© IBM 4.10.96 <wmi@zurich>



# Development of a Secure Electronic Marketplace for Europe

**M. Waidner**
**IBM Zurich Research Laboratory**
**CH 8803 Rüschlikon/Switzerland**
**Ph. +41 1 724 8220 • Fax +41 1 710 3608**
**<wmi@zurich.ibm.com>**

© IBM 4.10.96 <wmi@zurich>



# Outline

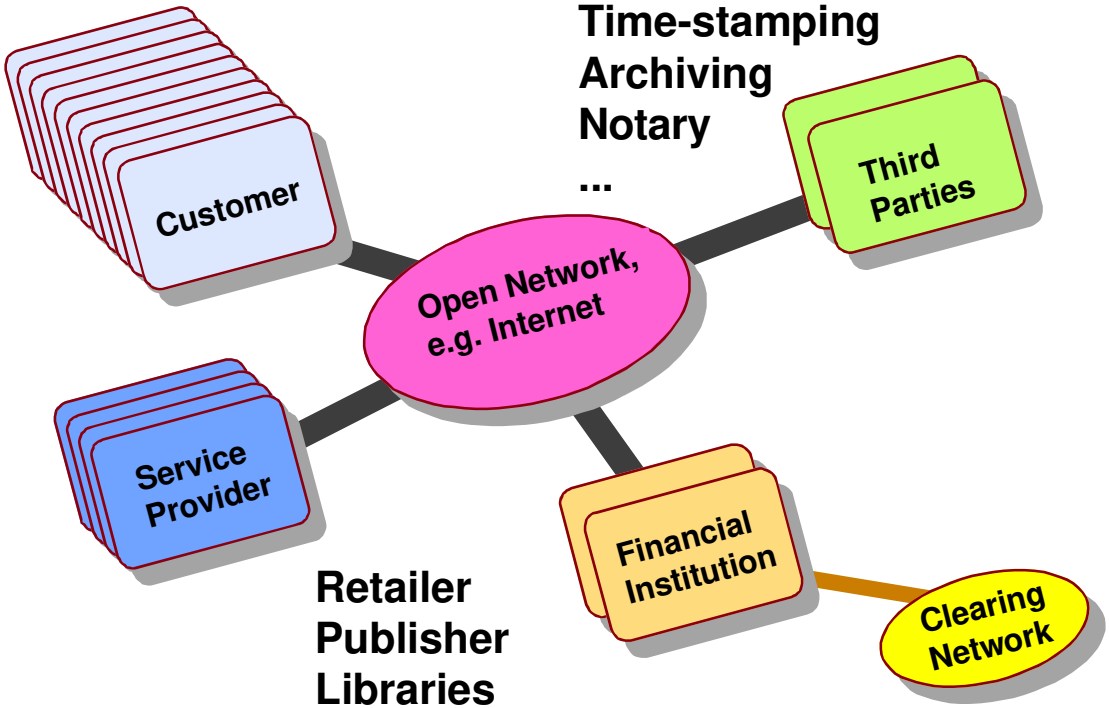
- Motivation: The Electronic Marketplace
- Project Overview
- Architecture
  - Overview
  - Trusted Interactive Graphical User Interface
  - Payment Block
- Trials
- Summary

