End User Acceptance of Security Technology for Electronic Commerce

Dale Whinnett dalew@iig.uni-freiburg.de
Albert-Ludwigs-University Freiburg, Germany
Institute for Computer Science and Social Studies

Abstract

This paper examines the current advantages and limitations of the developing Global Information Infrastructure (GII) for commerce from the point of view of today's players. It is based on the interim results of an Expert Survey being carried out as part of the ACTS project SEMPER (Secure Electronic Marketplace for Europe)[1]. The findings can be broadly categorised as 'network' and 'non-network' influences on participation in electronic commerce, i.e. those directly related to the use of computer technology for connecting to and navigating in open networks and the non-technical influences on the willingness or ability to conduct business in this environment. The analysis is primarily based on use of the Internet because it is currently the most widely used precursor of the GII.

1. Introduction

Secure communication over open networks cannot be achieved by technological innovation alone. Its success will also be determined by the ability of end-users (business, government, or the private consumer) to both appreciate the significance of security and make intelligent use of it. Further, the willingness of the end-user to conduct business in an advanced, networked environment will be determined not only by the performance of the enabling technology, but also the legal, financial and regulatory issues surrounding this activity.

Those who are professionally involved in the design and implementation of information technology are well aware of both the opportunities and risks of doing business in an advanced networked environment. The research on which this paper is based [2] indicates that the non-professional user is not fully aware of either the opportunities or risks related to network use. Restrictions on the infra-structure and continuing problems of inter-operability bar today's end-user from discovering many of the potential advantages of the "Information Highway". Misunderstanding or a lack of knowledge regarding the technologies involved, on the part of both users and regulators, prevents most users from conducting business securely.

A sketch of current Internet use and type of users is followed by a discussion of the research results, with particular emphasis on implications for the implementation or acceptance of security technology. Finally, suggestions are made regarding measures to support the development of secure commerce.

[1] The results of the Expert Survey form part of the document D05 *First Year Surveys Requirements and Trials* available at <www.semper.org>

[2] Research included a review of existing network user surveys and a series of extended interviews with experts in the field of electronic commerce.

2. Internet Use and Users

Truly global use of the Internet is still very much a vision of the future. The USA is leading the way with roughly 2/3 of all host computers in the world. Taken collectively, the countries of the European Union follow with 20%[3]. Estimates of Internet usage vary from 26 million [4] to as little as 6 million[5], however, due to the unreliability of all currently available user surveys, host count figures provide a conservative basis for estimating usage.

Recent studies [CNN95, HKN96] indicate that despite the growing numbers of total users, the *active* base of regular Internet users is, in fact, relatively small. In addition, it is estimated that 15% of all Internet users comprise 50% of all usage [CNN95]. The fact that this small group of relatively sophisticated computer users is still experiencing some very basic problems indicates areas which must be improved if electronic commerce is to become more widespread.

Today's active network users are young, well educated and well equipped. On average, they spend at least an hour a day on-line. Roughly half access the Internet from home, the other half from work, or an educational establishment. In spite of the fact that 28.8 Kbps modems are rapidly becoming the norm and most respondents have the hardware to support graphic-intensive content [GVU96], speed of connection to the Internet remains the greatest limiting factor for today's users (most common problem for 80.9% of the GVU survey).

Although e-mail is the number one Internet application, used by 3/4 of all PC users with Internet access,[6] browsing the WWW is clearly the fastest growing application. The number of PC users accessing Web services has shown a 250% increase compared to 1994.[7] Most users are aware of potential security risks when browsing the Net, but a surprising number are unaware that their e-mail travels via this medium and are, subsequently, also unaware of the potential threat to the privacy of the communications which they send in this way. Business customers, on the other hand, frequently avoid sending email via the Internet by dialling into their office networks in order to protect valuable company information.

The most popular computing platform for today's users is Windows. This broad base of non-technically oriented PC users places very high value on ease-of-use and they want security mechanisms to mirror the "drag and drop", "cut and paste", "click and go" environment of Windows. They view the management of multiple passwords and phrases, currently required for the use of subscription services, as inconvenient, and

[3] Data taken from Network Wizards Internet Domain Survey, January 1996. Method pinging 1% of all known hosts. Data available at http://www.nw.com.

