Privacy-Preserving Authorization Schemes

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, France

State-of-the art: client-server

- Server grants or denies privileges to client, according to client's identity
- Personal data must be recorded: evidence in case of dispute

This paradigm is obsolete

- Internet transactions involve more than 2 parties (e.g., customer, merchant, credit card company, banks, delivery company, …)
- The parties have different, competing interests
  => mutually suspicious

Need-to-know principle

- A merchant does not need to know the real identity of a customer, only the validity of the money order
- The customer's bank does not need to know the identity of the merchant, only the reference of his bank account
- Etc.

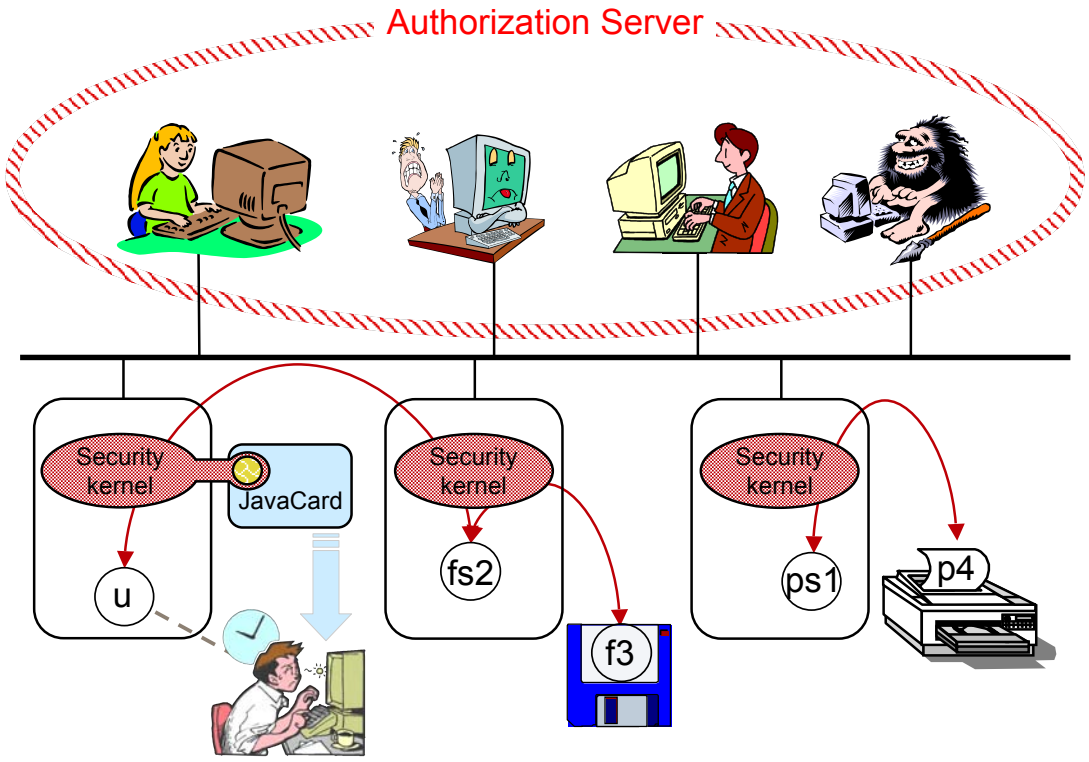
… of course

- Real identities would be disclosed to a judge in case of dispute, or on request by judicial authorities (to prevent money laundering, for instance)

Proofs of Authorization (1)

- Restricted certificates:
  - Different certificates as proofs of different attributes:
    ex. majority, driving license, …
  - "Partial Revelation of Certified Identity" by F. Boudot, CARDIS 2000
  - Pbs: linkability, evidence collection, revocation, …

Proofs of Authorization (2): MAFTIA



MAFTIA project

- **M**alicious- and **A**ccidental-**F**ault **T**olerance in **I**nternet **A**pplications
- European project IST-1999-11583
  http://www.research.ec.org/maftia
- Jan.2000 - Dec.2002
  5.5 M€, 45 person.years