CoreGRID

EchoGRID Third Strategic Workshop
June 9 – 10, 2008
NTUS-ICCS - Athens

Virtual Organisations - Management and Authorisation Technologies

Wolfgang Ziegler
Fraunhofer Institute SCAI

Athens – Greece, June 9, 2008

Acknowledgements

– *Some of the work reported in this presentation is funded by the German Federal Ministry of Education and Research through the D-Grid Infrastructure projects on VO-Management, Interoperable Virtual Organisation Management (IVOM) and AAI/VO. This presentation also includes work carried out jointly within the CoreGRID Network of Excellence funded by the European Commission's IST programme under grant #004265.*

Overview

- Motivation
- Background and Introduction
- Processes in VOs
- Current technology
- Future directions
- Conclusion
- Further resources

Motivation

Current Roadmap section on Virtual Organisations

- Discusses the roadmap on an rather abstract level
- Does not include technological aspects which are important for the 3-5 years roadmap period

Thus, this presentation is

- rather technology driven than visionairy
- presents ongoing work to approach to the state of the art

Background

Three D-Grid Projects

VO-Management – Creating a framework concept for VO-Management in D-Grid

IVOM – Addressing interoperability of D-Grid VO-Management Technologies

AAI/VO – Targeting dynamic, short-lived VOs, aggregation of attributes from different sources, required AAI

Introduction (1)

Virtual Organisations

Initial focus was on sharing resources for collaboration

A Virtual Organisation is a

consortium, either permanent or limited in time,
of geographically distributed
individuals, groups, organisational units or whole organisations,
joining part of their physical or logical resources and services, their knowledge and capabilities as well as parts of their informational basis in a way that
the jointly agreed upon goals may be achieved.

Essential for VOs is the authorisation based on attributes

Roles in the VO, IdP attributes like eduPerson

Introduction (2)

