VOMS/VOMRS convergence

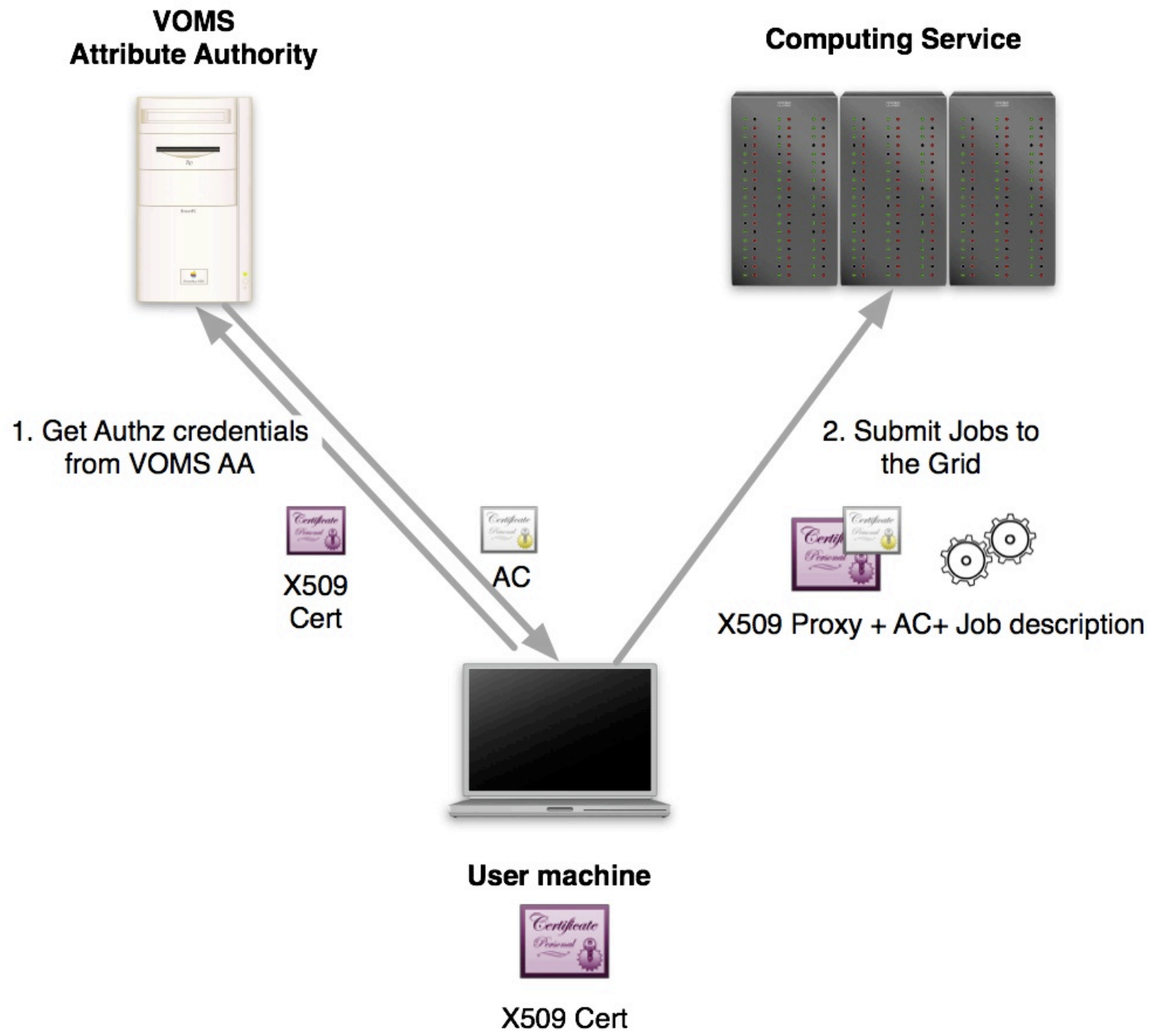
Andrea Ceccanti (INFN) - Speaker

Tanya Levshina (Fermilab)

