Electron Commerce Res (2006) 6:337–353
DOI 10.1007/s10660-006-8678-6

eInvoke: Secure e-Invoicing based on web services

Alexandros Kaliontzoglou · Pelagia Boutsi · Despina Polemi

Abstract Electronic Invoicing services (e-Invoicing) will have a pivotal role in all the stages of handling Value Added Tax (VAT) for European Member States. Through a systematic introduction of e-invoicing, tax administrators will be able to implement new tools and procedures to carry out alternative controls that are less intrusive on the trading partners. Nevertheless, successful European e-invoicing implementations need to be in compliance with the corresponding European Directive 2001/115/EC. Most contemporary e-Invoicing implementations are proprietary and based on EDI, thus demonstrating great deficiencies. This paper presents an open electronic invoicing system named eInvoke, based on XML, XML cryptography and Web Services, that addresses all security requirements imposed by the Directive.[1]

Keywords e-Invoicing · XML · Web services · Security · Advanced e-signatures · Cryptography

A. Kaliontzoglou (✉)
National Technical University of Athens, School of Electrical and Computer Engineering, 9 Herroon Polytechniou Str., Athens, Greece
e-mail: akalion@softlab.ntua.gr

P. Boutsi · D. Polemi
University of Pireaus, Department of Informatics, 80 Karaoli & Dimitriou Str., Pireaus, Greece
e-mail: pboutsi@webmail.unipi.gr

D. Polemi
e-mail: dpolemi@unipi.gr

A. Kaliontzoglou
Expertnet S.A., R&D Department, 1 Achilleos Str. & 244 Kifissias Ave., Athens, Greece

[1] Our e-Invoicing system has been accepted by "CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing relating to VAT Directive 2001/115/EC" and its summary appears in CEN 2003 report [13] (pg 79–85), forwarded to EC as a recommendation.

1. Introduction

A commercial invoice is the most important document exchanged between trading partners. In addition to its commercial value [41], an invoice is an accounting document that has legal implications to both transacting parties and constitutes the basis for Value Added Tax (VAT) declaration, VAT reclamation, statistics declaration for intra community trade, export and import declaration for extra community trade. Therefore, invoices have a pivotal role in the VAT system for Member States. They indicate the possibility of VAT refund by the receiver of an invoice and the VAT regime applied. Through a more systematic introduction of e-invoicing, tax administrators may be able to implement new tools and procedures to carry out alternative controls that are less intrusive on the trading partners [13].

The European Union Directive on VAT legislation on electronic invoicing and electronic storage of invoices [35] will have to take effect within Member States at the latest by January 1st of 2004 and has to be adopted in all European Union (EU) countries by 2008. Therefore, e-invoicing services deployment is a pan European consideration. Nevertheless, in order for e-invoicing implementations to be successful, they need to be in compliance with the EU Directive requirements i.e. acceptable, interoperable, secure and affordable by the majority of businesses and organizations operating in EU Member states.

Most contemporary e-Invoicing implementations are based on EDI, which is an option covered by the Directive. The usage of advanced e-signatures is the other option suggested in the Directive, but their adoption in e-invoicing systems is not widespread at the moment. In particular the Directive states: "*... Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed: by means of an advanced electronic signature...*"

Among other important points, the EU Directive determines the secure storage and safe keeping of invoices among Member States. "*...a taxable person shall ensure that copies of invoices issued and received are stored.* "*...authenticity, integrity and readability shall be guaranteed throughout the storage period...*".

This paper presents an alternative to EDI architecture of an electronic invoicing system based on the eXtensible Markup Language (XML) [29], XML Cryptography [8], Public Key Infrastructure (PKI) [4, 11] and Web Services [8] called eInvoke. eInvoke is an open, practical, cost-effective and secure solution in accordance to EU legislation to allow for its deployment in various sectors.

The paper is structured as follows: Section 2 presents a state-of-the-art on e-invoicing services in the European region as well as an overview of the legal framework which supports electronic invoicing. Section 3 summarizes the fundamental security requirements of e-invoicing, proposes countermeasures that address these requirements and have been implemented in eInvoke. Section 4 describes in detail the e-invoicing system architecture and its components, and finally Section 5 draws conclusions and gives an indication of future goals that will be pursued to enhance the already implemented secure e-invoicing service.

2. State-of-the art and legal framework of e-Invoicing services

This section presents the relevant European legislation for secure e-Invoicing systems, and describes e-Invoicing security requirements as well as the technical countermeasures that address these requirements. Current European implementations are also presented.

2.1. Legal framework

E.U. directives accelerate the envisioned harmonization of the national legislative frameworks necessary for the provision of a uniform framework for the European market, under which electronic invoicing is standardized and thus applicable in every European Member State. The immediate expected result of this effort is the facilitation of commercial transactions between Member States, through the exchange of electronic invoices. This harmonisation effort is evident by the introduction of the following directives:

- Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax [35]. This Directive clarifies the implementation of e-invoicing through the Member States and aims to introduce harmonized procedures for invoicing (paper or electronic invoicing) across Member State borders in a homogeneous home market. According to the Directive, businesses operating in EU Member States should have simplified invoicing regulations and procedures harmonized at EU Community level as of January 2004. The Directive additionally promotes the use of PKI by obligating EU countries to accept digitally signed electronic documents.
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures [33]. The Directive facilitates the use of electronic signatures throughout the EU, contributes to their legal recognition, establishes the legal framework for electronic signatures and certification services providers and ensures proper functioning of internal markets in certification services and e-signatures. According to the Directive ". . . an *advanced electronic signature* could guarantee the *authenticity of origin and integrity of the contents*". Member States may however ask for the *advanced electronic signature to be based on a qualified certificate and created by a secure signature device*, within the meaning of Article 2 (6) and (10) of the aforementioned Directive.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [31].
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [32].
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [30].

