Sachar Paulus, Norbert Pohlmann, Helmut Reimer (Editors)

Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe Conference 2003

Preface

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by EEMA and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar. The aim of ISSE is to support the development of a European information security culture and especially a cross-border framework for trustworthy IT applications for citizens, industry and administration. Therefore, it is important to take into consideration both international developments and European regulations and to allow for the interdisciplinary character of the information security field. In the five years of its existence ISSE has thus helped shape the profile of this specialist area.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- Jan Bartelen, ABN AMRO (The Netherlands)
- Ronny Bjones, Microsoft (Belgium)
- Alfred Buellesbach, DaimlerChrysler (Germany)
- Simon Corell, Corell Consulting (Sweden)
- Marijke De Soete, Mastercard (Belgium)
- Danny de Temmermann, CEC DG INFSO
- Jos Dumortier, KU Leuven (Belgium)
- John Hermans, KPMG (Netherlands)
- Jeremy Hilton, EEMA (UK)
- Dave Hobart, EEMA (UK)
- Patrick Horster, University of Klagenfurt (Austria)
- Dimitris Karagiannis, University of Vienna (Austria)
- Matt Landrock, Cryptomathic (Denmark)
- Gabriel Neagu, National Institute for R&D in Informatics - I.C.I. (Romania)
- Karel Neuwirt, The Office for Personal Data Protection (Czech Republic)
- Sachar Paulus, SAP (Germany)
- Norbert Pohlmann, University of Applied Sciences Gelsenkirchen/TeleTrusT (Germany)
- Reinhard Posch, TU Graz, (Austria)
- Bart Preneel, KU Leuven (Belgium)
- Helmut Reimer, TeleTrusT (Germany)
- Paolo Rossini, TELSY, Telecom Italia Group (Italy)
- Ulrich Sandl, BMWA (Germany)
- Wolfgang Schneider, Fraunhofer Institute SIT (Germany)
- Robert Temple, BT (United Kingdom)

Many of the presentations at the conference are of use as reference material for the future, hence this publication. The contributions are based on the presentations of the authors and thus not only document the key issues of the conference but make this information accessible for further interested parties.

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Sachar Paulus *Norbert Pohlmann* *Helmut Reimer*

EEMA (www.eema.org):

For 16 years, EEMA has been Europe's leading independent, non-profit e-Business association, working with its European members, governmental bodies, standards organisations and e-Business initiatives throughout Europe to further e-Business technology and legislation.

EEMA's remit is to educate and inform around 200 Member organisations on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and re-ports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its Members is available to other members free of charge.

Examples of papers produced in recent months are:- Role Based Access Control – a User's Guide, Wireless Deployment Guidelines, Secure e-Mail within the Organisation, The impact of XML on existing Business Processes, PKI Usage within User Organisations. EEMA Members, based on a requirement from the rest of the Membership, contributed all of these papers. Some are the result of many months' work, and form part of a larger project on the subject.

TeleTrusT (www.teletrust.de):

TeleTrusT was founded in 1989 to promote the security of information and communication technology in an open systems environment.

The non-profit organization was constituted with the aim of:

- achieving acceptance of the digital signature as an instrument conferring legal validity on electronic transactions;
- supporting research into methods of safeguarding electronic data interchange (EDI), application of its results, and development of standards in this field;
- collaborating with institutes and organizations in other countries with the aim of harmonizing objectives and standards within the European Union.

TeleTrusT supports the incorporation of trusted services in planned or existing IT applications of public administration, organisations and industry. Special attention is being paid to secure services and their management for trustworthy electronic communication.

Table of Contents

Strategy

Technology

Application

Practice

Strategy

A Quantitative Decision Support Model for Security and Business Continuity Management

Rolf von Roessing

Ernst & Young Austria
rolf.von-roessing@at.ey.com, rvr@scmltd.com

Abstract

Risks and the business impact of a critical event are often difficult to quantify. In many cases, the strategic decisions with regard to mitigating risk and minimising financial damage must be taken on the basis of qualitative estimates and expert opinion. However, formulating a continuity and security strategy requires quantitative support across several dimensions: temporal, financial and systemic thresholds must be defined to ensure the optimum level of investment. The paper outlines a strategic decision support model for quantifying risk and business impact. It is further shown how the resulting risk management decisions of the firm can be optimised, and how typical problems of event (disaster) frequency and severity can be resolved. The paper builds on earlier research in audit, insurance and business continuity management to present an innovative approach towards this well-known problem.