© IBM 4.10.96 <wmi@zurich>



# Electronic Marketplace

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



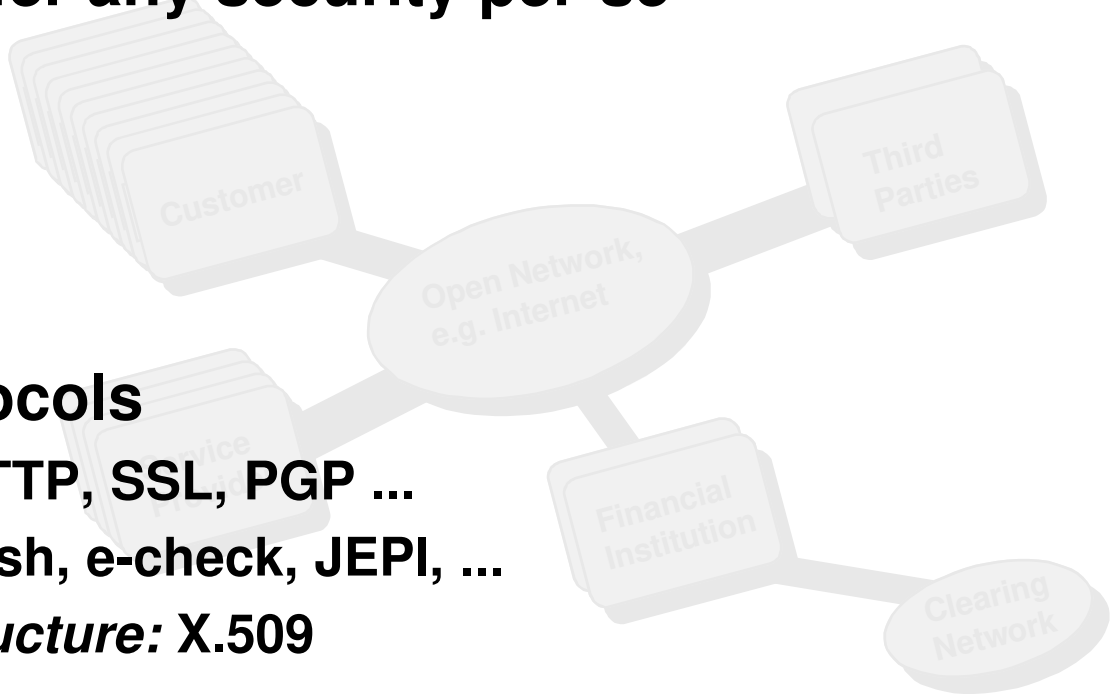
© IBM 4.10.96 <wmi@zurich>



# 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

© IBM 4.10.96 <wmi@zurich>



# 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.)

© IBM 4.10.96 <wmi@zurich>



# 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**

© IBM 4.10.96 <wmi@zurich>



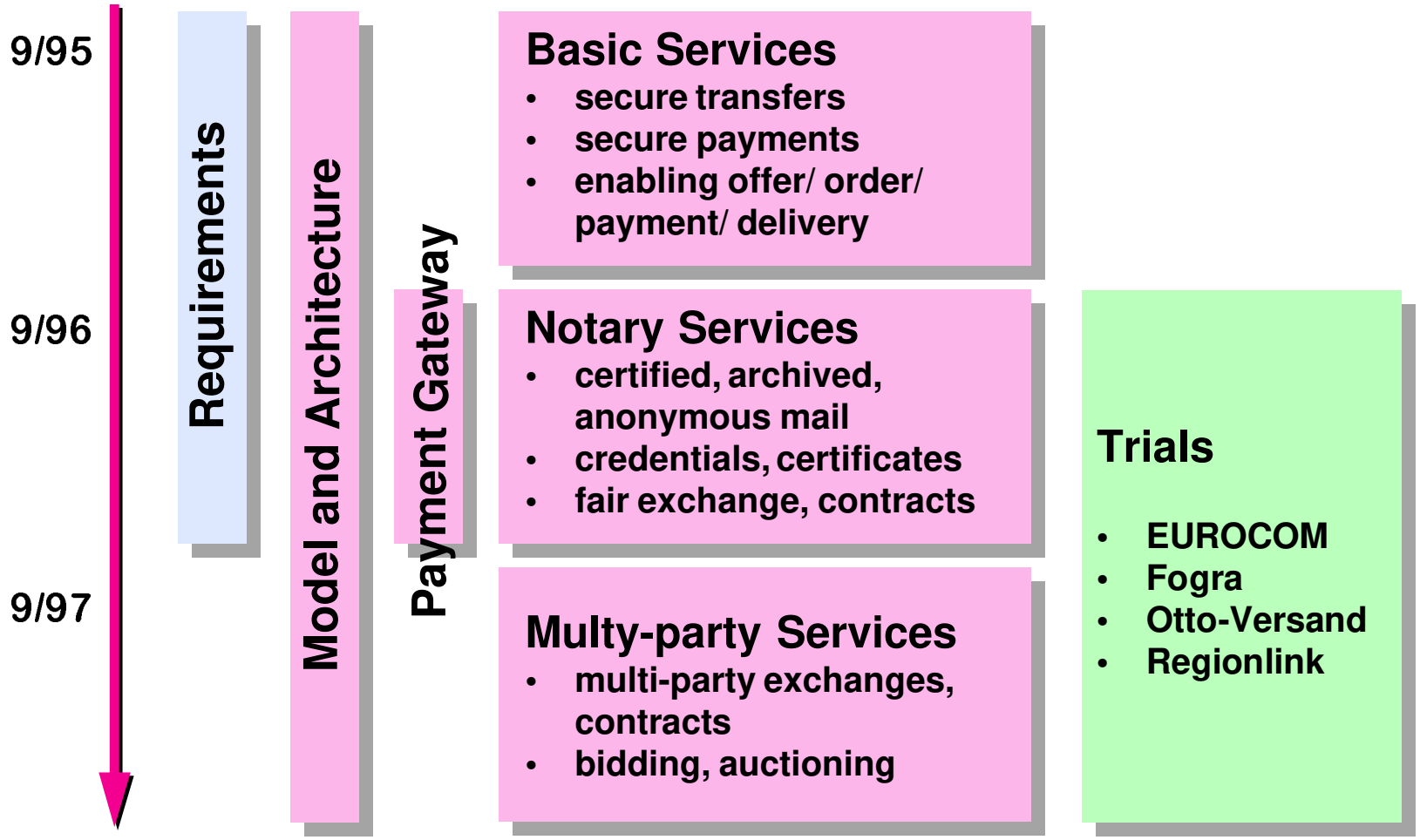
# Organisation

- 4th Framework of the EU: ACTS AC026
- Budget of ca. 9 MECU (14 M CHF)
- Funding 50% EU & Switzerland, 50% partners
- September 1995 - August 1998
- Consortium of 20 partners from 8 European countries
- Project leader: IBM France (Project Management) and IBM Zurich Research Lab (Technical Leader)

© IBM 4.10.96 <wmi@zurich>



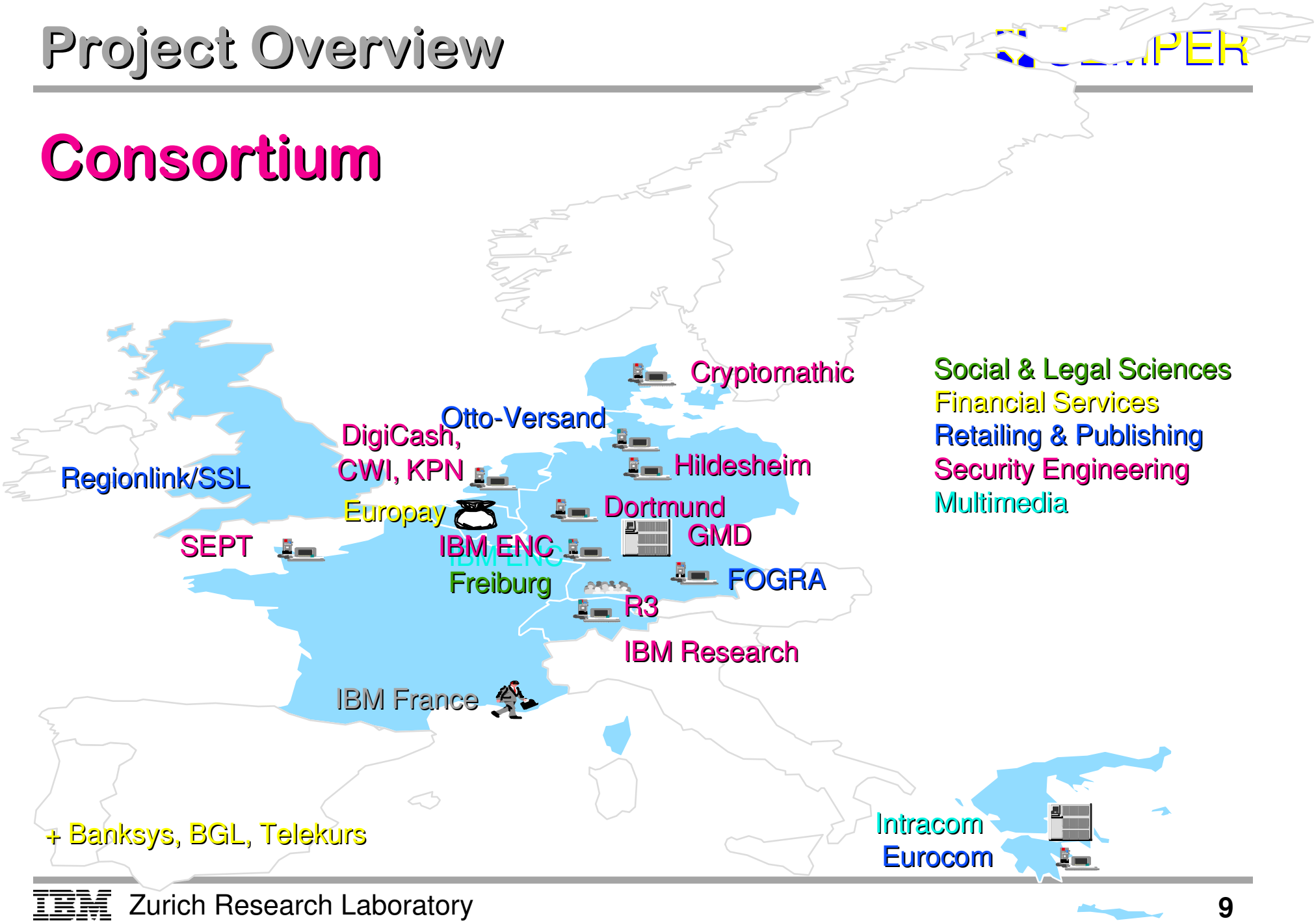
# Time Schedule



© IBM 4.10.96 <wmi@zurich>

# Project Overview

## Consortium

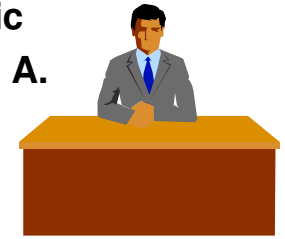


© IBM 4.10.96 <wmi@zurich>



# Model

- Notary Public
- Certification A.
- "Bank," etc.



