

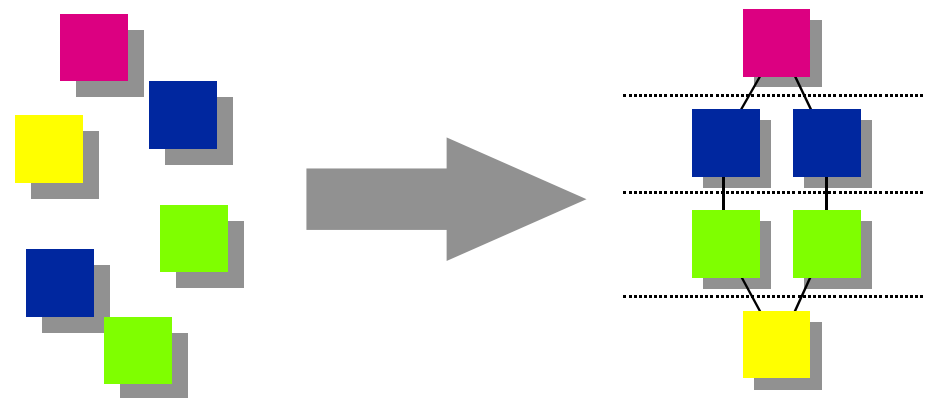
# Outline



## Frameworks for secure electronic commerce



## Frameworks for Secure Electronic Commerce



- u **Interoperability of components**
- u **Consistent and coherent user interface**
- u **Open for new components, e.g., new services, new protocols, new implementations**
- u **System, application, vendor neutral**



# Proposed Frameworks

---

- u **Vendor-specific Frameworks**

- u IBM (SecureWay)
- u Microsoft
- u Netscape

- u **Java Electronic Commerce Framework (Sun)**

- u **Research Projects**

- u SEMPER (EU ACTS Project)  
Secure Electronic Marketplace for Europe
- u eCo SYSTEM (CommerceNet)

## Secure Electronic Marketplace for Europe



- **EU ACTS Project, 20 Partners, 1995 - 1998**
- **Objective: “Establish an open and generic security architecture for the global marketplace”**
  - u **Define a model of the marketplace**
  - u **Specify the architecture and associated services**
  - u **Evaluate the architecture and the services**
    - u **Develop a prototype**
    - u **Run realistic trials**
    - u **Evaluate security and consumer response**
  - u **Disseminate the results**
    - u **Publish the architecture and the specifications**
    - u **Contribute to standardisation efforts**



# Consortium

## Service provision

- Otto Versand
- Eurocom
- Fogra
- Maris

## Banking

- Europay
- Commerzbank

## Telecom operators

- France Télécom
- KPN Research
- Intracom

## Social sciences

- Freiburg Univ.

