GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Wo stehen wir:
AAI, VO, Sonderinvestitionen

Stefan Piger, Christian Grimm
RRZN, Leibniz Universität Hannover
DGI FG3-4, in Abstimmung mit FG1-10 und FG2-3

Agenda

- Überblick Sonderinvestitionen
- VO-Management
- AAI
- Ausblick

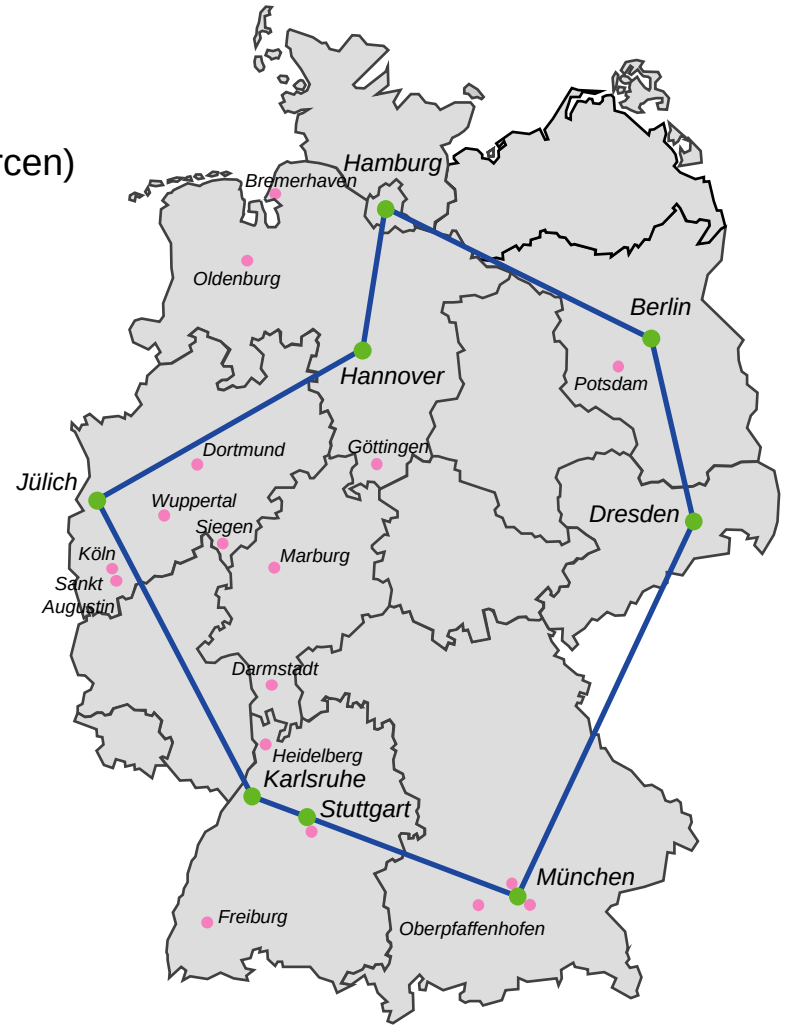
Sonderinvestitionen – Überblick

5,3 M€ Sachmittel für D-Grid Infrastruktur

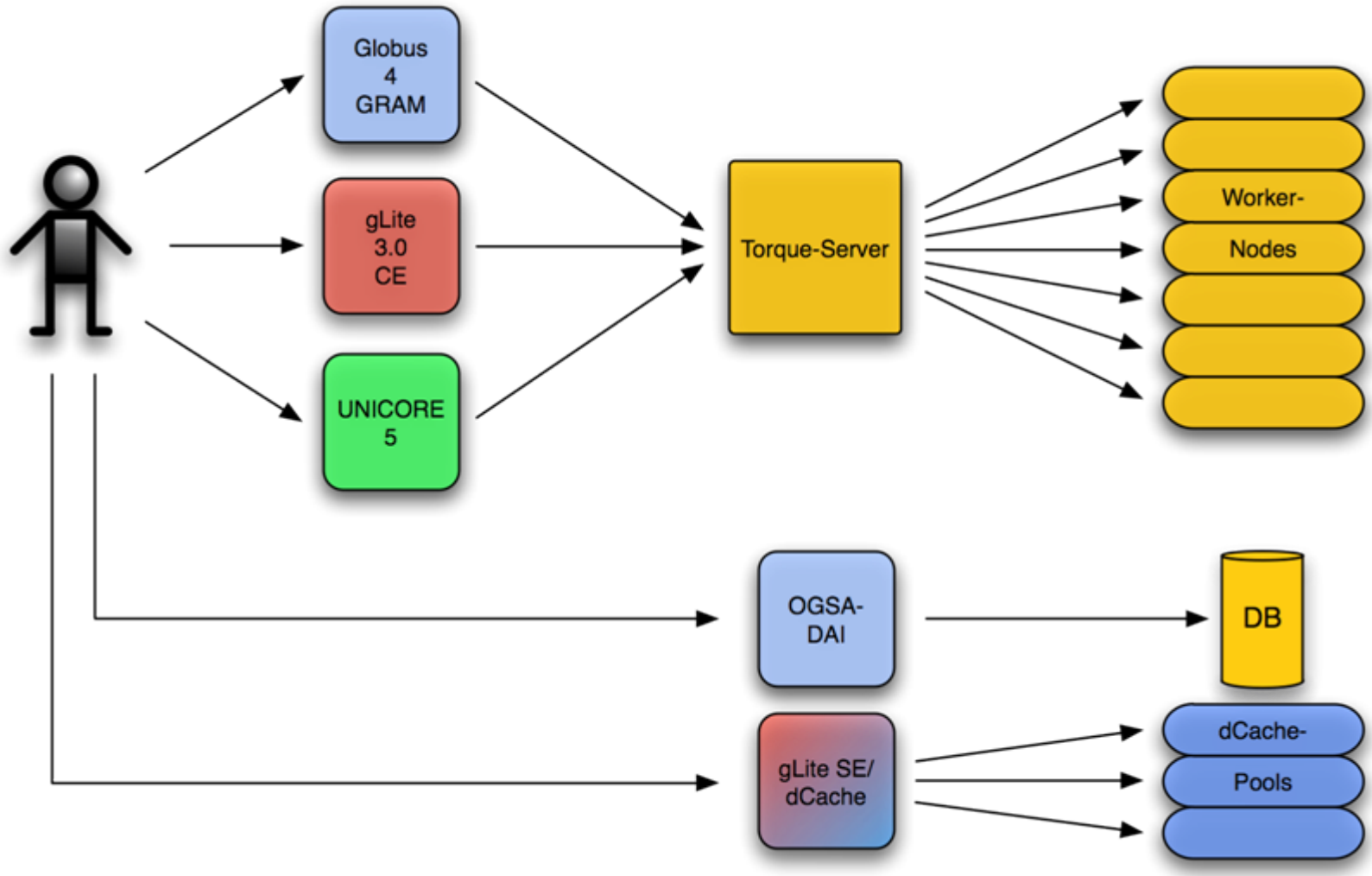
- acht Zentren bilden den D-Grid Backbone
  - diese erhalten jeweils 380.000 € Förderung
    (je 190.000 € für Compute und Storage Ressourcen)
- weitere 17 Partner mit geringerer Förderung
- beschafft wurden
  - ca. 2000 Cores mit min. 2 GB RAM/Core
  - ca. 2000 TB Speicher

Middleware-Unterstützung

- Compute Services
  - Globus Toolkit 4
  - gLite 3.0
  - UNICORE 5
- Datenmanagement
  - gliteSE/dCache-SRM
  - Globus OGSA-DAI



