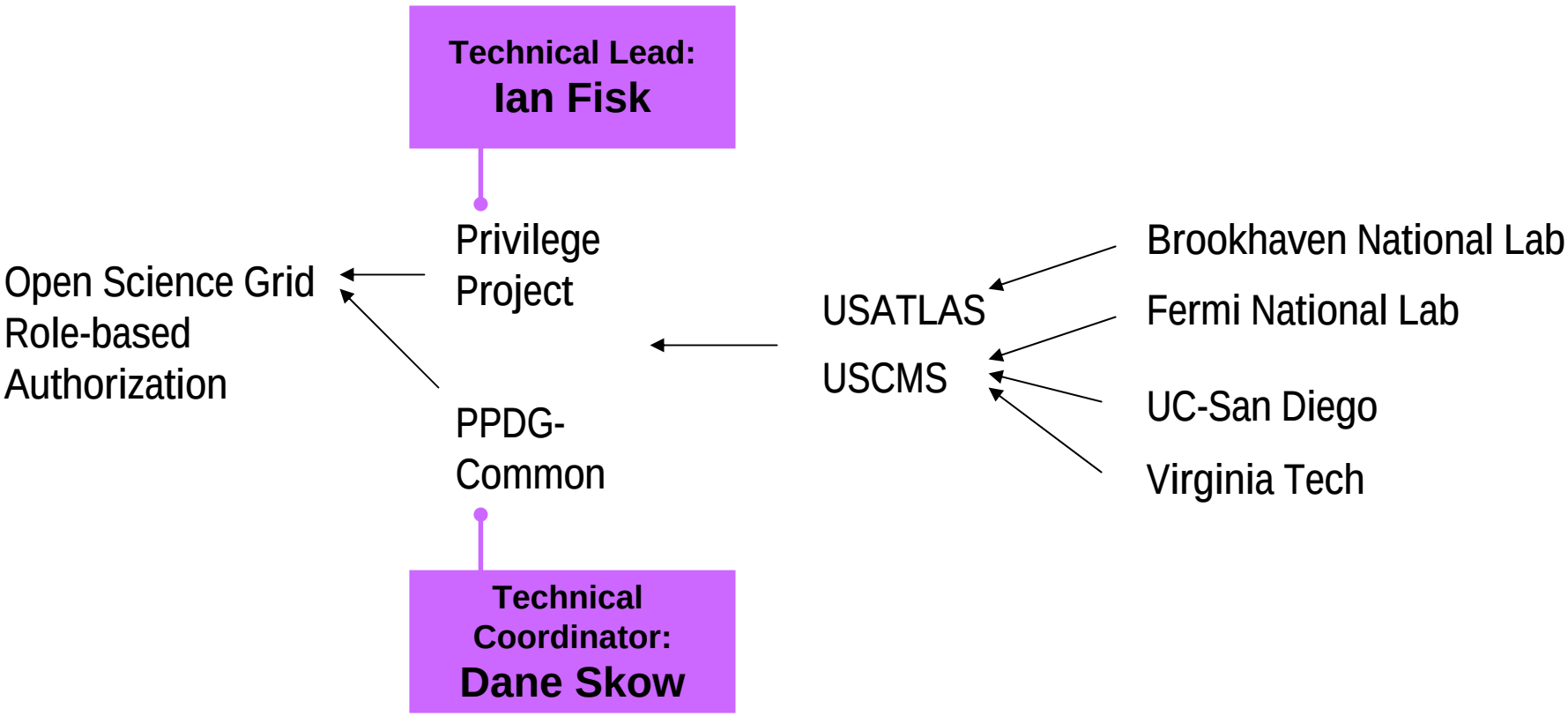
Open Science Grid Role-based Authorization Architecture

Abhishek Singh Rana, Frank Wuerthwein
(presenting the work of many)

