



Distributed Access Management - State



Peter Wittenburg

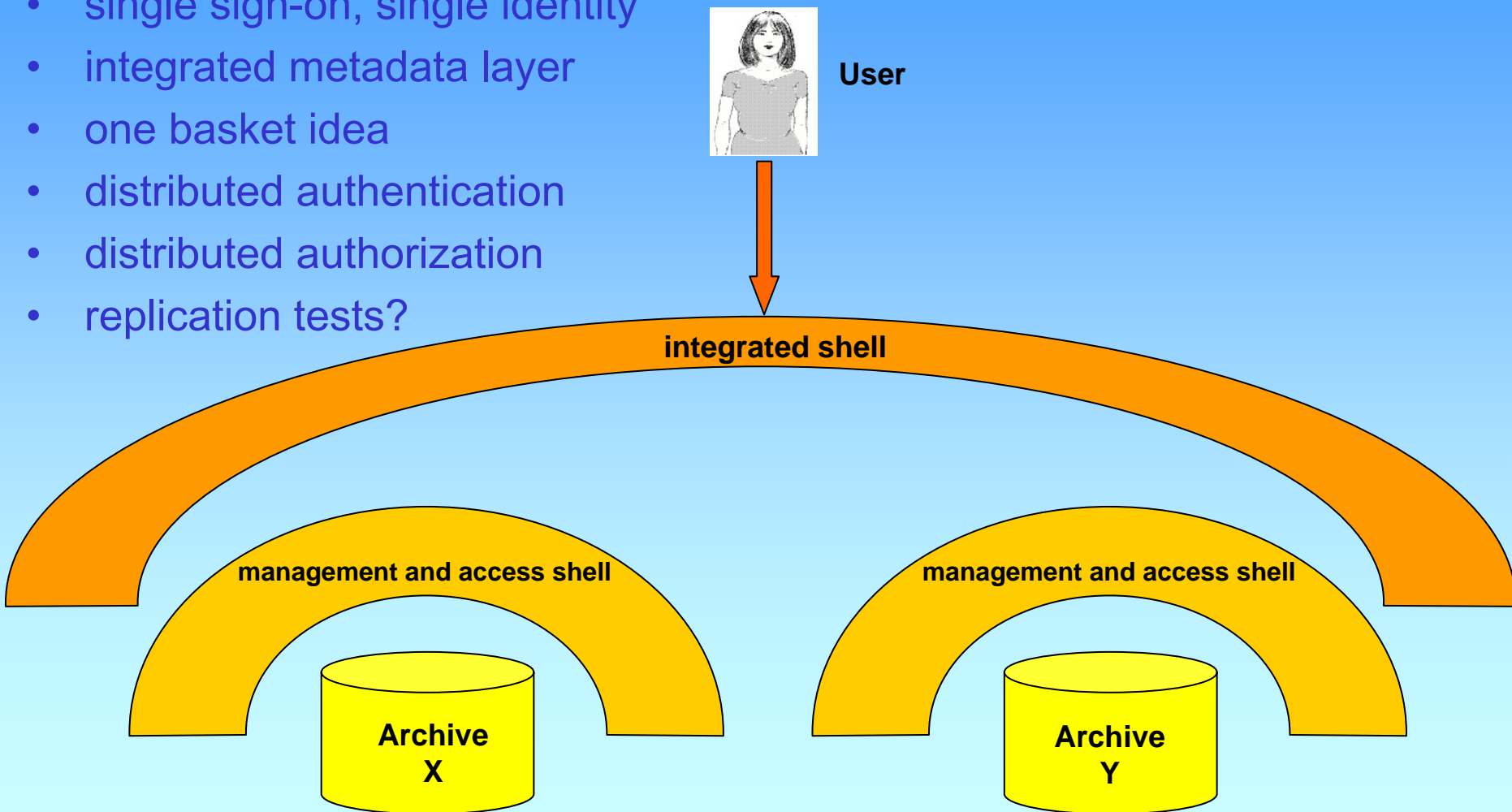
Daan Broeder



What do we want in DAM-LR



- single sign-on, single identity
- integrated metadata layer
- one basket idea
- distributed authentication
- distributed authorization
- replication tests?