[4] International Data Corporation, World Wide Web Surfers, May 1996 in CyberAtlas published by I Pro last updated 18 July 1996.

[5] O'Reilly & Associates, US users with direct access, July 1995 in CyberAtlas published by I Pro last updated 18 July 1996.

[6] CI (Computer Intelligence) Consumer Technology Index, July 1996. <http://www.ci.zd.com/news/ctinet2.html>

[7] Ibid.

frequently take unnecessary security risks in care and use. They lack confidence in their own ability to install and configure security interfaces.

In spite of positive signs of growth in electronic commerce, roughly half of Web users [GVU96] have never purchased anything on-line and few purchase regularly. Security fears appear to be the reason why. “As people learn more about the Web they become less likely to trust it with their financial transactions. People are less likely now than they were just six months ago to post credit-card information on-line.”[8] User reluctance is not restricted exclusively to the potential loss of financial information. It is expected that data privacy generally will become increasingly important as the Internet becomes a part of many people’s daily life. “While the majority of users understand the basic information that can be recorded per transaction, many do not know some of the advanced features like cookies. Additionally, the current HTTP specifications do not enable the user’s email address to be logged, thus indicating that 45.2% of the users hold a false belief about what is loggable. Yet, given the recent implementation bugs (enabled the user’s email address to be sent to whomever) of certain browsers that implement scriptable languages like Javascript, this result may be a bit ambiguous.” [GVU96]

The ability to *control* the use of demographic information collected and to visit Web sites anonymously are considered by users as essential aspects of their right to data privacy. Over a quarter of the GVU respondents reported having provided false demographic information when registering with Web sites and there was also strong support for the statement “ought to be able to take on different aliases/roles at different times on the Internet.” [GVU96]

3. Network Influences

> “Customer feedback, has been that they find the security in general an annoying feature.”[9]

3.1 Transmission Speeds

As mentioned above, connection speed is currently considered to be the greatest limiting factor for Internet users. One might argue that this is an infrastructure problem, but the ways in which users compensate for this restriction can have important implications for the success of security mechanisms. According to the FIND/SVP survey[FD/SVP95] more than a third of Web users (34%) turn off graphics in order to speed up browsing and most refuse to download any files over 25k to 35k. As a result, important transaction or security related information cannot depend on graphics being viewed online and the size of files a user is expected to download in order to install a security interface is likely to influence acceptance. Insufficient speed also discourages on-line shopping and creates the danger that users

[8] BYTE, March 1996.

[9] Financial Services Provider.

will interrupt transactions if they are not implemented quickly enough. There must always be a way to discover the status of a partially completed communication.

Transmission speeds also result in the at-work volume of Internet use being considerably higher than home use, indicating that security mechanisms must be designed for use in both the business and private environment, preferably for use in both environments by the same user. At work use is primarily within a company network which requires taking into account multiple users and possible firewall interference, but even private access is frequently shared. Recent surveys of German users [FOC96, IST96] indicated that 40 to 60% of users share their Internet access with others, with an average of 3.7 persons using an Internet connection.

3.2 Ease of Use

> “What do you do to your customer base and about a retail marketplace developing on the Net if you say that it’s a normal thing to expect of a customer, that he is capable of going to a different site and ftping Netscape in zipped or unzipped format and then putting those executable files on his hard disc and then putting them in a directory and then unzipping them and loading them and running them. What have you said about the type of person you expect to be able to access your Web site?”[10]

A simulation study on the use of digital signatures carried out by the GMD [ROS94] also identified ease of use as a key factor for user acceptance. GMD test participants avoided using digital signatures as much as possible because they found them much more inconvenient than using their handwritten signature. Even when it was made possible for them to use the PIN for a group of documents or a work session this wasn’t sufficient because the signing function wasn’t integrated in the word processing programme. GMD concluded that the signature function has to be integrated and implemented by the click of a mouse.

