

Einfache Nutzung von D-Grid Zertifikaten

Jürgen Falkner, Fraunhofer IAO

Projekt Gap-SLC

5. D-Grid Security Workshop, Göttingen





■ 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



Zertifikatsausstellung

VO Registrierung

Proxy Erzeugung/Upload

Credential Portlet Konfiguration

Credential Retrieval
um Anwendungen
zu nutzen

einmalig

1x pro Woche

jede Anwendung

Task 6:

Vereinfachung der Authentifizierung mittels
PKI-Zertifikaten für den Nutzer

Problemstellung



■ 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)



■ 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



■ 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



MediGrid Portal - Mozilla Firefox

https://portal.medgrid.de/gridsphere/gridsphere?cid=Grid

Abmelden
Willkommen, Juergen Falkner

Willkommen | Grid Workflows | Monitoring | Data Management | Grid | Genetic Tools | Clinical research | Bioinformatik | Ontology Tools | MediGRID Image processing

Credentials Resources Files Jobs

Info / Help

Credential Manager Portlet

Using applications with certificate-based authentication

In order to use applications which require certificate-based authentication due to data protection and security reasons you will need to go through the two steps listed below. First you will need to upload a so-called proxy (a copy of your certificate pair with a limited lifetime of 7 days) to the MediGRID MyProxy Server (a password-protected database in the MediGRID). Secondly you will need to retrieve a Credential derived from the proxy in the MyProxy Server.

Step 1: Upload Proxy to MyProxy Server

Contrary to Step 2, which you need to do each time before you use an application with certificate-based authentication, you only have to do this first step once a week as your proxy will have a lifetime of 7 days.

In order to upload a proxy of your D-Grid certificate to the MediGRID MyProxy Server you need to use the MediGRID Proxy Upload Tool. Please click on the button below.

[Upload Proxy](#)

A detailed How-To-Use (german) for the MediGRID Proxy Upload Tool can be found in the [MediGrid-Wiki](#) or in the **infohelp** section of this portlet (above left).

Step 2: Retrieve Credentials

In order to use applications with certificate-based authentication (more secure) you will need to retrieve a Credential in advance of your usage. For security reasons credentials have a lifetime of only about 2 hours.

If you do not see a Credential listed below you will need to configure a new Credential first. In order to do so, please carefully read the **infohelp** section of this portlet or the How-To-Use (german) for the MediGRID Proxy Upload Tool and for the configuration of the Credential Manager portlet, which can be found in the [MediGrid-Wiki](#) and then click on the button **New Credential**.

[List Credentials](#) [New Credential](#)

The following credentials can be retrieved from gwdu106.gwdg.de.

Credential	Certificate	Status	Time left	
jfalkner Grid DFN 2008	JC=DE=O=GridGermany/OU=Fraunhofer-Gesellschaft/OU=IAO-S/M/MCN=Juergen Falkner	Active	2 hours 14 minutes 50 seconds	Deactivate

Passphrase: [*****] [Retrieve Credentials](#)

Credential Label

18. Juni 2008

Suchen: gunia [Abwärts](#) [Aufwärts](#) [Hervorheben](#) [Groß-/Kleinschreibung](#)

MediGrid Portal - Mozilla Firefox

https://portal.medgrid.de/gridsphere/gridsphere?cid=CredentialManagerPortlet

Abmelden
Willkommen, Juergen Falkner

Willkommen | Grid Workflows | Monitoring | Data Management | Grid | Genetic Tools | Clinical research | Bioinformatik | Ontology Tools | MediGRID Image processing

Credentials Resources Files Jobs

Info / Help

Credential Manager Portlet

This credential can be retrieved from gwdu106.gwdg.de

Label: [frei wählbarer Name (Required Label to display for credential in portlet)] **Credential Label**

User Name: [MyProxyUsername (Required - 1 or more asterisks option to myproxy-asis)] **MyProxy Username**

Credential Name: [Optional - 1x or more asterisks option to myproxy-asis]

Credential Lifetime: [0100 (in seconds)] **Credential Lifetime (in s)**

Passphrase: [***** (Required - Your credential repository password)] **MyProxy Passwort**

[Apply](#) [Cancel](#)

18. Juni 2008

Suchen: gunia [Abwärts](#) [Aufwärts](#) [Hervorheben](#) [Groß-/Kleinschreibung](#)

MediGrid Portal - Mozilla Firefox

https://portal.medgrid.de/gridsphere/gridsphere?cid=CredentialManagerPortlet

Abmelden
Willkommen, Juergen Falkner

Willkommen | Grid Workflows | Monitoring | Data Management | Grid | Genetic Tools | Clinical research | Bioinformatik | Ontology Tools | MediGRID Image processing

Credentials Resources Files Jobs

Info / Help

Credential Manager Portlet

[List Credentials](#) [Refresh View](#) [Edit Credential](#) [Deactivate Credential](#) [Delete Credential](#)

keine Häkchen!

