Einfache Nutzung von D-Grid Zertifikaten

Jürgen Falkner, Fraunhofer IAO

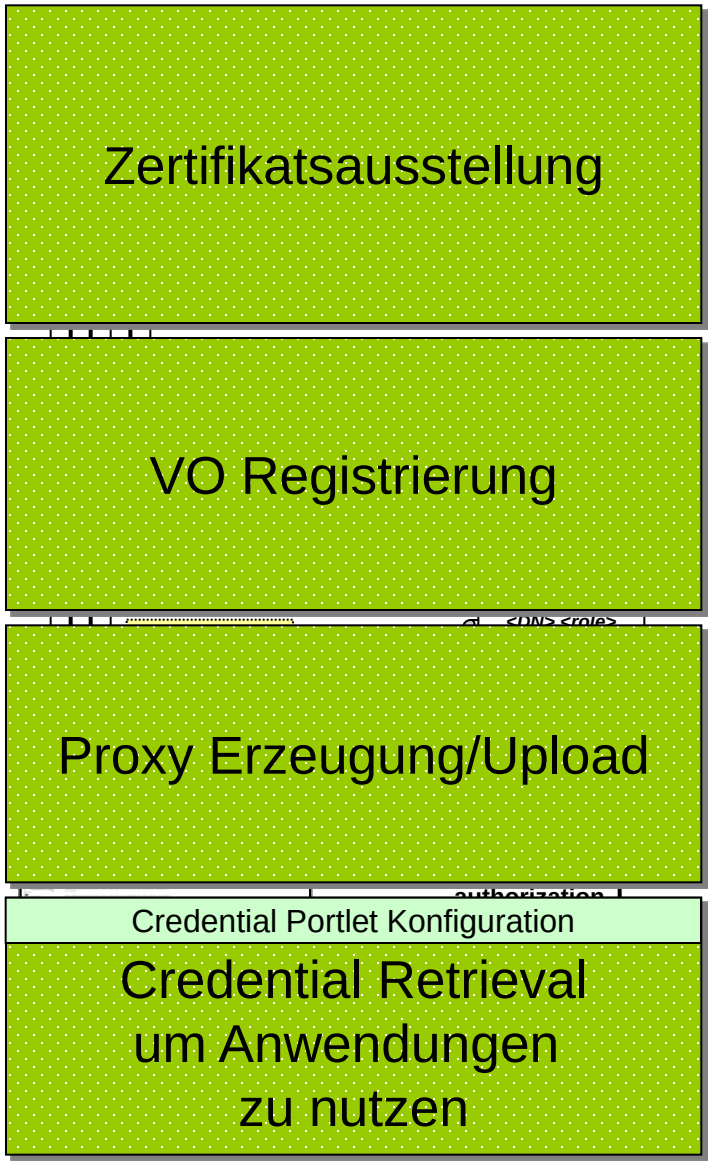
Projekt Gap-SLC

5. D-Grid Security Workshop, Göttingen

Motivation

- **Ausgangssituation**
  - Nutzerkreise mit geringen Erfahrungen bei der Verwendung von persönlichen Zertifikaten
  - hohe Einstiegsschwelle ins Grid
  - PKI-Nutzung aufwändig und komplex
  - gleichzeitig teils hohe Sicherheitsanforderungen
- **Ziele in Gap-SLC**
  - Senkung der Eingangsschwelle ins Grid
  - Verbreiterung der Nutzerbasis
  - Bereitstellung von Lösungen im Bereich AAI für die CGs

Zugang zum GRID bisher



einmalig

1x pro Woche

jede Anwendung

Task 6:

Vereinfachung der Authentifizierung mittels PKI-Zertifikaten für den Nutzer

Problemstellung

Zu lösende Probleme

- 1) Firewall-Problematik
  - Java Webstart und Applets laufen auf dem Nutzerrechner
  - Proxy Upload Tool (Webstart/Applet) baut eine direkte Verbindung vom Nutzerrechner zu Port 7512 des MyProxy Servers auf
  - Restriktive Firewalls (z.B. klinische) erlauben ausschließlich Kommunikation mit Port 80 (HTTP) und 443 (HTTPS)
- Lösung
  - Implementierung als Applet / Servlet Konstrukt
  - Das Applet läuft auch lokal beim Nutzer
    - Proxyerzeugung weiterhin lokal
    - Private Key des persönlichen Schlüsselpaars verlässt den Rechner nicht
  - Upload des Proxies erfolgt zunächst an ein Servlet im Portal
  - Dort erfolgt ein Redirect an den MyProxy Server
  - Der Nutzer kommuniziert ausschließlich über HTTPS (Port 443 des Portals)

