gPLAZMA

grid-aware PLuggable AuthoriZation MAnagement

A gPLAZMA module v0.1 in dCache-SRM

Abhishek Singh Rana, Timur Perelmutov

rana@fnal.gov | timur@fnal.gov

Acknowledgements

Leadership: Robert D. Kennedy

Technical Insight: Jon A. Bakken

Collaboration with:

Open Science Grid Consortium

FNAL VO-Privilege Project

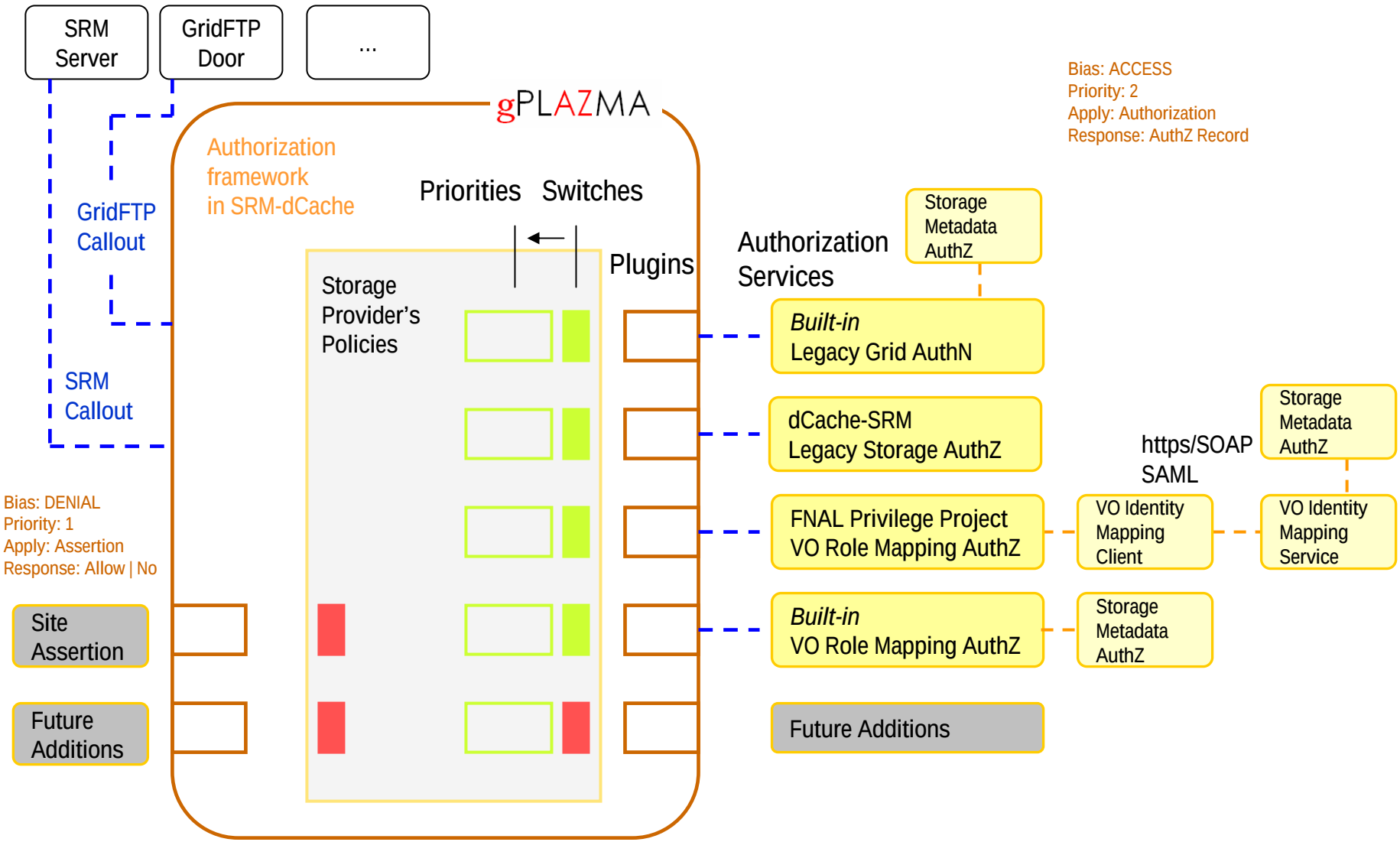
PPDG-Common

Open Science Grid
Storage Technical Group
Fermilab SRM-dCache Group

Authorization and Policy Control Framework in SRM-dCache
Architecture, Design Principles, and Implementation

Last Updated: 03-29-2005

Abhishek Singh Rana | Timur Perelmutov



Abhishek Singh Rana | Timur Perelmutov

gPLAZMAlite suite

A suite of *Built-in* lightweight authorization services.

