X.500 data privacy support

Protecting Data

Tutorial at the ITU-T Study Group 17 meeting

Geneva, 20 September, 2007

Erik Andersen
Andersen's L-Service
era@tdcadsl.dk

Purpose of this presentation

To establish awareness that we have been working on IdM related issues for the last 23 years.
This may be an overstatement, but anyway…

So we certainly got a head start

To avoid reinvention of the wheel

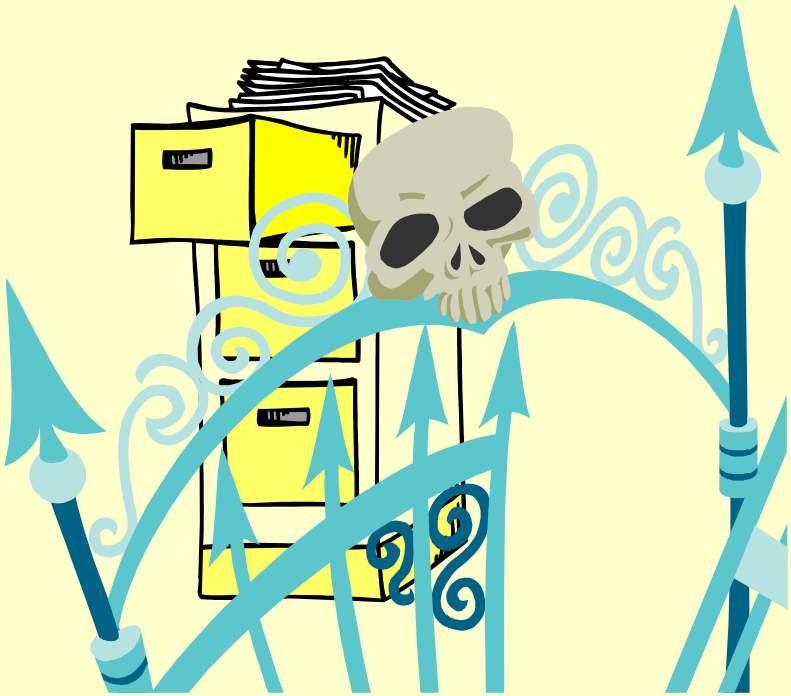
To explore ways to make reuse of a lot of good works

The X.500 set of Recommendations

- Consists of ten parts
- A lot of heavily skilled people have put enormous effort into this work during the last 23 years
- The **Not Invented Here** syndrome should not be an obstacle for its recognition
- It takes some effort to understand it, but it is a greater effort to reinvent it
- It is more relevant than ever

