V24
Service Zertifikate und Portal Security
Langfristige Anforderungen an die Sicherheitsmechanismen

Göttingen, 2. April 2008

Jürgen Falkner
Fraunhofer IAO

Ulrich Sax
Universitätsmedizin Göttingen

Fraunhofer IAO Institut Arbeitswirtschaft und Organisation

UMG

MediGRID

Übersicht / Agenda

- Service-Zertifikate und Portal Security
  (Jürgen Falkner)
  - Ausgangssituation und Anforderungen
  - User-Management im Portal / User-Management via VOMRS
  - Zertifikatbasierter Login am Portal
  - Zertifikats- und portalbasierte Nutzung von Anwendungen im MediGRID
  - Unterschiedliche Zugänge zum MediGRID
- Langfristige Anforderungen an die Sicherheitsmechanismen in MediGRID
  (Ulrich Sax)
  - Künftige Nutzungsszenarien
  - Ableitung von Anforderungen an VO-/Rollen-/Rechtemanagement
  - Ableitung von Anforderungen an die Autorisierungsmechanismen im Backend
- Fazit

Übersicht / Agenda

- Service-Zertifikate und Portal Security
  (Jürgen Falkner)
  - Ausgangssituation und Anforderungen
  - User-Management im Portal / User-Management via VOMRS
  - Zertifikatbasierter Login am Portal
  - Zertifikats- und portalbasierte Nutzung von Anwendungen im MediGRID
  - Unterschiedliche Zugänge zum MediGRID
- Langfristige Anforderungen an die Sicherheitsmechanismen in MediGRID
  (Ulrich Sax)
  - Künftige Nutzungsszenarien
  - Ableitung von Anforderungen an VO-/Rollen-/Rechtemanagement
  - Ableitung von Anforderungen an die Autorisierungsmechanismen im Backend
- Fazit

Portalbasierte Grid Nutzung – Security vs. Usability

vs. Performance vs. Affordability…

2 Randbedingungen:

- Hohe Sicherheitsanforderungen in Bioinformatik und Medizin
- Nutzerschaft, die i.d.R. jegliche technischen und organisatorischen Hürden scheut

2 Skill-Level

- Umgang mit PKI möglich
- Umgang mit PKI zu viel Aufwand

2 Sicherheitsstufen

- Verwendung und Verarbeitung von Daten, die Datenschutz unterliegen
- Verwendung und Verarbeitung unkritischer Daten (z.B. Gensequenzen von Tieren)

Automatic VO-based Portal User Management

Situation bisher:

- Nutzer registrieren sich bei einer VO
- Resource Provider können automatisch Nutzerkonten und User Mappings anlegen via Grid Resource Registration Service (GRRS)
- Portal Konten werden von Hand angelegt

MediGRID Lösung:

- ähnlich wie beim Account Management auf den HW-Ressourcen
- Portal bezieht VOMRS Daten für die VO
  - User DN / VO Mitgliedschaft / Gruppen Mitgliedschaft
- Portal Konten werden automatisch angelegt
- Vorteil: User Management nur an einer Stelle (d.h. im VOMRS) -> Grid-weite Konsistenz und Automatisierung

Zertifikatsbasierter Portal Login

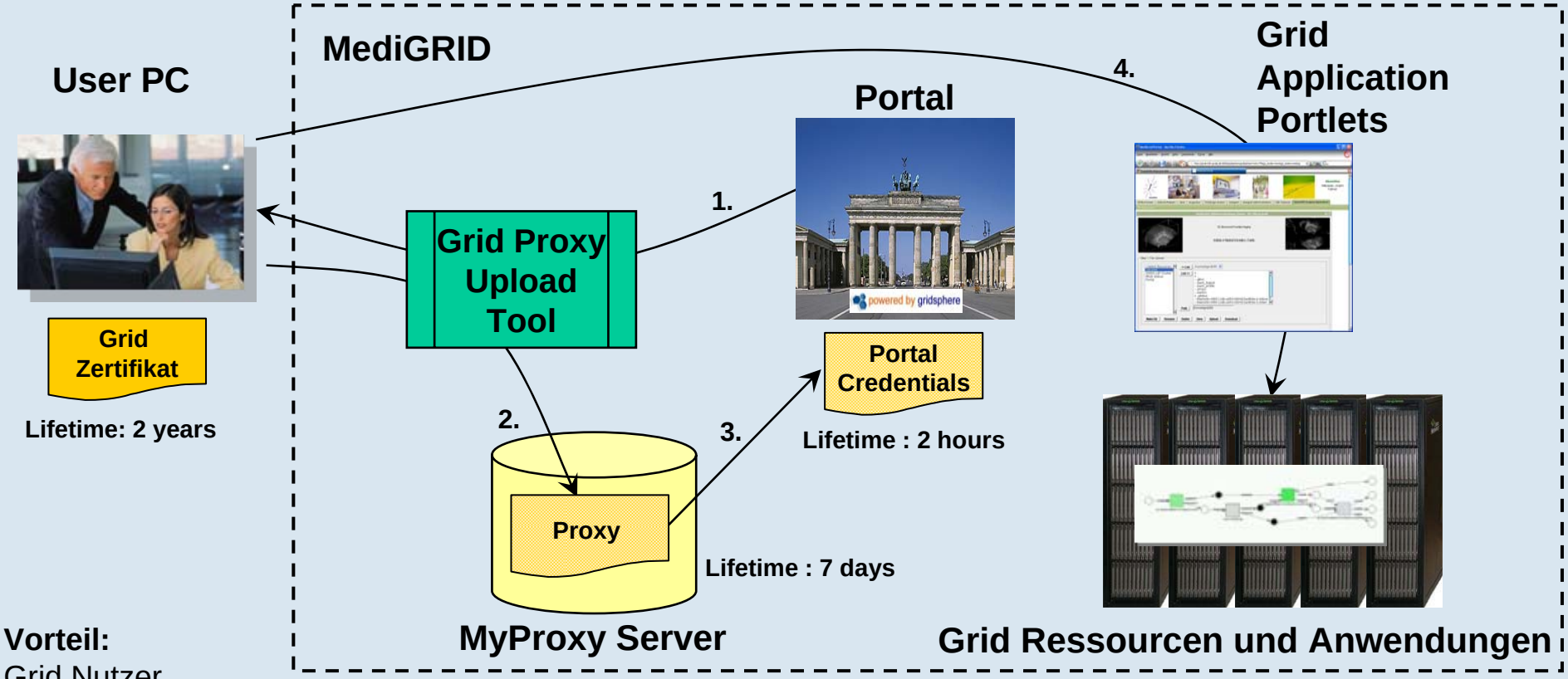
Situation bisher:

- Gridsphere login mit Username/Password
  - Nutzer müssen sich Passwörter merken
  - Nur mittlere Sicherheitsstufe da Passwörter leicht ausgespäht, erraten oder geknackt werden können

MediGRID Lösung:

- Zertifikatsbasierter Login mit Browser Zertifikat
  - Nutzer müssen ihre Zertifikate ohnehin für Grid A&A aufbewahren
  - Kein Vergessen des Passworts
  - höhere Sicherheitsstufe da es sehr viel schwerer ist den Private Key zu stehlen
  - DN-basierte Selbst-registrierung am Portal möglich

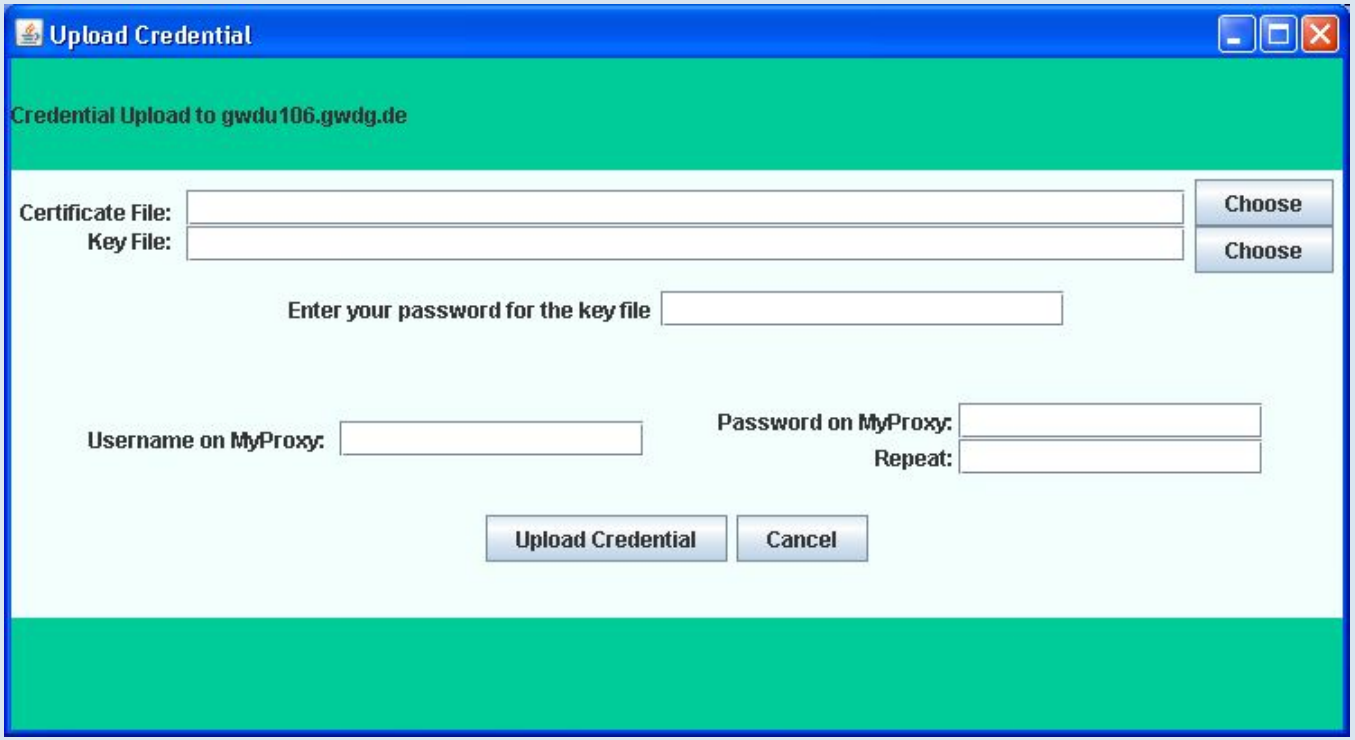
Credential Upload ins Grid



Vorteil:
Grid Nutzer **brauchen keinen** direkten Zugang zu einem Grid Konten/ **keine** Middleware-Installation nötig

1. Portal Authentifizierung/Download des Proxy Upload Tools via Java Webstart
2. Erzeugen eines Proxys und Upload auf den MyProxy Server
3. Erzeugen von Credentials im Credential Management Portlet
4. Nutzung der Portal Anwendungen mit zertifikatsbasierter Autorisierung