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [36].
- Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [34].

The above directives and regulations impose restrictions that electronic invoicing implementations have to take into account to comply with the legal framework of EU Member States.

2.2. e-Invoicing security requirements

In order for e-Invoicing to become part of the financial and legal practices of an organization, it is important that it satisfies strict security requirements. This section gives a detailed presentation of the fundamental security requirements and measures that can be taken to address them. The majority of these requirements is imposed by Directive 2001/115/EC.

- *Authentication of origin* ensures that senders of invoices are really the ones who they claim to be. Authentication of the taxpayer engaged in an e-invoicing transaction is necessary for the tax authorities to uniquely and irrevocably identify the parties involved in a taxable transaction. This requirement can be addressed by the application of XML digital signatures in combination with tamper resistant cryptographic modules such as smart cards. Furthermore, the use of Qualified Certificates may cover the corresponding requirement as set out in the Directive.
- *Integrity of the content* of the invoices ensures that invoices cannot be altered intentionally or accidentally during transmission or storage. Thus, the involved parties can be confident with respect to the content of the invoice. A cryptographic hash function [4] provides message integrity checks and can be used either separately or as part of the digital signature process.
- *Non-repudiation of origin and receipt* ensures that neither the sender nor the recipient can deny the invoicing exchange occurred. The application of digital signatures and time stamping [24] on specific messages accomplishes non-repudiation. An XML Advanced Electronic Signature (XAdES) also offers non-repudiation based on a predefined signature policy [20].
- *Confidentiality and privacy* ensures that no one other than the sender and the designated recipients can read the e-invoice. XML Encryption as specified in the W3C Recommendation [14] and the Web Services Security recommendation for encryption in SOAP messages [3, 8] provide confidentiality.
- *Integrity of the sequence* of the invoices assists in avoiding any gaps occurring in the outgoing invoices and in strengthening company and tax authority control. This requirement is implementation specific and can be fulfilled by enforcing a tight sequence issuance scheme for the reference number embedded in each invoice.
- *Availability* ensures that companies or Revenue Services can use an e-invoicing service at any time without disrupting their accounting practices. On one hand, the

system should be robust and protected against intrusion and hacking, which can be ensured by standard network elements such as intrusion detection systems, antivirus and firewalls. On the other hand, some form of public directory usage for publishing the offered services will foster services dissemination.
- *Electronic Storage* of e-invoices. The conditions for electronic storage of e-invoices and the technical requirements of the electronic storage system are integral components of the security requirements concerning e-invoicing. Authenticity, integrity and readability should be guaranteed throughout the storage period, according to the e-Invoicing Directive. A native XML database can ensure that XML invoices are stored exactly in the original format in which they were received for any future audit. Furthermore, the combination of XAdES and such a database can guarantee the secure long-term archiving of e-invoices.
- *E-Invoicing application security policy*. An e-invoicing application should be accompanied by a corresponding policy, which would identify the signature policy issues (how and why an electronic signature is used in the context of the application) and other policy issues, like for example the cross-border communication restrictions that presuppose an established trust framework between different countries.

2.3. Existing e-Invoicing implementations

Currently, there exist various e-invoicing solutions, which while ensuring compatibility with pre-existing financial applications in different ways, do not satisfy all the requirements stated in the previous section.

- In some solutions the invoices are stored and managed centrally by the companies that provide the invoicing service, which therefore act as Trusted Third Parties. Some provide transformation services from one invoice format to another [5, 18].
- Electronic invoices are created either by a component of a financial suite that the invoice issuer operates [5], or by some plug-in to the pre-existing financial package [21], or even by an autonomous web-based e-invoicing facility.
- The exchange of e-invoices is carried out either over secure leased lines, or over the Internet using Message Authentication Code (MAC) and Secure Sockets Layer (SSL) [4] technologies for ensuring the integrity, confidentiality and authentication during the exchange of invoices [6, 18, 26].
- Some solutions achieve non-repudiation with PKI and XML signatures [21, 27]. Some even provide the capability to access centrally stored private keys and certificates in order to provide a way for digitally signing e-invoices from any access point.
- Some solutions involve the dispatch of email notifications between the parties that exchange e-invoices in order to initiate the manual retrieval of the invoices. Thus, they reduce the complexity of the security infrastructure required by other approaches, by providing access to a secure server where the invoice is created [19].
- A significant portion of the existing solutions complies with the EDI standard or provides translators for it [26].
- One existing e-invoicing service is based on the ETSI TS 101 903 (commonly known as XAdES, which stands for "*X*ML *Ad*vanced *E*lectronic *S*ignatures") standard [20] aiming at the long-term preservation of digitally signed documents [40].

- There exist several invoicing solutions that do not transfer any kind of electronic data. They handle data contained within an invoice after having scanned its paper version [42].

Although, there are e-invoicing systems that use advanced e-signatures [13], there are no existing implementations that guarantee a robust interoperable service provision and at the same time satisfy the security requirements on the exchange and management of the e-invoices.

