gPLAZMA: grid-aware Pluggable AuthoriZation Management

(Introducing Role-based Access Control in dCache)

The XVth International Conference on
Computing in High Energy and Nuclear Physics (CHEP'06)
February 15, 2006
TIFR, Mumbai

Abhishek Singh Rana
UC San Diego
rana@fnal.gov

Frank Würthwein
UC San Diego
fkw@fnal.gov

Authors

RANA, Abhishek Singh (University of California, San Diego, CA, USA)
WÜRTHWEIN, Frank (University of California, San Diego, CA, USA)
PERELMUTOV, Timur (Fermi National Accelerator Laboratory, Batavia, IL,USA)
KENNEDY, Robert (Fermi National Accelerator Laboratory, Batavia, IL, USA)
BAKKEN, Jon (Fermi National Accelerator Laboratory, Batavia, IL, USA)
SKOW, Dane (Fermi National Accelerator Laboratory, Batavia, IL, USA)
FISK, Ian (Fermi National Accelerator Laboratory, Batavia, IL, USA)
FUHRMANN, Patrick (DESY, Hamburg, Germany)
ERNST, Michael (DESY, Hamburg, Germany)

Outline

- OSG AuthZ approach
- gPlazma architecture
- gPlazma implementation
- Example of end-to-end AuthZ for CEs and SEs
- Status
- Future Work

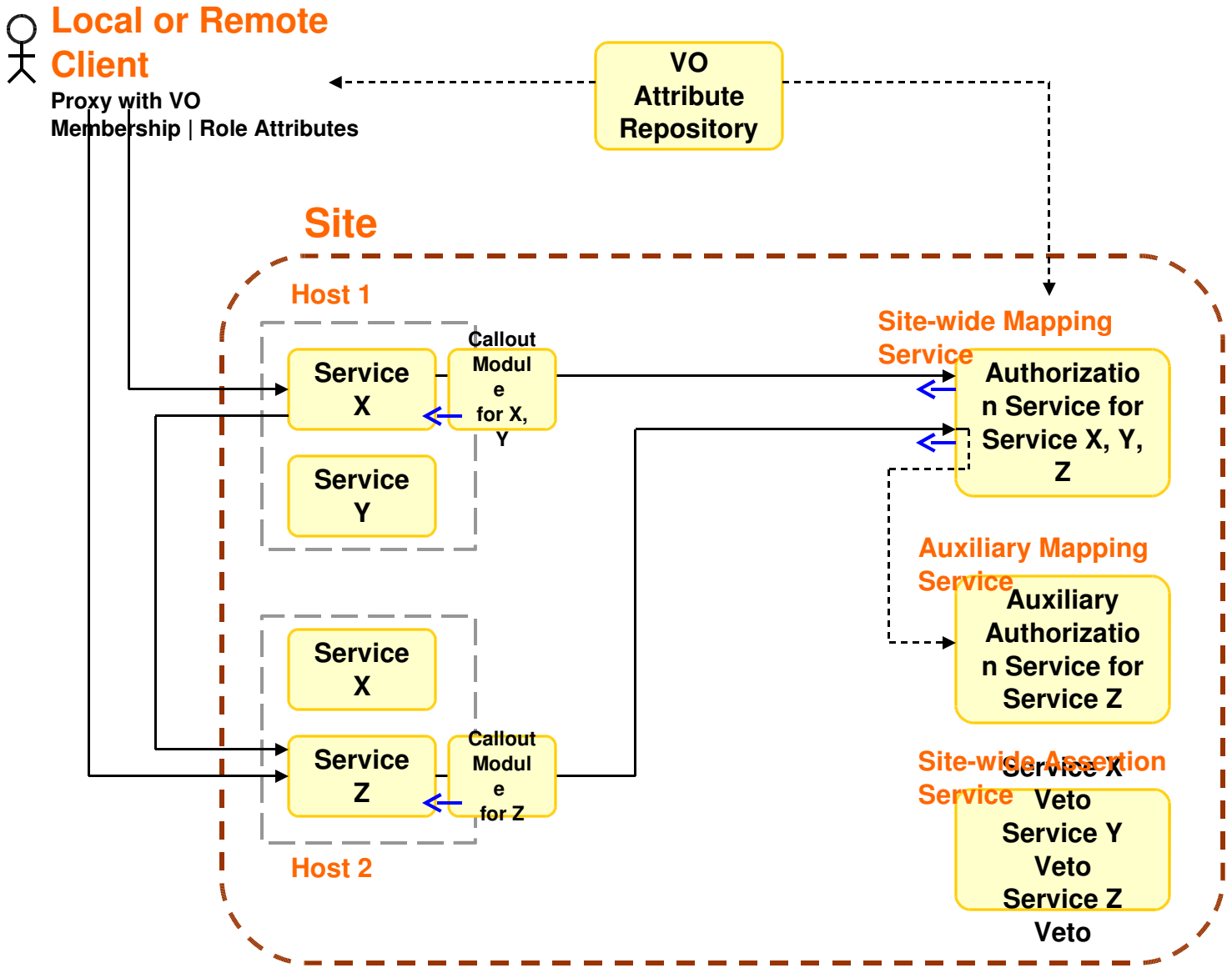
OSG AuthZ Approach

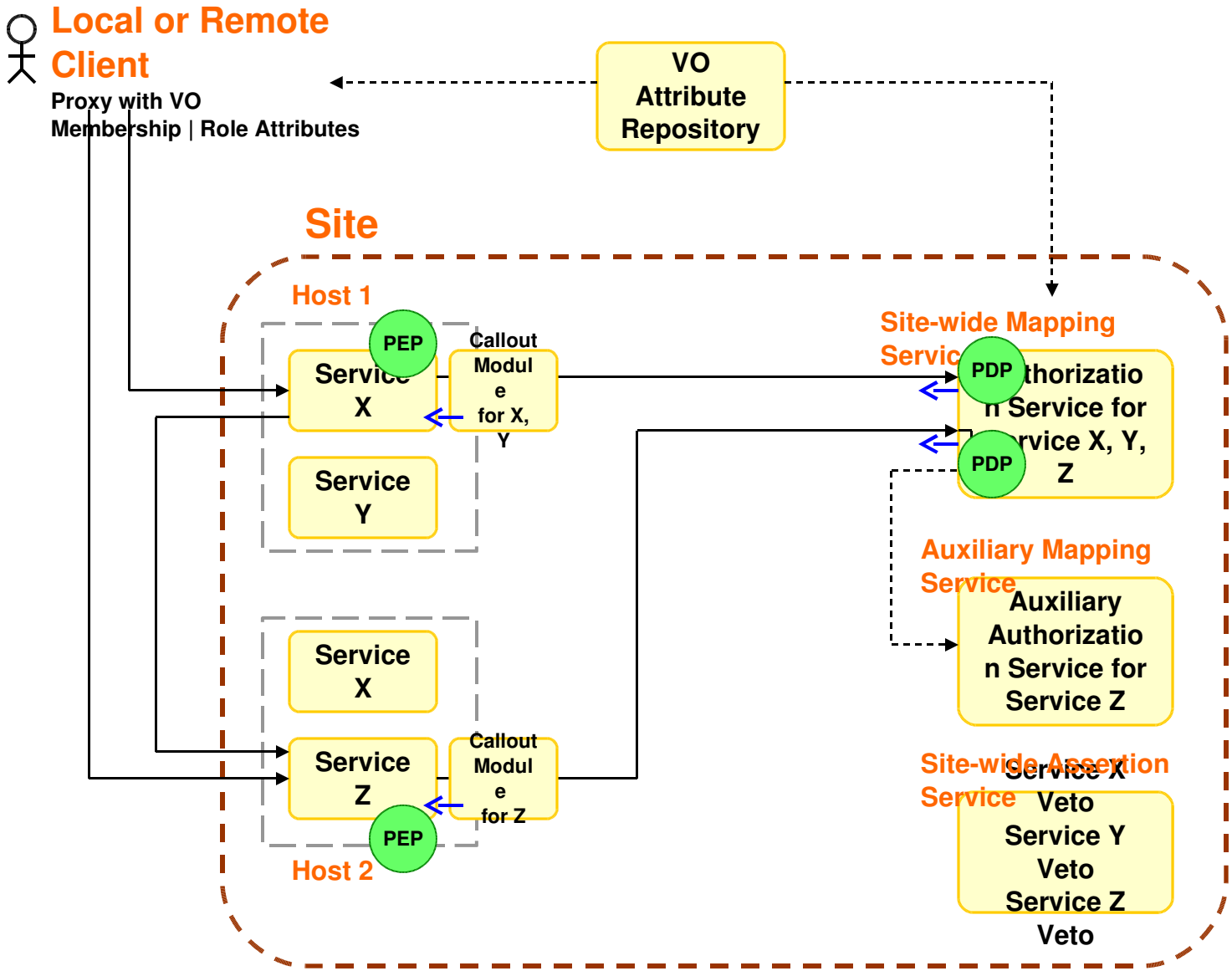
- VO-Global specification of privilege attributes per Role.
- Site central mapping of Role to site's implementation of privilege attributes.
- Local enforcement of privilege attributes.