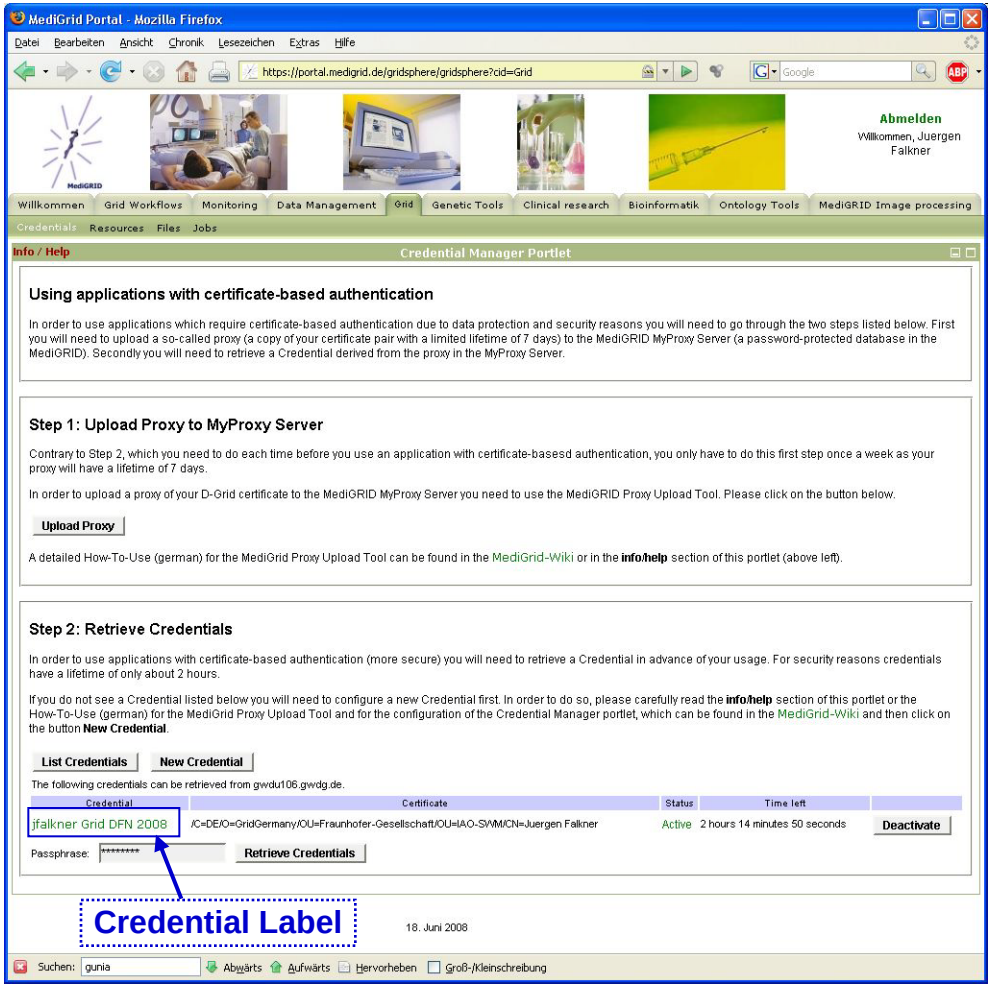
Zu lösende Probleme

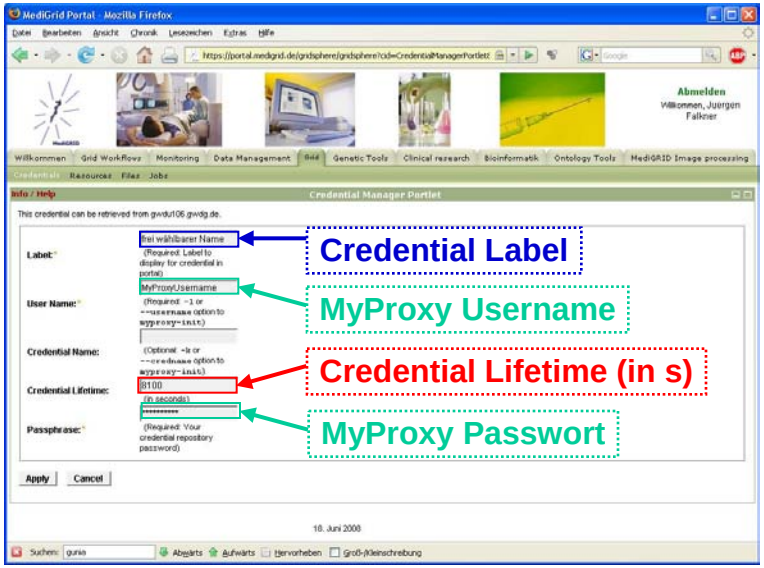
- Bedienbarkeit
  - Diverse Eingaben erfolgen bisher doppelt
  - Wenn diese Eingaben differieren erfolgen Fehler, die den Nutzer verwirren
  - Lösung: engere Integration von gPUT mit Credential Portlets und Login Portlets
- Formatswirrwarr
  - Der Nutzer erhält sein Zertifikat i.d.R. als PKCS12 (Dateiendung „.p12“)
  - Um ein Proxy zu erzeugen wird aber das PEM Format benötigt
  - Ein (automatischer) Konvertierungsmechanismus ist erforderlich