Some of the above features satisfy a subset of the requirements for e-invoices mentioned in the Directive, while others do not address all the security aspects. Most of the existing implementations are proprietary and closed solutions. On the other hand, eInvoke addresses the security and storage requirements as set out in the Directive 2001/115/EC so that they are compliant with the European legal framework, by employing technologies such as Web Services and XML, the public Internet, the XAdES standard, XML Cryptography and Web Services Security, an XML-based database and finally support for Qualified Certificates [2]. Moreover, it is based on widely accepted standards, which ensure interoperability and allow coherent transaction flow and easy integration to existing infrastructures. Finally, the service is cost effective since it is an open network solution.

3. eInvoke: a secure e-Invoicing service

This section describes the architecture of our e-Invoicing service, the entities that may use the service to perform e-Invoicing and the procedures these entities have to go through in order to complete an e-Invoicing transaction.

3.1. Service architecture

In this section we present the eInvoke architecture. The system design adopts the most advanced and widely adopted standards for secure interoperable service provision, while satisfying all the requirements for the exchange and management of electronic invoices as described in Section 2.2. The service relies on XML and Web Services for security and interoperability, a fact which enables smooth integration with existing accounting software that organisations may use, as well as stand-alone operation of the service that would suit smaller companies or individuals. This is achieved by publishing the provided service in UDDI (Universal Description, Discovery and Integration Protocol) based directories [28], from which the service description can be retrieved formulated as specified by WSDL (Web Services Description Language) [16]. This enables other Web Services conforming to the appropriate message formats to interact with the eInvoke Web Service.

Figure 1outlines the system architecture which comprises three major components: the User Interface, the eInvoke Web Service and the XML Database.

A detailed description of these components is provided as follows:

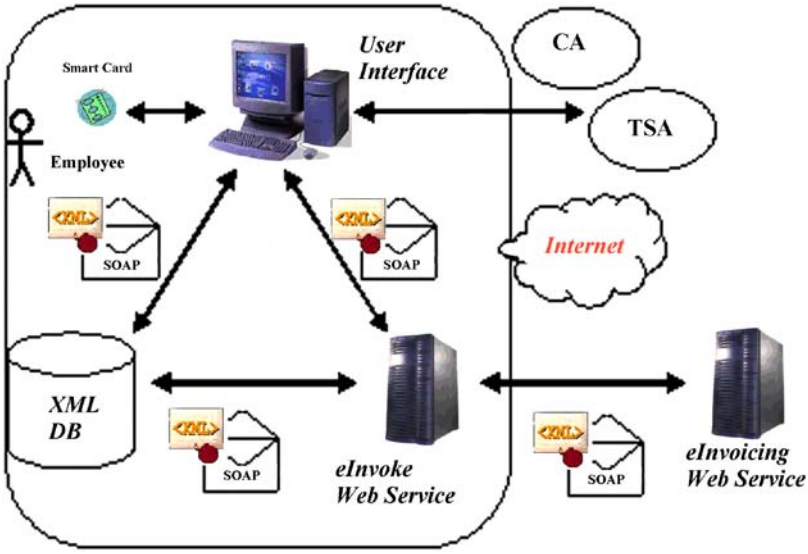

Fig. 1 eInvoke architecture

(a) User interface

The User Interface is a Signed Java Applet [12] running on a standard web browser. The user interacts with the system through this interface to create, manage and send e-invoices. The interface is able to produce XAdES signatures according to the hosting organization signature policy. It communicates with five other entities:

- The user's smart card for authentication and signing purposes. The communication protocol uses the PKCS#11 standard [4].
- The eInvoke WS to deliver e-invoices. The communication is performed through the use of SOAP over HTTP.
- The CA (Certification Authority) to request certificate status information used as part of the validation of digital signatures. The protocol used is OCSP (Online Certificate Status Protocol) [4, 11].
- The TSA (Time Stamping Authority) to request time stamps. This communication uses an implementation of the standard time stamping protocol based on RFC 3161 [10].
- The XML database to retrieve invoice specific information (existing invoices, contact details etc.). The communication protocol is SOAP over HTTP.

(b) eInvoke web service

The eInvoke Web Service is a Java based implementation of a Web Service [15], running as a servlet on an Apache Tomcat web server. As depicted in Fig. 1, it communicates with three entities:

- The User Interface, as previously described.
- The XML Database in order to store invoices and receipts, using as a protocol SOAP over HTTP.
- Another Web Service as part of the eInvoicing process. The messages exchanged in the communication are based on SOAP with WS security extensions (including digital signatures and encryption) over HTTP.

(c) Native XML database

The Database used is the eXist native XML database [38]. It is running as a stand alone server and communicates with the User Interface and the eInvoke Web Service.

The message format integrated in the current version of the system uses the XML Common Business Library version 4.0 (xCBL 4.0) [39], 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. The XML schema adopted for the e-invoice is a subset of xCBL, which covers nonetheless all mandatory fields defined in Directive 2001/115/EC. The selection of xCBL is based on its maturity, level of completeness and clarity.

The system utilizes XML digital signatures as defined in the ETSI XAdES standard to sign the issued XML eInvoices. An open source implementation of XAdES [7] was used. This implementation has been corrected and improved at points that did not fully conform to the standard and it has been modified and augmented with time stamping, which was not part of the original implementation. The XAdES creation process includes three separate sub-processes which occur transparently:

- *digital signing* of the e-invoice and certain other properties according to the W3C XML Digital Signature standard,
- *time stamping* by requesting, and embedding a time stamp token on the generated signature according to the IETF 3161 standard [10], and finally
- *revocation information inclusion* by embedding certificate revocation status data after requesting them on-line from the OCSP [4, 11] server of the CA that has issued the signer's certificate.

