VRE: Management und Virtuelle Organisationen

Virtuelle Forschungsumgebungen aufbauen
mit DGrid

H. Enke, AIP

19.01.2011

Virtual Research Environment (VRE) II

Anliegen:

- Gemeinsames Forschungsvorhaben
- Gemeinsame Datensammlungen / Archive
- Gemeinsame Ressourcennutzung

Bezugsrahmen :

- Fachgebiet
- Interdisziplinäre Gruppen

Organisationsstrukturen:

- Nationale Verbund-Projekte
- Europäische Vorhaben und Verbund-Projekte
- Internationale Zusammenschlüsse

IT-Ressourcen

- Umfang / Komponenten / Verteilung
- Fachspezifische Kultur

Finanzierung - Rahmenbedingungen

Ein VRE benötigt eine flexible und den Anforderungen des Vorhabens leicht anzupassende Organisationsform, in der auch die zugehörigen Ressourcen in adäquater Weise zur Verfügung gestellt werden können: eine Virtuelle Orgaisation (VO).

Die VO stellt insbesondere in Bezug auf IT-Sicherheitsaspekte wichtige Schlüsselfunktionen bereit.

Sicherheitsanforderungen :

Niedrig: Zugang zu Daten in Archiven

GBIF, IVOA Astronomy, Europeana, ...

Lösung: Webserver-Portale

maximal: HTTP basierte Authentifizierung/Autorisierung

Mittel: Zugang zu noch unpublizierten Daten, IT-Ressourcen, Dienste

C3 / Astro / HEP

Lösungen: HTTPS, X509 Zertifikate, Portale, Web-Services

maximal: individuelle Zertifikate, rollenbasierte Autorisierung, Robot-Zertifikate

UNIX-Gruppenrechte

Hoch: Zugang zu Individual-Daten (Datenschutz etc.)

SOFI / Medizin

Lösungen: HTTPS, X509 Zertifikate,

Webservices mit erhöhten Sicherheitsanforderungen,

UNIX-User-und Gruppenrechte, materielle Zugangsbeschr.

Klassifikation von Sicherheitsanforderungen

Anforderungen an die Infrastruktur

- *Einfache Nutzbarkeit* (Commandline – Rich Client)

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

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

Virtuelle Organisationen

- Verwaltung der VO-Mitgliedschaft und der VO-Gruppen durch den VO-Management-Prozess
    - Community basierte Entscheidungsstrukturen
    - Schnelle und leichte Bildung von Arbeitsgruppen
    - X509 Zertifikatsbasierte Authentifizierung
- Web-basierte Mechanismen für das Zertifikats-Management
    - Erfüllung von Sicherheitsanforderungen
    - Zugriff auf Daten in einer Umgebung, die verschiedene Sicherheitskriterien zusammenführt und erfüllt
- Für den einzelnen Nutzer mit weniger Aufwand verbunden

Zertifizierungs-Infrastruktur

Certificate Authorities (CA, Root-CA)