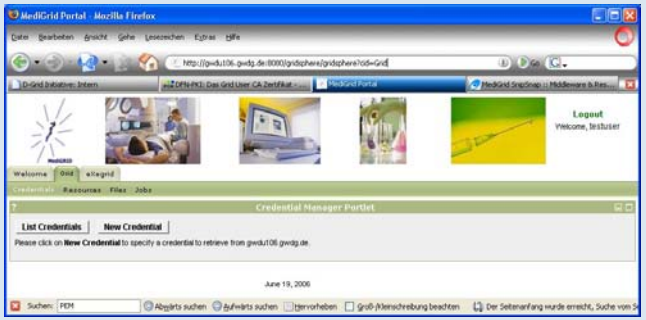
Grid Proxy Upload Tool

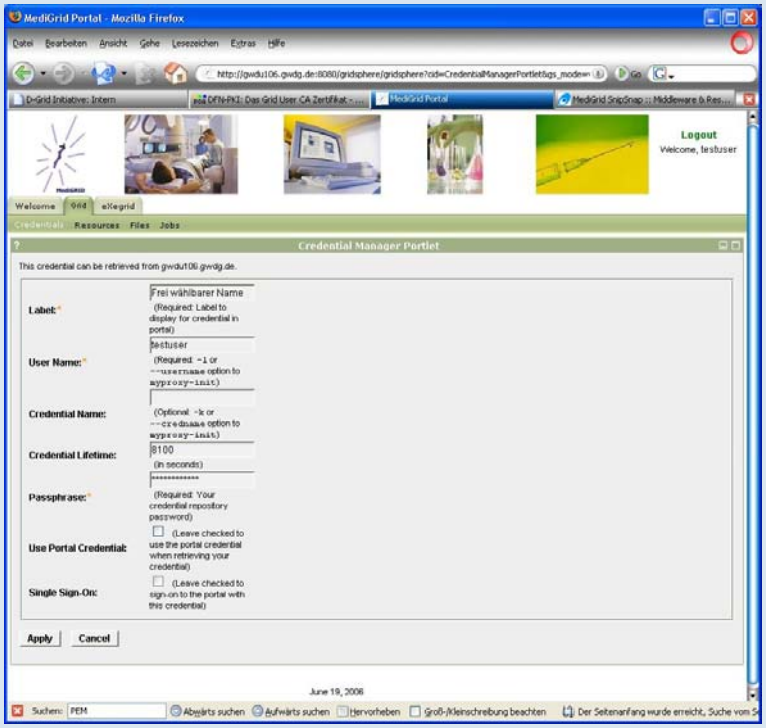


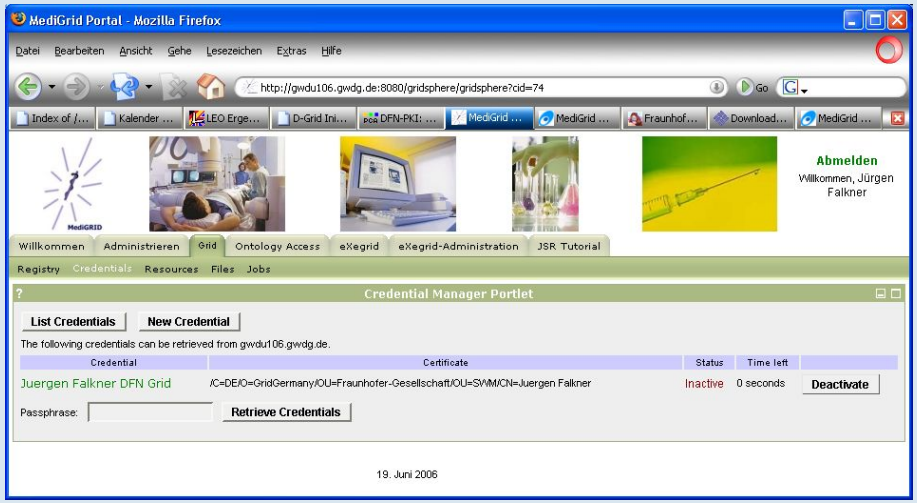
Tool ist für MediGRID vorkonfiguriert

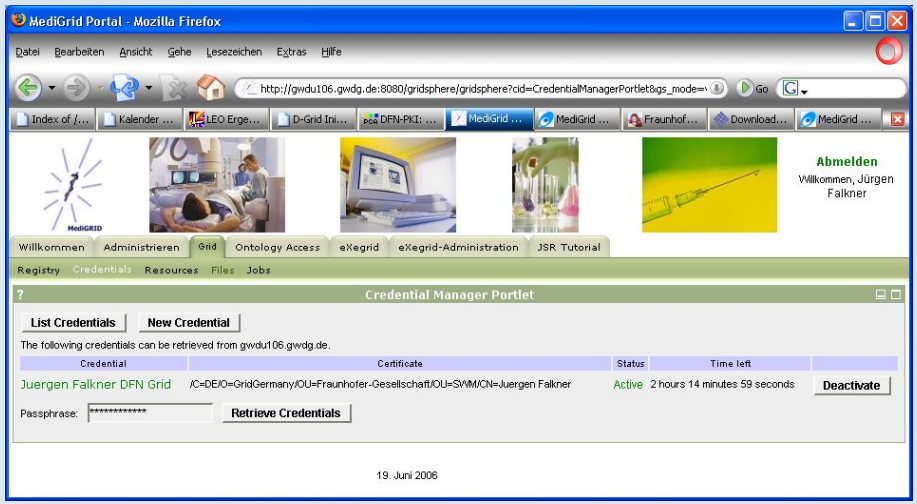
- kein Konfigurationsaufwand beim Nutzer
- Anpassung an unterschiedliche Umgebungen erfolgt serverseitig durch Admin

