

AuthZ Interop report out

- > for the authz-interop.org collaboration
David Groep,
with many thanks to Dave Dykstra's CHEP talk

V Participants

- > EGEE
- > VO Services ('Privilege') Project
- > Globus
- > Condor
- > VDT (OSG)

Joint development and definition effort 2007 until early 2009

In production phase as of mid 2008

Institutes:

ANL, BCCS, BNL, FNAL, INFN, Nikhef, Switch, UvA, UWMadison

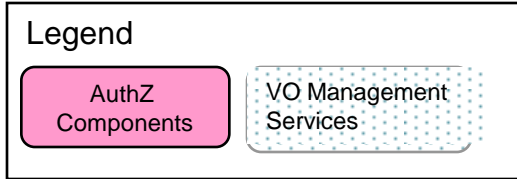
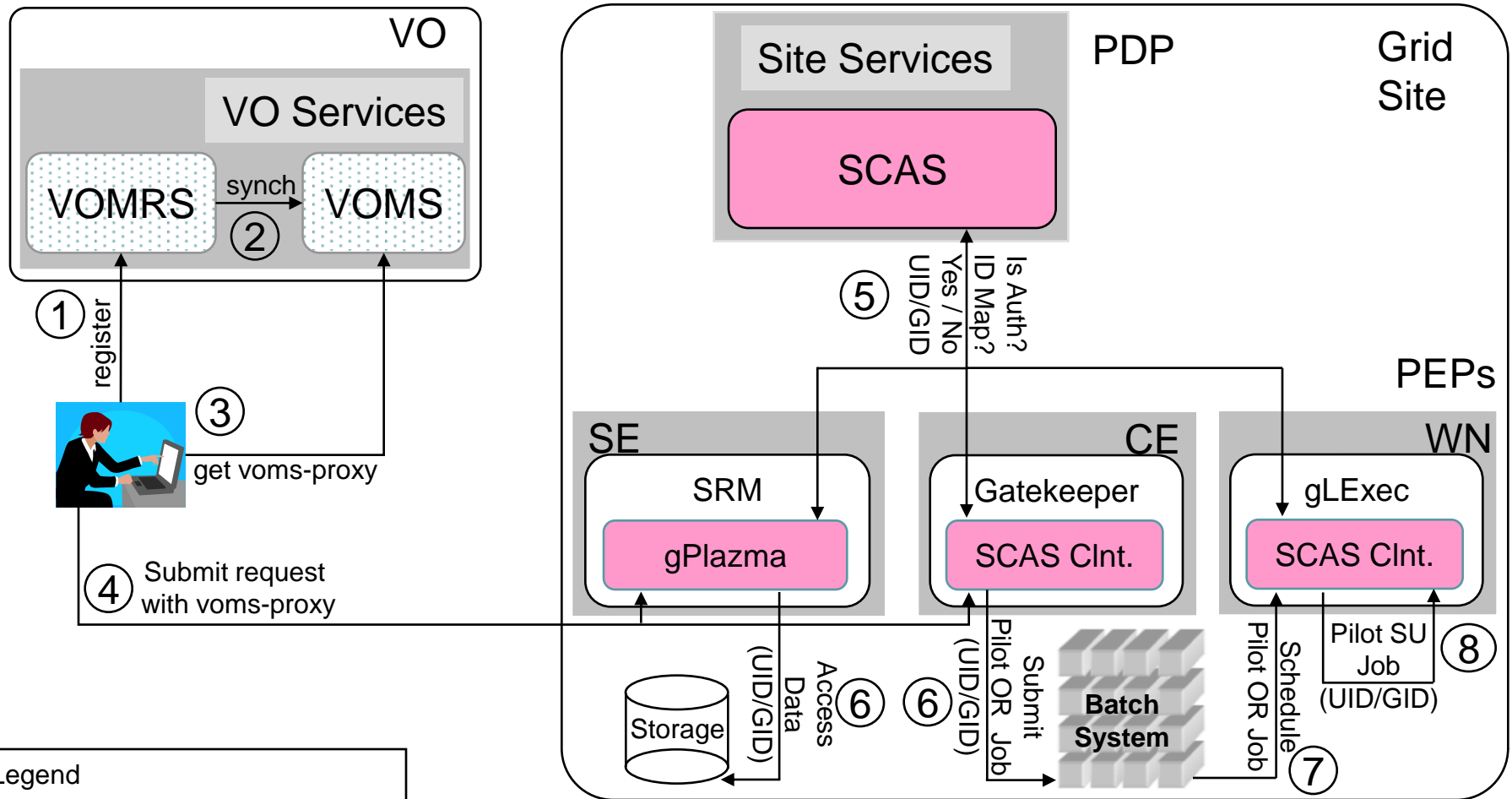
✓ What did we start with?

