# Einbindung eines externen PDP in die Globus-basierte TextGrid-Infrastruktur

**Peter Gietz, Stefan E. Funk,**

**Markus Widmer, Martin Haase,**

**DAASI International GmbH**

**D-Grid Security-Workshop 2010,**

**Göttingen 29.-30.09.2010**

**Gefördert vom:**

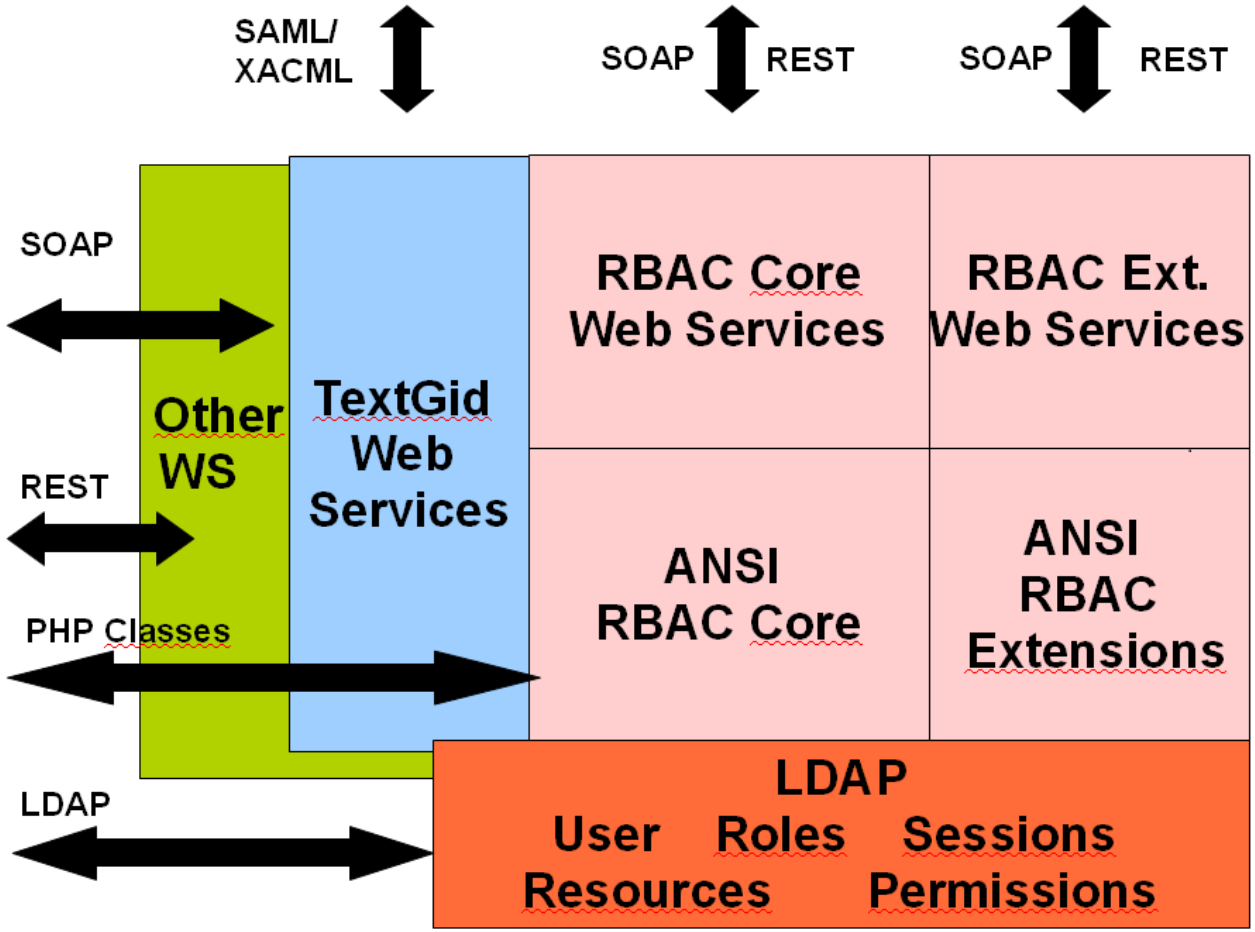
Bundesministerium
für Bildung
und Forschung

