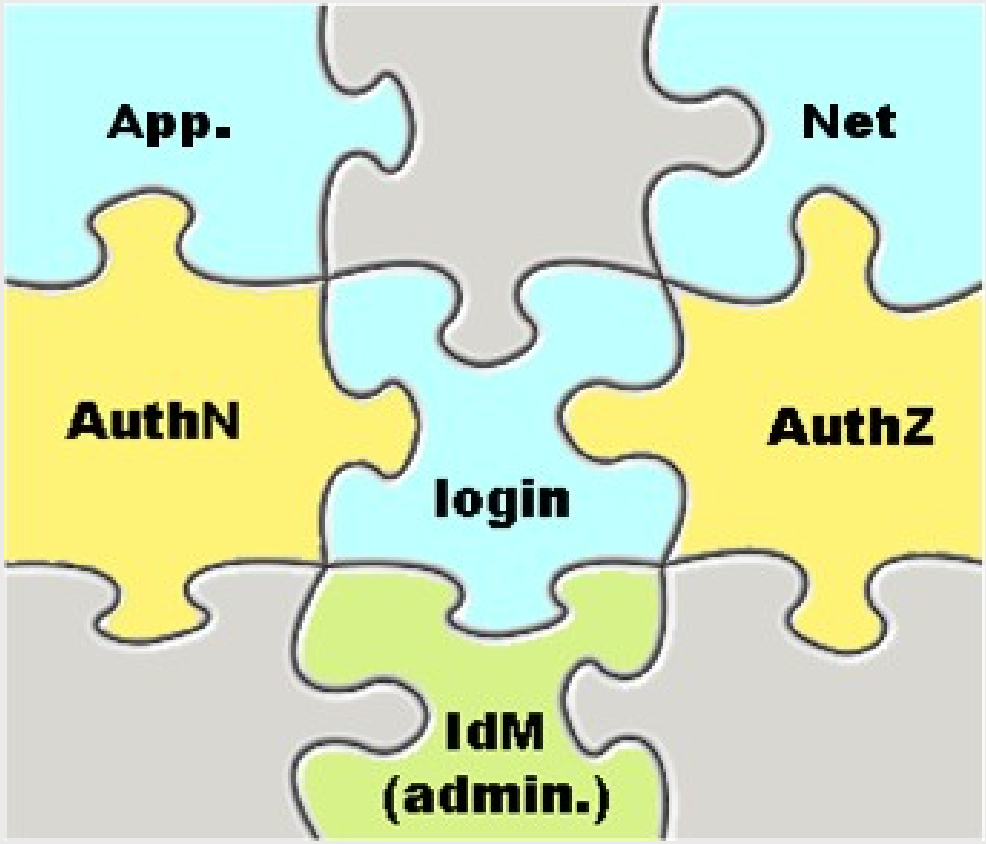
AOSI: The Identity Management System for AAI@EduHr

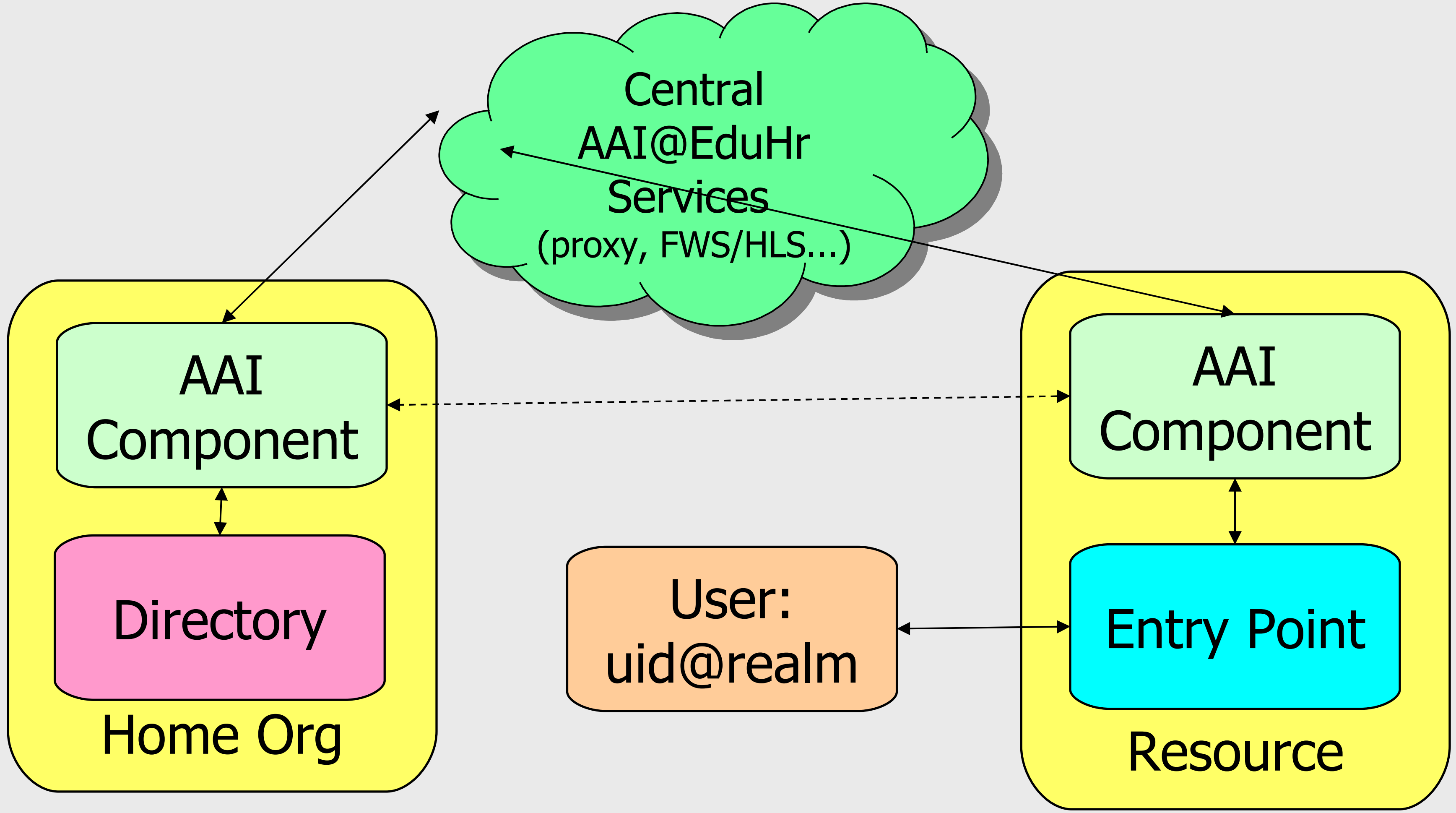
Denis Stančer, Mijo Đerek, Miroslav Milinović
University Computing Centre - Srce
<*aosi@aaiedu.hr*>