1 Introduction

Modern information security and business continuity significantly depend upon an initial risk and business impact assessment. Adverse events as well as critical situations represent risks to an organisation, and they strongly influence the subsequent investment decision in security, disaster recovery, emergency planning and business continuity programmes. The term "risk" as such has been subject to various definitions, often including the notion of "event" and "consequence" as well as risk in the proper sense of the word. Traditional risk analysis and evaluation relies on quantitative and qualitative methods. While the former attempt a reasonable degree of quantitative accuracy by including probabilistic estimates and frequency distributions, the latter seek to leverage the experience of experts and other subjective input to form an overall picture of the risks identified in the process. Existing business impact assessment techniques, on the other hand, are a means of estimating the damage resulting from the fact that one or more risks have materialised, causing some sort of disruption to the organisation.

Traditional literature on risk appears to be preoccupied with managing risk rather than analysing it, usually in a portfolio-type approach. The insurance perspective on risk [Brüh94, Dohe00, GaGM97, Poll01] – one specific risk is shared among many entities – is less useful for the organisation or company having to identify and analyse risks to its own assets and processes, quite simply because the existing risks cannot be "shared" across many business entities, in a manner often suggested by risk management models [Imbo83, Roes01]. Indeed, the managerial aspect of reducing or transferring risk may not be valid if no clear data exists on how frequent the risk-related events are and what their significance is to the organisation or company being reviewed. Similarly, formalised risk transfer may fail [Lind86] where the entity transferring (company, government or other) is perceived as having ultimate responsi-

S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 3-20

bility for an event and its consequences [UK02]. This is often the case where stakeholders or the public at large focus on international companies or governments in terms of moral obligation and reputational damage [SmIr84].

Business impact, on the other hand, is seen as an ex post tool that determines the actual damage caused by an adverse event or disruption. While it can be used in an ex ante sense, it is rarely implemented to serve its original purpose: forward-looking risk management.

Both risks and business impacts impinge on investment strategy and budgeting [Neub89, Schl98, YoKo01], inasmuch as they influence resource allocation to certain risk reduction or impact reduction measures. Given that the financial resources available are limited, risk reduction and impact reduction form part of the strategic planning process within the organisation. In this sense, they can no longer be seen as low-priority projects that are implemented by choice rather than necessity: if a risk emerges as a going concern issue, meaning that it may threaten the existence of the company as a whole, its immediate reduction, transfer or elimination is in the interest of the firm and therefore essential. Recent developments suggest that the notion of good corporate governance [CodG02, CodÖ02] includes the ongoing analysis of such risks and business impacts that may endanger the company [WoRu00] or its sound financial background and viability. Furthermore, the discussion of "operational risk" [BIS03, BIS03b, DEGK01, EmKS02] has broadened the perspective on risk in general and given specific examples of what may constitute a risk to day-to-day business, at least in the financial sector. Regulatory pressure and formalisation of "risk" as a technical term are therefore progressing, and any current and future analytical or empirical models will have to consider the new, wider sphere of business risk instead of restricting themselves to the field of information technology.

2 Problems

2.1 Risk, Events, Consequences

Both risk evaluation and business impact assessment are subject to known problems that are, at first sight, difficult to resolve. The initial problem arises from the technical term "risk" as such, as this is often erroneously interpreted as "event" or "consequence". The term as used in this paper denotes the probability of something (an event) happening, regardless of the immediate consequences. A risk manifests itself as an event, and the immediate consequences of this event will determine the impact. Again, the word "risk" often encompasses the notion of adverse consequences and negative impacts. Conversely, the word "opportunity" will be used where the very same event will lead to positive consequences as perceived by the firm. Practically speaking, an event is often experienced as a risk by one or more firms, whereas other companies (their competitors) make the most of it by turning the event into an opportunity.

"Risk" is therefore often used subjectively and as a collective term that includes:

- the (estimated) probability of an event happening
- the fact that this event will have negative consequences for the firm
- the fact that there is a causal relationship between event and impact

This empirical use of the term appears impractical. It requires a more differentiated and more objective treatment prior to applying formal methods to it. It will be shown that reversing the deductive chain of "risk – event – consequence" yields a more objective and impartial basis for quantification when seen from within the company.

