Towards an XML-based Data Exchange Mechanism for the Portuguese SMEs

Miguel Mira da Silva	Artur Romão	Alberto Silva
IST & INESC	Universidade de Évora	IST & INESC
Lisboa, Portugal	Évora, Portugal	Lisboa, Portugal
mira-da-silva@ip.pt	artur@dmat.uevora.pt	Alberto.silva@inesc.pt

1. ABSTRACT

This paper describes traditional EDI from a critical point of view and explains how XML could one day replace EDI in order to be used by SMEs to exchange business messages. Although it seems a simple task, EDI has faced many problems for the last 30 years that will be faced again by XML if we are not careful enough. So, more than explaining how XML can replace EDI, this paper focuses on the issues faced by that replacement and in particular the security issues that are of utmost importance.

1.1 Keywords

Data exchange, XML, EDI, Small and Medium Enterprises, SME, Electronic commerce.

2. INTRODUCTION

Electronic **D**ata **I**nterchange (EDI) was first introduced 30 years ago to exchange business messages between companies using teletext. EDI is composed by a set of standard business messages (such as order, invoice and so on) that companies exchange by electronic means instead of sending their equivalent in paper. Using EDI, companies can save greatly on paperwork. As a result, EDI has been adopted by some public authorities and many large companies (retailers, port authorities, auto makers and so on).

However, EDI has been introduced very slowly in SMEs. Price is surely a major factor, followed by the need for "configuring" EDI software that prevents EDI from being commodity software like a word processor. Probably another reason has to do with EDI software being old, cumbersome, and complex, thus expensive to operate.

On the other hand, there are many SMEs on the Internet. The Internet is used mainly in an ad-hoc (i.e. non-structured) way in order to exchange data using e-mail or ftp. Structured data interchange like EDI is much more powerful since it can be used to describe *business messages* effectively. However, EDI technology still remains to be introduced in SMEs and (if the past means anything) will not be introduced anytime soon.

There are three main reasons for replacing EDI with an Internet-based technology for exchanging data:

- EDI carries the stigma of being very expensive, complex to install and difficult to operate and so it is regarded as a technology for large corporations rather than SMEs;
- a solution based on standard Internet tecnologies will indeed be much more cheaper, easy to install and operate than its EDI equivalent; and
- it is unclear whether the messages that will be exchanged in the future are EDI standards or can even be standardised.

Public authorities and large companies would interact much better with SMEs if we could bring the benefits of EDI to these smaller companies by using popular, easy-to-use Internet technologies. By EDI we mean exchanging electronic business messages and thus achieving efficient relationships between companies without the cost and complexity of EDI. The benefits of EDI would then be available for the majority of companies.

In fact, we envisage that most of the EDI benefits enjoyed by large companies can be extended to the SME environment without using EDI at all. This objective can be achieved in four phases:

- prepare a "research path" to move existing EDI-based data exchange to an XML-based technology, including security and other EDI features;
- study what kind of messages are actually exchanged by modern companies and formalise those messages in XML;
- build a software prototype using only standard Internet technologies such as SMTP, MIME, HTTP, HTML and emerging Internet technologies such as XML and digital signatures; and
- stage a trial application with some SMEs to evaluate the prototype.

The main benefits from using a solution based on XML are those already enjoyed by large companies that exchange their business messages with EDI: no repetitive paperwork, faster communication, time and other savings, and virtually no errors. These benefits lead in turn to much more important benefits such as tight relationships with business partners and better integration of the supply chain. In principle, HTML could be used, although (as we will see in this paper) XML offers a much more powerful language for specifying business messages than could be achieved with plain HTML.

In this paper we will address only phase one because it is very important to understand the problems facing EDI in order to avoid repeating the same errors again. However, in our research work we have already started phases two and three.

3. DATA EXCHANGE AND SMES

In this section we explain why exchanging data containing business messages by electronic means is so important in general and even more important for SMEs.

3.1 Exchanging Messages as Data

Although a lot of progress has been recently made regarding information systems, state of the art in the business application area is that many, more or less isolated, applications have been implemented.

As a result, companies spend much of their time preparing information to be sent to other companies and registering information that has just arrived from other companies. For example, when something has to be bought, an order has to be created, printed, photocopied, put on an envelope and sent by surface mail. When an order is received, it has to be opened, introduced in the computer and sent to someone else. This process costs something between 5 and 50 ECU per order, depending on the company, but the main problem is really the time it takes – 15 days to process an order is not unusual. Using a digital order transmitted electronically, these numbers come down to something between 10% and 50% of the original values [1] [4] [8].

