 电子商务中的安全技术主要指密码技术和交易的安全机制。 密码技术有：对称密码技术、公钥密码技术、数字签名技术、Hash函数、公钥认证技术、双重签名加密技术等。在一个加密系统中，信息使用加密密钥加密后，接收方使用解密密钥对密文解密得到原文。数字签名用来保证信息传输过程中信息的完整和提供信息发送者的身份认证。双重数字签名是保证在电子交易过程中三方安全的传输信息的技术。认证技术分实体认证和信息认证。实体认证是对参与通信实体的身份认证，信息认证是指对信息体进行认证，以决定该信息的合法性。 安全机制用来保证电子商务中交易的安全性，如SET、SSL、S/MIME、S-HTTP等，这里我们主要介绍常用的SET标准。 安全电子交易SET是一种电子支付过程标准，用以保护网上支付卡交易的每一个环节，由VISA和Master Card合作产生，同时采用IBM、GTE、Microsoft、Netscape、RSA、SAIC、Terisa、VeriSign等多个公司的技术，是专为网上支付卡业务安全所制定的唯一有意义的标准，保证电子支付卡交易的安全进行，加密付款信息被安全地发送。SET标准主要由三个文件组成：SET业务描述、SET程序员指南和SET协议描述。 SET结合强大的加密功能和保证支付过程中每一步保密性和可靠性的一系列认证过程，主要包括四个方面： 信息的保密性：SET通过综合使用对称密钥加密技术、公钥加密技术与Hash函数实现信息的保密性； 确认能力：SET使用一种认证技术将持

卡人和一个专用帐号连接在一起，确认能力通过数字签名和认证实现；数据的完整性：SET使用Secure Hash和数字签名方法来确保交易的完整性；多方的操作性：SET协议使用的协议和信息格式来保证在不同的软硬件平台上运行。 一项SET交易有五个部分组成： 持卡人，即客户； 商家； 发行人，客户的金融机构，给客户提供支付卡，给商家提供支付；收单银行，商家的金融机构，保证商家能接受一种支付卡品牌并将获得的支付转发给商家；认证授权机构，一个可信任的第三方，能够验证客户、商家和收单行之间身份。 其中，发行人通过安全的网络或其他交流渠道与获得者通信，因此不需要用安全的网络技术。其他4部分则需要他们自己的SET软件。由于SET是一项开放协议，所以任何软件开发者可以为这些机构的任意一方开发兼容的软件，即持卡人软件、商家软件、支付网关软件和认证授权机构软件。 SET使用综合的密码技术（包括对称密钥加密技术、公钥加密技术与Hash函数）以达到安全交易的要求，从而确保交易的安全性和可靠性。虽然多层次的复杂安全技术使所有的四方成员都受益，但很少需要使用者看见它们，并且它们在后台的执行过程是透明的。 