电子商务安全技术：电子商务安全协议电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/515/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_515837.htm 一、增强的私密电子邮件（PEM） 增强的私密电子邮件（PEM）是因特网工程任务组（IETF）从 20 世纪 80 年代后期开始着手的一项工作的成果，这也是试图建立因特网邮件安全系统的首次正式努力。 有关 PEM 的工作导致了因特网标准提案于 1993 年面世，这是一个由四部分内容组成的提案。PEM 规范非常复杂，其第 I部分（ RFC 1421）定义了一个消息安全协议，而第 II 部分（RFC 1422）则定义了一个支持公开密钥的基础设施体系。PEM 的消息安全协议主要用于支持基本的消息保护服务。PEM 是这样运作的，首先获得一个未保护的消息，将其内容转换为一条 PEM 消息，这样，PEM消息就可以象其他消息一样通过正常的通信网络来进行传递了。PEM 规范认可两种可选的方法来进行网络身份验证和密钥的管理：一种是对称方案，还有一种是公开密钥方案。但是，只有公开密钥方案实施过。PEM 为消息安全协议的发展树立了一个重要的里程碑。但 PEM 在商用领域几乎从未成功过，主要原因是 PEM 与在同期发展起来的多用途网际邮件扩充协议 MIME 不兼容。 二、安全多用途网际邮件扩充协议（S/MIME） 电子邮件已经成为 Internet上最普及的应用，电子邮件的方便和快捷，以及低廉的费用赢得了众多用户的好评。电子商务活动离不开电子邮件，但是，电子邮件内容的安全正引起人们的关注。 （一）电子邮件内容的安全问题 如果用现实世界中的事物来比喻在 Internet上传送的电子邮件，最合适的恐怕就是明信

片了。就像写在明信片上面的信息一样，在机器之间传送的电子邮件都是公开的，每个人都可以查看上面的内容，至于看还是不看，这只取决于人们的诚实、对信息的不了解或漠不关心。而比明信片还要糟糕的是，电子邮件的发信人根本不知道一封邮件是经过了哪些中转站才到达目的地的。对于传统的通过邮政系统传送的邮件，国家可以制定相关的法律来保护邮件中传输的内容不受侵犯。而对电子邮件来说，事情就没这么简单了，邮件内容的安全取决于邮件服务器的安全、邮件传输网络的安全以及邮件接收系统的安全。 正是因为电子邮件的安全与上述方方面面密切相关，因而使得电子邮件的安全问题变得更加复杂。对邮件服务器的安全，我们可以用加设防火墙软件，控制用户对服务器的访问等方法来保障，但这并不能从根本上解决电子邮件内容本身的安全问题。 涉及电子邮件内容的安全问题主要有：（1）发送者身份认证：即如何证明电子邮件内容的发送者就是电子邮件中所声称的发送者。（2）不可否认：即发送者一旦发送了某封邮件，他就无法否认这封邮件是他发送的。（3）邮件的完整性：即能否保证电子邮件的内容不被破坏和篡改。（4）邮件的保密性：即防止电子邮件内容的泄漏问题。为了解决上述安全问题，历史上曾经提出过许多解决方案，其中三个经常提到的安全协议是 PEM，S/MIME 和 PGP。它们的共同特点是：采用公钥和私钥密码算法对电子邮件内容进行加密或签名，并且按照自己规定的标准格式对加密或签名的结果进行编码和重排，使接收方能够对电子邮件内容做出正确的解释。（二）S/MIME（secure/m ultlpurpose internetm ailextension） 1995 年，以 RSA 公司为首的几家大公司联合推