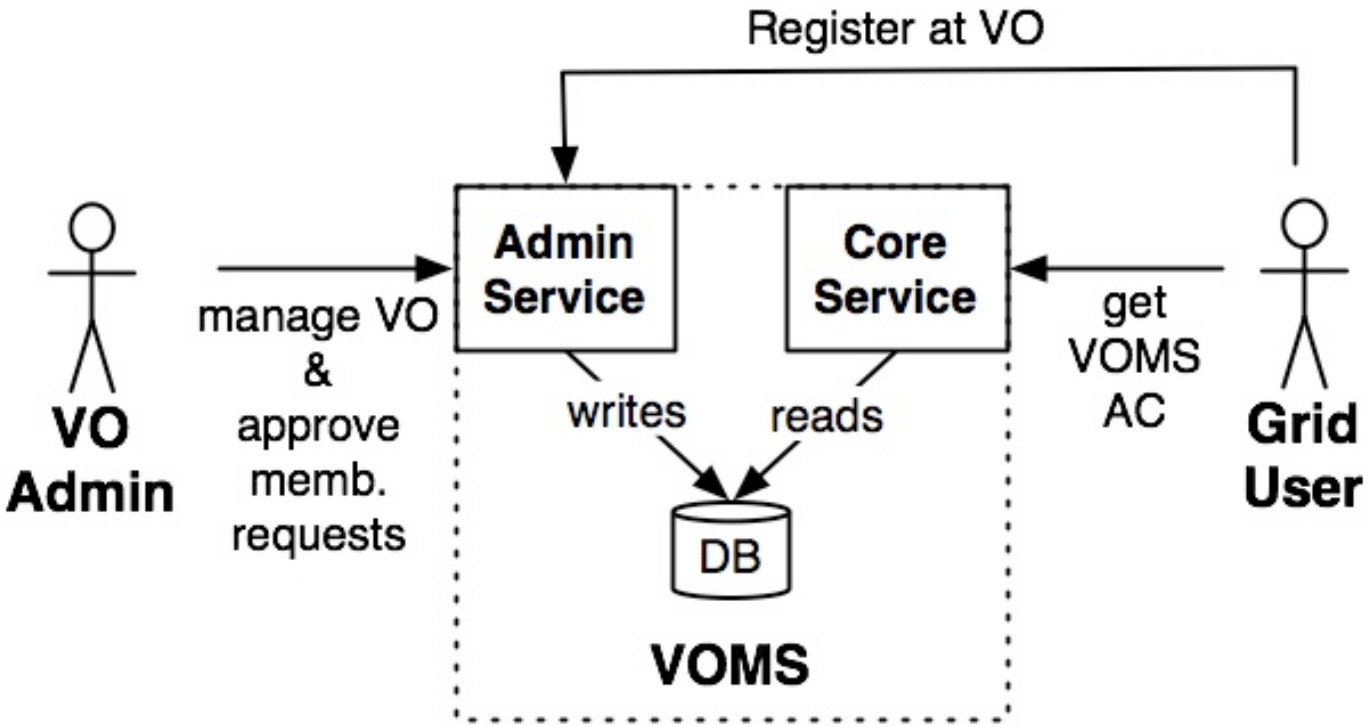
VO membership service

- An **Attribute Authority** (AA)
  - issues attributes (in the form of signed assertions) expressing membership information of a subject in the context of a Virtual Organization (VO)
- A **source of trust** for authorization on the Grid
  - access to Grid resources is typically regulated according to user's VOMS attributes
- A **VO registration and management service**
  - Grid users must be registered at a VO in order to obtain credentials that can be used to access Grid resources
  - Administrators handle users registration requests and define the structure of the VO by defining groups, roles, attributes that will be assigned to users

VOMS interaction



VOMS services



- The **VOMS Admin** service is used to administer the VO structure and handle registration requests
- The **VOMS core** service is contacted to obtain X.509 attribute certificates (ACs) containing VOMS attributes

VO Registration requirements

- VO registration services in use in WLCG must satisfy a set of requirements, i.e. must support
  - Multiple administrative roles (VO manager, Institute Representative)
  - Support for multiple certificates per user
  - Collection and management of personal user information
  - Suspension/expiration/renewal of VO user's membership
  - Management and versioning of VO Acceptable Usage Policies (AUP)
  - Ability for users to request group membership and role assignments

