Security Issues of the Supply Chain Management with Web-Services

Serap Atay, Izmir Institute of Technology, Turkey
Kaan Kurtel, Izmir University of Economics, Turkey
Şaban Eren, Ege University, Turkey
Ahmet Koltuksuz, Izmir Institute of Technology, Turkey

This paper presents the importance of the security parameters of the e-process of supply chain management for the logistic participants. Today, many companies would like to outsource their logistic operations to logistic companies. However, the very critical point is that, these logistic centers should have the necessary information technology infrastructure and secure applications on the web. Otherwise, they can not guarantee the reliable operational platform and all the competitors in the virtual world can cause threats for the fair competition, prestige continuality of the firms.

Throughout the 20th century, evolutions of manufacturing, marketing and finance changed the business life but after 80's information technology driven trends defined completely new directions for all the business operations which are called web-services applications or e-business. Specifically the Internet has changed the business landscape, the information technology (IT) and communication infrastructure improved the global trade.

Therefore many contemporary companies are investing in information technology (IT) infrastructure and enterprise applications. The managers know that these technology investments and their applications can translate into productivity. The migration of logistic operations to the web based services and the necessity of real time integration for all participants for supply chain management are unavoidable.

Web services represent a major emerging trend whose potential for becoming an important factor of change derives from the fact that it lies at the junction of several developments, some of which are changing business organization and interaction and others which could give a new direction to the future of computing. Web services can have a powerful impact on the efficiency of processes such as inventory control and routine purchasing. They can also be extremely useful for the integration of heterogeneous IT systems. To materialize this potential, the interoperability of Web services developed on competing platforms is essential.

In this paper web-based logistic operations will be explained in detail. Security risks and related requirements will be covered and discussed.

The Motivation and Components of Web-Based Logistic Operations

The business driven trends such as reducing cost, similarities between the products, and other competitive factors, forced the companies to seriously consider reengineering, to evaluate outsourcing for non-core business functions and to work collaboratively with supply chain members. All these changed the nature of business to move from internal planning to the control of synchronized collaborative relationships with supply chain participants.

The major objective is to speed up all the processes that start from customer order to payment, from inbound logistics to shipment. As a result the greatest improvements in logistics productivity are achieved. Online information concerning production schedules and capacities at multiple online supplies and customer lead time requirements enable companies to make and keep an online promise to deliver their products and assemble them en route.

This IT based logistic system has included five important subsections as presented in the following headings (Frazelle, 2002).

- The Management Systems

  These are managed customer response, inventory, transportation, supplied chain activities and warehouse systems. These systems can be called Logistic Execution System (LES).

- The Planning Systems

  Planning is another important operation for the logistic and it is called as Logistic Planning System (LPS). It includes planning components for the customer response, inventory, supply chain, transportation and warehouse operations and integration.

  Collaborative planning is a popular phrase in logistics that refer to two or more corporations communicating and developing logistic plans together.

- The Logistic Data Warehouse

Real time data sharing and a suitable infrastructure is a necessity for the collaborative planning and management. In other words, a real or virtual logistic data warehouse service is recommended. The execution systems should feed data to the logistic data warehouse and logistic planning system should take data from the logistic data warehouse. Eventually, the execution and planning modules will be linked, permitting automatic and real time changes in planning and management systems.

- The Decision Support and Risk Management Systems

  The logistic systems include the inherent inter dependencies, multiple constraints, thousands of item numbers, complex and non-linear objective functions. Therefore, the logistic decision support system is another important component to prevent any operational risks.

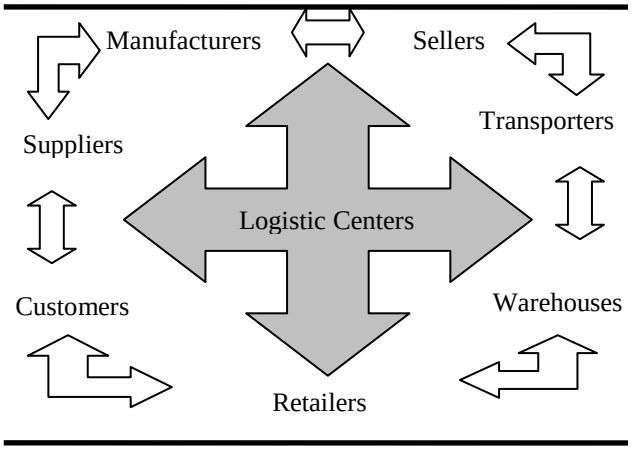
  Logistic center should be following all supply chain operations in real time and detect any operational problem or risks. This module presents a NP-Hard problem due to its nature (Frazelle, 2002). It means that no such algorithm exists that can solve this problem in less than infinite time using a fast computer. Therefore, each customer and its relations with participants in logistic supplied chain should be evaluated by the logistic center as a specific case and, the best solution for these logistic problems can be found by computer-based tools. But the most important part of this solution is to feed the logistic data warehouse by the online information in real time. Thus, the system should use the Internet as a powerful tool.