Even mechanisms which are less sophisticated than the digital signatures tested by the GMD meet with user resistance. If they are to be accepted security mechanisms must be as simple as possible, virtually automatic. However, some products which contain features to assist users in coping with multiple passwords, such as the password file included in Windows 95, actually create security weaknesses, e.g. anyone gaining access to the computer also gains access to this file. In respect of Win 95 it was also felt that many users will ignore the product advice to disable shared files and printers before accessing the Internet. Most recommendations for increasing security by correct use of passwords or phrases are ignored by users. Even well-informed experts admitted to laxness in security principles, e.g. using the same PIN or pass phrase for all electronic accounts, simply for convenience. “Human short term memory is limited to a certain amount of information (seven plus or minus two chunks)... “ [LUSI96]

There is some evidence that consumer will only take proper care in creating and protecting security information if forced to do so. However, this approach conflicts with the ease of use requirement discussed above and supports those who argue that,

[10] Business Development Director, Financial Services.

in order to be successful, security options should be independent of the computing hardware which would facilitate both ease of use and user control.

It was suggested that consumer education in respect of security mechanisms could be carried out in stages. “A service dialogue that is structured to support users new to the service might become frustrating over time, and users will want to speed up the interaction and reduce the number of procedures required to complete their tasks.” [LUSI96]

Although it may be possible to simplify certain aspects regarding security procedures once the user has become familiar with them, it should never be possible to disable a warning at the point where the user takes an action which cannot be revoked. In addition, mistakes should be easy to correct. “One of the best ways of achieving this is to allow the user to undo the previous action or to step back. If there is no chance of easy recovery then it is good practice to make the user confirm the action.” [LUSI96]

3.3 Incompatibility

> “...the superhighway should provide a “seamless” web of features and services to users, with thousands of systems and components interacting, or interoperating, in a way that is transparent to users. Achieving interoperability will require manufacturers to cooperate with standards-setting bodies to establish common interfaces and protocols.”[11]

The second greatest technical problem (apart from speed of connection) currently facing service providers and end users alike, is browser incompatibility. Browser incompatibility is not only an impediment to the development of electronic commerce in general, it can also have serious implications for the success of security mechanisms. According to respondents one of the principal features of the Internet, its universal accessibility, is being threatened by the introduction of incompatible extension sets.

The fact that Netscape and Microsoft have extended the HTML command set in ways that only their own browsers can read creates formidable problems in the virtual world. [12] There are also some who don’t think the competitive battle will be restricted to browser software. “It’s not just technology. I’m sure they (Microsoft) will start playing games with integration with their TCP/IP stack. I’m sure they’ll start bundling the browser with the operating system.”[13]

For the Internet user this incompatibility renders Websites that have been designed for a browser other than the one they have installed, from simply difficult to use, to totally inaccessible. It also presents the possibility that they will either have incomplete access to valuable consumer information (product descriptions, conditions of sale, etc.) which an electronic enterprise has included in its Website and that important transaction related information could be overlooked due to poor visual presentation

[11] United States General Accounting Office Report to the Congress, *Information Superhighway : An Overview of Technology Challenges,* GAO January 1995.

[12] Convergence, Mar. ‘96

[13] Founder of a company which makes Web authoring software.

(warnings may be illegible, instructions misunderstood). In the worst case the user is barred from using the site at all.

Companies currently operating in the Internet are forced to deal with the problem by 1. restricting Website design to the lowest common denominator, 2. supplying their customer base with the appropriate browser for their site or 3. modifying their website to offer different levels of service depending on the features of the customer's browser. [14] "The Web should be open to all access providers, interoperability is the key." [15] The same principle must be applied to the design of security services and emphasises the necessity for non-proprietary solutions.

4. Non-Network influences

> "Security problems are more problems of awareness than a technical issue. People don't take the care that they need to take, either because they don't know, or because it's too difficult."[16]

In general, the experts consulted felt that consumer, or end-user perceptions of security threats currently result more from media coverage of the issue than personal knowledge, or experience. As a result, awareness of a threat tends to result in *"non-use"* rather than *"care in use"*. [17]

Experts felt that very few end-users understand Internet technology well enough to appreciate where security threats occur, or to prevent their abuse by personal intervention. Misunderstanding of Internet technology is seen to lead to resistance on the part of both endusers (business or private users) and the official bodies or agencies which must co-operate if electronic commerce is to be successfully implemented. This applies particularly to legal issues , but also has implications for the way services can be made available. Respondents referred to a frequent misconception that the Internet is a broadcast medium, similar to radio or television. They felt the fact that that information in the Internet is essentially *made available* for retrieval is widely misunderstood, i.e. that it is essentially a *pull* rather than a *push* medium.