Third Parties

Customer

Certificates

Certificates

Signed Offer

Signed Order

Fair Contract Signing

Fair Payment for Receipt

Delivery

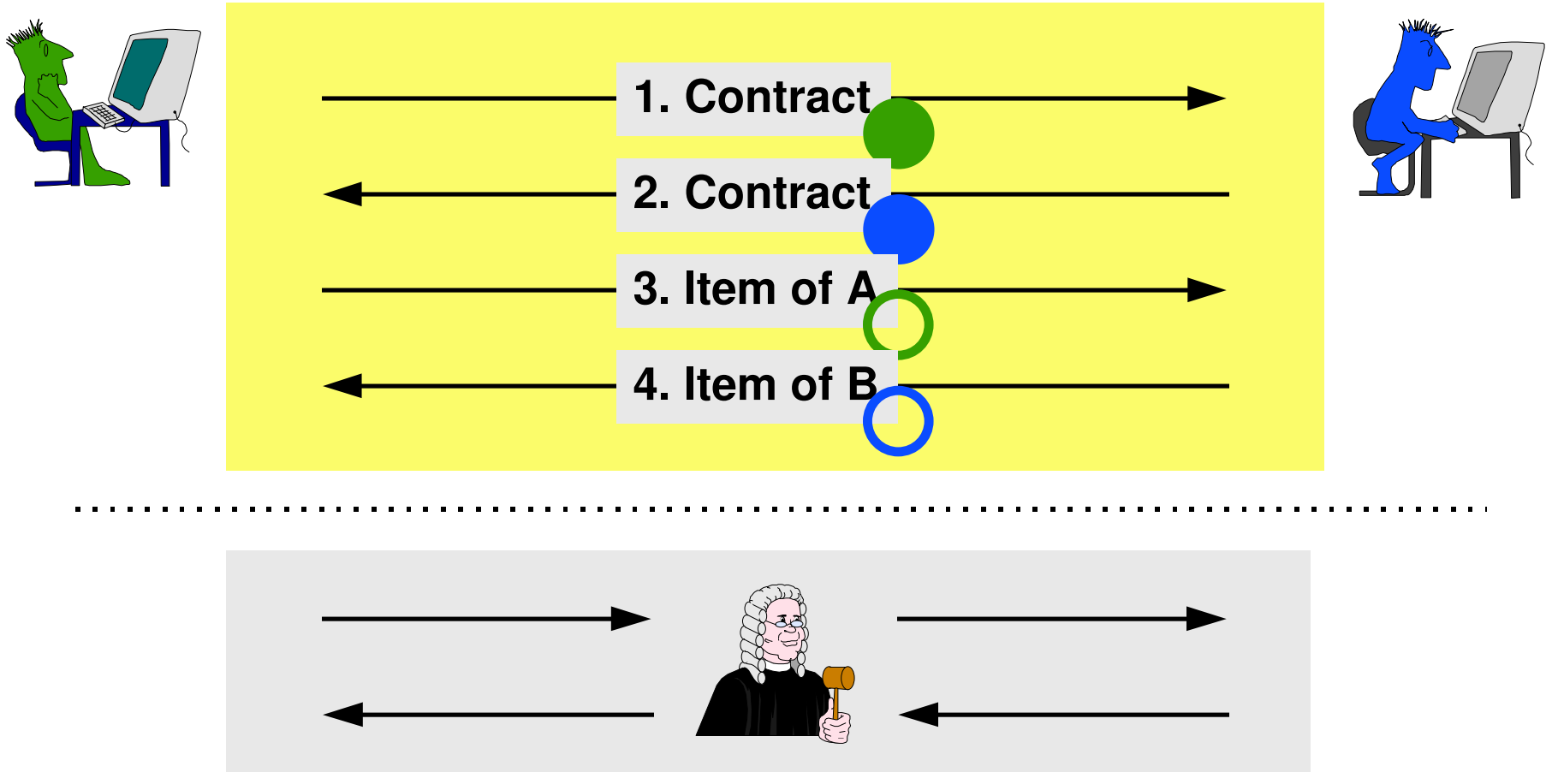
Merchant

Dispute Handling

© IBM 4.10.96 <wmi@zurich>



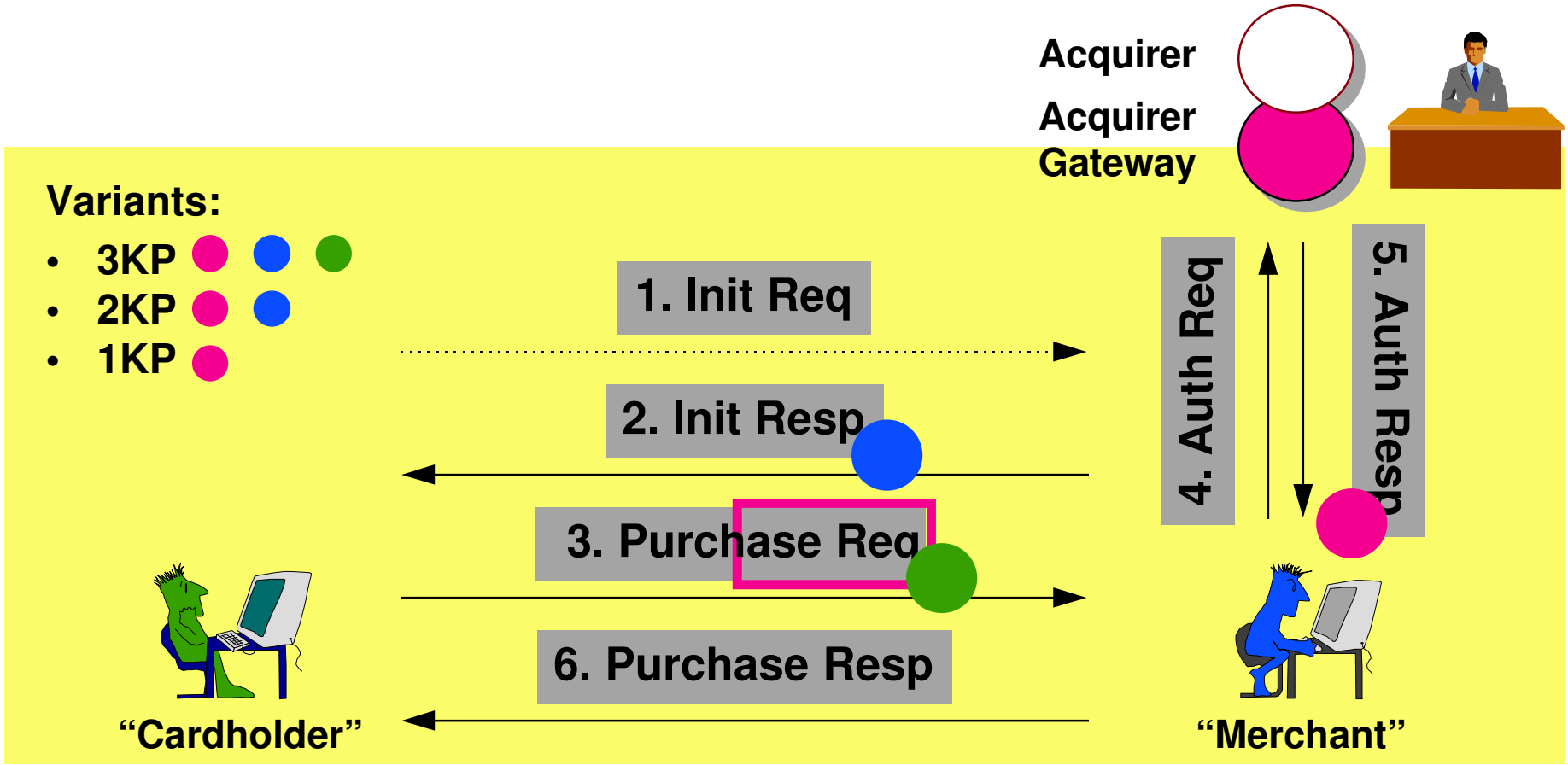
# Example: Generic 2-Party Fair Exchange