Credential Management Portlet

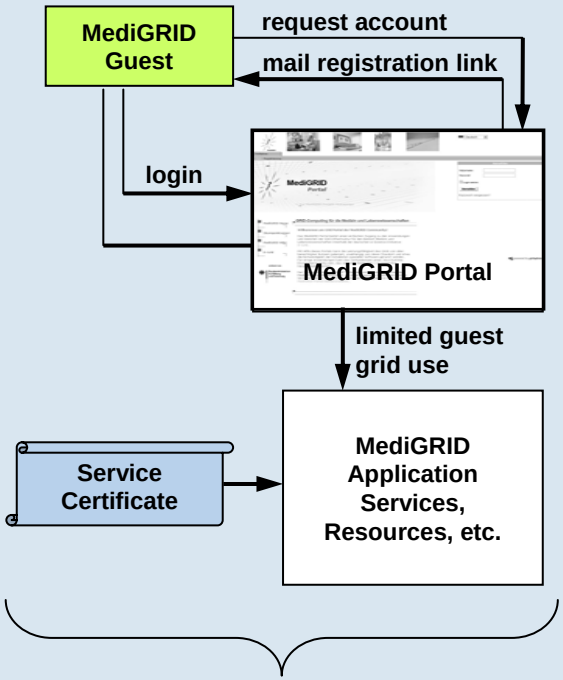






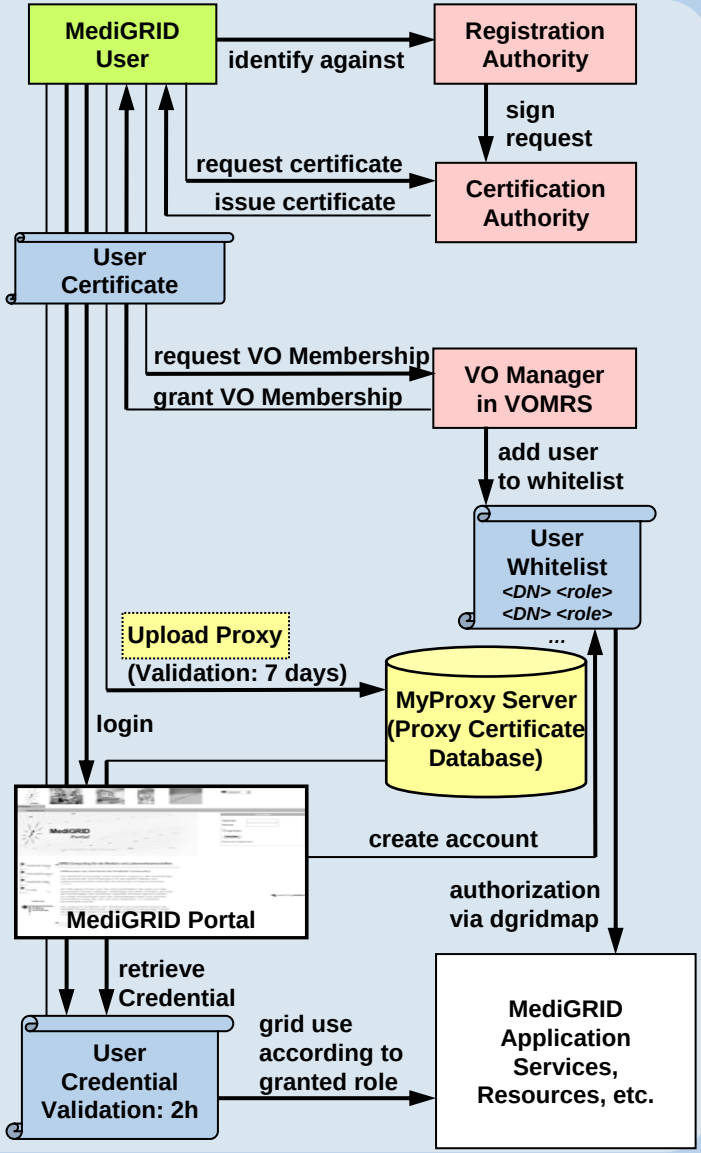


Sicherer Zugang zu MediGRID



Guest-User Registration

Standard-User Registration



Gastnutzer Registrierung – Zusammenfassung

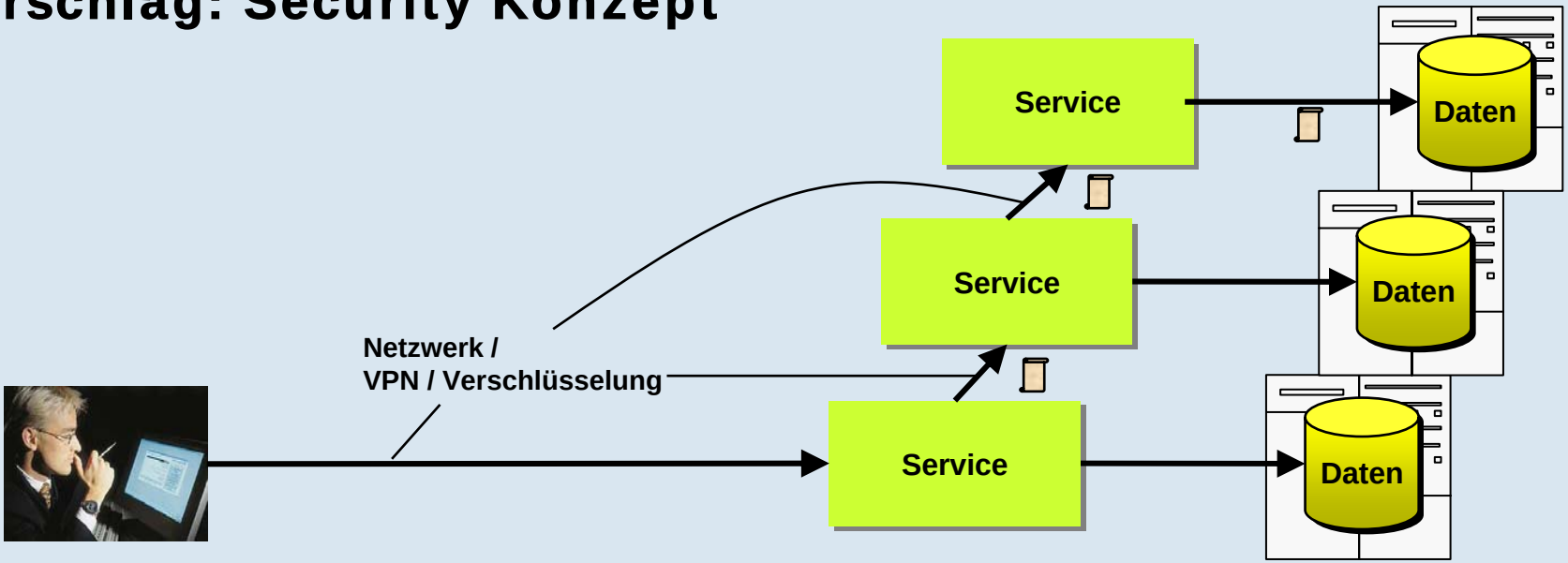
Gast-Nutzer:

- kein Nutzerzertifikat erforderlich
  - d.h. keine RA aufbauen, keine Zertifikate besorgen, keine Anmeldung am VO-Management System, kein Zertifikatsupload zum MyProxy Server, keine Konfiguration des Credential Management Portlets, kein Credential Retrieval
- Selbstregistrierung am Portal
- Überprüfung der E-Mail-Adresse des Nutzers via Registration Link
- personalisierte Gastnutzer Accounts (mit Login/Passwort)
- in beschränktem Maße rückverfolgbar

Anwendungen:

- benötigen Service-Zertifikate
- technisch: Grid-Server-Zertifikat
- im VOMRS: werden als Nutzer im VOMRS registriert
- verwenden immer eigenes Server-Zertifikat für jegliche Nutzung
- Service-Provider / Service-Admin trägt letztenendes die Verantwortung für seine Gast-Nutzer

Vorschlag: Security Konzept



- Weiterleitung der Nutzer-Einstufung zwischen den Services (Single Sign-On)
- Services wissen, ob sie sich gegenseitig vertrauen können – und welche Aktionen für den anderen Service zulässig sind
- Service-Service-Kommunikation verschlüsselt über PKI
- Frage: End-to-End-Verschlüsselung? (hier packt jeder Service das Paket aus und verpackt es erneut… -> Skalierbarkeit…?)