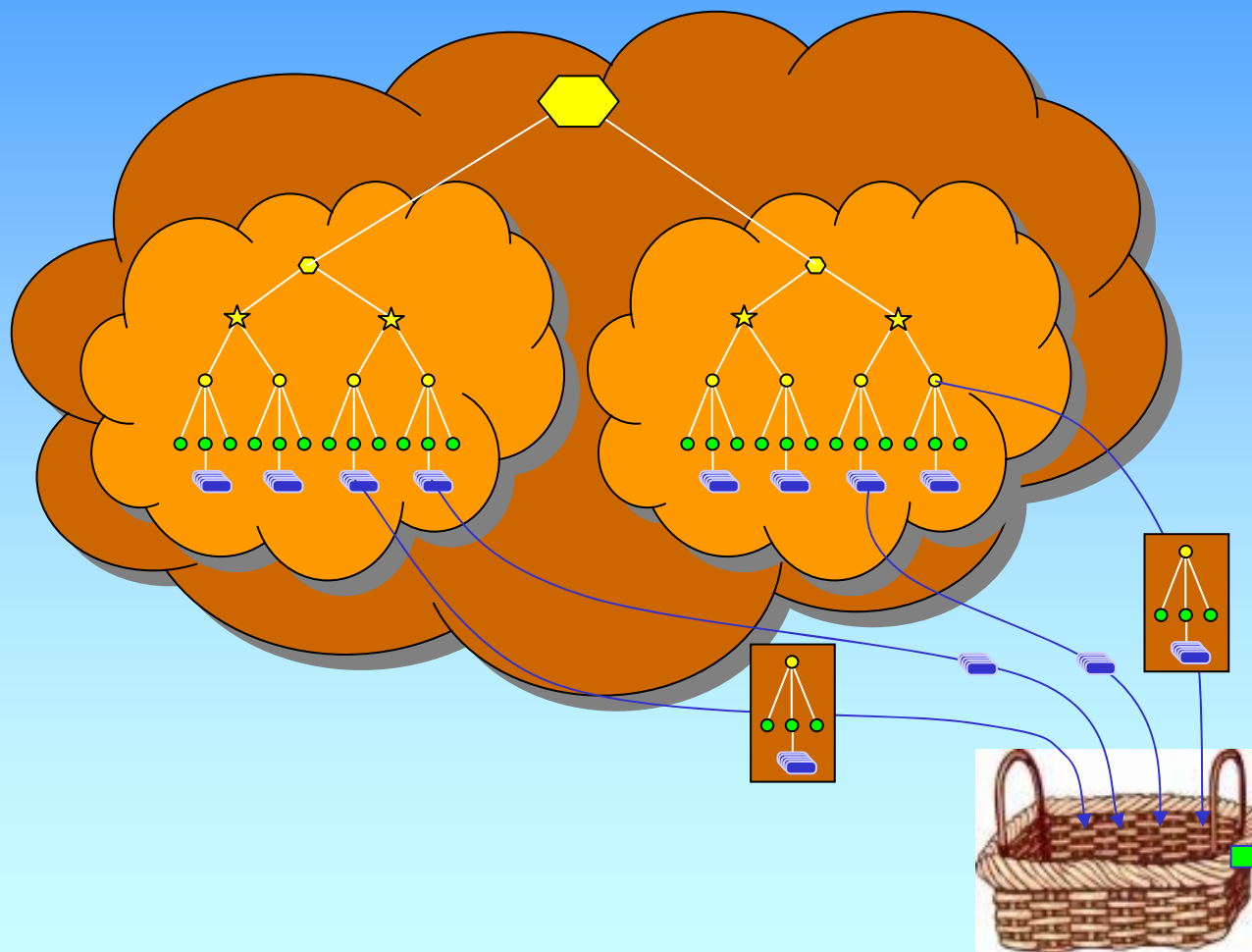




eHumanities Vision



- user selects resources from everywhere
- this is his/her private virtual temporary domain
- can store it as profile
- invoked by session
 - one authentication step
 - one authorization step
- then search (MD + content)
- visualization/listening/...
- comparison
- ...



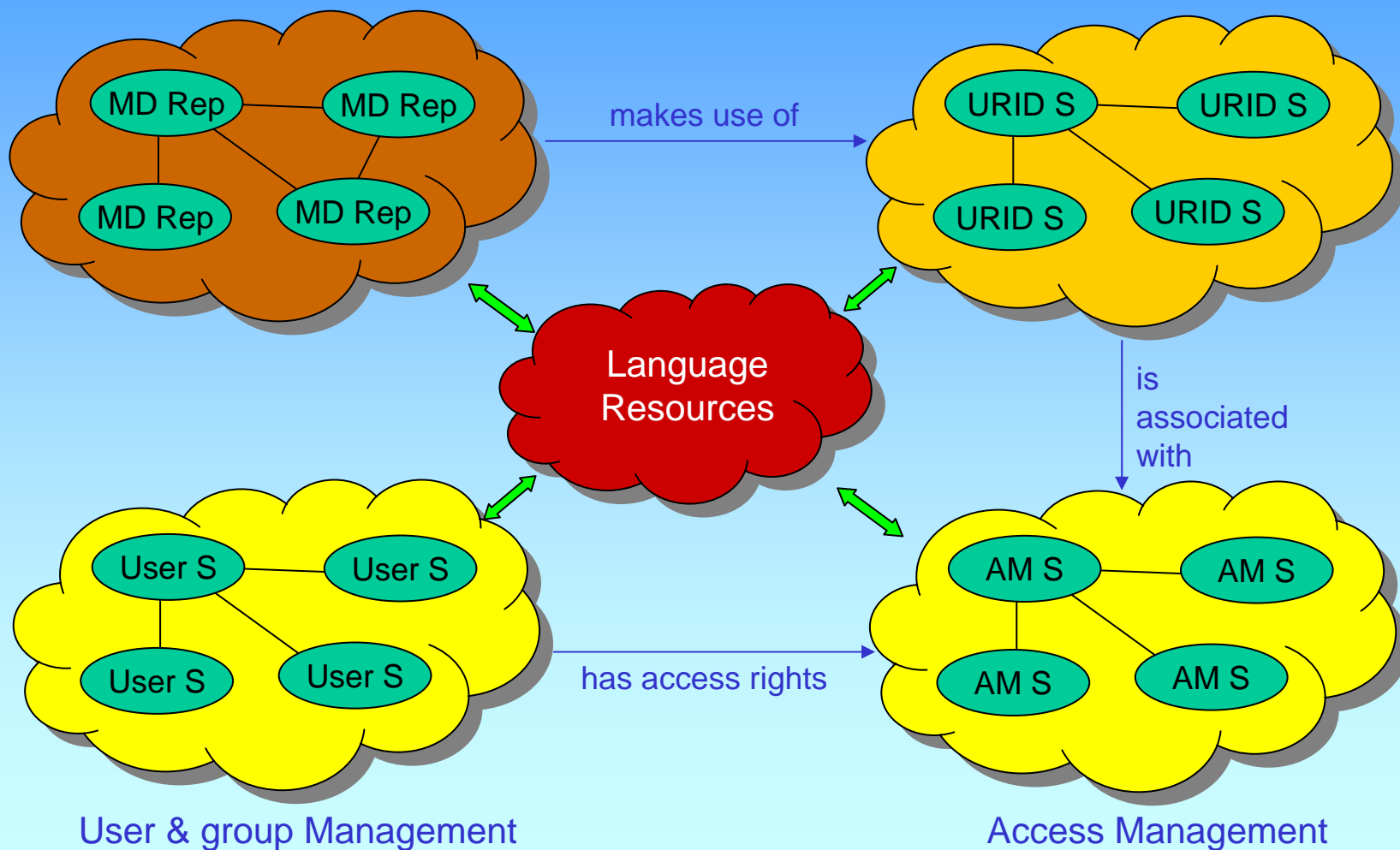


DAM-LR Pillars



Distributed Metadata Domain

URID Resolving Service



User & group Management

Access Management

Authentication

Authorization

Distributed Access Management - State



a few agreed DAM-LR principles



- at the end: demonstrate an integrated domain
- **but: every institute has to be able to work stand-alone!**
- all based on trusted servers and services
 - PKI as basis – is being settled via certificates from EUGridPMA and key registration at TERENA TACAR
- no central user administration – registration at home institution
- every institute can decide about its authentication system (but need agreements about sufficient authentication)
- no exchange of sensitive information such as passwords
- Unique Resource ID records have authorization information
- every institute maintains its own URID service for its resources
 - i.e. authorization info is equal for all instances
 - each institute has an own prefix
 - each institute can decide about suffix
- redundant URID resolving services by one party