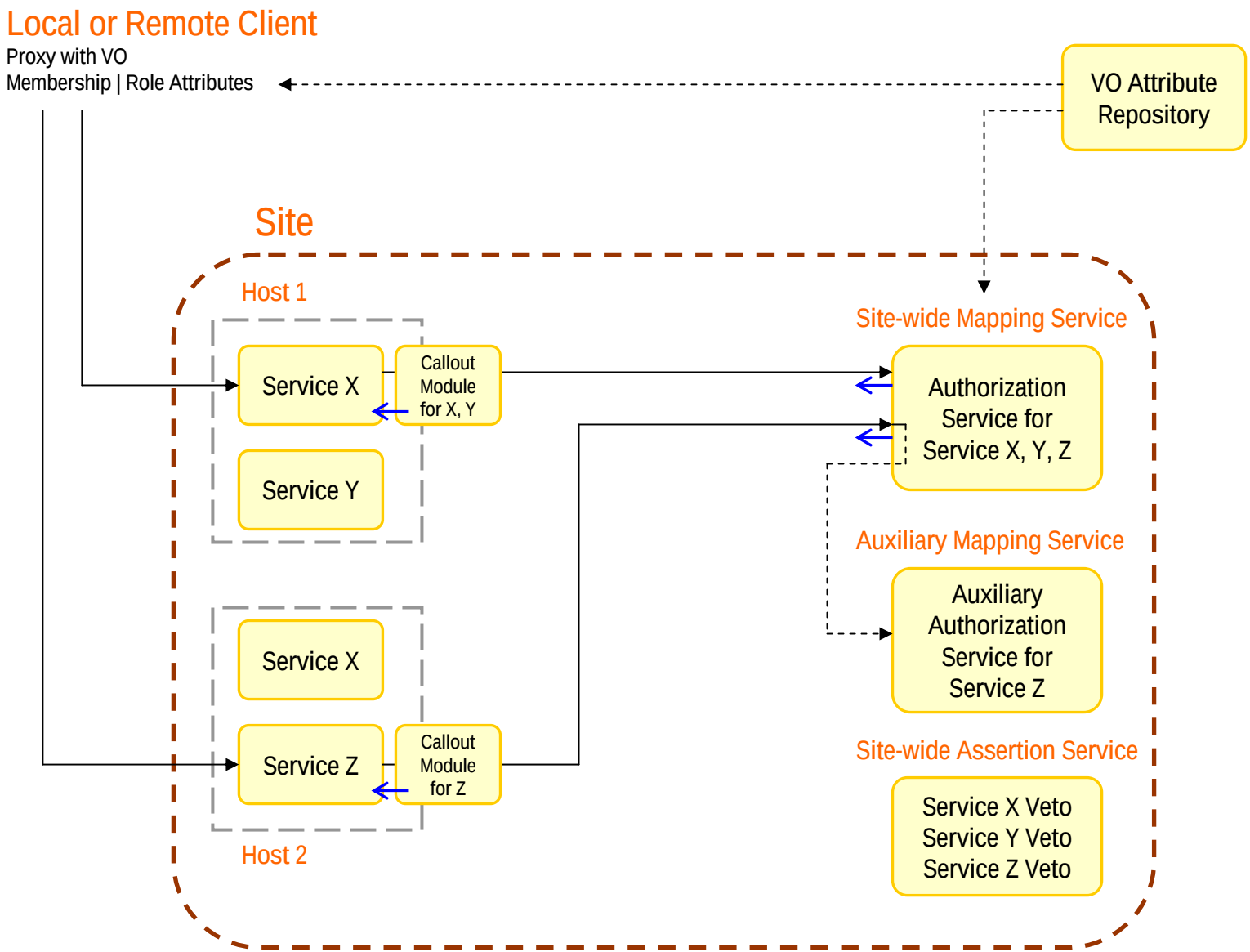
Collaborative Effort

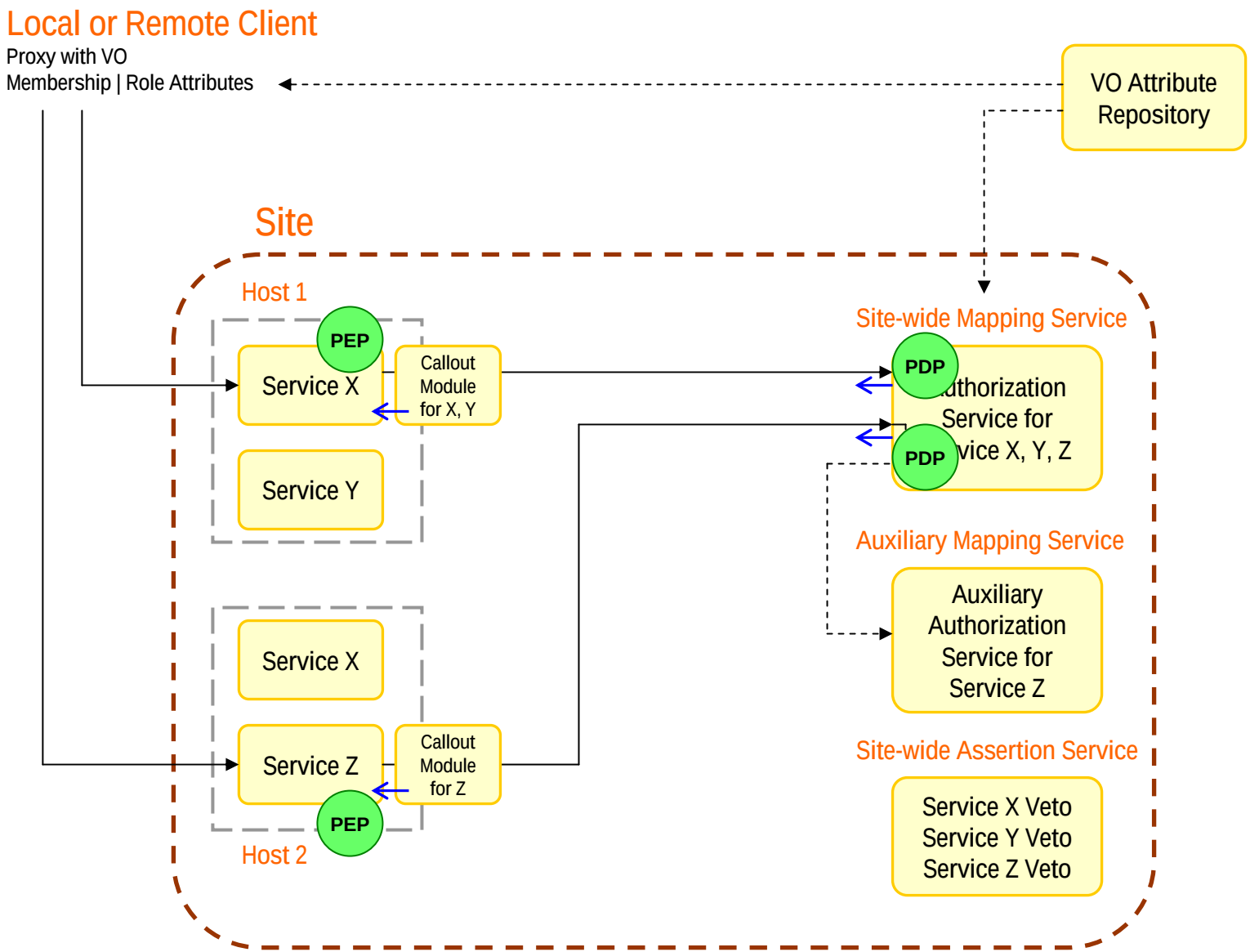