What is available

- Different solutions and implementations rather static VOs

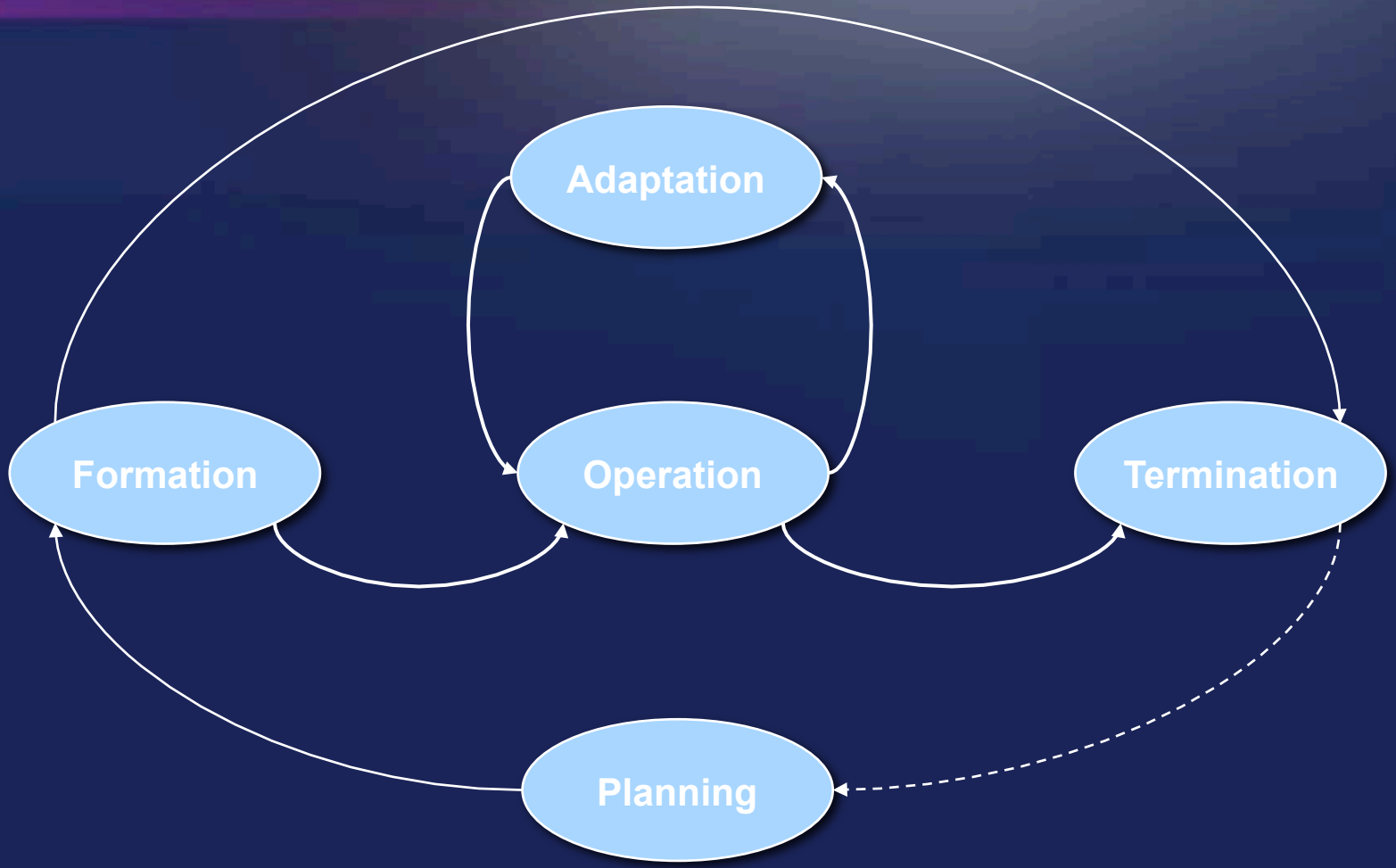
What is lacking

