The New dCache Authorization

gPLAZMA

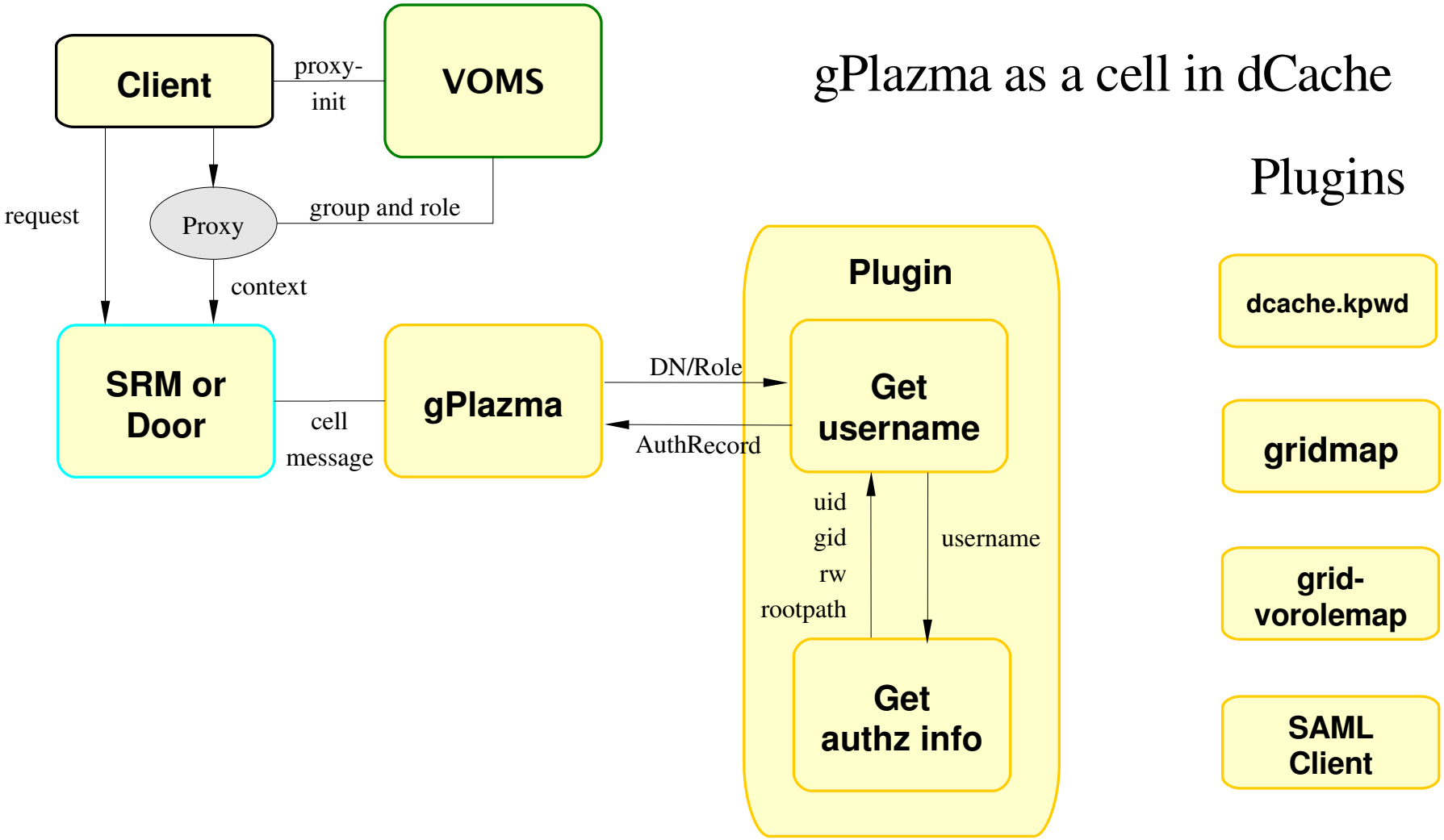
grid-aware PLuggable AuthoriZation MAnagement

Ted Hesselroth
dCache Collaboration

gPlazma

- Centralized Authorization
- Selectable authorization mechanisms
- Compatible with compute element authorization
- Role-based

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.
- Alternative: An LCMAPS Plugin

