GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Authentifizierung und Autorisierung in einem Portal-basierten Grid (C3-Grid)

Siegfried Makedanz

Jörg Matthes

Hans Pfeiffenberger

HELMHOLTZ GEMEINSCHAFT

AWI

Computer Center

Alfred-Wegener-Institut

siegfried.makedanz [at] awi.de

Motivation

- Lösung des AAI- und VO-Problems für ein Portal-basiertes Grid
  - Grid-Zugang nur über das Web-Portal
- Praktische Umsetzung für das C3-Grid
  - Collaborative Climate Community Data and Processing Grid
  - Community der Klima- und Erdsystemforscher
  - 1. D-Grid Call

Anforderungen Community

- Komplexität des Grid-Zugangs für den Nutzer mindern
  - Shibboleth als Access AAI
  - „Einfacher“ Web-basierter Zugang
    - Kein globusrun-ws für den Nutzer
- Weitgehend transparente AuthN- und AuthZ-Vorgänge
  - Login mit Username und Passwort üblich
- Resource Provider: Individuelle Unterscheidung der Nutzer
- Feingranulare Autorisierung
  - Zugriffsrechte für Daten

Werkzeuge/Software

- Grid Middleware: Globus TK 4
- AAI: Shibboleth (DFN-AAI)
  - Secure Assertion Markup Language (SAML)
- Portal: GridSphere
  - mit Shibboleth Plugin
  - Unterstützung durch DGI2
- GridShib
  - SAML Tools - Einsatz am Portal
  - GridShib for GT - bei den Resource Providern

Herausforderungen

- Shibboleth bis zum Portal
- X.509 PKI im Grid
  - Plus SAML Assertions für AuthZ
- In Portal-basierten Grids agiert der Nutzer **nicht**
  - direkt mit der Grid Middleware
  - direkt mit dem VO System
- **Es müssen sichere und vertrauenswürdige Wege gefunden werden, um Nutzer-Credentials und -Attribute in das Grid zu bringen**

Neuland

- IVOM-Ansätze basieren auf Software, die tlw. noch in Entwicklung ist
  - GridShib CA (v0.5.0 am 31.01.2008)
  - Gridshib for GT (v0.6.0 Alpha am 31.01.2008)
  - VOMS SAML Service (Final Release Ende Februar 2008)
  - Shibboleth-Plugin für GridSphere
- Traue keiner Roadmap
  - Auch nicht der eigenen

VO Management

- Derzeit sind Shibboleth-basierte VO Management-Systeme nicht produktionsreif
  - myVocs (UAB, USA)
  - IAMSuite (MAMS, AUS)
- VOMS SAML Service

