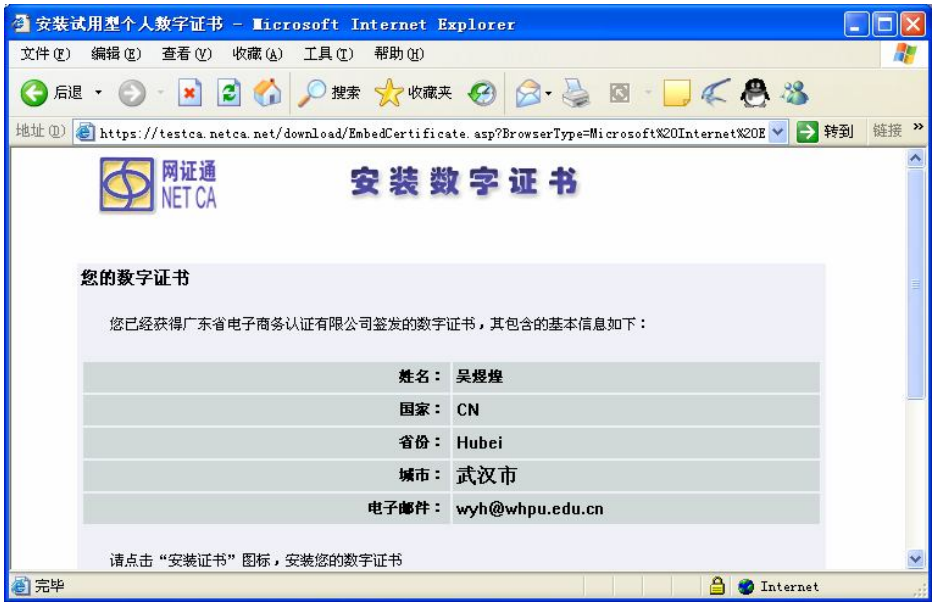

图 3-15　安装数字证书信息确认

出现如图 3-16 所示的提示框，单击“是”按钮。

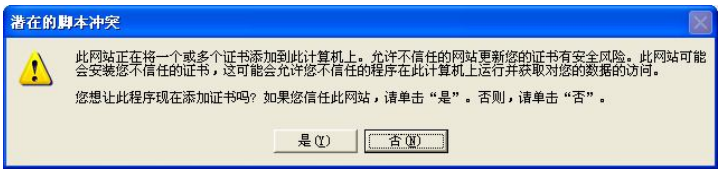

图 3-16 “潜在的脚本冲突”对话框

最后，出现“证书成功下载”的提示，如图 3-17 所示。

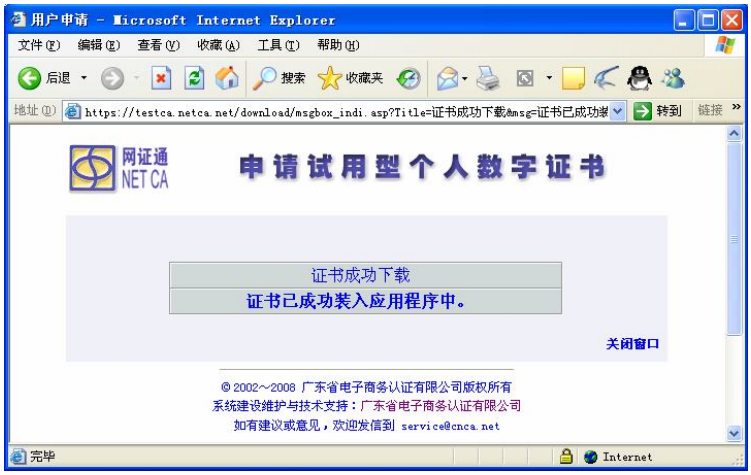

图 3-17 证书成功下载

我们可以查看已安装的数字证书，方法为：在 Internet Explorer 的菜单栏上选择“工具”→“Internet 选项”，在“Internet 选项”对话框中，打开“内容”选项卡，单击“证书”按钮，如图 3-18 所示，在“证书”对话框中，打开“个人”选项卡，就可以看到已经安装的个人数字证书列表，如图 3-19 所示，选定要查看的个人数字证书，然后单击“查看”按钮，可以查看详细的证书信息，如图 3-20 和图 3-21 所示。