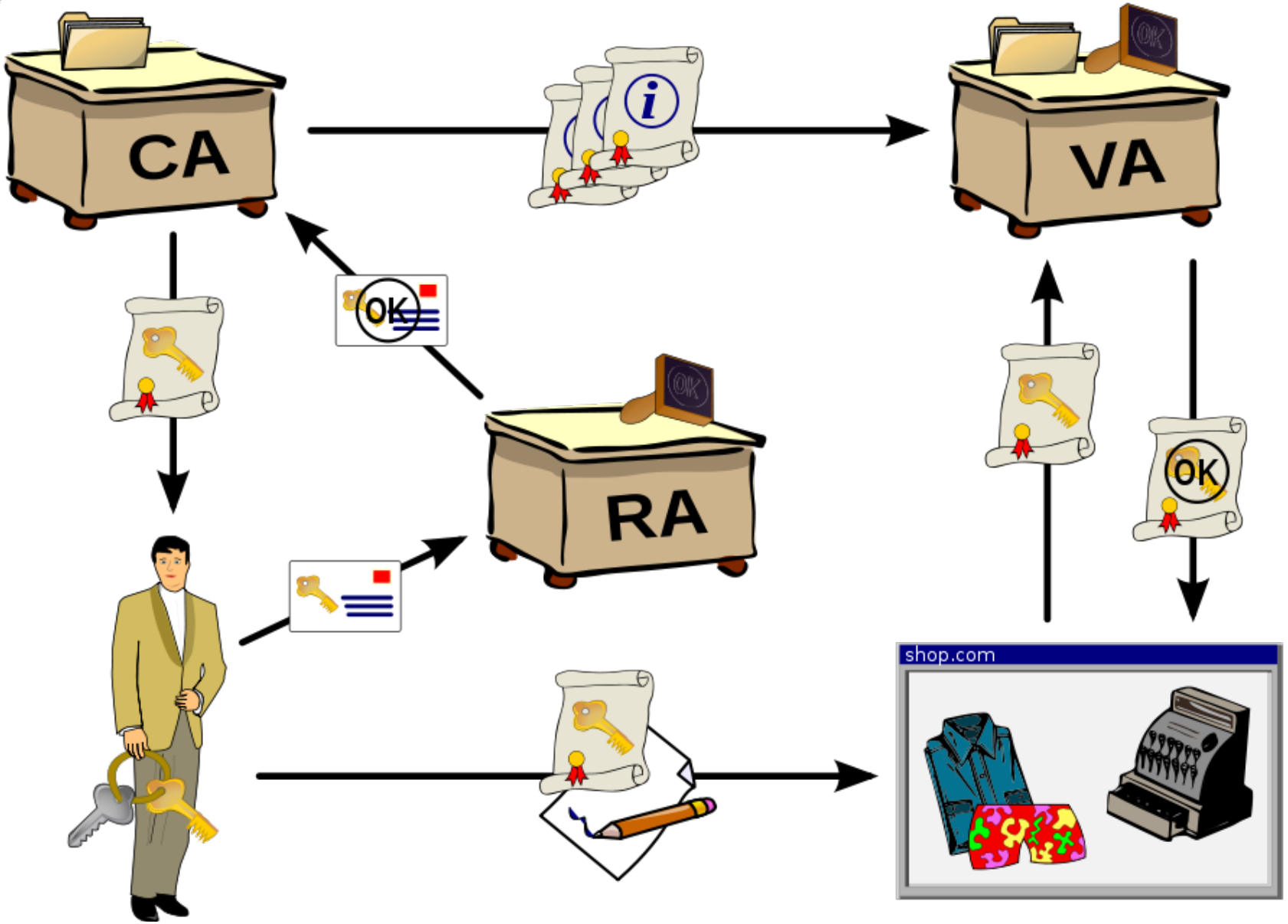
Chain of Trust: Delegation von Vertrauen über Zertifikate

- Internationale Organisationen: IGTF, EUGridPMA, ...
  - Kommerzielle Anbieter: (VeriSign, Thawte,...)
  - Staatliche und quasi-staatliche Zertifikate
    (Niederlande, ELSTER-Zertifikate)

- 2 Root CA in Deutschland (EUGridPMA akkreditiert)
  - GridKA (KIT, ehem. FZK)
  - DFN

- Registration Authorities (RA)
  - Lokale Authentifizierungsstellen für Zertifikatsanträge
  - Nahezu jede Uni und akademische Einrichtung hat eine RA

Public-Key Infrastruktur (PKI) / X509 Zertifikate



DGrid: Security Komponenten

Grid Security Infrastruktur : (Middleware)

