© SEMPER 4.10.96

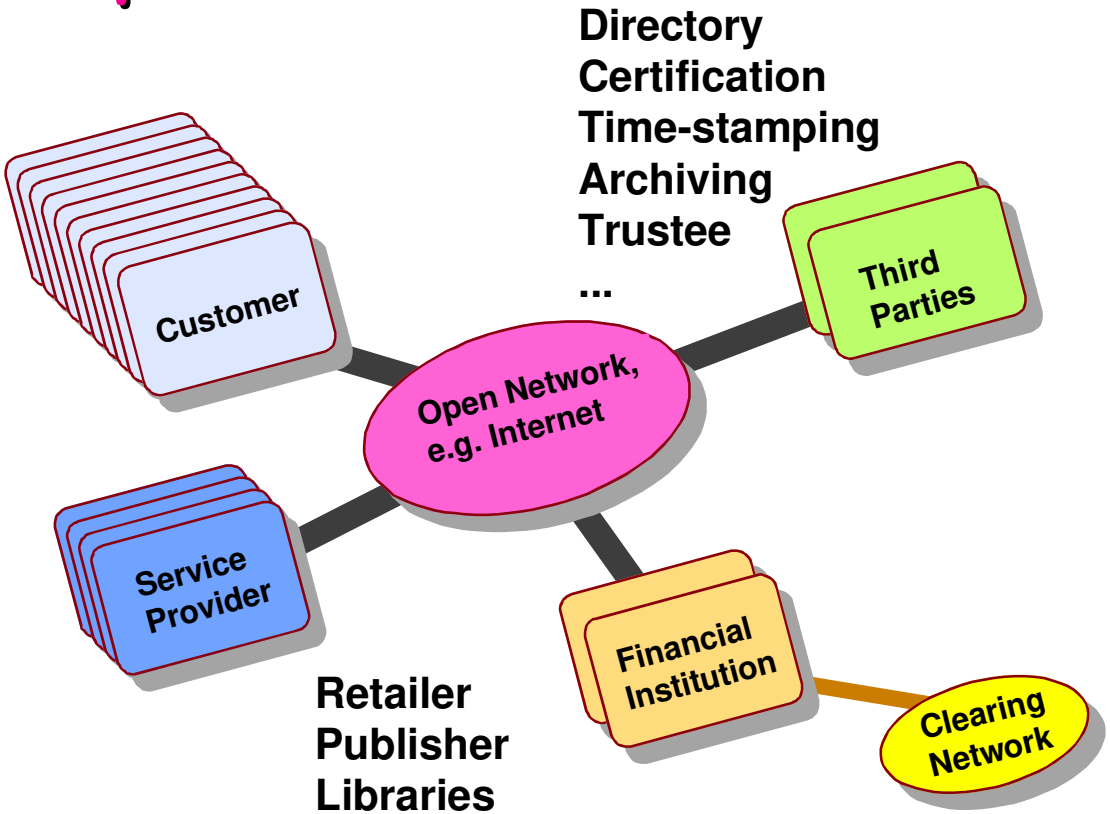
Overview

Michael Waidner, IBM Zurich Research Laboratory
CH 8803 Rüschlikon, Switzerland
Ph. +41 1 724 8220 • Fax +41 1 710 3608 • <wmi@zurich.ibm.com>
<http://www.semper.org> • <http://www.zurich.ibm.com/~wmi>

© SEMPER 4.10.96

Electronic Marketplace

- Mail Order Retailing
- Information Broker
- Contract Signing
- Subscriptions
- Insurances
- Auctioning
- Ticketing
- Document Transfer, Email
- Online Purchase of Information