2.2 High-Impact, Low-Frequency Events

When analysing extraneous events and their likelihood in a quantitative manner, the typical "high impact, low frequency" (HILF) events often encountered in real life are difficult to predict in the absence of meaningful statistics. However, it is the HILF event – a scenario of widespread disruption, catastrophic events, and massive damage to the environment – that is invoked much more often than the smaller event, due to psychological reasons [Linn01]. Likewise, a constant trickle of small but costly events is seen as less threatening than a single HILF event [KaTv79].

Hence, techniques have been developed to estimate rather than calculate such risks. However, this inevitably reduces the accuracy of the end result, and it has become popular wisdom that, since some events cannot be anticipated, the quantitative risk analysis approach in itself is rejected for corporate use. It has also been argued that an event that may occur once in a hundred years cannot be considered within the scope of "normal" risk analysis due to cost restrictions and the overall level of plausibility. Hence, the qualitative approach towards risk identification and evaluation has been favoured both in literature and corporate management [Krei97, Küpp97, Pepe94].

This subjective approach pre-empts reality by excluding a whole class of events, although they might still happen at any moment in time, albeit with a limited probability. It is nevertheless characteristic of current management practices that risks and impacts will be "defined out" of the model when they appear to be unmanageable. In other words: if you cannot swim, you will deny the existence of water in order not to be too scared. The "bounded rationality" problem has been known at least since 1957 [Simo57], and has received extensive theoretical attention since then [Turn76]. In order to define the problem for the purposes of this paper, it is subdivided into the following steps or stages:

- Adverse events of a HILF nature exist; by definition, these events are big or damaging enough to potentially endanger the existence of the business, but their probability is low
- Low probability is conducive to "taking a gamble"
- High impact (often catastrophic) induces simplification and "bounded rationality"
- Risk analysis and management activities are restricted to manageable risks
- Correlated HILF events are ignored
- Reality is – in the final stages of this process – adapted to the wishes and prerogatives of senior corporate management: risk-related thinking is subject to "tunnel view" narrowing

Conversely, if HILF events are being recognised as inevitable, their likelihood and the consequences for organisations or firms are often misunderstood. As a result of limited empirical data, high-impact events rarely lend themselves to quantitative analysis. Hence, qualitative estimates are applied to such events, and subjective perception of an event will often dictate its subsequent managerial treatment. An extreme example is the round table discussion where events will be considered qualitatively and as a function of hierarchy: the most important risks are those that the CEO is most afraid of. While this is a deliberately controversial example, it nevertheless demonstrates the fallacies of subjective (qualitative) risk analysis [BaCo96, Neub89]. Qualitative assessments have been further challenged on grounds of misperception [Renn01, Renn84, SBCC00]: regardless of experience, it is likely that people will overestimate the impact and severity of HILF events whilst underestimating high-frequency, low-impact events such as day-to-day accidents.

Technology

Trends in Cryptology Research

Bart Preneel

Katholieke Univ. Leuven, Dept. Electrical Engineering-ESAT/COSIC,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Abstract

Cryptology is an essential building block for any IT security solution. In the past decades, cryptology has evolved from a secret art to a modern science. Political controls of cryptography have diminished substantially, crippled algorithms are disappearing, and secure and efficient cryptography is becoming more and more a commodity. This may lead us to believe that the cryptography problem is "solved." However, this article will show that there are still many challenging problems ahead of us in the area of cryptographic algorithms. We will discuss the increasingly powerful attacks on implementations that are based on side channels, faults and errors (the recent SSL problem), but also the more fundamental problems such as the conjectured difficulty of factoring and the progress of quantum computers. Part of the work discussed in this paper is based on the STORK (http://www.stork.eu.org) and NESSIE (http://www.cryptonessie.org) projects.

1 Introduction

While cryptology is getting increasingly important in the information society, it is also becoming less and less visible. Cryptology has been integrated into smart cards for financial transactions, web browsers, operating systems, mobile phones and electronic identity cards. This may give the false impression that cryptography is a research discipline that has ran out of practical problems and that should be left over to theoreticians who can keep trying to solve the question whether or not one-way functions exist. While our intuition seems to suggest that it is very straightforward to design a function that is "easy" to compute but "hard" to invert, so far the best theoretical result can prove that there exist functions that are twice as hard to invert as to compute [Hilt92]; it is clear that such functions would be completely useless to cryptology.

