Michael Waidner
(wmi@zurich.ibm.com)
IBM Zurich Research Laboratory
CH8803 Rüschlikon -- Schweiz

Secure Electronic Marketplace for Europe

OCG Arbeitskreis "Electronic Commerce"

Wien, 20. November 1998

Outline

- What is SEMPER?
- Reasoning behind design
- Glimpse on the architecture

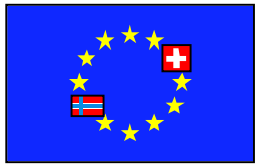
More information:

- See <http://www.semper.org>
- Final Report, LNCS Springer-Verlag, early 1999

mi@zurich.ibm.com

What is SEMPER?

SEMPER



acts

- European R&D Project, 1995-1998
  - ~ 30 people, 20 partners, lead by IBM
  - ~ 13.000.000 CHF
  - EU ACTS Programme: 50% EU & CH, N
- Objectives
  - secure B2B/B2C/P2P e-commerce
  - coherent, complete, extensible framework
  - leitmotif: fairness and multi-party security
- Results:
  - architecture & protocols for secure e-commerce
  - SEMPER electronic commerce agreement
  - prototype, trials & evaluations
  - demonstrator: Fair Internet Trader

mi@zurich.ibm.com

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
- r³
- SINTEF
- Dortmund Univ.
- Saarbrücken Univ.

mi@zurich.ibm.com

Outline

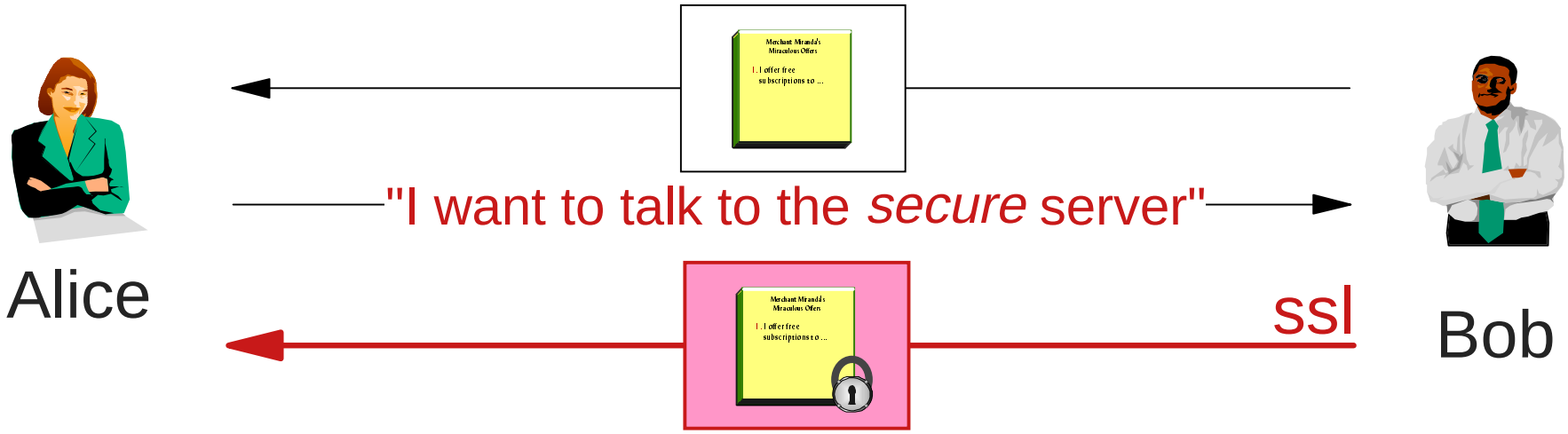
- What is SEMPER?
- Reasoning behind design
- Glimpse on the architecture

More information:

- See <http://www.semper.org>
- Final Report, LNCS Springer-Verlag, early 1999

mi@zurich.ibm.com

Current situation



Certificate really on "Bob"?
Issueing CA trusted? And: so what?

"Now I'm talking to Bob!"