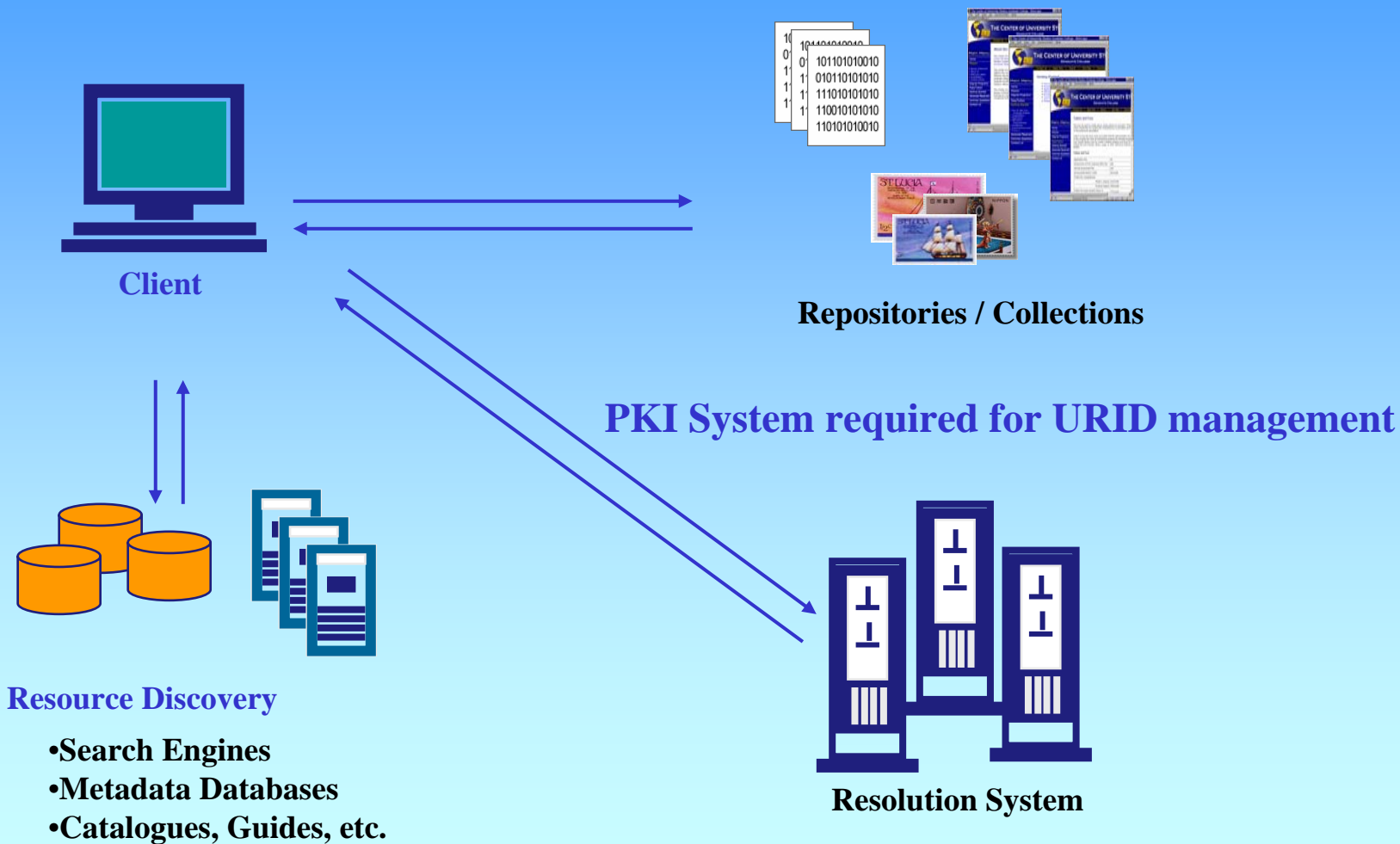
URID Resolving



- it's agreed to use the Handle System (CNRI)
- good, solid, fast and widely agreed (future support)
- at MPI suffix is probably a random string (2 characters reserved)
10.123/xx-456...

