A Secure e-Ordering Web Service

Despina Polemi, Spyridon Papastergiou
University of Pireaus, Informatics Department,
80 Karaoli & Dimitriou Str, 185 34, Pireaus, Hellas
{dpolemi,paps}@unipi.gr,
http://thalis.cs.unipi.gr/~dpolemi

Abstract. The electronic order (e-Ordering) service as an e-business process allows the true business-to-business secure collaboration by giving the opportunity to salesmen and purchasers to execute trustful processes of electronic trading opening new markets. The W3C working draft “Web Service Architecture (WSA) Requirements” and a set of EU Directives impose several security and privacy requirements that the e-Ordering implementations have to satisfy in order to achieve a secure transaction. This paper presents a set of these requirements and describes an e-ordering system (TOES) that address them based on eXtensible Markup Language (XML), XML Cryptography, Public Key Infrastructure (PKI), Web Services Policy Language (WSPL) and Web Services. The proposed e-Ordering service TOES is open, secure, interoperable, and affordable respecting the EU legislation.

1 Introduction[16]

One of the most important aspects in electronic business is the establishment of trustful, legally accepted cross border transactions via electronic means encouraged by various European Union (EU) Directives. The EU Directive on electronic commerce (2000/31/EC) [13] is fundamental in cross border e-business in the European continent, the Directive on electronic signatures (1999/93/EC) [12], the Privacy and Electronic Communication Regulations (97/66/EC) [9] that clarify the principles that are applied in the e-commerce’s processes in order to achieve a secure and trustful transaction.

The electronic Ordering (e-Ordering) as an important process in the electronic trading has to respect the existing legal framework and to satisfy the security and privacy requirements that are imposed. This is caused by the fact that the orders may contain business data (e.g. VAT code) or private data (e.g. ordered items) that should

[16] The research of the present paper has been supported by the eTen project SELIS (selis.unipi.gr) and by the GSRT(PENED) programmes.

not be revealed or modified. So, they should be trustful documents requiring all four dimensions of security (confidentiality, integrity, authenticity, non repudiation).

The contemporary e-Ordering implementations vary in terms of the underlined technologies. The existed systems can be discriminated in two types: The ERP inclusive systems that manage the sources within and beyond an enterprise. These systems are not affordable for Small and Medium Enterprises (SMEs), blocking them from entering B2B profitable applications (e.g. e-procurement). In addition, although they satisfy several security requirements, they neither achieve interoperability nor take into account privacy issues. The second type, are customized solutions offering e-Ordering as an autonomous service. Existing systems of this type ignore various security and privacy requirements.

The purpose of this paper is the presentation of the security and privacy requirements of e-ordering services driven by the EU legislation and Directives, as well as the proposition of an open, affordable and scalable e-ordering architecture (TOES) that satisfy these requirements. TOES [22] is built using open technologies, such as eXtensible Markup Language (XML), XML Cryptography, Public Key Infrastructure (PKI), Web Services Policy Language (WSPL) and Web Services.

The rest of this paper is organized as follows. Section 2 provides the fundamental security and privacy requirements of e-ordering. Section 3 describes in detail the e-ordering system architecture and its components. Section 4 provides an assessment of TOES. Finally Section 5 provides conclusions and directions for further research.

2 State-of-the art and requirements

In this section we present the security and privacy requirements of the e-Ordering services [18], [22] as implied by the W3C working draft "Web Service Architecture (WSA) Requirements" [5] and by the EU legal framework.

2.1 Security and Privacy Requirements

The e-Ordering systems have to satisfy certain fundamental security requirements:

AR006.2.1: *Authentication of origin*. The confirmation of the source that sends the orders is a critical issue of the ordering exchange process and its identity needs to be proven.

AR006.5: *Integrity of the content*. During transmission or storage time, the orders should be protected from unauthorized (intentionally or accidentally) modification or their replacement.

AR006.6: *Non-repudiation of origin and receipt*. The ordering exchange can not been denied neither from the sender nor from the recipient.

Long lasting integrity. The electronic signatures of the orders should remain valid over long periods.