  - Problem: der Nutzer muss die Java Cryptography Extension installiert haben – diese ist NICHT Bestandteil der Standard Java Runtime (rechtliche Beschränkungen in US-Ausfuhrbestimmungen)
  - Lösung: One-Click-Installation der JCE durch gPUT

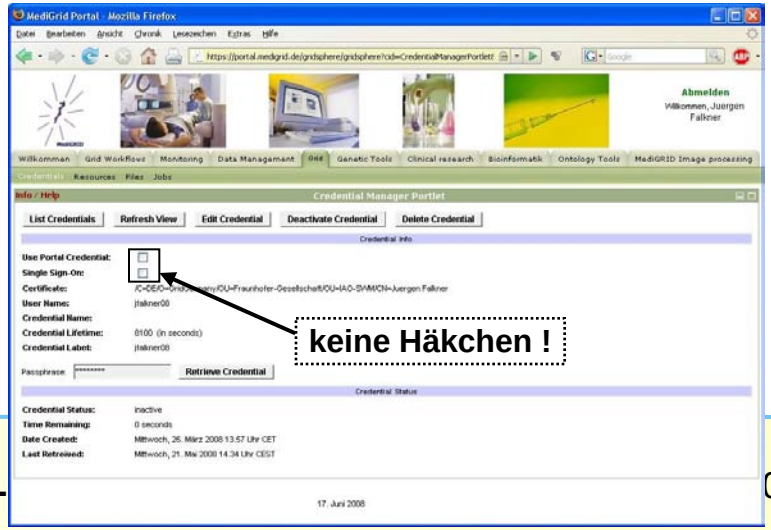
Zu lösende Probleme

- Proxy und Credential Lifetime
  - Credential Lifetime muss größer sein als die voraussichtliche (und vor allem als die tatsächliche) Job-Lifetime
  - GridSphere: Credential Lifetime muss fest im Credential Manager konfiguriert werden
    => Konfiguration überfordert die Endanwender
  - Proxy Lifetime muss größer sein als die gewünschte Credential Lifetime
  - Proxy Lifetime i.d.R. nur über Kommandozeilen-Clients frei wählbar

