PRIVACY ENHANCING TECHNOLOGIES

A CONTRIBUTION TOWARDS A STRUCTURAL SOLUTION FOR INFORMATIONAL PRIVACY PROBLEMS

Drs John J. Borking

Associate Board Member

Data Protection Authority

The Netherlands

Where are PETs in the debate?

- Legal framework
- Privacy Enabling & Privacy Enhancing Technologies

1. Anonymity
2. Pseudonymity
3. Privacy Knowledge Engineering (PYKE)
4. Control & feedback

The Privacy Principles applicable to the processing of personal data

- Purpose specification
- Fair and lawful collection
- Proportionality
- Data quality
- Transparency
- Data subject’s rights
- Storage duration
- Right to object
- Security

Legal context for PETs

- Nine privacy principles
- and
- "… against unlawful processing"

ARTICLE 17 (95/46/EC) + RECITAL 46 OUTLINES:

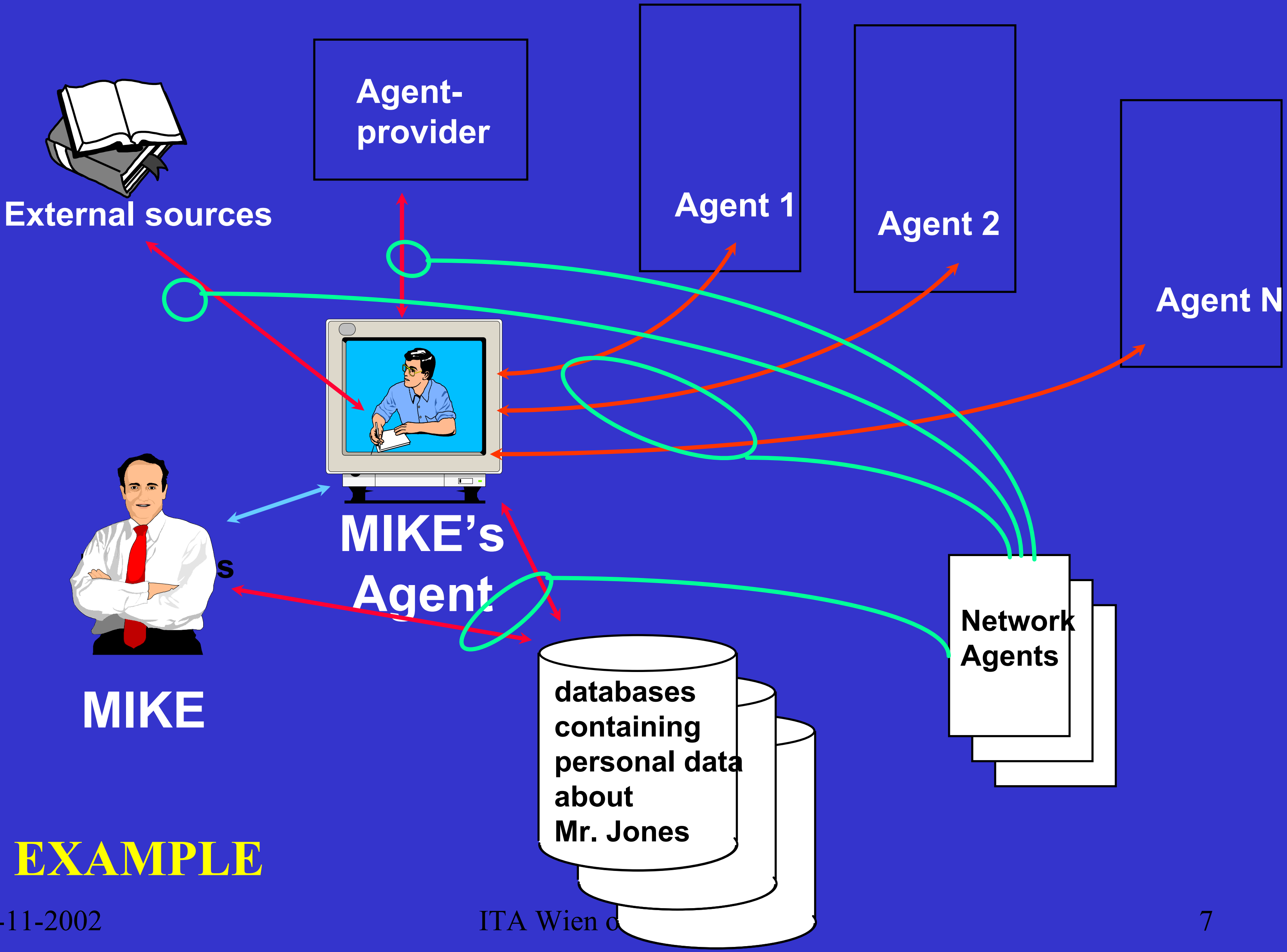
The person responsible shall take suitable technical and organizational measures to protect personal data both at the design & processing phase of the system:

- **AGAINST LOSS**
- **AGAINST ANY FORM OF UNLAWFULL PROCESSING**
- **TO PREVENT UNNECESSARY COLLECTION AND FURTHER PROCESSING**
- **CONSIDERING STATE OF ART, COSTS, RISKS**

UNDERSTANDING:

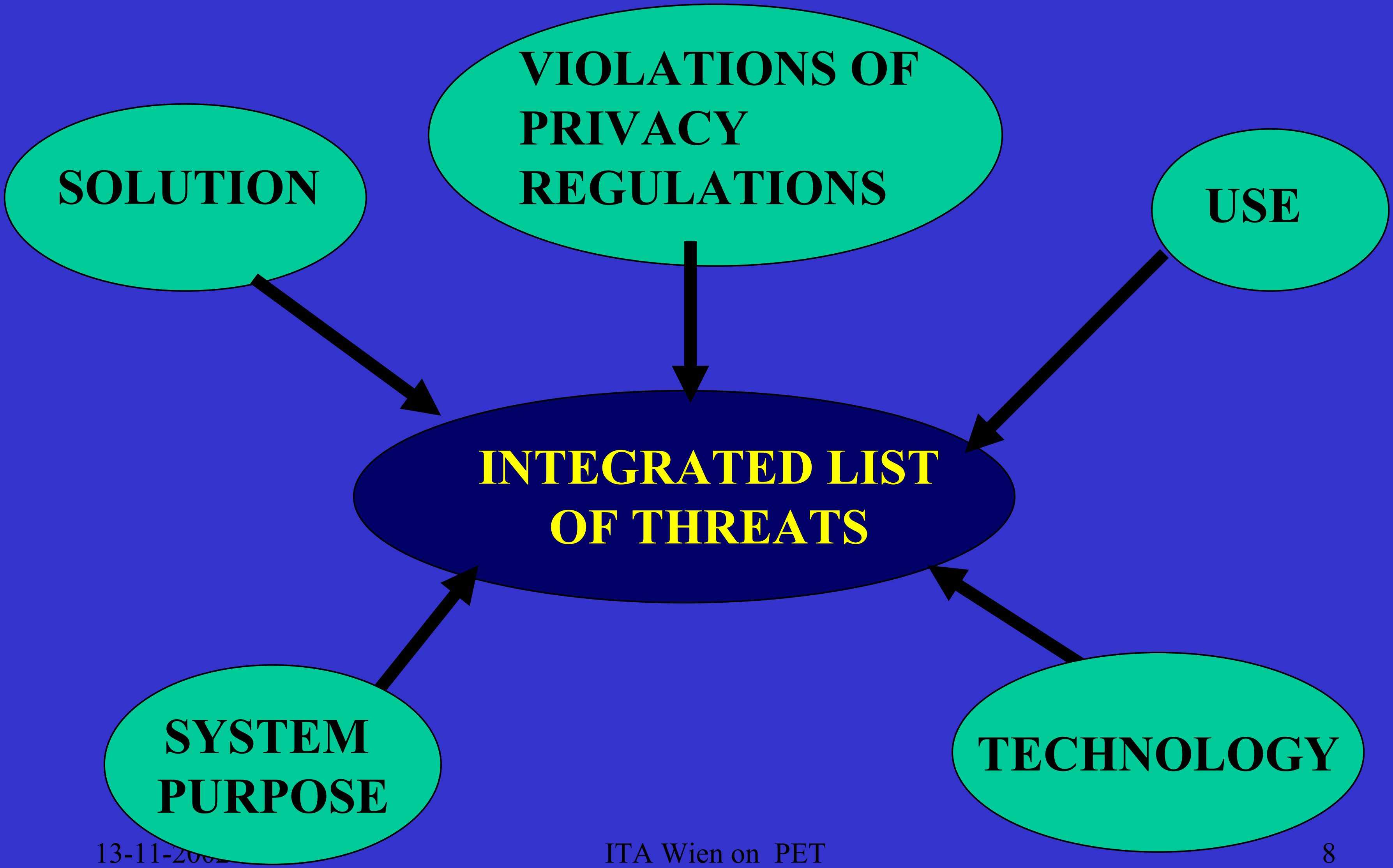
- Incidental vs. Structural = how to solve the privacy problem!
- The law alone can’t protect privacy
- From reactive to proactive
- The Cholera metaphor

VISUALIZATION OF THE AGENT AND PERSONAL DATA FLOW



AN EXAMPLE

PRIVACY THREATS



VIOLATIONS OF PRIVACY REGULATIONS

SOLUTION

USE

INTEGRATED LIST OF THREATS

SYSTEM PURPOSE

TECHNOLOGY

PET POLICY

Can the EC directive 95/46 be translated into hard specifications?