To know me is to love me

Protecting data



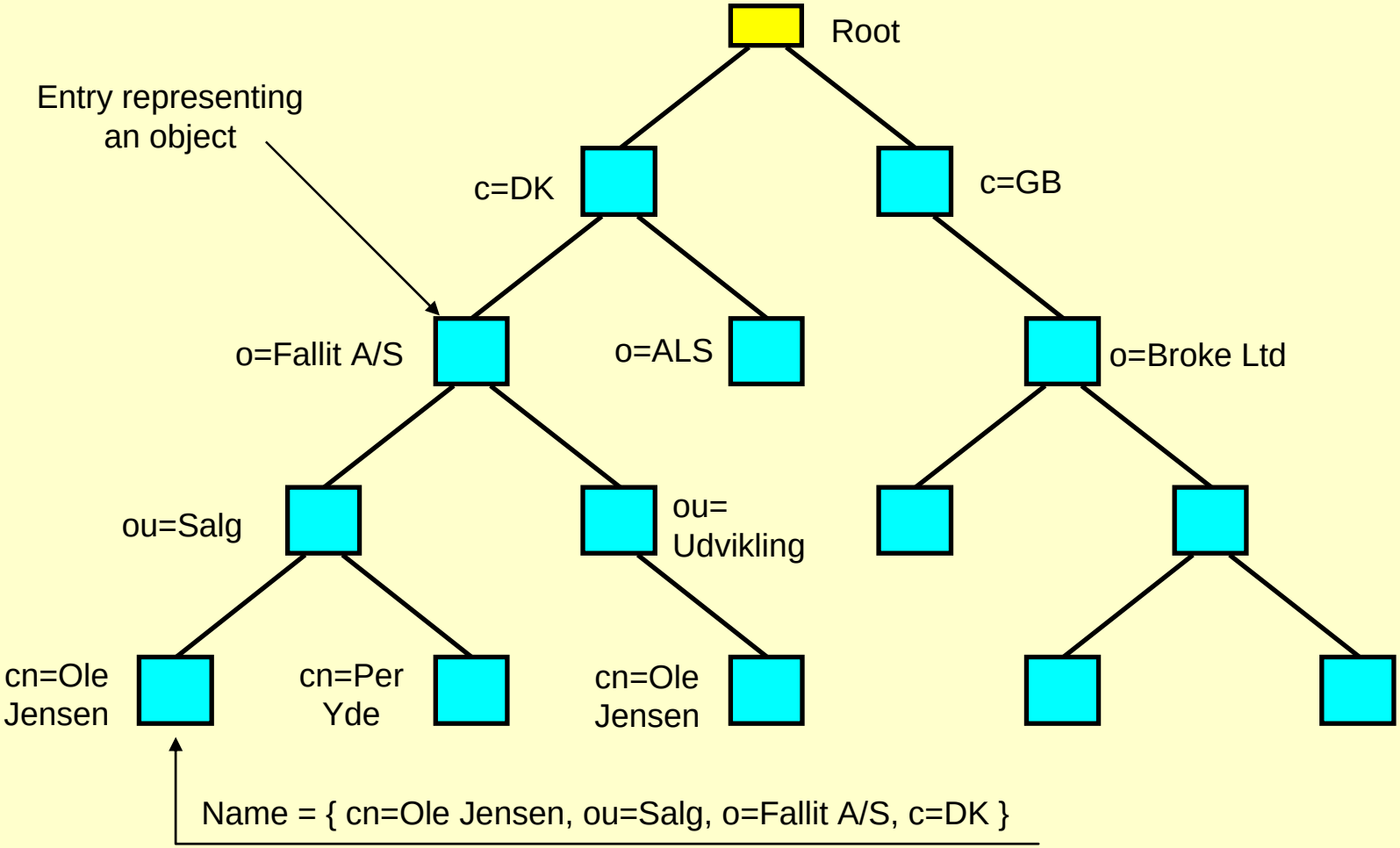
Protection parameters:

- class of user accessing
- sensitive level of information
- “subscriber” requirements
- administrative policies
- legal requirements

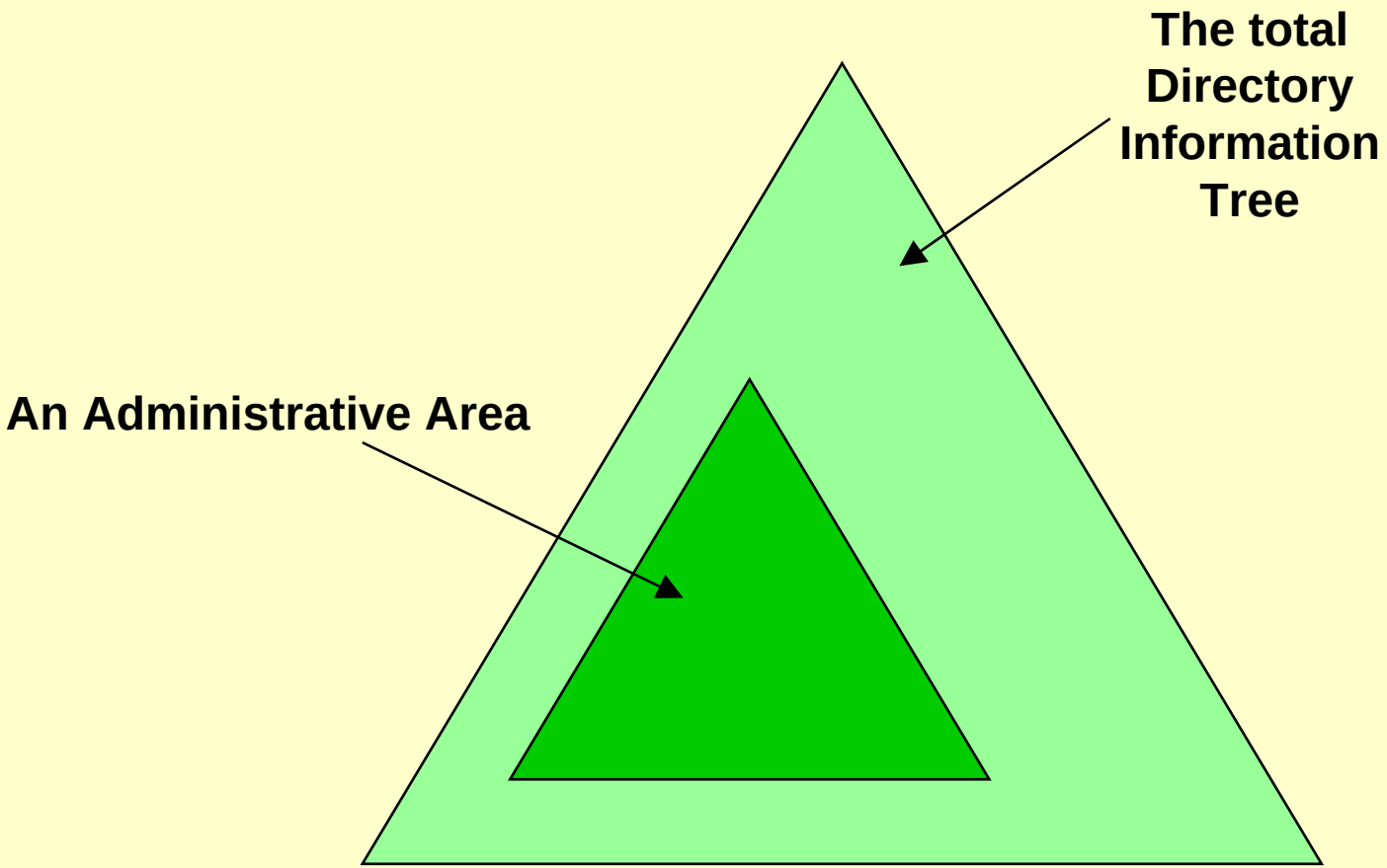
Protection involves:

- individual pieces of information
- combinations of information
- data trawling

Directory Information Tree - DIT

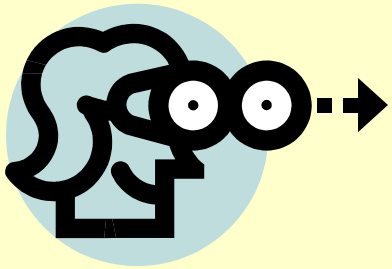


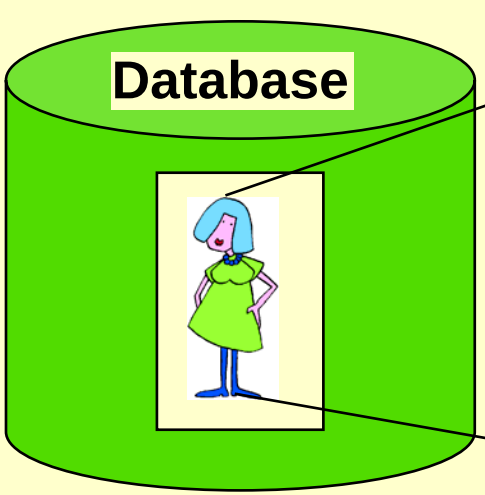
Autonomous Administrative Areas



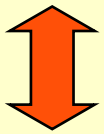
Participants in data protection

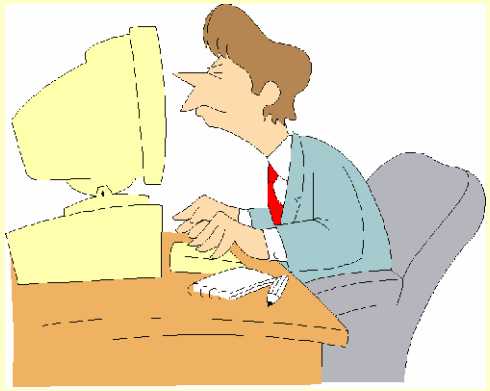
Accessing user





Subscriber





Administrator

Two aspects

Two aspects are treated by this presentation:

- **Access Control**
- **Service Administration**

They are both very complex areas – only a ridiculous high-level description is possible here