Built-in
Legacy Grid AuthN

`grid-mapfile`

Introducing the next generation of grid-mapfile:

Built-in
VO Role Mapping AuthZ

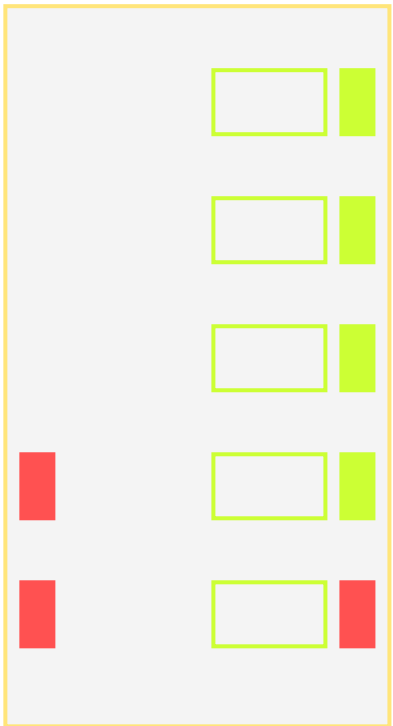
`grid-vorolemap`

Authorization and Policy Control Framework in SRM-dCache
Architecture, Design Principles, and Implementation

Abhishek Singh Rana | Timur Perelmutov

${dcache-home}/etc/dcachesrm-gplazma.policy

Dynamically loaded on-demand. A combination of Switches and Priorities (of different authorization modes) can be used to enforce an Over-riding access policy. Priorities are translated into *priorities of access* (first success at a mode). Select users can be given access selectively.



```
grid-mapfile = ON
grid-mapfile-priority = 4

dcache.kpwd = ON
dcache.kpwd-priority = 1

VO-role-mapping = ON
VO-role-mapping-priority = 2

gPLAZMA-vo-role-mapping = ON
gPLAZMA-vo-role-mapping-priority = 3

Unknown-authz-service = OFF
Unknown-authz-service-priority =
```

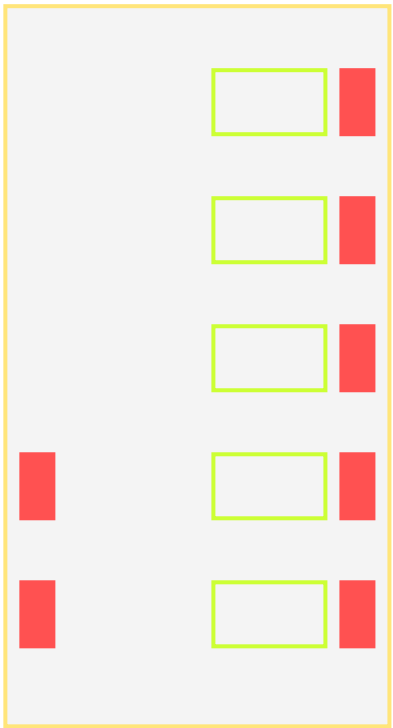
Authorization and Policy Control Framework in SRM-dCache
Architecture, Design Principles, and Implementation

Abhishek Singh Rana | Timur Perelmutov

${dcache-home}/etc/dcachesrm-gplazma.policy

Response to 'Grid Incidents' →

Site Storage Admins can declare a *Quasi-Firewall* policy without a need to shut storage services down. Possibly give restricted access by switching ON an unaffected mode.



