

基于 WS-Security 的电子商务安全支付系统

郭悦红^{1,2}, 齐莉丽¹

(1 天津工程师范学院 经济与管理学院, 天津 300222; 2 天津大学 管理学院, 天津 300072)

摘 要: 为实现电子商务交易的安全支付, 采用 WS-Security 规范和 XML 技术结合构建电子商务安全支付系统. 该系统使订单信息和支付信息在同一个过程中进行不同的处理, 保证了在消息层上任意敏感信息的安全性, 并实现了交易的不可否认性, 从而提高了电子支付的安全性和灵活性.

关键词: 电子商务; WS-Security; XML; 电子支付

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)03-0151-03

Security Payment System of Electronic Commerce Based on WS-Security

GUO Yue-hong^{1,2}, QI Li-li¹

(1 School of economics and Management, Tianjin University of Technology and Education, Tianjin 300222, China;

2 School of Management, Tianjin University, Tianjin 300072, China)

Abstract: It puts forward a security payment system of electronic commerce by combining WS-Security specification and XML technology in order to realize security payment of electronic commerce transactions. The system realizes different treatments of payment information and order information in a process, ensures security of any sensitive information in the message layer, realizes non-repudiation of transactions, which improve the security and flexibility of electronic payment.

Key words: electronic commerce; WS-Security; XML; electronic payment

1 引言

随着电子商务的蓬勃发展, 电子支付已经是电子商务中的重要环节, 如何解决在线支付的安全问题愈显突出. 电子支付的安全性^[1]尤其是在支付额比较大的情况下, 直接影响着支付环节实施, 也可以反映出企业开展网上产品贸易的顺利程度, 主要表现在四个方面: 机密性、完整性、身份验证、不可否认性.

2 基于 WS-Security 支付系统

2.1 WS-Security 规范

WS-Security (Web Service Security) 是基于 XML 的安全性元数据容器的规范. WS-Security 规

范本身并没有定义新的安全协议, 而是在已存在的安全标准和规范中强调安全性. WS-Security^[2]提供了一个可扩展的框架, 用来在 SOAP 消息中嵌入安全性机制包含数字签名、消息摘要和数据加密等. 在基于 WS-Security 扩展的 Web Service 中, SOAP 传输的不再是简单的 XML 文本消息, 而是实现了 WS-Security 扩展的 XML 文件, 数字证书作为 XML header 中的一个属性被用户私有密钥加密, 传输的 XML Body 内容也进行了数字签名. 接收端对客户传输来的信息根据客户用户解密进行验证, 这样就保证了信息来源的准确以及信息完整性、保密性.

文中通过一个具体运用 WS-Security 规范的 Soap Envelop 例子解释 WS-Security 中使用 XML 安全组件. 下面介绍一下 XML 安全体系结构, 其框架

收稿日期: 2009-03-13; 修回日期: 2009-06-09

基金项目: 劳动和社会保障部科技项目(LB2007-03)

图 1 所示.

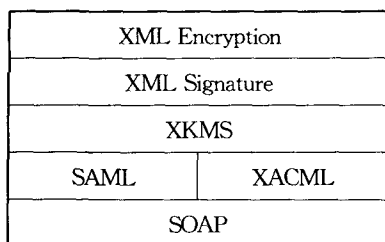


图 1 XML 安全体系框架

(1) XML Encryption: 在支付系统中, 主体之间传递的消息是通过 XML 文件表示的. XML 元素级加密只对传输消息的一部分内容进行加密, 而不是加密整个 XML 信息, 它利用不同接收对象的公用交换密钥对 XML^[3] 信息中不同的敏感信息进行加密, 对于同一条消息, 不同的接收实体只能获取属于自己的元素信息, 而无权查看其它实体的敏感信息.

(2) XML Signature: 对 XML 文档进行签名以及签名验证, 为电子商务提供确认性和不可否认的服务.

(3) XKMS: 密钥管理规范 (XML Key Management Specification, XKMS) 提供类似于 PKI 的密钥管理功能.

(4) SAML 和 XACML: 提供可迁移的信任体系和 XML 资源操作的权限控制. SAML^[4] 使信任可以移植. XACML 是用来决定是否允许一个请求使用一项资源, 比如它是否能使用整个文件, 多个文件, 还是某个文件的一部分^[5].

(5) SOAP: 提供基于 SOAP 协议的 XML 信息传输服务.

WS-Security 扩展 SOAP 消息结构如图 2 所示.



图 2 WS-Security 扩展 SOAP 消息结构图

2.2 电子商务安全支付系统

基于 Web 的电子支付系统^[6]框架如图 3 所示. 该框架在逻辑上主要包括客户端 (消费者和用户)、

企业服务器 (商家)、网络认证中心、电子支付工具、支付网关和金融网络等.

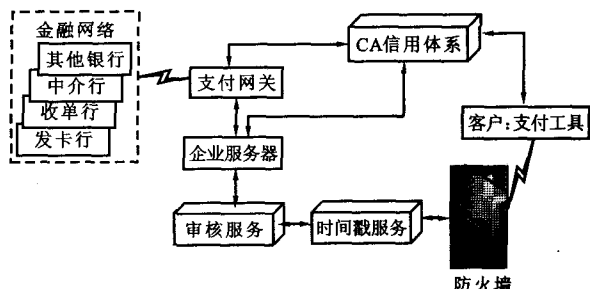


图 3 电子支付系统框架图

在电子商务交易中, 基本步骤如下:

(1) 消费者在企业网站选购货物, 完成订单的填写, 系统自动为订单添加创建日期.

