

AAI in TextGrid

Peter Gietz, Martin Haase, Markus Widmer
DAASI International GmbH

IVOM-Workshop
Hannover, 19. 2. 2008

DAASI
International

Directory Applications
for Advanced Security
and Information Management



TEXT
GRID

GEFÖRDERT VOM

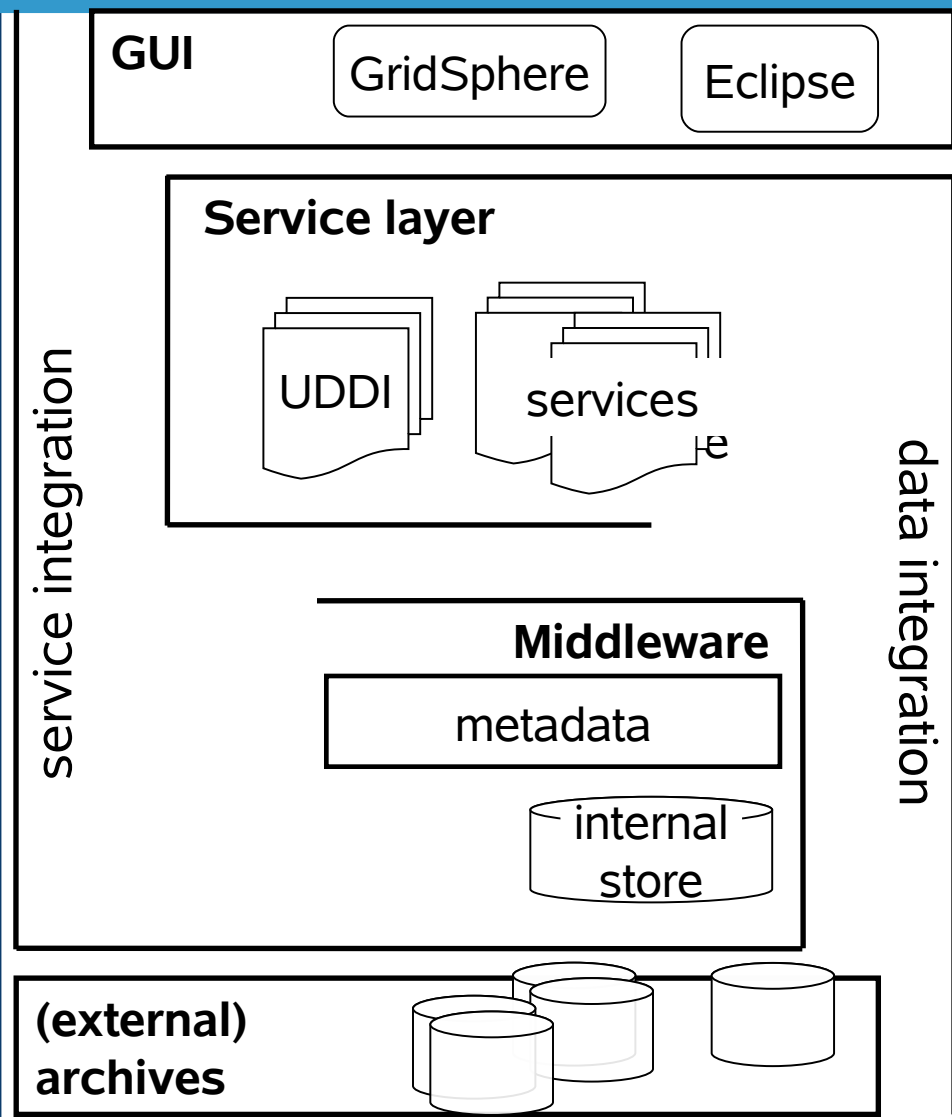


Bundesministerium
für Bildung
und Forschung

- Anforderungen von TextGrid
- Architektur
- AAI
- TextGrid und IVOM

- Virtuelle Forschungsumgebung
 - Zunächst für Textwissenschaftler und Lexikographen
 - Weitere Zielgruppen: Linguisten, Historiker und Kulturwissenschaftler
 - Benutzer haben keine Zertifikate
- Generische Plattform für wissenschaftliche Textverarbeitung, Text-Retrieval und -Analyse
- Zugriff auf verteilte Ressourcen
- Konzept für Projekt und Projektrollen