The exchange mechanism for e-invoices relies on the SOAP messaging with Web Services Security extensions [3, 8]. This adds a second level of protection based on digital signatures and encryption, directly adding strong confidentiality, integrity and non-repudiation to the message routing and transport layer.

In the current stage of implementation, storage is handled by a native XML database to satisfy the requirement for storage of the exchanged e-invoices in the form in which they were sent and received. Long-term validation of a stored invoice signature is ensured by the XAdES information already embedded in the invoice.

3.2. e-Invoicing entities and roles

This section presents the entities involved in an e-Invoicing transaction with the eInvoke system and their roles. As in common invoicing practice, an e-invoicing transaction occurs between the issuer of the invoice who charges for a set of services or products and the receiver who is called to pay for them. Both parties have to be able

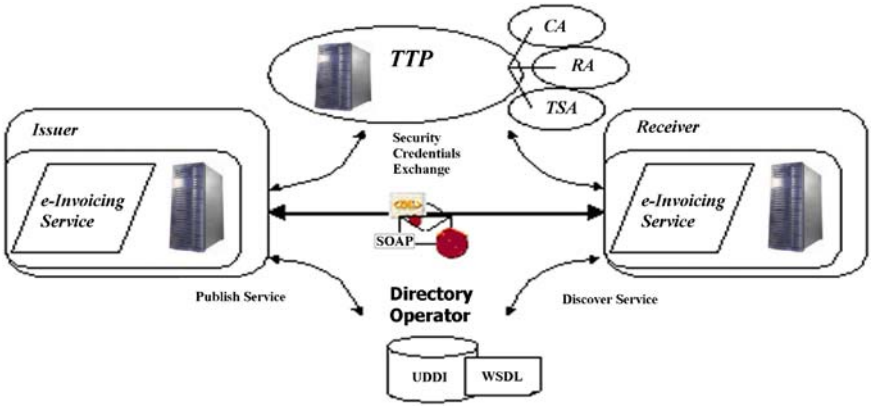

Fig. 2 e-Invoicing transaction scheme

to view and process e-invoices and be able to understand the security policy applied in a user-friendly manner.

All entities and their relationships are depicted in Fig. 2:

The actors that take part are:

(a) The issuer

This organization hosts the e-Invoicing service infrastructure. It takes the appropriate steps to deploy the service and publish it in the Registry, so that other organizations may find it. It also communicates with the TTP to get the proper security credentials.

(b) The receiver

The Receiver organization may be hosting the same e-Invoicing service or another implementation of a service, which understands the xCBL invoice schema, and SOAP messages with WS security extensions. In the latter case, the Receiver will have to search for the description of the eInvoke Web Service in the UDDI and be configured to understand its messages. The Receiver organization will also have to communicate with the TTP to get its proper security credentials.

(c) The TTP

Before any secure messaging can take place, all participants need to have established an adequate security framework with Trusted Third Parties (TTPs) [11]. The required TTPs in our solution are at a minimum a Certification Authority (CA) and a Registration Authority (RA) offering the PKI services of registration, certification and revocation status information with OCSP, as well as a Time Stamping Authority (TSA) offering standard based time stamping services.

(d) UDDI directory operator

This operator hosts a public UDDI directory where Web Services can be published and thus become publicly available.

3.3. e-Invoicing processes

The e-invoicing process can be divided into four phases, namely pre-invoicing, issuing, dispatch/reception and storage, comprising the following processes:

(A) Pre-invoicing phase

The steps that take place in this phase include the optional communication with the UDDI registry for publication and retrieval of the service from the Issuer and the Receiver respectively (Fig. 3), and communication with the TTP for acquisition of the security credentials (Fig. 4).

During publishing, the Issuer uploads the WSDL description of the service to the UDDI. The Receiver searches the UDDI through the web interface it offers, retrieves

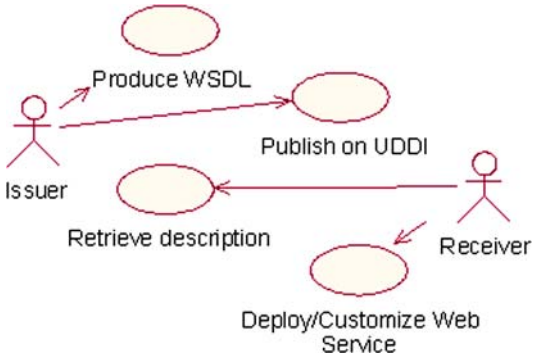

Fig. 3 Service publication and retrieval

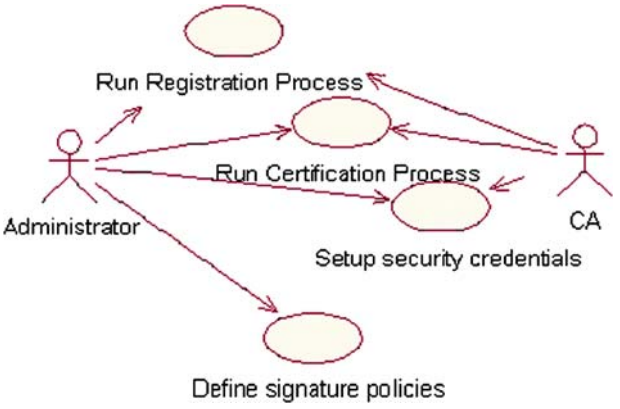

Fig. 4 Security technical and organization setup procedure

the WSDL document and configures its service to be able to send and receive SOAP messages based on that WSDL document (see Fig. 3).

