

An XACML profile and implementation for Authorization Interoperability between OSG and EGEE

Overview

- OSG & EGEE Authorization Models
- Authorization Interoperability Profile
- Implementations and Deployments

Mar 26, 2009

On behalf of the Authorization Interoperability Collaboration

Dave Dykstra

Computing Division, Fermilab

The Collaboration

Ian Alderman⁹

Mine Altunay¹

Rachana

Ananthakrishnan⁸

Joe Bester⁸

Keith Chadwick¹

Vincenzo Ciaschini⁷

Yuri Demchenko⁴

Andrea Ferraro⁷

Alberto Forti⁷

Gabriele Garzoglio¹

David Groep²

Ted Hesselroth¹

John Hover³

Oscar Koeroo²

Chad La Joie⁵

Tanya Levshina¹

Zach Miller⁹

Jay Packard³

Håkon Sagehaug⁶

Valery Sergeev¹

Igor Sfiligoi¹

Neha Sharma¹

Frank Siebenlist⁸

Valerio Venturi⁷

John Weigand¹

¹ *Fermilab, Batavia, IL, USA*

² *NIKHEF, Amsterdam, The Netherlands*

³ *Brookhaven National Laboratory, Upton, NY, USA*

⁴ *University of Amsterdam, Amsterdam, The Netherlands*

⁵ *SWITCH, Zürich, Switzerland*

⁶ *BCCS, Bergen, Norway*

⁷ *INFN CNAF, Bologna, Italy*

⁸ *Argonne National Laboratory, Argonne, IL, USA*

⁹ *University of Wisconsin, Madison, WI, USA*

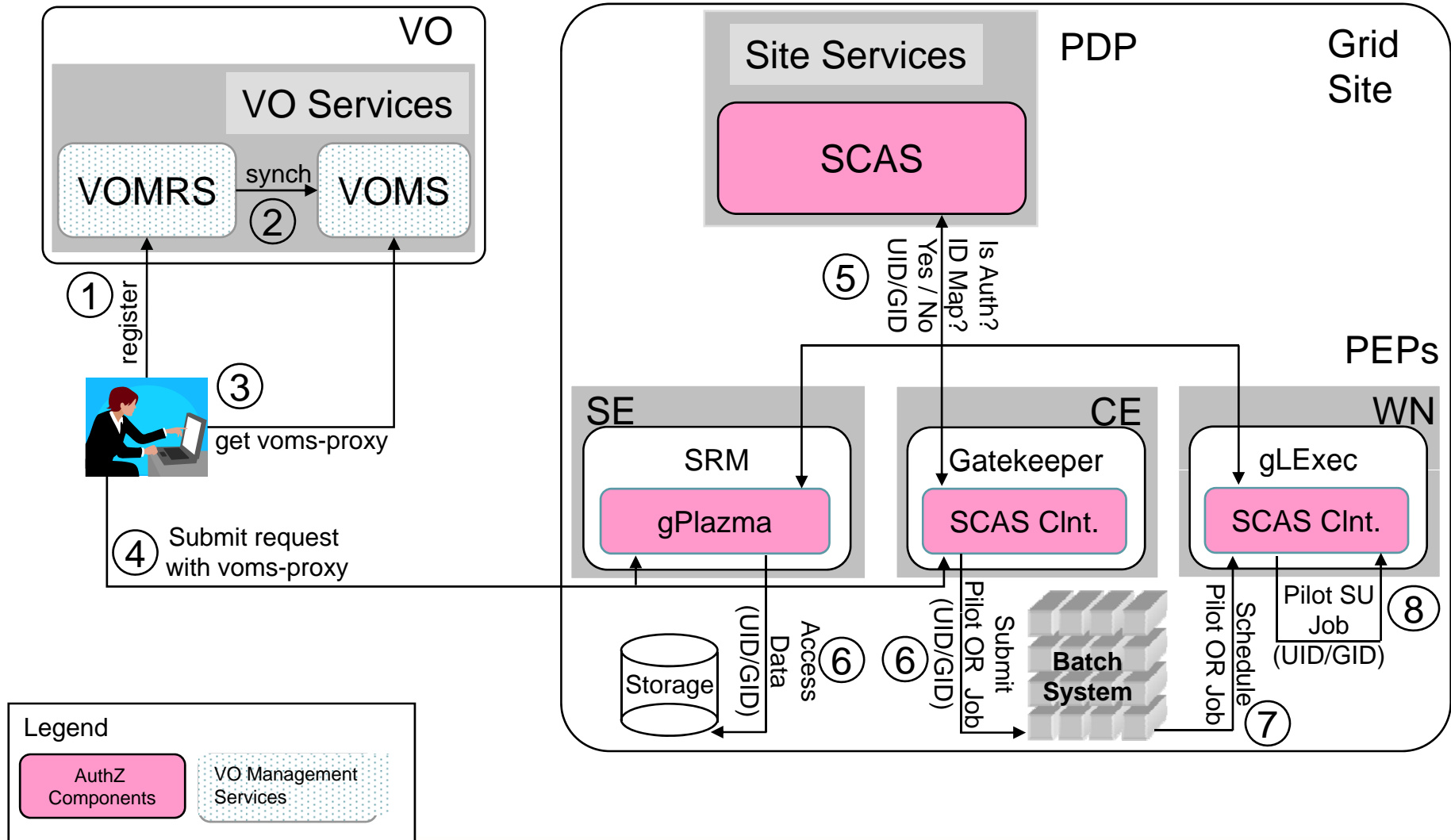
The Authorization Model

- The EGEE and OSG security model is based on **X509** end entity and proxy **certificates** for single sign-on and delegation
- Role-based access to resources is based on **VOMS Attribute Certificates**
- Users **push credentials** and **attributes** to resources
- Access **privileges** are granted with appropriate **local identity mappings**
- Resource gateways (Gatekeeper, SRM, gLExec, ...) i.e. Policy Enforcement Points (**PEP**) **call-out** to site-central Policy Decision Points (**PDP**) for authorization decisions