- Interoperability, flexibility, dynamicity

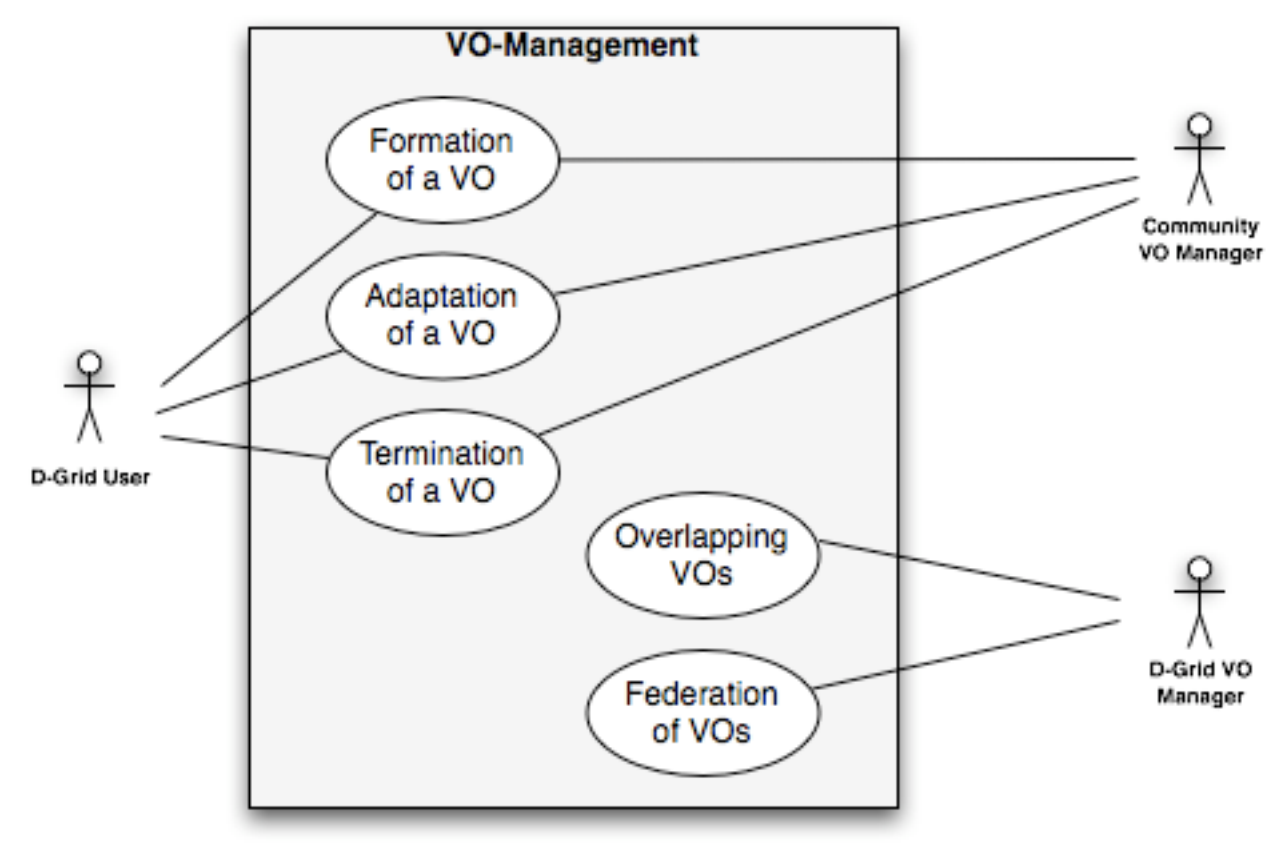
Wishes and Trends (to some extent still a vision)