Most of the applications are covered by the block ciphers DES and triple-DES [FI46], the hash function SHA-1 [FI180-2] (in some applications RIPEMD-160 [DoBP95]) and RSA [RiSA78]. In addition there are a number of proprietary algorithms in GSM (A3/A8, A5/1 and A5/2 [BiSW00,Vedd91]) and the stream cipher (`alleged') RC4[1] which is widely deployed for SSL/TLS; recent results cast some doubts on the security of the key setup of RC4 [FlMS01,MaSh02].

What we will try to explain in this article is that there remain many challenging problems in practical cryptography.

[1] RC4 is claimed to be a trade secret of RSA Security Inc.

S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 51-58

2 New Algorithms and Standards

This section will briefly discuss the recent algorithms proposed by NIST (National Institutes for Standards and Technology), ETSI (European Telecommunications Standardisation Institute) and the research project NESSIE (New European Schemes for Signature, Integrity and Encryption).

2.1 NIST

Even if triple-DES offers a security level of 80 bits (which means that even a well-funded opponent would take more than 10 years to recover a key by exhaustive search), this will not be sufficient for long term security (15 years or more). Moreover, the performance of triple-DES is not very good (115 cycles/byte on a Pentium III) and the block length of 64 bits implies that at most 2^{32} blocks can be encrypted under a single key in the common modes due to the birthday paradox.

In 2001, NIST has published the AES (Advanced Encryption Standard) [DaRi01,FI197], which offers a high security level (key lengths of 128, 192 and 256 bits and block length of 128 bits) and a much better performance (15 cycles/byte).

The security level of SHA-1 against collisions is also limited to 80 bits. In 2002, NIST has published new hash functions SHA-256, SHA-384 and SH-512 [FI180-2] which offer a security level of 128, 192 and 256 bits, matching the AES key sizes. In contrast to AES, these new hash functions are substantially slower (21-40 cycles/byte) compared to SHA-1 (8 cycles/byte).

2.2 ETSI

In 2000 ETSI has published the block cipher KASUMI that will be used in 3GPP/UMTS, which was a substantial change of policy. KASUMI is a 64-bit block cipher with a 128-bit key, that is a slightly simplified version of the block cipher MISTY1 (published in 1996). In July 2002 ETSI has also announced A5/3, a variant of KASUMI, that will replace A5/1 and A5/2. Weaknesses of A5/1 and A5/2 have been reported for example in [BiSW00] and [BaBK03] respectively.

2.3 NESSIE

NESSIE (New European Schemes for Signature, Integrity, and Encryption) [NESSIE] is a research project within the Information Societies Technology (IST) Programme of the European Commission. NESSIE is a 40-month project, which started in January 2000. The goal of the NESSIE project is to put forward a portfolio of strong cryptographic primitives that has been obtained after an open call and been evaluated using a transparent and open evaluation process. In February 2000, the NESSIE project has launched an open call for a broad set of primitives providing confidentiality, data integrity, and authentication. These primitives include block ciphers (not restricted to 128-bit block ciphers), stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption schemes. In September 2000, more than 40 primitives have been received from major players in response to the NESSIE call. Two-thirds of the submissions came from industry, and there was some industry involvement in every 5 out of 6 algorithms. During 12 months, a first security and performance evaluation phase took place, which was supported by contributions from more than 50 external researchers. In September 2001, the selection of a subset of 26 primitives for the second phase has been published. In February 2003, the portfolio of recommended NESSIE

primitives has been announced. It contains the following 17 algorithms (twelve of these are NESSIE submissions and five have been selected from existing standards):

- block ciphers: the 64-bit block cipher MISTY1, the 128-bit block ciphers Camellia and AES, and the 256-bit block cipher Shacal-2;
- MAC algorithms TTMAC and UMAC, and the standardized algorithms EMAC, HMAC from [IS9797];
- hash functions Whirlpool and SHA-256, -384, -512;
- asymmetric encryption algorithms: PSEC-KEM, RSA-KEM, ACE Encrypt;
- digital signatures schemes RSA-PSS, ECDSA, SFLASH;
- asymmetric identification scheme: GPS.

The goal of NESSIE is to publish the recommended primitives and to submit these primitives to standardization bodies.