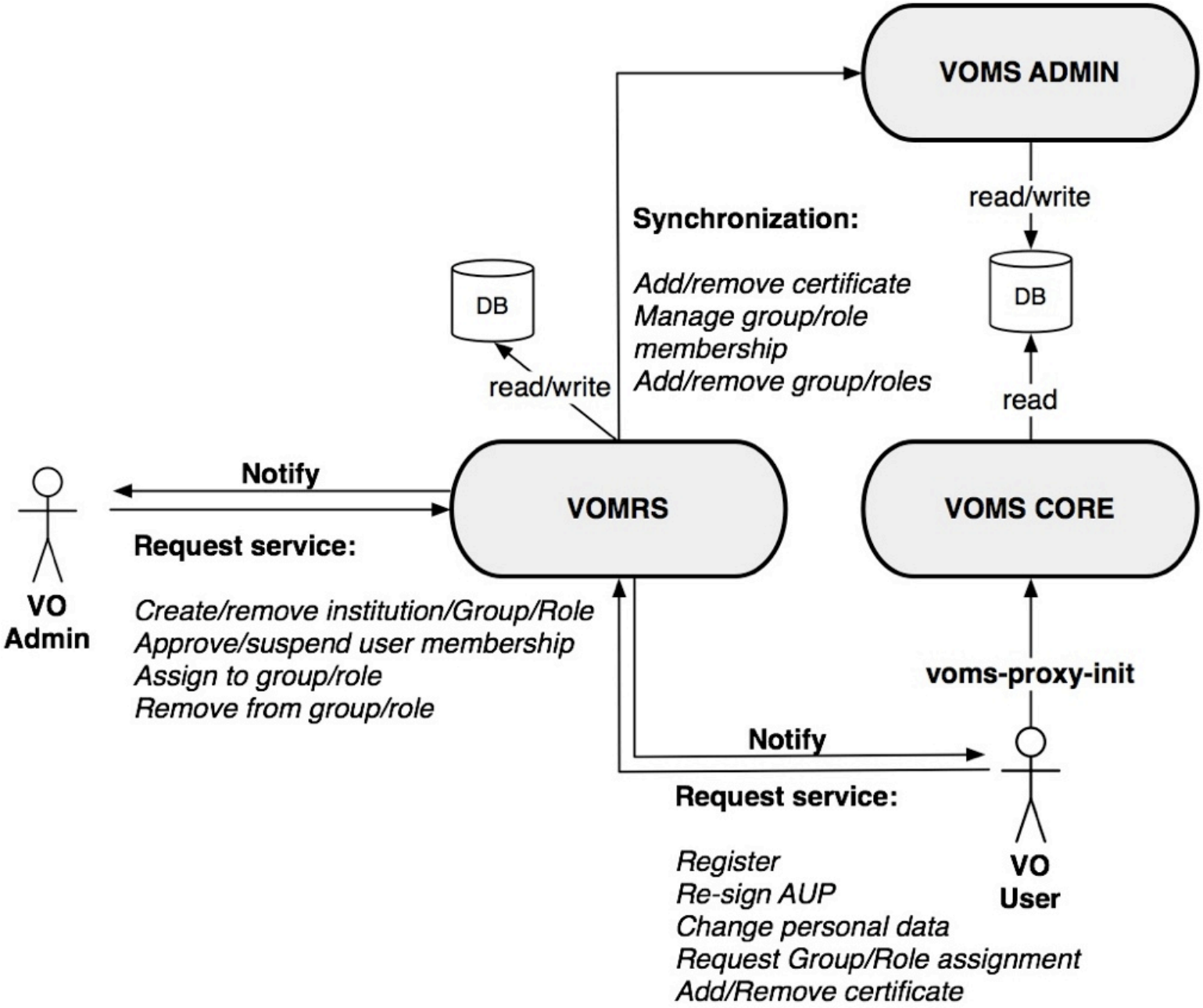
- JSPG requirements page:
  - http://www.jspg.org/wiki/Virtual_Organisation_Membership_Management_Policy