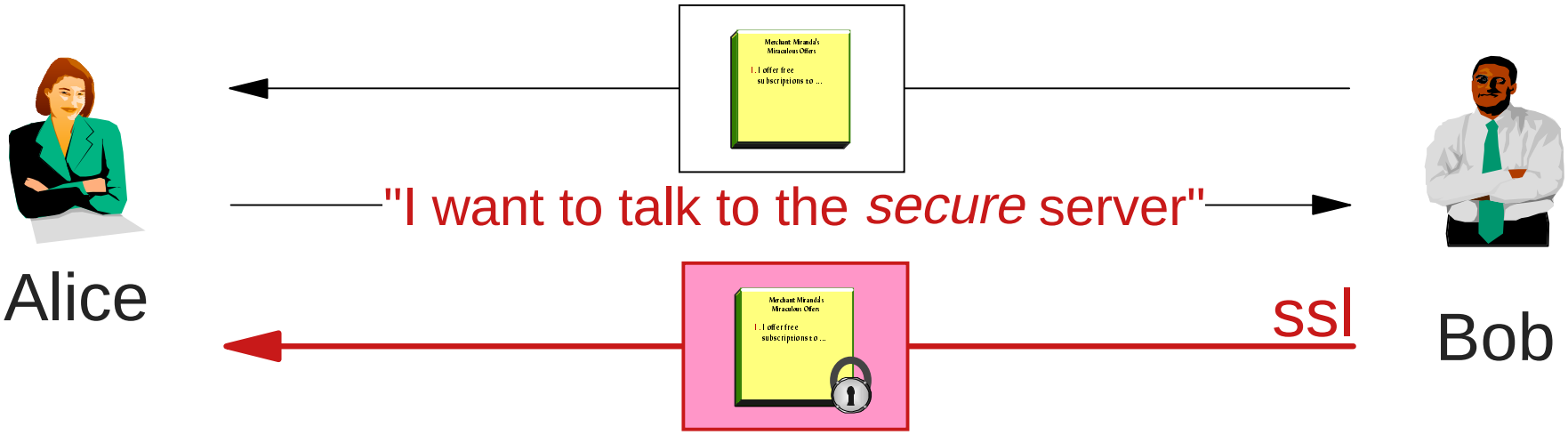
US export-controlled crypto?

"My messages are secure!"

"If he cheats me I can go to court"

SSL is transparent
to the application,
thus, *no signatures!*

Current situation



User interface + SECA,
Liability Cover Certificates

Certificate really on "Bob"?
Issueing CA trusted? And: so what?

Cryptography made
in Europe

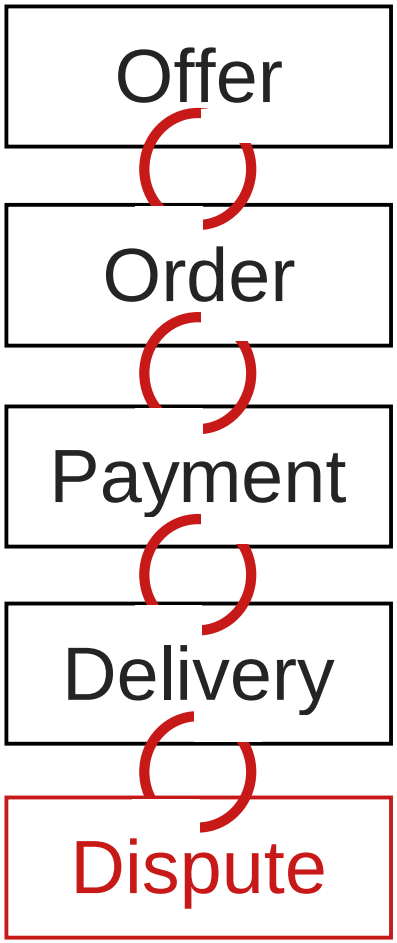
US export-controlled crypto?

Secure documents,
not (just) secure connections.

SSL is transparent
to the application,
thus, *no signatures!*

mi@zurich.ibm.com

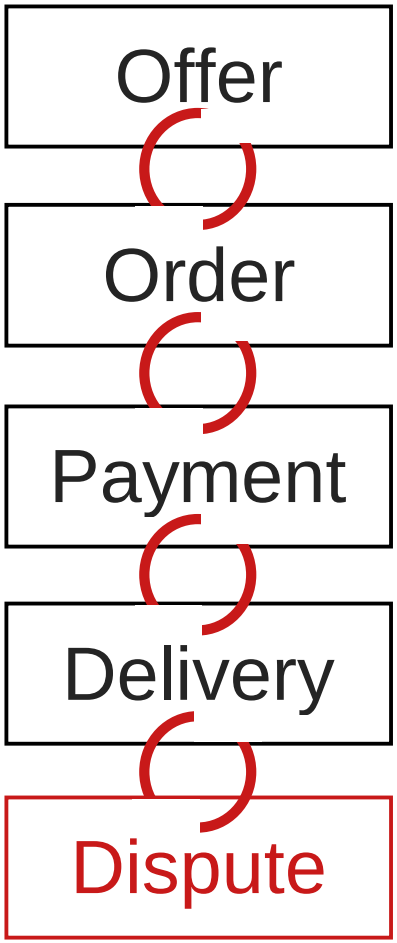
Processes, not just steps



- *Processes* are the entities that need to be trustworthy, not (just) the single steps.
- Security requirements like *anonymity cannot* be fulfilled on the step-level.
- Authorization policies naturally depend on processes.
- *Small* number of *generic, evaluated and certified* business processes are needed.

