The New dCache Authorization

gPLAZMA

grid-aware PLuggable AuthoriZation MAnagement

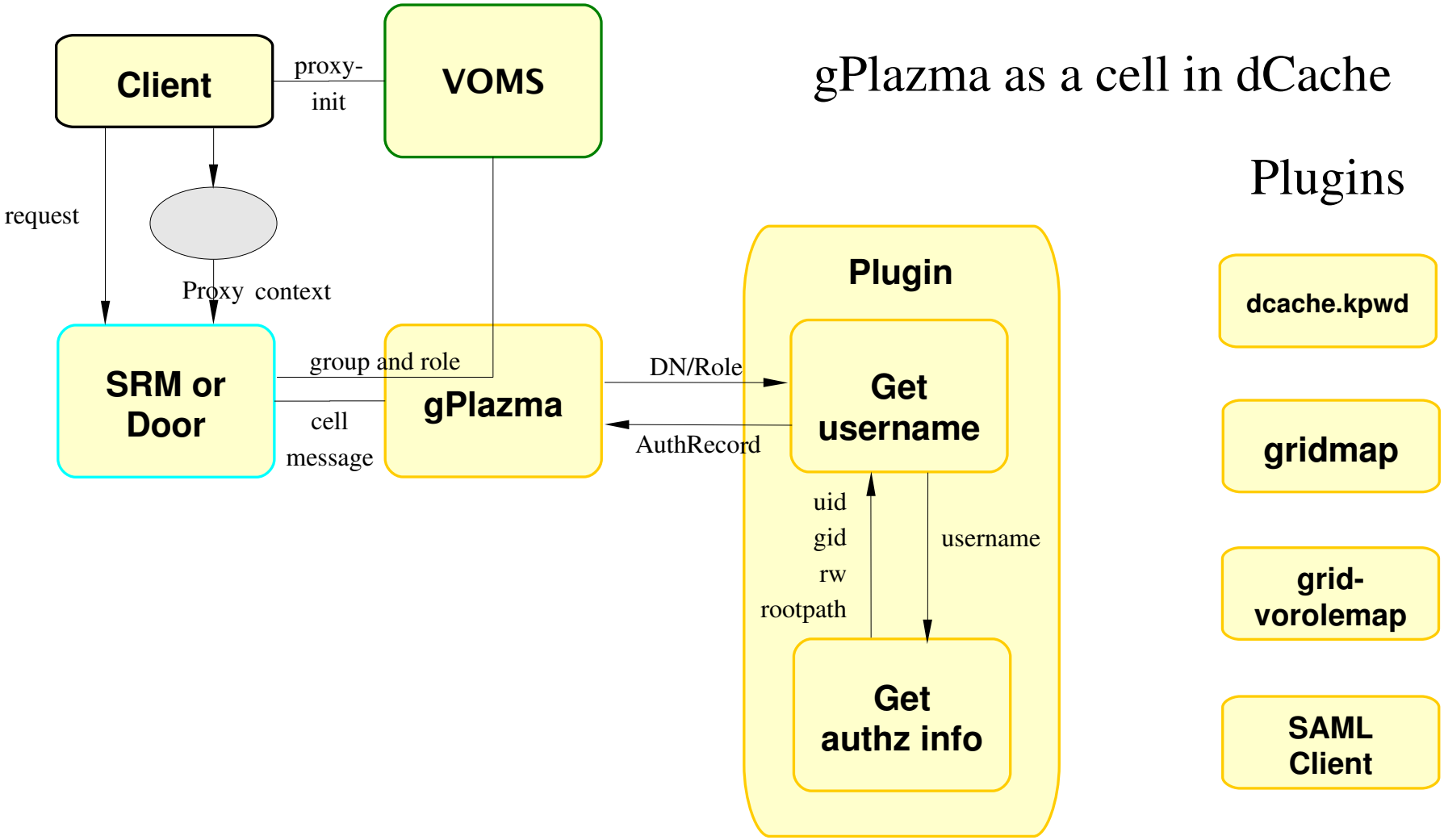
Presenting talk: Steven Timm—Fermilab

Adapted from talk written by and work done by
Ted Hesselroth—Fermilab, dCache Collaboration
to whom followup should be addressed.
Work also done by Abhishek Rana, Markus Lorch.