- The Cooperative Logistic Management with Web Services

  The Internet connects stationary and mobile equipments such as cellular phones, PDAs, notebooks and wireless devices. It provides an infrastructure to follow the real time logistic transactions at anytime from anywhere. Hence, the nature of e-commerce increases the control and orchestration capability of logistic centers or companies.

The real time integration of all participants of logistic operation can be established by the selection of suitable IT applications and web-services. The Figure 1 represents the information flow on the web for a supply chain structure. Logistic centers play a significant role for orchestration of the activities between all the participants of the supply chain such as manufacturers, sellers, transporters, suppliers, retailers and customers.

Figure 1. Information flow of supply chain with web services.



The real-time integration needs data, process and application level integration. Exchanging information is not enough. Business rules, processes, and sequences need to be shared as well (Linthicum, 2001).

Business to business (B2B) data integration is the earliest and well-known level of integration and involves structured data. Data generally found in different databases across the organization and traditionally moved between systems in batch mode. However, this type of integration already changed in the last few years. Today's real-time access capability between multiple and heterogeneous operational data stores provide much more attractive solutions for B2B. All steps of data source accessing such as indexing, caching, query, views, and transforming need the information security aspects (Bernstein and Ruh, 2005). These aspects are generally related to the data warehousing, and database system security concerns. The security aspects in data integration are obtained by accessing to the data source by specific authentication, authorization and access rules.

The purpose of process integration is increasing business efficiency and agility. Process-level integration provides B2B integration an abstract business-oriented layer. The best suited process solutions include Business Process Management, Business Process Integration, Business Process Automation, Workflows Automation, Activity Monitoring and Web Service Orchestration (Linthicum, 2001, Bernstein and Ruh, 2005). The process level integration needs tightly coupled systems. This is restricted to business varieties but this is a good point of providing a secure system. The platform should include role-based authorization including access right.

Application integration enables two or more applications to communicate together to perform a business function. Application integration is well suited to web-services and also mobile devices. The necessary architecture includes messaging and connectivity, data transformation, message brokers, application interfaces, portals and platforms. It needs the firewall, including suppliers, partners and, customers. The integration has many challenges due to mobility concept as well. Any mobile device can try to connect with a malicious application to another application or database system. The mobile environment is inherently insecure and unreliable.

Hence, the identification of mobile application owner become more and more important with variety of these interfaces A secure application integration with web-services and also mobility is provided by encryption, authentication through digital certificates, information protection, identity management and non-repudiation services (Bernstein and Ruh, 2005).

The Security Risks and Requirements

Despite the many positive items of supply chain integration the most common disadvantage is not to have enough face-to-face contact between the virtual trading participants. All these participants can be defined with their requirements, roles and responsibilities and followed virtually in this web environment. This subject could trigger major security problems. Even though, security risks are real handicap of business itself.

For instance, the CommerceNet's study presents the top ten handicaps for e-commerce and web based applications. This study includes many security risks as a major problem in the following sequence (CommerceNet, 2000);

#1 Security and Encryption

#2 Trust and Risk

#6 User Authentications and Lack of Public Key Infrastructure

#8 Fraud and Risk of Loss

Tilburg University research explains how security of payment is the most important purchase criterion for online purchases (Tilburg University, 2001). Also, the European E-Business Report 2004 identified and summarized the security concerns as a major problem (European Commission, 2004). This report includes a problem list as cultural problems, negative market trends, limited degree of computerization and diversity of information systems and IT skills gap (European Commission, 2004).

Today's information architectures are more complex than in the past. Organizations have to communicate with their virtual customers, suppliers and stakeholders and each of them has several kind of IT infrastructures such as mainframes, databases, back-office applications, personal computers, networks and the Internet. Therefore, all integrations of suppliers will be done in a heterogeneous platform.