mi@zurich.ibm.com

Processes, not just steps

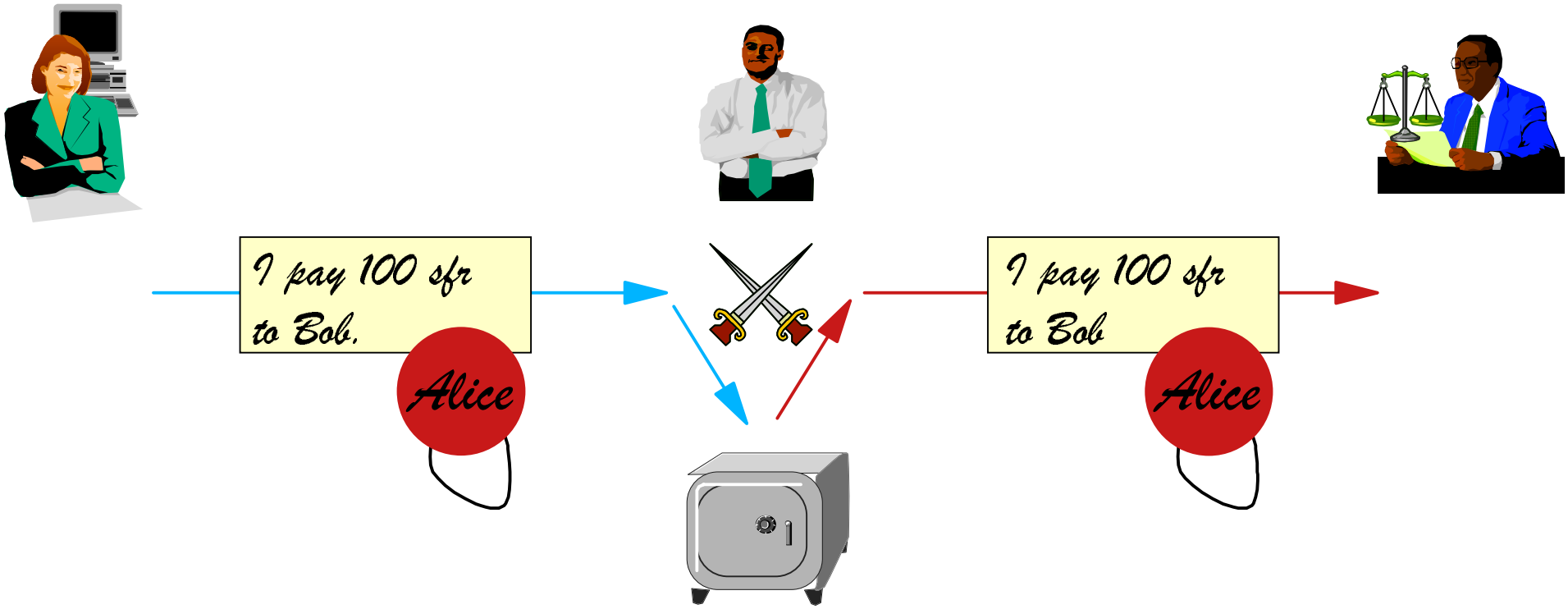


- *Processes* are the entities that need to be trustworthy, not (just) the single steps.
- Security requirements like *anonymity cannot* be fulfilled on the step-level.
- Authorization policies naturally depend on processes.
- *Small* number of *generic, evaluated and certified* business processes are needed.

