Project Number	AC026
Project Title	Secure Electronic MarketPlace for Europe SEMPER
Deliverable Security Class	Public
CEC Deliverable Number	AC026/SMP/CT2/DS/C/005/b1
Contractual Date of Delivery	August 31, 1996
Actual date of Delivery	December 18th, 1996
Title of Deliverable	Deliverable D05 Survey Findings, Trial Requirements, and Legal Framework - Results from First Year of Project SEMPER
Contributing Workpackages	
Nature of the Deliverable	Report
Author(s)	Christoph Baert (Europay), Thomas Hecht (FOGRA), Ralf Kuron (FOGRA), Gérard Lacoste (IBM), Dimitris Livas (EUROCOM), Christian Petersen (Otto Versand), Matthias Schunter (Univ. Dortmund), Arnd Weber (Univ. Freiburg), Bruno Wildhaber (r3), Dale Whinnett (Univ. Freiburg)
Editor(s)	Christian Petersen (Otto Versand)
Reviewer(s)	Ingo Husmann (Otto Versand), Gérard Lacoste (IBM), Michael Waidner (IBM), and three external reviewers
Keywords	Electronic Commerce, Survey, Evaluation, Trial

SEMPER is part of the European Commission's ACTS Programme (Advanced Communications Technologies and Services). Funding is provided by the partner organisations, the European Union, and the Swiss Federal Department for Education and Science. The members of the SEMPER consortium are

- Cryptomathic (DK),
- DigiCash (NL),
- EUROCOM EXPERTISE (GR),
- Europay International (B),
- FINTEL(B),
- FOGRA Forschungsgesellschaft Druck (D),
- GMD - German National Research Center for Information Technology (D),
- IBM European Networking Center (D),
- IBM La Gaude (F),
- IBM Zurich Research Lab (CH),
- INTRACOM (GR), KPN Research (NL),
- Otto Versand (D),
- r3 security engineering (CH),
- REGIONLINK (B),
- SEPT (F),
- Stichting Mathematisch Centrum / CWI (NL),
- System Synthesis Ltd. (UK),
- University of Freiburg (D) and
- University of Dortmund(D).

- Banksys (B),
- Banque Générale du Luxembourg (L) and
- Telekurs (CH)

are associated with SEMPER.

This report was edited by C. Petersen (Otto Versand). It contains contributions by C. Baert (Europay), T. Hecht (FOGRA), Ralf Kuron (FOGRA), G. Lacoste (IBM), D. Livas (EUROCOM), C. Petersen (Otto Versand), M. Schunter (Univ. Dortmund), A. Weber (Univ. Freiburg), B. Wildhaber (r3), D. Whinnett (Univ. Freiburg).

Table of Contents

1 MANAGEMENT SUMMARY 8

1.1 Introduction 8

1.2 Surveys 8
1.2.1 Trends on the Internet 8
1.2.2 Technical issues 8
1.2.3 Legal Issues 9
1.2.4 Business Issues 9

1.3 Requirements and Definition for the Basic Trial 10
1.3.1 The Consumer Perspective 11
1.3.2 Services Offered for the Trials 11
1.3.2.1 Eurocom 11
1.3.2.2 Fogra 12
1.3.2.3 Otto Versand 12
1.3.3 Security Threats 13
1.3.4 Registration and Certification 13
1.3.5 Advanced Trials 13

1.4 Legal Framework 14

2 INTRODUCTION 15

3 MARKET DEVELOPMENTS AND REQUIREMENTS 16

3.1 Review of Existing Internet (World Wide Web) User Surveys 16
3.1.1 World-wide Use of the Internet 17
3.1.2 Growth of the Internet 19
3.1.3 Comparison of US and European Internet Use 21
3.1.3.1 General Demographics 21
3.1.3.2 Connection Speed 21
3.1.3.3 Computing Platform 22
3.1.3.4 Primary Place of Access 22
3.1.3.5 Internet Connection 23
3.1.3.6 Time Spent On-line 23
3.1.3.7 Reasons for Using the Internet 24
3.1.3.8 Problems Using the Internet 26
3.1.3.9 Costs of Internet Access: 28
3.1.3.10 Type of Internet Access 29
3.1.3.11 Subscriptions to Commercial On-line Services 29
3.1.3.12 Security as an Obstacle to On-line Shopping 30
3.1.3.13 Data Privacy 31
3.1.3.14 Web Authors Opinions of Java (GVU) 32
3.1.4 Summary of Points with Potential Relevance for SEMPER 33

3.2 Individual Expert Interviews 34
3.2.1 Technical Aspects 34
3.2.1.1 Browser Incompatibility 35

3.2.1.2 Firewall Interference....37
3.2.1.3 Understanding/Misunderstanding of Internet Technology....38
3.2.1.4 Data Storage....41
3.2.2 Legal Issues....41
3.2.2.1 Issues Related to Jurisdiction....42
3.2.2.2 Digital Signatures....43
3.2.2.3 Viewing Terms and Conditions of Sale....45
3.2.2.4 The Need for Legislation Governing Electronic Business/Contracts....46
3.2.2.5 People will do Business Electronically, Regardless of the Legal Position....47
3.2.3 Business Requirements....48
3.2.3.1 Protection of Intellectual Property....48
3.2.3.2 Secure Transmission of Data....49
3.2.3.3 Secure Email....50
3.2.3.4 Encryption....51
3.2.3.5 Non-Repudiation....52
3.2.3.6 Requirements for Electronic Notary Services:....53
3.2.3.7 Electronic Payment Mechanisms:....54
3.2.3.8 Certification Authorities - Trusted Third Parties....56
3.2.4 The Growth of Intranets....57
3.2.5 Summary of Points with Potential Relevance for SEMPER....59

3.3 Information From Presentations of SEMPER to Experts....60
3.3.1 General Feedback....60
3.3.2 Single Services....63
3.3.3 Implementation Issues....67
3.3.4 Conclusions....72

4 DEFINITION OF CONSUMER AND TECHNICAL SERVICES....74

4.1 Introduction....74

4.2 The Consumer Perspective....75
4.2.1 General....75
4.2.2 Some Basic Consumer Requirements....75
4.2.2.1 Access and Ease of Use....76
4.2.2.2 Desirable Non-Commercial Options....78
4.2.3 Specific Issues....79
4.2.3.1 Use of Digital Signatures and Storage of Valuable Information....79
4.2.3.2 Universality....80
4.2.3.3 Openness....80

4.3 EUROCOM Expertise....80
4.3.1 Current Situation....80
4.3.2 Existing Digital Services - CATE®....81
4.3.2.2 Business Level....82
4.3.2.3 Organisational Level....82
4.3.2.4 Technical Level....83
4.3.2.5 Training Services Level....84
4.3.3 General view and strategy for electronic commerce....85
4.3.3.1 General View....85
4.3.3.2 Electronic Commerce Strategy....86
4.3.3.3 Offering....87
4.3.3.4 Billing, Payment....88
4.3.4 Security Threats....88
4.3.4.1 Service Provider....88
4.3.4.2 Service User....88
4.3.5 Basic Trial....89
4.3.5.1 Specification of consumer services....89
4.3.5.2 Infrastructure....89

4.3.5.3 Trial scenario 89
4.3.5.4 Test and Evaluation 90

4.4 FOGRA 91
4.4.1 Current Situation 91
4.4.2 FOGRA's Business Services 91
4.4.2.1 Business Process 92
4.4.2.2 Fogra, Clients and the Market 92
4.4.2.3 Organisational Structure of FOGRA 93
4.4.2.4 Technical Infrastructure for Online-Services 94
4.4.3 General View and Strategy for Electronic Commerce 94
4.4.3.1 Perspective and Goals 95
4.4.3.2 Expectations on Means of Payment 96
4.4.4 Security Threats 96
4.4.4.1 Security Threats for FOGRA 96
4.4.4.2 Security Threats for the Clients of FOGRA 97
4.4.5 Basic Trial 97
4.4.5.1 Monthly Literature Survey Service 97
4.4.5.2 Organisation and Infrastructure 99
4.4.5.3 Consumer Services Offered in the Basic Trial 100
4.4.5.4 Requirements for Technical Services 101
4.4.5.5 Test and Evaluation 101

4.5 OTTO VERSAND 102
4.5.1 Current Situation 102
4.5.1.1 Existing Services 102
4.5.1.2 Existing Digital Services 103
4.5.1.3 Organisation 104
4.5.2 General View and Strategy for Electronic Commerce 105
4.5.2.1 General View 105
4.5.3 Specification of Online Consumer Services 106
4.5.3.1 Technical Infrastructure 106
4.5.4 Security Threats 107
4.5.4.1 Threats for Otto Versand 107
4.5.4.2 Threats for customers 108
4.5.5 Basic Trial 109
4.5.5.1 Business Aspects 109
4.5.5.2 Organisation and Technical Infrastructure 110
4.5.5.3 Test and Evaluation 110

4.6 Common Implementation Strategy 111
4.6.1 Registration and Certification 111
4.6.1.1 Possible Registration Procedures 111
4.6.1.2 Registration for the first trial 116

4.7 Detailed Implementation Strategy 117
4.7.1 Overview 117

4.8 Outlook to Advanced trials 118
4.8.1 EUROCOM 118
4.8.2 FOGRA 118
4.8.3 Otto Versand 120

4.9 Summary 120
4.9.1 The three Service Providers 121
4.9.2 Trial Scenario 121
4.9.3 Authentification 122
4.9.4 Integrity Protection 122
4.9.5 Transfer of signed statements 122
4.9.6 Payment 122

4.9.7 Confidentiality 123

5 LEGAL FRAMEWORK FOR ELECTRONIC COMMERCE 124

5.1 Legal Scenario 124
5.1.1 Current Situation 124
5.1.2 Recommended Structure 125
5.1.3 Legal Nature of a Typical SEMPER Transaction 126

5.2 Sales and Trade Practices 127
5.2.1 Introduction 127
5.2.2 International Regulations 128
5.2.2.1 Contracts for the International Sale of goods 128
5.2.2.2 Regulations on Distance Selling 128
5.2.2.3 Seasonal sales 129
5.2.3 Offer 130
5.2.3.1 Legal Status 130
5.2.3.2 Issues in Electronic Commerce 130
5.2.3.3 Guidelines for the SEMPER architecture 131
5.2.3.4 Recommendations for SEMPER Subscriber Agreement 132
5.2.4 Acceptance and conclusion 132
5.2.4.1 Legal Status 132
5.2.4.2 Issues in electronic commerce 133
5.2.4.3 Guidelines for the design of the SEMPER architecture 133
5.2.4.4 Recommendations for SEMPER Subscriber Agreement 133
5.2.5 General Conditions of Sale 134
5.2.5.1 Legal Status 134
5.2.5.2 Issues in Electronic Commerce 135
5.2.5.3 Guidelines for the design of the SEMPER architecture 135
5.2.5.4 Recommendations for SEMPER Subscriber Agreement 135
5.2.6 Applicable and conflicting Laws 135
5.2.6.1 General 135
5.2.6.2 Examples of Conflicting Laws 136
5.2.6.3 Sale 137
5.2.6.4 Solutions and Recommendations 137
5.2.6.5 The Role of SEMPER 139
5.2.7 Advertising 139
5.2.7.1 Misleading Advertising 139
5.2.7.2 Comparative Advertising 140
5.2.7.3 Other Advertising Restrictions (language requirements, indication of prices, advertising towards children) 140

5.3 Copyright 141
5.3.1 Transmission Rights 141
5.3.2 Private Copying and other Exceptions 141
5.3.3 Technical Protection 141
5.3.4 Freedom of Contract and Collective Licensing 141

5.4 Data Privacy 142
5.4.1 The Privacy of a Sales Transaction 142
5.4.2 EU Data Protection Law 142

5.5 Cryptography related Laws 143
5.5.1 Background 143
5.5.2 Digital Signature Regulations 144
5.5.3 Trusted Third Parties (TTP) 145
5.5.4 SEMPER Recommendations 146
5.5.4.1 Regulating strong cryptography 146
5.5.4.2 Privacy-enhancing technologies (PETs) 146

5.6 Recommendations for the Parties in Electronic Commerce 147
5.6.1 Policy Recommendations for a Regulatory and Legal Framework 147
5.6.2 SEMPER 148
5.6.3 Next Steps 149
5.6.4 Draft Technical Annex to Legal Framework 150

6 FINAL REMARKS 152

7 REFERENCES 153

1 MANAGEMENT SUMMARY

1.1 Introduction

This report deals with the results from the first year of the SEMPER project from a non-technical point of view. Individual expert interviews were performed and existing surveys were evaluated. The results are described briefly in the first part of this summary. The services and requirements needed for the first trial were specified by the participating service providers and are described in the second part of this summary. This section concludes with a brief preview of intended services for further trials. A section proposing a legal framework for electronic commerce concludes the document.

1.2 Surveys

Chapter 3 of this report presents an analysis of the results of existing user surveys, of individual expert interviews, and of reactions gathered through conference participation and presentations of the SEMPER project. Trends on the Internet are reported first, followed by a discussion of the technical, legal, and business issues.

1.2.1 Trends on the Internet

Existing Internet user surveys show that, while the USA dominates in terms of the number of hosts, the growth of the Internet is occurring mostly outside North America. However, Internet development is limited by the expansion of the network infrastructure, problems of interoperability across computing platforms, difficulties related to the acceptance of technological innovations and the cost of network access.

The review supplies a portrait of the average Internet user:

> About 30 years old and well educated, he or she uses the Internet mostly from work and for about 1 hour per day. Most users primarily use the Internet for electronic mail and web browsing. Some use on-line banking. Few of them actually buy regularly from the Internet. Subscriptions to commercial on-line services are mainly driven by promotional activities.

1.2.2 Technical issues

Insufficient network performance is regarded by most users as a major problem. It results in some of them shutting off their browser graphic functions. Organising retrieved information represents a hurdle for the Internet users, as much as finding the information on the Net.

Lack of security is another obstacle that results in users abstaining from certain types of use rather than taking appropriate steps to protect themselves. Providing a secure environment is seen as an essential pre-requisite for the spread of commercial offerings on the Internet. The protection of intellectual property rights is considered inadequate and is seen as a block to more widespread open commerce. It is expected that data privacy will become an increasingly important criterion for the Internet to become a part of everyday life.

Through individual expert interviews, conducted with people who have a professional interest in electronic commerce, several additional limiting factors on the growth of the Internet and electronic commerce were identified:

Universal access to the Internet is being threatened by the introduction of HTML incompatible, browser-specific, extensions which can prevent access or obscure important transaction-related information. To counter them, service providers are forced to restrict their web site design, offer free browsers suited to their site, or adapt their services to match their customers' browser. Interoperability is viewed as key to the growth of the Internet and of electronic commerce.

The firewalls protecting company intranets. can also act as a barrier to electronic commerce by blocking secure protocols. This could inhibit both private and business use of electronic commerce from the office.

The lack of understanding surrounding Internet technology results in security laxism, not only for data transmission, but also for data storage. Users are reluctant to deal with complicated security mechanisms and require virtually automatic solutions. Misunderstanding of Internet technology also leads to resistance from the official bodies which will have to co-operate in the development of electronic commerce.

1.2.3 Legal Issues

According to legal experts, inadequacies of existing legislation for electronic commerce act as a serious hindrance to establishing a global marketplace, both in terms of vendor strategies and consumer protection. The patchwork of laws available from different countries and the change of business practices and actors dramatically increases the complexity of resolving disputes in the electronic environment.

Digital signatures raise considerable legal problems because the term "signature" is frequently understood in relation to the paper-based business world. Digital signatures should be related to the goals they are meant to achieve and not only seen as an analogy to traditional signatures. Jurisdictions of convenience may well appear where legal expertise on the use of digital signatures develops

New rules are required for concluding contracts electronically and legally proving them. Various levels of security may also be needed, depending on the requirements of the parties involved and multi-party security is required to ensure that all partners to a transaction are protected. Business currently being conducted electronically on an insecure basis results primarily by the lack of alternative.

1.2.4 Business Issues

Moving to a digital environment makes protection of copyright very difficult to achieve. This applies to software, data banks and other electronic information products and can stifle innovation and destroy the financial incentives for creating applications. It is a paramount to address this issue in electronic commerce.

Secure transmission of other data is equally important, as the value may be high, for example, patents, personal information, or sensitive company information. Such assets must also be kept confidential for long periods of time which requires protection which is high enough to still be efficient 20 years from now. However, the current limitations imposed by the US export controls on strong encryption make global solutions difficult.

Non-repudiation of transactions must be ensured. It requires legal acceptance of electronic information as evidence in case of dispute, which has not yet been clarified. Notary services in the electronic world will be extremely helpful for neutral authentication of identity, for holding funds, deeds, etc. In addition, they may also help the parties to understand contracts correctly and could provide an electronic seal for certain types of certification.

Currently, business is restricted by the absence of universally available and secure electronic payment systems, but it is developing anyway, using payment methods like membership with monthly billing, credit card payment, withholding part of a product until payment is received, and traditional invoicing for products ordered on-line and delivered off-line. Digital cash would be more convenient for online payment, in particular in the context of low value consumer transactions.

Secure electronic commerce accompanied by on-line payments is also viewed as a potentially affordable substitute for EDI (Electronic Data Interchange) which is too costly for small and medium sized enterprises (SMEs). It could also enable consumers to implement transactions among themselves using the Internet.

The use of certificates and trusted third parties to manage certification systems is seen as important for the development of electronic commerce. The general opinion is that it is important to start establishing such services now. Companies are already doing business over open networks, despite the restrictions, and anything that can increase the certainty of the situation is welcome.

It must be expected that users will have to handle several computers from which they take part in electronic commerce, and equally, that a computer will be used by several individuals. It is also anticipated that users will have to differentiate between company and private use. As a result secure key handling is a particularly important issue.

1.3 Requirements and Definition for the Basic Trial

The chapter on requirements and the definition of the basic trial (chapter 4) describes the three different types of on-line services planned for the SEMPER trials. The chapter details the procedures and services which are being provided by Eurocom, Fogra, and Otto Versand in order to evaluate the SEMPER architecture and the technical services. A description of the consumer perspective is followed by a review of the general requirements for electronic commerce, essentially from the standpoint of service providers. Then, the business, organisational, and technical specifications of each provider are discussed, as well as their strategy for approaching electronic commerce.

1.3.1 The Consumer Perspective

For access and ease of use consumers should not be required to purchase expensive equipment or be restricted to particular platforms in order to participate in electronic commerce. It should be possible to conduct electronic commerce from any place, whether it is the home, the office, or public areas. A variety of forms of payment must be available, but the level of complexity must be kept as low as possible. In particular, warnings will have to be issued to consumers at points of no-return in the buying process. Five stages need to be considered when discussing the electronic shopping process:

- gathering information
- negotiation and ordering
- payment
- order fulfilment
- post-purchase.

During the first stage, gathering information, consumers must be able to select sellers by taking their credentials and the offered means of payment into account. Consumers should be able to seek information on the products or services they require from multiple vendors before reaching a final decision. They might even need to conduct several negotiations in parallel, placing one on hold or resuming a negotiation at the same point where it was interrupted. When they are ready to make a decision consumers will have to be fully aware of the point of the negotiation which has been reached: the goods, or services they have selected, and the terms and conditions which will apply to the transaction. Post-purchase queries should be supported, in case of dispute or to enable the establishment of longer term contracts.

In addition, consumers will need to understand their financial position, the current balance of their accounts, and be able to act upon this information. They may also need to implement payments which are not part of a market transaction, such as donations. Electronic commerce technology requires reconsidering market rules. The related procedures must aim at transparency, universality, openness, and security.

1.3.2 Services Offered for the Trials

1.3.2.1 Eurocom

Eurocom has extensive experience in providing training programs and services in the area of telecommunications, information technology, telematic services, and total quality management. Eurocom develops training and educational packages for distance learning through Intranets. These use computer-based training systems and run electronic classrooms with a multimedia interface which allows teachers to develop and manage their courses and students to attend courses, develop projects, and take exams. The system can combine animation, sound, graphics and other media to present concepts efficiently. It also keeps track of students' progress and provides them with advice. These courses are described by means of on-line catalogues. Customers may register, attend, and get billed through the network. Currently, payment is invoice-based.

For the first trial of Eurocom, marketing, secure interactive real-time multimedia communication, secure on-line billing, and payment will take place with SEMPER support. User authentication will be required. It will be based on public key solutions and individual certificates which expire upon completion of the course. Courses will be accessed using normal browsers. Payment will be on a pay-per-view basis, or for a series of courses.

1.3.2.2 Fogra

Fogra is a research institute serving the printing, publishing, and graphic arts industry. It offer services such as consultancy, seminars, symposia, publications, and literature database services. Fogra supports its clients in the digitisation of production processes. Orders are taken from either members, or non-members of the institute. As the latter pay a higher fee than the former, they need to be differentiated. Payment is currently invoice-based and includes cash, cheques, and bank transfers.

In the future, Fogra intends to offer convenient on-line access to their services, possibly in an anonymous manner, based on payments such as electronic cash and bank transfers. The initial trial of Fogra will operate with a closed group of members, in order to minimise risks. Subscription services will be offered with surveys delivered monthly. Payments can be made monthly or annually. In addition, a virtual shop will provide literature data files in exchange for payment. To support such operations, mutual identification is required, as well as ensuring that both parties share the same information, including proof of order and delivery. Services will be available, for Macintosh, Windows, and Sun platforms. Access will be possible with any type of browser.

1.3.2.3 Otto Versand

Otto Versand is the largest mail-order organisation in the world, active in most international markets, including America and Asia. It offers a whole range of goods such as kitchen equipment, furniture, clothing, shoes, etc., as well as services, such as travel tickets. In order to place an order with Otto Versand, the customer has to have access to a catalogue. This can be a printed catalogue, a catalogue on CD-ROM, or one which can be viewed on the Internet. For existing customers, customer authentication is achieved through customer identity numbers. Authorisation is granted on the basis of the customer's past payment history, in the case of established customers and a scoring system based on buying patterns, credit ratings and location is used to assess new customers. Orders can be placed around the clock, 365 days a year, by telephone, fax, letter, BTX or via the Internet. For most articles delivery is available the same day, the next day or a day specified by the customer. Payments are invoice-based. Invoices are payable two weeks after receipt of the goods. If not satisfied with the goods, customers may return them at no charge.

Otto Versand views electronic commerce as a cheaper, more efficient and convenient way of marketing than traditional mail-order and one which is capable of reaching new customer target groups. Price reductions and advertisement of new goods can be instantaneously reflected, space constraints for product presentation in catalogues can be dramatically reduced, a product can be viewed from several perspectives and hyperlinks can provide customers with advice and assistance.

The first trial of Otto Versand will use SEMPER for offering, ordering, and payment of physical goods via the Internet. Initially, payment will be based on paper invoices. Participants for the trial have been identified, using a questionnaire, and comparing the results to the SEMPER trial requirements. These selected customers will receive the SEMPER software and the required certificates. A hotline will provide assistance to customers and record problems during the trial. Disputes, however, will be handled outside the trial. The evaluation of SEMPER-based services will be compared to results from a sample of customers not taking part in the trial.

1.3.3 Security Threats

Eurocom, Fogra, and Otto Versand share common views on security threats: Their assets must be protected against intrusion in the central systems which could result in modifications of customer data. Cancellation of requests, the generation of fake orders, or modifications of the delivery status of goods and services must be prevented. Eurocom courses must be protected against illegal copying by dishonest competitors. For all three service providers, means of protection against fake servers that could ruin EUROCOM's, FOGRA's, and Otto Versand's reputation have to be found. Unauthorised customers must be prevented from gaining access to goods or services and charges must be assigned to the correct customers. Customer data, whether it is related to payment, to the services subscribed to, or to personal information, must be kept confidential in order to avoid damaging a customer's credit reputation, loss of customer privacy, or the denial of service from the service providers.

1.3.4 Registration and Certification

The three service providers share a common approach for registration and certification of new trial users. Customers, shops and services will have to register with the SEMPER-partner GMD as a registration and certification authority. Key-certificates will be marked with the method of registration in order to limit the liability of users and, thus, the risk associated. For the first trial, the users will not be held liable at all. The range of registration methods proposed includes no registration, point-and-click registration, phone-call registration, letter registration, notary registration, and mutual contract registration. Eurocom will implement the point-and-click registration method. Fogra prefers letter registration or, alternatively, mutual contract registration for members equipped with secure hardware. Otto Versand will implement letter registration for established users. The basic trial will be a closed trial, therefore, all participants have to be customers of one of the service providers.

1.3.5 Advanced Trials

For the second trial, Eurocom will port a full multimedia system to the security services that SEMPER is expected to provide for ATM broadband networks. The system will run on the Greek National Host provided by Intracom. For the third trial, Eurocom services may become available Europe-wide, depending on connection availability and costs. The communication platform of Fogra will be integrating telephony, videophony, and data communications. Accounting services will be required. If possible, services will be offered which provide Fogra customers with anonymity. The Otto Versand trials will be opened to previously unknown customers, thus requiring an appropriate certification mechanism. Virtual trolleys and a large database with intelligent search engines will be offered. Selling of travel tickets, games, software and music maybe included. Depending on the costs and the potential customer base, alternative methods of payment will be implemented.

Also services for the Regionlink companies will be defined and implemented. Regionlink joined the consortium during 1996.

1.4 Legal Framework

In complement to the above survey on legal issues, the report provides an analysis of the legal framework required for electronic commerce. It discusses its basic elements within the context of the retailer-consumer relationship and suggests guidelines on them, including the offer, the acceptance, the general conditions of sale, the applicable laws and the competent courts.

Further, the analysis suggests recommendations for a regulatory and legal framework as an absolute necessity to facilitate electronic commerce. The main results of the analysis are:

- diverse and contradictory laws in European countries on advertising, sales and trade practices, and
- use of cryptography represent barriers to the development of electronic commerce.

Removal of these barriers require harmonisation of laws in Europe. Strong copyright and intellectual property protection is critically important to the development of the Information Society. The use of smart cards containing a chip raises major challenges to Europe foundations regarding privacy. Anonymity must be kept whenever identification is not required. The right to control the uses others make of personal information must be preserved.

Furthermore, it is suggested to design an Electronic Commerce Agreement to be signed by all parties involved in electronic commerce, such as buyers, sellers, banks and certification authorities. The objective of such an agreement is to produce a well defined legal situation for all players. Therefore, such an agreement defines a set of rules to which all parties agree, e.g. on which law applies, how a withdrawal of an offer can be made or how contracts can be cancelled.

2 INTRODUCTION

The goal of the SEMPER consortium 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. Whereas most of the current developments in this field are limited to proprietary, or closed solutions, SEMPER will integrate existing architectures, tools and services where appropriate, with the aim of ensuring compatibility and interoperability of different services and service implementations. The development of the model is driven by market requirements and the state of the art in security and online information services. As a result, it will be possible to extend the model to accommodate new services and technologies as they develop. In contrast to most security solutions for the electronic marketplace, the SEMPER model is designed to fulfil the security requirements of all participants in the marketplace, i.e. it aims to provide multi-party security.[1]

In the first phase of the project, the consortium has concentrated on the development of the model and architecture and the provision of the most fundamental electronic commerce services, i.e. secure electronic offering, ordering, payment and delivery of on-line information services. The technical description of the architecture can be found in document "D03 - Basic Services, Architecture and Design", available at <http://www.semper.org> .

The evaluation of the first year trials will contribute to the planning of the subsequent phases which will concentrate on more advanced services, such as the fair exchange of documents, credentials, advanced document processing, notary services and multimedia-specific security services.

In order to ensure its broad applicability, the technical development of the architecture has been accompanied and supported by an investigation of the current commercial, legal, and social developments which influence the requirements and options for electronic commerce. The results of this investigation are presented in the surveys section of this document. The surveys are based on both a review of related research and an empirical survey of expert opinion in different OECD-countries.

The initial trials of the SEMPER architecture will be performed on the WWW infrastructure and have been tailored to meet the specific security requirements of the three participating service providers, EUROCOM, FOGRA and Otto Versand. The service providers offer three different approaches to electronic commerce in which to test the generic SEMPER model. The Definition of Consumer and Technical Services, which can be found in the fourth chapter of this document, forms the basis for the implementation of the phase 1 trials. In this section each of the service providers describes the digital product or services which will be offered in the trial, outlines its company strategy for electronic commerce and provides detailed specifications of the consumer services and test scenario.

The final section of this document proposes a legal framework for electronic commerce.

[1] For an overview see "Development of a Secure Electronic Marketplace", [WA 96] available at <http://www.semper.org/info/431ZR056.ps> More documents on security can be found at<www.semper.org/sirene>. The reader can also find useful information regarding public key concepts on the Web-sites of companies providing solutions such as "digital signatures" or "certificates".

3 MARKET DEVELOPMENTS AND REQUIREMENTS

The investigation of market developments and requirements was implemented in three phases: 1. a review of the existing Internet user surveys and related literature, 2. in-depth, semi-structured personal interviews with experts, and 3. participation in conferences and presentations, dealing with various aspects of electronic commerce.

This report contains an interim report of the survey results based on the first 12 months of the project. The aims of the surveys will be refined according to these initial findings and continue. A final survey report will be produced.

3.1 Review of Existing Internet (World Wide Web) User Surveys

User surveys directly related to the SEMPER architecture will be conducted among trial participants during and after the initial trails. In preparation for the trials the following surveys were reviewed placing particular emphasis on information regarding European users and with the aim of identifying user characteristics which could have an effect on the implementation of security measures.

[CNN95]	CommerceNet/Nielsen Internet Demographic Survey, 1995, sample size: 4,200 (US).
[FD/SVP95]	FIND/SVP, Inc., Sept.-Dec. 1995, sample size: 1,000 (US).
[FOC96]	Focus On-line Nutzerbefragung, Mar. 1996, sample size: 3,491 (Germany).
[FOR95]	Forester Research, “Conducting Business on the Internet”, O’Reilly & Associates, 1995, sample size:1030 companies, (US).
[GVU95]	GVU (Graphics, Visualization, & Usability Center, a research center affiliated with Georgia Tech’s College of Computing)-Fourth WWW User Survey, Oct.-Nov. 1995, sample size: 23,000 (global).
[GVU96]	GVU - Fifth WWW User Survey, April - May 1996, sample size: 11,700 (global).
[IST96]	IST On-line Umfrage, Nov.- Jan. 1996, Frauenhofer Institut, Südwest Funk, Telecooperation Office Universität Karlsruhe, sample size: 3,000, (Germany)

[NOP95]	NOP Internet User Profile Survey, Nov.-Dec. 1995, sample size: 1,000 (UK).
[SRI95]	SRI International, Feb.-May 1995, sample size: 1,000 (US).
[TM95]	Times Mirror Americans On-line Survey, June 1995, sample size: 4.005 (US).

3.1.1 World-wide Use of the Internet

The distribution of Internet hosts illustrated in the Table 1. below makes it clear that, in respect of the existing infrastructure, truely global use of the Internet is still very much a vision of the future. The USA continues to dominate with by far the largest number of Internet hosts in the world. Taken collectively, the countries of the European Union follow with 19% of all host computers.

Rank Jan-96	Rank Jul-95	Country	Hosts	% Total
1.	1.	US	6,053,402	64%
2.	2.	Germany	452,997	5%
3.	3.	UK	451,750	5%
4.	4.	Canada	372,891	4%
5.	5.	Australia	309,562	3%
6.	6.	Japan	269,327	3%
7.	9.	Finland	208,502	2%
8.	7.	Netherlands	174,888	2%
9.	10.	Sweden	149,877	2%
10.	8.	France	137,217	1%

Table 1 Internet Domain Survey, Network Wizards, January 1996[2]

According to Network Wizards' count of January 1996 there were almost 9.5 million host computers in the world. Although counting hosts gives a general indication of the distribution of Internet activity throughout the world, care should be taken not to translate number of hosts into number of users. "No one has any clue how many users there are, but most people would agree that there is at least one user per host." [3]

The host count figures established by Network Wizards [4] are used as a *conservative* point of orientation for examining Internet activity in Europe and are the basis for the following table.

[2] Data available at http://www.nw.com
[3] Network Wizards' Survey Observations, July 1996.
[4] Method pinging 1% of all known hosts.

Rank Europe	Rank world-wide	Country	No. of Hosts
1	2	Germany	452997
2	3	United Kingdom	451750
3	7	Finland	208502
4	8	Netherlands	174888
5	9	Sweden	149877
6	10	France	137217
7	13	Italy	73364
8	14	Spain	53707
9	16	Austria	52728
10	17	Denmark	51827
11	19	Belgium	30535
12	29	Ireland	15036
13	34	Portugal	9359
14	36	Greece	8787
15	51	Luxembourg	1756
		EU Total	1.872.330

Table 2 Distribution of Internet hosts in the European Union[5]

The rankings in the tables above indicate that, excluding the US, both world-wide and within Europe, Internet activity is greatest in Germany and the UK, with roughly 450,000 Internet hosts per country. This geographical distribution of Internet usage has guided the research presented here in two ways: 1.) it prompted an investigation of the similarities/dissimilarities of US usage (the vast majority) to European usage and 2.) led to the decision to conduct expert interviews with respondents from the three countries in the world with the most developed Internet infrastructures.

Existing survey methods for measuring the total number Internet users are subject to a number of criticisms, for example, the element of self-selection which is inherent in the response to an on-line survey and the various ways of defining Internet use. As a result, estimates of Internet usage vary from 26.4 million to as little as 5.8 million.

Source	Date	Definition	Users
International Data Corp. (IDC)	May - 96	World-wide Web surfers (May 1996)	23.5M
Computer Intelligence Infocorp	May - 96	Year-end 1995 US Internet users	15.0M
Hoffman/Novak	Apr - 96	US Internet users	16.4M
Wall Street Journal	Mar - 96	North American home/office users	17.6M
Morgan Stanley	Feb - 96	1995 Net/Web users	9.0M
Matrix	Feb - 96	1995 World-wide Internet users	26.4M

[5] Data taken from Network Wizards Internet Domain Survey, January 1996

FIND/SVP	Jan - 96	US users 1 -Internet application besides email	9.5M
Nielsen	Oct - 95	North Americans (16+) who used Web in past 3 months	23.0M
O'Reilly & Assoc.	Jul - 95	US users with direct net access	5.8M

Table 3 Cyber Atlas [6]

When interpreting survey results regarding Internet usage it is, perhaps, even more important to bear in mind the likelihood that *enthusiastic,* or exceptionally *active* users could be distorting the results. According to the CommerceNet/Nielsen study [CNN95] 15% of Internet users comprise 50% of all usage. Hoffman, Kalsbeek and Novak [HKN96] identified four user segments which also indicate a smaller group of active users.

- 1.8 mio. hard core Web users
- 2.4 mio. regular Web users
- 4.2 mio. occasional Web users
- 3.0 mio. infrequent Web users

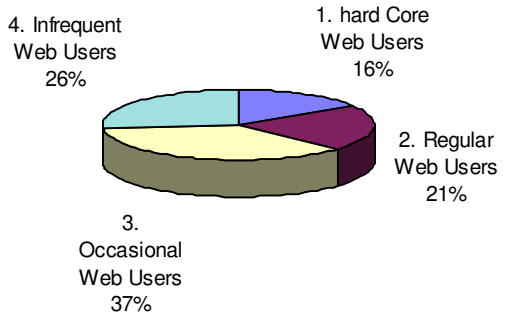

Table 4: Internet use in the U.S. 1995: Baseline Estimates and Preliminary Market Segments [7]

3.1.2 Growth of the Internet

In view of the fact that Internet use in the US is vastly ahead of that in the rest of the world and use in Canada is ranked number 4 world-wide, it is not surprising to discover that the fastest growing markets for the Internet are currently outside North America. According to an analysis made by Digital Media, significant growth is taking place among the following language groups.

[6] CyberAtlas published by I Pro last updated 18 July 1996.
[7] Ibid.