- > GUMS and PRIMA using proprietary SAML1 based protocol
- > SAZ (authorization service)
- > GT3, GT4 ‘authz callout’ for PRIMA by Markus Lorch
- > LCAS/LCMAPS
- > gLExec
- > gPlazma

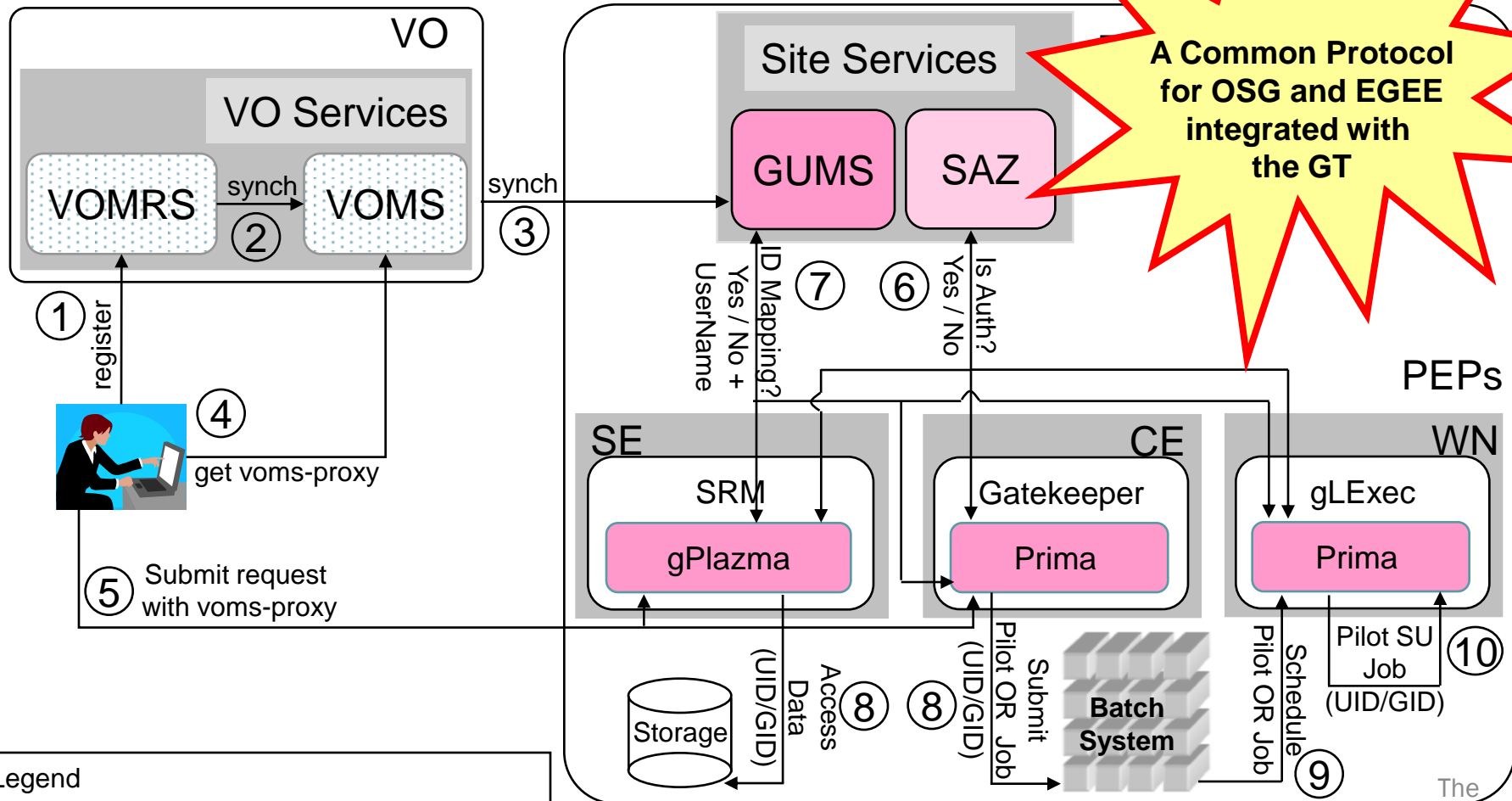
Not only used GUMS and the ‘EGEE’ a different logical model of dealing with attributes and authorization (local VOMS dumps vs. VOMS attribute push)