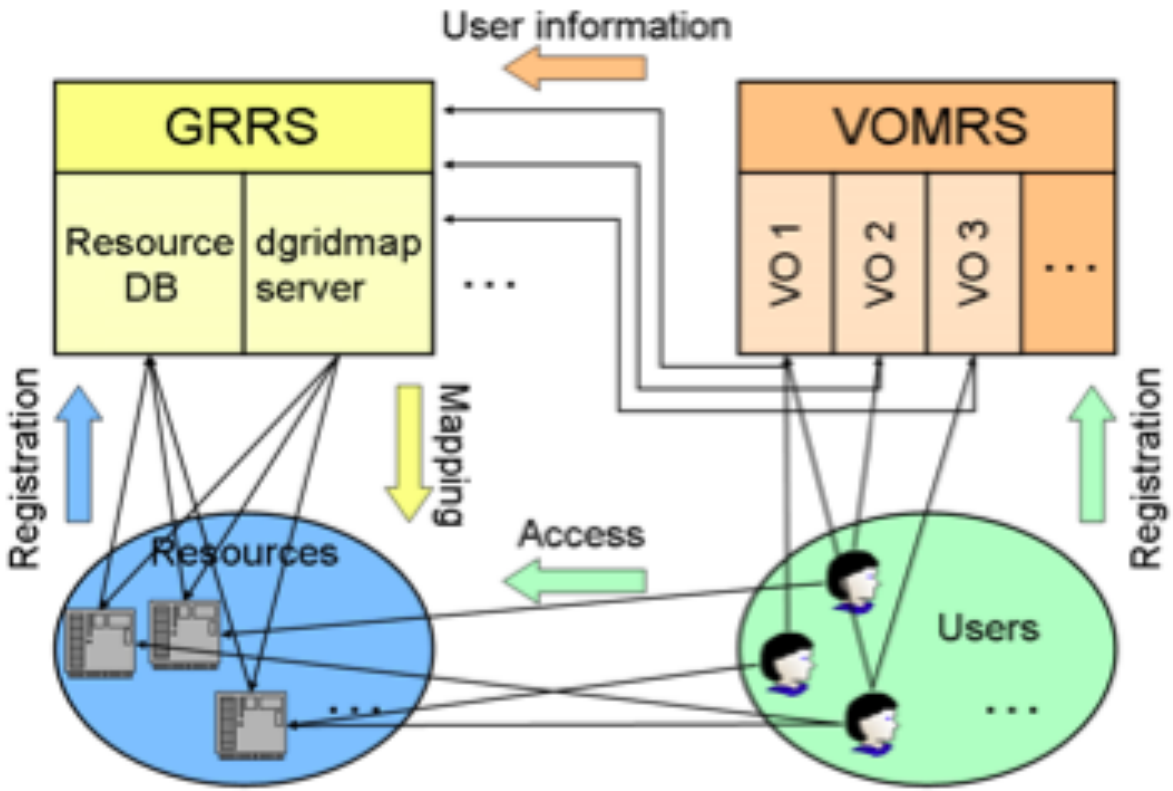
- Zertifikatsbasierte Authentifizierung
  - Durch zeitlich limitierte Proxy-Zertifikate Single-Sign-On
- Vorhandener „Chain of Trust“ durch GridKA und DFN mit (lokalen, universitären oder institutsweiten)

  Registration Authorities (RA) für Zertifikate
- Nutzer basierte Autorisierung auf (lokaler) Grid-Ressource
- Gruppen- und Nutzerrechte bei lokaler Autorisierung
- Virtuelle Organisationen (VO) mit einer (hierarchischen) Struktur
- Einfaches Management der Mitgliedschaft in verschiedenen

