SEMPER

Project AC026
ACTS Programme

© SEMPER Consortium, La Gaude, March 1995 and July 1995.

This document is based on the initial sections of the proposal and technical project plan (“Technical Annex”) of ACTS Project AC026, *SEMPER*, Secure Electronic Marketplace for Europe. It represents the view of the consortium.

Consortium

Acronym	Partner	Country
CRM	Cryptomathic	Danmark
CWI	Stichting Mathematisch Centrum	Netherlands
DIC	Digicash	Netherlands
EPI	Europay International	Belgium
ERC	EUROCOM EXPERTISE	Greece
FOG	FOGRA Forschungsgesellschaft Druck	Germany
FRE	Universität Freiburg, Institut für Informatik und Gesellschaft	Germany
GMD	Gesellschaft für Mathematik und Datenverarbeitung	Germany
HIL	Universität Hildesheim, Institut für Informatik	Germany
IBM	IBM France	France
INC	INTRACOM	Greece
KPN	KPN Research Netherlands	Netherlands
OTV	Otto-Versand	Germany
R3S	R3 Security Engineering AG	Switzerland
SPT	Service d'Etudes communes de La Poste et de France Télécom	France
ZRL	IBM Zürich Research Laboratory	Switzerland

For more informations on *SEMPER* please contact

Jean Marie Blachere (Project Manager)
IBM La Gaude
Centre d'Etudes er Recherches
Le Plan du Bois
F-06610 La Gaude, France
Ph. La Gaude: 33 92 11 50 90
Fax 33 93 24 45 45
Mail <blachere@vnet.ibm.com>

Michael Waidner (Technical Leader)
IBM Zürich Research Laboratory
CH-8803 Rüschlikon, Switzerland
Säumerstrasse 4
Ph. 41 1 724 8 220
Fax 41 1 710 3608
Mail <wmi@zurich.ibm.com>

<http://semper.darmstadt.gmd.de/~semper>
or <http://www.zurich.ibm.com/Technology/Security/extern/semper/>.

Brief Technical Summary

Project Title	**Secure Electronic Marketplace for Europe**
Project acronym	**SEMPER**
Workplan Areas/Tasks	Area 5, Task 503

Background. Networked information systems are experiencing a tremendous growth in terms of users and traffic as well as publicity. The dominating application is the Internet-based World Wide Web (WWW), with its potential of 3 million connected individual computers and an order of magnitude more actual users. WWW is still dominated by free-of-charge information systems, but this is expected to change dramatically in the near future. WWW will be used for all sorts of electronic commerce and trade, like online offering, ordering, payment, and delivery of services, information, and exchange of business documents. The same development can be expected for the *IBC networks* and "Information Highways".

There are already some projects and services that aim at electronic commerce via Internet, almost exclusively in the US. Most of them aim at *closed* solutions and concentrate on *electronic payments* only. None of them aims at the *complete* electronic marketplace. None of them provides a *coherent model or architecture*. Moreover, not even the non-technical and security *requirements* on such an electronic marketplace are understood completely.

Objectives. *SEMPER* will provide

- a detailed description of legal, commercial, social, and technical requirements and options for an electronic marketplace;
- a coherent model and a generic, open architecture of an electronic marketplace, independent of specific hardware, software, and network architectures;
- specifications, designs, and prototype implementations and evaluations for basic and advanced services enabling electronic commerce;
- information to the technical/scientific and general public, input to standardisation, input to other ACTS projects, stimulation of business developments based on the consortium's exploitation plans.

Technical Approach. *SEMPER* will be executed by an interdisciplinary consortium, combining experts from social sciences, finance, retail, publishing, IT and telecommunications, selected from across the academic, industrial, and SME environment in Europe.

The non-technical requirements part of *SEMPER* will be based on existing social and commercial expertise within the consortium, as well as on expert surveys performed in different European countries. The development part of *SEMPER* will be organised in 3 phases, one phase per year, each phase corresponding to an enhanced set of services and trials. The first phase will concentrate on modelling and architecture, and the provision of the most fundamental electronic commerce services, namely, secure electronic offering, ordering, payment, and delivery for multi-media online information services. The following phases will concentrate on more advanced services, including fair exchange of documents, credentials, advanced document processing, notary services, and multi-media specific security services like protection of intellectual property rights.

SEMPER will use and integrate existing architectures, tools, and services where appropriate. Early trials will be performed on the Internet, since the WWW infrastructure already exists and is well accepted, while later ones will use ATM-based broadband networks provided by National Hosts. This will prove the broad applicability of *SEMPER's* architecture and services.

Development will be driven by market requirements and the state of the art in security and online information services. For authentication services, state-of-the-art digital signatures will be used. Requirements for multi-party security and the protection of the users' privacy will receive prime attention.

Relation to ACTS Programme. *SEMPER* will cover all aspects of Task 503, and will contribute to Tasks 605, 122, 123, 124 and the ACTS Impact Assessment.

Table of Contents

CONSORTIUM 2

BRIEF TECHNICAL SUMMARY 3

1 PROJECT OBJECTIVES AND BACKGROUND 5

1.1 Objectives of the Project 5

1.2 Relationship with Programme Area Objectives 5

1.3 Background and Technical Contribution of *SEMPER* 6
1.3.1 State of the Art 6
1.3.2 Technical Contribution of *SEMPER* 10
1.3.3 Relation to Standardisation 12
1.3.4 Relation to Other EU Projects 12

1.4 Economic and Social Impact 13

2 PROJECT PLAN 15

2.1 Technical Approach 15
2.1.1 Overview 15
2.1.2 Defining Requirements 16
2.1.3 Architecture and Technical Services 18
2.1.4 Trial Implementation and Operation 21
2.1.4.1 Technical Approach in General 21
2.1.4.2 The Greek National Host Trial Infrastructure 23
2.1.4.3 The German National Host Trial Infrastructure 24
2.1.5 Evaluation of Results 24
2.1.6 Public Discussion and Dissemination of Results 24

2.2 Work Breakdown Structure 25
2.2.1 Core Tasks 25
2.2.2 Development and Trial Phases 26

2.3 Interrelationship of Work Packages 27

3 OVERALL PROJECT SYNTHESIS 29

3.1 Goal Description 29

3.2 Workpackage Description 29

1 Project Objectives and Background

1.1 Objectives of the Project

1. To develop a coherent, extendible, generic *model* and *architecture* of an electronic marketplace that is
   - independent of hardware platforms, operating systems, communication networks and protocols, and
   - as independent as possible of the commercial services to be offered on this marketplace.

   The initial focus will be on electronic offering, ordering, payment, and delivery, on trust services, and on credential schemes (e.g., accreditation of trading partners).
2. To demonstrate the meaningfulness and quality of the developed model, architecture, and services by means of *trials*.
3. Towards the above objective and based on the model and architecture,
   - to integrate and improve existing services, and
   - to identify and develop new services

   required for the secure operation of an electronic marketplace.

   Where different options for one service class are identified, different implementations will be designed.
4. To evaluate the *security* of the architecture and the integrated and developed services, especially taking into account multi-party security and privacy requirements.
5. In support of the architecture, to provide *requirements* for an open, multi-national electronic marketplace, from a legal point of view as well as from the point of view of all players involved in the marketplace.
6. To *disseminate results* to the scientific and technical community and to inform the general public by means of, e.g., articles, press releases, demonstrations on conferences and trade fairs, and to provide a platform for co-ordination between different projects dealing with electronic commerce.
7. To conduct an *independent evaluation* of the developed architecture and services, e.g., with the help of sponsoring partners.
8. To provide input to international *standardisation*.
9. To provide input to the *ACTS Impact Assessment*.

1.2 Relationship with Programme Area Objectives

SEMPER covers all aspects of

Task 503: Services Supporting an Electronic Marketplace.

Additionally, *SEMPER* will cover some aspects of

Task 605: Anonymity Management

Task 122: Copy Protection for Distribution Services

Task 123: European Multimodal and Secure Access to Multimedia Services

Task 124: Accounting and Audit Functions Management for Multimedia Access

and the ACTS Impact Assessment.

The consortium is composed of all necessary skills and expertise to guarantee that the results will have a direct impact on European economic and technological competitiveness. The involvement of partners from all over Europe, the strong orientation towards the market, and the inherently transnational character of the services considered by *SEMPER* will support the general process of the European economic, scientific, technological, and political unification.

1.3 Background and Technical Contribution of *SEMPER*

1.3.1 State of the Art

Electronic Marketplace and the Internet. Today, the most powerful networked information systems exist on the *Internet*. The Internet connects world-wide more than 3 million individual computers with an order of magnitude more actual users. Its current, almost exponential growth is mainly based on networked information systems, primarily the "World-Wide Web" (WWW).

WWW, originally developed by CERN, is a distributed hypermedia system combining the concepts of hyperlinks with multimedia. Through its URLs (Universal Resource Locators), WWW can represent links to any Internet information service like Gopher or FTP.

Characterising the tremendous amount and diversity of information services available via WWW is beyond the scope of this brief introduction. (A good starting point is [http://info.cern.ch]) In most cases, these services are provided free of charge by non-profit organisations like research institutes and universities. But a growing part of the Web is used for commercial *marketing* purposes. (For examples, see [http://www.openmarket.com/].)

There are already commercial start-up companies which offer support for online-shopping. In most cases, ordering requires user registration, and access is conditional on PIN or password-based authentication. Where online payments are supported, this is often done by sending credit card data more or less protected over the Internet to the merchant. None of these systems can be considered as leading, and most of them are still in the state of prototypes and business trials.

Most of the leading payment system companies as well as some internationally active banks have announced that they will support online payments via Internet in the very near future.

In some countries, especially in France, systems based on the videotex standard are used for online-shopping and other commercial services. The security properties of the PSTN-operated, closed videotex systems and the a priori open, chaotic and insecure Internet-based WWW are completely different. One cannot use the existing videotex tools in an Internet environment securely. But those companies that already support commerce via videotex demand services supporting electronic commerce that work *independent* of the type of network used.

Why Internet? The consortium considers Internet/WWW as the perfect first test environment for services enabling an electronic marketplace:

- The Internet connects a large number of users, both customers and vendors, world-wide, and grows fast. Getting access to the Internet via commercial service providers is inexpensive, and is supported by most hardware and operating system platforms. The leading personal computer and workstation operating systems already include or will include support for Internet access.
- The Internet protocol suite can be used with all types of networks, and has become a de-facto standard in communications. This enables trials "for real" on narrow-band Internet as well as on experimental broadband networks provided by National Hosts, based on the same set of payment and electronic commerce services and implementations.
- WWW provides a good framework for online multimedia information services, and is already accepted by a large user community and known to the general public.
- Internet poses the strongest security challenges: It is completely open, without a central network security management, without any provisions for communication integrity, authenticity, or confidentiality. Even worse, the structure and openness of Internet makes life for attackers as easy as possible. For instance, it is a trivial task to check the traffic routed through a node controlled by an attacker for Telnet or FTP passwords, or to send emails under an arbitrary sender address via SMTP.

  Thus, showing the feasibility of a secure and advanced electronic marketplace on the Internet would prove feasibility for almost all other types of networks.