Privacy-Enhancing Technologies PETs

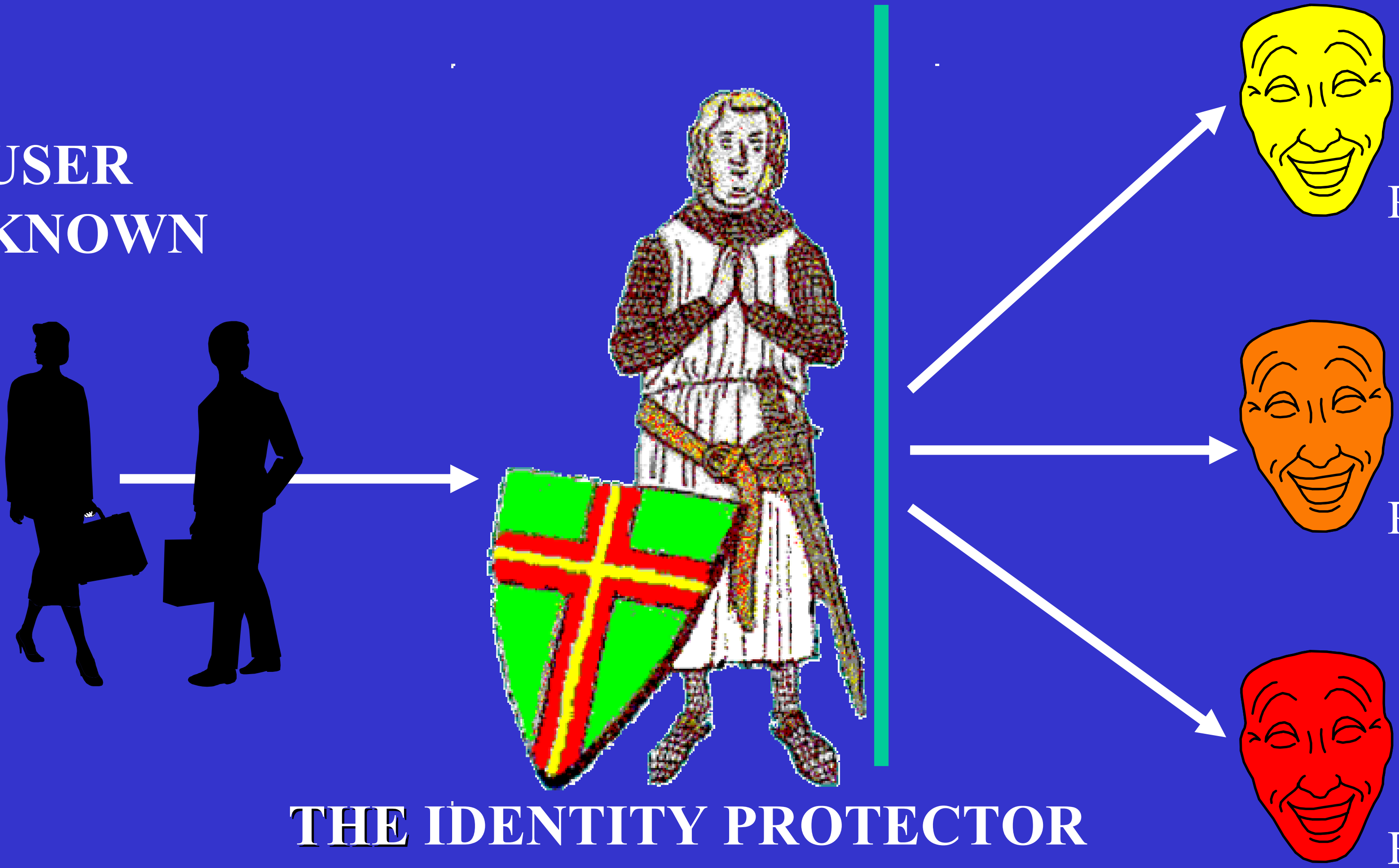
The Path to Anonymity, Augustus 1995

The concept of the Identity Protector

And Identity Domains + 6 design models

ISBN:90 74087 12 4

PRIVACY-ENHANCING TECHNOLOGIES



USER
KNOWN

THE IDENTITY PROTECTOR

PID 1

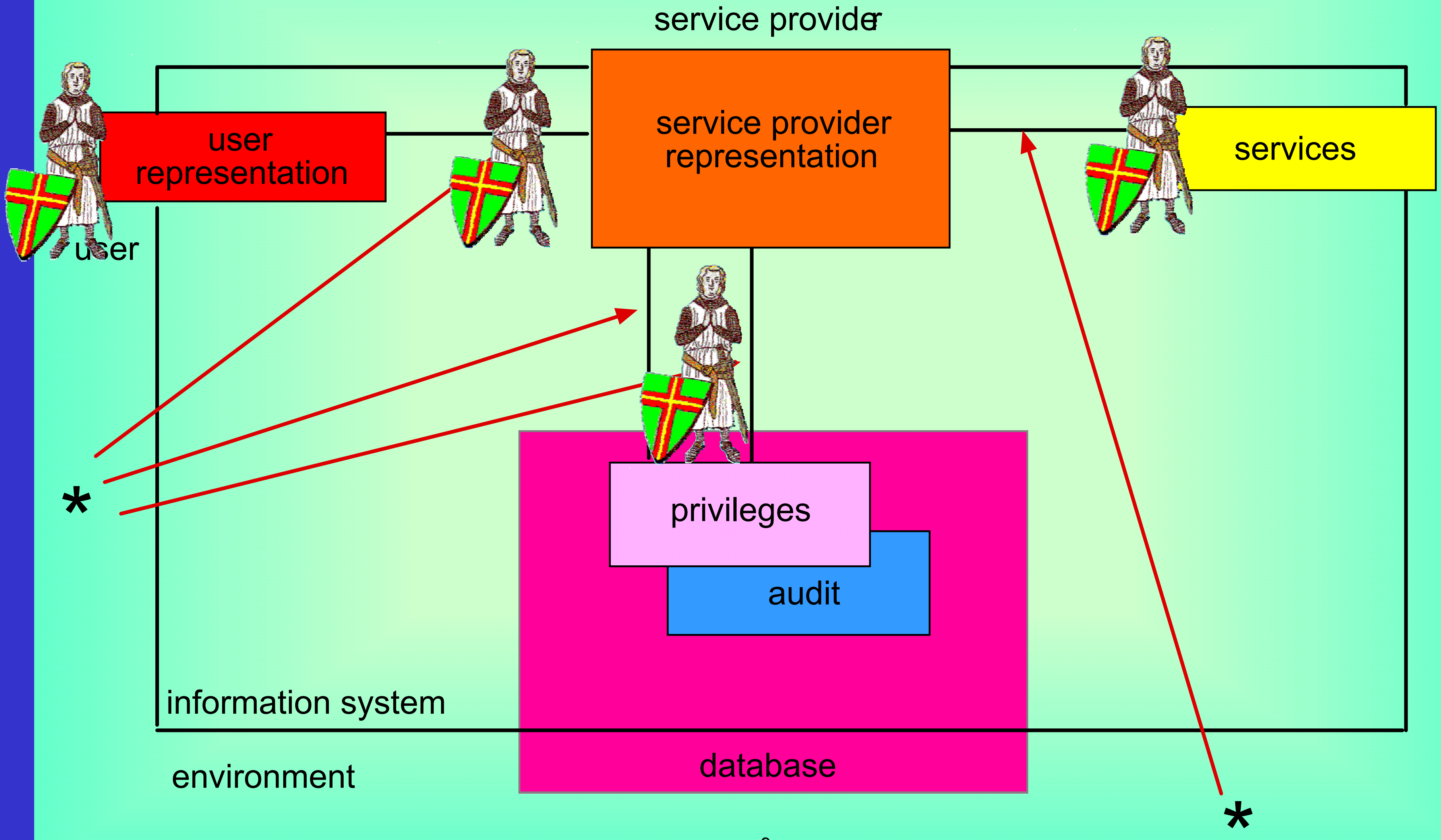
PID 2

PID 3

IDENTTY DOMAINS

PSEUDO IDENTITY DOMAINS

STRUCTURE OF AN INFORMATION SYSTEM



* = interaction lines

DEFINITI0N OF PETs

PETs IS A SYSTEM OF ICT MEASURES PROTECTING THE INFORMATIONAL PRIVACY BY ELIMINATING OR MINIMIZING PERSONAL DATA OR BY PREVENTING UNNECESSARY OR UNWANTED PROCESSING OF PERSONAL DATA, WITHOUT LOSS OF FUNCTIONALITY

WHAT'S PETs DOING?

