电子商务安全技术：认证技术电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/515/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_515838.htm 一、数字签名 使用密码机制对文件进行加密只解决了信息的保密性问题，但是如果他人对加密的文件进行破坏，或者你向一家公司下了订单但事后又加以否认，或者你冒充某人从账户上支取钱款等，对于这些问题，单靠密码技术是不能解决问题的。而数字签名技术（Digital Signature）则是一种很好的解决方法。签名是不能伪造的，接收者和第三方能够验证该文档确实来自签名者，并且在进行数字签名后文档未被修改过。一个安全的数字签名系统包括签名方法和验证方法，而且不可否认。实现数字签名的算法有很多，但利用公开密钥加密技术的数字签名则是应用得最广泛的一种。基于密钥加密和数字摘要技术，可以实现数字签名。 （一）数字摘要 数字摘要又叫消息摘要，也是一种加密方法，该方法又称为散列编码（Hash 编码）。散列编码利用单向的散列函数将需要加密的明文“ 摘要 ”成一串固定长度（如 128 位）的散列值，称为数字摘要，又叫做数字指纹（Finger Print）。根据所用的散列函数，生成的散列值有固定的长度。一定信息的散列值具有惟一性，即不同的信息摘要生成的散列值，其结果一定是不同的，而同样的信息其散列值则一定是一样的。散列函数还是一种单向函数，即只能从原信息摘要成散列值，而无法从散列值还原成原信息。散列算法不需要密钥，其算法原理对发送方和接收方是公开的。 （二）数字签名 由于散列算法是公开的，所以电子商务交易中的采购订单很有可能会被不怀好意者中途

拦截，在更改了订单内容后再重新生成数字摘要，然后将新生成的数字摘要与更改后的订单信息发送给接收方。为防止这种欺诈，就要对数字摘要进行加密。 发送方用自己的私有密钥对数字摘要进行加密，就形成了数字签名。 对于信息的安全来说，利用数字签名进行验证可以保证传输数据的完整性，实现信息在公开网络上的安全传输。 利用数字签名进行验证的过程如下：（1）发送方对要传输的信息运用散列函数形成数字摘要；（2）发送方用自己的私有密钥对数字摘要进行加密，得到数字签名；（3）发送方将数字签名附加在原信息后通过网络传输给接收方；（4）接收方用发送方的公开密钥对接收到的数字签名进行解密，得到信息的数字摘要；（5）接收方用同样的散列函数对接收到的信息重新计算数字摘要；（6）接收方将计算得到的数字摘要与解密得到的数字摘要进行比较，若两者相同，则说明信息的完整性未被破坏，即该文件不是伪造的。 数字签名可以用来防止电子信息因容易被修改而有人做假，或冒用别人名义发送信息，或发出（收到）信息后又加以否认等情况的发生。（三）数字时间戳 在电子商务中，除了要考虑数据的保密性、完整性、不可否认性及不可伪造性，还需要对交易数据的日期和时间信息采取安全措施，而数字时间戳服务（Digital Time-stamp Service，DTS）就能提供电子信息在时间上的安全保护。 数字时间戳服务是网上的安全服务项目，一般由大家均信任的第三方机构提供。数字时间戳其实是一个经加密后形成的凭证文档，包括三个部分：（1）需要加时间戳的信息的摘要；（2）数字时间戳服务机构收到该信息的日期和时间；（3）数字时间戳服务机构的数字签名。 数字时间戳