Übersicht / Agenda

- Service-Zertifikate und Portal Security (Jürgen Falkner)
  - Ausgangssituation und Anforderungen
  - User-Management im Portal / User-Management via VOMRS
  - Zertifikatbasierter Login am Portal
  - Zertifikats- und portalbasierte Nutzung von Anwendungen im MediGRID
  - Unterschiedliche Zugänge zum MediGRID
- Langfristige Anforderungen an die Sicherheitsmechanismen in MediGRID (Ulrich Sax)
  - Künftige Nutzungsszenarien
  - Ableitung von Anforderungen an VO-/Rollen-/Rechtemanagement
  - Ableitung von Anforderungen an die Autorisierungsmechanismen im Backend
- Fazit

Anwendungsklassen

- **Projekte mit**

AK1	• Daten bzw. Material nicht von “Mensch” • Anonymisierte Daten bzw. Material von Patienten
AK2	• Anonymisierte Daten bzw. Material von Patienten mit Re-Identifizierungsrisiko (z.B. genomische Daten)
AK3	• Pseudonymisierte Daten bzw. Material von Patienten • Nicht pseudonymisierte Daten bzw. Material von Patienten

Anwendungsklasse 1

- Daten bzw. Material nicht von “Mensch”
- Anonymisierte Daten bzw. Material von Patienten

- geringe Datenschutzanforderungen
- Service-Zertifikate
- Focus auf Akzeptanz und Bedienbarkeit
- Focus auf Intellectual Property (Industrie)

MediGrid Portal - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten

Adresse https://portal.medigrid.de/gridsphere/gridsphere?cid=snpselection Wechseln zu Links

Vorwärts




Abmelden

Willkommen, Ulrich Sax

Willkommen | Grid Workflows | Monitoring | D-GRDL | D-GRDL Admin | Grid | Genetic Tools | MediGRID Image processing | Ontology Tools

SNPSelection

Info / Help

SNPSelection

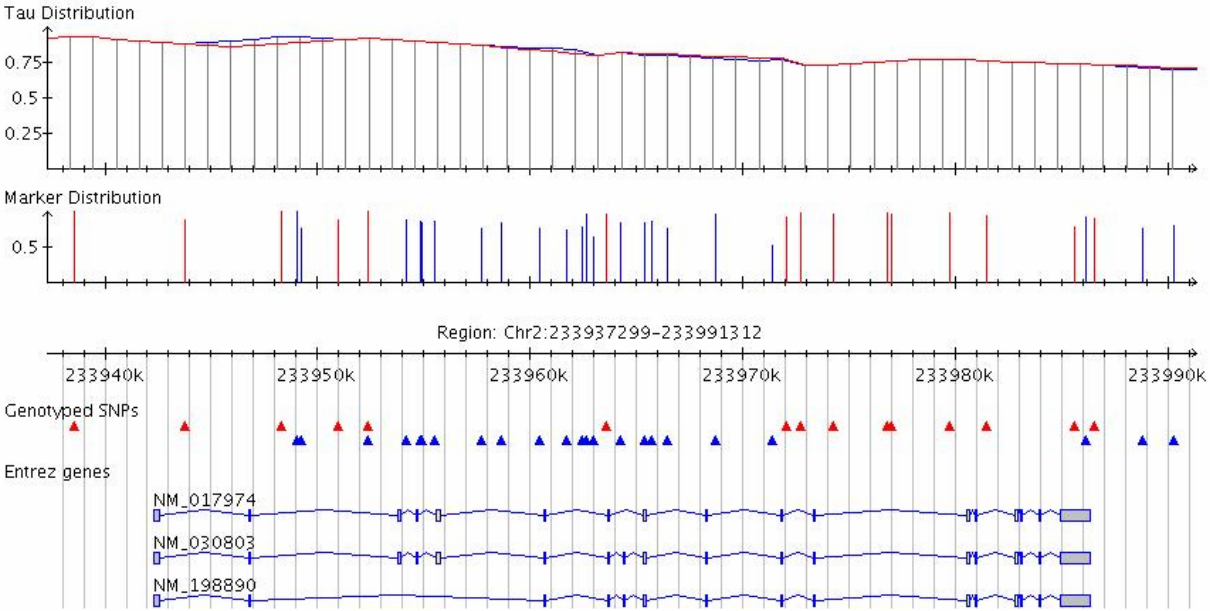
Results

Selection Parameter:

Target Amount	16
Population	YRI
Vendor	HapMapRel20
Region:	NM_030803

Region Information

16 from 40 marker were selected in defined interval.



Tau Distribution

Marker	Q1	median	Q3

Start EndNote 9 -... Posteingan... 47 Erinneru... http://www... MediGRID H... MediGrid Po... 2 Window... Microsoft P... DE 08:20

Anwendungsklasse 1: Services@MediGRID

PHARMAFORSCHUNG

Hamburg wird zur Spitzenadresse Europas

Unter dem Namen European Screening Port Hamburg hat jetzt ein Zentrum für die moderne Wirkstoffforschung. Sein Ziel ist es, Wirtschaft und Wissenschaft enger zu vernetzen. Der Fördertopf des Bundes ist 800 Millionen Euro schwer.