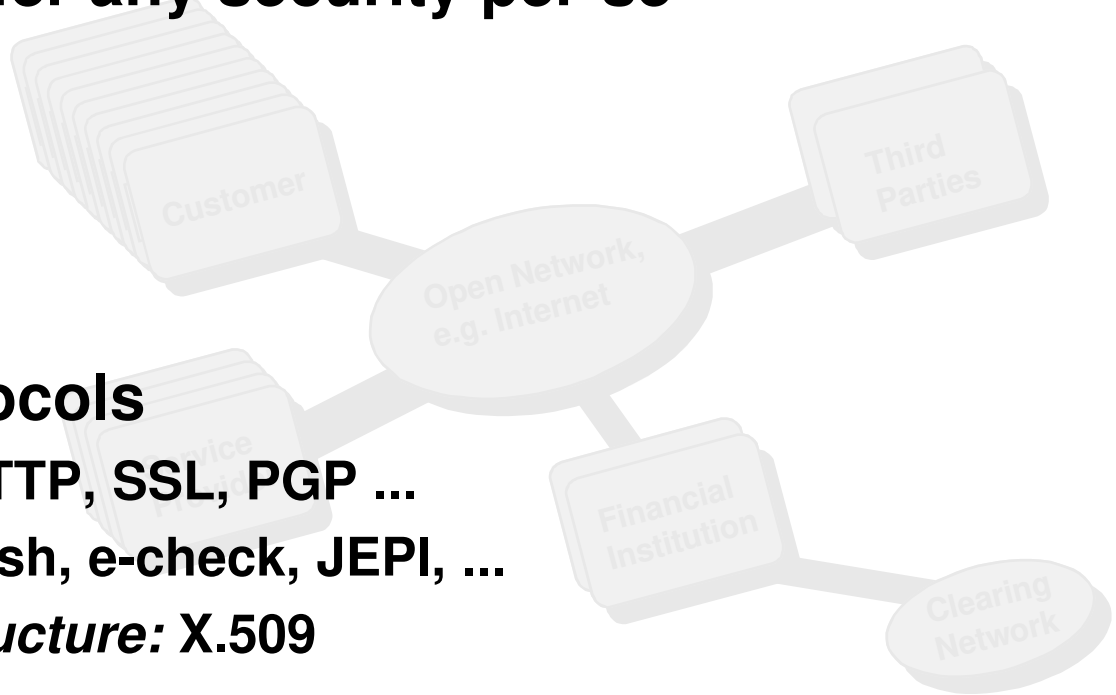


© SEMPER 4.10.96

Electronic Marketplace “Internet & WWW”

Internet does not offer any security per-se

- *No* integrity
- *No* authentication
- *No* confidentiality



Standards and protocols

- *Communication:* SHTTP, SSL, PGP ...
- *Payments:* SET, e-cash, e-check, JEPI, ...
- *Certification infrastructure:* X.509

Various closed or proprietary systems

© SEMPER 4.10.96

What is Missing?

No coherent model or architecture, few standard API's

- closed, proprietary, not publicly specified & verifiable solutions
- limited interoperability, extensibility
- often 2-party master-slave models: no multi-party protocols

Most technology developed by US-based projects

- US export regulations for cryptographic systems (treated as "munition")
- Designed for *domestic* market with *one* currency, *one* legislation, etc.

Limited scope of solutions

- Only "shopping" is supported: what about notaries, contract signing, fair exchanges, auctioning, etc.?
- *Multi-party* security often not supported
- Missing support for *decision procedures* or *dispute handling*
- Customer *privacy* not sufficiently considered yet
- No support for secure hardware (smartcards, wallets, etc.)

© SEMPER 4.10.96

Secure Electronic Marketplace for Europe

- Complete Picture: *electronic commerce*...
  - needs a coherent *model* and *architecture* that covers all aspects
  - must satisfy the requirements of *all* parties
  - is more than just “electronic payment”
  - is inherently *global*, not domestic
- Open Architecture for Secure Electronic Commerce
  - independent of specific hardware, systems, networks
  - independent of specific components and products
  - independent of specific business applications
- Open Design
  - public design and security evaluation
  - input to standardisation