  Substrukturen der VO über den

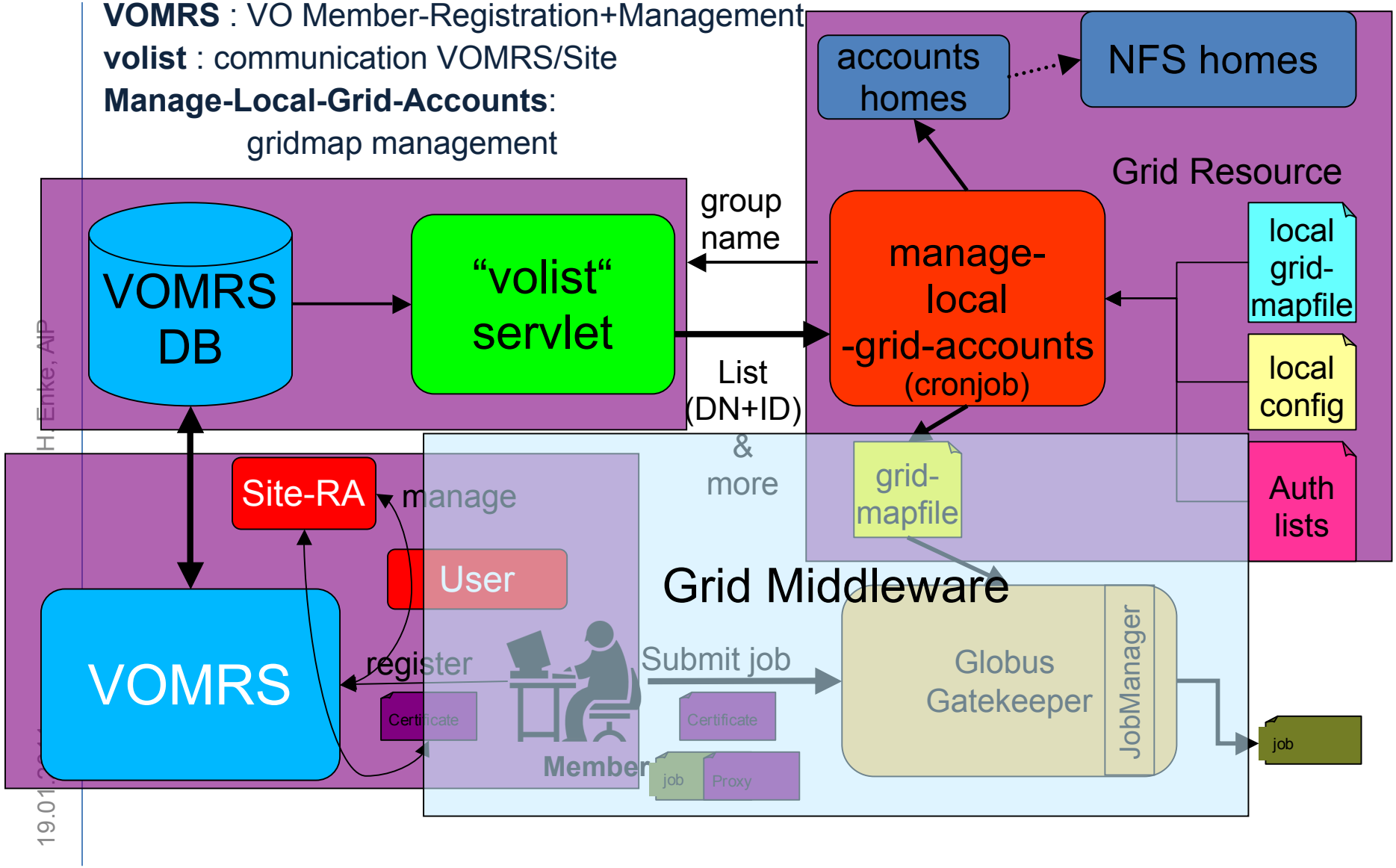
  VO Membership Registration Service (VOMRS)
- Verwaltung des VOMRS durch Community / Projekt