- IT INCREASES THE POSSIBILITIES TO PROTECT BETTER THE PRIVACY OF THE INDIVIDUAL

- IT INCREASES THE POSSIBILITIES FOR CITIZENS TO CONTROL AND HAVE A SAY OVER THEIR OWN PERSONAL DATA

ERGO: Protection of Privacy starts with the design of Information Systems 0nline and Offline

General trends on PET’s

- Growing awareness (since 1995)
- Increasing availability online and offline
- Rising expectations
- Evaluation & guidance
- Marketing effort is needed!

Analysis of Data Streams and the Deployment of PET

- Phase 1: Capture of Personal Data (Intake)
  - -Built-in tools data minimization
  - -Fending off Classes of Data for purpose binding
- Phase 2: Processing and Storage of Data
  - -Identity Protector & workflow Mgt
- Phase 3: Distribution of Data
  - - Access protocols, PKI/TTP, P3P

Basic strategies for PET's

- Minimize: identifiable data
- Eliminate: identifiable data
- Optimize: lawful processing
- Combine: additional solutions
- Convince: responsible stakeholders

A few of the realized PET projects

- ICL Health Care systems (1997)
- Anonymous customer tracking system LADIS (1998)
- NCR Teradata Warehouse- privacy enabling tools (1999)
- Biometrics with decentralized storage of templates (1999)
- Privacy Incorporated Software Agent (PISA) (under construction)
- Mobimiles (Electronic Road Pricing)