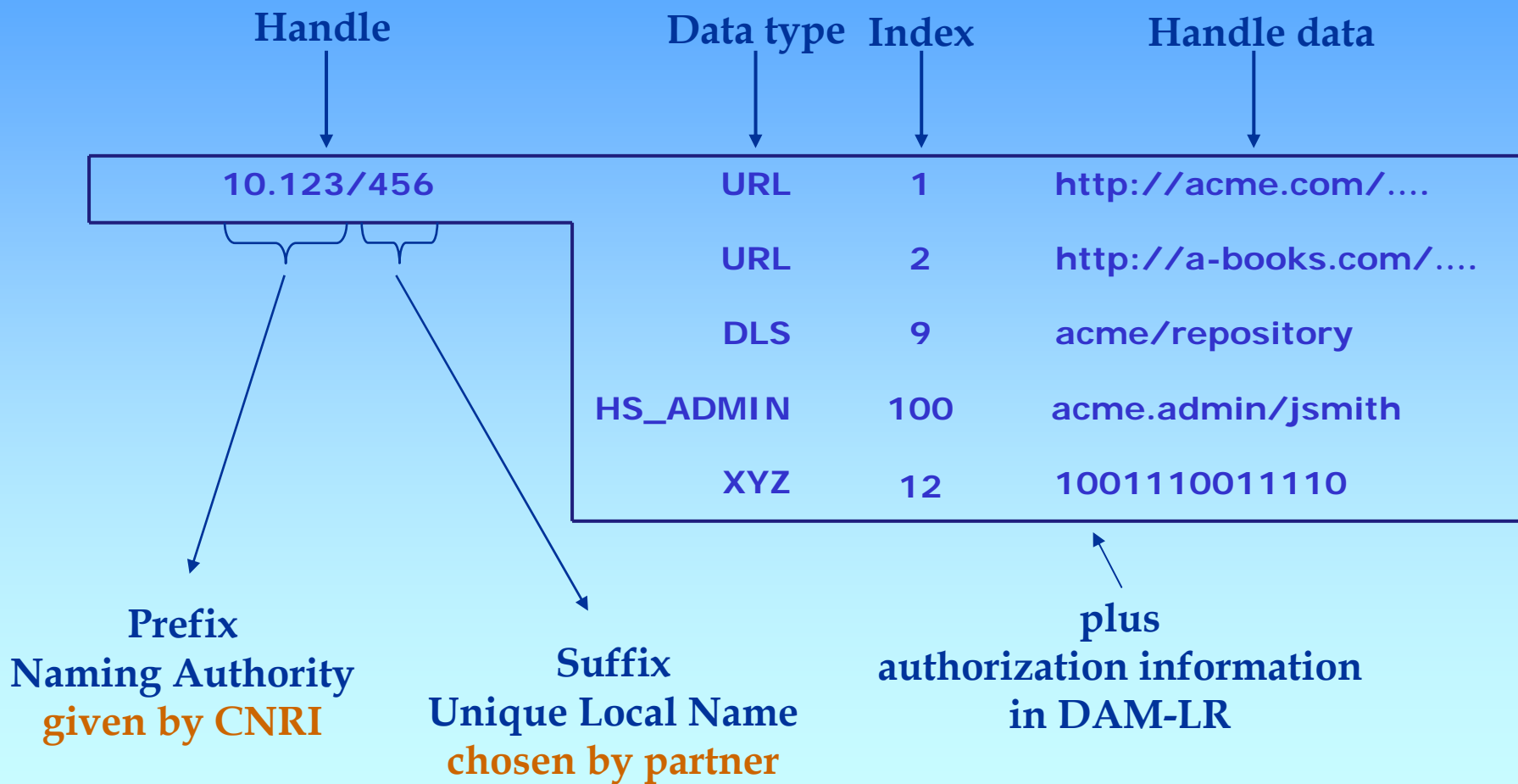


URID Resolving based on Handle System





Prefix/Suffix Authorities

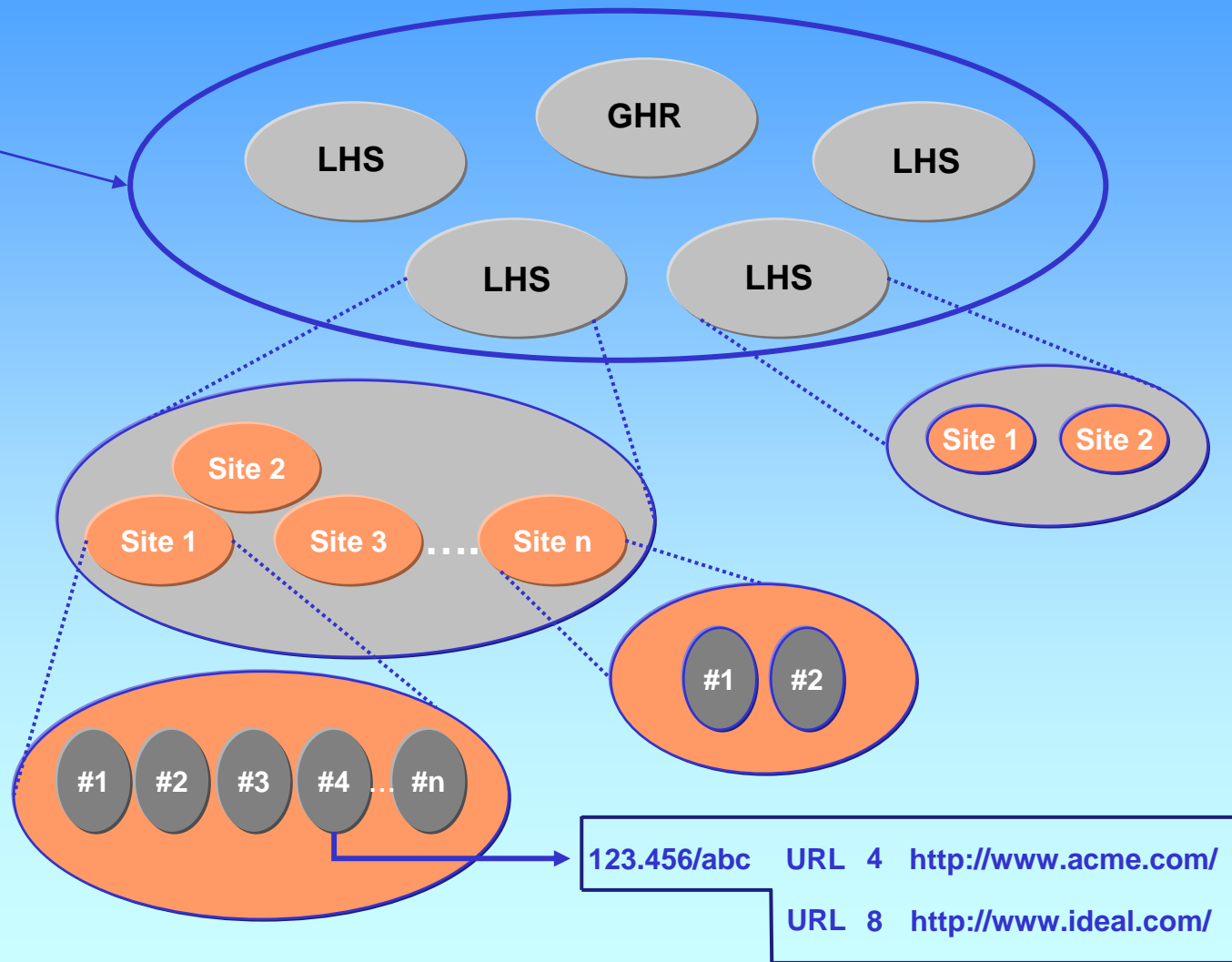




Redundancy in Handle Setup



The Handle System is a collection of handle services, each of which consists of one or more replicated sites, each of which may have one or more servers.