DGrid VO Struktur

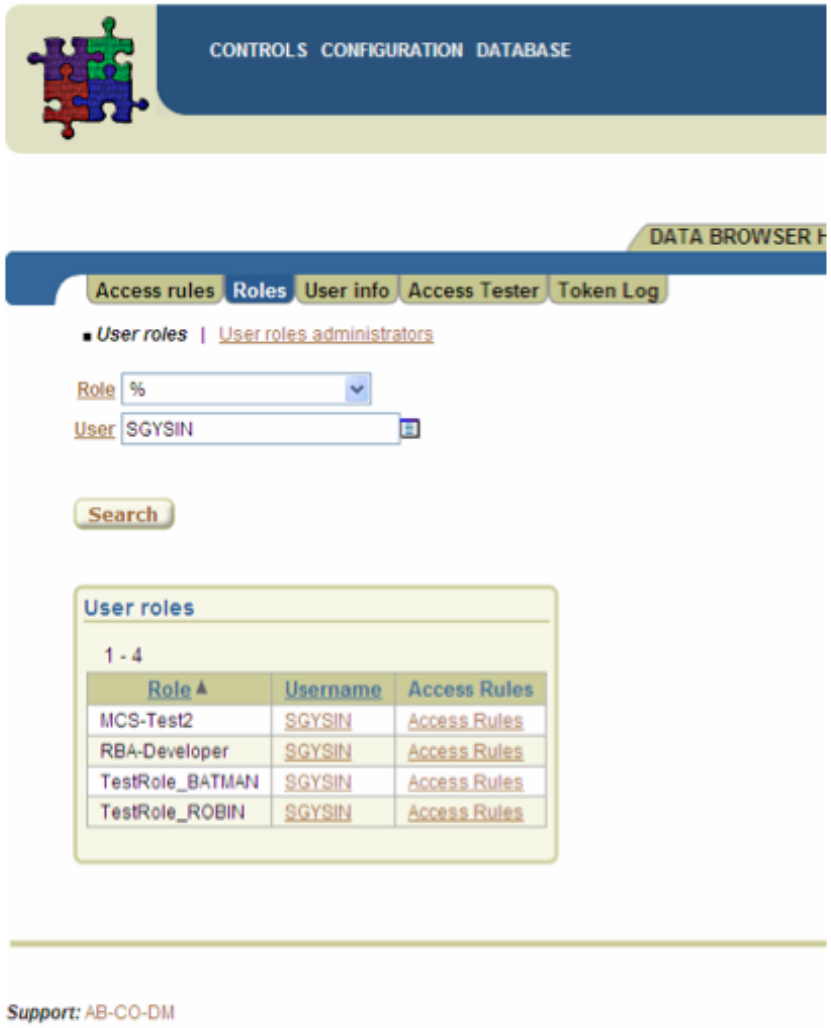


VO/Grid Account Management (Beispiel AstroGrid-D)

VOMRS : VO Member-Registration+Management
volist : communication VOMRS/Site
Manage-Local-Grid-Accounts:
gridmap management



