A Secure E-Commerce Platform to Enable the Worldwide use of Standards

Ilidio G. Chaves
Ichaves@ipn.pt
+351 239 700983
Pedro Nunes Institute
CISUC - Centro de Informática e Sistemas da Universidade de Coimbra
Rua Pedro Nunes, Quinta da Nora 3030 Coimbra, Portugal

Henrique S. Martins
smartins@mail.ipq.pt
Portuguese Institute for Quality
+351 21 294 8116
Rua António Gião, 2
2829-513 Caparica, Portugal

Fernando Boavida, Edmundo Monteiro
{boavida, edmundo}@dei.uc.pt
CISUC - Centro de Informática e Sistemas da Universidade de Coimbra
Departamento de Engenharia Informática
Polo II, Pinhal de Marrocos, 3030 Coimbra, Portugal

Abstract

The nature of the standardization world has always imposed a demand on technology development to accommodate needs in terms of process automation and digital manipulation of documents. With the rapid growth of the Internet, on-line access to important information on standardization activities, including access to electronic catalogues has proven essential to promote Standardization Bodies and to ease the process of information access and enlarge the scope in terms of end-users. Now, the development of E-Commerce technology creates suitable conditions to move one step ahead, where automatic selling and delivery of standards in electronic format may be done in a safe and efficient way. This paper presents a new architecture that is aimed to fulfil the requirements of the standardization world.

I. Introduction

Nowadays the world is progressing towards the globalization of economy, supported by free-market rules that follow the policy established by the WTO (“World Trade Organization”).

To facilitate world trade and remove technical barriers, international standards are used as reference documents, adopted by all concerned parties, namely, manufacturers, commercial partners, consumers, authorities, etc. These organizations agree on specifications and criteria that should be applied consistently in the process of choosing and classifying materials, product manufacture and the provision of services.

Standards also play a critical role at other levels such as health, safety and environment protection. These are very important for everyone, either in any country, region, or in the world.

Under this context, a standard must be a document established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines and characteristics for procedures or their results.

Consequently, the availability and access of standards is the main goal of standardization bodies that are responsible for the preparation of these documents, in order to assure that all private and governmental entities, and general public use the standards that they need.

Nowadays, getting a standard from any standardization body located far away may prove to be very difficult. Many times, customers waste an unnecessary amount of time with postal services that transport paper copies of purchased standards. This cost is increased when payments are not processed electronically, leading to inefficient methods, where, for instance, cheque payments have to be cleared between countries.

Taking into account these limitations and considering the ultimate goal of customer satisfaction, standardizers should prepare new and efficient processes where standards are immediately available to customers after electronic search and purchase. Nowadays, standardization bodies are becoming aware of these needs and are investing resources in order to implement new mechanisms that enable the worldwide use of standards. This it is the case of IPQ (*Instituto Português da Qualidade*), the national standardization body of Portugal, who has decided to implement a fully automatic electronic standards delivery service. The system has been developed by the E-Commerce research team of the *Pedro Nunes Institute* and the *University of Coimbra*, and includes:

- Electronic catalogue
- Electronic order
- Electronic invoicing
- Electronic payment
- Electronic delivery

With this platform, IPQ intends to establish a friendly and safe environment, accessible through the Internet, with the main goal of satisfying the needs of customers in terms of efficient electronic transactions and fully secure payment and delivery procedures.

Some of these principles have been applied in the INES (*Internet Network for European Standardization*) project [1], supported by the European Commission, which has the main goal of allowing CEN and its national members to provide a more visible, friendly, open and productive European standardization service.

This paper continues with the description of the components of the proposed E-Commerce platform and in which ways they cater for the particular needs of the standardization world. Section III describes implementation considerations in the IPQ environment. Finally, conclusions and future work are discussed.

II. System components

Figure 1 illustrates the general architecture of the proposed E-Commerce platform. It is represented as a layered architecture with the external entities interacting with the system through specific interfaces.