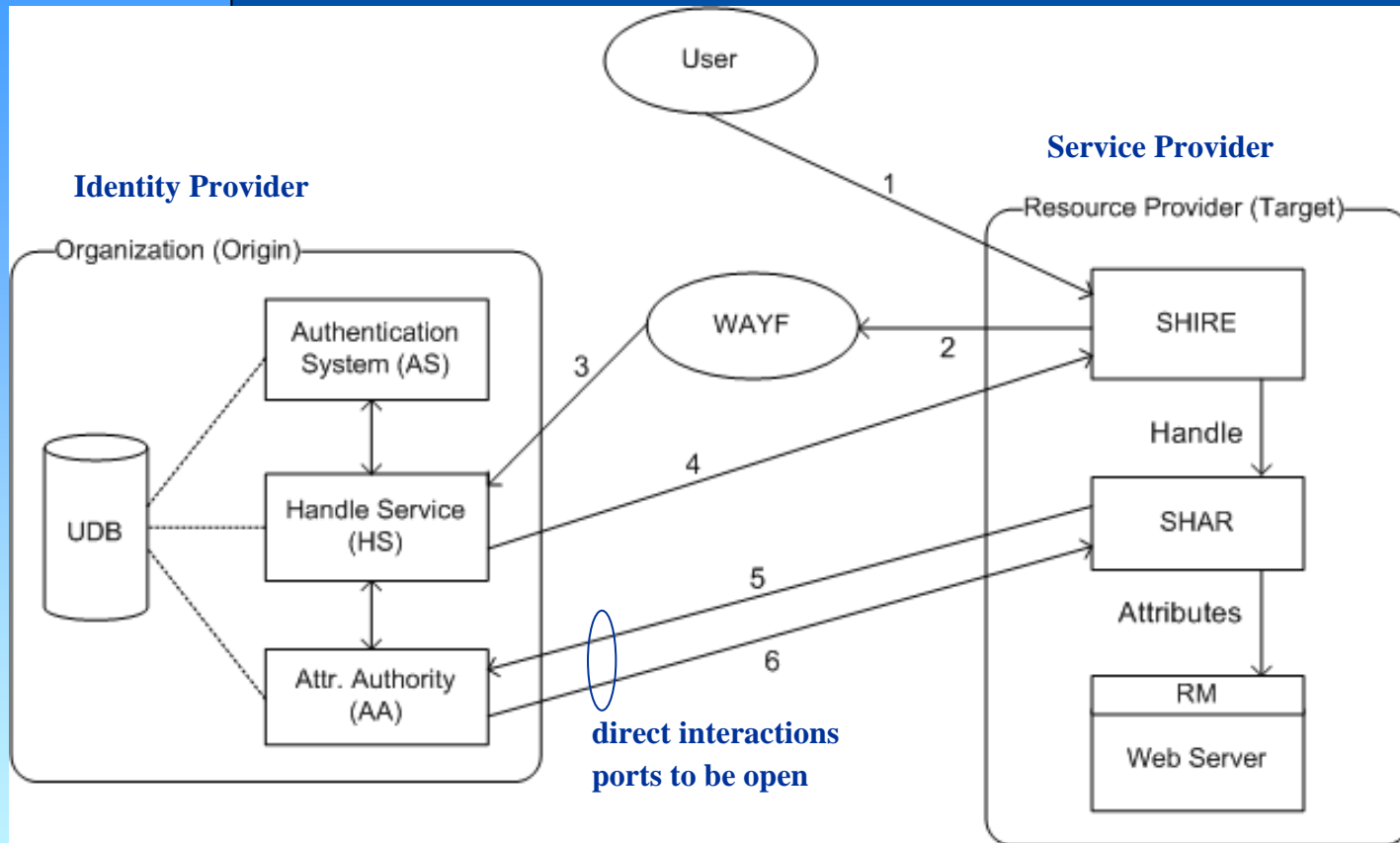
Authentication and Authorization



- no central user administration – registration at home institution
- every institute can decide about its authentication system (but need agreements about sufficient authentication)
 - MPI will move towards LDAP soon
- some information has to be exchanged in a trustful way
- Shibboleth is a candidate
 - not yet decided in DAM-LR – wanted to wait on DELAMAN III
 - discussion in January
 - but we don't fit to the Shibboleth scenario
 - our researchers act as individuals
 - so no simple grouping such as “all researchers from SOAS”
 - perhaps some student classes



