Anforderungen von BauVOGrid und DGSI

Andreas Hoheisel

September 2009

Fraunhofer FIRST

Überblick

- Probleme mit kurzlebigen Zertifikaten
- Anforderungen GWES Workflow Management
- Anforderungen BauVOGrid
- Vorschlag für eine Grid-Sicherheitsarchitektur ohne kurzlebige Zertifikate (YAGSI)
- Anforderungen DGSI

Fraunhofer FIRST

Probleme kurzlebiger (Proxy-)Zertifikate in D-Grid

- Zeitliche Einschränkung der Zertifikate bringt kaum zusätzliche Sicherheit; Zertifikate sollten statt dessen an den Zweck (z.B. Job) gebunden werden
- Keine absoluten Kriterien zur Festlegung der Gültigkeitsdauer (daher meist willkürlich festgelegt)
- Dauer des Grid-Jobs zuvor in der Regel nicht bekannt – Ablaufen des Zertifikats während der Laufzeit möglich
- Keine eingeschränkte Delegation von Rechten; das Proxy-Zertifikat wird bei der Autorisierung meist wie der private Schlüssel des Nutzers behandelt; Man darf alles oder nichts
- Nicht nutzerfreundlich, CAs in der Regel nicht allgemein akzeptiert – siehe Vortrag von Dagmar Krefting
- Realisiert Sicherheitskonzept aus Sicht der Ressourcenprovider aber nicht aus Sicht der Nutzer (Proxy-Zertifikate werden z.B. für Root-Nutzer lesbar beim Provider abgelegt)