- Use of VOMS extended X.509 Attribute Certificate specification for defining extra attributes (FQANs or Fully Qualified Attribute Names).
- Based on RFC-3281. FQANs contain Role and VO membership information for a User.

OSG AuthZ Approach

- VO defines Roles and associated privileges by specifying expected functionality.
  - E.g. ***cmssoft*** may install software in area that is read-only by all ***cmsuser*** jobs running on site/campus.
  - E.g. ***cmsphedex*** may have special access to SRM/dCache system.
- Site maps VO scope identities to local scope identities.
  - Site wide management of mapping.
  - Service level granularity of mapping.
- Site enforces VO privilege policies within local scope identities.
- Authorization = (VO-allowed) && !(Site-vetoed)

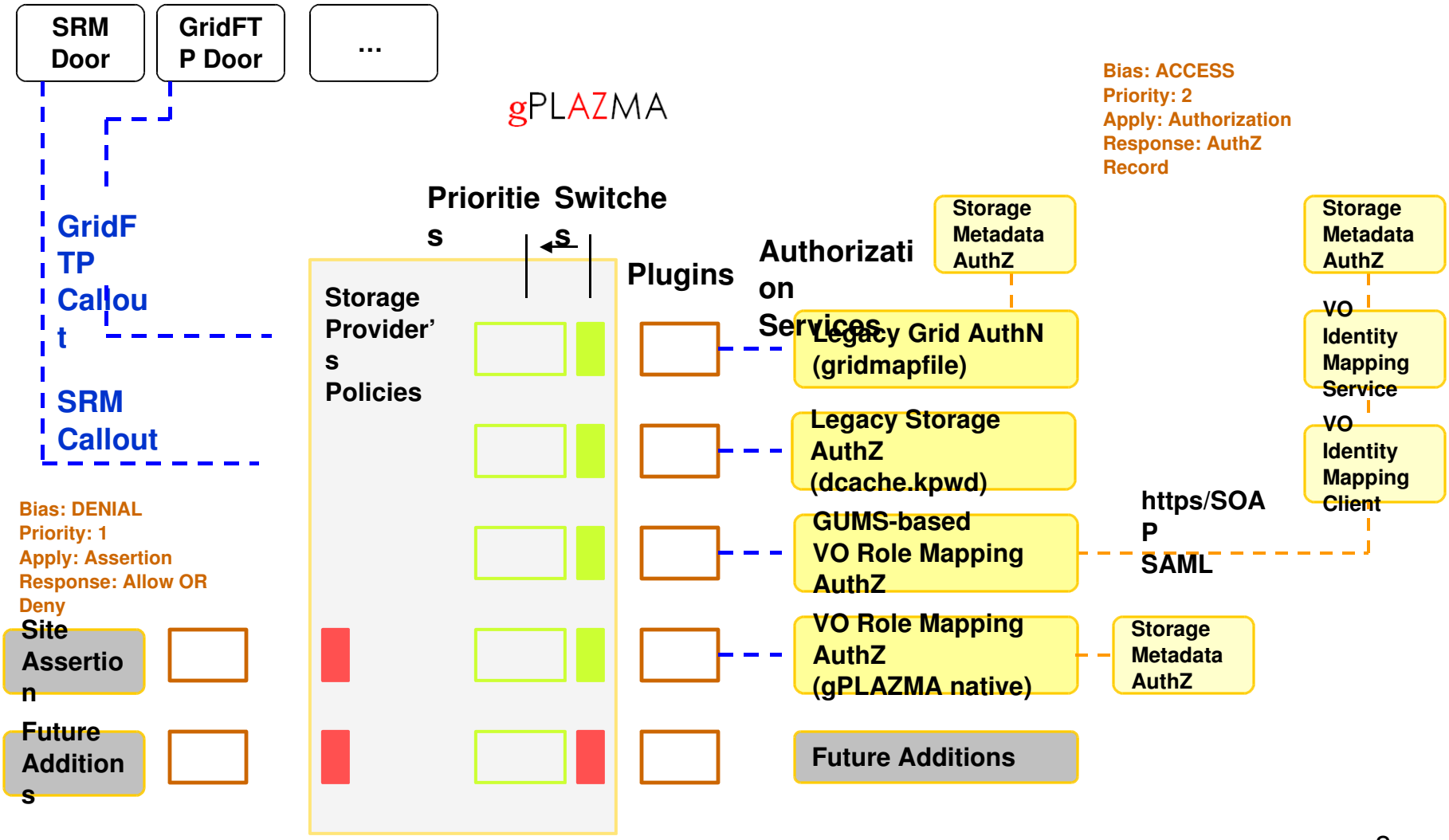

Local or Remote Client
Proxy with VO Membership | Role Attributes
VO Attribute Repository
Site
Host 1
Service X
Callout Module for X, Y
Service Y
Service X
Service Z
Callout Module for Z
Host 2
Site-wide Mapping Service
Authorization Service for Service X, Y, Z
Auxiliary Mapping Service
Auxiliary Authorization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