CUC 2005
Dubrovnik, November 2005

Authentication and Authorization Infrastructure

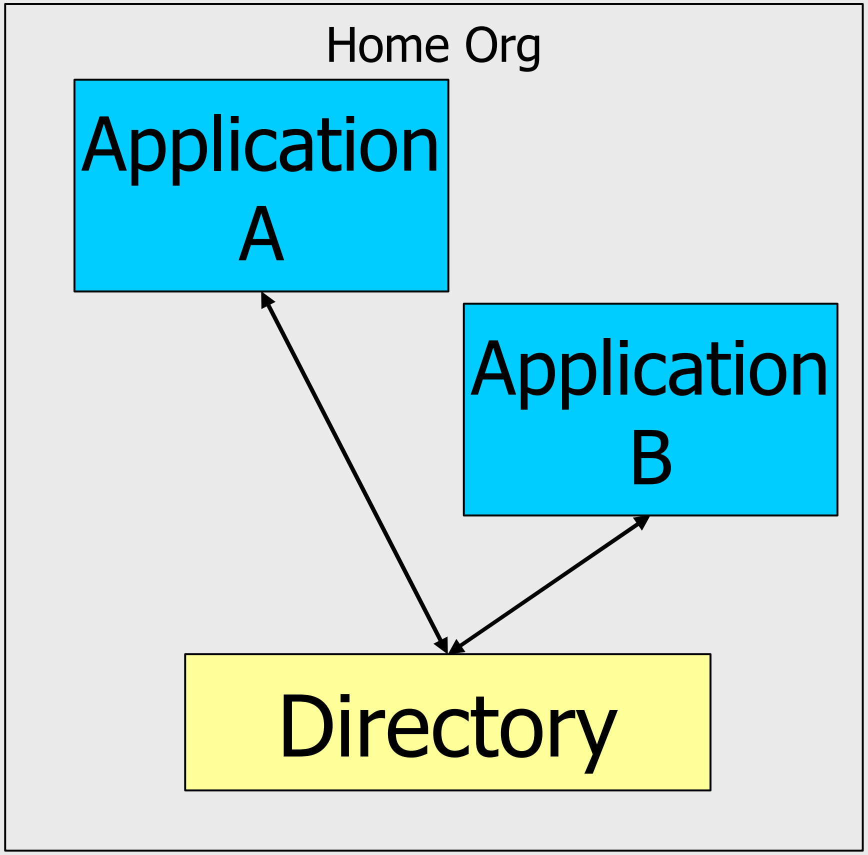


AAI@EduHr Today



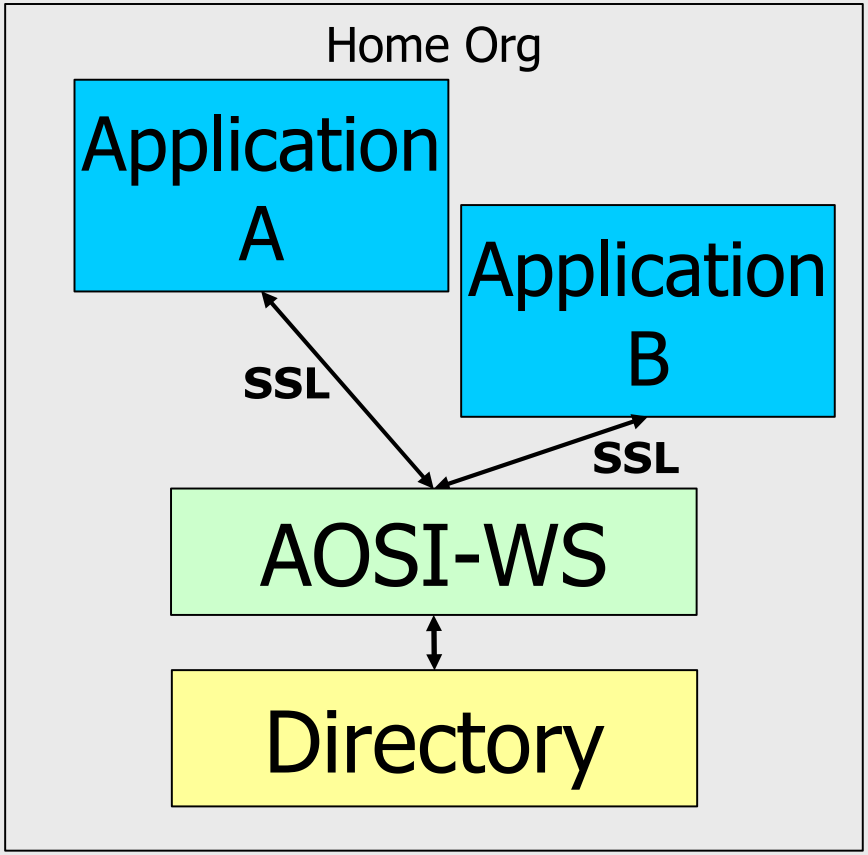
Identity Management (before)

- To manage (other persons') identities every application had to "know" the administrators password
- Unsecure!!!
- Each application had to cope with directory access challenges