PET EXAMPLES

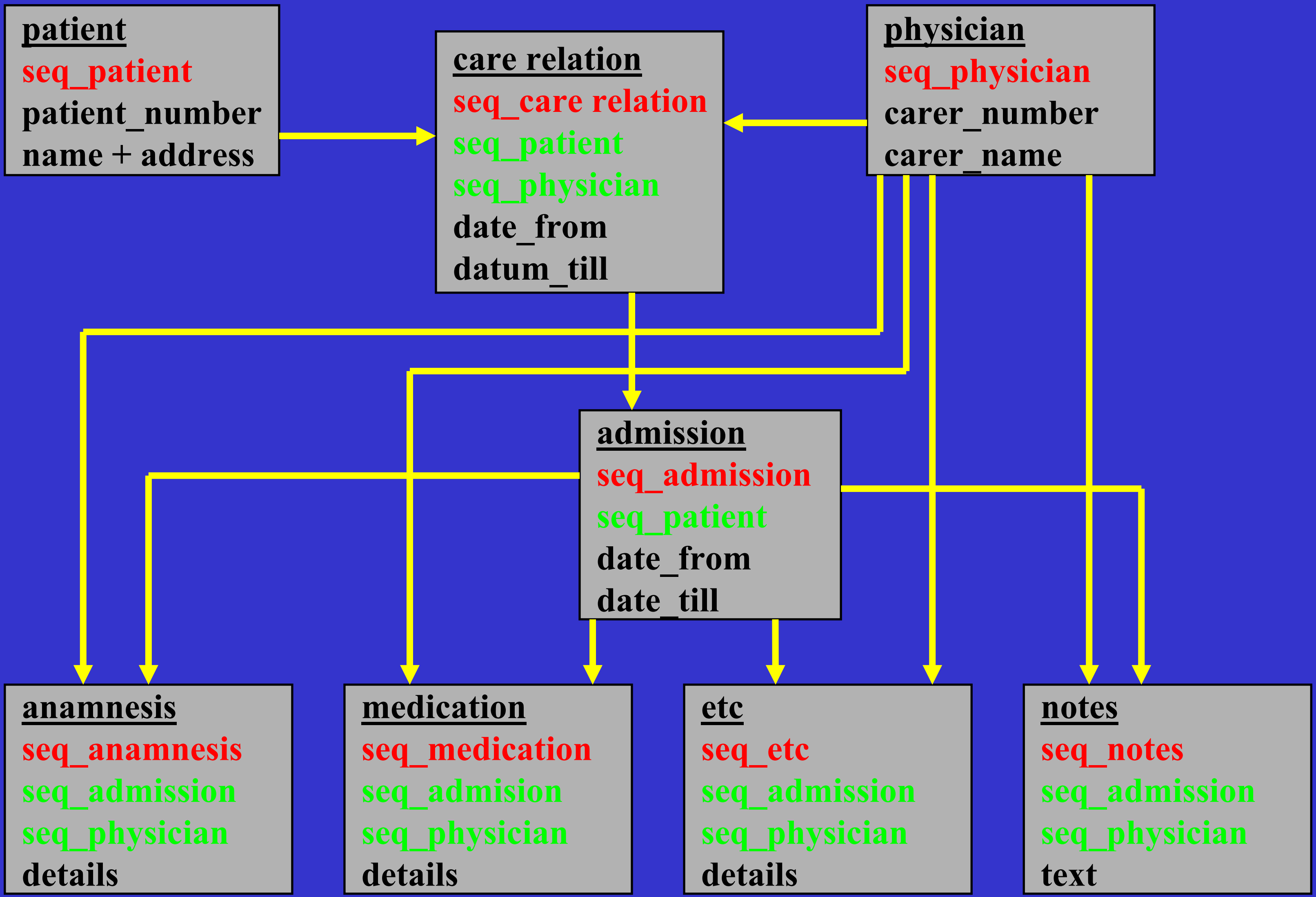
PRIVACY INCORPORATED DATABASE ®

Prior Conditions

- Relational Database
- Client / Server Architecture

HOSPITAL INFORMATION SYSTEM

Basic Tables with relations



patient
seq_patient
patient_number
name + address

care relation
seq_care relation
seq_patient
seq_physician
date_from
datum_till

physician
seq_physician
carer_number
carer_name

admission
seq_admission
seq_patient
date_from
date_till

anamnesis
seq_anamnesis
seq_admission
seq_physician
details

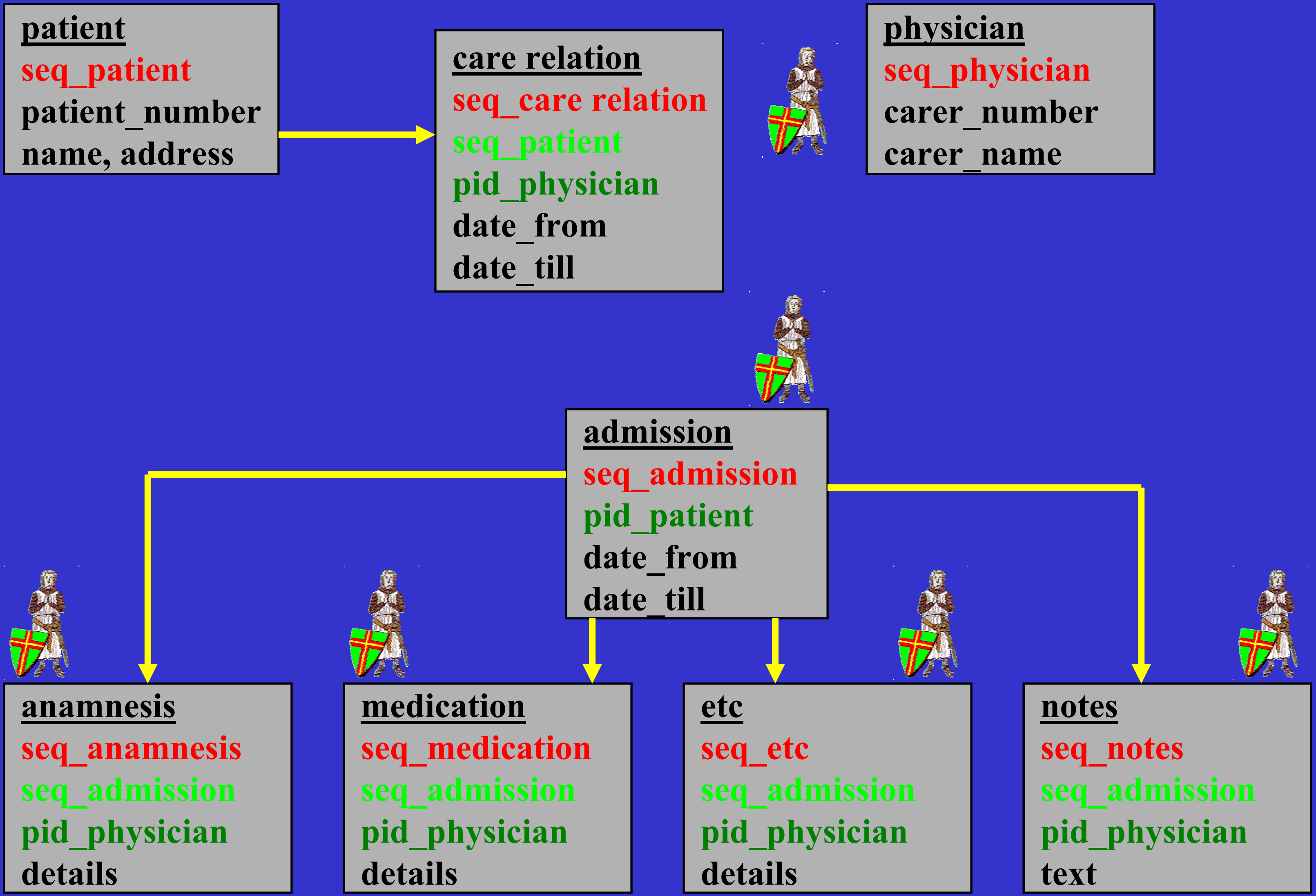
medication
seq_medication
seq_admision
seq_physician
details

etc
seq_etc
seq_admission
seq_physician
details

notes
seq_notes
seq_admission
seq_physician
text

Hospital Information System

Basic tables with Pseudo Identities



patient
- seq_patient
- patient_number
- name, address

care relation
- seq_care relation
- seq_patient
- pid_physician
- date_from
- date_till