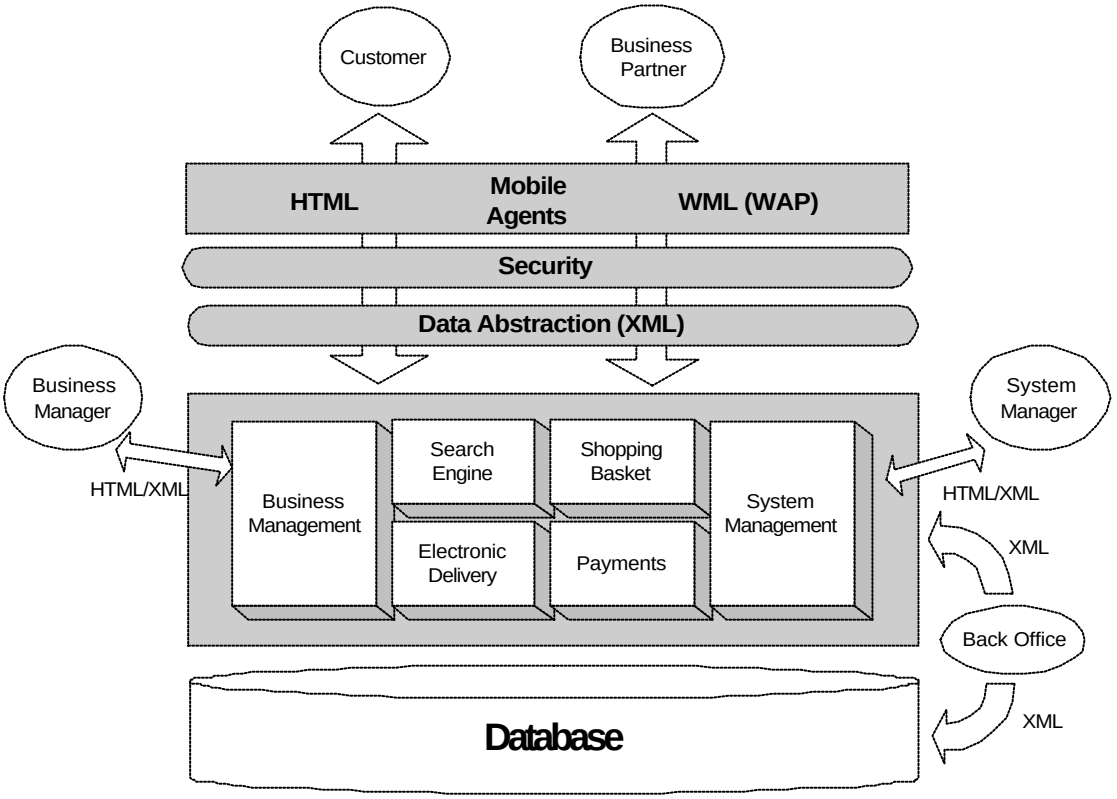

Fig. 1 – Components of the proposed E-Commerce System

A. External Entities

The main external entities that interact with the system are:

- *Customers* – for Business-to-Client transactions
- *Business Partners* – for Business-to-Business transactions.
- *Business Managers*
- *System Managers*

While Customers use the site to purchase products, Business Partners (i.e. other standardization institutions) interact with the system for automation of inter-institutional transactions, for example the clearing-house mechanism used in INES to fulfill orders that include standards that are fetched from remote document servers. These entities interact with the system using different types of communication channels and always pass through a security layer before reaching any of the application modules.

Managers access the system in a protected Intranet environment and interact directly with the Management Modules that take care of their needs (including security). While the *Business Manager* transacts with business-related information (i.e. reports, data mining, order management, catalog management, etc.), the *System Manager* guarantees the correct operation of the system (i.e. user management, log file verification, intrusion detection, scalability etc).

B. Communication channels

The standard way to access the system is via **HTML**, using a Web Browser. In modern client-server applications, this kind of approach has proven very advantageous due mainly to the following aspects:

- There is no need to install client applications
- Users are becoming very familiarized with Web Browsers
- It is possible to access the system from virtually anywhere on the Internet

This system is using *Microsoft Internet Information Server* (IIS) as the Web Server with *Active Server Page (ASP)* technology to program the functionalities. The reason for the choice to use ASPs is mainly due to performance since the ASP technology, developed by Microsoft, is clearly optimized for IIS. Nevertheless, the next version of the platform will be programmed using *Java Server Pages* to guarantee portability.

The main goal will be to keep two versions: one optimised for IIS and another applicable on any other web server.

Using **Mobile Agents** is another possible way to interact with the system, although still at an experimental phase. This is an emergent technology in E-Commerce that will be widely used in the near future as a common form to conduct commercial transactions. By having support for Mobile Agent interaction the system will be open to a vaster universe of end users and marketplaces. More information on this technology and its potentialities as an E-Commerce enabler can be found in [2] and [3]. The server-side mobile agent interaction module is being developed by the MATE (*Mobile Agent Technology for Ecommerce*) project at the Pedro Nunes Institute [4].