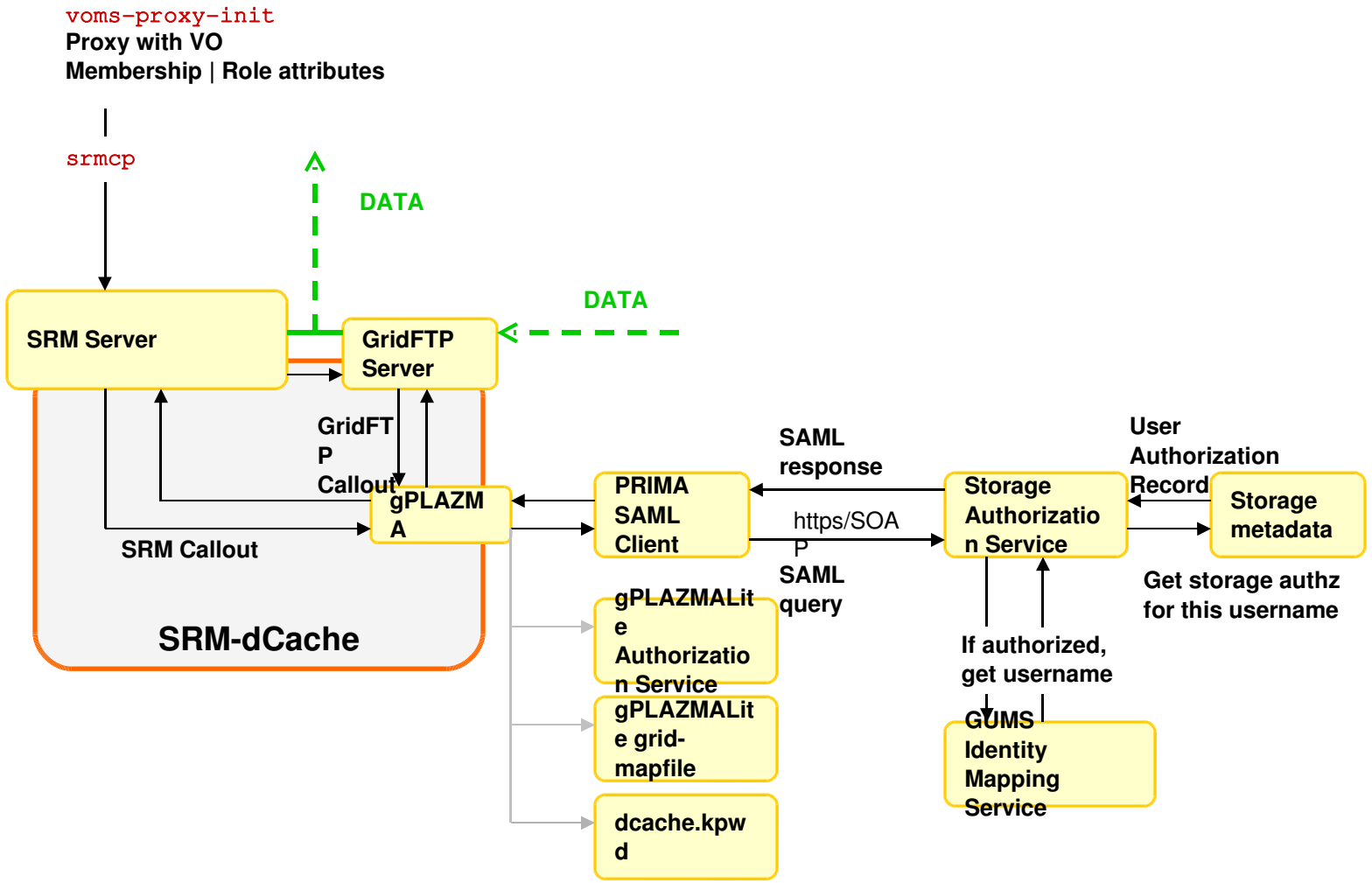
PEP Policy Enforcement Point

PDP Policy Decision Point

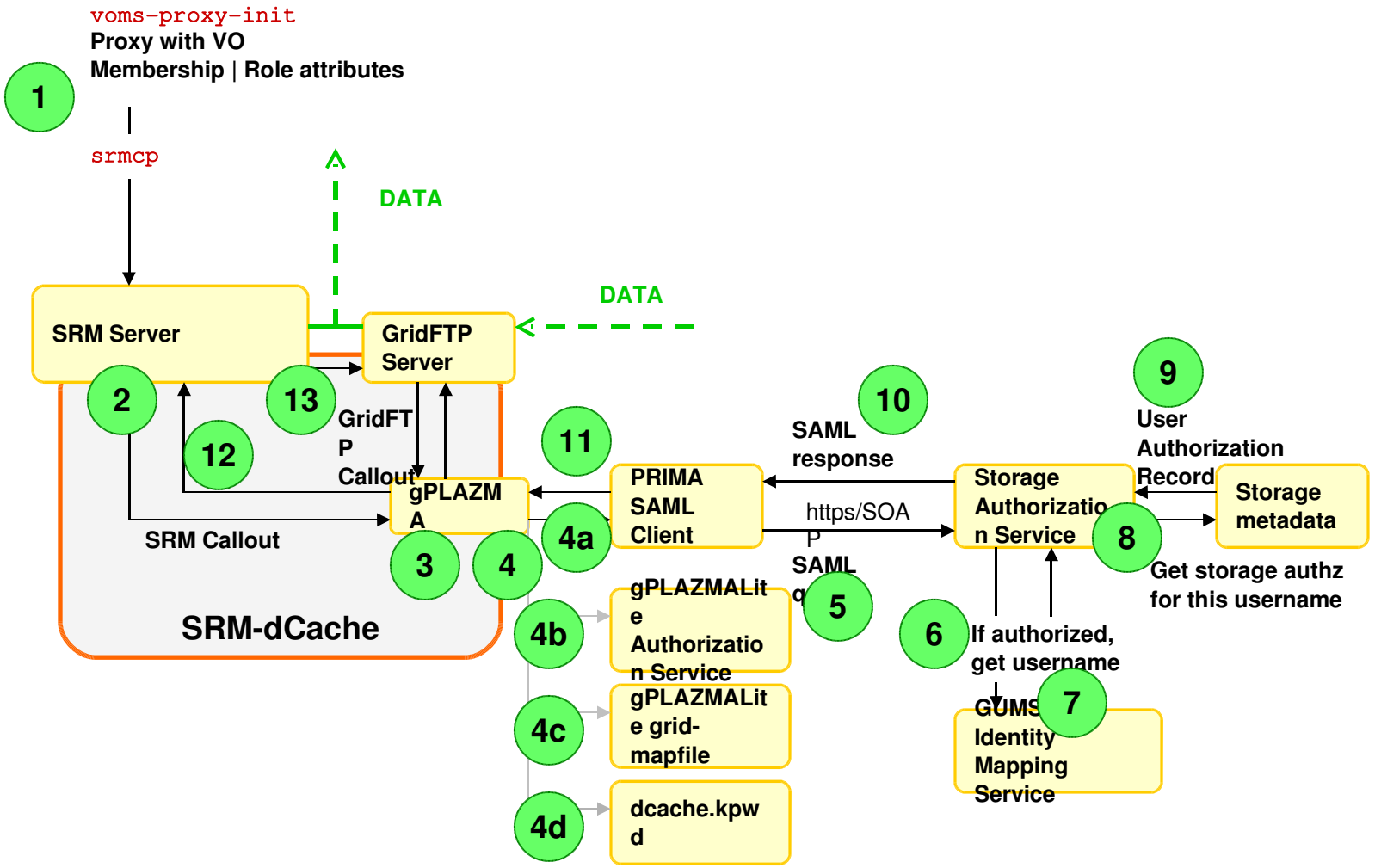
gPLAZMA Architecture



gPLAZMA Implementation



gPLAZMA Implementation



Example of end-to-end AuthZ for CEs and SEs

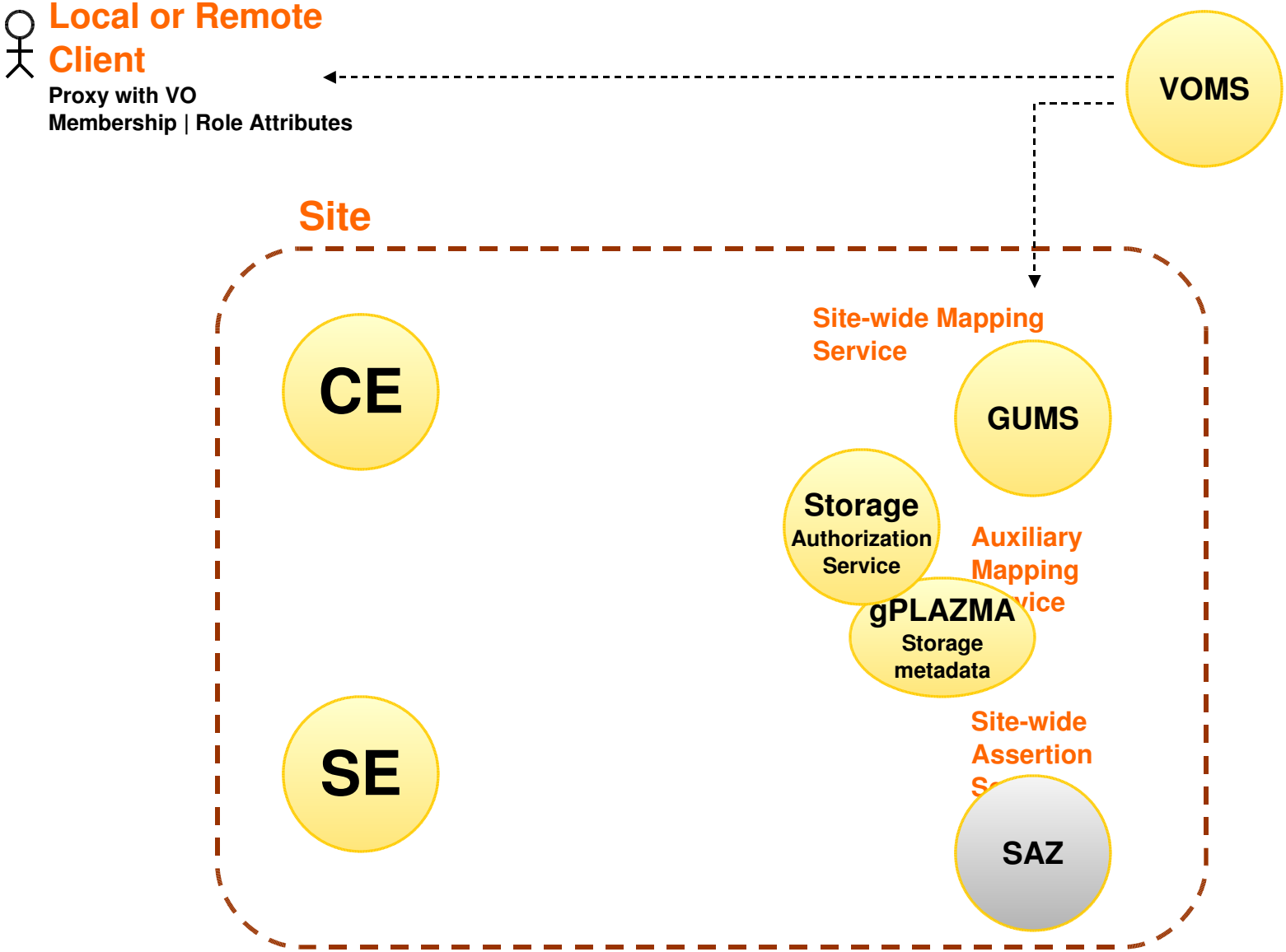
SE: SRM-dCache

