A Status Report on the SEMPER Framework for Secure Electronic Commerce

Matthias Schunter
Universität Dortmund
Informatik 6
D-44221 Dortmund, Germany
<schunter@acm.org>

Michael Waidner
IBM Zurich Research Laboratory
Säumerstr. 4
CH-8803 Rueschlikon, Switzerland
<wmi@zurich.ibm.com>

Dale Whinnett
Universität Freiburg
Friedrichstrasse 50
D-79098 Freiburg, Germany
<dalew@iig.uni-freiburg.de>

Abstract

Backed by the European Commission, a consortium of partners from European industry, financial institutions, and academia has embarked on a research project to develop the fundamentals of secure electronic commerce. The goal of the ACTS Project SEMPER (Secure Electronic Marketplace for Europe) is to provide the first open and comprehensive solution for secure commerce over the Internet and other public information networks. SEMPER's flexible open framework is based on a model of electronic commerce which comprehends a business scenario as a sequence of transfers and fair exchanges of "business items" which are payments, data, or credentials.

This is reflected in the framework: The exchange layer provides fair exchange whereas the transfer layer handles transfers of parcels with electronic goods. The commerce layer provides methods for downloading certified commerce services and the necessary trust management. The commerce services implement the terms of business of a seller using the exchange and transfer layer services.

The basic framework described in [4] has been implemented in the Java programming language. It includes the payment systems SET, Chipper, and ecash™. The prototype uses a distinguished user-interface for trustworthy user in- and output which enables to use SEMPER on secure hardware.

A revised version including fair exchanges, anonymous communication, and other third party services is currently being implemented.

Keywords: Electronic Commerce, Framework, SEMPER, Fair Exchange.

1. Introduction

A wide range of businesses are rapidly moving to explore the huge potential of networked information systems, especially with the Internet-based WWW (World-Wide Web). Although the Internet has its roots in academia and is still dominated by free-of-charge information, dramatic changes are expected in the near future.

The goal of the 9-million ECU project, *SEMPER* (Secure Electronic Marketplace for Europe) [5, 6], is to provide the first open and comprehensive solution for secure commerce over the Internet and other public information networks.

The members of the SEMPER consortium are *Commerzbank* (D), *Cryptomathic* (DK), *DigiCash* (NL), *EUROCOM EXPERTISE* (GR), *Europay International* (B), *FOGRA Forschungsgesellschaft Druck* (D), *GMD – German National Research Center for Information Technology* (D), *IBM* (CH, F), *INTRACOM* (GR), *KPN Research* (NL), *Maris* (NL), *Otto-Versand* (D), *r^3 security engineering* (CH), *CNET* (F), *SINTEF* (N), *SSL* (GB), *Stichting Mathematisch Centrum / CWI* (NL), *Universities of Dortmund, Freiburg, and Saarbrücken* (D). Sponsoring partners are *Banksys* (B), *Banque Generale du Luxembourg* (LU), and *Telekurs* (CH). IBM Zurich Research Laboratory provides the technical leadership for the project.

1.1 Roles and Services in the Marketplace

Like in a physical marketplace, the main purpose of an electronic marketplace is to bring potential *sellers* and *buyers* together:

- Sellers *offer* their goods and buyers *order* these goods; together this is a two-party *negotiation*, sometimes ending with an *agreement.*
- Sellers *deliver* their goods and buyers make *payments*; together this is a two-party *(fair) exchange.*
- Buyers or sellers might be dissatisfied with what has happened so far, i.e., several *exception handlers* and *dispute handlers* which may involve an *arbiter* are necessary.

In all these actions, the parties have specific *security requirements,* namely integrity, confidentiality, and availability. Confidentiality includes anonymity, which is often a requirement for browsing catalogues or for low-value purchases. Examples of typical scenarios of electronic commerce are:

- *Mail-order Retailing*: A retailer accepts electronic orders and payments, based on digital or conventional catalogues, and delivers physical goods.
- *On-line Purchase* of Information and Subscriptions: Like mail-order retailing, but with digital, maybe copyright-protected goods that are delivered on-line.

- *Electronic Mall*: An organisation offers services for several service providers, ranging from directory services ("index") over content hosting to billing services.
- *Contract Signing*: Two or more parties exchange signed copies of the same *statement*.

Naturally, an open system for electronic commerce cannot be restricted to these scenarios. It should be easily configurable and extensible to a broad range of different scenarios.

1.2 What is New in SEMPER?

SEMPER is the first project that aims at the *complete* picture of secure electronic commerce, not just on specific pieces (like electronic payments), specific scenarios (like electronic on-line purchases) or specific products and protocols (An overview can be found at <http://www.semper.org/sirene/outside-world/ecommerce.html>).

SEMPER provides an open framework which enables the integration of any protocol and product providing the necessary services. Therefore, applications are not restricted to specific proprietary technology or specific protocols.

Special attention is paid to customer anonymity and privacy. SEMPER develops an integrated anonymity management scheme extending the existing concepts for anonymous communication and credentials.

1.3 Recent Changes

Compared to an earlier description of SEMPER [4], this revision describes recent changes to the architecture such as a new framework for fair exchange as well as new anonymity services. Furthermore, it includes an extensive description of the SEMPER trials.

2. Model for Electronic Commerce

The framework described in this paper is based on a generic model for two-party electronic commerce. This model describes the flow of control as well as actions, and decisions for any commerce service. The main idea of the model for electronic commerce is describing business scenarios in terms of sequences of *transfers* and *exchanges* of data with decisions based on the success of these actions (see Figure 1). This model is similar to the *dialogues* of interactive EDI.

2.1 Atomic Actions: Exchanges

The interactive actions between two players are *transfers* and *exchanges*. In a *transfer*, one party sends a package of business items to one or more other parties. The sending party can define certain security requirements, such as confidentiality, anonymity, or non-repudiation of origin.

A *fair exchange* is a simultaneous exchange of packages of business items among two parties. The parties have the *assurance* that their packages are sent if and only if the peer entity send their package as expected. Either both packages are exchanged or none. If no fairness guarantee is required, we can model such an exchange by two transfers.

Business items which can be exchanged include

- *credentials*, such as access rights,
- *statements*, such as signed documents, certificates, or program and video data, and
- *money,* such as credit-card, cash, or bank transfer payments.

Figure 2 gives an overview of the possible exchanges of these primitive types. Transfers are included as exchanges of "something" for "nothing."

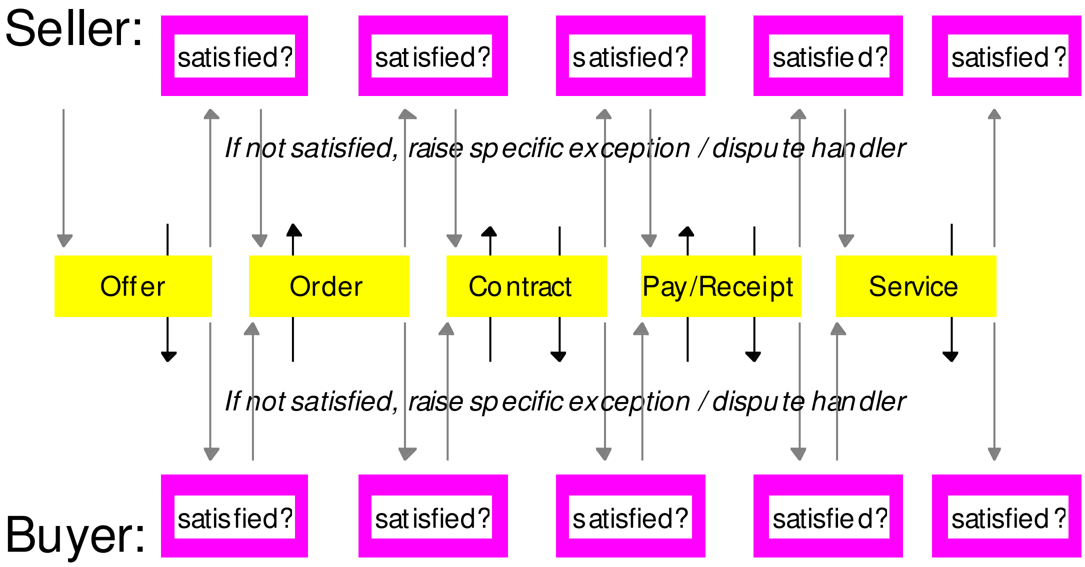


Figure 1 Electronic Commerce is a Sequence of Transfers and Exchanges.
Note that the protocol might enable other sequences as well, e.g., after "Contract" "Payment without Receipt" might also be enabled.

Transfer / Exchange *of* → *for* ↓	Money	Credential	Information
Nothing (i.e., Transfer)	Payment	Certificate transfer etc.	Information transfer
Money	Fair money exchange	Fair payment with receipt	Fair purchase
Credential	*Same as* …	Fair contract signing	Fair conditional access
Information	… *in upper* …	… *right half*	Fair information exchange

Figure 2 Transfers and exchanges of primitive types.

2.2 Electronic Commerce: Sequence of Exchanges

The transfers and exchanges are fixed in our model given the data types and security attributes. Any business scenario is modelled as a sequence of exchanges with user-interaction and local decisions between successive exchanges (see Figure 1).

In the course of an ongoing business, after each transfer or exchange, the parties are either

- *satisfied,* and thus willing to proceed with a certain number of other transfers or exchanges, or
- *dissatisfied*, in which case an *exception* or *dispute* is raised which might end up at a real court if all else fails,

depending on the success of the previous exchange, the items received, and possibly user-input. After each round, a decision as to whether and how to proceed is made.

3. The SEMPER Framework

The SEMPER framework (Figure 3) is structured in layers. The lowest layer deals with low-level security primitives and other *supporting services*, whereas the highest layer deals with commerce issues only:

- The *supporting services* are the usual cryptographic services, communication, archiving of data (keys, non-repudiation tokens, audit trail), setting preferences, access control and the trusted user interface. Furthermore, it provides secure communication services implementing security services such as anonymity which must be guaranteed for multiple atomic actions in one commerce session.
- The *transfer layer* provides services for transferring and grouping business items. This includes transfer-related security services such as non-repudiation of origin.
- The *exchange layer* supports fair exchange of business items, i.e., both participants input some business items and a description of the items expected in exchange. Fairness for exchanges means that the participants send their items if and only if they receive a transfer of the expected items. It implements the fair exchanges of the electronic commerce model such as contract signing, fair purchase, or non-repudiation of receipt.
- The *commerce layer* offers high-level services for business scenarios like "mail-order retailing," "on-line purchase of information," or

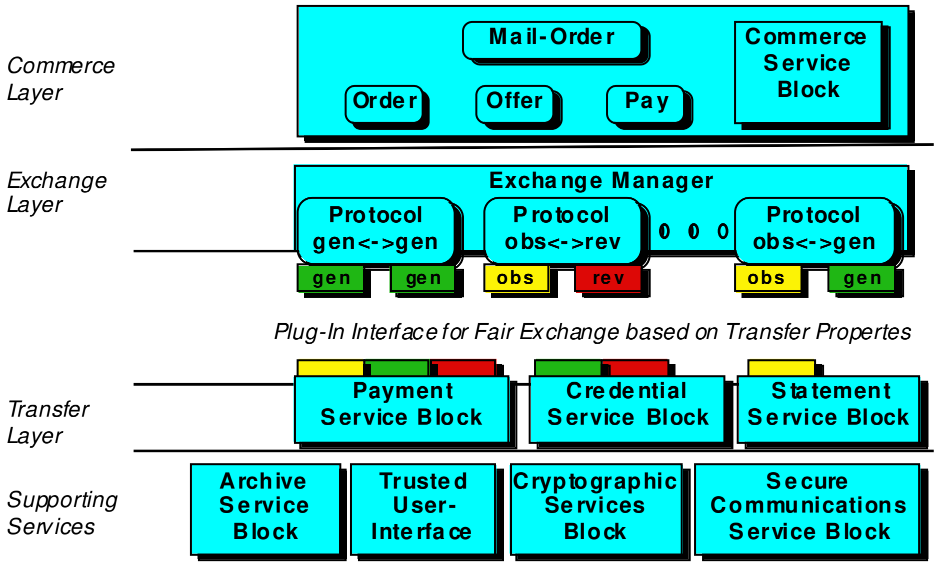


Figure 3 Revised Electronic Commerce Framework of *SEMPER*

“registration with service provider.” It is configurable by downloading new services or extending existing ones.