In order to be able to improve the performance of the supply chain as a whole, attention must be paid to the way companies *exchange messages* between them. This information determines the workload at the internal levels of the company but is also responsible for the exterior image of the company. Companies that process orders automatically and quickly can differentiate themselves for better, not to mention the savings on paperwork.

However, simply sending an e-mail with an order or an invoice is not enough. Someone would still have to read the mail and that would be only a relatively small improvement compared with a letter or a fax. *The electronic message has to be structured* in such a way that both computers (sender and receiver) know what is written where, and agree on what each field exactly means.

In the rest of the chapter we will see how EDI has tried to solve – without actually solving – this problem. But first we need to understand the most relevant business messages and why SMEs are so special.

3.2 Relevant Business Messages

Companies exchange many types of business messages - such as orders, invoices, designs, specifications, and so on - but these can all be grouped in two basic types of information:

- *administrative information* – concerning customer orders and other bureaucratic information needed to run the company on a daily basis, and
- *technological information* – that is based on what the company actually produces, makes, or sells, such as engines, groceries, etc.

Administrative information determines: *what* will be produced; *when* the final product must be delivered to the customer; *what* must be bought or sub-contracted from external suppliers and when it must be available. On the other hand, technological information specifies the detail that allows effective production to occur.

Both administrative and technological information are exchanged among each company and its customers and suppliers (see figure 1). Definition of due dates and prices arrive from suppliers. The company sends progress reports to its customers informing them about the status of their orders.

Specification of product characteristics may be defined by the customer, but might also result from interaction with resellers. Communication with sub-contractors may concern purchase orders of pre-defined (catalogue) products as well as sub-contracting production with particular specifications.

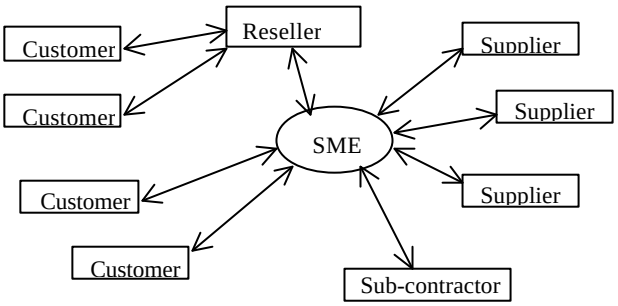

Figure 1: Relationship between an SME and other companies

EDI mainly addresses administrative information. However, certain industries (such as the automotive industry) have exchanged technological information by electronic means for many years without using EDI at all. This means that EDI cannot cover roughly half of the company needs for data exchange, a situation that has given rise to other competing standards such as STEP.

The conclusion to be taken here is that, although EDI addresses an important part of the data exchange needs for SMEs, there are still many types of business messages for exchanging technical information that are not covered by EDI. So any new proposal that aims at replacing EDI should take advantage of being new to also cover these other kind of technical messages.

3.3 The Special Needs of SMEs

Everyone agrees that SMEs are one of the most important parts of modern economies. There are at least 200,000 SMEs in Portugal, and several million in Europe. Today,

SMEs are seen as the fastest, cheapest and best way to create and maintain jobs, diversify production, and introduce innovation that Europe badly needs.

However, life for an SME is not easy in Europe. They have to fight against lack of venture capital, high tax levels, rigid labour market, high labour costs, government bureaucracy, and, on top of that, to fight against themselves and the competition of large companies, sometimes backed by the government – not to mention the government itself. In this business climate, any technological help is very welcome.

SMEs need to exchange business messages between themselves, and between them and other companies (clients, suppliers, etc) and/or the public authorities (tax service, social security, etc). This of course also happens with larger companies, but – due to their size – a proportionally larger part of their business has to be conducted outside the company. As a result, SMEs need to exchange relatively more messages with external organisations (e.g. accountants) and other people (e.g. lawyers) than their bigger rivals – which conduct most of their business in-house with specialised departments.

This situation will not change anytime soon because the obvious solution of integrating computer systems belonging to different SMEs is not an option. Companies love their independence and they want to know what is being sent to, and received from, outside the company. The only way to achieve better integration is to let information flow inside and outside the company by means of well-defined messages with well-defined recipients.