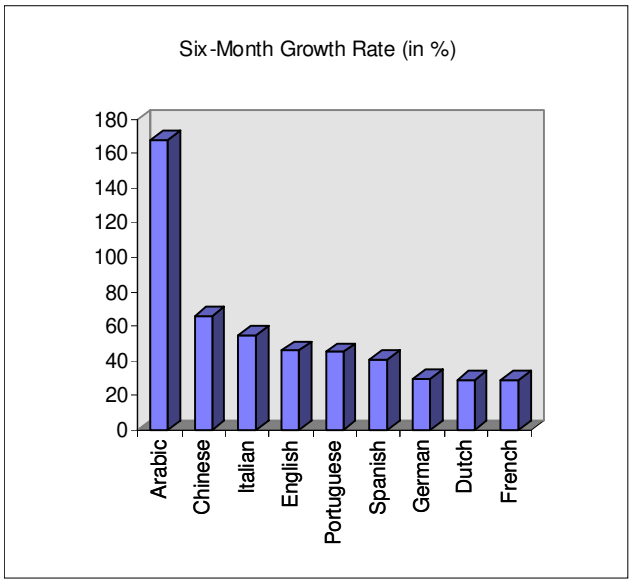

Table 5: Six-Month Growth Rate: Digital Media[8]

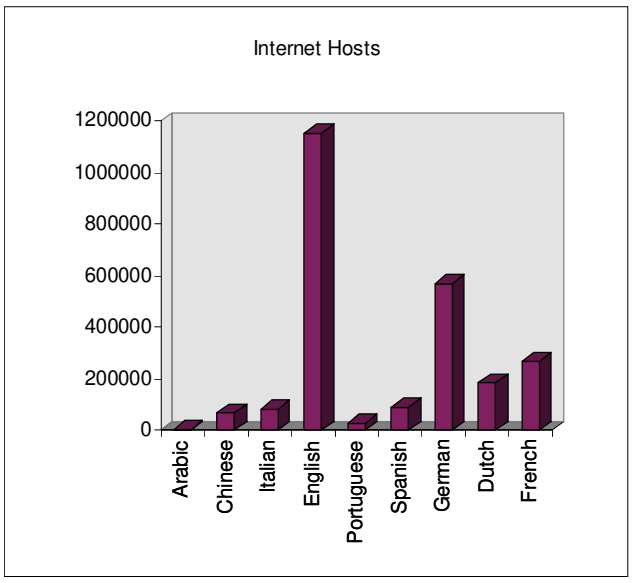

Table 6: Internet Hosts: Digital Media[9]

[8] Digital media in CyberAtlas, July, 1996.
[9] Digital media in CyberAtlas, July, 1996.

In the context of this research, however it is not important to establish exact numbers of Internet, or WWW users, or to make highly accurate predictions regarding the speed of Internet growth, but rather to establish the user characteristics and behaviour which must be taken into account when developing and implementing a security architecture for electronic commerce on a global scale. To this end the statistical reliability of the existing surveys is less important than the insights they provide into the problems end-users encounter on open networks, such as the Internet, the way they use this new medium and the requirements which are prerequisite for their participation in what is increasingly referred to as the "virtual marketplace".

To date, no comprehensive studies have been made of European Internet use, but a certain amount of comparative information is available, in particular from the GVU's 5th WWW Survey [GVU96], in which the second largest category of respondents came from Europe, comprising 10.8% of the total sample

Apart from the security and privacy issues regarding electronic commerce, which will be discussed separately, the most widely recognised hurdles in this development are the expansion of the infrastructure, the capability and inter-operability of computing platforms (hardware/software), user acceptance and understanding of the technological innovations employed and the influence of costs on access.

3.1.3 Comparison of US and European Internet Use

3.1.3.1 General Demographics

Male, young, well-educated

The average age of all Web users who responded to the GVU's Fifth WWW Survey [GVU96] was 33.0 years. One of the recurring differences between European and US users is age profiles, with European users (average age 28.8) being younger than their US counterparts (33.9). Average income in Europe is also lower than in the US and both this and average age are attributed to the stronger presence of students in the European Web user community. The US segment also appears to be integrating more female users into its base than in other countries, with 34.4% of US users being female in contrast to only 15.2 % in Europe.

3.1.3.2 Connection Speed

28.8 Kbps is becoming the norm

According to IDC/Link Resources 64% of all (US) modem users surf at 14.4 Kbps, however, the International Data Corp predicts that 19 million modems will be sold in 1996. Since most of these will be of the 28.8 Kbps variety, the make-up of the modem installed base will change significantly. [10] This prediction is supported by the findings of the GVU [GVU96], where the most common connection speed reported in the 5th WWW Survey was 28.8 Kb/sec. (39.0% of total sample) and the next most common speed 14.4 Kb/sec. (25.5%). This was a reversal of the 4th survey where 14.4 Kb/sec. connections were the most common. According to the GVU Survey [GVU96] European respondents, in general, have faster connection speeds. This is probably related to more widespread ISDN access and also to the fact that more European users access the Internet from universities and their place of work (see below).

3.1.3.3 Computing Platform

Windows predominates

More than half of the respondents (58.6%) in the GVU survey [GVU96] reported using some form of Windows, with almost as many respondents still using Windows 3.1 (27.4%) as Windows 95 (28.6%). In Europe there are a significantly higher number of UNIX users than in America (a likely result of high proportion of student users) and a lower number of Mac users, although Mac usage in Europe is increasing (20.2% in the 5th WWW survey compared to 14.1% in the 4th).

3.1.3.4 Primary Place of Access

For more Europeans than Americans, work is the primary place of access

More than half of the respondents in the most recent GVU study [GVU96] said their primary place of access was at home (55.4%) This number was also found to correspond to questions such as “Who pays for your access?”, where over half of the respondents indicated that they pay for their own access. In the US, both FIND/SVP and Nielsen Media Research discovered more respondents with Internet access at home than at work -- 68% and 62% respectively. However, an important distinguishing factor suggested by the Nielsen study is that the at-work Internet *volume* of use is higher.

According to the GVU study [GVU96], more European users than US users consider work to be their primary place of access (46.3% vs. 32.2%). It has already been pointed out that this may, in part, account for the fact that European users generally have faster connection speeds and it is, subsequently (see Section 3.1.3.9), also seen to affect the readiness of European users to pay for access to Web pages.

In the IST survey [IST96] 32% of the respondents reported using a dedicated or leased line for access (a strong indication that they are going on-line from university or work). These same users also indicated that they go on-line primarily during working hours. Users in the IST survey who access outside working hours connect exclusively through telephone lines.

[10] CyberAtlas, July 1996.

3.1.3.5 Internet Connection

Most users share an Internet connection

An aspect of Internet usage which is not directly investigated in the GVU questionnaires [GVU96], but is extremely relevant for the implementation of security, is the extent to which users share their connection to the Internet. It can be assumed that a high proportion of the 44.6% of GVU respondents [GVU96] who connect to the Internet from somewhere other than home share this connection with other persons, but even connecting from home is not necessarily an indication of exclusive individual use. Where the question was asked directly, e.g. in the Focus On-line Survey in Germany [FOC96], 63% of the respondents reported sharing their Internet access with others and 41% of the respondents in the IST survey [IST96] also indicated shared access.

> Focus On-line Survey, March 1996
> "Who apart from you uses your Internet connection?"

- 26% colleagues at work
- 18 % partner
- 14% friends
- 5% children or grandchildren

The Focus results indicated that, on average, 3.7 persons use an Internet connection.

There are no statistics available on shared access in the UK, but the advertising of Internet access providers makes it clear that it is a common occurrence. "...with your ordinary service provider, people sharing Internet accounts are forced to share a name too. Not on Dial from PIPEX, Europe's most popular Internet provider. With Dial you get up to five mailbox names on every account you open." [11]

3.1.3.6 Time Spent On-line

Average 1 hour per day

In Germany the majority of users appear to spend roughly 1 hour per day in the Net. 70% of the respondents in the IST survey [IST96] indicated sessions with a duration of 15-60 min. and the Focus user survey indicated an average of 7.9 hours per week. This is comparable to the general duration of access reported in the fifth WWW survey, where 63.8% of users indicated that they spend more than 7 hours a week using their browsers.

[11] Taken from an advertisement for Dial from PIPEX in Net User 1996.

3.1.3.7 Reasons for Using the Internet

	1994	1995
E-Mail	78%	74%
Browse Web	38%	62%
Read Newsgroups	39%	35%
Telnet/FTP	31%	23%
Interactive Chat	22%	22%
Access Commercial Services	17%	16%
On-Line Banking	N/A	3%

Table 7 - % of Internet PCs using each type of service or activity (at year end) CI's Consumer Technology Index, 1996 [12]

Electronic Mail

Email continues to be by far the number one Internet application being used by 3/4 of PC users with Internet access (see Table 7 above). However, it should, perhaps, be noted that a surprising number of email users are unaware that their mail travels via this medium and, subsequently, may also be unaware of any potential threat to the privacy of the communications which they send in this way. Business customers, on the other hand, are well aware of this problem and frequently avoid sending email via the Internet by dialling into their office networks (although this is inconvenient and expensive for the businessman abroad), in order to protect valuable company information. (see Section 3.2.3.3)

World Wide Web

Although email is the most used Internet application, browsing the World Wide Web is clearly the fastest growing application. The number of PC users accessing Web services has shown a 250% increase compared to 1994 and is now clearly the second most used Internet application. [13]

According to the GVU Survey [GVU96], which focuses specifically on Web use, search engines are the most popular user destination (65.6%). The other most frequently visited sites were on-line newspapers (37.9%), CNN (35.9%) and "other" (26.0%). A greater percent of Europeans than Americans (47.6%) report using on-line news frequently.

[12] CI's Consumer Technology Index, July 1996.
[13] Ibid.

Offering - often/very often	IST	GVU
search programmes	65%	65.6%
updates/hotlines	59%	
data banks/reference books/archives	24%	51.3
product information	45%	56.4%
leisure information	43%	
newspapers	41%	37.9%
radio information	36%	
music information	31%	
film information	27%	
special events	26%	
homebanking	23%	
travel information (e.g. train schedules)	24%	
economic information	24%	24.8% (few times)
TV information	18%	
shopping	2.2%	14.2%
travel reservations	1.2%	

Table 8 - IST/GVU Areas of use of the WWW [14]

On-line Banking

There appears to be an exceptionally high level of interest for on-line banking in Germany in contrast to other countries. 46% of the respondents in the IST Survey [IST96] indicated that they would like to be able to check balance of account and implement money transfers electronically, and 23% of the sample stated that they currently use home banking often, or very often (compare to the 3% of PC users on the whole recorded in CI's Consumer Technology Index- see Table 7). This was interpreted as evidence of German Telekom's evaluation that much of the success of the T-Online service can be attributed to the growing attractiveness of electronic banking. There is no data on homebanking in the GVU Survey.

On-line Shopping:

There are a considerable number of "electronic commerce success stories" and strong indications of a business case for electronic commerce. According to Computer Intelligence Infocorp's latest study, 2.7 million people had used the Internet for shopping, or to obtain commercial services such as banking or travel information. Nielsen Media Research [CNN95[confirms that more than 2.5 million people have purchased products and services over the Web. The success of electronic commerce is taking hold first in the most popular of all Web site categories, music. About 10,000 music sites have sprouted up all over the Web and among the 350 music distribution sites, the top five are selling more than 25,000 CDs each day. "If there's any lingering doubt about the Web's viability, Sharper Image Inc.'s chairman Richard Thalheimer dismissed them entirely: "We're already selling on the Web. We don't think there's a security problem, and apparently our customers don't either. Our sales have tripled in the last three months, and we're going to be making from $2.0 to $5 million (this year on Web sales)." [15]

[14] Adapted from Table 4.4.1, p. 16 IST96 and comparable survey results from GVU96.

[15] CyberAtlas, The Internet Research Guide, published by I PRO [CA96].

The NOP Research Group has unveiled the first wave of a comprehensive syndicated study into the commercial use of the Net in the UK [NOP95]. According to the study over 150,000 British people have used the Internet to purchase products and services in the past six months." The Internet is still very much in its early stages as a commercial tool, but our research suggests that the volume of those willing to consider a purchase in the next six months is almost three times those purchasing in the last six months." [16] Of those users who expressed an interest in home shopping, 9% said they would consider buying holidays, 11% books, 12% computer software, 9% CDs, 5% videos and 5% would be interested in buying clothes. [17]

In spite of the positive signs of growth in electronic commerce described above, roughly half of the Web users who responded to the GVU survey [GVU96] have never purchased anything on-line. Internet users appear to be gathering a lot of product information, according to the GVU [GVU96], product information is one of the most popular types of information accessed. Only 7.6% of respondents have never accessed product information on the Web; 30.1% access it on a weekly basis and 26.3% on a monthly basis) and certainly many users are taking advantage of free offers (to download software, for example), but the *majority* are not buying, at least not frequently.(See GVU data below.)

In Europe an even higher percentage of users have never used the Web for shopping but, interestingly, there are also more European users who use the Web to shop on a daily basis. What is unclear is which, of a number of obstacles, is most significant. These obstacles to on-line shopping are discussed below under problems using the Internet.

GVU All Web Users

46.4% have never used the Web for on-line shopping
33.5% have used it a few times

GVU European Web Users

58.8% have never used the Web for on-line shopping
7.6% use the Web to shop on a daily basis

3.1.3.8 Problems Using the Internet

According to the GVU survey [GVU96] the most common problems using the Web are:

- speed (80.9%)
- organising retrieved information (33.6%), and
- finding information (32.4%)

[16] Rob Lawson of NOP Network in Campaign, 23 Feb. 1996.
[17] Campaign, 23 Feb. 1996.

In respect of problems directly related to the infrastructure there appears to be little difference between the US and Europe. Regardless of location, users complain that their biggest problems is transmission speed. The problem of speed appears be growing along with Internet usage and would appear to support user perceptions of "traffic jams" on the information highway, or "Internet overload". 11.8% more respondents in the 5th WWW Survey reported this as being their most common problem than in the 4th WWW Survey [GVU95](an increase from 69.1% to 80.9%).

The same pattern was found in the IST Survey [IST96] in Germany, where 41% of respondents complained that the Net is overloaded and 3/4 of the total sample complained about slow transmission rates, in particular, for connections to the USA. A further indication of an increasingly overloaded infrastructure can be found in Network Wizards' Domain Survey Observations [NWa96] where they reported an increase in the domains they could not survey, due to servers refusing answers, or connection problems, as having risen from 20% to 34% in the last six months. [18]

Users attempt to compensate for this in a number of ways. FIND/SVP [FD/SVP95] found that 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 unless they've got a really compelling reason, because they don't want to wait. Although the GVU survey [GVU96] indicated that most respondents seem to have the hardware to support graphic-intensive content and are reporting higher modem speeds than in the past, their advice (and that of most other sources) to website designers is to consider the real limiting factor for most users, i.e. speed of connection to the Internet. An interesting finding by AT&T, reported by FIND/SVP Inc., is that "the consumer perception of on-line speed is tied more to the perception of activity than the actual delivery of content." Consumers complained that the AT&T Interchange service was "slower" than other on-line services, although the speed was, in fact, comparable. This was traced to the fact that Interchange had been presenting graphics as a *fait accompli,* rather than developing them on screen. [19]

Speed is also seen to influence users willingness to participate in electronic shopping. According to a provider of financial-information services on the Internet, what people most want is convenience. [20] "The Hermes researchers established that it is possible to accomplish a purchase using a catalogue and the telephone in two and a half minutes, whereas in the Net it took ten minutes." [21]

[18] Data available at http://www.nw.com
[19] FD/SVP95
[20] Andrew Singleton, president of Money.Com Cambridge, MA,.in BYTE, March 1996.
[21] Handelsblatt, Nr. 46 / 5.3.1996.

Difficulties organising retrieved information are a personal user problem, which, perhaps, the software manufacturers can address, but user problems with actually finding information are both an indication of the growth and complexity of the Web and also a challenge to businesses which want to establish a commercial presence. Although search engines (designed to resolve this problem) are by far the most used Web application: "It's becoming increasingly evident that search engines are no longer effective in the vast majority of searches. No search engine catalogues the entire Internet - there simply isn't a spider or enough storage space to manage such a feat. Even Digital Equipment's Alta Vista engine, which is considered the largest search engine with 11 billion words on 22 million Web pages and 13,000 newsgroups, covers little more than half the Internet's estimated 40 million Web pages. So it's no surprise that only 16% of users are satisfied with their ability to find information on the Web." [22]

3.1.3.9 Costs of Internet Access:

In the GVU Survey [GVU96] about twice as many Europeans as US respondents reported that cost was a problem, although in the IST Survey [IST96] in Germany 41% reported that they pay nothing for access, the costs being paid by universities, employer, parents or friends, which is comparable to the GVU result which indicates that European users are still more likely than US users to have their access paid for by work (43.2% of Europeans vs. 28.4% of US users). However, more Europeans are now paying for access than in the 4th WWW Survey [GVU95] (42.6% in contrast to 38:6%).

In the UK, where there are currently over 50 Internet access providers, cost of access does not appear to be such an issue. In France, however, although the apparent lack of enthusiasm for the Internet in France is generally explained by the widespread use of Minitel with 15 million regular users ($1.3 billion annual business with 25,000 Minitel services), the high cost of telephone access is also seen as an obstacle. Telecom charges in Germany are also used to explain the fact that Internet users in Germany access more from work or universities than their American counterparts. When French and German Telecom lose their monopolies in 1998 and the introduction of competitive services to the market takes place it is expected that prices will gradually begin to sink which could well be accompanied by changes in the Internet usage in those countries.

According to the GVU [GVU96] cost of Internet access may be *indirectly* affecting users' willingness to pay for accessing or viewing WWW pages. The feeling is that users who have to pay for commercial on-line services as well as telephone charges are reluctant to pay further additional charges. With each WWW survey the percentage of respondents who are not willing to pay for access to WWW pages has been increasing. In the 5th WWW Survey [GVU96] 65% said they would not pay. Users in Europe are more agreeable to paying than their US counterparts, perhaps because more of their access is subsidised by universities and businesses.

[22] CyberAtlas, July 1996.

3.1.3.10 Type of Internet Access

There are some indications that the growth of new Internet users is beginning to slow, but opinion on this is highly divided. The GVU [GVU96], for example, interpreted its findings in respect of length of Internet usage as an indication that growth is slowing. Whereas, 43.1% of their respondents reported being on Internet for less than 1 year and a further23.6% less than 6 months, 34.9% of respondents reported having been in the Internet for 1-3 years, the highest percentage ever reported in this range. "This suggests that the flood of new Internet users seen over the past year is slowing somewhat." [GVU96] Miller and Elliott would appear to agree with the GVU. In their "Informed Predictions about the personal Information Revolution in 1996" [EM95] they predict: "The number of people who will *try* the Internet in the next 12 months could grow by 5 million or more, but the number who *use it regularly* for personal communications will grow more slowly, by no more than 3.5 million people..." [23] They seem to make the same distinction as Hoffman, Kalsbeek and Novak [HKN96] (see Table 4) between *regular* use and *occasional* use.

3.1.3.11 Subscriptions to Commercial On-line Services

The growth of subscriptions to on-line services should be easier to measure, but, just as in every other area of Internet use, the statistics regarding these are also extremely unreliable. This is, at least in part, due to the fact that the promotional activities of the on-line service providers make it difficult to distinguish between real users and those who are 'just looking.' In Germany, "The companies offering on-line services are reluctant to answer when questioned about the current number of users. This is not surprising, as a result of trial offers most current users can hardly be described as customers." [Zor96] [24] "As competition for customers increases and client interest cools, companies roll out higher discounts and more special offers. Users take full advantage of them --- and switch to another company when the promotion is over." [25] Of, perhaps, even greater significance is the assertion that "As of last summer, more Americans had cancelled an on-line service than were currently subscribed to one." [26]

[23] Miller, Thomas E. & Elliott, Brendan P in "Informed Predictions about the Personal Information Revolution in 1996", FIND/SVP95.
[24] Zorn, Prof. Dr. Ing. Werner, Universität Karlsruhe, in "Visionen zur Zukunft des Internet und elektronischer Dienste", CW Nr. 3/96 19 Jan.
[25] Convergence, March 1996.
[26] Ibid.

An even greater reduction in subscriptions to commercial on-line services is expected to accompany the growth of company Intranets (see Section 3.2.4), due to the fact that a large number of these are business related subscriptions. However, neither of these observations indicate a *decrease* in Internet use, but rather a change in the type of usage as user experience increases. As private users feel more comfortable with the Internet they have less need of the support offered by a commercial on-line service provider and are more likely to choose the cheaper option of connecting to the Internet via an access provider. According to the Times Mirror's Americans On-line Survey [TM95] : "Americans who access the Internet directly are more satisfied than those who use commercial services. They consider on-line access much more indispensable than do those who use commercial on-line services." In the most recent GVU survey [GVU96] 51.6% of current users, and an even higher number of Europeans (59.2%), do not subscribe to an on-line service.

This pattern of access is reflected in the German market: "Alongside T-Online and CompuServe, with a market share of 36% together, independent Internet Providers such as MAZ, Eunet or X-Link play an important role (35%) in the access market. The category "other access" covers above all university and company access.

- own Internet access 35%
- T-Online/Btx/DatexJ 21%
- CompuServe 15%
- America On-line 6%
- Microsoft Network 2%
- "other access" 42%

Focus On-line Befragung März 1996 [FOC96]

"Forester Research believes that on-line memberships will peak at 15.8 million in 1998 and gradually decline after that. America On-line believes it can reach 10 million subscribers in 1998. Dataquest estimates on-line services revenues will reach $3.3 billion in 1997." [27]

3.1.3.12 Security as an Obstacle to On-line Shopping

"According to an ongoing survey of over 23,000 Internet users done by Georgia Tech and the University of Michigan, one major obstacle to on-line purchases is security. 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. The reason most often cited is security concerns: 60 percent of those surveyed agreed somewhat or strongly that security concerns are a primary reason for not buying." [28]

[27] CyberAtlas, 1996 I/PRO.
[28] BYTE, March 1996.

42% of the IST Survey [IST96] reported that they would like to have some form of e-cash and that, for many, this is viewed as a *prerequisite* for the spread of commercial offerings in the Internet. Older respondents (only 6% of the survey was over 40) were more interested in shopping via the Internet, the desire for a secure method of payment, however, was shared by the majority of respondents.

3.1.3.13 Data Privacy

The authors of the GVU WWW Survey [GVU96] predict that data privacy will become increasingly important as the Internet becomes a part of many people's daily live. As a result they included questions investigating this area in their most recent survey. Of particular relevance for SEMPER are their findings regarding how much users *understand* about the potential for collecting user information through the Internet and the effect this has on their behaviour. (For more detail on understanding Internet technology see technical problems section of the expert interviews section.)

"This question reveals that 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]

information recorded during a Web transaction	**% aware**
time of request	87.1%
name of requested page	82.7%
name of user's machine	71.0%
name of user's browser	59.0%
user's email address	45.2 (believed)
user's operating system name	37.9%
site id persists across sessions (aka cookies)	37.7%
user's physical location	31.7%
unaware of loggable information	14.7%

Table 9 Awareness of information automatically recorded per page request, GVU 5th WWW User Survey, July 1996

For a significantly high number of respondents in the GVU survey [GVU96] the ability to *control* the use of demographic information collected and to visit Web sites anonymously were considered essential aspects of their right to data privacy. In view of the high number of respondents who believed their email address could also be recorded during an Internet session, the fact that over a quarter reported having provided false demographic information when registering with Web sites would appear to be an attempt on the part of users to protect their data themselves. There was also strong support for the statement "ought to be able to take on different aliases/roles at different times on the Internet."

To a large extent the issue appears to be more one of control over personal data than the demand for absolute privacy (only 5.9% of the respondents reported that they would not give a site demographic information under any condition). Presented with conditions under which they would agree to provide information 78.5% agreed that they would agree "if a statement was provided regarding how the information would be used" and 59.1% would agree "if a statement was provided regarding what information was being collected". It has to be assumed that a further underlying condition would be agreement with the use stated and the type of information being collected.

3.1.3.14 Web Authors Opinions of Java (GVU)

According to the GVU Survey [GVU96], only 17.3% of respondents who identify themselves as Web authors have programmed in Java, but more than half plan to use it in the next year (58.1%). The largest category of authors see Java as somewhat secure (46.9%) and an equal amount think that Java is either very insecure, or somewhat insecure. No cross analysis was made of the level of expertise with Java (actual use) to perceptions of security, but this point was raised in the GVU report and may be investigated at a later date.

3.1.4 Summary of Points with Potential Relevance for SEMPER

- number of **active** Internet users roughly **1/2 of total** users (4.5-5 mio. persons)
- 1/2 of Internet users use **Windows** (Win. 3.1 - 27.4%, Win. 95 - 28.6%)
- modem speeds increasing - **28.8 Kbps becoming norm**
- roughly 50 % of Internet **users access from work**
- at work volume of Internet use higher than at home use
- **3.7 persons share** an Internet connection
- decrease in subscriptions to commercial on-line services
- users **shut off graphics** to increase speed, unlikely to download more than 25k
- users **unaware of all data logged** during a Web session
- 1/4 have provided **false demographic information**
- strong support for **right to use aliases**
- reluctance to transmit credit card data via Internet increases with Internet experience
- 1/2 of **Web authors see Java as somewhat secure**, 1/2 as somewhat or very insecure

3.2 Individual Expert Interviews

Persons were interviewed who have an active professional interest in electronic commerce or network technology, at a research and development level, or through their direct involvement in commercial activities, business to business, as well as business to the general public. Opinion was also sought from respondents who offer legal or professional advice to businesses engaged in electronic commerce.

Twenty in-depth, semi-structured interviews (using a topic guide) were carried out with respondents from 4 countries, the USA, UK, Austria and Germany. The average duration of the interviews was 1 1/2 hours.

Respondents came from the following areas:

- Computer related:
    - Retail Sales Software/Hardware
    - System & Software Development
    - Association representing the interests of software manufacturers
- Financial Services
- Internet Service Providers
- Legal Services
- Printing Industry
- Federal Printing Office

Presentation of Findings:

The findings from the individual expert interviews have been arranged under four broad headings: technical aspects, legal issues, business requirements and the growth of intranets. Supplementary material is used to illustrate or support interview material where appropriate.

3.2.1 Technical Aspects

In this section the problems which are being encountered in the practical implementation of existing technology are presented. These include browser incompatibility, firewall interference, restrictions arising from the misunderstanding of Internet technology and user understanding of, and resistance to, current security mechanisms. It includes the solutions which are currently being used to compensate for these problems and suggestions for improvement.

3.2.1.1 Browser Incompatibility

According to respondents one of the principal features of the Internet, its universal accessibility, is being threatened by the introduction of incompatible extension sets and there is real fear that the Net could be doomed to a future of "haves" and "have nots", depending on which software a user has.

The greatest and most frequently discussed technical problem (apart from speed of connection mentioned in the review of user surveys) facing service providers and end users alike, is browser incompatibility, or what is referred to by some as the "Web standards mess". "Until recently HTML was relatively simple and was read in the same way by all browsers. Now Netscape and Microsoft have extended the HTML command set in ways that only their own browsers can read." [29]

There are 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." (Founder of a company which makes Web authoring software).

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

> "..that's why we view our site using different browsers. With Netscape 1.1, for example, this page (laptop demonstration of site) is just a string text because it doesn't support colour HTML and doesn't support forms and tables. This is one reason we're doing so much by email, because the minimum we know customers can do is email. We deliver prices by email, offer our data download service by email, etc. We expected this problem from the start." (Financial Services Provider)

Companies operating in the Internet are currently forced to cope with the problem by:

a) Restricting Website design to the lowest common denominator

> "...the idea that the Internet allows you to provide a generic service has got to be heavily qualified. We've held back on redesigning our site for quite a long time because we knew customers had browsers which couldn't support all the functionality we were offering and also what we were trying to do was to attract customers without imposing on them an expectation that they were so knowledgeable about computers and networking that they would find it a simple and straight-forward exercise to go to Netscape.com and FTP a copy of the new browser.

[29] Convergence, Mar. '96

> 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?" (Business Development Director, Financial Services)

b) Offering customers the appropriate browser for their site (free download, special rates for appropriate browser, etc.)

> "We're an authorised reseller...which means we can give people Netscape on floppies, which is much easier and much more familiar. Netscape is industry standard. If Microsoft ran on 3.1 instead of Windows 95, I would very seriously consider Microsoft Explorer." (Ibid.)

c) Online service providers modify Web site to offer different levels of service according to the features of the customer's browser:

> "We modify the Web server and depending on they type of browser the user is coming in on. We can modify the HTML on the fly, so that it can use as many features as their browser can cope with. Initially we'll have, say, 'simple', 'medium' and 'cool'. The customer does nothing. We adjust according to the capabilities we think the browser has.
>
> I think it's just a temporary thing though, one of these days HTML is going to settle down." (Managing Director, Distributed Software Company)

According to a survey carried out by Forrester Research among Website managers, 48% chose to work with an "agile" browser (i.e. offer various levels of service according to the browser type being used), 38% chose to design their websites according to the lowest common denominator and the remaining 14 % chose to ignore users with less sophisticated browsers.[30]

A related issue which many respondents felt was crucial to the widespread development of electronic commerce is the ease of developing services. There are strong feelings that it has to become possible for normal end-users to create comprehensive Web services. The is applies to consumers, who wish to create their own homepages, and organisations alike. Bearing in mind the current rate of growth of the Internet, the general feeling is that, even at the business level there won't be enough computer programmers to cope with the demand for new services.

> "There just aren't enough programmers to go around, and, furthermore, you also want the people who understand the purpose of the content of the service to be the one's developing it, not people who happen to understand how to work with C++." (Founder of company which makes Web authoring software)

[30] online aktuell, April 1996

The problems of browser, or HTML incompatibility, mentioned in the preceding section also affect this requirement for electronic commerce. The fact that there is not a single accepted standard results in the products, which companies are developing to facilitate the development of services, also being incompatible.

> "Every view should be a good view and that's not the case at the moment. We have this problem with our authoring tool that makes HTML files from drag and drop. You don't have to learn HTML to make pages. We've made the HTML so it looks OK in Netscape and then people complain that it doesn't look good in Mosaic. And we say you can't do it because the rules are not well spelled out. In a way that's also the World Wide Web Consortium's fault. Because it wasn't specified really clearly...wasn't specified clearly in the spec. exactly what their behaviour should be and Netscape implemented it with one behaviour and Mosaic with another." (Director of Advanced Technology, software company)

According to Hakon Lie, INRIA programmer:

> "The Web should be open to all access providers, interoperability is the key." [31]

Mr. Lie, who is currently working on the development of style sheets which would standardise the presentation aspects of page-fonts, coloured text and headline sizes, no matter what kind of browser one uses, wants to guarantee a future in which every Web site is accessible to every Web user with the same quality. [32]

3.2.1.2 Firewall Interference

According to several respondents the biggest barrier to secure communication of any type via the Internet will be the company firewalls. Some had already experienced difficulty when trying to use homebanking or e-cash from their company's internal system. As commercial use of the Internet increases companies are expected to strengthen the firewall protection of their internal networks. This not only has implications for business to business communications, but may well also influence private use.

As has already been seen in the analysis of user characteristics, users frequently access electronic networks from a variety of locations, among these, in Europe to an even greater extent than in America, is place of work which is increasingly likely to have a firewall in place. As companies continue to introduce Internet technology internally by establishing Intranets (see section 3.2.4) the incidence of *mixed access* (i.e. business and private use from the same location) can only be expected to increase. Respondents mentioned two aspects of this development which have implications for secure electronic commerce.

[31] Convergence, Mar. 1996
[32] Ibid.

The most obvious one is when a company firewall prevents secure protocols from coming through, thus making it impossible for company employees to conduct private commerce from the office. In the UK, at least, circumventing this problem by connecting an independent modem connection to the Internet, is generally viewed as grounds for disciplinary action, or even dismissal.

> "Previously I wasn't too concerned about an employee hooking up a modem and going onto the Internet, while working on the internal system, but now with Java and the changes Microsoft are proposing I will most certainly ban anyone connecting to the Internet without going through our company firewall." (Managing Director of Distributed Software Company)

The second, is the records of traffic which firewall administrators keep; the whole purpose of firewalls being to control access to sensitive internal information.

A respondent who designs and installs firewalls described their function as follows:

> "The basic rule is if you don't understand a protocol, you ban it. If you're setting up a firewall you should only let through things you understand."

> "On the Internet there are well over 100 different types of protocols which you are effectively switching on and off. Time slots are even more complicated, whereby a certain protocol is only allowed at certain times, e.g. once a week when a certain type of information has to be transferred. A good firewall will only open that window for as long as the required data is being transferred and then close it down." (Software Company)

The same respondent mentioned as one of the greatest problems for security was the speed of technological change.

> "You've got the problem of the set top boxes merging with browsers and the protocols changing so quickly, the problem is to find a solution which doesn't go out of date (Ibid.)

3.2.1.3 Understanding/Misunderstanding of Internet Technology

Strong opinions were expressed regarding the extent to which Internet technology is misunderstood.. In respect of consumer perceptions, it is felt that very few end-users understand Internet technology well enough to either appreciate where the security threats occur, or to prevent abuse by personal intervention.

> "The most obvious factor by miles is lack of understanding of the Internet. To be concerned about security you have to know what TCP IP is, what HTML is, you have to know what a router is, how the Internet developed, what it was originally for, what the conception was and, if you know all that then you know how a browser communicates with the browser software, etc. and it's only then that you can start questioning whether it is secure or not." (Financial Services Provider)

In general, the experts consulted felt that consumer, or end-user perceptions of security threats 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"*. [33]

> "Security problems are more problems of awareness than a technical issue and that is just as true with corporate computing in corporate networks as it is with anything that might be considered in commerce. People don't take the care that they need to take, either because they don't know, or because it's too difficult." (Consultant to the Printing Industry)

Again, and again, it was emphasised that any security mechanism which is to be successful must be as simple as possible to use, virtually automatic.

> "Customer feedback, from the majority of those who have expressed an opinion, has been that they find the security in general an annoying feature of the system and they would much rather they didn't have to enter a user ID and password in order to be able to navigate the system. They would prefer to be able to just click on a button, HTML and graphics and get around. They find it annoying, and frustrating and irritating that they have to keep on typing in...We live in a windows world where people just want to point and click." (Financial Services Provider)

One expert was of the opinion that security can not be left to the discretion of the user, but rather has to be *enforced.* In his own company employee passwords expire after one month of use. In his opinion, the consumer would also only take proper care in creating and protecting security information if forced to do so. He also mentioned a weakness of the new Windows 95, which he was convinced few users had taken into account, i.e. the advice to disable shared files and printers if the computer is to be connected to an open network. His recommendations to the end-user on currently available ways to increase security:

> "Never use the same password from one organisation to another. You never know how securely they are storing your data.
>
> Never use the same password you use for your own internal security for an outside service. The most important password is the one which locks your computer.
>
> Passwords should be made up of letters and numbers, they mustn't be a real word and they should be over 6 digits." (Distributed Software Company)

Having made these recommendations the respondent then referred to the user problem of managing a growing number of passwords for different services, a problem which was repeatedly cited. Windows 95 has a password file, but if the security of the computer is compromised, access to this file would also be gained. He felt that it is likely that there is currently a very high number of persons who are registered with services which they no longer use because they have forgotten the password. 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, although they were well aware of the security risk involved in doing so.

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

In order to successfully deny any claims made by a customer that non-authorised transactions have been carried out, the vendor, or service provider, must be able to prove that he cannot access customer passwords. (See Section 3.2.3.5) As a result, there is little that the service provider can do to ease this user problem. A respondent from the software industry said that if a customer forgets the password to a protected file all they can do is tell him to throw it away. His recommendation was that customers be given a warning to this effect when they receive the product.

It was suggested that consumer education in respect of security mechanisms could be carried out in stages.

> "You should have functionality which you allow someone to disable. Netscape gives you all these warnings, secure, insecure, whatever, but you should also be able to say disable that now. I know what I'm doing.
>
> The user should have to disable the function himself. Personally, the first time I used the system I would want to go all the way through it very slowly and carefully and see what was going on. At that point one should be able to get additional information, e.g. there should be a link to a FAQ." (Financial Services Provider)

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.

Misunderstanding of Internet technology is also seen to lead to resistance on the part of official bodies or agencies, the co-operation of which is required to successfully implement electronic commerce. This applies particularly to legal issues, but also has implications for the way services can be made available. Under English law, for example, collecting and collating data is considered a creative act which can be protected by intellectual property rights, as a result a respondent whose company provided access to information via a data bank was bound by contract to the creators of that data bank only to offer their services to a closed user group.

> "I think that, in part, had to do with understanding new technology, with the depth of understanding of the Internet. I think one key misconception was that the Internet is a broadcast medium and, therefore, distribution of ---------- would be like putting it out on Channel 4." (Financial Services Provider)

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.