Business Applications

mi@zurich.ibm.com

Dispute handling

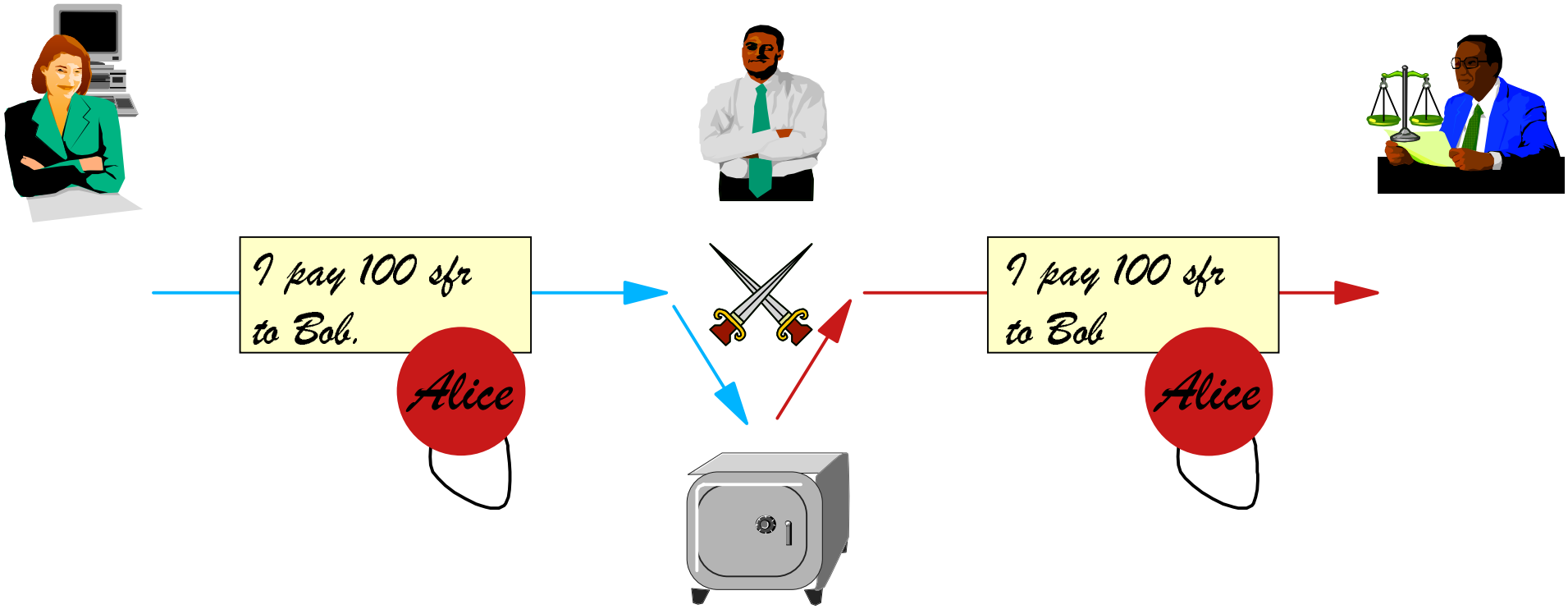


Intended run of a payment system: SET, ecash, ...

Does not exist in existing payment systems, e.g., SET!

mi@zurich.ibm.com

Dispute handling



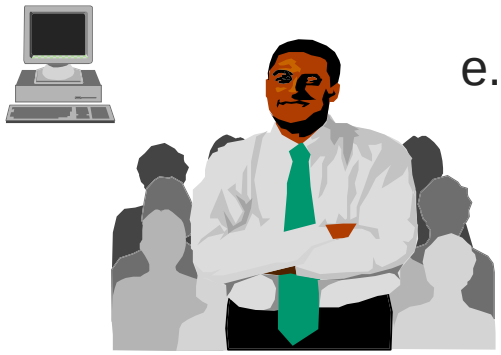
Intended run of a payment

Does not exist in existing systems, e.g., SET!

Deal & transaction browser, dispute interfaces for payments

mi@zurich.ibm.com

Multi-party security



e.g., Kerberos

e.g., SET/iKP

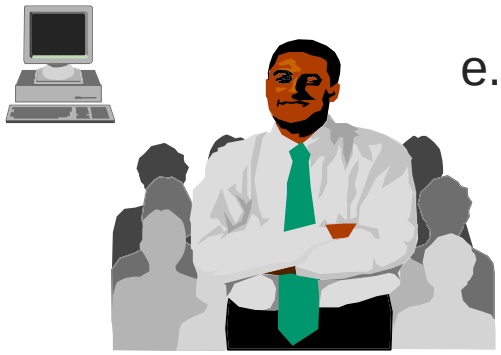
Centralized trust

- everybody's security is based on trust in security admin

Multi-party security

- make trust assumptions explicit; don't require to put trust in opponents
- minimize trust requirements
- distribute trust on many TPs
- leave some choice whom to trust