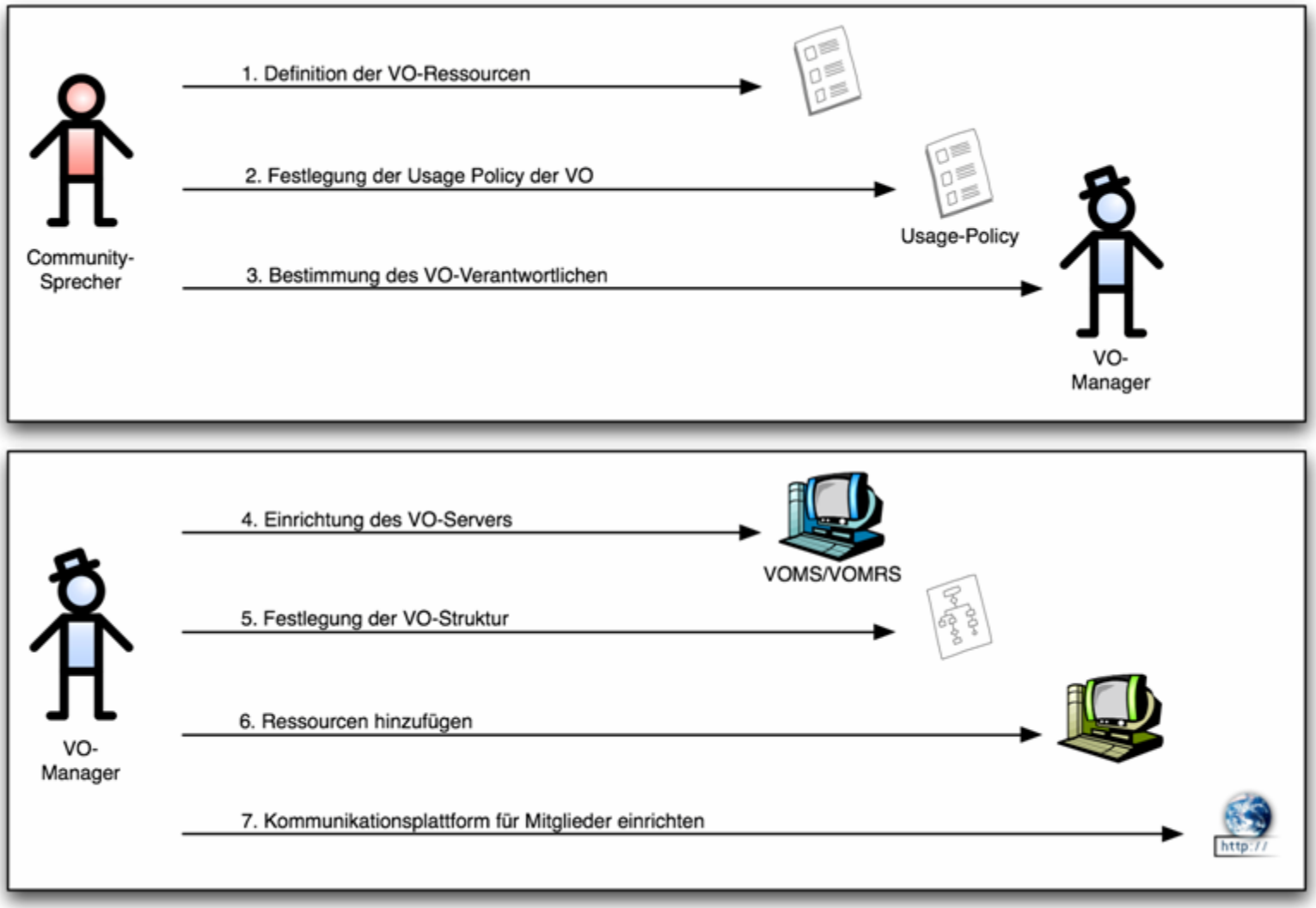
Sonderinvestitionen – Referenzinstallation



VO – Definition

- zeitlich begrenztes oder permanentes Konsortium
- besteht aus geographisch und institutionell verteilten Individuen, Gruppen, Organisationseinheiten oder ganzen Organisationen
- Mitglieder bringen Ressourcen, Dienste und Daten in eine VO ein
  - diese werden gemeinsam genutzt
- Mitglieder einer VO verfolgen gemeinsame Ziele

Einrichtung einer VO



VO – Sonderinvestitionen

VO-Konzept für Sonderinvestition deckt grundlegende Anforderungen ab

- ist noch mit VO-Rahmenkonzept abzustimmen
- Registrierung von Ressourcen
  - alle Sonderinvestitionen unterstützen alle D-Grid VOs
  - über D-Grid Provider Portal: https://www.d-grid.de/?id=288
- Registrierung von Nutzern
  - mittels Virtual Organization Management Registration Service (VOMRS)
  - https://vomrs.zam.kfa-juelich.de:8443/vo/*VO-Name*/vomrs

VOMRS

- im Vergleich zu VOMS zusätzliche Funktionalität
  - verbesserter Prozess zur Registrierung von Nutzern
  - mehrere Zertifikate pro Nutzer
  - Nutzer können vorübergehend gesperrt werden
- Abgleich (unidirektional) mit VOMS
  - wird momentan für die Sonderinvestitionen nicht durchgeführt
  - d.h. keine VO-Attribute im Proxy-Zertifikat

AAI für Sonderinvestitionen – Überblick

Ziele

- Unterstützung aller drei (D-Grid) Middleware Pakete
- einmalige Anmeldung für Nutzer an ihrer VO
- kurzfristige Betriebsbereitschaft

Folge

- gemeinsamer Nenner aller drei Middleware Pakete
  - Authentifizierung per X.509 (Proxy-) Zertifikat
    - akzeptierte Zertifizierungsstellen sind alle EUGridPMA kompatiblen CAs
    - jeder Nutzer und Grid-Service bekommt ein End-Entity Zertifikat (EEZ)
  - nur grundlegende Autorisierungsmechanismen
    - ja/nein Entscheidung
- Authentifizierung/Autorisierung per Shibboleth nicht möglich
  - wird in zukünftiger AAI für die Sonderinvestitionen berücksichtigt