3.2.1.4 Data Storage

Although, the experts consulted were well aware of the risks of sending personal data over open networks (and only one was prepared to so), they perceived a very significant security threat to lie with the protection of data banks. In view of the amount damage which has been traced to "insider fraud" in the past, this concern does not appear to be unwarranted. Secure transmission of data was considered very important, but, secure storage of data once it has reached its goal was judged to be equally, by some even more, important. A solution which is currently being implemented by one respondent is PGP encryption of data banks.

> "If you supply credit card information to a data bank in unencrypted form it's very easy to run a snooper programme which looks for say, the first 4 numbers of a Barclays Card."

> "There was a recent example on the Internet. Someone compromised the firewall of a company, got onto the internal network and then published the customers' credit card details, just to prove it could be done. If the data bank had been encrypted this would have been less damaging." (Distributed Software Company)

3.2.2 Legal Issues

The legal experts consulted identified a number of key issues which influence the legal position of participants in the GII (Global Information Infrastructure). 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 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.

> "It is often said that existing data networks (such as the Internet) are 'unregulated'. This is, however, patently incorrect. There are innumerable laws, statutes and regulations which apply to the development, financing, and operation of, as well as the content transmitted via such networks, even though most people who use and operate these networks are unaware of the various laws which apply to their activities. This is a problem which is compounded by the ease with which such networks, and the traffic on them, span legal jurisdictions. Additionally, some who are aware of the laws in question simply choose to ignore them. Because of the nature of large-scale broadband data networks, many of these laws may prove difficult, if not impossible, to police and enforce. Thus networks such as the Internet are not 'unregulated', but in some aspects they may be 'unregulatable.' [CM96]

3.2.2.1 Issues Related to Jurisdiction

Having made the point that there are, in fact, laws which can be applied to electronic commerce, the question was raised of *which laws* will apply. In most countries parties to a contract are free to choose which law will be applicable to the contract, and it can be assumed that contracts negotiated electronically could also include a clause of this nature. This *choice of law clause*, however, does not always answer questions like whether or not the contract has been validly executed, i.e. validly signed, and under most choice of law rules this question may have to be resolved by reference to the law of the *place* where the document was executed.

> "Unfortunately, there are no hard and fast rules and depending on whether you're dealing with a cheque, a bank instrument, a bill of lading, shipping goods, a letter of credit, a contract for delivery of goods, a contract for the performances of services, contract for the delivery of both goods and services, whether the contract is domestic, international, or multinational, one jurisdiction, two jurisdictions, three jurisdictions. If you put together all those permutations you end up with probably thousands of possible answers and sometimes you have to trace through each of those branches of the chain to determine which law applies to each step of the transaction.
>
> The problem is that the technology and business practice have moved on quite a bit from when all of these laws were made. These laws are out there now and this is how courts now will have to resolve any dispute in an environment of open exchange and that's why all the multinational EDI and even most of the domestic EDI arrangements that you'll see are all based on closed user groups." (Lawyer whose practice focuses on the regulation and licensing of computer and telecommunications technology and services.)

The quote above gives an indication of the complexity of resolving disputes in a *global marketplace*. It is not only technology and business practice which have changed, however, but also the 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, small businesses and ordinary consumers are becoming involved in international small scale transactions for the first time raises an entirely new set of concerns.

A special section of the Rome Convention which deals with consumer protection, provides that even if a foreign jurisdiction is chosen for a consumer contract, the foreign law will only apply to the extent that it will not deprive the consumer of any protection he would receive under the law of the country in which the consumer has his habitual residence. From the vendor point of view, however, it is clearly impracticable to consider all the possible consumer protection laws which could apply to a customer carrying out a transaction electronically before making a sale.

If the consumers are members of a defined group, e.g. because they sign a subscription agreement, i.e. 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, or prior agreement, 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. In spite of the choice of law clause, however, customers will still be afforded protection under their national consumer protection laws. [CM 96]

> "For the merchants it opens up huge uncertainty, but from the legal perspective a lot of people believe that's the right result because consumers are usually people who don't have a great deal of resources available to them." (Ibid.)

The conditions described above will not only apply to retail transactions, but also to other transactions which may comprise a home shopping service, e.g. the contracts which bind the parties who provide or convey the advertising information, the orders, the payments and the goods.

> "The jurisdiction applying to these 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." [CM 96]

Attempts to evade jurisdictions also present a potential legal problem. This refers to the ease with which companies can move their activities from one country to another in order to take advantage of more liberal legislation. . It doesn't, of course, influence the consumer rights related to an electronic transaction discussed above, but there are those who feel it could have serious implications for data privacy, for example.

> "Data protectionists criticise that companies can build up comprehensive data banks in other countries in order to get around the strict German and American data protection limitations." [34]

3.2.2.2 Digital Signatures

In the opinion of several of the experts interviewed one of the greatest legal problems accompanying the concept of a digital signature is the very specific legal interpretation of a "signature".

> "They shouldn't call it a signature, they should call it something else. Digital authorisation, for example. You create problems for yourself by calling it a signature. At least in English common law, signature is not a term that is capable of definition. A signature is a signature and, to the extent it has been defined, it is the result of case law." (Financial Services Provider)

[34] Handelsblatt, 05.03.96.

In his paper, "EDI: the Technology of the Financial Services Revolution", Chris Reed makes an observation which could well be extended to other aspects of electronic commerce:

> "Perhaps the most important task in attempting to regulate financial EDI through contract is to analyse the transaction, not in terms of its paper analogue but in terms of what it is attempting to achieve. An EFTPOS transaction (Switch or Visa) is an analogue of a payment by cheque, but its structure is quite different. Instead of the customer issuing an order in writing to his bank, something which is clearly impossible to do electronically, the transaction is structured so that the customer merely gives his bank a mandate to debit his account. This mandate arises from the terms of the contract between bank and customer, which additionally enables the bank to include terms covering disputed transactions and who should bear the burden of proof. By structuring the legal effect of the transaction in this way, the problems posed by the Bills of Exchange Act 1882 are avoided. It should be obvious, however, that if the banks had structured EFTPOS transactions as if they were electronic cheques, using the card terms to define the EDI message as "writing" and the use of the Personal Identification Number as a "signature", there would be real doubt as to the legal effectiveness of those transactions." [Ree 94]

A frequently used current solution 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. It is similar to the banking solution described above.

> "What you have to distinguish between is what a signature is and what signifying assent is. Now, you can electronically signify assent in all different kinds of ways, because signifying assent is something you can define. I can define in a contract what signifying assent is. I can't define what a signature is because it's a concept in common law. So I have to have a signature which says that for the purposes of future use of the system my authorisation will be this." (Financial Services Provider)

The respondent's company included the following clause in its User Terms and Conditions:

> "You acknowledge and accept that instructions and actions transmitted via the ---------- system will be deemed to have originated from you, if your password and identification have been used. It is your responsibility to maintain the security of such passwords and identifications. You agree, acknowledge and accept that clicking the visual button labelled "confirm" on your screen signifies assent by you to the action or instruction being confirmed." (Ibid.)

Until the legal position regarding digital signatures is resolved it is likely that a large number of companies carrying out business electronically will continue to use solutions similar to that above. However, there are also numerous examples of companies supplying products online, without the benefit of a paper contract. Many of these appear to have enough confidence in the bindingness of electronic negotiations to make the *electronic acknowledge* of their licensing agreements, or terms and conditions of sale, a prerequisite for obtaining their product (see Section 3.2.2.3 Terms and Conditions of Sale section below).

A further complication which was mentioned in respect of digital signatures, with particular reference to the Utah Digital Signature Law, is that they will require a whole new area of legal expertise. One expert felt it was conceivable that pockets of legal expertise could develop for the affixation of digital signatures and litigation of disputes arising from their use. As a precedent for this type of development, he cited the example of the US state of Delaware, which is the jurisdiction of convenience for the purpose of incorporating companies in the US. According to him approximately 50% of all limited companies in the United States are notionally incorporated in the state of Delaware.

> "The company or corporate law of Deleware has had a lot of practice being litigated in Delaware courts. They've developed specialised courts for resolving company law disputes. There's a whole sub-culture and a whole industry around getting corporations incorporated and resolving company disputes and probably 50% of the lawyers who live in Delaware do nothing but company law all the time. If very sharp commercial lawyers in Utah try to sell Utah Law as a place for affixing signatures, that might be interesting." (Lawyer whose practice is focused on the regulation and licensing of computer and telecommunications technology and services.)

3.2.2.3 Viewing Terms and Conditions of Sale

Respondents emphasised the fact that 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. In traditional commerce, for example, an oral contract can be a legally binding for certain types of business. The absence of a requirement for a written signature, or a digital signature as a substitute for a written signature, however, does not eliminate the requirement for proof that a contract was made.

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.

> "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." (Advice of a German lawyer to companies wishing to do business on the Internet.)

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.

3.2.2.4 The Need for Legislation Governing Electronic Business/Contracts

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 and see an urgent need for new legislation:

> "I think the biggest problem at the moment is that judges don't understand electronic anything and the real issue, even here in the UK, which is pretty forward-looking in these things, is are contracts concluded electronically valid contracts? We need not only the technical capability, but also the legislation to say, yes, pushing a button, under certain circumstances, amounts to a legally binding, enforceable contract, which our courts will recognise." (Legal advisor to the software industry)

There is a need for clear contracting 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.

> "Maybe the European Commission should draft the legislation. DGXV, for example, did the Data Protection Act and has drafted some good legislation for software, if they got hold of electronic contracting it might not be a bad thing at all. Another possibility would be to work with one of the member states." (Ibid.)

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. "It could implement the (UK) Law Commission's recommendation on reform of the hearsay rule in civil proceedings. 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 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][35]

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

3.2.2.5 People will do Business Electronically, Regardless of the Legal Position

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.

> "The majority of our ordering in Germany is done via fax. The question of whether or not this is legally binding does come up a lot, but in a practical sense this is a business partner who we work with and will continue to work with. If a fight starts, essentially the partnership is going down the tube. I have no problem with fax or electronic ordering. A lot of our faxes never get printed out. They come in, sit on my computer, get dealt with, get deleted.
>
> In the past year we've bought three companies, one in Switzerland and two in Germany and all the contracts were exchanged between here and the States and all over the place by fax - and signed. The hard copy with the actual signature only came later, an original to file, but the processes were bound by fax." (Manager, software/hardware retailing company)

There is evidence that there may well be a business requirement for various "levels" of security, depending on the parties involved in the particular business application. 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]
>
> "The fax works as an implicit contract, but still, in a contested case the real contract is still the one on paper. I negotiate contracts using email. I trust people and I invest money, but I do know that if I don't get the hard copy I have no contract. I would look pretty stupid, but I do it. It's a condition of business nowadays. If you want to move you have to move very fast, particularly in this business."(Financial Services Provider)
>
> "There can hardly be a more stark contrast in the age of the "Global Village" than between the image of a computer user who may, with the press of a button, send a message almost instantaneously to a large number of correspondents around the globe and that of the political process which would inevitably be followed before all the Member States of the European Union could be persuaded to approve such a transfer. In such a situation, it is difficult to imagine most computer users doing anything other than pressing the button without any regard to the legal regime in which they operate." [CM 96]

3.2.3 Business Requirements

In this section the primary needs perceived by business in the electronic environment and the evaluation of existing solutions or proposals from the business point of view are presented. These requirements include the protection of intellectual property rights, the secure transmission of data and the related debate in respect of encryption restrictions, the importance of non-repudiation, requirements for electronic notary services, comments on payment mechanisms and opinions regarding suitable certification authorities.

3.2.3.1 Protection of Intellectual Property

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 between this section and the following ones.

> "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. The computer environment and, in particular, the Internet, makes it possible for users to obtain data extremely easily and makes it very difficult to enforce copyright protection or fair compensation for the creation of intellectual property. By many respondents the fact that there are not yet any viable solutions to this problem is seen to be holding back a lot of potential developments for electronic commerce.

> "I'm very interested in a way for people to get paid for their intellectual property, because our product makes it possible for people to deliver intellectual content on the Web. They can take anything they have published with postscript, or any of the authoring tools, and can immediately turn it into PDF and put it on a Web site. The problem is if they say this is too valuable I'm not going to put it up there. There should be an easy obvious way for them to put that on a Web site and give it to anyone who will pay them." (Director of Advanced Technology, software company)

Respondents were actively seeking solutions.. One talked about his frustration that progress in this area is so slow, that solutions aren't at least being tried. He referred to a conference presentation from the CCC (Copyright Clearing Center) that he had attended in the US and his own visions of the type of system which might be presented:

> "Before I went I started imagining what type of solutions he might propose, for example, in every electronic document there will be this little token showing who owns it, or authored it, whose intellectual property it is, with some kind of accounting number and when you open it, it pings back and counts that you used it...

> He said he was starting a consortium and wanted companies to join because there was a lot of discussion which had to take place. I acted up a bit. I said you represent the current system, why aren't you transferring this into the Web and making an electronic analogue? I was very disappointed." (Ibid.)

The software industry estimates that it lost more than $15.2 billion in 1995 due to software theft. [36] According to a Computerworld survey of information systems professionals, 47% of the respondents admitted to copying commercial software illegally, despite the fact that 78% agreed it should never be done. [37] Whereas, a large portion of the software industry's losses can be attributed to pirated software in the form of CD-ROMS and diskettes, distribution of pirated software via the Internet is also widespread.

> "Software piracy stifles innovation, destroys the financial incentives for creation of new programs and applications, and menaces the continued growth of this industry."[BSA 94] [38]

A respondent who gives legal advice to the software industry described a case in Sweden where one of the largest caches of illegal software copies was found on the Internet in Stockholm. A student had set up a server with virtually every software product on the market and was advertising it via a bulletin board. According to the respondent the legal situation regarding such activities is very unclear. The person running the bulletin board was not violating copyright law because he was not copying and distributing, but the people visiting it to obtain products were. The situation at the moment is usually judged on a "knowledge or notice" test, which means if you know of a violation and have the physical ability to close it down you should. However, he also went on to cite a case which went to court in the US against a young man who had distributed over a million dollars worth of software. There was a problem with the criminal code because he hadn't done it for profit. It was possible to bring a civil case against him but according to the law a criminal case is not possible without a profit motive.

Solutions for secure delivery of software through the Internet were 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 encryption keys to open each one, delivering keys separately by email, etc.

3.2.3.2 Secure Transmission of Data

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, for example. Encryption is generally viewed as the most efficient form of protection.

---

[36] Business Software Alliance press release 4/96, t:\bsa\globeinfo.doc
[37] Computerworld, May 22, 1995.
[38] The Business Software Alliance, Worldwide Report, 1994.

> "Headers or electronic envelopes, encryption and other tools will be essential to maintaining the integrity of works." [39]

A respondent from the Federal Printing Office in Germany emphasised the requirement for secure data transmission using two examples, the distribution of patents and the transfer of the personal data required for passports. In respect of patents, the financial value is extremely high. They are currently distributed via CD-ROM. If it were possible to make patent information available online (which would require absolutely reliable data security) it would be possible for smaller companies to purchase smaller amounts of information at more favourable prices. In respect of personal passport data, it is currently transported physically by courier.

3.2.3.3 Secure Email

For 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." (Internet Access Provider)

> "The outsourcing of information services continues unabated, and it does indeed make sound financial sense for international travellers to use a global service provider. But information is a valuable commodity and the subtler implications of information security should not be overlooked in the name of convenience." [40]

> "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."[41]

[39] The Business Software Alliance, Worldwide Report, 1994.
[40] Somogyi,Stephan, "Netting from Anywhere", Digital Media Perspective, 15.03.96.
[41] Robert Carolina, Attorney from London law firm Clifford Chance, in Convergence, March 1996.

In the opinion of virtually all respondents the problem is not one of a lack of products, but rather the effect of US export controls on strong encryption (see below). The only indication of change in these restrictions, however, will ease this problem for the US traveller abroad, but does nothing to help the European user. An Amendment to the International Traffic in Arms Regulation passed on 16 Feb. 1996 [PUE96] [42] introduces a "personal use exemption" clause. The implications of this amendment are that "secure communication" will be available to the US user abroad, as well as at home. It permits use of strong encryption for permanent US residents/citizens for temporary use outside the US. This will facilitate, for example, the sending of secure email over open networks and eliminate the necessity of using expensive "dial-in" services to reach internal company networks.

One respondent indicated that his company was using PEM (Privacy Enhanced Mail) for particularly sensitive areas of business, in this example for high value transactions:

> "The broking service requires you to have a separate alpha-numeric identifier with which you authorise buy and sell orders. So you've got a user ID and you've got a password and you've got what's called an URN, unique reference number. And within the brokerage service we run privacy enhanced mail, so even if you don't have secure email, if you're on the brokerage service you get email from the broker within a secure environment. It doesn't go to your normal email box."(Financial Services Provider)

Security fears often result in companies not using email for commercial correspondence. According to a representative of one of the UK's major banks:

> "There's not a strong enough business reason to compromise security by getting external email links for the company."[43]

3.2.3.4 Encryption

The examples above illustrate the business requirement for the use of strong encryption which was voiced by most of the respondents.

> "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." (Legal Advisor to the software industry)

> "Some of the solutions proposed, e.g. the position of the French government, have exactly the opposite effect of the one we want, i.e. being able to facilitate economic arrangements between countries. French software manufacturers and French users are at a huge disadvantage to their international counterparts, because following the letter of the law (and I'm not sure they always do), because Banque de France, or whoever, unless they've complied with French regulation will have to use much less secure systems than people outside France." (Ibid.)

[42] Federal Register, Vol. 61, No. 33, Department of State, Public Notice 2294.
[43] Spokesman for Britain's National Westminister Bank, PLC, in Convergence, March 1996.

In view of the rapid advances in computing power it is also assumed that 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.

> "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 decades. DES, for example, has been in use for more than 20 years and will probably continue to be employed for several more. In particular, the life of a cryptosystem is likely to exceed the lifetime of any individual product embodying it."

> "to provide adequate protection against the most serious threats - well-funded commercial enterprises or government intelligence agencies - keys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years in the face of expected advances in computing power, keys in newly-deployed systems should be at least 90 bits long." [BDR96]

3.2.3.5 Non-Repudiation

As mentioned above, the question of non-repudiation is clearly linked to the legal question of the type(s) of (electronic) information which will be accepted as evidence should a dispute arise (see Section 3.2.2.4) and also creates technical problems for the user who forgets a PIN or password (see Section 3.2.1). Companies currently doing business on the Internet take advantage of every available possible means to protect themselves.

> "I prefer to be as safe as safe can be at this point and the principle problem which we face, given the threat analysis that we performed, is not hacking, it's repudiation by a known user. That's why I'm very keen on continuing to require users to self-certify effectively...having to enter their user ID and their password in order to be able to navigate their way around the system because we log all that on the audit. We log user activity and it means that, if necessary, we can go back and say on this day at this hour, minute, second you accessed this page. And I have to be able to do that, not because I'm trying to collect demographics on user behaviour, but because a user could perfectly well come back to me and say..."I didn't buy these shares, I only buy shares that go up." (Financial Services Provider)

When questioned about the extent to which the evidence produced by the system used by his company is considered legally binding the respondent mentioned that they had sought legal advice when setting up the system.

> "The test seems to be how the access log is written and whether it could be edited. Our audit logs are written automatically, straight from the Web server and there is no way of editing them. The way the system is set up, they can't be written by anything other than the Web server and they can't be edited. The only way I could get a page to be written by the Web server saying that you had come in, is if I came in with your user ID and password." (Ibid.)

3.2.3.6 Requirements for Electronic Notary Services:

The notary services described here do not refer to the notary services which would be involved in the administration a certification system, i.e. would provide such services as time stamping of certificates, maintenance of revocation lists, etc. but, rather, notary services which businesses currently require for traditional transactions and could envision being conducted electronically.

Respondents drew parallels between their experience of notary services in traditional commerce, applied these to the electronic context and then evaluated the usefulness, or the feasibility of implementing such services electronically. This process almost always resulted in the identification of suitable applications, as well as notary services which could not reasonably be duplicated in the electronic environment. The four main roles of the notary in traditional commerce which were mentioned by respondents were:

1. Neutral authentication of identity and/or other information regarding a person or business
2. Acting as a Trusted Third Party by holding funds, deeds, etc.
3. Ensuring that a party to a contract had read and understood it.
4. Certifying that the party to a contract was in sound mind and acting of his/her own free will.

.

> "I'm trying to think of the role of the notary and if everything he does could be done electronically. One part of the notary's role is as a silent, unbiased party to state that this person is this person, that he understood what he was doing, because what happens with contracts when a fight comes is that the person says he didn't really know what he was signing. Part of the notary's role is to make sure the whole contract has been read through and understood by the person signing it and that they were in sound mind, weren't drunk, or there wasn't somebody standing behind them with a gun - how could you do that electronically?
> The notary also often becomes a sort of clearing house, often neutral ground where the money is held, but that works well electronically."(Software Retailer)

In general, respondents felt that the notary services 1. and 2. could not only be achieved well in an electronic environment, but would, in fact, offer a considerable improvement over the current situation.

> "I'll give you my very frank, personal opinion of notaries. I think the notary is a dinosaur. It's a holdover from days gone by. I've seen a lot of things done over a notary's stamp that weren't worth the paper they were printed on.

> It's 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." (Legal Advisor to the software industry)

When asked who should, or could, implement such a system, the reply was similar to the opinions expressed regarding certification authorities in general (see below), i.e. it doesn't matter who does it as long as their authority is recognised:

> "You could have any range of people, as long as the thing were fairly automated. For example, if a US, or UK company were doing business in Russia (which is probably the worst example of this kind of business) and the company had its corporate registration on file with the Trade Registry, or Companies House, or something similar and wanted to get a message to the Russian Ministry of International Investment that this is a real company and here are the details. If the company could address such a request, push the button and it would go to the Trade Registry which would forward the information electronically to the Russian Ministry, that would be a very useful function." (Ibid.)

The notary's role is 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. (Manager R&D, German Federal Printing Office)

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* of certification to cater to the requirements of various business situations.

3.2.3.7 Electronic Payment Mechanisms:

Among the experts interviewed (only one was directly involved with an electronic payment system) there was a high level of awareness of the various solutions which are currently being developed, but there was no strong support for any one system, or form of payment. The general feeling was that electronic commerce will be similar to traditional commerce to the extent that a *variety* of payment methods and mechanisms will be required. Respondents felt that the choice of payment method will continue to be determined by the personal situation of the customer and the requirements of the particular purchase situation. Predictions from various market research companies also indicate that there is no clear preference.

> "While Killen predicts that e-money will be a major force in online payment systems, Forrester believes that credit cards will be the primary option for consumer purchases made over the Web. According to Forrester Research, 84% of a sample of 50 online retailers and content providers already accepts payments online and the majority of these payments are made with credit cards."[44]

[44] CyberAtlas, The Internet Research Guide, published by I PRO, last updated 18 July 1996.

Forrester's results are not surprising, considering the fact that payment by credit card is the only online payment method which is widely available at the moment.

There was consensus that the way business is currently being conducted over the Internet is restricted by the absence of a reliable electronic payment system, but it is developing in spite of this restriction.

The methods which are currently being used include:

1. Membership, or subscription, with monthly billing which allows payment by the usual variety of payment methods (credit card, direct debit, standing order) and also facilitates low value transactions

2. Credit card payment with the credit card details being submitted to the vendor via the Internet or traditional means (fax, post, telephone)

3. Withholding part of a product until payment details have been received, e.g. software - online delivery of partial, or "trimmed" products (full version supplied after payment), full product documentation withheld until payment is received, fully featured version which "dies" (time limit on URL).

4. Traditional invoicing, or C.O.D. (collect on delivery), for products ordered online and delivered off line.

Several respondents mentioned that the current situation results in the telecoms which offer Internet access having a considerable advantage because they have an established billing system.

The advantages of digital cash were mainly seen for low value consumer transactions involving digital products (products delivered online, such as software, or information) and the general attitude was, "as soon as the banks, the regulators, etc. have got it all sorted out, we'll use it." For businesses selling on the Internet consumer acceptance of digital cash was also seen to be a leading factor:

> "We'll look at different kinds of currency and the different kinds of banking mechanisms and we'll do our best to make sure we can match buyers and sellers. That's what my business is. If, in five years time, I've got people who have Mondex wallets, then we'll do our best to deal with Mondex wallets." (Financial Services Provider)

A number of criticisms of the systems currently being developed were also expressed, in particular, having to tie up sums of money in special bank accounts (First Virtual), or coins (DigiCash). The disadvantages were compared to those accompanying the use of traveller's cheques, with the obvious questions regarding the influence of fluctuating interest and exchange rates. The question of currencies available as ditital cash also arose and, of those who were unconcerned about records of their transactions being kept, some would prefer some sort of "virtual charge account".

> "If I have to go and do some transaction to get myself some kind of "virtual" 20 dollar bill, or electronic coinage...say to someone take some real money out of my bank account and give me some virtual money. Why not pay at the end of the month, just like the phone?" (Director of Advanced Technology, software company)

In respect of non-digital products the general feeling was that it would be unreasonable to expect customers to pay online for a product which they would only receive later, although some potential was seen for the payment of an online deposit for high value orders.

The greatest advantage of online payment for business to business transactions was seen in the enabling of speedy, reliable transactions between businesses which had no previously established business relationship and no reason to establish one (infrequent, or one-off purchase situation).

3.2.3.8 Certification Authorities - Trusted Third Parties

There was no clear opinion regarding agencies or organisations which would prove acceptable as a certification authorities. Suggestions included officially recognised bodies such as the department of trade and commerce, the post office, banks, through to non-governmental organisations. There also seemed to be a distinction between organisation which would be recognised by private individuals and those which would be accepted by businesses, with a tendency to the opinion that private consumers would trust governmental organisation, whereas trade and industry would not. The general view seems to be that the process will be an evolutionary one and the critical factor at the moment is not who plays this role, but rather that it is set in motion, that its effectiveness can only be evaluated by practical application.

A frequently voiced opinion was that there is no reason to believe that the technical solutions to the requirements of electronic commerce will function perfectly from the start, but that shouldn't be a reason for delaying their implementation. As has already been mentioned in the legal issues section, companies are doing business over open networks in spite of the restrictions and anything which has the potential for increasing the certainty of their situation is welcome.

> "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. We have to have digital certificates that France and Germany and the US and everyone agrees to. 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." (Director of Advanced Technology, software company)

One respondent was able to report first hand experience of a problem with server authentication.

> "One of the companies in the States that was doing server registration had some problem which meant that a lot of its certificates out there in the world expired and it didn't notify anybody. One of them was us. We found out, fortunately, just by doing random checking, because we're very aware of security. Can you imagine if you're dependent on a third party for server certification that the third party forgets? It happened. Just imagine if some customers had come along and checked that we really were registered and got a message...don't know, server not registered." (Financial Services Provider)

3.2.4 The Growth of Intranets

The significance of Intranets for the development of electronic commerce generally and the implementation of a security architecture specifically will depend on the extent to which firewalls create problems for security protocols and the relative importance of business to business applications for the development of electronic commerce. In any case, the growth of Intranets is one of the most striking recent developments in the area of electronic communication and should be taken into consideration.

> "It's all very well to talk about the Internet for communication between businesses. We believe the real explosion in Internet-usage is as an internal communication system. The key to exploiting the Internet is to deploy it within the corporation as a cheap alternative to the family of software programs known as workgroup products. External access to the local Intranet can then be guarded by security software that bars unauthorised access." [45]

According to Forrester Research, nearly one out of four Fortune 100 companies already uses an internal Web-server today and Netscape, the Internet software supplier, reports that most of its Web server software sales to companies are for internal rather than external use. [46]

Intranets offer large organisations two distinct advantages that the Internet does not:

> **Security:** Because intranets reside in secure organisational networks, intranets routinely offer valuable information companies do not make available to outsiders.
>
> **Bandwidth:** intranets run on ethernet, or even faster ATM networks, are able to offer full-motion video, something most Internet users won't experience for a while.[47]

"Most analysts predict rapid adoption of intranets by corporations world-wide. Two thirds of all large companies either have an internal Web server installed or are thinking about it, and industry analysts believe that soon internal Web servers will outnumber external ones ten to one." [48]

[45] Bill Martorelli of CSC in "High level of anxiety over security measures", Financial Times Review, April 3 1996.
[46] "First the Internet: now the Intranet phenomenon", Financial Times Review, April 3 1996.
[47] Ibid.
[48] CyberAtlas, July 1996.

"The market research company Input estimates that the market for firewall software and services will grow to DM 16.2 bn by the year 2000. (average growth rate or 70% per year). [49]

[49] Handlesblatt, 06.03.96.

3.2.5 Summary of Points with Potential Relevance for SEMPER

- **Browser incompatibility** is causing confusion and inconvenience for users and makes developing services difficult for merchants. Could influence understanding of any security procedures/mechanisms which must be viewed using a browser.
- **Company firewalls** can block protocols. Growth of Intranets is accompanied by growth in use of firewall technology.
- Users are aware of security threats, but not of how to avoid them. Awareness of risks results in **non-use** rather than **care-in-use.**
- End-users want **simple to use**, virtually automated **security procedures.** Management of multiple passwords/phrases is becoming a problem.
- Merchants want to protect their data banks from internal, as well as external attacks. Some are **encrypting** their **data banks.** Need to be able to repudiate any claims of manipulation of data or unauthorised access.
- **Inadequate methods for protecting IPR** are seen as barrier to "open" commerce, results in formation of closed user groups.
- Business wants **strong encryption** to protect data transmission, secure email.
- **Levels of authentification** are required:
    - "electronic assent" - for consumer transactions which don't require a signature
    - "electronic signature" - for consumer and business transactions which require signature
    - "electronic handshake" - authentification between established business partners
    - "electronic seal" - to replace notary's seal (level higher than digital signature) for very high value transactions
- **Need for legislation** which reflects technological advances, i.e. clear contracting rules for electronic contracts, clarification of proof, etc.
- Businesses are **willing to experiment** with solutions, electronic commerce will only progress through practical experience.

3.3 Information From Presentations of SEMPER to Experts

In this section results from interviews and discussions concerning the initial architecture, single technical services as part of the architecture, and the implementation as planned for the basic trials (see chapter 4 of this document) are presented.

The feedback has been gained from several sources. The first source is feedback from presentations of SEMPER at conferences and to groups. The basis for the presentations was (Wa 96).).)).The presentations described here were given in Germany, Japan, Norway and the US. The second source is feedback from presentations to individuals. Twelve such presentations were conducted in Belgium, Germany, Luxembourg and the US, lasting from one to three hours. Respondents came from the areas of retailing, multimedia, banking, the electronics industry and Internet service providers. The third source is short interviews made about SEMPER and its building blocks like payment or signature schemes. Such interviews were made at conferences or via phone. 47 such experts came from Belgium, Finland, France, Germany, Japan, Norway, Sweden, Switzerland, the United Kingdom and the US. Respondents were not only from the areas mentioned above, and also from telecoms and government.

3.3.1 General Feedback

In general it was appreciated that SEMPER covers the whole business cycle from authentication and offers to secure delivery and clarification of disputes.

> "I don't think that anyone is taking the high level approach to it and looking at all the various pieces and trying to pull it together as one cohesive electronic commerce whole." (Internet technology provider)

Respondents also like the concept that other scenarios such as auctioning or contract signing can be added to the commerce layer. It was also unanimously appreciated that different modules for providing services, such as payment mechanisms, can be hooked into the SEMPER architecture depending on what the parties wish to use. Several speakers at the Electronic Payments Forum (EPF, July 1996 in San Francisco) emphasised that they are looking for a system which offers the integration of payment into purchasing, fulfilment, IPR (intellectual properties rights) protection, and sufficient digital documentation for dispute resolution, preferably automated dispute resolution.

Respondents viewed SEMPER as ambitious and unique. Similar goals are only covered by the US-American ECOSYS proposal, by Sun's Java Electronic Commerce Framework and by the initiative by the Norwegian Regnesentral, called "Open Networks as the Future Marketplace." Some respondents said that an architecture covering all steps from offer to delivery is, in principle, already available for EDI users (e.g. a representative of a Chamber of Commerce).

Respondents generally liked the concept of multi-party security, in particular not having to rely on a computer record of the other party, to get digitally signed statements of what was transmitted, to have fair exchange (e.g., of information against digital cash), and to protect privacy where required.
Also in Japan interest in security technologies has increased, where in the past it was reported to have been less of an issue. Recently NTT had to pay for a fraud of $ 500 million with counterfeit "pachinko" magnetic prepaid cards used in gambling. Stolen readers were used to write amounts on stolen empty cards. Part of the problem was that the "readers were capable of writing" (a representative of the National Bank of Japan). The Japanese respondents found the architecture attractive because digital cash can be hooked into it (more on this below).

Respondents also appreciated that the consortium intends to publish the specifications of the architecture as done with the payment protocols SEPP and SET (e.g. a member of the IETF).

Respondents expressed that consumer understanding will be an obstacle to any secure electronic commerce and that "a huge educational effort" (an Internet technology provider) will be necessary before trust can evolve whatever the solution will be. To some people digital signatures would just be "black magic" (an Internet service provider).

- **Fields of Electronic Commerce**

Respondents liked the concept of having different business applications, depending on the business in question and on what is available as a service on the commerce layer. Some scenarios envisaged affect the design of the architecture and the required tools to be implemented and are therefore reported here.

- **Business-to-Business and Business-to-Government Commerce**

As opposed to what has been discussed in the media for the last few years, discussions were focused not only on the case of a merchant selling from his server to private customers, but also on peer-to-peer like settings. Some experts believe that this is the major field to come. For instance, the US government with its National Information Infrastructure (supported by NIST) and the Swedish government are active here (see Hor 96). A possible path is that the government defines the rules first for transactions within the government, e.g., when transmitting documents from one agency to another. The second step would be that the government uses electronic documents for procurement. Finally businesses would use the same procedures among each other.

> "The (US) government is really an important player. It has hundreds of thousands of trading partners... There is a spin-off from there." (Internet technology provider)

If this path should not be taken it can expected that businesses will use the Internet for transactions among each other without government incentives out of their own interest.

Examples of why this is attractive are given in chapter four where the SEMPER partners Fogra and Eurocom describe how they want to do business-to-business transactions. In Europe it is being discussed that there are millions of SMEs requiring cheap access to electronic commerce not only for selling to private customers, but also to other companies, similar to EDI, as became clear from statements of SME-representatives at conferences in the framework of the G7-initiative "A Global Marketplace for SMEs". Some companies require a cheap replacement for EDI with easy accessibility. Also other examples have been thought of, e.g.:

> "Can the Internet be used to improve the payment systems?" (a banker)

The question here is whether an "improvement of the efficience of the backend" is possible. It is considered to make clearing cheaper as well as to make the credit card authorisation networks cheaper by going on the Internet and reorganising procedures at the same time.

Electronic documents can be very attractive in cases where businesses cannot wait for an express courier, as it was discussed in CommerceNet. As the value of such transactions is usually quite high, it is imaginable that prior registration in order to get a certificate and the cost of key management can relatively easily be justified.

With such transactions between businesses it can be expected that players will be both selling and buying, sometimes using a WWW-server, sometimes communicating only via email. In such settings bank transfers or electronic cheques may be used more often than credit card payments or digital cash. Very trustworthy implementations will also be required because of the high values involved. There is a potential of millions of SMEs who could participate in such commerce and who will require implementations which are easy to install and use.

- **Consumer-to-Consumer Transactions**

Respondents also referred to the possibility of consumer-to-consumer transactions. For instance, a computer scientist from Norway reported that it was a great success when consumers were given the possibility to "advertise used cars." In one survey it was found that

> "many 'consumers' are busy becoming 'providers', setting up home pages" (FD/SVP 95)

With a home page, consumers can easily offer something for sale. This market segment is small today, but attractive as there is a potential of many millions of users who could trade among each other. Many solutions developed for business-to-business transactions as described above can be reused for consumer-to-consumer transactions, e.g. payments with other means but credit cards.

- **SEMPER and Telephony**

Some suggestions on possible integrations of SEMPER and telephone systems were made:

- It was pointed out that in many European countries there are more GSM-users than Internet users (3-4 million GSM users in Germany compared to around 5 million active Internet users world-wide according to section 3.2.1 of this report). Can SEMPER be designed for the use on GSM? The use of handheld phones leaves only very little space for security interfaces, as a representative from a trading company emphasised.
- It was also referred to using mobile phones for browsing the WWW. This will also leave little space for security interfaces. On the other hand, it was suggested that mobile phones could be turned into "secure hardware" displaying contracts, amounts etc. in a trustworthy way.
- A researcher working for telecoms suggested that it could be possible to pay for the Internet access or the telephone access using the same payment tools which are also used on the net, e.g., digital cash (see <www.eu.net>). This suggestion leads to a more general requirement. If a system also exists outside the SEMPER-supported environment, then the user should be able to use it also outside SEMPER.