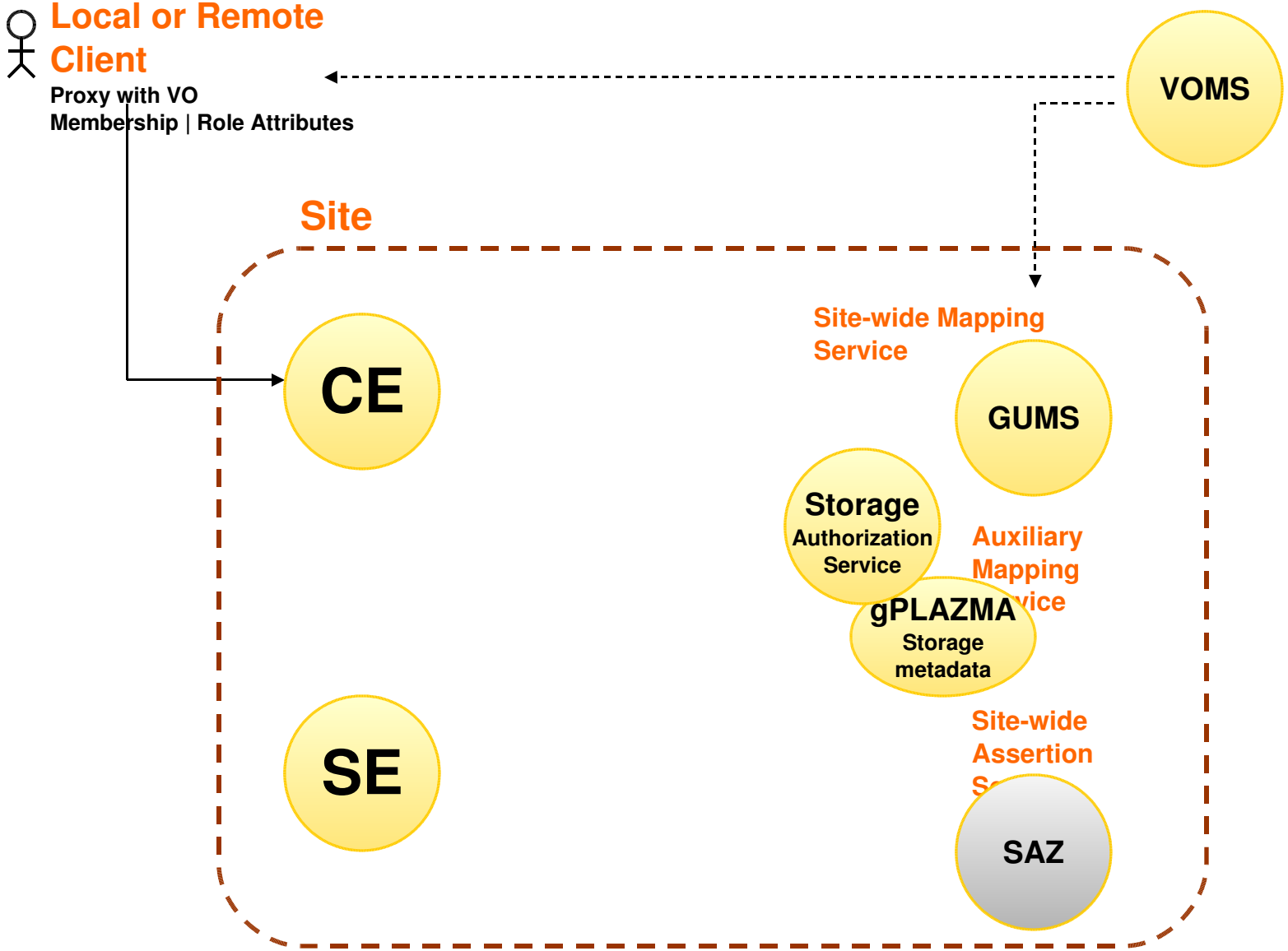
- Different *doors* for different authz methods.
- Same underlying local authz mechanism.
- Can be mapped to site's UID/GID domain.
- Or be restricted to SRM-dCache only.
- Examples:
  - USCMS-VO at FNAL: Site UID domain.
  - CDF-VO at FNAL: Site Kerberos domain.

