DAM-LR Distributed Access Scenario Complete

Peter Wittenburg

Daan Broeder

Adarsh Mehta

Freddy Offenga

Thomas Soddemann

Public Version

Federation

Partners synchronize on what they see as a federation.

Is there something beyond technical agreements?

At least there has to be trust!!!!

PKI System 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

URID System (already agreed!)

- all partners agree on using the Handle System (CNRI)
- each partner will become a handle authority and request a handle from CNRI
- each partner decides about the postfix of its handles
- MPI will setup mirror sites for all partners (others can do as well)
- each partner has full control about its Handle instance!!!

- each partner will install and maintain a Handle server
- each partner has to take care that the database is in good order

These actions have to be done until summer!!!

In case of questions Thomas is offering help and/or come to Nijmegen.

System for Authentication and Attributes to exchange

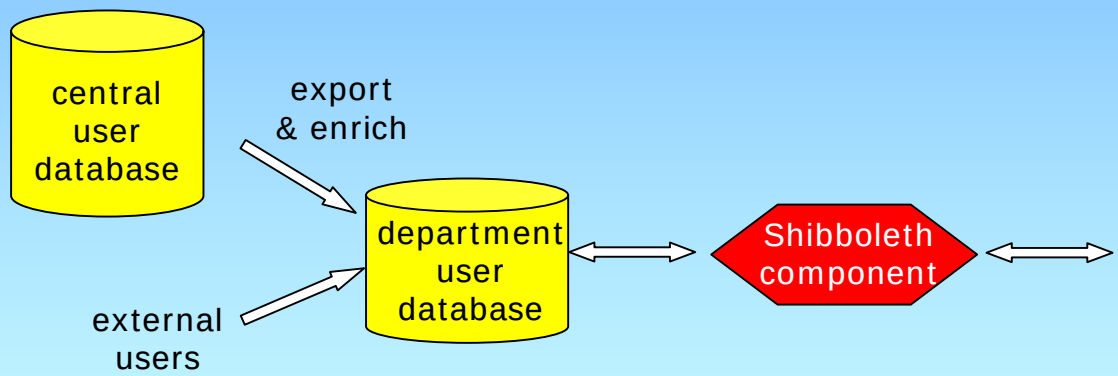
Open LDAP is chosen as the prototypical system to do user management
- widely used at universities, much functionality, many interfaces etc
- there is a possibility to create a joint LDAP domain (one search space)
- is partners do it differently then they have to adapt

have to agree on attributes that are stored in LDAP in addition to local username and password that we will exchange to identify persons
- first name
- last name
- affiliation
- hosting institute (in case of external user – always a federation member)
- email address
- status (researcher, guest, student, ...)
- class* (group membership)
- userID (most important – unique within federation)

Problems and Questions for Authentication System

- do we want a misbehavior flag?
- need a duration for external accounts (criteria?)

- what if computer center refuses to house externals?
- what if computer center refuses to add attributes?



LDAP comes with functionality that could help to implement such a scenario easily.