- **Price Comparison**

The comparison of prices came up as an issue in several interviews. E.g., a representative of a US mail order company reported that consumers interviewed required this. It was also said that one of the main advantages of the Internet is to be able to compare prices and buy abroad if necessary. Also bargain finders were discussed enthusiastically, e.g., at a conference in Norway. The current implementation of SEMPER with several sessions in parallel will support price comparison and can thus handle requirements for price comparison.

3.3.2 Single Services

SEMPER provides for integrating different service implementations. Respondents found it particular attractive to be able to integrate different payment mechanisms. They also found it important to be able to integrate different encryption tools. With regard to signatures, experts emphasised that there are still some uncertainties and that digital signatures can be designed in many different ways. First, reactions regarding payments are described.

- **Payment**

SEMPER is designed to handle different kinds of payment technology. This is particularly attractive for the following reasons:

- The definition of SET is not yet finalised and there is a possibility that different solutions for credit and debit cards, for debit/credit chip cards or for cards from specific payment systems or banks will emerge (several US respondents). "We cannot use SET for everything", as an Internet service provider put it.

- Some US banks expect that there will be a business case for electronic cheques, e.g., in order to have a non-revocable means of payment (less risk for the retailer), for less creditworthy individuals, for higher amounts, because of smaller fees for large transactions (ECU 1,000 to 100,000) as compared to credit card disagios, for business-to-business or consumer-to-consumer payments, or with a payment guarantee as with a Eurocheque (see FSTC [Financial Services Technology Consortium] electronic cheque project; discussions at the Electronic Payments Forum EPF). It was suggested to store the electronic cheques in tamper-resistant devices in order to avoid double presentation by mistake or on purpose (fraud).
- Digital cash (stored value, ecash) is intensively discussed in Japan, Europe and the US. One, but not the only driving force is to find cheap methods for micropayments. Particular emphasis to digital cash was given by a Japanese speaker, Yasuhisa Shiozaki, member of the House of Councillors, who said that "electronic money will obscure the difference between cash and deposits" (at the EPF). Different variants of digital cash are expected (special ecash accounts, anonymous and non-anonymous transactions, fast transfer of large sums, etc.).

- **Confidentiality**

Respondents generally liked the idea that different encryption tools can be hooked into the architecture depending on what the players wish to use and what is available in their respective countries. Several respondents referred to PGP being a de facto standard, and to the issue of exporting strong encryption procedures out of the US. It was said that the restriction to short key length no longer makes sense as criminals can use strong tools anyway. Leiberich, the former head of BSI, the German agency for certifying the security of computer systems, stated:

> "In general it will no longer be possible to decrypt information, which has been encrypted by criminals, by making a crypto-analysis." (Lei 96, p. 10)

For European companies competing with US or Russian companies strong encryption was recommended as their secret services are capable of scanning all business communication. Recently, the German industry suggested strong encryption:

> "Strict opposition to the regulation of cryptography for the purpose of maintaining the wire-tapping capabilities of the security services.(...)Against the background of measures of evasion, any regulation would miss the mark." (Statement by the German Industry on Cryptographic Policy on the occasion of the OECD consultations on September 26-27, 1996; Nie 96)

It was also said that it will be beneficial for users to have separate keys for decryption as for signing because they will wish to have a backup of the decryption key, whereas they do not need a copy of a signature key because they can easily generate a new one.

Pseudonymity of orders and hiding who communicates with whom was also mentioned.

- **Signatures**

In general, delivering parties require non-repudiation of an order. It was also pointed out by a legal expert that digital signatures under commercial documents are advantageous for the buyer, too, who gets protection against having to pay for goods not ordered or against wrong debits.

With the SEMPER-architecture one can in principle handle both PGP-signatures and signatures systems with X509 certificates. The respondents generally favoured the X509-approach which provides the advantage that a third party can confirm who signed. It was, however, questioned by one security expert whether X509 v.3 certificates can be managed on a global scale because of their size and complexity. To learn what the certificate and thus the signature means, what the certification authority has done and the signer agreed, and finding out whether the key was revoked, can be very time consuming if not close to impossible on a global scale with hundreds of certification authorities and lots of options in the certificates. Such a global effort would be“doomed to failure”, as that computer security expert put it.

One legal expert said that also out of a PGP-like structure legal bindingness can arise if businesses increasingly used such an approach. As respondents said that little experience has so far been made with X509 v.3 certificates for private customers (applications should be put into a “hall of fame”) it is advisable that SEMPER remains open for different signature mechanisms.

Some respondents pointed out that digital signature procedures have some general weaknesses to which the parties and their lawyers could refer to in a dispute, e.g., at court. These are reported here because the consortium will have to take them into account when designing solutions. The following issue were mentioned:

- Two persons may have the same secret key by coincidence.
- A foreign secret service may have broken the algorithm, but won't tell.
- Passphrases and PINs may be too short so that criminals can relatively easily make an attack on a secret key being in encrypted form on a disk or a chip card. Persons who could make copies from key files on disks are office mates and service personnel. Long passphrases make such attacks more difficult, except if the attacker can observe the PIN or password entry. Accordingly, SEMPER could give a recommendation about the minimum requirements for a passphrase or the software should reject passphrases which are too short or trivial.
- In a system which uses escrow of a signature key, or in which key pairs are distributed to users, users can say that the trusted party was not trustworthy. Whereas such systems may be seen on the market, it was questioned whether they can achieve non-repudiation.

The issue of secure key handling will be discussed below as a question of implementation. As opposed to the situation in the area of payments where a number of different instruments with their pros and cons are well known and established on the market, in the area of signatures different variants are possible, too, but well-known and stable ones have not yet been developed by the market. The notion "variant" does not refer to the underlying mathematical function, but to the commercial meaning of the signature, its bindingness, applicability, revocability, etc. I.e. the meaning of a digital signature depends on a number of design decisions. The variants are visible from the options of X509 v.3 certificates and from the different certification policies which are being discussed or which are developed by the different certification authorities emerging. In the US the provision of information on what a certificate means and accordingly to what a degree a user can be held liable when signing has been nicknamed the "nutritional information". With this notion it is meant that a relying party has to inform itself about what exactly the signatory and his or her certification authority did and committed themselves to. In the SEMPER trials one will have to make decision regarding all the options discussed or one will have to select or negotiate them with a certification authority. The questions to be answered by a certificate or by the "nutritional information" to be learned are (personal communication with Jim Galvin, Ver 96, Fro 96):

- What for is the signature applicable? It can either be used specifically for a certain purpose, or generally. Specifically means, e.g., that an individual is only allowed to use it when using a certain bank card product. Another example of a specific signature is one which can only be used when signing for a certain employer. General applicability would mean that one can use one's signature like today for signing all kinds of documents. Another variant is that a signature may only be valid with a second digital signature, e.g. by one's boss.
- What is the upper amount of money the signature has been made for?
- Which are the steps the certification or registration authority took to verify the owner (check, e.g., email or real address, creditworthiness, passport)? Was a notary involved?
- Is the certification process designed in a way that it is possible to achieve non-repudiation even if the individual was not identified beyond doubt, because he or she used the signature for several times without challenging it?
- What is the liability of the certification authority (e.g., for issuing a certificate to somebody with a well made counterfeit passport; is there an upper limit of liability)?
- Which are the criteria for revocation (when can a relying party demand revocation of a signature because the signatory did not pay? Can an employer demand revocation because the employee was cheating or left the company? These criteria are quite important because a CA can "play god", as experts put it: if it deletes you from the list, you stop to exist electronically.
- How are the certificate revocation lists handled (maximum delay between revocation and updating the list, having a separate suspension list for unclear cases)?
- In which hierarchy is the certification authority in? How can a relying person learn that a CA is not fake?
- How does the CA manage their own keys? How does a relying person learn securely whether it lost control over it's secret keys?

Another issue, not concerning the bindingness, is whether the CA sells or abuses the information obtained. A merchant may not wish to check a certificate revocation list because the certification authority learns who buys from whom. It was reported by a security specialist that there are certification authorities which consider to sell the information obtained. Merchants might trust only a certification authority which does not sell their information. Otherwise, they might decide not to work with client certificates at all. It was suggested that public institutions run a certification authority which would be more neutral. Also one could expect that a public institution will have to be more restrictive with "playing god" and making somebody disappear.

3.3.3 Implementation Issues

- **Integration into Existing Systems**

Respondents mentioned that an implementation of SEMPER should take three things into account.

1. Users will operate different computers. Computers will be operated by several users, e.g., by secretary and boss, or by several family members. Users will wish to use the same function at home, in the office and when travelling (discussion in CommerceNet).
2. Access may be from inside an Intranet and behind a firewall (mentioned at a meeting of the Public Key Infrastructure group of CommerceNet and at the meeting of the Electronic Payments Forum).
3. Users may have to operate other security systems, too. In both Europe and the US it was expected by the respondents that companies will introduce digital signature systems for company use, that banks will introduce home banking systems with digital signatures, and that more such systems will emerge, e.g., for electronic commerce or for use with the government. It was reported that there are already incompatible signature systems existing, e.g., for use with several agencies of the Swedish government. It is expected that the handling of keys and certificates can thus become difficult. It was also expressed that it might be inconvenient for the user to have the same security function (e.g., RSA-software) from several vendors several times on the hard disk. It was proposed that the users need not run several security packages on one computer (see Bla 96). SEMPER could here make a proposal on how to share passphrases, secret keys and certificates between applications.

In addition, it shall be mentioned that respondents liked the idea that the Tinguin could be integrated into the browser or the operating system. The user would then have to handle the information displayed in the browser's WWW-window, and the information displayed on the browser's surrounding bars. Thus the user needs not handle a window in addition to the browser or operating system's window as it will be the case in the basic trials.
Ease of use was, of course, also mentioned as a requirement. Striking was a quotation made by a social scientist, who reported that users said:

> "A hand-written signature is just so easy to make," compared to a digital one.

- **Trustworthiness of Hard- and Software**

Respondents liked the idea that there is a trusted user interface (Tinguin) as opposed to having to trust what is displayed on the browser window. This immediately led to two discussions:

1. How to get the software securely?
2. Is it sufficient to have a software-only solution? Respondents were eager to learn what we mean with having part of the Tinguin or the whole of it on secure hardware.

The discussions regarding secure hard- and software is in particular related to achieving non-repudiation of orders and contracts. We now sketch the most interesting findings of these discussions.

- **You Do Not See What You Sign**

A signatory may not have been aware of the full contents of a contract. A lawyer might argue that the link between the signature and the body of a contract is not as direct as on a piece of paper. In particular the contents of a large contract will not be visible. A secure wallet, in particular an organizer-like one with a relatively large display, can offer substantial remedy, but cannot close the gap completely.

- **No Link Between the Secret Signature Key and the Person**

This argument refers to the principal gap between the computer and the person. The respondent argued that the digital signature should rather be called “an electronic seal” (a computer security expert).

It was even reported that versions of digital signatures appeared on the market which mirror the problem that no link to the person is possible, i.e., where the mathematical procedure called “digital signature” is used to identify and bind just the company. Such a procedure resembles a stamp or a seal. Biometric identification could certainly help here. Iris-scan is reported to meet Barclays bank's false accept and rejection rates (see also Financial Times of May 14, 1996).

- **How to Receive SEMPER Securely?**

Respondents discussed how to get trustworthy soft- and hardware. The guidelines of the American Bar Association on digital signatures rightly state that there is

> “a range of trustworthiness technologically available” (ABA 95, p. 44).

The decision is left over to the system provider. SEMPER must accordingly make decisions on which technology is appropriate

Respondents were aware of that just downloading SEMPER-software from some server provides no secure starting point. Respondents appreciated the suggestion to digitally sign SEMPER-software using PGP though, of course, there is a principal risk that a user might have a fake version of PGP. As it was explained that the SEMPER-tools like the Tinguin-window might in the future be integrated in a browser or operating system, a more secure distributing channel becomes possible when computer vendors would distribute it. Similarly, respondents were aware of that distributing SEMPER-software via diskettes or Compact Disks is more secure than just downloading it from somewhere. Of course, it is possible that physical carriers be distributed with counterfeit software. Respondents were aware of that secure hardware would be much more difficult to forge. The usage of hardware would also prevent a very simple attack respondents immediately thought of: that a server transmits something resembling a Tinguin. Certainly some people would enter their credit card numbers or bank card-PINs if asked to do so.

- **No Secure Key Handling with Software Only**

Even if one has received SEMPER securely, SEMPER is running on a machine which is accessible through the Internet and usually also through other persons, like office-mates or computer maintenance personnel. Respondents are aware of the issue of secure key handling:

> "A hugely crucial question is: How are issues of security of end-user private keys dealt with? Because whether I got one or ten key pairs, they are on my hard drive. Someone can come in with a disk and load my Netscape navigator off and has all my private keys!" (an Internet technology provider)

The recent VeriSign Certification Practice Statement puts the burden on the user:

> "each ... subscriber (is) responsible for protecting his, her or its private key(s) from compromise, loss, disclosure, modification, or unauthorised use." (Ver 96, p. 34)

Is it fair to impose this risk on the user or will such a clause be challenged at court? One legal expert stated:

> "I don't see any way to hold a user liable for his signature unless we can show full control over the secret key... And I don't see any sensible way to do that at the moment other than with secure hardware that is a portable and controllable token, gizmo, smart card, wallet, whatever."

- **Chip Cards as a Solution**

Some players discuss to use chipcards which generate the signature in their chips. Experts interviewed reported, however, that some threats remain. An important threat appears to be that somebody designs a virus which the user somehow receives (diskette, CD, FTP) and executes. First Virtual had pointed out that credit card numbers can be intercepted by a virus eavesdropping the keyboard. With a chip card that number may never have to be keyed in, but other important information will have to be entered using the keyboard. The Hamburg Sparda bank writes on their WWW-page that with the new proposal for home-banking in Germany, HBCI, even when a chip card is used a virus can attack a PC in order to manipulate a transfer order (see <www.sparda-hh.de>). Such a manipulated system could display a different amount of an order on the screen than what is actually being signed, or a different account number. One expert had made an estimate of the effort to make such attacks and pointed out that it would only be

> "a few days programming effort to manipulate a smart card-based signature system" if the latter is part of a PC connected to the Internet (a computer security expert)

This demonstrates that the cost of such manipulations can be very low. Several experts from banking, electronics industry and computer security expressed that the introduction of digital signature schemes for home-banking with PCs alone or with PCs and chip cards shifts the risk to the users, as compared to clearly insecure solutions like telephone banking:

> "The customer will be responsible himself for keeping his access secure." (a banker)

If the chip card is the bank card, the question arises of what to teach the user with regard to the handling of his or her secret key. It will be difficult to tell the user to keep the carrier in a safe place, and at the same time advise him or her it can safely be handed to a waiter who disappears with it or to a cash dispenser which swallows it for quite a while. In other words, it can be psychologically difficult to teach at the same time that it is a valuable piece of information, and that one can safely give it away. There is the possibility to argue that the key is protected by a password, but once the carrier is out of control for a while, a criminal could try out passwords or use eavesdropped ones.

- **Secure Wallets as a Solution**

At the APSON meeting (Advanced Payment Systems for Open Networks, Interoperability for Network Payment, USA, November 1995) it was discussed that there is a need for "protected devices":

> "Protected devices encompass more than the card/token but include reader/keyboard (I/O) as well. This is to prevent Trojan Horse attacks for input and interfacing the protected device." (p. 7)

With "Trojan horse" it is meant that some application contains functionality which does harm to the user. Similarly, one computer security expert suggested unprompted to use a badge-like device with a small keyboard and a small display:

> "My favourite: keyboard, display, keys stored securely."

Respondents generally liked the idea to have all security related information such as a full contract or at least the core information, such as an amount or an account number, displayed using secure hardware. It was also appreciated that information such as passphrases or credit card numbers should be entered on a secure keyboard. Of course, a certain remaining risk of Trojan horses exists also with secure wallets. It can be reduced by having independent suppliers of components and an independent analysis of design (see PPSW 96).

A number of suppliers produce devices which could be modified to be used as a secure wallet, e.g., manufacturers of GSM-phones, organizers, PCMCIA-cards, palmtop computers or chip card readers. Some companies already supply “mini-banks” with a contactless interface. Estimates from the industry of the costs of secure wallets vary from ECU 50 each for 10,000 pieces down to ECU 30 if the batch size is around one million.

In the interviews, the question rose: who should pay for secure wallets? The answer to this question depends on the setting. For instance, if an employer designs a system for use inside the company, the employees will not be willing to pay for the wallets. The employer may then wait and see how many transactions will be challenged (this is the strategy one respondent from a government pursues). If the signature function is provided by a bank to a private customer, the bank may be the player to provide the wallet. However, as a bank representative put it, he would rather like to pay for the disputed transactions and buy wallets only when the fraud is larger than the cost of providing wallets. This may be cost efficient for the bank. From a multi-party security point of view this may be more difficult. If such an attack happens the consumer depends very much on the individual employee of the bank or other service provider (CA) whether he believes it was a fraud by someone else or whether he believes the customer did authorise the transaction him- or herself. In case of disagreement, the consumer may have to go to court. Also users are encouraged to simply pretend that they became victim of a virus which can increase the costs of the bank substantially. Furthermore, if attacks get widely publishised, consumer confidence into electronic commerce can be diminished.

The situation is different if one is talking about business-to-business transactions with higher values. The risk of a dispute will here be quite high and can easily justify measures for secure key handling. Also the costs are not that high compared to the savings possible with electronic transactions. The costs of the wallet can be covered if only one or two express deliveries are saved.

Also from the consumer point of view the costs can be justified. First, the risk is here different as for the service provider because a dispute in the range of several thousand ECU is large compared to the cost of wallets. Second, the wallet can in principle be marketed like an existing wallet, i.e., holding documents and cash like a traditional wallet does. Nobody expects a bank to give away traditional wallets for free. Third, the willingness to pay for such wallets has never been tested. Only simulations and mockups of somewhat similar wallets, suitable for transferring payment information to a point of sale via infrared, have been topic of interviews done for the CAFE-project. This kind of wallets was discussed with frequent card users. The interviews lead to the conclusion that such users can be willing to pay up to ECU 50 if the wallet replaces other cards and is thin enough to be put into existing wallets (WCP 95). Wallets would also be beneficial in order to achieve portability between different computers as required by the security experts interviewed. What can be concluded?

1. There are possibilities that the users are willing to purchase wallets when the risks involved are high or when portability is required.
2. Free distribution can be considered if the costs are in the range of ECU 30 which means just a few ECUs per year of operation.
3. If it cannot be justified economically to distribute wallets, it can be justified to do so ethically. A reason would be to protect the weaker party, which is usually the individual customer.
4. A provider might publicly announce to take over the risk and fix this in its contract, just as it is done in today's credit card contracts. However, also in this case it is up to the individual on the provider side handling the dispute whether the transaction is cancelled or whether the debit or the bill is maintained and taken to court.
5. A completely different consequence is to reconsider whether non-repudiation of documents is necessary at all. If a transaction is of *small value or prepaid*, a merchant may not need a binding order. Also in an *ongoing trust relationship* to the customer, the merchant may not need a binding order. *The binding signature can also be made traditionally with off-line delivery,* as in the SEMPER-trial of Otto Versand.
6. Still another solution, also reducing non-repudiation, is to consciously use less binding types of signatures. Such a kind of signature has emerged on the market when one gets a "weak" certificate on-line. This is discussed in the next section.

- **Use Weak Certificates**

A pragmatic solution would be to use a signature with a weak certificate, like the class 1 certificates of VeriSign. These can quite easily be obtained on-line. An Internet service provider pointed out that merchants can develop a trust relationship to the user of such a "weak" certificate. It can provide quite a good protection against becoming impersonated:

> "If I am registered, somebody else will find it difficult to pretend to be me." (computer security expert)

Reportedly, more than 100,000 users have registered within the first few months. The merchant could even accept such a certificate if it is from a pseudonym. A certificate for "Donald Duck" or just for a serial number could make sense. Other solutions can be thought of which provide for a certain level of authenticity, without requiring to go to a notary or have a secure wallet. Such a "signature" would then resemble a signed fax, providing "peace of mind", without giving proofs useful at court.

Possible consequences for SEMPER would be to develop a strong solution, providing a high degree of non-repudiation, and a more pragmatic solution, providing increased security against threats like fake orders, without incurring most of the costs of the strong solution. The multiplicity of options in the design of digital signatures discussed above shows that there are more options for SEMPER than just a strong and a weak one.

3.3.4 Conclusions

- **Multi-User, Multi-Computer, Multi-Security-Systems Issues**

- The architecture must be able to handle that one individual uses different computers and one computer is used by different individuals.
- The consortium should propose how the requirements from several systems, e.g., from a company system, a home-banking system and a system using SEMPER, to have passwords/passphrases and secret signature and decryption keys can be handled conveniently and securely with or without secure hardware.

- **Handling of Security Threats**

- Disputes are expected where digital signatures will be challenged (insecure key storage, key known to third party, algorithm not provably secure, by coincidence somebody else has same secret key, virus, no link to person). The consortium should give recommendations for how to minimise such challenges (e.g., secure wallets, key generation by signatory, no escrow of signature keys with third party). In particular the remaining threat of viruses causing unintended transactions should be investigated further and SEMPER should give recommendations.

- **Handling of a Multiplicity of Certification Policies**

- The consortium should give recommendations on certification policies (e.g., key generation while being at notary, updates of CRL within a certain time, full liability of CA for all its errors).
- The consortium should investigate whether there are one or several solutions feasible which reduce the efforts of registration, certification and secure key handling and still lead to a significant reduction of threats (e.g., “weak” certificates, enhanced trust relationship with repeated application).

4 DEFINITION OF CONSUMER AND TECHNICAL SERVICES

4.1 Introduction

The goal of this chapter is to define the new online services of the consumer service providers EUROCOM, FOGRA and Otto Versand taking part in Semper. The purpose of these service definitions is to provide three different approaches to electronic commerce which supports the generic modelling of an electronic marketplace. We are looking at the semper software as a black box. No technical details are described here. Therefore the definition of the consumer services includes the specification of requirements for the respective technical services needed. To complete the description, an overview on implementation issues is given as well as an outlook on advanced trials.

This chapter is structured in a way that each of the consumer service providers EUROCOM, FOGRA and Otto Versand define in separate subchapters their approach for the Basic Trial of the first project year. To get a clearer view of the similarities in the technical approach an extra chapter summarising the similarities is included.

In each subchapter for the three service providers, we first describe the current situation of the corresponding provider in order to support the understanding of the individual businesses and markets. Business organisational and technical aspects are covered. In the second part of each subchapter the general view and strategy for electronic commerce is described. This acts as an umbrella and a basis for the identification of each providers attitude towards electronic markets. The third part of each subchapter outlines the services that could be relevant for SEMPER in the future in brief. The purpose is to give an overview on potential services, especially for the second and third project year. Then, the consumer services and the test scenario of the Basic Trial are specified in detail.

In a separate subchapter the possible different ways of registration and authorisation for the trial participants are systematically explained and the choices made by the individual service providers are summarised here.

Finally we provide an outlook to advanced trials for all three service providers. Here the intended services for subsequent trials are specified.

The consortium will also publish the requirements by the Regionlink companies, which joined the consortium during 1996.

4.2 The Consumer Perspective

4.2.1 General

The main body of this chapter is devoted to defining the requirements for electronic commerce from a vendor point of view, i.e. defining the requirements of the service providers who will participate in the SEMPER trials. However, because the aim of the SEMPER architecture is to provide multi-party security, equal emphasis has been placed on identifying the characteristics which will influence the consumer's ability or willingness to participate in electronic commerce. In formulating their requirements the service providers have applied the general guidelines described below to the needs of their customers. The consumer reaction to the SEMPER architecture will be evaluated both during and after the trials.

The intention here is not to attempt to provide a precise or comprehensive definition of all actions and tools which exist in traditional markets, or to propose that it is either feasible or desirable to mirror all of these in an electronic marketplace, but rather to draw attention to a number of relevant consumer issues. Because the initial trials will provide the most fundamental aspects of commerce, secure order, payment and delivery, the description which follows is primarily focused on the electronic shopping experience. Other, equally important aspects of electronic commerce, such as data privacy, anonymity and untraceability are discussed in chapter 3.

Subsequent to the more general discussion of consumer requirements, some issues related to specific proposals under consideration (e.g. digital signatures, electronic wallets, etc.) are introduced.

4.2.2 Some Basic Consumer Requirements

The following recommendations are based on the aim of making electronic commerce attractive and available to as many consumers as possible. The main aim is to identify similarities and differences which will need to be taken into consideration. In view of the fact that the development of any market is an evolutionary process and that the technical requirements for secure electronic commerce are particularly demanding, it is also considered advisable to distinguish between criteria which should be viewed as essential requirements for consumer participation in electronic commerce and those which would be desirable attributes.

4.2.2.1 Access and Ease of Use

The ability to participate in electronic commerce should not be restricted in respect of equipment or location. Consumers should not be forced to invest in expensive new technology. The architecture designed should allow for implementation on any hardware and software platform. It should also be possible for consumers who do not personally own computer equipment to participate by using a computer at work, at a friend's or relative's, or through some form of public access, e.g. the Cyber Cafes which are beginning to emerge. Even if a consumer possesses the required hard and software it can be assumed that he or she will also want to continue the electronic shopping experience when away from home. Some sort of device enabling mobile access via a broad range of computer equipment would appear to be highly desirable.

In support of the same aim, i.e. enabling access for as broad a segment of the population as possible, a variety of forms of payment should be supported. Some sort of stored value, electronic cash or means of payment by bank transfer is required for those not eligible for credit (due to age, income, employment status, etc.). It can also be expected that, just as in non-electronic markets, even those consumers eligible for credit will want to use a variety of payment means depending on the purchase situation, value of the purchase, etc. For example, a consumer may prefer to use credit to book and pay for a holiday, some form of pay-as-you-go for services being consumed on-line, and want to defer payment of goods ordered on-line but delivered off-line until they have actually been received (thereby, protecting his right to withhold payment if not satisfied). It can also be expected that consumers will require some form of receipt for tax purposes, business expense forms or simply as a means of personal bookkeeping.

A frequently heard complaint among consumers today is the ever-increasing number of cards, PINS, etc. which they are expected to manage. An aim of electronic commerce should, therefore, be to avoid increasing the complexity of actions required by the consumer to implement an exchange. It is also essential that the consumer understand the electronic exchange process. The consumer interfaces must be designed in such a way that the significance of his/her actions is absolutely clear to the consumer at every stage of the electronic shopping experience (from the first requests for information, through the negotiation process to the implementation and completion of a transaction). A parallel to the type of support the consumer will need can be found in way the requirements of a layman confronted with new technology have been taken into account in the development of home computers. Some similar techniques for consumer support, such as an on-line help function, should be considered. An essential requirement is that some sort of warning mechanism is implemented at the point where the consumer initiates an action which cannot be revoked (e.g. confirms an order or implements payment). This might be similar to the way the software in a personal computer has been designed to protect the user from inadvertedly deleting files by giving an audible warning that something significant is about to take place and requiring confirmation, or repetition of such commands.

- **Specific Consumer Requirements at Particular Stages of the Electronic Shopping Experience**

Most of the related literature describes the electronic shopping experience as consisting of three phases: negotiation and ordering, payments and order fulfilment. Two equally important phases are seldom discussed. These are the phase which preceeds negotiation and ordering, i.e. the search process which usually involves gathering information about comparable products or services and the vendors who provide them, and the post-purchase reaction to the shopping experience, which can range from satisfaction creating a strong potential for repeating the experience through to complete dissatisfaction requiring the initiation of dispute proceedings and or claims for redress. The following recommendations take these two additional stages into account.

An important initial step in any form of commerce is to select a business partner. In the electronic context there are at least two requirements which need to be fulfilled before the consumer can decide which shop to enter, or which service provider to approach, i.e. the identity of the merchant and the means of payment which can be used have to be established. Due to the fact that it is possible to create fake shopfronts and to display false logos in open networks, the consumer needs to be able to check the credentials of the shopping location and establish that his preferred means of payment will be accepted before proceeding any further with the electronic shopping experience. If authentication of the business partner or means of payment were to take place at a later point in the purchase process the consumer would be deprived of important selection criteria.

Consumers frequently seek a wide range of information before they finally decide to make a purchase and there is every reason to believe that this form of behaviour will be even more widespread in the electronic marketplace due to ease with which they can move from one vendor to another. They are likely to seek every type of information, e.g. price, available forms of payment, availability, delivery times, guarantee or maintenance terms, etc. from a number of different vendors (for the purpose of making comparisons) before reaching a final decision. On the other hand the shops are interested to communicate directly with the customer. Searchengines might interfere with this interest. It is likely, therefore, that consumers will initiate proceedings which appear to be the negotiation phase prior to ordering, even continuing these to the point of obtaining an offer, when, in fact, they are only gathering information. Once the consumer has had the opportunity to compare the information and/or offers he has collected he will want to re-establish contact with the merchant of his choice. For this reason a very desirable option for electronic commerce would be some means for the consumer to re-establish contact to a vendor at the same point where the previous negotiation was interrupted, rather than having to repeat the query process. This would imply some means of receiving an electronic offer from the vendor which could be re-submitted at a later point in the form of an order (the vendor would, of course, have to confirm that the offer is still valid).

Whether the consumer is simply seeking information for comparison, or actually intending to place an order, in almost every purchase situation a certain level of bi-directional communication will be required. Even in a relatively straight forward situation where the customer selects an item from an electronic catalogue, it is likely that he will expect to be able to take part in some form of interactive negotiation before confirming an order, for example, establish availability, delivery times, etc. Frequently the consumer has very specific requirements before he begins to shop. In this case a particularly attractive option would be an opportunity for the consumer to initiate the shopping experience by supplying a description of the article or service he is seeking, together with relevant terms (price range, delivery date, quantity).

At the point where the consumer finally decides to make a purchase it is essential that he or she fully understands all of the actions required. and that the order being placed is unambiguous. This description of goods and terms of the exchange have to be made very clear to the consumer immediately before a transaction is activated. It may be that a number of steps have taken place in a negotiation process, and the fact that the consumer isn't physically confronted with the items being purchased make this re-statement of terms before agreement very important. This is similar to the way a service agreement has to be described in a paper contract in order to make it tangible.

Finally there needs to be some mechanism for introducing post-purchase queries, in particular when the goods have been delivered on-line. In this case the question of liability, should any aspect of the transfer fail, may be extremely difficult to resolve, but it can be expected that there will be a clear requirement from the consumer for a recognised dispute mechanism and certain rights to redress if a transaction fail. In respect of on-line delivery it would be desirable for the consumer to be able to activate this dispute mechanism, or initiate a query immediately (i.e. the moment the failure is discovered), perhaps by maintaining the on-line order/payment interface long enough for the consumer to indicate successful receipt of goods. The faster both vendor and consumer can begin negotiating a dispute, the more likely it is that it will be resolved satisfactorily without the intervention of third parties. The consumer post-purchase query will not necessarily always be negative. It may be that consumer satisfaction with the transaction is so positive that he will want to establish more permanent links to the vendor, by subscribing to a service, for example. It might be convenient for the consumer and advantageous for the vendor if this option were somehow linked to the on-line delivery of goods.

4.2.2.2 Desirable Non-Commercial Options

A further desirable function for the consumer, which is not strictly a commercial requirement, would be the ability to check the current status of his or her finances while participating in the electronic marketplace, similar to looking into one's purse before making a purchase in a traditional market. The consumer would then be able to model his shopping behaviour accordingly. He would be unlikely to attempt to implement an electronic transaction when his credit limit hasbeen reached, for example, a useful attribute for both vendor and consumer. On the other hand, continuous and detailed knowledge of the current balance of his account or stored value could also encourage him to continue his electronic shopping trip, place him in a better position to take advantage of special offers (buying 10 rather than 1 as originally planned when a particularly attractive offer was made), or increase his ability to negotiate by providing him with an on-line credit reference.

It is also possible to locate payment requirements which are outside the generic definition of a market transaction, but would be desirable or attractive to the consumer. An example is the ability to transfer value without receiving anything in return. This is not a market requirement in the strictest sense, but it is easy to find illustrations of why this would be an attractive option, for example in order to make a donation to an organisation which the consumer has located and established contact to via an open network.

4.2.3 Specific Issues

It is probable that the unique requirements of electronic commerce will require the introduction of new procedures or alterations to some existing market rules. The fact that the consumer has no previous experience of these creates a demand for careful implementation. The major requirements are for transparency, universality, openness and security. The provision of multi-party security in the context of electronic commerce is the central goal of SEMPER. In the following the impact on the consumer of certain security mechanisms is discussed.

4.2.3.1 Use of Digital Signatures and Storage of Valuable Information

One of most important proposed security mechanisms which will require full understanding by the consumer is the use of digital signatures. Previous research [Ros 94] indicates that consumers are not always fully aware of the value of the secret key. Just as the security offered by a PIN is frequently compromised by user carelessness. The potential security which digital signatures could provide in an electronic marketplace will be dependent on consumer awareness of correct usage, e.g. when making a note of the PIN number .Users should have a maximum of two PINs to memorise, or one PIN and an additional pass phrase. A further advantage might be to provide an option for the consumer to choose his or her own PIN.

The location of the secret key should be transparent, by which is meant that it should be stored in such a way that it is clear to the user where the secret is located. This knowledge will enable the user to handle it appropriately, for example, store it in a safe place when going on holiday, not leave it lying around as they might a telephone card or a diskette. [Ros 94]

Due to the fact that a digital signature can be made by any person in possession of the secret key (or a copy of it) and bearing in mind that due to both misunderstanding and pure carelessness consumers do not always protect their own security adequately, it might be advisable for the consortium to investigate other security mechanisms for protecting secret keys, such as a biometric means of creating a link between the device holding the secret key and the consumeror tamper resistant storage of the key to ensure that it cannot be copied easily. Other solutions might include having a very close link between the order or transaction and the process of signing, such as that which could be provided by an electronic wallet.

It must be absolutely certain that the consumer has a clear understanding of the new processes and the potential impact using these can have for him or her personally, in particular the financial risks involved. Consumers may take greater care of the secret key if they have purchased the device in which it is stored. This would emphasise the fact that the key is a personal possession, not a mechanism provided by a third party.

4.2.3.2 Universality

By universality is meant that if a service, such as a digital signature function or a stored value device, is offered for electronic commerce it should also be possible to use this for non-electronic commerce, e.g. use the same stored value in vending machines, or the same signature at a cash dispenser, otherwise there is a danger that the new service might be less convenient than traditional signatures or cash. In order to be universal everyone should be able to accept stored value . A solution might be to offer limited transferability, for example, a taxi driver who has received stored value from his customers might be able to buy petrol off-line (without contacting a bank), but the petrol station would have to return the money to the bank. Universality also implies that a service provider or merchant should be able to make purchases and that the consumer should be able to sell something.

4.2.3.3 Openness

Openness would ensure competition with regard to services leading to new services being developed, technical progress and lower prices. Examples of openness which the Semper architecture should provide are:

- the use of several forms of electronic cash
- free choice of the type of encryption service used
- allow competition between Semper-approved technical services and others (e.g. one should be able to combine a SEMPER-approved tool with another one).

As a result merchants or customers would be able to select and combine services freely, e.g. use a signature function provided by Semper and a payment instrument from another supplier.

4.3 EUROCOM Expertise

4.3.1 Current Situation

EUROCOM EXPERTISE S.A. operational activities are primarily focused towards the provision of training programmes and services mainly in the areas of telecommunication, information technology, telematic services and Total Quality Management. Furthermore, the company is heavily engaged in the development of training and educational packages using CBT- (Computer Based Training) Systems and multimedia as part of its offered training activities, so it is anticipated that the company will have an active involvement in the European Union funded programs defined within the fourth framework, concerning distant learning and telematic services for education and training, including the use of multimedia.