Use Portal Credential:

Single Sign-On:

Certificate: [JC=DE=O=GridGermany/OU=Fraunhofer-Gesellschaft/OU=IAO-S/M/MCN=Juergen Falkner]

User Name: [falkner00]

Credential Name: [falkner00]

Credential Lifetime: [0100 (in seconds)]

Credential Label: [falkner00]

Passphrase: [*****] [Retrieve Credential](#)

Credential Status: inactive

Time Remaining: 0 seconds

Date Created: Mittwoch, 25. März 2008 13:57 Uhr CET

Last Retrieved: Mittwoch, 21. Mai 2008 14:34 Uhr CET

17. Juni 2008

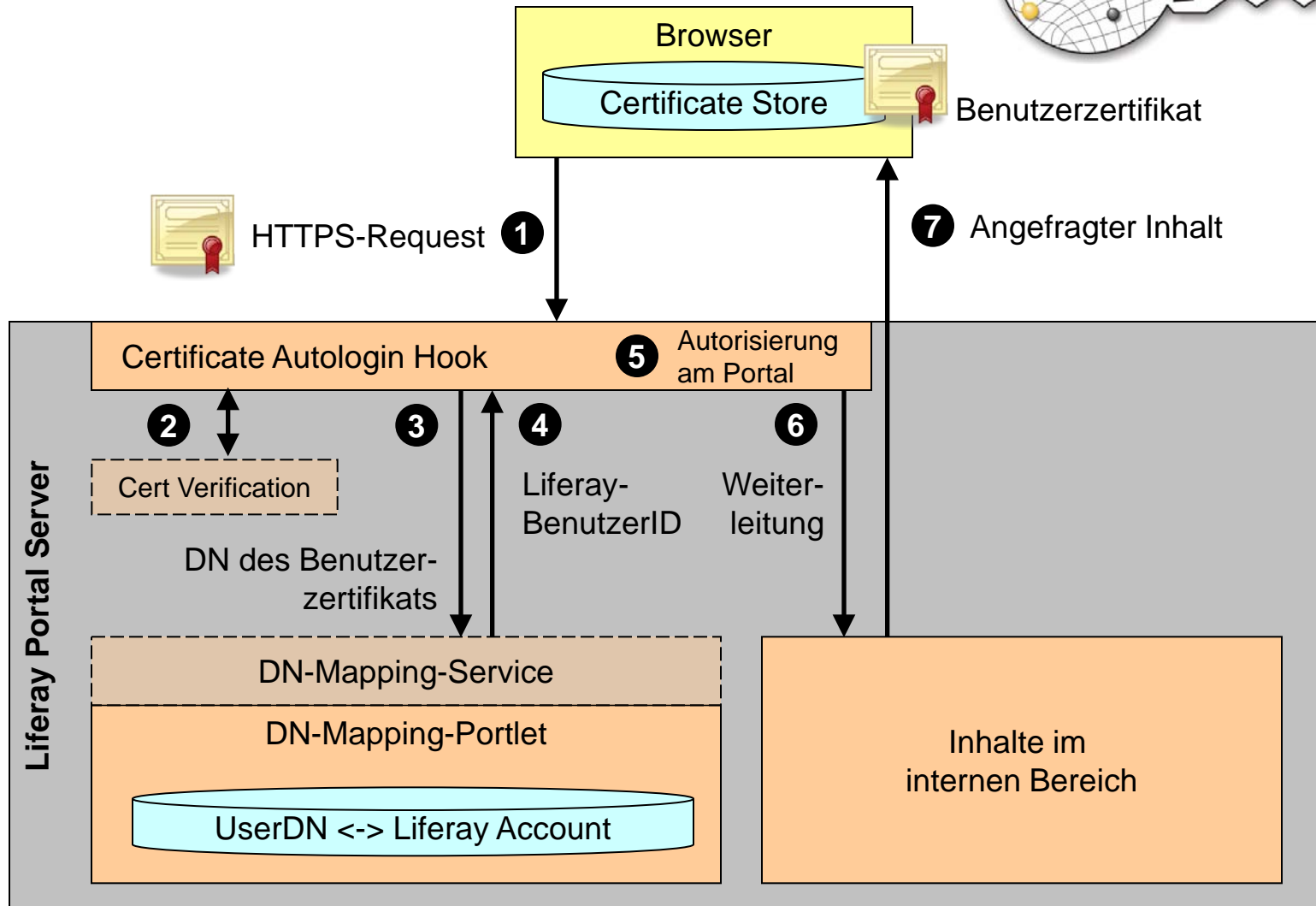


Task 6:

Vereinfachung der Authentifizierung mittels
PKI-Zertifikaten für den Nutzer

Lösung

Liferay Login mit PKI



Grid Proxy Upload Tool (gPUT)



GRID Proxy Upload Tool
by **Fraunhofer** IAO
with inspiration by **CHARITÉ**

[Install JCE Policy](#)

Certificate

Certificate: ?