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

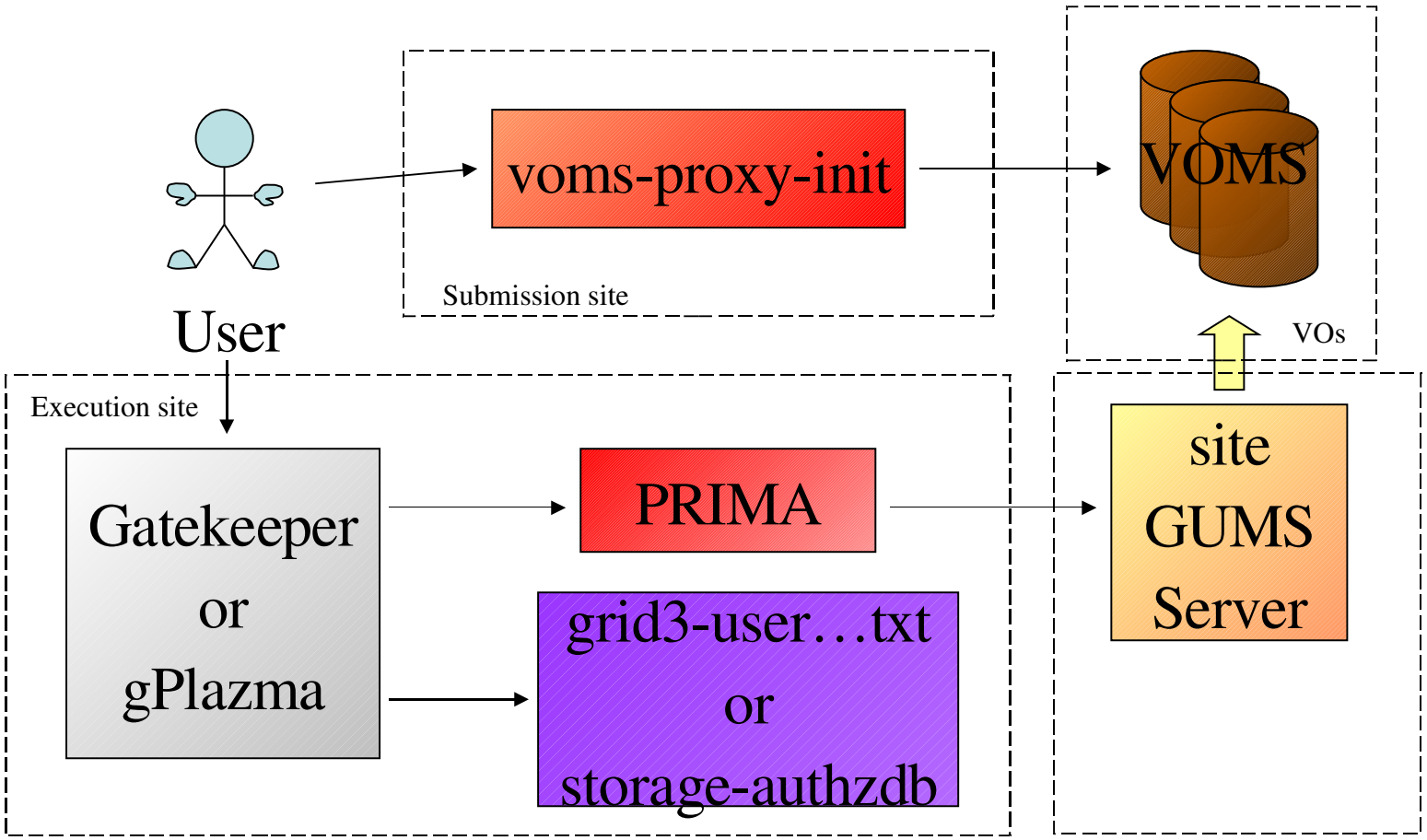


Diagram Credit: Ian Fisk and Gabriele Carcassi, "Role Based VO Authorization Services", July 20, 2005

The saz-client Method

- Acts as a client to SAZ (Site AuthZ) server
  - Sends certificate chain
  - SAZ returns a “yes” or “no” result
- If saz-client on, called before other plugins
  - At least one other plugin must also pass.

dcachesrm-gplazma.policy:

```
# SAZ Settings
saz-client="ON"
SAZ_SERVER_HOST="fledgling09.fnal.gov"
SAZ_SERVER_PORT="8888"
```

Fallback Authorization in gPlazma Cell

- If authorization fails or is denied, attempts next method

dcachesrm-gplazma.policy:

```
# Switches"
saml-vo-mapping="ON"
kpwd="ON"
grid-mapfile="OFF"
gplazmalite-vorole-mapping="OFF"

# Priorities
saml-vo-mapping-priority="1"
kpwd-priority="3"
grid-mapfile-priority="4"
gplazmalite-vorole-mapping-priority="2"
```