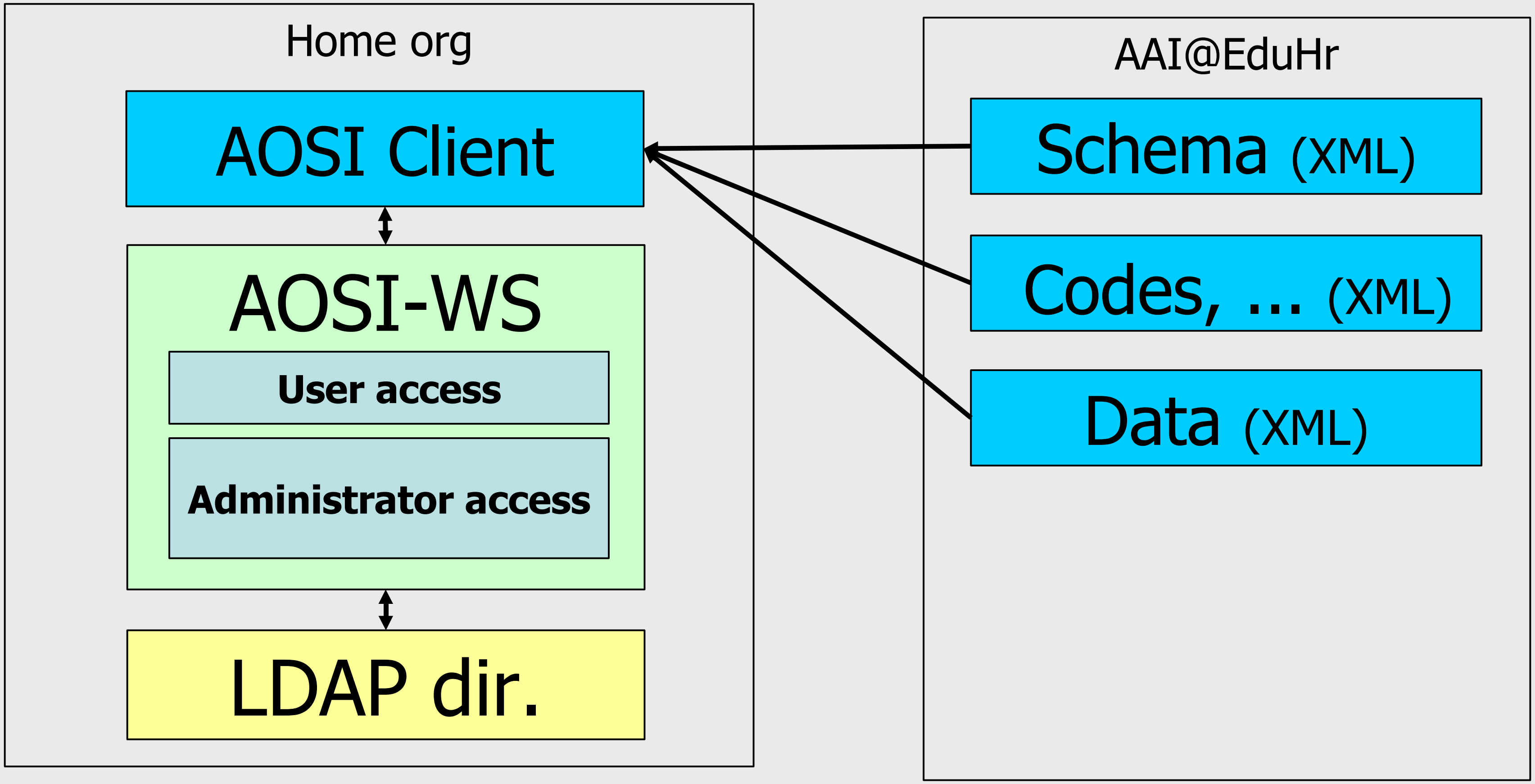


Identity Management (after)

- Administrators access the directory using their own credentials (i.e. no administrator password sharing)
- The communication is encrypted
- Directory access is handled by the web service

