



DAM-LR Distributed Access Management

Peter Wittenburg, Daan Broeder (MPI)

Remco van Veenendaal (INL)

Sven Strömqvist (Lund)

David Nathan (SOAS)

Vincent, Thomas I+II, Eric, et al



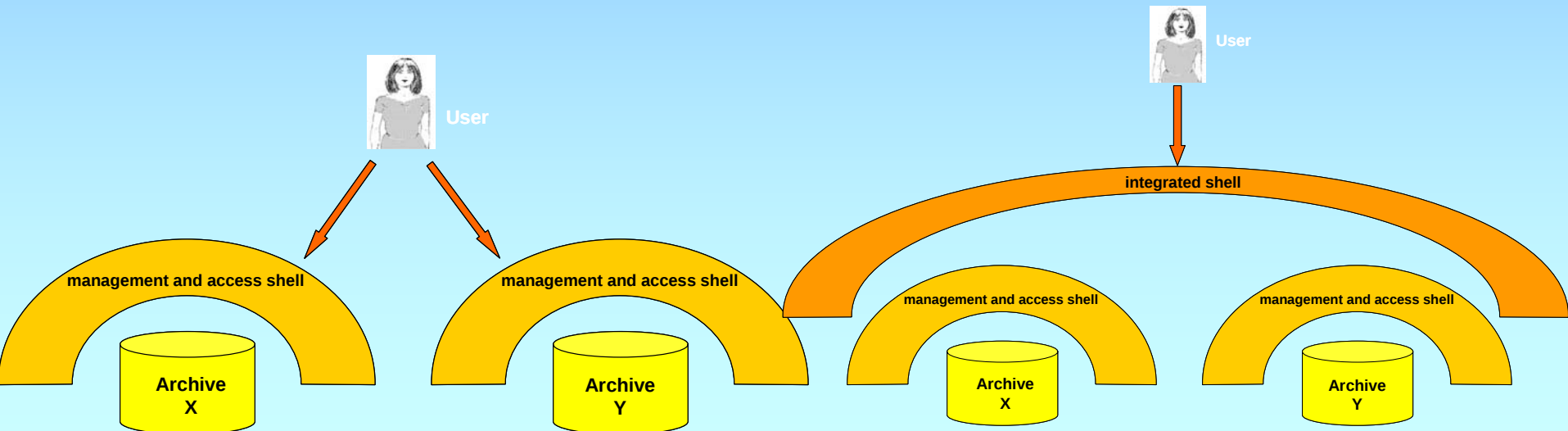
Goals – very old slide

lots of disadvantages

- idiosyncratic ways of access management
- several identities
- no joint operations on content
- etc