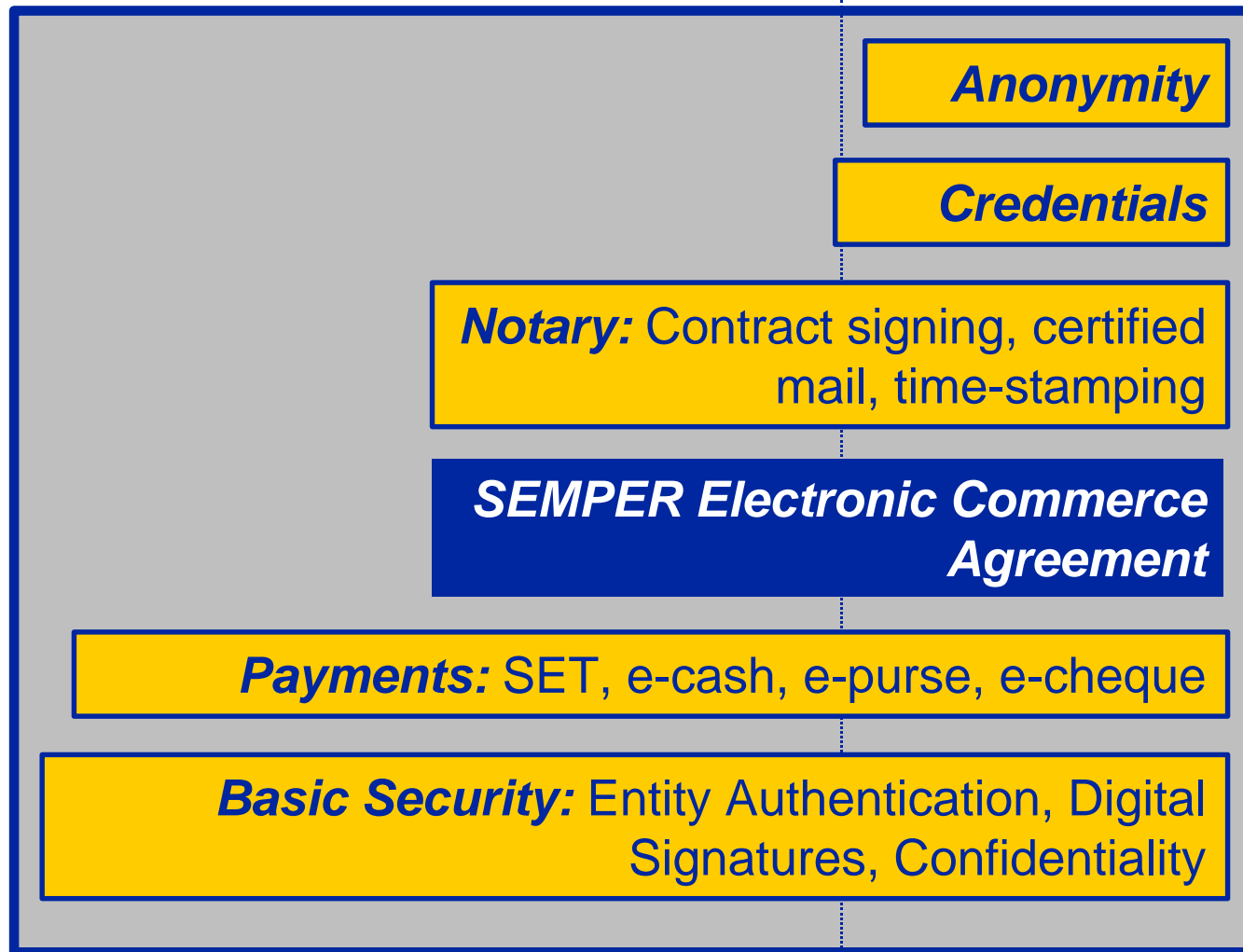
## Security engineering

- Cryptomathic
- CWI
- Digicash
- GMD
- IBM
- r<sup>3</sup>
- SINTEF
- Dortmund Univ.
- Hildesheim Univ.
- Saarbrücken Univ.



