电子商务中的网络安全中间件应用 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/492/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c67_492052.htm 现已被广泛采用的公共密钥基础结构（PKI），是目前唯一一种能为所有网络安全要素的具体实现提供所必需的基础平台和构架模块的基础技术。但是PKI本身并不能提供网络安全保证，它仅为新的网络安全模型提供舞台。 各机构必须根据自己的业务要求，自行在两种基本的电子商务安全执行策略中进行选择。 IP安全是用以保护IP网络上两点间通讯的一族行业标准协议，它更被人们熟悉的名字是VPN（虚拟专用网络）。IP安全在IP层提供基于加密的认证、完整性和保密服务。IP安全对于电子商务的用户、应用程序和协议来说是透明的。由于对上层信息没有滤过性，IP安全也缺乏网络安全的几个基本要素，包括不能提供数字签名、不能很好的检查和识别应用程序的数据流以便采用适当的安全对策、不能在VPN的内部通过应用程序认证个人用户的身份以及不能向特定个人授权使用特定电子商务资源等。相对而言，电子商务往往需要更强健的安全支持。 对基于Web的应用程序而言，当前的安全标准是SSL（套接层安全）及其第三版TSL（传输层安全）。SSL这一机制被绝大多数web浏览器和服务器所支持。SSL提供对私密性和完整性的保障，并支持可选的服务器认证和客户认证。 最适合采用SSL的，是那些无需严格验证用户身份的电子商务提供者。如同IP安全一样，浏览器中使用的SSL也不支持电子商务所依赖的网络安全的若干基本要素，如：客户认证迫使用户学习在web浏览器中使用数字证书的复杂流程，SSL不能提供

用于电子商务事务认证的数字签名SSL的证书认证并非行业标准。绝大多数web服务器没有提供电子商务所要求的监视、日志记录和存取控制认证等防护措施。 为了有效地在web框架下实现网络安全的7点要求，下列的功能应当被补充进来：1．增加某种辅助web浏览器的客户端软件以便更透明地使用数字证书来进行客户认证，同时具有提供数字签名的能力 2．增加某种辅助web服务器的服务器软件来验证证书、监视和记录日志，并实现在网页或URL层的精细存取控制。 SSL对web浏览器的支持尽管并不完备，但已经提供了web下电子商务安全的基础框架。对于那些并非基于web的应用程序，要保证其电子商务安全性相比而言要困难得多，因为一个替代客户端软件必须在没有web浏览器的前提下执行其功能。有两种途径可以帮助我们达到目的：1．使用由开发商提供的PKI工具包来直接编写提供SSL支持的软件 2．使用支持SSL的PKI中间件来代表应用程序以实现电子商务安全 尽管工具包具有很大的灵活性，它也有一些弱点，它的全程开发和维护要花费大量劳力，推向市场节奏较慢，要求员工精通PKI和安全开发，不兼容大型主机，应用程序局限于特定的PKI开发商的许可、解释和协同工作，并依赖与开发商的技术支持。 因此，工具包最好用于PKI授权的厂商的商业软件以及试验，而并不十分适合大范围推广。 网络安全中间件与基于web的应用程序通过浏览器实施SSL安全服务有类似之处，然而，此时中间件的客户端软件将为所有的应用程序，包括基于web的应用程序来提供SSL服务。精心实现的网络安全中间件并不要求用户接受过培训或自行配置参数，同时依然能够提供支持各种应用程序协议的网络安全服务，并支持数字签名的使用和对所有桌面

程序的适度监控。 网络安全中间件解放了客户，使他们不再需要亲自处理复杂的基于PKI工具包的针对性解决方案，或是购买所需要的PKI授权的商用软件。一行代码都不用写，所有的应用程序，无论是遗留应用还是贸易应用程序，都可以无差别地使用一或多个PKI提供商的数字证书。 