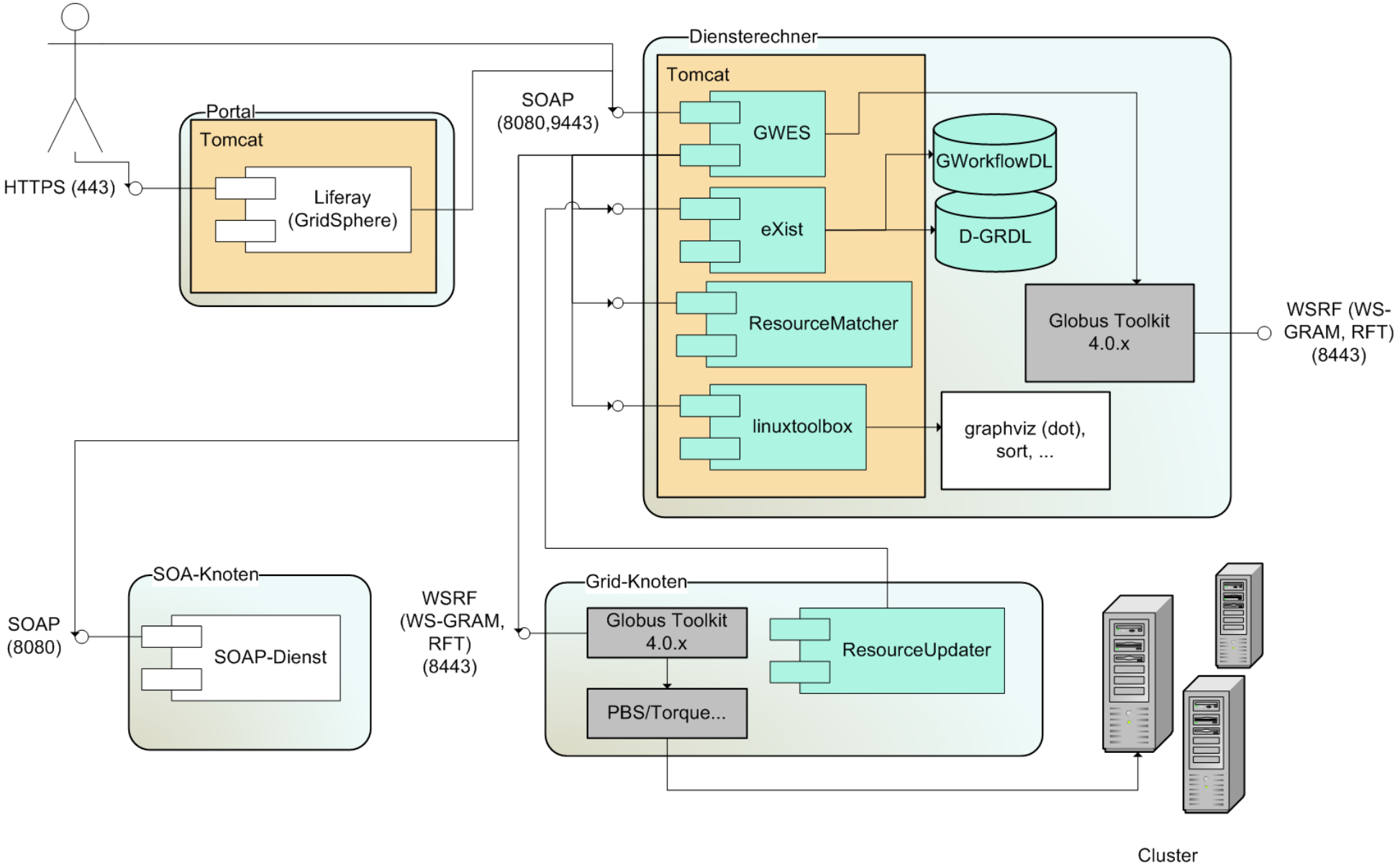
Anforderungen GWES Workflow Management

Der GWES ist ein Workflow-Management-Dienst, der die Ausführung von IT-Prozessen in D-Grid automatisiert indem es die Prozesse automatisch auf die verfügbaren Ressourcen abbildet (Meta-Scheduling) und fehlertolerant ausführt.

Anforderungen:

- Delegation von Rechten:
  Nutzer → Portal → GWES → GT4 → PBS → Job (→ SRB)
  Nutzer → GWES → GT4 → PBS → Job
  Nutzer → lokale Anwendung → GWES → GT4 → PBS → Job
  Nutzer → Portal → GWES → WebService
  …
- Firewall-freundlich: Alle Kommunikation sollte über Port 80 bzw. 443 möglich sein
- Derzeit: Sicherheit über Transport-Layer-Security (TLS).
  - Proxy-Zertifikate werden zur Delegation von Rechten als Methodenparameter einer Web-Service-Methode an den GWES übergeben
  - Oder Verwendung eines GWES-Dienstezertifikats
- Geplant: Eingeschränkte Delegation von Rechten auf Basis von Signaturketten (YAGSI)

