Michael Waidner
(wmi@zurich.ibm.com)
IBM Corporation, Research Division
Zurich Research Laboratory

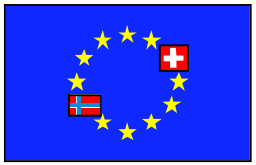
Secure Electronic MarketPlace for EuRope:
Quick summary and some conclusions

IST'98 -- Information Society Technologies Conference

Vienna, December 2, 1998

What is SEMPER?

SEMPER

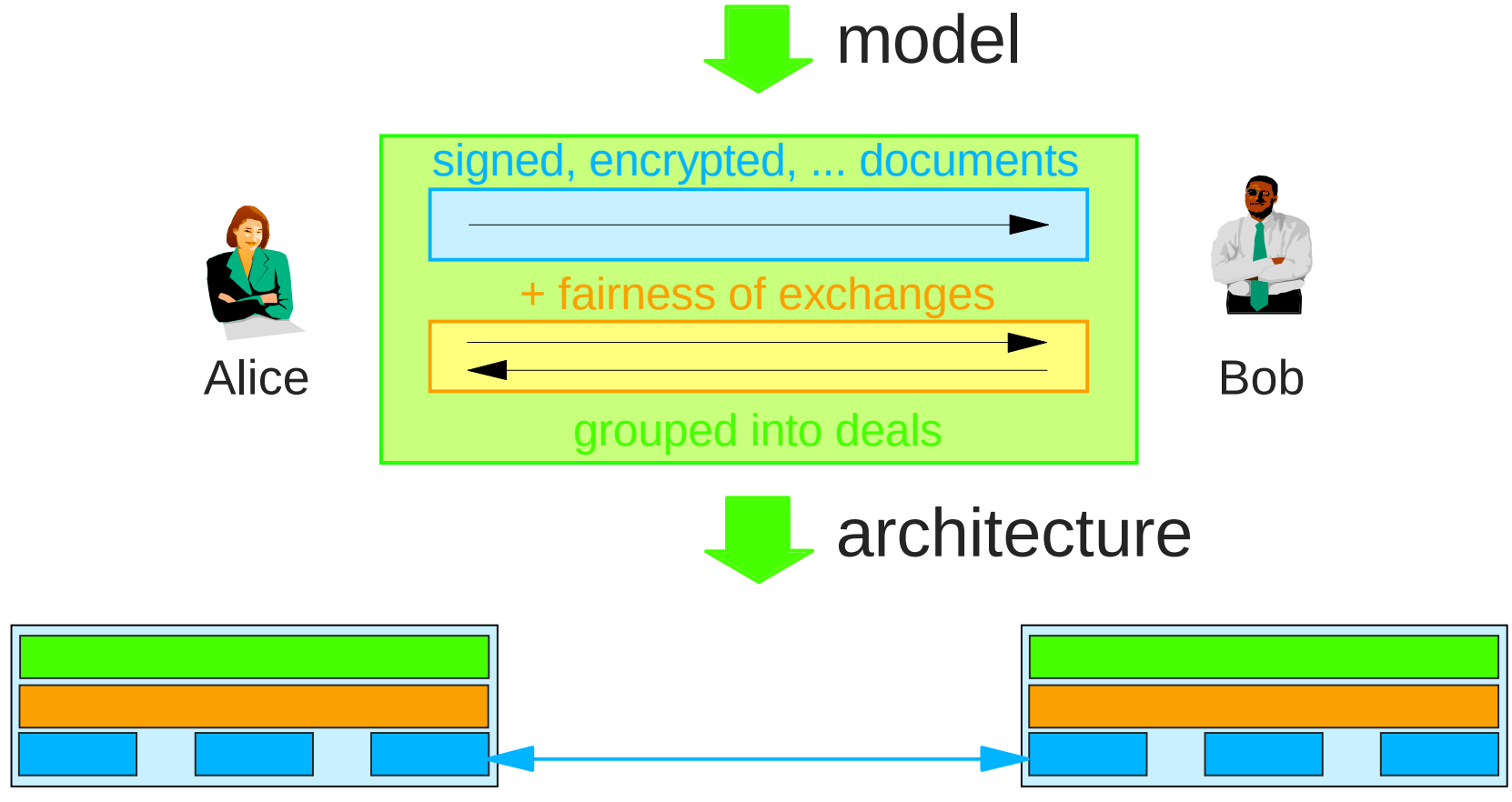


acts

- ACTS-funded R&D project 1995-1998
  - ~30 people, ~20 partners
- Extensible, coherent and complete framework for secure electronic commerce
- Results
  - architecture and protocols
  - prototype, trials & evaluations
  - Semper electronic commerce agreement