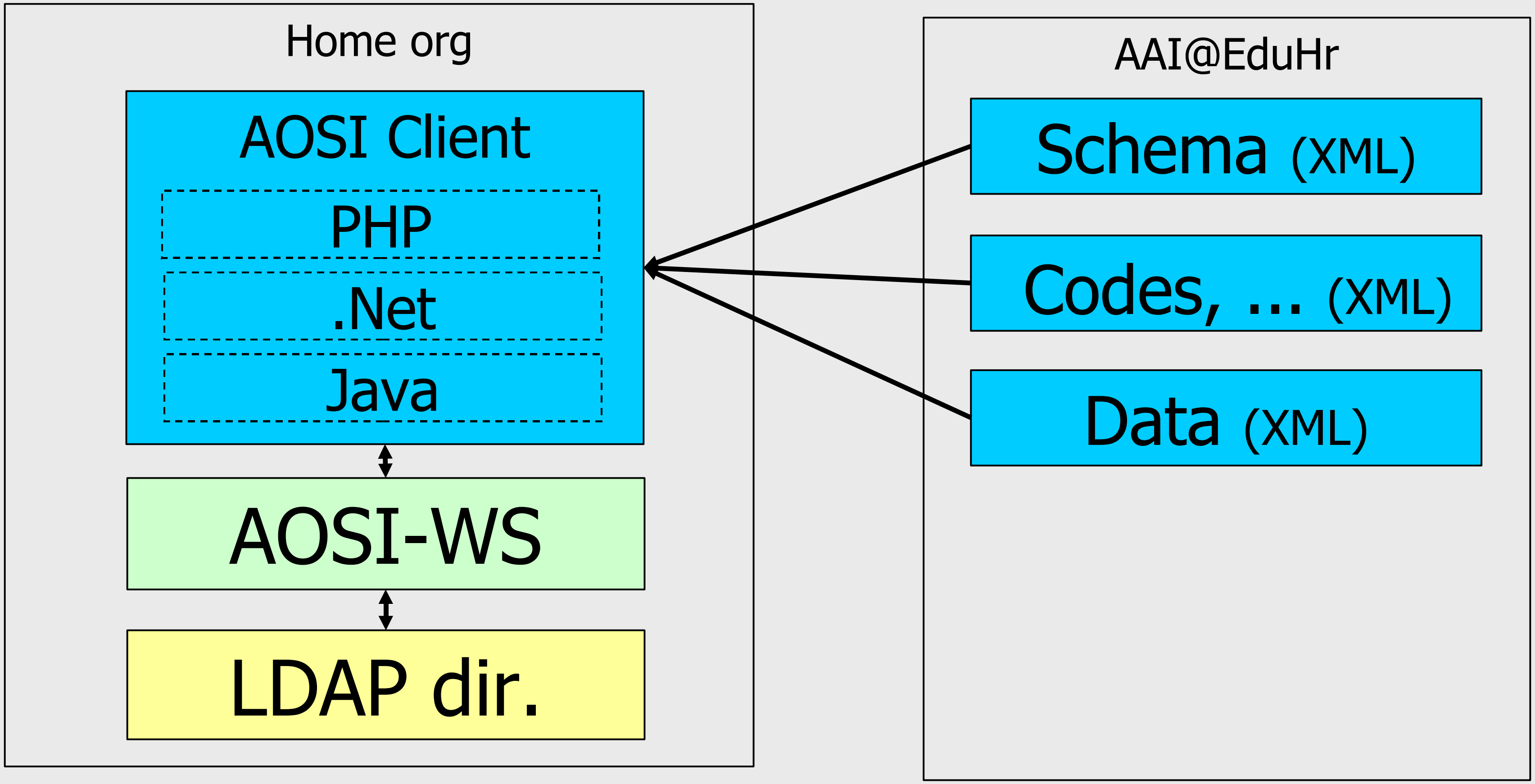


AOSI System



Home org
AOSI Client
AOSI-WS
User access
Administrator access
LDAP dir.
AAI@EduHr
Schema (XML)
Codes, ... (XML)
Data (XML)

AOSI System (2)