Fallback Authorization by Direct Calls

- If authorization from gPlazma cell fails or is denied, attempts authorization by direct call of gPlazma methods.

config/gridftpdoorSetup or config/gridftpdoorSetup:

```
useGPlazmaAuthorizationModule=true
useGPlazmaAuthorizationCell=true
```

Blacklisting

- Denial of specific DN and Role combinations

/etc/grid-security/grid-vorolemap:

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

dcachesrm-gplazma.policy:

```
# Switches
saml-vo-mapping="OFF"
kpwd="ON"
grid-mapfile="OFF"
gplazmalite-vorole-mapping="ON"

# Priorities
saml-vo-mapping-priority="2"
kpwd-priority="3"
grid-mapfile-priority="4"
gplazmalite-vorole-mapping-priority="1"
```

Logging

- ssh command “set LogLevel <level>”
- ERROR
  - Exception or authorization denied by gPlazma
- WARN
  - Authorization denied by plugin
- INFO
  - Authorizations granted by plugin
- DEBUG
  - Program trace

ThreadManager

- Supplies threads and runs processes in them.
- Queues runnables to wait for an available thread.

config/srm.batch:

```
create diskCacheV111.util.ThreadManager ThreadManager \
       "default \
       -num-threads=10 \
       -thread-timeout=15 \
"
```

diskCacheV111/srm/dcache/PinCompanion.java:

```
public void answerArrived( final CellMessage req , final CellMessage answer ) {
        diskCacheV111.util.ThreadManager.execute(new Runnable() {
            public void run() {
                processMessage(req,answer);
            }
        });
    }
```

New in Version 1.8

- No delegation
- SAZ plugin
- Regular expression support in storage-authzdb
- Priority field in storage-authzdb
- StorageAuthorizationService

Appendix: Use Cases

Use Case – Roles for Reading and Writing

- Write privilege for cmsprod role.
- Read privilege for analysis and cmsuser roles.

/etc/grid-security/grid-vorolemap:

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

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

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

/etc/grid-security/storage-authzdb:

```
authorize cmsprod  read-write  9811 5063 / /pnfs/fnal.gov/data /
authorize analysis read-write 10822 5063 / /pnfs/fnal.gov/data /
authorize cmsuser  read-only  10001 6800 / /pnfs/fnal.gov/data /
```

Use Case – Home Directories

- Users can read and write only to their own directories

/etc/grid-security/grid-vorolemap:

```
"/DC=org/DC=doegrids/OU=People/CN=Selby Booth" cms821
"/DC=org/DC=doegrids/OU=People/CN=Kenja Kassi" cms822
"/DC=org/DC=doegrids/OU=People/CN=Ameil Fauss" cms823
```

/etc/grid-security/storage-authzdb for version 1.7.0:

```
authorize cms821 read-write 10821 7000 / /pnfs/fnal.gov/data/cms821 /
authorize cms822 read-write 10822 7000 / /pnfs/fnal.gov/data/cms822 /
authorize cms823 read-write 10823 7000 / /pnfs/fnal.gov/data/cms823 /
```

/etc/grid-security/storage-authzdb for version 1.8:

```
authorize cms(\d\d\d) read-write 10$1 7000 / /pnfs/fnal.gov/data/cms$1 /
```

Appendix: GUMS

Grid User Management System

GUMS (Grid User Management System)

- Is a Policy Decision Point
- Implemented as a web service
- Checks VOMS servers for user membership
  - No maintenance of individual users at storage site
  - Ensures that users are in a VO
- Maintains MySQL database of users and roles
- Checks users DN, maps to Group and Role to username
  - Group and pool accounts
  - Individual accounts, NIS or LDAP query

GUMS Configuration

- Example entry for a username mapping

/opt/gums-service/var/war/WEB-INF/classes/gums.config:

```
...
<groupMapping name="uscmsprod" accountingVo="uscms" accountingDesc="CMS">
    <userGroup className="gov.bnl.gums.VOMSGroup"
        url="https://lcg-voms.cern.ch:8443/voms/cms/services/VOMSAdmin"
        persistenceFactory="mysql"
        name="cmsprod"
        voGroup="/cms/uscms"
        voRole="cmsprod"
        matchFQAN="exact"
        sslCertfile="/etc/grid-security/http/httpcert.pem"
        sslKey="/etc/grid-security/http/httpkey.pem"/>
    <accountMapping className="gov.bnl.gums.GroupAccountMapper"
        groupName="cmsprod"/>
</groupMapping>
...
```

StorageAuthorizationService

- Web service
  - Adds uid, gid, etc info from storage-authzdb