Die im Juli dieses Jahres von Bundesforschungsministerin Annette Schavan gestartete Initiative soll die Pharma-Forschung stärken. Foto: AFP

European Screening Port c.a.r.u.s, Evotec in Services@MediGRID

High Throuhput Screening (HTS) bei Bayer Technology Services in Services@MediGRID

High Throughput Screening (HTS)

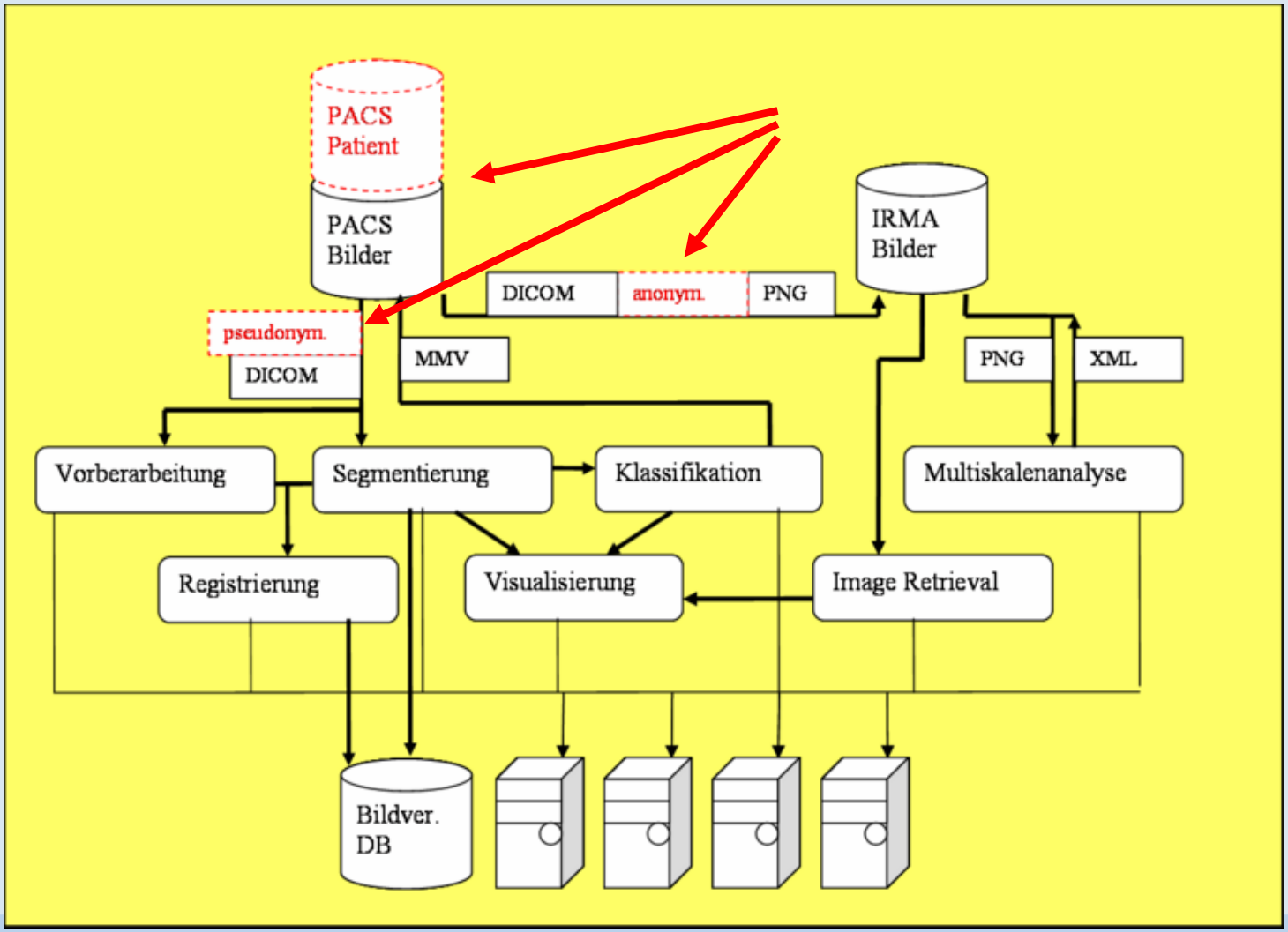
Quelle: Bayer http://www.viva.vita.bayerhealthcare.de/uploads/tx_csrbayernews/Gen_001_01.jpg

Anwendungsklasse 2

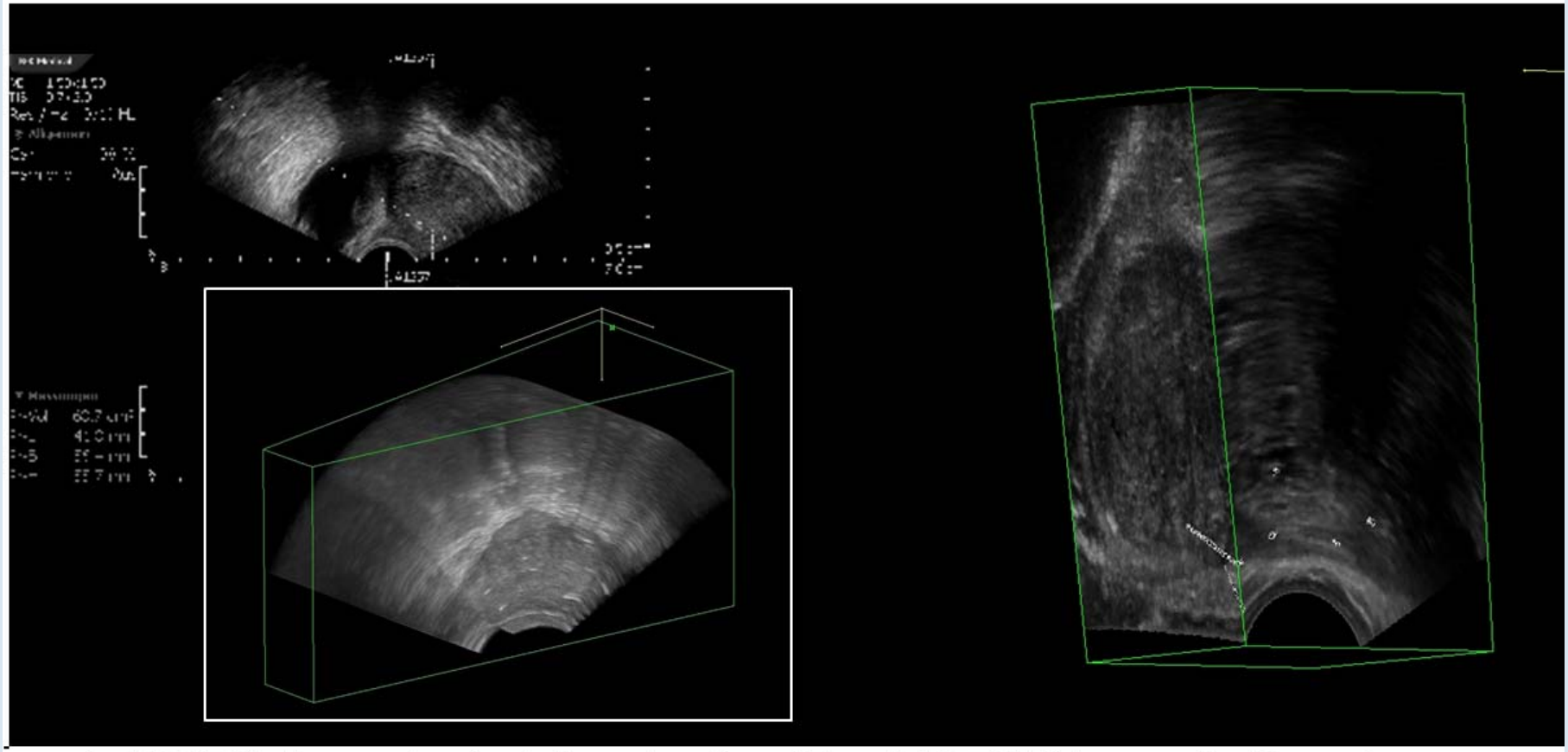
- Anonymisierte Daten bzw. Material von Patienten mit Re-Identifizierungsrisiko (z.B. genomische Daten, Bilddaten)