EUROCOM EXPERTISE S.A. (former INTRACOM Training Center), has extensive experience in providing training services, covering the needs of the local as well as the international market. Among its major customers are:

- The Greek PTT (OTE),
- INTRACOM,
- HTC (Hungarian Telecommunication Company),
- MOLD-TELECOM (Moldavian Telecom Operator),
- ERICSSON MOSCOW,

- PANAFON,
- ETM S.A (a Dutch subsidiary of ERICSSON),
- FATME S.A (an Italian subsidiary of ERICSSON).

General public attending traditional (in classrooms) as well as online (network based multimedia presentations) courses.The training courses are offered on a general or a customized basis, depending on their content and target market. They fall into six main categories, covering the domains of :

- TELECOMMUNICATION TECHNOLOGY AND SERVICES
- DATA COMMUNICATIONS AND NETWORKS
- SOFTWARE ENGINEERING AND APPLICATIONS
- TELECOMMUNICATION BUSINESS MANAGEMENT
- TOTAL QUALITY MANAGEMENT
- TRAINING MANAGEMENT

Customer authorisation is done via customer identity numbers, and initially via a location-based (city, street) data base of credit ratings. Payment is invoice based. Instalment purchases are possible. No credit cards are accepted yet.

4.3.2 Existing Digital Services - CATE®

EUROCOM is currently setting up a Computer Aided Training Environment (CATE®) that automates class organisation and the process of teaching. This system is an electronically organised classroom with a multimedia interface. Connected through a network of computers, teachers may develop and manage their courses and students may attend the courses, develop their projects and take their exams. Students may attend the courses independently. The courses are self presented interactive multimedia presentations.
This system is currently operating in an INTRANET environment at the EUROCOM site in order to provide training services.

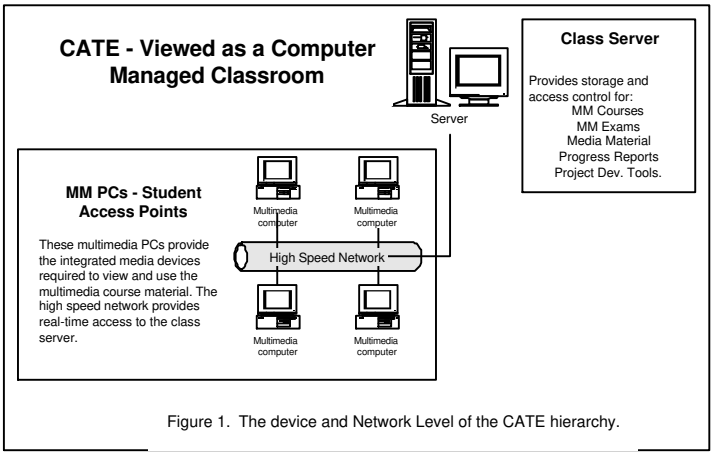

Figure 1: CATE

4.3.2.2 Business Level

The courses offered by EUROCOM are described in detail in on-line course catalogues (http://www.eurocom.intranet.gr/TrPrgrm/) and advertised through different media. Customers eitherperform on-line registration requests to courses or attend seminars at standard classrooms at EUROCOM's site or at their own sites. An electronic confirmation (e-mail) or standard mail confirmation is than sent to the customer specifying which of the requested courses he can attend (for groups with limited number of participants). Billing is specified based on the length, the complexity of the course and the site at which the course is given. After the completion of a seminar an invoice is sent to the customer. CATE courses have been available to the customers since January 1995. Payments take place through invoices as well. In the future the billing will be generated by the CATE system based on the duration of attendance and the title of the course.

4.3.2.3 Organisational Level

4.3.2.3.1 CATE Services

CATE services are provided to administrators, teachers, and students.

An administrator can:

- organise the catalogue of the courses offered,
- add/remove courses to/from the system,
- add/remove CMSusers. Students that take courses and/or teachers that manage courses,
- assign courses to students (access rights),
- assign courses to teachers (access rights).

A teacher can:

- use provided templates to develop self presented interactive multimedia course material such as lectures and exams.
- The Progress Tracking allows teachers to review the progress of a set of students specified by certain characteristics like name, sex, prerequisite courses etc.

A student can:

- use provided templates to develop self presented interactive multimedia presentation material such as assignments and class projects.
- The Course Management System allows students to: register to or addend a specific course (interactive multimedia presentation)
- In addition he takes the exams, assignments and projects of a course and can review his own activity (progress)

4.3.2.3.2 CATE® System Structure

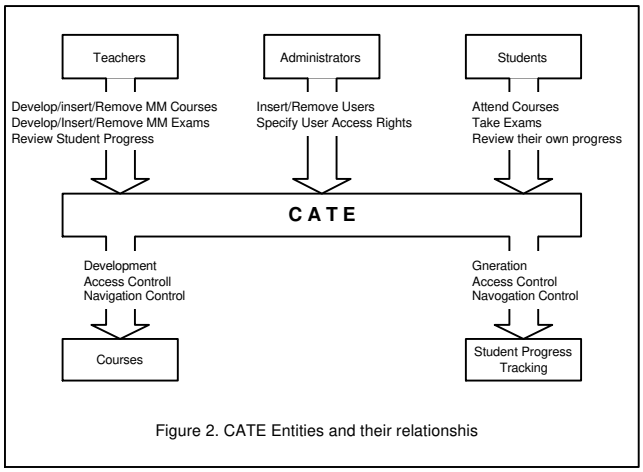

Figure 2: CATE Structure

Figure 2 presents the entities of the CATE environment and their relationships. CATE is an interactive multimedia electronic classroom. It abstracts the notions of teachers, students, courses, exams, and progress reports and defines a framework of operation. Teachers, students, and system administrators are the clients of CATE. Courses and student progress reports are the CATE products and services.

4.3.2.4 Technical Level

4.3.2.4.1 The CATE Layers

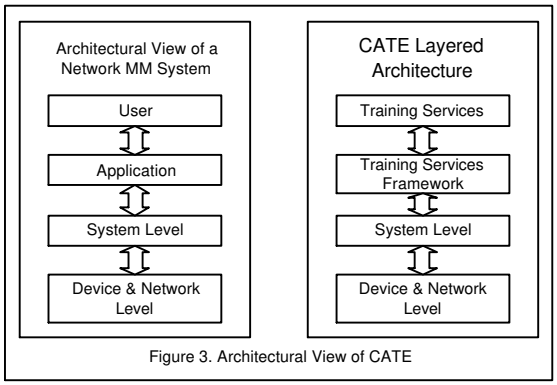

Figure 3: CATE Layers

CATE is a network multimedia system architecture as it is shown in figure 3. It is divided into four basic layers. This makes CATE portable and expandable. The two lower layers, system level and Device & Network level abstract CATE from specific hardware, operating system and network platforms, where the two higher levels provide the framework that abstract the notion of concepts like course, exam, progress report and allows their easy and structured development.

4.3.2.5 Training Services Level

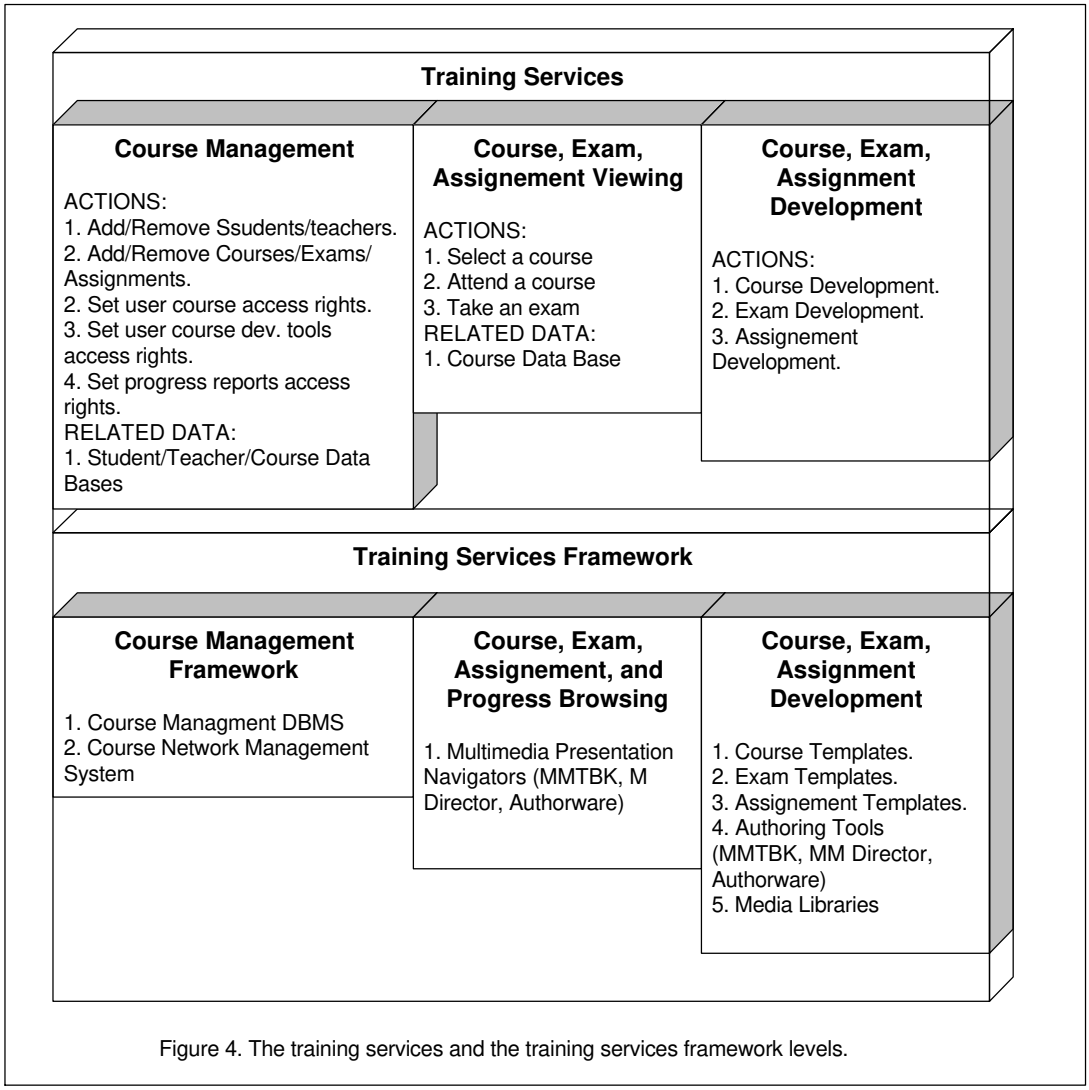

Figure 4. The training services and the training services framework levels.

Figure 4: A MPC and MS-Windows CATE System and Physical Level Implementation

The following table shows as an example an INTRANET based CATE physical level implementation. This is the set up of the pilot CATE system at the EUROCOM site.Recommended H/W, S/W for every 12 students and 24 courses			
Quantity	Hardware Description	Software Description	
1	MPC: Pentium/100 2 GB HDD 32 MB RAM 256 KB Cache Memory Ethernet Card	Windows NT EUROCOM's CMS Package (Includes the course development system and the course management system)	
12	MPC: 486/66 or more 1 GB HDD 16 MB RAM 256 KB Cache Memory SVGA Card 2MB/LB Colour Monitor 17'' 256 colours FDD 1.44 MB Ethernet Card CD ROM Drive 4xSpeed 16 bit Sound Card Ear-speakers/Microphone	Win95 EUROCOM's CMS Package (Includes the course development system and the course management system)	

Table 10 Recommended Hardware and Software for CATE

4.3.3 General view and strategy for electronic commerce

4.3.3.1 General View

Today's professionals and employees have to get periodic training to keep up with the innovations in their field. New technologies, systems and theories come out in a rate that makes it hard for an educational institution to provide an updated course programme. There is a lack of trainers, experts in these new technologies.

Computer Aided Training provides training systems with the following advantages:

- The expert trainer is needed only for the preparation of the course. This makes knowledge transfer possible without trainer or trainee transfer.
- A MM CBT (Multimedia Computer Based Training) system may combine animation, sound, graphics and other media to present concepts that are difficult to describe with the conventional teaching media (a board or a projector).
- The course can be presented to the student by a general purpose personal computer. The expense of having a teacher to present the course is limited to the expense to provide the course material. Preparing a CBT (Computer Based Training system) is not more expensive than preparing printed material for the course.

- The system may also provide the student with multiple choice exams. Keep track of the progress of the student and provide him/her with appropriate advice. The progress reports can be obtained to the students or course administrators immediately (students an administrators don't have to wait for days or weeks to get the results).
- Standard teaching quality. Well developed CBTs have been proved to be better teachers than the average teacher of a specific course. Moreover, no matter how many times a CBT is presented, it is exactly the same quality CBT.
- Students may register, attend, get billed and pay for their home or other site computers, remotely over a BBN network.
- Audio-visual material can provide valuable help for training, Moreover, a training system is only useful if the learner remains active and motivated. Today's personal computers support the execution of sophisticated interactive multimedia education systems. The use of media like sound, video and animation for the explanation of certain concepts makes a CBT a better teacher than an average trainer with limited presentation media.
- Interactive multimedia CBT systems can be offered on stand alone computers, on INTRANETs and on the INTERNET. If the appropriate network infrastructure is available an interactive multimedia CBT can be offered in the INTERNET environment.

4.3.3.2 Electronic Commerce Strategy

EUROCOM wants to provide interactive multimedia courses to customers over a broad-band network system that provides secure course material transfer, billing and payment. The consumer services are the INTRANET CATE services offered in an INTERNET environment plus electronic billing and payment. Marketing, billing and payments will take place through SEMPER. The users of the Internet based CATE should be able to:

- View catalogues of courses offered. This can be done by accessing EUROCOM Interface on-line course catalogues through a SEMPER Directory service, or by direct access tothese on-line catalogues.
- Register and billed for a series of courses. Users can register for a series of courses and get billed for this set of courses. Then users can attend these courses by using some kind of ID that shows the status of the user. The status consists of the following attributes:
  - Payment: Completed, or not completed. This attribute will show how much the user has paid out of the total payment.
  - Attendance: Completed, or not completed. This attribute will show how many, and which courses the user can still attend.
- Pay for courses to attend. SEMPER has to provide secure on-line billing and payment through existing financial institutions.
- Attend interactive multimedia courses online. SEMPER should support secure interactive real-time communication of multimedia applications. By secure communication of material, we mean that, it is guaranteed that:
  - The media communicated between the merchant and the buyer cannot be retrieved during communication by someone else over the network. That is, confidential peer to peer communication is guaranteed.

    - User Authentication. User authentication should be provided through private/public keys or other mechanisms. This can guarantee that the course paid by a specific user is not attended by another one. Example: A key can be given to a user registered to a course. Thus, only the owner of the key will be able to access this course. This key will expire when the user has finished the course.
- EUROCOM EXPERTISE will offer interactive multimedia courses within the following areas:
    - Telecommunications
        - Transmission
        - Switching
        - New Telecom Technologies
        - Telecom Systems Planning
        - Telecom Services
        - Telecom Business Management
        - Telecom Users Training
    - Information Technologies
        - Computer Networks
        - Database Systems
        - Telematic Services
        - Office Automation
        - S/W Engineering
        - EDI
        - INTERNET
    - Quality Assurance

These courses will be accessed through WWW navigators on the Internet or other similar interfaces for other ATM or ISDN networks where these services will be provides (SEMPER may be implemented on an ISDN network specified by the national Hosts, in the second or third year).

The number of courses offered in the basic trial will be limited (3-5 courses). The courses need complicated adjustments to be operable in an Internet environment.

4.3.3.3 Offering

The above described services will be offered on WWW pages. They will be accessed either through a SEMPER directory service or from other Web pages referring to EUROCOM services.

4.3.3.4 Billing, Payment

Marketing, billing and payments will take place through the SEMPER system. The users of the Internet-based CATE will get billed for the following scenarios:
Pay per view. In this case users pre-pay online for the interactive multimedia course they want to attend. The payment interaction should take less than 2 minutes. This interaction will take place before the users attend the course. The following pay per view scenarios should be supported:

- Fixed value payment. In this scenario a fixed money amount is paid in advance (e.g. for a specific course).
- Time of use-based payment. In this scenario the amount of money that will be retrieved from the account of the user (Bank, or other institution account), will be based on the time of use of the system.
- Hybrid. This scenario is a combination of a (fixed value) base payment at the beginning of the course and a final payment dependent on the time of use.
- Pay for a series of courses. In this scenario the users register and pay for a series of courses. The users can afterwards attend the courses using a course ID and PIN given to them at payment time.

- Clients should be able to pay through:
  - credit-card (Eurocard, VISA, Mastercard, etc.).
  - stored value (E-cash, E-purse, etc.).

EUROCOM will use only some of the means of payment available from SEMPER.

4.3.4 Security Threats

4.3.4.1 Service Provider

- Loss of security in the central system: Intruders, impersonating legitimate users might change the user data (e.g., address of delivery), might cancel orders, or might generate fake orders.
- Multimedia course material might be collected by a dishonest competitor.
- Loss of reputation by fake EUROCOM server: In principle someone could offer another WWW server using the same name that is used by EUROCOM and could impersonate EUROCOM.

4.3.4.2 Service User

- Fake users using the system and courses are charged to other existing users.
- Paying without getting the online courses offered.
- Loss of confidentiality: The customer might give secret personal data (like credit card number, name and address) or customer identification data (like PINs, passwords) to a fake EUROCOM server, or to an eavesdropper.
- Loss of privacy: Network users may get information on the use of EUROCOM online courses by specific customers.

4.3.5 Basic Trial

4.3.5.1 Specification of consumer services

EUROCOM will provide distance learning services over the SEMPER environment. It will provide an interface that will allow to retrieve, register, pay, and attend, real-time multimedia CBT courses.

This interface will be first tested on the Internet and it will be later ported to the Broadband Network (BBN) interface provided by the national hosts.
The provided CBT course access interface will be based on one of the following environments:

- NETSCAPE navigator and Macromedia Director, Shockwave
- Sun's JAVA language supported by the NETSCAPE navigator and Sun's JAVA (available for Windows95, WindowsNT, UNIX Workstations, Macintosh System 7.5).

4.3.5.2 Infrastructure

4.3.5.2.1 Service Provider

The EUROCOM EXPERTISE WWW server will be used to provide the SEMPER services. The server is an HP NetServer 5/100 LH2, running Windows NT 3.51 and Netscape Commerce Server (provides support for SSL, Authentication through authentication authorities, claims secure transfer through encryption and data integrity).

4.3.5.2.2 CLIENT

The client in order to access the EUROCOM services is required to have a multimedia PC, with a minimum of 16M RAM, soundcard, running windows 95 (or NT), Netscape 2.0b3 or later (That provides support for JAVA, DIRECTOR movie play back and general plug-in interface). Moreover the client is required to have an INTERNET connection

4.3.5.3 Trial scenario

4.3.5.3.1 Scenario overview

On the top level (www.eurocom.gr) the user can choose between going to the non-SEMPERised version of the EUROCOM-server in order to become a user of SEMPER[50], or to start the SEMPERised version.
In the SEMPERised version, the user can choose between the following options:

1. checking the authenticity of the server (by asking for certificates, thereby initiating a secure channel between customer and server),
2. checking the availability of certain payment instruments (again by checking certificates),
3. view the course catalogues with the course offers

[50] meaning to get the necessary tools.

4. pay and attend a specific course he/she selects (This may not be available for the basic trial) The customer pays online using one of the SEMPER provided banking tools and then attends a course.
5. register for a list of courses and pay for these courses. The user selects a series of courses and pays for these courses to attend them a later time. A user may do this because he/she may get a better offer when paying for more than one course.
6. attend a course he/she has already register and pay for, using a EUROCOM user ID. (This may not be available for the basic trial) The user attends a course he/she has already paid for in the past.

4.3.5.4 Test and Evaluation

Phase 1: Technical training of client test group to get familiar with the system.
Repeated browse and purchase actions. Interactive real-time phone hotline support.
Phase 2: Simulated regular browse and buy actions of test group under normal conditions.
Phase 3: Evaluation through questionnaire and interviews.

4.4 FOGRA

4.4.1 Current Situation

FOGRA is a non profit research institute of the printing and publishing industry located in Munich. Over 600 companies are member of FOGRA. For over 40 years FOGRA was and is an international active independent research institute serving the graphic arts industry. In this field FOGRA was active by means of scientific research and development and by developing national and international standards.

FOGRA has about 60 employees, both scientists and technical personnel working in different departments, i.e. prepress technology, information and documentation, offset printing, screen printing, newspaper printing, printing ink, printing paper, chemistry and environment, print finishing and advanced technologies (expert systems, Multimedia,...). We are closely co-operating with the industry sharing our knowledge as consultants, in seminars, in publications and in conferences.

FOGRA provides practical research for the industry, technical and market development consultancy, work in standardisation bodies, studies, information and documentation, training and congresses. Further we sell software and hardware production support tools.

In effect FOGRA provides a complex transfer service of innovation and research knowledge to its members and to the industry: Products and information of different types are provided through different channels and media.

4.4.2 FOGRA's Business Services

The list contains the most important services and products of FOGRA. Prices given are referring to non-members without any guarantee of validity.

- **consultancy** and expert opinions concerning print, finishing and prepress; (price dependent on time and costs of material and equipment, DM 200 p.h.)
- **seminars** (different topics, prices from DM 770 to DM 1730)
- **symposia** (different topics, different prices)
- **publications** (newsletters, journals (DM 50), research and practice reports (DM 200))
- **literature database services:**
  - literature searches in arbitrary databases (basic fee DM 230 per database + DM 7 per reference + time of search)
  - patent searches (DM 990)
  - copy service (price per page with minimum price)
  - procurement of literature
  - literature survey service (monthly publication of new abstracts, DM 495 p.a.)

- literature profiles (standard and customised profiles, quarterly publication of new abstracts, DM 495 p.a.)
- patent review service (monthly publication, DM 700 p.a.)
- FOGRA literature database parts on disk (DM 4 per reference)

- **Sales of products**: Control equipment and measuring devices

4.4.2.1 Business Process

Below the business process - including marketing, offering, ordering, confirmation, delivery, invoicing, payment and dun management - is described:

FOGRA´s services are offered through FOGRA´s own publications, symposia and direct marketing activities. Additionally advertisement and articles in specialist publications address the target group directly.

Most services have fixed prices published in a special price list. This list is sent out upon request and is included in regular mailings.

Usually a written order is required (mail or fax). For publications and literature database services a phone call of known members is accepted, too. Only for the literature database search service a phone call of members and non-members is accepted. Here the information needs are discussed and specified on phone in parallel with the actual retrieval. The result (a list of literature references) is either printed out or stored on a floppy disk and mailed or faxed directly.

The orders are only confirmed on request. Means of delivery are fax, mail or parcel services. Invoices are sent along with the ordered product, expert opinion report or publication. Symposia and seminars need to be invoiced (and paid) in advance, whereas consultancy services, afterwards. Three different modes of payment are accepted today:

- cash (only during fairs and symposia)
- cheque
- bank transfer

Clients with open overdue invoices are listed on a black list which is distributed to all FOGRA employees having contacts with clients. Further services are refused until payment. If several reminders are not successful an external cash-in company is engaged.

4.4.2.2 Fogra, Clients and the Market

The clients of FOGRA need to be separated into the members of FOGRA and non-members (others).The difference between them is that members:

- do have a free priorized communication channel into FOGRA (consultancy, support, information)
- Services and products are cheaper (up to 30% discount)
- Exclusive and free distribution of FOGRA´s periodically publication „FOGRA Aktuell“

- All FOGRA publications are free of charge
- can play a part in defining research activities of FOGRA

For these privileges members pay an annual subscription of at least DM 1080. Non-members do get most of the services, but for higher fees.

There are more than 600 members of FOGRA. About half of them are printing businesses (prepress, print, finishing), while the other half are suppliers. 20% of the members are based outside Germany.

The budget for 1995 is around DM 9 million and can be broken down into:

receipts	Million DM
Membership fees	2.0
Grants from the state and the BVD	3.0
Donations	0.6
FOGRA services	3.4
Total budget	9.0

Table 11: FOGRA budget

FOGRA has concentrated on the German market in the past. Recent activities aimed at expanding to other countries and markets.

4.4.2.3 Organisational Structure of FOGRA

FOGRA is organised in 13 departments. Eleven research departments are specialisedwith respect to specific aspects of the print production process. Research and consultancy is done in the functional independent departments: Printing ink, Printing paper, Print finishing, Continuous stationary printing, Screen printing, Newspaper printing, Offset, Innovation research, Prepress technology, Chemistry and the environment.

The two departments „Information and Documentation“ as well as „Administration“ have different roles: the first one is responsible for public relations, documentation of research results, produces publications, organises conferences and provides the literature database. The Administration department is obviously responsible for all administrative matters, secretariat, order processing and especially all business transactions.

In general there are two ways to contact FOGRA:

- General contact through the secretariat, where the telephone exchange is located
- Direct contact to specific departments (or employees)

Usual communication means are mail, telephone and fax.
Once a direct contact is established, the requested service or product is provided completely within the respective department (can be any of the 13 departments). After the „content part“ is fulfilled, delivery, invoicing and all subsequent business operations are handled in the Administration department. The following figure shows this process:

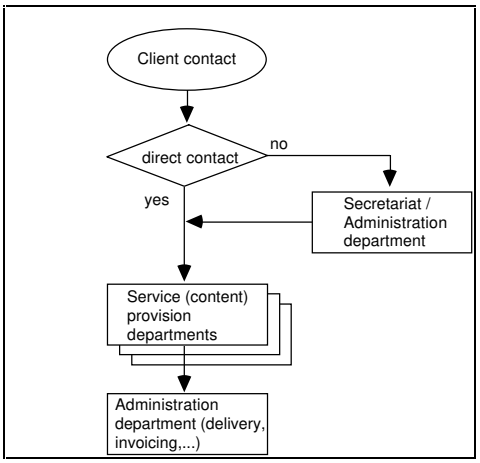

Figure 5: FOGRA businessflow

4.4.2.4 Technical Infrastructure for Online-Services

4.4.2.4.1 At FOGRA

The in-house communication is based on phone, paper and a TCP/IP based core network with a gateway to the Internet. A WWW server, an anonymous ftp server and a mailserver are existing.

The gateway to the internet is provided by XLink represented by the local provider ISAR. Technical basis is a Router(BANZAI) and a single B-channel (64 kb/sec) ISDN connection. To improve the connectivity the WWW server will be hosted by ISAR. The connection speed from ISAR to the Internet is 2Mbit/s.

Platforms used are mainly MacOS, some Windows/DOS and two Suns (Solaris 2.3). The literature database is situated on a Windows PC in the department „Information and Documentation“. Only a mirror of this database will be accessible through the network.

4.4.2.4.2 At Client

The clients of FOGRA have different types of computers, but mainly Macintoshes and increasingly Windows-PCs. As a basis for wide area data communication ISDN is broadly used.
The available Macintosh based solutions for data transfer across ISDN are using non-standard protocols. In practice this causes no serious problems because there are only two main manufacturers (Hermstedt and Planet). There are also special cross platform solutions for file transfer as well as a PPP solution which allows TCP/IP connections over ISDN. Our provider ISAR confirms that links between a BANZAI router and Macintoshes with a Hermstedt ISDN card are running well.

4.4.3 General View and Strategy for Electronic Commerce

There are two aspects important for FOGRA regarding electronic commerce:

The digitalisation of production processes in the printing and publishing industry proceeds. Traditional company and market structures change. Digital data transfer between clients and providers becomes a normality. The next step is electronic business communication like EDIFACT. New electronic markets evolve with their own rules. It is the task of FOGRA to support clients and members in this difficult process. Therefore FOGRA needs to acquire knowledge early.

This is one reason why FOGRA offers its services on-line. On the other hand the communication and quality of services for clients will be improved and new markets can be addressed.
In any case it is our duty to identify specific opportunities and dangers for our clients and members. Through the participation in projects like SEMPER the necessary expertise in electronic commerce is guaranteed. Therefore an active contribution to the set up and modelling of electronic markets through SEMPER is considered to be a necessary task.

4.4.3.1 Perspective and Goals

FOGRA´s strategy and long term goals are to evolve to a research, support and consultancy service provider for publishing based on a completely digitised information infrastructure. Electronic services will be provided both for free and cost effective in an efficient and secure way for the benefit of our clients.

So in the future FOGRA wants to create and offer integrated Multimedia-Information-Services to its members and a wider audience in the publishing industry covering and enhancing the „old“ services and adding new services like:

- Easy On-line direct access to our literature database with optional human help or human operator mode
- On-line ordering and delivery of secondary literature database services (monthly literature survey service (Literaturdienst), monthly customised literature selection service (Literaturprofil)
- Easy access to people for technical consultancy
- Easy access to reports (expanded to multimedia content containing more than still images, text, graphics - thus animation, living tables, sound, etc. to make the reports more usable)
- Easy access to public data/files
- Electronic sale of products (electronic production support tools, physical goods,...)
- Easy access to our Print Problem Diagnosis Expert system
- Provision of a (multimedia) company presentation
- Easy access to training courseware (maybe with human on-line help)
- On-line information on FOGRA´s activities and services
- On-line booking of symposia, seminars

The communication platform for services like this of the future will have to support and integrate telephony, videophony and data communication. A Multimedia information database is obviously needed with controlled access. A publishing or workflow system will support the efficient production of publications. For the cost-effective external services accounting functionality is required. Since we distinguish members and non-members, FOGRA needs to identify communication partners usually.

An interesting option for the future could be to provide services blindly: Possibly a client could prefer to be anonymous because his interest in specific topics is related to sensitive business activities. As long as payment is guaranteed any service could be provided.

4.4.3.2 Expectations on Means of Payment

We see, in principle, 3 ways for payment in on-line environments:
1) Bank transfer of the client following electronic invoices, coming along with non-physical goods (i.e. data) or sent in parallel with physical goods.
2) A electronically sent (and signed) allowance for a debit bank transfer performed by FOGRA will be exchanged with non-physical goods or sent in parallel with physical goods.
3) Electronic cash is exchanged with non-physical goods or sent in parallel with physical goods.

Obviously, the first option implies some necessary hope that clients will pay the invoice, whereas the other two options guarantee payment by the exchange operation: goods versus money!

Today the first option is applied based on paper invoices. In order not to discriminate between on-line customers and standard customers we need to offer the first option for on-line, too. Nevertheless, the other options are more attractive. One way to stimulate clients to use these new options could be to apply discounts (or surcharges respectively).

4.4.4 Security Threats

4.4.4.1 Security Threats for FOGRA

- Loss of security in the central system
- There is a direct connection from the Web-Server to the LAN of FOGRA. Good protection (i.e. firewalls) are a must.
- Loss of reputation by a fake FOGRA server
- Since we provide significant (technical) information with direct business implications based on our reputation, clear identification of the authentic FOGRA is a must.
- Fulfilling orders without getting paid
- This is a minor problem today but could become more serious for on-line services. Money losses should be reduced in general to a minimum.
- Fulfilling orders on wrong assumption

- Special conditions are valid for (paying) members. Only members should get these conditions through identification means in order to avoid frustration and to stimulate membership.

4.4.4.2 Security Threats for the Clients of FOGRA

- Fake orders:
  An impersonator might order under another identity X at the expense of X. Who will pay for the damage ?
- Paying and Ordering without getting the goods or services ordered.
  It may be possible to intercept the order and the money.
- Unsecure client infrastructure
  Most clients are businesses with more than one employee.
- Access rights to on-line services and the payments system need to be defined and administered based on an appropriate system. Such potentially open and distributed systems need to be part of SEMPER services or at least to be connected to and therefore could be a line of attack.
- Lossof confidentiality
  Secret and personal client data are transmitted. An eavesdropper or a fake FOGRA server could get this data.
- Denial of service
  An adversary might cause the clients exclusion from FOGRA services by issuing forged orders. This was no problem in the past but could possibly happen in a new on-line environment with a partial hacker culture.

4.4.5 Basic Trial

For the initial trial FOGRA will select a small closed group of its members and use „fake money“ in order to minimise risks.
In this Basic Trial FOGRA will implement its monthly literature survey service (Literaturdienst) and an online shop for reports in electronic form (pdf).

4.4.5.1 Monthly Literature Survey Service

The literature survey service provides a current selection of interesting articles. FOGRA has developed a specialised literature browser application for Apple Macintosh and as a beta version for Windows. The literature data files are separated from the browser and are generated on a monthly basis.
The literature survey service will be offered in a variety of delivery and payment modes

4.4.5.1.1 Subscription

This is a „push“ type of service where delivery is initiated each month by FOGRA. Payment can be:

annually - in advance (reduced price)

monthly - simultaneous to delivery (normal price)

4.4.5.1.2 Shop

This is a „pull“ type of service where the client has to come to the virtual FOGRA shop (the FOGRA Web-server), select the desired literature data file(s) and buy it (download or traditional disk delivery). Payment then occurs simultaneously (normal price). For the first trial only the shop mode with file download will be implemented. This Shop mode is easily expandable to other digital products like research reports.
During the first phase of the project only a restricted test group of clients will be addressed.

4.4.5.1.3 Offering

Most services of FOGRA have fixed prices published in a special price list. This list, including detailed product/services description, is published on the FOGRA Web-server. Samples of the services, in particular of the literature survey service, are given. A disclaimer will be displayed on all Web-based offers transferred insecurely. Secure offering will be realised through SEMPER as well as „shttp“ based on a Netscape Webserver. Secure, means that every client can check that (s)he is genuinely connected to the FOGRA server.

Orders are initiated directly from form-based Webpages but must be confirmed only with the SEMPER software. Which also provides the exchange mechanism money versus good. For the first trial „fake“ money will be used.

It is a must for FOGRA to differentiate between members and non-members. Therefore FOGRA needs to be able to identify the client.

Furthermore, FOGRA will need to be able to track the diffusion of the literature data files: this is necessary because in principle it is possible for an anonymous client to collect all the distributed monthly data files, build up an independent literature database and to sell this database. Non-anonymous clients will be more sensitive to this problem.

Every client is sure that (s)he is connected to the FOGRA server. The order (which files, which price) needs to be a valid order (using the digital equivalent of a signature) for both FOGRA and the client.

FOGRA must be sure that the correct file was received by the client. FOGRA must get the agreed amount of money simultaneously with the file transfer (or it must at least be guaranteed within a specific time).

The client must be sure and able to prove that (s)he paid a specific order.
In the future, as a preferred option the money should be transferred directly from the client (or the client’s bank account) to FOGRA’s bank account, in order to avoid any additional administration and electronic cash handling within FOGRA. In the first project phase (fake) electronic money (with a secure exchange mechanism) can be transferred to FOGRA to facilitate the process (i.e. without banks) and to gain experience with electronic cash in general. The process will switch to real money after some initial successful steps.

4.4.5.2 Organisation and Infrastructure

4.4.5.2.1 Service Workflow

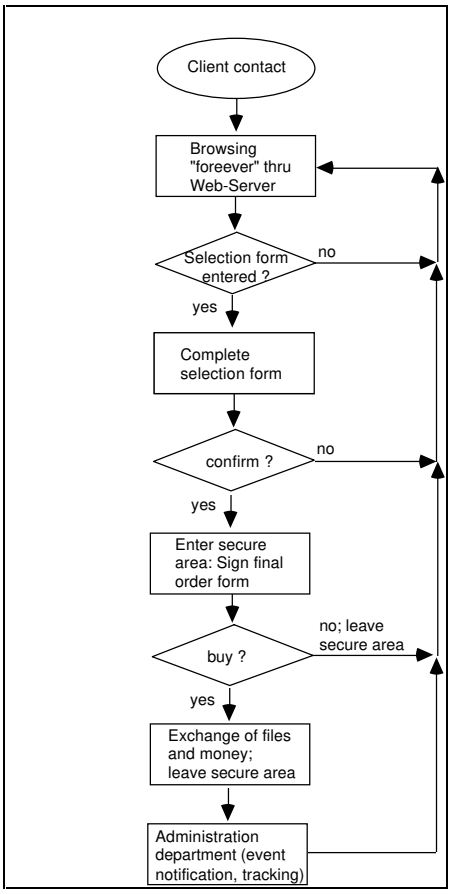

Figure 6: Service Workflow

4.4.5.2.2 Service Production Process

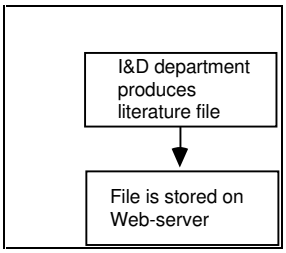

Figure 7: Service Production

4.4.5.2.3 Network Organisation

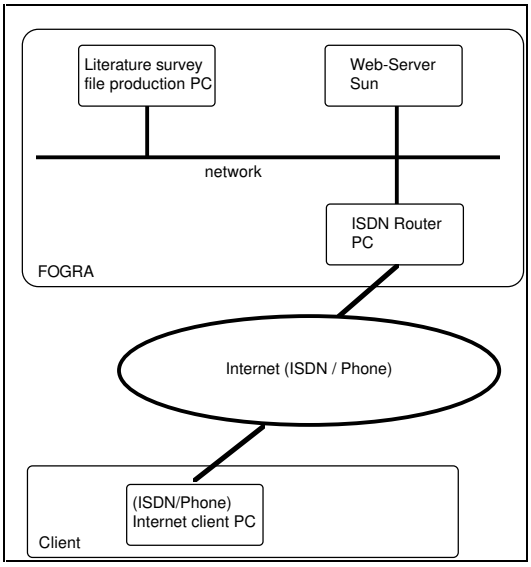

Figure 8: FOGRA NET

The infrastructure at FOGRA is the existing Intranet described above.
Clients have an Internet (TCP/IP) connection (ISDN preferred, but phone/modem is possible too) plus a Macintosh or Windows PC with appropriate Internet equipment (ISDN card / modem, TCP/IP stack, Web browser, Mail tool).
Typically three types of Internet access exist for our clients:

- Direct access through an Internet provider (ISDN and phone/modem),
- Indirect access via T-Online (German Telekom On-line Service),
- Indirect access via CompuServe.