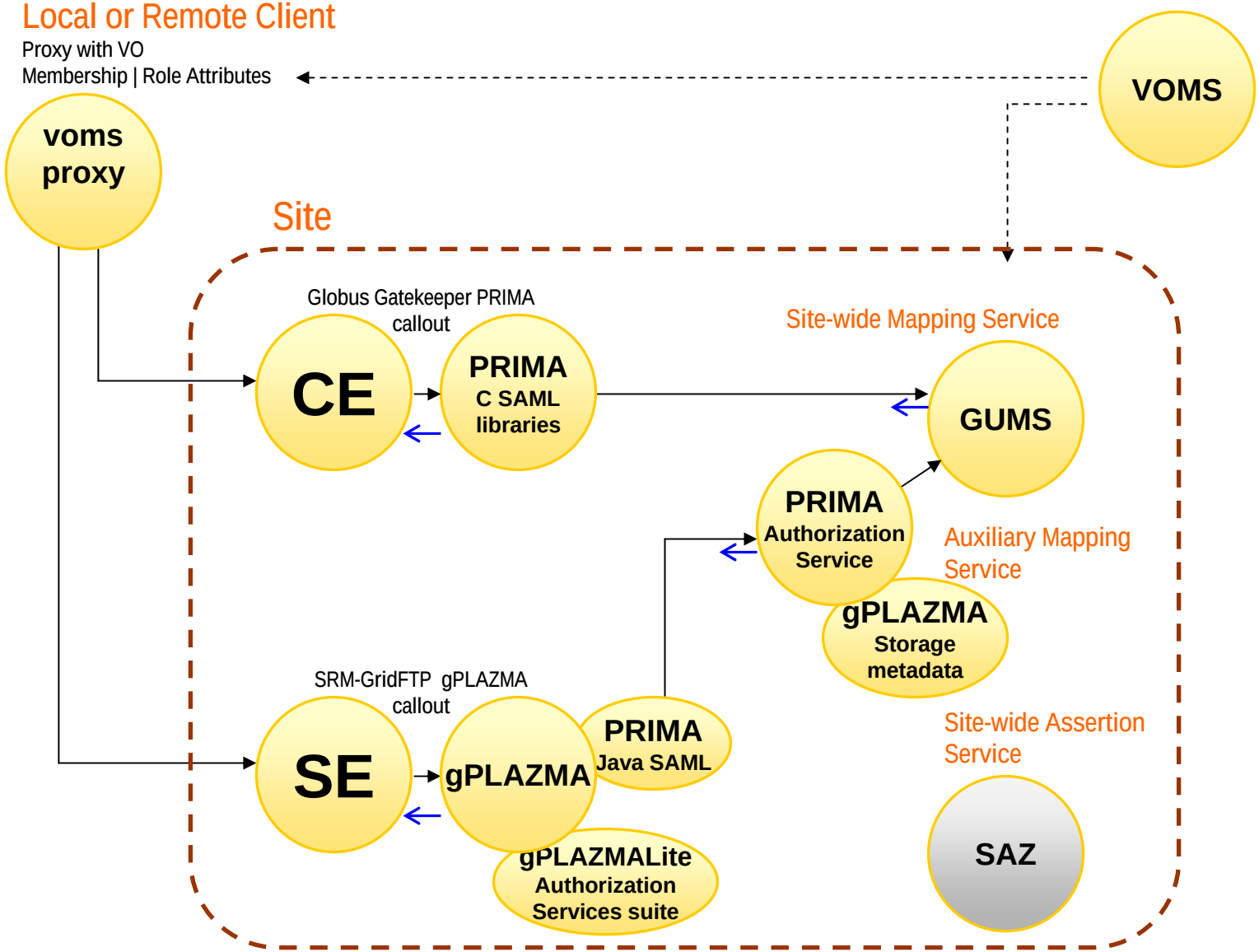
Open Science Grid