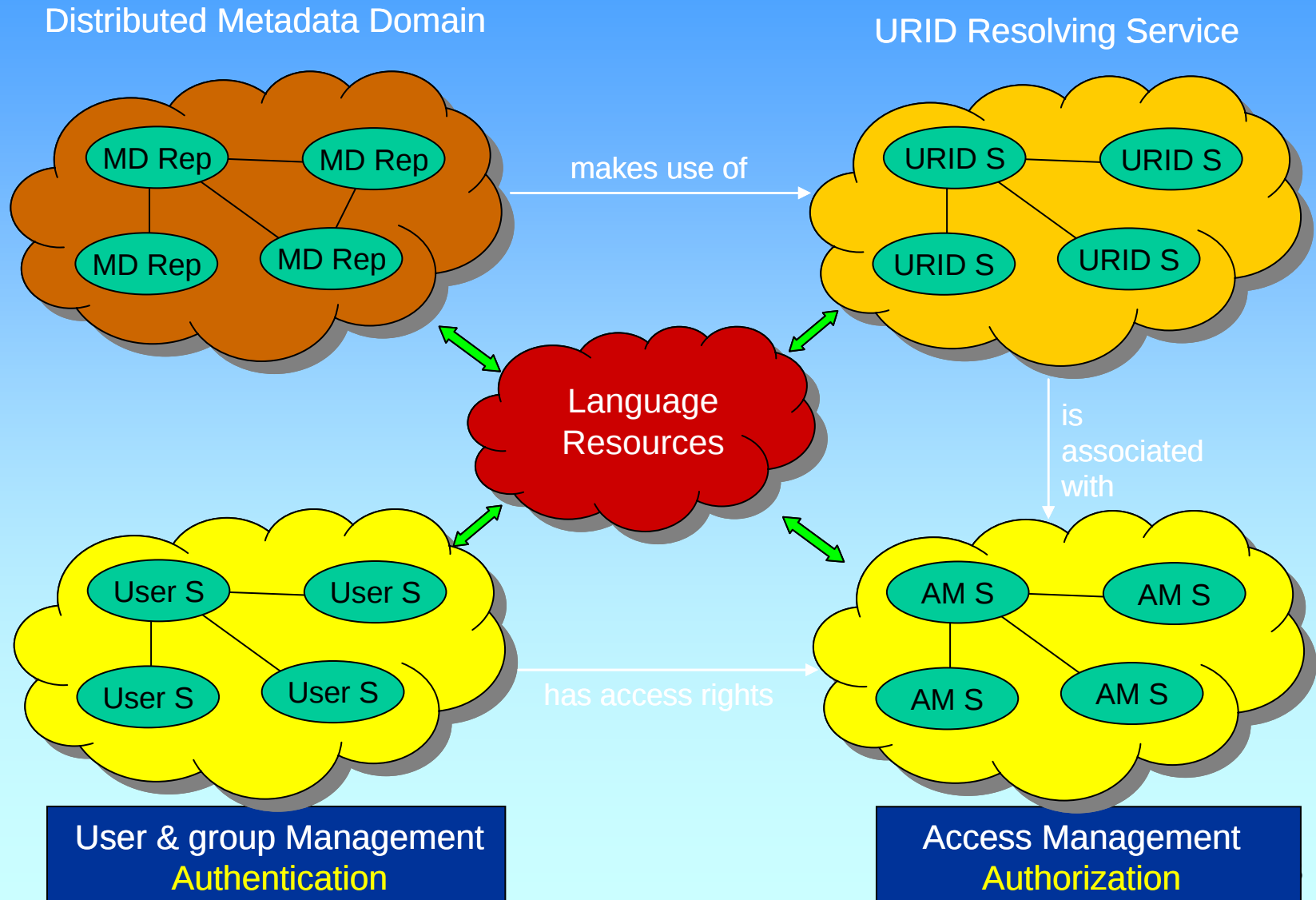
improvements

- single sign-on + identity
- integrated metadata layer
- one basket idea
- federated authentication