© IBM 4.10.96 <wmi@zurich>



# Example: iKP/SET for Credit Cards



© IBM 4.10.96 <wmi@zurich>



# Basic Architecture

Customer

Merchant

Any WWW Browser

Any WWW Server

Generic Client Business Application

SEMPER

Certificates

Certificates

Signed Offer

Signed Order

Fair Contract Signing

Fair Payment for Receipt

Delivery

Generic Server Business Application

SEMPER

© IBM 4.10.96 <wmi@zurich>

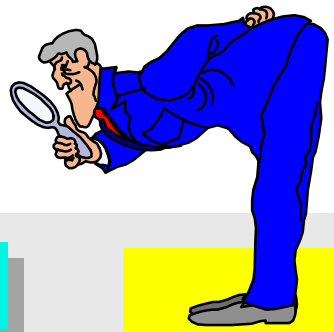
# Architecture

SEMPER

Browser/ Server

Third Parties

WWW Integration



Tinguin

Business Applications

Commerce Managers

Transfer and Exchange Managers

Payment Block

Certificate Block

Statement Block

Tinguin Block

Prefer. Block

Access Control

Archive Block

Crypto Block

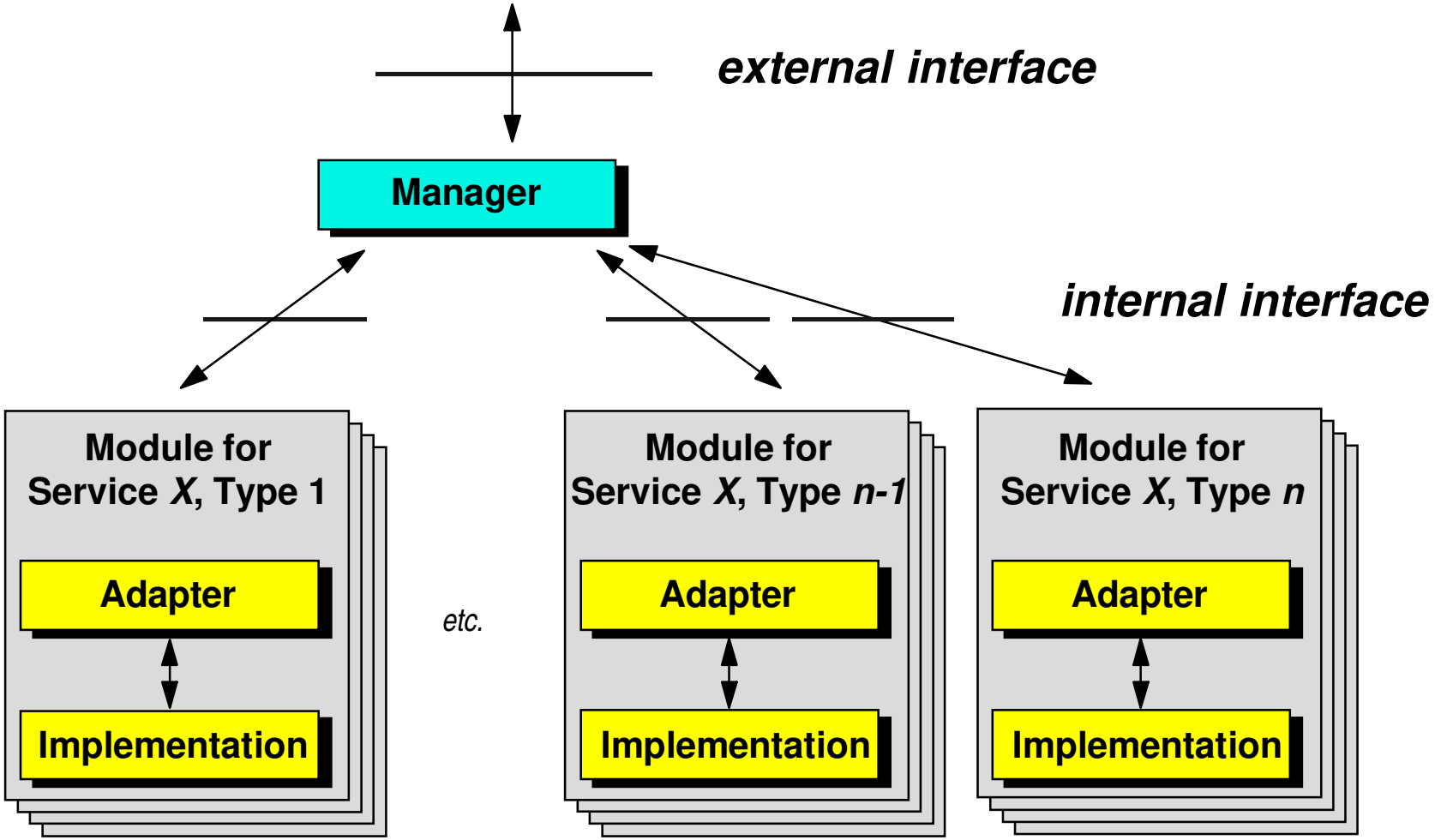
Comm. Block

...

© IBM 4.10.96 <wmi@zurich>



# Service Blocks

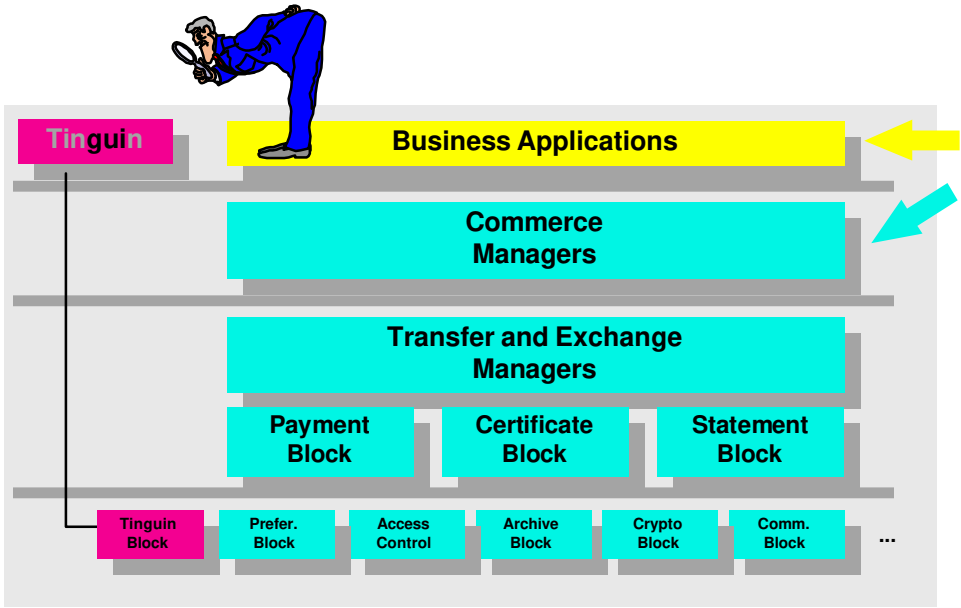


© IBM 4.10.96 <wmi@zurich>

# Architecture: *TINGUIN*

SEMPER

***T**rusted*
***IN**teractive*
***G**raphical*
***U**ser*
***IN**terface*




- **Why?**
  - **Never trust a window on an untrusted PC or in a browser ...**
- **How?**
  - **Approximation in software: Dedicated window**
  - **Ideal solution: “Electronic wallets” with keypad & display**
- **More general problem: Untrusted Hardware**

© IBM 4.10.96 <wmi@zurich>



# General problem: Untrusted Hardware

## PC + Software-only

Trojan Horse,
Virus

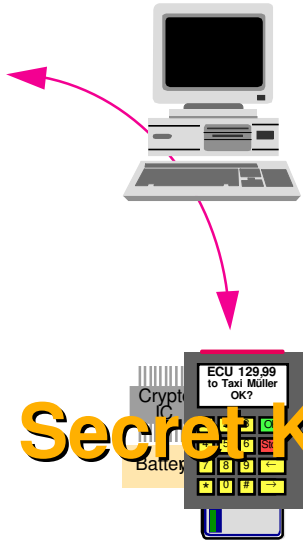
Net

User

## PC + Secure Hardware

Smartcard

User




"Wallet"