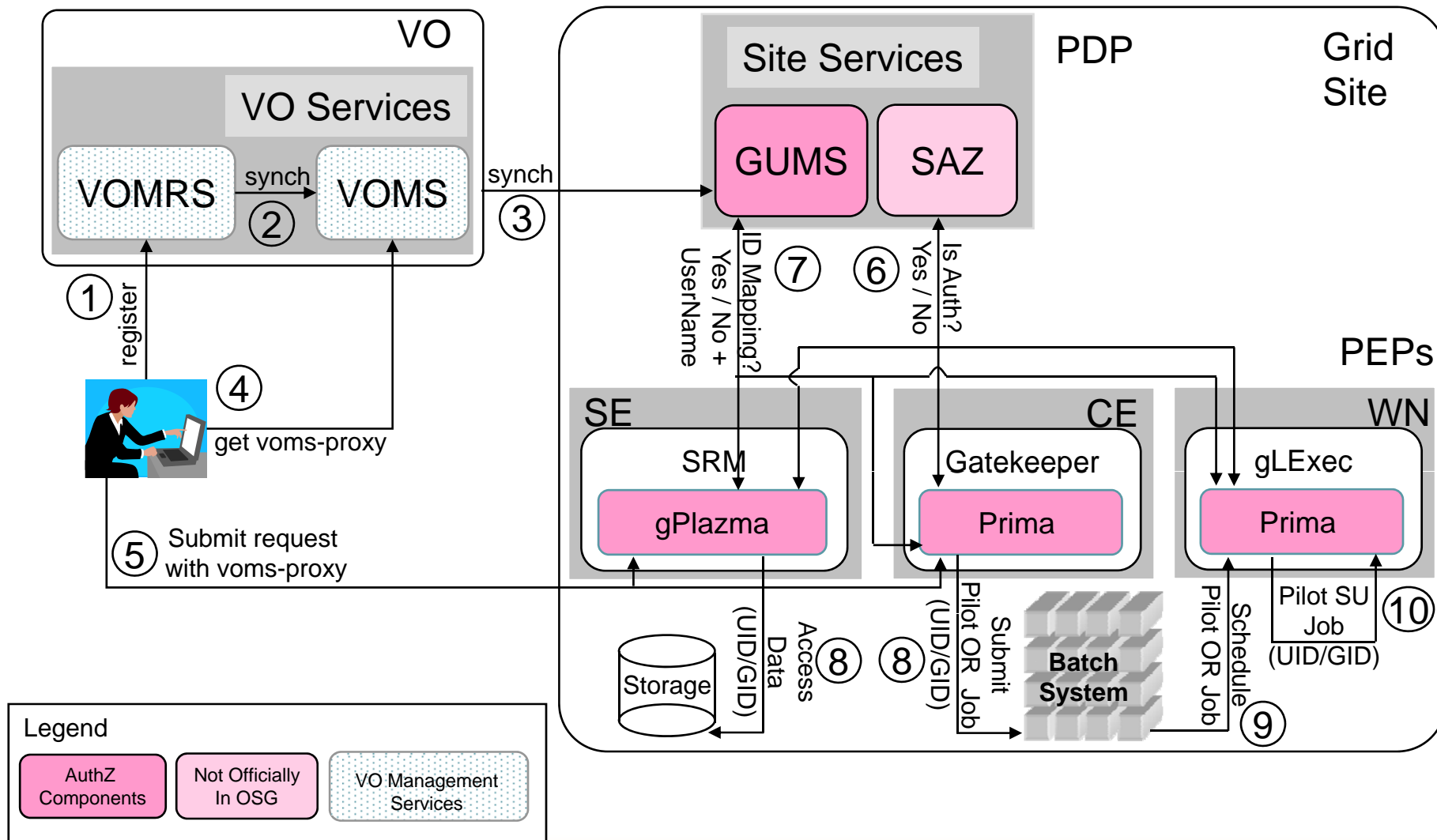
The Interoperability Problem

- **EGEE** and **OSG** had developed **different authorization infrastructures**
- The two Grids now have a **common PEP to PDP call-out protocol** to enable interoperability:
 - 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
- The common call-out protocol was developed in **collaboration** with the **Globus Toolkit** and **Condor** groups

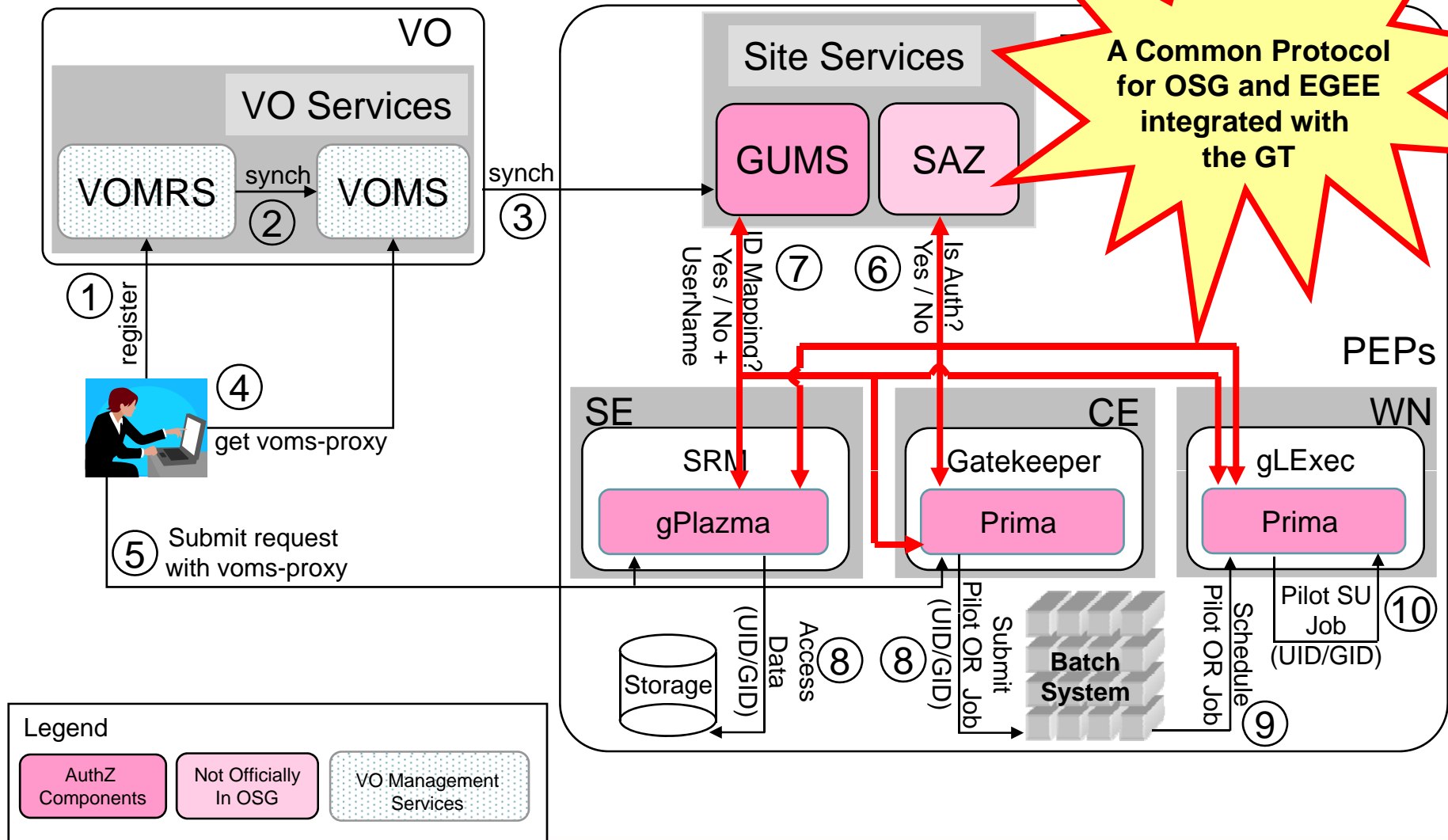
Authorization Infrastructure (the EGEE case)