In order to securely communicate, both the Issuer and the Receiver take part in the Registration and Certification procedures (see Fig. 4) as demanded by the Certification Practice Statement of the TTP, and setup the acquired security credentials (possibly in the form of a smart card) to be used by the e-Invoicing infrastructure.

Furthermore, it is important that these organizations define the necessary signature policies that will be referenced while producing and validating XAdES signatures, as described in the XAdES standard.

(B) e-Invoice issuance phase

As depicted in the sequence diagram of Fig. 5, an employee of the issuer organization (represented by the class user on the figure) initiates the e-Invoicing process. He first authenticates himself by means of his smart card and PIN through the User Interface. Based on the authentication credentials the system performs an authorization check. Our prototype implementation performs simple authorization checks by comparing the information contained in a credential with information stored on the back end XML database. More elaborate authorization schemes are foreseen in future work. Other approaches on how invoice data may appear on screen have been taken into account during the design of the interface [43].

The User Interface enables the user to create a new Invoice and supply the necessary data to complete the invoice or manage existing invoices (e.g. received, drafts etc.). This data input is automatically checked for prevention of errors. According to the user's privileges, the option for signing and dispatching the eInvoice is enabled or disabled. If the user has the right of signing and presses the "Sign and Send" button, the User Interface transparently completes a series of steps:

- the form data are gathered and are used to structure an e-Invoice,
- the time stamps and revocation status information data are gathered from their respective sources and
- the XAdES signature is formulated based on the cryptographic primitives in the smart card, the user's certificate and the invoice data.

The distinction between types of users provides flexibility for both the employee that feeds in the data and the person who is responsible for signing the invoices, if they are not the same person.

The signing and authentication certificates might be different or they might be the same, something which is governed by the organizations policies. In case they are different, the user is prompted to use one or the other, according to what he is trying to accomplish at that particular time.

(C) e-Invoice dispatching & receipt phase

After the successful creation of the XAdES signature, the User Interface packages the invoice in a SOAP message and sends it to the eInvoke Web Service A, as depicted

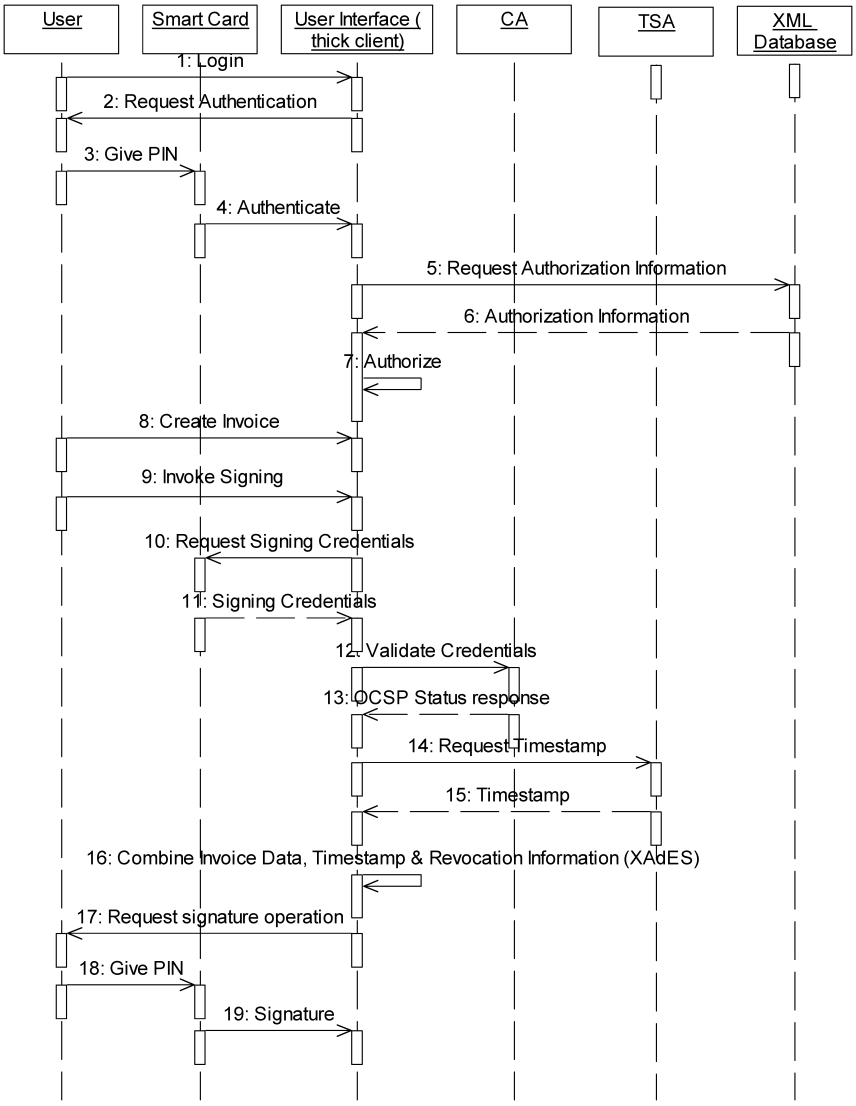

Fig. 5 e-Invoice issuance phase

in the sequence diagram of Fig. 6. The eInvoke Web Service A is hosted in the same platform as the User Interface. The eInvoke Web Service is responsible to extract the eInvoice and package it in a new SOAP message destined for the receiver. The receiver's details are extracted from the eInvoice itself, and at this phase the eInvoke Web Service also applies the WS Security extensions to the SOAP message, so that it becomes encrypted with the Receiver's public key, and digitally signed with the Issuer's server private key. Finally the protected SOAP message is dispatched over HTTP to the Receiver.