Also, the services build in one ecosystem (e.g. ‘EGEE’) could not be used in the other (‘OSG’) → hacks and double work

V Original (interim) EGEE scenario plan



OSG Authorization Infrastructure



V Aims of the authz-interop project

- > Provide interoperability within the authorization infrastructures of OSG, EGEE, Globus and Condor

Through

- > Common communication protocol
- > Common attribute and obligation definition
- > Common semantics **and** actual interoperation of production system

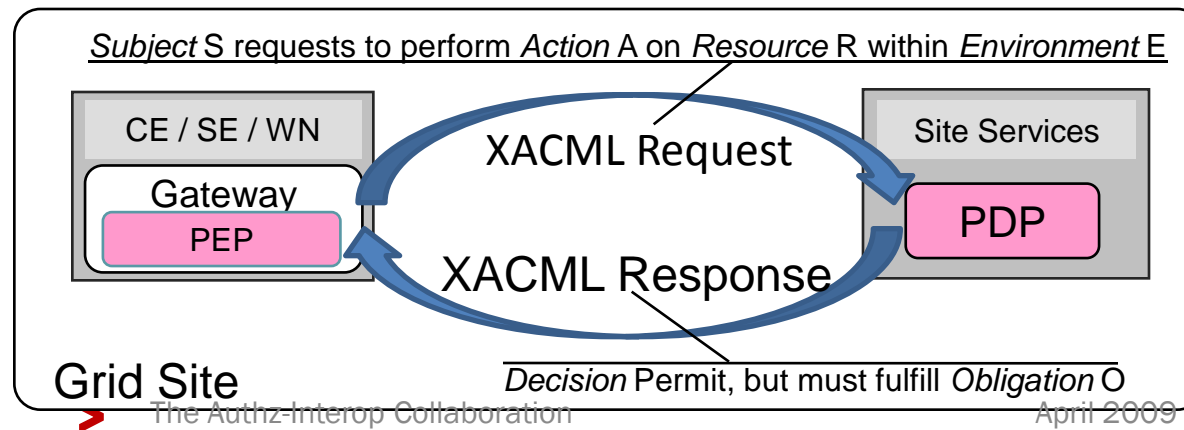
So that services can use either framework and be used in both infrastructures