Multi-party security



e.g., Kerberos

e.g., SET/iKP

Centralized trust

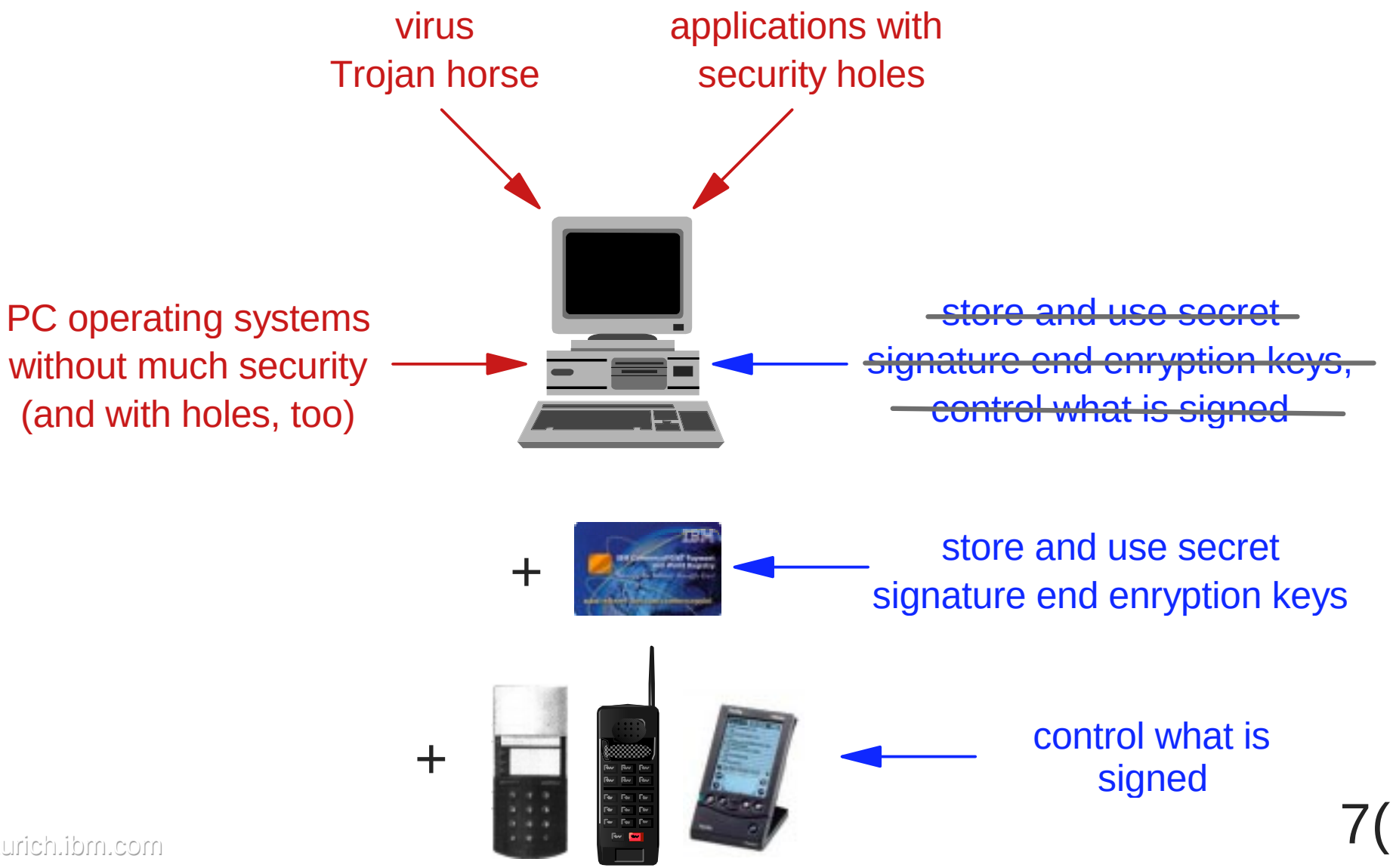
- everybody's security is based on trust in security admin

Multi-party security