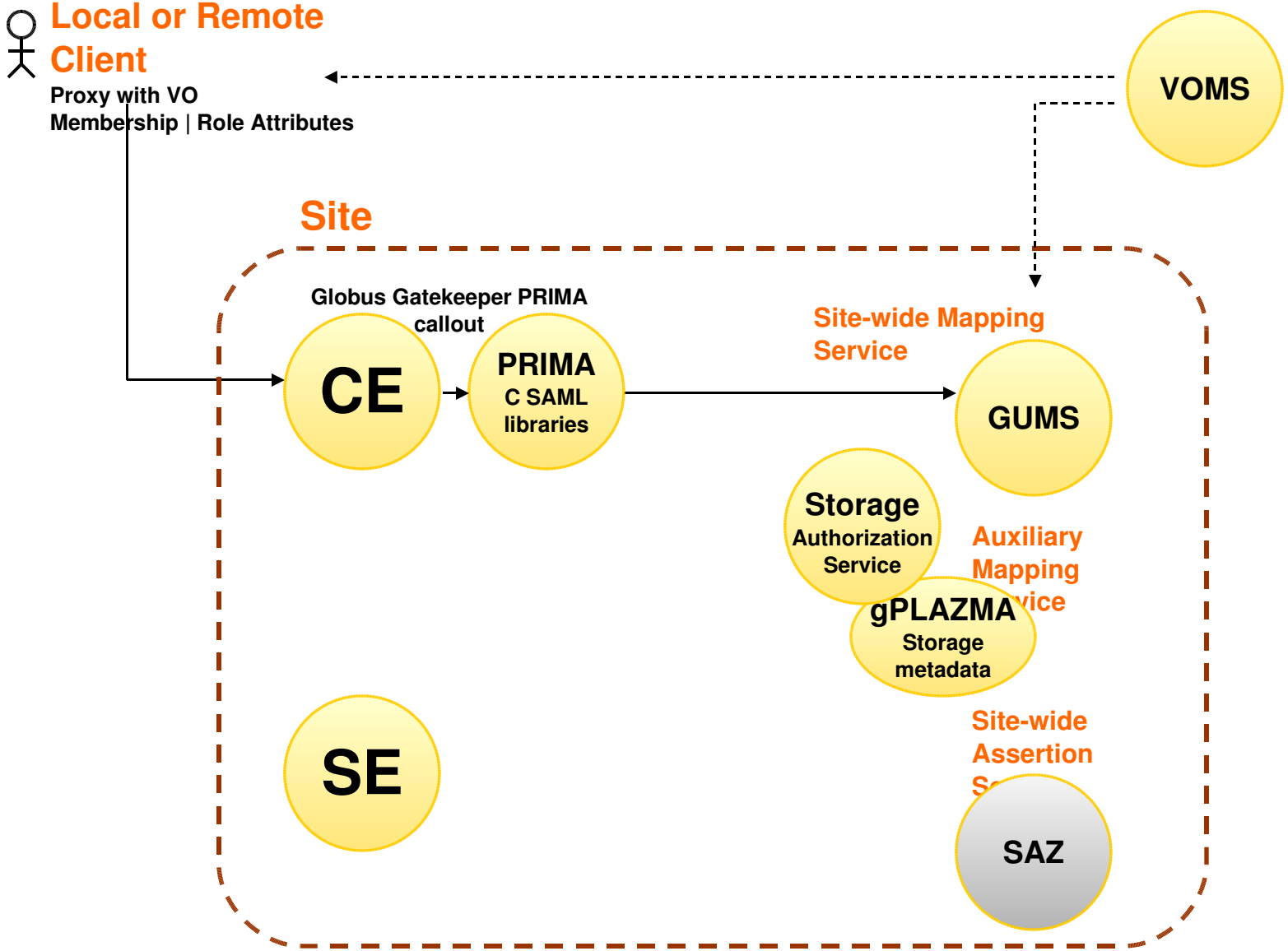
SE: SRM-dCache

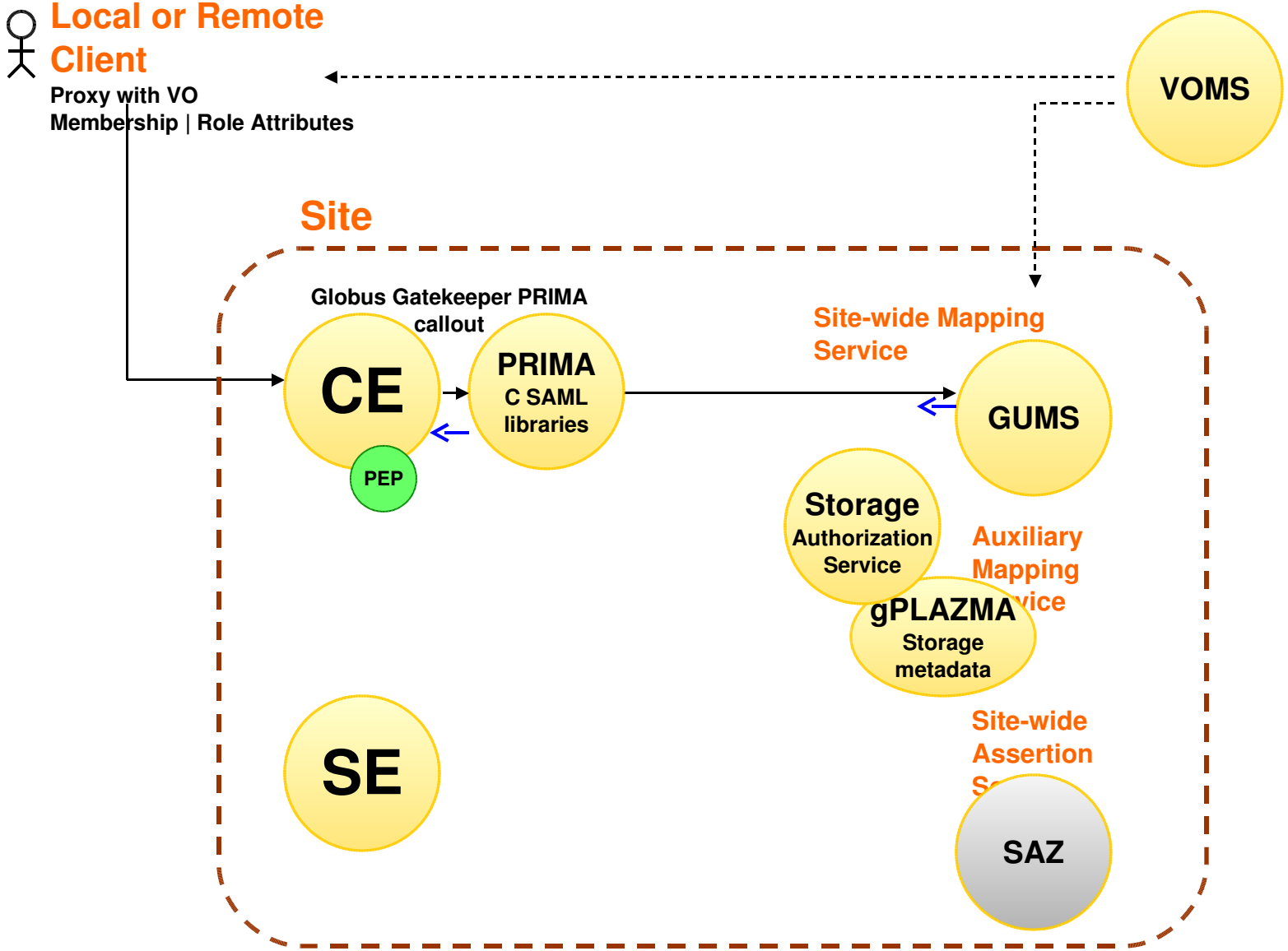
- gPLAZMA extends SRM-dCache separation of SE authz and CE authz to OSG approach.

