Vereinfachung der AAI durch ein Proxy Upload Tool und Nutzung von ROBOT-Zertifikaten

Jürgen Falkner[1], Oliver Strauß[1], Peter Gietz[2], Martin Haase[2], Bernadette Fritzsch[3]
1.) Fraunhofer IAO 2.) DAASI International GmbH 3.) Alfred-Wegener-Institut für Polar- und Meeresforschung

Zertifikate einfach nutzen mit dem GRID Proxy Upload Tool gPUT

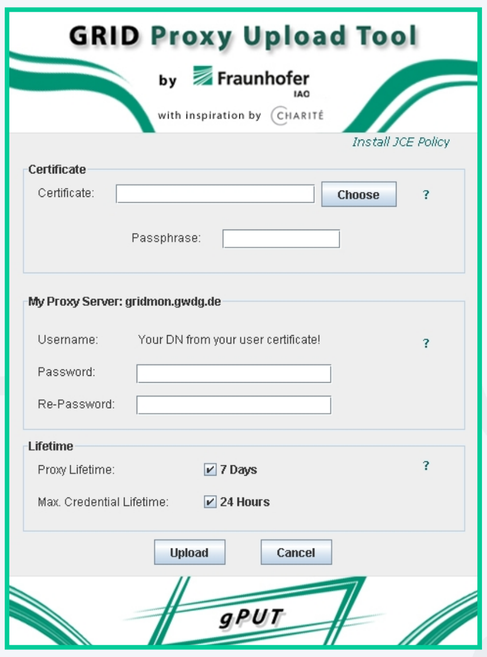
Problemstellung:

- Umgang mit Zertifikaten und Proxys zu komplex
- Hochsichere Services und Ressourcen erfordern aber ein persönliches Nutzerzertifikat

Lösung:

- Starke Vereinfachung von Proxy- und Credential-Management
- Unterstützung für Portal-basierte Grid-Nutzung
- Unterstützung von Liferay und Vine Toolkit
- Kombinierung von zertifikatsbasiertem Login, Proxy Upload und Credential Retrieval
- One-Click-Solution

Einfacher Proxy-Upload via Applet:



Vorteile:

- Keine Installationsvoraussetzung auf dem Nutzerrechner außer Standard Java Runtime Environment
- Automatische Formatkonvertierung des Nutzerzertifikats auf dem Nutzerrechner
- Sicherer Proxy Upload auf einen MyProxy Server via Portal ⇒ Kommunikation ausschließlich über HTTPS (funktioniert auch in Kliniknetzwerken !)
- **Maximierung der Nutzerfreundlichkeit !**

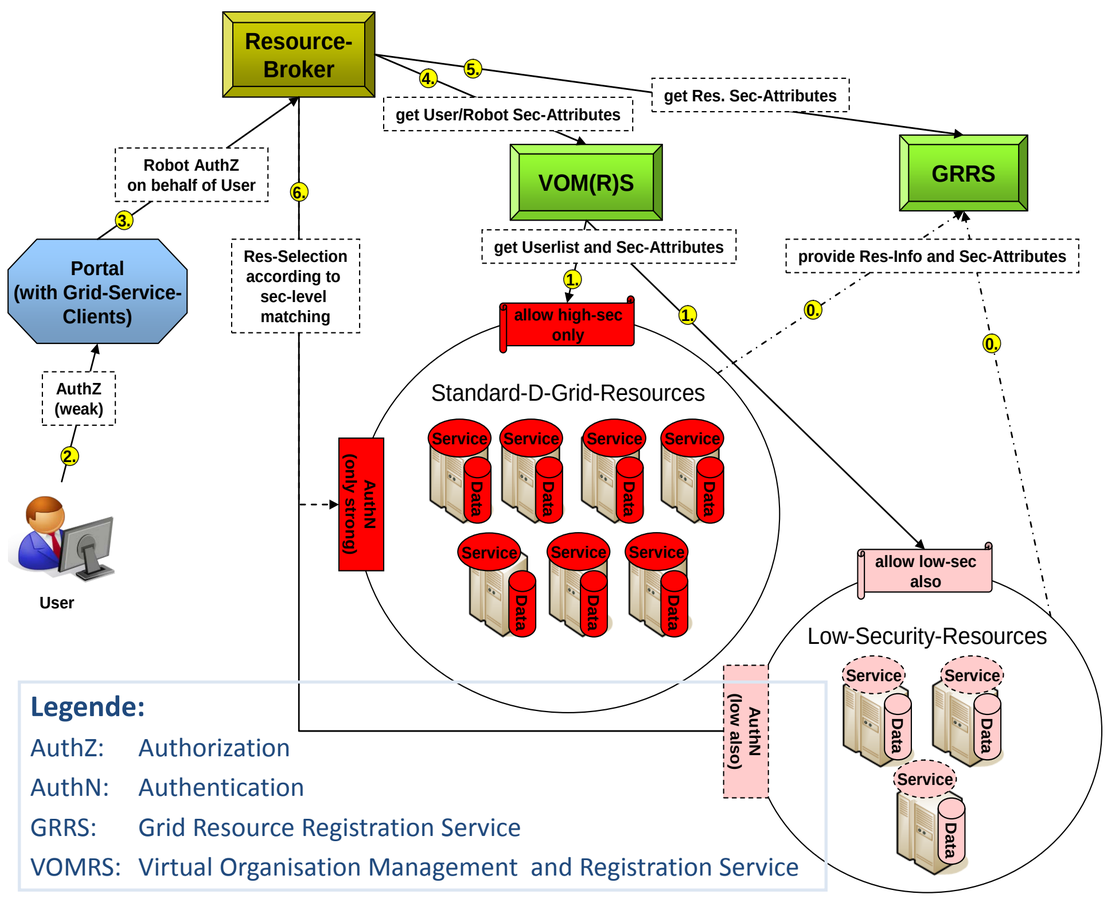
Einfache Nutzerzugänge ohne persönliche Zertifikate