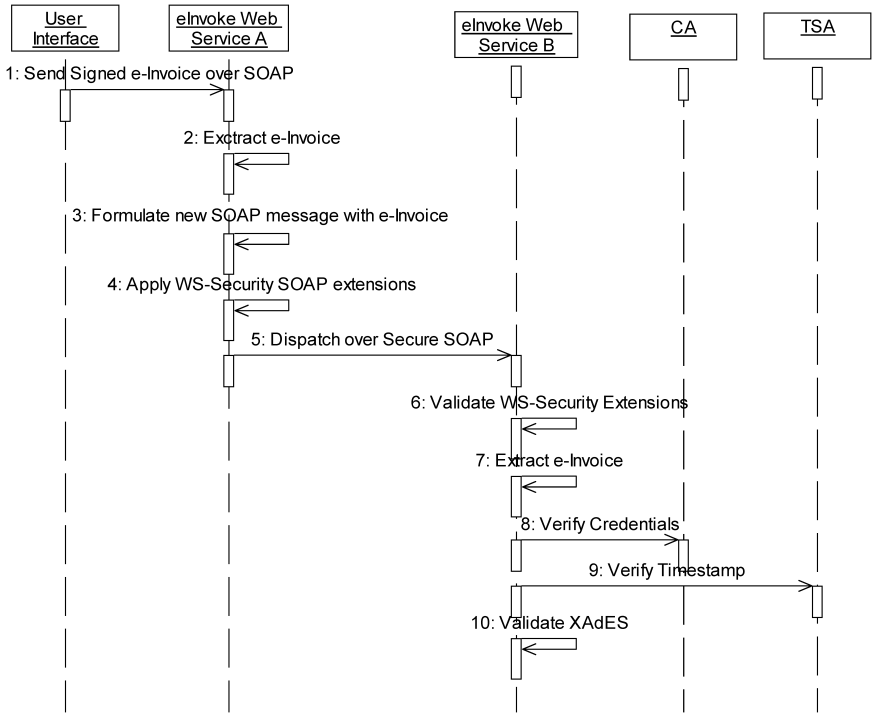

Fig. 6 e-Invoice dispatching and receipt phase

The reception of the invoice, at the Receiver's eInvoke Web Service B (or equivalent), is a fully automated process that requires no human intervention. The SOAP message containing the invoice is received and 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-invoice 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-Invoice as well as verification of any timestamp that was included in the document. Finally the XAdES signature is validated.

(D) e-Invoice storage phase

During the last phase, initially the e-invoice is stored in the database of the Receiver, as shown on Fig. 7. That makes it available for parsing and further processing by the Receiver's users. The process is finalized by the dispatch of a SOAP reply (receipt), referencing the newly received invoice, and containing the status of the whole process. This reply is signed in a similar way using WS Security extensions by the Receiver's server in order to be valid as a receipt. When the Issuer eInvoke Web Service receives this signed SOAP reply, it is stored in the Issuer XML database along with the sent invoice.

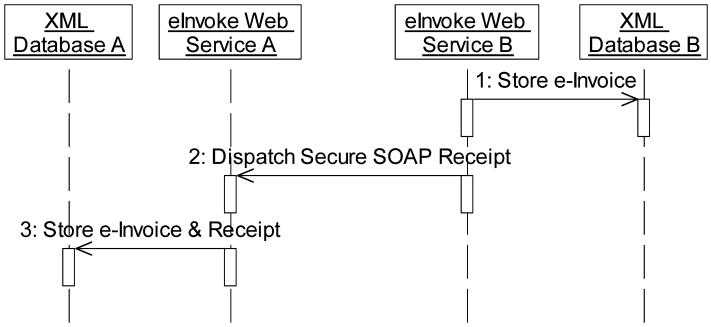

Fig. 7 e-Invoice storage phase

The above functional description illustrates that the most active actors are the complementary Web Services that handle all the underlying complexity of the exchange process, enabling services semi-automation. Complete automation cannot be achieved due to the restrictions posed by the Directive on e-Invoicing that requires the invoices to be monitored by actual persons responsible for the validity of the invoices' content.

4. Research directions and conclusions

This paper has presented an innovative secure e-Invoicing service architecture, based on XML, XML digital signatures and encryption, xCBL and Web Services, in order to offer an interoperable, affordable, state-of-the-art standards compliant and scalable solution, addressing the security requirements imposed by EU legislation.