GWES – Typische Systemarchitektur



Sicherheitsarchitektur BauVOGrid

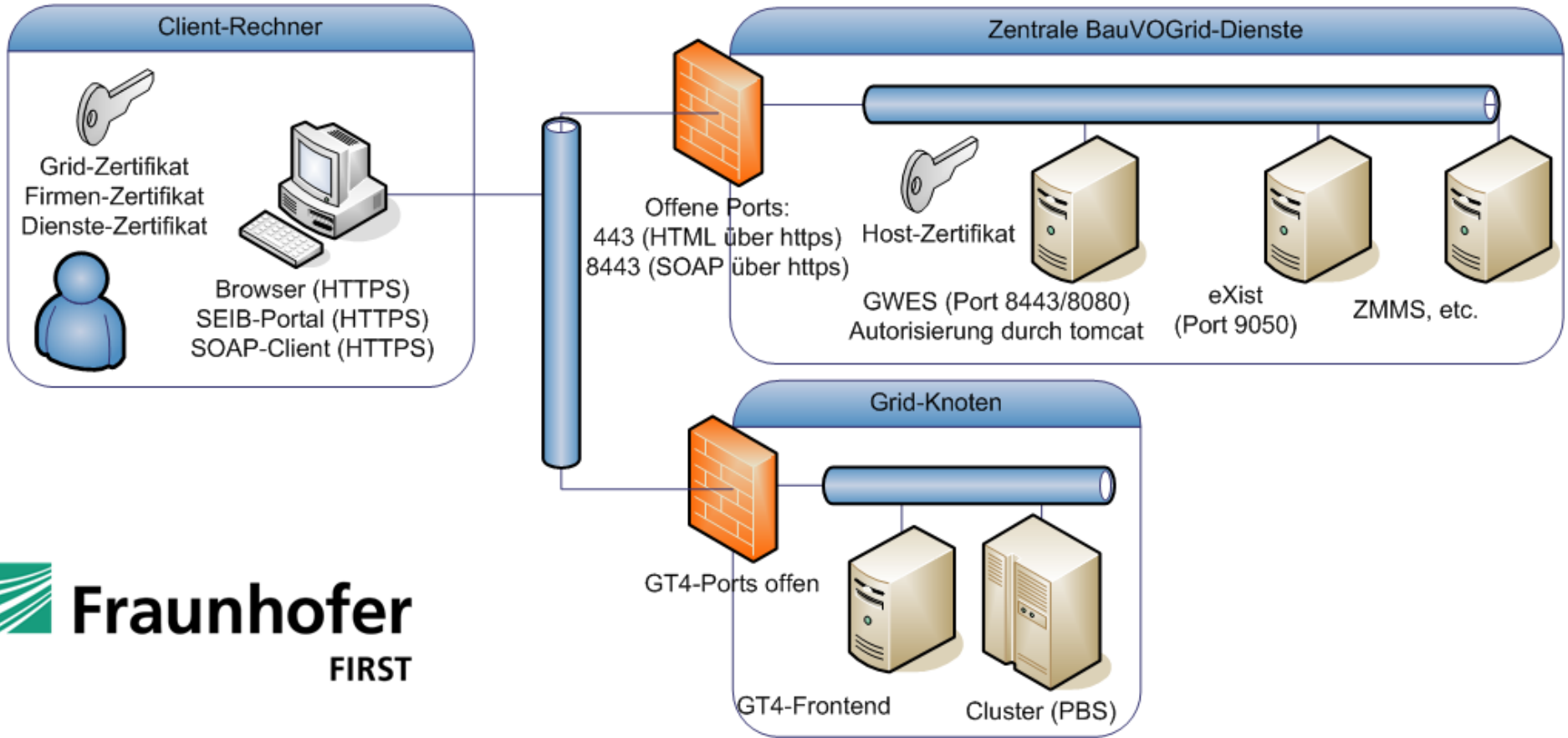
- Nutzungs-Szenario: Mängelmanagement (Aufnahme von Mängeln auf Baustellen)
- Standard Web-Security-Mechanismen (keine komplexe GT4-Security)
- Verwendung von „Transport Layer Security“ (TLS)
- HTTPS mit X509-Zertifikaten
- Unterstützung von Client-Autorisierung (Browser, Applets, Komandozeilenprogramme)
- Nutzer sind z.B. Bauleitung auf Baustelle, daher wichtig: Unterstützung unterschiedlicher Nutzercredentials: Grid-Zertifikate, Firmen-Zertifikate, Smartcards, Dienste-Zertifikate, ggf. auch Nutzername/Passwort…
- Grid-Zertifikate (DFN) können, aber müssen nicht unbedingt genutzt werden
- Zusätzliche feingranulare Autorisierung kann auf Basis des „Rollen-auf-Nutzer“-Abbildungsdienstes der TU-Dresden in den Web-Services selber implementiert werden
- Sicherheit Server-seitig direkt mit Bordmitteln des Web-Service-Containers (tomcat) realisiert (JSSE)
- Ausführung vordefinierter Grid-Jobs in D-Grid mit Dienstezertifikat (transparent für den Nutzer)

BauVOGrid über https (TLS – Sicherheit in Transportschicht)

- Client-Rechner schickt SOAP-Request verschlüsselt über HTTPS direkt an den GWES (Port 8443 oder alternativ 9443)
- Der Web-Service-Container (tomcat), in dem der GWES bereitgestellt wird, führt die Authentifizierung und Autorisierung auf Basis des Client-Zertifikats durch
- Interne Aufrufe (von innerhalb Firewall) von anderen BauVOGrid-Diensten können direkt unverschlüsselt über Port 8080 erfolgen
- Externe Aufrufe (von außerhalb Firewall) können nur über abgesicherte Ports erfolgen

Einschränkungen:
- Direkt keine feingranulare Autorisierung möglich (entweder dürfen alle GWES-Methoden aufgerufen werden oder keine)
→ Dies kann durch speziellen Autorisierungsdienst bzw. Rollenzuordnungsdienst der TU-Dresden realisiert werden