AR006.4: *Confidentiality and privacy*. The orders should be readable by the designated recipients.

Integrity of the sequence of the orders. The avoidance of missing orders.

AR006.1: *Availability*. The e-ordering service will be able to be used at any time from the enterprises.

Secure Electronic Storage. Primary requirements, such as authenticity, integrity and readability should be guaranteed throughout the storage period of the e-ordering documents [11].

Legal Compliance. All e-ordering implementations have to be compliant to a set of regulations and directives that are defined from the legal framework of EU member states e.g. Digital Signature Law [12], Privacy and Electronic Communication Regulations [9], Electronic Commerce Directive [13], Electronic Storage Directive [11], Protection of Privacy [14], Free movement [10].

Privacy [21] has an important role in the e-Ordering service and is discriminated in two directories. The first one concerns the privacy of the information that is published in an untrusted UDDI. The requirements of this category are the following:

UDDI Privacy. The e-Ordering service can be published to an untrusted Directory where the (existed or future) user can invoke it [15].

Requestor Privacy. The Web Service requestors' query information should be protected [15].

The second direction has as primary scope to facilitate the interaction and strengthen the interoperability of the participants. These requirements are described as follows:

AR0020.1: The WSA must enable the expression of a Web service's privacy policy statements.

AR0020.3: The WSA must give consumer access to a Web service's advertised privacy policy statement.

AR0020.5: The WSA must enable privacy policy delegation and propagation.

AR0020.6: Web services must be allowed to support interactions with anonymous parties.

The above requirements impose restrictions that e-Ordering systems have to consider.

3 TOES: A Secure e-Ordering Service

In this section we will present the standards that are adopted by TOES in order to address the requirements from Section 2.1. Furthermore, we describe the proposed e-Ordering service architecture, the entities that are involved in the service, the procedures and all the necessary steps that these entities have to follow in order to complete an e-Ordering transaction.

3.1 Adopted Standards

The proposed system utilizes XML and Web Services (Simple Object Access Protocol (SOAP) [7], Universal Description, Discovery and Integration Protocol (UDDI) [17], Web Services Description Language (WSDL) [16]) as the basic technologies for the formulation and transfer of messages within the platform. The choice of these technologies is based on the achievement of interoperability and security.

The message format integrated in the system uses the XML Common Business Library version 4.0 (xCBL 4.0) [8], which is a set of XML building blocks and a document framework that allows the creation of robust, reusable, XML documents to facilitate global trading. Furthermore, xCBL has been also adopted as the used schema for the e-Order documents that are stored in a XML database. The use of XML for formatting the e-order document, allows the use of XML digital signatures and the integration of timestamping tokens to the document ("***X***ML ***Ad***vanced ***E***lectronic ***S***ignatures XAdES") [6]. The selection of xCBL is based on its maturity level of completeness and clarity that gives the possibility to a system to be parameterized properly in order to be used in different cases.

The WSDL has as basic objective to represent the functional aspects of the e-Ordering Service. Specifically, it is used to describe the interfaces of a service and how to invoke it. Thus, TOES uses Web Services Policy Language (WSPL) [20] in order to represent all non-functional attributes of the offered Service.