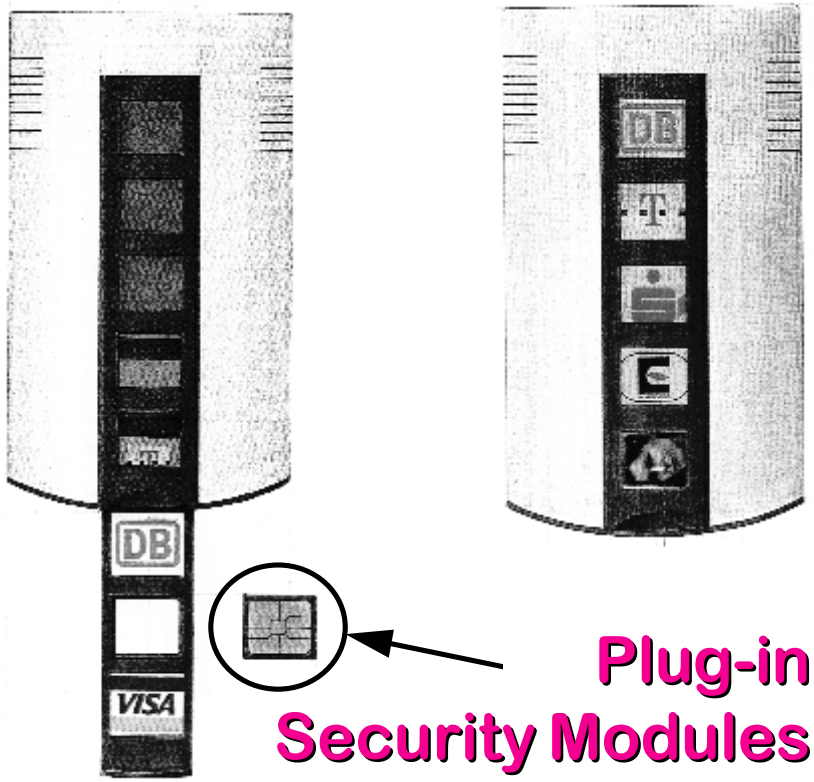
User

Design: © Fachhochschule Hildesheim, 1996



# Wallet Design Example

Infrared




Plug-in Security Modules

Back

Screen

Keypad

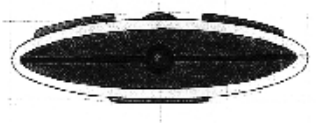
Front

Design: © Fachhochschule Hildesheim, 1996

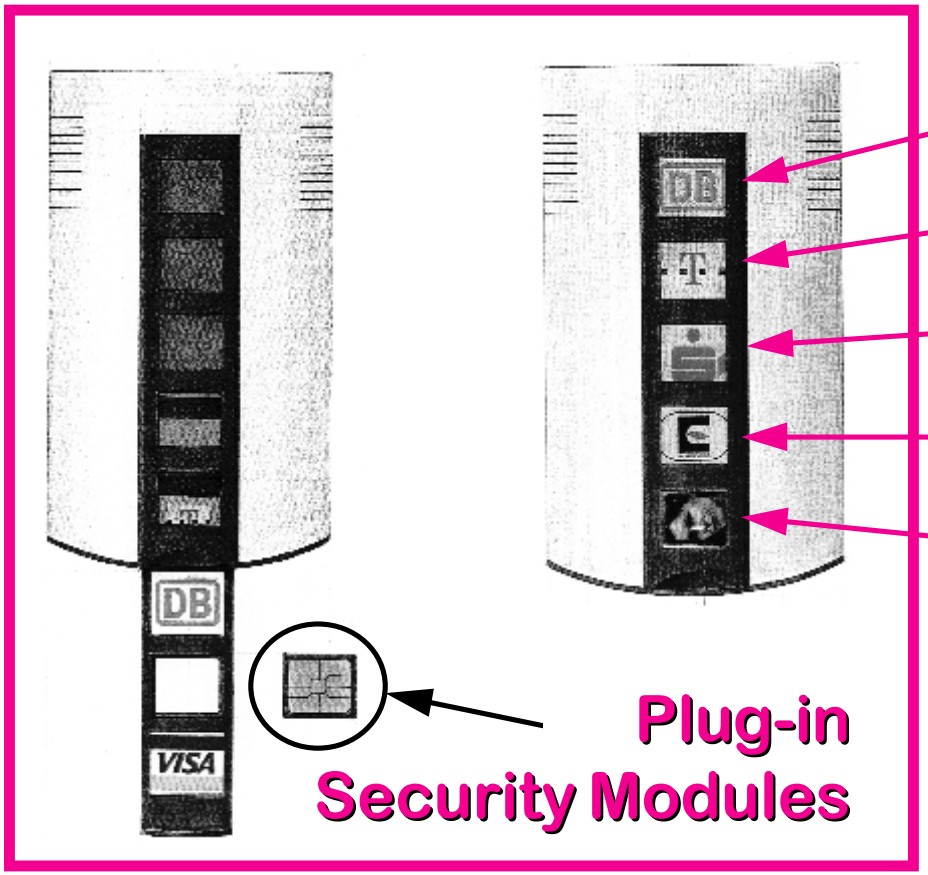
# Architecture: *TINGUIN*

SEMPER

## Wallet Design Example



Infrared



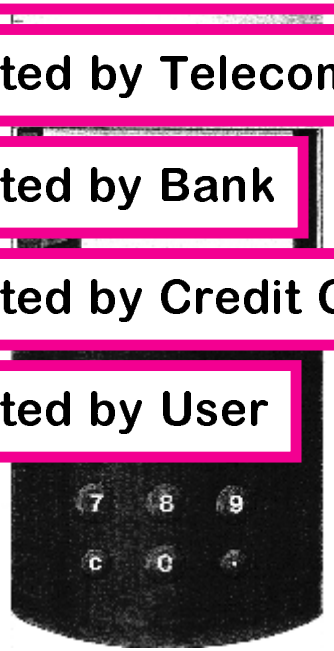

Trusted by Railway Organisation

Trusted by Telecom

Trusted by Bank

Trusted by Credit Card Organisation

Trusted by User




Screen

Keypad

Back

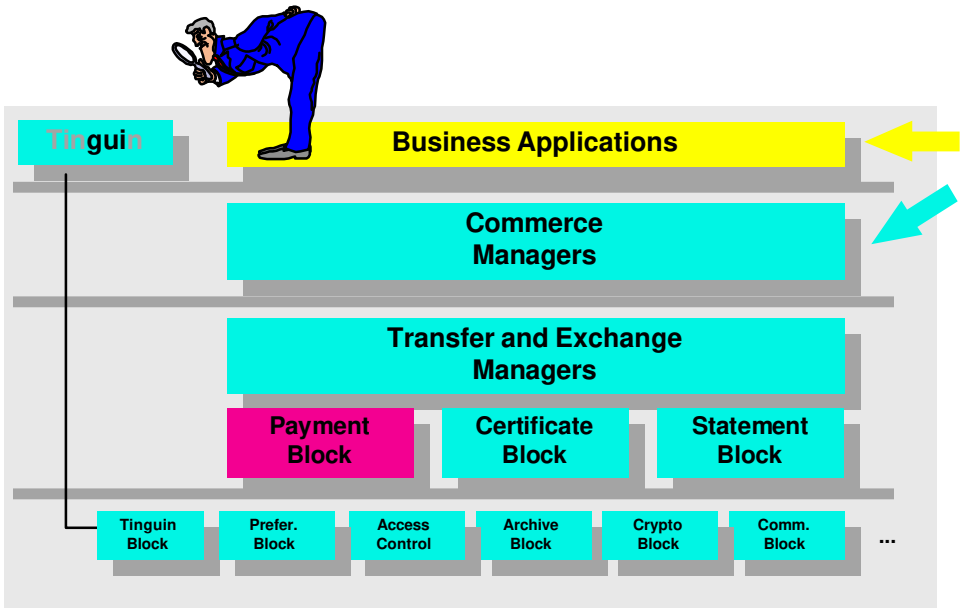
Front

© IBM 4.10.96 <wmi@zurich>

# Architecture: *Payment Block*

SEMPER

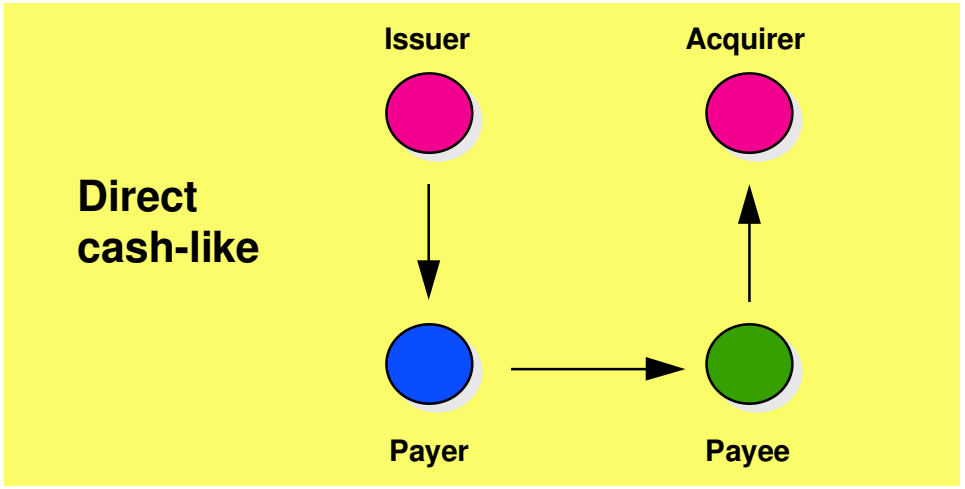
## Example: *Payment Block*

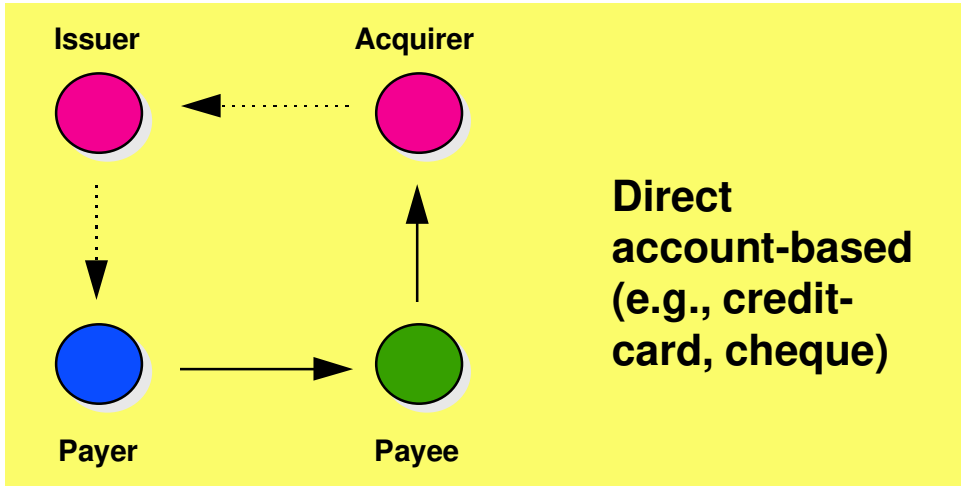


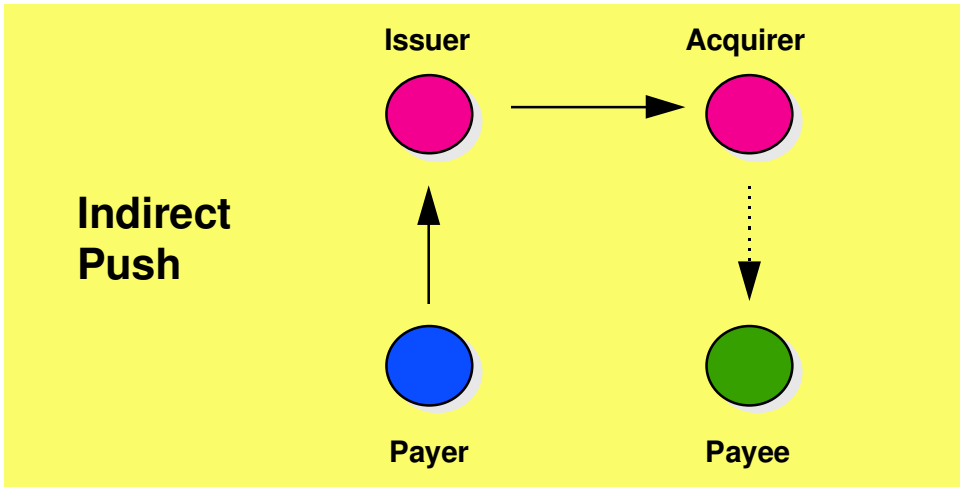