VO registration services

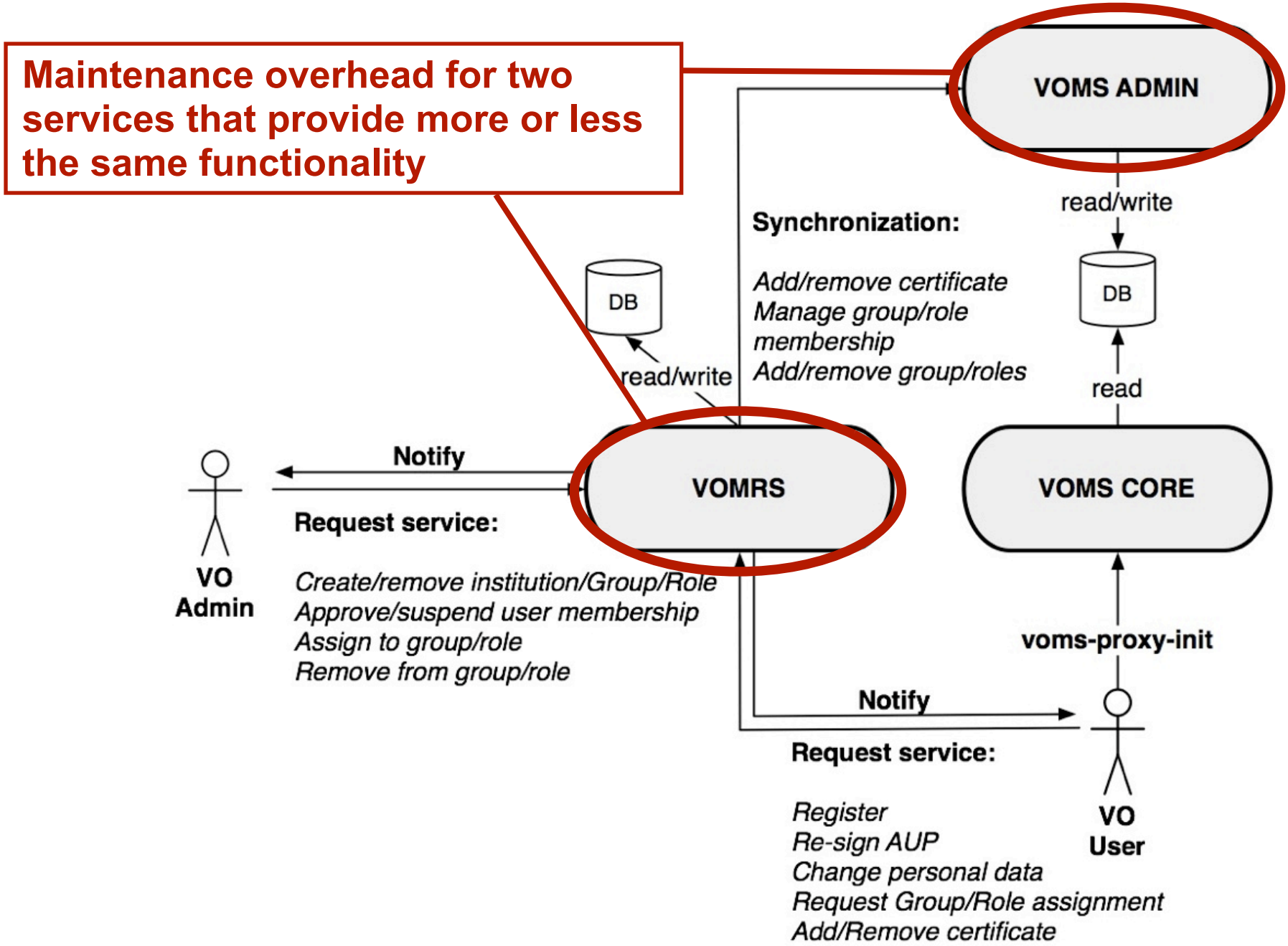
- VOMS Admin
  - main VOMS administrative and registration service
  - now compliant with JSPG rules for VO registration services
    - starting with version 2.5.x (i.e., since last april)
  - typically used by smaller VOs

- VOMRS
  - mature and flexible registration solution
    - built on top of VOMS Admin to extend its registration functionalities
  - compliant with JSPG rules for VO registration services
  - well suited to large VOs (LHC experiments)