Shibboleth Scenario

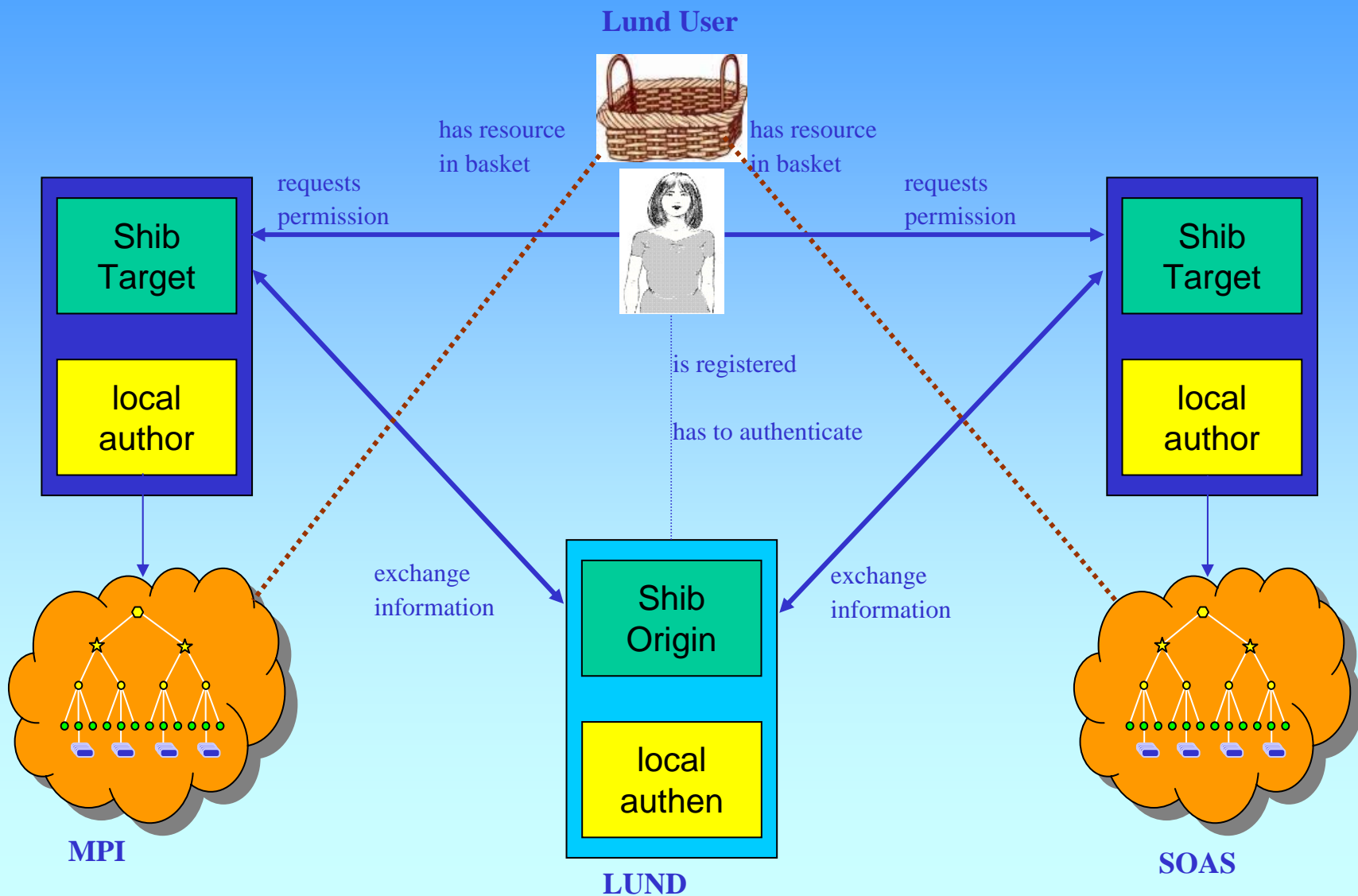


- 1 User finds a resource with MD and selects it
- 2 Shibs target SW redirects request to WAYF
- 3 WAYF presents form with all federation members and user selects
- 4 WAYF passes request to Shibs Origin SW
- 5 The Handle service connects with the AS system and if all ok provides an "assertion"
- 6 SHIRE checks correctness and SHAR requests attributes for the handle
- 7 The local RM checks whether person with that attributes is allowed to access

- **SHIRE** Shib Indexical Reference Establisher
- **WAYF** Where are you from
- **SHAR** Shib Attribute Requester
- **RM** Resource Manager
- **Shib is modular and Open Source**

