Architecture and Design of a Secure Electronic Marketplace

Matthias Schunter <schunter@acm.org>
Michael Waidner <wmi@zurich.ibm.com>

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 architecture 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 rights.

This is reflected in the architecture: The exchange and transfer layer handles transfers and fair exchanges of items. 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.

A prototype of this architecture implemented in the Java programming language will be trialed for sales of multimedia courseware (EUROCOM, Athens, GR), on-line consultancy and subscriptions (FOGRA, München, D) as well as mail-order retailing (Otto-Versand, Hamburg, D). It will integrate the payment systems SET (provided by *IBM*), *Chipper* (provided by *KPN Research*), *and ecash™* (provided by *DigiCash*)). *The prototype uses a distinguished user-interface for trustworthy user in- and output which enables to use SEMPER on secure hardware.*

I. 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) [1, 2], 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 *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), *Otto-Versand* (D), *r³ security engineering* (CH), *CNET* (F), *SINTEF* (N), *SSL* (GB), *Stichting Mathematisch Centrum / CWI* (NL), *Universities of Dortmund, Freiburg, and Saarbrücken* (D). *Banksys* (B), *Banque Générale du Luxembourg* (L) and *Telekurs* (CH) are associated with SEMPER. IBM Zurich Research Laboratory provides the technical leadership for the project.

I.A. 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.*
- Both seller and buyer might need certain *certificates*. For instance, a buyer might only want to buy from sellers that are accredited with a well-known payment system provider in order to use a certain payment instrument. A buyer may only trust a seller if a consumer organisation has declared them trustworthy. A seller might be allowed to deliver certain goods only to residents of the European Union.
- 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.
- Many services require that buyer and seller have some relations already established, e.g., to banks or government agencies. This requires *registration*, *certification*, and in most cases also *directory* authorities.

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.

I.B. 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/>).

SEMPER provides an open architecture 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.

II. Model for Electronic Commerce

The architecture 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.

II.A. 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."

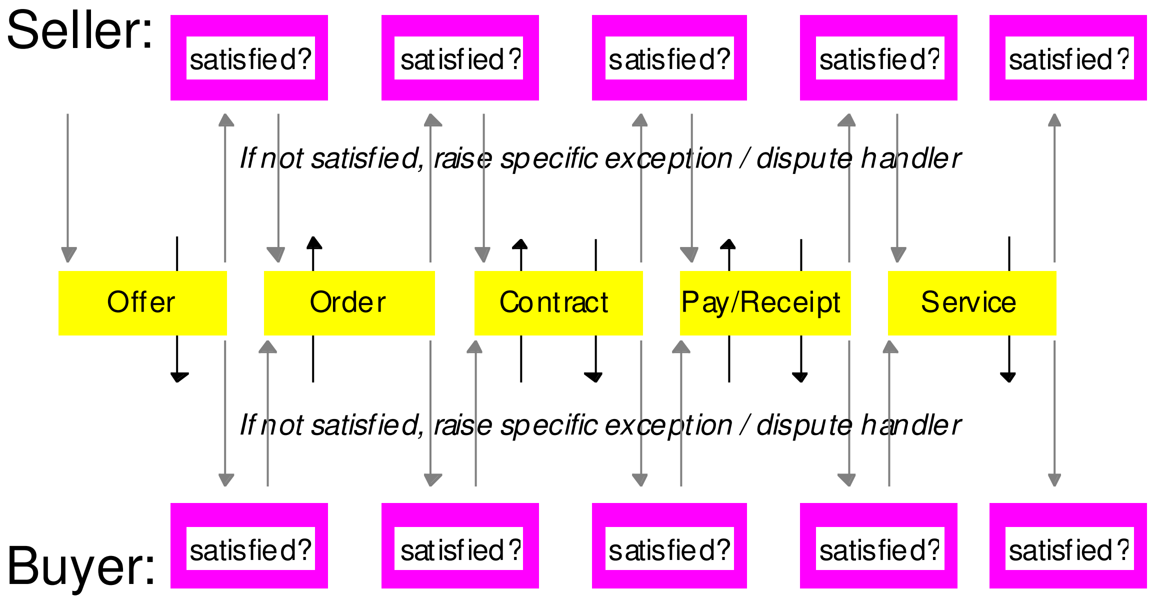

Figure 1 Electronic Commerce is a Sequence of Transfers and Exchanges.
Note that the protocol might enable other sequences as well, e.g., after "Contract" "Payment without Receipt" might also be enabled.

