综合辅导：数字证书在电子商务中的应用电子商务考试 PDF 转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/516/2021_2022__E7_BB_BC_E5_90_88_E8_BE_85_E5_c40_516856.htm [摘要] 随着Internet的普及，电子商务在日益发展，电子商务在为人们带来无限商机的同时，也给人们提出一个十分严峻的课题，即如何防范电子交易及支付过程中的欺诈行为，保证交易信息的机密性、有效性、完整性和不可否认性。将基于公钥理论的数字证书技术应用到电子商务中是保证电子商务安全的一个有效措施。 [关键词] 电子商务数字证书公开密钥 随着计算机、网络、信息技术的日益发展和融合，Internet已渗入到我们社会生活的各个方面。电子商务就是近几年随着信息技术的高速发展和Internet的普及而出现的一种崭新的数字交易方式。电子商务作为一种新型的商务手段，相对于传统商务模式，具有便捷、高效的优点。它正在迅速地改变着人们经济活动中传统的交易方式和流通技术，它改变了贸易形态，也正在改变人们的生活方式和思想观念，它的迅猛发展对全球经济和社会生活都产生了巨大影响。尽管如此，当今全球通过电子商务渠道完成的贸易额仍只是同期全球贸易额中的一小部分。究其原因，电子商务是一个复杂的系统工程，它的实现还依赖于众多从社会问题到技术问题的逐步解决与完善。其中，电子商务安全是制约电子商务发展的一个核心和关键问题。为了电子商务的安全,需要考虑的主要安全因素有以下几个方面:一是有效性。电子商务以电子形式取代了纸张，那么如何保证这种电子形式的贸易数据在确定的时间、确定的地点是有效的，是开展电子商务的前提。二是机密性。电子商务作

为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过可靠的通信渠道发送商业信息来达到保守机密的目的。电子商务建立在一个开放的网络环境上，因此防止信息在传输过程中被非法窃取是全面推广电子商务应用的重要保障。三是完整性。贸易各方信息的完整性是电子商务应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。四是不可抵赖性。在传统的纸面贸易中，贸易双方通过在交易合同、契约等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约的可靠性并预防抵赖行为的发生。在无纸化的电子商务方式下，如何确定贸易各方的真实身份并对其发生的行为不能抵赖，这一问题是保证电子商务顺利进行的关键。 因此，为了保证互联网上电子交易的安全性，防范交易及支付过程中的欺诈行为，必须在互联网中建立并维持一种令人信任的环境和机制。基于公开密钥技术的数字证书解决方案，现已被普遍采用。百考试题提供 一、数字证书的概念及其内容 数字证书是是一种权威性的电子文档，形同网络环境中的一种身份证，用于证明在网上进行信息交流及商务活动的各主体（如人、服务器等）的身份，它是由一个权威机构发行的。每一个数字证书包含了用户身份的部分信息、用户所持有的公开密钥及认证机构的数字签名。 国际电信联盟（ITU）制定的标准X.509对数字证书格式进行了定义，证书中包含如下内容：* Version:代表证书的版本格式是版本1、版本2或版本3。 * Serial number:由认证机构发放的代表该证书的惟一标识号。 * Signature Algorithm：认证机构用来对证书进行签名所使用的

数字签名算法的算法标识符及算法参数。 * Issuer Name:发放证书的认证机构的X.500名称。 * Validity:证书的起始和终止的日期和时间。 * Subject Name:与相应的被验证公钥所对应的私钥持有者的X.500名称。 * Subject Public Key:主体的公钥值以及该公钥被使用时所用的算法标识符及算法参数。 * Issuer Unique Identifier:颁发者惟一标识。 * Subject Unique Identifier:主体证书拥有者惟一标识。 * Extensions：证书扩充部分，用来指定额外信息。 * Signature：认证机构的数字签名。 二、数字证书的认证原理 数字证书基于公钥技术。在公开密钥系统中，为每个用户生成一对相关的密钥：一个公开密钥和一个私有密钥。公开密钥用于对机密信息的加密，通过非保密方式向他人公开；私有密钥用于对加密信息的解密，由用户自己安全存放。这样贸易双方进行信息交换的基本过程是：发送方通过网络或其他公开途径得到接收方的公钥，然后使用该密钥对信息加密后发送给接收方；接收方用自己的私钥对收到的信息进行解密，得到信息明文。在这里，只有接收方（而不是其他第三方）才能成功地解密该信息，因为只有接收方拥有与之相对应的私有密钥，从而保证了信息的机密性。如果发送方在发送信息时附上自己的数字签名（数字签名是指用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据），则接收方通过验证数字签名可以保证信息的完整性和不可抵赖性。 由此可见，采用了公钥技术可以确保网上交易的安全性，但前提是必须确保用户所使用的正是另一通信方正确的公钥。如果入侵者用其他公钥值替代了有效的公钥值，那么加密信息内容就会被泄露给非预期的通信方，信息的安全保密性就会受到影响。采用数字证书可以很好地

解决这一问题，每一个证书包含了证书主体的一个公钥值和对其所作的无二义性的身份确认信息，这样就把用户身份和他的公钥绑定在一起。证书本身不需要保密，又因为证书中包含了认证机构的数字签名，所以具有自我保护功能，不可能被入侵者篡改，这样数字证书同时也能起到公钥分发的作用。百考试题收集整理 三、数字证书的类型 从证书的使用者来看，数字证书可分为个人数字证书、机构数字证书和设备数字证书。 1．个人数字证书：证书中包含个人身份信息和个人的公开密钥，用于标识证书持有人的个人身份。 2．机构数字证书：证书中包含企业信息和企业的公开密钥，用于标识证书持有企业的身份。 3．设备数字证书：证书中包含服务器信息和服务器的公开密钥，用于标识证书持有服务器的身份。 从证书的用途来看，数字证书可分为签名证书和加密证书。 1．签名证书：主要用于对用户信息进行签名，以保证信息的不可否认性。 2．加密证书：主要用于对用户传送的信息进行加密，以保证信息的真实性和完整性。 四、数字证书的发放 数字证书是由一个权威机构CA(Certification Authority)证书管理机构发行的。CA认证机构，作为电子商务交易中受信任的第三方，具有权威性、公正性和惟一性的特点，它承担公钥体系中公钥的合法性检验的职责。它负责数字证书的申请、签发、发放、撤消和管理，并提供用户信息和密钥的管理。 五、结束语 电子商务是互联网应用发展的必然趋势，它将逐渐成为我们经济生活中一个重要部分。不要让安全问题成为电子商务发展的瓶颈，基于公钥技术的数字证书能够全面支持电子商务应用的各种主要模式，确保交易信息的安全性，从而极大地推动电子商务的发展。F8F8"