- Interoperable technologies for VO-Management
- More flexible Virtual Organisations
- Highly dynamic Virtual Organisations

Life-cycle of VOs



Roles and Processes in (D-Grid) VOs



Current Technologies (1)

Authentication

- X.509 certificates - static
- Identity provider (Shibboleth approach) – more dynamic

Authorisation

- Attribute certificates (VOMS server) – more dynamic
- SAML Assertions (idP) – more dynamic

Current Technologies (2)

- VO-Formation
  - VOMS - Virtual Organization Membership Service
    - Management of Virtuel Organisations and VO Attributes
    - VO Attributes are embedded in a proxy of the user's X.509 certifikate
    - Attributes are evaluated by the gLite Policy Decision Point using the information in the local gridmap file
  - VOMRS - Virtual Organization Management Registration Service
    - Management front-end for VOMS
    - Management of VOs and VO-Attributes
    - No direct interaction with the Grid Middleware
    - VOMRS information is to be exported into the respective gridmap file

Current Technologies (3)

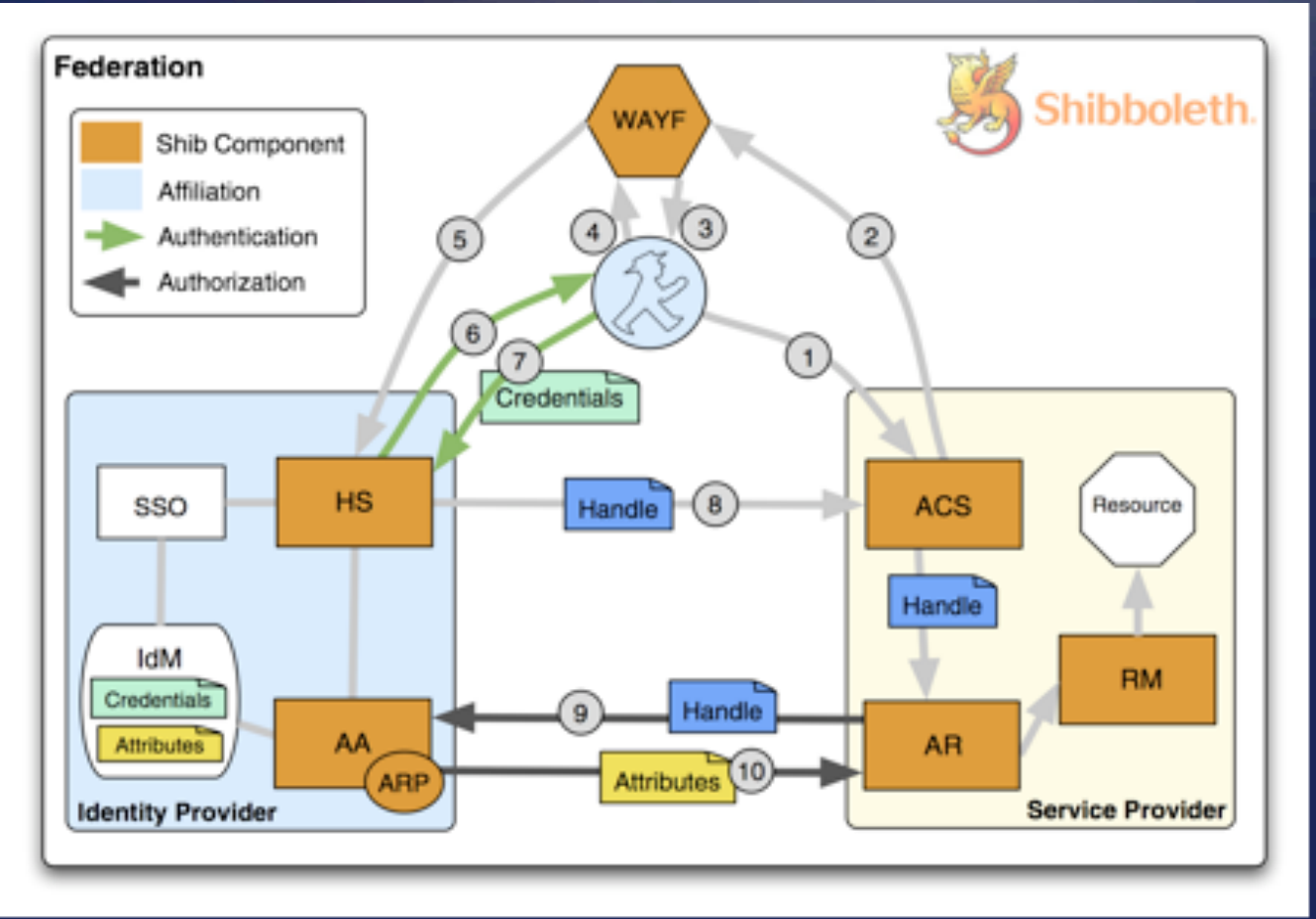
VO-Formation

- **Federation, e.g. using Shibboleth**
  - **Attributes of users are managed by his home organisation , the Identity Provider (IdP)**
  - **Campus Attributes of a user are transferred to the PDPs of the Service Providers**
  - **No direct interaction with the Grid Middleware**

No matter which technology is used:

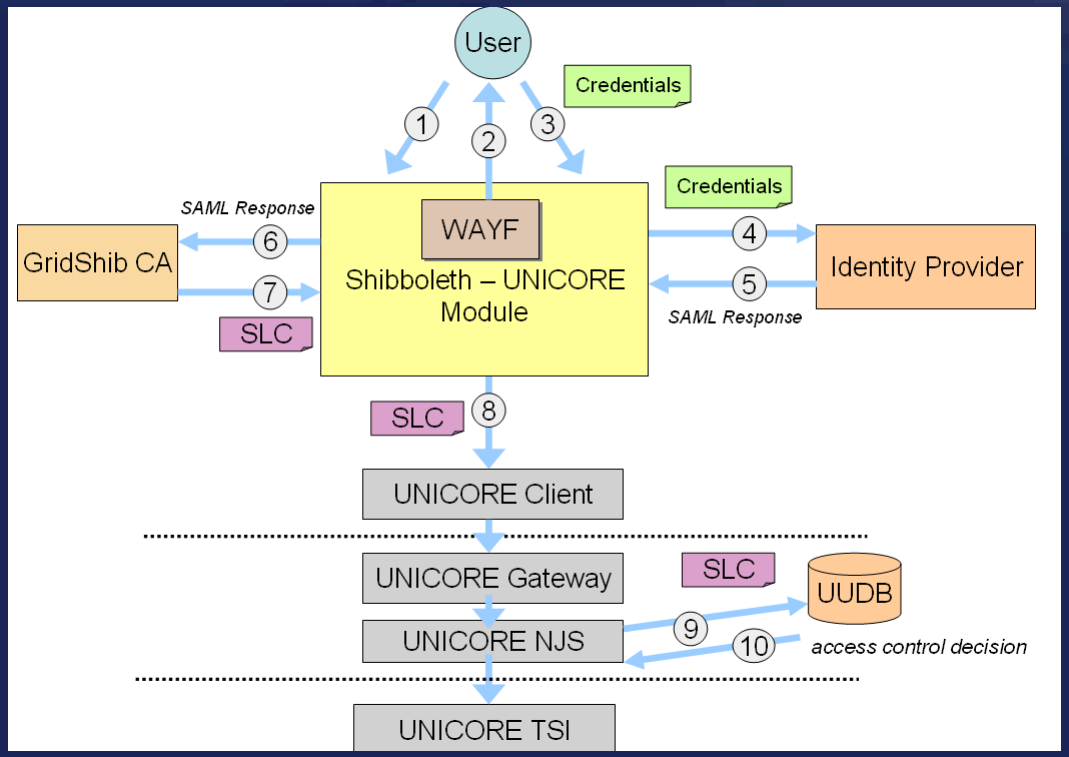
Legal issues, framework contracts have to be considered beforehand.

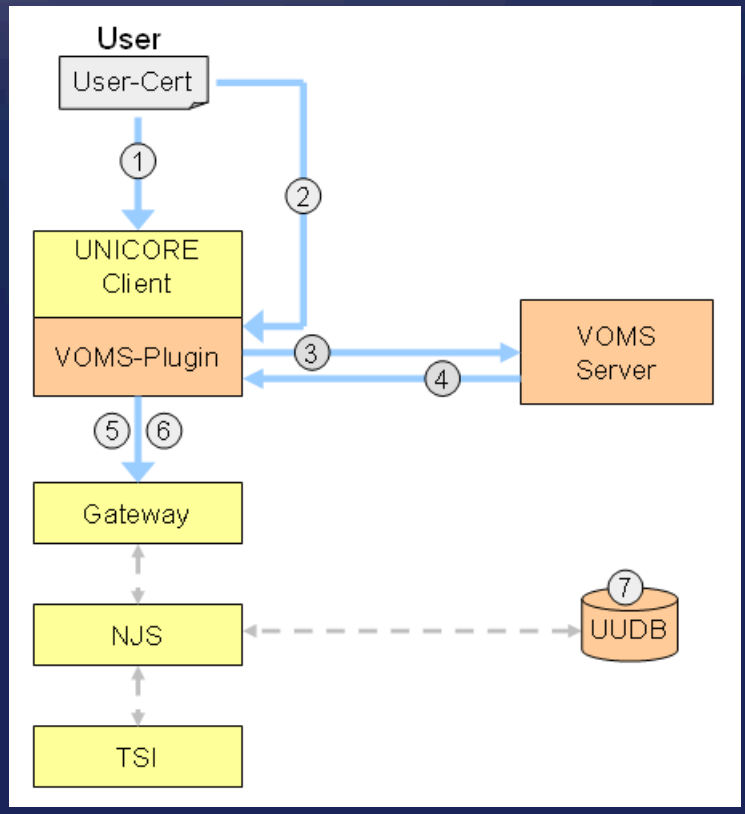
Technology Example



Interoperability Example

- Environment for Authorisation based on DNs and VO specific Attributes
- Extend UNICORE for support of VO/Attributes, UNICORE 5 as initial code base