4.1 Existing Laws are Inadequate for Regulating Electronic Commerce

> "The jurisdiction applying to contracts will depend on the facts of the situation, the choice of law clauses in the various contracts, the location of the parties and the location of the equipment attached to the network." [MC96]

Legal experts identified a number of key issues regarding the legality of business conducted electronically. These included the inadequacies of existing legislation for application to the new communication medium, the question of establishing legal jurisdictions, the legal acceptance of digital signatures and the burden of evidence for electronic contracts. At the same time they were careful to point out that until new

[14] online aktuell, April 1996.

[15] Hakon Lie, INRIA programmer in *Convergence,* Mar. 1996

[16] Consultant to the Printing Industry.

[17] According to [GVU96] users are now less likely to enter credit card information via the Internet than they were a year ago.

legislation is passed, existing laws will be applied to electronic transactions and it is the responsibility of legal advisors to create as much certainty as possible.

Parties to traditional contracts are generally free to specify the jurisdiction which will regulate the contract. It can be assumed that contracts negotiated electronically will also include a clause of this nature, but the *global* nature of electronic commerce will make disputes more difficult than ever to resolve. In addtion to the changes in technology and business practice which are currently taking place, an equally important factor is the change of participants in the global market. Whereas previously, with high level international transactions, you had businesses taking advantage of expert (and expensive) legal advice, the fact that, via the Internet, for the first time small businesses and ordinary consumers are becoming involved in international small scale transactions raises an entirely new set of concerns.

If the consumers are members of a defined group, e.g. because they sign a subscription agreement, (the closed user group model which is being used for much of the electronic commerce which is currently taking place), then that agreement should specify the jurisdiction in which future transactions will take place. In the absence of such a provision, such as in the commercial situation addressed by SEMPER, where no pre-established relationship between the buyer and seller is assumed, the consumer should be warned, at the point of sale, that as a condition of sale a certain jurisdiction will be used.

4.2 Acceptance of Digital Signatures

> “They shouldn’t call it a signature, they should call it something else.” [18]

Digital signatures are currently viewed as the most viable option for concluding legally binding contracts in a global network environment, but their use is also subject to criticism and their legal status remains uncertain. One of the greatest legal problems accompanying the concept of a digital signature appears to be the very specific legal interpretation of a *signature.* A fresh approach is required to resolve the legal issues related to electronic commerce. Taking too narrow a view, or attempting to mirror traditional contracts, is viewed as an impediment to finding the solutions required.

4.2.1 Possible Solutions

A solution which is currently being used for electronic commerce is to use a traditional paper contract to establish the conditions and terms for business, which will subsequently be carried out electronically. This has the disadvantage, of course, that the consumer has to establish a relationship to the vendor and mitigates against spontaneous transactions. The legal experts within the SEMPER consortium aim to

[18] Financial Services Provider.

develop an initial legal framework for electronic contracts which can be used in the spontaneous business context.[19]

In order to achieve some level of clarity many businesses now construct their web sites in such a way that the consumer is forced to view and acknowledge their terms and conditions of sale before proceeding with a transaction, e.g. before entering order details, confirming, or sending an order. This method is frequently employed by software manufacturers which allow their products to be downloaded via the Internet. The consumer has to acknowledge (by clicking) acceptance of the licensing agreement, before the download can proceed.

> "A clearly visible hyperlink should guide the consumer from the product offering to the terms of condition and sale and the ordering procedure should be structured in such a way that the consumer must view these terms and conditions before it is possible to place an order."[Zor96][20]

It appears that many Internet entrepreneurs have enough confidence in the bindingness of electronic negotiations to conduct business make the *electronic acknowledge* of their licensing agreements, or terms and conditions of sale, a prerequisite for obtaining their product. It may well be, however, that this results more from the lack of an alternative (e.g. easy to implement digital signatures) and it is usually restricted to products where the financial gains of an Internet presence outweigh the financial losses resulting from occasional abuse.

In traditional commerce and electronic commerce alike, not all contracts require a written signature. Virtually any commercial transaction constitutes a contract being formed between the two parties and what is lacking is clarification of the legal status of these contracts when they are concluded electronically. A distinction was made here between the need for legal recognition of digital signatures and the need for electronic contract law.