# Frameworks

## Schedule



9/95

8/98





# Trials

## u Business contexts

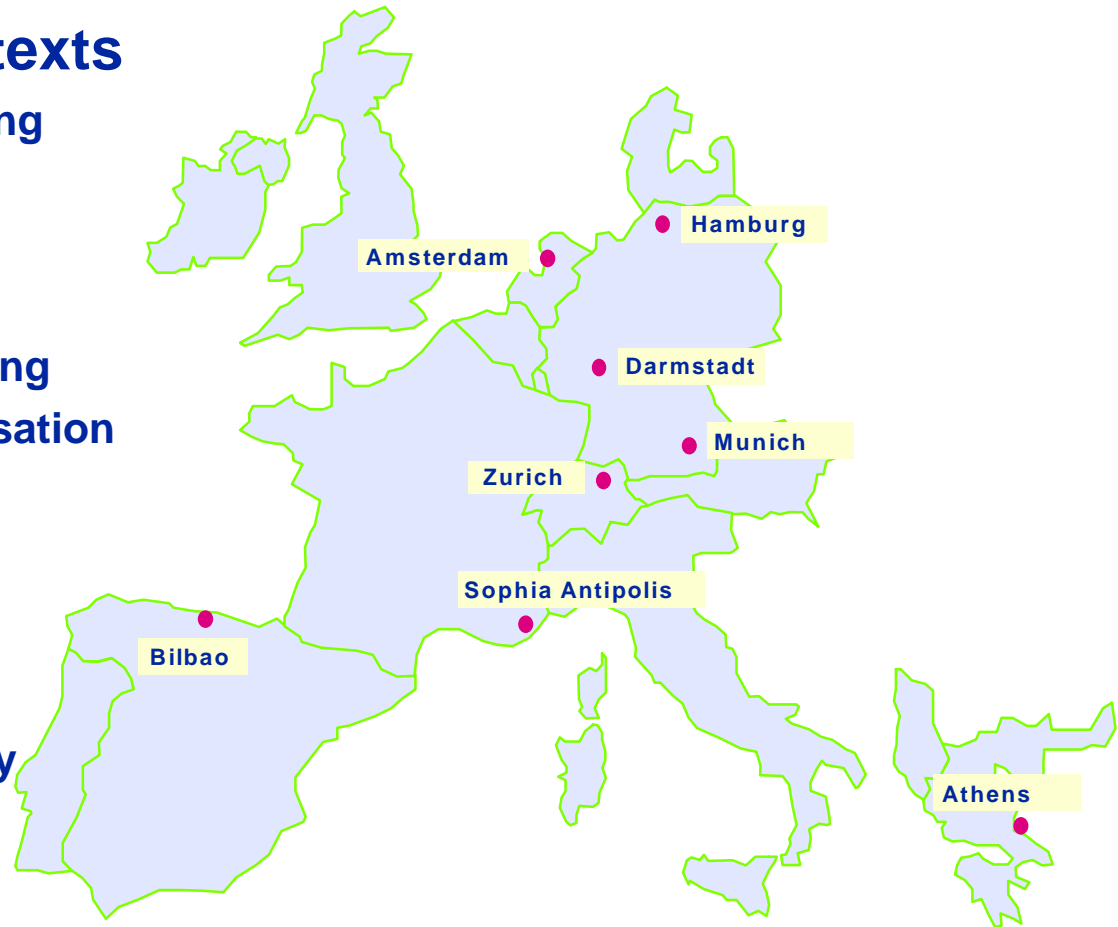
- u Distance learning
- u Mail order
- u Library
- u Travel
- u Image processing
- u Software localisation