Security and Electronic Commerce. The development of electronic commerce on the Internet exhibits a very fast but highly disorganised start. Currently, there is only limited understanding of the functionality and security properties of services that are required by electronic vendors and their potential customers. Coherent strategies for marketing, advertising, accounting, and payment are missing. Neither a comprehensive model of an electronic marketplace nor a generic functional and security architecture exists.

Most of the existing work on electronic commerce services concentrates on the development of *electronic payment systems*. The spectrum of systems offered via Internet includes

- systems that do not use any strong protection methods and require prior registration of user accounts (e.g., First Virtual), and may be considered as insufficiently secure or impractical,
- systems that implement a credit card model, processing customer authentication and payment information by standard security methods (e.g., OpenMarket, NetMarket),
- one system (DigiCash's ecash) that implements an anonymous electronic cash model.

Most secure online payment systems are developed in the US, i.e., they are subject to US export regulations (from those mentioned here, only ecash was developed in Europe). Therefore it is likely that those systems that provide a sufficient degree of security based on public-key digital signatures will be either not available in Europe, or available only in a form offering significantly reduced security.

Outside the Internet, some interesting, smartcard-based offline payment systems were developed, which could be used online as well. The spectrum ranges from classical electronic wallets and purses (e.g., Mondex and Proton) to systems that provide strong multi-party security and anonymity (e.g., the system developed by the ESPRIT Project CAFE). The leading payment system companies, Europay/Mastercard/VISA intend to support transactions based on smartcards (they published joint specifications), and the US FSTC (for more information see [http://www.llnl.gov/fstc]) initiated a project that will use a PCMCIA card as "Electronic Checkbook," also via Internet. All these approaches share the problem that the customer's stations need an interface to smartcards, PCMCIA cards, etc., which is not the case in general.

Partners of the consortium are involved in some of these developments and projects on online and offline payment systems, and will provide their experience and technology to the project as a starting point.

None of the different existing or proposed online payment systems are interoperable. Most of them do not provide strong multi-party security or user privacy.

Beyond payment, few other services are available for electronic commerce. The experimental NetBill system (Carnegie Mellon University, Pittsburgh) supports accounting and billing based on central billing servers. Recently, VISA announced to cooperate with Carnegie Mellon University, Pittsburgh, on the further development of NetBill. Surety Technology offers an advanced time-stamping service, and Electronic Publishing Resources (EPR) proposes technology for metering and copyright protection. OpenMarket announced similar technology.

There are mechanisms and standards for key certification, e.g., CCITT X509. Up to now, there is no sufficient certification infrastructure for public keys, but several projects aim at this. Examples are the TEDIS Project FAST, and activities within RARE and TERENA, based on the results of the EU VALUE Project PASSWORD.

Most of the advanced services that will be investigated by *SEMPER* -- especially fair exchange of documents, (unlinkable) credentials, advanced notary services -- are not provided by any current system and not addressed by any standard. The aspects of openness, universality, multi-party security, and customer privacy are not sufficiently considered by other projects or systems.

Since lack of protection of service providers' intellectual property rights is one of the main obstacles for electronic publishers to go online, *SEMPER* will also investigate techniques and services for copyright protection of digital information. Preventing software piracy is one important subproblem, and the techniques developed to make pirates' life hard will be used for general IPR protection as well. In general, completely secure solutions are infeasible since they require tamper-resistant hardware document containers everywhere. Partial solutions are based on registration, customisation of delivered information (which makes illegal copies less attractive), exact metering of use, and detection of IPR infringements by means of information marking ("fingerprinting").

Security Standards. Most aspects of electronic commerce on the Internet have not reached the maturity of being suitable for standardisation yet. It is not even clear which will be the winning approaches, and some aspects of commerce are not considered at all by existing projects.

Most of the basic mechanisms for secure protocols, including key certification and distribution, are covered by industry standards (e.g., *PKCS* by RSA Data Security, Inc.) as well as ISO and ITU standards (e.g., *X509*).

For electronic commerce via Internet, security improvements of electronic mail, HTTP (the protocol between WWW server and client), and IP are of particular interest.

PEM (described in RFCs 1421, 1422, 1423, 1424) and the controversial *PGP* (a specific program which has achieved the status of an industry standard) are important standards for secure electronic mail. They provide for integrity, confidentiality, and non-repudiation.

SHTTP (Version 1.1, Dec. 1994) is a proposal for secure HTTP. It will add integrity, confidentiality, and non-repudiation to HTTP documents, and could become a basis for the development of advanced security services. SHTTP is still under development. There are some competing efforts (e.g., SHEN).

Several "firewalls" and security enhancements on the IP or sockets layer are proposed, securing the link between server and client (e.g., SSL). They may be used to secure payment information (e.g., Netscape's Commerce Server), but this does not provide full multi-party security.

No standards for online Internet payment systems exist yet, though several serious efforts aim at producing de-facto standards. In November 1994, VISA and Microsoft announced that they will jointly produce specifications with a first public release in 1995. The US FSTC initiated a project that will develop an "Electronic Checkbook" based on tamper-resistant PCMCIA cards, and applicable to online payments via Internet. Not much has been disclosed about these efforts.

Standards for offline payment systems are evolving (within CEN), but the market is dominated by non-standard, proprietary designs.

Hypermedia Standards. There are a number of existing and emerging standards for structuring, exchange, and presentation of hypermedia documents and related services, which will be the basis for the consumer services in *SEMPER's* trials. The most important standards for information structuring and exchange are SGML and HyTime. SGML is a markup language for defining the logical content of documents. Because of its flexibility it has become an important tool in hypermedia systems. WWW and Hyper-G are both based on (subsets of) SGML.

MHEG and Acrobat are (proposed) industry standards for representing multimedia documents platform-independently. Another standard of importance is AVIs (Audio-Visual Interactive services) for multimedia services across telephone or ISDN networks.

Important standards for WWW are the drafts on "HyperText Transfer Protocol," HTTP/1.0 (94/11/28), on "Uniform Resource Locators," URL (94/08/04), on "HyperText Markup Language," HTML/2.0 (95/02/08) and several RFCs on MIME (RFC 1521, 1522, 1524, 1563, 1590).

Competing Efforts in Electronic Commerce. There are many individual academic and industrial projects with results and prototypes addressing isolated problems, primarily online payment systems (see above), and the problem of establishing a certification infrastructure (e.g., the EU TEDIS Project FAST).

The only other project that aims at the complete electronic marketplace is the US Project *CommerceNet.*, launched in April 1994 and funded by the US government's Technology Reinvestment Project. (For more information see [http://www.commerce.net].)

The founding members of CommerceNet are BBN/BARRNet, Enterprise Integration Technologies (EIT), and Stanford University's Center for Information Technology (CIT). Any US organisation can become a sponsoring or associate member of CommerceNet. Currently, CommerceNet has around 70 sponsoring members, primarily from the electronics, computer, information service, and financial service industries.

The technical work in CommerceNet is organised around the development of *SHTTP*, the security-enhanced version of HTTP mentioned earlier. Specifications are published, and prototypes for server and client software are available for members. Some trial projects based on SHTTP are defined and will be executed by members.

Currently, there are no significant efforts within CommerceNet on the development of advanced services in the sense of *SEMPER*. *CommerceNet* considers itself as a forum for discussion, not as a research or development project.

The consortium will establish good relations to CommerceNet, using already established individual contacts. This will be a chance to ensure the openness and international applicability of services developed by *SEMPER*.

1.3.2 Technical Contribution of *SEMPER*

SEMPER will be the first project, to our best knowledge, that covers the security in electronic marketplaces completely and systematically.

SEMPER will develop the first coherent model and open architecture of an electronic marketplace.

Such a model and architecture is necessary to ensure compatibility and interoperability of different services (e.g., payment and delivery) and service implementations (e.g., different payment systems). Incompatibility and non-interoperability is at least an inconvenience for users, service providers, and developers. But the resulting undefined interactions and dependencies is also a dangerous source of insecurity.

In contrast to most other projects, *SEMPER* will use a modern multi-party security architecture, i.e., the security concerns of all parties will be considered individually. As required by ACTS Task 503, *SEMPER* will also investigate the need for anonymity in electronic marketplaces, which is done up to now only for electronic payments, primarily by the ESPRIT Project *CAFE* (where the *SEMPER* partners *CWI, DigiCash, Univ. Hildesheim, KPN, SEPT* participated) and several projects at *Digicash*.

Initially, *SEMPER* will concentrate on electronic ordering and payment, but the model and architecture will be continuously extended to cover advanced services in the course of the project, finally covering the complete marketplace.

Note that *DigiCash, Europay, IBM,* the sponsoring partner *Banksys*, and those partners that were involved in Project *CAFE* represent the full range of proposed electronic payment system technology, which will ensure the openness of our architecture. *IBM* as one of the leading companies in network security, *Cryptomathic* and *R3* are among the leading European companies in EDI-security, and *Europay* as one of the three leading payment system companies (besides their US partner *MasterCard*, and *VISA*) guarantee that the results of *SEMPER* will affect international standardisation.

Most projects concentrate on a few problems like secure communication, electronic payment, key certification and registration. But many of the services that will be needed for a secure electronic marketplace do not exist at all, or on paper only.

For example, fair exchange of documents, on-line arbitration of conflicts, fair two-party and multi-party contract signing, and credentials are only investigated in theory. Copyright protection is considered as essential for electronic commerce, but no satisfying approach is known yet.

SEMPER intends to develop solutions for these unsolved problems.

1.3.3 Relation to Standardisation

The *SEMPER* consortium will provide input to international standardisation via partners that are already represented in all important international standardisation bodies. Existing close business relations with companies outside the EU will increase *SEMPER*'s influence.

Committee	Title		Partner
CEN	TC224	Inter-industry machine readable cards, related device interfaces and operation	EPI
	TC224 WG10	Definition of an open inter-sector electronic purse as an application on a multi-application card.	DIC, EPI, IBM, KPN
DIN	NI 17.10	Intersector Electronic Purse	FRE
ECBS	TSC	European Banking Standards	EPI
	TC1	Plastic Cards	EPI
	TC3	Cheque Processing	EPI
	TC4	Security: Digital Signatures and Certification Authorities	R3S (for the Swiss Bankers Association)
ECMA	TC36-TG1	IT-Security Evaluation Criteria	R3S
UN/EDIFACT	SJWG	Sec. Joint Working Group/Security in EDIFACT	CRM, R3S
ETSI	SAGE	Secure Algorithm Group of Experts	KPN
	STAG	Security Techniques Advisory Group	KPN, R3S
EWOS	EGSEC	European Workshop on Open Systems: Security	CRM, R3S
IEEE	1003.6	POSIX Security Extensions	IBM
	P1363	Standard for RSA, Diffie-Hellman, and Related Public-Key Cryptography	R3S
ISO	TC68/SC2/WG2	Operations and Procedures	IBM
	TC68/SC6	Financial Transaction Cards	EPI, IBM
ISO/IEC	JTC1/SC17/WG4	ICC and related devices	EPI
	JTC1/SC17/WG8	Contactless ICC and devices	EPI
	JTC1/SC17/WG9	Optical Memory Cards and devices	EPI
	JTC1/SC21/WG1	OSI Architecture	IBM
	JTC1/SC27/WG1	Security Techniques	CRM, IBM, R3S

1.3.4 Relation to Other EU Projects

SEMPER will build on the results of previous activities of the consortium, and will co-operate with concurrent activities.