Role-based Authorization Architecture

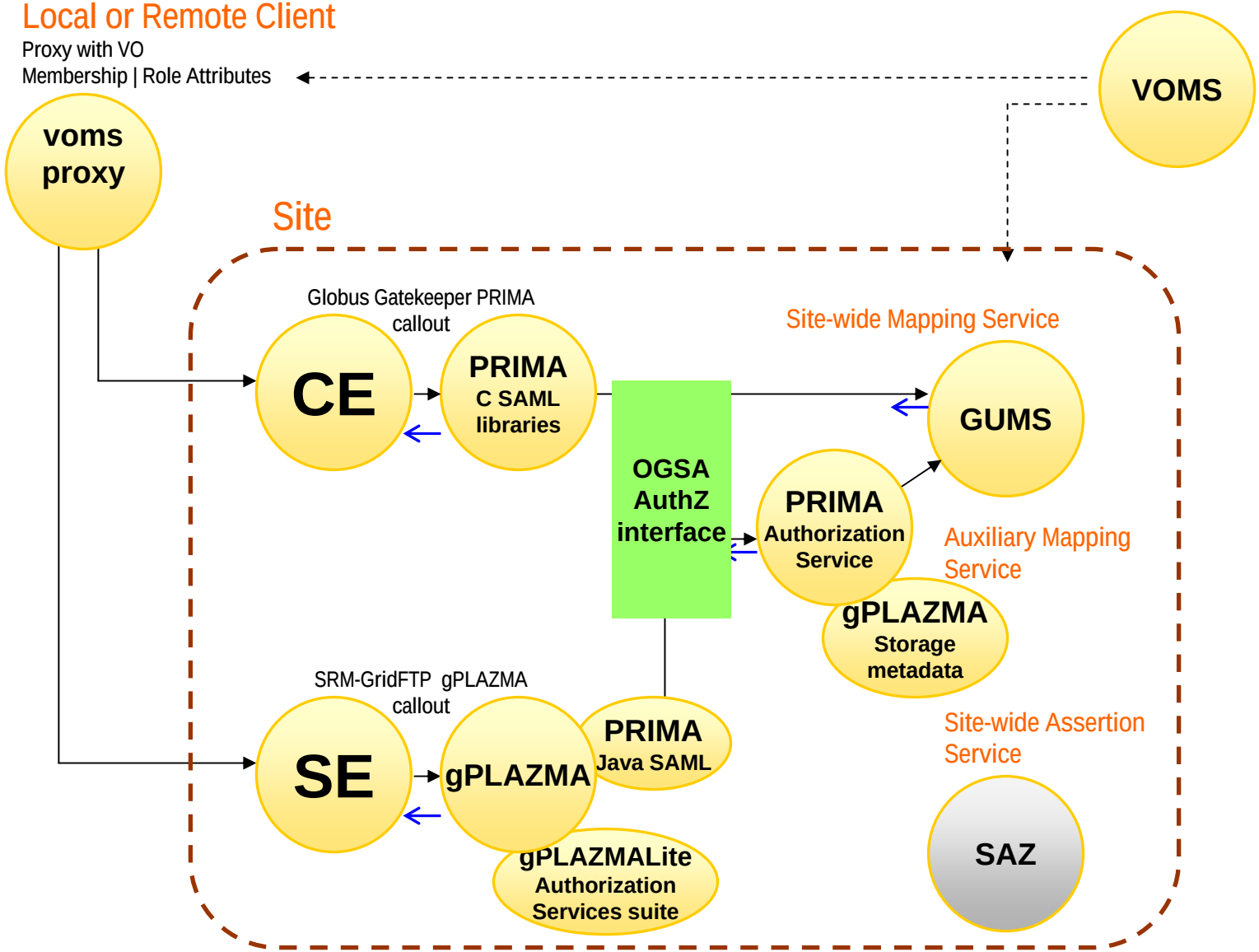
Goals:

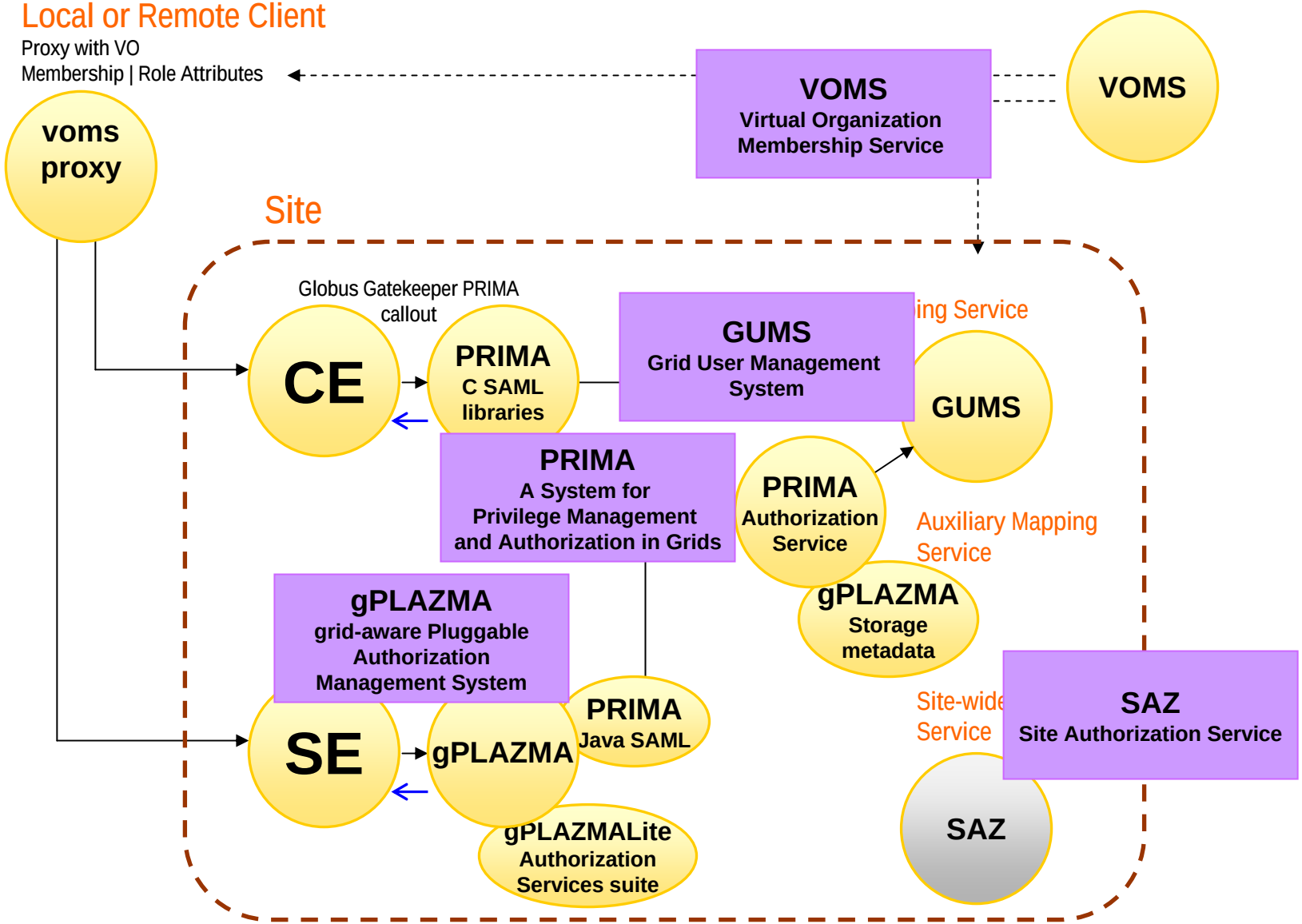
- Move from host-based to site-based authorization.
  - authorization = !(Site-vetoed) && (VO-allowed)
- Move from host-based to service-based granularity for authorization.
- Allow humans to have multiple roles.
  - Same DN can have multiple roles with privilege depending on role.
  - Multiple roles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