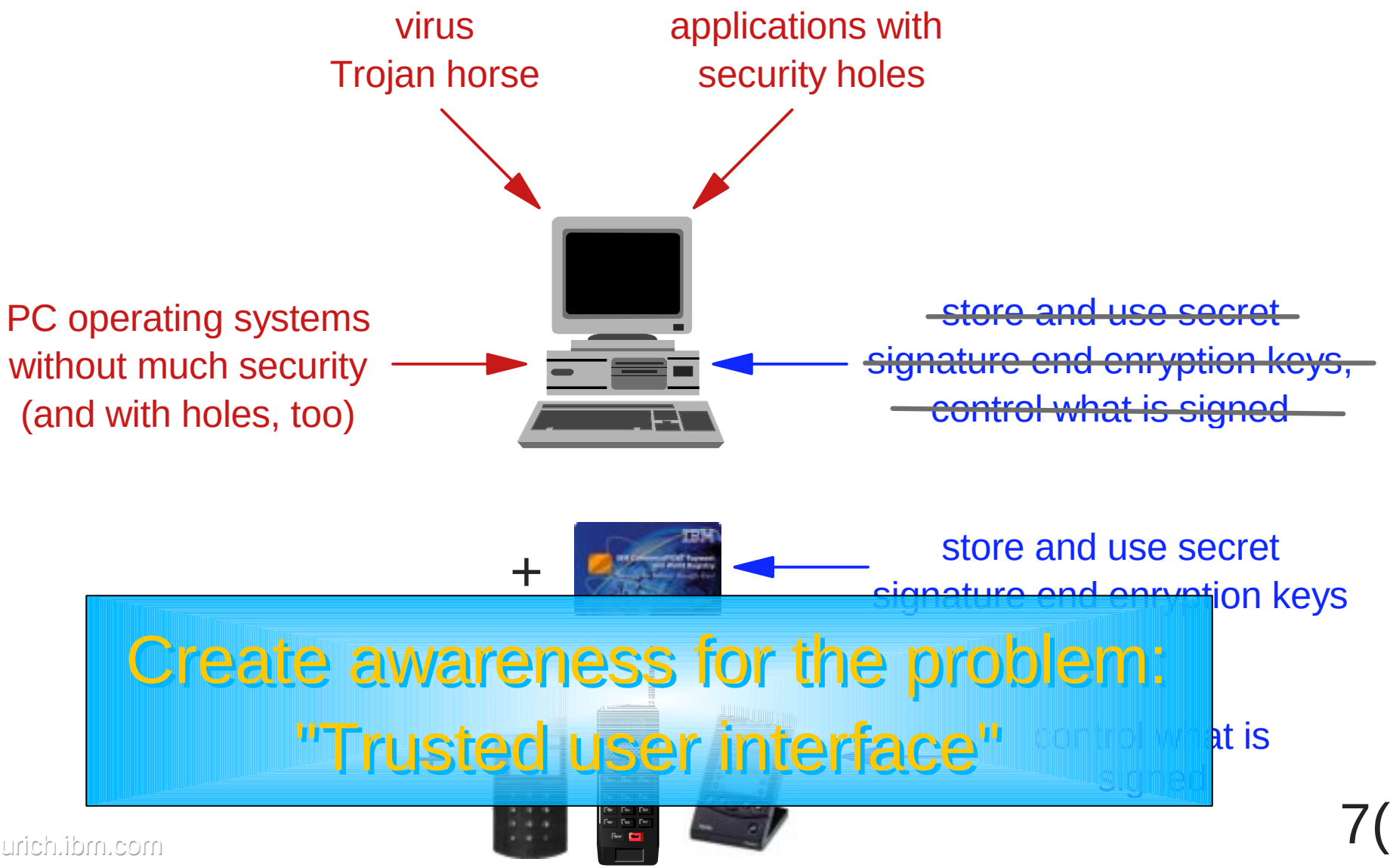
- make trust assumptions explicit; don't require to put trust in opponents
- minimize trust requirements
- distribute trust on many TPs
- leave some choice whom to trust

