Betrachtungen zur akademischen Sicherheitsinfrastruktur im D-Grid

Harry Enke
Bernadette Fritzsch
Christian Grimme
Frank Schlünzen

Einführung

- Verschiedene Projekte aus dem akademischen Bereich in D-Grid
- Sicherheitsaspekte:
  - In prototypischer, erster Projektphase oft nur am Rande behandelt
  - Im Laufe der Projekte haben sich die Anforderungen ergeben
  - Teilaspekte wurden umgesetzt, GAP-Projekte beantragt
- Insgesamt kein einheitliches Konzept oder Vorgehen
- Hier: Strukturierte Analyse der Sicherheitsanforderungen
  - Sammlung aus den fünf akademischen Communities
  - Einordnung und Klassifizierung der Konzepte und Methoden/Lösungen
  - Aufzeigen offener Punkte und des möglichen Synergiepotentials

Übersicht

- Akademische Communities im D-Grid
- Betrachtung der einzelnen Communities
  - Sicherheitsanforderungen
  - Konzepte und technische Umsetzungen
- Klassifikation
  - des Zugangs zur Infrastruktur
  - von Sicherheitsanforderungen
- Einordnung der Lösungsansätze
- Offene Punkte und mögliche Synergien

Akademische Communities im D-Grid

Etablierte Community-Grids

- AstroGrid-D
  - Astrophysikalische Analysen
  - Verteilte Daten und Instrumente
- C3Grid
  - Analyse und Processing von Klimadaten, Klimafolgenforschung
  - Verteilte Datenbestände
- HEP-CG
  - Datenanalyse für Grundlagenforschung der Hochenergiephysik
  - Daten des LHC Experiments am CERN
- MediGRID
  - Klinische, biomedizinische und bildverarbeitende Forschung
  - Patientendatenbestände
- TextGrid
  - Infrastruktur für geisteswissenschaftliche Datenverarbeitung
  - Forschungsdaten von Wissenschaftlern und Bibliotheken

Betrachtung von AstroGrid-D

Anforderunge

- Allgemein:
  - untersch
- Nutzer:
  - individue
    Daten, Eigentumsvorbehalte
  - vereinfachte Gruppenbildung
    und einheitlicher Zugang
- Datenprovider:
  - Zugriffsregeln für Daten
  - Nachvollziehbarkeit
  - geringes kommerzielles
    Interesse
- Ressourcenprovider:
  - Nachvollziehbarkeit der Nutzung
    limitierter Ressourcen

1. Persönlicher Zertifikate zur Job-Submission via Globus
2. Dienstnutzung über Dienstezertifikat
3. Interaktiver Zugriff auf Ressourcen (konventionell Username/Passwort)

Umsetzung und Konzepte

- Allg. Sicherheitskonzept:
  - Abbildung von Anforderungen auf Unix-Permissions (VO-Account/Gridmap)
  - Zertifikatsbasierte Nutzung der Grid-Dienste
- Technische Umsetzung
  - VO-Management über VOMRS
  - Usermapping durch eigenen Dienst (ManageLocalGridUser)
  - Globus Toolkit und enthaltene Dienste (gsissh, gsiftp, …)
  - MyProxy

Betrachtung von C3Grid

Anforderunge

- Allgemein:
  - verschie
    unt
    Nutzung
- Nutzer:
  - Einfache Nutzung
  - Sicherheit von Nutzerdaten, Ergebnissen und Produkten
- Datenprovider:
  - Autorisierungsmechanismen
  - Anbindung externer gesicherter Datenbestände
- Ressourcenprovider:
  - Nachvollziehbarkeit der Ressourcennutzung

1. Nutzung persönlicher Zertifikate: personalisierter Zugriff auf Daten und Tools
2. SLCs: Nutzung des SLC-Dienstes des DFN und Heimateinrichtung
3. Nutzung spezieller Dienste über Dienstezertifikate bis hin zu anonymer Nutzung

Umsetzung und Konzepte:

- Konzept der Sicherheits-infrastruktur:
  - Zertifikatsbasiert
  - Vertrauensverhältnis zwischen Diensten
  - Delegation von Nutzeridentität
  - Rechtefestlegung auf Ressourcenebene
- Technische Umsetzung
  - Globus Toolkit 4.0.x
  - DelegationService

Betrachtung von HEP-CG

Anforderunge

- Allgemein:
  - verschie
  - HEP gro
- Nutzer:
  - Photon: Einfache Nutzung , Schutz von Daten und Audit von Zugriffen
  - HEP: keine speziellen Anforderungen
- Datenprovider:
  - Photon: Schutz sensitiver Daten
  - HEP: Daten public domain
- Ressourcenprovider:
  - Schutz vor Ressourcen-Exploit