Cryptomathic, Digicash, GMD, R3, and *IBM* are involved in most of the relevant research and development projects in Europe.

The results of the EU projects *AMIDE, BOLERO, CAFE, MANDATE, FAST, PASSWORD,* and *TESTFIT* will be used by *SEMPER*. The same holds for industrial projects on electronic on-line payments at *DigiCash, Europay,* and *IBM Zurich Research.* Via the common partner *GMD*, close relations to the proposed EU projects *E2S* (IT Programme) and *ICE* (Telematics Programme) will be established.

Through connections to the US *IBM Corp.,* the consortium is linked to the main activities in the US as well, namely *CommerceNet* (see Section 1.3.1) and the *US FSTC Electronic Check* project.

The workplan of *SEMPER* is based on the availability of existing technology and results from previous projects. Otherwise, it would be impossible to finish the first phase of *SEMPER* within the first 12 months. Especially for electronic payment and key certification and registration, *SEMPER* must reuse existing technology.

On the other side, *SEMPER* will join its forces with these and other projects. This will be ensured by a *Special Interest Group on Secure Electronic Commerce* that will be established by *SEMPER* (see Section 2.1.6).

1.4 Economic and Social Impact

Economic impact: *SEMPER* technology has the potential of playing a crucial role in global commerce and facilitating considerably new online trading services. The open architecture and security services developed by *SEMPER* will lead to an increased use of online business. Transactions can take place without a prior exchange of written documents. Thus transaction costs will be smaller than with today's paper-based contracts. Rapid creation of new services will be facilitated. With the services developed by *SEMPER*, the paperless trade can also take place across borders. Thus trade within Europe is expected to increase, and geographically disadvantaged areas can also participate. This should help to stabilise employment in Europe in the communications industry and with the service providers.

Social impact: Multi-party security is of crucial importance in open networks. Only if this can be provided can it be expected that hundreds of thousands or even millions of non-trusting partners will trade valuable information and goods without prior written agreements between all parties. With such world-wide electronic trade, end-users will need to protect their assets, i.e., their valuable information, their credentials, and their money. With the help of *SEMPER* technology it will not be necessary to transmit a valuable information such as a credit card number in clear over the Internet. Security shall be provided using public-key technology, thus avoiding the necessity to share secret keys with a service provider who may not be trusted completely by the consumer. National security, consumer privacy, and other legal considerations will be taken into account during the specification phase of the payment and electronic commerce services.

World-wide electronic trade can be expected to grow tremendously -- with or without any multi-party security architecture including all players involved. Experience shows that service providers as well as service users would start even with completely insecure tools, provided they offer sufficient functionality and performance compared to non-electronic trade. This may lead, however, to serious damage of innocent parties, at least in the long run. Also many parties may be reluctant to participate initially because of the risks involved. Thus, *SEMPER* increases the acceptance for electronic commerce, and will contribute significantly to preventing insecure systems from becoming de facto standards, by providing feasible secure alternatives.

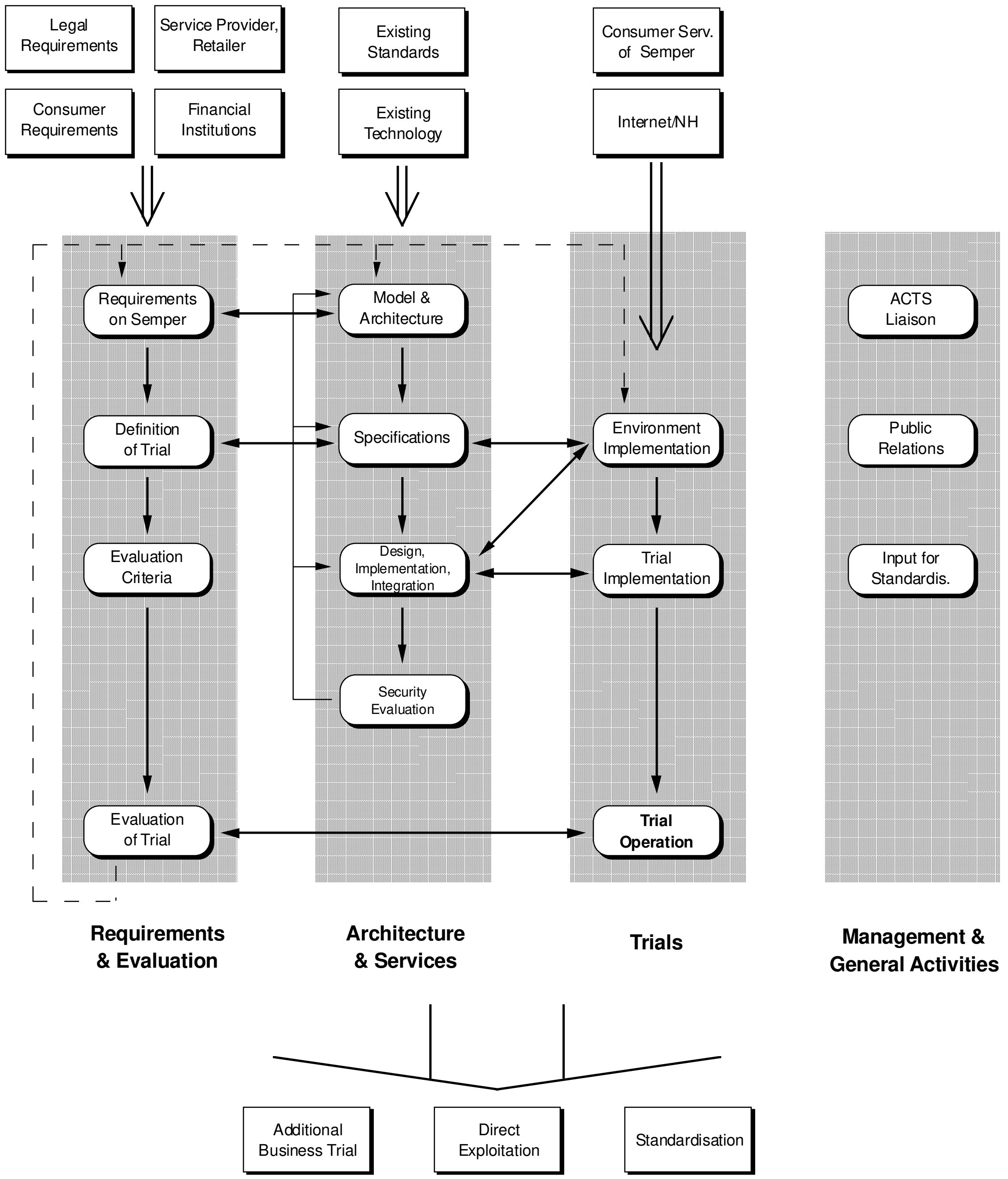
Legal Requirements
Service Provider, Retailer
Consumer Requirements
Financial Institutions
Existing Standards
Existing Technology
Consumer Serv. of Semper
Internet/NH
Requirements on Semper
Definition of Trial
Evaluation Criteria
Evaluation of Trial
Model & Architecture
Specifications
Design, Implementation, Integration
Security Evaluation
Environment Implementation
Trial Implementation
Trial Operation
ACTS Liaison
Public Relations
Input for Standardis.
Requirements & Evaluation
Architecture & Services
Trials
Management & General Activities
Additional Business Trial
Direct Exploitation
Standardisation

Figure 1 Overall Project Plan

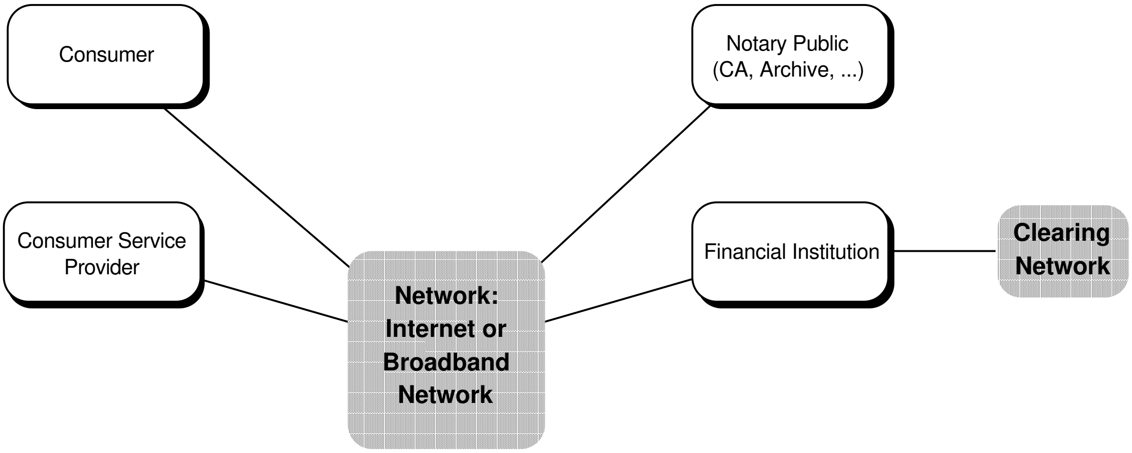
Consumer
Notary Public (CA, Archive, ...)
Consumer Service Provider
Financial Institution
Clearing Network
Network: Internet or Broadband Network

Figure 2 Basic components of an electronic marketplace

2 Project Plan

The overall project plan for *SEMPER* is shown in Figure 1, and described in detail in the following sections.

2.1 Technical Approach

2.1.1 Overview

Like a physical marketplace, an electronic marketplace connects a number of users and enables some specific commercial transactions.

We call those services that are the subject of commerce **consumer services** (e.g., online publication of a newspaper, online shopping at a mail order retailer), and those services that enable the secure provision of consumer services **technical services** (e.g., secure ordering and electronic payment).

The main components which will be included in *SEMPER's* architecture are shown in Figure 2. These are

- **Customers** of consumer services.
- **Providers of consumer services** including **directory services**.
- **Notaries**, responsible for all kinds of certification, dependable storage (archiving), trustee services, etc.
- **Payment service providers.**

Additionally, **arbitrators** for resolving disputes are necessary, either online or offline. Since arbitrators are not involved in business, usually, they are not shown in Figure 2.

SEMPER aims at an electronic marketplace that is open to any citizen, both as customer and as provider of consumer services. The business relations between customers and consumer service providers will be established inside the electronic marketplace, which requires public-key technology and the presence of third party services, like a Notary Public, for certification.

The architecture will allow customers to access the electronic marketplace, e.g., either
- using a *personal* terminal, e.g., a PC at home or in the customer's office, or
- using a *public* terminal that is located in a shop or any other public place, or
- a combination of both, e.g., using a smartcard or a PDA-like device that interacts with a personal or public terminal and manages the user's credentials, electronic financial assets, etc., dependably.

The latter approach offers maximum security, but its commercial and technical feasibility as well as its customer acceptance must be investigated carefully. Also, the need for tamper-resistant devices like smartcards should be investigated.