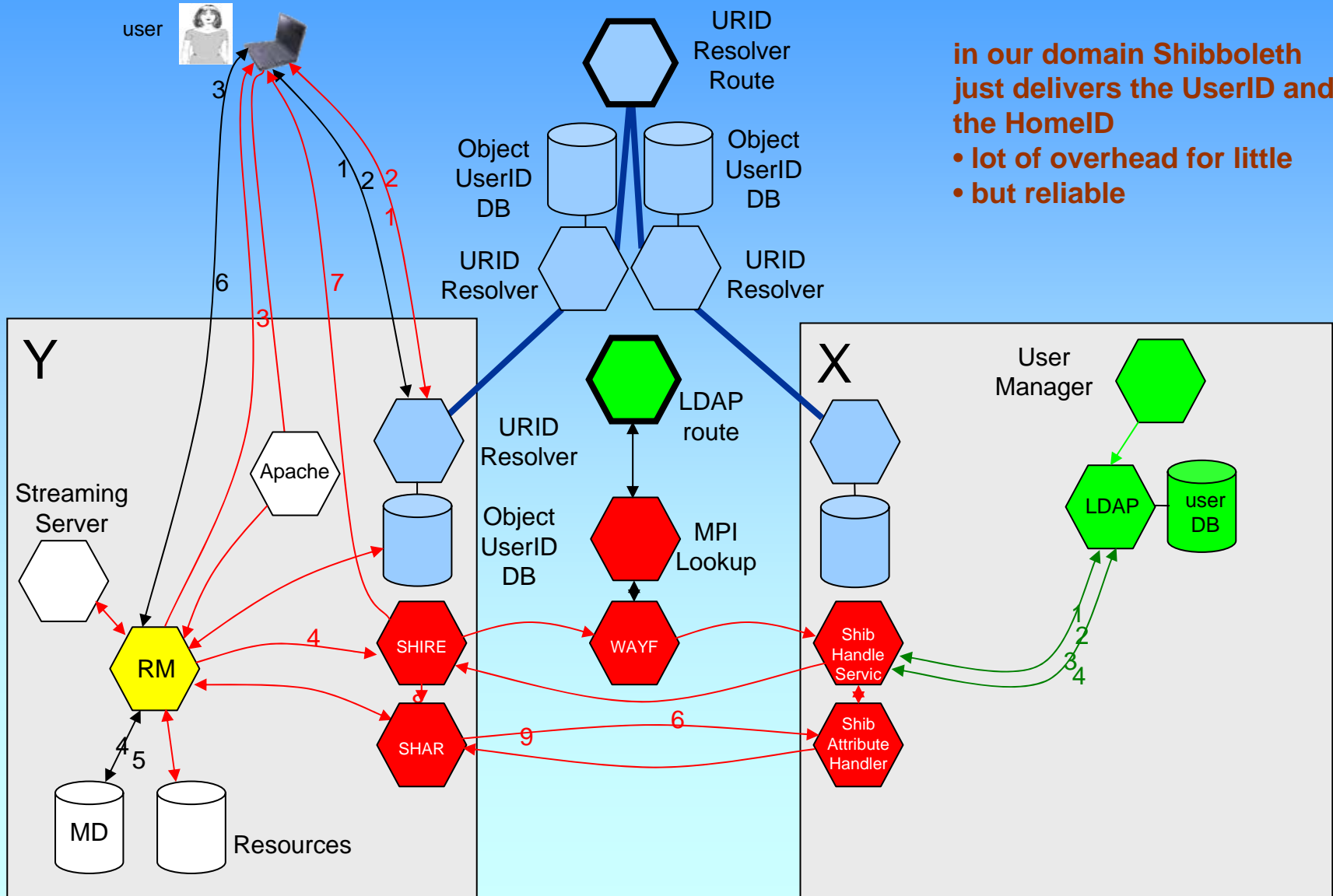


Integrated Scenario





Information Flow in A&A

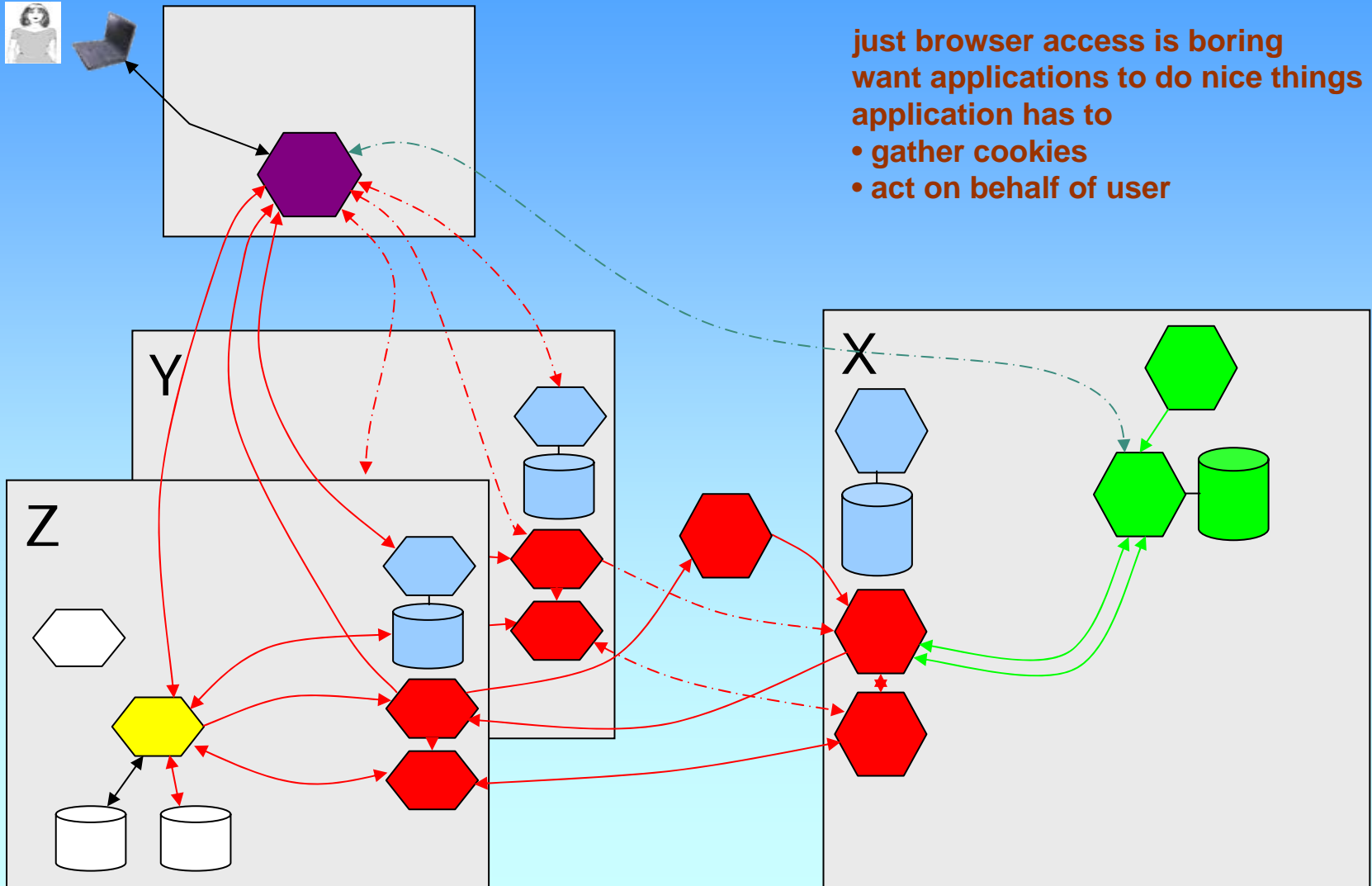


in our domain Shibboleth just delivers the UserID and the HomelID

- lot of overhead for little
- but reliable



IF in case of an application



just browser access is boring
want applications to do nice things
application has to

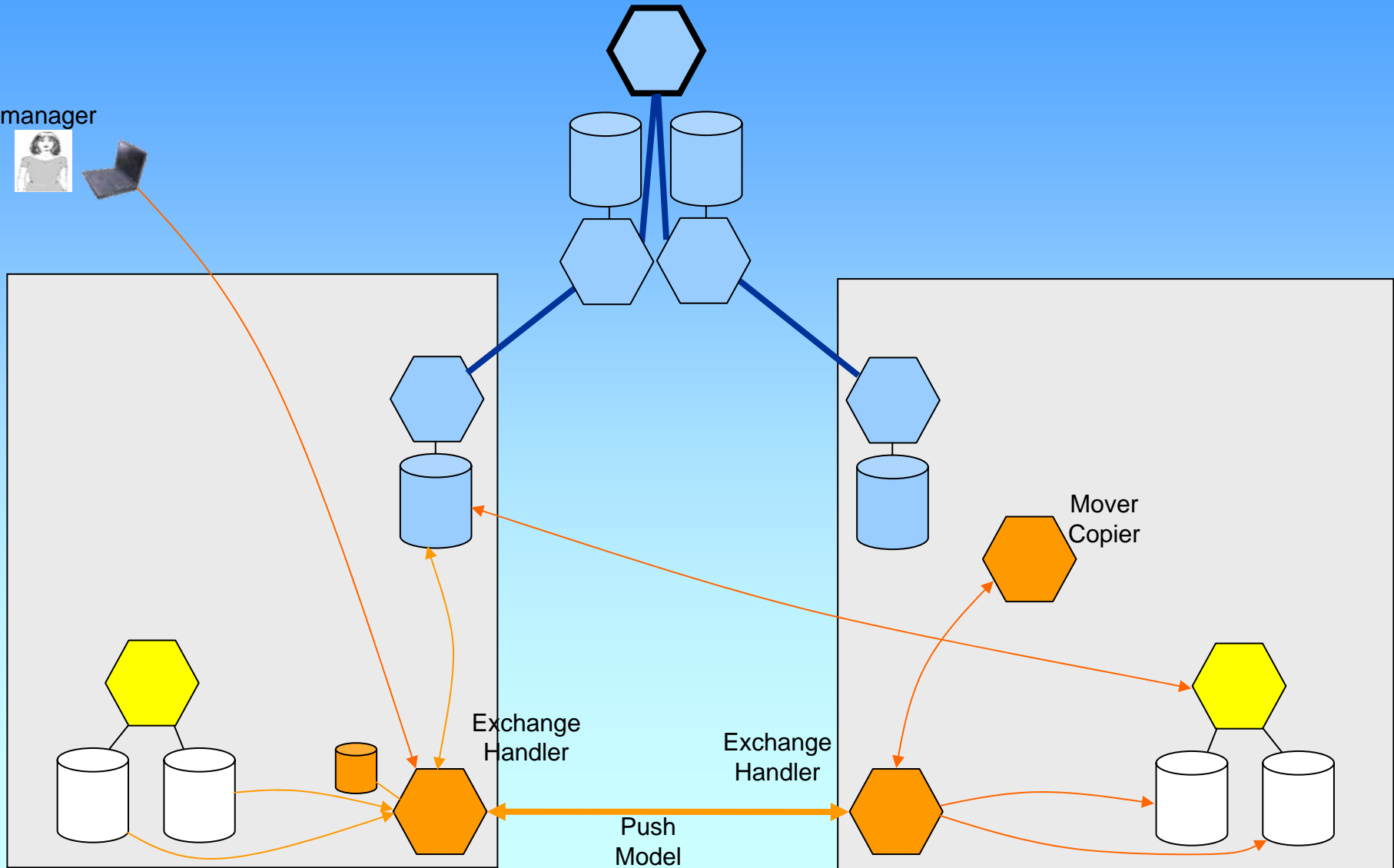
- gather cookies
- act on behalf of user