Some of the important conclusions from the NESSIE project are:

- The submitted stream ciphers were designed by experienced researchers and offer a very good performance, but none of them seems to meet the very stringent security requirements;
- In 2002, a new class of attacks (algebraic attacks, e.g., [CoPi02,MuRo02] has been introduced. They seem to form a very powerful tool to cryptanalyse stream ciphers, but they may also be apply to certain classes of block ciphers. One year after their announcement, it is still unclear how effective these attacks are on block ciphers; further research is clearly needed.
- Most asymmetric primitives needed small modifications and corrections between the 1st and 2nd phase, which shows that many subtle issues are involved in the specification of these primitives;
- The NESSIE project has influenced many designers to make their algorithms less expensive to use. Thirteen algorithms (out of 17) are in the public domain and the conditions for PSEC-KEM are very mild. Only one algorithm was eliminated due to IPR problems.

3 Cryptographic Algorithms for New Environments

While the algorithms discussed in Sect. 2 present a substantial improvement in the state of the art, we will argue in this section why further cryptographic research is needed.

3.1 Highly Secure Cryptographic Algorithms

All of the new symmetric algorithms discussed above have only *heuristic* security. This implies that for the time being we are now aware of any attack which can break these schemes. However, it may well be that tomorrow or next year a new clever attack is discovered which demonstrates that the scheme is much weaker than anticipated.

For the asymmetric primitives, the situation is slightly better: the seven primitives listed in Sect. 2.3 have a “proof of security”; this means in practice that if the primitive can be broken, then a problem believed to be hard (such as factoring, computing a discrete logarithm in an elliptic curve group) can be solved. However, in most cases the proof uses some additional assumptions. A more serious problem is that a problem widely believed to be hard (such as the factoring an integer that is the product of two large primes) may not be hard at all. For exam-

ple, if large quantum computers can be built, factoring may be very easy (a result by Shor [Shor94]). While early experiments are promising [VSB+01], experts are divided on the question whether sufficiently powerful quantum computers can be built in the next 15-20 years.

This clearly shows the need to develop new algorithms: for symmetric algorithms, we need better heuristics and proofs of resistance against a larger class of known attacks; it would be even better if we could reduce their security to well known problems. For asymmetric algorithms, there is a need for algorithms based on a wider range of problems believed to be hard, and more in particular for algorithms which would be secure even if large quantum computers can be built.

3.2 Low Cost Algorithms

While symmetric cryptographic algorithms are inexpensive on modern PCs with 2 GHz clocks, there is a clear need for highly efficient algorithms that would be suitable for environments where the gate count and power consumption is absolutely critical; one can think for example of distributed sensor networks (piconets [RASP+00]) or ubiquitous computing models. For the time being we don't know how to build a stream cipher or a block cipher that offers a security level of 80 bits or more, that offers a reasonable performance, and that fits in less than 1000 gates.

For asymmetric cryptographic algorithms, this is clearly way beyond reach. However, here we would like to have algorithms that require less than one second for a public or private key operation on an 8-bit processor with a few hundred bytes of RAM (currently this is only feasible with a co-processor). Another challenge is the design of secure public key algorithms that have short block lengths (160-bit for encryption and 80 or 160-bit digital signatures).

3.3 High Performance Cryptography

At the other end of the application spectrum, there are requirements for hard disk encryption, bus encryption and high speed connections (Gigabit/s to Terabit/s). For such applications, the main requirements would be high performance and a high degree of parallelism. As the NESSIE project has demonstrated, for the time being there does not exist a highly secure stream cipher that runs at a few cycles/byte, that is, 5 to 10 times faster than the AES block cipher.

4 Cryptography Against New Attack Models

Even if the cryptographic algorithms are more secure, the way they are used and implemented has to change substantially. In the last decade, we have learned that weaknesses in modes and in implementations are even more of a problem than most mathematical attacks on the underlying algorithm.

4.1 Blockwise Adaptive Attackers

A first type of new attacks are attacks on modes where the attacker does not submit the complete plaintext to the encryption device, but rather block by block [JoMV02]. This may have as implication that a provably secure way of using a block cipher becomes highly insecure. New modes of block ciphers are being developed that take into account this problem. A similar attack on stream ciphers exploits the resynchronization mechanism of synchronous stream ciphers (a typical example is the attack on the use of RC4 in the IEEE 802.11 WLAN standard WEP, which has been exploited in [FlMS01] and demonstrated in [StIR02]).