Other Solutions Around

GridShib

- Makes Campus Attributes of a user available in Globus Toolkit 4
- PDP for evaluation of attributes integrated in GT 4.2

ShibGrid

- Supports Shibboleth Attribut-based Authentcation within the UK National Grid Service
- Access to NGS Ressources through federated mechanisms for Authentification using dynamically generated (Proxy-)Certificate

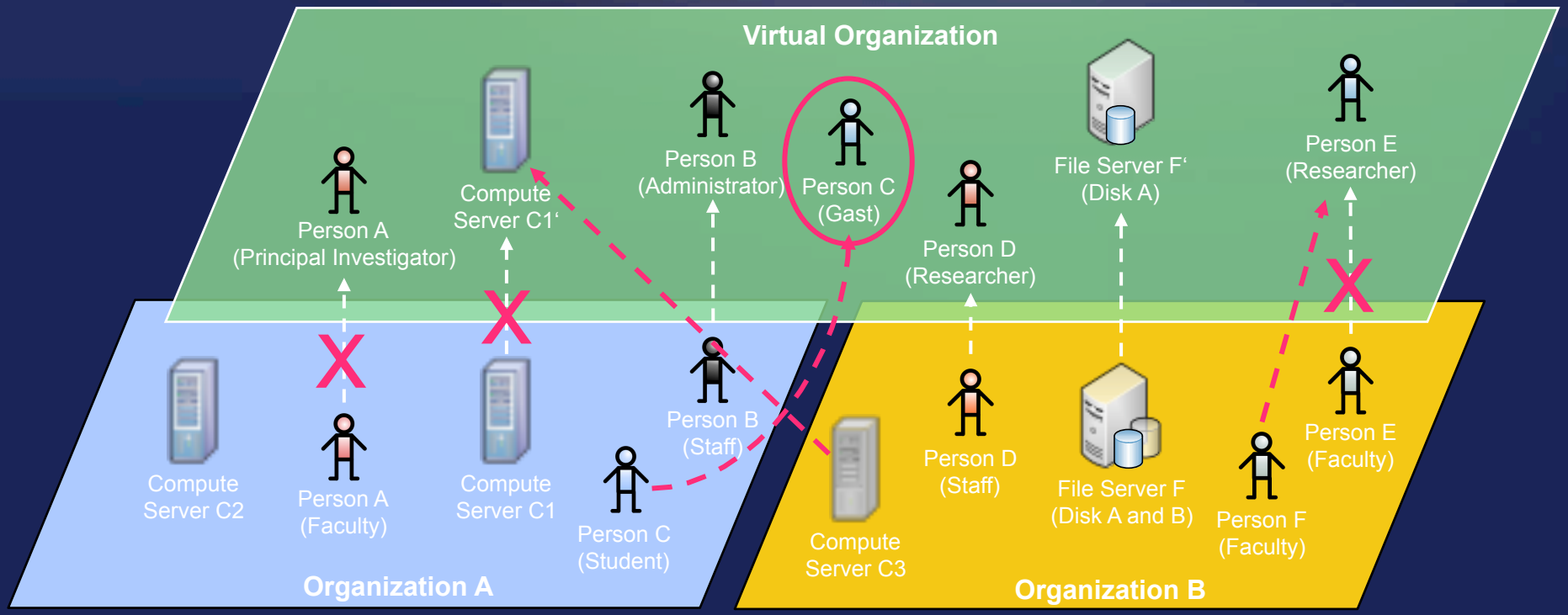
VASH - VOMS Attributes from Shibboleth

- Developped by SWITCH for EGEE users
- Brings together Shibboleth and VOMS Attributes integrated in Proxy Certificates integriert also using SLCS