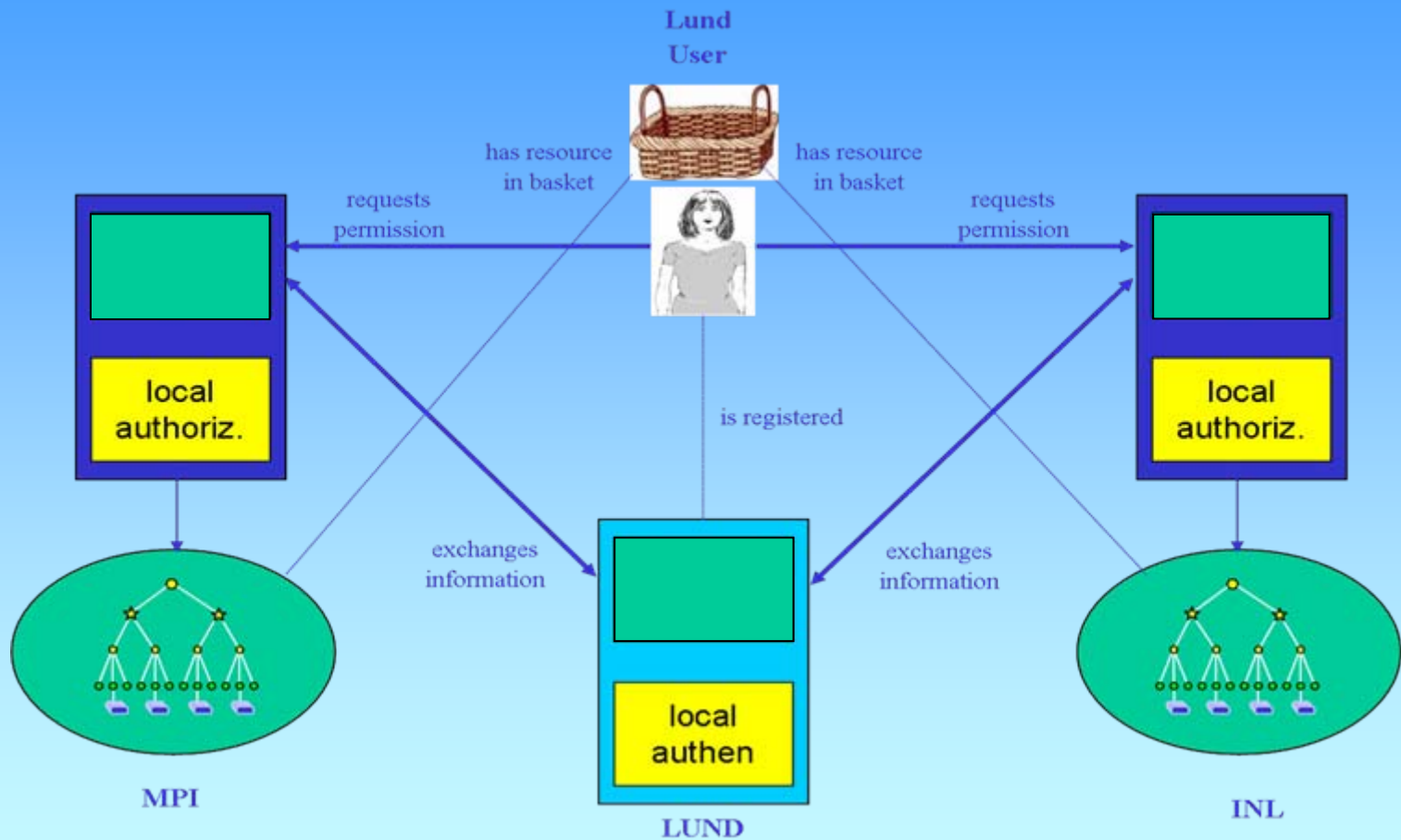


Ingredients – very old slide





Scenario - new slide



This is what we want: a transparent integration to build and access virtual collections across various archives/repositories and to access them.

1. you need to know what is out there!!! -> metadata



Pillars to get this done

a number of technologies are ready to get this all into play

- computers talk to each other with sensitive information
- joint metadata domain
- handling unique and persistent identifiers
- intermediating between authentication and authorization and adapting all components

brief overview to show system and complexity/effort
details later



Pillar 1: Certificates + PKI for trusted Services/Servers

The EUGridPMA is the European authority that is accepted to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organizational access to distributed resources. As its main activity the EUGridPMA coordinates a **Public Key Infrastructure (PKI)** for use with Grid authentication middleware. To support this it maintains the **TACAR (TERENA Academic CA Repository)** repository which is a trusted repository which contains verified root-CA certificates and which can be entered into local lists.

For DAM-LR this is the way to go, since it includes the certificates from

- the **German DFN** - the MPI is RA within the DFN domain
- the **DutchGrid/NIKHEF** - the INL should become RA within that domain
- the **NorduGrid/SwUPKI** – the Lund university should become RA within that domain
- **UK eScience** – the SOAS should become RA within that domain

CA = Certificate Authority; RA = Registration Authority



Pillar 2: Joint Metadata Space based on **IMDI**

- metadata is boring but necessary for managing and discovering relevant data
- different MD sets are around (IMDI, OLAC, TEI, etc)
- for pragmatic reasons IMDI with add. profiles as common language (will change this in CLARIN as mentioned)
- harvesting via XML downloading (or OAI PMH)
- portal software is around (MPI, INL)
- the problem in general: too few people to create MD (ENABLER)
- other aspects: improper terminology, schema flexibility