Authorization Infrastructure (the OSG case)



Authorization Infrastructure (the OSG case)



An XACML profile and implementation for Authorization Interoperability between OSG and EGEE

Overview

- ✓ OSG & EGEE Authorization Models
- **Authorization Interoperability Profile**
- Implementations and Deployments

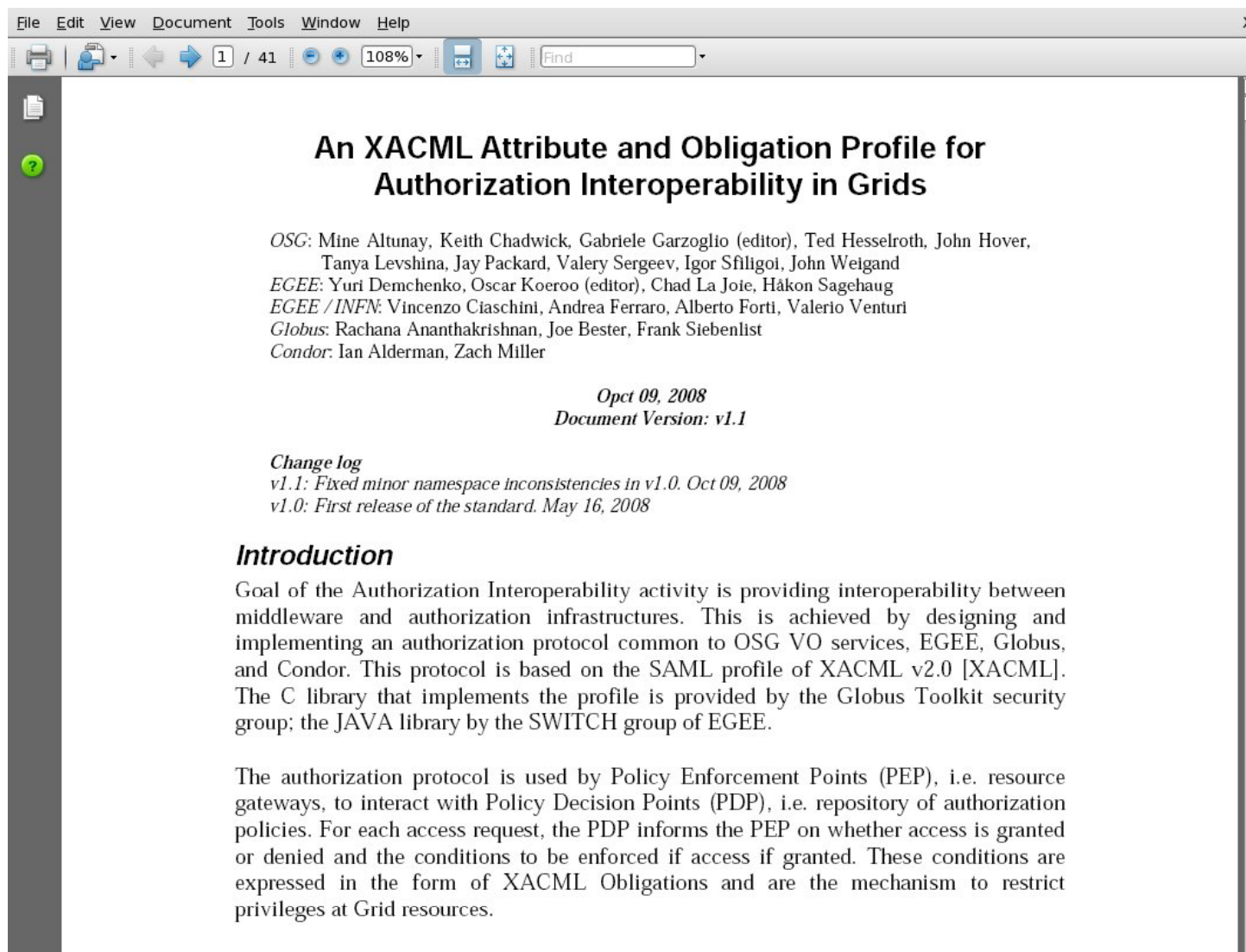
Mar 26, 2009

On behalf of the Authorization Interoperability Collaboration

Dave Dykstra

Computing Division, Fermilab

An XACML AuthZ Interop Profile



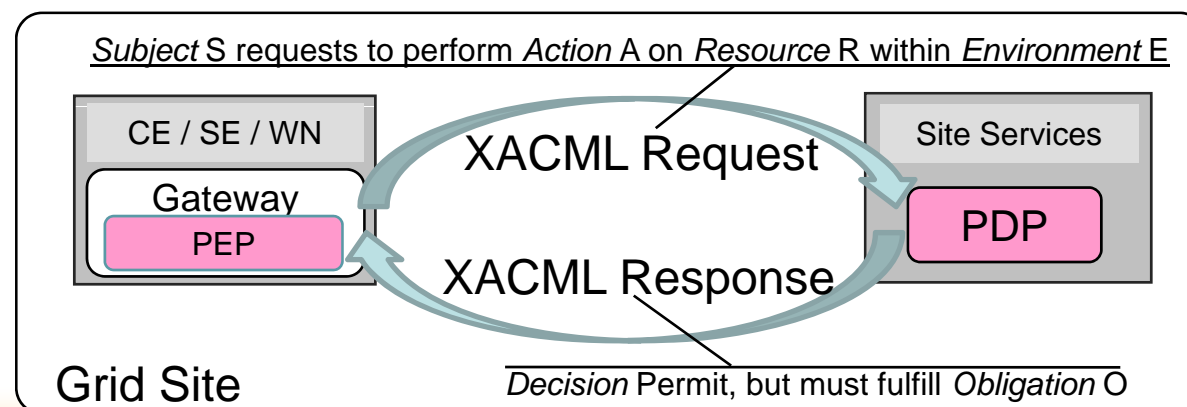
- Authorization Interoperability Profile based on the SAML v2 profile of XACML v2

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

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

SAML, XACML, AuthZ Interop 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.



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>*

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”

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”

An XACML profile and implementation for Authorization Interoperability between OSG and EGEE

Overview

- ✓ OSG & EGEE Authorization Models
- ✓ Authorization Interoperability Profile
- **Implementations and Deployments**