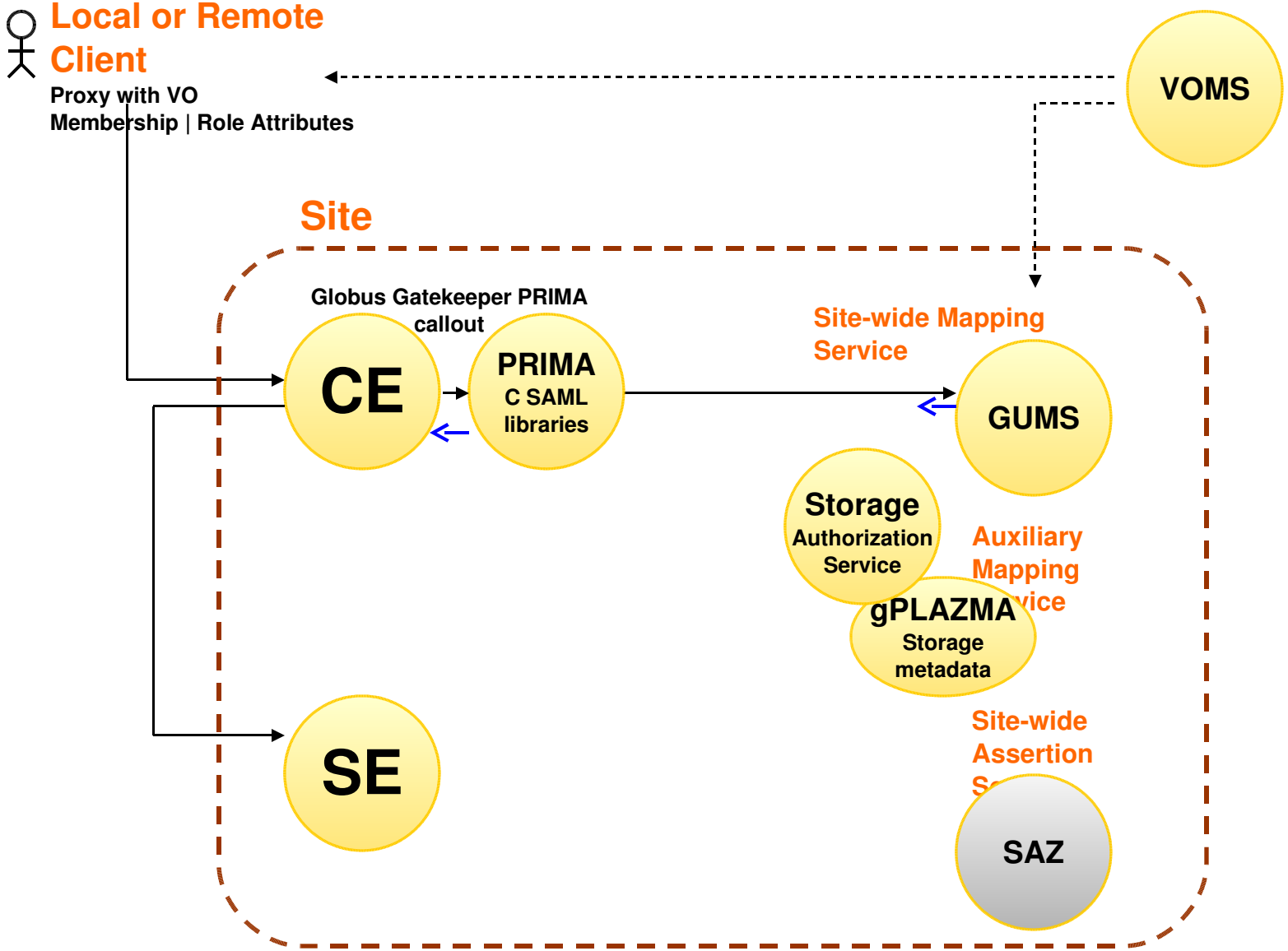
  - gPLAZMA authenticates.
  - gPLAZMA uses PRIMA Java SAML libraries to form a SAML query and contacts Storage Authz Service.
  - Storage Authz Service contacts GUMS and Storage Metadata Service.
  - GUMS translates {DN, Membership, Role} to Username.
  - Storage Metadata Service translates Username to Storage-privilege Set.
  - Storage-privilege Set is {UID, GID, permitted storage area, R/W permissions}.
  - Storage-privilege Set is User-level ACL governed by {DN, Membership, Role}.
  - Storage Authz Service forms a User Authorization Record into a SAML response and sends it back to gPLAZMA at SE.

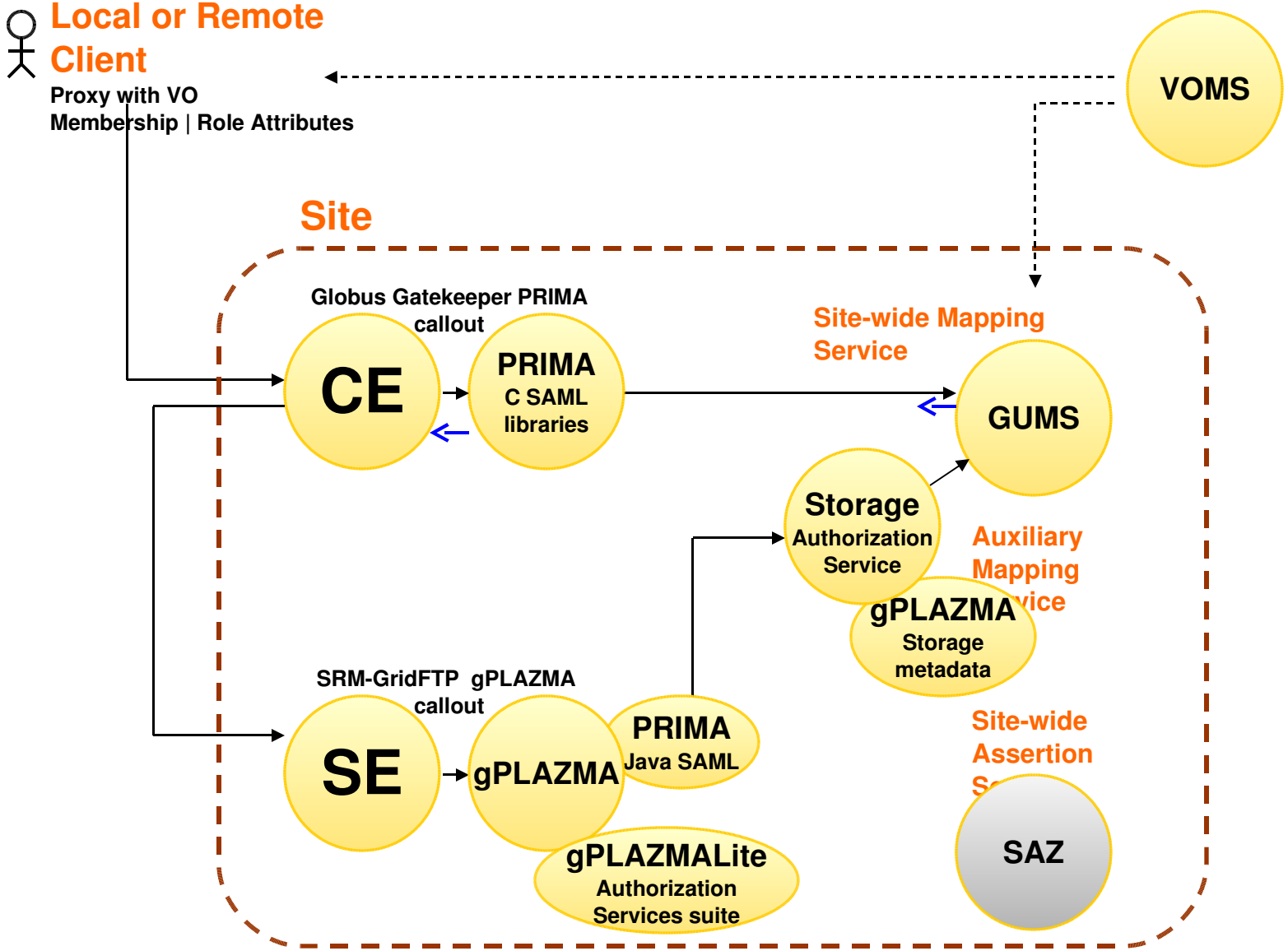

Local or Remote Client
Proxy with VO Membership | Role Attributes
VOMS
Site
CE
SE
Site-wide Mapping Service
GUMS
Storage Authorization Service
Auxiliary Mapping
gPLAZMA Storage metadata
Site-wide Assertion
SAZ