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.

II.B. 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 modeled 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.

III. The SEMPER Architecture

The SEMPER architecture (Figure 4) 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),

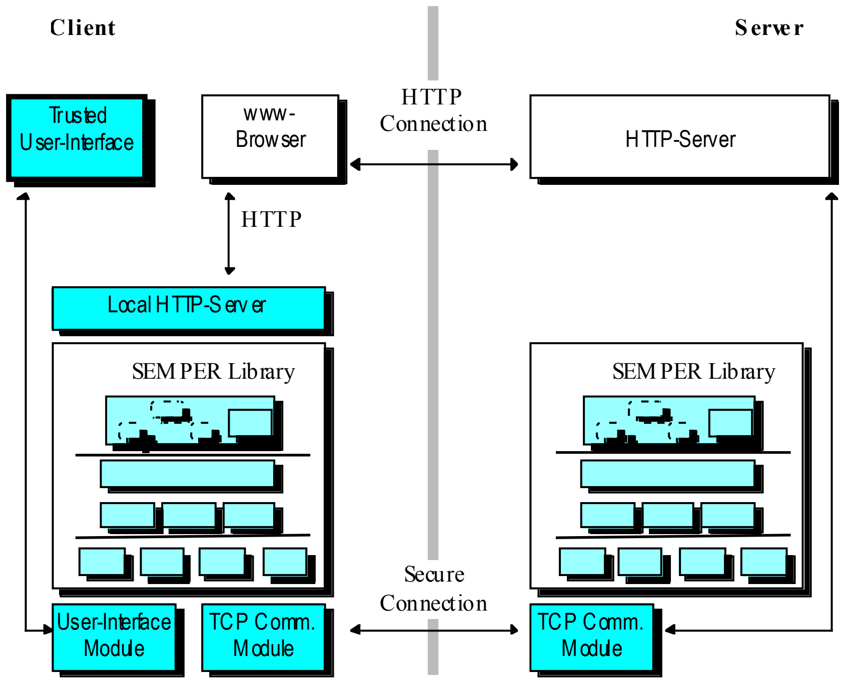

Figure 3 Client- and Server-Side Integration of the SEMPER Electronic Commerce Library.