Security is the most significant feature for the integration, cooperative planning and management concepts, which is called e-trust. E-trusting includes electronically controlled, and well defined, concepts in the Internet age. Believing to someone without having any proof is too dangerous. We will never ever know who is trustworthy or not, when taking an order, giving a price, sending a product or planning an activity. All these threats are improving the importance of reliable relations and also increasing the quantity of secure operations in all levels of web-based relationships between organizations and suppliers.

As a result, all the participants of logistic operations should have to send their orders or any other detailed information about their operations via the Internet in an unsecured environment. Therefore, they face all the Internet security and heterogeneous IT infrastructure problems.

The general information security concepts are listed and shortly defined in the following sections.

- Data Authentication

Data origin authentication focuses on determining the details about the origin of the sending data, such as the originator and the time of creation. For instance, the productivity level of a manufacturer is determined by the received orders. Therefore, the manufacturer should know the originator of the order message or the transaction on the web. The security solution of the system should guarantee the correctness of the originator of the order to the manufacturer.

- Authorization

Once we have authenticated the user and the user has valid credentials, it is time to check authorization. Authorization is a process in which the security infrastructure checks whether the authenticated user has sufficient rights to access the requested resource. If the user has sufficient rights to access a resource, for example, the user has "write rights" on a file, then the operation succeeds; otherwise the operation fails.

This is very important for all the real time transactions on the logistic data warehouse. Each virtual participant can execute only their authorized transactions. For instance, any virtual seller can not execute any transaction to control the transportation.

- Confidentiality

Only related parties should read and process the information. Therefore, confidentiality should be established. All orders and transactions should be transformed to a readable and an executable form between the authorized participants by the cryptographic tools of the logistic system. For instance, the secrecy is very important for competition in global markets. Any virtual trade should not learn the commercial operations of the others.

- Data Integrity

Transmission errors might occur or the information sent might be intercepted and modified before it reaches the intended recipient. This problem must be detected before the process of receiving information by the recipients. Cryptographic tools of the logistic system can establish this service. For instance, the interception and modification of a payment order can be a danger.

- Impersonation and Non-Repudiation

Impersonation is a process in which a user accesses resources by using the identity of another user.

Non-repudiation is particularly important in electronic commerce applications, where it is important that a consumer cannot deny the authorization of a purchase.

The impersonation and non-repudiation looks like a different security concern, but both of them can be solved by strong identification solutions.

- Identification

Identification is used to specify entity authentication, which is concerned with providing the identity of the parties involved in a communication. In order to do this, the security infrastructure collects the user's credentials, usually in the form of user ID and password or some biometric equipments, checks those credentials against any store's credential. If the credentials provided by the user are valid, then the user is considered as an authenticated user.

- Digital Signatures

One of the most important features of a paper and ink letter is the signature. When a document is signed, an individual's identity is tied to the message. The assumption is that it is difficult for another person to forge the signature onto another document. Electronic messages, however, are very easy to copy. How do we prevent an adversary from cutting the signature off from a document and attaching it to another electronic document? The digital signature applications guarantee that. For instance, VeriSign offers "VeriSign Intelligent Supply Chain Services" platform to retail supply chain participants, and builds upon the secure, scalable infrastructure. It has been announced on October 25, 2005(VeriSign, 2005).

The public key infrastructure (PKI) establishes the necessary secure environment for the online transactions of web-based applications. It relies on public key technology in which the hash (or message digest) of a message is cryptographically signed. Because of the nature of public key signatures, anyone with the signer's digital certificate (or public key) can validate that the signer indeed signed the message, providing legal proof that the signer cannot refute. The Certification Authority as a trusted third party can look at the message and validate that the message was indeed digitally signed by the sender.

PKI technology has been approved and legalized in the USA in 2001. Department of Commerce, Federal Commission and the National Security Council monitor global encryption technology closely. Both the US Congress and the European Union have supported PKI development and legalized digital signatures that validate an online transaction. Restrictions continue for some countries such as Iran, Iraq, Libya and Sudan (Weiner, 2002).

As a result of using the PKI and digital signatures, the count of virtual participations can be increased in logistic chain with mobile equipments and their applications, and new trade partners.

Table 1 summarizes the relation between the security concepts and web-based integration levels.