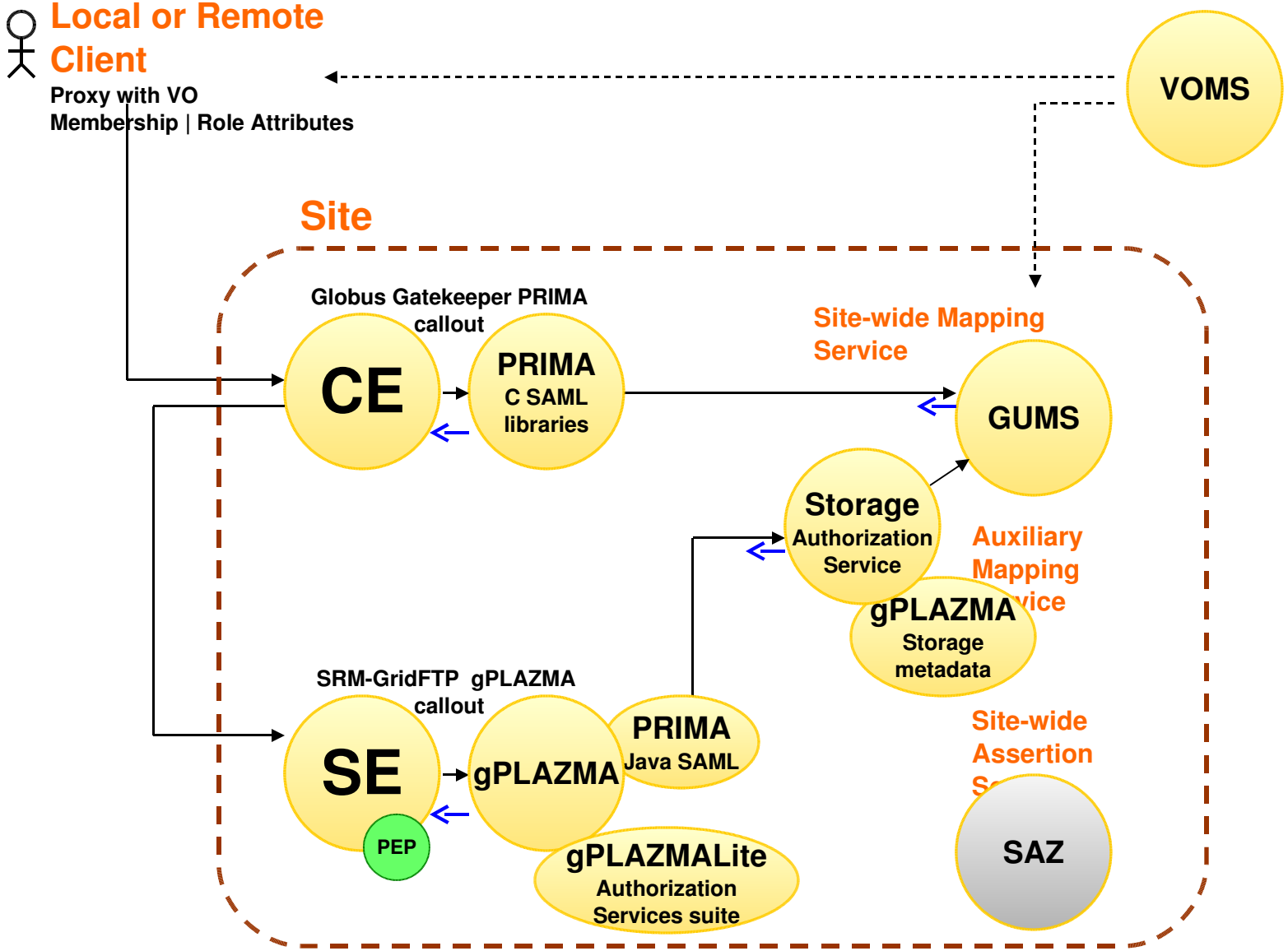

Local or Remote Client
Proxy with VO Membership | Role Attributes
VOMS
Site
CE
SE
Site-wide Mapping Service
GUMS
Storage Authorization Service
Auxiliary Mapping
gPLAZMA Storage metadata
Site-wide Assertion
SAZ

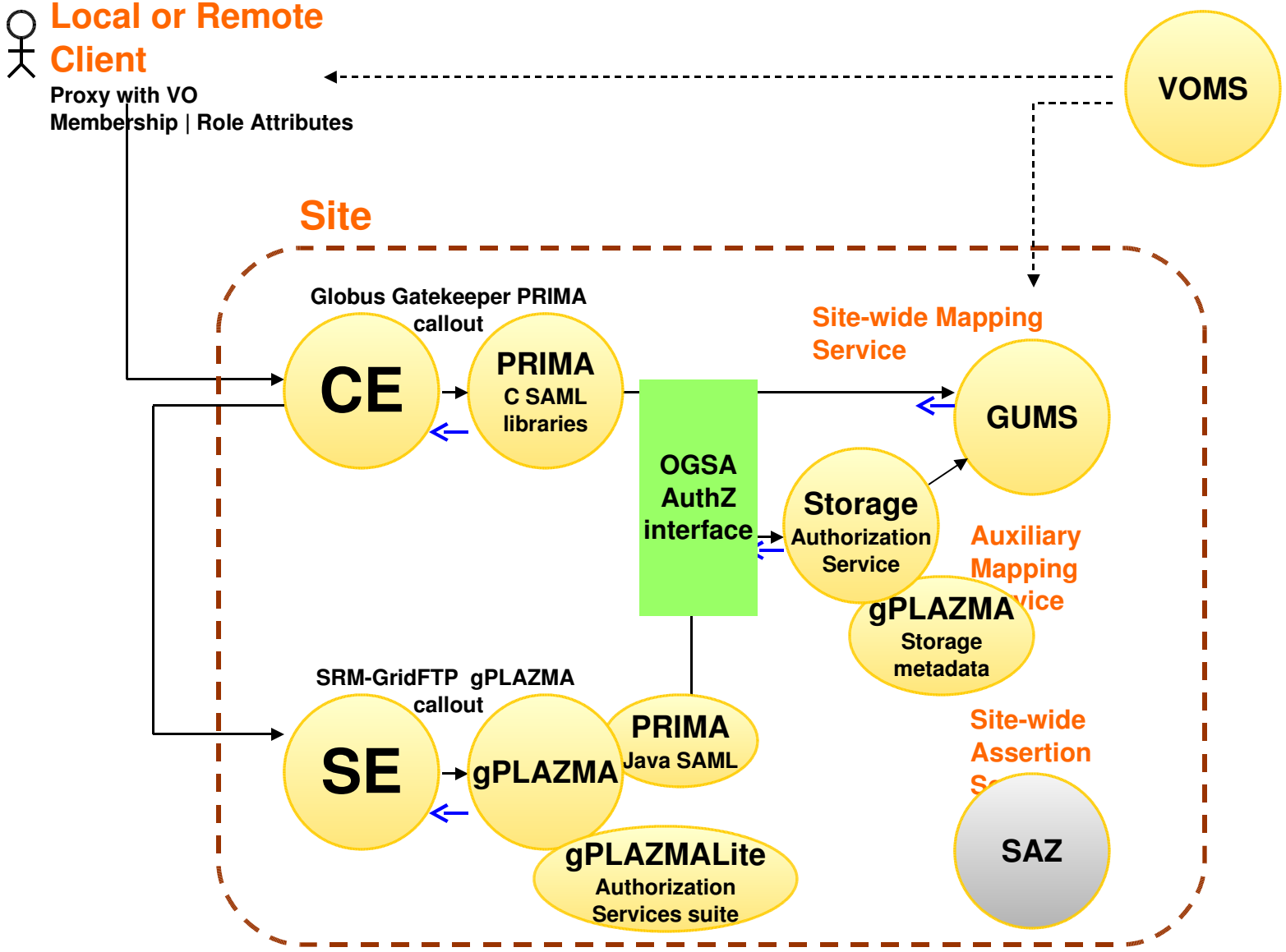

Local or Remote Client
Proxy with VO Membership | Role Attributes
VOMS
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
Site-wide Mapping Service
GUMS
Storage Authorization Service
Auxiliary Mapping
gPLAZMA
Storage metadata
SE
Site-wide Assertion
SAZ

