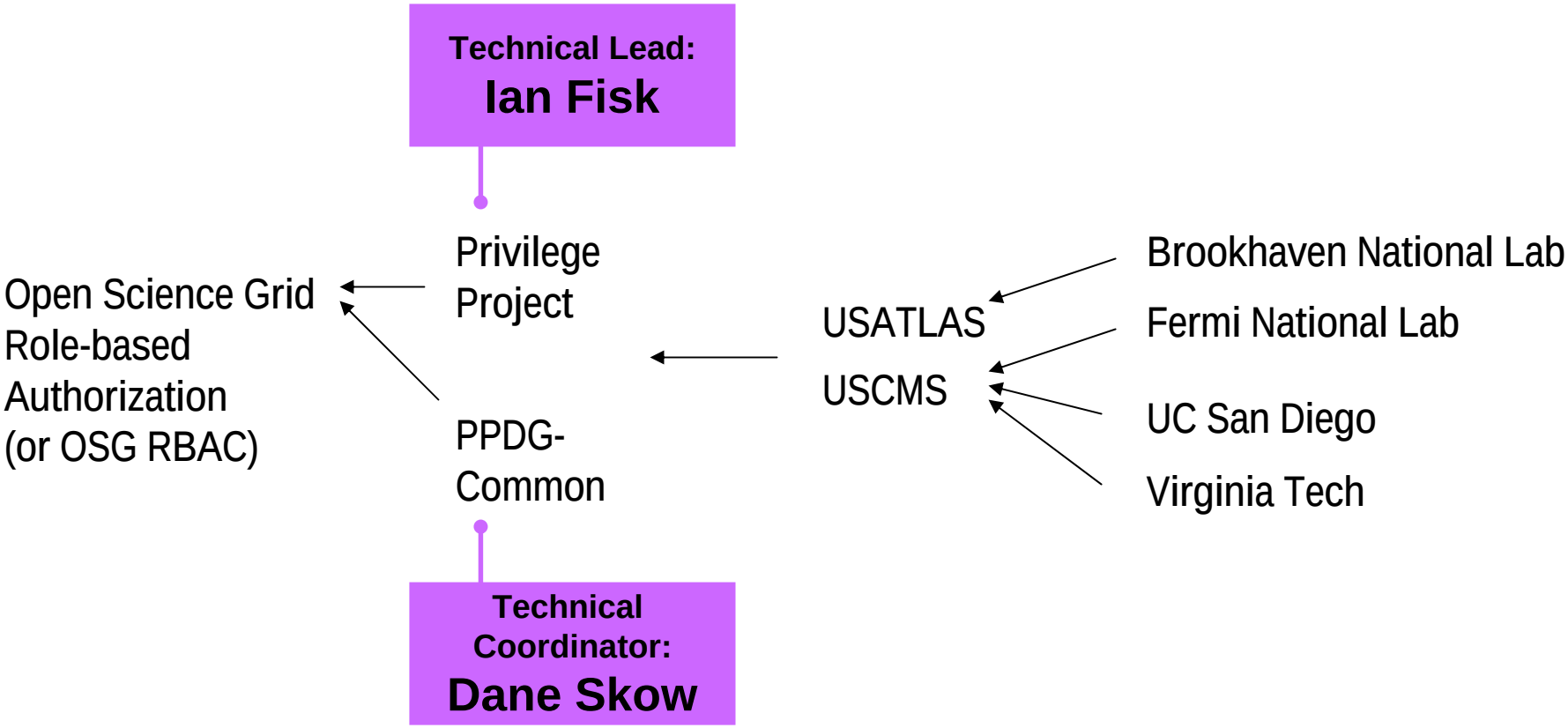
Open Science Grid
Role Based Access Control