Companies are already doing business over open networks, in spite of the current restrictions and anything which has the potential for increasing the certainty of their situation is welcome.There is widespread willingness to trial security solutions.

> "They're holding up the electronic thing to much higher standards than the manual system. People are saying the whole world has to agree on this before we can move forward. I guarantee it won't happen if that's the approach we take. What we need is...this little geography has certificates and they work and they spread their experience to other people. If we let governments and politicians and standards people dictate for the Internet, it ain't gonna happen."[21]

[19] The initial proposals for this can be found in Chapter 4 - Framework for Electronic Commerce in D05 *First Year Surveys Requirements and Trials,* available at <www.semper.org>.

[20] Advice of a German lawyer to companies wishing to do business on the Internet.

[21] Director of Advanced Technology, software company.

4.2.2 Electronic Notary Services

> "It (the notary's stamp) is a formality which delays things, doesn't particularly prove anything and mostly is used to satisfy governments which like to see a lot of stamps, red tape and sealing wax. If there's an electronic way to speed up that process, where somebody in one country can push a button and have it verified that, yes, they're a real company, that would be extremely useful."[22]

Respondents felt that two services currently provided by notaries could not only be achieved well in an electronic environment, but would, in fact, offer a considerable improvement over the current situation. These were: 1. the neutral authentication of identity and/or other information regarding a person or business and 2. acting as a trusted third party by holding funds, deeds, etc. The notary's role is also frequently viewed as one of selling trust which extends beyond the individual or company.

> "In Germany, the notary has a lot to do with personal trust in a person. A digital signature is nothing more than a substitute for a normal signature. The notary is at a much higher level and, in addition to his signature, he also adds a seal."[23]

The comments above seem to indicate that in certain business situations there is a perceived requirement for an *electronic seal*, which, if necessary, could be added to the digital signature. In view of current discussion regarding certificates, this might be viewed as support for different *levels* or *degrees* of certification to cater to the requirements of various business situations.

4.2.3 Legislation Governing Electronic Business/Contracts

> "I think the biggest problem at the moment is that judges don't understand electronic anything." [24]

Legal experts stressed the fact that technology is much more advanced than the laws which must be applied to settle disputes arising from its use. There is a need for clear rules for the exchange of electronic contracts. Some form of proof of contract will be required, as well as the legislation which says this is a valid way of concluding a contract.

According to one expert, although there are number of factors which are seen to be legitimately holding back the development of legislation for electronic commerce, among these, the need for more detailed research to discover the extent to which current definitions (of *document, writing, signature, record* and *instrument*) produce legislative barriers. In his opinion, however, there are also some areas where legislation could provide an immediate improvement of the legal situation:

1. "There is no justification for imposing different requirements for the admissibility of computer records as evidence from those imposed for other types of documentary evidence.
2. It could remove some of the uncertainty about how computer records are to be authenticated in civil proceedings. This could be achieved by setting up a certification

[22] Legal advisor to the software industry

[23] Manager Research & Development, German Federal Printing Office.

[24] Legal advisor to the software industry.

> scheme, under which particular technical methods of authentication would be certified as providing sufficient proof of the accuracy of computer records. Legislation would then provide that such records were prima facie presumed to be accurate, on proof that the certified authentication method had been used, whilst of course leaving open to the parties the possibility of adducing evidence to the contrary. The certification (and decertification) of authentication methods would allow the law to respond rapidly to technical change." [Ree 94] [25]

A number of respondents stressed the point that much traditional business is conducted on the basis of mutual trust and unwritten business relationships which are built up over time. As one respondent put it, great deal of business has been conducted on a handshake. In the situation where the negotiations between these two established business partners take place electronically what may be more important than the question of a legally binding signature, is simply that the *electronic handshake* can be authenticated as actually coming from a known business partner. This indicates further support for a requirement for *levels* of security, depending on the parties involved in the particular business application, or the value of the transaction. At the same time, however, there is also evidence that much of the business being currently being conducted electronically (on an insecure basis) results from the lack of an alternative.