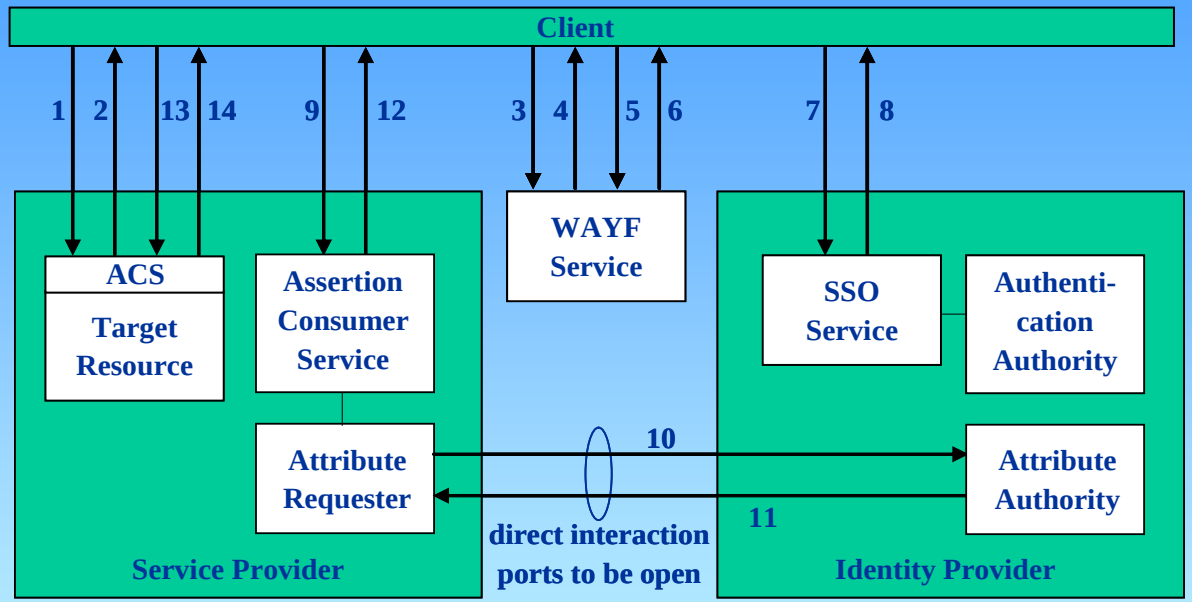
Authorization General Aspects

- 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

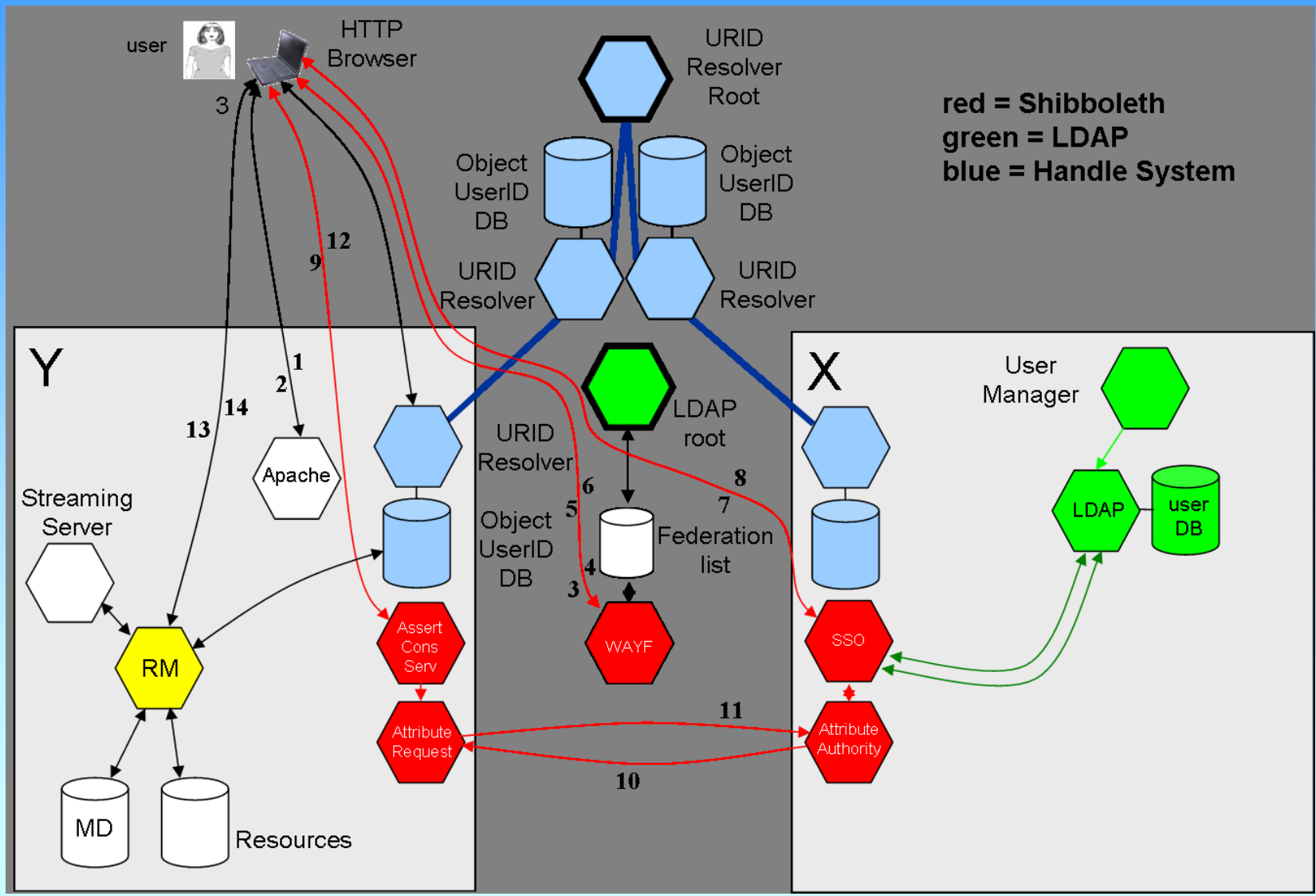