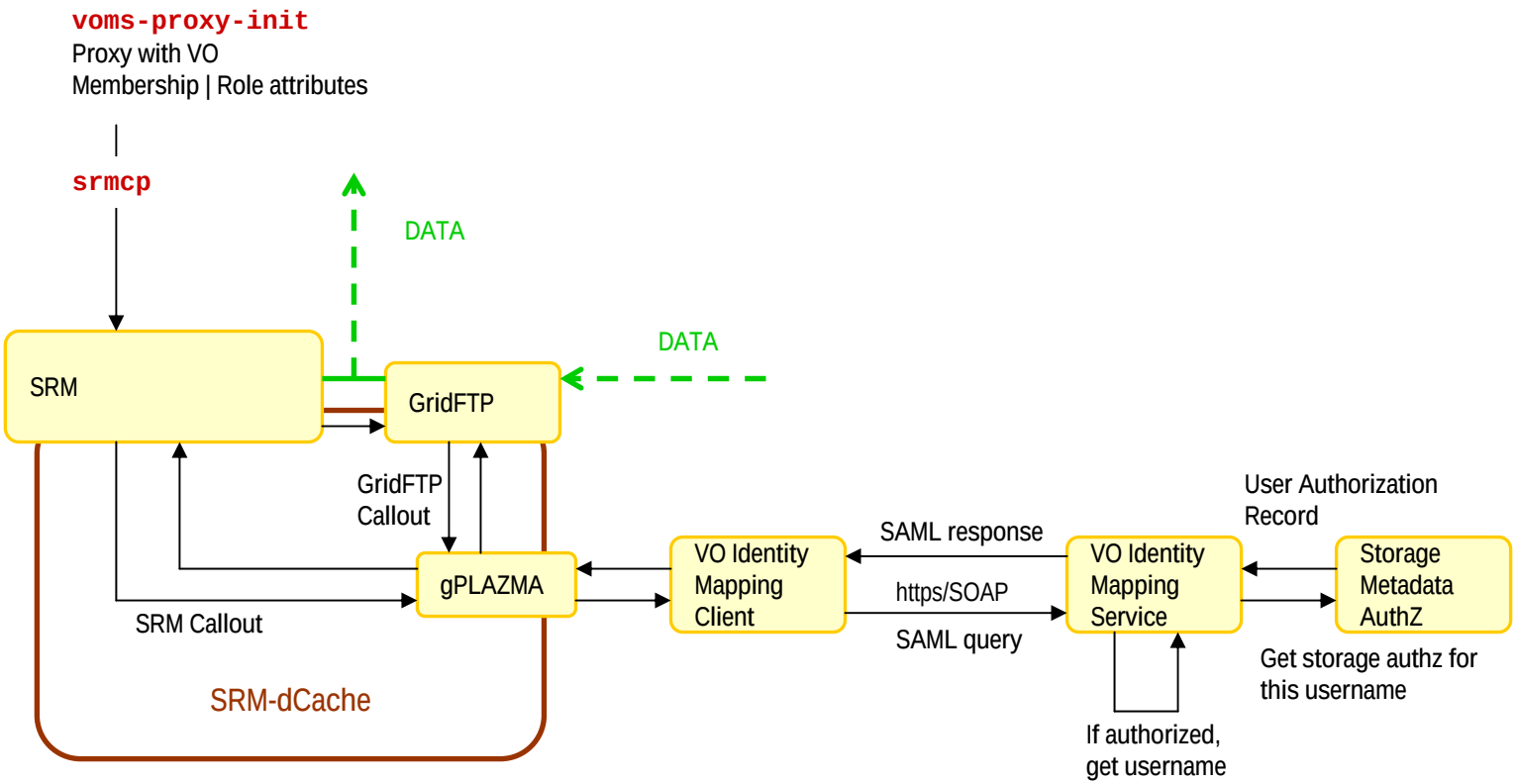
→

```
grid-mapfile = OFF
grid-mapfile-priority = 4

dcache.kpwd = OFF
dcache.kpwd-priority = 1

VO-role-mapping = OFF
VO-role-mapping-priority = 2

gPLAZMA-vo-role-mapping = OFF
gPLAZMA-vo-role-mapping-priority = 3

Unknown-authz-service = OFF
Unknown-authz-service-priority =
```

Authorization and Policy Control Framework in SRM-dCache
Architecture, Design Principles, and Implementation

Abhishek Singh Rana | Timur Perelmutov

An example use case: Fermilab VO-role mapping AuthZ



Authorization and Policy Control Framework in SRM-dCache
Architecture, Design Principles, and Implementation

Abhishek Singh Rana | Timur Perelmutov

Functionality Description

	Legacy AuthN, AuthZ	Fine-grained Security (VO, Roles)	Centralized Management
Built-in Legacy Grid AuthN	✓		(in future)
dCache-SRM Legacy Storage AuthZ	✓		(in future)
FNAL Privilege Project VO Role Mapping AuthZ		✓	✓
Built-in VO Role Mapping AuthZ		✓	(in future)

Abhishek Singh Rana | Timur Perelmutov

References

Open Science Grid Document 96, "*Storage Element Authorization Architecture*", Abhishek Singh Rana and Timur Perelmutov (Eds.), *work in progress and a Draft*, March 2005.

http://computing.fnal.gov/cgi-bin/docdb/osg_public/ShowDocument?docid=96