© IBM 4.10.96 <wmi@zurich>

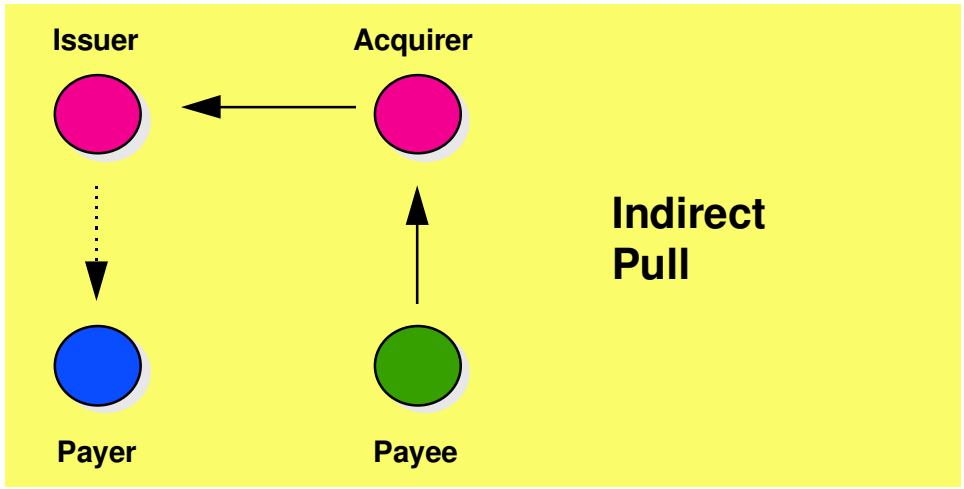


# Existing Payment Models



© IBM 4.10.96 <wmi@zurich>

# Architecture: *Payment Block*

SEMPER

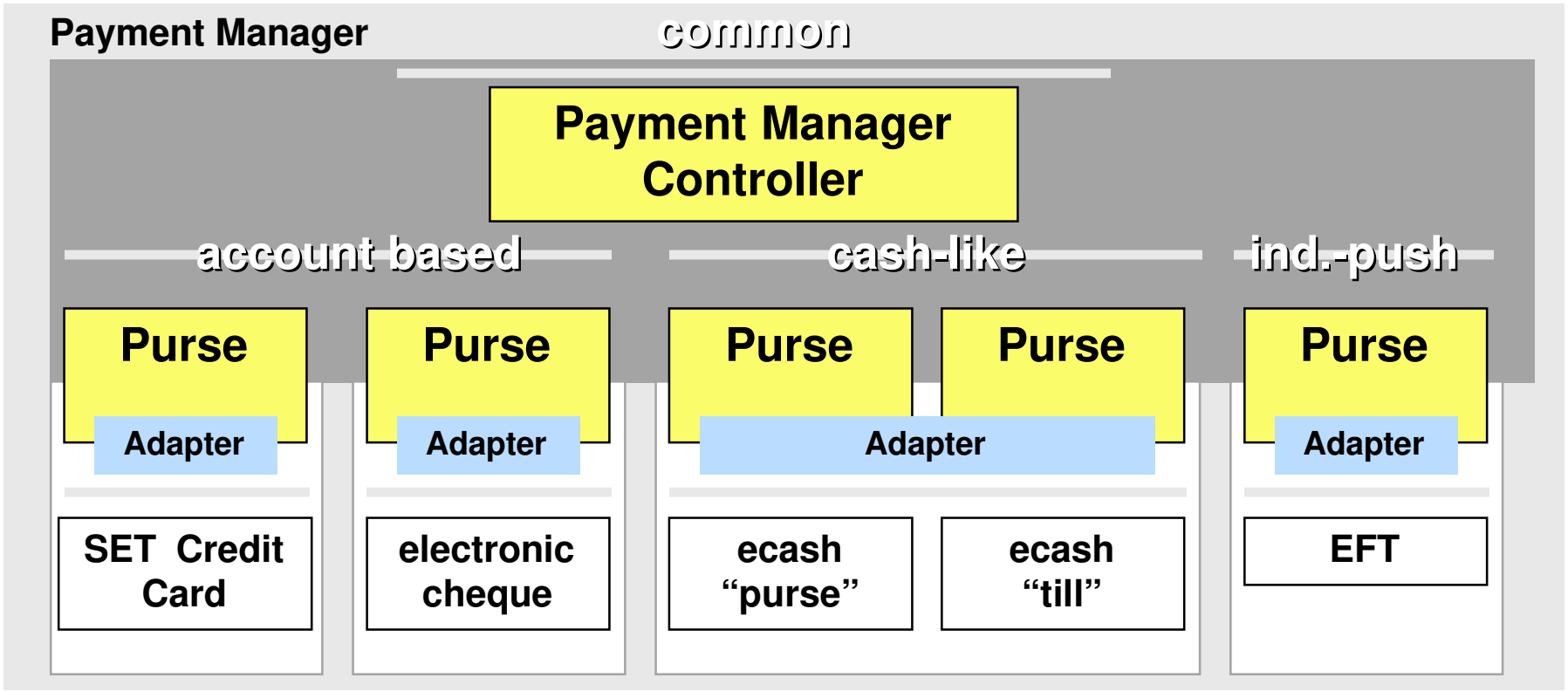
| | Online Payments | Offline Payments |
|---|---|---|
| Traceable | ◆ **Crypto-less Systems:** *FirstVirtual + just-do-it*<br>◆ **Encrypted CC:** *just-do-it, e.g., SSL*<br>◆ **Secure CC:** ***iKP / SET***<br>◆ **Secure Cheques:** *FSTC e-check*<br>◆ **Billing server for Micro payments:** *NetBill, NetCash*<br>◆ **Micro payments:** *CAFE, iKP, Millicent, MikroMint* | ◆ **Smartcard-based electronic purses**<br>◆ **Shared-key:** *Danmont, Proton*<br>◆ **Public-key:** ***CLIP***<br>◆ *Mondex:* **P-to-P payments, wallets**<br>◆ **CEN IEP Standard** |