An open research issue of major importance to the eInvoke service, is the validity period of electronic signatures currently offered. XAdES ensures that the signature is secured by means of an archive time-stamp. This archive time-stamp, which can be added to a signature as an unsigned attribute, includes the content of the document, the signed attributes, the corresponding signature value, selected verification data and preceding archive time-stamps. A drawback of XAdES is that only individual signatures are renewed and the renewed electronic signature does not include all the preceding signatures of the document [25]. Therefore measures are required to improve the performance of secure archiving, because the updates of a document bearing a XAdES signature document entail a cumbersome time-stamping process. As an example of update we can mention the re-signing of the document due to an obsolete signature algorithm or new revocation information after the compromise of a certificate. To increase the performance, the minimization of all the necessary time-stamps should be considered. Another important issue is the fact that the definition of a purely XML based time-stamp protocol is still missing [1, 22], and we have to embed a BASE64 encoded version of a binary time stamp into the XML XAdES document.

Regarding the service itself, we are already working on the following improvements:

- The provision of support for more XML Schemas for e-invoices based on European and world wide standardization efforts such as the Business Application Software Developers Association (BASDA) electronic Business Interchange standard using

XML (eBis-XML suite) [17], the Universal Business Language (UBL) [9] and the Open Applications Group Integration Specification (OAGIS) [23].
- Integration testing with existing ERP systems for invoice management.
- Implementation of complete authorization system. We are also planning to look into the XACML standard regarding the specification of authorization policies.
- Support for native XML key management, by integrating XML Key Management System (XKMS) [37] functionality, which will provide smooth and transparent integration with the required PKI services.
- Wireless access to the e-Invoice service, allowing mobile submission of e-Invoices, as well as mobile supervision of the service's data, in order to satisfy the mobility requirements that in certain cases may be crucial. Mobile access should provide the same level of authentication control as local/wired access.

We consider the horizontal approach to integrating several existing schemas for e-invoices as the most important future target at this point, in order to maximize the service interoperability. All extensions though will enhance the functionality of our service end will improve its interoperability and performance features.

Acknowledgements The authors would like to thank the "CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing relating to VAT Directive 2001/115/EC" for their encouragement and Mr. Ioannis Mavroudis for his constant support throughout the implementation and deployment phase of the e-invoicing service.

References

[1] Apvrille, A., & Girier, V. (2002). XML security time stamping protocol. In *Proceedings of Information Security Solutions Europe Conference (ISSE 2002)*, Paris, France.
[2] Kaliontzoglou, A. et al. (2003). Secure e-Invoicing service based on web services. In *Proceedings of the 1st Hellenic Conference on Electronic Democracy*, Athens, Greece.
[3] Nadalin, A. et al. (ed.). (2004). Web Services Security: SOAP Message Security 1.0 (WS-Security 2004). OASIS Standard, docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.
[4] Nash, A. et al. (2001). *PKI: Implementing & Managing E-Security*. McGraw-Hill Osborn Media Publishing.
[5] Accountis Enterprise. (2003). Make the switch to EIPP. White paper-datasheet, www.accountis.com/website/accountis_general.pdf.
[6] Alysis Enterprise. www.alysis.com.
[7] Sertifitseerimiskeskus, A. S. (2003). The Esthonian ID Card and digital signature concepts: Principles and Solutions. white paper, www.id.ee/file.php?id=122.
[8] Hartman, B. et al. (2003). *Mastering Web Services Security*. Wiley Publishing.
[9] Meadows, B., & Seaburg L. (eds). (2003). Universal Business Language 1.0 Beta – OASIS committee draft.
[10] Adams, C. et al. (2001). Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Internet Eng. Task Force RFC 3161.
[11] Adams, C., & Lloyd, S. (1999). *Understanding Public-Key Infrastructure — Concepts, Standards and Deployment Considerations*. 1st Edition, Macmillan Technical Publishing.
[12] Austin, C., & Pawlan, M. (2000). *Advanced Programming for the Java 2 Platform*. Addison-Wesley.
[13] CEN/ISSS e-Invoicing Focus Group. (2003). Report and Recommendations of CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing. www.cenorm.be/isss/Projects/e-Invoicing.
[14] Eastlake, D., & Reagle, J. (ed.). (2002). XML Encryption Syntax and Processing, W3C Recommendation, www.w3.org/TR/xmlenc-core.
[15] Armstrong, E. et al. (2002). *The Java Web Services Tutorial*. Addison-Wesley.
[16] Christenssen, E. et al. (2001). Web Services Description Language (WSDL) 1.1. W3C Note, www.w3.org/TR/wsdl.