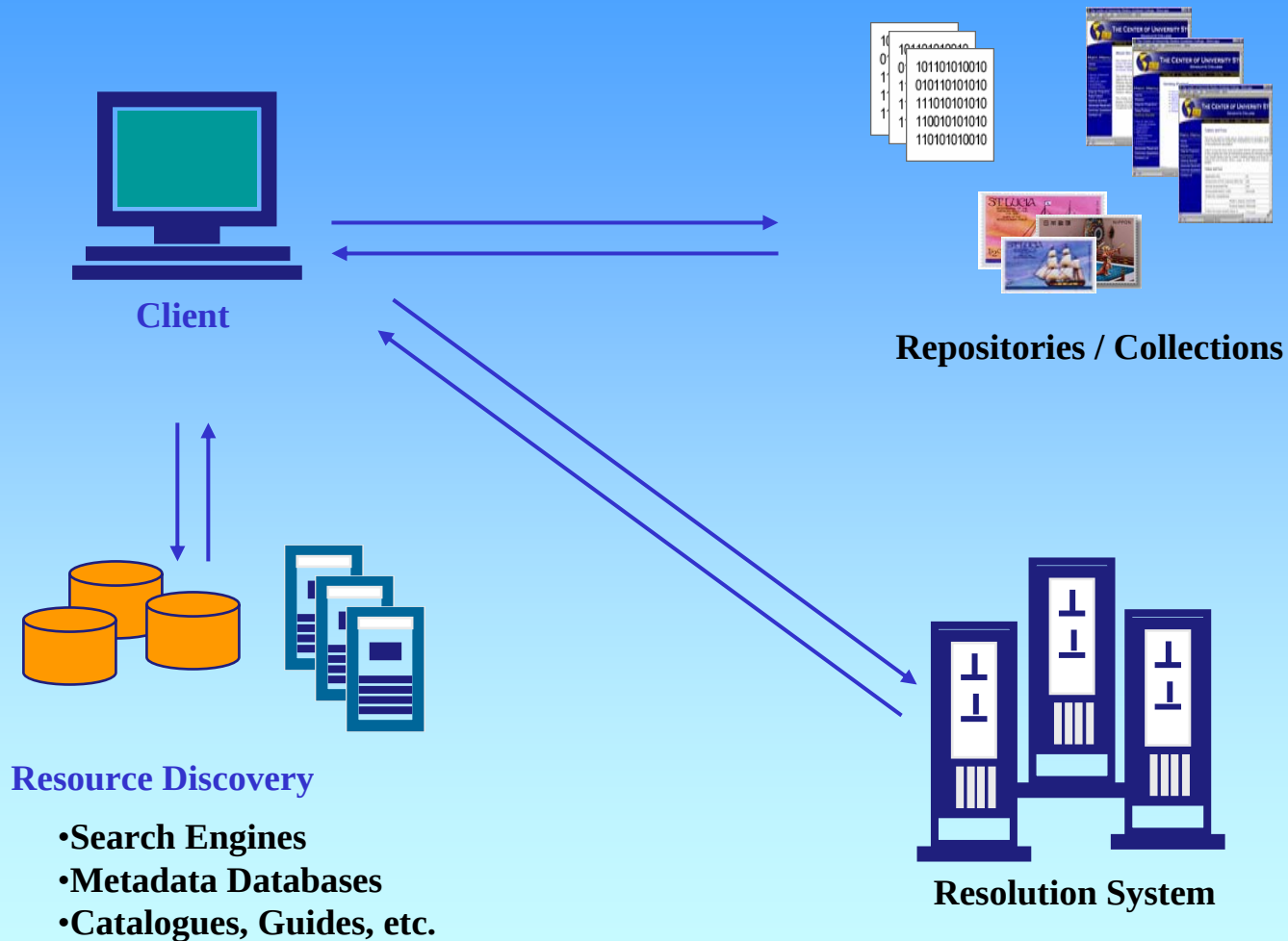


Pillar 3: URID System

- managing Digital Objects is a huge task
- give resources a unique and persistent ID before virtual integration
 - don't worry about where it is since this can and will change
 - don't worry about what it's made of
 - similar to ISBN
- make archive ready for all sorts of references that have to be stable independent of physical changes
- make us ready for copying scenario – multiple instances + one identity
- just one place to carry out changes – tractability issue
- therefore: standardization proposal on the desk of ISO