Authorization Services, High-level Architecture and Usage in Spring/Summer 2005

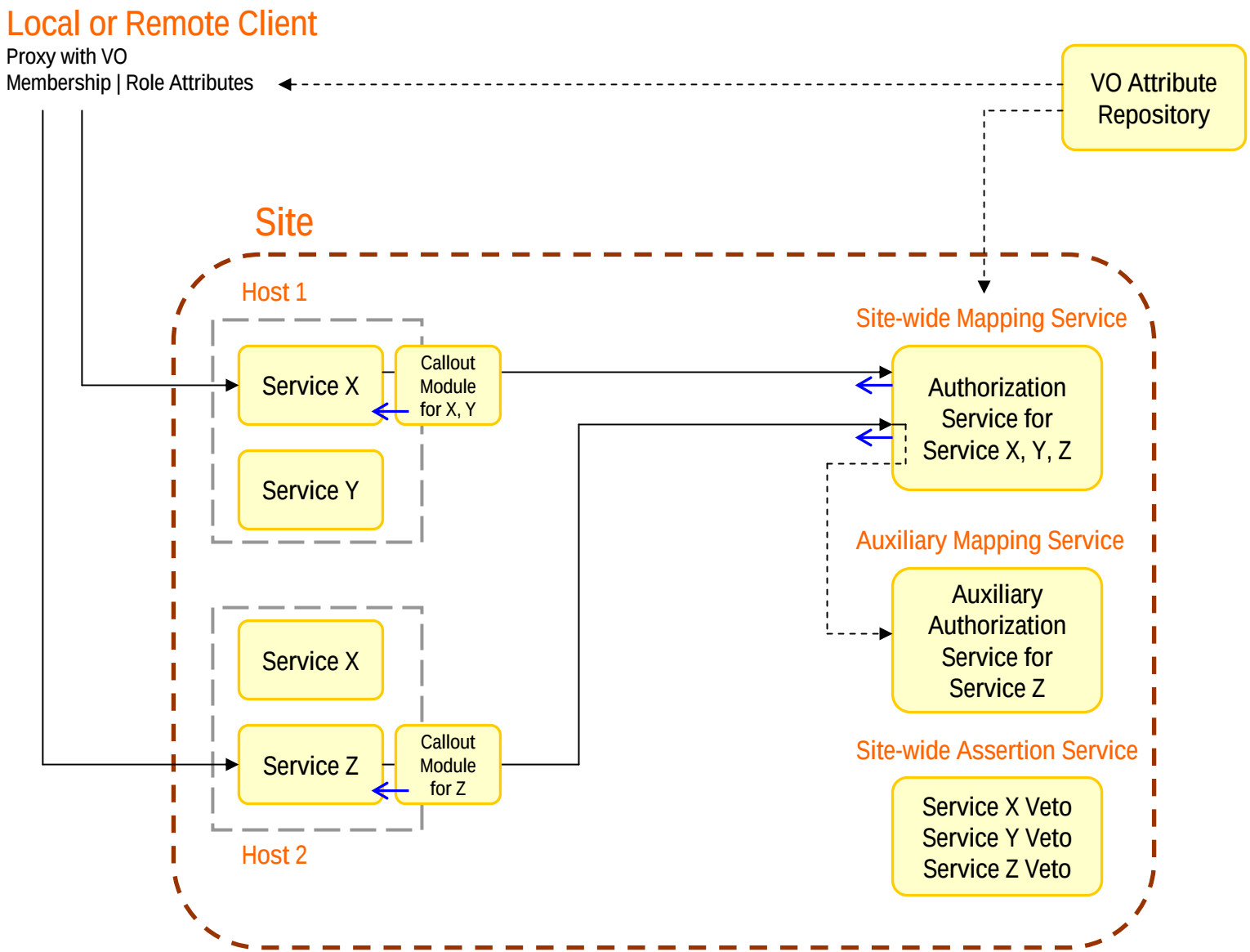
Abhishek Singh Rana
UC San Diego

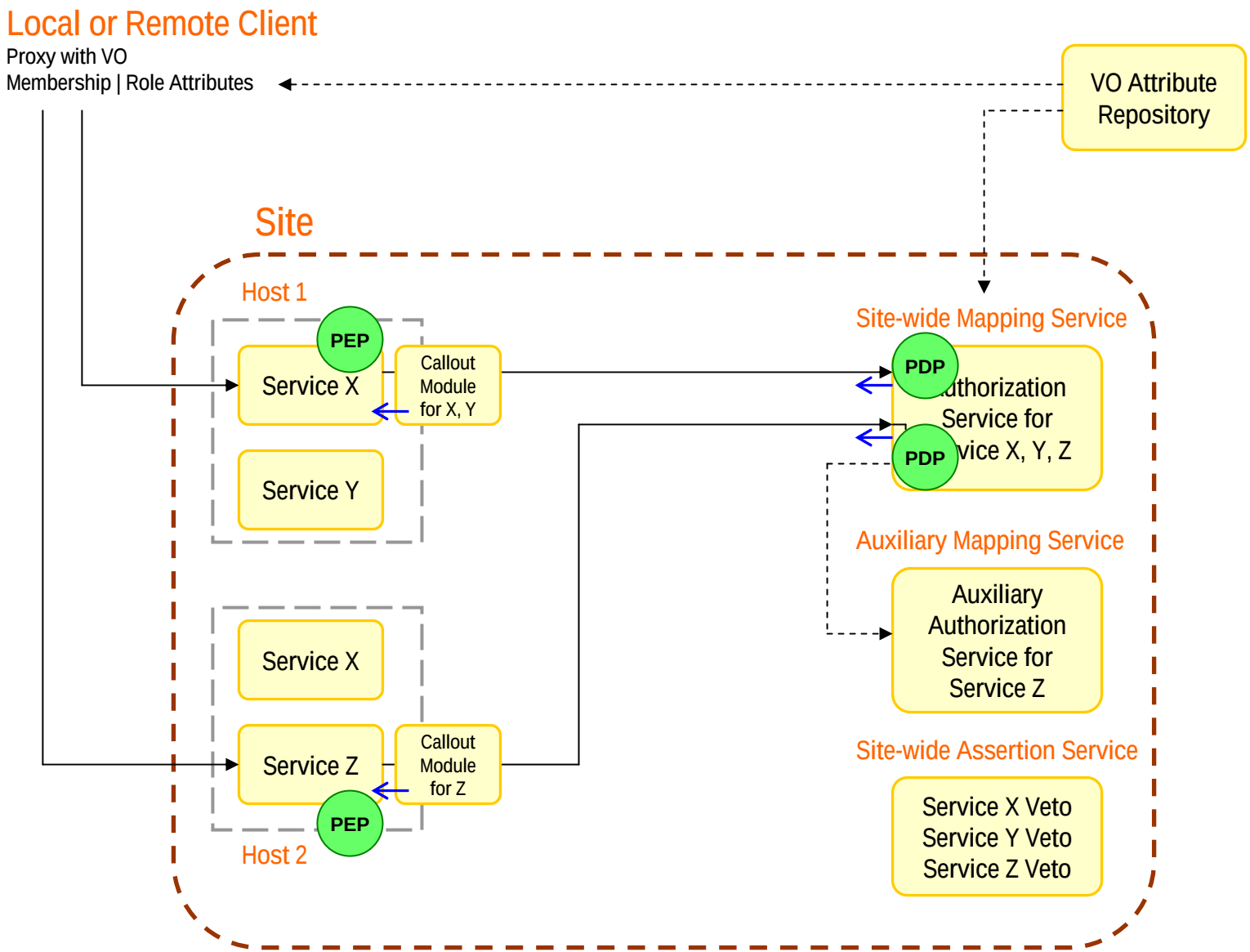
Collaborative Effort

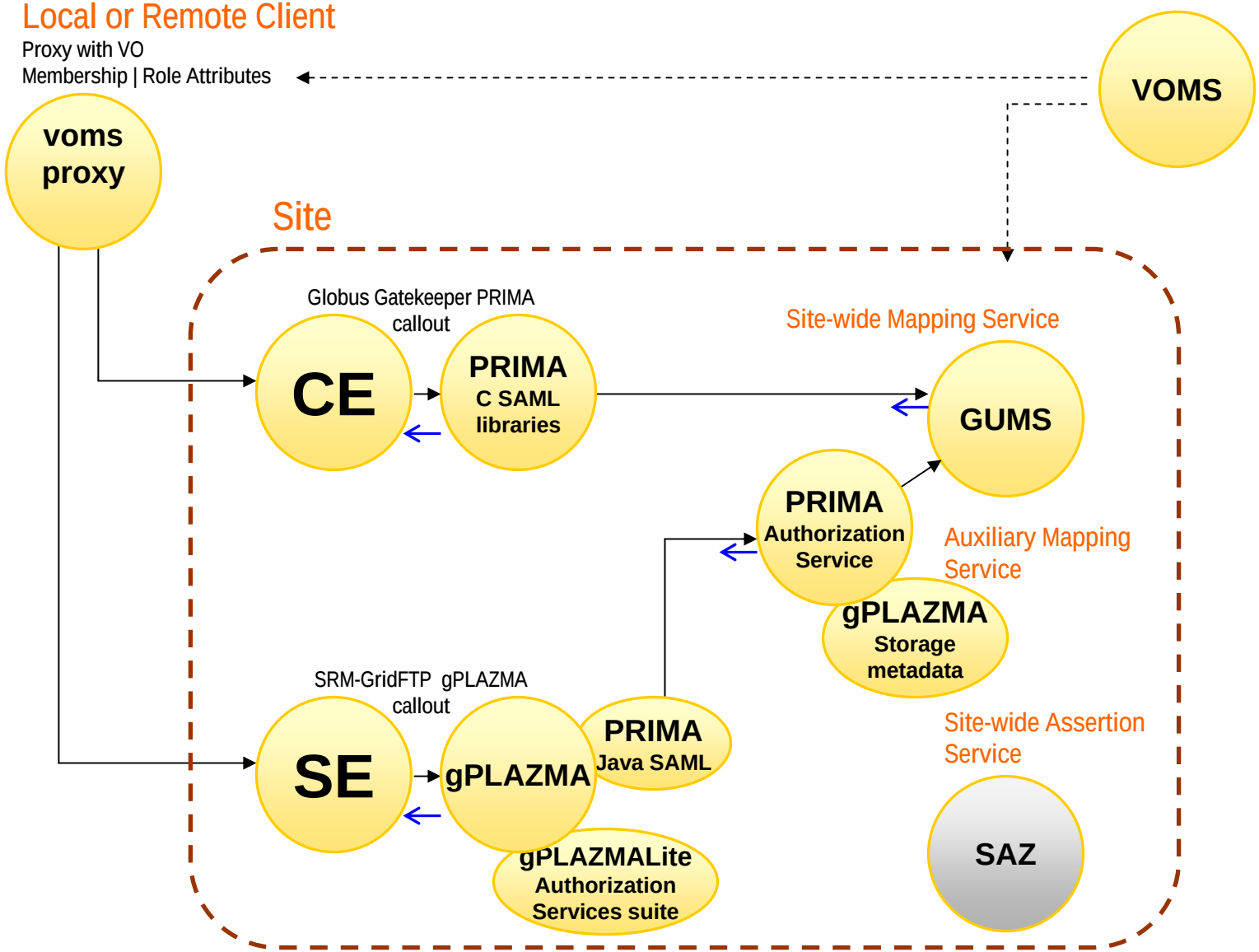


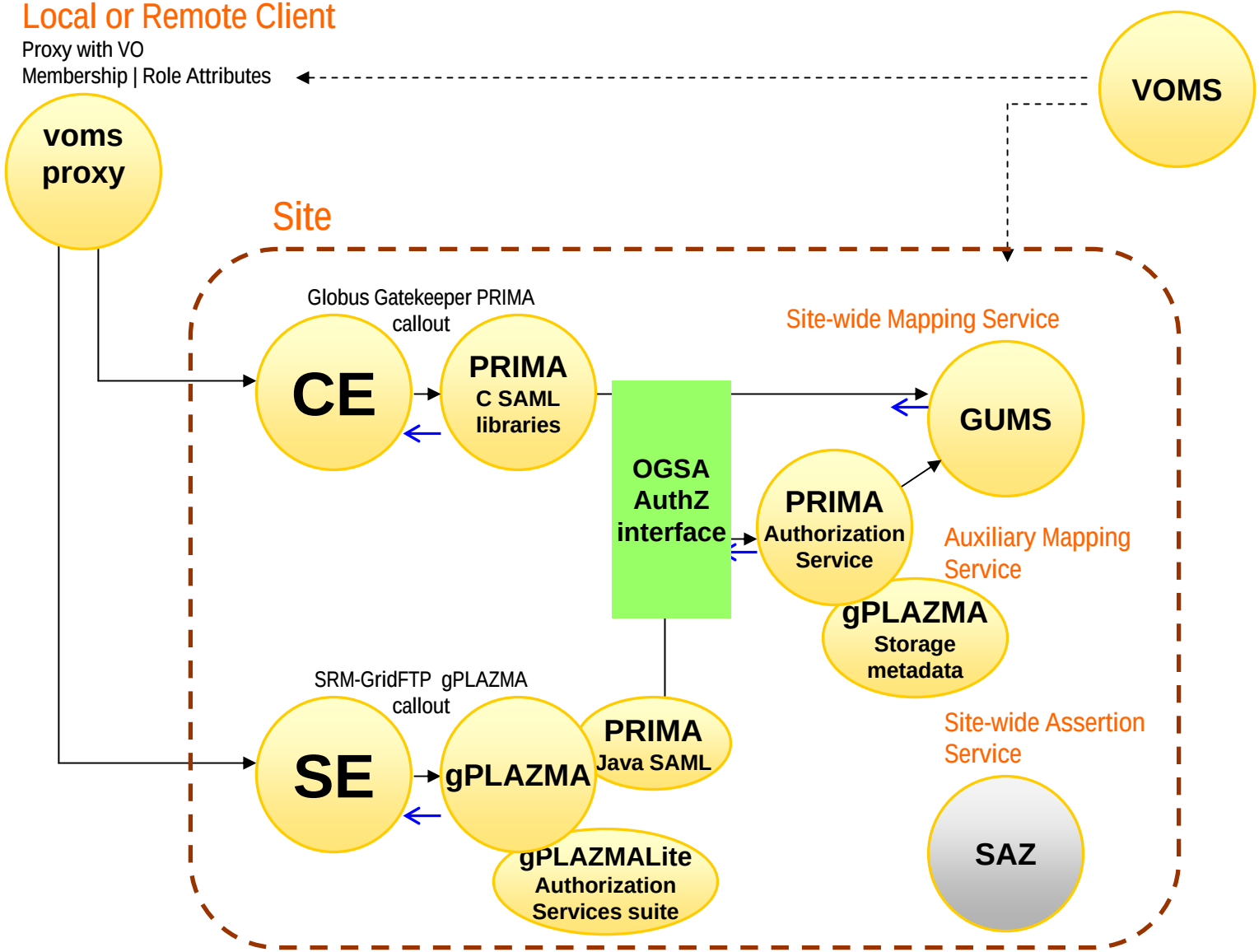