Shibboleth Scenario



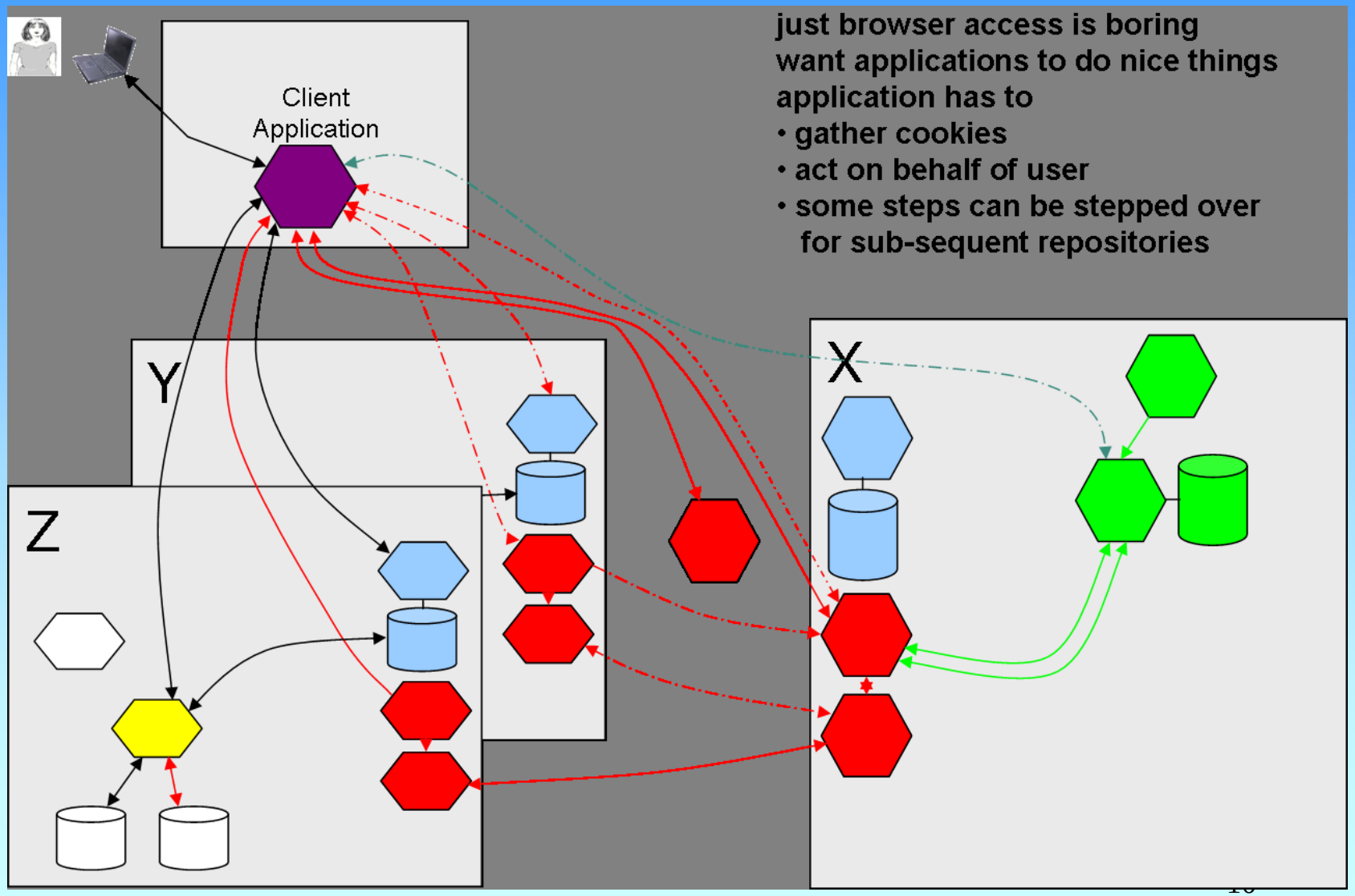
- ACS
  Access Control Service
- WAYF
  Where are you from service
- SSO
  Single Sign-On