Mar 26, 2009

On behalf of the Authorization Interoperability Collaboration

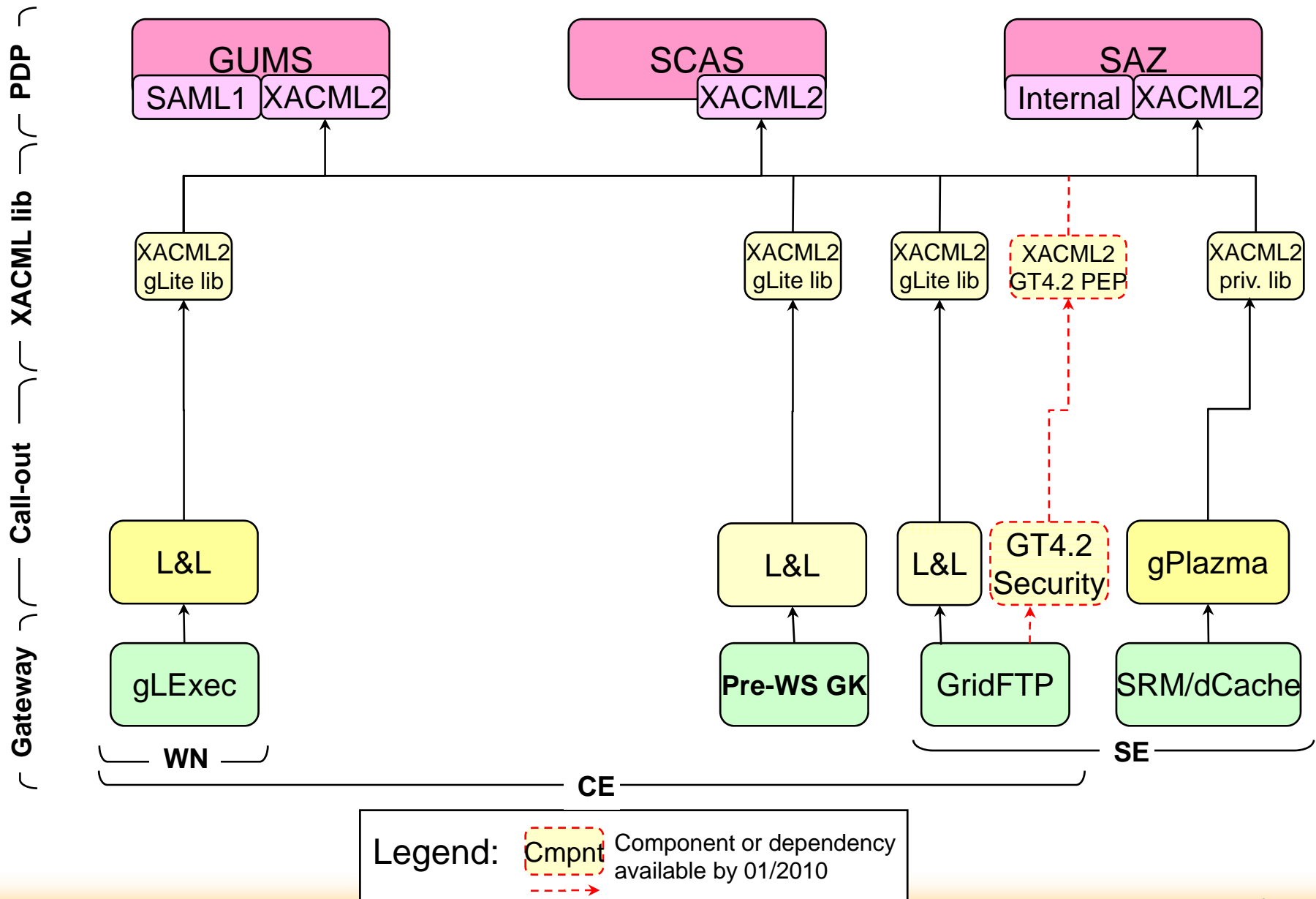
Dave Dykstra

Computing Division, Fermilab

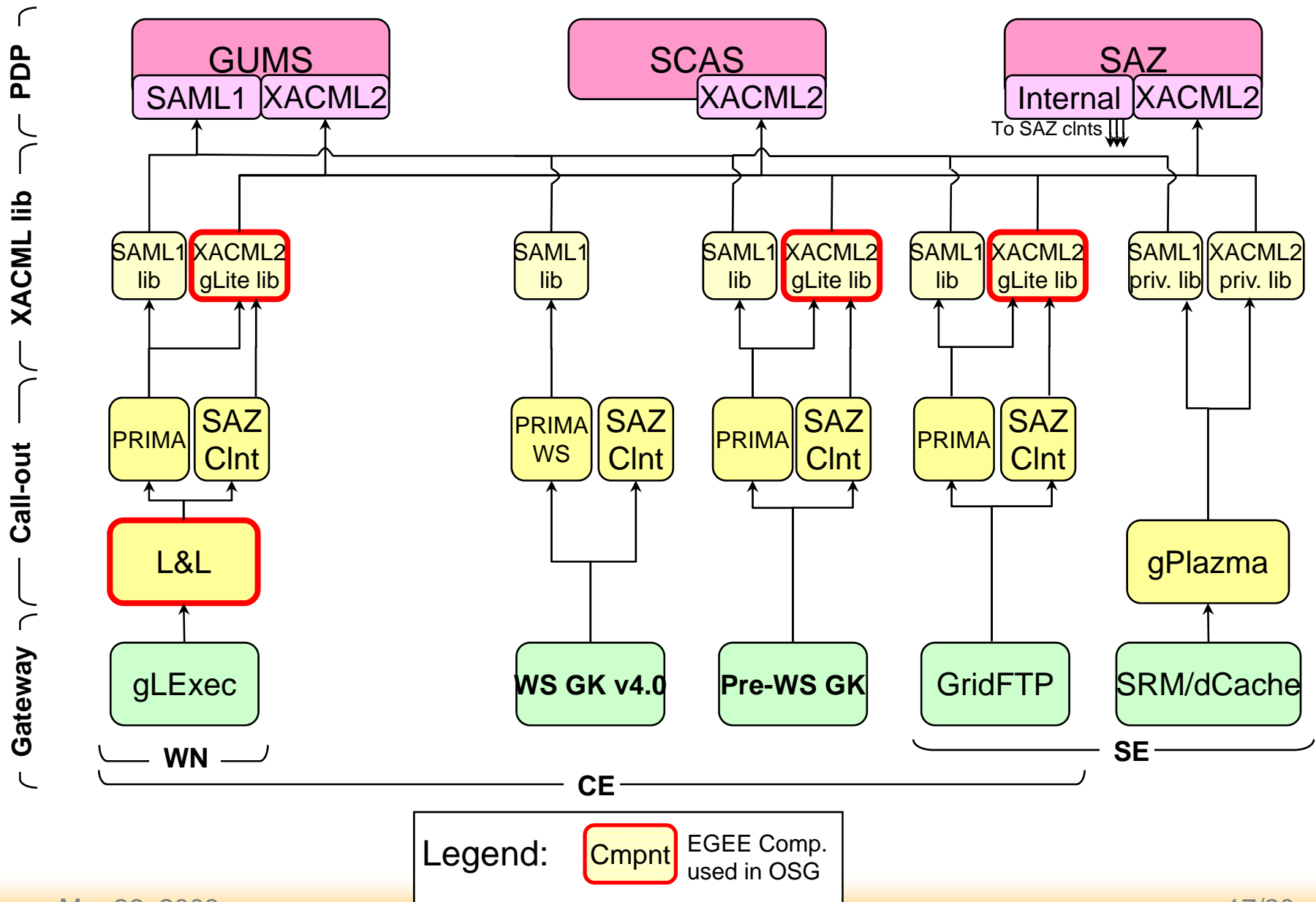
Implementation

- SAML-XACML libraries
 - OpenSAML (Java); Globus XACML (C)
- Authorization Modules
 - XACML messages within a SOAP envelope over SSL transport
 - LCAS / LCMAPS (L&L) / SCAS plug-in (EGEE); PRIMA / gPlazma plug-in (OSG)
- Resource Gateways
 - Computing Element
 - Pre-WS Gatekeeper; WS-Gatekeeper (native call-out)
 - Storage Element
 - SRM / dCache; BeStMan; GridFTP (native call-out in progress)
 - Worker Node
 - gLExec