V Two Elements for interop

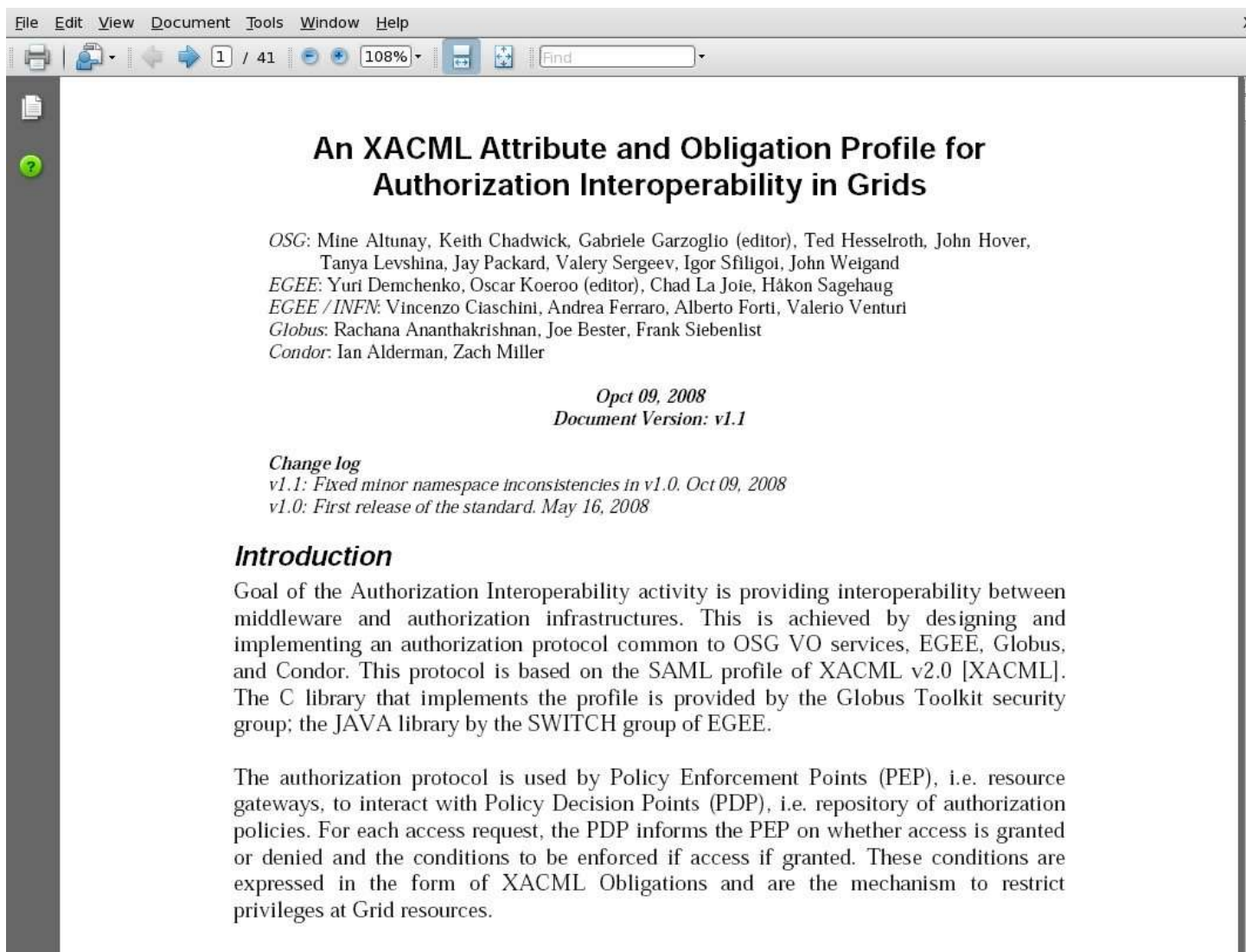
- > Common *communications* profile
 - > Agreed on use of SAML2-XACML2
 - > <http://www.switch.ch/grid/support/documents/xacmlsaml.pdf>
- > Common *attributes and obligations* profile
 - > List and semantics of attributes sent and obligations received between a 'PEP' and 'PDP'
 - > Now at version 1.1
 - > <http://cd-docdb.fnal.gov/cgi-bin/ShowDocument?docid=2952>
 - > <http://edms.cern.ch/document/929867>

V Profile in a nutshell

- > Existing standards:
 - > **XACML** defines the XML-structures that are exchanged with the PDP to communicate the security context and the rendered authorization decision.
 - > **SAML** defines the on-the-wire messages that envelope XACML's PDP conversation.
- > The Authorization Interoperability profile augments those standards:
 - > standardize names, values and semantics for common-obligations and core-attributes such that our applications, PDP-implementations and policy do interoperate.



