2006电子之如何构建安全的电子商务网站二 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/64/2021_2022_2006_E7_94_B5_E5_AD_90_c40_64787.htm 电子商务应用中遇到的各种问题：（1）采用数字信封技术保证数据的传输安全；（2）采用数字签名和双重数字签名技术进行身份认证并同时保证数据的完整性、完成交易防抵赖；（3）采用口令字技术或公开密钥技术进行身份认证。（4）结合数字信封和数字签名就可以满足电子商务安全中对数据的安全性、数据的完整性和交易的不可抵赖性的要求，同时可以使用数字证书来进行交易双方身份的认证。3、PKI体系结构 提起电子商务的安全性，我们就不得不提到PKI（Public Key Infrastructure），即公钥基础结构。PKI利用公钥加密技术为网上电子商务的开展提供了一套安全基础平台，用户利用PKI平台提供的安全服务进行安全通信。 PKI（公开密钥体系）一词被解释成为是一种框架体系，通过它，在不安全的信道上的通信的用户可实现信息数据的安全交换，满足商务对保密性，完整性，身份认证及不可否认性的安全需求，其构成主要包括硬件、软件、人员、指导原则及方法。它的好处在于：第一，网上交易双方可通过值得信赖的第三方机构完成交易，由于金融机构的特殊身份常使其充当第三方认证机构的角色，因此可将交易双方的风险降至最低；其次，PKI的应用发展已从区域型逐步发展到全球性，如著名的Identrust 组织建立了一套支持全球数字证书发放的体系，包括不同证书机构之间合作的程序以及对争议、索赔等问题的处理等，使具有法律约束力的电子商务得以在全球范围内展开。PAA：政策批准机构，创建整个PKI系

统的方针，批准本PAA下属PCA的政策，为下属PCA签发公钥证书，建立整个PKI体系的安全政策，并具有监测各PCA行为的责任。 PCA：政策CA，制定本PCA下的具体政策，可以是PAA政策的扩充或细化，但不能与之相背离。这些政策可能包括本PCA范围内密钥的产生，长度，证书的有效期规定，CRL的处理等。并为下属CA签发公钥证书。 CA：不具备或具备有限的政策制定功能，按照上级PCA制定的政策，担任具体的用户公钥证书的生成和发布，或CRL生成发布职能。 RA：进行证书申请者的身份认证，向CA提交证书申请请求，验证接收到的CA签发的证书，并将之发放给证书申请者。必要时，还协助证书作废过程。 