Above all

Sure Authentication of accessing user is the prerequisite for privacy

Simple authentication

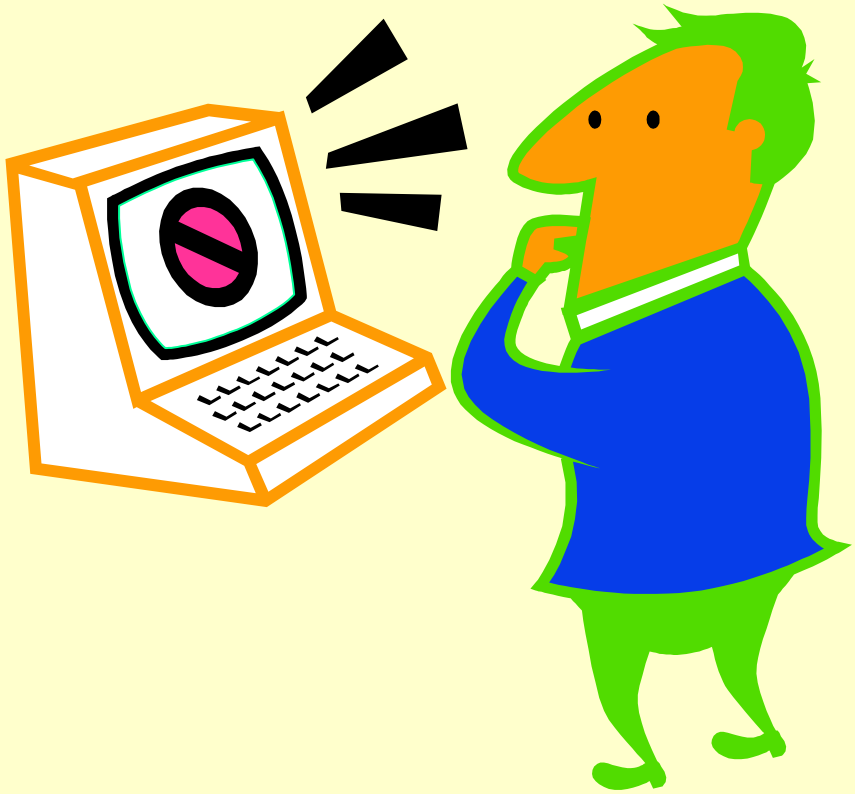
X.500 has support for:

- Distinguished name only
- Distinguished name and password in clear
- Distinguished name and encrypted password

Strong authentication

- Based on electronic signatures
- Requires the presence of a Public Key Infrastructure (PKI)

ITU-T Rec. X.509 is here the key specification



Access control

What is access control?

Who may do what or not do what based on the level of authentication

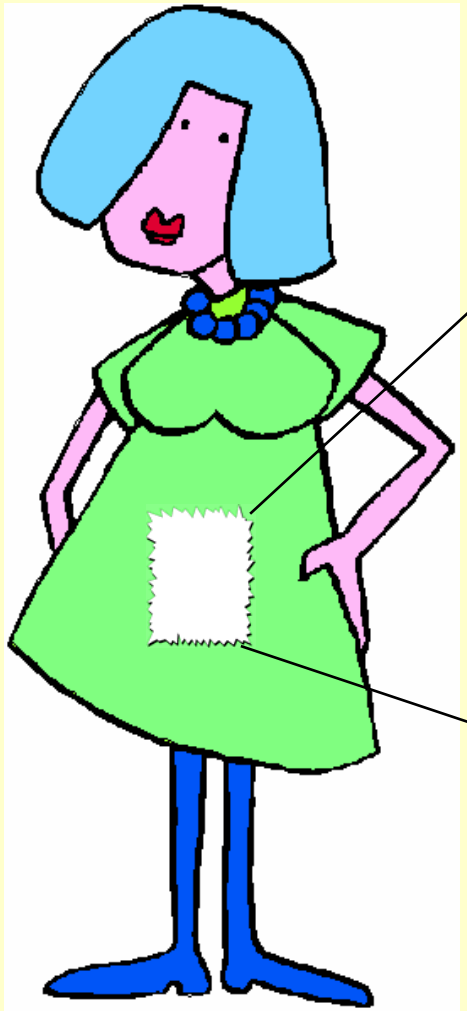
What can be protected (protected items)

- **User information – this could be:**
  - Complete information about an entity represented in the directory; or
  - Fragments of that information
- **Operational information**
  - Access control information
  - Directory schema definition
  - Etc.