Key elements of SEMPER architecture

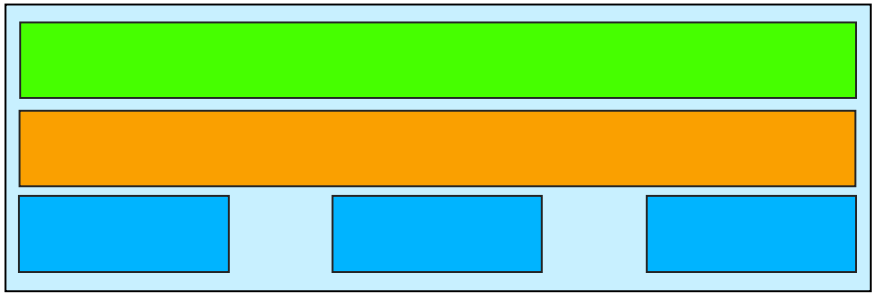
Offer/order 10t banana, buy 100'000 IBM, re/re/re/negotiate and sign and fulfil (and dispute) a contract, file a document at court, ...



Key elements of SEMPER architecture

standard buyer/seller scenarios, ... +
interactive person-to-person ecommerce (FIT)

generic APIs and SPIs



inline, optimistic fair exchange, ...

SET, ecash, Mandate, ...

X.509, ...

signing & encrypting documents

confidential & anonymous "channels"

Objectives

- Quick summary
  - for details see <www.semper.org>

- Some conclusions
  - research in secure electronic commerce for the next few years

Research topics in secure electronic commerce for the next few years

- There is no trustworthy computing base for e-commerce.
- There is no sufficiently secure legal basis for using digital signatures now, accross borders, using insecure SW&HW.
- There are many secure steps (payment, signatures), but only few secure *processes*.
- Users and developers don't understand security well enough. The need for multi-party security in e-commerce is often ignored.

Research topics in secure electronic commerce for the next few years

There is no trustworthy computing base for e-commerce!

- secure operating systems, secure mobile user devices, evaluation criteria, formal methods in security