Goals of Open Science Grid RBAC

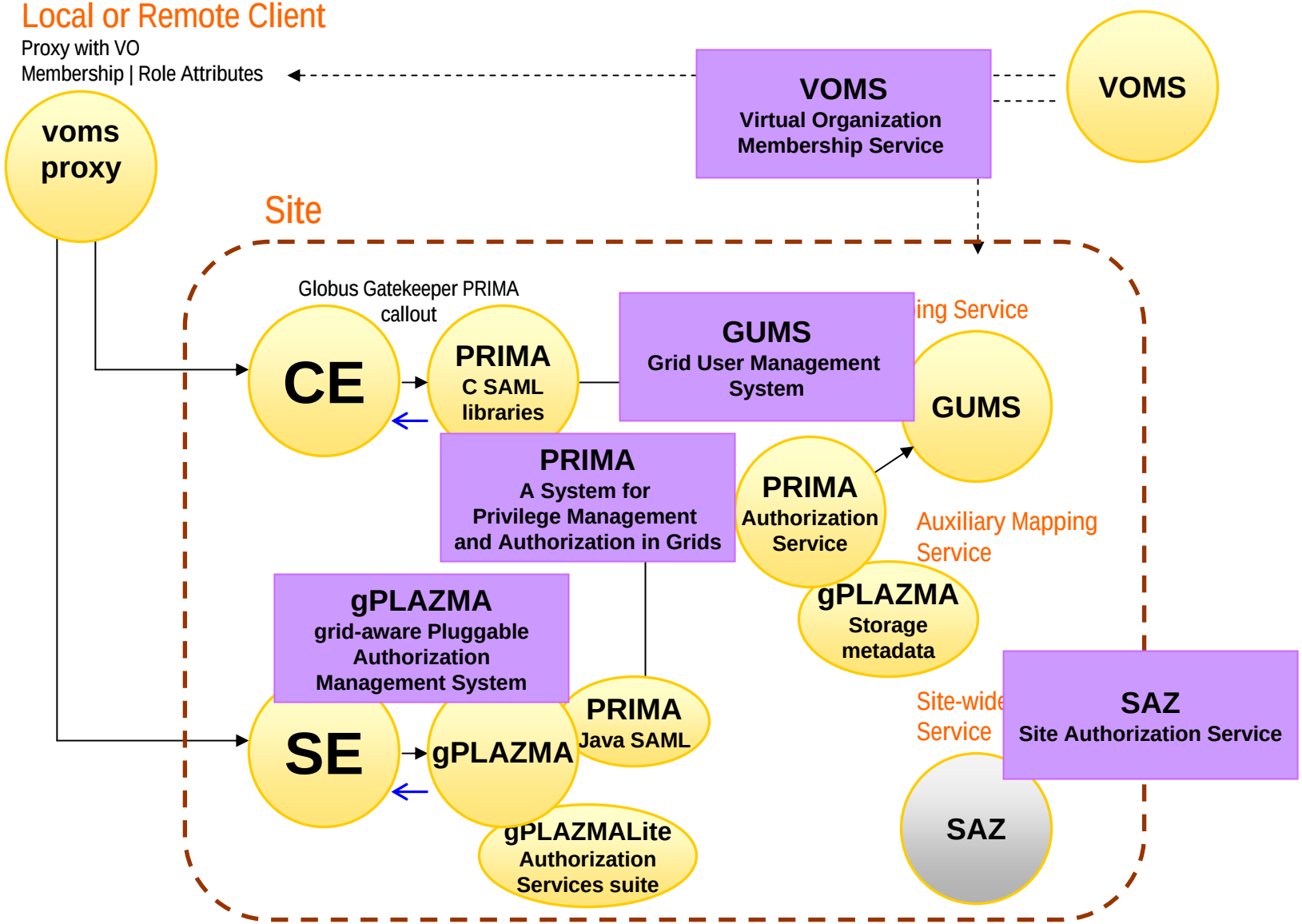
- Move from host-based to site-based authorization.
  - authorization = !(Site-vetoed) && (VO-allowed)
- Move from host-based to service-based granularity for authorization.
- Allow humans to have group membership and multiple roles.
  - Same DN can have plural group membership and multiple roles with privilege depending on role.
  - Multiple roles per DN means multiple privileges, at the same time.
- Create multi-user environment in which traditional UID based auditing is possible if desired.