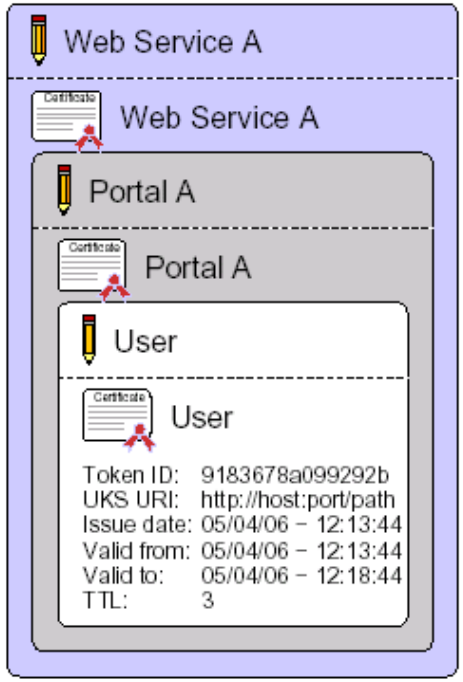
Alternativen:
- Verwendung von apache-redirect anstatt tomcat-eigener Sicherheit



Fraunhofer FIRST

Alternative: Grid-Sicherheitsinfrastruktur: „Yagsi“

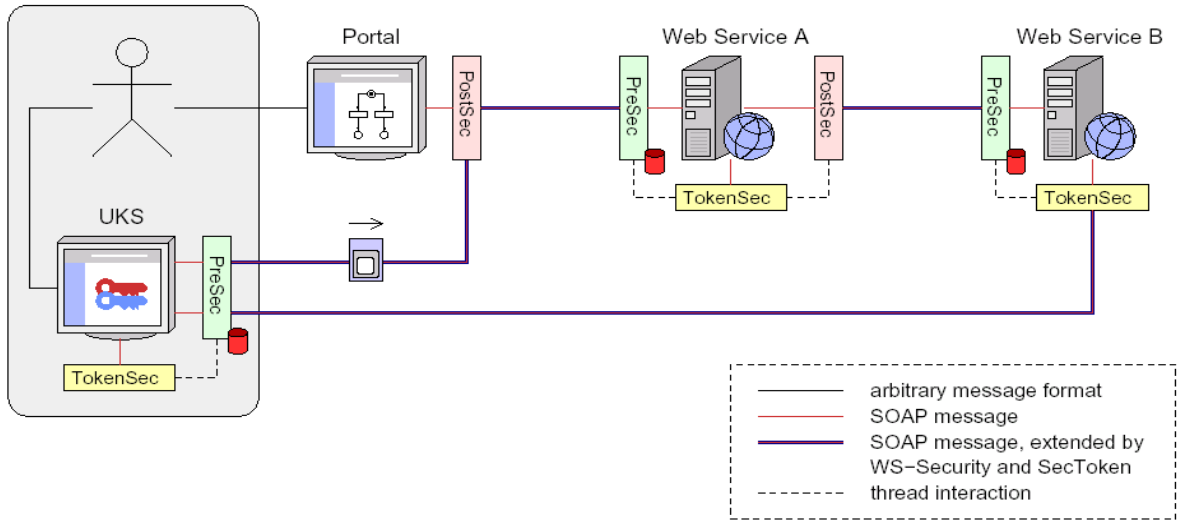
- **Mögliche Alternative zur Weitergabe von kurzlebigen Zertifikaten: Authentifizierung und Autorisierung auf Basis von Signaturketten**
- **Exemplarischer Ablauf:**
  - Nutzer signiert Anfrage mit privatem Schlüssel und schickt Anfrage an Portal
  - Portal überprüft Signatur und signiert selber die vom Nutzer signierte Anfrage mit dem Portal-Dienstezertifikat und initiiert Workflow im GWES
  - GWES überprüft Signaturkette (Nutzer/Portal), signiert die Anfrage und delegiert die Job-Ausführung an Grid-Knoten.
  - Grid-Knoten überprüft Signaturkette (Nutzer/Portal/GWES) und führt Job aus…
  - ➔ Job wird **im Auftrag** des Nutzers ausgeführt, **nicht im Namen** des Nutzers
- **Nachteil:** Autorisierungsmechanismen der Grid-Middleware müssen erweitern werden