Recent developments in wireless technology have lead to the definition of **WAP** (*Wireless Access Protocol*), which has introduced the possibility of mobile E-commerce. By programming pages and functionalities in *WML (Wireless Markup Language)*, the system interacts with mobile phones and is open to commercial transactions with mobile users. One of the layers of the WAP stack, known as WTLS (*Wireless Transport Layer Security*), provides encryption and authentication for server-to-client security. This prevents fraudulent access to WAP transactions, thus taking care of security needs. Detailed technical information on these concepts and latest developments can be found in [5].

C. Security

This is a key factor to build up the customer's confidence during his interaction with the system. It is important for the user to know that his personal information is confidential and that important transactional data is kept private. It is also fundamental to protect the system against external violations.

In the system, security is viewed as a layer between the customer and the application layer and covers four important requirements:

- *Authentication* – that guarantees the identities of parties involved in a transaction
- *Privacy* – that guarantees that the data is safely transmitted and not intercepted
- *Integrity* – that guarantees that the information is not changed during transmission
- *Non-repudiation* – to avoid denial of transactions

To fulfil these requirements all users are authenticated, using a username/password mechanism, at the beginning of each commercial transaction. Confidential information is then encrypted using SSL (*Secure Sockets Layer*) [6]. For this, 128-bit encryption is achieved, using a certificate issued by Verisign [7]. Apart from providing strong encryption, using a certificate at the server side also builds trust on the end-user, who may be assured that he is dealing with a legitimate source by reading the details of the certificate.

D. Data Abstraction Layer

Although the system supports several communication channels, the internal applications interface with external modules and entities using **XML** [8]. In this way it is possible to develop all modules using a uniform communication interface, that is becoming the main standard in the E-Commerce domain. The Data Abstraction Layer will perform all of the necessary translations from and to XML to communicate with the external entities of the system.

E. Management modules

The Application Layer contains two Management modules, available for restricted access, to business and system managers. These are trusted users that access the system to perform administration tasks, such as:

Business Manager	System Manager
Order Management	User Management
Customer Care	System Scalability
Catalogue Management	Log Verification
Data Mining	Intrusion Detection
Reporting	Performance Monitoring
Mailing	Backups

Table 1 – Management Tasks

The system has specialized modules that handle all of these tasks, through a private web server, with restricted access.

F. Search Engine

Continuing with the description of the *Application Layer*, the search engine is the module that is focused on finding information in an efficient way. Since it is the main tool to find items in the catalogue, it should not only be fast, but also intelligent in the way it presents results to the user. The results of each query can be ordered using weighed criteria of the following aspects:

- String matching of words
- The user's profile
- What other users have bought using similar search criteria

While the first case reflects traditional searching mechanisms (and is generally the factor with most weight), the last two involve intelligent processing of user profiles and shopping transactions with the system.

Proving *search refinement* capabilities is also another important aspect that helps the user to find exactly what he needs. In this case a clear identification of the relevant

fields that define a product is very important. In the case of standards, the fields used for search refinement could be:

- Standard type (i.e. ISO, EN, IPQ,…)
- Reference
- Number
- Title
- Abstract
- Technical committee
- Year

Combination of all of the search refinement fields can be done using an AND or an OR operator.

G. Shopping Basket

This is the module that guides the user interactively through his shopping session with the system. The functionality simulates a typical 'real-world' environment where a customer browses through the shelves and displays of a store and adds his desired items to the basket. In the end, the customer checks out by paying the amount at the counter and leaving the store. The main goal of a system of this nature is not only to simulate this scenario, but also to make the whole process easier and more attractive, saving the customer the burden of traveling to the store and performing 'physical' transactions, which may be time-consuming, specially when products are goods that have no need for prior real-time evaluation (like clothing or food). In this way, the system provides value-added features, such as:

- Multiple payment methods
- Automatic currency translation

- Multiple delivery methods
- Order tracking

All of the transactions are stored in the database, which enables the user to come back afterwards and finish a commercial transaction, which has been left open. This is a good way to avoid using cookies, which is a common way of implementing this functionality on many well-known commercial products. The choice of not using cookies is due to the security risks they entail, such as, anybody being able to perform transactions with the users' browser, under his name.