Further developments

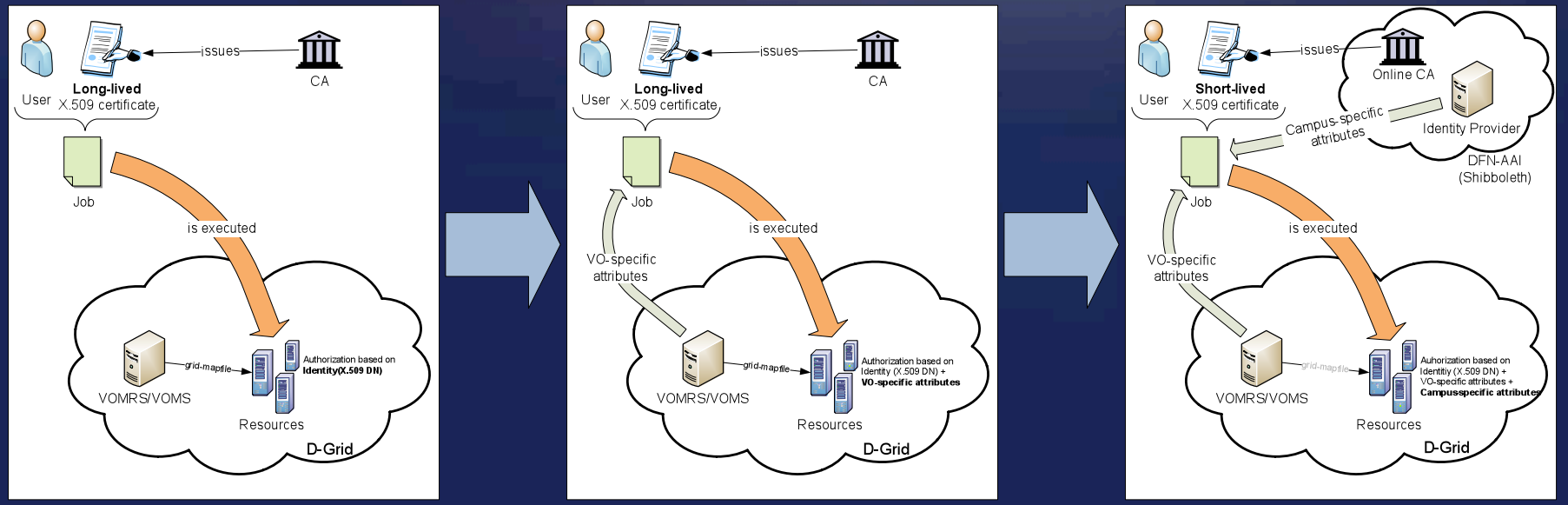
myVocs, PERMIS, MAMS (Details can be found in the IVOM reports IVOM)

Dynamics in VOs



Foster, Childers, 2005

Towards more dynamic VOs



Future directions (1)

- Dynamic VOs
  - Short Lived Credential Service
  - International Grid Trust Federation GridPMA
- Introducing SLAs in VOs: Guarantees
  - SLAs between the actors
    - User and VO
    - VO and Resource Provider
    - User and Resource Management Systems
- Current concepts resource usage oriented
  - Need to increase of granularity: resource, application, application feature, data bases, services

Future directions (2)

Considering VO membership/attributes for Grid Scheduling and service orchestration

Considering VO membership/attributes for commercial applications: license issues

Transition from user certificates to SAML assertions for user attributes (lean PKI for servers, scalability)

Conclusion

State of the art

- Basic technology like VOMS or Shibboleth is in place and used.
- Interoperability is advancing only slowly
- SLCS becoming an important cornerstone for interoperability
- Procedures for VO-Management becoming more generic

Trends

- Interoperability
- Increased flexibility

Outlook/Vision

- Highly dynamic, short lived VOs, easy to manage
- Transition from user certificates to SAML assertions for user attributes

Trust & Security, VOs in Clouds?

Further Resources

Several Reports of the VO-Management and IVOM projects can be found here:

http://www.d-grid.de/index.php?id=336&L=1

(all but the VO-Management Framework Concept for D-Grid in English)