可以作为电子商务交易信息的时间认证，在一旦发生争议时作为时间凭证。 二、数字证书 由于在电子商务交易中，买卖双方在交易过程中是互不照面的，因此就需要有一种事物来表明自己的身份，以示自己是一个合法的用户或合法的商家。电子商务中的数字证书就是这样一种由权威机构发放的用来证明身份的事物。 在网上，双方要想谈一笔生意，任何一方都要鉴别对方是否是可信的，也就是要确定交易双方的身份。但是，如何才能保证所得到的公开密钥的正确性，即如何保证交易对方的真伪呢？为了解决这个问题，就引出了认证机制。认证机制包含两个部分，即数字证书（Digital Certificates）和认证中心（Certificate Authorities，简称 CA）。 （一）数字证书 数字证书是用电子手段来证实一个用户的身份和对网络资源的访问权限。证书就是一份文档，记录了用户的公开密钥和其他身份信息。数字证书是由 CA 认证中心颁发的、包含了公开密钥持有者信息以及公开密钥的文件，证书上还有 CA 认证中心的数字签名。就像驾驶执照能将照片、姓名、出生日期进行有公证效果的关联一样，一个用户的数字证书就是一个有公证效果的将公开密钥与所有者的身份信息相联系的“ 数字身份证 ”。在网上的电子交易中，如果双方出示了各自的数字证书并用它来进行交易操作，那么双方都可不必为对方的身份担心。数字证书可用于与电子商务相关的各个领域。 1、数字证书的内容 数字证书中一般包含证书持有者的名称、公开密钥、认证中心的数字签名，此外还包括密钥的有效时间、认证中心的名称以及该证书的序列号等信息。交易伙伴可以利用数字证书来交换彼此的公开密钥。 国际电信联盟（ITU）在其制订的 X.509 标准（信息技

术开放系统互联目录：鉴别框架）中，对数字证书进行了详细的定义。一个标准的 X.509 数字证书包含如下主要内容：（1）证书的版本信息。（2）证书的序列号。每个证书都有一个惟一的证书序列号。（3）证书所使用的签名算法。（4）证书的发行机构名称。命名规则一般采用 X.509 格式。（5）证书的有效期。现在通用的证书一般采用 UTC 时间格式，其计时范围为 1950 年～2049 年。（6）证书所有人的名称。命名规则一般采用 X.500 格式。（7）证书所有人的公开密钥。（8）证书发行者对证书的签名。2、数字证书的类型 数字证书一般分为三种类型：（1）个人数字证书 个人数字证书主要为某一个用户提供证书，以帮助个人用户和其他用户交换信息或者使用在线服务时，验证用户的身份，保证信息的安全，主要是针对个人的电子邮件安全。个人身份的数字证书通常安装在浏览器内，并通过安全的电子邮件来进行操作。目前常用的 Netscape 浏览器和 IE 浏览器都支持该功能。个人数字证书一般分为两个级别：第一级提供个人电子邮件的认证，仅与电子邮件地址有关，并不对个人信息进行认证，是最初级的认证。第二级提供个人姓名、个人身份等信息的认证。个 人数字证书是通过浏览器来申请获得的，认证中心对申请者的电子邮件地址、个人身份及信用卡号等进行核实后，就发放个人数字证书，并将数字证书安置在用户所用的浏览器中或电子邮件的应用系统中，同时通知申请者。个人数字证书的使用方法集成在用户浏览器的相关功能中，只要在浏览器中进行相应的选择就可以了。个人数字证书用于电子邮件时，可起到类似密封的信封和手写签名的作用。让接收方确定信件确实由你发出，并为邮件的内容和附件加密，