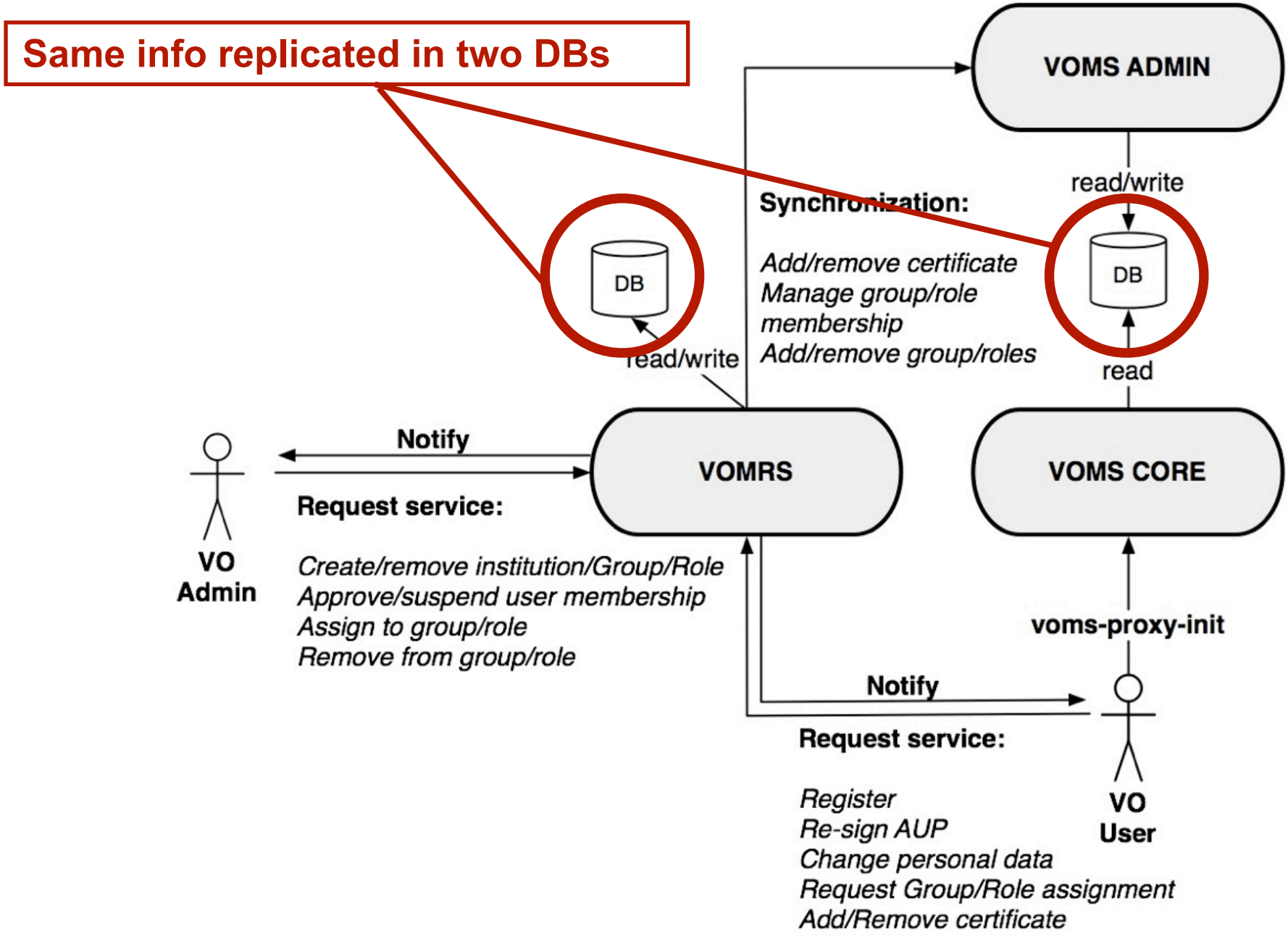
Typical VOMS/VOMRS setup



Typical VOMS/VOMRS setup



Typical VOMS/VOMRS setup



VOMS/VOMRS convergence

- Goal:
  - extend VOMS Admin functionalities so that all the main VOMRS features are implemented
- Why?
  - VOMS Admin and VOMRS share a large set of common functionality
  - Converge on a single solution that satisfies all user requirements
  - Easier deployment, maintenance, evolution
- When?
  - work started at the beginning of EGEE III
  - detailed schedule presented at CHEP 09
  - convergence is now reaching the final phases