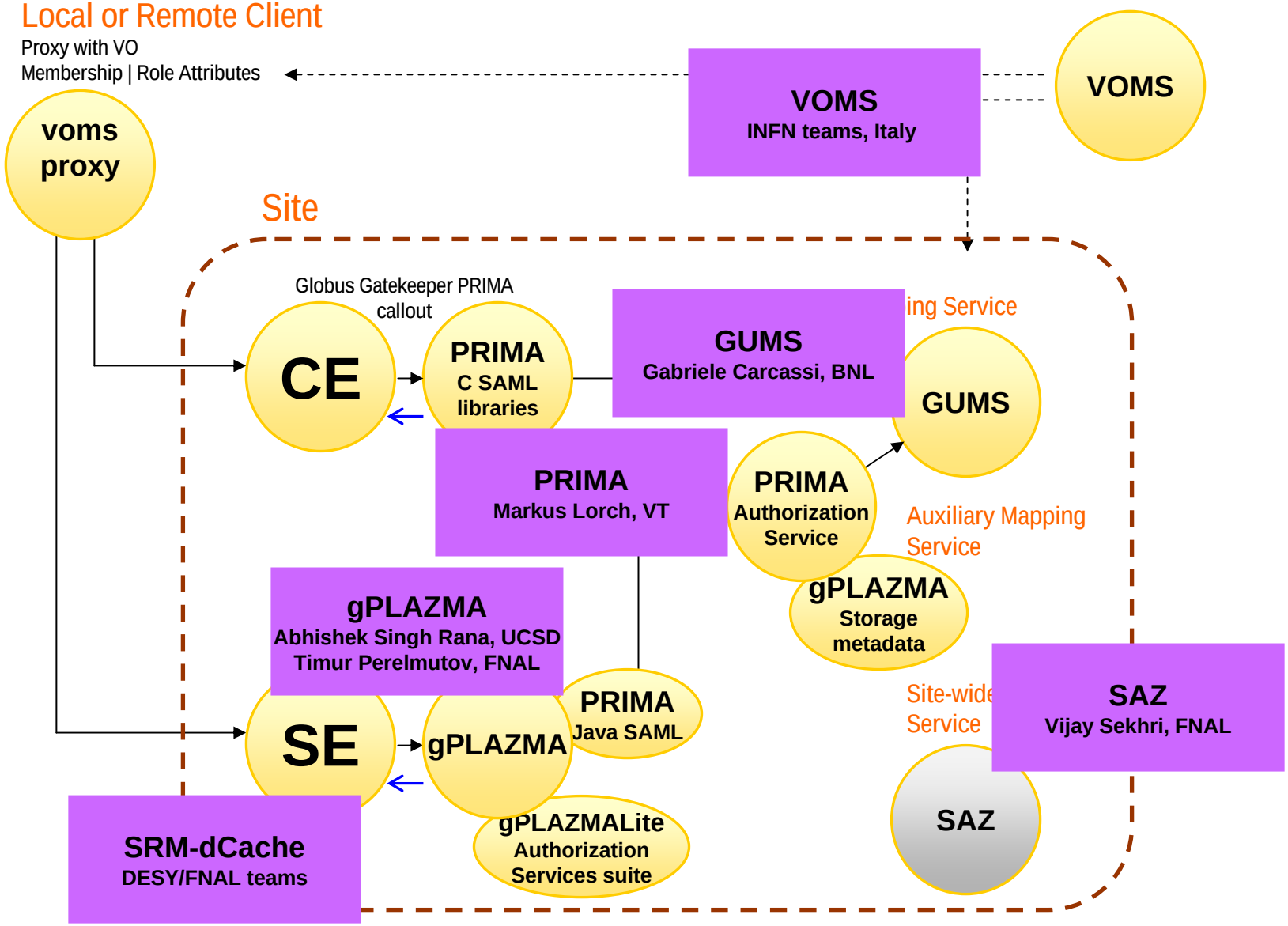

Local or Remote Client
Proxy with VO
Membership | Role Attributes
VO Attribute Repository
Site
Host 1
Service X
Callout Module for X, Y
Service Y
Site-wide Mapping Service
Authorization Service for Service X, Y, Z
Auxiliary Mapping Service
Auxiliary Authorization Service for Service Z
Service X
Service Z
Callout Module for Z
Site-wide Assertion Service
Service X Veto
Service Y Veto
Service Z Veto
Host 2