| Untrace-able | ◆ **Anonymous "exchangers":** *Anonymous Credit Cards, NetCash*<br>◆ **Blind Signatures:** ***ecash*** | ◆ **Smartcard-based or Electronic Wallets + Blind Signatures:** ***CAFE*** |

+ many other proposals and projects ...

© IBM 4.10.96 <wmi@zurich>



# Architecture of Payment Block




*e. g.*

© IBM 4.10.96 <wmi@zurich>



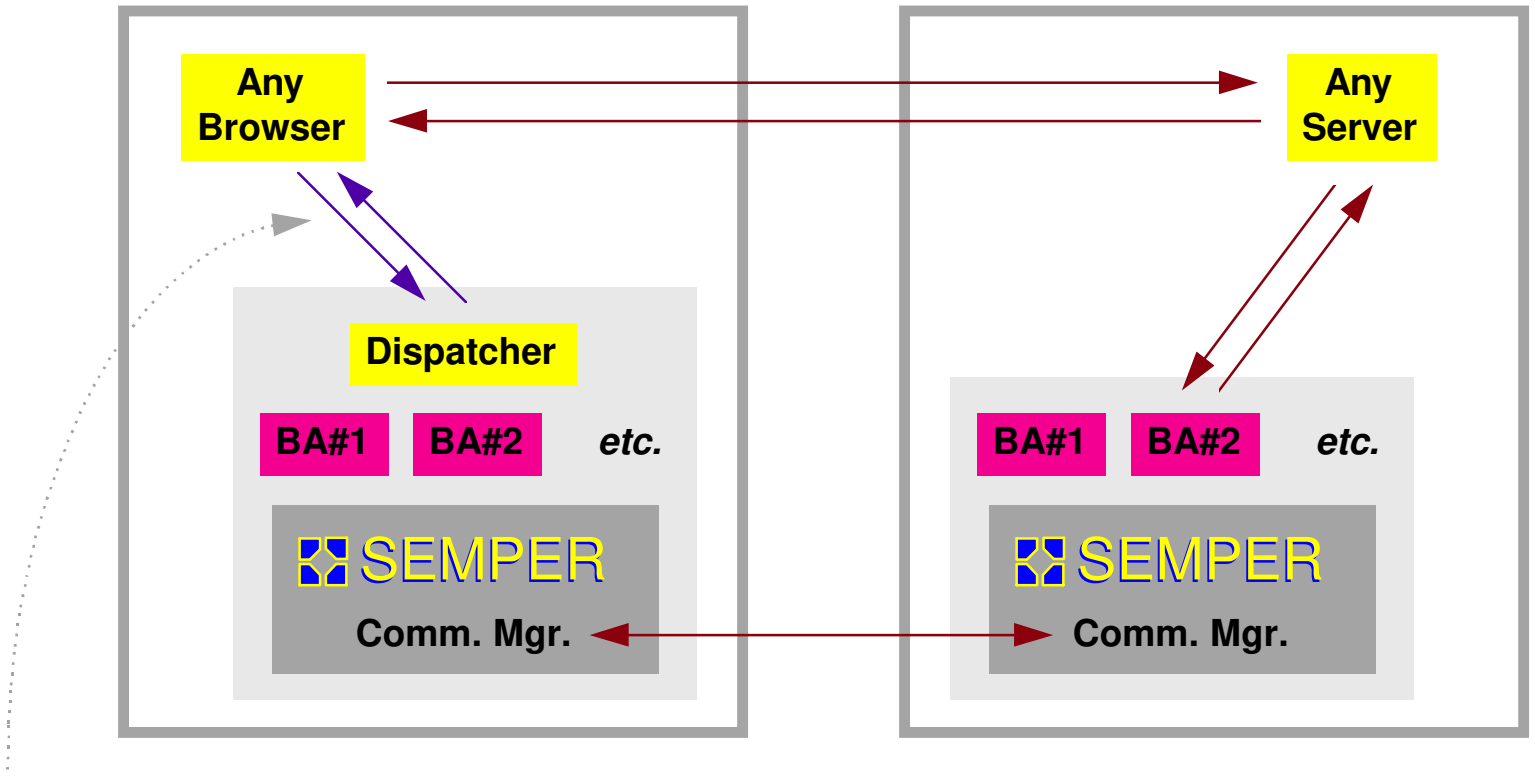
# Services of Payment Block

- **Value Transfer**
  - **payment + reversal + conversion/currency exchange + authorisation/capture + loading / deposit**
- **Purse Management**
  - **create + initialise + renew + synchronize + delete purses**
  - **preferences management, access control**
- **Information Services**
  - **dump of complete transcripts + reports (book-keeping tools)**
- **Transaction Management**
  - **status + cancellation of transactions**
- **Recovery and Dispute Management**