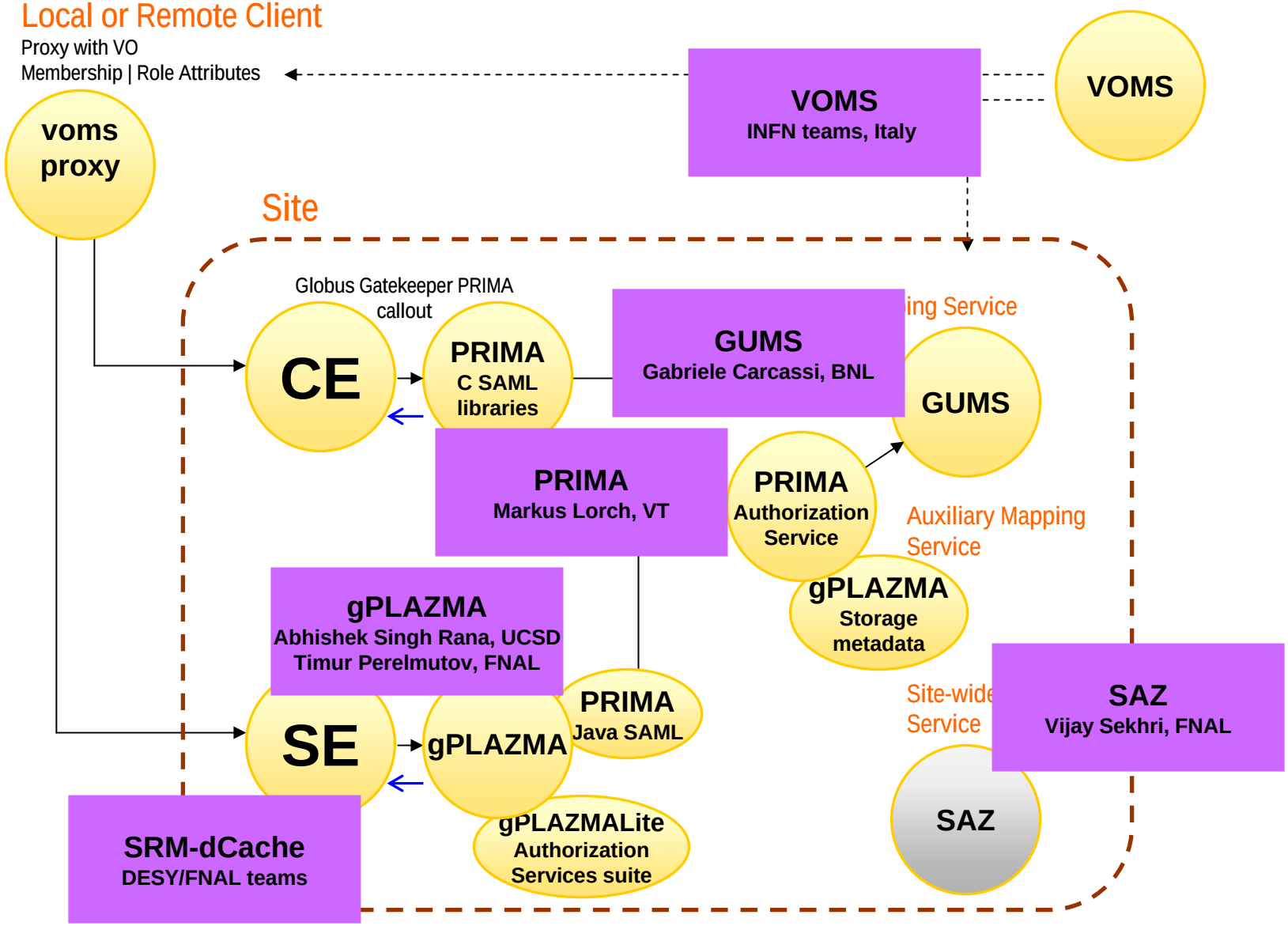

Local or Remote Client
Proxy with VO
Membership | Role Attributes
VO Attribute Repository
Site
Host 1
Service X
Callout Module for X, Y
Service Y
Site-wide Mapping Service
Authorization Service for Service X, Y, Z
Auxiliary Mapping Service
Auxiliary Authorization Service for Service Z
Service X
Service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