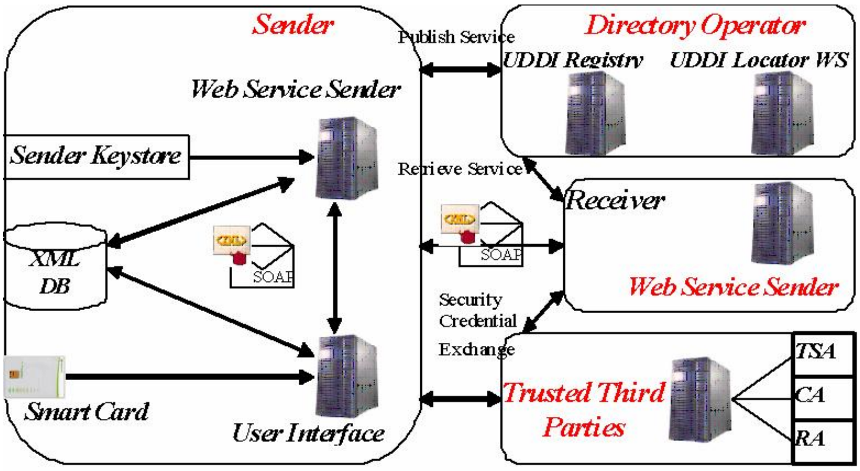

Fig. 5. System Architecture

3.2 Service architecture

Figure 1 depicts the four major entities that take part in the e-Ordering process. The two major entities that participate to the transaction are the Sender that initiates the process and the Receiver that receives the order. A detail description of these entities is the following:

a) *The Trusted Third Parties (TTPs)*: The Trusted Third Parties that are required in the proposed architecture are a Certification Authority (CA) and a Registration

Authority (RA), and a Time Stamping Authority (TSA). The Certification Authority (CA) and the Registration Authority RA offer the PKI services of registration, certification and revocation status information with OCSP [2], while the Time Stamping Authority (TSA) offers standards based time stamping services [4].

b) *The Sender*: The Sender is an organization (e.g.central point of sales, telecomm provider, stores) that hosts TOES architecture. The Sender deploys the e-Ordering service, publishes it in the UDDI Registry and defines a specific privacy policy that corresponds to the used mechanisms of the e-Ordering service. It also communicates with the Trusted Third Parties to get the proper security credentials.

c) *The Receiver*: The Receiver is an organization (e.g. store, private user) that hosts TOES architecture or a similar one. The Receiver retrieves the e-Ordering service from the UDDI, it is configured to understand the messages and defines a specific privacy policy that corresponds to the used mechanisms of the e-Ordering service. It also communicates with the Trusted Third Parties to get the proper security credentials.

d) *Directory Operator*: The Directory Operator Entity is composed of the UDDI Registry, and UDDI Locator WS. The UDDI Registry is an untrusted directory where Web Services can be published, while the UDDI Locator WS makes possible the discovery of the UDDI in which a Web Service has been published.

Furthermore, Figure 1 depicts the three major components i.e. User Interface, Web Service Sender and XML Database of TOES architecture. These components are described in details as follows:

i) User Interface: The User Interface gives the possibility to the user to create, manage and send orders. In order to achieve this, it communicates with six entities: the User card to sign the orders, the CA to request certificate status information [3], the TSA to request time stamps in order to produce XAdES signature [3], the XML database to retrieve order's information, the Web Service Sender in which the orders are sent, the UDDI Registry to publish the e-Ordering Service.

ii) Web Service Sender: The Web Service Sender communicates with five entities: the User Interface that sends the orders to the Web Service Sender, the XML Database to store orders and receipts, the Sender Keystore to receive sender certificate and receiver certificate, the Web Service Receiver, which receives the orders, the UDDI Registry to retrieve the URL of the Web Service Receiver.

iii) Native XML database: The XML database [1] communicates with two entities: the User Interface, which retrieves orders' information and the Web Service Sender, which stores orders and receipts.

3.3 e-Ordering processes

The Sender and the Receiver of the order, before, initiate the e-Ordering process, have to accomplish a set of actions which are divided in three phases.

The first phase includes the definition of the Privacy Policy of the Sender and the Receiver. The second phase constitutes the communication with the UDDI Registry for the publication and retrieval of the e-Ordering service. In the second phase the Sender and the Receiver have to communicate with the Trusted Third Parties for acquisition of the security credentials.

Phase1-Privacy Policy: The Sender and the Receiver have to define the necessary Privacy Policies using the Web Services Policy Language (WSPL). Each of the Privacy Policy documents is signed using the qualified certificate of the corresponded party. The major objective of the defined Privacy Policy [19] is to convey conditions on an e-Ordering interaction between two Web service endpoints. All information provided in the Privacy Policy is aimed to describe the capabilities and requirements of the Web Service entities.