Administrator’s Access

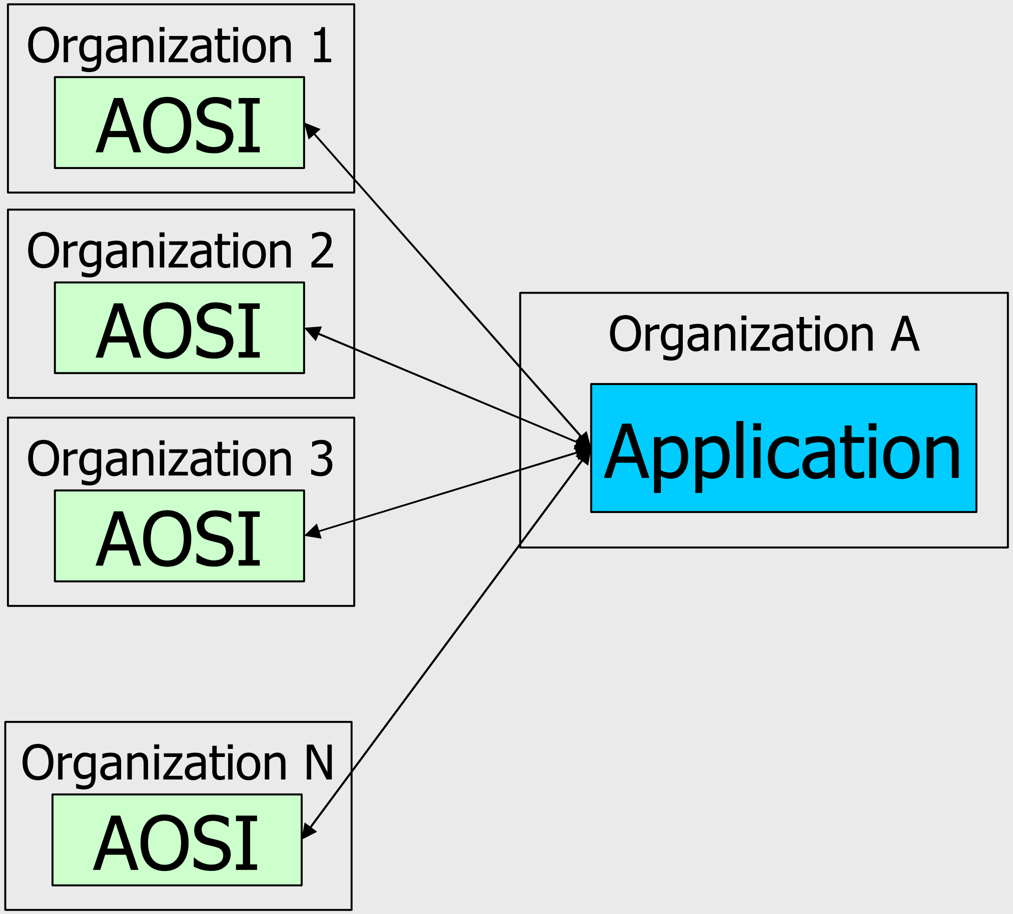
- Administrator can :
  - get the list of all users in directory
  - add a new user to the directory
  - delete a user from directory
  - list all the attributes for any user in directory
  - change the attributes for any user in directory