只有你所指定的接收方才能解密，从而防止了其他人截获阅读。（2）服务器证书 服务器证书主要为网上的某个 Web 服务器提供证书，拥有 Web 服务器的企业就可以用具有凭证的互联网站点进行安全的电子交易。拥有数字证书的服务器可以自动与客户进行加密通信，具有数字证书的 Web 服务器会自动地将其与客户端的 Web 浏览器的通信加密。服务器拥有者有了证书，就可以进行安全的电子交易了。 服务器证书的发放比较复杂。因为服务器证书是一个企业在网上的形象，是企业在网络空间信任度的体现，所以一个权威的认证中心对每一个申请者都要进行信用调查，包括企业的基本情况、营业执照、纳税证明等。此外，认证中心还要做如下的工作：①对企业服务器的管理情况进行考核。这一般是通过事先准备好的详细验证步骤来进行的，主要考察其是否具备了完善的管理规范。 ②对企业的技术条件进行考核。主要看其是否有完善的加密技术和保密措施。 ③对其设备的安全性、可靠性进行调查。主要包括是否有多层逻辑访问控制、生物统计扫描仪、红外线监视器等。 认证中心通过考察来决定是否发放或撤销服务器数字证书。一旦认证中心发放了数字证书，该服务器就可以安装认证中心提供的服务器证书，成功后即可投入服务。服务器得到数字证书后，就会有一对密钥（公开密钥和私有密钥），它与服务器之间是密不可分的。数字证书与这对密钥一起代表了该服务器的身份，是整个认证的核心。（3）开发者证书 开发者证书通常为互联网中被下载的软件提供证书。开发者证书又称为代码签名数字证书，借助这种数字证书，软件开发者可以为软件做数字标识，在互联网上进行安全地传送。在用户从互联网上下载软件时，

开发者证书与微软的 Authenticode（认证码）技术共同提供他们所需的软件信息和对该软件的信任。当客户从开发者网站上下载经过数字标识了的 ActiveX 控制命令、Java 程序、动态链接库、HTML 内容时，就能够确信该代码的确来自于开发者，而且没有被改变或破坏。开发者证书就好像是软件的外包装，如果它被篡改了，客户就知道代码实际已经不可信了。 在上述三类证书中，前两类是常用的证书，第三类则用于特殊场合。大部分认证中心都只提供前两类证书，能提供全部三类证书的认证中心并不多。 三、CA认证中心 CA又称认证权威、认证中心、证书授予机构，是承担网上认证服务，能签发数字证书并能确认用户身份的受大家信任的第三方机构。CA 通常是企业性的服务机构，其主要任务是受理数字证书的申请、签发及对数字证书进行管理。 CA是保证电子商务安全的关键，是公正的第三方，它为建立身份认证过程的权威性框架奠定了基础，为交易的参与方提供了安全保障，为网上交易构筑了一个相互信任的环境，解决了网上身份认证、公钥分发以及信息安全等一系列问题。 CA对含有公开密钥的证书进行数字签名，使证书无法伪造。每个用户都可以获得 CA 的公开密钥，以此来验证任何一张数字证书的数字签名，从而确定该证书是否由某 CA 签发的，该数字证书是否合法。数字证书与驾驶执照一样，用来表示个人的身份，且有一定的有效期，有效期结束后必须重新申请。CA 作为证书的发行机构具有一定的权威性，因而数字证书被社会所承认和接受。 数字证书与 CA 相结合为电子商务带来的好处是，如果两个用户都信任 CA 并从 CA 处得到一个证书，那他们就可以通过互相交换证书来得到对方的公开密钥。由于证书上

有 CA的数字签名，所以用户只要得到正确的 CA 的公开密钥，就可以通过对 CA 数字签名的鉴定来判断证书中的内容是否正确。数字证书和 CA 减轻了公开密钥交换过程中验证公开密钥的麻烦。也就是说，有了数字证书和 CA，用户就不再需要通过验证来信任每一个想要交换信息的用户的公开密钥，而只要验证和信任颁发证书的 CA 的公开密钥就可以了。在电子商务的认证体系中，CA 担当了权威的认证中心的职责。在电子交易中，无论是数字时间戳服务还是数字证书的发放，都不是靠交易双方自己就能完成的，而需要由一个具有权威性和公正性的第三方来完成。这个第三方可以是某个政府机构，也可以是某个独立的企业，但关键的是大家都要信任它。因此，电子商务需要建立一个全国乃至全球性的认证中心。 目前，在全球处于领导地位的认证中心是美国的 VeriSign 公司。VeriSign 公司提供的数字证书服务遍及世界各地，提供了我们在前面提到的所有三类数字证书，即个人数字证书、服务器数字证书和开发者数字证书。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com