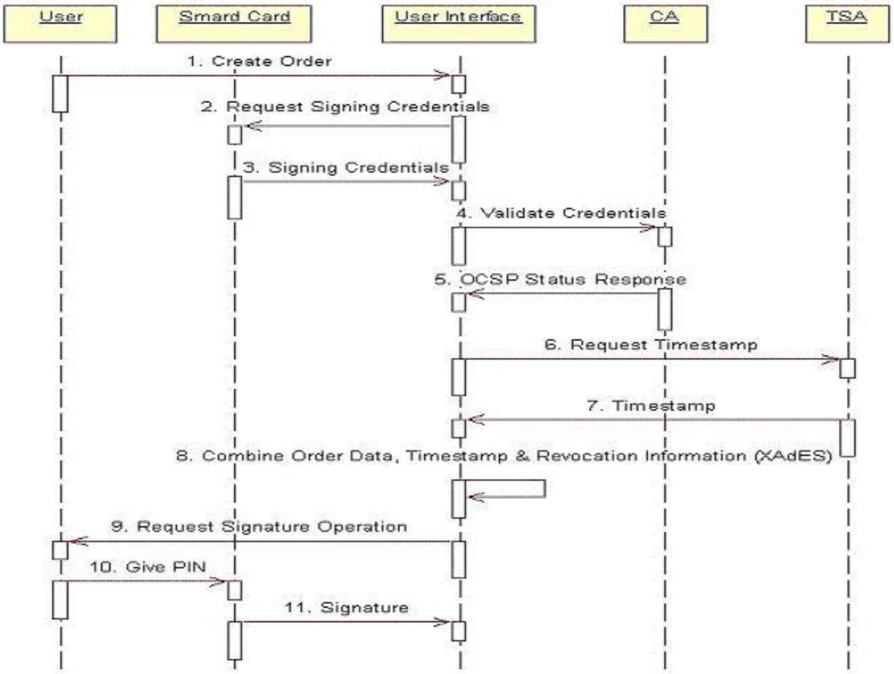

Fig. 2. Sequence diagram for the e-Ordering process (Actions 1-11)

Phase2-Service publication and retrieval: The Sender produces the WSDL document and uses a standard hash function to a subset of the e-Ordering service information that the Sender wants to publish to the UDDI Registry. The Sender's information that remains as clear text corresponds to the contact information, the URL of the WSDL document and the URL of the Privacy Policy document. All other information such as Web Service properties and private data (e.g. VAT code) are hashed. Then the Receiver searching for a service with certain properties generates a query specifying all the conditions on the properties as hashed values. The UDDI Registry returns to the Receiver the URL of the Sender's WSDL document. Now the Receiver has the description of the Web Service in order to configure its service to be able to receive and send SOAP message according to this description. Furthermore, the Receiver produces the WSDL document that corresponds to its service and publishes its service to the UDDI Registry following the same way.

Phase3-Set up security Credentials: The Sender and the Receiver take part in the Registration and Certification procedures as demanded by the Certification Practice Statement of the TTP, and setup the acquired security credentials, in order to achieve a secure communication. Moreover, they have to define the necessary signature policies that will be referenced while producing and validating XAdES signatures, as described in the XAdES standard [3].

When the Sender and the Receiver have accomplished the aforementioned phases, they are ready to initiate the ordering process. The necessary steps to complete this process are illustrated below:

Step1: Access User Interface and Create Order Document (Figure2: Action 1)

The e-Ordering process is initiated by an employee of an organization who accesses a User Interface using a browser. The User Interface enables the user to complete the necessary order's data. The data input is automatically checked for prevention of errors and is used to create the order document.

Step2: Sign Order Document (Figure2: Actions 2-11)

The User Interface transparently gathers the time stamps and revocation status information data from their respective sources. Then, the XAdES signature is formulated based on the cryptographic primitives in the smart card, the user's certificate and the order data. At the end, the order document is signed using the qualified certificate of the user which is located in the smart card.