图 3-18 “Internet 选项”对话框

图 3-19　个人数字证书对话框

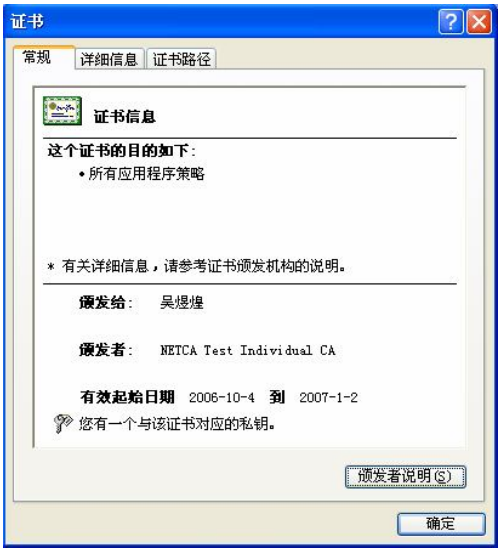

图 3-20　数字证书的基本信息

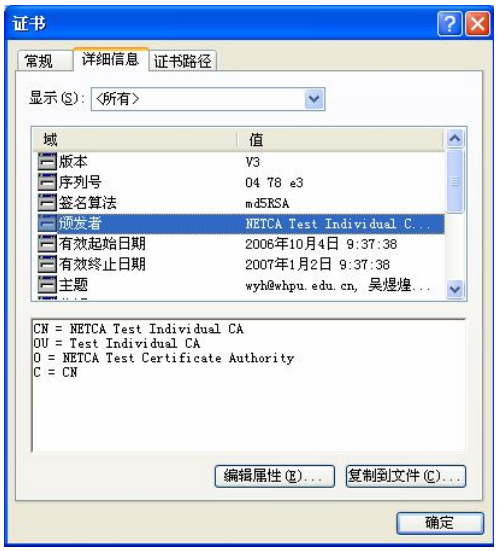

图 3-21　某数字证书的详细信息

3.5　Outlook Express 的操作实例

由于越来越多的人通过电子邮件发送机密信息，因此确保电子邮件中发送的文档不是伪造的变得日趋重要。同时保证所发送的邮件不被除收件人以外的其他人截取和偷阅也同样重要。

Microsoft 公司的 Outlook Express 是目前功能较完善、使用较方便的一个电子邮件管理软件，其中所提供的安全特性就支持前述的加密与数字签名，在 Internet 上可以发送和接收安全的电子邮件。下面具体介绍其使用方法。

要使用 Outlook Express 中的安全电子邮件，需要数字标识。数字标识（也叫证书）提供了一种在 Internet 上验证身份的方式，与司机驾照或日常生活中的其他身份证的验证方式相似。这里所说的数字标识即前面提到的公开密钥 PK 和秘密密钥 SK。

通过使用 Outlook Express 的“数字标识”，可以在电子事务中证明身份，就像兑付支票时要出示有效证件一样。也可以使用数字标识来加密邮件以保护个人隐私。数字标识结合了 S/MIME 规范来确保电子邮件的安全。

数字标识允许给电子邮件签名，这样真正的收件人可确保该邮件确实是由用户发来的并且没有受损。另外，数字标识也允许其他人给用户发送加密邮件。

1. 数字标识的工作方式

数字标识由公用密钥、私人密钥和数字签名三部分组成。当在邮件中添加数字签名时，就把数字签名和公用密钥加入到邮件中。数字签名和公用密钥统称为证书。可以使用 Outlook Express 来指定他人向用户发送加密邮件时所需使用的证书。这个证书可以不同于用户的签名证书，如图 3-22 所示。

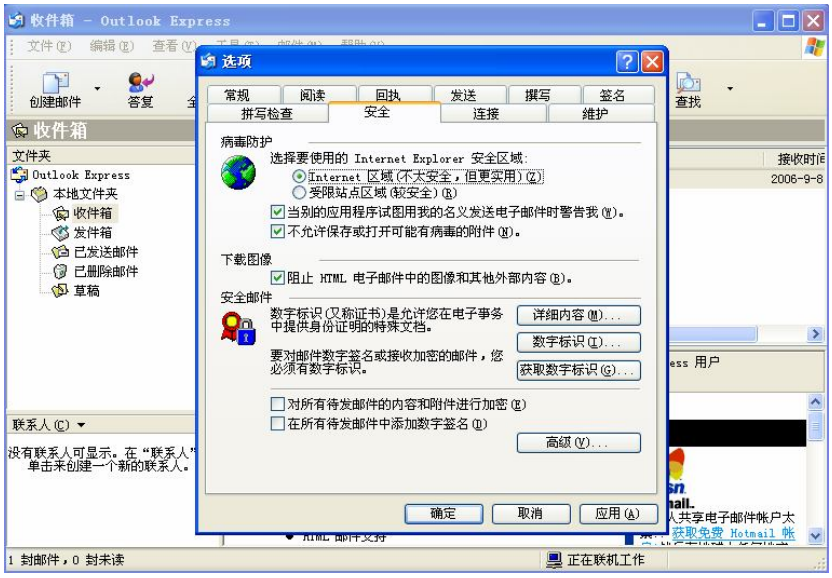

图 3-22 Outlook Express 的界面

收件人可以使用数字签名来验证身份，并可以使用公用密钥发送加密邮件，这些邮件必须用私人密钥才能阅读。要发送加密邮件，通讯簿必须包含收件人的数字标识。这样，就可以使用他们的公用密钥来加密邮件了。当收件人收到加密邮件后，用他们的私人密钥来对邮件进行解密才能阅读。