Consumer services that might be offered are
- directory services;
- electronic shopping, i.e., online offering (e.g., catalogues), ordering, and payment, combined with offline delivery of goods or online delivery of information services;
- notary services like certification and archiving of electronic documents, and all kinds of trusted third party services;
- special mail security options, e.g., certified mail.

Note that online information services range from electronic publication of static information to all sorts of customised information and interactive services.

The bottom line for the security required for services should be the security of the non-electronic marketplaces: Electronic commerce should be at least as anonymous and secure as today's "non-electronic" commerce, and no customer should be forced to trust a central authority or their business partners unreasonably. Multi-party security, including reasonable anonymity measures, will be among the main focuses of *SEMPER*. Anonymity and confidentiality will be provided only in a way that is compatible with the different national law, security, and criminal investigation concerns.

The technical approaches to the basic steps -- defining requirements, developing an architecture and technical services that satisfy them, implementing and performing a trial, and evaluating the results -- are discussed in Section 2.1.2 - 2.1.5. Details on *SEMPER's* publication policy are provided by Section 2.1.6.

2.1.2 Defining Requirements

The definition of requirements will reflect the needs for technical and consumer services as they are perceived by the players of the marketplace and as they will emerge during the trials. The requirements will cover issues such as security, privacy, performance, dependability, usability, quality, acceptability, and costs of services. The analysis of requirements will also consider today's handling of these issues, related risk perception, actual handling of services in the trials and ergonomic aspects. All requirements will be analysed in order to understand the needs and risks involved in depth. The result of this analysis will lead

- to a non-technical definition of technical services
- to recommendations on how electronic commerce should be handled by the market participants to minimise their risks
- to recommendations with regard to legislation.

All requirements will be captured both internally to the consortium, and externally, which will be the larger part of the work. Internally, the expertise of the consortium's service providers, retailers, and the financial industry are gathered to define the trials. Externally, experts and consumers not participating in the trials are interviewed, as well as users participating in the trials.

Consumer requirements. Person-to-person interviews of private and business users with semi-standardised questionnaires will lead to an in-depth understanding of the consumer requirements. Consumer surveys will be made with the support of the service providers (retailers, financial industry) in the consortium. Surveys will include users of the World Wide Web inside and outside the trials.

Service provider and retailer requirements. Requirements of service providers and retailers will on the one hand be defined internally, by the service providers and the retailer in the consortium. On the other hand, international expert surveys will be performed.

Requirements of financial institutions. The payment system provider in the consortium will contribute to define the requirements of the financial industry by providing their expertise and interviewing their members. Representatives of banks and other financial institutions will also be interviewed during the expert surveys.

Legal requirements. Legal issues have to be investigated on three levels. The first level refers to requirements stemming from existing legislation, such as banking laws, export legislation, or data protection legislation. The second level refers to requirements of different parties with regard to electronic commerce, e.g., requirements for signatures, proofs of transaction, non-repudiation. The services to be built have to mirror these requirements appropriately. The third level refers to recommendations on how legislation should support electronic commerce. The consortium intends to provide recommendations. The legal requirements will be collated by collecting the internal expertise, studying the relevant literature, and by interviewing experts. Legal aspects will also be covered in the user interviews.

The resulting non-technical definition of the requirements will give input to the technical specifications of the architecture and the technical and consumer services. These, again, will be reviewed against the non-technical definition in an iterative process lasting for the whole duration of the project.

2.1.3 Architecture and Technical Services

The selected **system architecture** has to be able to support changing requirements and the integration of varied commercial aspects.

Technical services will be separated from the concrete consumer services and the multi-media, communication, operating system, and hardware architecture aspects by means of well defined **service specifications** and **application programming interfaces** (APIs; see Figure 3). Formal specification and verification methods as well as techniques for integrating functional and security specifications will be investigated.

The "local electronic commerce server" will provide a unique interface to the application (in Figure 3, a multi-media browser), and will provide the management functions that are common to all technical services (e.g., user access control, accounting, audit).

Separation of technical services and communication services could be done by utilising already existing communication channels at the consumer service application level, e.g., Generic Security Services API (GSS-API; RFC 1508, 1509) if present.

The isolation of technical services from the specific network and consumer services has its limitations

- where the technical services require additional communication, e.g., to third parties, and
- where the technical services require additional hardware components, e.g., smartcards or interfaces to PDAs or electronic wallets.

Media-specific technical services like integrity protection of video data, protection of copyright, and metering of usage might require specific solutions.

Protocol design will be based on the state of the art in security. *SEMPER* will deal primarily with integrity, authentication, and non-repudiation, since these are the most essential security requirements on electronic commerce. Digital signatures based on appropriate certification infrastructure will be used as the main means for authentication.

Existing, available designs will be considered and integrated. Members of the consortium agreed to contribute their relevant technology to *SEMPER*, especially in the area of highly secure electronic payment systems.

Where technically appropriate, alternative protocols for technical services will be provided, with different functional and security properties.

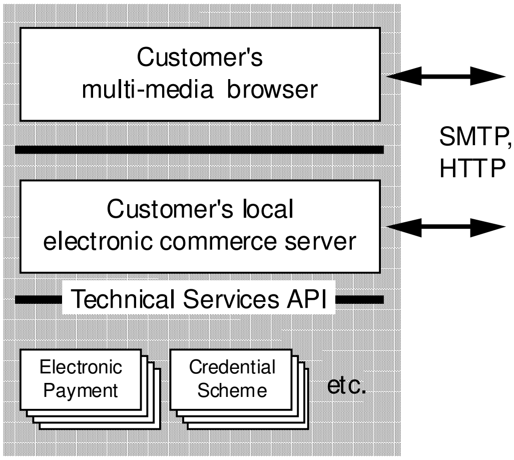
Customer's multi-media browser
SMTP, HTTP
Customer's local electronic commerce server
Technical Services API
Electronic Payment
Credential Scheme
etc.

Figure 3 Separation of technical services and multi-media and communication services. The architecture shown for the customer will be applied to the other components as well.

The security and functional properties of the protocols will be clearly specified, and validated by means of

- formal verification and mathematical proofs of security, where feasible,
- internal reviews, based on the independence of design and review groups,
- external reviews as part of the public discussion process,
- extensive testing during implementation and integration,
- trials.

Protocol implementation will be based on standard programming systems and tools, ensuring the portability to all required platforms.

Existing security standards, mechanisms, and tools as well as results from previous projects will be used.

For the client components, initially, *SEMPER* may use software-only solutions. Later, for commercial processes where appropriate, tamper-resistant hardware will be used, e.g., smartcards. An example where this might be necessary are payments, especially if already existing offline payment systems should be integrated. The necessary, specific hardware and software technology for tamper-resistant devices is available within the consortium.

Financial institutions, public notaries (including certification authorities, archives, etc.), and online arbitrators will be implemented by specialised server components. These servers will be operated within a physically protected, trusted domain and will be connected to the electronic marketplace through appropriate security firewalls.

Specific services. Initially, *SEMPER* will concentrate on **trading**, which requires at least the following **basic technical services**:

- Establishment of the necessary trust relations and security management services, which requires certain basic notary services. The minimum requirement here is certification of public keys, and directory services (e.g., X.500).
- Negotiation of type and quality of security services.
- Standard communication security services.
- Services for *secure* purchasing and payment of goods.
- Goods might be physical goods or information. In case of information, secure delivery may be provided as well.

For these basic services *SEMPER* will use existing technology wherever possible. For example,

- technology for "certification of public keys" (X.509) might be imported from the EU projects PASSWORD, FAST, ICE;
- technology for "standard communication security" might be imported from ICE, E2S, and other projects providing publicly available implementations of standard security protocols;
- technology for "payment of goods" might be imported from the EU project *CAFE* and the systems *e-cash* and *iKP* developed by DigiCash and IBM, respectively.

Examples for **advanced technical services** are (besides security enhancements and extensions of the basic technical services):

- Fair exchange of values, i.e., simultaneous or notarised exchange of electronic payment and electronic goods.
- Media specific aspects, e.g.,
  - metering of usage
  - protection of copyright (IPR).
- Secure document processing, e.g.,
  - time stamping;
  - certification of documents, (unlinkable) credentials;
  - certified mail, i.e., non-repudiation of delivery;
  - secure archiving;
  - two-party and multi-party contract signing;
  - fair (i.e., simultaneous) exchange of documents.
- Online arbitration of conflicts.
- Secure multi-party protocols.

Three sets of technical services, Basic Services and Advanced Services I/II, will be defined in the course of the project (by Core Task 2, WP2.1), taking into account the requirements and the definition of consumer services (provided by Core Task 1). For the timing of decisions see the timing of results in the detailed workplan.

2.1.4 Trial Implementation and Operation

2.1.4.1 Technical Approach in General

Based on the requirements analysis and the technical services described in Sections 2.1.2 and 2.1.3, consumer services will be designed that allow conducting electronic commerce across open networks. The system will use existing approaches and tools to the extent possible and will integrate to them the technical electronic commerce services developed by the project. Only where necessary will new development be undertaken. Selected approaches and tools will be standard-based as much as possible.

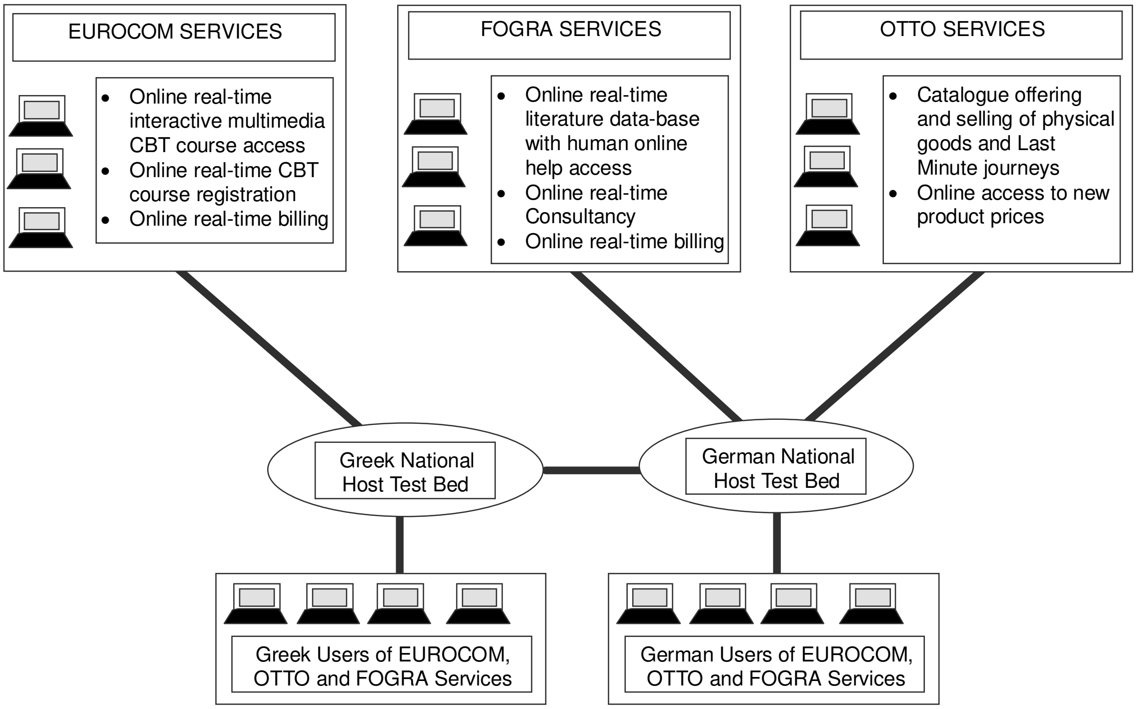
EUROCOM SERVICES
Online real-time interactive multimedia CBT course access
Online real-time CBT course registration
Online real-time billing
FOGRA SERVICES
Online real-time literature data-base with human online help access
Online real-time Consultancy
Online real-time billing
OTTO SERVICES
Catalogue offering and selling of physical goods and Last Minute journeys
Online access to new product prices
Greek National Host Test Bed
German National Host Test Bed
Greek Users of EUROCOM, OTTO and FOGRA Services
German Users of EUROCOM, OTTO and FOGRA Services