The Convergence Schedule

Phase I	Implement JSPG requirements in VOMS Admin	**Done**
Phase II	Migrate essential VOMRS features to VOMS Admin	**Done**
Phase III	Interface with third party directory services (CERN HR db)	**Done**
Phase IV	Validation and certification tests	**Ongoing**
Phase V	Data migration from VOMRS to VOMS Admin	**?**

VOMS Admin 2.5

- Covers convergence phases I-II
  - Released on May 2010

- Main new features
  - Support for multiple user certificates
  - Support for versioned AUP management
  - Membership expiration, suspension, renewal
  - VO members can request group membership/role assignment
  - VO members can request membership removal
  - Support for multiple member operations (deletion, suspension)

Multiple certificate support

- Multiple certificates can be linked to the same VO membership
- These certificates share VOMS attributes information
  - Groups
  - Roles
  - Generic attributes
  - VO AUP acceptance records
- Users, once registered, can request the addition of other certificates to their membership
  - These requests require VO admins approval

AUP management

- AUP acceptance records are linked to each VO membership
- AUPs have a re-acceptance period
  - Each user's acceptance record is checked against this period and if the record has expired the user is requested to sign again the AUP in a configurable amount of time (24 hours is the default)
  - If the user fails to sign the AUP in time, he/she is suspended
- VO admin can request AUP re-acceptance from users at any time

Membership suspension

- VOMS membership can now be suspended
  - user is notified of the suspesion reason by email and by voms-proxy-init
  - Suspended members will not get VOMS attributes out of voms-proxy-init
- When a membership is suspended, all the certificates linked to that membership are suspended

Membership expiration/renewal

- An expiration date is linked to each membership
  - Default membership lifetime is configurable (default = 12 months)

- When a membership expires
  - the user is suspended (and informed of the suspension)
  - An administrator needs to take action to renew the membership
  - The user can be requested to sign the VO AUP again

VOMS Admin 2.6

- Covers convergence Phase III
  - under testing @ CNAF now
- Main new features
  - Pluggable request and membership validation framework
  - CERN HR database integration plugin

Phase IV

- VOMS Admin 2.6 is currently under testing at CNAF
  - Official release will be come as part of EMI-1 release (scheduled for April 2011) or as an update for gLite 3.2

- A meeting with VO managers is being organized at CERN for February 2011
  - present the new VOMS Admin to VO managers
  - gather feedback on the new features
  - assess that all the functionality requested has been migrated
  - discuss VOMRS to VOMS Admin data migration strategies and tools

Backward compatibility remarks

- VOMS Admin 2.6 and VOMS 2.0 will be certified together
  - It's suggested that you upgrade both services to get all the new functionality
- VOMS 2.0 is compatible with older clients
  - voms-proxy-init >= 1.6.16
  - you don't have to require updates on all your clients!
- VOMS Admin 2.6 is compatible with older clients
  - voms-admin, VOMRS, MkGridmap, Replication scripts based on VOMS Admin WS, ...
  - obviously new functionality is not covered by older clients (e.g., new certificate management WS)

Conclusions

- Converging on a single, mature VO registration management solution that covers all user requirements has several advantages
  - Simplified deployment and service operation
  - Simplified software maintenance and evolution
- The VOMS/VOMRS convergence project, started at the beginning of EGEE-III, is now reaching its final phases
  - Development is done, testing is ongoing
  - A meeting with VO manager is scheduled for February 2011 to gather feedback on recent developments
- The last phase of the convergence will focus on VOMRS/VOMS data migration tools and will likely be completed during the lifetime of the EMI project

Useful links

- VOMS/VOMRS CHEP convergence paper
  - http://www.fnal.gov/docs/products/voprivilege/documents/VomsVomrsConvergenceCHEP09-final.pdf
- VOMS Admin 2.5
  - User's guide:
    - https://twiki.cern.ch/twiki/bin/view/EGEE/VomsAdminUserGuide
- Contacts:
  - andrea.ceccanti@cnaf.infn.it
  - tlevshin@fnal.gov

Thanks!

EMI is partially funded by the European Commission under Grant Agreement INFSO-RI-261611