## u Players

- u Buyers
- u Sellers
- u Banks
- u RA/CA authority

## u Payments

- u SET
- u Ecash
- u Chipper



# SEMPER Architecture



**Customer**

Any WWW Browser


Generic Client Business Application



**Merchant**

Any WWW Server

Generic Server Business Application





# SEMPER Architecture



## Business Applications

“Generic BA” used by Otto-Versand, FOGRA, Eurocom

## Commerce Block

Standard Business Processes, “Scripts” and “Templates”

## Transfers & Fair Exchanges

“Containers” + Time Stamping, Contracts, Certified Mail, etc.

### Payments

“Money”

### Certificates

“Credentials”

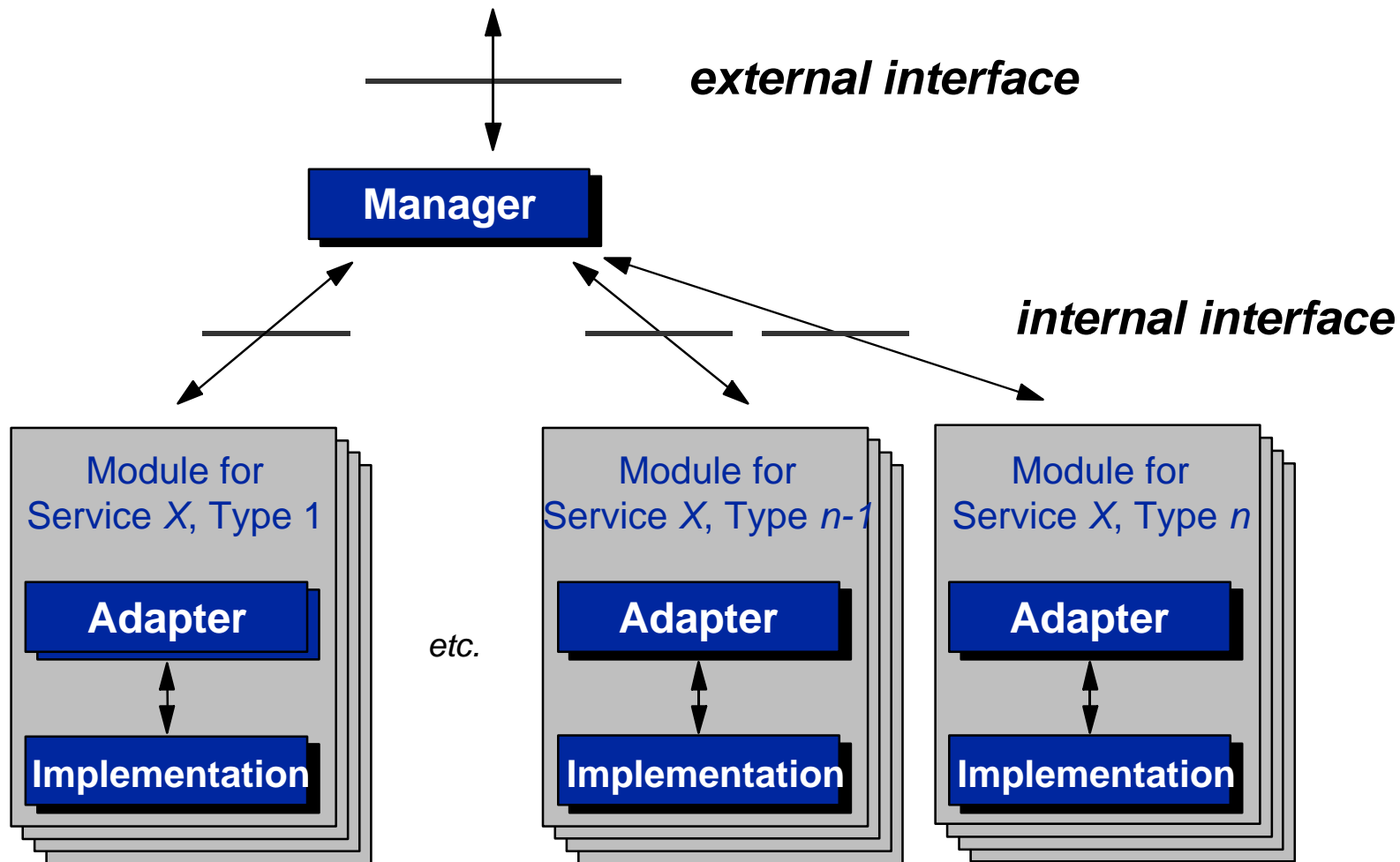
### Statements

“Documents”

## Supporting Services

Communication, Crypto Engine, Trusted User I/O (TINGUIN),  
Archive, Access Control, Preferences

# Service Blocks





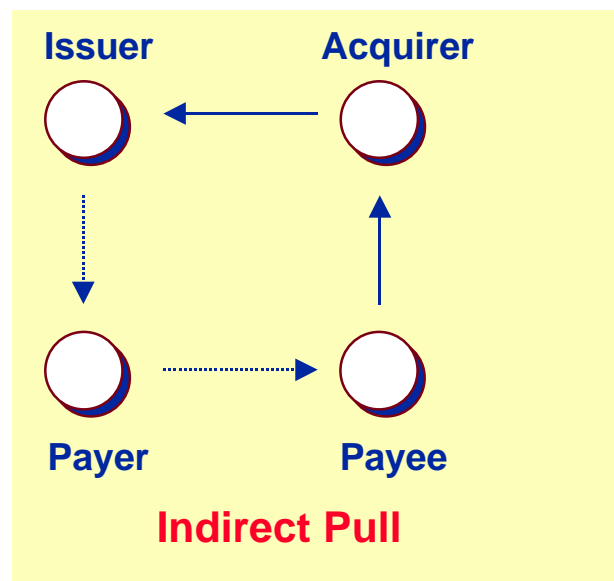
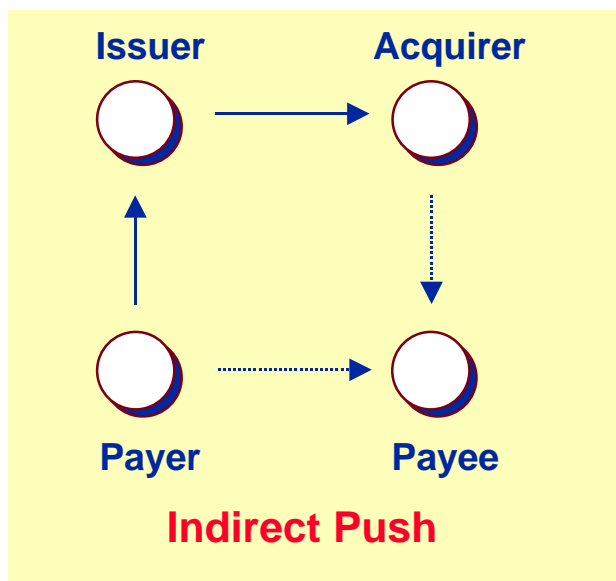
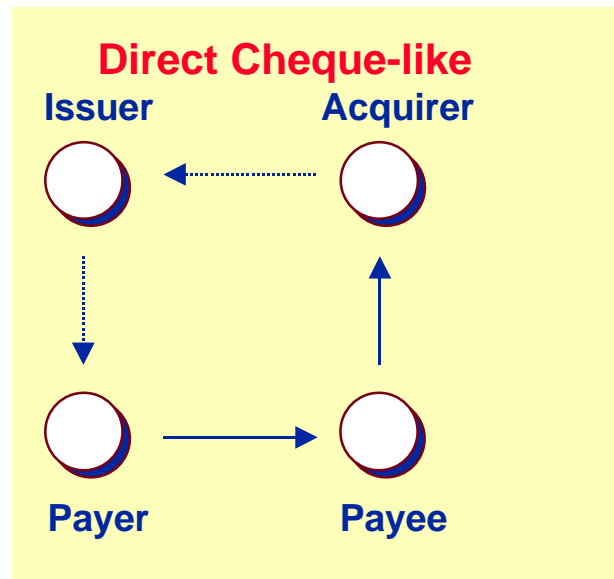
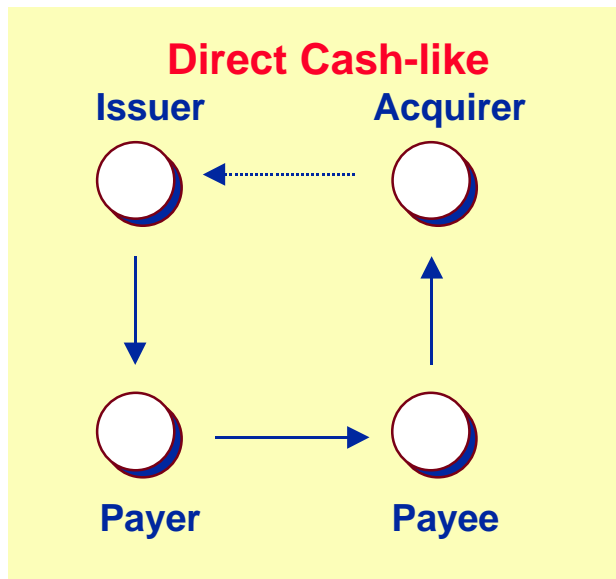
# For Instance ...