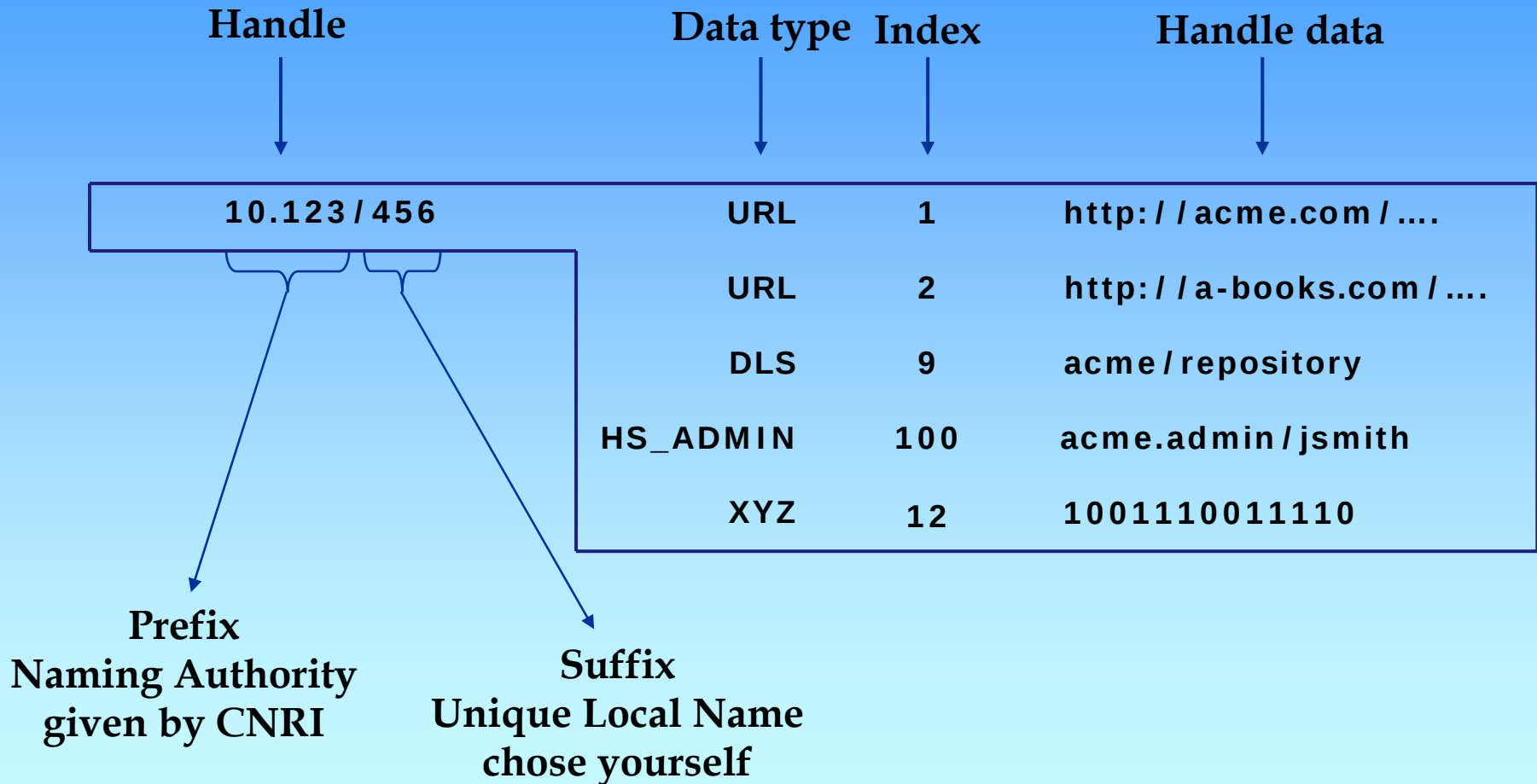
Pillar 3: URID handling with **Handle System**