+

+

OS without security, security holes in standard software, virii, Trojan horses

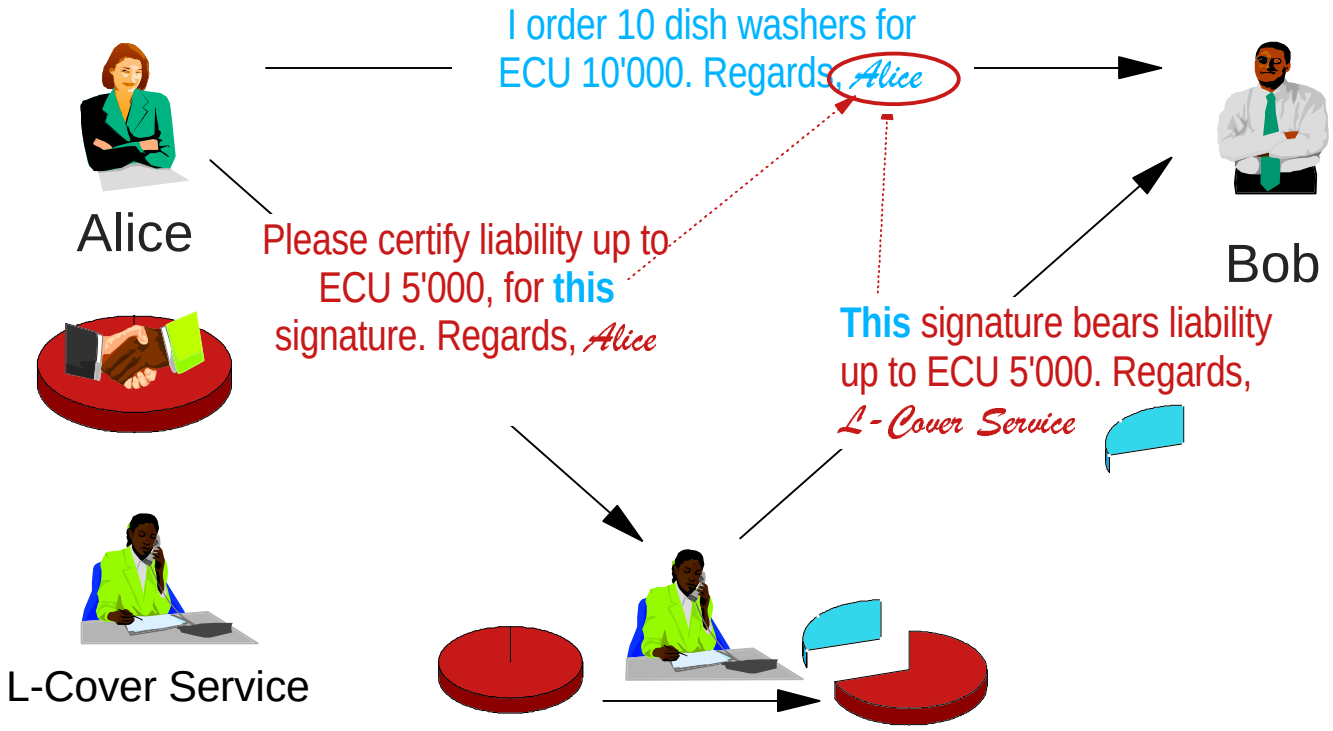
no trusted i/o path to the user (and limited tamper-resistance)

no secure OS (and more)

Research topics in secure electronic commerce for the next few years

There is no sufficiently secure legal basis for using digital signatures now, accross borders, using insecure SW&HW.

- e.g., SEMPER: SECA + instant certificates for liability limits



Research topics in secure electronic commerce for the next few years

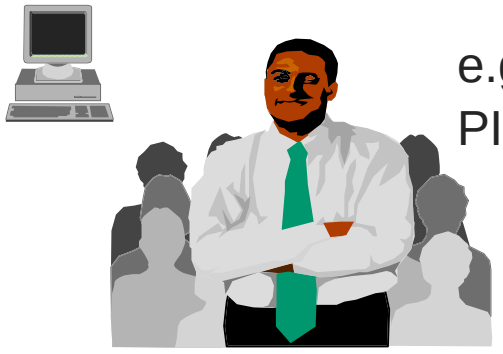
There are many secure steps, but only few secure *processes.*

- secure business applications, workflow, supply chain, ...
- evaluation criteria and methods
- standardized & certified solutions
- needs to include dispute handling

Research topics in secure electronic commerce for the next few years

Users and developers don't understand security well enough. The need for *multi-party security* in e-commerce is often ignored.