Application

E-Invoicing and New VAT Directive – Challenges for Cross Border Transactions

Stefan Engel-Flechsig

Chairman CEN/ISSS focus group on electronic invoices and VAT
CEO Radicchio
Stefan.engel-flechsig@radicchio.org

Abstract

CEN/ISSS has been asked by the European Commission in 2002 to examine the issues surrounding standards relating to e-Invoicing and VAT in relation to the new Council Directive 2001/115/EC, which has to be implemented by Member States by 1st January 2004. CEN/ISSS has created a focus group on electronic invoices and VAT (e-IFG) which will publish its final report in October 2003.[1]
Council Directive 2001/115/EC, details the requirements on taxable persons and their service providers to the guarantee of integrity of content and authenticity of origin of electronic invoices for VAT purposes. This relates mainly to the invoices exchanged electronically and to the storage of invoices.
Based on a questionnaire the e-IFG report describes the main issues around the implementation of electronic invoices for VAT purposes in the European Member States; the report identifies standards available and makes recommendations for usage of electronic invoices across Europe.
The report is based on the contributions from the members of the e-Invoices Focus Group and on the contributions received during the Open Conference held in Brussels, where some 150 participants reviewed the first draft of this report. Some 53 comments were received following the Open Conference.

1 Introduction: The Regulatory Environment

The Council Directive (2001/115/EC) regarding invoicing requirements for the Member States is intended to simplify and harmonize VAT regulations across the Member States. Businesses operating in EU Member States should have simplified invoicing regulations and procedures harmonized at EU Community level as of January 2004. This will naturally flow through onto new acceding Member States in time.

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.

The regulatory environment which on the European level directly related to these issues, is mainly built upon:

- the European Directive 2001/115/EC,
- the European Directive 1999/93/EC, and
- the European Commission Recommendation 1994/820/EC.

[1] The final version of the report will be available at: www.cenorm.be

S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 131-137

1.1 The European Directive 2001/115/EC

The European Directive 2001/115/EC clarifies the implementation of e-Invoicing through the Member States and aims to introduce harmonised procedures for e-invoicing (and paper invoicing) across Member State borders in a homogenous home market.

The Directive 2001/115/EC, details the requirements on taxable persons and their service providers to the guarantee of integrity of content and authenticity of origin of electronic invoices for VAT purposes. This relates mainly to the invoices exchanged electronically and to the storage of invoices.

With regards to the **exchange of invoices** for goods or services by electronic means, the exchange 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 (AES). Member States may however ask for the advanced electronic signature to be based on a qualified certificate,
- or by means of electronic data interchange (EDI) as defined in Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects (See annex 7.3 for the recommendation);
- Invoices may, however, be sent by other electronic means subject to acceptance by the Member State(s) concerned.

Although the Electronic Data Interchange (EDI) invoice message has been defined and adopted by several industry and trade sectors in Europe, it has not been implemented to its full potential. Paper invoices were usually maintained to overcome difficulties surrounding the VAT regulation. Several Member States introduced special procedures to allow EDI paperless invoicing but still requiring companies to apply for permission from tax administration and in some cases to exchange summary VAT control messages, electronically or on paper. For cross border electronic invoicing, companies are exchanging electronic invoices for company administration application, but are forced to parallel the exchanges with paper invoices for Member State VAT requirements.

1.2 The European Directive 1999/93/EC

The European Union has introduced a legal framework to guarantee EU-wide recognition of electronic signatures – a prerequisite for ensuring the security of data that is transmitted electronically (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures). The purpose of the Electronic Signature Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a general framework for **electronic signatures** and certain **certification services** in order to ensure the proper functioning of the internal market.

The commercial invoice is the most important document exchanged between trading partners. In addition to its commercial value, the invoice is an accounting document, it has legal implications to both transacting parties, it is the basis for VAT declaration and reclamation, statistics declaration for intra community trade, export and import declaration for extra community trade.

While the EDIFACT Invoice was the first message to be accorded UN Recommendation status, companies have chosen to implement other trade messages instead (Orders, Despatch advice) and limiting the implementation of electronic invoice just for inter company accounting application. Implementation of electronic invoice is being held back because of the di-

verse, often restrictive and conflicting legislation in some Member States. This is one of the weakest link in the electronic trade chain which limits competitiveness of European firms and impedes the development of electronic commerce.