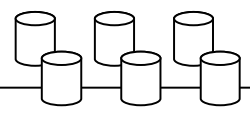
- Eclipse-basierte grafische Benutzerschnittstelle
- Service-Infrastruktur
 - Werkzeugkasten für kollaboratives Arbeiten
 - als SOA implementiert
 - Möglichkeit der Integration projektexterner Werkzeuge über SOAP/WSDL
- Workflow Management
- Data Grid
 - virtuelles Archiv für nachhaltige Datenhaltung
 - Replikation der Daten
- Authentifizierung und Benutzerattribute über die DFN-AAI-Föderation
- Rollenbasierte Authorisierung



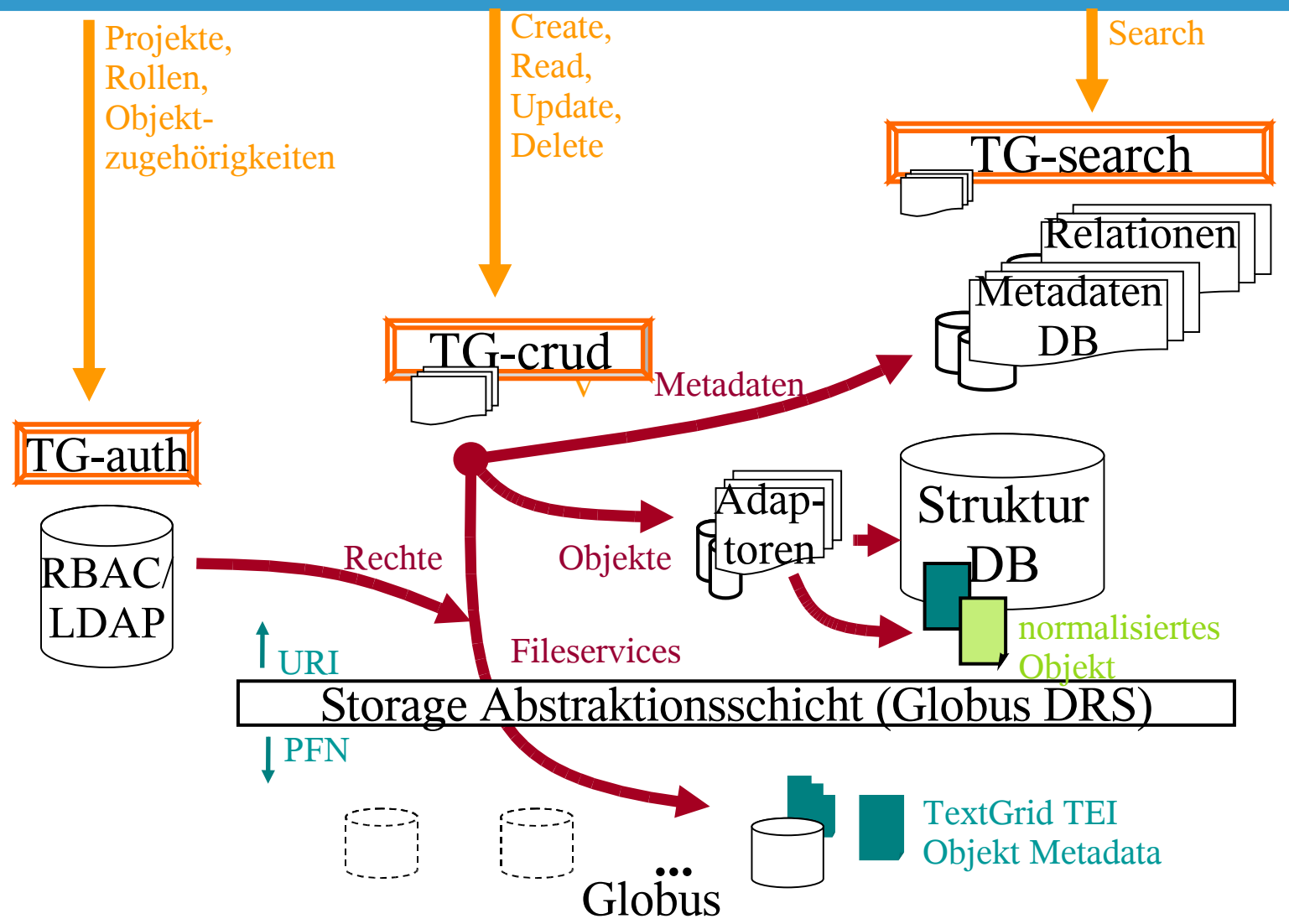