3.1 Integration into the World-Wide Web

The integration of the Framework into the World-Wide Web is depicted in Figure 4. The integration code does not perform any security services but rather enables integration of SEMPER into different environments. It may use existing protocols such as “cgi” or “http” for this integration.

3.2 Commerce Services

The commerce layer implements the flow of control of our model using the transfer and exchange service for interactions with the peer, and the supporting services for user-interaction and persistent storage. It also performs the trust management and access control necessary for downloading certified commerce services.

The *Commerce Layer* provides services that directly implement protocols of business scenarios, e.g., how specific merchants or types of merchants handle customer registration and offering, ordering, payment, and delivery of goods. It implements the flow of control, i.e., the enabled sequences of exchanges, of the electronic commerce model. A set of client and server commerce services is the electronic equivalent of the “terms of business” for the seller. The commerce layer does not only offer entire commerce protocols, but also building blocks that may be of more general use, in particular services to manage and fill out standardized order forms.

In order to provide overall security, the commerce layer sets up security contexts called “deals” which provide secure communication and signal certain commerce security attributes to all ongoing protocols. An example for a security service signalled by a context is anonymity: Anonymity can not be provided from individual actions but is a service which needs support by all layers starting with anonymous communication provided by the secure communications block on the supporting services layer.

Since one cannot fix the set of services in advance, the commerce layer includes services for secure downloading of services. This allows customers to participate in business scenarios they never encountered before. Since arbitrary terms of business may be implemented in a new commerce service, a downloaded service need not be secure at all. Security of the implemented services can only be ensured by a separate evaluation, e.g., by trusted consumer organizations who issue certificates on fair commerce services. The secure downloading process together with trust management and access control then ensure that

- each merchant fixes the terms of business in advance, in a non-reputable way,
- that each merchant keeps to its own terms during the whole business, and
- that services which have not been evaluated by a trusted authority cannot do any harm.

3.3 Exchange Services

The *Exchange Layer* provides services for fair exchange of business items: Both participants input a busines item to be sent as well as a description of the business item exptected in exchange. The items are exchanged if and only if both expectations can be met by the item input by the peer. The optimistic protocols [1] proposed by *SEMPER* use a third party in case of faults to restore fairness. In the *SEMPER* framework, fair exchange should be independent of the actual items exchanged. This is achieved by defining a minimal set of “exchange-enabling properties” which are required to be implemented by transferable goods in order to guarantee fairness:

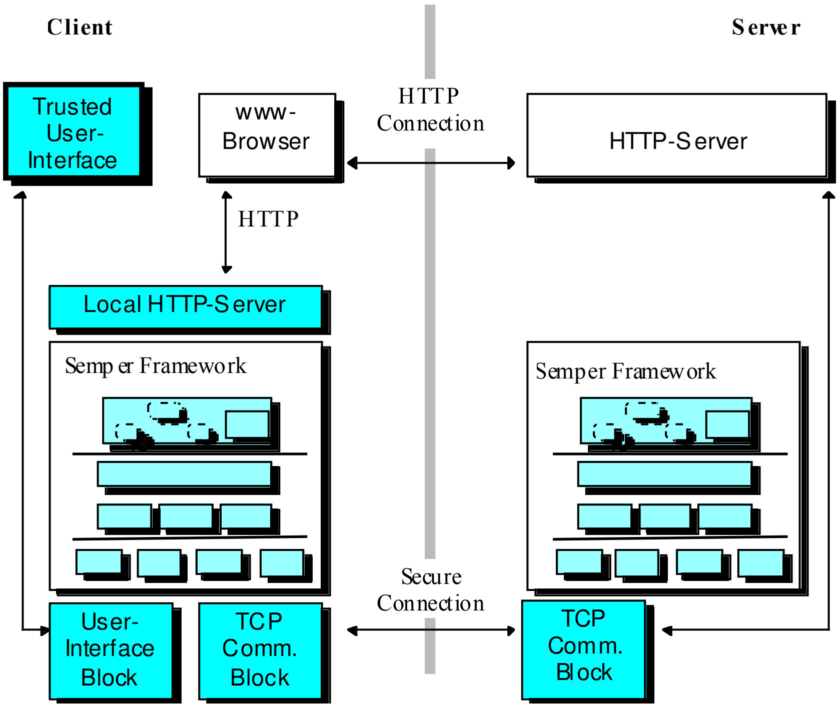


Figure 4 Client- and Server-Side Integration of the Electronic Commerce Framework into the World-Wide Web.

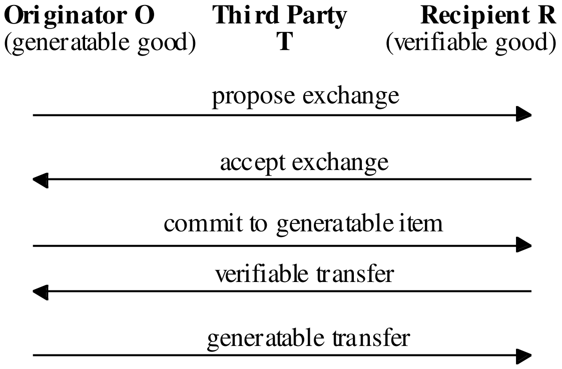


Figure 6: Exchanging Externally Verifiable and Generatable Goods

External Observability: The third party is enable to check whether an item is transferred or not.

Revocability: The third party is able to undo a transfer.

Generatability: The third party is able to redo a transfer.

The exchange manager then negotiates with its peer which of the generic fair exchange protocols shall be used based on the exchange-enabling properties of the two goods to be exchanged. An example for such a protocol is described in Section 4.

3.4 Transfer Service

The *Transfer Layer* provides services for packaging and trading business items. It implements the transfers of the electronic commerce model. The basic items are electronic payments, credentials, and general statements which include digital signatures and data. These business items can be bundled in tree-like packages called *containers*. The security attributes attached to each transfer determine the level of security which is required for the transfer or exchange of the transfered container.

Each type of item is managed by a separate manager which provides unified services integrating existing implementations. The payment manager for example provides three generic services for handling account-based (which includes credit-card payments) and cash-like payments together with the negotiation of the means of payment. Several payment systems of each of these classes can be installed. During a payment, the payer and the payee’s payment manager then automatically negotiate which payment system shall be used based on the preferences of the users.

Furthermore, the transfer services define the interfaces of the properties enabling fair exchange. These interfaces can then be supported by any good which may be plugged into a fair exchange protocol. Note that some properties may be trivial for some items while being unachievable for others: For messages, generatability is trivial while revocability is impossible. For signatures, generatability signatures requires additional cryptographic protocols [2].

3.5 Supporting Services

The *Supporting Services* provide user preference management, persistent object storage, communication, crypto services, and other supporting services such as access control. Furthermore, this layer provides secure communication services, i.e., a secure connection guaranteeing a given set of security attributes such as anonymity, authenticity, and confidentiality. The design of the anonymous communication service is describe in more detail in Section 4.2.

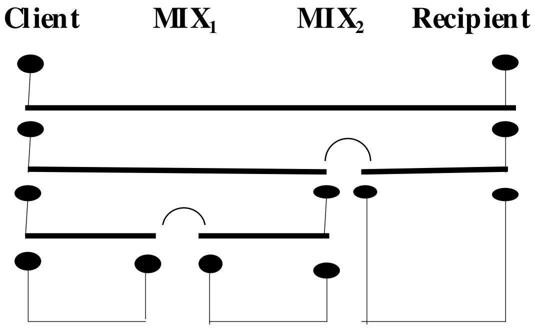


Figure 5: Anonymous Communication (Thick lines are secure and thin lines are insecure communication. Half-circles denotes message forwarding).

4. Recent Updates to the Framework

4.1 A Generic Fair Exchange Protocol

We now describe an example for the exchange protocols used in SEMPER. The protocol can be used to exchange generatable goods for externally observable goods. After the same pattern, other protocols can be built which guarantee fairness if one of the items provides generatability and the other external observability or if both offer generatability or revocability. The protocol is similar to the protocol described in [1]. It assumes that one of the goods offers optimistic external verifiability whereas the other good offers optimistic generatability. The basic idea is that the participants first commit on the generatable good and then the externally verifiable good is sent. Finally, the generatable good is sent. If the generatable good is not sent, the third-party is invoked to generate it after verifying that the externally verifiable good was really transferred. The behavior of the scheme in the fault-less case is sketched in Figure 6. A more detailed description will be published in [8].

4.2 Anonymity and Anonymous Communication

In SEMPER, anonymity services have to be provided by all layers. This is determined by a global anonymity security attribute: If this attribute is set, the supporting services layer provides anonymous communication by default. Furthermore, all services of higher layers only communicate via this anonymous connection and select anonymous protocols during negotiations.

The design of the SEMPER anonymous communication module uses a concept of layered secure communication sessions with multiple session oriented MIXes [3] to provide client anonymity[1]: In principle, the client opens a secure connection to the first MIX. Then, the first MIX opens a secure connection to the second MIX and redirects incoming messages. Then, the client opens a secure session with the second MIX. The recipient then acts like the last MIX in the chain. This ensures that the first MIX, for example, cannot read messages sent to the second MIX and thus, is not able to determine the recipient of a MIXed connection.

5. The *SEMPER* trials

The purpose of the trials is to evaluate the applicability and the soundness of the security architecture and services proposed by *SEMPER*. A map of the trial sites is depicted in Figure 7. The trials are based on the *SEMPER* software prototype which implements the architecture and the basic security services. The trials are being conducted in various business contexts, both internally and externally. Trial evaluation includes interviews of the trial users to measure the degree to which software meets perceived security requirements, to gain information about users' levels of understanding and trust in security options and in order to obtain input to the advanced trials. Only the trials related to the basic services of *SEMPER* are discussed here. An advanced prototype will be evaluated at the end of the project.

5.1 Internal SEMPER trials

In July 1997 the *SEMPER* prototype was tested by two service providers which are members of the project, Eurocom and Fogra. The Eurocom site, located in Athens (GR), offers distance learning services. Eurocom intends to use *SEMPER* to enable students to browse their offering of courses, register and pay online and, subsequently, gain on-line access to the selected course presentation, notes, and examinations. Fogra, a research institute for the printing industry, located in Munich (D), offers its customers on-line ordering and delivery of documents and software. In the advanced trials, Fogra plans to offer on-line consultancy.

The "Basic Trial" *SEMPER* software was used for the supervised trials which took place at Eurocom's premises. The trials were integrated in a series of seminars for SME employees with the title *"Conducting Business over the Internet"*. After a brief presentation of the *SEMPER* architecture, the participants were able to run the *SEMPER* software and to make a purchase of a seminar from the Eurocom electronic store. Due to constraints of time, the *SEMPER* client software was pre-installed and user registration had also been performed prior to the trials. As a result, the participants experienced only the purse creation and purchasing procedures. 30 people participated in the Eurocom trials. None of the participants' companies currently has a website and less than 1/3 of them advertise on another website, however, 1/3 plan to operate a website in the future. Their current interest in the Internet stems from the fact that they feel it would help them to reach a larger market and to remain competitive. More than half also reported that they would expect electronic commerce to enable them to do business more quickly.

Figure 7: SEMPER trial sites.

In general, the Greek trial participants didn't think that Internet is mature enough yet to perform business-to-business, or business-to-customer transactions, not due to the technology itself, but due to its limited use in their customer base. The lack of legal framework regarding the validity of electronic authentication was also viewed as an obstacle to performing important business transactions over the Internet. However, the general feeling was that these obstacles will be resolved and that electronic commerce has much to offer small and medium-sized enterprises. The *SEMPER* software met most of the participant's current business requirements for traditional commerce, apart from cheques as a form of payment. An electronic cheque is, in fact, planned for implementation in the advanced prototype.

Fogra demonstrated the *SEMPER* trial for three days in June 1997 at the IMPRINTA fair. It was demonstrated using a PC with Win95 and ISDN-access to the Internet through CompuServe. Due to both software and access problems, trial of the scenario was only partially successful. Before releasing the *SEMPER* code for external testing, Fogra remedied the problems which had occurred at IMPRINTA. A separate Fogra trial site was set up as the starting point for their participants and a new version of the trusted user interface (*TINGUIN*), including status bars and other enhancements, was integrated. In July 1997 5 persons from the Fogra customer base participated in "unsupervised trials".

The functionality and flexibility of the *SEMPER* architecture was greatly appreciated by the Eurocom and Fogra trial participants, but the state of the user interface was considered to be insufficiently developed for the ease of use to which non-specialists are accustomed (e.g. windows applications). As a result a new round of supervised trials, with participants selected on the basis of their networking experience, was conducted.

---

[1] In the current version, we assume that sellers are not anonymous.

5.2 Supervised Basic Trial

In December 1997 the *SEMPER* software was installed at the Institute for Computer Science and Social Studies at the University of Freiburg, Germany and tested by 12 trial participants. Twenty hours of in-depth interview material was recorded and has been analysed as the basis of the trial report, project deliverable D09 - Evaluation of Phase II Trials [7]. In order to obtain a more critical evaluation of the software, trial participants with extensive computing experience (and a minimum of 3 years Internet use) and a good awareness of secuity issues were selected. The participants subjected the prototype to particularly thorough testing, checking, for example, the software's response to incorrect input (seed too short, incorrect password entry, attempting to obtain a second certificate from the CA, attempting to continue without inputting the requested information, rejecting offers, etc.) and were favourably impressed by its performance.

The Fogra business application and trial website, mentioned above, was used as the trial site. The trial bank was also run from the Fogra server. The Certification Authority (CA) was provided by the *SEMPER* CA at the GMD in Darmstadt, Germany. Each trial participant initialised the locally installed *SEMPER* software for individual use by entering a personal log-in name and password (these were freely chosen by the participant), completing the registration process and creating one, or more, purses. The registration procedure was based on the participant's personal data (name, organisation, city) which had been submitted to the certification authority prior to the trial in order to simulate off-line personal registration. The participant also entered a personal registration key which the CA had assigned to him/her. It was explained to the participants that, under normal conditions, in order to obtain strong certificates, they would have had to personally visit the certification authority and present proof of their identity (passport or ID card) and, in return, have received their registration key and the fingerprint of the CA for verification during the on-line registration.

Having completed the initialisation process, participants used the *SEMPER* software for their first "semperised" experience of electronic commerce. They used the prototype to securely identify the Fogra website. They then browsed the Fogra website and selected a digital product (an abstract from the Fogra literature databank). Once they had selected the product they wanted and filled out the order form on the Fogra website, they then requested that their local *SEMPER* software process this order securely. They obtained a digitally signed on-line offer from Fogra. They used their locally installed *SEMPER* software to send a digitally signed order to Fogra and used the purse function of the *SEMPER* prototype to make a (simulated) on-line payment. The abstract was delivered to the participant in the Netscape browser.

As achieving legal certainty in electronic commerce will not only depend on the quality of the security technology, but also on the user's understanding and handling of it, during the initialisation of the *SEMPER* software particular attention was paid to the participants' understanding of the actions they were taking, as well as those factors which influenced their ability to successfully complete the process.
The trusted graphical user interface, *TINGUIN*, where all security relevant communications take place, is the visible and vital link between the user and the *SEMPER* software, as a result, it was subject to particular scrutiny. The credibility of the test for the participants was enhanced by the fact that it was possible for them to check the DOS (Java) window at all times during the test (and many did so). This ensured them that the test was actually *live*, i.e. that they were really exchanging certificates and containers with the CA and the bank and website servers in Munich.

5.3 SME Trials

Currently, external trials are being conducted by SMEs in Holland and France. They are also supported by the *SEMPER* basic security services and, in contrast to the previous trials, include real on-line payment. The OPL site (Oilfield Publications Limited - http://www.oilpubs.com/semper) is supported by *SEMPER* partner KPN and associate partner Maris (NL). OPL is offering books, maps, documents, and database access for the oil and gas industry. Online payments using credit cards and stored-value smartcards have been implemented. Two additional sites, supported by *SEMPER* partner, IBM France, are located in Sophia Antipolis (F). ACRI (http://eurosud1.eurecom.fr/acrimall) provides access to a databank of satellite images, processed and marked up with simulation results, e.g. the evolution of a polluted area, forest fires, etc. Communication is via ATM. The second site is an electronic shopping mall operated by Cicom. The *SEMPER* trial site is Actimédia (http://www.cyberlandpro.com), which will be selling CD-ROMs. Payments are to be made by credit card.

6. Acknowledgements

This work was supported by the ACTS Project AC026, *SEMPER*. However, it represents the view of the authors. *SEMPER* is part of the Advanced Communication Technologies and Services (ACTS) research program established by the European Commission, Directorate General XIII. This description is based on joint work of the *SEMPER* consortium. It is a pleasure to thank all of them for their cooperation and contributions. Furthermore, we would like to thank Jörg Veit for valuable comments.

The *SEMPER* home-page is at www.semper.org.

7. References

[1] N. Asokan, M. Schunter, M. Waidner: Optimistic Protocols for Fair Exchange, 4th ACM Conference on Computer and Communications Security, Zürich, April 1997, 6-17.

[2] N. Asokan, V. Shoup, M. Waidner: Optimistic Fair Exchange of Digital Signatures, IBM Research Report RZ 2973, IBM Zurich Research Laboratory, Zürich, November 1997

[3] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead, 7th IFIP International Conference on

Information Security (IFIP/Sec '91), Elsevier, Amsterdam 1991, 245-258.

[4] M. Schunter, M. Waidner: Architecture and Design of a Secure Electronic Marketplace, Joint European Networking Conference (JENC8), Edinburgh, June 1997, 712.1-712.5

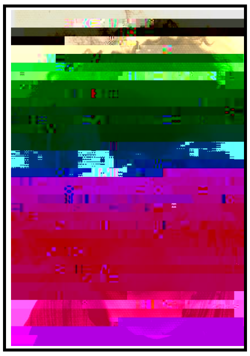
[5] *SEMPER* Consortium: Basic Services: Architecture and Design; *SEMPER* Deliverable D03; Århus, October 1996.

[6] *SEMPER* Consortium: Survey Findings, Trial Requirements, and Legal Framework -- Results from First Year of Project *SEMPER*; *SEMPER* Deliverable D05; Hamburg, December 1996.

[7] SEMPER Consortium: Evaluation of Phase II Trials; SEMPER Deliverable D09; Freiburg, to be published in 1998.

[8] *SEMPER* Consortium: Architecture, Services and Protocols; *SEMPER* Deliverable D10; La Gaude, to be published in 1998.
Available at <www.semper.org>

8. Vitae



Matthias Schunter has been a researcher in computer science at the Universities of Hildesheim and Dortmund since 1994. In SEMPER, he coordinated the design and implementation of the transfer- and fair exchange layers. His research interests include formal modelling of privacy and the design of protocols providing multi-party security. He has participated in the projects CAFE on off-line electronic payments, and in *SEMPER* aiming at an open integrated solution for global electronic commerce. Both projects were funded by the European Union. He received a diploma in computer science from the University of Hildesheim. He is a member of IEEE, ACM, and IACR.

Michael Waidner received the Diploma in Computer Science and the Doctorate (Dr. rer.-nat.) from the University of Karlsruhe, Germany. Since 1996 he has been the manager of the Network Security research group at the IBM Zurich Research Laboratory. His research interests include cryptography, secure protocols, and all aspects of dependability in distributed systems. He is (co)author of about 60 papers in cryptography and security. He is a member of ACM, GI, IACR and SIAM.

Dale Whinnett has been a researcher at the Institute for Computer Science and Social Studies, Albert-Ludwigs University Freiburg, Germany since September 1995. Research focus: user requirements and understanding of security technology. She is currently working in the project SEMPER and previously participated in the EU Esprit project CAFE on electronic payments at the Institute for Social Research, University of Frankfurt. She received her diploma in Marketing and German Studies from the University of Lancaster, GB.