1. HEP: Datenzugriff via gLite mit grober Zugriffskontrolle über VO-Zugehörigkeit
2. Photon: Webbasierter Datenzugriff mit feingranularer Kontrolle, ACLs und Nutzerrollen

Umsetzung und Konzepte

- HEP:
  - Zertifikate und PKI Infrastruktur, VO Management
  - Technische Umsetzung im Kontext von gLite
- Photon:
  - Sicherheitskonzept in Planung
  - Nutzerverwaltung notwendig
  - Nutzung von Zertifikaten unwahrscheinlich

Betrachtung von MediGRID

Anforderungen:

- Allgemein:
  - mehrere
  - Sich
- Nutzer:
  - Einfachheit der Nutzung
  - Datenschutz für Patientendaten
  - Trackability der Datennutzung durch Patienten
  - Schutz von Ergebnissen und Produkten
- Datenprovider:
  - Datenschutz
  - Audit-Trail (Nachvollziehbarkeit)
  - Accounting / Berechtigungen
- Ressourcenprovider:
  - Ressourcensicherheit

1. Nutzung persönlicher Zertifikate
2. Kurzlebige Zertifikate
3. Dienstezertifikate

Umsetzung und Konzepte

- Konzept der Sicherheitsinfrastruktur:
  - Zertifikatsbasiert
  - Delegation von Nutzeridentität auf Ebene der Middlewaredienste
  - Autorisierung auf Ressourcenebene
- Technische Realisierung:
  - Globus Toolkit 4.0.x
  - DelegationService
  - Secure-DICOM zur Pseudonymisierung von Bilddaten
  - MyProxy-Server
  - Grid Proxy Upload Tool gPUT für Proxy und Credential Management via Portal

Betrachtung von TextGrid

Anforderungen:

- Allgemein:
  - Nutzung
  - Ve…
- Nutzer:
  - Feingra… Rechtemanagement
  - Einfache Nutzung (UI), möglichst ohne Zertifikate
- Datenprovider:
  - Schutz von Datenbeständen
  - Zugriffskontrolle
  - Lizenzrechtliche Anforderungen
- Ressourcenprovider:
  - Nutzeridentifikation

1. Nutzung der Infrastruktur durch einen Rich Client (TextGridLab)
2. Meist Aufgaben- und Projekt-bezogene Anwendungsfälle, die in einem integrierten System ablaufen