Typical browsers are either

- Netscape or
- Mosaic

4.4.5.3 Consumer Services Offered in the Basic Trial

Outline of the functionality:

- HTML/HTTP based presence of FOGRA in the Internet (referred to as FOGRA On-line). This Web-Server provides a general presentation of FOGRA and some useful information for free. The cost-effective part (Product and Service Catalogue) is part of this server.
- Product and Service Catalogue (Produkt- und Dienste-Katalog): HTML based pages for offering and ordering.
- File download (literature browser) for free via HTTP from the HTML pages.
- File download (literature files) and payment via a SEMPER-specific “secure and fair exchange” function from the HTML pages.

Outline of the user interface:

- Window with Web browser UI displaying HTML pages with text, graphics, images, buttons representing FOGRA product and service offers and order screens.
- Separate window for security functions.

A prototype version of FOGRA Online is available since end of November 1995. Please inspect this site for details; the address is: <http://www.fogra.org>.

4.4.5.4 Requirements for Technical Services

The requirements extracted out of a) can be described as:

mutual identification during an on-line session,
any important communication item (order, literature file,...) should be identical for both parties,
the "send out" should be provable (sender, item, receiver),
the "receive" should be provable (sender, item, receiver).

The technical services should be available on the platforms described above (Macintosh, Windows and Sun). They should co-operate with the existing Web-Server of FOGRA. Further they should co-operate with any Web-browser (especially Netscape and Mosaic browsers). The speed of the Link should be sufficient. This will change during the project.

4.4.5.5 Test and Evaluation

Phase 1: Technical training of client test group to get familiar with the system. Repeated browse and buy actions. Interactive real-time phone hotline support.
Phase 2: Simulated regular browse and buy actions of test group under normal conditions.
Phase 3: Evaluation through questionnaire and interviews.

4.5 OTTO VERSAND

4.5.1 Current Situation

Otto Versand, established in 1949 is the largest mail-order business in the world. Otto is present in most international markets, including America and Asia, and offers, via 250 different catalogues, goods for all kinds of customer target groups almost everywhere in the world. The range of goods offered by the Otto Group covers everything, from shoes and clothes, kitchen equipment to furniture for the entire house.

Total annual turnover: 24 billion DM
Number of employees: 54,000 (world-wide)
Printed catalogues per year: 350 million

4.5.1.1 Existing Services

Otto offers one main catalogue which is updated twice a year to serve the basic needs of the main customer groups. Furthermore Otto provides a broad variety of specialist catalogues to serve either special requirements of the main customer target group (e.g. wedding catalogues, parents' catalogues) or to serve the needs of smaller customer groups (e.g. oversized clothes). Most catalogues are issued twice a year. The first issue covers the spring-summer season and the second issue covers the autumn-winter season. Obviously seasonal catalogues, like the Christmas catalogue, are issued just once a year.

Today, the logistics and the service of Otto Versand has nothing in common with the mail order business our parents were used to. A customer can order 24 hours a day on 365 days a year. If a customer places his order before 12 o'clock, he can get most goods delivered the next day. On selected goods like television-sets, Otto guarantees the customer a delivery on the same day if the order is placed before 12 o'clock. (If the customer is prepared to pay a surcharge for this services). For these services it does not matter where in Germany the customer lives. For a surcharge the customer can choose the day of delivery or he can choose that the goods are delivered in the evening. Without any surcharge an individual delivery address for each article can be specified. Therefore a customer can get the goods delivered to some friends or even to the company where he works.

If a customer is not entirely satisfied with his goods, he can simply call Otto Versand and the goods are revoked without any charge for the customer.

The only intangible goods currently offered by Otto Versand are travel tickets and last minute travel tickets. Some device drivers for hardware sold by Otto Versand are provided as a free service for the customers.

Customer authorisation is done via customer identity numbers, and initially via a location-based (city, street) data base of credit ratings. 98% of our sales are based on invoices which are usually paid by the customers two weeks after receipt of the goods. The remaining 2% of the sales are based on a „goods against money" basis. This applies for customers who do not meet the requirements for credit.

Delivery is done via the Otto-owned *Hermes* parcel service, all over Germany. Orders are accepted from within Germany only, but there are several subsidiaries of Otto Versand in other European countries (e.g., *Les 3 Suisses* in France, see <http://www.trois-suisses.fr/>). In the case that the customer does not match the criteria for credit, the debt collection in exchange against goods is done by Hermes.

Payment is invoice based. Instalment purchases are possible.[51] No credit cards are accepted yet.[52]

For legal reasons Otto Versand does not offer any special conditions to customers, except for so-called *Sammelbesteller* who make collective orders for a group of customers.

4.5.1.2 Existing Digital Services

Otto Versand currently offers three digital services:

4.5.1.2.1 Catalogue on CD-ROM

Currently most of the goods offered in the main catalogue (1,400 pages, 30,000 articles) are on display on a CD-ROM for Windows-PCs. Interested customers can buy the CD-ROM for a small amount of money, which they can deduct from their next invoice if they buy goods from Otto. The CD-ROM contains functions for checking availability and ordering which can be done online via a modem. The transfer of data between the customers PC and the Otto mainframe-system is done via the BTX-interface which is explained in the next paragraph.

The process of dialling and connecting to the Otto-System is completely transparent for the customer, meaning that the customer is aware of what is happening, but he does not need to know how things are done. The CD-ROM is produced regularly every half year. Currently the sixth edition is available. The customer interface on the CD-ROM was subject to many changes during the last editions, so that we now have a version, the customers pretty much understand. Therefore Otto intends to model the business application within SEMPER as similar to the customer interface on the CD-ROM.

4.5.1.2.2 BTX

BTX is the German version of videotex, known also as Datex-J or T-Online, provided by Deutsche Telekom. BTX is similar to the French Minitel system. BTX is a rather old fashioned system using either the CEPT or the KIT standard for presenting information. BTX is a closed online service. Users have to be registered by Deutsche Telekom and they have to pay a certain flat fee per month plus some fees depending on their online times. Based on the technical limitations of the BTX-System goods can only be described via BTX, no pictures can be shown within the BTX-System.

[51] Certain financial services are provided via the Otto-owned *Hanseatic* bank.
[52] Note that in Germany credit cards are not very popular, especially not in the mass market Otto Versand aims at.

4.5.1.2.3 Internet

The internet presentation that can currently be seen at <http://www.otto.de> was developed as a first step for the SEMPER project. Via WWW, catalogues and special offers advertised can be ordered. It is possible of course to order any other item the customer wants to purchase via the world wide web as long as the customer knows the order number for the specific article. (Therefore the customers need to have either the CD-ROM or one of the catalogues if he wants to purchase goods that are not on offer within the internet presentation.)

The services offered via WWW are half interactive: Orders are sent to Otto Versand via email, as soon as Otto receives the email, the availability of the ordered goods is being checked and the customer gets a confirmation of his order stating the delivery times immediately via email.

4.5.1.3 Organisation

4.5.1.3.1 Management Organisation

The central group company in Hamburg is divided in the following departments:

- Purchasing Departments (for hardware and textile)
- Marketing
- Sales Department (including 'New Media - on-line services')
- Internal Consulting
- Group Controlling
- Economics
- Finance/Accounting
- Human Resources
- Organisation and EDP
- Logistic

4.5.1.3.2 Process Organisation

The commercial process starts with offering goods by catalogues, CD-ROM, via Internet or via BTX. All articles are uniquely identified with an article number. The interested customer contacts Otto to ask for assorted goods he (or normally 'she') would like to buy by naming the article number.

There are several ways to contact Otto Versand:

- Telephone,
- Telefax,
- Letter or postcard,
- Datex-J (*otto#) and
- Internet (www.otto.de).

If a customer is a first time customer, he is included in a huge database and gets a customer number subsequently. As customers get the goods first and then receive an invoice to be paid two weeks afterwards, the customer has to meet the requirements for credit. For existing customers a credit-scoring based on his behaviour in the past is performed. For the first contact customer authorisation is done via a location (city, street)- and buying pattern-based data base of credit ratings.

If the inquired goods are available and the customer meets the requirements for credit, the order will be confirmed by Otto including the approximate delivery date for the ordered goods. Goods will then be called from one of the Otto warehouses all over Germany and sent to the customer's or any other address specified by the customer.

At the same time an invoice is written and send to the customer, who makes a transfer from his home bank to the Otto home bank Hanseatic. If the customer does not have an account, he can pay his invoice at any bank. Please note that a surcharge for delivery has to be paid. If you order any number of goods this is currently 6,95 DM (4 ECU) per order (not per article).

In Germany some laws against price reductions to individual customers apply. Therefore Otto Versand does not offer any special conditions to customers, except for so-called Sammelbesteller who make collective orders for a group of customers.

If the customer is not entirely satisfied with the delivered goods, it is a daily part of Otto's customer service to withdraw each piece without invoicing any fees.

After taking back the undesired goods, the invoice will be reduced automatically to the remaining sum for both the customer and the financial department.

4.5.2 General View and Strategy for Electronic Commerce

4.5.2.1 General View

Otto Versand is highly interested in developing electronic media for commercial measures for three reasons. The first reason is that order processing, using electronic means is much cheaper for Otto than ordering via mail or telephone. The second reason is that some of the existing customers find it more convenient to shop via electronic media. The third reason is that the use of electronic media enables Otto Versand to contact new customer target groups that would never have used the old fashioned mail order business our parents were used to.
Electronic shopping has the following advantages for both, the customers and the company:

1) The main advantage is obviously the validity of information. Price reductions can be communicated within seconds, new goods can be offered as soon as they are in stock and new services can be communicated within seconds, once they are available.
2) No limitations in space for product presentations. Therefore views from more than just one angle per article are possible. One day even VR-Models or Videos of the articles could be possible.

3) Articles can be connected via links, so that the customer gets some help when choosing clothes that are supposed to be worn together. Even different services can be linked together, for example when offering expensive goods like kitchen interior, a direct link to a bank with a special credit scheme for this offer could be provided. Even links to the promotion information provided by the producers of branded goods can be provided, giving the producer a chance to concentrate his marketing activities directly at the point of sales.
4) Through the use of electronic shopping, mail-order companies like Otto Versand can compensate many of the disadvantages they used to have in comparison with normal stores.

   Since the first steps of the German videotex-system 'Btx' in the early 1980' Otto established consequently this way for mail-order retailing. In the beginning 1990' new techniques such as CD-ROM, 'IATV' (interactive television) and Internet appeared and Otto is making efforts to participate and co-operate in such projects.

4.5.3 Specification of Online Consumer Services

There are no further new services planned apart from the ones mentioned above. The implemented and accepted payment method depends on detailed proposals of the SEMPER-specialists and the involved cost-structure. A trial implementation of some sort of online payment system might be possible. For the basic trial no new methods of payment will be accepted.

Micropayments for information or services are still in discussion, on the other hand there might be a negative perception by the Internet-consumer. There will be definitely no charge for product presentations or sales related information for the customer.

4.5.3.1 Technical Infrastructure

The Otto Internet presentation is hosted by the service provider 'Point of Presence (POP) - Hamburg' on sun computers.

The 'New Media - online services' department of Otto and most of the customers are using Windows-based PCs, browsers like Netscape, Microsoft Explorer and Mosaic, 14400 or 28800 bps modems and login via universities, companies, service providers or online-services like CompuServe, America-Online or T-Online.

Since September 96 the processing of orders and emails is done by the customer service centers throughout Germany 24 hours a day, 365 days a year. At present the Otto mainframe is not accessible from the WWW directly.

The technical infrastructure of Otto Versand is the responsibility of the department 'Organisation and EDP'.

4.5.4 Security Threats

In the current situation most of the security threats from this paragraph are non-existent. But as soon as a direct access from the internet to the Otto fulfilment system is realised, without any human interface, the following threats will exist and must be faced.

4.5.4.1 Threats for Otto Versand

- Loss of security in the central system
    - Intruders, impersonating legitimate users might change the user data (e.g., address of delivery), might cancel orders, or might generate fake orders.
- Delivery situation could be retrieved by competitor
    - Data about the delivery situation and goods on stock might be collected by a dishonest competitor by simply ordering in a third persons name.
- Demand could be faked by a dishonest supplier
    - If a supplier desperately wants to sell more goods to Otto Versand, he could create artificial demand for his goods by ordering the respective goods for thousands of non-existent customers.
- Customer Data could be collected by competitor
- In mail order business, the main asset of a company is the customer database. If a dishonest competitor or a dishonest adressbroker has access to one of the Internet servers through which most of the customer data are routed on the way to Otto, he can collect valuable information about the customer. As these information are highly qualified, including the information that the customer is interested in mail order retailing, they have got a high value on the address-market.
- Loss of reputation by fake Otto Versand server
- In principle someone could offer another WWW server using the same name that is used by Otto Versand, e.g., <www.otto.de>, and could impersonate Otto Versand.
- Fulfilling orders from customers without getting paid
- This risk is not present in case payment is done on-line by a method that cannot be revoked afterwards. For invoice based payments Otto Versand has a procedure for risk management, based on demographical statistics for new customers and on knowledge of previous behaviour for established customers. Obviously this presupposes correct customer identification.
- Fake Orders
- Some people could try to create thousands of fake orders in the name of other people. The internal checks done at Otto can only check if a person really exists and if this person is applicable for credit or not. Therefore if the intruder gets hold of addresses of real people (which is no problem) he could generate thousands of fake orders without any chance for Otto to find out that these orders are fake.

- Obtaining confidential data about people
- Assuming that someone wants to know if a second person is applicable to credit (at least in Otto's view) he could simply generate a fake order for an expensive good. If the order is confirmed by Otto, that means that the second person has a good credit reputation, if the order is denied, this means that the second person has a bad credit reputation.

4.5.4.2 Threats for customers

- Fake orders:
- An impersonator might order something under the customer's identity, and might even be able to receive the goods, while the customer will be asked to pay or return the goods.
- Paying without getting the ordered goods:
- Insiders might be able to acquire the customer's on-line payment without forwarding the order (and money) to the fulfilment system.
- Loss of confidentiality:
- The customer might give secret personal data or customer identification data (like PINs, passwords) to a fake Otto Versand server, or to an eavesdropper.
- Loss of privacy:
- Since we are talking about hard goods delivered to the customer via mail or parcel services, the customer is necessarily traceable by the service provider. Outsiders might learn about the customer's behaviour and interests by observing the communication between customer and Otto Versand. Depending on the payment system used, the payment system provider can observe the customer's behaviour and interests as well. This might be a serious risk given the broad spectrum of goods offered by Otto Versand.
- Denial of service:
- Someone, pretending to be the customer, could cause the customer's exclusion from the Otto Versand services by issuing many forged orders.
- Espionage of personal Credit Data
    - As mentioned above: Somebody pretending to be somebody else can get information about the creditworthiness of the second person. (At least a creditworthiness in Otto's View)

4.5.5 Basic Trial

4.5.5.1 Business Aspects

The initial trial will include offering, ordering, and payment of physical goods via the internet, using the semper functionality to minimise the risks that were mentioned in the paragraph before. The trial will be based on the existing WWW infrastructure. The only functions from SEMPER implemented in the first trial will be customer- and merchant identification and an encrypted transfer of sensitive data between the customers PC and the Otto website.

The customer has any type of WWW browser installed and running, and knows how to connect to Otto Versand. As the basic trial is a closed trial, the trial customer will have received the SEMPER software including a manual for use and he will (hopefully) have received a certificate. The user group will be restricted to at about 100 existing customer who meet the hardware requirements.

The scenario includes the following steps:

- The customer receives the SEMPER software via normal surface mail. Further he gets some printed information like a manual and some additional information about SEMPER. These information contain a detailed description how to use the software and how to obtain the necessary certificates for the basic trial. Further the information contain the URLs for the service providers' web sites.

- The customer can browse through Otto Versand´s offers which can either be presented in the Internet or the customer has access to a printed or a CD-ROM catalogue. The customer will be able to fill his virtual shopping trolley with goods he wants to buy from either source.

- The only means of payment a customer can choose **for the basic trial** will be based on paper invoices.

- The customer can retrieve the state of availability and delivery times for the goods in his virtual shopping trolley. Therefore he will need to identify himself before he can get any information about the availability of goods. Absolutely no availability information can be given to an anonymous customer.

- If the goods are available and can be delivered in a satisfying time, the customer places an order for these goods and will get an electronic confirmation via the Internet.

The goods which will be offered in the first trial via the Internet are real physical goods, which are physically shipped to the customer. Therefore orders have to be paid by the participants of the first trial with real money. For the first trial no alternative payment systems will be implemented.

Goods are delivered off-line, since only tangible/physical goods are being considered for the initial trial. Disputes are handled outside the system.

To encourage the customers to place as many orders as possible, existing customers who shop regularly at Otto are chosen for the trial, further these customers will get a 5% discount for the ordered goods. As an additional incentive, the participants will get a voucher worth 10,- or 20,- DM.

4.5.5.2 Organisation and Technical Infrastructure

The initial trial will include offering, ordering, and (offline) payment of physical goods.

Basis for this trial will be the existing WWW server <www.otto.de> hosted by POP. This server will be mirrored by and at IBM ENC in Heidelberg, and the SEMPER functionality will be integrated in the mirrored version at ENC. The existing realised gateway between Datex-J and Otto HOST will be used for the basic trial. So the Semper WWW solution could set up upon this interface for checking availability and ordering for chosen goods to implement some kind of interactive dialogue between the customer and the Otto-Presentation.

The participants for the basic trial were identified via a questionnaire that could be filled in by all visitors of the Otto-Homepage. Amongst about 1000 answers, we identified the customers that meet the requirements to run the SEMPER software. These requirements were:

- Hardware: 486 or higher, CD-ROM device or 3 ½ '' disc drive, Modem, LAN or ISDN-Card to connect to the internet.
- Software: The customers have to have the right and the ability to install new software on their system. For most companies and universities this is not the case. Further they need to run either Windows95, AppleOS or UNIX.
- Experience: The participants should have at least half a year of experience on the internet. Otherwise they would have difficulties to understand what SEMPER is about and they would not understand the system.
- Relation to Otto: For the basic trial we decided to use only existing customers from Otto, meaning that people who answered the questionnaire and met the above mentioned criteria which were no Otto-Customers can not participate in the trial. For subsequent trials these people can be invited.

4.5.5.3 Test and Evaluation

There should be no specific training necessary for the first trial. The system has to be self explanatory and easy to use for a customer who is confident with the normal internet procedures. The trial can be evaluated by examining the customers´ behaviour in terms of inquiries, orders and payment behaviour. These results can be compared with the results of a second customer group which is similar to the first one with the main difference that the second group will not be invited to the test.

For two reasons it will be necessary to implement a hotline for the basic trial. The first reason is obviously the customer himself who might need support. The second reason is that the hotline will collect all problems and customers´ reactions in one central place.

4.6 Common Implementation Strategy

4.6.1 Registration and Certification

Registration on a normal market as well as on an electronic market is used in different situations. User and clients or members and participants are registered to enable a stronger binding and set up groups with different rights. The relation of EUROCOM and its clients, FOGRA and its clients and members, and Otto and its customers are examples. In the start up phase of the SEMPER trial there will be users registered already in some way and there will be users which register online during the trial. Typically a mechanism to proof the identity of a registered user will be set up. This user registration is in the first step something special between the clients and the service providers.
To enable an open market some general procedure must exist. Therefore certification authorities (CA) provide a special service. One can register a public key at a CA. The CA signs an electronic document (certificate) stating that the user of this public key is registered at this CA and that the CA has checked the identity of the owner of this public key. The shops will register also at a CA. All participants who accept the certificates of a special CA will now be able to identify each others.
The functionality of a CA could be combined with a membership, different CAs can accept each others' certificates and certificate can be more general, stating for example that the owner of a certificate is only liable up to 10 $.
In the basic SEMPER trial all potential participants will be asked to register at GMD.
So in the situation of the trials the goal of user registration is not to establish a new electronic business relation with a new user but to transfer an existing customer relation from the „conventional" marketplace to the electronic marketplace.
The business relation of the electronic marketplace is normally „bound" to the electronic identity of the user. The electronic identity is the public key of the user. For reusing established relations to customers, we need to be able to relate the electronic ID (i.e., public key) with the well-known identity (i.e., name, address, or customer number). This is done by a key certificate. To limit the risk of the users, all key-certificates should be accompanied by attribute certificates stating the method of registration (which fixed the liabilities) and fixing an upper limit of liability for the user.
Here we describe examples for initial user registration from the user's point of view and give recommendations for the SEMPER trials. Additional background information about registration can be found in the SEMPER deliverable D03 or Verisign's "Certification Practice Statement" (CPS) at <https://www.verisign.com/repository/CPS/>.
.

4.6.1.1 Possible Registration Procedures

4.6.1.1.1 No Registration

Just to illustrate that registration is not always necessary, we explain a „No Registration" purchase. The basic idea is that the customer sends a payment together with a key later used for secure delivery to the shop. It consists of the following steps:

1. Customer obtains SEMPER software (e.g., by download or from a service provider).
2. Customer starts SEMPER software.
3. The customer enters a shop (i.e., clicks a logo)

4. The identity of this shop is checked and displayed on the TINGUIN.
5. Shop sends signed offer
6. Customer selects goods (e.g., an HTML-page) and therewith acknowledges the price.
7. The „purchase“ commerce service generates a new random session key.
8. The „purchase“ commerce service sends the order (i.e., URL), this session key and a payment to the shop. This „package“ is encrypted with the shops public key.
9. The shop decrypts the package and deposits the payment.
10. The shop encrypts the goods with the session key contained in the package.
11. The shop sends the encrypted goods to the customer.
12. The customer decrypts the goods and displays them.

Discussion: The user bears the risk. However, if the user paid and the shop did not deliver, the user could try to make the shop liable based on the signed offer. Since the goods are just data, the shop is able to resend them. Better the implemented transfer mechanisms should provide for fair exchange of information against payment.

4.6.1.1.2 The Point-and-Click Registration

This is a fully electronic registration for SEMPER.
It consists of the following steps:

1. Customer obtains SEMPER software (e.g., by download or from a service provider).
2. Customer starts SEMPER software.
3. Customer starts the „Point-and-Click“ Registration commerce service (may also be executed by default after starting the software).
4. The commerce service asks the user for a new initial pass phrase.
5. The script generates a public key and a randomly assigns a new customer number.
6. The script encrypts the public key and the customer number of the user with the public key of the CA (which is contained in the script) and sends the public key to the CA.
7. The CA stores the ID to prevent registration of multiple keys under the same ID and certifies the key together with a note stating that the registration has been performed according to the point-and-click registration procedure.
8. The CA sends the certificate back to the user.
9. The script stores the certificate. The certificate may automatically used for subsequent sessions with this provider.

Note that only Points 1-4 involve interaction with the user. This registration establishes a unique identity of a customer. Since there is no check of this identity at all, the unique identity is just a pseudonym (e.g., number). If the user reuses his customer number in subsequent sessions with this service provider, the service providers enabled to re-recognise an individual, i.e., several actions of the same user can be linked. This can be used to slowly establish a business relation: I do not know who you are, but since you have paid the last ten $0.1 pages, I'll now send some $0.2 pages, etc.
Discussion: The provider bears all the risk. The user can not be made liable at all. The advantage is that it encourages new user to join, since registration is very simple and still enables the provider to establish a customer relation if the user wants to.

4.6.1.1.3 Phone Call-Back Registration

Since the „Point-and-Click" registration may be performed fully electronically (and thus registration of many fake names would be possible), the following phone call-back registration requires some user interaction.
It consists of the following steps:

1. Customer obtains SEMPER software (e.g., by download or from a service provider).
2. Customer starts SEMPER Software.
3. Customer starts the Phone call-back Registration commerce script (may also be executed by default after starting the software).
4. The script asks the user for a new initial pass phrase.
5. The script generates a public key and randomly assigns a new customer number and a random pass phrase.
6. The script encrypts the public key of the user, the customer number, and the pass phrase with the public key of the CA (which is contained in the script) and sends the encrypted package to the CA.
7. The CA stores the ID to prevent registration of multiple keys under the same ID and waits for a phone-call.
8. The user calls the CA and reads the pass phrase and his customer number to the operator.
9. The CA calls the user back after verifying the phone number.
10. The CA certifies the key together with a note stating that the registration has been performed according to the phone registration procedure.
11. The CA sends the certificate back to the user.
12. The script stores the certificate. The certificate may automatically used for subsequent sessions with this provider.

Note that now no totally automatic processing is possible: The user has to make a phone call. Only points 1-4 involve interaction with the user. This registration establishes a unique identity of a customer. Since there is no real check of the identity, the unique identity is just a pseudonym (e.g., phone number). The use of this registration is to enable the service provider to re-recognise an individual, i.e., several actions of the same user can be linked. This can be used to slowly establish a business relation: I do not know who you are but since you have paid the last ten $0.1 pages, I'll now send some $0.2 pages, etc.

Discussion: This procedure is similar to the „Point-and-Click“ procedure and goes with the same liabilities. However, an attack is more difficult, since human interaction is needed: In the „Point-and-Click“ procedure, any host can generate huge numbers of bogus registrations at virtually no cost. In the “Phone Call-Back” procedure, each of these registration also requires a phone call by a user which limits the amount of bogus registrations which can be generated, and raises the cost of such an attack.

4.6.1.1.4 The Letter Registration

Customer obtains a letter from e.g. OTTO stating that the customer has been selected for the trial and that the software will be delivered by GMD.

1. Otto sends the address and customer number of these customers to GMD.
2. The CA sends the SEMPER software to the customer together with a letter stating Name, Address and a random pass phrase.
3. Customer starts SEMPER Software.
4. Customer starts the „Letter“ Registration commerce script (may also be executed by default after starting the software)
5. The script asks the user for a new initial pass phrase.
6. The user copies name and pass phrase from the letter.
7. The script generates a public key.
8. The script encrypts the public key of the user, the name and the pass phrase with the public key of the CA (the script contains this key) and sends the encrypted package to the CA.
9. The CA checks the name and passphrase received in the letter.
10. The CA certifies the key together with a note stating that the registration has been performed according to the „Letter“ registration procedure.
11. The CA sends the certificate back to the user.
12. The script stores the certificate. The certificate may automatically used for subsequent sessions with this provider.

4.6.1.1.5 The Notary Registration

We now describe the most secure registration procedure which may enable signatures which are legally binding for limited applications and values. This may be used for general purpose registration, i.e., not specific to a service provider but rather for all shops trusting the CA.

1. Customer obtains SEMPER software (for instance by download or from a shop).
2. Customer starts SEMPER Software.
3. Customer starts the „Notary“ Registration commerce script (may also be executed by default after starting the software).
4. The script asks the user for a new initial pass phrase.
5. The script generates a public key.
6. The user enters his name.

7. The script prints the public key and the name and a notice about the legal implications and the limit of liability.
8. The user visits a notary and signs the printout. The notary checks the identity of the person (e.g., passport) and sends the signed letter together with a letter stating that he checked the identity of the signatory based on the well-established notary rules to the CA.
9. The script encrypts the public key of the user together with the Name with the public key of the CA (which is contained in the script) and sends the encrypted package to the CA.
10. The CA checks that the public key on the notary's letter is the public key sent to the CA by the user. It certifies the key together with a note stating that the registration has been performed according to the notary registration procedure.
11. The CA sends the certificate back to the user.
12. The script stores the certificate. The certificate may automatically used for subsequent sessions with this provider.

Discussion: This procedure is the procedure with the strongest proof of identity. The liability would be based on two signed contract between customer and CA and between service provider and CA. The notary would only be liable that he really checked the passport and compared the signature with the signature on the passport. However, the risk of the user must be limited, i.e., a overall maximum amount of liability for transactions with a certain key must be fixed and secure hardware to store the users secret key should be used.

4.6.1.1.6 Registration by Mutual Contract

We now describe another secure registration procedure. Instead of a more general registration, this procedure establishes a registration for exactly one provider which still may be of legal relevance (under the restrictions stated above). The basic idea is that both parties fix on the public-key as part of a mutually signed contract.

1. Customer obtains SEMPER software (for instance by download or from a shop).
2. Customer starts SEMPER Software.
3. Customer starts the „Contract" Registration commerce script (may also be executed by default after starting the software).
4. The script asks the user for a new initial pass phrase.
5. The script generates a public key.
6. The user enters his name and address (and provider specific information).
7. The script prints a contract between service provider and user which includes customer data (public key, name, etc.) and the limit of liability.
8. The user (person) visits the service provider.
9. Both parties sign the contract while identifying each other. A copy of this contract is send to the CA.
10. The script encrypts the public key of the user together with the Name with the public key of the CA (which is contained in the script) and sends the encrypted package to the CA.

11. The CA checks that the public key on the contract is the public key sent to the CA by the user. It certifies the key together with a note stating that the registration has been performed according to the „contract“ registration procedure.
12. The CA sends the certificate back to the user.
13. The script stores the certificate. The certificate may automatically used for subsequent sessions with this provider.

Discussion: This procedure may enable legal liability. However, it restricts the use of the public key to one service provider. For additional providers, additional contracts would need to be signed.

4.6.1.1.7 Subsequent Registrations

We described methods for initial electronic registration of customers. Naturally, these procedures can also be used for subsequent registrations with other entities. However, one may also use the existing registration for issuing additional certificates. If a customer has already registered with a third company (without legal liability), the service providers may mutually accept their certificates. The same holds, if a user has already been registered centrally. I.e., in a business database or at the chamber of commerce. However, if the registration would imply some liability of the user, the user still needs to sign a contract extension, that this key may also be used for purposes other than those agreed upon in the initial contract.

4.6.1.2 Registration for the first trial

After describing several possible registration procedures, we now recommend procedures for our initial trials.

4.6.1.2.1 Otto

For new Otto customers who responded to their web site, „Phone Call-Back“ registration would be the most appropriate way. Note that for the basic trial only existing customers will take part. For these customers „Letter Registration“ will be the implemented way of registration.

4.6.1.2.2 FOGRA

FOGRA aims at legal bindingness of electronic contracts. However, since it is recommended to provide legal bindingness only with secure hardware, we do not recommend the “Notary Registration” but rather use the „Letter registration” instead.

4.6.1.2.3 EUROCOM

For EUROCOM the Point-and-Click registration will be used.

4.7 Detailed Implementation Strategy

4.7.1 Overview

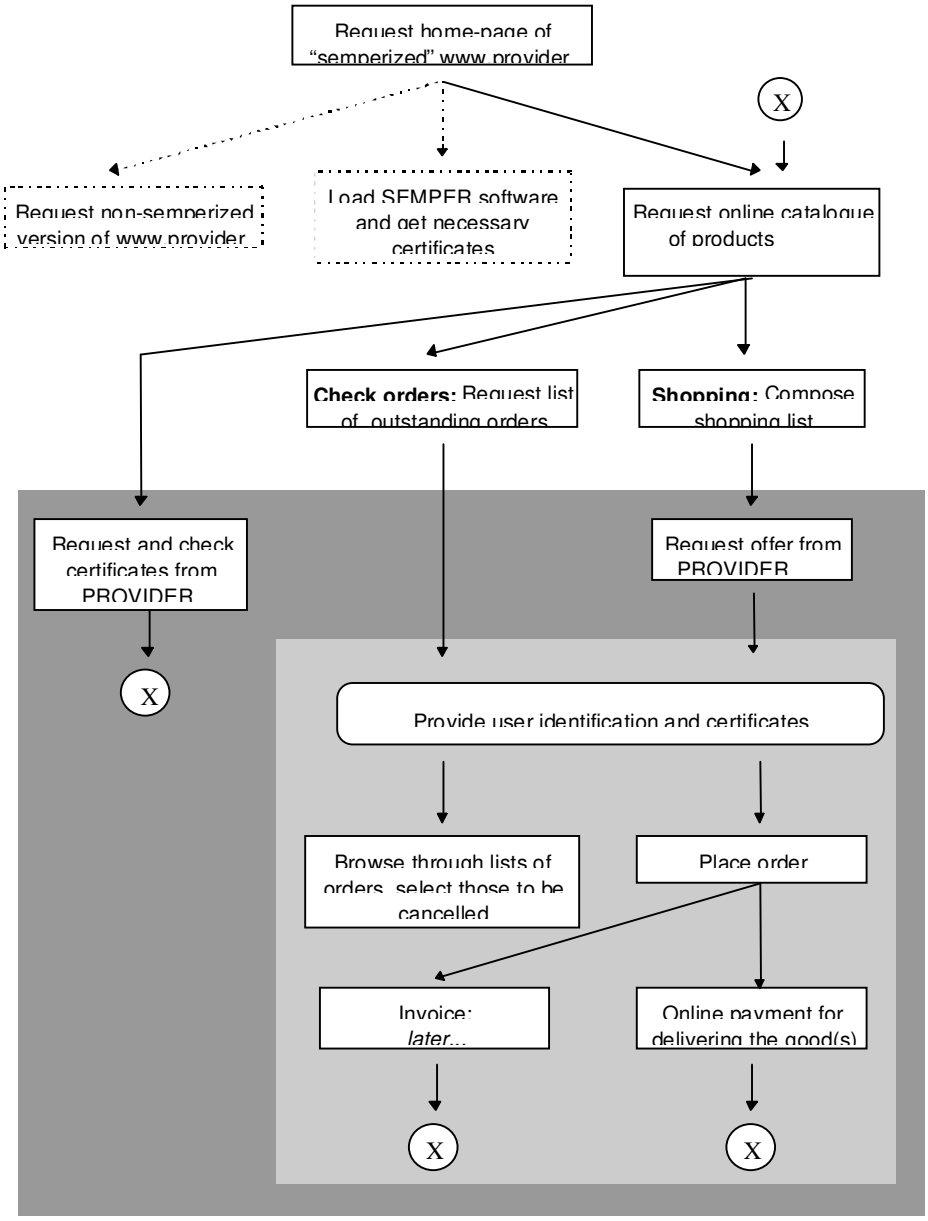

Figure 9: Diagram of possible user actions

Figure 9: Diagram of possible user actions summarises the three scenario: On the top level (home page of Provider) the user can choose between going to the non-semperised version of the providers (EUROCOM, FOGRA, OTTO) -server to become a user of *SEMPER*, or to start the semperised version.

In the semperised version, the user can choose between

- checking the authenticity of the server (by asking for certificates, thereby initiating a secure channel between customer and server),

- checking the availability of certain (on-line) payment instruments (again by checking certificates),
- managing outstanding orders,
- select the goods or services to be ordered

The first two actions always end at the same point the customer started, i.e., on the same web page.

For the third choice, the customer must have checked the authenticity of the server, identifies herself, and finally signs the list of changes required from the server. Afterwards, the customer is back to the first page of the semperised version. For subsequent actions in the same session no mutual authentication is required anymore.

For the fourth choice, the customer pays on line using one of the provides online payment systems and receives the good(s) / services.

4.8 Outlook to Advanced trials

4.8.1 EUROCOM

The courses offered by EUROCOM will be accessed through WWW navigators on the INTERNET or other similar interfaces for other ATM or ISDN networks where these services will be provides (SEMPER may be implemented on an ISDN network specified by the national HOSTS, in the second or third year).