H. Payments

The system offers flexibility in choosing several payment methods, although only payment by credit card enables the user to receive the products in electronic format immediately, because, in this case, credit can be verified *on-the-fly*. If, however, the user is registered as a subscriber (or 'correspondent' in the Portuguese Institute for Quality context), he will also be able to access documents immediately. This depends on his profile, which grants him access to specific types of subscribed information, according to his subscription contract.

Looking first at the traditional methods, implementing standard payment mechanisms is trivial: the system registers the payment method in each transaction and sends this information to the sales department. After payment has been taken care of the Business Administrators may pass the order to the Delivery Module, which will then prepare the package for electronic retrieval at the site.

Implementing VISA payment is, however, much more complex, not only because of the extra security involved, but also because of the automatic verification of the credit cards. The technology used for implementing this functionality is based on the SET (*Secure Electronic Transactions*) [9] protocol. Two variations are considered:

- SET – with full certificates

- MOSET (Merchant-Originated SET)

In both cases, the Merchant Server (which is the E-Commerce server installed at the standardization institution) has a SET certificate that is a key component to enable all of the security requirements in transactions with the bank's (or acquirer's) payment gateway (which is connected to VISANET). This involves *authentication*, *encryption*, *integrity* and *non-repudiation*. A full-SET environment is obtained by using a certificate also at the Customer side. The certificate is used as a digital wallet, plugged into the browser to validate the cardholder. In this scenario, a credit card number is validated only if the certificate is used in the transaction. Figure 2 describes this case.

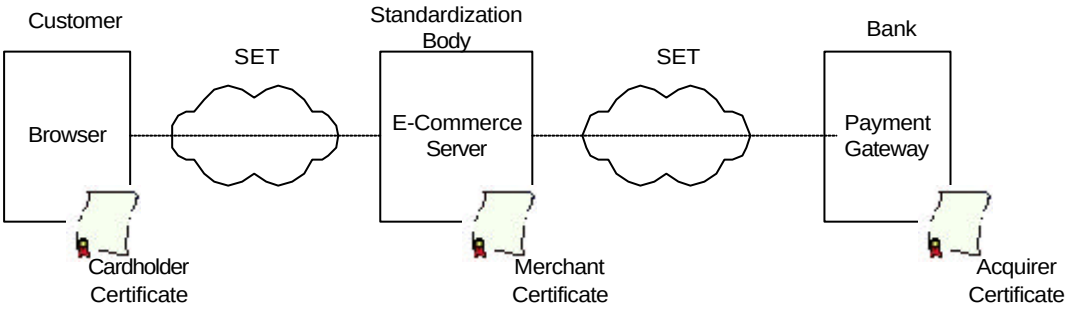

Fig. 2 - Full-set transaction

The problem with a full-SET environment arises from the fact that in many countries there is still lack of conditions to have certification authorities for customer certificates. With the maturity of SET-based technology, banks and card issuers will provide this service to cardholders, who will then have the credit card and a binary file (in a diskette for example) that will permit them to conduct secure transactions on the Internet.

Although the system is prepared for full-SET transactions, at the moment it also accepts MOSET transactions, which uses SSL encryption and a username/password mechanism to validate users. In this case, the SET environment starts at the Merchant Server, which takes advantage of a fully automatic and secure environment

in the process of communicating with the credit card network (i.e. VISANET). Figure 3 illustrates this scenario.

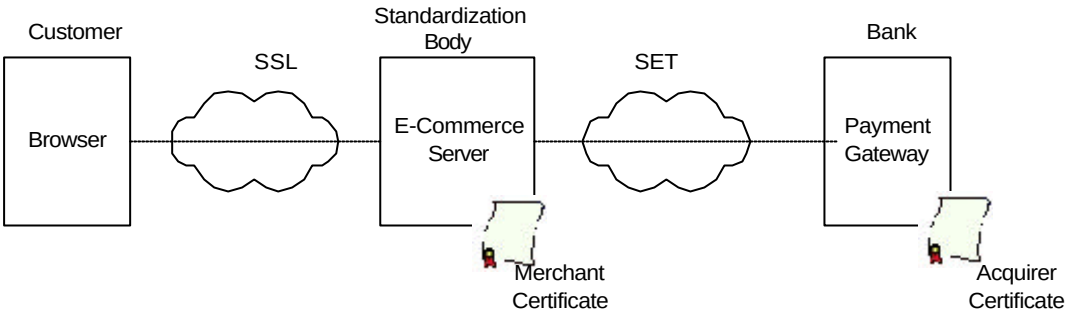

Fig. 3 - Merchant-Originated SET transaction

In this case, the bank (or acquirer) that owns the payment gateway handles the issuing of the certificate for the merchant server.