Symmetric design, all security requirements can be satisfied locally

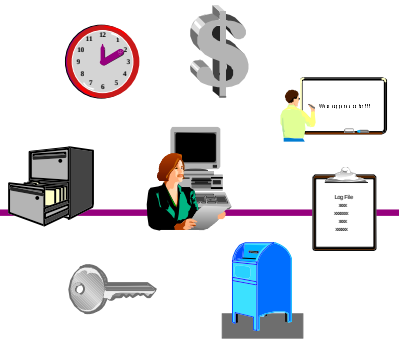
Trusted computing base



Trusted computing base



What are the steps?



Buyer

Code loading

Negotiation

Contract

Delivery

Payment

Merchant

or

Dispute

mi@zurich.ibm.com

What are the steps?

Authentication
Confidentiality
Non-repudiation
Fairness

Buyer

Request for offer →

← Signed Offer

Signed Order →

← **Goods**

Receipt →

Money →

← Receipt

Authentication
Confidentiality
Non-repudiation
Fairness

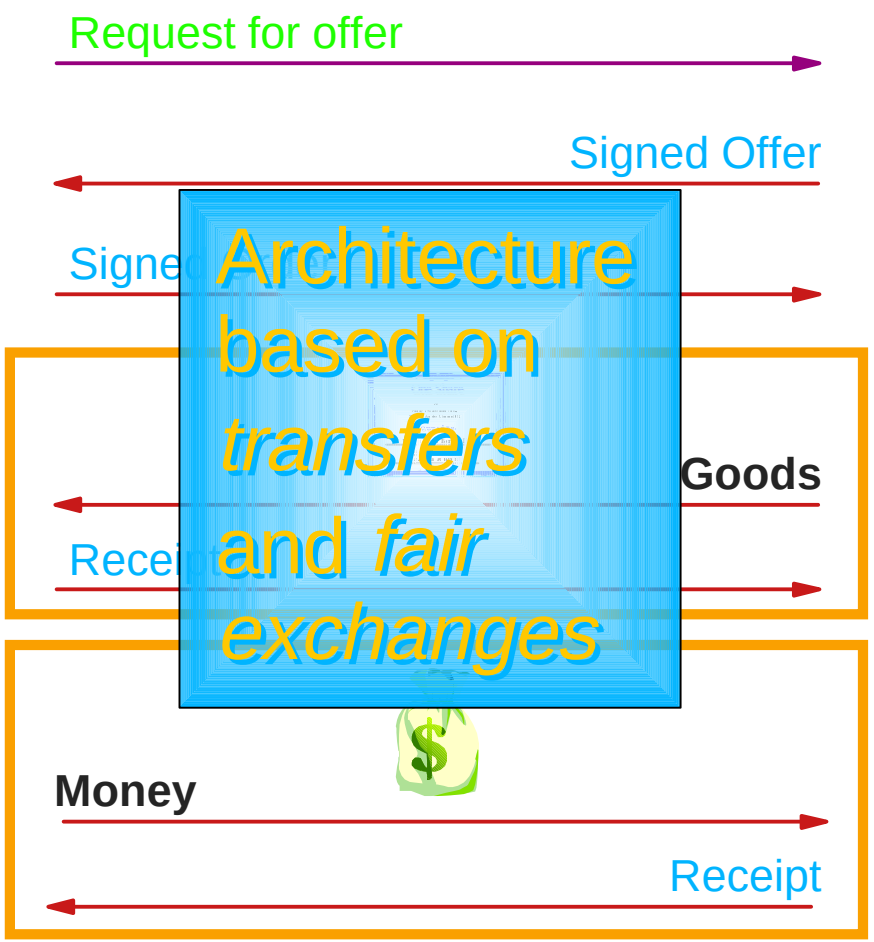
Merchant

mi@zurich.ibm.com

What are the steps?

Authentication
Confidentiality
Non-repudiation
Fairness

Buyer



Authentication
Confidentiality
Non-repudiation
Fairness

Merchant

mi@zurich.ibm.com

Outline

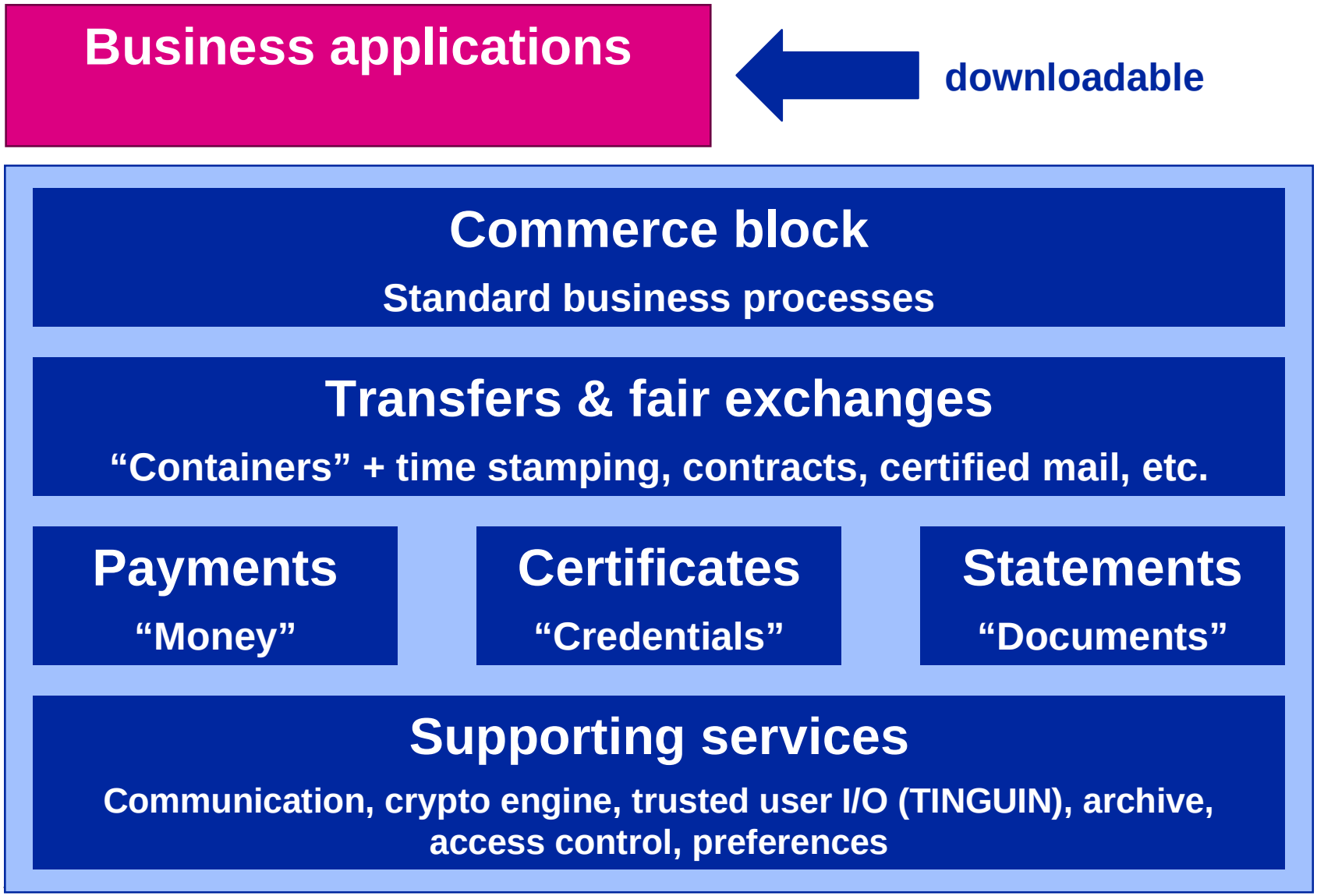
- What is SEMPER?
- Reasoning behind design
- Glimpse on the architecture