Local or Remote Client
Proxy with VO
Membership | Role Attributes
VO Attribute Repository
Site
Host 1
PEP
Service X
Callout Module for X, Y
Service Y
Site-wide Mapping Service
PDP
uthorization Service for vice X, Y, Z
PDP
Auxiliary Mapping Service
Auxiliary Authorization Service for Service Z
Service X
Service Z
Callout Module for Z
PEP
Host 2
Site-wide Assertion Service
Service X Veto
Service Y Veto
Service Z Veto


Local or Remote Client
Proxy with VO
Membership | Role Attributes
VOMS
voms proxy
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
Site-wide Mapping Service
GUMS
PRIMA
Authorization Service
Auxiliary Mapping Service
gPLAZMA
Storage metadata
SRM-GridFTP gPLAZMA callout
SE
gPLAZMA
PRIMA
Java SAML
Site-wide Assertion Service
SAZ
gPLAZMALite
Authorization
Services suite


Local or Remote Client
Proxy with VO
Membership | Role Attributes
VOMS
voms proxy
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
Site-wide Mapping Service
GUMS
OGSA AuthZ interface
PRIMA
Authorization Service
Auxiliary Mapping Service
gPLAZMA
Storage metadata
SRM-GridFTP gPLAZMA callout
SE
gPLAZMA
PRIMA
Java SAML
Site-wide Assertion Service
SAZ
gPLAZMALite
Authorization
Services suite


Local or Remote Client
Proxy with VO
Membership | Role Attributes
voms proxy
VOMS
Virtual Organization
Membership Service
VOMS
Site
Globus Gatekeeper PRIMA
callout
CE
PRIMA
C SAML
libraries
GUMS
Grid User Management
System
ing Service
GUMS
PRIMA
A System for
Privilege Management
and Authorization in Grids
PRIMA
Authorization
Service
Auxiliary Mapping
Service
gPLAZMA
Storage
metadata
gPLAZMA
grid-aware Pluggable
Authorization
Management System
SE
gPLAZMA
PRIMA
Java SAML
Site-wide
Service
SAZ
Site Authorization Service
SAZ
gPLAZMALite
Authorization
Services suite

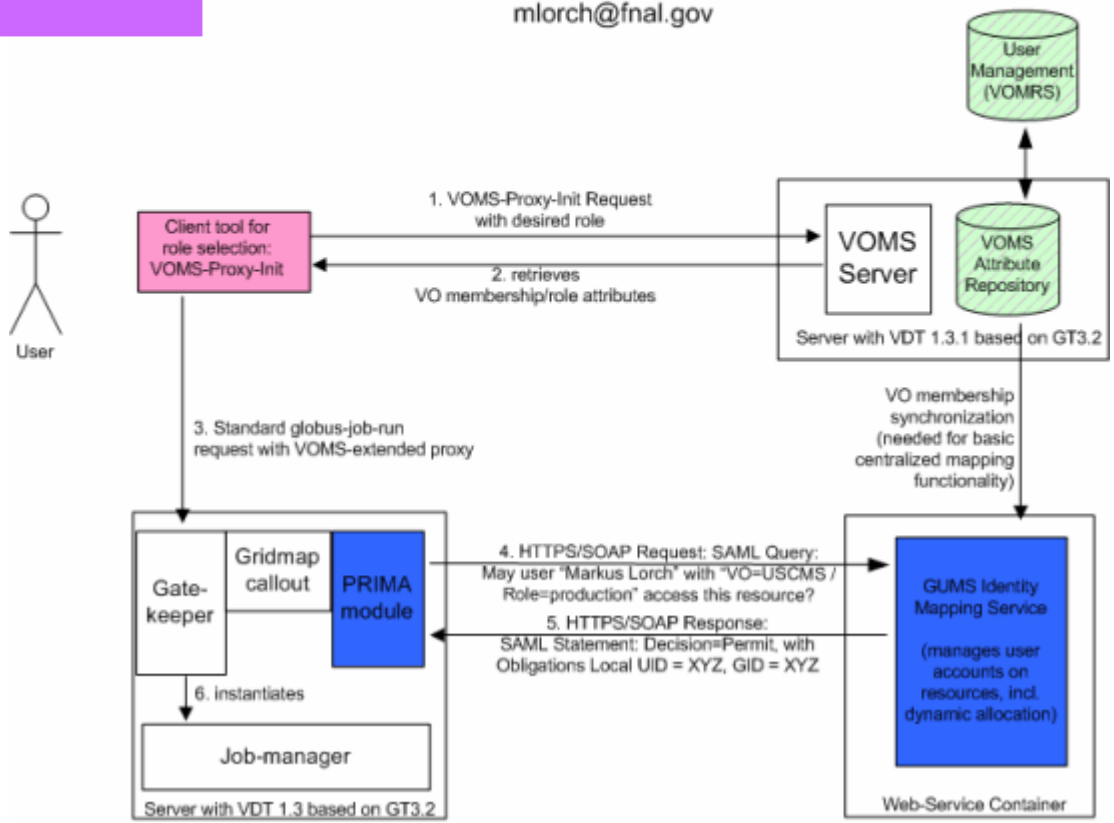

Local or Remote Client
Proxy with VO
Membership | Role Attributes
voms proxy
VOMS
INFN teams, Italy
VOMS
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
GUMS
Gabriele Carcassi, BNL
ing Service
GUMS
PRIMA
Markus Lorch, VT
PRIMA
Authorization Service
Auxiliary Mapping Service
gPLAZMA
Storage metadata
gPLAZMA
Abhishek Singh Rana, UCSD
Timur Perelmutov, FNAL
SE
gPLAZMA
PRIMA
Java SAML
Site-wide Service
SAZ
Vijay Sekhri, FNAL
SAZ
gPLAZMALite
Authorization Services suite
SRM-dCache
DESY/FNAL teams