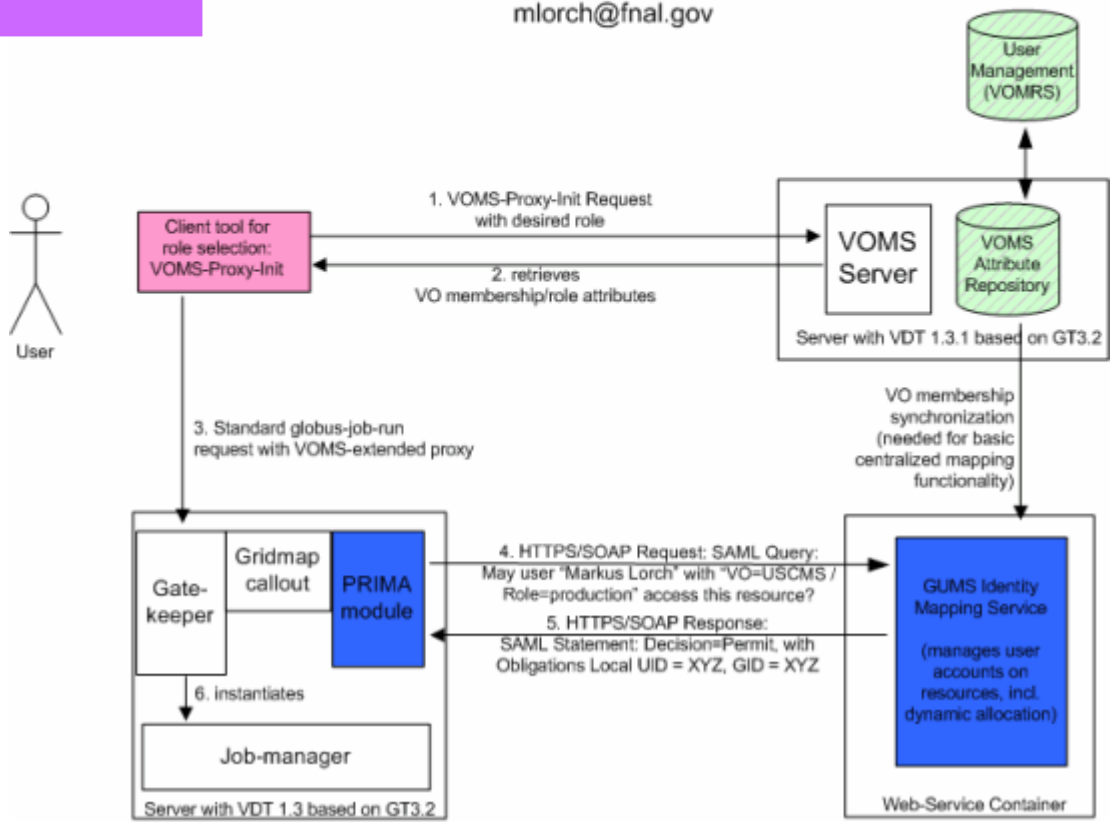

Local or Remote Client
Proxy with VO
Membership | Role Attributes
voms proxy
VOMS
INFN teams, Italy
VOMS
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
GUMS
Gabriele Carcassi, BNL
ing Service
GUMS
PRIMA
Markus Lorch, VT
PRIMA
Authorization Service
Auxiliary Mapping Service
gPLAZMA
Storage 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