© IBM 4.10.96 <wmi@zurich>



# Architecture for WWW Integration




http://localhost:1234/BA#1/[tx=23]

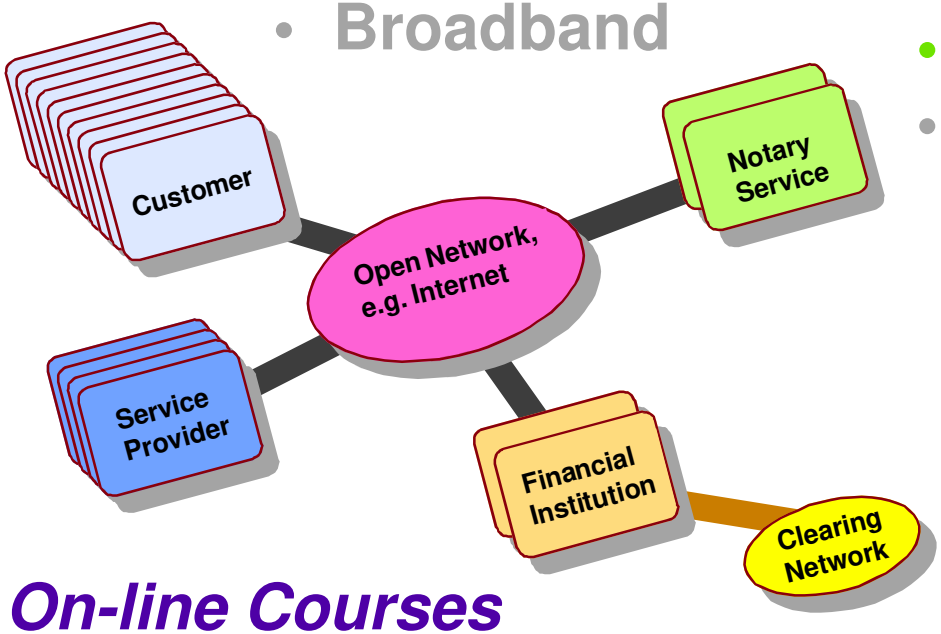
© IBM 4.10.96 <wmi@zurich>



# Basic Trials

- internal
- field trials

- Internet
- Broadband




- GMD: *Certification*
- IBM, ...

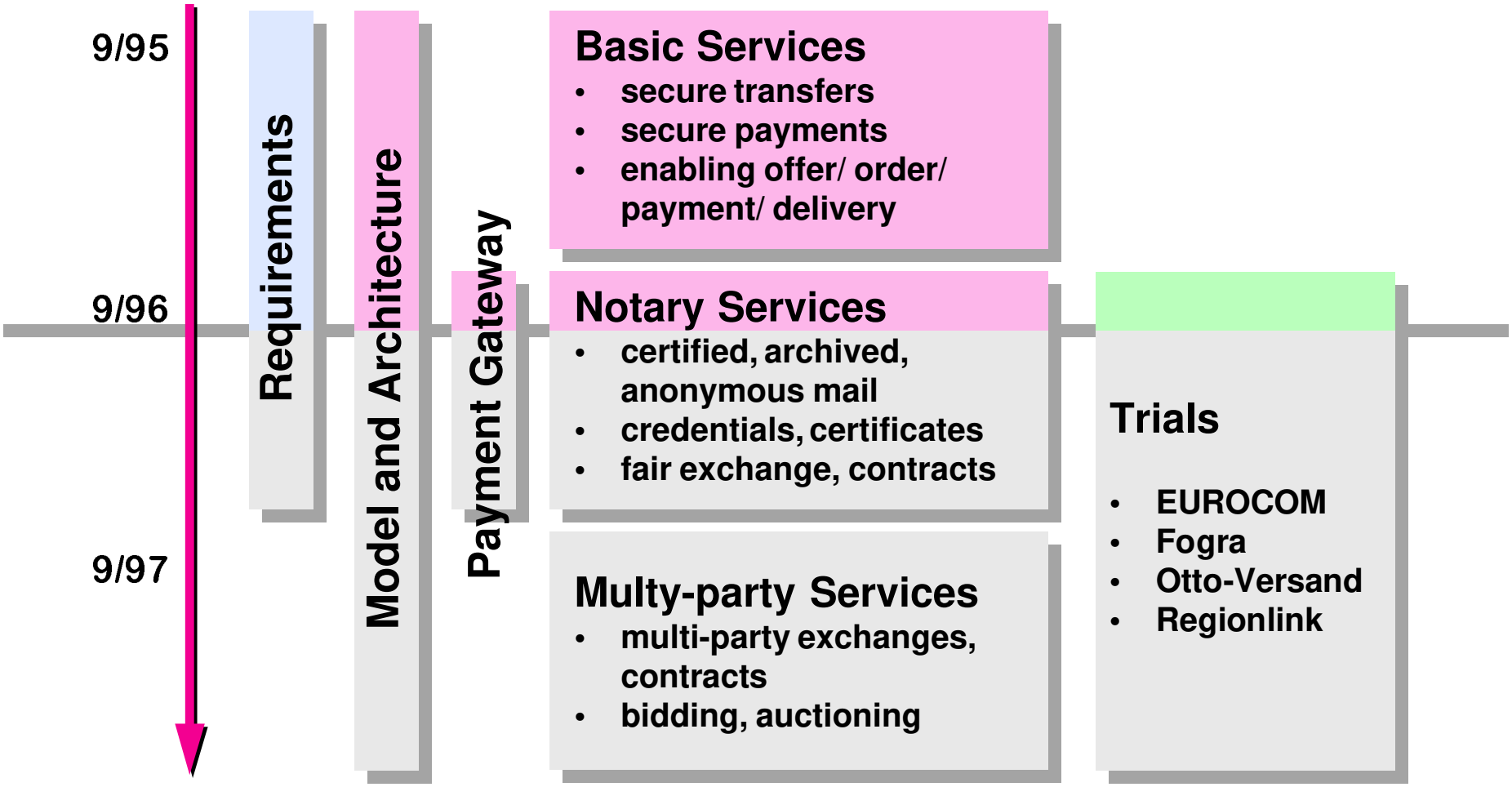
- EUROCOM: *On-line Courses*
- FOGRA: *Newsletter*
- Otto-Versand: *Mail-order*
- Regionlink: *Mail-order*

- DigiCash: ecash
- IBM: SET
- Europay:CLIP, ...

© IBM 4.10.96 <wmi@zurich>

# Summary

SEMPER



© IBM 4.10.96 <wmi@zurich>

# Summary

SEMPER

- **SEMPER aims at**
  - **Complete picture of security in electronic commerce, not just payment**
  - **Open architecture, public designs, prototypes, public validation**
  - **Multi-party security, including privacy protection**
- **So far ...**
  - **Comprehensive architecture of electronic commerce**
  - **Service block concept with internal / external APIs,**
    - **First designs of all blocks, limited to secure transfers**
    - **E.g., TINGUIN, Payment Block**
  - **Easy-to-extend Business Application for Web integration**
  - **Demo of first version on October 2nd, 1996, in Zurich**
- **Next steps ...**
  - **publication of specs on <www.semper.org>, trials on Internet**
  - **provide generic fair exchange, advanced services**
  - **promote design to other parties**

© IBM 4.10.96 <wmi@zurich>



# More information ...

- **Public SEMPER Reports, Mailing lists, etc.**

  **<http://www.semper.org>**

- **Demonstration of SEMPER: PKS '96, Zurich, 96/10/02**

  **<www.r3.ch/conferences/pks96.html>**