An XACML AuthZ Interop Profile



The screenshot shows a PDF document viewer window with the following content:

An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids

OSG: Mine Altunay, Keith Chadwick, Gabriele Garzoglio (editor), Ted Hesselroth, John Hover, Tanya Levshina, Jay Packard, Valery Sergeev, Igor Sfiligoi, John Weigand
EGEE: Yuri Demchenko, Oscar Koeroo (editor), Chad La Jote, Håkon Sagehaug
EGEE / INFN: Vincenzo Ciaschini, Andrea Ferraro, Alberto Forti, Valerio Venturi
Globus: Rachana Ananthkrishnan, Joe Bester, Frank Siebenlist
Condor: Ian Alderman, Zach Miller

Opct 09, 2008
Document Version: v1.1

Change log
v1.1: Fixed minor namespace inconsistencies in v1.0. Oct 09, 2008
v1.0: First release of the standard. May 16, 2008

Introduction

Goal of the Authorization Interoperability activity is providing interoperability between middleware and authorization infrastructures. This is achieved by designing and implementing an authorization protocol common to OSG VO services, EGEE, Globus, and Condor. This protocol is based on the SAML profile of XACML v2.0 [XACML]. The C library that implements the profile is provided by the Globus Toolkit security group; the JAVA library by the SWITCH group of EGEE.

The authorization protocol is used by Policy Enforcement Points (PEP), i.e. resource gateways, to interact with Policy Decision Points (PDP), i.e. repository of authorization policies. For each access request, the PDP informs the PEP on whether access is granted or denied and the conditions to be enforced if access is granted. These conditions are expressed in the form of XACML Obligations and are the mechanism to restrict privileges at Grid resources.

> Authorization Interoperability Profile based on the SAML v2 profile of XACML v2

> Result of a 1yr collaboration between OSG, EGEE, Globus, and Condor

> Releases:
v1.1 → 10/09/08
v1.0 → 05/16/08

V Structure of the AuthZ Interop Profile

- Namespace prefix: *http://authz-interop.org/xacml*

Request Attribute Identifiers

- > Subject: *<ns-prefix>/subject/<subject-attr-name>*
- > Action: *<ns-prefix>/action/<action-attr-name>*
- > Resource: *<ns-prefix>/resource/<resource-attr-name>*
- > Environment: *<ns-prefix>/environment/<env-type>*

Obligation Attribute Identifiers

- ObligationId: *<ns-prefix>/obligation/<obligation-name>*
- AttributeId: *<ns-prefix>/attributes/<obligation-attr-name>*

V Most Common Request attributes

- > **Subject** (see profile doc for full list)
 - > Subject-X509-id
 - String: OpenSSL DN notation
 - > Subject-VO
 - String: "CMS"
 - > VOMS-FQAN
 - String: "/CMS/VO-Admin"

- > **Resource** (see doc for full list)
 - > Resource-id (enum type)
 - CE / SE / WN
 - > Resource X509 Service Certificate Subject
 - resource-x509-id
 - > Host DNS Name
 - Dns-host-name

- > **Action**
 - > Action-id (enum type)
 - Queue / Execute-Now / Access (file)
 - > Res. Spec. Lang.
 - RSL string

- > **Environment**
 - > PEP-PDP capability negot.
 - PEP sends to PDP supported Obligations
 - Enables upgrading of the PEPs and PDPs independently
 - > Pilot Job context (pull-WMS)
 - Pilot job invoker identity
 - Policy statement example: "User access to the WN execution environment can be granted only if the pilot job belongs to the same VO as the user VO"

see document for all attributes and obligations

V Most Common Obligation Attributes

> UIDGID

- > UID (integer): Unix User ID local to the PEP
- > GID (integer): Unix Group ID local to the PEP

> Secondary GIDs

- > GID (integer): Unix Group ID local to the PEP (Multi recurrence)

> Username

- > Username (string): Unix username or account name local to the PEP.