Figure 4 Consumer services and uses of the *SEMPER* environment based on Greek and German National Hosts

SEMPER's trials will be based on the **consumer services** provided by the partners FOGRA, EUROCOM, and Otto-Versand (see Figure 4) and on the Internet and the German and Greek National Hosts as **trial infrastructure** (see Section 5.2.3 for more details on the relation between *SEMPER* and these National Hosts). The different end-user profiles have to support also different consumer services, e.g.,

- Online access to literature databases (FOG);
- Access to online documentation, reports - full multimedia documents with animation, sound, etc. (FOG);
- Access to specific expert systems, e.g., problem diagnostic systems (FOG);

- Electronic booking of symposia and seminars (FOG);
- Selling of physical goods - special temporary offers and catalogues - (OTV);
- Offering of "Last Minute" journeys (OTV);
- Online access to new product prices (OTV);
- Offering and selling of multimedia training courses, Computer Based Training (CBT) Courses, (ERC).

Based on these options, the set of consumer services to be actually trialed will be defined after Month 3 of the project (by Core Task 1, WP 1.2), with revisions after the first and second year (see the detailed workplan).

For the management of the applications during the trials, directory services (yellow pages, X.500) will be provided by the Greek National Host.

On the **network level** the Internet protocols (TCP/IP) will be used. It guarantees world-wide availability of the services.

The first trial (in Year 1) will be based on the existing Internet infrastructure only (e.g. X.25, ISDN). This basic trial will be focused to specific areas in Europe, for reasons of trial management and evaluation, but in principle, they can be observed from all over the world.

The network infrastructure for the later, enhanced trials will be defined and specified depending on the actually available consumer services and the requirements of the technical services, as well as the costs and availability of services provided by National Hosts. The infrastructure required for the enhanced trials in Year 2 and Year 3 will be defined by the end of the first and second year, respectively.

Both the Internet and broadband networks provided by the German and Greek National Hosts, connected by a European backbone, shall be used for the Enhanced Trials (see Figure 4). GMD and INC are part of the German and Greek National Hosts, respectively (see their statements in Section 5.2.3).

Information management will be database oriented. Depending on the information services chosen for the trial, an existing database system will be selected. **Information modeling** will be standard-based. SGML and HyTime will be adopted.

Editorial workbench. To produce and maintain consumer services, authoring and editing tools for content and acquisition and maintenance will be integrated. The tools needed depend on the consumer services selected for the trials.

Customers' access. Customers need a browser which allows full usage of the multimedia information service and which is easy to use. Quality of service criteria such as tolerable delay in delivering information, navigational aid and improved feedback of the system have to be considered. Existing systems like WWW browsers or Hyper-G browsers will be used and improved where necessary.

Live trials involving consumers, merchants, and financial services will be conducted to collect feedback on usability, costs, accounting statistics, performance, and security of the developed technology.

Trial evaluation. Trials will be evaluated technically (dependability, performance, etc.) and by interviewing the trial users. Therefore, evaluation criteria and appropriate questionnaires have to be developed. The emphasis will be on personal interviews with semi-standardized questionnaires. The evaluation shall be done in close co-operation with the service providers and be input to the refined definition of services.

2.1.4.2 The Greek National Host Trial Infrastructure

Figure 5 shows the Greek trial infrastructure. In this scenario, EUROCOM is the service provider of multimedia training courses (see Section 2.1.4.1). The Computer Based Training (CBT) courses developed at EUROCOM will be downloaded off-line into the CBT Database, located at the INTRACOM National Host site, through an *n* * 64Kbps link. The customers of EUROCOM will be able to access the courses through the following connectivity options:

- Basic Trial: For the first year trials, Internet and ISDN connectivity will be provided to the end-users by the National Host infrastructure at INTRACOM.
- Enhanced Trial I & II: For the 2nd and 3rd year trials connectivity of the end-users to the National Host will be provided by 1Mbps Permanent Virtual Circuits (PVCs). The requirements for the PVCs (e.g., peak rate, sustainable rate, burst tolerance) will be determined by the *SEMPER* specific application requirements as well as the encoding methods employed. For example, one 4Mbps PVC for interconnecting the Greek and the German testbed sites is satisfactory for 5 trial sessions including video based on H261, MPEGI and MPEGII standards.Timing requirements for the connection will be determined by the project workplan in terms of the trial activities and service requirements and by the tariffs set by the PNOs.

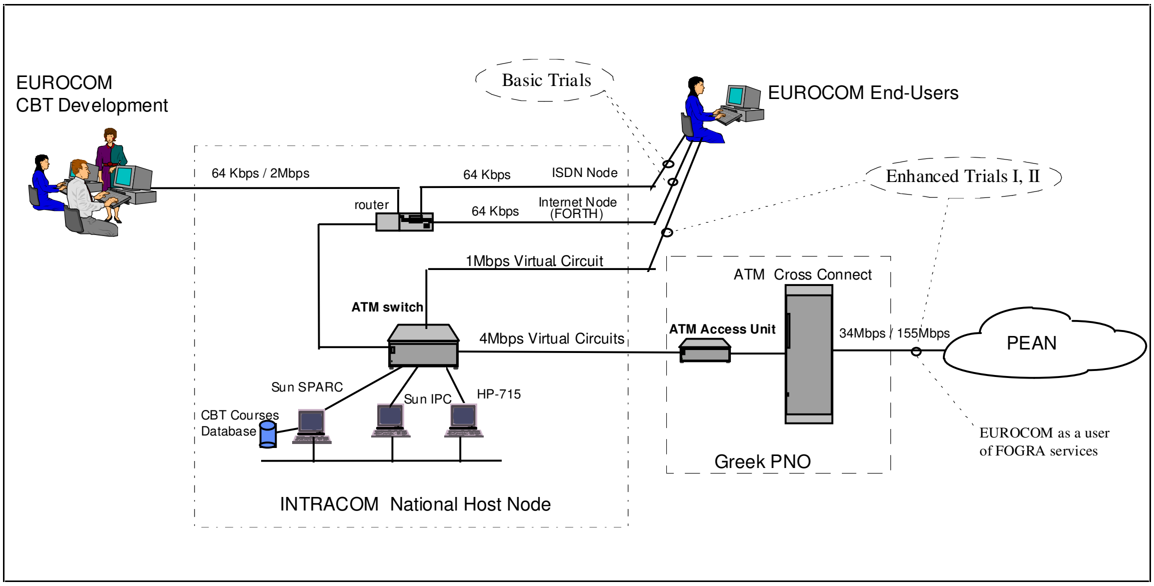
EUROCOM
CBT Development
Basic Trials
EUROCOM End-Users
64 Kbps / 2Mbps
64 Kbps
ISDN Node
Enhanced Trials I, II
router
64 Kbps
Internet Node
(FORTH)
1Mbps Virtual Circuit
ATM Cross Connect
ATM switch
4Mbps Virtual Circuits
ATM Access Unit
34Mbps / 155Mbps
PEAN
Sun SPARC
Sun IPC
HP-715
CBT Courses
Database
EUROCOM as a user
of FOGRA services
Greek PNO
INTRACOM National Host Node

Figure 5 Greek Trial Infrastructure

2.1.4.3 The German National Host Trial Infrastructure

The German part of the trials will be based on the Internet and the German National Host, especially the NH node at *GMD Darmstadt*, connected via PEAN to the Greek NH Hestia. Details on how the German NH can be used by *SEMPER* are described in Section 5.2.3.2.

The options for the consumer services that will build the German part of the trials are already shown in Figure 4. The details of how the service providers and users will access the trial infrastructure will be defined in the course of the project.

2.1.5 Evaluation of Results

The results of *SEMPER* will be evaluated *internally*

- by investigating the *security* of the architecture and services developed, based on state-of-the-art evaluation methods, tools, and guidelines; evaluation following ITSEC will be considered but is unlikely to be fully achievable within the project;
- by collecting and evaluating data on the *dependability* and *performance* of the services during the trials;
- by survey research on the *quality* and *acceptability* of trial services for users and service providers.

The evaluations will be published in a version that protects the IPRs and other commercial interests of the consortium.

2.1.6 Public Discussion and Dissemination of Results

Public discussion and the dissemination of results will be co-ordinated by Workpackage 4.3, "Dissemination of Results."

As a matter of principle, *SEMPER* aims at a maximum flow of information to the general and scientific public. This is the only way to obtain broad acceptance and public discussion of requirements, architecture, and services.

Results will be disseminated by

- means of a public FTP and WWW server on the Internet,
- regular press releases,
- publications and demonstrations at commercial and scientific conferences, exhibitions, and trade fairs, especially in the areas of networking, telecommunications, multi-media, and security.

A ***Special Interest Group on Secure Electronic Commerce*** will be established by *SEMPER*. This group will be open to all interested parties, and shall become a forum for discussion, co-ordination, and co-operation between the different projects and initiatives that deal with secure electronic commerce. Duplication of work will be prevented, especially within the different EU Programmes.

Input to standardisation will be provided via the consortium's representatives (see Section 1.3.3).

The consortium respects the national security concerns that pose specific requirements or restrictions on the application of cryptographic algorithms. The project will set-up a project internal clearing process for all publications, taking these concerns as well as the consortium's joint exploitation rights into account. As a matter of principle, the right to publish results should not be unreasonably withheld. The EU's *Senior Officials Group on Information Security* will be consulted with respect to the publication of security related material.

2.2 Work Breakdown Structure

Work in *SEMPER* will be structured along two dimensions:

- along a functional axis, work is divided into four core tasks (see Section 2.2.1, and for details Section 3 and 4).
- along a time axis, work is divided into three development and trial phases, described in more detail in Section 2.2.2.