physician
- seq_physician
- carer_number
- carer_name

admission
- seq_admission
- pid_patient
- date_from
- date_till

anamnesis
- seq_anamnesis
- seq_admission
- pid_physician
- details

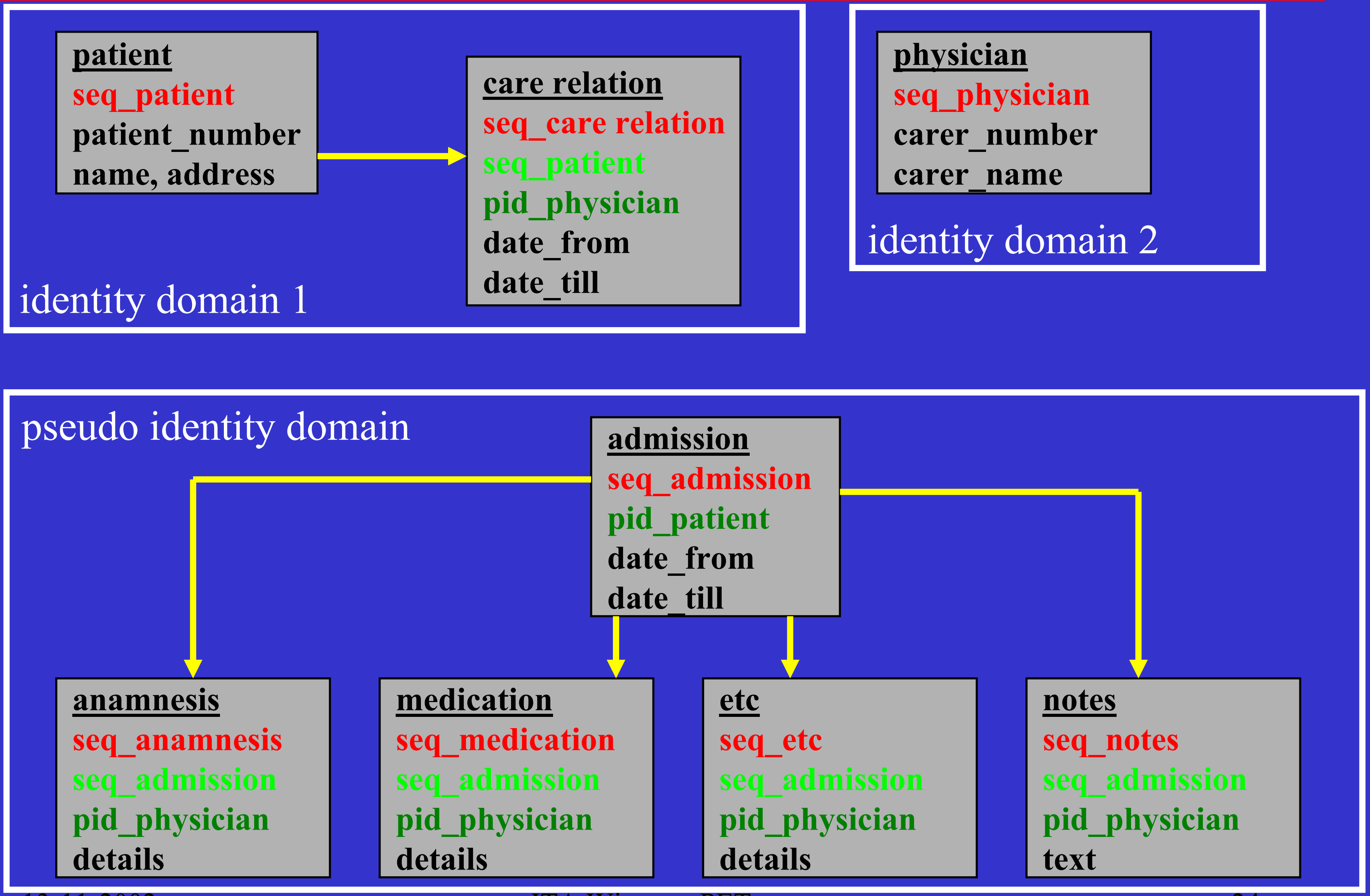
medication
- seq_medication
- seq_admission
- pid_physician
- details

etc
- seq_etc
- seq_admission
- pid_physician
- details

notes
- seq_notes
- seq_admission
- pid_physician
- text

Hospital Information System

Lay out showing the domains



patient
seq_patient
patient_number
name, address

care relation
seq_care relation
seq_patient
pid_physician
date_from
date_till

identity domain 1

physician
seq_physician
carer_number
carer_name

identity domain 2

pseudo identity domain

admission
seq_admission
pid_patient
date_from
date_till

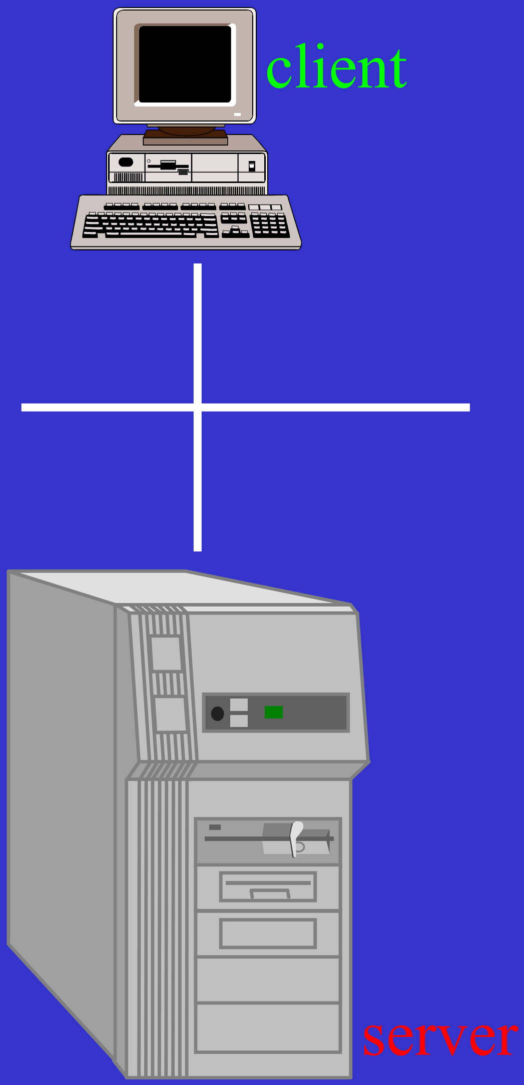
anamnesis
seq_anamnesis
seq_admission
pid_physician
details

medication
seq_medication
seq_admission
pid_physician
details

etc
seq_etc
seq_admission
pid_physician
details

notes
seq_notes
seq_admission
pid_physician
text

Dialogue in PID Hospital Information System



- login with 'physician name' (pn)
- transfer 'pn' to the server
- check in table 'physician'
- transfer 'sequence primary key of physician' to the client
- encrypt to 'pid_physician'
- transfer the 'pid_physician' to the server
- search table 'care relation'
  select 'sequence primary key of_patient'and
  search table 'patient'
- transfer identified patients to client
- select the required patient
  encrypt 'seq_patient' to 'pid_patient
  transfer 'pid_client' to server
- search table 'anamnesis' with pid of physician and of patient etc.

The PET principles

Pseudo - identity

Zero Knowledge Systems
Anonymous surfing the Internet
Dutch Burns Information System
Social Security Information System
etc. etc.