出了 S/MIME 标准，希望用它来解决上述有关电子邮件的安全问题。1998 年，S/MIME 推出了第 2 版，并在工业界获得广泛支持。但由于 S/MIME 第 2 版采用了 RSA 密钥交换算法，而该算法的专利权为 RSA 公司所有，其他公司不能自由使用，且采用的密钥位数长度不够，因此，S/MIME 第 2 版并没有被 IETF 接受为标准。 S/MIME 版本 2 由两个文档描述，分别是 RFC 2311和 RFC 2312。随后，IETF 负责了 S/MIME 第 3 版的修订工作，S/MIME 是在IETF 一致同意的情况下开发的，因而成为了 IETF 标准。S/MIME 的设计目标是，要使得自己能够比较容易地加入到已有的 E-mail产品之中。 为此，S/MIME 建立在两个已被广泛接受的标准之上：其一是 MIME（multipurpose mailextensions），其二是 PKCS（public key cryptography standard）。MIME 是目前几乎所有的 E-mail 都采用的格式，而 PKCS 是正处于建设当中的PKI的基础标准之一。因此，S/MIME 得到了各大软件厂商的大力支持。Microsoft公司的 Outlook Express和 Netscape公司的 NetscapeMessenger都提供了用S/MIME 发送和接收邮件的功能。目前，S/MIME 势头正旺，它很可能成为用户最终接受的标准。 S/MIME 所采用的安全标准包括：（1）信息格式：继承了MIME规格；（2）信息加密标准：包括 DES、三重 DES、RC4；（3）数字签名标准：PKCS；（4）数字证书格式：X.509。‘ （三）MIME 和 S/MIME Internet电子邮件由一个邮件头部和一个可选的邮件主体组成，其中邮件头部含有邮件的发送方和接收方的有关信息。对于邮件主体来说，特别重要的是，IETF 在 RFC 2045 ～ RFC 2049 中定义的 MIME 规定，邮件主体除了 ASCII字符类型之外，还可以包含各种数

据类型。用户可以使用 MIME 增加非文本对象，比如把图像、音频、格式化的文本文件加到邮件主体中去。MIME 中的数据类型一般是复合型的，也称为复合数据。由于允许复合数据，用户可以把不同类型的数据嵌入到同一个邮件主体中。在包含复合数据的邮件主体中，设有边界标志，它标明每种类型数据的开始和结束。S/MIME 在安全方面对 MIME 进行了功能扩展，它可以把 MIME 实体（比如数字签名和加密信息等）封装成安全对象。RFC 2634 定义了增强的安全服务，例如，具有接收方确认签收的功能，这样就可以确保接收者不能否认已经收到过的邮件。 S/MIME 还增加了新的 MIME 数据类型，用于提供数据保密、完整性保护、认证和鉴定服务等功能。如果邮件包含了上述MIME 复合数据，邮件中将带有有关的 MIME 附件。在邮件的客户端，接收者在阅读邮件之前，S/MIME 会处理这些附件。 三、安全超文本传输协议（S-HTTP） 安全超文本传输协议（S-HTTP）是致力于促进以因特网为基础的电子商务技术发展的国际财团 CommerceNet协会提出的安全传输协议，主要利用密钥对加密的方法来保障 W eb 站点上的信息安全。S-HTTP 被设计为作为请求 /响应的传输协议HTTP 的一种安全扩展版本，正是这一特点使得 S-HTTP 与 SSL 有了本质上的区别，因为 SSL 是一种会话保护协议。S-HTTP 的主要功能是保护单一的处理请求或响应的消息，这在某种程度上与一个消息安全协议保护电子邮件消息的工作原理相似。 事实上，S-HTTP 在很大程度上建立在消息安全协议的基础之上。S-HTTP 所提供的安全服务称为实体验证、完整性（ 通过完整性检查值进行）和机密性（通过加密）检验。此外还附加了一项可选的数字签名

功能，此项功能为附加的不可否认安全服务提供了基础。S-HTTP 在如何保护消息和管理密钥方面提供了很大的灵活，可以支持包括PEM（RFC 1421）和 PKCS#7 在内的特定消息保护格式，而密钥的管理也并不局限于严格的 PEM 架构或者其他任何严格的规则。加密密钥可以通过在 PEM 或PKCS#7 数字信封中传输的 RSA 密钥来建立，也可以通过人工方法预置，甚至可以用 Kerberos标签来建立。使用 S-HTTP 可以通过一个以“ shttp：// ”开头的统一资源定位符来说明，要注意的是，如果将其错误地混同为“ https：// ”，则意味着指定了 SSL 的使用。在万维网应用的早期，S-HTTP 曾经被一些网络安全通信服务提供商所采用，但现在它几乎已完全被 SSL 所取代，相对而言，SSL 普及的速度更快，所使用的范围也更广。 四、安全套接层协议（SSL） （一）SSL协议概述 安全套接层协议 SSL（secure socketlayer）最初是由 Netscape公司研究制定的安全通信协议，是在因特网基础上提供的一种保证机密性的安全协议。随后Netscape公司将 SSL 协议交给 IETF 进行标准化，在经过了少许改进后，形成了IETF TLS 规范。SSL 能使客户机与服务器之间的通信不被攻击者窃听，并且始终保持对服务器进行认证，还可选择对客户进行认证。SSL 建立在 TCP 协议之上，它的优势在于与应用层协议独立无关，应用层协议能透明地建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信加密的协商以及服务器的认证工作。在此之后，应用层协议所传送的数据都会被加密，从而保证了在因特网上通信的机密性。百考试题整理 SSL 是目前在电子商务中应用最广泛的安全协议之一。SSL 之所以能够被广泛应用，主要有两个方面的原因：（1