Step3: Dispatching Order to Sender's Web Service (Figure3: Actions 12-23)

The signed order document is packaged in a SOAP message and is dispatched to the Sender's Web Service. The Sender's Web Service extracts the order, queries the UDDI Locator WS in which UDDI Registry the Receiver has published its Web Service. The query is based on the VAT prefix of the Receiver that corresponds to the country code. When the Sender's Web Service receives the UDDI Registry URL, it queries the Registry in order to receive the Privacy Policy's and the WSDL's documents of the Receiver. All search criteria of the query such as VAT code are hashed. The Sender's Web Service retrieves the Receiver's and the Sender's Privacy Policy, verifies the digital signatures of the documents and merges the two Policies in order to produce a third one and checks the merged Policy in order to decide if it is acceptable and thus the e-Ordering transaction can be accomplished. Then, the order is packaged in a new SOAP message in which the Sender's Web Service applies the acceptable Policy, employing the WS Security extensions.

The Sender's Web Service retrieves the Receiver's WSDL document parses it and retrieves the URL of Receiver's Web Service.

Step4: Receipt of Order at Receiver's Web Service (Figure3: Actions 24-29)

The protected SOAP message is dispatched over HTTP to the Receiver's Web Service that receives the order and follows a fully automated process that requires no human intervention. The SOAP message containing the orders are decrypted with the Receiver server's private key and the validity of their WS Security extensions digital signature is verified, so that the point of origin is validated. Then the e-Order document itself is extracted. Validation of the embedded cryptographic information firstly requires communication with a CA for verification of the credentials that were used to sign the e-Order as well as verification of any timestamp that was included in the document. Finally the XAdES signature is validated.

Step5: Storage of Order at Receiver's XML Database and Dispatching a Receipt (Figure4: Actions 30-31)

The Receiver's Web Service stores the e-Order and a receipt in the Receiver's XML Database. From now on, the e-Order is available for parsing and further processing by the Receiver's users. The Receiver's Web Service dispatches the SOAP receipt, referencing to the received order, and containing the status of the whole process. The SOAP receipt is signed by the receiver's server.