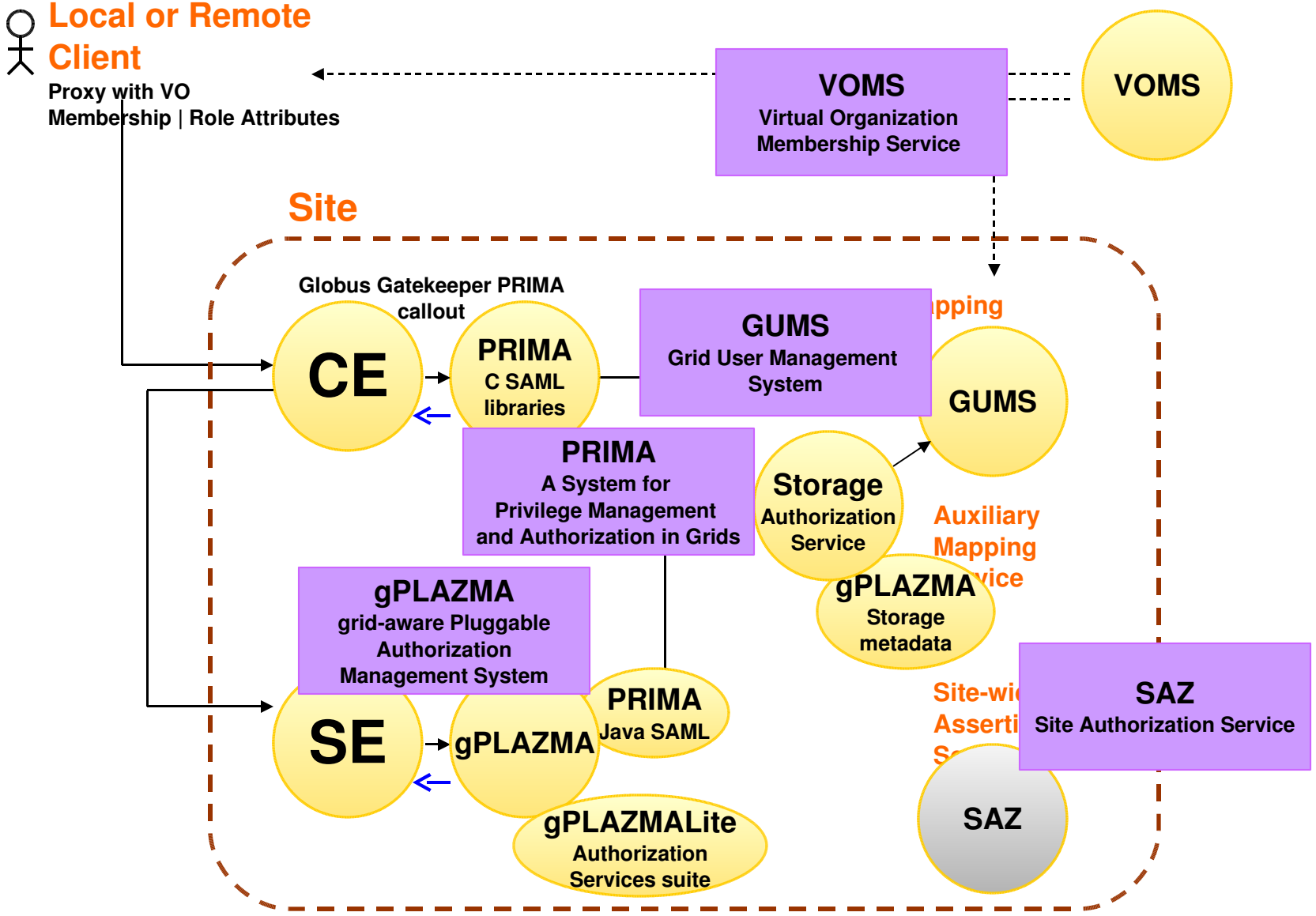

Local or Remote Client
Proxy with VO Membership | Role Attributes
VOMS
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
PEP
Site-wide Mapping Service
GUMS
Storage Authorization Service
Auxiliary Mapping
gPLAZMA
Storage metadata
SE
Site-wide Assertion
SAZ

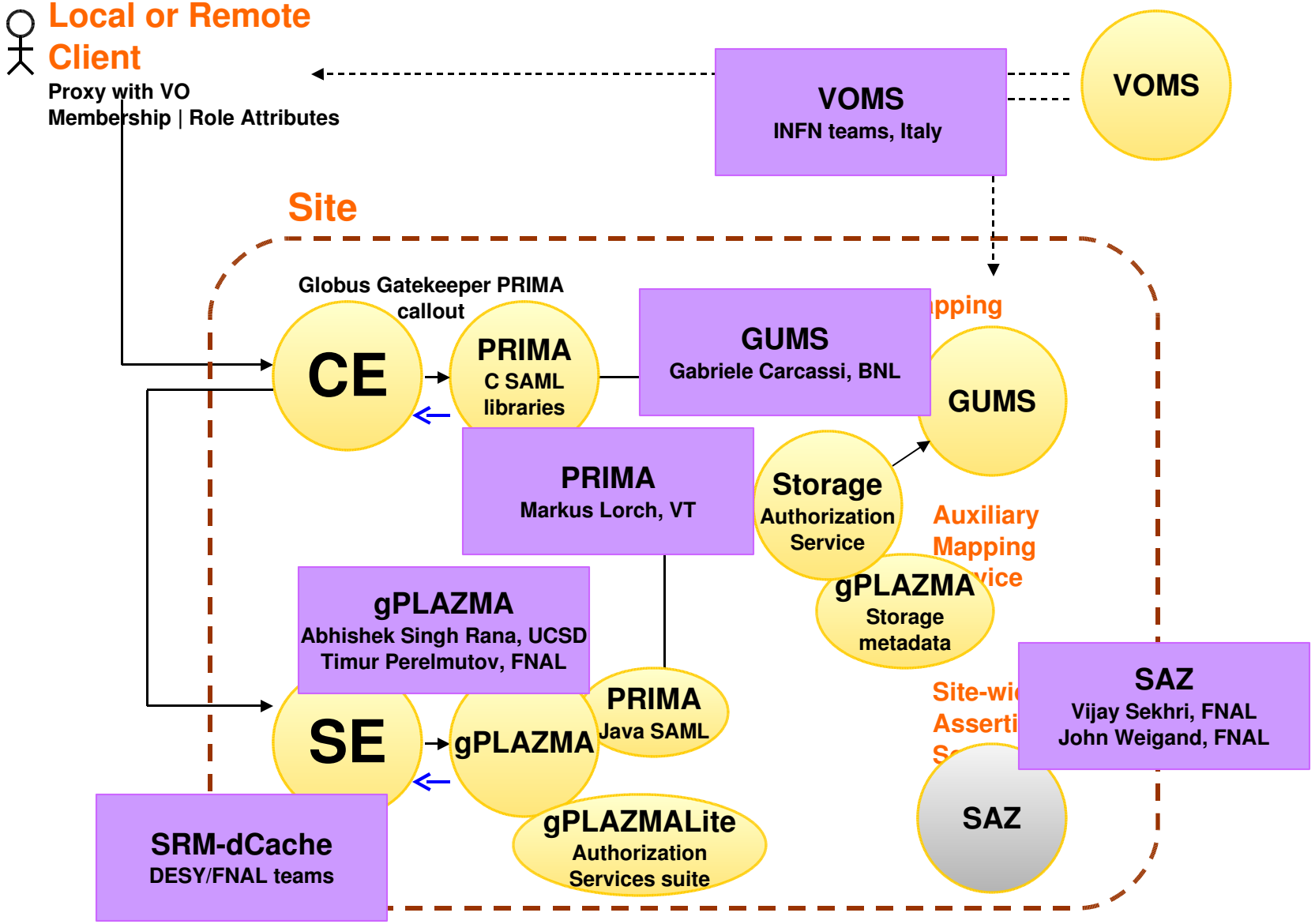

Local or Remote Client
Proxy with VO Membership | Role Attributes
VOMS
Site
Globus Gatekeeper PRIMA callout
CE
PRIMA
C SAML libraries
Site-wide Mapping Service
GUMS
Storage Authorization Service
Auxiliary Mapping
gPLAZMA
Storage metadata
SE
Site-wide Assertion
SAZ


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


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


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

Status

- gPLAZMA native role-based authz mode deployed at USCMS tier-2 production site at UCSD. Work in progress for deployment at tier-1 at FNAL.
- GUMS role-based authz mode in final stages of development/packaging.
- Deployment and usage of all modes on USCMS production dCache sites expected before Service Challenge 4.

Known Limitations

- Not (yet) implemented for dcap.
- Scalability of site central call-out not yet understood.(gPLAZMA native a viable fallback)
- vi/emacs is only administrative interface.
- Options for communicating desired policies from VO to site are less than satisfactory. (general problem of role based authz!)

Future Work

- Add MySQL based backend to replace *storage authz records* configuration file.
- Complete gPLAZMA for dcap.
- Understand scalability of site-wide call-out.
- Add XACML based authorization engine to dynamically assign storage authz mappings at Site.
- Explore XACML/SAML rule-based policy declaration (***VO-level***) and policy computation (***Site-level***).

Thank You.