The number of courses offered in the basic trial will be limited (3-5 courses). The course need complicated adjustments to be operable in an INTERNET environment.

For the second Year EUROCOM will port a full multimedia version of the system (material composed of video, sound, animation, etc.) used in the trial of the first year, to the security services ATM network interface provided by SEMPER.

The users of this system will be EUROCOM customers. The system server will run on the INTRACOM (Greek National Host Node) servers and the users at EUROCOM classrooms or other remote sites within Greece, will attend, register and pay for specific CBT courses.

In the third year EUROCOM will provide the distance learning services, described in the second year trials, to customers at European sites. This will depend on the connection availability and traffic cost provided by the Greek and German PNOS.

4.8.2 FOGRA

FOGRA´s strategy and long term goals can be circumscribed as:
FOGRA´s strategy is to evolve to an efficient research, support and consultancy service provider for publishing based on a completely digitised information infrastructure. Electronic services will be provided both for free and cost effective in an efficient and secure way for the benefit of our clients.

In the future FOGRA wants to create and offer integrated Multimedia-Information-Services to its members and a wider audience in the publishing industry covering and enhancing the „old“ services and adding new services like:

- Easy On-line direct access to our literature database with optional human help or human operator mode
- On-line ordering and delivery of secondary literature database services (monthly literature survey service (Literaturdienst), monthly customised literature selection service (Literaturprofil)
- Easy access to people for technical consultancy
- Easy access to reports (expanded to multimedia content containing more than still images, text, graphics thus animation, living tables, sound, etc. to make the reports more usable)
- Easy access to public data/files
- Electronic sale of products (electronic production support tools, physical goods,...)
- Easy access to our Print Problem Diagnosis Expert system
- Provision of a (multimedia) company presentation
- Easy access to training courseware (maybe with human on-line help)
- On-line information on FOGRA´s activities and services
- On-line booking of symposia, seminars, etc.

The communication platform for services like this of the future will have to support and integrate telephony, videophony and data communication. A Multimedia information database is obviously needed with controlled access. A publishing or workflow system will support the efficient production of publications. For the cost-effective external services accounting functionality is required. Since we separate members and non-members FOGRA needs to identify communication partners usually.

An interesting option for the future could be to provide services blind: Possibly a client could prefer to be anonymous because his interest in specific topics is related to sensitive business activities. As long as payment is guaranteed any service could be provided.

- Research-Reports are rather small, depending on the number of images. The main problem will be quality integrity.
- selling of test-images (ISO SCID)
- selling of software-packages (velvet)
- consultancy, with usage of video-conferencing, exchange and test of data, telephony
- next years symposia should be bookable via the net.

4.8.3 Otto Versand

Further trials will definitely be open trials, so that the problem of certification of unknown individuals has to be tackled. Further subsequent trials will run on the Otto server and the customers can chose if they want to use the normal version of the server or if they want to use the semperised version. Some optional payment modules could be implemented for further trials. The functionality on the Otto side will include a virtual shopping trolley, a database with some thousand articles and a search engine that supports queries like: „Show me all shirts, colour blue, from the company xxx priced 80,-DM or less“.

To enable as many customers as possible to use semper, the software has to be very easy to install and it has to be as transparent as possible.
Subsequent trials might include

- selling of travel tickets (last minute offers, etc.);
- selling of intangible goods like games, software, digital catalogues, video and music clips.
- Alternative payment methods
- The customer will be enabled to check the status of previous orders through the Internet, and can cancel those that are not already in the process of delivery.

4.9 Summary

SEMPER will implement three business contexts provided by the new on-line services of the participating service providers, EUROCOM, FOGRA and Otto Versand. They provide three separate platforms for evaluating the technical services which have been developed for the SEMPER architecture. Specification of requirements for the respective technical services was based on the definition of the consumer services.

An in-depth examination of the three participating organisations was carried out at the business level, organisational level and technical level, resulting in detailed requirement profiles specific to each business organisation. In addition, each service provider formulated a strategy for the introduction and subsequent development of electronic commerce in their respective market sectors. These strategy statements ensure that the initial SEMPER services, which will be implemented in the basic year 1 trial, take into account the broader future aims of the participating organisations, as well as the more advanced SEMPER applications planned for implementation in the trials of project years 2 and 3. A review of existing studies of consumer (end-user) requirements was also carried out in order to facilitate compatibility between the product offerings of the participating companies and customer requirements.

The company specific requirement profiles of the three participating service providers were then compared and evaluated in order to formulate a common set of service provider requirements. Close consultation with CT2 and CT3 during this process ensured that the service providers fully understood the technical options available to them at this stage. This process resulted in the identification of five basic categories for security requirements: Authentication (identification) Integrity, Signature, Payment, and Confidentiality.

4.9.1 The three Service Providers

EUROCOM's long-term strategy for electronic commerce is to provide interactive multimedia courses over a broad-band network system that provides secure course material transfer, billing and payment.
FOGRA's long-term strategy is to develop an efficient research support and consultancy service for the publishing industry based on a completely digitised information infrastructure. They require an efficient and secure environment for their electronic services.
Otto Versand's long term strategy envisions a gradual development of the 'virtual' shopping experience beginning with interactive catalogues and secure on-line ordering and extending in the future to digital media and interaction requiring secure on-line delivery and payment.

4.9.2 Trial Scenario

In the following a brief description of the common trial scenario is followed by a more detailed explanation of the Basic Trial requirements. The reader is reminded that the trial requirements described below apply exclusively to the Basic Year 1 Trial and not to the more advanced services which will be required by the service providers and implemented in the SEMPER architecture and technical services in years 2 and 3 of the project.

EUROCOM, FOGRA and Otto Versand have all established World Wide Web pages which will serve as their electronic shop-fronts. Potential customers will be able to contact the companies and obtain information about their products and services via the Internet. For the purposes of the trials, all orders of goods or services will be made by means of selection from the respective WWW pages. Because the customer may want to order more than one good or service during a particular shopping session (or may decide against purchase) it must be possible to review an order before confirming it. The option to cancel part or all of the order at any point in the negotiation must also be available. At least two of the service providers, EUROCOM and FOGRA, will also deliver their services on-line, by means of data transfer via the Internet. As a result, they will also require proof that this data has been received successfully by the customer. A variety of means of payment will be accepted, both on-line and off-line, and all three service providers require the ability to provide electronic receipts for their customers, regardless of the means of payment selected. Due to the fact that the companies distinguish between customer groups in respect of conditions of sale and/or access, all require a means of identifying customer credentials, or rights of access.

Participants in the first year trial will be selected by the respective service provider. Close contact to these participants throughout the trial, as well as follow-up surveys, will provide valuable first-hand input in respect of the end-user requirements for electronic commerce. The selection of customer groups for the initial trials will offer significant advantages in respect of the ability to test more innovative technologies than could reasonably be offered to the general public and in obtaining a quantifiable evaluation of the functionality of technical services offered.

4.9.3 Authentification

Authentification (reliable verification of identity) is frequently required by both the merchant and the customer at various stages in electronic commerce. The first example of this requirement arises at the initial point of contact between merchant and customer, the electronic shop-front. The customers entering this electronic shopping environment must be able to confirm, in a trusted manner, that he/she is genuinely in contact with the company he/she has selected and not an electronic impostor.

Authentification of the customer to the merchant is dependent on the specifics of each customer merchant relationship. Otto for example does not need to know the identity of a customer until an order is placed, while FOGRA or EUROCOM may restrict access to certain information to only those customers that they have authenticated. EUROCOM, for example, frequently deals with students attending prepaid courses, who should only be granted access to their services for the duration of that particular course. FOGRA requires controlled access because they offer different conditions for members and non-members.

Secure verification of customer identity can protect the merchant from fraudulent customers placing fake orders. To achieve this there is a requirement that the identity of merchant and customer can be verified by means of off-line or on-line registration and that this verification can be transmitted electronically to verify identity, both of vendor and customer.

4.9.4 Integrity Protection

Two of the service providers will be delivering their products on-line and, it is essential that the customer receive the correct service and that it be received intact. Both EUROCOM and FOGRA require confirmation that their services have been delivered to the customer.

4.9.5 Transfer of signed statements

The requirement for certification of the identity of merchant and customer mentioned above applies in particular to three aspects of the electronic transaction, i.e. offer, order and receipt. At each of these points in an electronic transaction both merchant and customer may require a secure and verifiable electronic exchange of information, e.g. the customer must be able to treat the merchant's offer as binding, the merchant must be able to regard the customer's order as binding and (as already mentioned) there must be proof of delivery/receipt of the "product". There is a requirement, therefore, for the exchange of three electronically signed statements: the offer, the order and the receipt.

4.9.6 Payment

The initial trials should support traditional forms payment by the means of invoice and bank transfer, but also include the secure transfer of payment card data. In addition, there should be the opportunity to test implementations of electronic money . All service providers in the trial require electronic invoices/receipts for their customers, regardless of whether they prefer to settle their accounts on-line or off-line.

4.9.7 Confidentiality

All the service providers perceive a potential customer requirement for confidentiality. For example customers seeking information or advice in respect of competitively sensitive areas of business, where the client might not necessarily wish outsiders to be aware of an active business interest in the particular field.

5 LEGAL FRAMEWORK FOR ELECTRONIC COMMERCE

5.1 Legal Scenario

5.1.1 Current Situation

The following picture shows the different legal relations between the parties in electronic commerce. It has been anticipated, that there will be one or more entities covering the needs for a public key infrastructure (here called TTP, Trusted Third Party). It is clearly shown that we have to cope with a:

- multi-national
- multiparty
- environment with a tremendous amount of possible contractual relations.

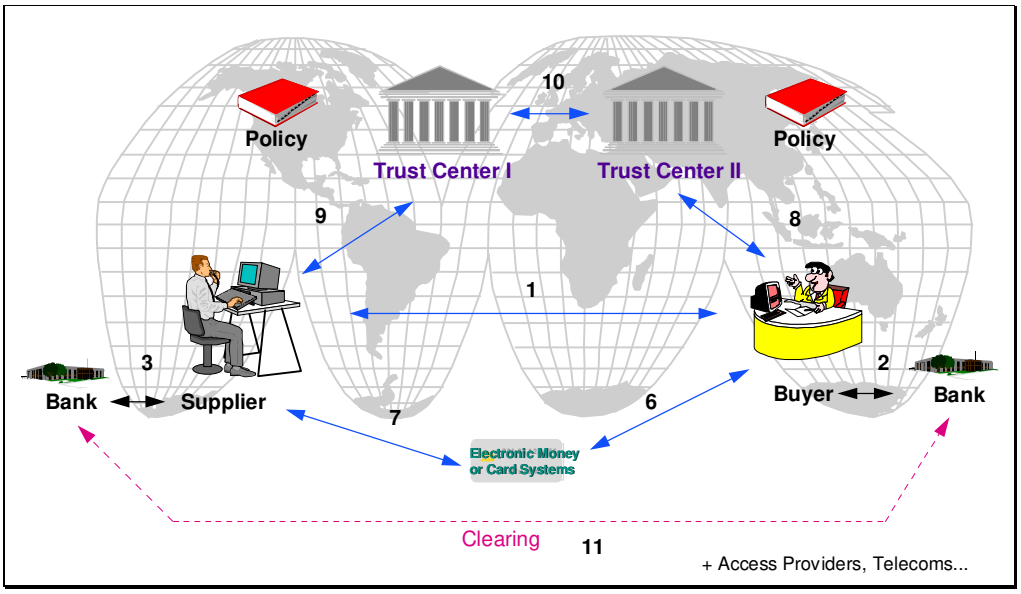

Fig. 1: Possible contractual relations

1. Underlying[53] transaction (sales) = contract between seller and buyer
2. Contract between buyer and buyer's bank
3. Contract between supplier and supplier's bank
6. Contract between „Electronic Money Provider" / Credit Card Organisation and buyer
7. Contract between „Electronic Money Provider" / Credit Card Organisation and supplier
8. Contract between buyer and Trusted Third Party (TTP)
9. Contract between supplier and Trusted Third Party (TTP)
10. Contract between TTP/PKI's
11. Contract between the Banks

[53] Underlying means the base contract the parties want to conclude

The disadvantages of such a situation are obvious:
- Too many contracts,
- Too many different legal systems,
- Uncertainties about the applicable law,
- Deterrent effect on suppliers and customers .

In this list contracts between access providers, telecoms and others with the parties listed are not even shown. However, the situation looks very complicated, and it must be the goal of a project like SEMPER to reduce this contractual web.

Therefore we have two main goals to accomplish:
1. Show the way of how to simplify the contractual relations
2. Show the topics which need to be addressed in the process of harmonising the different legal frameworks

The focus in SEMPER must be on 1, as we are aiming at setting up an electronic marketplace taking into consideration the current legal situation. In a longer term, topic 2 must be addressed and we will use the SEMPER trials to show the need for action related to the legal topics addressed.

5.1.2 Recommended Structure

The goals of SEMPER and the situation described in 1.2 lead to a proposal of a „SEMPER Electronic Commerce Agreement“ which will regulate the most important issues in an Electronic Marketplace. A proposed structure could look like this:
1. Underlying transaction (sales) = contract between seller and buyer
2. Contract between buyers and Buyers' Bank
3. Contract between supplier and suppliers' Bank
4. Contract between supplier and SEMPER
5. Contract between buyer and SEMPER
6. Contract between „Electronic Money Provider“ / Credit Card Organisation and Buyer
7. Contract between „Electronic Money Provider“ / Credit Card Organisation and Supplier
10. Contract between TTP/PKI's
11. Contract between the banks
12. Contract between SEMPER and TTP/PKI's
13. Contract between SEMPER and „Electronic Money Provider“

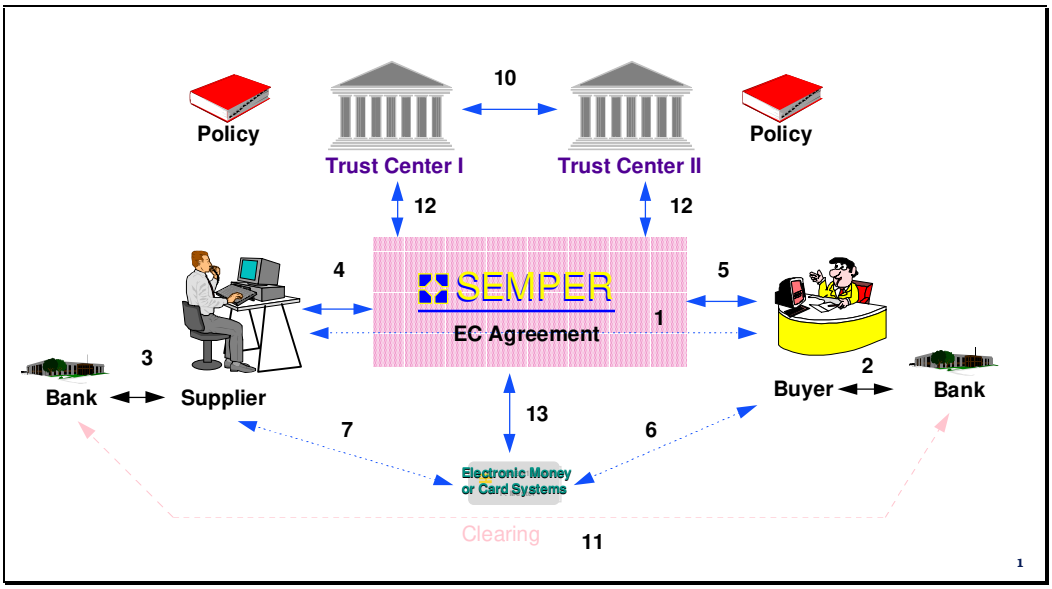

Fig. 2: SEMPER EC Agreement

This structure already looks less complicated, although it must be mentioned that the peremptory rules still apply and that the applicable law might be in question with some countries which will have strong rules on distance selling (see Chapter 5.2.2.2) or in other areas like hire-purchase.

This picture implies that SEMPER is a legal entity. This could be one way of addressing of the legal problems which we encountered. In general, there are different solutions to the question how the SEMPER rules become applicable and between whom. Currently, the SEMPER agreement should be considered as a multilateral agreement between the players in a SEMPER scenario, primarily covering the needs of buyer and supplier. How this set of SEMPER rules will be accepted and by whom will be part of the trial phase. This is not merely a legal question, it depends heavily on the acceptance of the market players how they wish to set their rules. Also the contents and extent of these rules are still open.

5.1.3 Legal Nature of a Typical SEMPER Transaction

SEMPER is an open architecture and does not restrict the parties to a specific legal transaction. However only the following transactions seem to be possible due to existing restrictions and the nature of the transaction:

- Sale of goods (non property) (first priority)
- Rent (second priority)
- Hire-purchase (personal loans, third priority)

Other transactions were not considered due to strong requirements on formalities. For a detailed study on contracts which can be concluded using electronic means please refer to [TEDIS II B 5]. Although the main goal of SEMPER will be to show the feasibility of an electronic market, we will refrain from discussing legal transactions which seem to have no impact on an electronic market in the near future, like the sale of property.

Besides the rules and regulation which directly affect the parties, there are also others which beforehand do not seem to influence an electronic market. Therefore, we have to consider the following rules and regulations:

- Trade law
- Rules on advertising
- Rules on unfair competition
- Data privacy
- Crypto regulations
- Rules on Trusted Third Parties
- Criminal code
- Frameworks for EDI (EC, UN)
- Tax regulations

5.2 Sales and Trade Practices

5.2.1 Introduction

In this section, we will analyse the formation and governance of a transaction involving the sale of goods or services; for each of these elements we have described their legal nature and looked for the equivalence in an electronic commerce environment. Based on this analysis we provide guidelines for the design of the SEMPER architecture and, where felt to be necessary, formulated recommendations for a general legal framework which would facilitate electronic commerce. This legal framework will be adapted to suit the needs of SEMPER, e.g. we will describe a generic „Subscriber Agreement“ which should be used to facilitate the legal situation between the parties. This agreement also contains the issues which should be addressed when harmonising national laws. Although we will not be able to cover all of the issues raised within this agreement, we should at least be able to define a common structure.

The analysis is made under different European laws. The policy recommendations should be applicable to trade throughout the EU and the G7 countries. It should be noted that the legal analysis does not only apply to the relationship between a registered retailer and an individual consumer. This might also include business to business transactions and transactions between individuals.

In a sale, we differentiate between the following actions [see UN Sale]:[54]

- Formation, offer and transmission of offer
- Negotiation
- Acceptance of an offer
- Withdrawal of offer and acceptance
- Conclusion of the contract (time)
- Settlement (delivery and payment)
- Conformity of goods
- Remedies for breach by buyer and seller
- Passing of risk

[54] For an overview see United Nations: Contracts for the Sale of Goods and Thesaurus by UNCITRAL, Sept. 19, 1995. [UN 95]

- Damages
- Technical measures (Technical Annex, see 5.6.4)
  In addition:
- Auditing / Archiving
  The following sections give an overview over some multinational regulations on sale.

5.2.2 International Regulations

5.2.2.1 Contracts for the International Sale of goods

We have already mentioned [UN Sale] which actually represents one major source of information to define a SEMPER Agreement. In this document, we will focus on business to private customer transactions, which is not the scope of application of [UN Sale]. However, for the detailed agreement which should be done in phase II (during and after the trials) of SEMPER, [UN Sale] must be used as a source for specific regulations.

5.2.2.2 Regulations on Distance Selling

The regulation of "distance selling" varies throughout Europe. The Council of Ministers recently reached a common position on a proposed Directive to harmonise national rules in this respect, but the Directive will probably have limited effect. This is because, like the Directive on misleading advertising, the distance selling Directive invites Member States to maintain or enact more restrictive measures if they wish to do so. The current framework of often divergent rules and regulations at the national level is therefore likely to remain intact. This is especially troubling for the potential development of electronic commerce, in which all transactions in effect constitute "sales at a distance".

National laws vary in two fundamental respects: (1) the degree to which companies may engage in unsolicited communications; and (2) the conditions that must be met in order to ensure the enforceability of agreements, especially with consumers, that are effected at a distance. These laws were originally enacted with direct mail and telephone solicitation in mind. Their application to new technologies, such as on-line services and interactive television is unclear.

With regard to unsolicited communications, it is strongly argued that this does not relate to electronic commerce over the Internet. No contacts are established unless the consumer deliberately chooses to visit a particular Web site.

In case Member States' laws on unsolicited communications seek to extend to Internet, it is useful to be aware of these domestic regimes. Germany, Luxembourg, and Denmark are among the countries in Europe that flatly prohibit cold calls. In Germany, the courts have invoked their broad powers under the "Gesetz gegen den unlauteren Wettbewerb" (UWG) to prohibit unsolicited telephone calls as a violation of public morals. The German courts have reinforced this jurisprudence by finding that direct mail advertisements to objecting consumers constitute a violation of their right of privacy. The German Supreme Court recently extended this ruling to unsolicited advertisements conveyed by electronic mail, and unsolicited computerised messages are similarly restricted in the Netherlands.

France, Belgium, and the UK have taken a more liberal approach to distance selling. Unsolicited commercial communications are permitted in these jurisdictions, but even then, complex and often inconsistent rules must be observed to ensure the enforceability of resulting sales agreements. In France, for example, an offer of sale by telematics, video transmission, or mail requires the disclosure "in writing" of a litany of information, including a description of the goods, their price, the identity of the company making the offer and disclosure of the consumer's right to return the goods within a seven day cooling-off period. While the law is ambiguous, it appears that 'written' documentation must be provided in 'hard' copy form and that setting forth this information on a screen display is not sufficient.

In addition, a recently enacted consumer code in France provides that consumers are bound by telephone sales only after they have returned a signed notice of confirmation that the seller must furnish. Legal commentators have expressed the view that this requirement applies to sales on Minitel, the country's principal on-line service, as well. If that commentary is correct, the paperwork requirements of the code presumably apply to transactions on other commercial on-line services as well as interactive television.

In the UK, distance sales are regulated principally by a voluntary code of conduct. A separate code of conduct applies to telemarketing. In both cases, however, the voluntary codes are supplemented by mandatory regulations. Sales resulting from unsolicited telephone contact are enforceable only if the consumer is provided with a confirmation notice and returns it. The application of these provisions to new technology services is unclear.

The Dutch distance selling regime also relies heavily on self-regulation, but the accepted rules of practice are relatively strict. Among other provisions, Dutch rules prohibit sellers from requesting more than 50% of the purchase price in advance of a sale. In Sweden, sellers engaged in solicitation by telephone must provide the consumer with a written confirmation of the transaction within three days. As in France, the seller must notify the consumer of his legal rights, including a standardised form for cancellation of the order.

In Switzerland there is also a „cooling off" period of five days for hire-purchase contracts, no special restrictions on distance selling contracts.

5.2.2.3 Seasonal sales

Many EC countries regulate the periods during which merchants may organise seasonal clearance sales, but the period differ from country to country. In Germany, seasonal clearance sales may be organised only for a period of 12 working days at the end of January and July. In Belgium, the periods for permissible sales run from January 3 to January 31 and from July 1 to July 31, while in France, the permissible starting dates are fixed at the local level and the sales duration may not exceed two months. In Luxembourg, seasonal clearance sales may be organised for a maximum of one month, but the exact starting and closing dates are set each year by Ministerial Decree. The Netherlands (in 1984) Austria (in 1992) and Switzerland (1994) eliminated any time restrictions on seasonal clearance sales, but in Austria the announcement of such sales requires the prior authorisation of the regional administrative authorities.

Divergent national practices of this kind may well make it impossible to offer seasonal sales in electronic commerce. In effect, companies mounting pan-European seasonal sales campaigns must consider inconsistent national rules in the aggregate. Such companies are placed at a significant competitive disadvantage as compared to companies mounting individual campaigns in traditional commerce in each country. Yet, it is difficult to see how consumers are benefited by the application of archaic rules that discourage innovative companies from using the new media and make it impossible for them to offer lower prices for products that consumers want to purchase in the convenience of their homes.

Currently there should be a recommendation not to advertise seasonal sales via SEMPER. This will avoid most of the problems identified. Whether there is a real need to have an equivalent to a seasonal sale in an electronic marketplace must be decided by the main suppliers. We would recommend to this only if there is a real business case.

5.2.3 Offer

5.2.3.1 Legal Status

The offer is a unilateral expression of will, whereby the seller (offeror) indicates to (a) potential buyer(s) (offeree(s)) his intention to enter into an agreement containing the essential terms of such agreement.

An offer is considered as being an offer to enter into an agreement when it is specific, firm and unequivocal as to the subject matter and terms (which must as a minimum include the price) of the proposed agreement. The offer may be directed to one or several specific persons or to the public. How long an offer will keep its binding character depends on the nature of the contract and whether the offer was given in written or oral form. As this will always be a controversial subject, it is recommended to define clear rules in the contract between the parties [TEDIS II B5].

5.2.3.2 Issues in Electronic Commerce

There are no specific requirements as to the form of the offer. Therefore, and provided that the substantial requirements mentioned above are met, an offer posted on a Web page on the Internet will be regarded as an offer in the legal sense. Catalogues are considered as being an offer to the public if they meet the criteria mentioned above, unless it is clearly indicated that items and prices are listed ‘subject to confirmation’ or with similar reservations. The same analysis would apply to a catalogue posted on one or more Web pages. Basically the seller will be responsible for the price and the characteristics indicated and displayed. Contrary to the display in a shop, this should be considered as a considerable risk to the seller. Although a similar risk applies when using a printed catalogue, possible misprints can be identified easily. In addition, there will be the need to clearly identify the currency and measures used.

5.2.3.3 Guidelines for the SEMPER architecture

These and all the following guidelines describe a broad specification of the SEMPER user interface. The SEMPER Agreement will also become part of this interface but will be handled like any other general terms (see 5.2.5).

- All specifications (price, measure, general conditions) must be on display. In addition, they need to be secured to prevent loss of integrity or there has to be a clear confirmation indicating the items ordered and the conditions. This information should be digitally signed by the seller. This also applies in cases where buyers order by phone or by email, sales personnel should be instructed that there might be a greater risk of wrong orders. Although this might be beyond SEMPER, it is important to plan the necessary measures.
- The conditions should be clearly displayed in a separate and trusted window. It is recommended that they can be accessed in a secure manner and that the actual version of the conditions are displayed (time stamping necessary).
- If a supplier does not want to rely on electronic conditions, there should be a notice which instructs the potential client how he or she can access the conditions in paper form.
  - *This applies specifically for **place of venue and applicable law**!*
- All general conditions of sale should be transmitted securely ! They might be applicable in case where SEMPER rules will not be accepted by a specific court. In countries where there are peremptory rules on certain legal transactions, like the requirement to have specific information in an offer, these requirements to be identified.
- Software at both ends should enable the seller and the buyer to retrieve (by allowing the possibility to keep a record or to make print outs) what was on display for which price at a given point in time. The purpose is to be documented for possible later dispute resolution purposes. This requires to store the information securely. It is recommended to store the data using digital signatures to seal the data, although this might not be necessary in every case. It will also be useful in case where tax authorities do not accept documents in electronic form. The applicable rules on archiving need to be considered.
- The display page of the seller should have the capability of containing a number of secured screen qualifiers such as ‘offer valid subject to stock availability’, ‘offer valid until such date’ if the conclusion of an agreement is subject to specific conditions.
- Currency of the prices should be indicated together with a qualifier that exchange rates may fluctuate between the date of purchase and the date the transaction will be charged.
- It is recommended that the user has a trusted environment where the data to be confirmed will be displayed. This User Interface needs to be designed in a way that the goods requested and the conditions are confirmed by the seller. It is recommended that the goods ordered will be checked for validity by the seller and will be sent back and displayed in the secure User Interface (TINGUIN). The use interface is one of the most critical parts of an EC platform.
- The user Interface should clearly indicate when a transaction is to be started, although most of the transactions might be revoked due to peremptory rules.

- The EC platform should be able to generate a log file (eventually producing reliable information using time stampin services or other services of TTP's like a notarial attestation).

5.2.3.4 Recommendations for SEMPER Subscriber Agreement

All open questions need to be addressed in a legal framework. This basically includes the following items:

- Sphere of application
- Applicable Law
- Formation, offer and transmission of offer
- Withdrawal of offer and acceptance
- Negotiation
- Acceptance of an offer
- Conclusion of the contract (Time)

It is obvious that the current legislations are to a certain degree covering the questions raised by an electronic offer. However, there will be a strong need to make clear statements on all of the points mentioned above.

5.2.4 Acceptance and conclusion

5.2.4.1 Legal Status

The agreement comes into existence when the acceptance by the buyer meets the offer made by the seller. There are different theories as to the exact time at which such meetings occur. *This point in time is critical as it determines the moment where the contract is irrevocably agreed between the parties.*

- Under a first approach (the acceptance declared theory), the agreement is formed when the buyer declares its willingness to accept the offer.
  When applied to the Internet, this would mean that the agreement is formed when the buyer enters the relevant data into the Web page dialogue box, before he presses the RETURN key on his key board or clicks on a SEND (or ACCEPT, or equivalent) button on the Web page.
- Under a second approach (the acceptance sent theory), the agreement is formed when the acceptance is sent by the buyer.
  This would mean that an agreement over the Internet is formed when the buyer presses the RETURN key or clicks on the SEND button after having filled in the Web page dialogue box (it does not matter whether the information has actually been transmitted to the recipient; the time of reception is not relevant for the buyer, but of great importance for the seller. Logically, this topic has been handled in all EDI or agreements).
- Under a third approach (the acceptance registered theory), the agreement is formed when the seller receives the notification of the acceptance by the buyer.
  Applied to Internet, this would mean that an agreement is formed when the data of the acceptance message sent by the buyer reaches the seller's server.

- under a fourth approach (the acceptance received or information theory), the agreement is formed when the seller has taken actual knowledge or read the acceptance message that was posted on his server.

Most European laws apply the "acceptance registered" theory, considering that the agreement is formed when the acceptance reaches the seller and when the seller can have taken notice thereof.

5.2.4.2 Issues in electronic commerce

There are no precedents on the application of this theory to electronic agreements, but it is clear that the acceptance declared theory could not work in a virtual environment. From a technical point of view the seller can take notice of the acceptance as soon as it reaches its server. In other words, and practically speaking, only the acceptance registered and the acceptance received theory would be operable in an electronic commerce environment.

5.2.4.3 Guidelines for the design of the SEMPER architecture

- The system should be designed in such a way that their is a clear line of demarcation between the pre-contractual phase (where the buyer is making enquiries about the products and prices) and the point where he irrevocably will have entered into an agreement with the seller (the point of no-return). The buyer should at all times be aware of his place in the process and at any time, prior to reaching the point of no return, be in a position to unscramble from the process. To this end, a trusted dialogue box should be put on the Web page where the buyer has to confirm and reconfirm that it accepts the seller's offer.
- Even though it is not legally required under the acceptance registered and acceptance received theory, for reasons of buyer's convenience and system confidence, the system should be designed in such a way that the buyer receives a screen acknowledgement of the fact that the transactions has been completed successfully. In other words, a message should be sent by the seller whereby it confirms the buyer's acceptance of its initial offer.
- The buyer should receive a signed order form (receipt, acknowledgement of order) by the seller which contains all details of the order.
- If the buyer has a right of cancellation (either offered by the seller or imposed by the law of the seller's country), this must be clearly referenced.
- It must be referenced if there are peremptory rules which apply to the right of cancellation in a specific country.
- All peremptory rules should be displayed.

5.2.4.4 Recommendations for SEMPER Subscriber Agreement

The agreement must contain the rules of how and when the contract is concluded and what rules apply to the withdrawal of an offer or the cancellation of a contract. This should be made within the SEMPER agreement if possible, not within the general conditions of sale. Rules can be taken from existing EDI model contracts or similar agreements.

There are differences in member state laws relating to the legal status of EDI messages. This situation has been caused by the different interpretations of the rules applying to the value of proof.

In many countries, the evidentiary value of electronic messages is considered inadequate or at least questionable. Although it is possible to proof that the procedures used where at least as trustworthy and accepted as others. The only exceptions are with true formalities.

In order to ease the burden of proof on the existence of contracts concluded over the Internet, Member States should be urged to harmonise and adapt the rules on proof, thus accepting properly secured and controlled electronic records as a means of proof. In this respect, the requirement of a paper document and a hand-written signature should be reviewed. Instead there should be a recommendation to accept equivalent or better procedures like the use of digital signatures using Trusted Third Parties. This will also force the legislative bodies to think about the legal situation on digital signatures.

A Directive formulating minimal functional conditions for harmonisation of the legal validity of electronic documents (and their evidential value) just like paper documents is due.

For SEMPER, this can be handled easily if the parties accept any digitally signed document to have the value of proof needed. If this has been made, there will only be some peremptory rules which will not allow this. Although according to current legal studies the legal acts requiring handwritten form and the use of paper documents are decreasing. This will also touch the area of Digital Signature Legislations.

5.2.5 General Conditions of Sale

5.2.5.1 Legal Status

Commercial companies very often include general conditions in their contracts of sale concerning the quality of the goods, clauses restricting the guarantee on products, delivery times, transfer of ownership and risks, exemption from liability and acts of God, deadlines for complaints, non-conformity, arbitration, etc. Two possibilities exist with regard to any challenge to these general conditions (opposability).

Firstly, the parties are able to take note of the general conditions or did actually do so during the conclusion of the contract without objecting to them. This is the case where the general conditions appear on the front of the offer or counter-offer or where they are printed in legible print on the back with a reference to them on the front. There are many Court decisions which state that the parties are then bound by these general conditions of sale.

A second type of situation exist if - during the conclusion of the contract - one of the parties refers to general conditions but does not send them to the other party or print them on the back of the documents forming the agreement. Two arguments are defendable in this case: either it is considered that this reference means it is for the recipient to ask about the conditions and that he is bound by them unless he objects; or, on the other hand, the view is taken that, in this case (i.e., mere reference to the general conditions) the general conditions do not form part of the contract.

The latter theory has been applied predominantly in recent Court rulings, especially if the parties do not have an on-going business relationship with each other and thus have not been able to familiarise themselves with the other party's general conditions.

5.2.5.2 Issues in Electronic Commerce

In order to guarantee the opposability of the general conditions of sale, the Web page should indicate the existence and place where the general conditions can be consulted. The conditions, must be made available securely.

5.2.5.3 Guidelines for the design of the SEMPER architecture

The system should provide space for containing the general conditions of sale in such a way that the buyer is invited to take notice of them prior to concluding a transaction. The conditions must be made available in a secure manner, see 5.2.3.3 (Offer).

5.2.5.4 Recommendations for SEMPER Subscriber Agreement

The subscriber agreement should explicitly refer to general conditions of sale and should describe how these conditions must be placed. There should be a clear rulebook of how the general conditions of sale and the SEMPER subscriber agreement interact.

5.2.6 Applicable and conflicting Laws

5.2.6.1 General

Applicable law in the Internet is a topic which cannot be solved within a legal study on SEMPER [UN Sales, Art. 7]. We know that there is a large gap between the business expectations and the way how the business transactions can be handled from a legal point of view. Currently, we must be aware that any information posted onto the net will be available in most countries worldwide.[55] The consequences are obvious. It is most possible that there will be at least one country a supplier will infringe at least one law.

The following sections give some examples of conflicts when posting information onto the Internet.

[55] Kuner, Christoph: Internationale Zuständigkeitskonflikte im Internet, Computer und Recht, VIII/96, p. 453f.

5.2.6.2 Examples of Conflicting Laws

Industry and consumers alike suffer from the divergence of national rules on advertising, promotion and sale. Companies acting lawfully under the rules of their own country repeatedly have been punished for inadvert or unavoidable violations of the importing countries' rules, and have incurred significant fines and the obstruction of their multi-country sales efforts. As a result, consumers have been prevented from taking advantage of promotions that were available to their counterparts just across the border.

A few examples illustrate the spill-over effects of conflicting national rules in Europe today. A British broadcaster aired two thirty-second English language advertisements for Mc Donalds hamburgers. The advertisements, which were oriented towards children, were broadcasted from the United Kingdom by satellite throughout Europe. After the advertisements were distributed on a Helsinki cable network, the Finnish authorities imposed substantial fines on the local outlets on the basis that they had violated Finnish law prohibiting advertisements that appeal to children.