Slide by:
Markus Lorch, VT

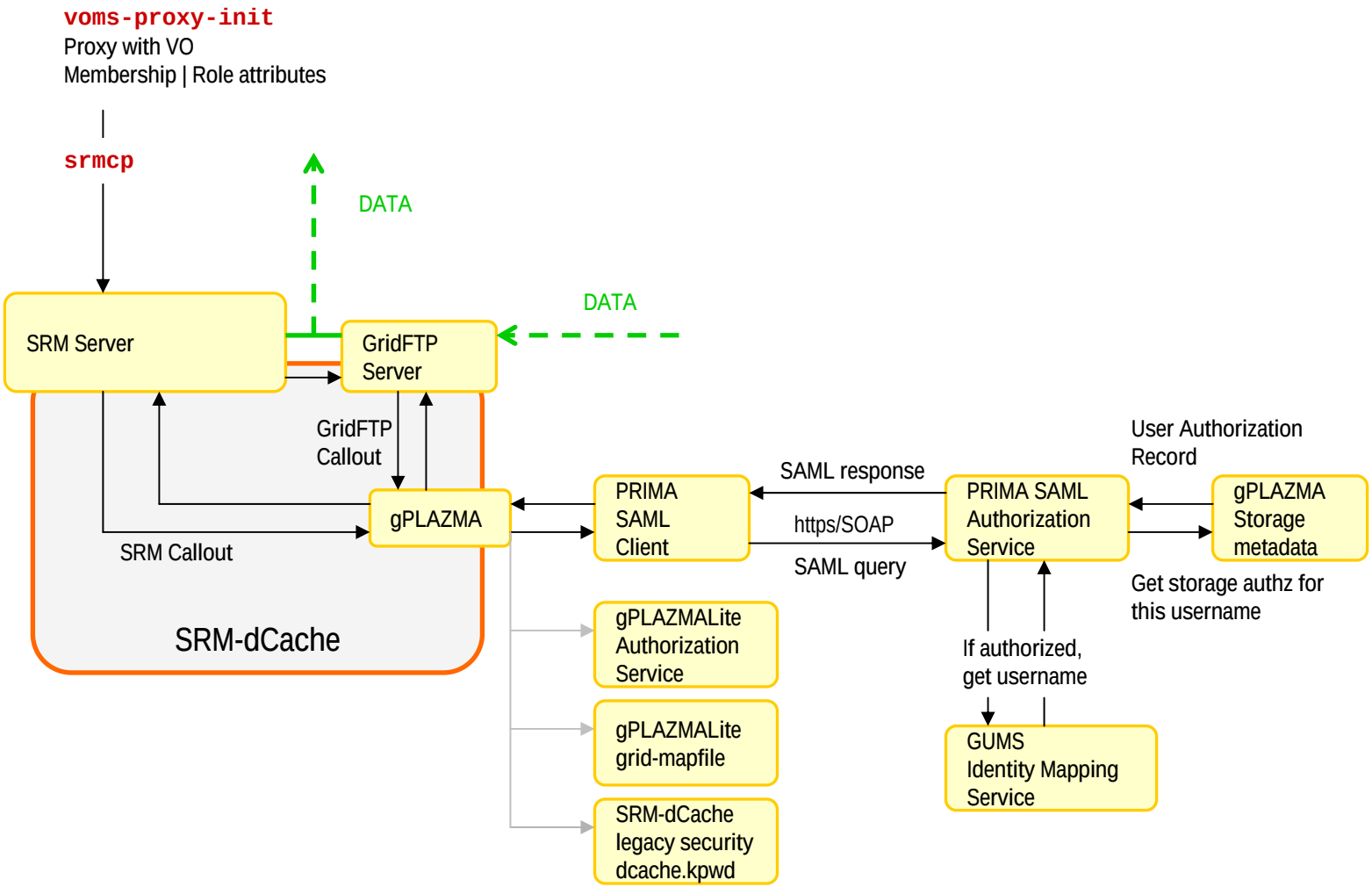
Authorization Architecture
Compute Node Functionality for OSG-0

FNAL Privilege Project

Version 4 - 2005-01-09
mlorch@fnal.gov



Authorization Architecture
Storage Element (SRM-dCache) functionality
(currently in alpha testing phase)



OSG RBAC Usage: An Early-phase Example (USCMS Tier-2 Center at UC San Diego)

- FQANs for members of CMS
  - /cms/uscms/Role=cmst2admin
    - Tier 2 administrators with superuser privileges
  - /cms/uscms/Role=cmsprod
    - Select users with production-level privileges
  - /cms/uscms/Role=cmsuser
    - All users with general privileges
  - /cms/uscms/Role=cmssoft
    - Dynamic installation of software by services
  - /cms/uscms/Role=cmsphedex
    - Data transfer using PhEDEx and SRM-dCache
  - /cms/uscms/Role=cmsfrontier
    - Dynamic deployment of squid DB caching service
- GUMS mapping logic (permutations for CMS)
  - ignoreFQAN=true, AccountPoolMapper
  - ignoreFQAN=true, GroupAccountMapper
  - ignoreFQAN=false, AccountPoolMapper
  - ignoreFQAN=false, GroupAccountMapper