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

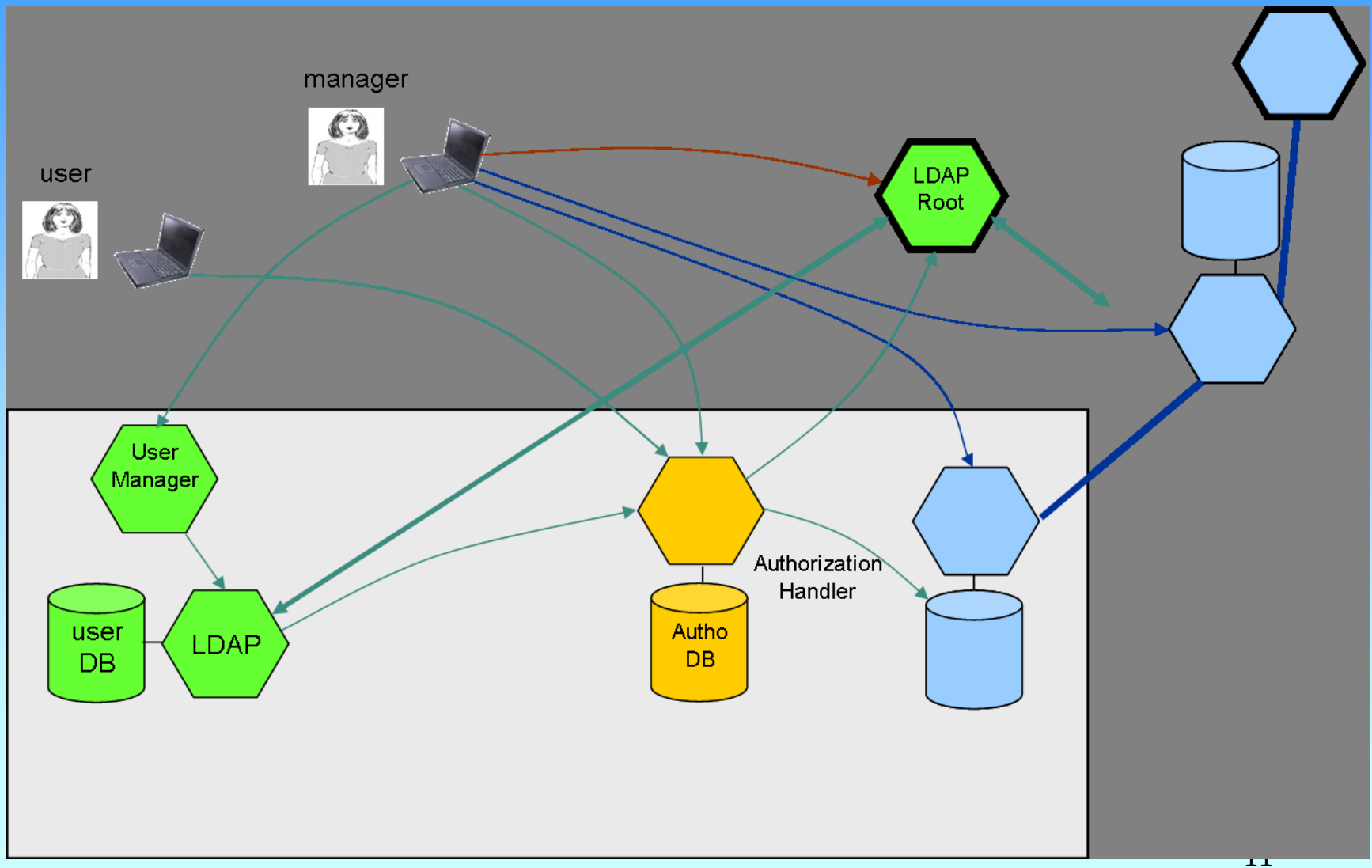
Typical Access Scenario



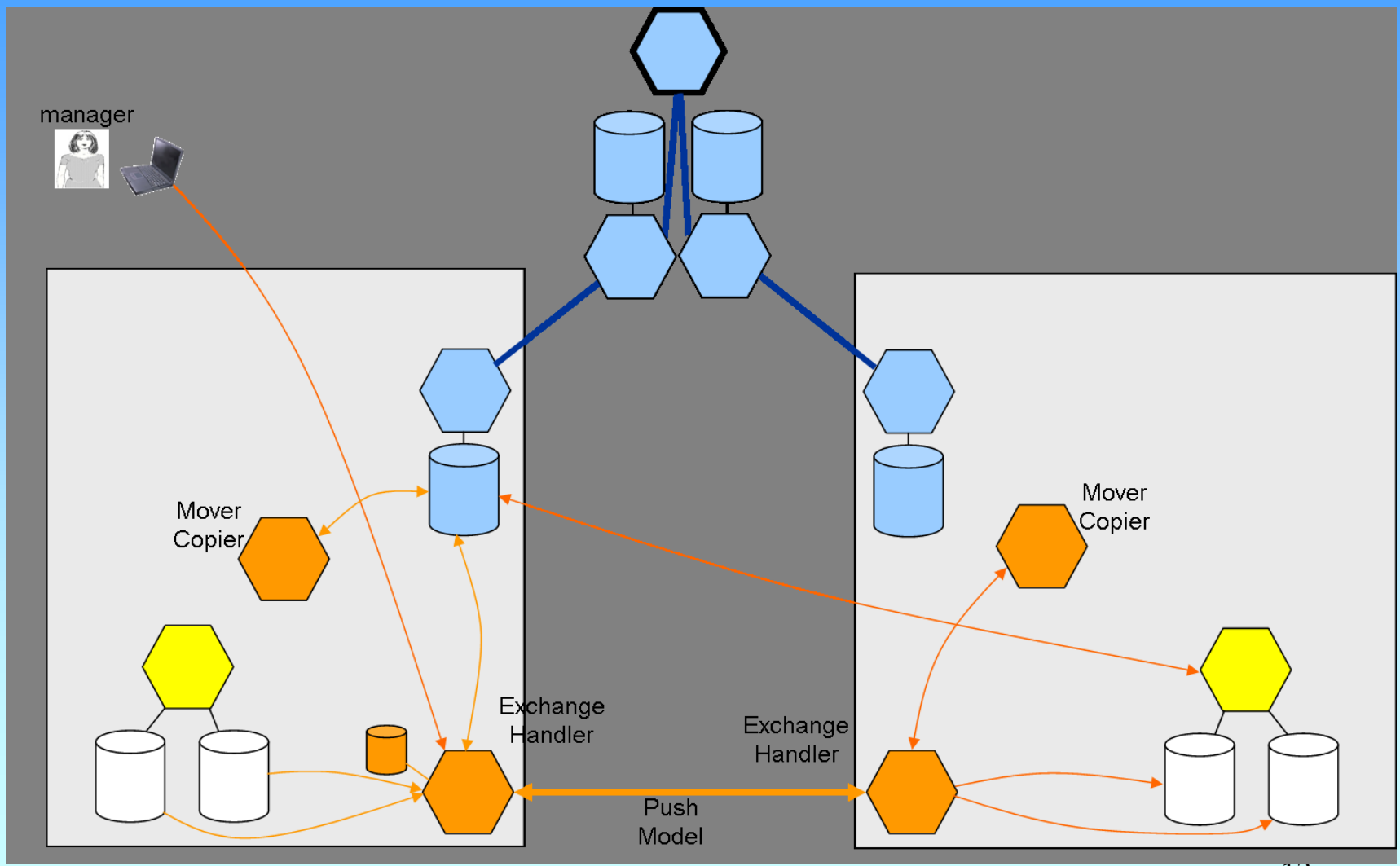
Application Access



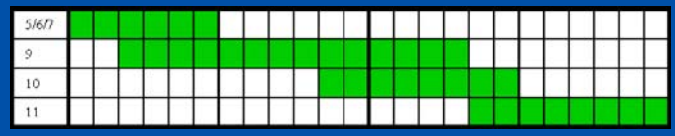
Management Scenario



Data Moving Scenario

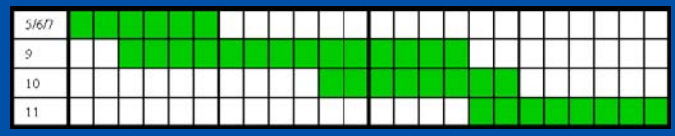


Summary: Federation, PKI, URID



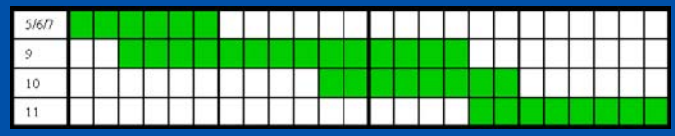
Action Points	deadline	init
agreement on what a federation is (trust, ...)	LREC Paper	SOAS?
Define a format for authorization records	2.06	MPI
become RA and setup a PKI system (inform with comp center)	6.06	all
Request a Prefix from CNRI	6.06	All
Define a handle postfix syntax	6.06	All
Setup a handle server	6.06	all