Similarly, when a Swiss magazine was distributed in Germany with a German language advertisement for Tampax, the local German distributor was found by the courts to have violated German consumer protection law. Specifically, the German court found that the advertisements violated the "guten Sitten" standard. The fact that the advertisements were lawful in Switzerland was deemed irrelevant. In another case, a Dutch advertising self-regulation board found that an advertisement for L'Oréal skin cream was misleading, and on this basis prohibited its further use in the Netherlands. The advertisement was distributed in much of the rest of Europe.

In another case, a Belgian mail order company operating throughout Europe was compelled by local courts to desist from using sweep-stakes to promote its goods. As a result, the company was forced to create two separate sets of promotional materials, one for use in Belgium and the other for use in the rest of Europe. In yet another case, French authorities prohibited a J&B whisky advertisement for violating a provision of French law requiring disclosure of the origin of the beverage. The French Supreme Court rejected J&B's argument that this requirement discriminated against foreign products and was unnecessary. The J&B advertisements were widely run elsewhere in Europe.

The foregoing examples involve traditional broadcasting and print media. They only faintly illustrate the far more vexing problems that face companies seeking to launch pan-European advertising and promotional campaigns through the new electronic media. The expected accessibility and persuasiveness of on-line networks and interactive television will make it virtually impossible for companies operating in these media to tailor their advertising and promotional campaigns to the rules of individual countries. If electronic commerce is to flourish, it is obvious that some relief must be found.

5.2.6.3 Sale

One of the most controversial legal topics is the question, which law will be applicable for sales contracts. There are several rules and regulations for the sales of goods. In cases where the rules on distance selling apply, there will be peremptory rules which will not allow that the applicable law can be changed to protect the individual customer. This makes it of course difficult to define a legal framework which will be valid throughout Europe. In this section, we will analyse the most important national and supranational rules on sale of goods and will try to identify rules which should be considered as critical for the individual supplier and in which cases he or she should analyse current practices used in today's international sales.

Under most European laws, when the transaction is international, the law governing the transaction will be the law chosen by the parties. To this effect, the Web page could contain a choice of law clause. Practically, the choice of law clause will be imposed by the seller on the buyer rather than being an agreed choice between both parties.

Notwithstanding a given choice of law, in the event a decision of a foreign court requires recognition and execution in a specific country, a decision which would infringe rules of that countries "public order (ordre public)", will not be recognised. To this effect, local countries overriding statutes part of the public order will be applied by these courts irrespective of the applicable law chosen by the parties.

In the absence of choice, the contract concluded over the Internet with a consumer will in principle be governed by the law where the consumer has his normal place of residence. Where the contract is concluded between two persons of the same nature (two businesses or two private consumers), and in the absence of a choice of law clause, the contract will be governed by the law of the party having to deliver the service.

As to the Court competent to hear disputes resulting from the agreement, the Brussels Convention of 1968 will apply if both contracting parties are residing in the EU. In the absence of a choice of jurisdiction, it is the Court where the defendant has his place of residence or the Court of the country where the contract has to be executed which will be competent to hear the dispute.

5.2.6.4 Solutions and Recommendations

5.2.6.4.1 Harmonisation of Legal Framework

The borderless dimensions of electronic commerce make clear that individual Member States are not well positioned to regulate in this area. Steps should be taken to harmonise at a European level the rules governing commercial communications as they apply to electronic commerce. Legislation should embrace the following basic principles:

The impact of any harmonisation effort at the EC level will depend in significant part on the reach of the harmonising legislation. It should address commercial communications in all forms of electronic commerce, including the Internet and commercial on-line services, as well as other interactive services, such as those carried over television. A regime that includes all interactive services should be sufficiently progressive to accommodate innovation without disturbing existing rules governing traditional commerce. Legislation does not need to disturb long-standing rules governing "traditional" commerce.

5.2.6.4.2 Standards of Consumer Protection

Harmonisation should set forth basic standards of consumer protection in electronic commerce that distil and combine the policies of the Member States. A unified set of predictable rules should enable companies seeking to advertise and promote their products to understand and fulfil their obligations. It is true that 'perfect' harmonisation in this respect is not achievable. Member States will be responsible for enforcing the harmonised rules, and it is possible that divergent judicial attitudes will again assert themselves as a complicating factor. Unified rules will nonetheless be helpful in giving companies more precise notice of what is expected of them.

5.2.6.4.3 Balance of Interests

The harmonised rules should recognise that interactive services allow consumers far greater control than one-way media, such as convential television, newspapers and magazines. Thus, consumers can shape, solicit or silence the advertisements and promotions as the consumers' needs dictate. Taking this increased power into account, harmonisation should balance consumers' needs for protection from deceptive practices and companies' need for flexibility to promote their goods and services. In striking this balance, any legislation should guarantee the validity of appropriately-secure electronic signatures and the enforceability of ensuing transactions.

5.2.6.4.4 Uniformity of Standards

Genuine harmonisation will not be achieved if Member States are permitted to adopt and apply widely divergent national rules over and above the harmonised regime. The harmonised standards should therefore be reinforced by provisions that prohibit Member States from maintaining rules that are inconsistent with, or contradictory to, the EC measures. This will help ensure that the rules for commercial communications in electronic commerce are evenly applied and enforced throughout the Community.

5.2.6.4.5 Mutual Recognition

Harmonisation should be supplemented by the adoption of the country of 'origin' and 'mutual recognition' principles. A commercial communication that is lawful in the country from which it is sent must be recognised as lawful in the country in which it is received. These principles, which are already embraced in the EC Broadcasting and Satellite and Cable Directives, have great practical advantages. Mutual recognition is desirable because, even under a harmonised regime, Member States' interpretation and enforcement policy are likely to vary from one jurisdiction to the next. Mutual recognition will make it unnecessary to consider complex "conflict of law" issues presented by commercial communications that are uploaded in one jurisdiction, transmitted across multiple borders, and downloaded in several other jurisdictions. The country of origin and mutual recognition principles will also preserve an important role for Member States, while ensuring that differences in national approach do not create roadblocks to pan-European commerce.

5.2.6.5 The Role of SEMPER

Currently there are two tendencies to address the above mentionded issues:
a) use the applicable law of the entity which runs the server,
b) use the applicable law of location where offer was intended to be placed.
There are court decisions which point into both directions.[56]

Although SEMPER is designed for the European market, we must be aware of this fact and should design the SEMPER rules in a way which will allow for maximum protection of the supplier in the first phase (because he/she must be convinced to use the technology and thus needs to limit the risk). It is strongly recommended that the suppliers will at least make a disclaimer that their offers are not valid in explicitly specified countries and what law will be applicable. There will still be a danger of a country to misuse the law to impede foreign activities in their local market.

This is the most critical issue concerning the setting up of EC platforms.

There might be a solution using the „mutual recognition“ principle (see 5.2.6.4.5) or establishing „older“ forms of protection like closed user groups. From a technical point of view, we should evaluate the possibility of creating closed user groups, this would solve most of the legal problems we currently have, although this might not be very popular from a Electronic Commerce point of viewIt might be helpful in countries where customer and supplier could risk to infringe local laws and which could lead to high risk situations.

The user terms and conditions should contain a clause indicating which law will apply. This includes also other rules with respect to the SEMPER architecture, especially upcoming rules like Digital Signature legislations, although it might be easier to define these rules independent of any evolving law.

5.2.7 Advertising

5.2.7.1 Misleading Advertising

Web pages contain product promotional material with cross-reference to advertising pages. All Member States prohibit ‘misleading’ advertising in one form of another. An EC Directive adopted in 1984 (Directive 84/450/EEC concerning misleading advertising) sought to harmonise national rules in this area but the Directive has been largely ineffective, both because it did little to specify the precise rules that should apply and because it explicitly preserved the right of Member States to enact more restrictive measures. National legislators have responded accordingly, affirming traditional rules and embracing new ones that vary widely in their criteria for determining whether advertising misleads.

Although the following sections will not directly have an influence on the SEMPER architecture, the importance for a service provider or supplier can not be underestimated.

[56] See Kuner, 456.

5.2.7.2 Comparative Advertising

National rules on comparative advertising span a range of extremes. Italy, Belgium and Luxembourg flatly prohibit comparative advertisements, irrespective of their truthfulness. France, the UK, Spain, Portugal, the Netherlands, and the Scandinavian countries are generally permissive in the comparisons they allow. Germany and Greece also allow comparative claims, but only under very limited circumstances. It should be noted that there is a proposal for a European Parliament and Council Directive concerning comparative advertising (Com(91)147 final 13).

5.2.7.3 Other Advertising Restrictions (language requirements, indication of prices, advertising towards children)

Divergent national rules and practices are not limited to misleading and comparative claims. They extend also to other aspects of advertising, such as the language in which advertisements are presented and the currency in which prices are declared. France, for example, requires that advertisements be stated in the French language alone; advertisements in any other language are a prohibited misdemeanour. Belgium and the Netherlands require that prices be declared in their respective currencies, even though consumers can readily convert the prices declared by consulting currency exchange tables available in most newspapers. Other countries, such as Germany and the UK, impose no such restrictions.

The global reach of advertisements on Web pages means that merchants should be able to choose the language and currency that meets the needs of their customers.

Advertising regulation also varies widely by product type. The rules governing advertisements for toys and other products for use or consumption by children are illustrative. In France, for example, advertisements may not lawfully feature children unless they are accompanied by a parent. French law also prohibits celebrities from advertising toys for children, and it further forbids children, even when accompanied by a parent, from naming a specific toy brand or wearing colours associated with the brand in an advertisement.

In Denmark, advertisements directed at children are forbidden to feature characters from children's television shows. Sweden goes even further by completely banning television spots aimed at children under the age of 12. Similarly, Greece recently enacted a law banning the television advertisements of any toy between the hours of 7:00 a.m. and 10:00 p.m.

In the Netherlands, advertisements for confectionery may not be directed at children, may not be aired before 8:00 p.m., and may not feature children under the age of 14. In addition, such advertisements must display a toothbrush, either at the bottom of the screen during the entire spot, or as the exclusive depiction on the entire screen during the last one and a half seconds. Germany prohibits advertisements that feature children discussing a product's benefits and further prohibits any "direct" appeals to children in advertising.

5.3 Copyright

Support for the maintenance and extension of strong intellectual property protection is critically important to the development of the Information Society. The current levels of protection for intellectual property rights must be transposed to the new technologies. These issues are discussed in the EC Green Paper on Copyright and Related Rights in the Information Society.

5.3.1 Transmission Rights

All digital transmissions, including transmissions from private PCs to networks or other private users, should be protected by copyright and related rights. There is currently some uncertainty as to the precise scope of such protection in certain jurisdictions.

5.3.2 Private Copying and other Exceptions

It is easier to copy digital than analogue works and far more difficult to detect such copying. Perfect digital copies can be instantaneously transmitted globally without the rightholder's knowledge or consent.

As digital transmissions and reproduction from networks become a normal form of the commercial exploitation of works, we believe that existing exceptions to the rightholder's exclusive rights, such as private copying and inter-library 'loans', should be discussed in the new digital environment.

5.3.3 Technical Protection

Copy protection devices are playing an increasingly important role in enabling rightholders to control, monitor and receive payment for use of their works. The production, importation and use of software and hardware devices to circumvent copy protection devices should be made a criminal offence.

5.3.4 Freedom of Contract and Collective Licensing

Licensing works in the Information Society should be developed on the basis of open negotiations and freedom of contract. Rightholders and users should be free to enter into contractual arrangements regarding the use of works and the appropriate remuneration. Any arrangements for collective licensing of digital works should be purely voluntary.

5.4 Data Privacy

5.4.1 The Privacy of a Sales Transaction

The flows of data will rise dramatically in the information society of the next century. The expected use of smart cards and other small but powerful memory hardware in various applications raises major challenges to existing data protection laws and to our fundamental ideas about privacy.

To give just one example: the chip on smart cards can be programmed to create records of consumers in order to build profiles of customers' preferences and habits. Technologies are available to ensure anonymity (so-called 'Privacy-enhancing technologies' or PETs as discussed further). Privacy concerns can be met by requiring that the purchases are matched via a number so that the identity of the purchaser remains unknown to the retailer since the name connected to the number is held by the issuer in confidence or using real anonymity techniques where the contractual details concerning the person are hidden completely.

Two basic underlying policy objectives can be identified:
(i) the right to remain anonymous where it is not necessary for the purpose of the transaction that the other party knows who one is; and
(ii) the right to control the uses others make of personal information they hold about one (i.e. to consent to certain uses and to veto certain others).

As discussed below, the Commission has spoken out in favour of anonymous payment systems whereby, as is the case with cash payments today, an individual can pay for transactions without leaving any trace of his identity and the nature of his purchase.[57]

5.4.2 EU Data Protection Law

Data protection laws in most countries have usually concentrated their efforts upon a number of procedural principles about the terms on which personal data of certain sorts may be collected and handled. Enforcement efforts have focused on registration of databases. The laws have to a certain extent failed to reassure those concerned about abuses. Many of the principles contained in data protection laws are not adapted to the new technological applications which smart cards will bring about.

The 1995 European Directive lays down common rules to be observed by those who collect, hold or transmit personal data. Its substantive provisions can be summarised as being, on the one hand, a collection of obligations on those who collect and process personal data and, on the other hand, a set of rights for the individuals who are the subjects of the data.
Undoubtedly, the Directive will give data subjects greater control over the disclosure of their personal information, and of how consumers' names and the information attached to them is likely to be used. In the context of electronic payment systems and instruments, the following provisions of the Directive need to be emphasised. However, the Directive fails to specify in detail exactly how some of these principles should be implemented:

- Personal data can only be collected for specified, explicit and legitimate purposes and must not be used in a way incompatible with those purposes (the 'Purpose Principle');

[57] Draft Working Document on a Commission Policy Concerning New Means of Payment, XV/111/96.

- Personal data may be processed only if one of the grounds of Article 7 are satisfied; the first of these grounds is the requirement that the data subject give his prior consent (the 'Legitimacy Principle');
- In order to enable a data subject to give his full and free consent to the processing of his personal data, it is important that he is fully informed about the processing operation. This is recognised by Articles 10 and 11 of the Directive which provide that the data subject has a right to be informed about the identity of the data controller, the purposes of the processing and, where necessary, to guarantee fair processing, any further information such as the recipients of the data, etc. This 'Privacy Transparency' provision is particularly important in cases where a customer wishes to allow a full tracing of his electronic payments, for instance to check expenses or errors;
- Regarding 'Security', Article 17 of the Directive provides that the controller of the processing must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised alteration, disclosure or access. Encryption might be one of these measures;
- With regard to 'Responsibility of the controller', the controller is responsible for any damage persons may have suffered as a result of unlawful processing. The data subject has a right to redress and to receive compensation;
- For processing which takes place in several Member States, the Directive lays down the principle that the law of the Member State where a data controller is established, applies. A company established in one of the Member States only needs to observe the data protection law of that Member State for its processing activities in 15 different national markets. For cases where data are transferred to non-EU countries, the basic rule is that the non-EU country receiving the data should ensure an adequate level of protection;

Member States have to transpose the principles of the Directive into their national laws by October 1998. They are required to have independent supervisory authorities to provide advice and monitor data processing on their territory. These authorities will have significant powers of investigation and intervention, as well as the power to involve judicial authorities where rules have been breached. The supervisory authority also has an important role in hearing complaints from the individuals who consider that their rights have been infringed.

5.5 Cryptography related Laws

5.5.1 Background

Many of today's governments restrict the use of cryptography for encryption purposes. This restrictions are based on the Trade of Arms regulations (arms embargo), nowadays ruled by the so called „New Forum" (ex Cocom). The trade of cryptographic devices was always restricted, but with the implementation of strong cryptography in software, controls become a critical factor.

Data can be encrypted for security reasons. In principle, this might solve most of the problems about privacy. However, governments around the world have made a variety of efforts to control the use of encryption by private individuals and companies. The extent to which encryption systems will provide security for the privacy of personal data is therefore going to be determined partly by whether and how governments choose in future to regulate the use of strong cryptography.

Many government security and policing bodies regard the private use of strong cryptography with great disfavour. The argument has been that terrorists, enemy states, drug traffickers and others might use strong cryptography. In order to ensure that government code breakers are always capable of cracking the available codes, everyone should use a system which permits this. In fact, what some governments fear is a scenario of 'too much privacy'.

Whatever the national security arguments, there is no point in trying to prohibit private individuals and companies from having access to strong cryptography.

5.5.2 Digital Signature Regulations

For a basic overview of current regulations see TEDIS II B5 and FAST Task 1.2.

The variability among national regimes applies not only to requirements for written confirmation of sales agreements negotiated at a distance, but also to the most basic criteria governing their validity. The status of digital signatures is illustrative. Most, if not all, Member States require the consumer's handwritten signature for the perfection of a contract (not as a peremptory rule, but more in practical guided by the procedural laws). While such a requirement is understandable in conventional transactions, it makes little sense in the context of interactive services, where the consumer manifests his consent by clicking a mouse or remote control device after consulting the relevant information on screen.

The new services are convenient for consumers primarily because they permit almost instantaneous transactions without burdensome administrative procedures or ordering forms. The requirement for conventional signatures would undermine this advantage, and do so unnecessarily. The giving of an 'digital signature' requires no less of an affirmative act by the consumer than does the giving of a conventional signature, and the authenticity of the consumer's authorisation in digital transactions can be validated by other means. There is thus no policy justification for applying traditional rules to the new paperless media.

Under current law, however, the validity of digital signatures varies from one country to the next, and depends significantly on the facts of the particular case. In the UK, for example, one commentator has argued that digital signatures should be recognised valid because they fulfil the purpose of authenticating the message more conveniently than hand-written signatures. The commentator noted, however, that no UK authorities apparently exist on this point. In Switzerland, digital signatures are not sufficient where the law requires a written contract. Similarly, in Germany courts are likely to require the vendor to provide the customer with the terms of any agreement in writing before the electronic agreement is considered valid. In Spain, although an electronic agreement is probably valid, its enforceability is questionable in the absence of a written agreement. The same is true in France. In Portugal, an digital signature without a prior "paper signature" would probably not be considered valid. The validity of such signatures is also doubtful in Belgium.

Disparate national rules on signature and written documentation requirements cast a cloud over "distance sales" in electronic commerce. There is no doubt that buyers and sellers must be protected from the imposition of obligations that they do not intend to assume, but these protections should run consistently throughout Europe and should reflect the technological advances in media that are now available. At the very least, digital signatures should be valid throughout the EC, and agreements consummated through them should be enforceable on the basis of the "best evidence" principle, embracing any persuasive evidence of the party's intent, whether or not contained in electronic form.

5.5.3 Trusted Third Parties (TTP)

Electronic commerce will only become reality on a large scale if the players (industry, public authority and the general public) are as comfortable and confident with the concept of electronic communication and commerce as they currently are with paper based systems. In the paper world for instance, a third party (notary) is used to 'authenticate' legal transactions.

In the electronic commerce environment, there will be a need for a legally recognised entity which will provide services to support authentication, confidentiality, data integrity, non-repudiation, accountability and audit capability. The technical means (in the form of encryption techniques and digital signatures) are today available to achieve these objectives.

That is where the notion of TTP comes in. A TTP can be defined as an entity which one or more entities use as a trusted intermediary in a communication or verification process or as a trusted information service.

TTPs will need to perform a number of functions, such as registration, certification, certificate revocation, key directory and optionally other functions such as key generation or dispute clarification.

The question remains whether such TTP will indeed be trusted, either by consumers, or by companies or indeed by government. The private sector, especially the banks in Germany have made clear that they will not accept any intervention by the government.
.
Potential players to become TTP include payment schemes, notaries, Chambers of Commerce, national governments, professional bodies, and trade associations. Eventually, there will be a need for inter-operation between TTPs. In our opinion, TTP should be independent of government. It is recognised, however, that in some instances an accreditation process could be useful to enable potential users to have confidence in the reliability of TTPs whose services they plan to use.

A possible blueprint of an electronic commerce architecture is one in which a payment scheme will issue an acquirer's certificate (certifying the bank), the acquirer will issue a merchant's certificate (certifying the merchant) and the issuer will give the cardholder with a trusted means of verifying both certificates. The payment scheme thus performs the role of a TTP.

The Commission is currently discussing a draft "proposal for a Council Decision concerning the establishment of Europe-wide Trust Services". The proposal calls for the establishment of Trust Services for business and the general public. Unfortunately, it has been impossible to obtain more details on this draft proposal.

The legal situation concerning Trusted Third Parties in Europe is part of the TTP discussion, currently held e.g. in Germany where there is a draft for a Digital Signature Law. In the US, several states have decided to regulate the use of Digital Signatures, although there are big differences between these legislations or proposals.

The contents of these laws depends mainly on the proposed legal state of the digital signature. It must be decided whether the acceptance of the Digital Signature as an equivalent means of authentication will be written down in a special law or whether the current rules will be modified, as this would be the case in Switzerland.

5.5.4 SEMPER Recommendations

5.5.4.1 Regulating strong cryptography

The capacity of governments to restrict individuals' and companies' access to strong public key cryptography, and to compel them to use some form of escrow system, is now very limited. Now that many systems are widely and in some cases almost freely available, prohibition would be ineffective. Strong cryptography will be an appropriate measure to respect privacy. At the same time, it is acknowledged that there will always be extraordinary situations, for which the police and security services can be given specific authority to override individuals and companies' rights of privacy that should otherwise be inviolate. This should be done using the well known procedures (search warrants).

5.5.4.2 Privacy-enhancing technologies (PETs)

There are several means by which the flow of identifiable data can be capped. Devising smart card or other tamper resistant hardware systems to incorporate protection of privacy is not difficult. The public policy question is whether issuers of smart card systems or other hardware can be persuaded to use these privacy-enhancing technologies. Laws have done little to promote the use of technologies that respect anonymity. There is a strong case for the next phase of regulation to regulate in this area.

As discussed above, cryptographic features can be provided on smart cards and the related central database systems and reader devices, which would go some way towards protecting the cardholder against intrusions into his or her personal privacy. Public policy should promote their use. Meanwhile, industry could agree on some codes of practice that encourage such systems. The 1995 European Directive encourages the development of such codes.

Furthermore, a trusted third party could keep a master key, linking the digital pseudonym with the real identity of the cardholder. This third party could be called upon under certain conditions, when it is essential to acquire the user's identity.

A Commission's Working Document on New Means of Payment refers to the technology by which an identity protector is built into the system. The protector generates pseudo identities. Each pseudo identity is unique to a particular individual and so cannot be used by or related to another individual. In order to protect the financial institution's or service provider's interests, the user's real identity can be exposed in specific circumstances, for instance in cases of fraud or non-payment.

Meanwhile, there is little point in rushing to legislate before the technologies are well understood among data users and before the willingness of business to use them without heavy pressure is known. Practically, governments could encourage standard setting bodies to adopt and promote standards for privacy-enhancing technologies.

5.6 Recommendations for the Parties in Electronic Commerce

The following recommendations are based on the results of the above studies on current legislation and the resulting legal inconsistencies and problems.

5.6.1 Policy Recommendations for a Regulatory and Legal Framework

The information society has a tremendous potential for stimulating pan-European commerce and strengthening the internal market in Europe. However, this potential will not be realised if divergent national rules on advertising, sales and trade practices, copyright, cryptography, privacy, censorship, a.o. are applied to the Information Society. These divergences put suppliers at a competitive disadvantage relative to other countries. The definition of a regulatory and legal framework is considered an absolute priority as it will create the favourable environment which is needed for new networks and services to develop.

EU policy-makers can make a significant contribution to the emergence of new information technologies by promoting early adoption of flexible rules that facilitate commercial communications in electronic commerce. By harmonising this area of the law and thereby creating a European regulatory framework, policy-makers will promote the emergence of new applications to the benefit of the European economy and its consumers.

Companies' ability freely to promote their goods and services is critically important to the success of the Information Society. As we have shown, inconsistent and contradictory national laws governing advertising and promotion are likely to hinder pan-European and global commerce in goods and services.

Although it is obvious that there should be a harmonisation of European Laws in the near future, we will give recommendations how to set up an Electronic Commerce infrastructure with today's legal restrictions. It should be noted that the points identified in the following alinea should be covered by this future legal framework.

5.6.2 SEMPER

SEMPER currently is a consortium according to the EU rules. As this does not give a legal personality to SEMPER, we will concentrate on a future professional and commercial role that SEMPER might have as a provider of an electronic marketplace. As shown in figure 3, SEMPER should reduce the legal complexity. Therefore, SEMPER should provide a rulebook which covers the main aspects in a sales transaction, as described in (**5.1.2**), which we called „SEMPER Agreement“. Basically, this consists of a set of rules for the buyers and the suppliers (contracts 4 and 5 in Figure 2). We recommend that SEMPER will use its own PKI in a first phase. Contracts between the providers of electronic money depend on the type of electronic money used and cannot be covered here.

In the first phase, the SEMPER agreement must be a multilateral agreement between as many parties as possible. Despite the fact, that there will also be parties participating who have not signed the agreement, this should be encouraged by the consortium.

Technically, buyer and supplier should indicate which set of rules they are willing to offer/accept. This could typically consist of the SEMPER Agreement, but in parallel, general conditions and in addition, special rules for a specific transaction.

Parties who will not sign the SEMPER agreement will have a much less defined legal situation. Which can be accepted for an individual case, but is not in the interest of the promoters of an Electronic marketplace due to juridical insecurities.

The SEMPER Agreement will also form part of a quality label for the SEMPER idea.

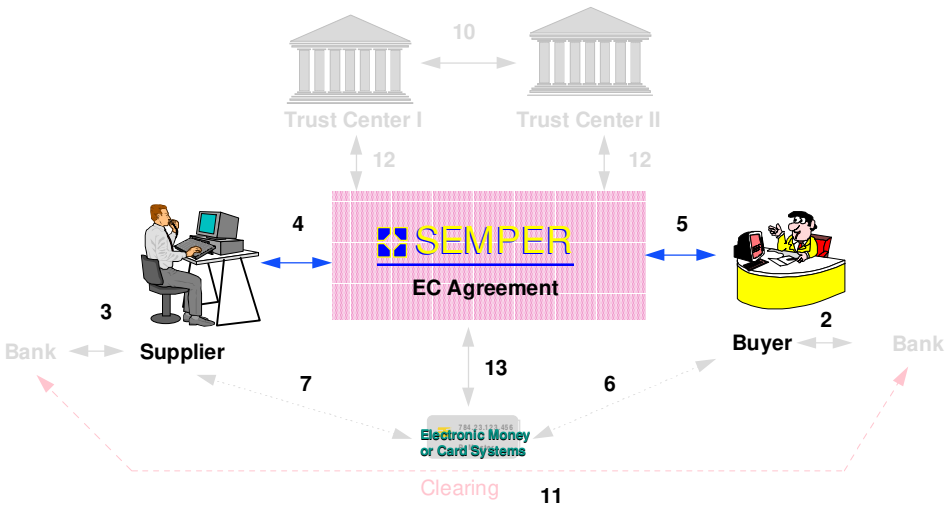

Fig. 3: SEMPER Contracts

The rules between SEMPER and the buyer/supplier (contract 5) should consist of:

- Formation, offer and transmission of offer
- Negotiation
- Acceptance of an offer
- Withdrawal of offer and acceptance
- Conclusion of the contract (Time)

- Settlement (Delivery and Payment)
- Conformity of goods
- Remedies for Breach by buyer and seller
- Passing of Risk
- Damages
- Technical Measures (Technical Annex, see below)
  In addition
- Auditing / Archiving
- Copyright
- Privacy

5.6.3 Next Steps

To build the SEMPER agreement, the following steps will be required:

1. Analyse current multinational agreements on sale
2. Analyse other EC agreements (International, national, sector oriented)
3. Draft SEMPER agreement
4. The suggestions for legislation can then be derived from the SEMPER agreement.

5.6.4 Draft Technical Annex to Legal Framework

There will be a requirement for a technical annex to a legal framework or SEMPER Subscriber Agreement. This will contain details about the security (SEMPER) architecture and describes a guideline how to set up a trustworthy and „state of the art“ system.

Topic	Contents	Description
Acknowledgements	Technical Application Time limits Working hours	Specification of messages to be acknowledged. Technical and/or application acknowledge
Audit trails	Requirements Logging facilities Organisation Information	Overview of the mechanisms used to assure the reconciliation of messages.
Interruption of service and business contingency	Alarm concept Levels Teams Procedures Recovery procedures Business contingency planning Precautions Organisation	What are the precautions to prevent the system going off line? Recovery procedures and emergency scenarios need to be compared and harmonised.
Data privacy	Consent of data subject Right of access and information Technical measures (see „security“) Transfer to third countries	Procedures which have to be followed when handling personal data
Digital signatures	Procedures: Install signature keys Modify signatures/keys Revoke signatures/keys	Description of all relevant key management procedures
Operational requirements	Message standards Equipment (HW) SW / HW versions Services Communication services Communication protocols Codes	Operational framework to make the system operational
Retention, recording and storage	Legal rules Format Media Time of storage requirements System requirements (HW, SW) Third party recording	Contains the legal rules and private arrangements specific to this contract. Describes time and place of archiving and format. Indicates, which HW and SW platforms will be used and what

Topic	Contents	Description
	Use of digital signatures	the requirements for reproducing the archived data are. How digital signatures are used and which data needs to be archived to be able to reproduce the verification procedure and other legal relevant processes.
Security	Classification of data Security „quality“ Integrity Availability Secrecy Mechanisms: Identification / authentication Access control Audit trail Recovery Contingency Planning Functionality Telecom security Encryption TINGUIN security features Base line Security	Define security level and mechanisms used to achieve it. Needs several of the listed mechanisms to grant: • verification of origin • verification of integrity • non repudiation of origin / receipt • confidentiality and to prevent unauthorised access Define base line security environment of end user systems
Test procedures	Scenarios Pilot use Parallel implementation Responsibilities Regular test procedures.	Proper testing is a key factor for the correct integration of services. Description of tests and associatedprocedures (develop-ment and operation).

6 FINAL REMARKS

This document presents findings from the first year of SEMPER. The reader is invited to comment on the document by sending email to:

semper-admins@semper.org

Future updates and new documents will report on the ongoing survey activities, on the evaluation of the basic trial and on the definition of the advanced trial. In such documents also the requirements from the Regionlink companies, which have joined the consortium in July 1996, will be described. Also requirements for multi-party security, like fair exchange and dispute clarification, will be covered. It is also anticipated that more documents covering the legal arrangements will be published.

7 REFERENCES

[ABA 95] ABA (American Bar Association): *Digital Signature Guidelines*, Draft of October 5, 1995. Final version can be ordered from: <http://intermarket.com/ecl/>

[BDR 96] 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.

[Bla 96] Blakeley, Bob: *Architecture for Public-Key Infrastructure*, 1996 <www.osf.org>

[Bra 95] Branscomb, Anne W., Common Law for the Electronic Frontier, Scientific American, (The Computer in the 21st. Century) Special issue, 1995.

[BSA 94] Business Software Alliance, Worldwide Report, 1994. Available from: The Business Software Alliance, 2001 L Street, NW, Suite 400, Washington, DC 20036.

[BSA 96] Business Software Alliance, <http://www.bsa.org/pressrel/polpressrel.html> 4/96.

[CA 96] CyberAtlas, The Internet Research Guide, published by I PRO, last updated 18 July 1996. <http://www.cyberatlas.com/>

[CI 96] CI (Computer Intelligence) Consumer Technology Index, July 1996. <http://www.ci.zd.com/news/ctinet2.html>

[CNN 95] CommerceNet/Nielsen Internet Demographic Survey, 1995, Executive Summary available at: <http://nielsenmedia.com/commercenet/exec_sum.html>

[Den 96] Denning, D., *The future of cryptography:* 1996, Available at <http://www.cosc.georgetown.edu/denning/crypto/Future .html:5>

[EM 95] Elliot, Brendan P. & Miller, Thomas E., in *Informed Predictions about the Personal Information Revolution*, FIND/SVP95. <www.findsvp.com>

[FD/SVP 95] FIND/SVP, HSF Consulting, C+C Data, *American Internet User Survey,* Sept. - Dec. 1995, <www.findsvp.com>

[FOC 96] Focus Online Nutzerbefragung, Will & Partner Marktforschung, Augsburg Burda Medien Forschung/Studienleitung New media, March 1996. Available from: Focus, Arabellastrasse 23, 81925 München.

[FOR 95] Forester Research, *Conducting Business on the Internet*, O'Reilly & Associates, <http://www.ora.com/survey/> 1995.

[Fro 96] Froomkin, A. Michael: *The Essential Role of Trusted Third Parties in Electronic Commerce:* <www.law.miami.edu/~froomkin/articles/trusted1.htm> Version 1.0, May 18, 1996.

[FTR 96] Financial Times Review, *First the Internet: now the Intranet phenomenon,* April 3, 1996.

[GVU 95] GVU (Graphics, Visualization, & Usability Center, a research center affiliated with Georgia Tech's College of Computing)-Fourth WWW User Survey, <http://www.cc.gatech.edu/gvu/user_surveys/survey-10-1995/>

[GVU 96] GVU - Fifth WWW User Survey, April - May 1996, sample size 11,700 (global), <http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996/>

[HKN 96] 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.

[Hor 96] Horning, Richard: *Has Hal Signed a Contract: The Statute of Frauds in Cyberspace,* <www.iway.fr/groupecx/uae/Horning.html>

[IST 96] 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>

[Lei 96] Leiberich, Otto: *Bedeutung und Möglichkeiten der Kryptographie.* Paper, presented at "Sicherheit in Netzwerken", Bad Homburg 1996

[Mar 96] Martorelli, Bill, *High level of anxiety over security measures*, Financial Times Review, April 3 1996.

[MC 96] Millard, Christoper, Carolina, Robert, *Commercial Transactions and the Global Infrastructure: A European Perspective*, in The Marshall Journal of Computer & Information Law, Winter 1996.

[Nie 96] Niehoff, Wilhelm: *Business impact of public key solutions to the German banking sector.* Presentation given at: Public Key Solutions 1996, Zürich-Glattbrugg.

[NOP 95] NOP Internet User Profile Survey, Nov.-Dec. 1995, <http://www.nopres.co.uk/inet/proposal.html

[NWa 96] Network Wizards' *Survey Observations*, July 1996, <http://www.nw.com/zone/WWW/observations.html>

[Nwb 96] Network Wizards, Internet Domain Survey, January 1996. Data available at <http://www.nw.com/zone/WWW/dist-bynum.html>

[PPSW 96] Pfitzmann, Andreas; Pfitzmann, Birgit; Schunter, Matthias; Waidner, Michael (1996): Mobile User Devices and Security Modules: Design for Trustworthiness; IBM Research Report RZ 2784 (#89262) 02/05/96, IBM Research Division, Zürich

[PUE 96] ITAR Personal Use Exemption, Federal Register, Vol. 61, No. 33, US Department of State, Public Notice 2294, 16 Feb. 1996, <http://www.law.miami.edu/~froomkin/personal-use.txt>

[Ree 94] Reed, Chris, *EDI: the Technology of the Financial Services Revolution*, 1994.

[Ros 94] Rossnagel, Alexander et al. (1994): Die Simulationsstudie Rechtspflege. Eine neue Methode zur Technikgestaltung für Telekooperation. Berlin.

[SET 96] SET (Secure Electronic Transaction Specification), Book 1: Business Description, Draft for public comment, February 23, 1996, <http://www.mastercard.com/set/set.htm>

[SH 96] Sparda Hamburg 15 September 1996 <www.sparda-hh.de>

[Som 96] Somogyi, Stephan, *Netting from Anywhere*, Digital Media Perspective, <http://www.198.93.25.10/perspective/960315.html> 15.03.96.

[SRI 95] SRI International, *Exploring the Web Populations's Other Half*, 06/15/1995 <www.future.sri.com/vals/vals-survey.results.html>

[TM 95] Times Mirror Americans On-line Survey, June 1995, (US).

[UN 95] United Nations: Contracts for the Sale of Goods and Thesaurus by UNCITRAL, Sept. 19, 1995.

[Ver 96] Verisign Certification Practice Statement, August 1996, <www.verisign.com>

[Wa 96] Waidner, Michael (1996): *Development of a Secure Electronic Marketplace for Europe*. Proceedings of Esorics '96, Rome, September 1996, also available at <www.semper.org/>

[WCP 95] Weber, Arnd, Carter, Bob; Pfitzmann, Birgit; Schunter, Matthias; Stanford, Chris; Waidner, Michael; (1995): *Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet.* Frankfurt (Project CAFE)

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