- höhere Datenschutzanforderungen
- Pseudonymisierungsdienst
- Reidentifizierungsrisiko senken z.B. durch Trennung der Datenbestände (Binning)
- KEINE Service-Zertifikate
- Dennoch: Focus auf Akzeptanz und Bedienbarkeit

AK2: MediGRID BV: Prostatabiopsie - workflow



AK2: MediGRID BV: Prostatabiopsie - Result



a) PROBIP: Integrating the information from 2D and 3D TRUS images for diagnosis support and therapy planning.

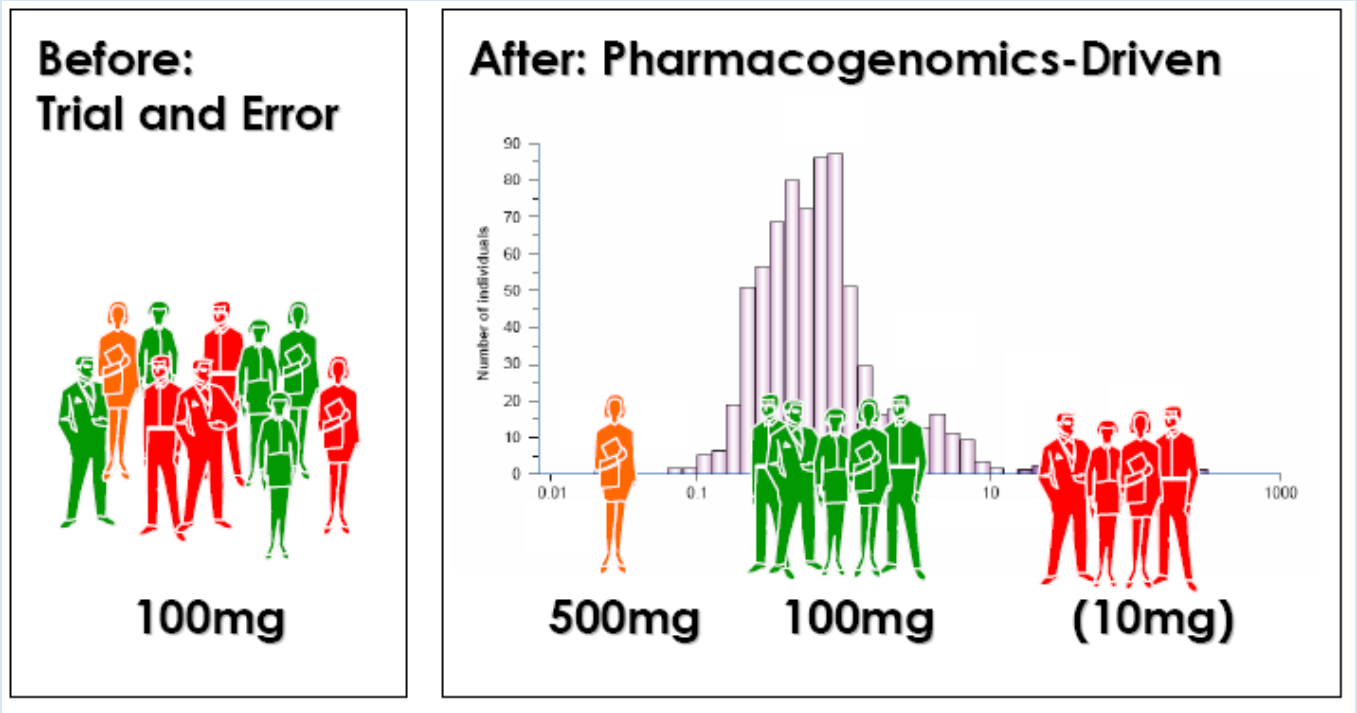
Anwendungsklasse 3

- Pseudonymisierte Daten bzw. Material von Patienten
- Nicht pseudonymisierte Daten bzw. Material von Patienten