4. TRADITIONAL EDI

In this section we explain EDI and why EDI cannot solve the need for SMEs to exchange structured business messages.

4.1 Electronic Data Interchange (EDI)

EDI has been defined as "the transfer of structured data, by agreed message standards, from one computer application to another by electronic means and with a minimum of human intervention".

EDI was introduced more than 30 years ago and has been used since then to exchange business messages (orders, invoices, delivery, and so on) between large companies and their suppliers.

EDI offers a number of potential benefits:

- *Cost savings* – costs related with processing of (paper) business documents including envelopes, stamps, photocopying, and so on; time spent on gathering and collecting data, data entry, typing, archiving, etc; frequent errors produced when data is keyed in manually
- *Faster trading* – reductions in inventory; better cash flow; release of working capital
- *Strategic benefits* – greater customer satisfaction; improved supplier relations

On top of these general benefits, there are a number of other technical advantages:

- EDI is a well-known, standard data format;
- EDI is backed by large computer companies such as IBM;
- there are many EDI products available on the market such as EDI-TIE; and
- there are lots of companies around with know-how and experience.

So, in principle, SMEs could and should use EDI. Unfortunately, we have seen very little adoption of EDI by SMEs. In fact, it has been shown that, in each country, only the major retailers and their top suppliers actually use EDI. This means that SMEs only use EDI when they are coerced (or even forced) by their much bigger customers.

In Portugal, for example, this situation has happened with SONAE (the largest retailer) and AutoEuropa (the biggest Portuguese auto maker jointly owned by Ford and Volkswagen). A quick survey over a few mechanical industries working for AutoEuropa has revealed that not even relatively large SMEs use EDI. This is worrying, to say the least, since it has been rumoured with insistence that AutoEuropa helps and rewards those suppliers that use EDI. Overall, it is estimated that only 200 companies in Portugal use EDI from a total of more than 200,000 companies – less than 0,1 per cent!

4.2 Main Problems with EDI

Nobody really knows why SMEs were never enthusiastic about EDI – some people even suggest "psychological reasons" from a lack of a better argument – although there seems to be at least three important technological problems that will be described in this section: configuration, data alignment, and profiling.

4.2.1 Configuration

First and foremost, *EDI products are not "off the self" software packages* such as word processors or spreadsheets. They need to be *configured* before the company is able to send any EDI message. This configuration maps the fields on the internal database with fields on the EDI messages.

This means EDI cannot be "tried for 30 days or your money back" like most software. It also means that a consultant has to configure the software, something that takes time and becomes quite expensive.

4.2.2 Data alignment

The second problem is called the *data alignment problem* and is related with the actual data being exchanged, not the EDI message format. The problem is: even if two companies agree on a standard format for exchanging data, the numbers inside the message may still mean different things for different companies. Although it is

perfectly acceptable to agree on numbers between any two companies, this becomes more and more difficult (read expensive) when the number of customers and suppliers using EDI grows. It is also virtually impossible for "first time" or "ad-hoc" EDI relationships between companies such as those foreseen for electronic commerce.

The solution usually lies on brokers that do nothing else except publish standard data (numbers, codes, and so on). In Portugal, there is a company - called *Catálogo Electrónico de Produtos* - that provides this service [2]. There are similar companies in other countries, although these companies could easily provide international services as well. The "Catálogo" for example is trying to sell their services in Spain.

Using a proprietary interface (a Windows client application) companies that want to use EDI can register their products together with their EAN numbers – an international standard identification mechanism for products, companies, and locations. Other companies can then use the Catálogo to get the EAN number for each product they want to order. Without that number, the EDI message can still be sent, although in this case EDI looses many of its potential benefits since it has to be filled by humans in the sending side and interpreted by humans on the receiving side.

However, these brokers require even more EDI messages, are expensive to subscribe, somewhat awkward to configure and usually not integrated with either the EDI product or the internal database.

4.2.3 Profiling

A third problem – mostly neglected by EDI vendors and experts alike – is that EDI standards are too complex and make no sense before they are properly "adapted" or "specialised" to some specific industry or market niche. This problem is sometimes called "profiling" by the EDI community because this word suggests a good thing.

However, the problem is real and the reason is that most, if not all, EDI messages have far too many "optional" fields that can be (or not be) actually used when sending a message. So, before any exchange take place, the two partners have to agree which fields on that particular EDI message type they will actually use and how each one will be used.