）SSL 的应用范围很广，凡是构建在 TCP/IP 协议上的客户机/服务器模式需要进行安全通信时，都可以使用 SSL 协议。而其他的一些安全协议，如 S-HTTP 仅适用于安全的超文本传输协议，SET 协议则仅适宜 B-to-C电子商务模式的银行卡交易。]（2）SSL 被大部分 Web 浏览器和 Web 服务器所内置，比较容易应用。目前人们使用的是 SSL 协议的 3.0 版，该版本是在 1996 年发布的。（二）SSL 协议的功能 SSL 协议工作在 TCP/IP 体系结构的应用层和传输层之间。在实际运行时，支持 SSL 协议的服务器可以向一个支持 SSL 协议的客户机认证它自己，客户机也可以向服务器认证它自己，同时还允许这两个机器间建立加密连接。 这些构成了 SSL 在因特网和其他 TCP/IP 网络上支持安全通信的基本功能： 1、SSL 服务器认证 允许客户机确认服务器身份。 支持 SSL 协议的客户机软件能使用公钥密码技术来检查服务器的数字证书，判断该证书是否是由在客户所信任的认证机构列表内的认证机构所发放的。例如，用户通过网络发送银行卡卡号时，可以通过SSL 协议检查接受方服务器的身份。 2、确认用户身份使用同样的技术 支持 SSL 协议的服务器软件能检查客户所持有的数字证书的合法性。例如，银行通过网络向消费者发送秘密财务信息时，可以通过 SSL协议检查接受方的身份。 3、保证数据传输的机密性和完整性 一个加密的 SSL 连接要求所有在客户机与服务器之间发送的信息由发送方软件加密和由接受方软件解密，这就提供了高度机密性。另外，所有通过 SSL 连接发送的数据都被一种检测篡改的机制所保护，这种机制自动地判断传输中的数据是否已经被更改，从而保证了数据的完整性。（三）SSL 的体系结构设计 SSL是为了利用 TCP 提供可

靠的端到端的安全传输。SSL 不是一个单独的协议，而是两层协议，即 SSL 记录协议和在记录协议之上的三个子协议。其中，最主要的两个 SSL 子协议是记录协议和握手协议。SSL 体系结构记录协议定义了要传输数据的格式，它位于 TCP 协议之上，从高层 SSL 子协议收到数据后，对它们进行封装、压缩、认证和加密。SSL 握手协议是位于 SSL 记录协议之上的最重要的子协议，被 SSL 记录协议所封装。该协议允许服务器与客户机在应用程序传输和接收数据之前互相认证、协商加密算法和密钥，SSL 握手协议包括在初次建立 SSL 连接时使用 SSL 记录协议在支持 SSL 协议的服务器与支持 SSL 协议的客户机之间交换的一系列信息。 通过这些信息交换可实现如下操作：（1）向客户机认证服务器；（2）允许客户机与服务器选择他们都支持的加密算法或密码；（3）可选择地向服务器认证客户；（4）使用公钥加密技术生成共享密码；（5）建立加密 SSL 连接。 由于SSL提供了两台机器间的安全连接，支付系统经常通过在 SSL 连接上传输银行卡卡号的方式来构建。虽然基于 SSL 的银行卡支付方式促进了电子商务的发展，但如果想要电子商务得以成功地广泛开展的话，必须在 SSL 基础上采用更先进的基于 PKI体系结构的银行卡支付系统，因为 SSL 仅为通信双方提供了安全通道，并没有解决持卡人的身份认证和交易的不可抵赖等问题。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