# TextGrid

- TextGrid entwickelt eine Virtuelle Forschungsumgebung für Geisteswissenschaftler, augenblicklich für Editionsphilologen, Linguisten, Musikwissenschaftler und Kunsthistoriker
- Das **TextGridLab** bietet Zugriff auf fachwissenschaftliche Werkzeuge, Services und Inhalte
  - GUI über Eclipse Rich Client (RCP) und verteilte als WebServices realisierte Werkzeuge
  - Workbench beliebig über neue Web Services erweiterbar
- Das **TextGridRep** ist ein im Grid verteiltes Repository für geisteswissenschaftliche Forschungsdaten und zielt auf langfristige Verfügbarkeit und Zugänglichkeit
  - TG-auth* für Autorisierung und Authentifizierung (Shibboleth und RBAC)
  - TG-search: XML-Datenbank für Metadaten und Volltexte, RDF-Datenbank für Relationen
  - TG-crud Service (create/retrieve/update/delete)

  Autorisiert Nutzer via SID, speichert Daten im Grid, Zugriff über JavaGAT auf Globus Toolkit

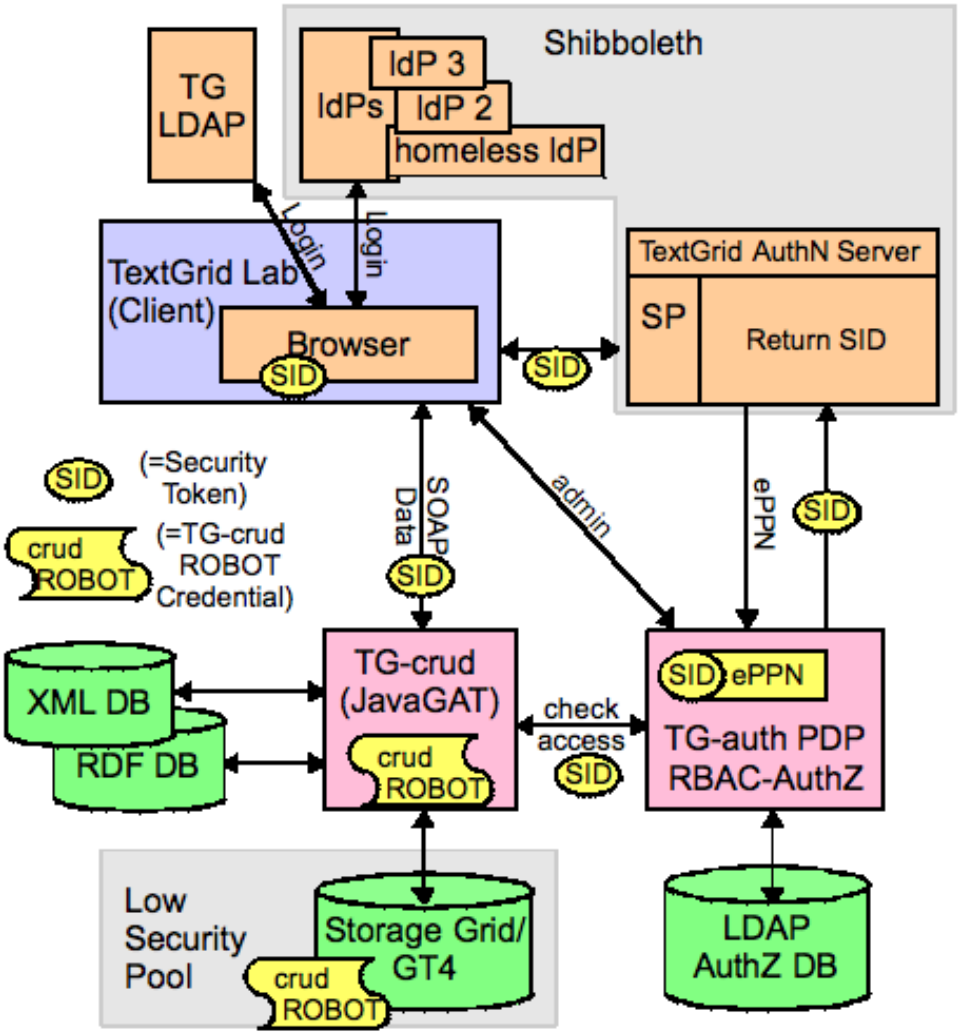
# TextGrid-PDP mit OpenRBAC



# Szenarien für Einbindung eines externen PDP

1. Kontaktierung des PDP über TG-Crud (unabhängig von Globus)
   - E-Mail-Verifikation (TextGrid LDAP) / Shibboleth-Authentifizierung
   - TG-crud authentifizier sich im Grid  über ROBOT-Zertifikat
   - Augenblicklicher Status Quo
2. Zusätzl. Mapping der PDP-Policy auf POSIX ACLs
   - Shibboleth-Authentifizierung und SLC (Short Lived Credential)
   - Userrechte werden auf Dateiebene durchgesetzt
   - ROBOT-Zertifikat wird nur noch für anonyme Zugriffe verwendet
3. Zusätzl. direkte Kontaktierung des PDP durch Globus (XACML-Callout)
   - Shibboleth-Authentifizierung und SLC (Short Lived Credential)
   - Userrechte werden auf Globus-Ebene durchgesetzt