This is like "a second standardisation process" that, like the first one, is better accomplished by some industry association or major partner. Otherwise, a partner would have to agree with every other partner how to "profile" each EDI message type.

For example, in Portugal the banks are now trying to send EDI messages between them – although mostly to support their clients payments needs, not theirs. But banks use at least three different numbering mechanisms to identify a bank account (internal, external and international).

In order to exchange information on bank accounts, they rely on SIBS (a company owned by banks to operate the national ATM network) to define what should actually go on each field (in this case, the bank account number) of EDI messages like CREMUL, DEBMUL, and PAYMUL. As a result, SIBS has published a document with dozens of pages specifying exactly what should go in each field for each message. This is quite interesting, as these messages were supposed to be standard already…

4.2.4 Other Problems with EDI

These three problems described above would be relatively easy to tackle if not by many other, smaller but annoying, problems found with all EDI implementations.

- EDI is relatively expensive for an average SME to buy and configure – 10,000 ECU is typical for an up-and-running EDI installation, although sometimes EDI vendors prefer to sell it cheap to make much more money later on selling communication facilities (see next bullet).
- EDI is even more expensive to operate since proprietary VAN-based messaging technology is terribly high-priced, e.g. compared with the Internet.
- EDI may require technical expertise to operate on a daily basis.
- EDI has a terrible reputation of being designed and useful only for large companies with lots of orders (so the investment on EDI has a quick ROI).
- EDI is based on legacy, previous generation, expensive technology (such as X.400 and X.25) and not based on open, available, cheap, modern, popular technologies (such as Internet, CORBA, ODBC, etc).
- EDI cannot be easily extended with modern "add-ons" like multimedia data, digital signatures, digital certificates, electronic payment technologies, and so on.

Given this large set of difficulties – not only technical and economical but also psychological and historical – we hope it is now obvious for everyone why SMEs have been so reluctant to adopt EDI.

4.3 "Modern EDI" Is Not Enough

Fortunately, the problems described above with EDI technology and its use have been recognised by the EDI industry, not the least because they have been unable to sell their EDI products and services. (We know of at least two cases in which the companies involved have sold *no* EDI products over a number of years.)

As a result, there have been several attempts to what we generally call "modernising EDI". These efforts mainly try to give new "packaging" to EDI, a technology that is typically recognised as being very difficult to sell. Examples include Lite EDI and XML/EDI, presented below as representatives of these efforts, but there are many others.

4.3.1 Lite EDI

It has always been argued by the EDI community that a key for EDI popularity is *simplification* – thus implicitly assuming that EDI is too complicated. Lite EDI [6] is just a simpler form of EDI based on the Internet with six main differences from traditional EDI.

- EDI is still regarded as the basic foundation but now seen only as a technology – not a final ready-to-use tool.
- A company does not need to change its internal processes and practices to take advantage of Lite EDI – so there is no need for configuration.
- Lite EDI only uses a core set of messages from the original EDI standard, and within each message only a core set of data – so there is no need for profiling.
- Lite EDI proposes a "simplified interface" that happens to be just a formatted computer screen (called an "EDI Form") for each standard message so that a company can use Lite EDI just by entering data on the screen.
- Lite EDI uses the same EAN numbering system as EDI, as this standard forms the basis for companies understanding each other – so there is no need for data alignment.
- Lite EDI can use any one of the following communication media: modem, X.25, X.400, VAN or the Internet (a low-cost solution).

The most important benefit, however, is not even explicitly stated: Lite EDI provides an opportunity for large companies to use EDI with all their trading partners, not only other large companies or SMEs that were "forced" to implement EDI by their much larger partner. This is achieved by providing an interface – potentially on the Web – to those users that directly accesses their internal EDI systems.

Although at first glance it seems a great idea, we believe SMEs will be worse off with Lite EDI if all factors are carefully taken into account.

If one removes all the buzzwords, Lite EDI actually means that smaller companies will have to use their partner's EDI products remotely via a client/server application or directly on the Web, maintaining no data whatsoever related with EDI locally in their internal systems. This in turn means that someone – that is, an expensive, slow, error-prone human being – will have to type in (letter by letter, errors included) the data for every outgoing business message. The opposite is also true: for every incoming message, someone will have to read the message's data and either print it or copy it onto another computer form.

All this means that Lite EDI is great for large companies that already use EDI with some of their suppliers since they now can use EDI with their smaller suppliers as well.