- → Forschung

Individualisierte Medizin

Novel Markers for Response and Toxidity beyond Pharmacogenomics



Quelle: http://www.fda.gov/cder/genomics/scienceForum2005.pdf

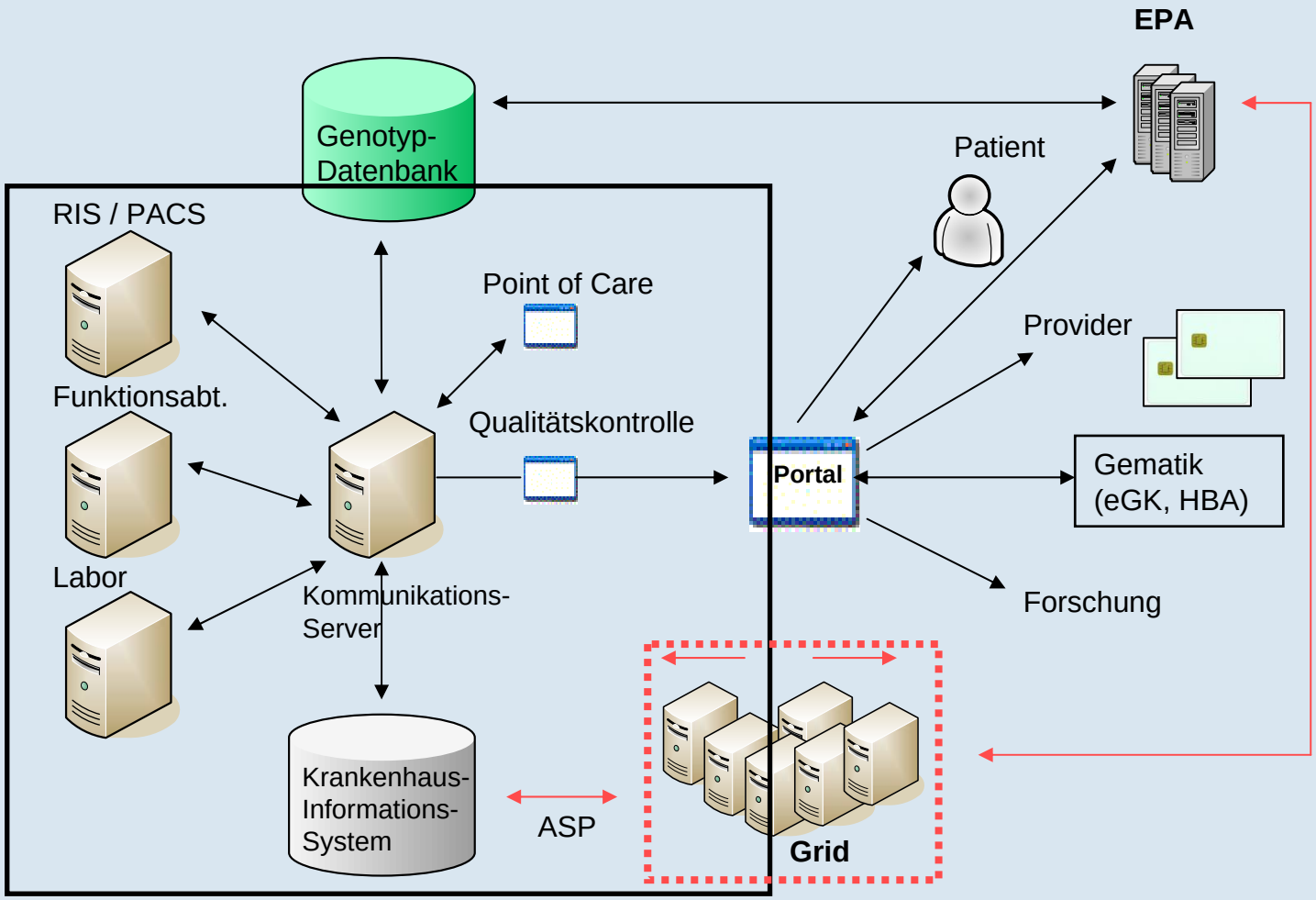
Anwendungsklasse 3

- Pseudonymisierte Daten bzw. Material von Patienten
- Nicht pseudonymisierte Daten bzw. Material von Patienten

- → Forschung
- → Versorgung

- hohe Datenschutzanforderungen
- Pseudonymisierungsdienst, Ethikvoten, Datenschutzkonzepte
- Reidentifizierungsrisiko senken z.B. durch Trennung der Datenbestände (Binning)
- KEINE Service-Zertifikate
- Focus auf Rechtskonformität (FDA, GCP, MPG etc.)

Architektur: Grid-Services für EPA



Klinikbereich

Quelle: Sax, Weisbecker: Telemed 2007, Berlin

Implikationen für die IT: Ausblick auf EHR Grid Services

Storage

- Massendatenverwaltung (Rohdaten)
- incl. Verschlüsselung und Replikatverwaltung

Retrieval

- Vergleich mit ähnlichen Fällen
- Kontrollierte Freigabe für Forschung und für Versorgung

Präsentation

- Rendering, Segmentierung etc. bei Bildverarbeitung
- Korrelationsmechanismen als Grid-Services

Sicherheit

- AAI (eGK, HBA), Pseudonymisierung, Verschlüsselung, feingranulare Zugriffsrechte auf Datenbestände
- Audit, Tracking

Quelle: Sax, Weisbecker: Telemed 2007, Berlin

Anwendungsklassen

- **Projekte mit**

AK1
- Daten bzw. Material nicht von “Mensch”
- Anonymisierte Daten bzw. Material von Patienten

AK2
- Anonymisierte Daten bzw. Material von Patienten mit Re-Identifizierungsrisiko (z.B. genomische Daten)

AK3
- Pseudonymisierte Daten bzw. Material von Patienten
- Nicht pseudonymisierte Daten bzw. Material von Patienten

- **Verantwortlichkeit für Daten / Material**
  - Erhebung
  - Transport
  - Verarbeitung
- **Rollenbasierte Zugriffskontrolle in dynamischen Systemen**
- **Transparenz für den Patienten**

Langfristige Sicherheitsanforderungen für HealthGrids

Voraussetzungen für HealthGrids
- Stabilität
- Bedienbarkeit, Akzeptanz
- Verbindlichkeit

Voraussetzungen für Phase I**:**
- Grundlegende Infrastruktur (AAI)
- Audit trails (!)
- Beobachtung der HBA und eGK-Projekte im Hinblick auf Phase II

Voraussetzungen für Phase II**:**
- Feingranlulare Zugriffsrechte nicht nur im Frontend
- Präzise Abstimmung mit Backend-Providern **(Spezialisierung?!!)**
- Berücksichtigung andere PKI-Projekte (HBA, eGK, eCard Österreich etc.)

Voraussetzungen für Phase II**: Trackability** (Policies +)

V24
Service Zertifikate und Portal Security
Langfristige Anforderungen an die Sicherheitsmechanismen

Göttingen, 2. April 2008

Jürgen Falkner
Fraunhofer IAO

Ulrich Sax
Universitätsmedizin Göttingen

Fraunhofer IAO Institut Arbeitswirtschaft und Organisation

UMG

MediGRID