alternative: DOI – also Handle System based – expensive business model



Pillar 3: Handle syntax



Handle Syntax is basis of ISO proposal

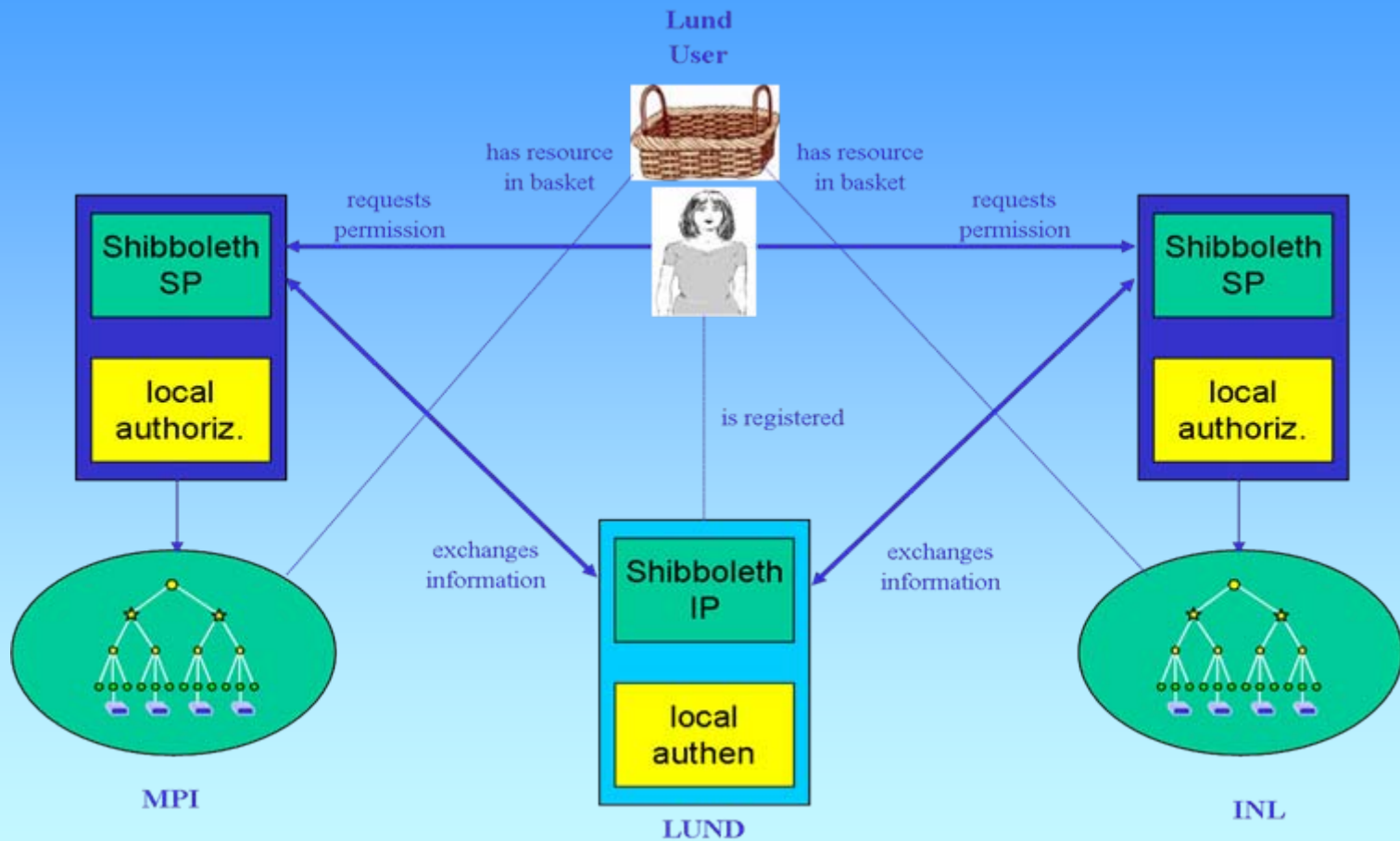


Pillar 3: Authentication + Authorization General Aspects

- we want
 - single identity
 - single sign-on
 - one basket idea
 - replication option
- access handling is done by originating institution
- access information is associated with the URID – not the individual copy
- usage scenarios for LR
 - **individual** researcher for some research question
 - **individual** students writing a thesis
 - **individual** journalists who want to create a story
 - student classes who are in a teaching course



Pillar 3: distributed AAI with Shibboleth

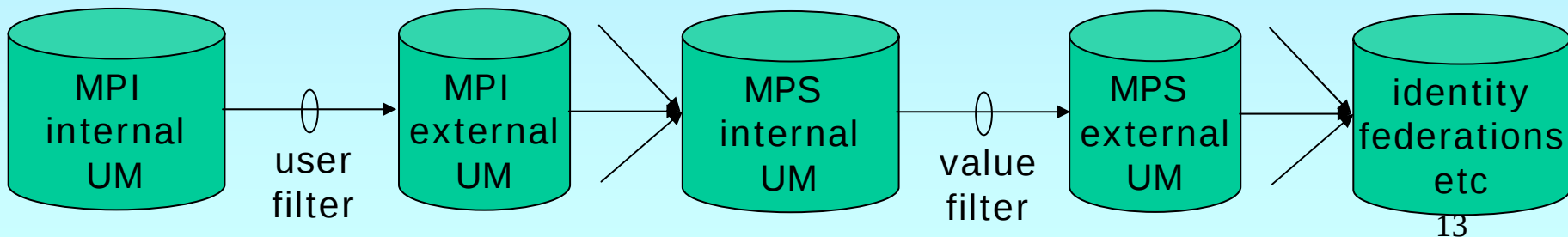


Shibboleth is the core



Pillar 3: Attributes to exchange

- driven by the big game (publishers etc)
eduPerson, inetOrgPerson
had some discussion about additional “roles” but not realistic
- still some debate how to use certain attributes
eduPerson.Entitlement vs. eduPersonEntitlement etc
- at MPI a layered system
 - internal user management with all “dirty” accounts
 - filtering to the MPS world with only trusted accounts
 - MPS will need additional roles (attribute values) ie.
filtering to the big world