But for small suppliers it means very little, because:

- SMEs will have to type or read manually all EDI data;
- SMEs will have to use a different interface for each EDI-enabled customer, and
- SMEs will have to pay the communication costs.

It may be even worse for SMEs because they may have already an internal computer system that they used to print messages automatically. Now they have to retype the message again. For many SMEs, Lite EDI will be seen as only another way for large companies to push costs onto their suppliers with no obvious savings for them, making it even more difficult for them to compete with bigger companies that can afford to pay for proper EDI.

4.3.2 XML/EDI

Another popular technology that has been evolving from EDI is XML/EDI [12] proposed by the XML/EDI Group. XML is well positioned to replace HTML as the standard language to format data on the Internet (see below). On the other hand, XML/EDI is backward compatible with EDI, meaning that companies already using EDI will be able (in theory, at least) to use XML/EDI.

At first glance, it seems that XML/EDI is the best of both worlds. However, XML/EDI is not an application, it is a "framework to provide open solutions for electronic business scenarios". Four "core models of use" have been identified – star, ad hoc, hybrid and web – each with its own "requirements and goals". The overall goal of the XML/EDI framework happens to be only "to provide interfaces between components" for electronic commerce. It has also be rumoured that Microsoft is behind the XML/EDI group, not a popular supporter these days (although Microsoft is also strongly pushing for XML).

In one sentence, XML/EDI is not a concrete technology, it is an idea, and it should not be taken seriously for the time being. But having said that, the XML/EDI group does offer an appropriate environment on which EDI, XML, and their related technologies can and should be discussed.

5. AN XML-BASED PROPOSAL

We propose to use XML as the basis for exchanging business messages between SMEs and their business partners. However, EDI can still be used as a source of inspiration and to integrate SMEs with legacy information systems.

A general messaging mechanism for SMEs based on XML should incorporate all the traditional EDI benefits without carrying any of its historical difficulties. In order to achieve this ambitious objective, we need to keep the basic EDI functionality, get rid of the problems, understand the main technical issues, then utilise only novel, open, Internet-based technologies and finally run an application trial to show that it really works for real SMEs in a real case study.

This paper, however, addresses only the first part: the problems with current EDI technology and the issues involved for an XML-based approach.

5.1 Introduction to XML

XML is basically a subset of SGML, the language that gave origin to HTML. SGML is a standard language to structure documents that contain both content (data) and structure (how it is organised) information. Each SGML document is composed by two parts:

- a DTD (document type definition) – a specification for a class of documents, e.g. an order, an invoice, a health record, and so on; and
- an instance of that DTD – a concrete document that may be used, for example, to actually order something.

HTML is defined in terms of an SGML DTD in which the meaning for tags like <TITLE> and <H1> were specified once and forever by its original creator. This is simple and effective, and has been seen as the main reason for the popularity of HTML. However, since all HTML documents belong to the same DTD, they all belong to the same document class as well. This means there is no way in HTML to separate orders from invoices, for example. It is like storing all data types as strings, we loose the benefits of strong typing.

Unlike HTML, XML is a subset of SGML. Using XML, it is possible to define arbitrary document classes and create instances of that classes.

XML is not "just another standard" since it was proposed and is being pushed by the World Wide Web Consortium [14]. Microsoft is also strongly supporting XML, while Netscape and other well-known Internet players are also backing XML. The new Internet Explorer 4 has already a C++ XML parser built-in and Microsoft has also made publicly available on their web pages another XML parser written in Java. Microsoft has also said the next version of Office will read and write XML documents in addition to their proprietary formats.

In general, there is already no lack of decent XML tools and many more are being made available every week. The market will explode once XML evolves from a real standard *de jure* to become a standard *de facto* as well, something that will happen in the next 2 years. The interested reader is referred to the following references for more information on XML and its applications: [9] [10] [11] [13] [15]. Much more material is available on the Web.

5.2 Advantages of XML over EDI

XML has a number of advantages compared with EDI as a formatting language to be used for exchanging business messages on the Internet.