Play with HS and learn it	7.06	all
Create a program that generates your postfixes	7.06	all
Setup of mirror servers	10.06	MPI
Connect all servers	12.06	MPI
Adapt software	12.06	MPI
Local adaptations by other partners	2.07	all

Summary: authentication



Action Points	deadline	init
Agree on attributed that can be exchanged	1.06	mpi
Agree on account duration details (externals)	1.06	all
Discuss with computer center (external users, attributes, ...)	3.06	all
Setup an LDAP system or offer Shib compl. interface	6.06	all
Partners make an formal agreement about careful user management and attribute exchange	6.06	all
Setup of LDAP root domain if necessary	7.06	mpi

Summary: authorization



Action Points	deadline	init
Requirements for authorization process per partner	2.06	all
Make web-request forms (new user, access, ...) per partner	2.06	all
Setup a Shib test site at MPI	7.06	mpi
Setup Shib instances	9.06	all
First tests between Shib instances (MPI-INL-Lund?)	10.06	?
Develop a prototypical authorization handler	10.06	mpi
Develop a prototypical resource manager	12.06	mpi
Integrate all with final Shib instance	2.07	mpi
Install resource manager and/or adapt to local system	4.07	all
Install authorization handler and/or adapt to local system	4.07	all
demo applications	7/8.07	mpi
Start testing	7/8.07	inl

Last Slide

if useful ask Thomas for support/help
(he is from MPG computer center and active in the DEISA Grid project)