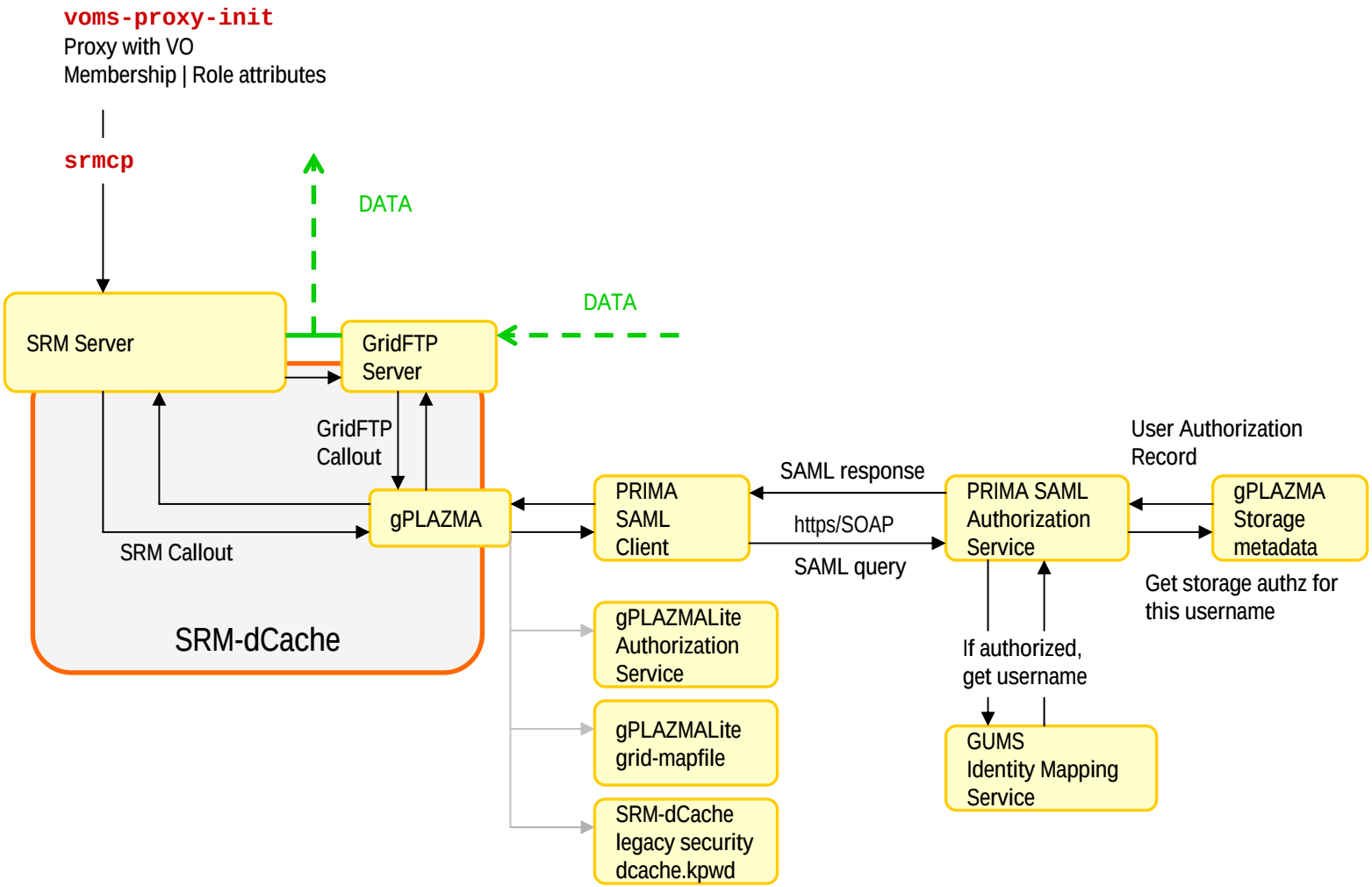
Authorization Architecture
Compute Node Functionality for OSG-0

FNAL Privilege Project

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



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



Status

- PRIMA: Already deployed+used on OSG ITB (Spring'05)
- GUMS: Already deployed+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).