Who may and who may not

- owner of information
- specific user
- user group
- all users
- subtree

Protected item focus



Piece of Information (Protected item)

Read

List of users/groups

Browse

List of users/groups

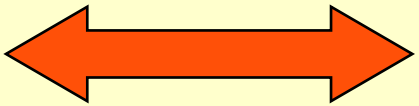
Update

List of users/groups

Change name

List of users/groups

User focus



Protected item

Grant and denials

Protected item

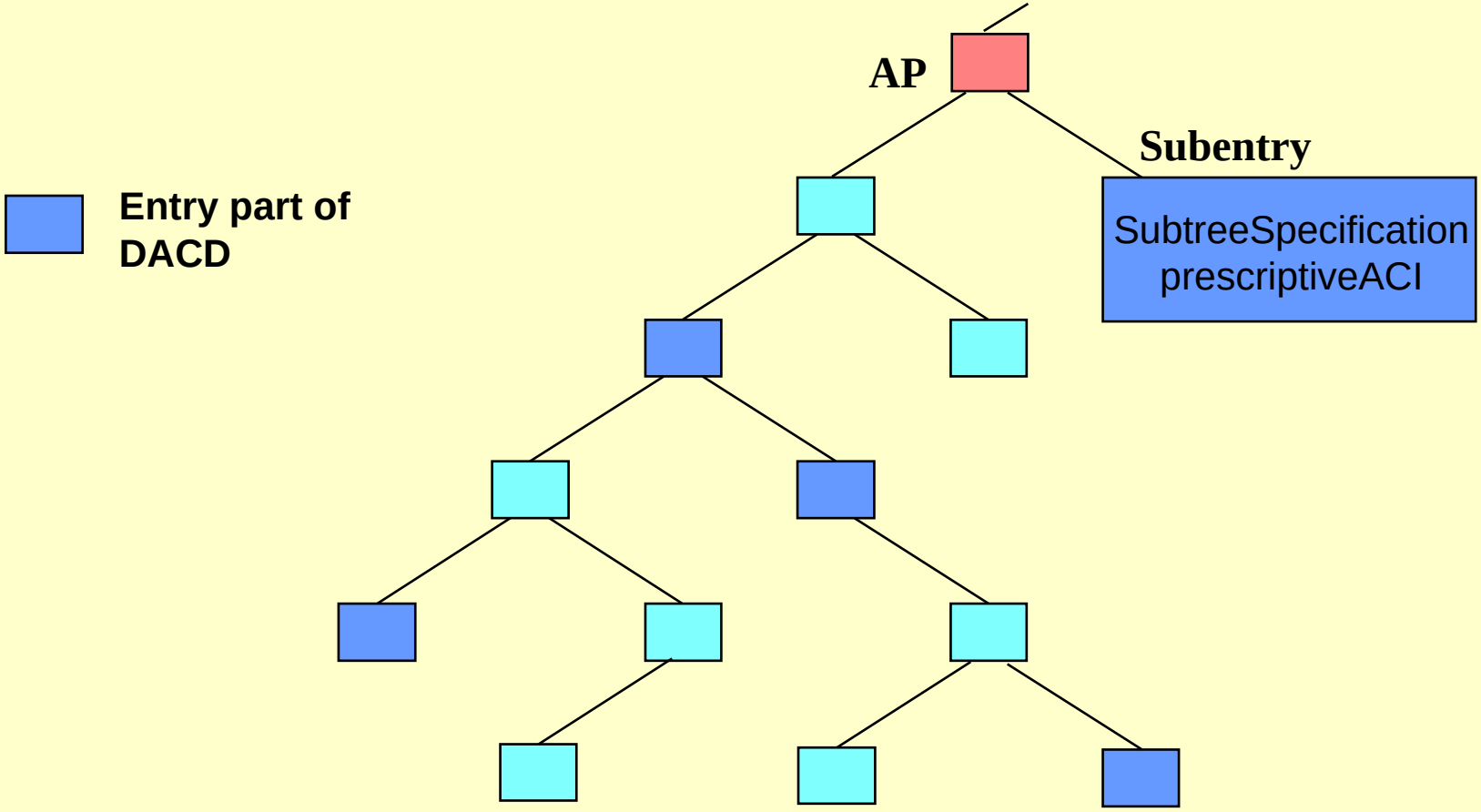
Grant and denials

Protected item

Grant and denials

Etc.