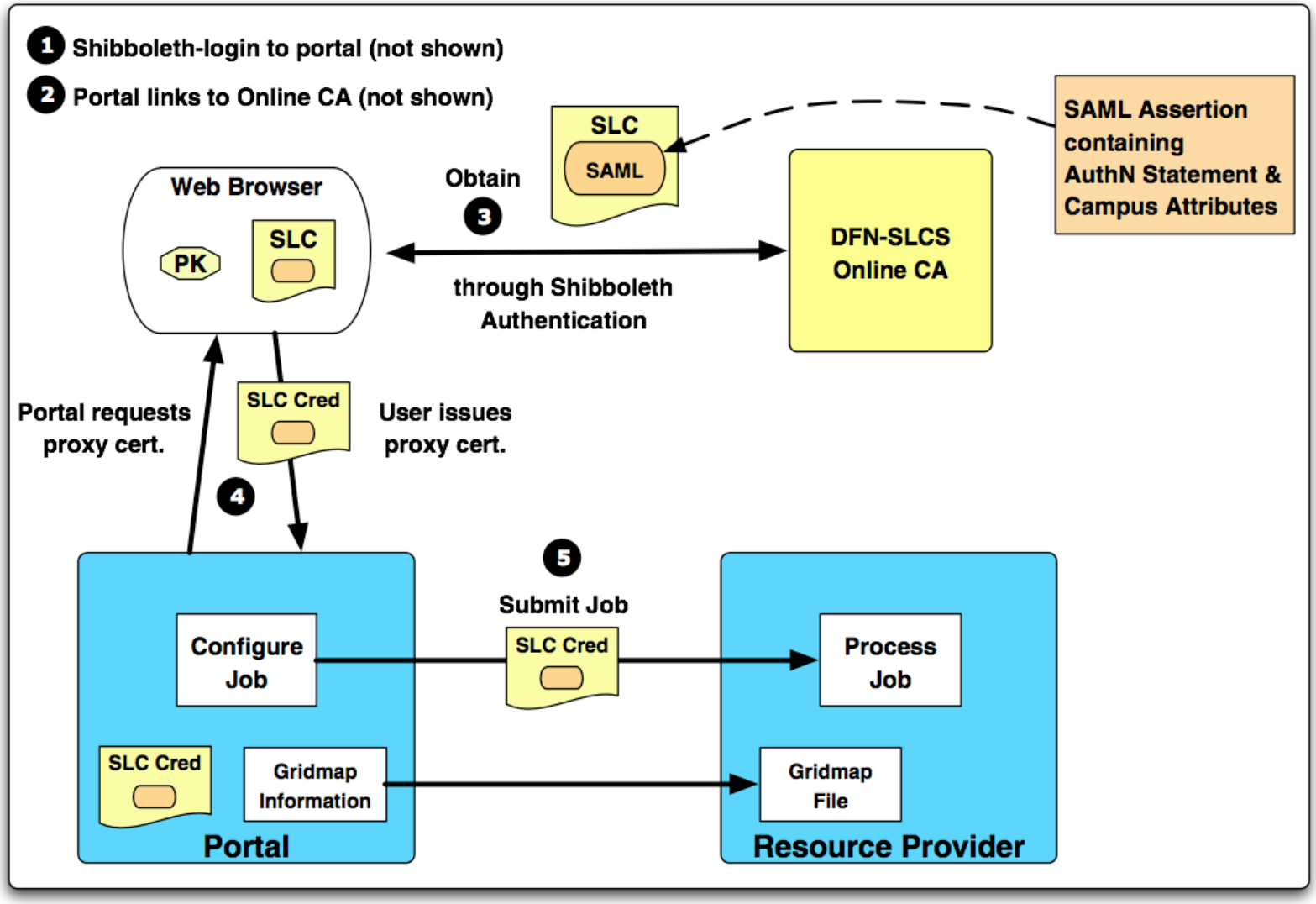
Lösungsansätze für Grid-Portale

- Community Account Model (TeraGrid)
  - AuthN/AuthZ am Portal
  - AuthZ wird in Community Credential eingebettet
  - Mapping auf einen Community Account im Grid
  - Keine Akzeptanz bei C3 Resource Providers
- SLC per Portal Delegation
  - Portal bezieht SLC im Namen des Nutzers von Online CA
  - Erhebliche Sicherheitsbedenken
- SLC
  - Nutzer bezieht SLC direkt von Online CA
  - Aber: Wie kommt das SLC dann ins Portal?