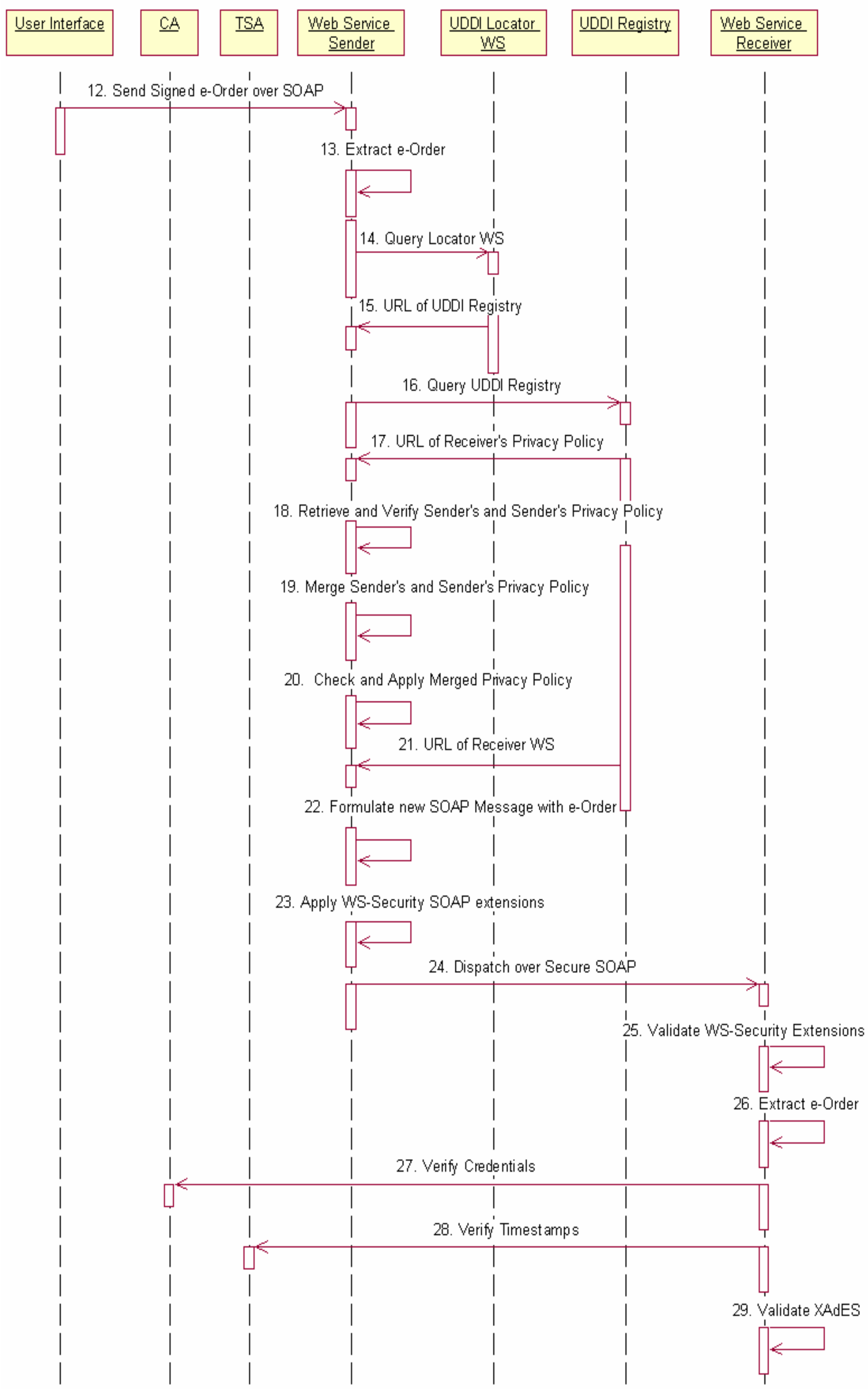
User Interface
CA
TSA
Web Service Sender
UDDI Locator WS
UDDI Registry
Web Service Receiver
12. Send Signed e-Order over SOAP
13. Extract e-Order
14. Query Locator WS
15. URL of UDDI Registry
16. Query UDDI Registry
17. URL of Receiver's Privacy Policy
18. Retrieve and Verify Sender's and Sender's Privacy Policy
19. Merge Sender's and Sender's Privacy Policy
20. Check and Apply Merged Privacy Policy
21. URL of Receiver WS
22. Formulate new SOAP Message with e-Order
23. Apply WS-Security SOAP extensions
24. Dispatch over Secure SOAP
25. Validate WS-Security Extensions
26. Extract e-Order
27. Verify Credentials
28. Verify Timestamps
29. Validate XAdES

Fig. 3. Sequence diagram for the e-Ordering process (Actions 12-29)

Step6: Storage of Order at Sender’s XML Database (Figure4: Actions 32-33)

The Sender’s Web Service receives the signed SOAP receipt and it stores it in its XML database along with the sent order.

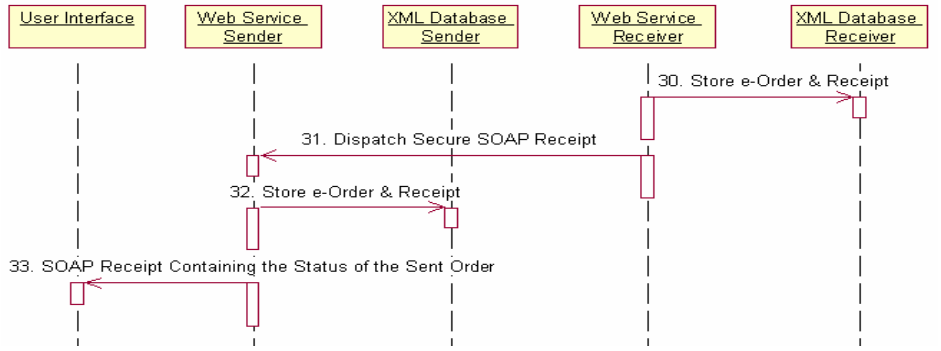
User Interface
Web Service Sender
XML Database Sender
Web Service Receiver
XML Database Receiver
30. Store e-Order & Receipt
31. Dispatch Secure SOAP Receipt
32. Store e-Order & Receipt
33. SOAP Receipt Containing the Status of the Sent Order

Fig. 4. Sequence diagram for the e-Ordering process (Actions 30-33)

4 Assessment

The fundamental purpose of TOES is to address the requirements described in Sections 2.1 deploying a trustful platform, applying the following countermeasures:

Security Requirements

Authentication of origin: using XML digital signatures in combination with tamper resistant cryptographic modules such as smart cards.