Directory Access Control Domain (DACD)



A DACD is determined by a subtree specification

DACD may overlap (an entry may member of several DACDs)

Levels of protection

Anything goes

↓

Protection of individual entries based on right-to-know (traditional access control)

↓

Protection of individual entries based on right-to-know and need-to-know (service view)

↓

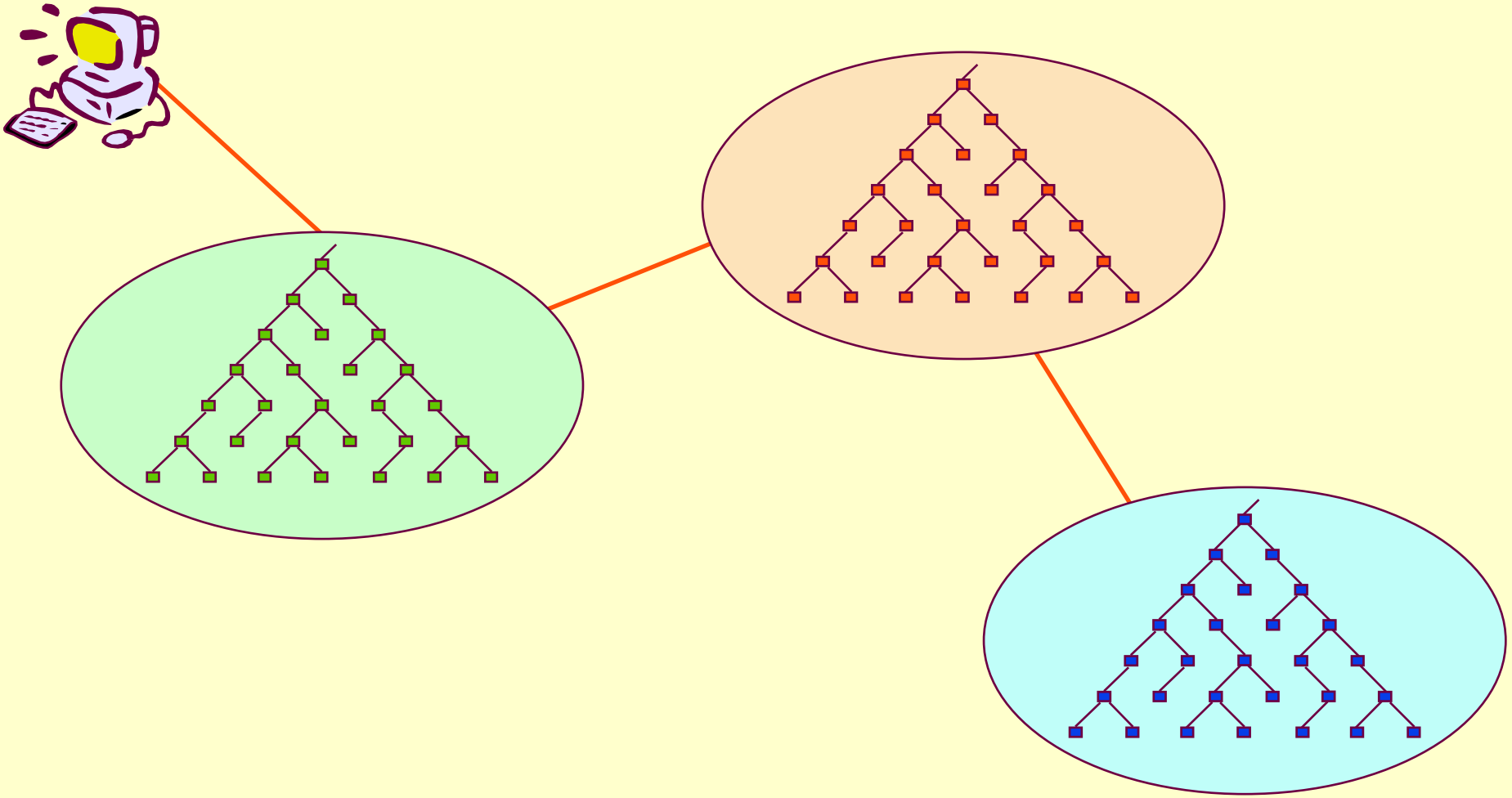
Protection against devious searches

↓

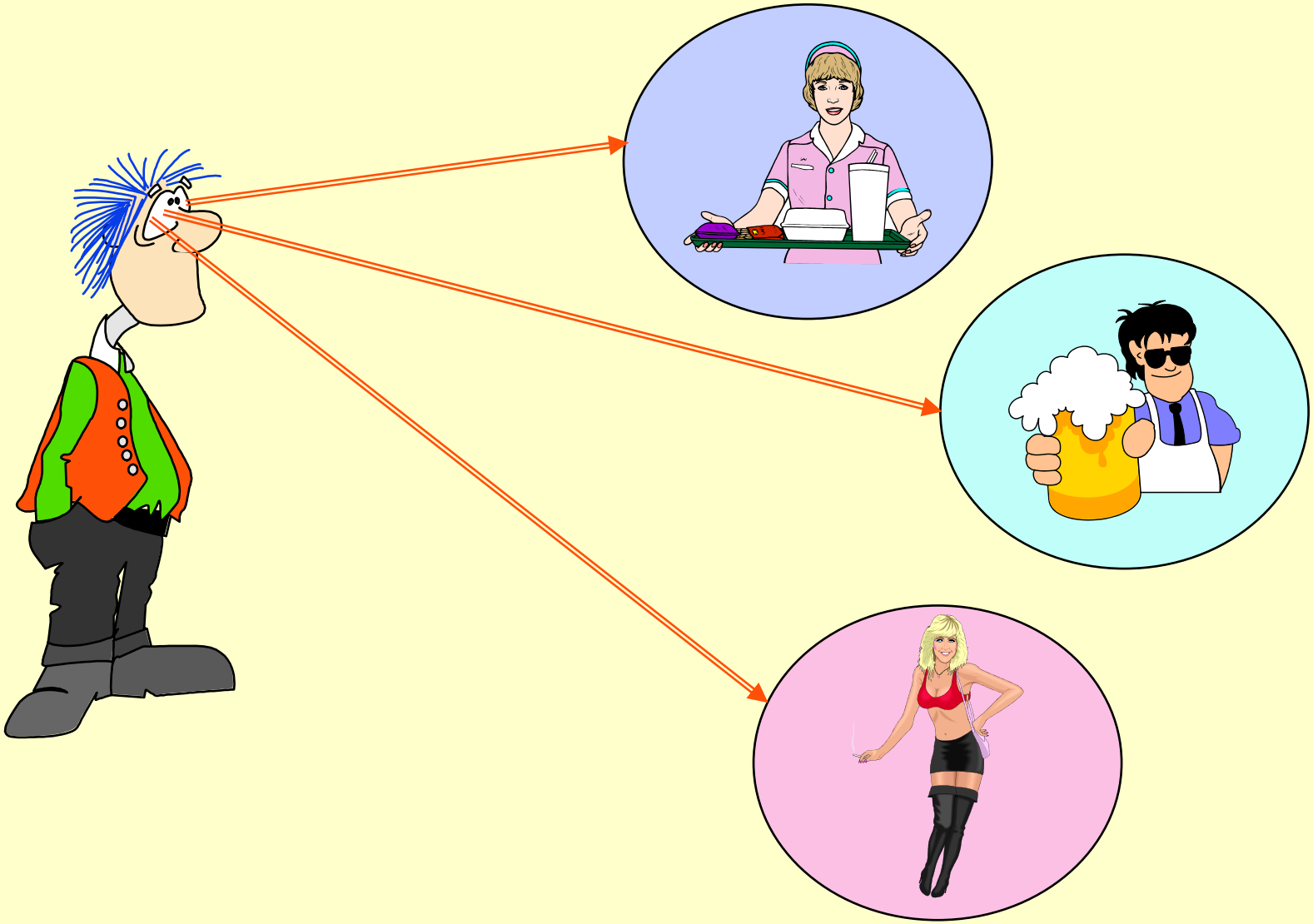
Protection against information trawling

Service administration

Global Directory Service View



Focused service view



The heart of the service concept

Directory search-rules

Search-rules:

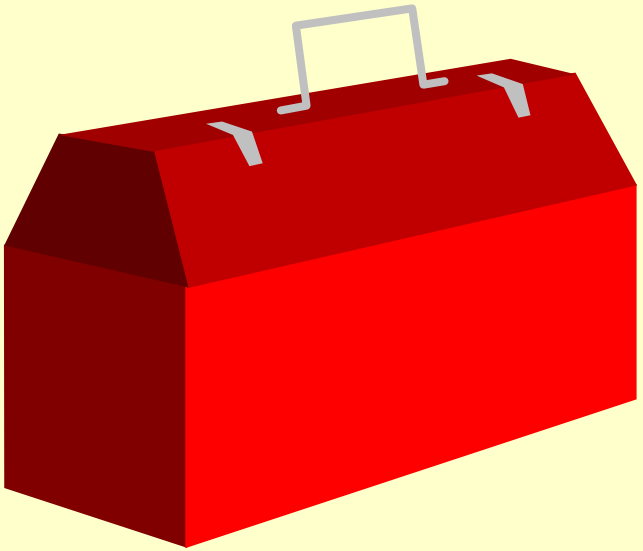
- Polices what searches can be performed by certain users
- Polices that the right search criteria are being used
- Adjusts the search request to increase chance of success
- Determines what information to be returned
- Etc

Services and users

Service administration is concerned with:

- **Services to be provided**
- **Level of service**
- **User types/groups for each level of service**
- **Tools for administrators**

Providing a toolbox for the administrator

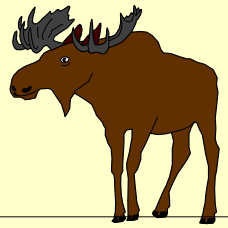


- Restrict searches to well defined searches
- Tailor output to what is needed for the service in question
- Tailor output according to legal or subscriber requirements
- Restrict what search criteria that can be used for each type of service

The tools are very general allowing for all types of restrictions and for flexible tailoring of returned information

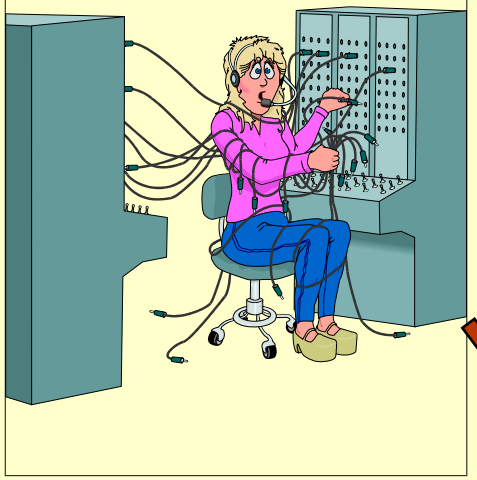
Service type examples
(taken from F.510)

- Search for state or province
- Search for locality
- Search for subscribers within locality
- Search for subscribers group entries
- Search for subscribers within state or province
- Search for subscribers within country
- Search for street address
- Search for subscribers by street address
- Search for subscriber by communications address



Same information - different user-groups

Operator



Intelligence/ police

Telephone sale

Directory

X.500

Casual user

Emergency centre

Same information - different user-groups (2)

Information burglar

Hacker

Crook

Differentiation of users

Users

- User class 1
- User class 2
- • • •
- User class n

- User group a
- User group a
- • • •
- User group a

Search Rules

- When a search is initiated, the Directory will find a suitable Search Rule governing the execution of the search
  - Suitable for the user group
  - Applicable for the type of service requested
- The X.500 defines elaborate rules for how the relevant search rule is selected
- If no suitable Search Rule is found, the search is rejected
- Search rules are protected by access control

Search Rule content

- Global identification
- Service type
- User class
- Input attribute types in filter
  - Restriction of values
  - Attribute combinations
  - Matching restrictions
  - Plus some more
- Service controls
- Output as relevant for the service and the user group
- How mapping based matching shall be performed

Search-rules

Local public users

- Search-rule 4a
- Search-rule 3a
- Search-rule 2a
- Search-rule 1a

Local operators

- Search-rule 5b
- Search-rule 4b
- Search-rule 3b
- Search-rule 2b
- Search-rule 1b

Public users from France

- Search-rule 3m
- Search-rule 2m
- Search-rule 1m

Operators from France

- Search-rule 4a
- Search-rule 3a
- Search-rule 2a
- Search-rule 1a

Public users from Finland

- Search-rule 4u
- Search-rule 3u
- Search-rule 2u
- Search-rule 1u

Operators from Finland

- Search-rule 4v
- Search-rule 3v
- Search-rule 2v
- Search-rule 1v

FBI

- Search-rule 3x
- Search-rule 2x
- Search-rule 1x

Where to go

The central source for information on the X.500 Directory Standard.

www.x500standard.com