RoleBasedAccessControl



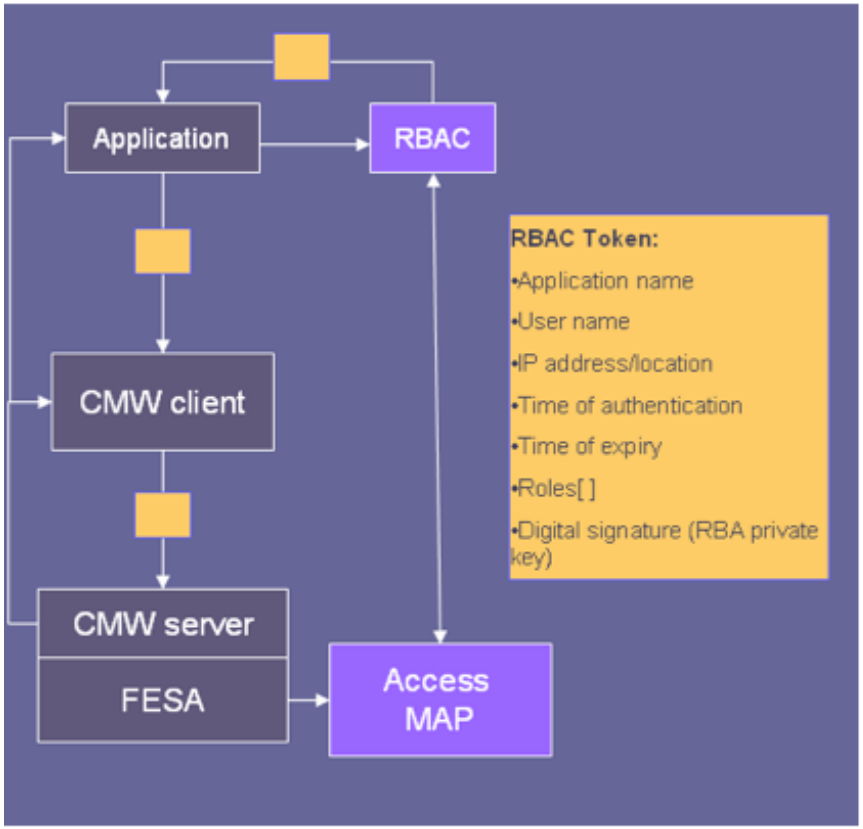


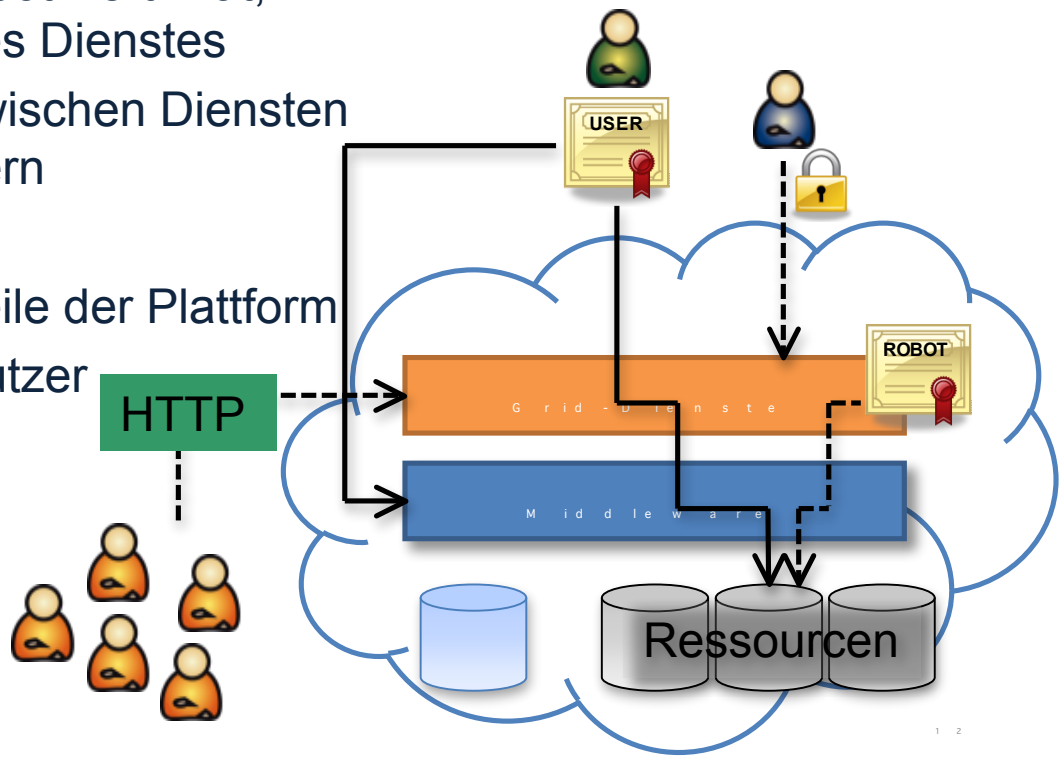
Figure 2: RBAC tokens and access maps.

System for the LHC community

Zugang zu Ressourcen

Zugangswege zur Forschungsplattform

- Persönliche Zertifikate
  - Direkter Zugriff auf Ressourcen oder Zugriff über Middleware
  - 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
- Password basiert
  - HTTP/HTTPS
  - SSH



Einordnung der Grid-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 / Rollen basiert (RBAC)
  - 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