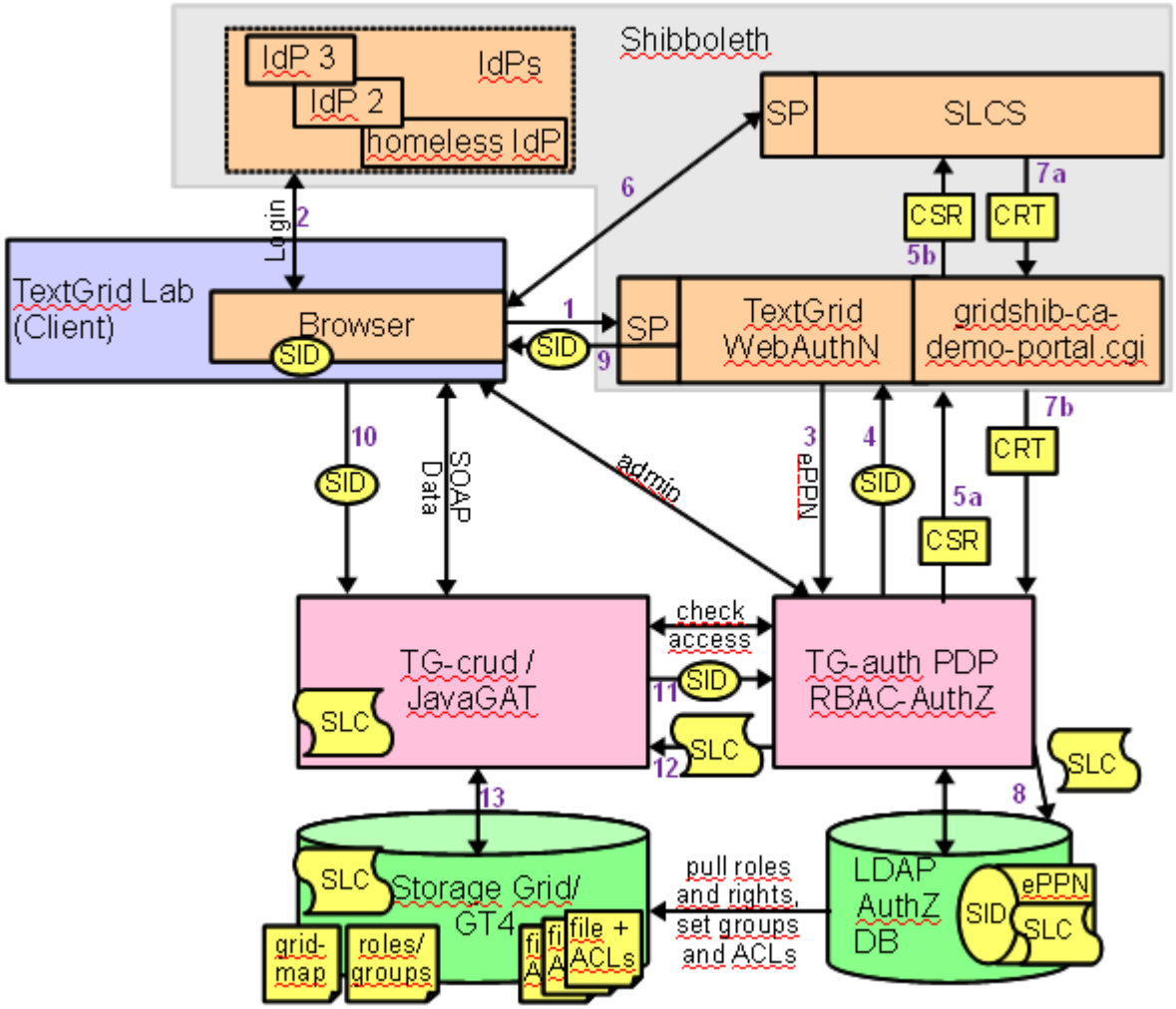
# Szenario 1 – Architektur



# Szenario 2 – POSIX-ACLS

- Nutzer authentifiziert sich über Shibboleth (TG-auth*)
- TG-auth* generiert Schlüssel und SLC-Zertifikat-Request (private key ist nur im RAM, nicht auf Festplate)
- Portal leitet Request an SLCS weiter, SLCS signiert SLC
- signiertes Zertifikat wird im TG-auth* abgelegt
- TG-crud holt sich SLC von TG-auth*
- Daten werden im Heimat-Verzeichnis des SLC-Nutzers abgelegt
- Zugriffsrechte werden von TG-auth* (RBAC) in das Dateisystem der Grid-Middleware gemappt (ACLs)