Fraunhofer FIRST

Grid-Sicherheitsinfrastruktur: „Yagsi“

- Abgestufte Sicherheit für SOAs (Web-Services, Grid-Services)
- Unterstützung virtueller Organisationen (VO)
- Feingranulare und rollenbasierte Autorisierung
- Eingeschränkte Delegation von Rechten unter Kontrolle des Nutzers



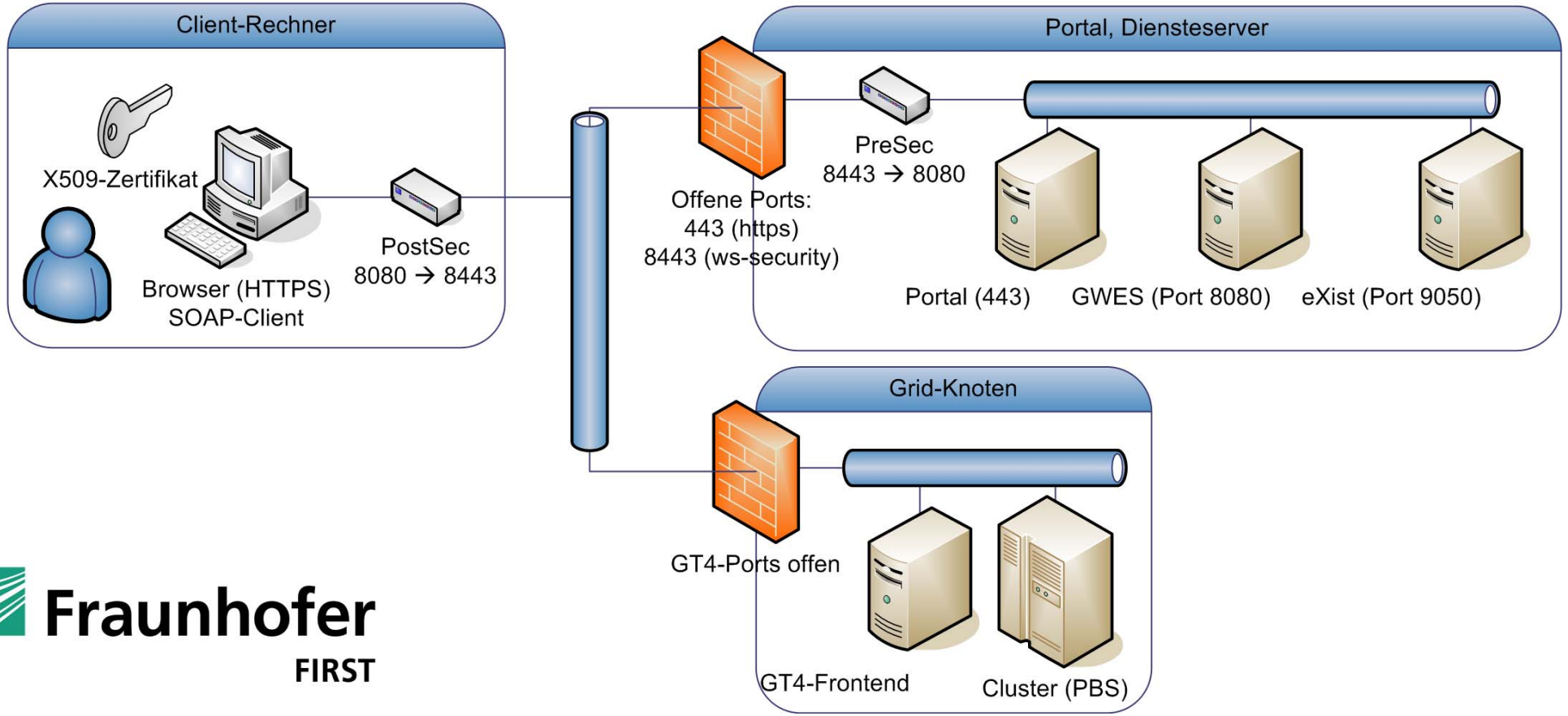
In Zusammenarbeit mit der Uni-Potsdam (Bettina Schnor, Stephan Müller)

Fraunhofer FIRST

Sicherheit mit YAGSI (WS-Security)

- Client-Rechner schickt SOAP-Request an den GWES (Port 8080).
- Der unverschlüsselte SOAP-Request wird an einen HTTP-Proxy umgeleitet (PostSec), der die Nachricht mit einer Nutzer-Signatur versieht, verschlüsselt (WS-Security) und über Port 8443 an das Portal weiterleitet
- Dort nimmt die PreSec-Komponente den SOAP-Request entgegen, führt die Authentifizierung und die attributsbasierte Autorisierung durch.
- Falls die Autorisierung erfolgreich war, wird die Anfrage entschlüsselt und an den GWES Port 8080 weitergeleitet.