> Path restriction

- > RootPath (string): a sub-tree of the FS at the PEP
- > HomePath (string): path to user home area (relative to RootPath)

> Storage Priority

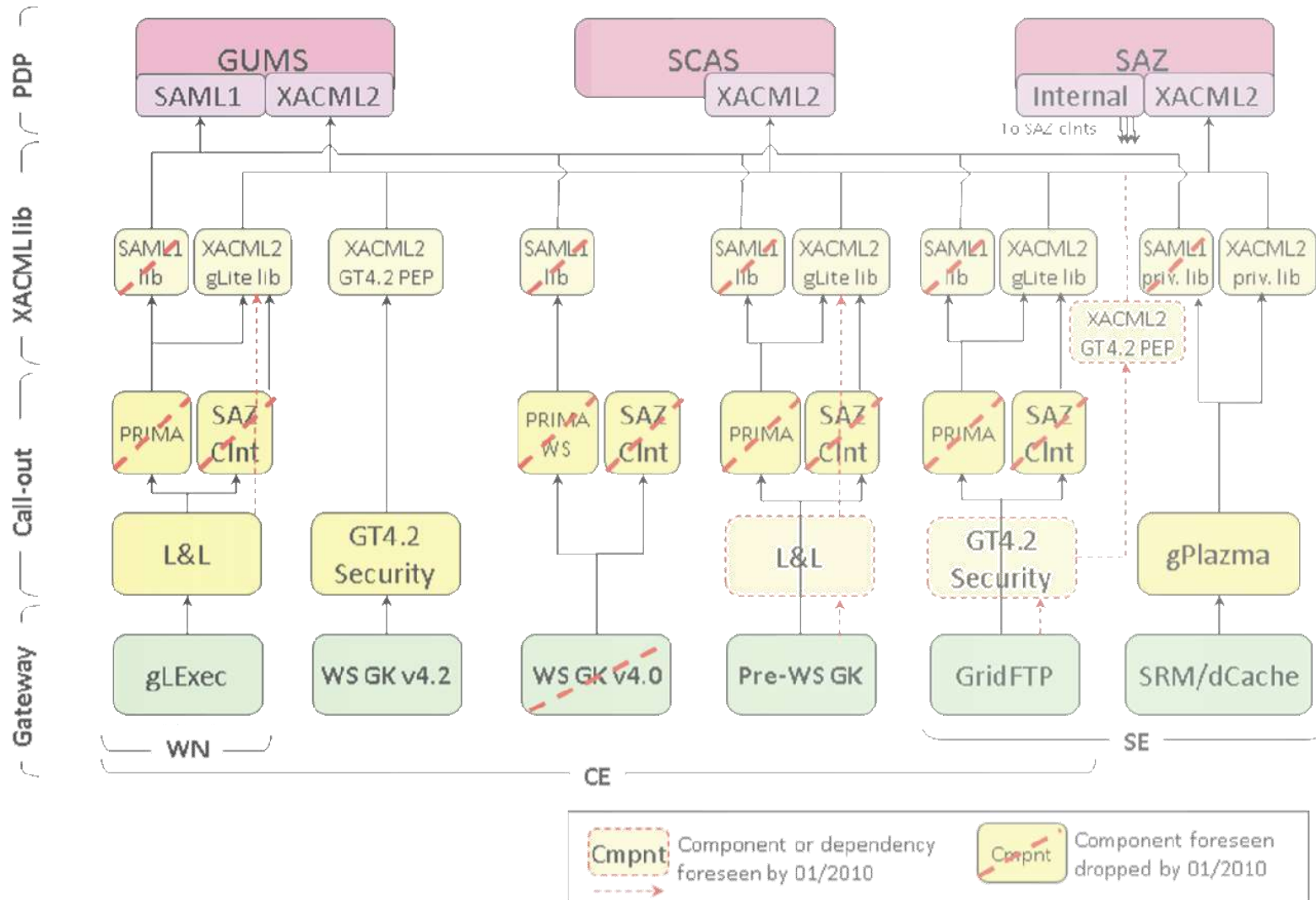
- > Priority (integer): priority to access storage resources.