1.3 Commission Recommendation 1994/820/EC October 1994

The Commission Recommendation from October 1994 was developed on the request of European trade and industry EDI user groups to provide the required legality, acceptability and security in the use of EDI in European Member States. The Recommendation includes the '**Model European Interchange Agreement'**, which was developed in line with the work carried out by the International Chamber of Commerce and several major industry sectors, e.g. automotive, electronics, retail and distribution. Trading partners prior to commencing the exchange of EDI messages are advised to agree and sign interchange agreements based on the European model.

2 The CEN/ISSS e-Invoicing Focus Group

The scope of the CEN/ISSS e-Invoicing Focus Group (e-IFG) has been:

- To provide an overview of the standardization aspects of electronics invoicing
- To assess existing standards and their implementation
- To provide proposals for additional activities should these be considered necessary.

The group should also ascertain that the standardization framework ensures 'Authentication and Integrity' requirements as stated in Directive 2001/115/EC are met in a cost effective manner, whilst maintaining an adequate level of interoperability and functionality.

Particular attention should be paid to the electronic signature and EDI standardization issues, as well to those posed by technology advances, e.g. web services. The group should also examine archiving.

2.1 The Report and Recommendations of the e-Invoicing Focus Group

Following the review and approval of the e-Invoicing Focus Group Terms of Reference, the group indicated that four – five meetings would be sufficient to prepare the report and requested CEN to contract a Technical Editor to take responsibility for compiling the report. The participants in the e-IFG have represented a broad range of expertise:

- Electronic signature
- Law practice specialising in legal aspects
- Tax administrator
- e-Business and EDI experts
- Business process experts
- Third party service providers
- International accounting practice with expertise in e-Invoicing
- Financial institution

Practice

ChamberSign Bridge CA

Maike Bielfeldt

ChamberSign aisbl
Bielfeldt@chambersign.com

Abstract

ChamberSign a.i.s.b.l. (international non Profit Association) is an initiative set up by Chambers of Commerce with the aim to create a comprehensive architecture for secure business-to-business electronic commerce across international borders. The ChamberSign focus is to promote and enable the digital signature technology, making it widely available to the business community and achieving international recognition and interoperability.
With Certificate Authority's in nine different countries throughout Europe issuing digital certificates to its members, ChamberSign. has implemented a Bridge CA. The solution is an initiative set up by Chambers of Commerce with the aim to create a comprehensive architecture for secure business-to-business electronic commerce across international borders. The ChamberSign focus is to promote and enable the digital signature technology, making it widely available to the business community and achieving international recognition and interoperability. Today with various CA infrastructures available in each member country, the ChamberSign Bridge CA is the approach to meet the objectives.

1 Background

The European Chambers of Commerce and Industry, EuroChambres[1], founded the association "Chambersign"[2] in July of 1999 to promote and support the distribution of the digital signature and the development of applications within an international context. Its current member countries are *Austria, Belgium, France, Germany, Italy, Luxembourg, the Netherlands, Spain, Sweden and the United Kingdom*[3]. Thus, ChamberSign´s main focus is international with a main emphasis on European projects regarding the acceptance and usage of the qualified digital signature application.

ChamberSign is currently the political framework and organisation to support the Study on legal and market aspects of the application of Directive laying down a Community framework for electronic signatures and on the practical applications of the electronic signature. ChamberSign's approach is by setting up an international network of registration authorities in all membership countries to allow for easy access to the qualified digital signature according to the EU Directive 1999/93/EC based on common standards.

---

[1] http://www.eurochambres.be

[2] http://www.chambersign.com

[3] Represented by the Wirtschaftskammer Österreich, the Federation Nationale des Chambres de Comerce et D'Industrie de Belgique/Nationale Federatie der Kamers voor Handel en Nijverheid van Belgie, the Assemblee des Chambres Françaises de Commerce et D'Industrie, the Deutscher Industrie- und Handelskammertag (DIHK), the Unione Italiana delle Camere di Commercio, Industria Artigianato e Agricoltura, the Chambre de Commerce du Grand-Duché de Luxembourg, the Consejo Superior de Camaras de Comercio, Industria y Navigacion de España, the Svenska Handelskammarförbundet, and the British Chambers of Commerce.

S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 185-190

At this point, the Eurochambres organisation represents 36 national Chamber Organisations, 1,500 regional and local Chambers of Commerce and Industry, thus 15 million enterprises, most of which are SMEs. Thus, the impact ChamberSign has both on a European, but also on a global level will allow for standard-setting regarding the digital signature application. Since interoperability is one of the key for the acceptance of the digital signature in the future, ChamberSign´s approach by setting-up this project tackles the wide acceptance and diffusion of digital signature applications throughout various applications.