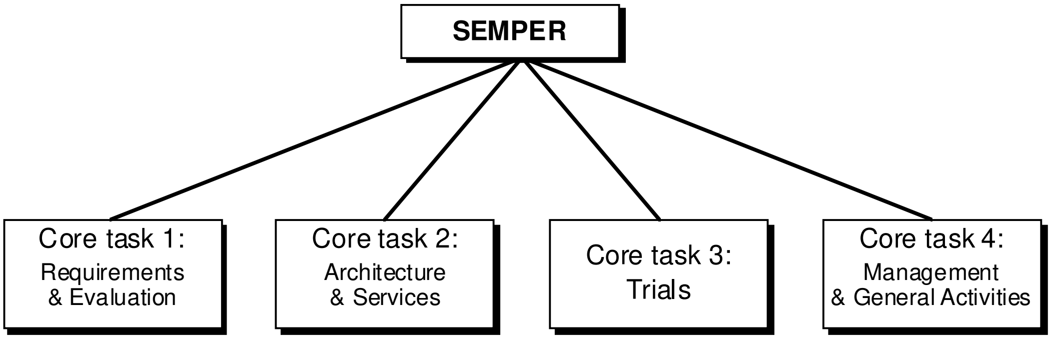

Figure 6 Core tasks of *SEMPER*

SEMPER will start September 1st, 1995 and will end December 31st, 1998.

2.2.1 Core Tasks

Work in *SEMPER* will be divided into four core tasks, CT1 - CT4 (see Figure 6). Each core task will consist of several workpackages, and each workpackage will consist of several activities.

The core tasks correspond almost exactly to Sections 2.2.1.2, 2.2.1.3, 2.2.1.4, with an additional core task responsible for management and general activities.

Core Task 1: Requirements and Evaluation

CT1 will be responsible for

- determining the European and international commercial, legal, and social requirements of an electronic marketplace;
- definition and evaluation of the trials conducted by CT3;
- positioning of the trials on the market.

Core Task 2: Architecture and Services

CT2 will be responsible for

- providing a survey of existing technology,
- defining a generic architecture of an electronic marketplace,
- identifying and specifying the necessary technical services,
- designing and implementing protocols that implement these services,
- providing resulting components to CT3,
- providing a security analysis of the resulting designs.

Core Task 3: Trials

CT3 will be responsible for the deployment of successive trials. There will be 3 trials, each building on the achievements and lessons of the preceding ones.

- All three trials will build up increasingly sophisticated consumer services defined by CT1 on the *Internet,* using an increasingly powerful electronic payment and commerce infrastructure provided by CT2.
- The trials in Year 2 and Year 3 will be performed on broadband testbeds provided by National Hosts. Consumer services will be enriched by multimedia information and the improved quality of service of the broadband communication network.

Each trial will include deployment of infrastructure, implementation of consumer services, integration of technical payment and commerce services, and operation of the trial itself.

For the management of applications during the trials, directory services (Yellow Pages, X.500) will be provided by the Greek National Host.

Core Task 4: Management, ACTS Liaison, and General Activities

CT4 will be responsible for

- project management and co-ordination,
- ACTS Liaison, interaction with other projects,
- dissemination of results, publications, and standardisation,
- management of a *Special Interest Group on Secure Electronic Commerce,*
- co-ordination of the production of *SEMPER*'s final report,
- IPR management for the consortium.

2.2.2 Development and Trial Phases

The work of Core Tasks 1-3 is divided into 3 phases, all following the same pattern of requirements analysis, specification, design, implementation, and trial, and each one corresponding to one project year, approximately (see Figure 7).

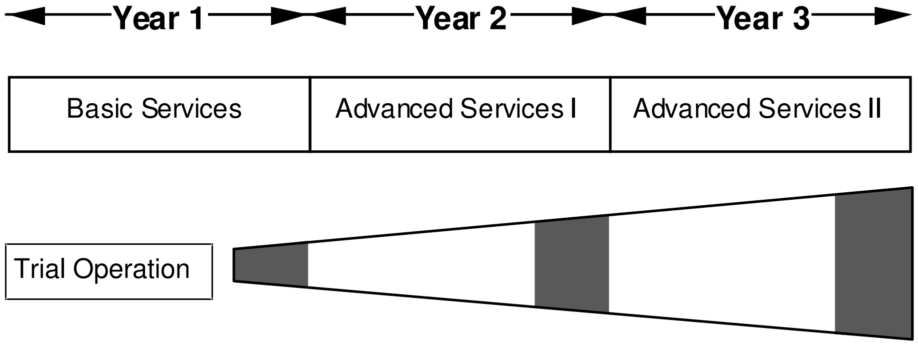

Figure 7 Basic time schedule. Grey boxes indicate the time of trial evaluation.

Phase 1: Basic Services

This will be the initial phase of the project, spanning the first year. The main result of this phase will be a model and architecture of an electronic marketplace, for both the technical services and the trial infrastructure, and a proof of concept by means of a first trial.

Technical services to be provided are those which are needed immediately to start electronic commerce. The exact selection of services will be done after a short initial requirements analysis and technology survey, but it is expected that most of the *basic technical services* mentioned in Section 2.1.3 will be part of Phase 1.

This first phase will involve a trial of basic services on the Internet. Evaluation of this first trial will last until the beginning of Year 2. For details on the contents of this and the following trials see Section 2.1.4.

The time allocated for Phase 1 is minimised in order to enable early visibility of *SEMPER*, and early exploitation of results. The tight time schedule will be met by using existing technology and results from earlier projects provided by members of the consortium.

Phase 2: Advanced Services I and Enhanced Trial I
Phase 3: Advanced Services II and Enhanced Trial II

These two phases will provide additional technical services, based on the list of advanced services in Section 2.1.3, and extensions and improvements of *SEMPER's* architecture.

There will be two trials in Phases 2 and 3. As already explained in Section 2.1.4, these trials will be based both on the Internet and on broadband networks provided by the German and Greek National Hosts, connected by a European backbone.

2.3 Interrelationship of Work Packages

The interrelationship of work packages is shown in Figure 8 (time).

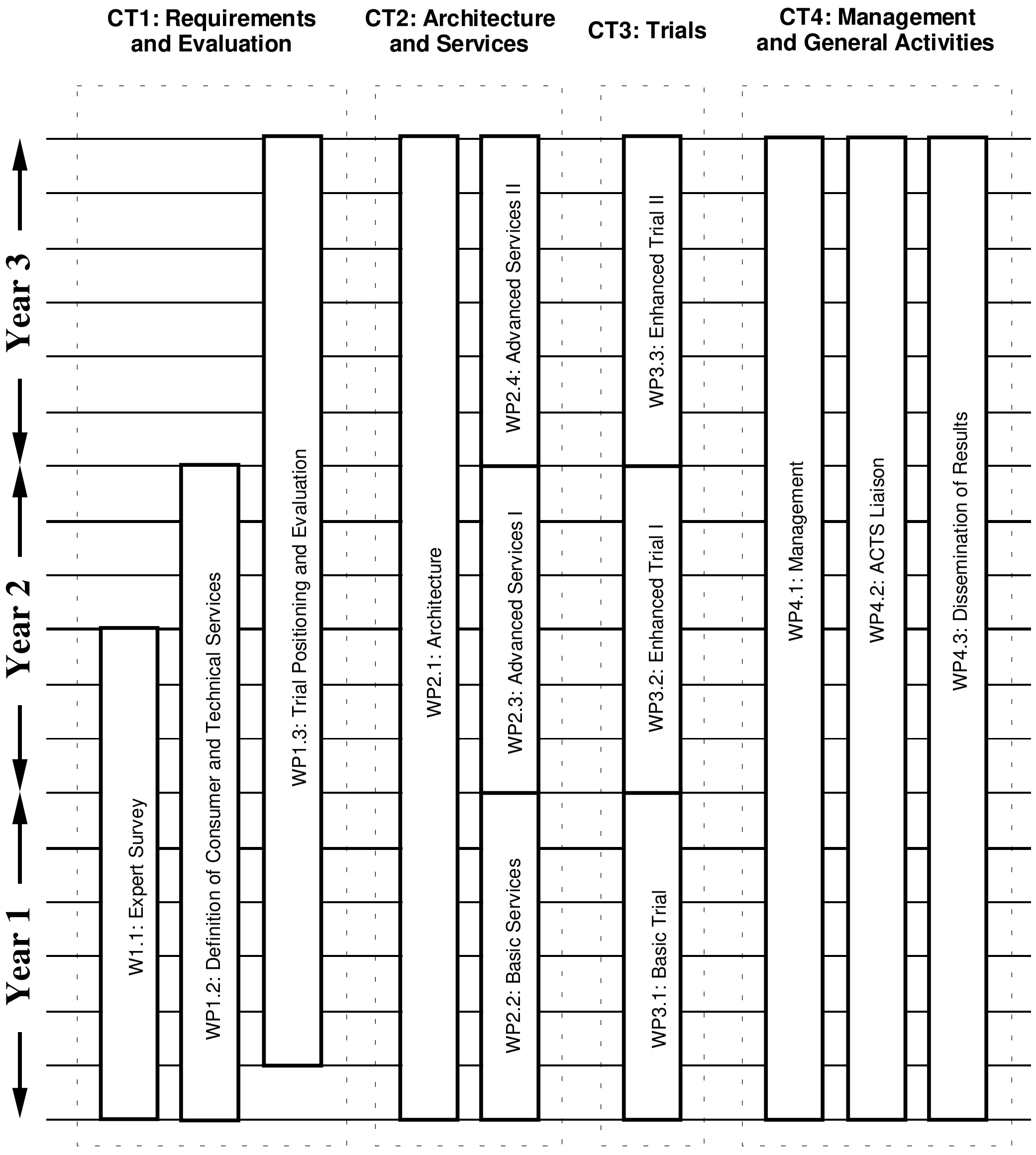
CT1: Requirements and Evaluation
CT2: Architecture and Services
CT3: Trials
CT4: Management and General Activities
Year 1
Year 2
Year 3
W1.1: Expert Survey
WP1.2: Definition of Consumer and Technical Services
WP1.3: Trial Positioning and Evaluation
WP2.1: Architecture
WP2.2: Basic Services
WP2.3: Advanced Services I
WP2.4: Advanced Services II
WP3.1: Basic Trial
WP3.2: Enhanced Trial I
WP3.3: Enhanced Trial II
WP4.1: Management
WP4.2: ACTS Liaison
WP4.3: Dissemination of Results

Figure 8 Interrelationship of Work Packages and Core Tasks

3 Overall Project Synthesis

3.1 Goal Description

Following the objectives listed in Section 1.1, the *main goals* of *SEMPER* are:

CT1: A detailed understanding of the requirements for electronic marketplaces, taking the results of the trials into account, and focusing on the European situation.

CT2: A generic architecture and a set of specifications, designs, and reference implementations for *basic* services for ordering, payment, and delivery of online information services, suitable for international standardisation and direct exploitation.

This is essential for openness and interoperability of the electronic marketplace. It is considered as the most important short-term result of *SEMPER* and should be achieved within the first project year.

A set of specifications, designs, and reference implementations for *advanced* services based on

- what is expected to be required by the market in the near future, and
- what is achievable based on current knowledge in security.

This is considered as the most important long-term result of *SEMPER*.

CT3: Live trials enabling electronic commerce in a secure way, based on the Internet and broadband networks.

CT4: Broad dissemination of the results of *SEMPER* and close coordination and cooperation among the different projects dealing with electronic commerce.

3.2 Workpackage Description

The following describes objectives, technical approaches, and results of all core tasks and workpackages of *SEMPER*.

Core task	Activity	Core Task Title
CT1		**Requirements and Evaluation**

Starting Event: Start of project.