T6: Credential Management
Portlet Konfiguration





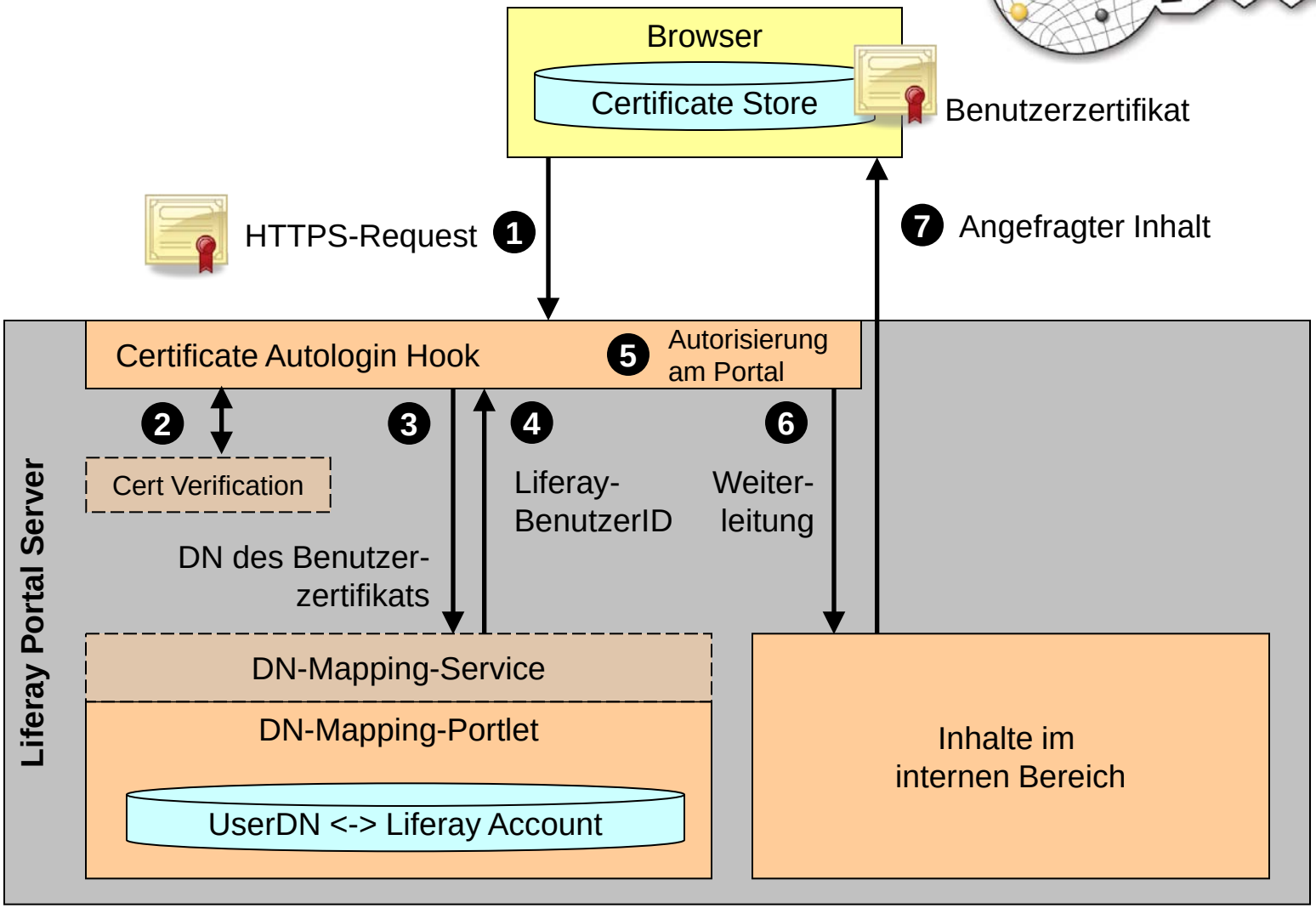


Task 6:

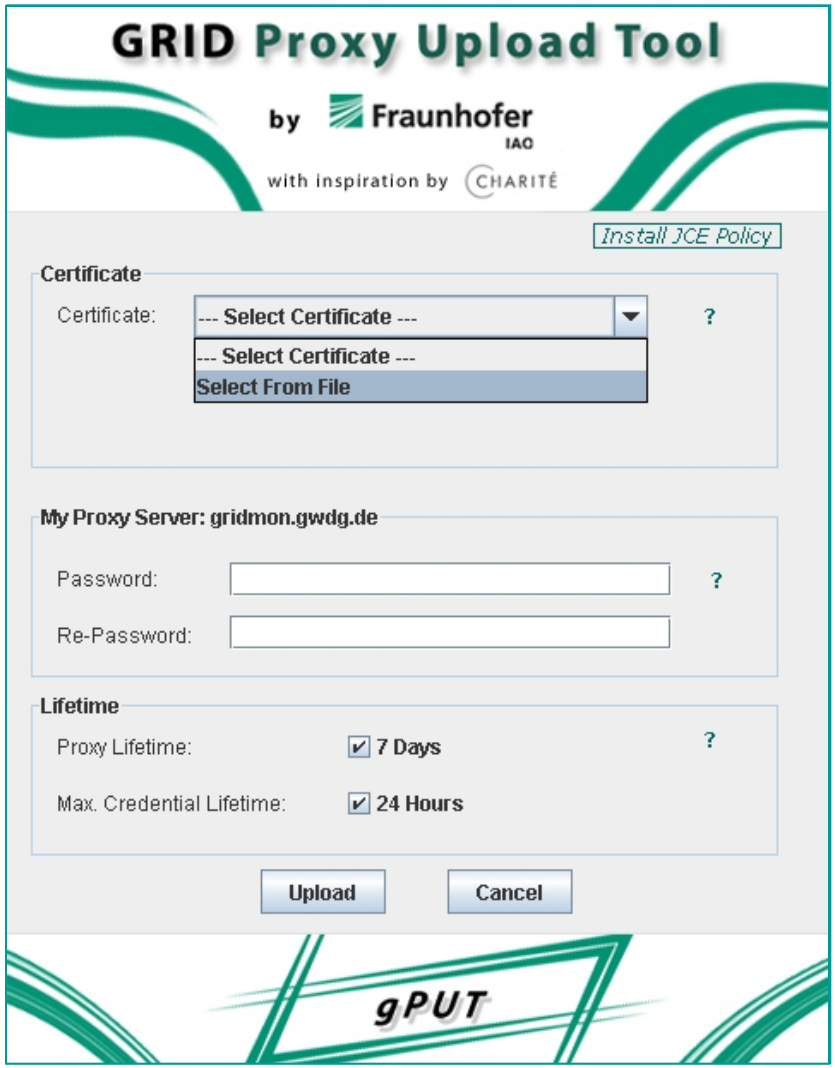
Vereinfachung der Authentifizierung mittels PKI-Zertifikaten für den Nutzer