- *Price* – XML is much cheaper to use then EDI because there are many (and there will be many more) products, tools and browsers that are able to understand (i.e. read) XML and translate to (i.e. write) XML.
- *Visibility* – XML is highly popular already and will probably become even more. XML will eventually replace HTML as the ubiquitous language to describe, transmit, and store documents on the Internet. For example, there are already XML compilers publicly available, specialised databases for storing XML documents, and so on.
- *Extensibility* – XML can be easily extendable with complementary technologies such as digital certificates, digital signatures, electronic payment mechanisms, multimedia data, and other features.
- *Flexibility* – XML can be integrated with modern technologies such as digital certificates and script agents that will dynamically extend the basic XML functionality on demand with security, reliability, intelligence, and so on.
- *Semantics* – XML can incorporate much higher-level functionalities than simple data, for example, formatting information (for several printing/translating media such as browser, paper, CD-ROM, mobile phone, etc) and Java programs (for virtually any kind of functionality desired).

For all these reasons XML is a much better alternative than EDI for exchanging business messages between SMEs and their business partners.

Of course, we need to define DTDs for business messages, but here we can build on top of the current EDI expertise and in the process attempt to solve its problems: configuration, data alignment, and profiling. This is the theme for a forthcoming paper.

5.3 Converting EDI to XML is not enough

From what we have said above, it follows naturally that XML could be used instead of EDI as the basis for exchanging business messages between companies. In fact, there are already efforts to design standard XML document types (DTDs) based on standard EDI messages: both the XML/EDI Group and the Open Trading Protocol (OTP) Consortium are attempting to translate current EDI formats to XML.

However, there are many reasons why simply re-defining EDI in terms of XML cannot be considered good enough.

- EDI is an old technology, so just translating EDI to XML does not take into account what happened in the last 30 years in terms of economic, business, technological, and psychological evolution.
- It may not work well for SMEs simply because EDI was designed for large companies and has certainly been evolving based on the requirements for large companies.
- EDI has a core set of messages but has been specialised in several vertical markets (transport, customs, finance, construction, statistics, insurance, tourism, health care, and social administration) that are not necessarily those sectors where most SMEs operate.

- EDI cannot be easily extended with "modern needs" such as those necessary for security, payment, signatures, multimedia, and so on.

5.4 What then should be done ?

We could and should take advantage of this "paradigm shift" – from expensive proprietary communication systems to the cheaper open Internet – to really modernise EDI in ways that will make it suitable for SMEs as well as large companies and public authorities.

In particular, we should take special care with the three most important problems described above in Section 4.2 that cannot be solved by simply re-packaging the old EDI mechanisms in XML.

- *Configuration* – how to map the EDI message to the internal database.
- *Data alignment* – how to agree on the data (codes, numbers, etc) being exchanged.
- *Profiling* – how to make sure that all partners actually use the same fields on each message, with exactly the same meaning.

These issues will have to be properly addressed in order to avoid ending-up with the same problems found in EDI. Although this paper does not address these problems, we are currently working on them and expect to report on proposed solutions very soon.

There are also other, more up-to-date, issues that should also be taken into account.

- How to *make data exchange safe and secure* so that people will trust the technology for sending their sensitive data over the open Internet ?
- How to *promote awareness of information technology* so that *all* SMEs will have access to the benefits of electronic communication with other companies ?
- How to make the whole service *easy to be understood and to be used* by people that are not necessarily computer literate ?
- How to make it so cheap that *price will not be a determinant factor* whether to use or not use structured messages ?

In the rest of this paper we will concentrate on the first topic and leave the others for subsequent papers.

6. SECURITY ISSUES

In every system that manages data in an electronic format, and in particular those connected to the Internet, many potential threats have to be faced. This means that *security mechanisms* have to be put in place to prevent, or at least detect, security attacks. These mechanisms aim at assuring different *security services*, and in our case we are especially interested in the following services below.

Integrity – Protection of the information being transmitted, preventing accidental or malicious data modifications.

Confidentiality – Protection from information disclosure by unauthorised parties.

Authentication – Proof of identity of each party involved in a transaction.

Non-Repudiation – Protection from the risk that a party could deny the participation on a given message transmission process. Non-repudiation can then be sub-divided into three kinds of more specific services:

Origin – if the creator of a message cannot deny its authorship;

Submission – proof that a message was sent at a particular date and time; and

Delivery – proof that a message has been delivered to the intended receiver.

Although these generic security services apply to all data in an electronic format, in this paper we are particularly concerned with data that represents business messages being exchanged between business partners.