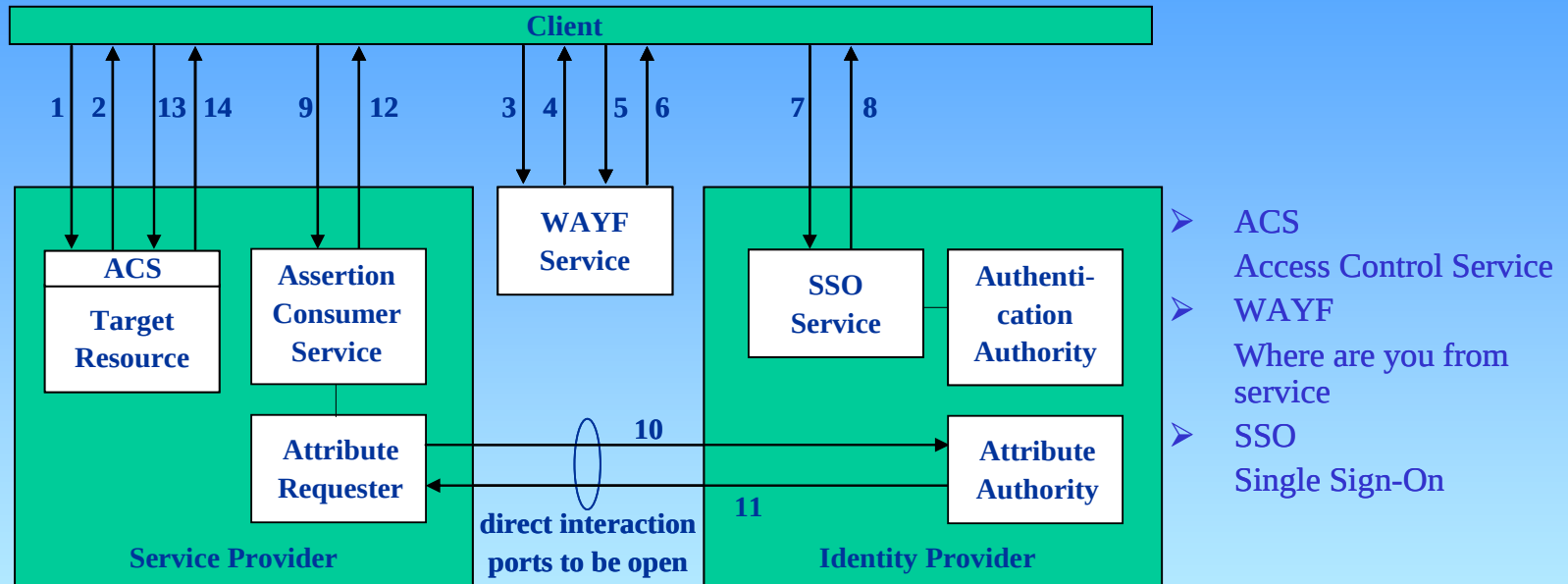
DAM-LR conclusions



- have gained much hands-on experience ☺
- are also linking up with the Grid world (D-Grid, NL-Grid, ...)
- built up knowledge in/for SSH – are at competitive level
- need strong centers (machinery set up and maintenance)
 - most LRT centers not ready for this
 - need proper user management and authentication system
 - need proper repository system (SRB, Fedora, Lamus, ...)
- need proper technical agreements
- need to influence discussion about attribute usage
- need a clear picture about an “LRT Federation”
- need to link up with national identity federations
 - and EU/international activities (TERENA, etc)
- need IT support people – fire brigade



Shibboleth Scenario



1 Get Resource

2 Redirect (302)

3 Get Form

4 Send Form (200)

5 Submit Form

6 Send Cookie and redirect (302)

7 Request Authentication

8 Authentication Response

9 Send an Assertion Profile

10 Request Attributes

11 Send Attributes

12 Redirect with attributes

13 Send attributes for check

14 Provide Resource