My Proxy Server: gridmon.gwdg.de

Password: ?
Re-Password:

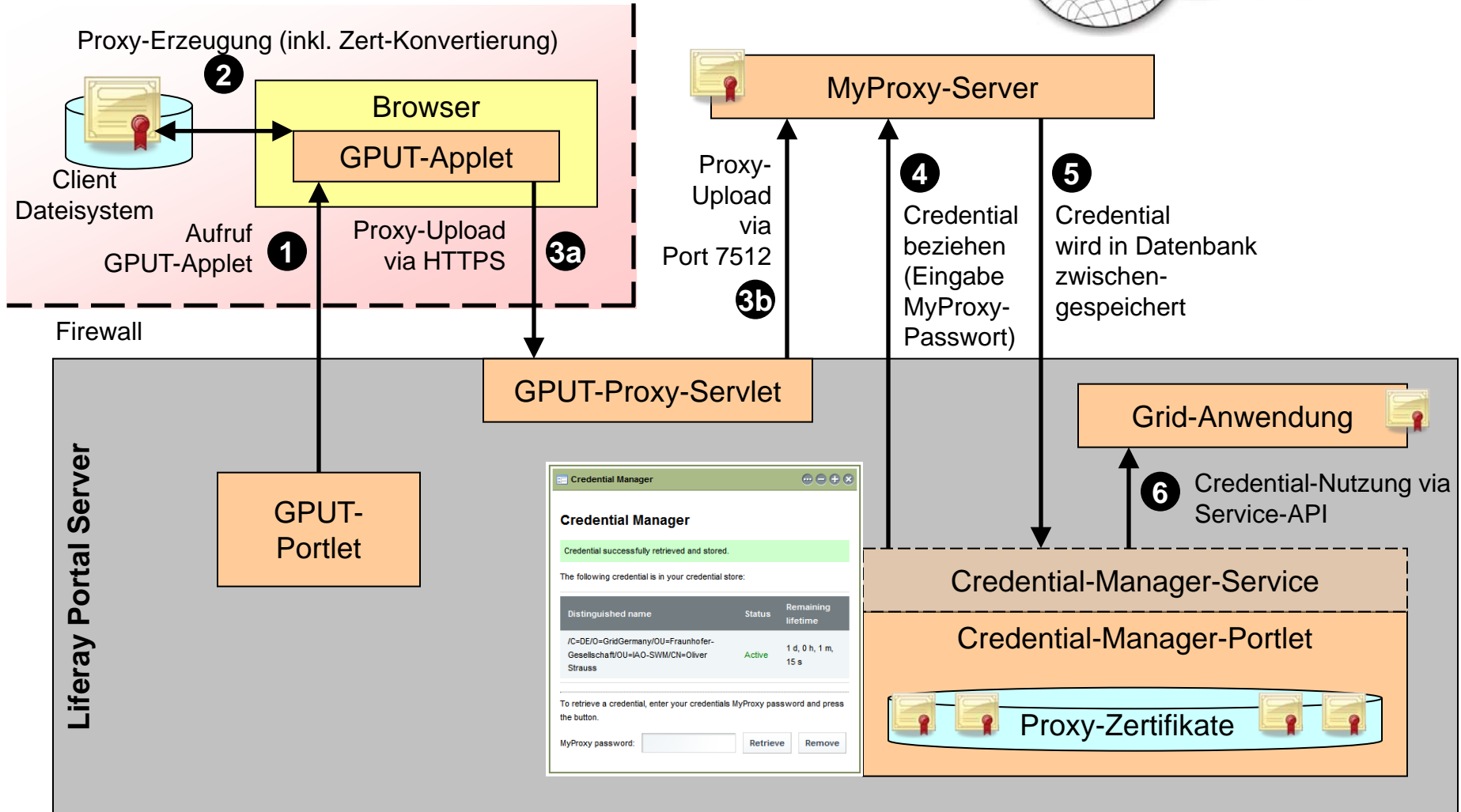
Lifetime

Proxy Lifetime: 7 Days ?
Max. Credential Lifetime: 24 Hours

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





- 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 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!



IT-POTENZIALE INTELLIGENT NUTZEN
PROZESSINNOVATIONEN ERFOLGREICH UMSETZEN
SYSTEME INTUITIV GESTALTEN

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