Lösung

Liferay Login mit PKI

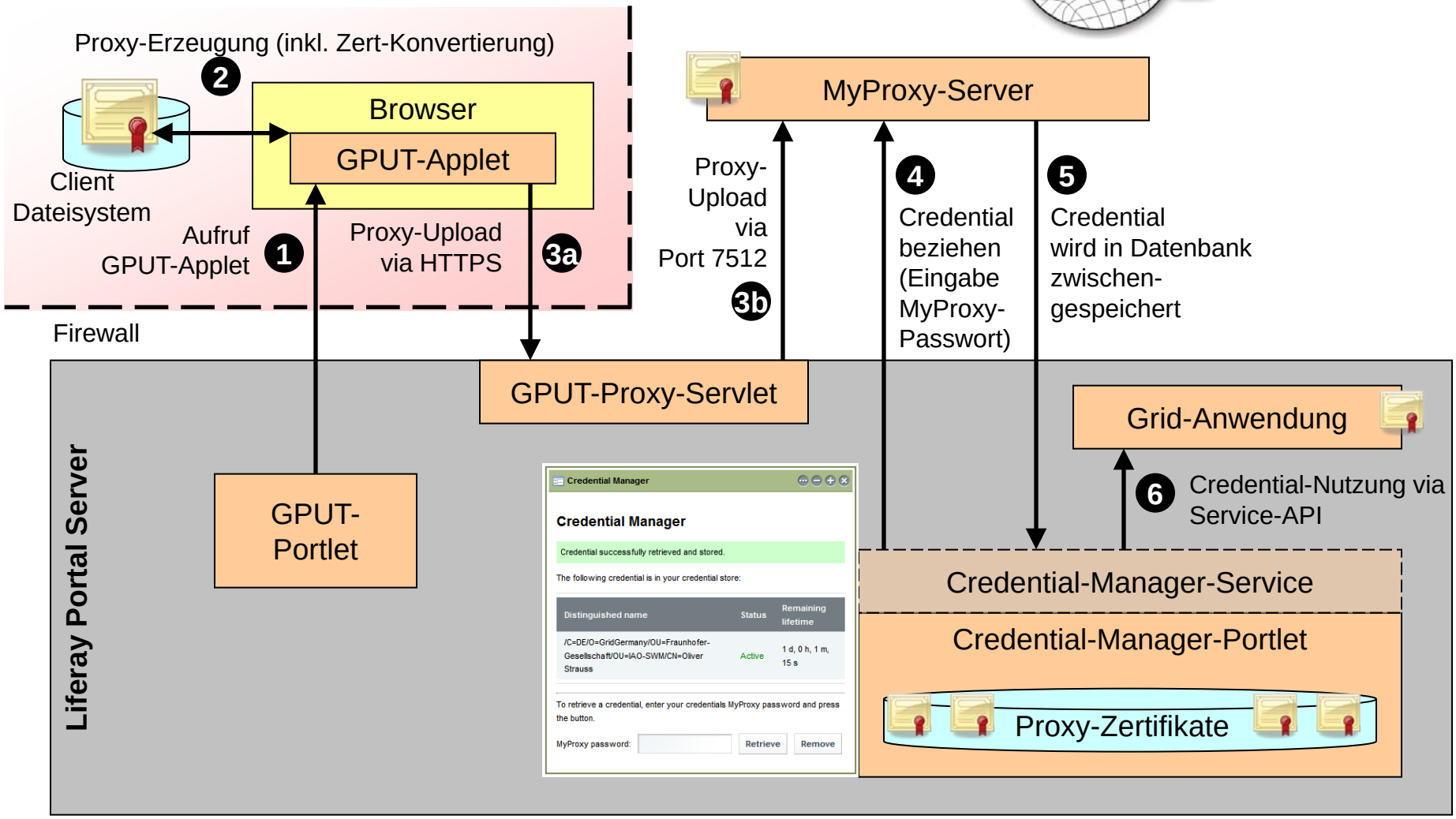


Grid Proxy Upload Tool (gPUT)



- Tool ist für das Community Grid vorkonfiguriert
  - kein Konfigurationsaufwand beim Nutzer
  - Anpassung an unterschiedliche Umgebungen erfolgt serverseitig durch Admin
  - Als MyProxy Username wird der DN aus dem Benutzerzertifikat verwendet
    - eindeutige und konfliktfreie MyProxy Usernamen
    - weniger Eingaben beim Nutzer

Credential Retrieval in Liferay



gPUT – Features

- Keine Installationsvoraussetzung auf dem Nutzerrechner außer Standard Java Runtime Environment
- One-Click-Installation der Java Cryptography Extension (JCE)
- Automatische Formatkonvertierung des Nutzerzertifikats auf dem Nutzerrechner
- Lokale Erzeugung von Proxies auf dem Nutzerrechner
- Sicherer Proxy Upload auf einen MyProxy Server via Portal
  ⇒ Kommunikation ausschließlich über HTTPS (Port 443)
  ⇒ funktioniert auch in Kliniknetzwerken !
- MyProxy-Server ist durch den Portal-Admin via Applet-Parameter konfigurierbar
- Trusted CAs sind ebenfalls durch den Portal-Admin via Applet-Parameter konfigurierbar (kryptographische Verifikation der Echtheit)
- Enge Integration mit Authentifizierung und Credential-Verwaltung am Portal
  ⇒ Minimierung der Eingabeaufwands
- **Maximierung der Nutzerfreundlichkeit !**

gPUT Paket

- gPUT als Komplettlösung
  - Login / DN Management Portlet für zertifikatsbasierten Login
  - Grid Proxy Upload Tool als Applet / Servlet Kombination
  - Credential Management Portlet
- Installation
  - Community-spezifische WAR-Datei zum Upload via Liferay Kontrollbereich
  - Community-Anpassung durch XML-Parameter-Datei vor Build
- Anwendung
  - Login mit D-Grid Zertifikat im Browser
  - Proxy Erzeugung via gPUT Applet
  - Credential Retrieval ohne vorherige Konfiguration
  - Proxy und Credential Lifetime nach Bedarf frei anpassbar

Vielen Dank für Ihre Aufmerksamkeit!

Fraunhofer-Institut für
Arbeitswirtschaft und Organisation IAO
Nobelstraße 12
70569 Stuttgart
www.iao.fraunhofer.de

Jürgen Falkner
Leiter Softwaretechnik und Sprecher der
Fraunhofer-Allianz Cloud Computing
E-Mail: Juergen.Falkner@iao.fraunhofer.de

www.swm.iao.fraunhofer.de
www.cloud.fraunhofer.de