gPLAZMA Introduction

- dCache has internal authorization scheme not linked to unix passwd/group file
- Each logical dCache user has uid,gid, and root path
- gPLAZMA provides centralized authorization scheme for dCache
  - Selectable authorization mechanisms
  - Compatible with CE authorization mechanisms
  - Role-based
- Shipping in current version of dCache (1.7)
- Deployed and working on big Storage Elements now.

gPlazma Authorization



gPlazma as a cell in dCache

Plugins

- dcache.kpwd
- gridmap
- grid-vorolemap
- SAML Client

The kpwd Method

- The default method
- Maps
  - DN to username
  - username to uid, gid, rw, rootpath

dcache.kpwd:

```
# Mappings for 'cmsprod' users
mapping "/DC=org/DC=doegrids/OU=People/CN=Ted Hesselroth 899520" cmsprod
mapping "/DC=org/DC=doegrids/OU=People/CN=Shaowen Wang 564753" cmsprod


# Login for 'cmsprod' users
login     cmsprod    read-write    9801   5033    /
/pnfs/fnal.gov/data/cmsprod    /pnfs/fnal.gov/data/cmsprod
        /DC=org/DC=doegrids/OU=People/CN=Ted Hesselroth 899520
        /DC=org/DC=doegrids/OU=People/CN=Shaowen Wang 564753
```

The grid-mapfile Method

- May use mapfile from compute element.

/etc/grid-security/grid-mapfile:

```
"/DC=org/DC=doegrids/OU=People/CN=Ted Hesselroth 899520" cmsprod
"/DC=org/DC=doegrids/OU=People/CN=ABHISHEK SINGH RANA 768382" cmsprod
"/DC=org/DC=doegrids/OU=People/CN=Keri Pembrook 651725" dzero
```

- Lookup in storage-authzdb follows for uid, gid, etc.
- Authorizes and provides site-specific storage obligations

/etc/grid-security/storage-authzdb:

```
authorize cmsprod read-write 9811 5063 / /pnfs/fnal.gov/data/cms /
authorize dzero   read-write 1841 5063 / /pnfs/fnal.gov/data/dzero /
```

The gplazmalite-vorole-mapping Method

- Role is appended to DN for lookup.

/etc/grid-security/grid-vorolemap:

```
"/DC=org/DC=doegrids/OU=People/CN=Ted Hesselroth 899520"
"/cms/uscms/Role=cmsprod" uscms01

"/DC=org/DC=doegrids/OU=People/CN=Keri Pembrook 651725" dzero

"*" "/cms/uscms/Role=cmsprod" cmsprod

"*" "/cms/uscms/Role=analysis" analysis
```

- Lookup in storage-authzdb follows for uid, gid, etc.

The saml-vo-mapping Method

- Acts as a client to GUMS

dcachesrm-gplazma.policy:

```
# Switches"
saml-vo-mapping="ON"

...
# SAML-based grid VO role mapping
mappingServiceUrl="https://flegling09.fnal.gov:8443/gums/services/
GUMSAuthorizationServicePort"
```

- Returns a username.
- Lookup in storage-authzdb follows for uid, gid, etc.