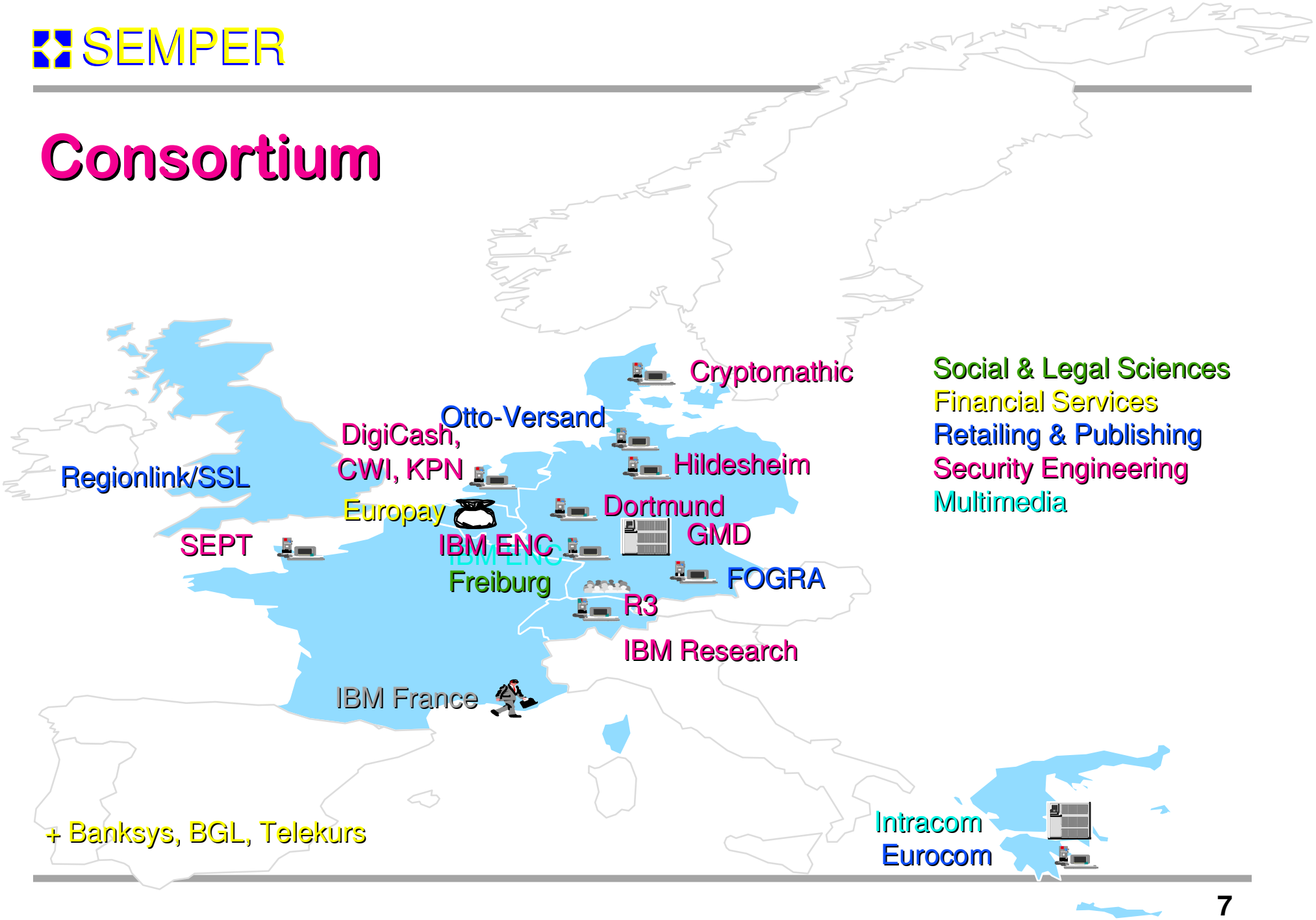
© SEMPER 4.10.96

Organisation

- 4th Framework of the EU: ACTS AC026
- Budget of 9 MECU (14 M CHF)
- Funding 50% EU & Switzerland, 50% partners
- September 1995 - August 1998
- Consortium of 20 partners from 8 European countries