Interfaces

Services

Middleware

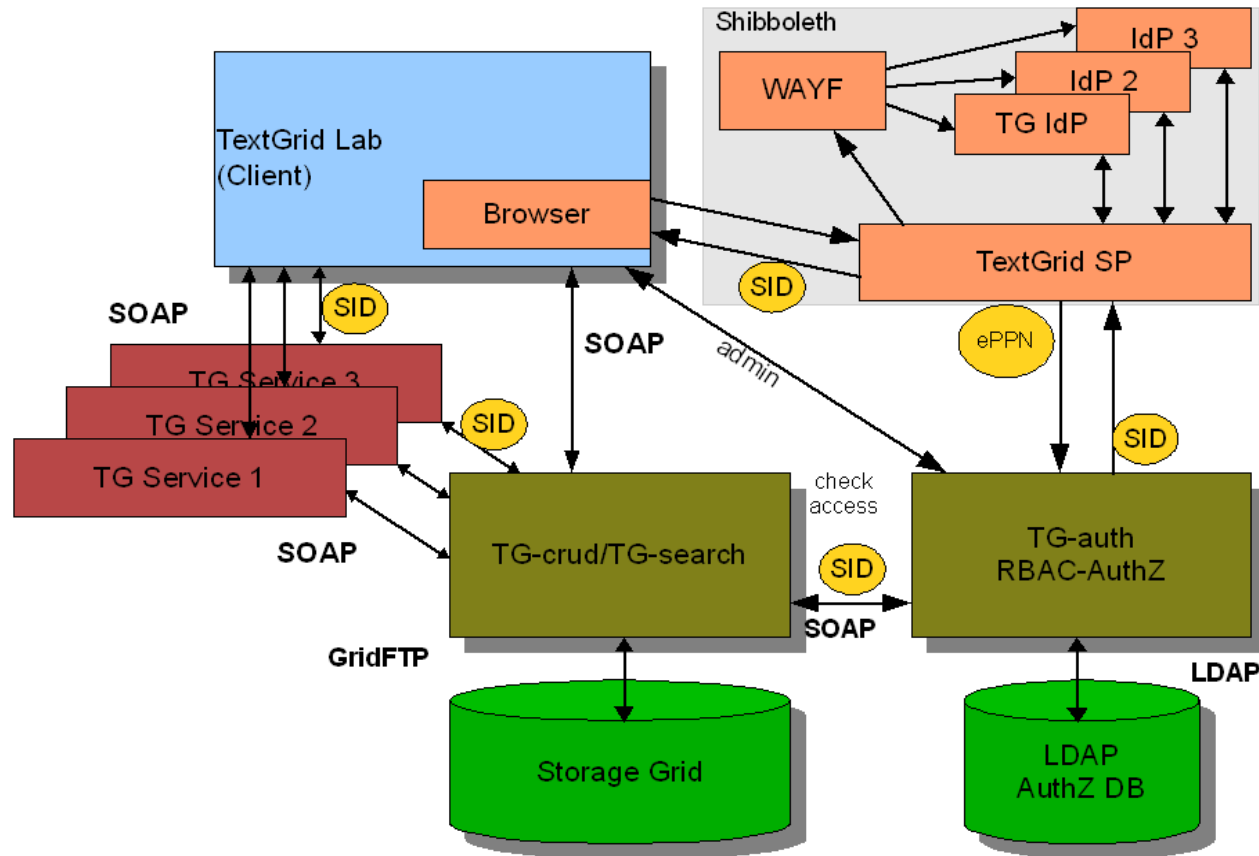


Archives

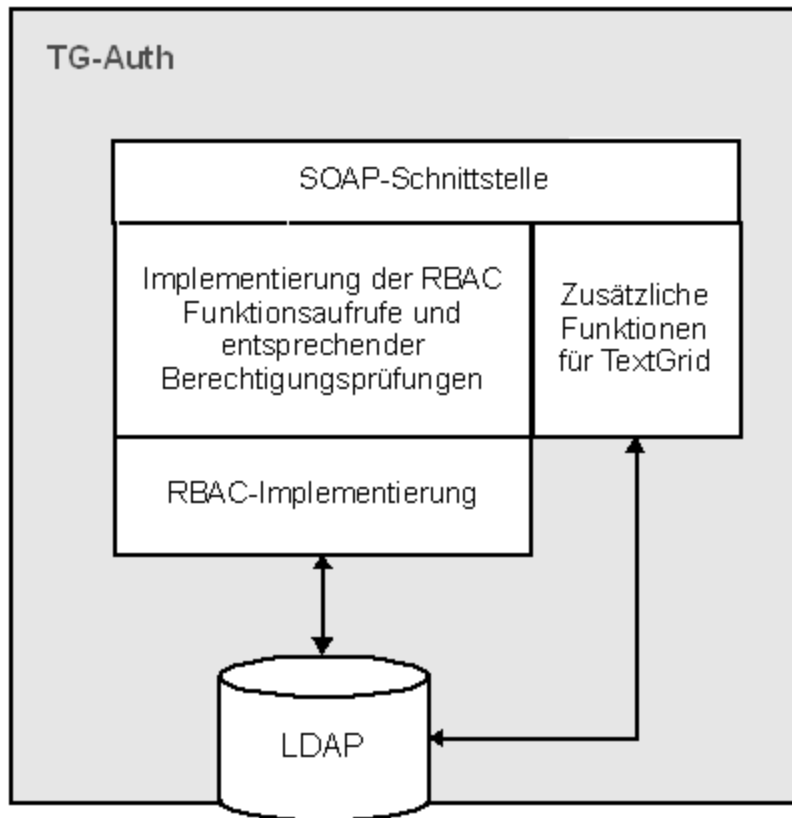


- **Projektleiter:** oberste administrative Funktion über ein Projekt. Einem Projektleiter ist es gestattet, Teilnehmer in das Projekt aufzunehmen, diese aus dem Projekt zu entfernen, Berechtigungen an projektinternen Texten zu verändern und administrative Funktionen zu delegieren.
- **Administrator:** übernimmt wie die Rolle des Projektleiters administrative Aufgaben. Ein Administrator kann Berechtigungen an Texten ändern, und hat ebenso wie der Verfasser eines Textes das Recht, diesen zu schreiben oder zu löschen.
- **Bearbeiter:** verleiht das Recht, neue Texte anzulegen, eigene zu ändern und projektinterne Texte zu lesen.
- **Beobachter:** eine rein passive Rolle in einem Projekt. Wer diese Rolle innehat, darf im Normalfall alle Texte des Projekts lesen, sofern es nicht durch einen Administrator oder einen Projektleiter untersagt wird.