I. Electronic Delivery

Considering that standards exist in digital format, the delivery module of the system supports full automation of the whole commercial process, where the purchased product is delivered to the customer just seconds after he completed the payment. This is in fact one of the most important success factors in a system of this nature.

All registered users have a personalized restricted area that they can access, by previous authentication, using a protected SSL interface. In this area, they can perform personalization tasks, such as editing their profiles and also view the whole history of orders that have been already fulfilled and that are still awaiting completion. In this last case, they can access the purchased documents and retrieve them using three possible protocols:

- *HTTP* – which is very good for overcoming problems with firewalls, since this is always the public port, but may suffer from slow connections.
- *Email* – which is also a good method for overcoming problems with firewalls, although problems may arise with long files, with some mail relays blocking the transport of such emails due to pre-established thresholds.

- *FTP* - It is considerably faster than HTTP but may suffer from blockage due to firewalls.

For every order, the system creates the package in a dynamic directory, only accessible to the customer by appropriate previous authentication. To perform these tasks there is a need of:

- A *Document Server*, to hold all documents that may be sold.
- A *Pointer*, in each catalogue entry, to each document. This may be a directory path or an address on a remote server, which enables a distributed environment such as the one used in the INES project.
- A *Watermarking [10] Module*, to mark every document with customer information to avoid illegal distribution. At the end it will save it in a non-revisable format (i.e. pdf).
- A *Messaging Module,* to inform the customer that the package is ready for retrieval.

The diagram in Figure 4, depicts the sequence used in the procedure of preparing a package for delivery to a customer that has already passed successfully the payment phase.

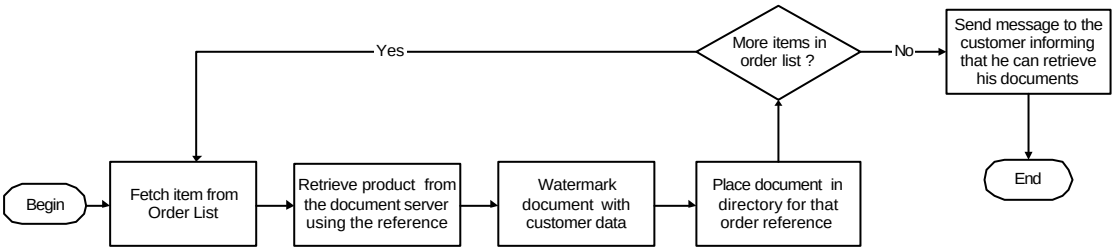

Fig. 4 – Preparing a package for electronic delivery

Every file that is retrieved by each customer is registered in the system that knows the status of every order, which may be *pending*, *partially completed* or *fully completed*. In this last case, the system leaves the area active for an amount of time (that is a configurable parameter), during which the customer may still retrieve the

products. After this period, the directory is deleted to optimise the space of the document server, although all transactions stay registered in the database.

J. Integration with the backoffice

In most cases, the E-Commerce system is integrated with the information system of the institution and must interact with it in a safe and efficient way. This is the best way to attain an efficient and pro-active environment. In standardization institutions, the most probable systems that are part of the backoffice and may need to integrate with the E-Commerce platform are:

- *The Standards Database*, where all information on standards and other documents that result from standardization activities are stored.
- *The Document Server*, where documents are stored in digital format as a result of the electronic production of standards and related documents.
- *The Financial System*, where all sales are registered, including businesses that are conducted outside the Internet environment.
- *The Customer Database*, where, for example, correspondents and subscribers are initially registered. These customers will then benefit from the added value of receiving information and subscriptions automatically via the E-Commerce platform.

In all cases, XML is used as the communication language between all sub-systems, since it is a uniform and effective way to exchange information and documents. Regarding to databases, replication of information in the E-Commerce platform database should be considered, opposed to direct access to the backoffice databases. The first case benefits from extra security although it has the drawback of duplication of data and the necessity to synchronise both databases. On the other hand, having a direct connection between the E-Commerce platform and the backoffice databases represent some level of risk, although using read-only views of

crucial information for interaction with the outside world and write permissions only in the administrator modules may solve this problem.

III. Implementing the system at IPQ

The implementation of the system in the IPQ environment followed a structured and modular way, where each component was inserted and fully tested before applying the next one. First of all, a study of the whole backoffice was conducted and the interfaces were clearly identified. Next, structured XML formats where used to enable data retrieval from the information that feeds the E-Commerce database (i.e. the catalogue).

Regarding to secure payments, IPQ has integrated the piloting phase of the implementation of the SET protocol in Portugal, which is lead by the national inter-banking institution that offers connection to VISANET. This has imposed a limitation on the software used to connect with the payment gateway (which has to be the one selected by the acquirer), but using simply the API, opened the possibility to include the module as a library, thus facilitating the ability to develop a proprietary commercial environment.

Integration with the financial system is achieved through communication with the sales database via data views, which enables the automatic registration of web-based transactions.

With the launch of the first version of the system, customers rapidly substituted the traditional method of browsing through the paper catalogue and performing manual purchases at location or via surface mail, with the new on-line process. At this moment, it is the main way to purchase standards and to keep informed of new additions to the catalogue.

IV. Conclusions

This paper presented an E-Commerce platform that caters for the imminent needs of the standardization world, where secure electronic distribution of documents in a cost-effective and efficient way are a priority.

The system is being integrated in the IPQ environment as a structured and modular process, where every module can be developed independently and integrated to provide value-added features, according to current technological and economical demands.

However, to take full advantage of the full E-Commerce environment in a standardization body requires several assumptions that should be considered when evolving to this reality.

First of all, it is fundamental to have all documents in digital format and stored in a structured way. Unfortunately this is not the reality at many institutions where most of the documents are still in paper format only. This disables the *electronic delivery*, which is a valuable feature that stimulates the worldwide use of standards through facilitation of access.

Another key factor is related to security policies and building up confidence in the customer by showing him that interacting with the system is at least as safe as the traditional way of conducting business.

Regarding to payment by credit cards, the policies and technology used by the national acquirers and banks vary in each country. While some are open and developed enough to implement the SET environment, others are still behind, thus creating difficulties in performing automatic payments. Even in the poorest scenario, where this isn't possible at all, the E-Commerce system may still be used, with deferred payment mechanisms or with subscribers. In the first case, users would

have to wait longer to fetch the documents (until payment clears), while, in the latter case, retrieval can be immediate if the purchased documents are covered by the subscription contract.

Finally, it is up to the standardization bodies to promote the usage of this technology as the most important means of conducting business and dealing with customers. Using automatic mechanisms of keeping in touch with the customers and providing them with updated information that is in their field of interest creates fidelity and a dynamic relationship. This can all be done without the need of human intervention. By using intelligent data mining techniques the system automatically relates to the customer and keeps him informed.

In fact, this is the last stage of the whole automated process that begins with the creation of a standard and ends with its delivery to the End User.

Future tasks include the development of the core modules of the system as a result of technical developments and tests. Accessing the system in a mobile environment still only permits limited interactions, like catalogue browsing and ordering, however, a secure environment for paying and retrieving information is being set up. The mobile agent interaction module is also being developed to fulfil complete commercial transactions, but success in this particular domain also depends on the development of client applications and motivation policies that will convince users of the benefits of this new promising way of conducting transactions. Finally, the migration to a full SET environment is also a priority, which depends mostly on the definition of strict bank policies for the creation and management of digital certificates, that should be associated to every issued credit card.

V. References

[1] S. Downe, I. Chaves - “Progress Towards Web-Based Electronic Committees in the CEN/INES project (Internet Network for European Standardization)”, SIIT’99 Proceedings, pp. 231-235, Aachen, September 15-17, 1999

[2] P. Maes, R. Guttman and A. Moukas - "Agents that Buy and Sell: Transforming Commerce as we Know It.", Communications of the ACM, March 1999 Issue

[3] K. Villinger, C. Burger – “Generic Mobile Agents for electronic Markets”, http://inforge.unil.ch/isdss97/papers/73.htm

[4] I. Chaves – “MATE – Mobile Agent Technology for Electronic Commerce”, Pedro Nunes Institute, Technical Report, March 2000

[5] Wap Forum – “Wireless Application Protocol”, http://www.wapforum.org

[6] D. Wagner, B. Schneier – “Analysis of the SSL 3.0 Protocol”, The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 1996, pp. 29-40.

[7] Verisign – “Enterprise and Internet Security Solutions”, http://www.verisign.com

[8] XML.org – “The XML Industry Portal”, http://www.xml.org

[9] L. Loeb, pbc Enterprises – “Secure Electronic Transactions: Introduction and Technical Reference”, Artech House, 1998

[10] S. Katzenbeisser, F. Petitcolas – “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, 2000