[17] eBIS-XML Specifications, Business Application Software Developers Association (BASDA), basda.net/twiki/pub/Core/DownloadTheSuite/eBIS-XML-3.05.zip.
[18] Elma Invoice Enterprise. (2000). *Enhanced Reliability in eInvoicing*. White paper, www.elmaeinvoice.com/pdf/Elma_eInvoice1100_eng.pdf
[19] Emergis Enterprise, www.emergis.com/en/solutions/invoicing/einvoicing/
[20] ETSI Technical Specification. (2002). ETSI TS 101 903 V1.1.1—XML Advanced Electronic Signatures (XAdES).
[21] Isabel eInvoice Enterprise, *Documentation about Isabel eInvoice*. www.isabel.behr/invoice/en/more/download.html.
[22] Wouters, K. et al. (2002). Towards an XML Format for Time-Stamps. In *Proceedings of ACM Workshop on XML Security*, (pp. 61–70). ACM Press, Fairfax, Virginia.
[23] Rowell, M. Open Applications Group (2002). OAGIS—A "Canonical" Business Language. white paper, version 1.0, www.openapplications.org/downloads/whitepapers/whitepaperdocs/20020429_OAGIS_A_Canonical_Business_Langugage-PDF.zip.
[24] Sklavos, P. et al. (2001). Time stamping in e-commerce. In *Proceedings of the E-Business & E-work Conference (EBEW) 2001*, (pp. 546–552). IOS Press, Venice, Italy.
[25] Brandner, R., & Pordesch, U. (2002). Long-term conservation of provability of electronically signed documents. In *Proceedings of the Information Security Solutions Europe Conference (ISSE 2002)*, Paris, France.
[26] Seagha Enterprise, www.seagha.com/0203.html
[27] StreamServe Enterprise. (2003). Secure Business Communication: How organizations can effectively safeguard their mission-critical business communication infrastructures, white paper, www.streamserve.com/pdf/whitepaper/WP_EnhancedSecurity_SESWP10-03-E-eng.pdf.
[28] Bellwood, T. (ed). (2002). UDDI version 2.04 API Specification, UDDI Committee Specification, OASIS Standard, www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm#uddiv2
[29] Bray, T. et al. (2004). Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, www.w3.org/TR/2004/REC-xml-2004024
[30] The European Parliament. (1997). Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[31] The European Parliament. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[32] The European Parliament. (1996). Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[33] The European Parliament. (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[34] The European Parliament. (2001a). Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
[35] The European Parliament. (2001b). Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax.
[36] The European Parliament. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[37] Ford, W. et al. (2001). XML key management specification XKMS, W3C note, www.w3.org/TR/xkms.
[38] Meier, W. (2002). 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*, (pp. 169–183). Springer-Verlag.
[39] xCBL. org, (2003). XML Common Business Library version 4.00 (xCBL v4.00). www.xcbl.org/xcbl40/xcbl40.html.
[40] XiCrypt Technologies GmbH, eBilling Suite by Xicrypt: Electronic Invoicing, www.xicrypt.com/ebilling_eng.php.
[41] Banerjee, S., & Kumar, Ram L. (2002). Managing electronic interchange of business documents. *Commun. ACM 45*(7), 96–102.
[42] Klein, B., Agne, S., & Dengel, A. (2004). Results of a Study on Invoice-Reading Systems in Germany. Document Analysis Systems VI: 6th International Workshop, Florence, Italy. In *Proceedings, Lecture Notes in Computer Science*, Springer-Verlag GmbH, Volume 3163/2004, 451.

[43] Korhonen, R., & Salminen, A. (2003). Visualization of EDI Messages: Facing the Problems in the Use of XML. In *Proceedings of the 5th international conference on Electronic commerce*, (pp. 465–472) Pittsburgh. Pennsylvania, ACM.

Alexandros Kaliontzoglou holds a Degree in Electrical and Computer Engineering from the National Technical University of Athens (NTUA), Greece. Since 2001 he is a PhD candidate in the area of Network and Information Systems Security at the Telecommunications laboratory in the School of Electrical and Computer Engineering of NTUA. Since April 2000 he has been working for Expertnet S.A. as a security engineer specializing at Web Technologies and network applications, and he has been active both in European research projects in the 5th and 6th Framework Programme (eMayor, Intelcities, SELIS, Reshen, La Mer, TSEC, WebSig) and projects of the Greek private sector. His research interests focus in the area of IT Security, Service Oriented Architectures, Web Services, Software Engineering, e-Government, e-Commerce and Public Key Infrastructures.

Pelagia Boutsi has obtained the Degree in Informatics from the University of Piraeus, Greece, in November 2001. Since April 2002, she is a PhD candidate in the area of Security Information at the Computer Science Department of University of Piraeus. Since September 2001 she is employed at Expertnet S.A. as member of the Technical Department. Her current research interests are in the fields of PKIs, XML and XML Security. She has participated in European research projects and projects of the private sector.

Despina Polemi has obtained the Degree in Applied Mathematics from Portland State University (USA) in 1984, Ph.D. in Applied Mathematics (Coding Theory) from City University of New York (Graduate Center) in 1991. She held teaching positions (1984–1995) in Queens College and Baruch College of City University of New York. From 1991 to 1996 was assistant professor (tenure track) in State University of New York at Farmingdale in the department of Mathematics. During 1996–2002 she was an associate researcher in ICCS. From 2000 to 2003 she acted as President of the BoD in a security consulting company Expertnet (www.expertnet.net.gr) and technical manager of the company from 2000–2004. She now a Professor in the University of Piraeus R&D department. Her current research interests are in the fields of cryptology, security and e-business. She has over ninety publications in the above areas. She has received many research grants from various organizations such as the Danish Research Foundation, MSI Army Research Office/Cornell University, IEEE, State University of New York (SUNY), and The Graduate School of City University of New York (CUNY). She has been project manager (PM)/technical manger (TM) in security projects of various programmes such as National Security Agency (NSA), Dr. Nuala McGann Drescher Foundation, Greek Ministry of Defense, INFOSEC TELEMATICS for Administrations (COSACC), the Fifth Framework IST Programme (HARP, BEE, SEED, WebSig, TSEC, CORAS, RESHEN, SEED, La Mer, SECRETS) and the 6FP (e-Mayor, Intelcities, BIOSEC, SELIS). She participated in the EC security projects of the programs COST, ACTS, and NATOs' security projects. She is a member of IEEE. She serves as an evaluator, reviewer and expert in the European Commission and consultant for the FP6.