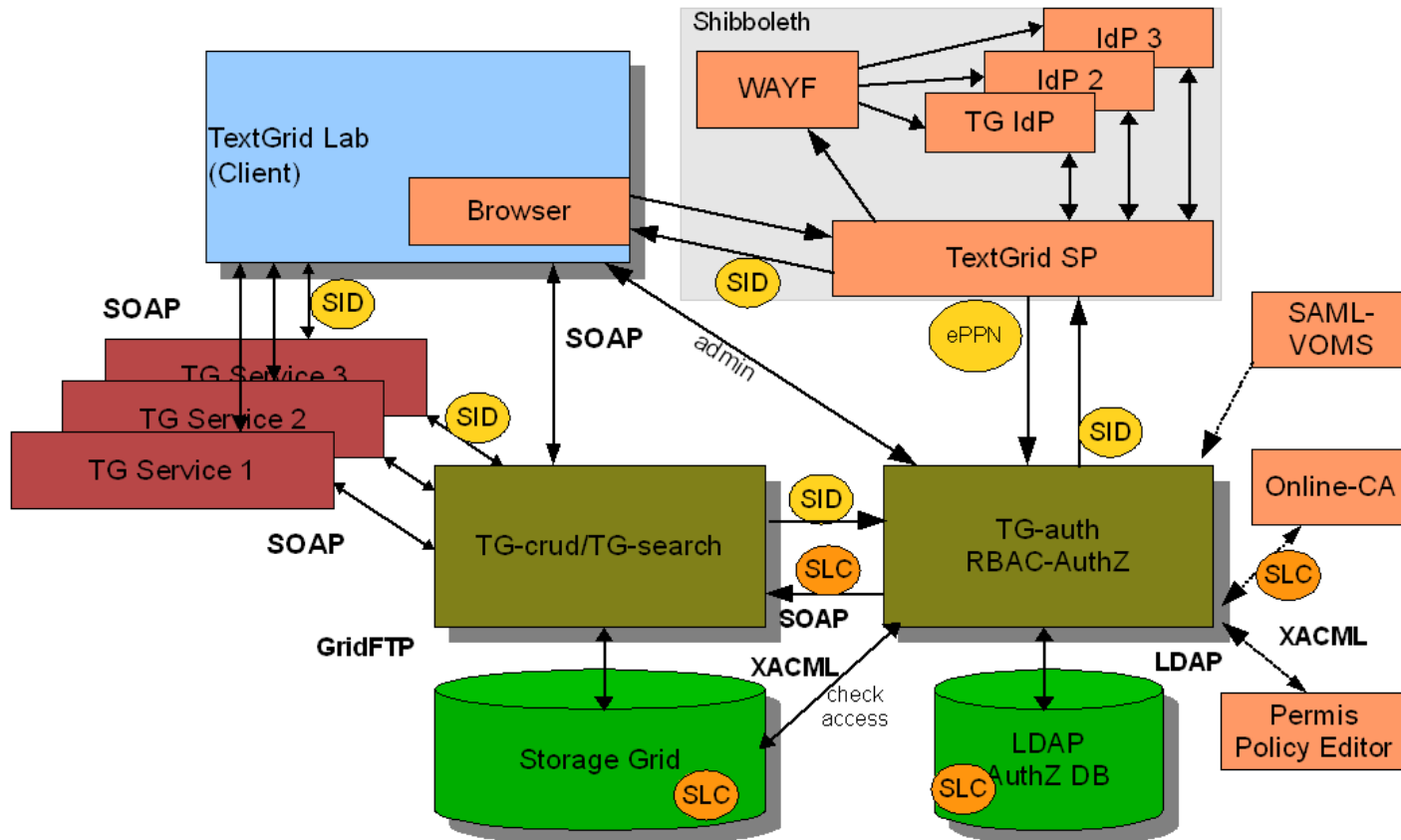
- Shibboleth integriert
- Der RBAC-Standard vollständig implementiert
 - limited hierarchical roles, dynamic und static separation of duty
- Alle Daten im LDAP-Server
 - user, roles, resources/permissions, sessions
- Alle RBAC-Funktionen sind über ein SOAP/WSDL-Interface verfügbar
- Zusätzlich spezielle Services für TextGrid
- Grid wird über ein Community-Zertifikat angesprochen
- Authentifizierung wird über eine Session-ID weitergereicht
 - Diese darf natürlich nur über verschlüsselte Verbindungen an bekannte Server weitergegeben werden