在能够发送带有数字签名的邮件之前，必须获得数字标识。如果正在发送加密邮件，通讯簿中必须包含每位收件人的数字标识。

2. 获得数字标识

数字标识由独立的证书颁发机构发放。在证书颁发机构的网站申请数字标识时，证书颁发机构在发放标识之前将确认身份。数字标识有不同的类别，不同类别提供不同的信用级别。

使用数字标识之前需要先获取数字标识（如图 3-23 所示），可以从发证机构获得数字标识，

那是一个负责发布数字标识的组织，并不断地验证数字标识是否仍然有效。然后可以将数字标识发送给需要给你发送加密邮件的用户，也可以用相同的数字标识发送签名邮件。有较多的商业发证机构，如果选用 Verisign 公司，可以通过以下步骤获得数字标识。

图 3-23　获得数字标签的界面

访问 http://www.verisign.com 站点，按提示填入个人信息及电子邮件地址，确认无误并提交后，稍过一会儿，可以从电子信箱中收到一封 Verisign 公司发来的电子邮件，其中就包含了你的 DigitalIDPIN。

根据刚收到的电子邮件的提示，访问 http://digitalid.verisign.com/mspickup.htm，然后根据提示输入你的 DigitalIDPIN 并提交，成功后，即可获得你的数字标识（数字标识将自动被加入到了本机的 Outlook Express 中）。

3. 使用数字标识

在发送签名邮件之前，必须注意电子邮件账号与数字标识的对应。为此，请选择“工具”菜单并单击“账号”，选择想使用标识的账号，单击“属性”，然后打开“安全”选项卡。检查名称为“发送安全邮件时使用数字标识”的对话框，然后单击“数字标识”，选择与该账号有关的数字标识（只显示出与账号的电子邮件地址相同的邮件地址的数字标识）。

4. 备份数字标识

数字标识的部分信息是存储在计算机上的不能替换的非公开关键字。如果该非公开关键字丢失，将无法再发送已签名的邮件或读取具有该数字标识的加密邮件。应该保留数字标识的备份，以防包含该数字标识的文件损坏或无法读取。要备份数字标识，先运行 Internet Explorer，然后选择“查看”菜单，单击“Internet 选项”，打开“内容”选项卡并随后单击“个人”按钮。“导入”和“导出”该页面上的按钮允许管理数字标识。

5. 验证数字签名

通过撤销检查，可以验证带数字签名邮件的合法性。进行检查时，Outlook Express 会向相应的证书颁发机构索取该数字标识的有关信息。证书颁发机构发回该数字标识的状态信息，其

中包括该标识是否已被撤销。证书颁发机构会监控由于遗失或终止等原因而被撤销的证书。

6. 安全电子邮件

已经申请拥有数字标识后，就可以发送安全电子邮件了。Outlook Express 中的安全电子邮件通过使用数字签名和加密对 Internet 通信提供保护。使用数字签名，可以在所发电子邮件上签署独特的标识，这样接收方就可以确认你是邮件的发送者，并且邮件在传送过程中未被篡改。对所发邮件进行加密有助于确保只有预定接收人员才能在传送过程中读取该邮件。

因为 Outlook Express 使用标准 S/MIME，所以其他人可以用支持该技术的工具阅读安全电子邮件。同样，也可以用支持 S/MIME 技术的电子邮件程序阅读他人撰写的邮件。Outlook Express 具有内置安全电子邮件，并提供具有下列特性的易用界面，如图 3-24 所示。

