综合辅导：PKI_PMI与电子商务安全电子商务考试 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_516852.htm 摘要： 随着网络的飞速发展，网络与信息系统的安全与保密问题越来越重要，电子商务安全问题引起了人们的密切关注。本文对电子商务安全的需求及PKI/PMI技术进行了探讨。 关键字： PKI/PMI 电子商务 安全 一、电子商务及其安全需求 近年来，随着网络技术和电子商务的迅猛发展，人们以各种方式使用着Internet从事电子商务活动。电子商务已经成为人们进行商务活动的新模式。电子商务有比传统商务方式更巨大的方便性和灵活性。 然而，网络面临的安全问题也随之而来，例如内部窃密和破坏，截收，非法访问，破坏信息的完整性，破坏系统的可用性等等诸多问题。于是需要构建一个安全的信息基础设施平台，为电子商务提供良好的应用环境。解决网络与系统安全的技术与设备有防火墙、入侵检测、漏洞扫描、网络隔离等。这些信息安全技术对防外来攻击、防非法入侵等发挥着较大的作用。但是，这些技术并不能全面地满足电子商务的安全需要，电子商务的发展对信息安全提出的不仅仅是信息的机密性，还包括信息的完整性和不可否认性。PKI技术能很好地满足这一需求。由于通过网络进行的电子商务活动缺少物理的接触，因而使得用电子方式验证信任关系变得至关重要。而PKI技术恰好是一种适用于电子商务的密码技术，它能够有效地解决电子商务应用中的机密性、真实性、完整性、不可否认性和存取控制等安全问题。 二、PKI/PMI技术 1．公钥基础设施PKI PKI（Public Key Infrastructure）即公开密钥体

系，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。简单来说，PKI就是利用公钥理论的技术建立的提供安全服务的基础设施。PKI技术是一种新的网络安全技术，是一个集硬件、软件、人力资源、相关政策和操作规范为一体的综合系统，它由公开密钥密码技术、数字证书、证书发放机构（CA）和关于公开密钥的安全策略等基本成分共同组成的。严格地讲，一个完善的PKI必须具有认证机构CA、证书库、密钥备份及恢复系统、证书作废处理系统、PKI应用接口系统等组成部分。其中，认证机构CA是整个系统的核心。用户使用由证书授权认证中心（Certificate Authority，CA）签发的数字证书，结合加密技术，可以保证通信内容的保密性、完整性、可靠性及交易的不可抵赖性，并进行用户身份的识别。PKI的基础是加密技术，核心是证书服务。 2．授权管理基础设施PMI PKI能够实现ISO7498-2定义的五大安全服务（身份认证、访问控制、数据保密性、数据完整性、不可否认性）中的大部分功能，但在访问控制上存在一些不足，这主要是因为作为PKI基础的CA证书只是绑定了用户的身份。在有些情况下，单独的身份认证技术不能完全满足系统要求，如基于角色的访问控制。电子商务系统不仅要求用户提供合法的身份证书用于身份认证，而且要求提供相应的授权管理机制，用于控制用户在系统中的行为和动作。授权管理基础设施(Privilege Management Infrastructure，简称PMI)是在PKI发展过程中被提出并逐渐从PKI中分离出来的一个新的概念。PMI提出了一个新的信息保护基础设施，能够系统地建立起对认可用户的授权，它是由属性证书（Attribute

Certificate AC）、属性权威、属性证书库等部件的集合体，用来实现权限和属性证书的产生、管理、存储、分发和撤销等功能。属性证书是经过签名的结构，将用户的一组属性和其它信息通过认证机构的私钥进行数字签名，使其不能伪造。其签名和颁发的机构是属性管理机构（Attribute Authority , AA）。赋予属性证书的签名不是用于证明公钥/私钥和身份之间的关系，而是用于证明证书所有者拥有的特权。PMI以资源管理为核心，对资源的访问控制权统一交由授权机构统一进行处理，即由资源的所有者来进行访问控制。基于PMI的集中授权系统采用基于属性证书的授权模式，向应用提供与应用相关的授权服务管理，提供用户身份到应用授权的映射功能。 PMI作为一个基础设施能够系统地建立起对认可用户的授权。通过结合授权管理系统和身份认证系统补充了PKI的弱点。PMI权限管理和授权服务基础平台应该满足下面的需求：作为权限管理和授权服务的基础设施，可以为不同类型的应用提供授权管理和访问控制的平台支持。 3．PKI/PMI的比较 PMI和PKI有很多相似的概念。如属性证书（Attribute Certificate, AC） 与公钥证书（PKC），属性权威（Attribute Authority, AA ）与认证权威（CA）。公钥证书是对用户名称和他/她的公钥进行绑定，而属性证书是将用户名称与一个或更多的权限属性进行绑定。数字签名公钥证书的实体被称为CA，签名属性证书的实体被称为AA。PKI和PMI之间的主要区别在于：PMI主要进行授权管理，证明这个用户有什么权限，能干什么，即“ 你能做什么 ”；PKI主要进行身份鉴别，证明用户身份，即“ 你是谁 ”。将PKI和PMI技术结合，实现可信的身份认证和可信授权管理是目前较为完善的安全保

障措施。百考试题编辑整理 三、小结 PKI和PMI是目前较为完善的Internet解决方案，其目的是为用户建立起一个安全的网络运行环境，为电子商务提供身份认证、访问控制、数据保密性、数据完整性以及不可否认性等服务。通过PKI/PMI系统，能够为电子商务提供强大的系统安全保障，使用户可以在多种应用环境下进行安全的电子交易，PKI/PMI技术在电子商务系统中发挥着重要作用。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