GUMS (Grid User Management System)

- Compute elements also authorize through GUMS

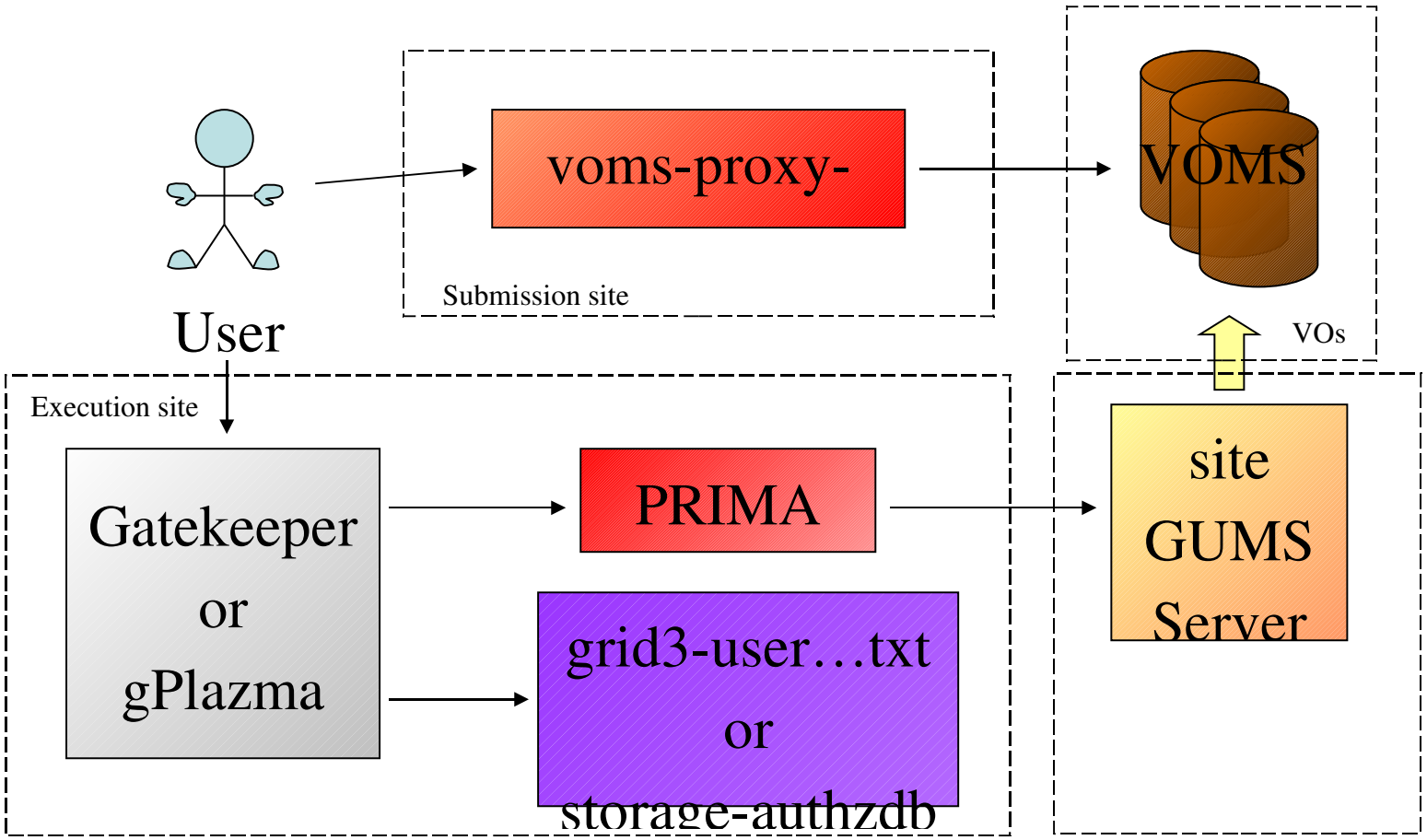


Diagram Credit: Ian Fisk and Gabriele Carcassi, "Role Based VO Authorization Services", July 20, 2005

Additional Features

- Optional SAZ plugin (coming in v1.8)
- Auto-fallback to alternate methods if one fails
- gPLAZMA methods available for direct call by other dCache components such as gridftp door.
- Denial of specific certificate and role combinations.
- Configurable logging levels.
- Regexp support in storage-authzdb (coming in v1.8)