我国移动电子商务应用安全问题探析电子商务师考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/630/2021_2022__E6_88_91_E5_9B_BD_E7_A7_BB_E5_c40_630421.htm 伴随因特网的迅猛发展，集互联网、移动终端、无线技术为一体的移动商务已对传统贸易方式形成巨大冲击，并将以其快捷、方便、高质高效的显著优势成为21世纪国际贸易的主要方式。电信趋势国际公司预测，全球移动商务至2008年将吸引17亿用户，使用手机进行的交易额预计将突破5540亿美元。据市场权威预测，2009年全球移动商务收入将突破880亿美元，手机铃声与标志logos将成为手机购物的流行元素。移动商务作为一种移动互联的贸易方式，将成为全球具有战略意义的贸易手段和信息交换的有效方式。移动网络的开放性和移动终端的移动性给移动商务的发展和工作效率的提高带来了诸多优势，但安全问题仍是移动商务推广应用的瓶颈。随着手机及相关移动终端功能的完善，信息存储量的加大，大量的商务数据和个人信息资料将存储于移动终端，移动终端的安全性、考|试/大移动商务交易过程的安全性、移动商务交易信息及大量商业秘密的安全性都将面临日益严峻的安全威胁。 一、我国移动电子商务应用安全主要存在的安全威胁 移动电子商务的发展对我们而言既是机遇也是挑战，我们可以充分利用这个机遇实现跨越式发展。安全问题是移动电子商务的基石，更是移动电子商务能否取得成功最关键的因素。由于我国移动电子商务的发展应用还处于起步阶段，如法律规范不完善，信用意识淡薄、移动终端限制了安全性能的提高和无线网络本身的开放性降低了安全性等原因导致移动电子商务应用过程中

存在诸多安全威胁。（一）无线通信网络的安全威胁 无线通信网络可以实现不受时间地理环境的限制，给无线用户带来通信自由和灵活性的同时也带来了诸多不安全因素。如通信内容容易被窃听威胁、网路漫游的威胁、针对无线通信标准的攻击、窃取用户的合法身份、对数据完整性的威胁。（二）移动终端面临的安全威胁 移动终端的安全威胁比较复杂。由于移动终端的移动性，移动终端很容易被破坏或者丢失。势必造成安全影响，甚或安全威胁。更由于移动终端的持有者和网络终端的所有者一般情况下分属于不同的实体，因此，他们尽管都属于终端的范畴，但是他们所面临的安全威胁是不尽相同的。概括起来移动终端的安全威胁，主要包括如下方面：移动终端设备的物理安全；移动终端被攻击和数据破坏；SIM卡被复制；RFID被解密；在线终端容易被攻击。（三）软件病毒造成的安全威胁 自从世界上第一个针对Symbian操作系统的手机软件病毒出现，移动终端就已经面临了严峻的安全威胁。况且，手机软件病毒眼下呈加速增长的趋势，每个星期至少有一款新的手机病毒产生，这就加重了这种安全威胁。（四）商家欺诈行为造成的安全威胁 在移动商务中，消费者对于产品的了解只能通过图片和文字的简单说明了解、去判断，考|试/大这就使消费者对商品的产地、规格、原材料来源、成分等真实情况缺乏全面、深入的了解。这种交易双方的信息不对称，现实中消费者购买的商品与广告的信息不符，这种虚假广告对消费者的欺诈行为，我国移动商务中的售后服务滞后，一旦消费者要向商家退货或索赔，商务网站需要提供该经营者的详细信息资料，但商务网站常常以商业秘密为由拒绝提供。（五）移动商务平台运营