6.1 EDI Security

The current security model for EDI transactions is mostly based on the security services offered by the VANs, and in particular by the X.400 mail system that is typically used to transport EDI messages. Since this technology seats among those that we identified as responsible for the failure of EDI, an XML-based system cannot rely on the security provided at the OSI transport level. Lower-level security systems such as SSL could help in securing business transactions, and in particular to ensure privacy. However, the challenge is to design a much more flexible and powerful security framework working at the document (read business message) level.

The EDI security standard X12.58 proposed by the Data Interchange Standards Association [5] already defines measures to protect documents according to their structural classification. However, this classification is based on the notions of *transaction set* (a complete business document, such as an invoice) and *functional group* (categories of business or activities). In other words, the X12.58 standard provides a framework for defining the security policies to be applied e.g. to invoices in the automotive industry or to health records in the health care industry.

As we will explain later, it is more convenient to consider a smaller granularity while defining the protection to be applied – instead of using entire documents. That should not be limited to a selection of the fields that need to be protected e.g. to decide whether personal data has to be protected (or not) depending on the fact that the person is the buyer of a car or a patient in a hospital. Security has to be much more flexible than that: personal data may have different security requirements, depending on the context in which it is used.

6.2 Embedding Security in XML Documents

The security services mentioned above are all relevant for exchanging messages on the Internet, particularly those messages used in business environments. So if we aim at replacing EDI with an open messaging mechanism we should provide those security services for exchanging XML-based business messages.

We propose to take advantage of the structuring capabilities supported by XML and use them to embed security functionalities into the document itself.

There is already lots of research work being carried out in this field, namely the *Signed Document Markup Language* (SDML) proposal [7] by the Financial Services Technology Consortium. The SDML technology enables the insertion of digital certificates and digital signatures into the business documents themselves. The signatures can then be verified by recipients or other third parties, thus providing integrity, authentication and non-repudiation of origin.

SDML defines its structure based on SGML – an approach similar to that of XML which is also based on SGML. In fact, recognising the XML popularity, it is intention of the FSTC to design future SDML evolution to be XML-compliant. Thus, we may find SDML facilities embedded into XML documents in the near future.

On the other hand, it should be noted that, among the security services listed above, confidentiality is absent from SDML. This is strange because it seems relatively easy to provide confidentiality simply by encrypting the document blocks with random symmetric keys, and sending these keys encrypted with the recipient's public key. All these fields could be structured according to some pre-defined DTD.

Finally, non-repudiation deserves a little more discussion. In particular, both non-repudiation of submission and non-repudiation of delivery are only possible through *message transfer agents* (MTA) such as those available in electronic mail systems. The MTA on the sender's side digitally signs a message, providing a proof that the message was submitted (which is the end of the sender's responsibility regarding the message delivery process). On the receiver's side, the MTA is able to provide a proof that the message was delivered.

Without this kind of agents, it would be very difficult to provide those proofs, if not impossible at all. Unless the XML messages are transmitted through e-mail – or, for this matter, any other kind of protocol with an intermediary – there is no way to provide non-repudiation of submission and delivery. The important conclusion here is simple: it is not possible to provide this kind of non-repudiation guarantees with document structuring alone.

6.3 Security Infrastructures

The mechanisms needed to implement the security features described above have to be as cheap as possible to SMEs. They are not ready to pay for services on top of a basically free Internet, neither they have money to pay for exchanging messages.

As we said above, we should not rely on security services provided by the message transport mechanisms because they are too low level. Instead, we should use mechanisms to enable security at the message level.

We propose to use cryptographic software and, depending on the algorithms chosen, a public-key infrastructure (PKI) may be needed. Managing the PKI needed for safely and securely exchanging XML business documents could be a service provided by several entities e.g. a PKI has been established for enabling SDML.

Cryptographic software is not among the cheapest classes of software products. It may even represent one of the most expensive elements for building a package to enable XML-based message exchange for SMEs. Nevertheless, its costs are still orders of magnitude lower than those for an average EDI software. And this cost will come further down as soon as cryptography gains momentum for generalised security in human-generated mail messages.

On the other hand, even cheaper technologies may be used to implement cryptographic software. PGP is an example of such a technology because it does not require the set up of any PKI – it is based on trust relationships established directly between business partners.

Another relevant issue has to be considered: the constraints on cryptographic algorithms imposed by several governments. Due to these limitations, the security mechanisms should find an acceptable choice among the available cryptographic technologies (algorithms and key lengths) during business transactions involving foreign partners. The same mechanisms can be used to select the available technologies to be used when dealing with small companies that may not be able to afford the most expensive software packages.