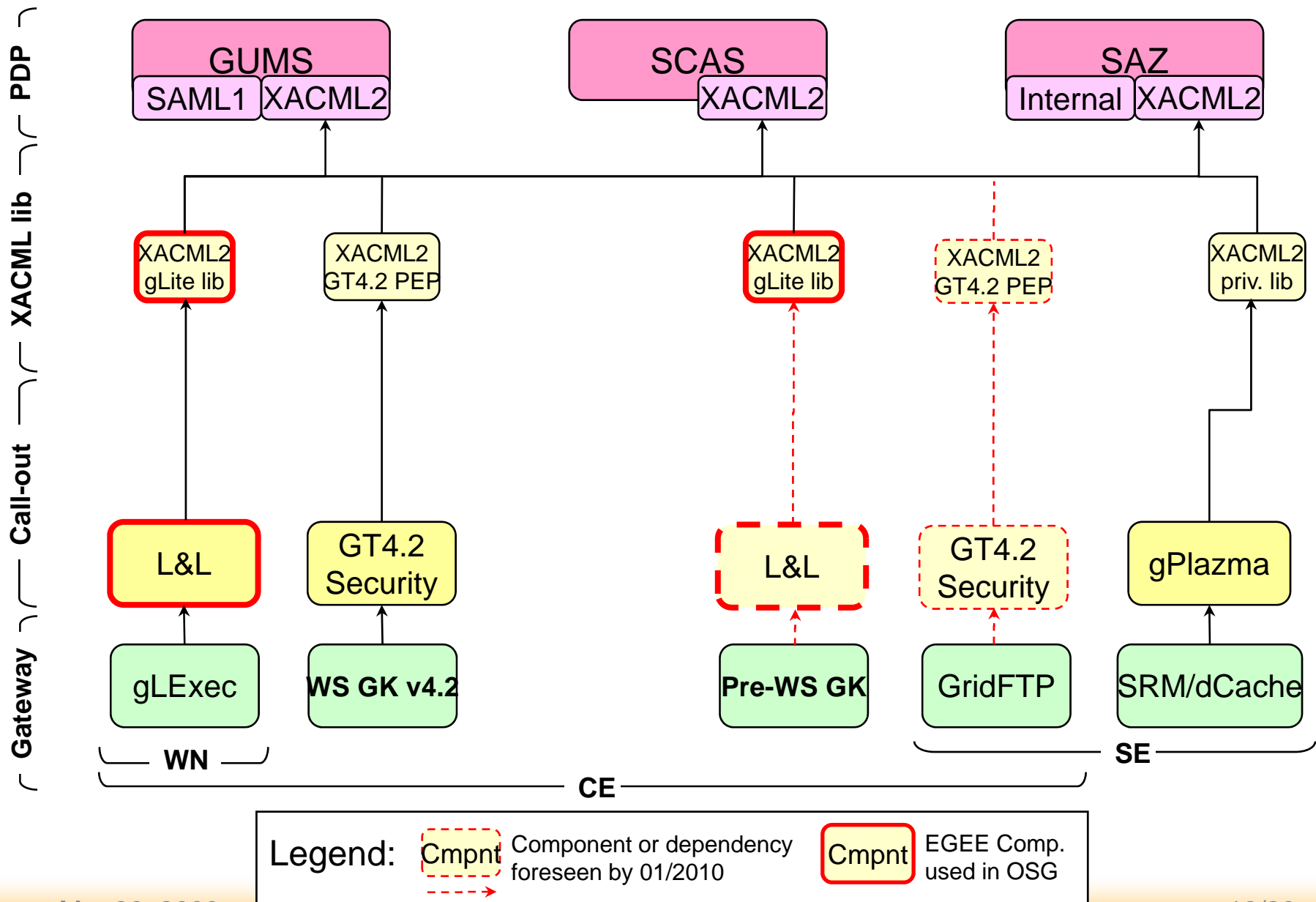
Module Dependencies (EGEE case)



Module Dependencies (OSG case)



Module Dependencies (OSG case in 2010)



Deployments

- The EGEE certification process is focusing on SCAS and gLExec. gLExec passed certification.
- EGEE Pre-Production Sites (PPS) are involved. gLExec/SCAS deployed in production at Nikhef.
- OSG Integration Test Bed (ITB) will certify the software stack for production at the end of March.
- OSG production is deploying the infrastructure as an Update to OSG v1.0 in April.