(2) 消费者选择在线支付, 输入支付信息.

(3) 消费者、企业服务器和支付网关分别与 CA 认证中心建立各自的加密安全通道, CA 认证中心完成认证.

(4) 消费者用私有密钥解密出企业公用交换密钥, 利用该交换密钥加密所需传输消息中的订购信息部分; 同样, 利用支付网关的公用交换密钥加密消息中支付信息的部分^[7].

(5) 消费者将 XML 消息标准模式 XML Schema 和已部分加密的 XML 消息连接在一起, 通过 WS-Security 算法, 产生唯一识别本次传送消息的消息摘要, 并用自己的私用签字密钥对该消息摘要产生数字签名集成到 SOAP 消息头中.

(6) 客户机与企业防火墙建立连接, 获准通过防火墙连接与时间戳服务, 在请求信息的头部加入时间标记.

(7) 时间戳服务将客户请求信息通过 SSL 连接传递给审核服务, 并将对信息的审查结果添加进消息头中.

(8) 企业服务器从邮戳服务得到消费者请求消息, 使用其公用签字密钥解开 Schema 和 XML 消息摘要的数字签名, 得到消息摘要.

(9) 业服务器选取与消费者相同的单向算法计算 Schema 和 XML 消息的消息摘要, 与接收到的消息摘要进行比较.

(10) 如果两摘要比较结果一致, 企业则使用自己的私用交换密钥解密出消费者的订购信息, 确认订购数据. 企业生成支付请求信息, 利用步骤 (5) 的方法产生该支付请求信息消息摘要的签名并附加在消息头上.

(11) 付网关得到企业传送的消息后,通过使用与企业相同的检验方法,支付网关解密出客户的支付信息以及企业的支付请求信息。

(12) 通过 CA 信用认证核实客户身份、支付信息和账户信息以后,支付网关向企业返回确认信息。

(13) 消费者发卡行将相应的交易金额从客户账号转出到中介行。

(14) 企业继而向客户返回响应信息,同时向配送服务发出运货信息,配送服务向企业、支付网关发出货物成功递送的确认信息及其摘要的数字签名,同时支付网关也将同一份确认信息和自己对该信息摘要的签名转发给消费者。

(15) 客户确认,中介行则将暂存的交易金额转送到企业的收单行,否则,将交易金额转回发卡行,结束交易。

3 结束语

文中讨论了如何通过 WS-Security 规范和 XML 技术实现电子商务交易中的安全支付。XML 安全组件集成了包括 XML 数字签名服务和元素级加密服务在内的多项重要功能,并且实现了交易的不可否认性。元素级加密非常灵活地对传输的信息进行选择性的加密,使订单信息和支付信息同一个过程中进行不同的处理,从而保证了在消息层上任意敏感

信息的安全性。WS-Security 保证了 SOAP 消息安全传递的增强,提供了一种构建安全模型和加密技术的灵活机制。

参考文献:

- [1] 张爱菊. 电子商务安全技术[M]. 北京:清华大学出版社,2008.
- [2] 黄伟峰. Web Services 的安全性[J]. 计算机工程与设计,2003,24(6):52-55.
- [3] 陈桦,麻风梅,韩艳艳. 基于 XML 的异构数据集成模式的研究[J]. 微电子学与计算机,2009,26(1):137-139.
- [4] 李慧盈,张长海,李德昌. 基于 SOAP 协议的 Web Services 安全性扩展实现[J]. 计算机应用研究,2006,23(1):106-107.
- [5] 刘义春. 电子商务中的信任机制研究[J]. 微电子学与计算机,2008,25(3):121-125.
- [6] 谢琳,卢建军. 电子商务中第三方电子支付平台分析[J]. 计算机应用研究,2003,20(12):149-151.
- [7] 郭瑞颖,毛明,吴明玉,等. 一种基于 Web 的 B2B 安全电子支付模型的探讨[J]. 小型微型计算机系统,2001,22(10):1274-1276.

作者简介:

郭悦红 女,(1977-),博士研究生,讲师.研究方向为信息管理。

(上接第 150 页)

参考文献:

- [1] Cui Y, Weng J J. Hand segmentation using learning-based prediction and verification for hand sign language [C]// Proc of ICCV'96. USA:San Francisco,1996:88-93.
- [2] Cui Y, Swets D L, Weng J J. Learning based hand sign language using SHOSLIF-M[C]// Proc of ICCV'96. USA:San Francisco,1996:61-636.
- [3] Grobel K, Assan M. Isolated sign language recognition using hidden markov models[C]// Proc. of the International Conference of System, Man and Cybernetics. USA:Orlando,1996:162-167.
- [4] Wen Gao, Ma Jiyong, Wu Jiangqin, et al. Lange vocabulary sign language recognition based onHMM/ANN/DP

[J]. International Journal of Pattern Recognition and Artificial Intelligence,2000,14(5):587-602.

- [5] Woods Richard E, Eddins Steven L. 数字图像处理[M]. 阮秋琦,译.北京:电子工业出版社,2003.
- [6] 章毓晋. 图像工程:上册——图像处理和分析[M]. 北京:清华大学出版社,2001.
- [7] 刘志镜,夏勇,李夏忠. 基于正交视图的多姿态人脸识别算法[J]. 微电子学与计算机,2004,21(3):11-15.

作者简介:

孙丽娟 女,(1976-),硕士研究生.研究方向为图像信息处理。

张立材 男,副教授,硕士生导师.研究方向为信号处理。