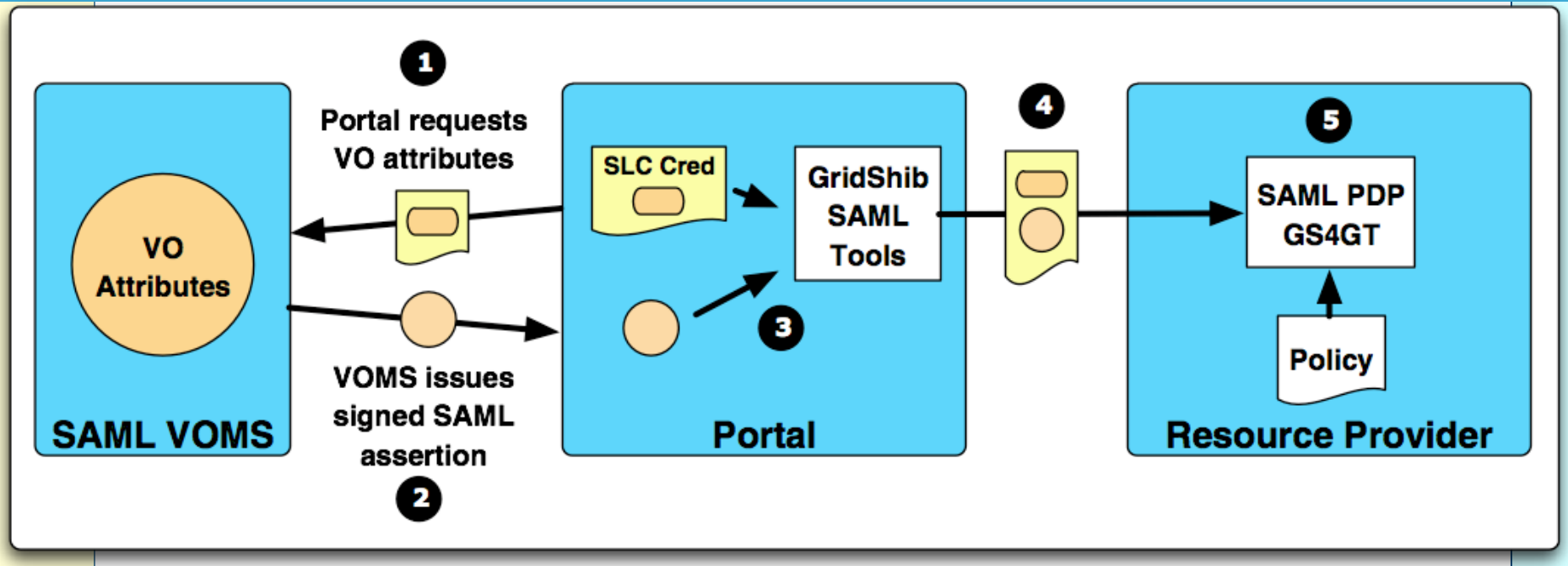
SLCs für Portal-Nutzer

- Neuer Lösungsansatz
- Ablauf
  - Shibboleth-Login am Portal
  - Portal verweist an Online CA
  - Nutzer bezieht SLC von Online CA
  - Portal bezieht Proxy-Zertifikat vom Nutzer
- Browser-Erweiterung notwendig, um Proxy Zertifikat beim Nutzer zu erstellen
  - DFN-PCA hat Unterstützung zugesagt

Portal-basiertes Grid
1. Schritt: Authentifizierung



Portal-basiertes Grid
2. Schritt: plus SAML-AuthZ



- Integration von SAML VOMS als VO Attribute Authority
- Portal: VO-Attribute werden in SLC Cred. eingebettet
- Auswertung Campus- und VO-Attribute durch GridShib for GT

Zusammenfassung

- Community-Anforderungen sind weitgehend erfüllbar
  - Ausnahme: Mehrere Schritte bei Nutzer-Login
  - Realisierung feingranulare AuthZ dauert länger
- 1. Schritt (AuthN) GSI-kompatibel
  - Einsatz vertrauter Verfahren bei RPs (gridmap)
- 2. Schritt (AuthZ) GSI-kompatibel
  - Gleitender Übergang zu SAML
- Lösung passt in die D-Grid Infrastruktur

Offene Punkte - Ausblick
Kurz-, Mittel-, Langfristig

- Browser-Erweiterung für Portal-Nutzer (Proxy-Zertifikate)
- *Nested SAML Assertions* in GridShib
- Internationale, föderationsübergreifende AA-Infrastruktur für Shibboleth
  - Community-Anforderung: Internationale Zusammenarbeit, IPCC (UN-Klimarat)
  - GÉANT JRA5, TERENA TF-EMC^2 arbeiten an einer Lösung (eduGAIN)
    - DFN beteiligt, Grid-Tauglichkeit noch unklar

Ende

- Danke für Ihre Aufmerksamkeit!