Integrity of the content: using a cryptographic hash function, that provides message integrity checks, as part of the digital signature process.

Non-repudiation of origin and receipt: using digital signatures and time stamping.

Long lasting integrity: using ETSI TS 101 903 that produced ETSI to define XML formats for advanced electronic signatures. A XAdES electronic signature offers also non-repudiation based on a predefined signature policy.

Confidentiality and privacy: using XML Encryption as specified in the W3C Recommendation and the Web Services Security recommendation for encryption in SOAP messages.

Integrity of the sequence of the orders: imposing a tight sequence issuance scheme by having a reference number embedded in each order.

Availability: Web Services are published in registries.

Secure Electronic Storage: the XML orders are stored with the original format in which they were received. Furthermore, the combination of XAdES and a native XML database guarantees the secure long-term archiving of e-orders.

Privacy Requirements

UDDI Privacy: using hashing techniques to a subset of published data so they can not be revealed.

Requestor Privacy: searching for a service with certain properties, generating a query specifying all the conditions on the properties as hashed values. As a result, the untrusted Directory can not infer the search criteria.

AR0020.1: the privacy policy is expressed using WSPL.

AR0020.3: the privacy policy is published in a UDDI Registry.

AR0020.5: the privacy policy is used in order to convey conditions under which the e-Ordering Service is provided.

AR0020.6: retrieving the privacy policy from UDDI Registry anonymously.

Performance

TOES achieves particularly satisfactory performance via the adoption of Digital Subscriber Line (DSL) technology. The use of XML and Web Services, as the basic technologies for the formulation and transfer of messages within the platform, expands the size of data several times over. The increase of the data size is translated into more storage, transmission and processing time.

Furthermore, a major factor that affects the performance of the TOES is the choice of the proper algorithm for the encryption of the SOAP messages. Secret key encryption is much faster than public key encryption, but secret keys do not scale as well as public keys. So, in order to achieve higher performance the adopted process is the following: a one-time generated secret key is used for the encryption and the decryption of the data, using a symmetric algorithm (triple-DES). The generated secret key is encrypted using a public key algorithm (RSA-V1.5) and the encrypted key is embedded in the SOAP message.

Benefits

The main anticipated benefit by adopting TOES is the significant operating costs reduction, which involves the minimisation of the workload required for handling paper orders, as well as the expenses involved in printing and delivering them and without purchasing expensive ERP solutions.

TOES service provides a suitable, friendly interface to the authorised user for inputting the necessary data for the order fields that have been defined, in an XML document. A native XML database ensures that the XML orders are stored exactly in the original format in which they were received for any future audit.

TOES is a stand alone, secure e-ordering solution based on open source technologies that can interoperate with existing ERP systems. It achieves to satisfy the requirements that have been posed in Section 2.1, respecting the EU legislation.

Cost

TOES is an affordable solution. SMEs do not have to invest in expensive ERPs in order to offer e-ordering and they do not need dedicated employees that are required to have a specific education background, while the system does not pose additional training and managing requirements.

TOES architecture can be offered as an outsourced service by an Application Service Provider (ASP). In this case, the user organizations (e.g. SMEs) do not have to deploy any infrastructure directly related to TOES. The costs of the ASP for deploying of the TOES are kept low due to the use of open source software (such as

Exist [1]) and are limited to the operation costs. The price policy that must be followed is the essential key factor of the success in order to develop the small, medium and large-sized enterprise market. Table 1 demonstrates a sufficient price policy to maintain such an emerging market.