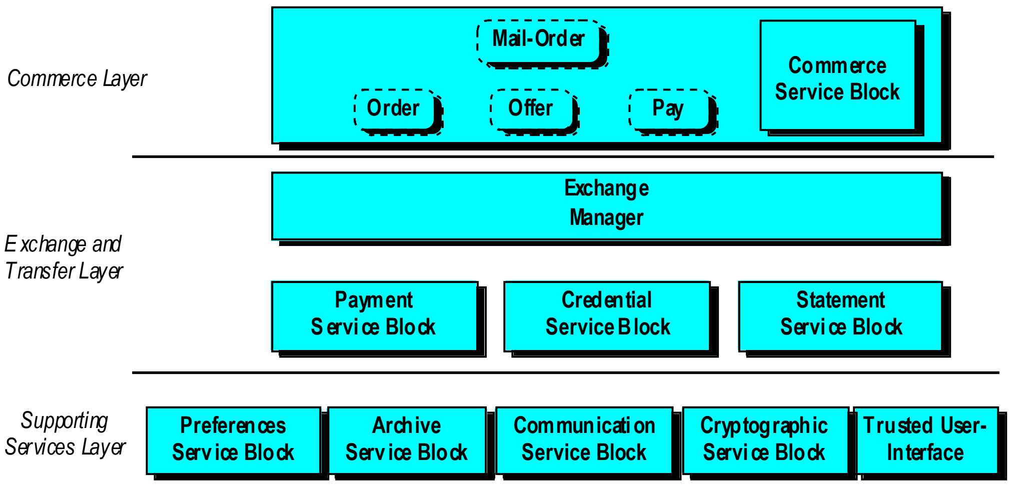

Figure 4 Architecture of *SEMPER*

setting preferences, and the trusted user interface.

- The exchange layer supports fair exchange and transfer services.
- The commerce layer offers high-level services for business scenarios like "mail-order retailing," "on-line purchase of information," or "registration with service provider." It is configurable by downloading new services or extending existing ones.

III.A. 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 such protocols, but also building blocks that may be of more general use, in particular services to manage and fill out standardized order forms.

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.

III.B. Exchange Services

The *Exchange and Transfer Layer* provides services for handling and packaging business items as well as transfer and fair exchange of packages. It implements the exchanges of the electronic commerce model. The basic items are electronic payments, credentials, and general statements which includes digital signatures and data. These items can be bundled in tree-like packages called *containers*. The security attributes stored in each internal node of this tree determine the level of security which is required for the transfer or exchange of the corresponding subtree.

Each type of items 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.

III.C. Supporting Services

The *Supporting Services* provide user preference management, persistent object storage, communication, crypto services, and other supporting services such as access control.

IV. The SEMPER Trials

IV.A. Basis

The SEMPER trials are based on the World Wide Web. The architecture is implemented by a library, as depicted in Figure 4 and described in detail in Section III. Service providers using SEMPER only need to implement the actual business terms (enabled sequences of transfers and exchanges) by configuring so-called commerce services (Figure 3). The integration into the World-Wide Web is done by interfacing with standard browsers and servers.

In order to support secure human-computer interaction, the SEMPER client provides a trusted user interface for security critical user in- and output, such as acknowledging a payment.

The first version of the SEMPER library supports only secure transfer services (i.e., no fair exchanges).

IV.B. EUROCOM: Courseware

EUROCOM is a consulting company offering multimedia courseware in the area of telecommunications. The EUROCOM trial implements on-line purchases of multimedia courses.

IV.C. FOGRA: Consultancy and Subscriptions

FOGRA is a research organisation of the German printing and publishing industry. They distribute information to their members on a subscription basis and sell consultancy to non-members. The FOGRA trial uses SEMPER for on-line purchase and processing of subscriptions as well as sales of consultancy.

IV.D. Otto Versand: Mail Order

Otto Versand is one of the largest mail-order retailers world wide. Currently, over 6000 articles can be browsed and ordered on the World-Wide Web. The Otto trial starts with on-line ordering of goods and may be extended to on-line ordering and delivery of tickets and other credentials.

V. 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. The SEMPER home page is at <http://www.semper.org>.

VI. References

[1] SEMPER Consortium: Basic Services: Architecture and Design; SEMPER Deliverable D03; Århus, October 1996.
Available at <www.semper.org>

[2] SEMPER Consortium: Survey Findings, Trial Requirements, and Legal Franework -- Results from First Year of Project SEMPER; SEMPER Deliverable D05; Hamburg, December 1996.
Available at <www.semper.org>.

Author Information

Matthias Schunter has been a researcher in computer science at the Universities of Hildesheim and Dortmund since 1994. 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 is the manager of the Network Security research group at the IBM Zurich Research Laboratory, Switzerland and Technical Leader of SEMPER. He has been working for the IBM Research Division since 1994. His research interests include cryptography, security, and all aspects of dependability in distributed systems. He has co-authored numerous publications in these fields. He received his diploma and doctorate in Computer Science from the University of Karlsruhe, Germany. He is a member of ACM, GI, IACR and SIAM.