2 ChamberSign and the EU Directive 1999/93/EC on Electronic Signature

The EU Directive 1999/93/EC goes to great length demonstrating the benefits of the digital signature for European eBusiness and eCommerce. The Directive itself is meant to facilitate the use and acceptance of the digital signature within the EU and beyond national borders. It is particularly aimed at levelling the divergent rules and regulations of every EU member state. The EU Directive, thus, tries to establish international standards that eventually will be adopted into national law by each member state to avoid meeting obstacles in international online business. It is a measure to support the free flow of goods and services within Europe. Thus, interoperability is a major objective of the Directive. It is aimed at enabling every participant in the global market to act within just that market. Thus, the Directive supports any effort that is aimed at improving the online business relationship between international companies and calling for standardisation and common security standards. While the EU Directive was written with the European business partners in mind, it cannot stop right there but is reaching out to other nations as well. For all players, both in the EU and the member candidate countries, it is of utmost importance to work within a framework of common laws and practices.

ChamberSign, aims to put the ideas expressed in the Directive into practice by offering its members a digital signature application that ensures interoperability starting with its member states and meets the EU Directive’s very high safety standards.

3 The ChamberSign a.i.s.b.l. Approach and Objective

With Certificate Authority’s in nine different countries throughout Europe issuing digital certificates to its members, ChamberSign. has implemented a Bridge CA. The solution is an initiative set up by Chambers of Commerce with the aim to create a comprehensive architecture for secure business-to-business electronic commerce across international borders. The ChamberSign focus is to promote and enable the digital signature technology, making it widely available to the business community and achieving international recognition and interoperability. Today with various CA infrastructures available in each member country, the ChamberSign Bridge CA is the approach to meet the objectives.

The Bridge CA project has been running since 2002, assessing solutions appropriate for ChamberSign to meet the defined aim. As the last phase of the project, ScandTrust AB was assigned the responsibility to be the supplier of the technical solution in the beginning of 2003.

3.1 PKI Concepts

Today most countries around the world have adopted the PKI concept both legally and in practice. As for Europe the European parliament presented a directive to implement a community framework for electronic signatures 1999 that now has been adopted by each country within the European Union.

Public Key Infrastructure (PKI) is a solution based on the innovation of public key encryption that makes it s possible to sign and encrypt without a shared secret. In the PKI environment certificate authorities (CA) are the trusted entities that issue certificates and provide status information about the certificates the CA has issued. To implement a PKI environment, three models are used:

The basic implementation of PKI is a single CA responsible for all PKI services; including issuing and revoking certificates, providing certificate status information, etc. This implementation results in a single user trust point, the CA's public key.

The hierarchical PKI configuration involves a superior-subordinate CA relationship, where all users trust the same "root" CA. In this configuration the "root" CA does not issue certificates to users, instead certificates are issued to subordinate CAs. These CAs issue certificates to users or another level of subordinate CAs.

Another configuration of PKI is to connect single CAs with a peer-to-peer relationship, defined as a mesh PKI. This require that each CA goes through a cross certification, where a cross certificate is issued by one CA which contains a CA signature key used for issuing certificates. The result is a certificate trusted within one CA in the mesh, also is trusted in another CA within the same mesh.

The implementation of PKI and the configuration used is dependent on the community it is supposed to operate in. As the single CA is the easiest, it may be used in a closed environment. The hierarchical CA provides scalability where several subordinate CAs can manage end users. With a mesh configuration the bi-directional trust relationship is established between each CA in the mesh.

3.2 Bridge CA Concept

The basic question that needs an answer for all PKI configurations is: "What is the easiest way for me to trust a message signed or encrypted by a user". As you move from an internal environment to a global, all configurations mentioned above turn out to be too isolated or too complicated. With this experience in mind, the development of the Bridge CA concept has turned out as a new dimension of PKI.

The implementation of a Bridge CA can be described as a mesh configuration with a hub or a hierarchical configuration with an established external relationship. One difference is that a Bridge CA does not issue certificates directly to users, neither is it intended to be used as a trust point by the users of the PKI. Instead the trust relationship is configured as a star to be a "bridge of trust", where the Bridge CA is the centre of trust in the community.

3.3 Technical Features

A Bridge CA can be implemented based on two different approaches:

- A Bridge CA that actually issues certificates for other CAs.