More information:

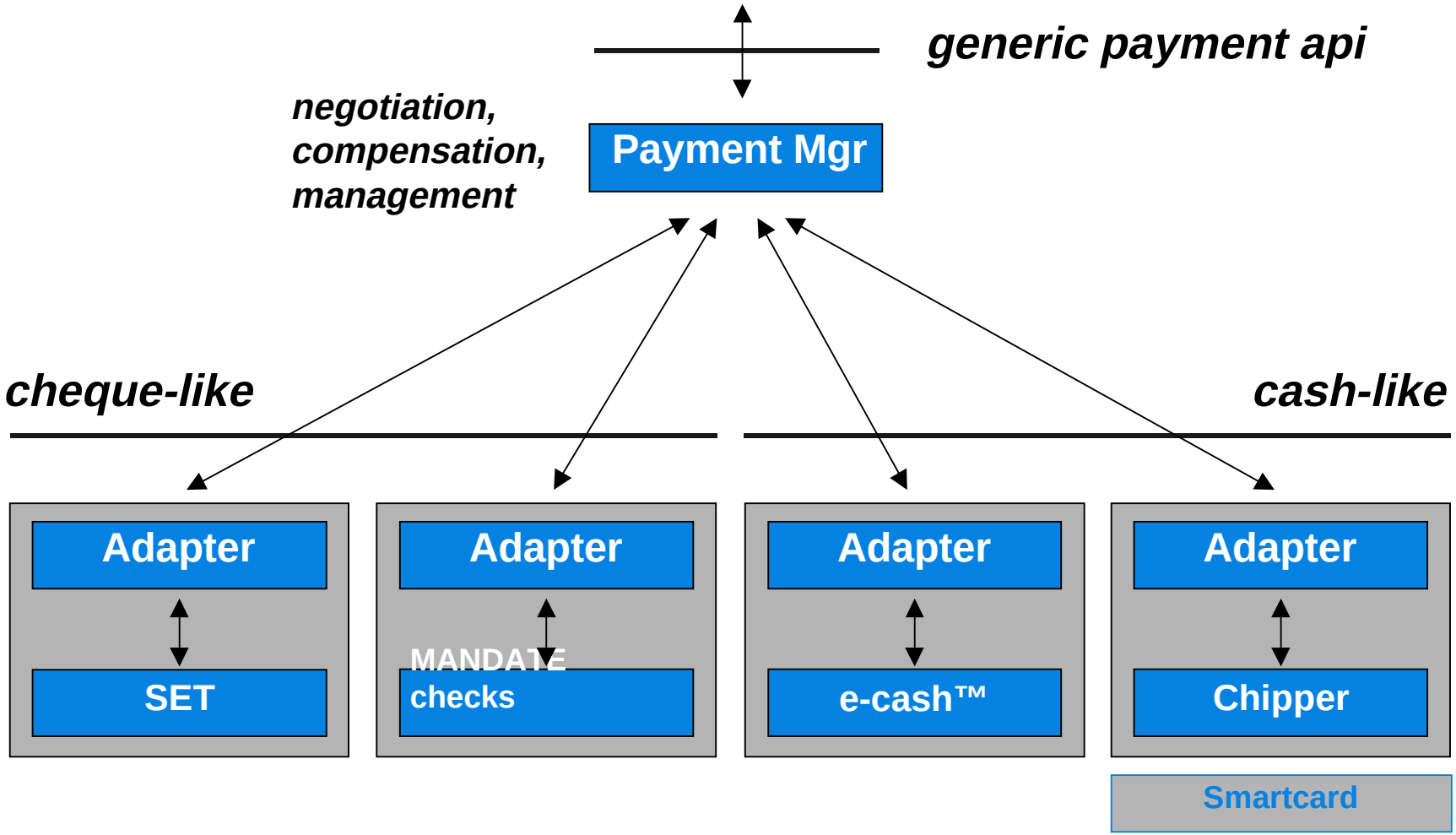
- See <http://www.semper.org>
- Final Report, LNCS Springer-Verlag, early 1999

mi@zurich.ibm.com

SEMPER architecture

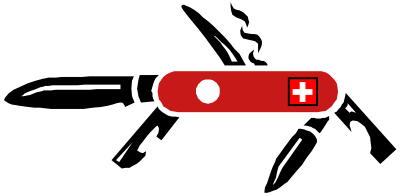


Frameworks



mi@zurich.ibm.com

What is SEMPER?



The Swiss Knife for Secure E-Commerce

- Framework for secure electronic commerce
  - coherent, comprehensive, extensible
- Principles
  - multi-party security
  - linking of secure steps into secure processes
  - document-level security
  - supports secure transfers and fair exchanges

mi@zurich.ibm.com