Objectives:

- To establish general requirements from
  - consumers (private and business),
  - service providers such as merchants of goods, information providers (news and other contemporaneous information, databases and statistics, entertainment, consultancy, software),
  - financial sector,
  - legislation.
- To establish specific requirements for the trials, i.e., with regard to specific user and business requirements and with regard to technical conditions with the service providers and their users.
- To position the trials on the market.
- To evaluate the trials with respect to consumer experience, service providers' experience, and experiences of the financial sectors.

Technical Approach: All requirements shall be captured both internally to the consortium, and externally, which will be the larger part of the work. Internally means in particular collating the expertise in the consortium and having the service providers, retailers and the financial industry in the consortium define their requirements. Externally means interviewing experts not participating in the trials (general surveys), and users participating in the trials (trial surveying and evaluation). All surveys shall be made using topic guides and semi-standardized questionnaires in order to gain an in-depth understanding of requirements. Both the evaluation of the surveys and the requirements as defined by the service providers in the consortium shall lead to a non-technical definition of the services. In order to refine the requirements and to improve the definition, the survey and evaluation activities shall be repeated during the duration of the project.

Workpackages:

WP	Leader	Title	
1.1	FRE	Expert Surveys	M01-M18
1.2	FOG	Definition of Consumer and Technical Services	M01-M24
1.3	OTV	Trial Positioning and Evaluation	M03-M36

Duration: M01 - M36

Responsible Partner: FRE

Workpackage	Activity	Workpackage Title
WP1.1		**Expert Surveys**

Starting Event: Start of project.

Objectives: To gather requirements on an electronic marketplace from potential consumers, from service providers and retailers, and from the legal and finance sector. To identify the legal requirements on electronic signatures and other means of authentication in the EU. To identify the legal requirements for privacy protection in the EU. To identify the legal requirements for multi-party security in the EU. To evaluate the usability of existing partial solutions (as discussed in Section 1.3.1) for electronic offering, ordering, payment, and delivery.

Technical Approach: This workpackage will complement the technical surveys of WP2.1. Requirements will be gathered by means of limited scale survey research and expert interviews. Appropriate groups of consumers and experts will be identified on a European scale. Interviews will be based on topic guides and semi-standardised questionnaires.

Duration: M01 - M18

Results:

R1.1.1	Requirements from General Expert Survey (Draft M09)	M12	RI
R1.1.2	Refined Requirements from General Expert Survey	M18	RI

Responsible Partner: FRE

Workpackage	Activity	Workpackage Title
WP1.2		**Definition of Consumer and Technical Services**

Starting Event: Start of project

Objectives: To define the consumer and technical services to be used for the trials (see Section 2.1.2). To review the architecture and specifications of CT2 against these requirements.

Technical Approach: For the first, rapid definition of the Basic Trial, requirements and services will be defined by a number of internal meetings. Later updates will take the surveys of WP1.1 and the results of the trial evaluations into account.

Duration: M01 - M24

Results:

R1.2.1	Definition of Consumer and Technical Services	M03	RI
R1.2.2	Refined Definition of Consumer and Technical Services (Draft)	M12	RI
R1.2.3	Refined Definition of Consumer and Technical Services	M15	RI
R1.2.4	Revised Definition of Consumer and Technical Services (Draft)	M24	RI

Responsible Partner: FOG

Workpackage	Activity	Workpackage Title
WP1.3		**Trial Positioning and Evaluation**

Starting Event: Finalisation of A1.3.1

Objectives: To position the trials on the market. To define evaluation criteria for the trials. To evaluate the trials.

Technical Approach: For the positioning of the trials on the market appropriate tools have to be developed. This can be based on the requirements and the specifications defined before. Tools may be appropriate online advertising or consumer leaflets, etc. Evaluation criteria and questionnaires will have to be developed. Service providers and consumers shall be interviewed. The providers of the new consumer services will evaluate their experiences, too. The evaluations are to be repeated each year. They will cover the business, the organisational and the technical level. The evaluation will also consider the data on the technical performance as gathered by CT3. The output of the evaluations is expected to be used to update the definitions produced by WP1.2.

Duration: M01 - M36

Results:

R1.3.1	Evaluation of Basic Trial	M12	RI
R1.3.2	Evaluation Enhanced Trial I	M24	RI
R1.3.3	Evaluation Enhanced Trial II	M36	RI

Deliverables: WP1.3 will be responsible for the deliverables

D05	First Year Surveys and Evaluation	M12	RP
D09	Second Year Surveys and Evaluation	M24	RP
D12	Third Year Surveys and Evaluation	M36	RP

Responsible Partner: OTV

Core Task	Activity	Core Task Title
CT2		**Architecture and Services**

Starting Event: Start of project.

Objectives: To produce a coherent model and a generic, open architecture of an electronic marketplace, independent of specific hardware, software, and network architectures, and satisfying the requirements defined by CT1. To specify, design, and evaluate basic and advanced services enabling electronic commerce, as described in Section 2.1.3. To implement these services and deliver them to CT3 for integration in the trials.

Technical Approach: See Section 2.1.3.

Workpackages:

WP	Leader	Title	
2.1	R3S	Architecture	M01-M36
2.2	CRM	Basic Services	M01-M12
2.3	HIL	Advanced Services I	M13-M24
2.4	KPN	Advanced Services II	M25-M36

Duration: M01 - M36

Responsible Partner: CRM

Workpackage	Activity	Workpackage Title
WP2.1		**Architecture**

Starting Event: Start of project

Objectives: To produce a uniform model and a generic architecture of an electronic marketplace including the connection to existing payment systems. To select the services that will be developed by WP2.2, WP2.3, and WP2.4.

Technical Approach: A technical survey on architectures, services, designs, and implementations in relation to electronic marketplaces and existing payment systems will be performed. Relevant classes of technical services, their functional and security properties and their design and implementation options will be identified, and assigned to the three sets of services "Basic Services," "Advanced Services I," and "Advanced Services II." The existing technology will be evaluated with regard to their usability. Based on the consortium's expertise, methodologies for specification, design, implementation, evaluation, and quality control will be selected.

A generic system model and a generic system architecture will be specified which include all identified services as well as enables the addition of any further services later.

Model and architecture will be continuously refined and adapted, with main reviews after each year.

Duration: M01 - M36

Results:

R2.1.1	Survey on Basic Services and Report on Methodology	M03	RI
R2.1.2a	Informal Specification of Basic Services	M04	SI
R2.1.2b	Initial Model and Architecture (Draft M04)	M12	RI
R2.1.3	Survey on Advanced Services I	M12	RI
R2.1.4a	Informal Specification of Advanced Services I	M13	SI
R2.1.4b	Refined Model and Architecture (Draft M15)	M24	RI
R2.1.5	Survey on Advanced Services II	M24	RI
R2.1.6a	Informal Specification of Advanced Services II	M25	SI
R2.1.6b	Final Model and Architecture (Draft M27)	M36	RI

Responsible Partner: R3S

Workpackage	Activity	Workpackage Title
WP2.2		**Basic Services**

Starting Event: Start of project.

Objectives: To specify, design, implement, and evaluate a set of Basic Services that are absolutely necessary for electronic commerce. This set will include (see Section 2.1.3)

- local access control and audit functions,
- set-up of the necessary security management functions,
- initialisation of the necessary trust relations, especially by means of public-key certification,
- negotiation of type and quality of technical services,
- communication security,
- electronic payment, including the link to the existing financial systems.

Technical Approach: Design, implementation, integration, and evaluation based on results of WP2.1 and already existing tools and services. The organisation of the design and evaluation activities will ensure the disjointness of designer groups and evaluator groups for all services.

Duration: M01 - M12

Results:

R2.2.1	Specification of Basic Services	M06	SI
R2.2.2	Design of Basic Services	M08	SI
R2.2.3	Implementation of Basic Services	M09	PI
R2.2.4	Security Evaluation of Basic Services	M12	RI

Deliverables: WP2.2 will be responsible for the deliverables

D02	Preliminary Report on Basic Services Architecture and Design	M06	RP
D03	Basic Services Architecture and Design	M12	SP

Responsible Partner: CRM

Workpackage	Activity	Workpackage Title
WP2.3		**Advanced Services I**

Starting Event: Finalisation of WP2.2.

Objectives: To improve the Basic Services developed by WP2.2. Multi-party security and anonymity requirements, media-specific extensions (e.g., metering as a basis for billing), and results of the Basic Trial should be taken into account.

To develop a first set of Advanced Services I. The contents of this set will be defined as described in WP2.1 (see description of WP2.1), by the end of Year 1.

The set should include services from the following two service classes, resulting in ***Advanced Notary Services:***

- *Class 1:* Secure document processing, e.g.,
  - Certified Mail
  - Anonymous Mail
  - Archived Mail
  - Management of (unlinkable) credentials
- *Class 2:* Fair Exchange of Documents, e.g.,
  - Simultaneous exchange of goods and money
  - Contract signing.

To develop protocols for the complete *online* arbitration of disputes between commerce partners.

The set should also include services for

- media-dependent protection of copyright,

dependent on the requirements provided by CT1 and the technical feasibility.

To provide a security evaluation of developed services.

Technical Approach: Design, implementation, integration, and evaluation based on results of earlier workpackages, and already existing tools and services. The organisation of the design and evaluation activities will ensure the disjointness of designer groups and evaluator groups for all services.

Duration: M13 - M24

Results:

R2.3.1	Specification of Advanced Services I	M15	SI
R2.3.2	Design of Advanced Services I	M20	SI
R2.3.3	Implementation of Advanced Services I	M21	PI
R2.3.4	Security Evaluation of Advanced Services I	M24	RI

Deliverables: WP2.3 will be responsible for the deliverables

D06	Preliminary Report on Advanced Services I Architecture and Design	M18	RP
D07	Advanced Services I Architecture and Design	M24	SP

Responsible Partner: HIL

Workpackage	Activity	Workpackage Title
WP2.4		**Advanced Services II**

Starting Event: Finalisation of WP2.3.

Objectives: To improve the services developed by WP2.2 and WP2.3, based on the results of the Basic Trial and the Enhanced Trial I.

To develop a set of Advanced Services II. The contents of this set will be defined as described in WP2.1 (see description of WP2.1), by the end of Year 2.

To develop services for electronic voting, bidding, and opinion research, dependent on the requirements provided by CT1 and the technical feasibility, resulting in ***Advanced Multi-party Services.***

To provide a functional and security evaluation of developed services.

Technical Approach: Design, implementation, integration, and evaluation based on results of earlier workpackages, and already existing tools and services. The organisation of the design and evaluation activities will ensure the disjointness of designer groups and evaluator groups for all services.

Duration: M25 - M36

Results:

R2.4.1	Specification of Advanced Services II	M27	SI
R2.4.2	Design of Advanced Services II	M32	SI
R2.4.3	Implementation of Advanced Services II	M33	PI
R2.4.4	Security Evaluation of Advanced Services II	M36	RI

Deliverables: WP2.4 will be responsible for the deliverables

D10	Advanced Services II Architecture and Design	M36	SP

Responsible Partner: KPN

Core Task	Activity	Core Task Title
CT3		**Trials**

Starting Event: Start of project

Objectives: The objective of Core Task 3 is to define, implement, and support trials that will take place throughout the project on the Internet and broadband networks.