Dutch Burns Information System

Practically all seven PET Principles

- Biometrics to authenticate users fingerprint and voice templates stored on a smartcard
- Trusted Third Party to verify identity
- Firewalls to prevent intrusion by unwanted third parties
- Virtual Private Network
- Database encryption
- Balanced dataset

The PET principles

Control & Feedback - 1 -

- Control is empowering people to find out what information is captured about them and who can get hold of it
- Feedback is informing people when and what information is being captured and to whom made available

The PET principles

Feedback and Control - 2 -

- Create audit trails

  to log access to personal data
  (technical measure)

  to monitor the files and action upon
  unexpected entries
  (organisational measure)

PYKE, the new branch of PET

Building the nine privacy principles into information systems to realize privacy knowledge engineering (PYKE). The use of ontologies is needed

The method : Design Embedded Privacy Risk Management (DEPRM) to assure a system design against privacy risks as discovered in the privacy threat analysis.

ONTOLOGIES

Definition:

Formal machine understandable description of terms and relations in a particular domain

For privacy protection:

Encapsulation of knowledge about the data protection domain in an unambiguous standardization

To resolve the mismatch between law and technology

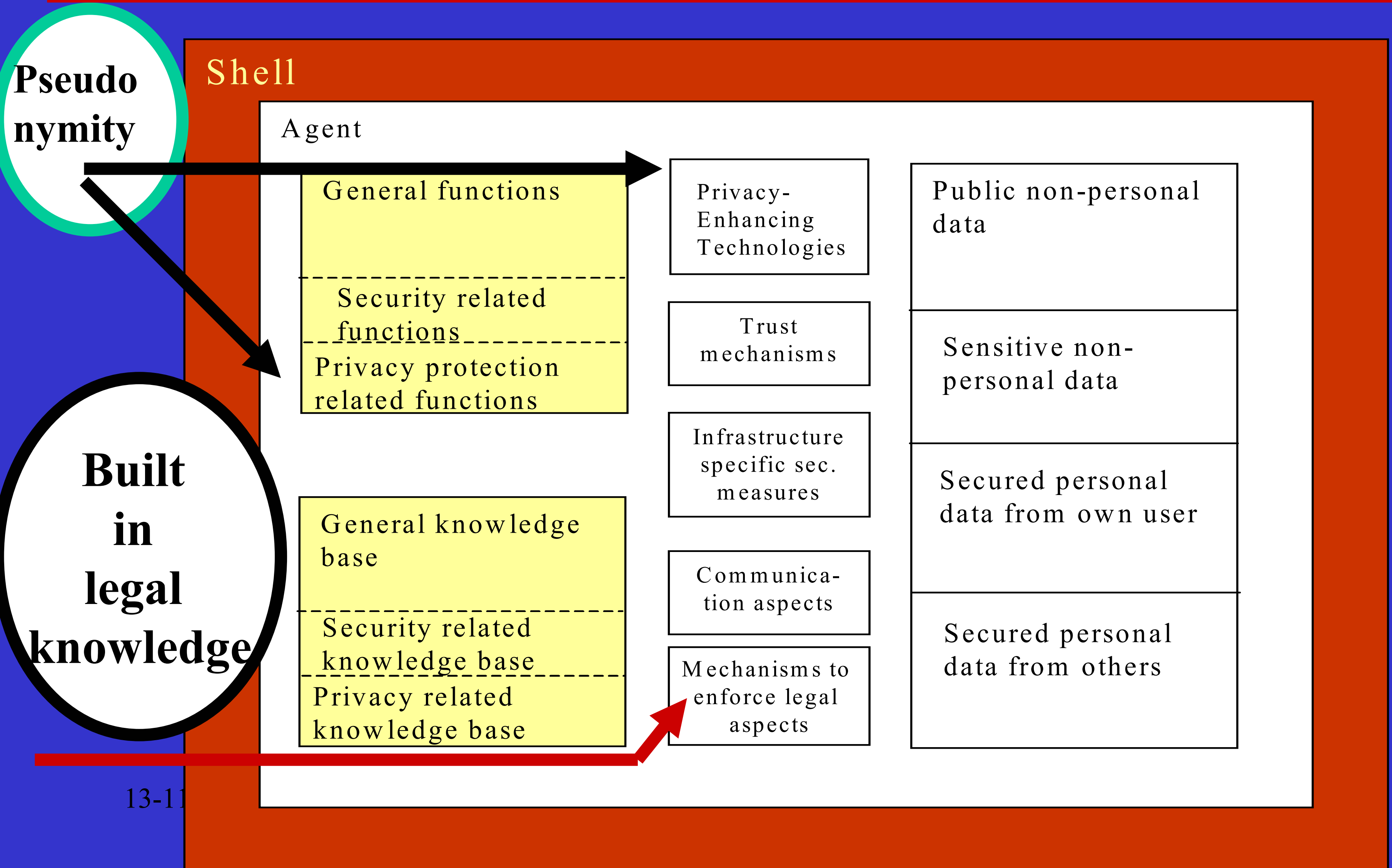
PYKE & DEPREM

1. Determine the privacy principles
2. “Chain” selected articles of the DPD that belong to the chosen privacy principles.
3. Split the principles into a sets of tiny elements
4. Find the ontologies and taxonomies leading to a simplified conceptual model of the principle
5. Add knowledge base to enable interpretation of the queries between the agents
6. Formulate transfer rules
7. Implement required security.

PISA: PRIVACY INCORPORATED SOFTWARE AGENT: MAIN OBJECTIVES OF EU PROJECT

TO PROVE AND SHOW THAT THE PRIVACY OF USER WHILE USING AGENTS IS PROTECTED IN ALL KINDS OF PROCESSES BY INCORPORATING PET FEATURES IN AGENTS

Structure of Privacy Incorporated Software Agent (PISA)


Pseudo
nymity
Shell
Agent
General functions
Security related functions
Privacy protection related functions
General knowledge base
Security related knowledge base
Privacy related knowledge base
Privacy-Enhancing Technologies
Trust mechanisms
Infrastructure specific sec. measures
Communication aspects
Mechanisms to enforce legal aspects
Public non-personal data
Sensitive non-personal data
Secured personal data from own user
Secured personal data from others
Built
in
legal
knowledge

Standard Transfer Rule in PISA

IF APS-1 MATCHES PISA privacy-preference-2 AND APS-2 MATCHES privacy-preference-1AND PII level 2 -1 MATCHES PII level 2 -2 THEN ALLOW disclosure and or exchange PII level 1 -1

PET internationally accepted

Common Criteria Technology Security Evaluation (ISO 15408)

- 9 Privacy - **defined as:**
  - **anonymity**
    - √ no identifiable data at all
  - **pseudonymity**
    - √ identifiable for authorised users only
  - **unlinkability**
    - √ no common identifier to link systems
  - **unobservability**
    - √ anonymous until required for identification

Financial case for implementation of PET

BASIC ASSUMPTION

- Data security is an integral part of the development of information systems
- Privacy protection is an integral part of the data security

THEN……..