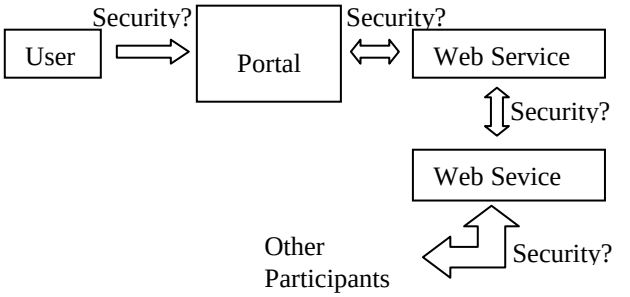
Table 1. Security concepts and the integration relationships.

Security concepts	Integration Levels		
	Data	Process	Application
Data Authentication	X	X	X
Authorization	X	X	X
Confidentiality	X	X	X
Data Integrity	X	X	X
Impersonation Non-Repudiation		X	X
Identification		X	X
Digital Signatures		X	X

The Solution with the Web Services

Satisfying all of the above security concerns for every step of web-based applications is very important. In Figure 2, a simple web transaction of an instance transaction is given. How the user is identified and authenticated for a web transaction by the portal and web services? If single sign on (SSO) is not available, the user or application has to provide password four times in this scenario. Also between the points in the figure, do the back-end applications have to authenticate, validate integrity or encrypt data to each other to maintain confidentiality? (Daconta, Obrst, Smith, 2003)

Figure 2. Security for every point of web services.



Fortunately, technologies for web services security have been evolving over the past few years. Some of these technologies are encouraged with digital signature, encryption and web services security (WS Security).

The WS-Security was released by Microsoft, IBM and VeriSign in April 2002. It provides the integrity, confidentiality and message authentication between web services. It combines encryption and digital signature with XML technologies.

XML Encryption is a recommended technology by the World Wide Web Consortium (W3C). It handles confidentiality. In an XML file, while the different parts of the document can be encrypted; other parts can be transferred as plaintext. This can be helpful for web services to establish different security levels.

XML Signature is another recommended technology by the W3C to provide message integrity and non-repudiation. Any part of XML document can be digitally signed by the XML Signature. It plays an important role in web services. For example in Figure 2, the user could sign part of the message that is initially sent to the portal and that initially needs to be read by the last Web service. When that part of the message is received by the final web service, it can validate that the user indeed sent the message (Daconta, Obrst, Smith, 2003).

Conclusion

The development of information technologies and the Internet have very critical roles in the grown trade. The real time integration, cooperative planning, faster transactions, decreasing costs, increasing productivity, effective competition, and the satisfaction of customers can be established for the supply chain management by the web services, the Internet and a selection of suitable Enterprise Resource Planning (ERP) software applications. All the trade partners and logistic center companies should select the suitable ERP package, which satisfies all the necessary security concerns for applications, processes and data layers.

Each of the supply chain members add value and create sustainable competitive advantages in the channel by the secure and private web services. However, the secure trading environment improves the volume of the trade.

References

Frazelle , 2002, Supply Chain Strategy, Mc Graw Hill, ISBN 0-07-137599-6

Linthicum, 2001, B2B Application Integration, Addison-Wesley, ISBN: 0-201-70936-8.

Bernstein, Ruh, 2005, Enterprise Integration, Addison-Wesley, ISBN 0-321-22390-X.

CommerceNet, 2000, CommerceNet Barriers to Electronic Commerce 2000 Study, www.commerce.net., http://osiris.sund.ac.uk/~cs0pco/iec/CommerceNet2000SurveyBarrierstoEC.doc

Tilburg University, 2001, Building Consumer Value Through The Internet , Tilburg, The Netherlands. Steenkamp, J.E.B.M. & Geyskens, I. (2001). Building Consumer Value through the Internet. Brussels,

http://www.aim.be/docs/AIMforumfinal.pdf

European Commission, 2004, The European E-Business Report 2004,

http://www.ebusiness-watch.org/resources/documents/eBusiness-Report-2004.pdf

Weiner, 2002, Public Key Infrastructure (PKI) Market Trends, Faulkner Information Services

VeriSign, http://www.verisign.com/information-services/supply-chain-services/supply-chain-information/retail.html

World Wide Web Consortium (W3C), http://www.w3.org/

Daconta, Obrst, Smith, 2003, The Semantic Web