User’s Access

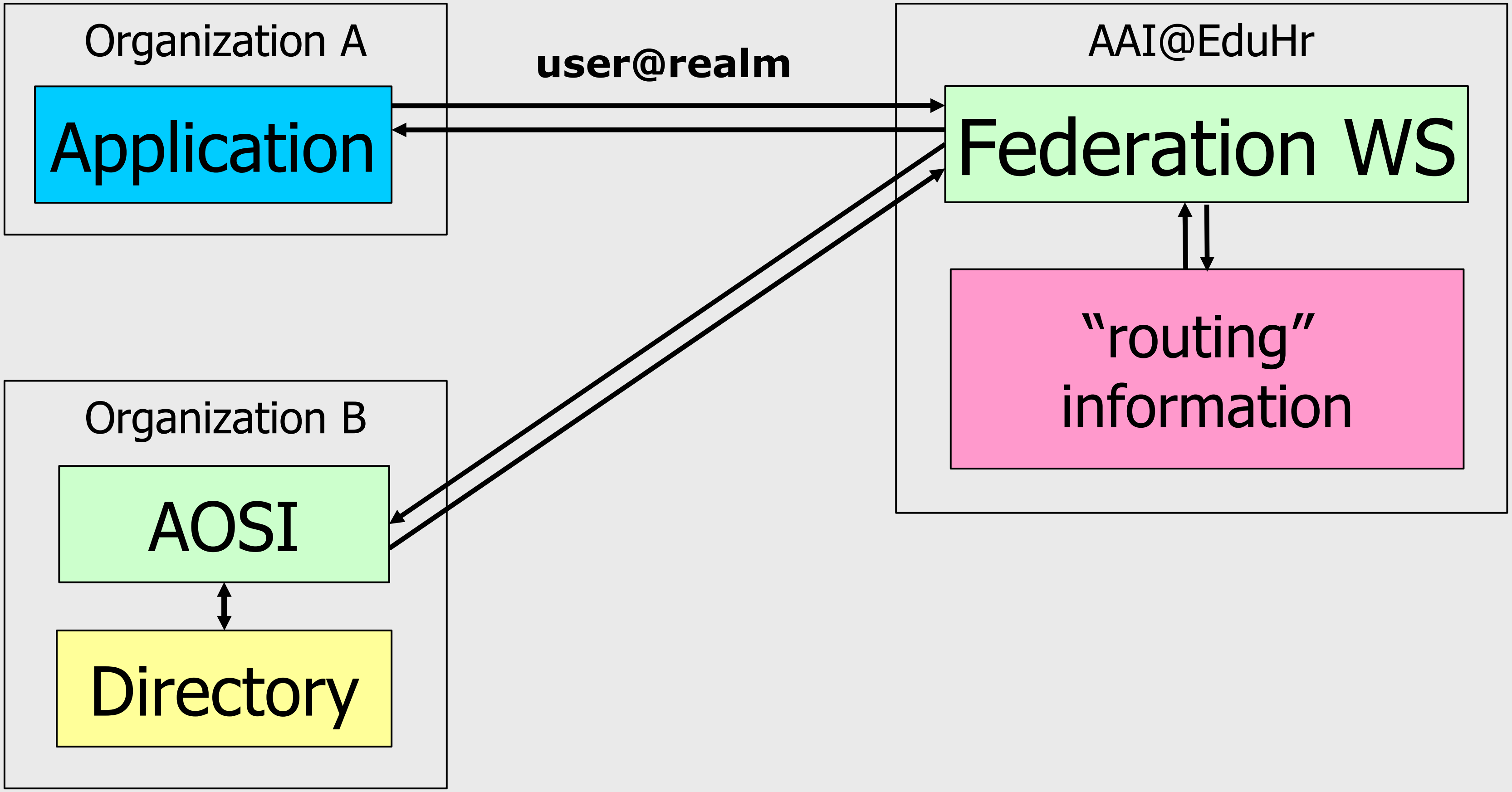
- User can:
  - list all their own attributes
  - list all public attributes of any user in directory
  - change specific attributes about them