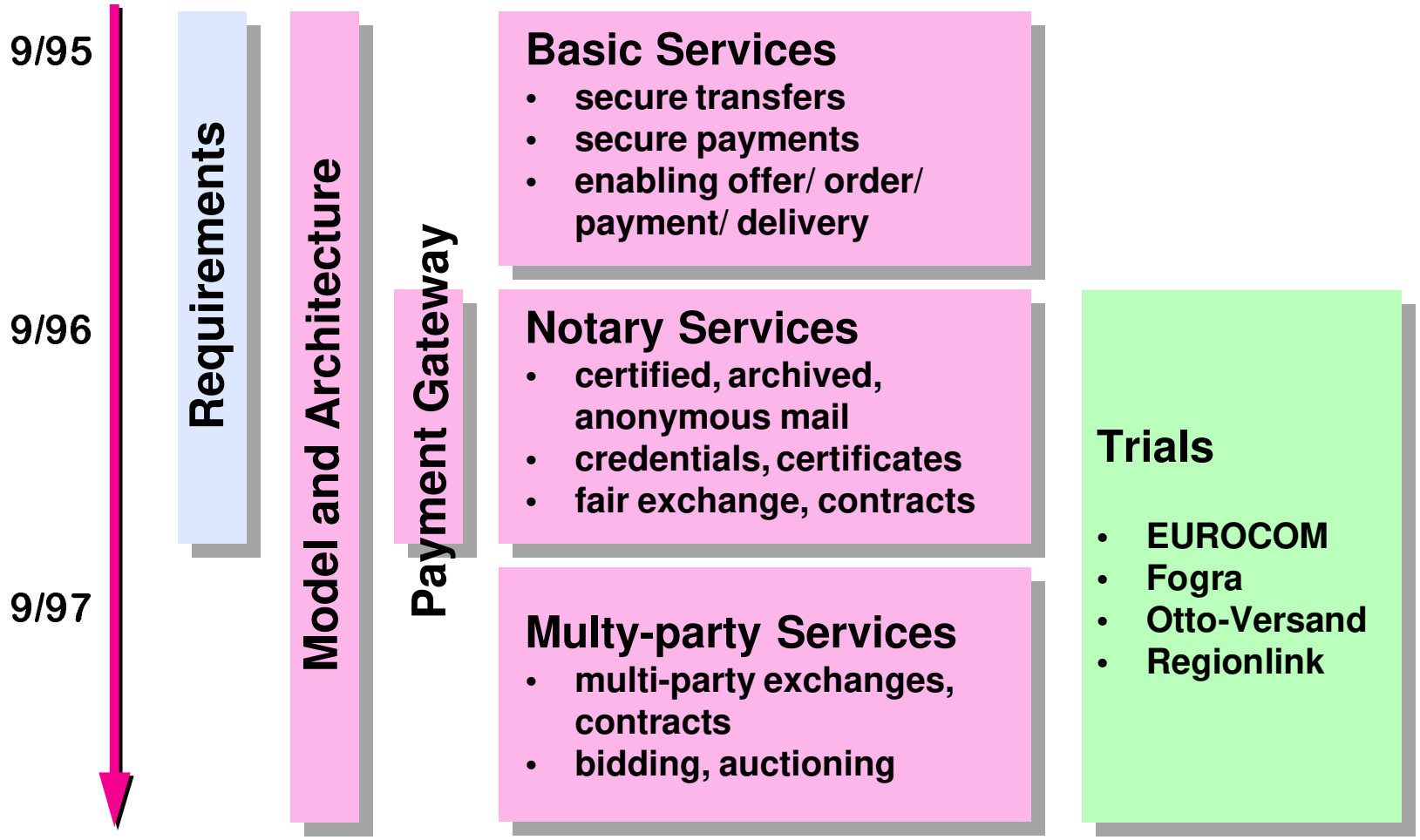
© SEMPER 4.10.96

Consortium



© SEMPER 4.10.96

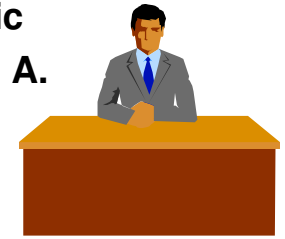
Time Schedule



© SEMPER 4.10.96

Model

- Notary Public
- Certification A.
- “Bank,” etc.



Third Parties

Customer

Certificates

Certificates

Signed Offer

Signed Order

Fair Contract Signing

Fair Payment for Receipt

Delivery

Merchant

Dispute Handling

© SEMPER 4.10.96

Basic Architecture

Customer

Merchant

Any WWW Browser

Any WWW Server

Generic Client Business Application

SEMPER

Generic Server Business Application

SEMPER

Certificates

Certificates

Signed Offer

Signed Order

Fair Contract Signing

Fair Payment for Receipt

Delivery

© SEMPER 4.10.96

Basic Architecture

Customer

Any WWW Browser

Generic Client Business Application

SEMPER

Certif
Certif
Signe
Signe
Fair Contra
Fair Paymer
Deli

- User Requirements for Electronic Commerce; *Ingo Saleck, Otto-Versand*
- Electronic Means of Payment; *John West, Europay International*
- Security Architecture; *Torben Pedersen, Cryptomathic*
- Trials and Prototype; *Maria Tsakali, INTRACOM*
- Demonstration of the SEMPER Prototype; *Dimitri Livas, EUROCOM*