> "It is tempting when faced with these problems to throw up one's hands in horror and say, 'We must wait for Parliament to reform the law'. This is not a realistic option for a commercial lawyer. If a transaction can be carried out using computer technology, it is certain that at some time or other a client will decide to do so." [Ree 94]

4.2.4 Government Restrictions on the Choice of Technology

> "Critics of federal involvement argue that current federal initiatives represent a danger to civil liberties, and that individuals should be free to choose the technical means for achieving information security." [GAO95]

In the minds of most respondents the protection of intellectual property, a requirement for secure data transmission and questions regarding the use of encryption are all closely linked, so there will be a certain amount of overlap in the discussion of these issues.

> "Giving away the fruits of intellectual labor without fair and equitable compensation is a policy not destined to survive the rigors of a marketplace economy." [Bra 95]

The ease with which "digital" products can be copied and distributed presents enormous challenges for electronic commerce. The information industry, which previously functioned on the basis of recognised arrangements between authors, publishers and libraries, is now facing a completely new economic environment. Most of the current solutions for secure delivery of software via the Internet are seen to be complicated by the conflict between facilitating legitimate enduser use of the software and protecting copyright, e.g. solutions which require the physical delivery of a dongle, delivery of code discs, placing up to 10 products on a single CD with separate

[25] The author of these recommendations felt that the most efficient approach would be for certification to be carrried out by independent, non-govermental bodies.

encryption keys to open each one, delivering keys separately by email, supplying trimmed versions of products, etc.

Respondents from the printing industry were particularly concerned about the secure transmission of their products. In the pre-press industry, for example, the electronic transmission of data is extremely efficient, but the value of the products is also very high, which means that high priority is placed on the fact that the data must be transferred intact and cannot be intercepted, by competitors. Encryption is generally viewed as the most efficient form of protection.

> “Headers or electronic envelopes, encryption and other tools will be essential to maintaining the integrity of works.” [26]

There are any number of examples of other types of high value or sensitive data which requires the same protection, e.g. patents, passport or health information. For most business users secure email is a top priority. There was a virtually unanimous demand among the experts interviewed for this facility. Most were reluctant to send mail containing sensitive company information over the Internet and few had found a solution which was both practical and secure.

> “For us secure email is almost more important than secure payment. We tried PGP and I think the technology is probably very good, but it’s public domain software which consists of a lot of individual programmes and it’s much too complicated. It should be integrated in a programme like Eudora or Netscape.”[27]

> “Failure to implement strong encryption on-line could even open on-line service companies to lawsuits from clients and customers who find their business secrets laid bare to competitors. People in the financial services sector owe certain duties of confidentiality to their clients.”[28]

According to respondents the problem is not merely a lack of suitable products, but also the effect of US export controls on strong encryption.

> “Business needs strong encryption just to function, not ‘it would be nice if’. I know of at least one major company which has told its government that it will move certain aspects of business out of the country if strong encryption is prohibited.”[29]

In view of the rapid advances in computing power it is also assumed that encryption key length will continuously have to be adjusted, i.e. what is referred to as a C.O.C.A. (cost of cracking adjustment) - a predetermined increase in the bit length of encryption keys every few years - will have to be included in new developments. It is important that any legislation regulating the use of encryption take this factor into account if the law is to keep pace with technological advances.

> “Because many kinds of information must be kept confidential for long periods of time, assessment cannot be limited to the protection required today. Equally important, cryptosystems - especially if they are standards - often remain in use for years or even

[26] Ibid.

[27] Internet Access Provider.

[28] Robert Carolina, Attorney from London law firm Clifford Chance, in Convergence, March 1996.

[29] Legal Advisor to the software industry.

> decades. The life of a cryptosystem is likely to exceed the lifetime of any individual product embodying it." [BDR96]

5. Conclusion:

There is a pressing requirement for clear, non-technical information regarding network technologies, in particular, those which employ controversial, or restricted technologies, such as strong cryptography, or where security protection relies on unfamiliar and technically complex mechanisms, such as digital signatures.

This information should be generated for two specific audiences; for those persons who will influence and implement new legislation for the regulation of their use and for those who influence public opinion (journalists/media). The aim should be to promote public discussion which is based less on the sensationalism which is prevalent in today's media coverage, and more on an informed evaluation of the existing options. The challenge is to "translate" technological achievements into unintimidating layman's language, with the aim of promoting not only understanding, but co-operation.