Then:

- From scratch:
  design phase might increase. The actual development costs increases only by 1% of the Total Costs of Ownership

- If not and / or existing systems have to be enhanced:
  prohibitive expensive due to breaking up the existing structure of the information systems

PET ONLINE

Types of online software tools

- **Anonymity and pseudonymity tools**
  - Anonymizing proxies
  - Mix Networks and similar web anonymity tools
    - Onion routing
    - Crowds
    - Freedom
  - Anonymous email
- **Encryption tools**
  - File encryption
  - Email encryption
  - Encrypted network connections
- **Filters**
  - Cookie cutters
  - Child protection software
- **“Agents of choice”**
  - Personal information managers
  - P3P

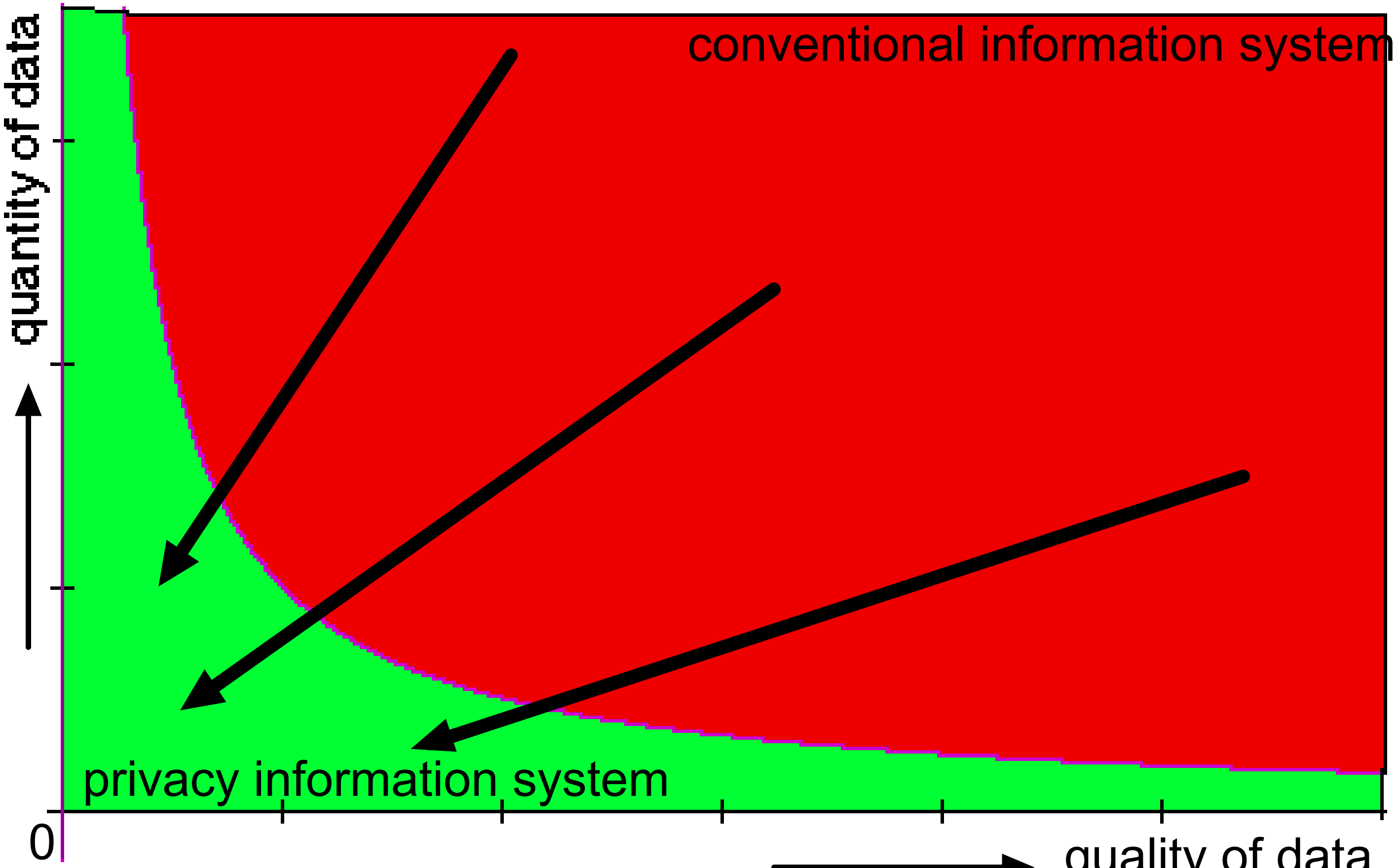
P3P v1.0

- Offers an easy way for web sites to communicate about their privacy policies in a standard machine-readable format
  - Can be deployed using existing web servers
- This will enable the development of tools (built into browsers or separate applications) that:
  - Provide snapshots of sites' policies
  - Compare policies with user preferences
  - Alert and advise the user

PRIVACY ENHANCING TECHNOLOGIES

Objectives:

Quantity
of data



PRIVACY

Can be compared to our skin.
It is a line of defence against intrusion from the outside world.
If we tear down these defences, we become vulnerable.

Privacy cannot be protected adequately unless legal requirements are translated into hard system specifications.

For ongoing activity:

COLLEGE BESCHERMING PERSOONSGEGEVENS

http://www.cbpweb.nl

http:// pet-pisa.nl

Thank you