Autorisierung

Randbedingungen

- VOMRS verwaltet Virtuelle Organisationen und deren Nutzer
  - Nutzer meldet sich beim VOMRS mit End-Entity Zertifikat an
  - SI-Ressourcen beziehen via *dgridmap* Skript (FZJ) von VOMRS regelmäßig neue Mapfiles
    - gridmap-file für Globus Toolkit und gLite
    - UUDB für UNICORE
- Delegation mittels Proxy-Zertifikaten
  - PZ für Nutzung von gLite und Globus vom EEZ abgeleitet
  - PZ enthalten keine Attributzertifikate von VOMS

Nutzerbasierte Autorisierung auf den Ressourcen

- Autorisierung auf Ressourcen mittels DN im Subjekt des EEZ
  - Beispiel: "/O=GermanGrid/OU=UniHannover/CN=Stefan Piger"
- Unterscheidung nach VO-Zugehörigkeit
  - nur über den Account auf den der DN des Nutzers abgebildet wird
- alle Nutzer der Sonderinvestitionen haben die gleichen Rechte
  - keine Differenzierung von Nutzern innerhalb der VOs möglich

Accounts

Pool-Accounts

- Pro
  - geringerer Aufwand bei der Konfiguration der Ressourcen
  - Unterstützung großer Nutzerzahlen
  - geringere Anzahl von Accounts gegenüber 1:1 Abbildung
- Contra
  - von den Communities teilweise nicht gewünscht
  - Tracking/Logging der Nutzer über mehrere Ressourcen hinweg aufwändig
  - keine ausreichende Unterstützung in den Middleware Paketen
    - in gLite unterstützt
    - in Globus Toolkit nur in den „Technology Previews“
    - Unterstützung in UNICORE ungetestet

Nutzer werden statisch auf Accounts auf den SI abgebildet

- Ressourcen-Provider erstellen eine Anzahl von Accounts pro VO
- 1:1 Abbildung von DN des Nutzers auf lokalen Account in grid-mapfile/uudb
- Nutzer erhalten einen „eigenen“ Account, dessen Name wird gebildet aus
  - 2-stelligem Prefix der Einrichtung
  - 2-stelliger Abkürzung der VO
  - 4-stelliger Nummer
  - Beispiel: uhkg0016

Ausblick – VO-Management

Konzeption einer (generischen) D-Grid VO-Struktur

- Definition von durch die Autorisierung unterstützten Attributen
  - generische Rollen
  - Attribute/Value Paaren

VO-Management für D-Grid Sonderinvestitionen

- (technische) Umsetzung der Abläufe für
  - die Einrichtung/Auflösung von VOs
  - die Administration von VOs
- implementiert Attribute Authority für Autorisierung auf Ressourcen

Ausblick – attributbasierte Autorisierung

Unterstützung für Attribute aus dem VO-Management

- VOMS-Attributzertifikate
  - durch gLite in aktueller Release
  - durch Globus Toolkit in „Technology Preview“
  - für UNICORE in IVOM geplant
- Shibboleth SAML-Assertions in Proxy-Zertifikaten
  - keine Unterstützung durch gLite
  - durch GridShib für Globus Toolkit
  - für UNICORE in IVOM geplant

Vergabe fein-granularer Berechtigungen für die Nutzung von

- Compute-Ressourcen
  - spezielle Ressourcen
  - einzelne Warteschlangen
  - Applikationen
- Datenmanagement
  - Berechtigungsvergabe für Nutzergruppen bzw. Virtuelle Organisationen

Ausblick – Virtual Workspaces

Pool-Accounts

- in gLite durch LCMAPS unterstützt
- in Globus Toolkit in Technology Preview
  - LCMAPS oder
  - datenbankbasierte Implementierung
- in UNICORE nicht direkt unterstützt
  - mittels dynamischen Einträgen in der UUD realisierbar

dynamische Accounts

- in gLite nicht unterstützt
- in Globus in Technology Preview
  - „useradd“
- in UNICORE nicht unterstützt

Virtualisierung

- in gLite nicht unterstützt
- in Globus in Technology Preview
  - Xen-basierte Lösung
- in UNICORE nicht unterstützt
  - an einer Xen-basierten Lösung wird gearbeitet

Zusammenfassung

Überblick Sonderinvestitionen

- Middleware Unterstützung
- Referenzinstallation

VO-Management

- Definition
- VO-Management für Sonderinvestitionen

AAI

- Ziele
- Autorisierung
- Accounts

Ausblick

- VO-Management
- Autorisierung
- Accounts/Workspaces