Stand der Entwicklung:
- Prototyp für PostSec und PreSec-Komponenten (YAGSI) sind vorhanden (siehe http://www.gridworkflow.org/snips/gridworkflow/space/Yagsi)

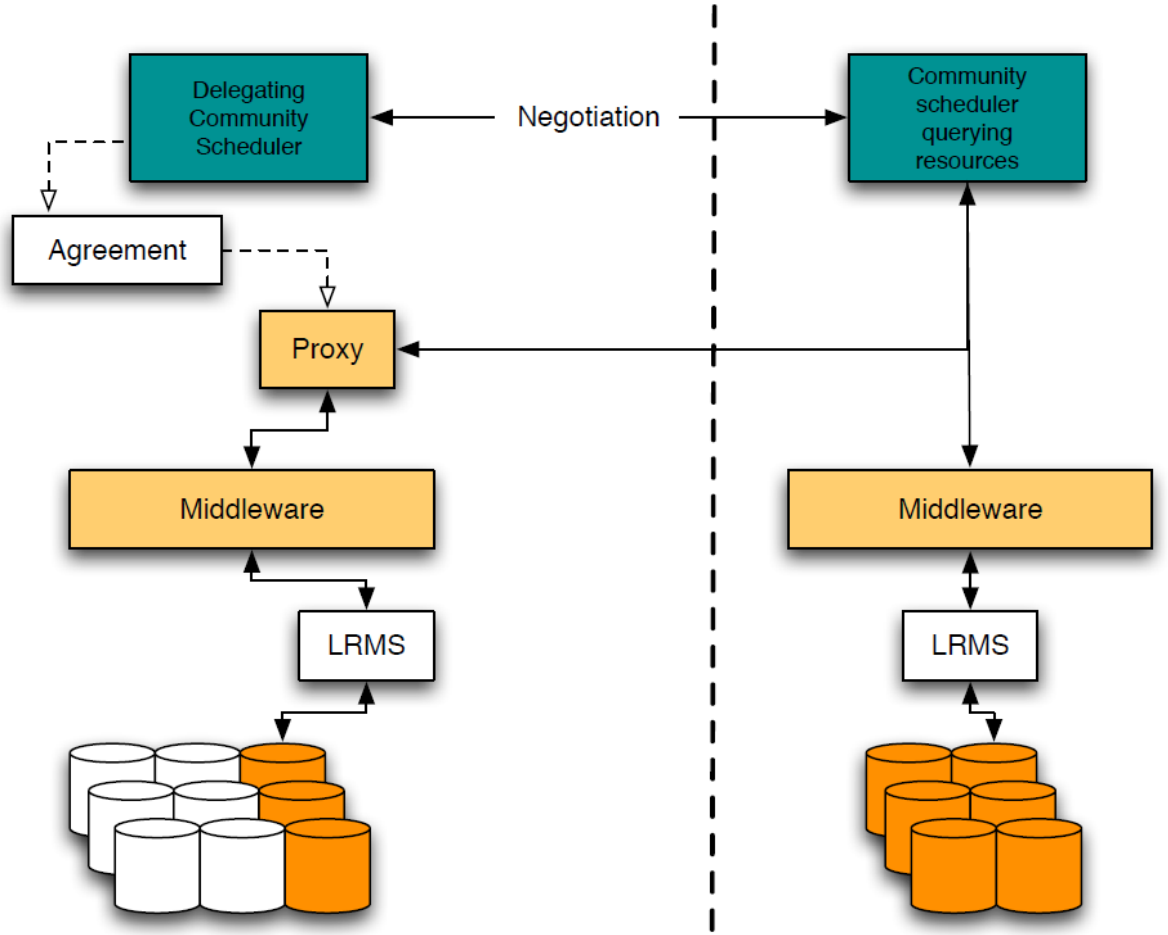


Fraunhofer FIRST

DGSI - D-Grid Scheduler Interoperability

Ziel:

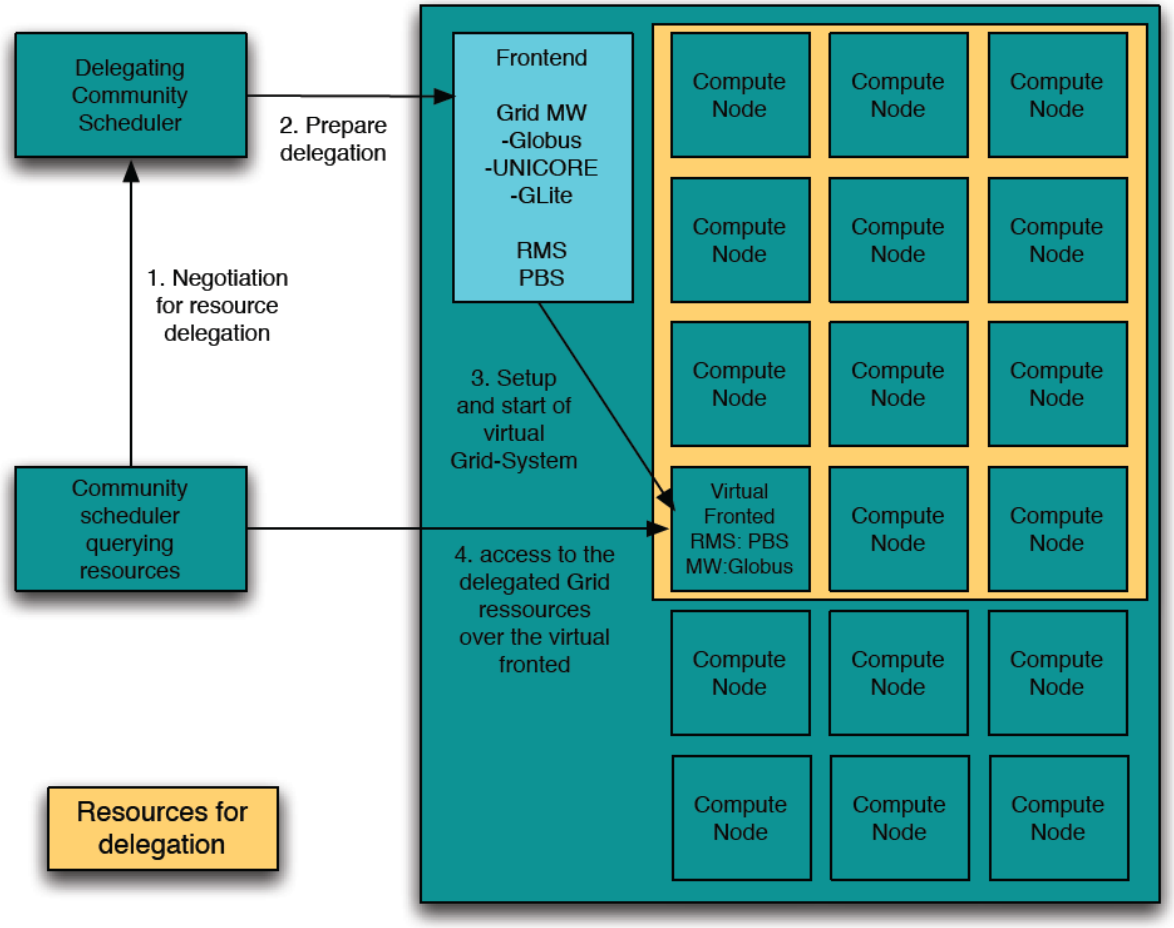
- Interoperabilität zwischen Meta-Schedulern in D-Grid
- Vorübergehende Verwendung von Grid-Ressourcen einer anderen Community



Fraunhofer FIRST

DGSI - D-Grid Scheduler Interoperability

– Besondere Anforderung: Temporäre Host-Zertifikate für virtualisierte Grid-Frontends



Fraunhofer FIRST

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

andreas.hoheisel@first.fraunhofer.de

http://www.first.fraunhofer.de/

http://www.andreas-hoheisel.de/

Download Grid Workflow Execution Service:

http://www.gridworkflow.org/gwes/

Fraunhofer FIRST