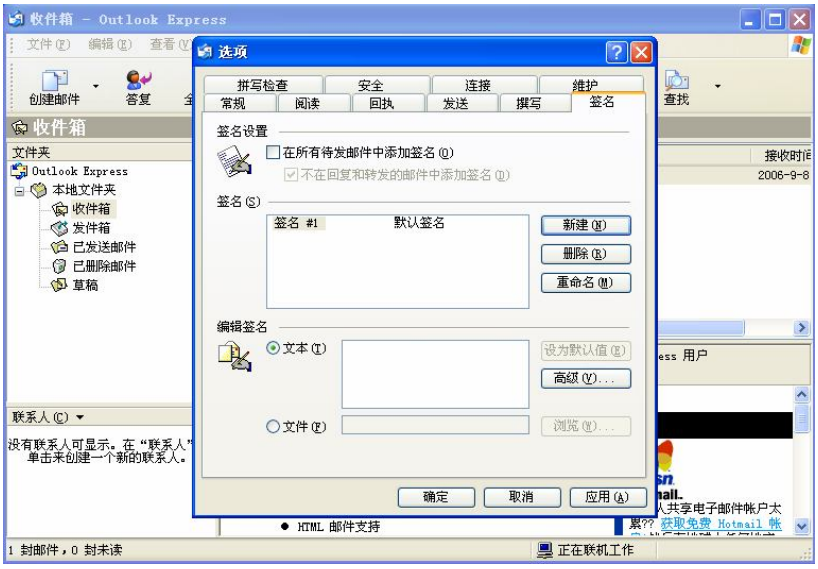

图 3-24 数字签名界面

（1）发送签名的邮件。签名电子邮件允许收件人验证你的身份。要对某邮件进行数字签名，可以选择“工具”菜单，然后单击“数字签名”（或使用邮件工具条上的按钮）。

（2）接收签名的邮件。来自其他人的已签名邮件允许验证邮件的身份——该邮件是否由指定用户发送、在发送过程中是否已更改。已签名的邮件带有特定的已签名图标。如果接收到的已签名邮件出现问题，则表明该邮件已被更改或来自其他发送人。

（3）发送加密的邮件。将某电子邮件加密会防止传输过程中有其他人阅读邮件。要将电子邮件加密，需要有收件人的数字标识。数字标识必须是“通讯簿”中所输入的那个数字标识的一部分。要发送加密邮件，请选择“工具”菜单，然后单击“加密”（或使用邮件工具栏上的按钮）。

（4）接收加密的邮件。收到加密的电子邮件信息时，Outlook Express 自动将电子邮件解密。

将你的数字标识发送给别人。他人必须知晓你的数字标识才能发送加密邮件。要将数字标识发送给他们，只要发送带有你的数字签名的电子邮件即可，Outlook Express 会自动包含数字标识。

（5）检索他人的数字标识。要向其他人发送加密邮件，必须知道他们的数字标识。Outlook

Express 允许通过目录服务检索数字标识。要查找数字标识，可以选择“编辑”菜单，然后单击“查找用户”，选择带有数字标识的目录服务（如 VeriSign 目录服务），在相应的搜索域中输入接受方名称或电子邮件地址，然后单击“查找”按钮，从结果窗格中选择列表，然后单击“添加到通讯簿”按钮。

获得他人数字标识的另一方法是让他给你发送签过名的邮件。要将一封签过名的邮件数字标识添加到你的“通讯簿”，请选择“文件”菜单并单击“属性”命令，打开“安全”选项卡并单击“将数字标识添加到通讯簿中”按钮。

本章小结

本章首先介绍了数字签名技术是公开密钥加密技术和报文分解函数相结合的产物，数字签名的目的是为了保证信息的完整性和真实性。CA 机构，又称为证书授权中心，作为电子商务交易中受信任和具有权威性的第三方，承担公钥体系中公钥的合法性检验的责任。CA 的作用有：自身密钥的产生、存储、备份/恢复、归档和销毁；提供密钥生成和分发服务；确定客户密钥生存周期，实施密钥吊销和更新管理；为安全加密通信提供安全密钥管理服务；提供密钥托管和密钥恢复服务；其他密钥生成和管理，密码运算功能。

接着介绍了电子证书是进行安全通信的必备工具，它保证信息传输的保密性、数据完整性、不可抵赖性、交易者身份的确定性。

最后介绍了认证中心的安全结构，包括物理与环境安全、网络安全、应用系统与数据安全、系统连续性管理、人员与日常操作管理这几大环节。

习　题

一、填空题

1．数字签名技术是_____和_____相结合的产物。

2．数字签名的目的是为了保证信息的_____和_____。

3．CA 体系由_____和_____部门构成。

4．电子证书是进行安全通信的必备工具，它保证信息传输的_____、_____、_____、_____。

5．X.509 数字证书包括_____、_____、_____三个可选的鉴别过程。

二、问答题

1．简述数字签名技术的基本原理。

2．什么是认证中心？电子商务的交易过程中为什么必须设定 CA？

3．简述 CA 的结构层次关系。

4．简述 CA 在密码管理方面的作用有哪些？

5．标准 X.509 数字证书包含哪些内容？

6．电子商务认证中心的安全结构包括哪些内容？