6.4 Security and Transmission Efficiency

The EDI standard already offers a "security framework" with a concept called *security context* ???in which data is separated according to their sensitivity. This approach is also applied to the connections and the messages used to transfer critical business data. But there is a limitation: all data transmitted through the same connection, or within a message, have the same sensitivity.

The flexibility provided by XML allows the inclusion of *sensitivity tags* applied to individual elements so that one XML message may contain several data items with different security requirements. For example, one item may be digitally signed, while another may be encrypted, and still another is both signed and encrypted, all this according to specific requirements for integrity, authentication, non-repudiation and confidentiality.

The ability to process these tags and its intrinsic flexibility avoids the need to open multiple connections, one for each sensitivity level. On the other hand, one single message is able to carry all data, instead of composing one message for each sensitivity level. Furthermore, considering that data belonging to different transactions should not be mixed, the problem becomes even more relevant.

Let us consider two transactions, each one defining three elements with three different sensitivity levels. Their safe and secure transmission on EDI would require opening as much as six connections, or composing six messages. On the opposite side, using an XML-based mechanism would require only one connection with two messages. And using a more convenient document structure, only one message would be enough. Managing security at the structure level, instead of doing it at the transport level, increases both flexibility and efficiency in a significant way.

7. CONCLUSION

We started the paper with a brief motivation to explain why exchanging business messages on the Internet is important for SMEs. We then presented why EDI cannot be used by SMEs for exchanging business messages on the Internet and proposed an XML-based approach. The paper also includes a discussion on the security issues involved, one of many topics that should be addressed if XML is supposed to replace EDI in the long term.

As future work in this area, we will continue working on EDI and XML-based data exchange for SMEs as well as related research such as databases and mobile agents. In particular, the areas that will are being addressed include:

- building a product catalogue with an EDI interface (to understand better how EDI behaves in a real case study),
- defining relevant business messages such as order and invoice in XML (phase two in the introduction) and
- designing and implementing a prototype for safely exchanging structured messages by electronic mail (phase three in the introduction).

We hope one day SMEs will be able to exchange business messages and take full advantage of the benefits enjoyed by large companies, such as spending 10% or less for each invoice sent electronically instead of paper.

8. ACKNOWLEDGEMENTS

This research work was carried out in the scope of the COSMOS project, an electronic commerce project partly funded by the ESPRIT Programme of the European Union.

9. REFERENCES

[1] Debra Cameron, Electronic Commerce: The New Business Platform for the Internet, Computer Technology Research Corp, First edition, 1997.

[2] Catálogo Electrónico de Produtos. http://www.-catalogo.mailcom.pt/

[3] P. Christmas. EDI Implementation and Security. Elsevier Advanced Technology, Oxford, UK, 1994.

[4] Soon-Yong Choi, Dale O. Stahl, and Andrew B. Whinston, The Economics of Electronic Commerce, MacMillan Technical Publishing, 1997.

[5] Data Interchange Standards Association. X12.58 Security Structures. 1998.

[6] EAN International, Position paper on Lite EDI, 1998

[7] Financial Services Technology Consortium. SDML – Signed Document Markup Language (V2). 1998. http://www.fstc.org/projects/sdml/sdml_det.html.

[8] David R. Kosiur, Understanding Electronic Commerce, Microsoft Press, 1997.

[9] R. Khare, A. Rifkin. XML: A door to Automated Web Applications. IEEE Internet Computing, Jul/Aug 1997.

[10] W. Lamersdorf and M. Merz. Trends in Distributed Systems for Electronic Commerce. Proceedings of the International IFIP/GI Working Conference (Hamburg, Germany, June 1998). Lecture Notes in Computer Science Vol. 1402, 1998.

[11] NetLingo: XML FAQ. http://www.netlingo.com/-more/xmlfaq.htm

[12] Bruce Peat and David Webber, Introducing XML/EDI, The XML/EDI Group, 1997. http://www.geocities.com/ WallStreet/Floor/5815/-start.htm.

[13] Simon St. Laurent. XML: A Primer. MIS Press. 1998.

[14] World Wide Web Consortium. Extensible Markup Language (XML). 1998. http://www.w3c.org/XML/

[15] Using XML for Electronic Commerce. 1998. http://-www.xmledi.com/book.htm.