The role of the end-user for the success of security technology cannot be emphasised enough. The greatest danger for the future of secure electronic commerce is the current lack of security solutions which are easy to understand and simple to use. There is a risk that the credibility of security technology will be undermined if users develop false confidence in security products and conduct business insecurely because the technology is insufficiently transparent.

The goal of the project, SEMPER (Secure Electronic Marketplace for Europe), is to develop the fundamentals for secure electronic commerce by providing the first open and comprehensive solutions for secure commerce over the Internet and other public information networks. SEMPER will integrate existing architectures, tools and services where appropriate, with the aim of ensuring compatibility and interoperability of different services and service implementations.

Electronic commerce is not a vision of the future. It is currently taking place, in spite of technological problems, insufficient security mechanisms and legal uncertainty regarding the transactions which are conducted. The question is no longer "Is there a business case for electronic commerce?", but rather, how can this business case be best supported?

6. Acknowledgments

This work was supported by the ACTS Project AC026, *SEMPER*. However, it represents the view of the author. *SEMPER* is part of the Advanced Communication Technologies and Services (ACTS) research program established by the European Commission, Directorate General XIII.

This description is based on joint work of the *SEMPER* consortium. It is a pleasure to thank all of them for their co-operation and contributions. The SEMPER homepage is at <http://www.semper.org>.

7. References

[BDR96] Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E., Wiener, M., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, <http://www.bsa.org/policy/encryption/Cryptographers.html>, January 1996.

[Bra95] Branscomb, Anne W., *Common Law for the Electronic Frontier*, Scientific American, (The Computer in the 21st. Century) Special issue, 1995.

[CNN95] CommerceNet/Nielsen Internet Demographic Survey, 1995, Executive Summary available at: <http://nielsenmedia.com/commercenet/exec_sum.html>

[D0596] D05 *First Year Surveys Requirements and Trials* available at <www.semper.org>

[FD/SVP95] FIND/SVP, HSF Consulting, C+C Data, *American Internet User Survey,* Sept. - Dec. 1995, <www.findsvp.com>

[FOC96] Focus Online Nutzerbefragung, Will & Partner Marktforschung, Augsburg Burda Medien Forschung/Studienleitung New media, March 1996. Available from: Focus, Arabellastrasse 23, 81925 München.

[FOR95] Forester Research, *Conducting Business on the Internet*, O'Reilly & Associates, <http://www.ora.com/survey/> 1995.

[GAO95] United States General Accounting Office Report to the Congress, *Information Superhighway : An Overview of Technology Challenges,* GAO January 1995.

[GVU96] GVU - Fifth WWW User Survey, April - May 1996, <http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996/>

[HKN96] Hoffman, Kalsbeek, Novak , *Internet Use in the United States: 1995 Baseline Estimates and Preliminary Market Segments,* <http://www2000.ogsm.vanderbilt.edu/baseline/1995.Internet.estimates.html> 12 April, 1996.

[IST96] IST On-line Umfrage, Nov. 1995- Jan. 1996, Frauenhofer Institut Systemtechnik und Innovationsforschung, Südwest Funk, Telecooperation Office Universität Karlsruhe. <http://www.teco.uni-kar> and <http://swf3.de>

[LUSI96] Clarke, Anne M.,Editor, *Human Factor Guidelines for Designers of Telecommunication Services for Non-Expert Users*, Volume 1, Published by HUSAT Research Institute (for LUSI Consortium), 1996.

[MC96] Millard, Christoper, Carolina, Robert, *Commercial Transactions and the Global Infrastructure: A European Perspective*, in The Marshall Journal of Computer & Information Law, Winter 1996.

[NOP95] NOP Internet User Profile Survey, Nov.-Dec. 1995, <http://www.nopres.co.uk/inet/proposal.html

[ROS95] Roßnagel, A , *Die Similationsstudie Rechtpflege: Eine neue Methode zur Technikgestaltung*, provet/GMD, Berlin: Ed. Sigma, 1994.

[SRI95] SRI International, *Exploring the Web Populations's Other Half*, 06/15/1995 <www.future.sri.com/vals/vals-survey.results.html>

[TM95] Times Mirror Americans On-line Survey, sample size: 4.005, June 1995, (US).

[Zor96] Zorn, Prof. Dr. Ing. Werner ,Universität Karlsruhe, *Visionen zur Zukunft des Internet und elektronischer Dienste*, CW Nr. 3/96.