Technical Approach: Work from each trial to the next in two directions:

- by building up the set of supported services using increasingly sophisticated secure payment and electronic commerce services from CT2,
- by porting the resulting trials from an initial trial phase to a later broadband base.

Each trial will include deployment of the infrastructure, implementation of consumer services, integration of technical services from CT2, and conduction of the trial.

Workpackages:

WP	Leader	Title	
3.1	IBM	Basic Trial	M01-M12
3.2	INC	Enhanced Trial I	M13-M24
3.3	GMD	Enhanced Trial II	M25-M36

Duration: M01 - M36

Responsible Partner: INC

Workpackage	Activity	Workpackage Title
WP3.1		**Basic Trial**

Starting Event: Start of project

Objectives: To integrate existing tools and technologies with new components developed by WP2.2 to provide a basic service offering on the Internet.

To set up and run a trial of the basic services for the secure offering, ordering, and payment of goods, services, and information across the European Union.

To select the communication infrastructure that will be used for the Enhanced Trial I.

Technical Approach: The trial infrastructure will be build by integrating existing technology components wherever possible to achieve rapid delivery. The approach will include integration of the offering (goods, services, information) of the consumer service providers and the payment system providers. The basic trial will be based on the Internet.

Criteria for the selection of the communication infrastructure for the Enhanced Trial I will be defined according to the results of the surveys of WP1.1, the communication requirements of the consumer services as defined by WP1.2, and the technical services as defined by WP1.2 and developed by WP2.2. The actual choice will be based on the service offerings of the German and Greek National Hosts, and the National Hosts interconnection backbone. Since the Internet is considered as the prime medium for electronic commerce, Internet will be part of this infrastructure.

Duration: M01 – M12

Results: An Internet based live trial enabling wholly electronic offering, ordering, and payment of goods, services, and information in a secure way.

R3.1.1a	Specification of the Basic Trial	M09	SI
R3.1.1b	Specification of Basic Trial Environment	M09	SI
R3.1.1c	Implementation of Basic Trial Environment	M09	PI
R3.1.1d	Selection of the Infrastructure for Enhanced Trials I	M12	RI
R3.1.2	Available Consumer Services for the Basic Trial	M09	RI
R3.1.3	First prototype for Basic Trial	M09	PI
R3.1.4	Basic Trial in Operation	M12	RP

Deliverables: WP3.1 will be responsible for Deliverable

D04	Basic Services Prototype and Internet Trial	M12	PP

The consortium will be prepared to demonstrate the trials and prototypes to other programme participants on request.

Responsible Partner: IBM

Workpackage	Activity	Workpackage Title
WP3.2		**Enhanced Trial I**

Starting Event: Finalisation of WP3.1.

Objectives: To implement additional consumer services, supplementing those from WP3.1, based on the infrastructure selected by WP3.1. The new consumer services exploit the Advanced Services I as provided by WP2.3; the design and specification will be based on the definition of the trials provided by WP1.2.

To set up and run a trial of these advanced consumer services across the European Union.

Technical Approach: The first activity of this workpackage will accommodate the appropriate setting of the communication infrastructure as selected by WP3.1. The Basic Services will be adapted so as to take full advantage of the available bandwidth. The new consumer services are merged into the existing implementation of WP3.1, using the tools and services delivered by WP2.3. Again, this will include integration with the offerings of the service providers and the payment system providers.

The selection of the communication infrastructure will be revised based on the experience from the Basic Trial and the Enhanced Trial I.

Duration: M13 - M24

Results: A live trial enabling wholly electronic advanced consumer services in a secure way.

R3.2.1a	Specification of the Enhanced Trial I	M21	SP
R3.2.1b	Specification of Enhanced Trial I Environment	M21	SI
R3.2.1c	Implementation of Environment for the Enhanced Trial I	M21	PP
R3.2.1d	Selection of the Infrastructure for Enhanced Trials II	M24	RI
R3.2.2	Available Consumer Services for the Enhanced Trial I	M21	RP
R3.2.3	First prototype for Enhanced Trial I	M21	PP
R3.2.4	Enhanced Trial I in Operation	M24	RP

Deliverables: WP3.2 will be responsible for Deliverable

D08	Advanced Services I Prototypes and Trials	M24	PP

The consortium will be prepared to demonstrate the trials and prototypes to other programme participants on request.

Responsible Partner: ICOM

Workpackage	Activity	Workpackage Title
WP3.3		**Enhanced Trial II**

Starting Event: Finalisation of WP3.2.

Objectives: To implement additional consumer services, supplementing those from WP3.2. These new consumer services exploit the Advanced Services II as provided by WP2.4; the design and specification will be based on the definition of the trial provided by WP1.2.

Technical Approach: The new consumer services are merged into the existing implementation of WP3.2, using the tools and services delivered by WP2.4. Again, this will include integration with the offerings of the Service Providers and the payment system providers.

Duration: M25 - M36

Results: A European-wide secure electronic marketplace, enabling the full employment of services developed by CT2.

R3.3.1a	Specification of the Enhanced Trial II	M33	SP
R3.3.1b	Specification of Enhanced Trial II Environment	M33	SI
R3.3.1c	Implementation of Environment for Enhanced Trial II	M33	PP
R3.3.2	Available Consumer Services for the Enhanced Trial II	M33	RP
R3.3.3	First prototype for Enhanced Trial II	M33	PP
R3.3.4	Enhanced Trial II in operation	M36	RP

Deliverables: WP3.3 will be responsible for Deliverable

D10	Advanced Services II Prototypes and Trials	M36	PP

The consortium will be prepared to demonstrate the trials and prototypes to other programme participants on request.

Responsible Partner: GMD

Core Task	Activity	Core Task Title
CT4		**Management and General Activities**

Starting Event: Start of project

Objectives:

- Ensure management of the project and relationship with the Commission.
- Contribute to the general activities of ACTS.
- Co-ordinate the dissemination of results of the project, and co-ordinate between *SEMPER* and related projects and efforts.

Technical Approach: CT4 is decomposed into 3 workpackages, each one corresponding to the above objectives.

Workpackages:

WP	Leader	Title	
4.1	IBM	Project Management	M01-M36
4.2	IBM	ACTS Liaison	M01-M36
4.3	ZRL	Dissemination of Results	M01-M36

Duration: M01 - M36

Responsible Partner: IBM

Workpackage	Activity	Workpackage Title
WP4.1		**Project Management**

Starting Event: Start of Project

Objectives:

- Manage the project and control its progress, in particular by ensuring:
  - Administrative and contract relationship inside the project;
  - Administrative and contract relations with the Commission;
  - Progress control of project, according to workplan;
  - Financial issues (e.g., Cost Statements)
- Manage the production of the Annual Review Reports (ARRs)
- Co-ordinate the production of the Final Report

Technical Approach:

- Management of project and ARRs production is performed following the approach specified in Section 5 hereafter in this document.
- WP4.1 will co-ordinate the production of the Final *SEMPER* Report (Deliverable D13).

Duration: M01 - M36

Results:

- Monthly Control Reports
- ARRs

R4.1.1	Internal Final *SEMPER* Report	M36	RI
D01	Project Linkages	M01	RP
D13	Final *SEMPER* Report	M36	RP

Deliverable D01 will describe the expected relations and identified dependencies to other projects in the ACTS Programme or other EU programmes. Since D01 is scheduled for the first month, the descriptions must be a preliminary and incomplete; if necessary, D01 will be updated in the course of the project. *SEMPER* aims at co-ordinating the efforts of the different European projects dealing with security aspects of electronic commerce. D01 will describe how *SEMPER* will achieve this goal, and will provide a proposal for a *Special Interest Group on Secure Electronic Commerce*.

The final Deliverable D13 will summarise the work performed in the project since its beginning, and will give a complete review of the results obtained, put in perspective with the objectives of the project and the objectives of Task AC503 of the ACTS workplan. This document will be the integration of the information produced by the related activities of Core Tasks CT1, CT2 and CT3. It will also include the exploitation plan/questionnaire as required by the Commission.

It is anticipated that this D13 will be public. If it appears that confidential information needs to be included in the document for completeness, it will be placed in a separate annex for restricted distribution.

Responsible Partner: IBM

Workpackage	Activity	Workpackage Title
WP4.2		**ACTS Liaison**

Starting Event: Start of Project

Objectives: Contribute to the general activities of ACTS, in particular

- ACTS concertation mechanism (e.g., ACTS Concertation Meetings, Special Interest Groups)
- Consensus building (e.g., CFSs and CPRs)
- Direct input to Horizontal Actions in a form to be defined by projects supporting Tasks 703, 704 and 705.

Technical Approach: The technical approach cannot be defined at this stage, as the general activities of ACTS and the workplan of projects supporting the consensus management (CFSs, CPRs) and supporting the horizontal actions tasks is not known yet. The necessary technical resources to support the technical activities of WP4.2 will be drawn, as required, from the resources allocated to the technical core tasks (CT1, CT2, and CT3). The resources allocated to WP4.2 in Forms M4C are those estimated absolutely necessary to ensure the co-ordination of the technical activities of the workpackage, and the contribution to the ACTS concertation meetings, assuming an organisation similar to RACE.

Duration: M01 - M36

Results: To be defined at a later stage, when the ACTS general activities and Horizontal Actions will be operational.

Responsible Partner: IBM

Workpackage	Activity	Workpackage Title
WP4.3		**Dissemination of Results**

Starting Event: Start of Project

Objectives: To ensure and co-ordinate the information flow inside the project as well as the dissemination of results to the general and scientific public. To provide input to standardisation bodies. To initialise and manage a *Special Interest Group on Secure Electronic Commerce (SIG-SEC).*

Technical Approach: As described in Section 2.1.6 and Section 5. Internal communication will use electronic mail, an FTP repository, and a WWW server on the Internet, accessible for members of the *SEMPER* consortium only.

Dissemination of results to the general and scientific public will be achieve by

- means of a public FTP repository and a public WWW server on the Internet,
- regular press releases,
- publications and demonstrations at commercial and scientific conferences and exhibitions, especially in the areas of networking, telecommunications, multi-media, and security,
- input to standardisation bodies via representatives of the consortium partners,
- the SIG-SEC.

Duration: M01 - M36

Results:

R4.3.1	Management Proposal "SIG on Secure Electronic Commerce"	M01	RP
R4.3.2	First Year Dissemination of Results and the SIG-SEC	M12	RP
R4.3.3	Second Year Dissemination of Results and the SIG-SEC	M24	RP
R4.3.4	Third Year Dissemination of Results and the SIG-SEC	M36	RP

R4.3.1 will provide input to Deliverable D01, "Project Linkages." No formal deliverable is produced by this workpackage, however, the Annual Review Reports and the Final Report will contain a list of the published papers, a summary of their content and information about the reaction of the audience and more frequent questions asked. In the case of demonstrations, their existence will be made known to the ACTS community at the Concertation Meetings. The consortium will be ready to organise, on a case by case basis, special sessions for interested ACTS projects or ACTS Commission's Officers.

Details concerning contribution to standards will be given in Annual Review Reports and the Final Report.

Responsible Partner: ZRL