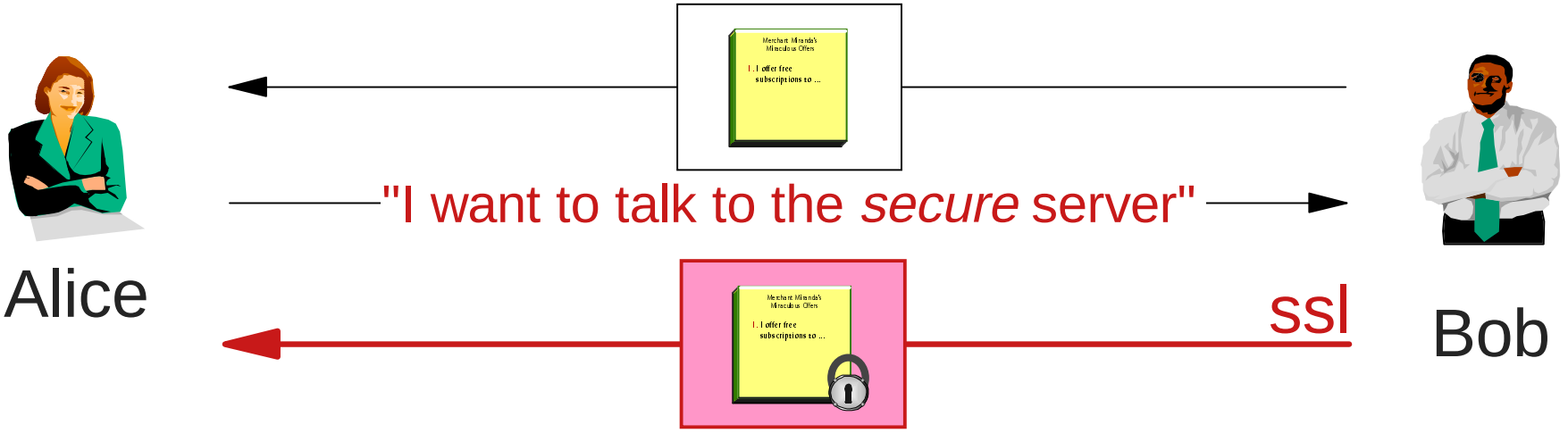
- create awareness, educate about weaknesses & techniques
- multi-party secure protocols, privacy-friendly technology



e.g., Kerberos, PINs, SSL

e.g., dig. Sign., iKP, optimistic fair exchange

Current situation



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

"Now I'm talking to Bob!"

US export-controlled crypto?

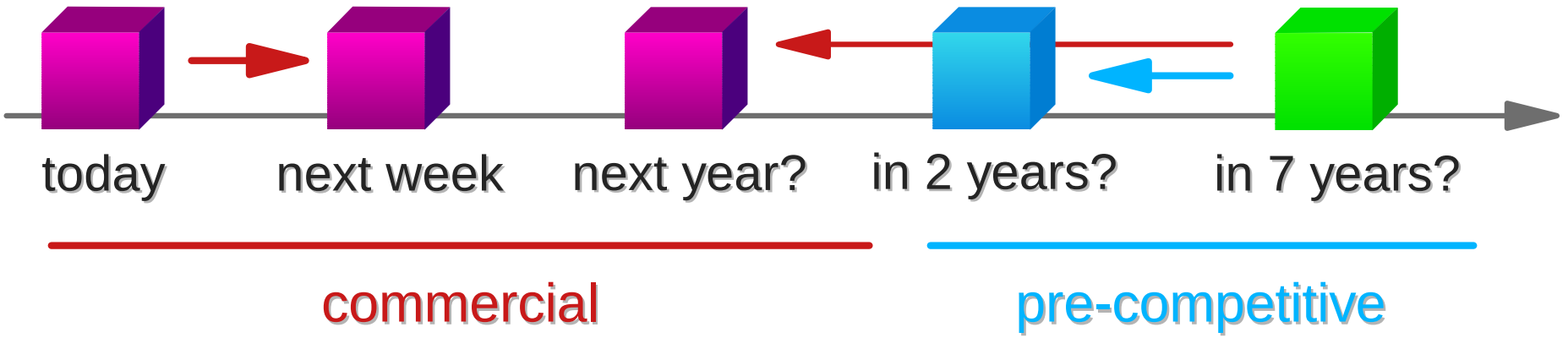
"My messages are secure!"

"If he cheats me I can go to court"

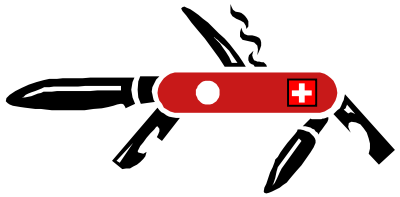
SSL is transparent to the application, thus, *no signatures!*

Three types of projects

- Projects and the EU must be clear about their goals
  - commercial product development
  - pre-competitive product development
  - no product development at all: research & proof of concept
- Bridging the gap between research and product



Summary



- SEMPER
  - Coherent, comprehensive, extensible framework for secure electronic commerce
  - Architecture, protocols, research prototype
- Important topics for research
  - Trustworthy computing base for e-commerce
  - Legal infrastructure for electronic commerce
  - Security for business processes, not for steps only
  - Build and verify multiparty-secure solutions