管理漏洞造成的安全威胁 随着移动商务的发展，移动商务平台林立。大量移动运营平台如何管理、如何进行安全等级划分、如何确保安全运营，还普遍缺少经验。移动商务平台设计和建设中做出的一些技术控制和程序控制的安全思考，急需要在运营实践中进行修正和完善，更需要把技术性安全措施和运营管理中的安全措施，交易中的安全警示和安全思考进行整合，以形成一个整合的、增值的移动商务安全运营和防御战略，确保使用者免收安全威胁 （六）移动商务应用主体缺乏安全思考面临的安全威胁 随着移动电子商务的发展，2.5G向3G的移植和提升，大量实测性项目进入试应用或试运营阶段。移动商务的应用会更加便捷，应用范围会进一步扩大。但是相当多的移动商务应用主体缺少安全防范意识，缺少安全使用意识。概括起来存在着“ 五个缺少 ”：缺少对移动终端的安全性使用、运营和管理意识；缺少进行移动商务运作中的安全性、警示性思考；缺少进行移动商务前的系统性安全教育；缺少前瞻性、安全性防范知识和防范措施；缺少对移动商务数据安全备份、恢复以及对非法入侵者的追踪、取证等法律思考。 二、我国移动电子商务应用安全问题的策略 在移动电子商应用过程中要提升移动商务的技术防范能力，是提高移动商务安全性的关键和核心环节。因为移动安全技术在移动商务中守护着商家和客户的重要机密，维护着商务系统的信誉和财产，同时为服务方和被服务方提供极大的方便，因此，只有采取了必要和恰当的技术手段才能充分提高移动商务的可用性和可推广性。 （一）端到端策略 端到端在移动电子商务中意味着保护每个薄弱环节，确保数据从传输点到最后目的地之间完全的安全性，包括传输过程中

的每个阶段。即找出每个薄弱环顾并采取适当的安全性和私密性措施，以确保整个传输过程中的安全性并保护每条信道。移动电子商务带来了许多的设备，它们运行不同的操作系统且采用不同标准，因此安全性已经成为更加复杂的问题。公司需要实用的安全解决方案，这些解决方案应能够被快速简便的修改以便满足所有设备的要求，除此之外还要考虑全局。安全策略将对一系列商业问题产生影响，单独考虑安全性是远远不够的。实施128位鉴权码也非理想选择，因为程序太长会影响到用户使用的方便。同样，性能、个性化、可扩展性及系统管理等问题都会对安全性产生影响，它们全是制订安全策略时必须考虑的因素。（二）采用无线公共密钥技术（WPKI） 可通过部署无线公共密钥基础设施（WPKI）技术来实现数据传输路径的真正的端到端安全性、安全的用户鉴权及可信交易。WPKI使用公共密钥加密及开放标准技术来构建可信的安全性架构，该架构可促使公共无线网络上的交易和安全通信鉴权。可信的PKI不仅能够安全鉴权用户、保护数据在传输中的完整性和保密性而且能够帮助企业实施非复制功能，考|试/大使得交易参与各方无法抵赖。（三）加强交易主体身份识别管理 在移动商务的交易过程中通过强化主体资格的身份认证管理，保证每个用户的访问与授权的准确，实名身份认证解决方案的应用，可以增强移动商务交易的安全性，保证交易双方的利益不受到侵害。（四）加强移动商务安全规范管理 为了保证移动商务的正常运作，安全运作，必须建立起移动商务的安全规范，必须加强移动商务的法制建设，必须提升移动商务主体的安全意识，必须营造移动商务的整体诚信意识、风险营销意识和安全交易意识。通过

移动商务安全规范的建设，完善管理体制，优化交易环境，加强基础网络设施建设，提高整体的安全交易环境和服务质量，充分发挥法律法规在交易中的规范作用，建立整个交易过程的良性互动机制，促进移动商务的健康发展。（五）完善相关法律和制度，规范产业发展，建构安全交易环境。 移动电子商务是虚拟网络环境中的商务交易模式，较之传统交易模式更需要政策来规范其发展。有了法的保障才能使交易的双方具有安全感，才能逐步转变用户固有的交易习惯参与到方便快捷的移动电子商务模式中。国家应完善相关法律和制度，明确行业的发展策略和政策导向，为移动电子商务的发展提供公平竞争的环境，并保障各参与团体间的利益分配，从技术和资金等方面支持广大企业从事移动电子商务的业务开发。移动通信的安全性还应该通过各种方式进一步增强，有效的解决安全问题是移动电子商务所必须的，从而能更好地鼓励交易服务。目前正在开展对电子商务安全体系的研究工作，电子商务的安全体系已经慢慢发展成型。 移动电子商务随着移动互联网技术的成熟发展迅速，其独特的应用领域使得其安全问题倍受关注。则安全性是移动电子商务取得成功最关键的因素，从技术角度上看，一方面无线通信的安全处在不断地发展和完善之中，其应用到移动电子商务中时要与其他的安全机制相结合才能满足实际应用的需要；另一方面有线电子商务的安全技术不能解决移动电子商务的安全问题，所以WPKI技术是一个现实的选择。因此，只有将这两方面进行改进并有机整合才能营造一个安全的移动电子商务环境。编辑推荐：电子商务师考试复习方案电子商务师考试—电子商务员辅导电子商务师考试模拟试题 100Test 下载频道