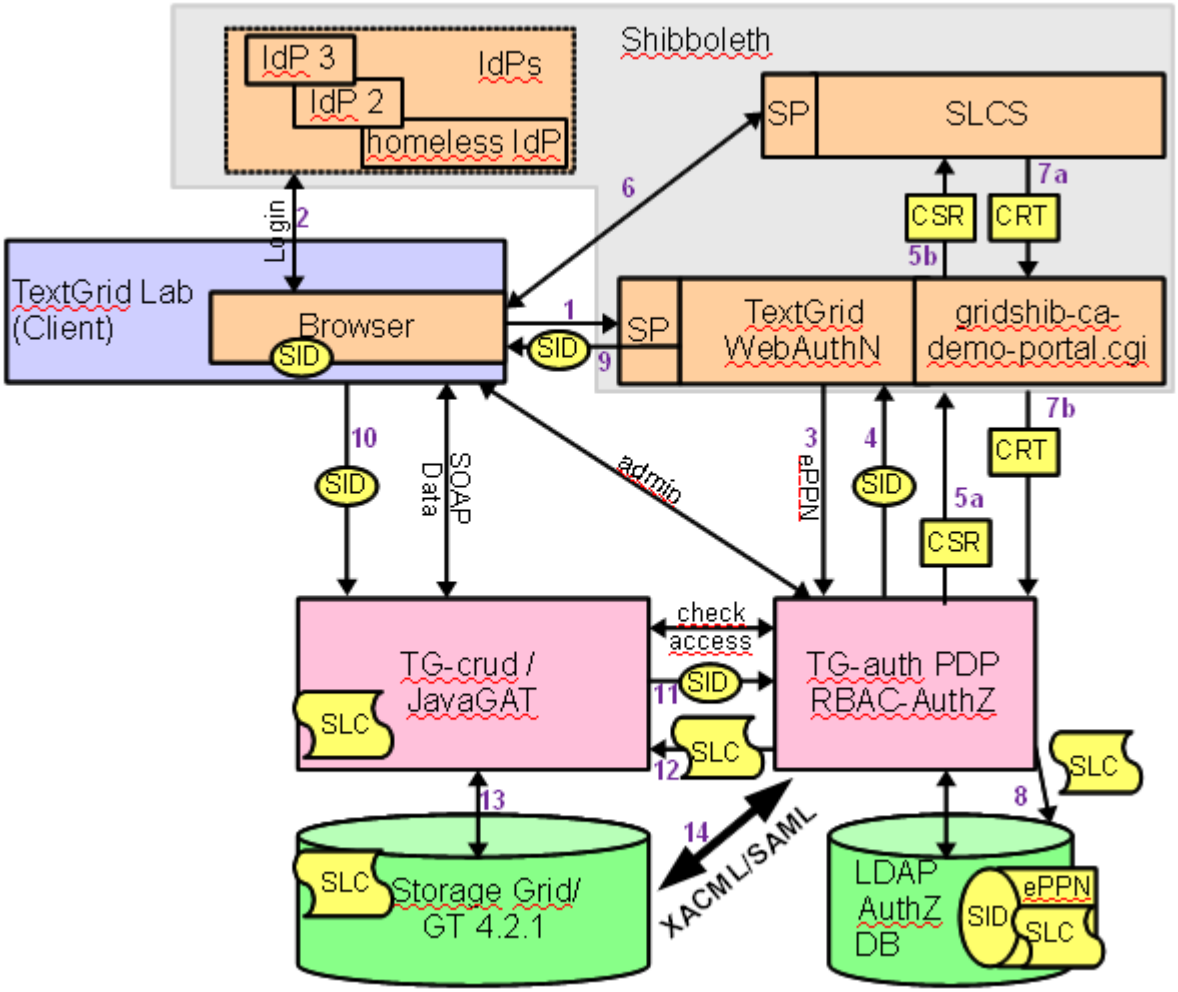
# Szenario 2 – Architektur



# Szenario 3 – XACML-SAML

- SLCs wie in Szenario 2
- Daten werden ebenso im Heimat-Verzeichnis des SLC-Nutzers abgelegt
- Zugriffsrechte werden von Globus als PEP direkt bei TG-auth* als PDP über das XACML-SAML-Request-Response-Protokoll abgefragt, wobei folgendes mitgegeben wird:
  - Subject-DN aus dem Zertifikat
  - Name der Ressource (Datei)
  - gewünschte Operation für Zugriff
- Auf Dateiebene erhält Globus über Gruppenzugehörigkeit alle Rechte auf die von ihm verwalteten Ressourcen

# Szenario 3 – XACML-SAML



# Bewertung

- Vorteile Szenario 2 und 3:
  - Ressource weiß, welcher Nutzer was macht
  - Gridknoten müssen nicht einzeln konfiguriert werden sondern können zentral über einen PDP verwaltet werden
- Nachteil Szenario 2:
  - Replikation der ACLs benötigt Root-Rechte
  - Nicht alle Policyregeln des PDP sind in ACLs abbildbar
    - z.B. keine delete permission
- Vorteile Szenario 3:
  - Es findet keinerlei zeitverzögerte Replikation statt (weder Gridmapfile noch ACLs)
  - Alle Regeln sind prinzipiell abbildbar, der gesamte Funktionsumfang von RBAC kann genutzt werden

# Vielen Dank!

## Gibt es jetzt Fragen?

- Wenn Sie später Fragen haben:

  peter.gietz@daasi.de

- Links:

  http://www.openrbac.de

  http://www.textgrid.de

  http://gap-slc.awi.de/

  http://www.daasi.de