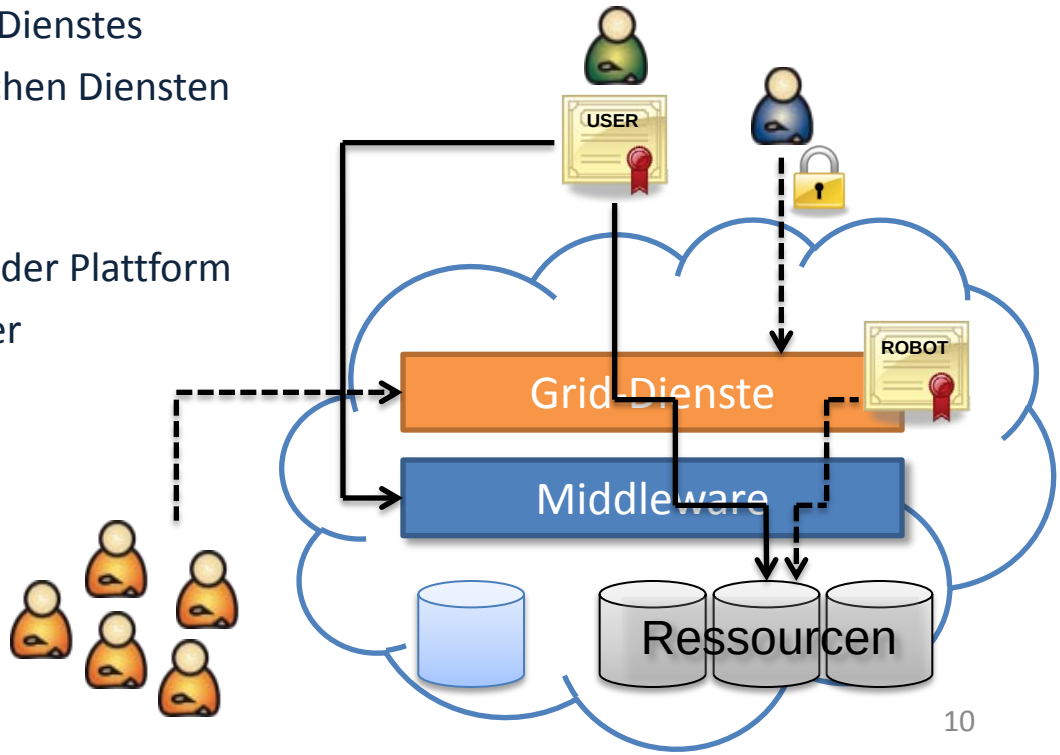
Umsetzung und Konzepte

- Konzept der Sicherheits-infrastruktur
  - Nutzeranmeldung per Username/Passwort
  - Unterliegende zertifikatsbasierte Infrastruktur
  - Single-Sign-On, eigene Lösungen
- Technische Realisierung
  - LDAP, Shibboleth
  - Dienstezertifikat, Vertrauens-verhältnis zw. Diensten
  - Eigenentwicklung TG-auth*

Klassifikation von Zugang und Anforderungen

Zugangswege zur Forschungsplattform

- Persönliche Zertifikate
  - Über Middleware: direkter Zugriff auf Ressourcen oder Job-Submission
  - Delegation der Nutzeridentität an Plattformdienste
- Service- oder Robot-Zertifikate
  - Dienstnutzung über Robot-Zertifikat, Stellvertreterfunktion des Dienstes
  - Vertrauensverhältnis zwischen Diensten und Ressourcenanbietern
- Vollständig offene Nutzung
  - Nutzung unkritischer Teile der Plattform
  - Zugriff als anonymer Nutzer



Klassifikation von Sicherheitsanforderungen

Anforderungen an die Infrastruktur

- *Einfache Nutzbarkeit* (Commandline – Rich Client)

- *Rechtemanagement / Datenschutz* (public domain – Personendaten)

- *Nachvollziehbarkeit* der Nutzung (freie Nutzung – Auditing)

Einordnung der Lösungsansätze

- Authentifizierung: Zertifikatsbasiert in unterschiedlichen Ausprägungen, abhängig von Nutzeranforderungen
  - Direkte Nutzung der persönlichen Zertifikate (langlebig oder kurzlebig)
  - Delegation der Rechte an höherwertige Dienste
  - Kapselung der Zertifikatsnutzung möglich
    - Robot-Zertifikate
    - Portal delegation, gPUT
- Autorisierung:
  - Globale Regelung über VO-Management
  - Individuelle Regelung auf Ressourcenebene (Ressourcenprovider hat letztes Wort)
  - SAML Assertions
  - Abbildung auf Unix-Permissions oder Umsetzung durch proprietäre Dienste
  - Lizenzrechtliche Regelungen noch offen
- Technische Umsetzung:
  - Nutzung von Middleware-Diensten und zugehöriger Sicherheitsinfrastruktur
  - Teilweise Einsatz von Drittanbieter-Technologien (Single-Sign-On)
  - Spezifische Bausteine und Dienste in den Projekten

Zusammenfassende Betrachtung

- Verschiedene Anforderungen der akademischen Communities
  - von großer Erfahrung mit technischen Systemen bis UI-Nutzer
  - von Open Access bis zu kritischen Nutzerdaten
  - von einfacher Nachvollziehbarkeit der Nutzung bis Auditing

➔ Klassifikation der Anforderungen ist aber möglich und erlaubt eine vereinheitlichte Betrachtung

- Verschiedene Lösungen in den Communities
  - sehr vielfältige Technologielandschaft (Middleware, Dienste)
  - oft jedoch mehrere Ansätze für ähnliche Probleme

➔ Vorhandene Ansätze bieten einen guten Einstiegspunkt für neue Communities in das Thema Sicherheit

Zusammenfassende Betrachtung

Wie kann man weiter vorgehen?

➔ Die Arbeit für das Projekt WissGrid beginnt hier und adressiert das Thema

- Dokumentation der Konzepte und des Technologieüberblicks
  - dieser Vortrag stellt den Einstieg dar
  - wird momentan im WissGrid-Projekt erarbeitet
  - Communities sind eingeladen ihre Lösungen einzubringen!
- Aktive Beratung bei der Realisierung
  - Unterstützung neu entstehender Communities bei der Analyse von Anforderungen und der Erstellung spezifischer Konzepte
  - Fachkompetenz
- Fachberaterteam: Thema Sicherheit
  - wird konstituiert aus Mitgliedern der akademischen Community
  - stellt die vielfältige Erfahrung aus den Communities zur Verfügung (nicht nur zum Thema Sicherheit)

➔ Kontakt: fachberater@wissgrid.de