OSG RBAC Usage: An Early-phase Example (USCMS Tier-2 Center at UC San Diego)

- FQANs for members of other VOs on OSG
  - /atlas
    - Members of (US)ATLAS
  - /cdf
    - Members of CDF
  - /vos/services
    - Members of iVDGL
  - /vos/osg
    - Members of OSG VO
  - /vos/fmri
  - /GRASE/grid
- GUMS mapping logic (permutations for other VOs on OSG)
  - ignoreFQAN=true, GroupAccountMapper
  - ignoreFQAN=false, GroupAccountMapper

OSG RBAC Usage: An Early-phase Example (USCMS Tier-2 Center at UC San Diego)

Frank

Robert

/cms/uscms/Role=cmst2admin → POSIX User = root

/cms/uscms/Role=cmsuser → POSIX User = uscms001 ... ... uscms999

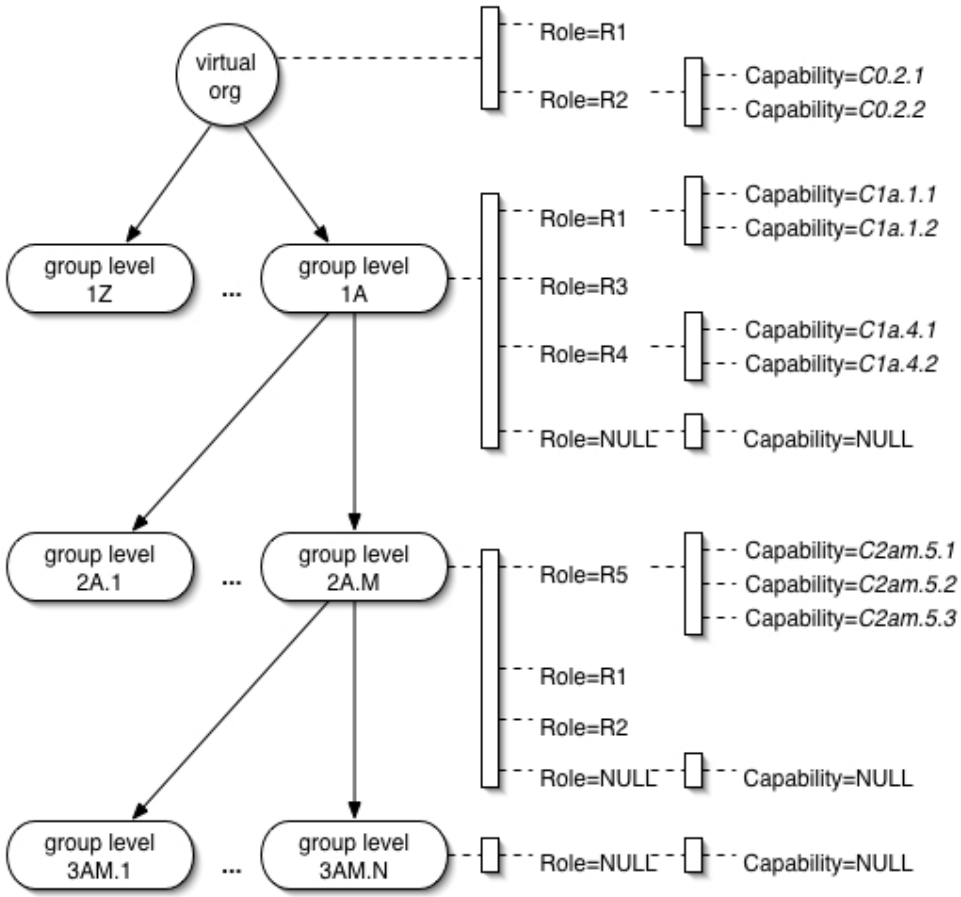
/cms/uscms/Role=cmsphedex → POSIX User = phedex

/cdf → POSIX User = cdf

/vos/osg → POSIX User = osguser

/atlas → POSIX User = usatlas1

OSG RBAC Usage: FQANs
Fully Qualified Attribute Names



FQANs descriptive of Group Membership with Roles and Capabilities in a Virtual Organization

OSG RBAC Usage: Responsibilities Matrix

- A VO's **Management Personnel** declare the FQANs relevant to this VO's virtual structure.
- **Members of a VO** request registration with a clearance to use FQANs that apply to them. **VO Administrators** maintain this information in registration databases.
- **Site Administrators** perform necessary tasks required to make use of RBAC. These tasks entail creation of POSIX accounts (UIDs, GIDs) and related triage for both compute and storage resources, deployment of GUMS for each such *account-domain*, populating GUMS from registration databases, maintenance of VOMS servers contact information, etc.
- **An OSG User (member of one or more VOs)** specifies an FQAN and a VOMS server (or list thereof, if duplicate servers are available) to contact, while requesting an X.509 proxy.

Status of Authorization/Mapping Services

- PRIMA: Already deployed and used on OSG ITB (Spring'05)
- GUMS: Already deployed and used on OSG ITB (Spring'05)
- gPLAZMA: Planned for Summer'05 deployment on Tier1 and Tier2 sites (tied to SRM-dCache, may not get deployed on all OSG sites).
- Storage Authorization Service (PRIMA-GUMS-gPLAZMA): Planned for Summer'05 deployment on Tier1 and Tier2 sites (tied to SRM-dCache, may not get deployed on all OSG sites).