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 are under way in OSG and EGEE

Additional Slides

Related Work

- The goal of the **Authorization Interoperability** collaboration is to provide a **common PEP to PDP call-out** protocol between **OSG, EGEE**, and major software providers, such as **Globus** and **Condor**
- The Open Grid Service Architecture (**OGSA**) **Authorization Working Group (WG)** in **OGF** defines the **specifications** needed to allow for **pluggable** and **interoperable authorization** components from **multiple authorization domains** in the **OGSA framework**.
- The **scope** of **OGSA-AuthZ WG** is **broader** and includes interoperability across several authorization standards.
- Several **members** of **our collaboration** also **participate** in the **OGSA-AuthZ WG**

Subject attributes (1)

- Subject-X509-id
 - String: OpenSSL oneline notation of the DN
- Subject-X509-Issuer
 - String: OpenSSL oneline notation of the Issuer DN
- Subject-Condor-Canonical-Name-id
 - String: “user@host[.domain]”
- Subject-VO
 - String: “gin.ggf.org”
- VOMS-signing-subject
 - String: OpenSSL oneline notation
- VOMS-signing-issuer
 - String: OpenSSL oneline notation
- VOMS-FQAN
 - String: “/gin.ggf.org/APAC/VO-Admin”
- VOMS-Primary-FQAN
 - String: “/gin.ggf.org/APAC/VO-Admin”

Subject attributes (2) - Optional

- Certificate-Serial-Number
 - Integer: 42
- CA-serial-number
 - Integer: 1
- Subject End-Entity X509v3 Certificate Policies OID
 - String: “1.2.840.113612.5.2.4” (Robot Certificate)
- Cert-Chain
 - base64Binary: “*MIICbjCCAVagA.....*”
- VOMS-dns-port
 - String: “kuiken.nikhef.nl:15050”

Action attributes

- Action-type: 'action-id' (enumerated type)
 - Queue
 - Requesting execution to a (remote) queue.
 - Execute-Now
 - Requesting direct execution (remotely)
 - Access (file)
 - Request for (generic) file access
- Action-specific attributes
 - Resource Specification Language
 - RSL string

Resource attributes

- Resource-type: 'resource-id' (enumerated type)
 - CE (Computing Element)
 - Can also be the head-node or entry point to a cluster
 - WN (Worker Node)
 - A node type that will process jobs, typically in a cluster
 - SE (Storage Element)
 - (Logical) storage facility or specific storage node
- Resource-specific attributes
 - Resource X509 Service Certificate Subject
 - resource-x509-id
 - Resource X509 Service Certificate Issuer
 - resource-x509-issuer
 - Host DNS Name
 - Dns-host-name

Environment attributes

- PEP-PDP capability negotiation - Supported Obligations
 - PEP sends to PDP a list of the supported obligations
 - The PDP can choose to return an appropriate set of obligations from this list
 - Allows upgradeability of the PEPs and PDPs independently by deploying new functionalities step by step
- Pilot Job context
 - To support pull-based job management model
 - 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”
 - Pilot job invoker identity
 - These attributes define the identity of the pilot job invoker

Obligations (1)

- **UIDGID**
 - UID (integer): Unix User ID local to the PEP
 - GID (integer): Unix Group ID local to the PEP
 - Stakeholder: Common
 - Must be consistent with: Username
- **Multiple Secondary GIDs**
 - Multi recurrence
 - GID (integer): Unix Group ID local to the PEP
 - Stakeholder: EGEE
 - Needs obligation(s): UIDGID
- **Username**
 - Username (string): Unix username or account name local to the PEP.
 - Stakeholder: OSG
 - Must be consistent with: UIDGID

Obligations (2)

- **AFSToken**

- AFSToken (string) in base64: AFS Token passed as a string
- Stakeholder: EGEE
- Needs obligation(s): UIDGID

- **Path restriction (root-and-home-paths)**

- RootPath (string): this parameter defines a sub-tree of the whole file system available at the PEP.
- HomePath (string): this parameter defines the path to home areas of the user accessing the PEP. This is a path relative to RootPath.
- Stakeholder: OSG
- Needs obligation(s): UIDGID or Username

Obligations (3)

- **Storage Priority**

- Priority (integer): an integer number that defines the priority to access storage resources.
- Stakeholder: OSG
- Needs obligations: UIDGID or Username

- **Access permissions**

- Access-Permissions (string): Access permissions to a file that is requested
- Allowed values: “read-only”, “read-write”
- Stakeholder: OSG
- Needs obligations: UIDGID or Username

OSG Integration Tests

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