## Design of the Payment Block



# Existing Payment Models





# Design Objectives

---

- ◆ **Symmetric Design for Payer and Payee**
- u **Unified Interface for Services**
  - u Enables development of application independent of payment systems
  - u Support for adapting new payment systems
- u **Management of multiple means of payment**
  - u “purse” selection, negotiation
- u **Framework for handling disputes**

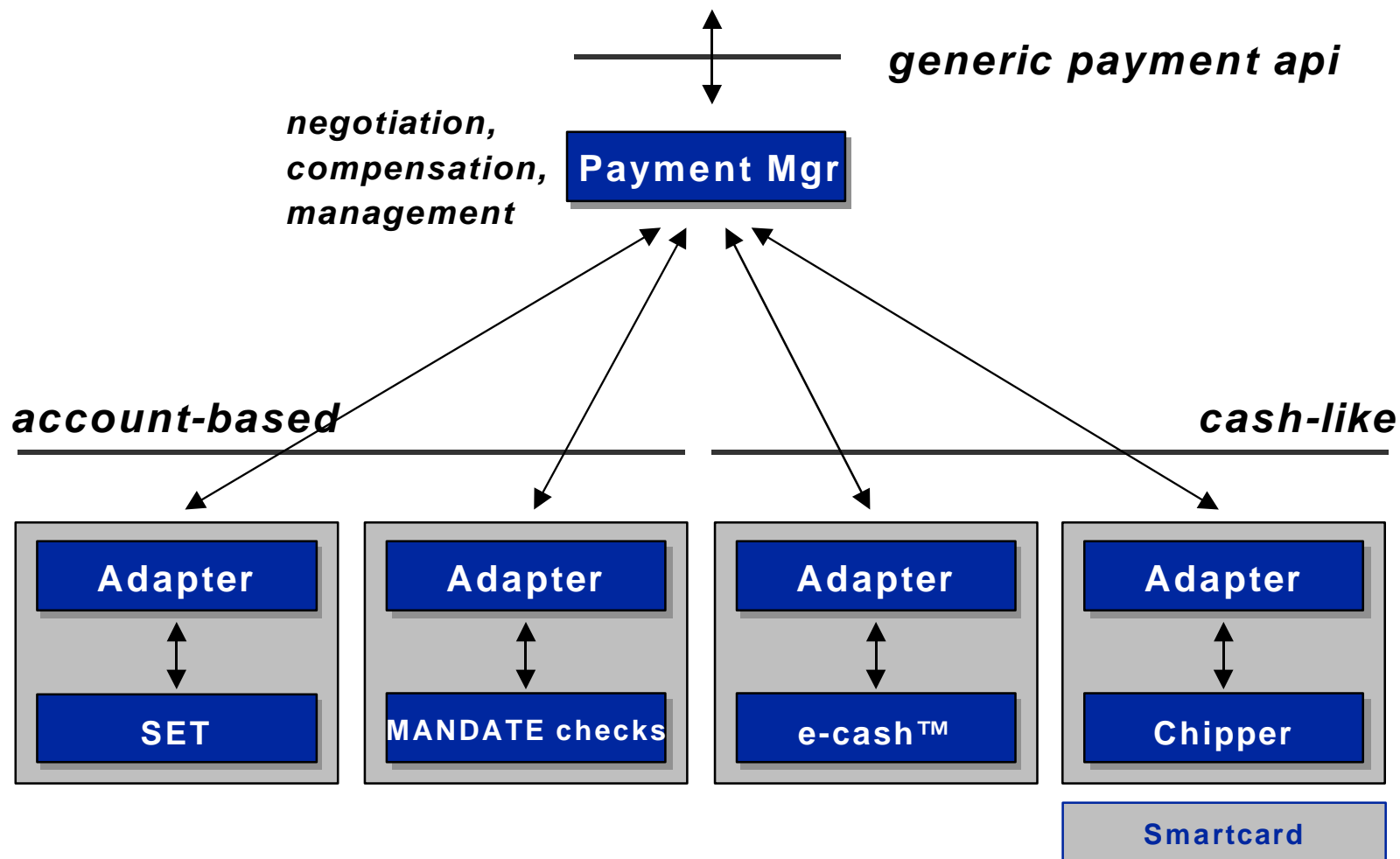
# Services

---

- u **Value transfer**
  - u payment/reversal + authorisation/capture + loading/deposit
- u **Purse management**
  - u create + configure + delete purses
  - u policy/preferences management, access control
- u **Purse selection**
  - u negotiations, preferences
- u **Transaction management**
  - u status, cancellation, and recovery of transactions
- u **Information services**
  - u dump of complete transcripts + reports (book-keeping tools)
- u **Dispute management**

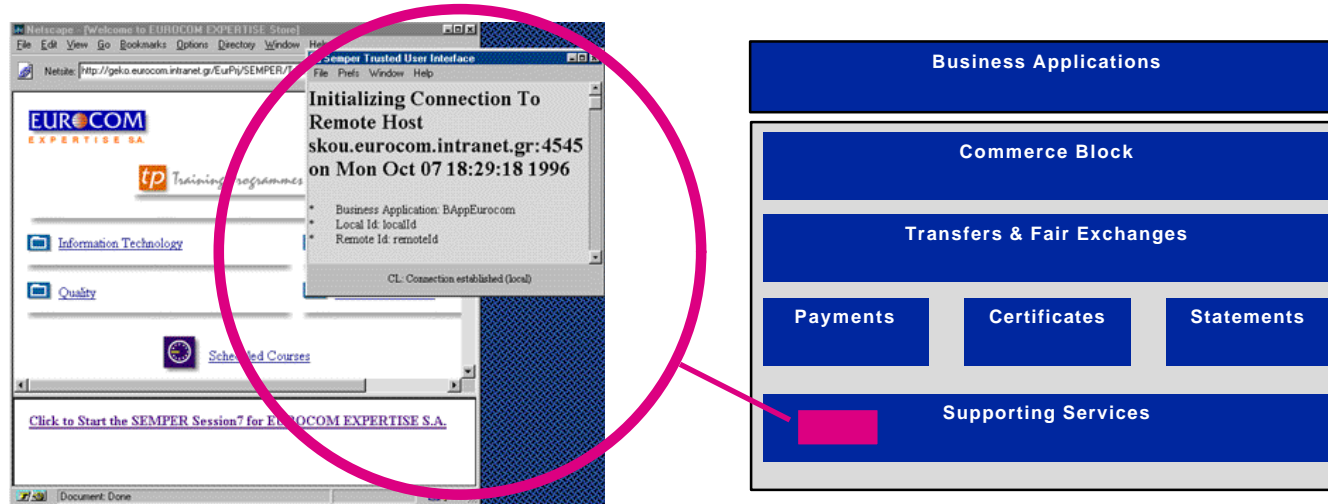


# For Instance: Payments





# Trusted Interactive Graphical User Interface



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