> Access permissions

- > Access-Permissions (string): “read-only”, “read-write”

see document for all attributes and obligations

Full interoperability



✓ What has been achieved now

- > All profiles written and implemented
- > Common libraries available in Java and C implementing the communications protocol
- > Common handlers for Joint Interoperable Attribute and Obligations
- > Integrated in all relevant middleware in EGEE and OSG:
 - > Clients: lcg-CE (via LCMAPS scasclient), CREAM and gLExec (ditto), GT pre-WS gram (both prima and LCMAPS), GT GridFTP, GT4.2 WS-GRAM, dCache/SRM
 - > Servers: GUMS, SCAS
- > Other (lower-prio) components in progress
 - > SAZ, RFT, GT4.x native-AuthZ, Condor (& -G), BeStMan

V OSG Integration Test Results

Component	Test	PDP Component		
		Old GUMS	New GUMS	SCAS
WS-Gatekeeper (Out of Scope)	Test call-out component	NO	YES	YES
	Run job w/o Delegation or File Transfer	NO	YES	out of scope
	Run job with Delegation and File Transfer	NO	YES	out of scope
SCAS / PRIMA cmd line tool (OOS)	AuthZ call via Legacy protocol call-out	YES	YES	NO
	AuthZ call via XACML protocol call-out	NO	YES	YES
Pre-WS Gatekeeper (VTB-TESTED)	Run job. AuthZ via Legacy protocol	YES	YES	NO
	Run job. AuthZ via XACML protocol	NO	YES	YES
GridFTP (VTB-TESTED)	Transfer file. AuthZ via Legacy protocol	YES	YES	NO
	Transfer file. AuthZ via XACML protocol	NO	YES	YES
gLExec (REL. Jan 20)	Run pilot job. AuthZ via Legacy protocol	YES	YES	NO
	Run pilot job. AuthZ via XACML protocol	NO	YES	YES
SRM/dCache gPlazma (REL. Jan 20)	Transfer file. AuthZ via Legacy protocol	YES	YES	NO
	Transfer file. AuthZ via XACML protocol	NO	YES	YES

✓ Latest news

- > dCache v1.9.2-4 has been released this week. Pre-release tests have been conducted successfully against GUMS and SCAS. Will be the recommended release in a few months!
 - > What are the EGEE deployment plans?
- > Development of native authz XACML call-out module for GridFTP: tests with the Globus Toolkit call-out module for authorization speaking the interop protocol start this week

V What next?

Keeping interop (in 'maintenance mode') is most important!

- > Continued software support from contributing partners
- > Interdependency in timing between OSG and GT may lead to Catch-22 in prioritizing native GT4.2 implementation
 - > Support in Delegation Service and RTF is needed for full production, and before existing legacy solutions can be phased out
- > Continued close coordination on the specification of the Authorization Profile. New uses cases **must** be coordinated and **no** 'proprietary' extensions should added, as that breaks the interop. Continuous communications and coordination remains essential.

V Conclusions

- > EGEE, OSG, Globus, and Condor have collaborated since Feb 2007 on an Authorization Interoperability profile and implementation
- > Interoperability is achieved through an AuthZ Interop Profile, based on the SAML v2 profile of XACML v2
- > Call-out module implementations are integrated with major Resource Gateways
- > The major advantages of the infrastructure are:
 - > Software developed in the US or EU can seamlessly be deployed in the EU or US security infrastructures
 - > Software groups in EGEE and OSG can share and reuse common code
- > Production deployments in OSG and EGEE