Accessing Directories

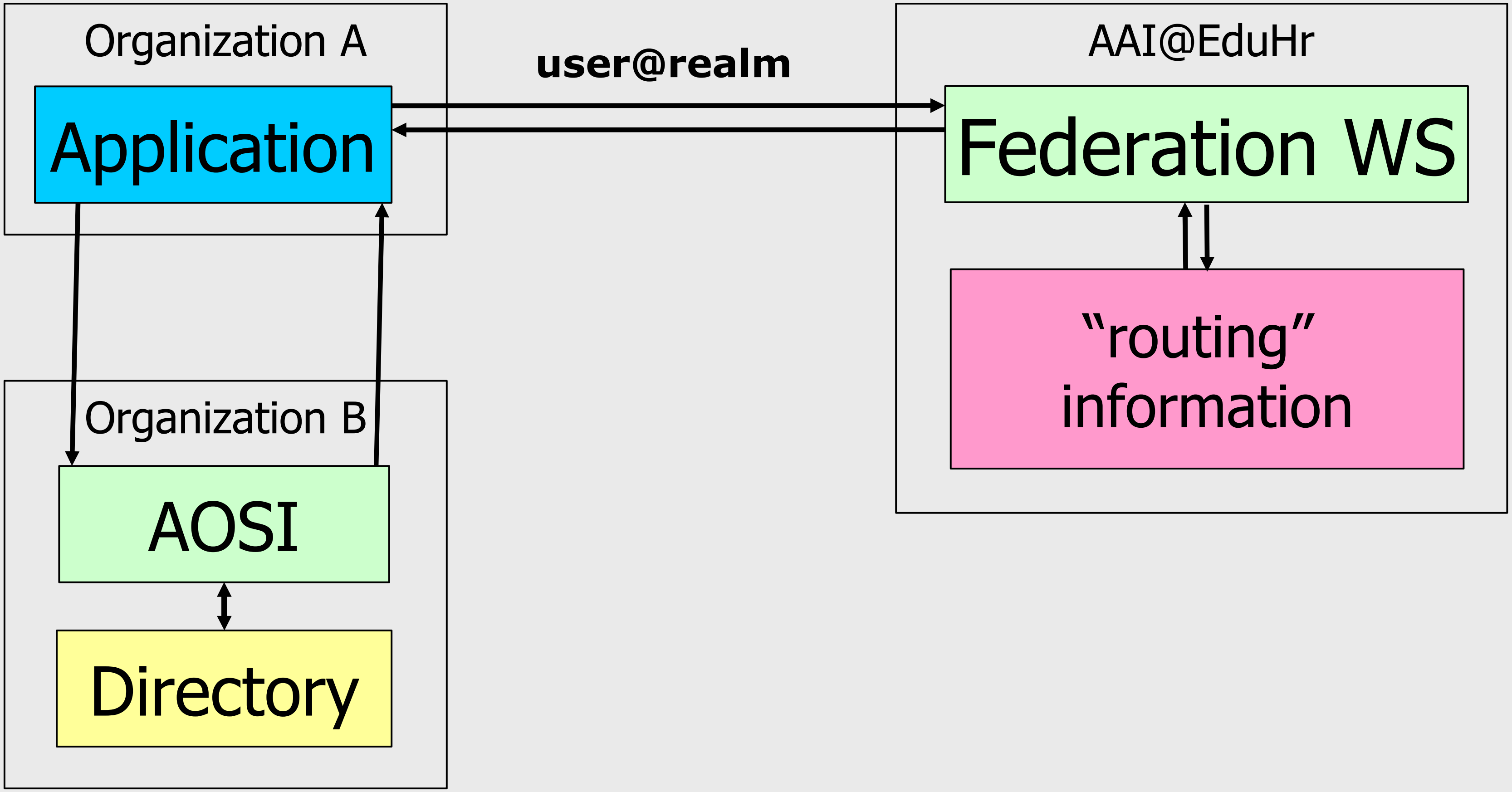
- Applications must be aware of the infrastructure
- Applications must "know" where a specific directory is located



AOSI in AAI@EduHr (1)



AOSI in AAI@EduHr (2)



Advantages for Applications

- Applications have a central place at which:
  - users are authenticated
  - attributes are acquired for authorization
- Applications do not have to be aware of the AAI infrastructure, they have a central point - WSDL file (http://www.aaiedu.hr/aosi/fws.wsdl)
- Each person which has an identity in AAI@EduHr can use any application (specific attributes can be required)

Advantages for Home Organizations

- The directory is accessed only from trusted places:
  - from inside the organization
  - from trusted point in AAI@EduHr system (Federation WS)
- Every user from organization that is in AAI@EduHr system can use any AAI enabled application or service

Advantages for Users (*Meeting Users Needs*)

- Every user with an AAI@EduHr identity can use any AAI@EduHr enabled application or service with his (already existing) credentials
- Each user with an AAI@EduHr identity can use eduroam service

Web service

- Based on Perl
- Each service is described in http://ldaphost.homeorg.hr/ldap/aosi.wsdl
- Generally runs at https://ldaphost.homeorg.hr:1443/AOSI
- Client platforms working with service:
  - Perl
  - PHP
  - .Net
  - Java

AAI@EduHr

http://www.aaiedu.hr/

team@aaiedu.hr

aosi@aaiedu.hr