Table 5. ASP Price Policy

Orders	Price/ Order
0 – 500	3,50 €
500 – 1000	3,00 €
1000 – 2500	2,50 €
2500 – 5000	2,00 €
5000 – 7500	1,80 €
> 7500	1,80 €

5 Conclusions and Future Work

In this paper, we presented the TOES architecture. The proposed system is a secure tool for enterprises which desire to send and receive electronic orders via the Internet in a trustful manner, satisfying the posed security and privacy requirements.

Our future research plan is to expand TOES to several directions, with the fundamental objective to enhance the functionality and interoperability features of the proposed architecture addressing two more requirements: mobility and automated negotiation of the functional parameters of the e-Ordering service.

6 References

1. W. Meier, eXist: An Open Source Native XML Database, In Lecture Notes In Computer Science, Revised Papers from the NODe 2002 Web and Database-Related Workshops on Web, Web-Services, and Database Systems, Springer-Verlag, pp.169-183

2. C. Adams, S. Lloyd, *Understanding Public-Key Infrastructure – Concepts, Standards and Deployment Considerations*, 1st Edition, Macmillan Technical Publishing, 1999.

3. A. Kaliontzoglou, P. Boutsi, D. Polemi eInvoke: *Secure e-Invoicing based on Web Services*, Eletronic Commerce Research, (Kluwer, 2006).

4. P. Sklavos et al ,*Time Stamping in e-commerce, In Proceedings of the E-Business & E-work Conference (EBEW) 2001*, IOS Press, Venice, Italy, October 2001, pp.546-552.

5. D. Austin, *Web Services Architecture Requirements,* (Working Draft 14 November 2002).

6. ETSI Technical Specification, "*ETSI TS 101 903 V1.1.1 - XML Advanced Electronic Signatures (XAdES).*

7. A. Nadalin et al., *Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)*, OASIS Standard http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

8. xCBL.org, XML Common Business Library version 4.00 (xCBL v4.00), 2003,. http://www.xcbl.org/xcbl40/xcbl40.shtml.

9. *Privacy Act in the Telecom Sector, Directive 97/66/EC.*

10. *Free movement, Directive 95/46/EC.*

11. *Legal protection of databases, Directive 96/9/EC.*

12. *Directive 1999/93/EC of the European Parliament on electronic signatures Official Journal* L 013 , 19/01/2000 pp. 0012 – 0020, http://europa.eu.int/ISPO/ecommerce/legal/digital.html

13. E-commerce, Directive 2000/31/EC. http://www.euro.cauce.org/en/timeline.html.

14. "Protection of Privacy, Directive 2002/58/EC". http://europa.eu.int/ISPO/ecommerce/legal.

15. B.Carminati, E.Ferrari, P.C.K. Hung, Exploring Privacy Issues in Web Services Discovery Agencies, IEEE Security & Privacy Magazine, 2005. **3**(5):14-21.

16. E. Christenssen et al.. *Web Services Description Language* (WSDL) 1.1, 2001.

17. T. Bellwood (editor), *UDDI version 2.04 API Specification, UDDI Committee Specification*, OASIS Standard, 2002, www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm#uddiv2.

18. D. Polemi, S. Papastergiou, A Secure, Open and Interoperable e-Ordering Service, 2nd *International Conference on Web Information Systems and Technologies, Webist 2006 INSTICC* Press (ISBN: 978-972-8865-46-7), pp.57-62, 2006, Setubal, Portugal.

19. S. Bajaj et Al, *Web Services Policy Framework* (WSPolicy, September 2004).

20. A. H. Anderson. An Introduction to the Web Services Policy Language (WSPL). *5th IEEE International Workshop on Policies for Distributed Systems and Networks*, Yorktown Heights, New York, **7-9 June** 2004.

21. D. Polemi, S. Papastergiou, *Achievements and future direction in security policies*, *Electronic Democracy Challenges of the digital era*, 2nd National Conference with International Participation, Athens, March, pp. 16-17, 2006, ACCI.

22. D. Polemi, S. Papastergiou, *TOES: Trustful and Open e-Ordering Service for SMEs*, International Conference on Internet Surveillance and Protection, ICISP 2006, August 26 - 29, 2006, Cap Esterel, Côte d'Azur, France.