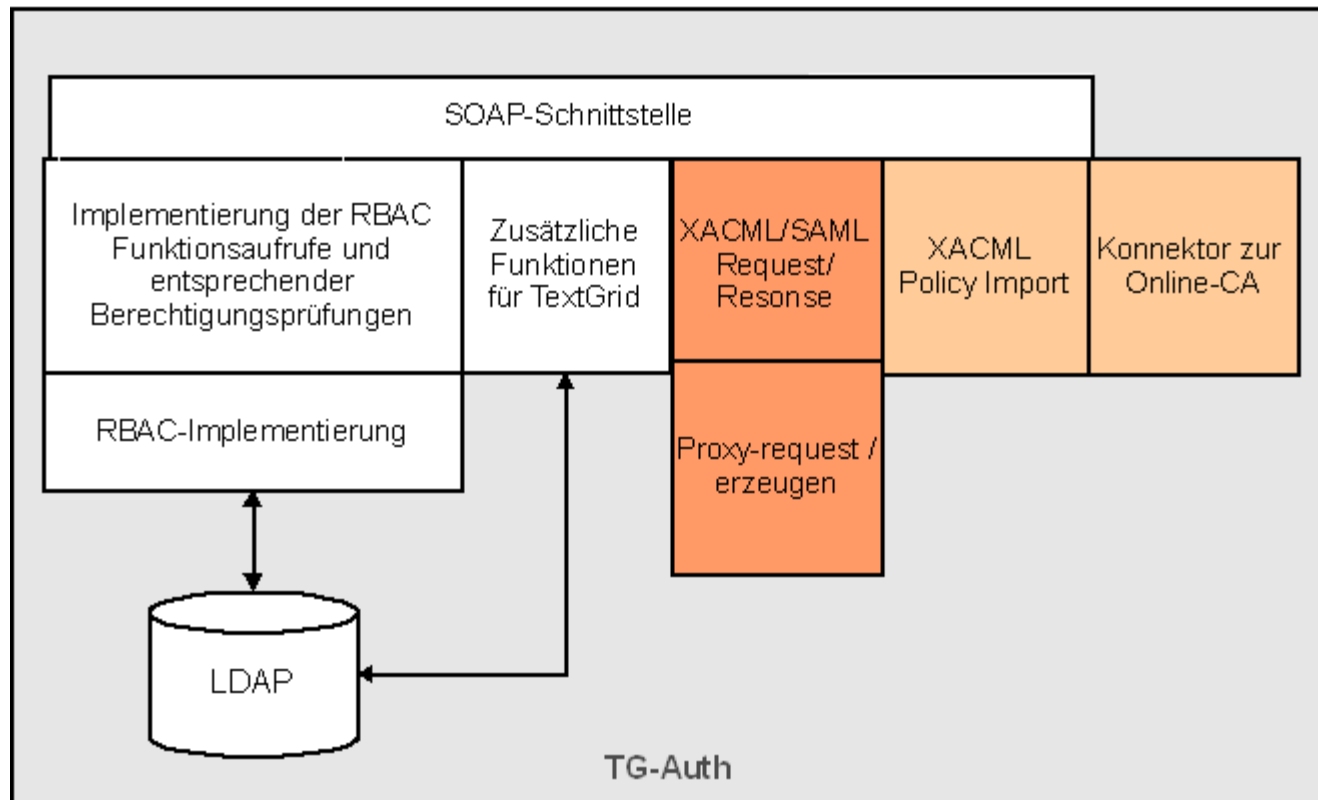
Grid wird über Community-Zertifikat angesprochen



- Jetzige Infrastruktur ist “autark”, also ohne Anbindung an DGI-VOMS
- Das soll mit IVOM-Ergebnissen nachgebessert werden
- Hierbei sind zwei Möglichkeiten angedacht:
 - TextGrid Middleware beantragt pro Session an Stelle des Benutzers ein SLC bei einer Online-CA; der private Schlüssel wird in der Middleware gespeichert
 - SLC wird vom Benutzerbrowser beantragt und der private Schlüssel dort gespeichert. Ein Proxy-Zertifikat wird pro Session beim Benutzer unterschrieben und in die Middleware eingebracht
- VO-Attribute können für Autorisierungsentscheidungen mit herangezogen werden
- Zusätzlich wird in TG-auth das XACML/SAML Request/Response-Protokoll implementiert, das sich zunehmend als Standard für die Kommunikation zwischen Grid-Ressource und PDP durchsetzt
- Permis kann genutzt werden, um Policy zu definieren und in XACML zu exportieren, welches in TG-auth importiert werden kann
 - Allerdings ist dies im Gegensatz zu dem Request/Response-Protokoll sehr komplex und aufwändig.



Privater Schlüssel im Server!



Kontakt und Information:

Peter Gietz

peter.gietz@daasi.de

<http://www.textgrid.de>

<http://www.daasi.de>



DAASI
International

Directory Applications
for Advanced Security
and Information Management