IF in case of Data Exchange

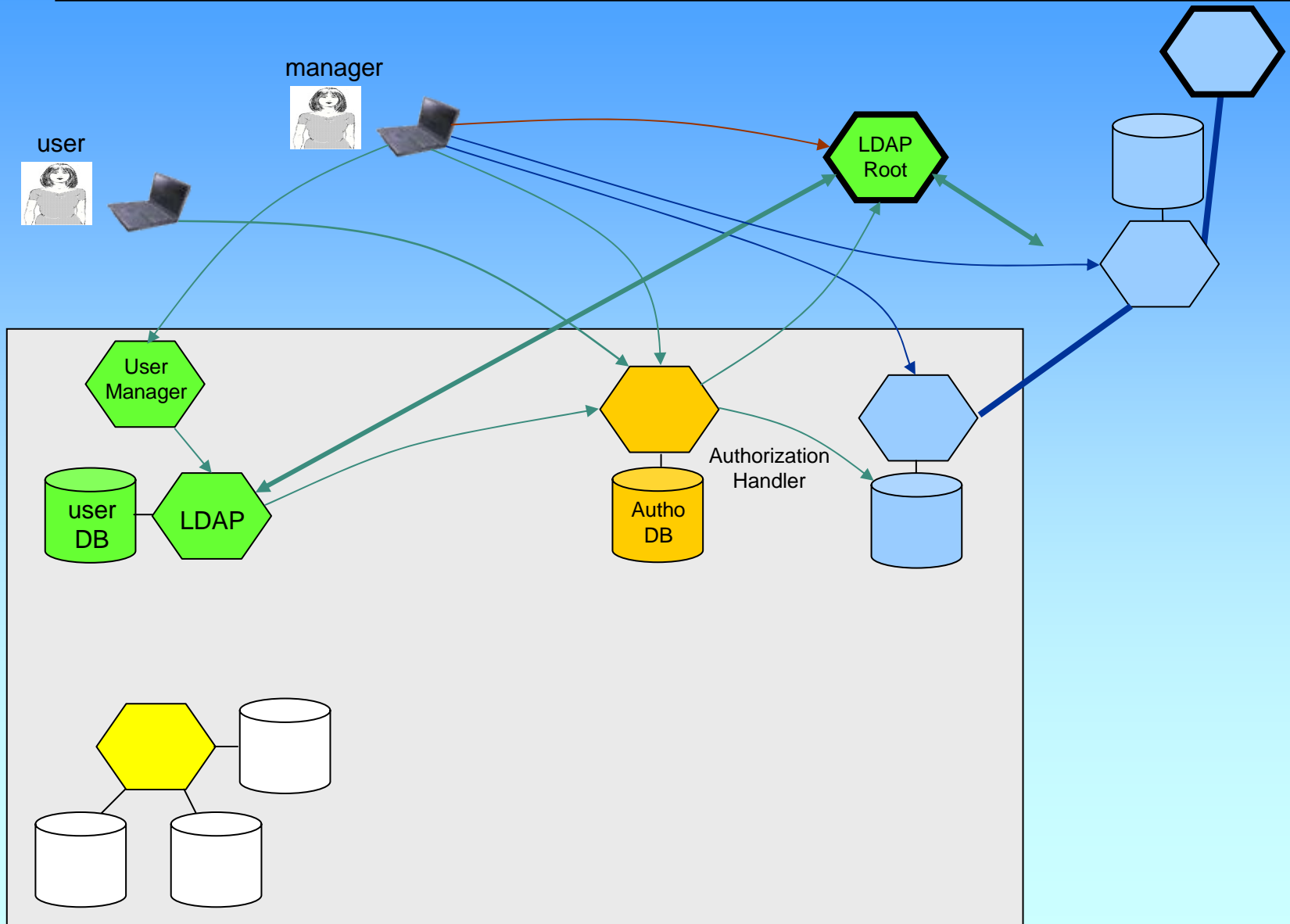


manager





IF during Management





To be developed in DAM-LR



- Resource Manager receiving Shib attributes and matching
- Authorization Handler combining attributes and resources
- Exchange Handler in case that we want to exchange data
- extend good web-applications

- all not simple programs – must be tested carefully
- in case of other components partners have to interface

- are in discussion with Handle System, Shib and other folks



•
•
•
End



- no way out if we want to go towards eHumanities scenario
- it is a complex scenario
- good is
 - EU wants to support all this and give it a long-term basis
 - so investments will not be lost