电子商务的安全技术 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/65/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_65119.htm 就是保密性、完整性和可认证性。 目前电子商务系统中使用的安全技术包括网络安全技术、加密技术、数字签名、密钥管理技术、认证技术、防火墙技术以及相关的一些安全协议标准等。 网络安全技术 计算机网络安全是电子商务安全的基础，它所涉及到的方面比较多，如操作系统安全、防火墙技术、虚拟专用网VPN技术和入侵检测、漏洞检测技术等。 防火墙 主要是在某个机构的内部网络和不安全的网络之间设置屏障，阻止对信息资源的非法访问，也可以被用来阻止专利信息从企业的网络上被非法输出。包括四大类：分组过滤网关、应用级网关、线路级网关和规则检查防火墙。 加密技术与数字签名技术 加密技术是电子商务采取的主要安全措施，贸易方可根据需要在信息交换的阶段使用。目前，加密技术分为两类：对称加密和非对称加密。 (1)对称加密：又称为私钥加密。即对信息的加密和解密都使用相同的密钥。也 就是说：一把钥匙开一把锁。使用对称加密方法将简化加密的处理，每个贸易方都不必彼此研究和交换专用的加密算法，而是采用相同的加密算法并只交换共享的私有密钥。如果进行通信的贸易方能够确保专用密钥在密钥交换阶段未曾泄露，那么机密性和报文完整性就可以通过对称加密方法加密机密信息和通过随报文一起发送报文摘要或报文散列值来实现。 (2)非对称加密：又称为公钥加密。密钥被分解成为一对，即一把公开密钥或加密密钥和一把私有密钥或解密密钥。这对密钥中的一把作为公开

密钥，通过非保密方式向他人公开，而另一把则作为私有密钥加以保存。私有密钥只能由生成密钥对的贸易方掌握，公开密钥可广泛发布，但它只对应于生成该密钥的贸易方。贸易方利用该方案实现机密信息交换的基本过程是：贸易方甲生成一对密钥并将其中的一把作为公开密钥向其他贸易方公开，得到该公开密钥的贸易方乙使用该密钥对机密信息进行加密后再发送给贸易方甲，贸易方甲再用自己保存的另一把私有密钥对加密后的信息进行解密。贸易方甲只能用其私有密钥解密由其公开 密钥加密后的任何信息。 (3)数字签名：是公开密钥加密技术的另一类应用。主要方式是：报文的发送方从报文文本中生成一个128位的散列值(或报文摘要)，用自己的私有密钥对这个散列值进行加密来形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出128位的散列值，接着再用发送方的公开密钥来对报文附加的数字签名进行解密，如果两个散列值相同，那么接收方就能确认该数字签名是发送方的，通过数字签名能够实现对原始报文的鉴别。 认证技术 基于网络的电子商务在交易过程中，双方一般通过计算机进行交流，为了保证商务交易、支付活动的真实可靠，需要通过一种机制来验证活动中各方的真实身份。目前，最有效的认证方式是由权威的认证机构为参与电子商务的各方发放证书，证书作为网上交易参与各方的身份识别，就好象每个公民都用身份证来证明身份一样。认证中心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，是一个负责发放和管理数定证书的权威机构。因而网络中所有用户可以将自己的公钥

交给这个中心，并提供自己的身份证明信息，证明自己是相应公钥的拥有者，认证中心审查用户提供的信息后，如果确认用户是合法的，就给用户一个数字证书。这样，每个成员只需和认证中心打交道，就可以查到其他成员的公钥信息了。采用认证技术，除了能鉴别网上交易参与者的真实身份外，还能防冒充、防抵赖、防窃听、防篡改。对于在网上进行交易的双方来说，数字证书对他们之间建立信任是至关重要的。