Problemstellung:

- Umgang mit Zertifikaten zu komplex
- Nutzung für Dienste mit Zugriff auf Daten ohne Zugangsbeschränkung
- Gastnutzerzugänge erwünscht

Lösung:

- Anwendungs-Services können mit ROBOT-Zertifikaten ausgestattet werden
- Einrichtung eines dedizierten Ressourcenpools für die Nutzung durch ROBOT-Services



Legende:

AuthZ: Authorization
AuthN: Authentication
GRRS: Grid Resource Registration Service
VOMRS: Virtual Organisation Management and Registration Service

Was sind Robot-Zertifikate?

- Robot-Zertifikate sind x509-Zertifikate für Dienste/ Anwendungen / Services
- Haftung bei Service-Betreiber
- **ROBOT-Zertifikate sind vom Europäischen Dachverband der Grid-Zertifizierungsstellen (EUGridPMA) reglementiert**

Umsetzungs-Szenario für die Nutzung von Robot-Zertifikaten

0: Ressourcen melden sich an der Resource- Registry an und melden ihre Sicherheitslevel (z.B. ROBOTs: ja/nein)

1: Ressourcen beziehen Nutzerinformationen aus dem VOMS und setzen lokale Account- Mappings um – auf Basis der Nutzerattribute
=> je nach Sicherheitslevel werden ROBOTs akzeptiert oder verweigert

2: Nutzer meldet sich z.B. über Gast-Login am Portal an

3: Die Authentifizierung im Grid erfolgt über einen Portal-Service mit ROBOT-Zertifikat

4+5: Über die Nutzer- und Ressourcenverwaltung wird ermittelt, welche Ressourcen
a) ROBOTs akzeptieren und
b) für den Grid-Job in Frage kommen

6: Grid-Job wird auf geeigneten Ressourcen ausgeführt →Sicherheitslevel der Ressourcen werden berücksichtigt!

→ Autorisierungssysteme der Ressourcen haben die letzte Entscheidung anhand der vorgeschriebenen DN-Erweiterungen für ROBOT-Zertifikate

Einsatz in TextGrid

- Benutzer werden über Shibboleth oder direkt am TextGrid Community LDAP authentifiziert
- Authentifizierungs- und Autorisierungskomponente TG-auth* generiert Security Token (SID)
- Zentraler Dienst für Dateioperationen TG-crud unterscheidet Benutzer anhand der SID
- TG-crud verwendet ROBOT-Zertifikat für Operationen im Auftrag derjenigen Benutzer, die nicht über ein eigenes Zertifikat bzw. Short Lived Credential (SLC) verfügen
- Die über das ROBOT-Zertifikat erreichbaren Ressourcen sind aus dem Low-Security-Pool

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

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung