SLCs
for use in
Grid-Portals

EUGridPMA F2F Copenhagen

27.05.2008

Reimer Karlsen-Masur, DFN-PCA

Technical Contact DFN-PCA: dfnpca@dfn-cert.de

Administrative Contact DFN-Verein: pki@dfn.de

Overview

- The Problem
- Solutions
- Grid-Portals/-Gateways
- DFN-PKI SLCS
- Architecture
- Open Questions

The Problem

Users w/o PKI/X.509 cert knowledge need immediate instant access to Grid resources

- Establishing initial Grid-RAs
- Personal identification
- Getting and handling (Grid-)certs
- Handling multiple certs/PKIs

all thought to be cumbersome

but the Grids authN (and authZ) is PKI based

Solutions (1)

- Community certs
  - Robot certs

used in

- Grid-portals / -gateways
  - Browser-based, eg. Grid-Sphere or even simple Web-form
  - Java-based, eg. Eclipse
  - Possibly others

Advantage: Grid map files are simple

Drawback: „reduces” every Grid user of a portal to one sDN/cert; authZ is handled by portal

Solutions (2)

- SLCs & AAI

used with

- gLite
- Grid-portals / -gateways
  - Browser-based, eg. Grid-Sphere or even simple Web-form
  - Java-based, eg. Eclipse

Advantage: Grid-users recognizable, well-defined ID vetting, authZ at Grid resources

Drawback: AAI necessary, Portals can't store the priv keys of their users SLCs because of CP

Grid-Portals

Grid-portals provide a simple userfriendly GUI to model & submit Grid jobs as well as to retrieve and display their results

- Implemented as Web-application, -form or Eclipse plug-in
- Username/Password or clientAuth (possibly Shibbed) credential to log-on to portal
- Anonymous access to predefined Grid jobs (running on insensitive data, eg. animal or plant DNA)

Grid-Gateways

Grid-gateways provide a Web-Services API to model & submit Grid jobs as well as to retrieve their results

In the following slides Grid-gateways are considered to be equivalent to Grid-portals.

DFN-PKI SLCS (1)

- DFN-PKI SLCS and SCLS-CA implemented and IGTF accredited planned for end of 2008
- Leveraging Shibboleth based DFN-AAI
- Using GridShib-CA software
- Embedding of IdP signed SAML attributes into SLCs possible

DFN-PKI SLCS (2)

- Additional features to be developed for the DFN-PKI SLCS:
  - Low-user-interaction semi-automatic Portal-driven subscription to SLCs and derivation of primary proxies thereof as well as delegated proxies of these
    - Automatic interaction with Grid-Portals
    - Automatic interaction with MyProxy Credential Store

to provide the Grid-user with a simple & pleasant experience to do his Grid stuff with real certs under the bonnet

DFN-PKI SLCS architecture overview (1)

- Shibboleth DFN-AAI with WAYF localisation service
- Shib Identity Provider (IdP) in all participating organisations
  - IDMS for the IdPs
- Grid-portals (or -gateways) as Shibboleth SPs
  - VOMS for the Grid-portals & Grid-resources

DFN-PKI SLCS architecture overview (2)

- SLCS as Shib Service Provider
- Online SLCS-CA with HSM on a back-end server to the SLCS-SP
- JavaWebStart application CredentialRetriever (CR) for Grid-users
- MyProxy Credential Store (MyProxyCS)

Architecture: Grid-Portals

Aside from doing the obvious Grid stuff Grid-portals need to

- provide a Shib log-on for the Grid-users
- redirect the Grid-users to the SLCS providing it with the information for the CR to request a SLC & upload a primary proxy of this to the MyProxyCS as well as give status information back to the portal
- retrive delegated proxies of the primary proxies in the MyProxyCS (myproxy-logon) with TLS clientAuthN

Architecture: CredentialRetriever (1)

GridShib CA comes with a JavaWebStart application named *CredentialRetriever* that will currently

- generate a key pair and CSR on the Grid-users computer
- submits it to a shibbed SLCS
- retrieves the SLC and
- saves both (key & SLC) in a standard path on the Grid-users computer to use at his discretion with standard Grid-software

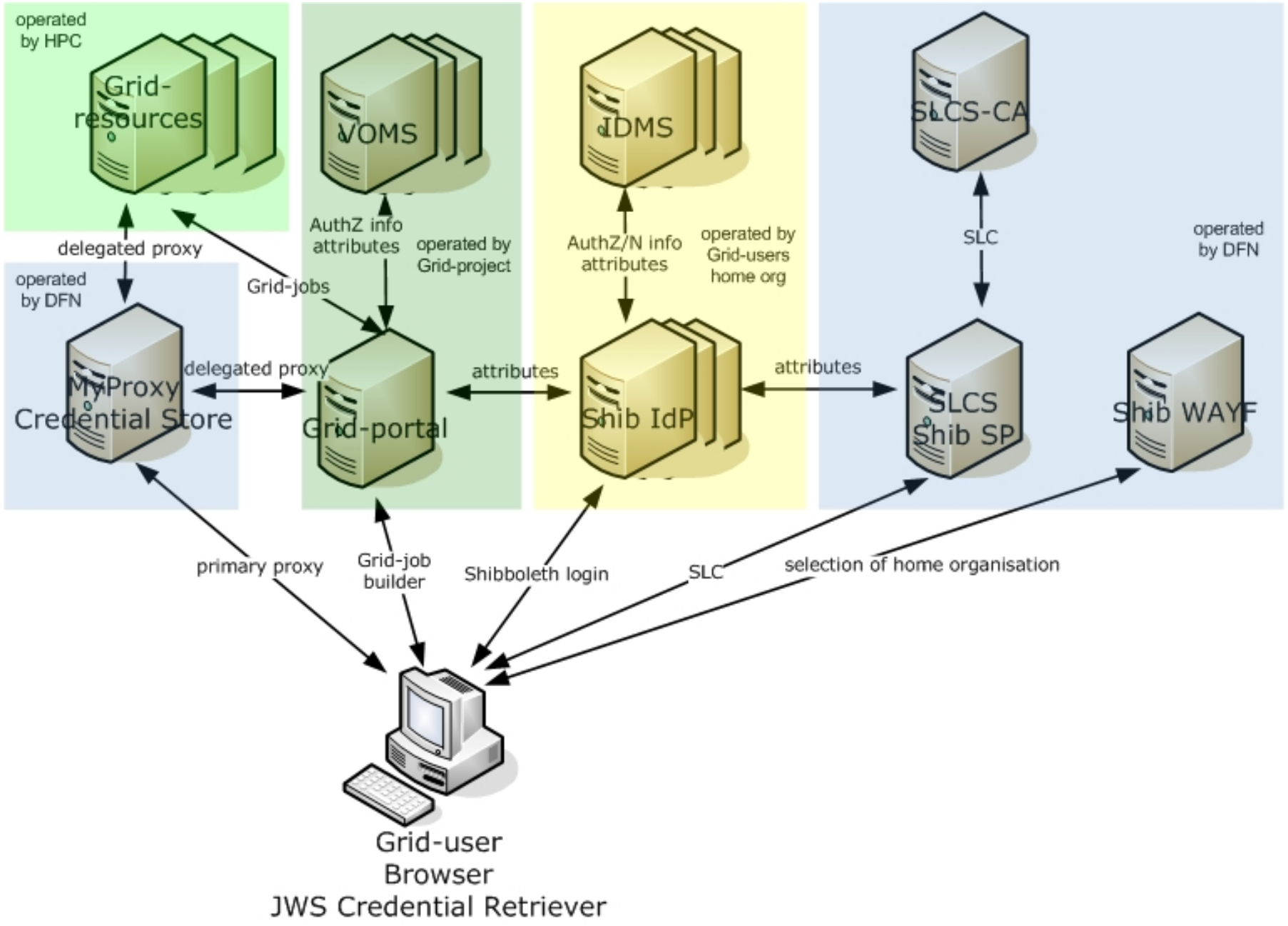
This is far from being a „simple & automated experience to get to a Grid cert for portal use”.

Architecture: CredentialRetriever (2)

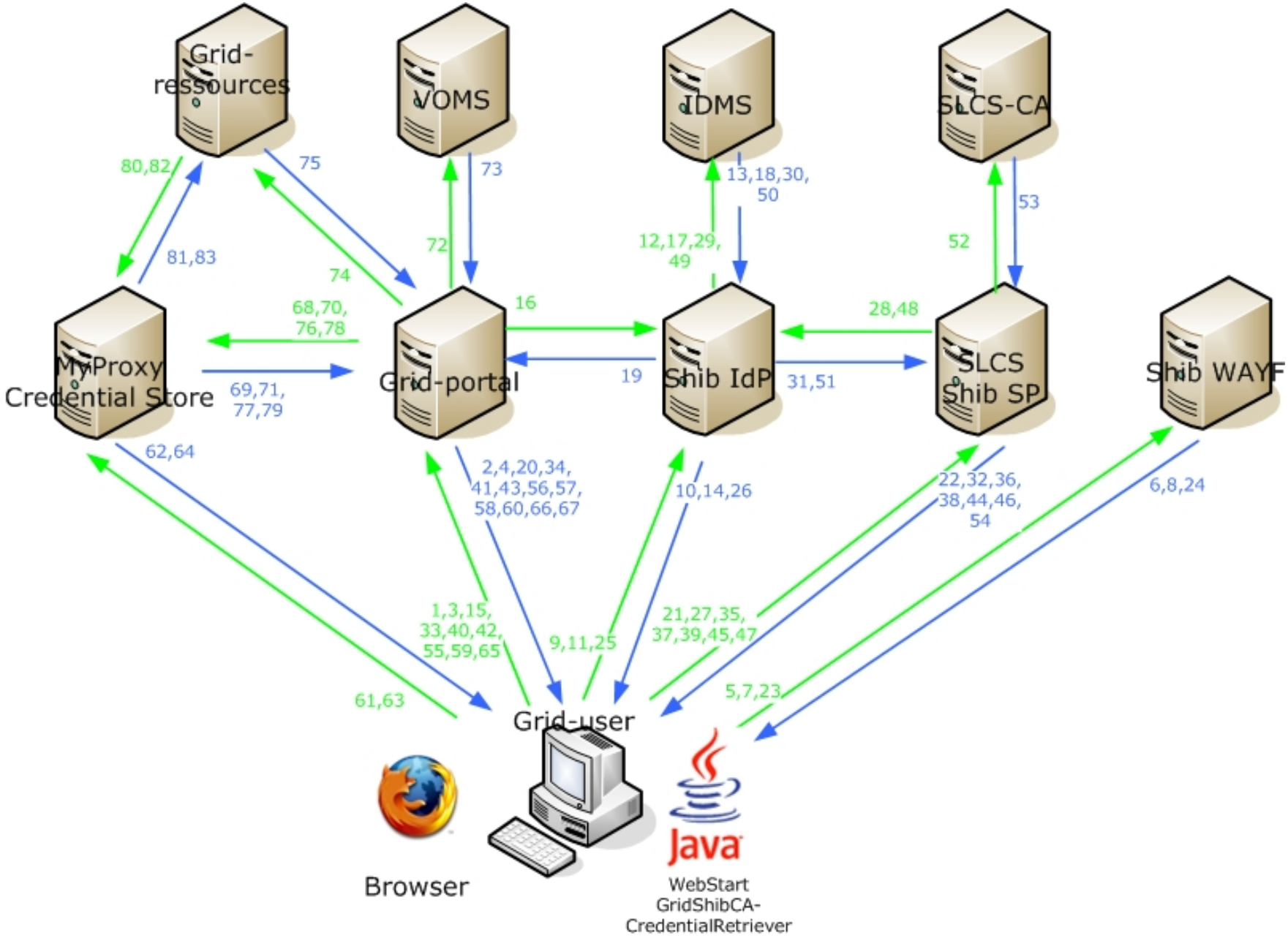
The CredentialRetriever needs to do more:

- Derives a primary proxy of the SLC and uploads that primary proxy onto the MyProxyCS (myproxy-init) making it available to the Grid-portal
- Provides feedback to the Grid-portal about the status of getting the SLC and generating and uploading the primary proxy thereof to the MyProxyCS

DFN-PKI SLCS architecture details (1)



DFN-PKI SLCS architecture details (2)



Workflow Phases

- Phase 1 (01-20): User logs on to Grid-portal via Shib
- Phase 2 (21-33): User logs on to SLCS via Shib
- Phase 3 (34-58): „User" is requesting & getting a SLC
- Phase 4 (59-67): „User" uploads a primary proxy to the MyProxyCS
- Phase 5 (68-71): Portal is getting a delegated proxy from MyProxyCS
- Phase 6 (72-83): Grid-portal/resources using the Grid

Necessary Grid-User Input to get Certs setup

- Shib log-on to Grid-portal (incl. selection of home org @ WAYF)
- Acknowledging the requesting of a SLC from the SLCS and the uploading of a primary proxy of the SLC to the MyProxyCS by clicking an „OK” button.

Certificate Chain

- SLCS CA cert; valid 10years; key in online HSM
  - SLC incl. opt. embedded SAML assertion; valid 1mio secs; key on users machine; key can be deleted once primary proxy is on MyProxyCS
    - Primary proxy; valid 1mio-2 secs, key in MyProxyCS
      - Delegated proxy incl. opt. embedded SAML assertion; valid 12hrs; key on Grid-portal/gateway/scheduler; automated renewal through Grid-portal/GW/sched
        - Further delegated proxies incl. opt. embedded SAML assertion; valid < 12hrs; key on Grid-resource; automated renewal through Grid-ressource
          - ....

Open Questions

- Use of alternative/project-owned MyProxyCS possible?
- Alternative AuthN of Grid-portal/gateway at MyProxyCS via Username/Password possible?
- How about availability & redundancy?
- Is the Grid-portal/gateway the instance that is getting the first delegated proxy or (sh|c)ould it also be the Grid job-scheduler?
- Grid + Portals + SLCS + MyProxyCS + Credential-Retriever are rather complex. Did we miss a simpler path to ease cert handling for Grid-users?

Thanks

Request & Retrieval of SLCs issued by DFN-SCLS-CA

Demo of current

GridShibCA

and

CredentialRetriever

GridShib CA

(Version 0.4.0)
GridShib Home Page

About

This is the GridShib-CA (version 0.4.0). This software allows you to acquire a short-lived (< 277 hours) Grid Credential through your web browser and Shibboleth. After successfully authenticating, a credential will be installed and is suitable for use with Grid Tools such as GT4.

Note that as with all Grid credentials this GridShib CA must be trusted by any resources you use and the identity from the Credentials (aka the Distinguished Name or DN) must be authorized (in the grid-mapfile). You may download the CA-Certificate of this GridShib CA and its signing policy file for installation in Grid middleware here.

For further documentation and the latest release please see http://gridshib.globus.org. Full documentation regarding this release can be found at http://gridshib.globus.org/docs/gridshib-ca-0.4.0

Prerequisites

Prior to using the GridShib CA on a new system, please make sure you have the system properly configured. Failing to do so may cause you headaches as well as being insecure.

The GridShib-CA will work for for any Institution with a Shibboleth server (Identity Provider, IdP) in the DFN-AAI-Test-Federation that will release an identity to the GridShib-CA. If your institution doesn't have a Shibboleth Identity server in one of the Federations named above (or it doesn't release your identity to us), it just won't work. To become a member of the DFN-AAI-Test-Federation or to get more information about the DFN-AAI-Test-Federation please visit its Website or contact mailto:admin@aai.dfn.de.

Go

Shibboleth logon via DFN-AAI Test-Federation

DFN-AAI-Test: Auswahl der Heimateinrichtung - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://wayf.aai.dfn.de/DFN-AAI-Test/wayf/?shire=https%3A%2F%2Fslcs.pca.dfn.de%2FShibboleth.sso%2FSAML%2FPOST&time=

DFN Deutsches Forschungsnetz

WAYF der DFN-AAI-Testföderation

WAYF - Where Are You From

Dies ist der Lokalisierungsdienst der DFN-Test-AAI. Sie ordnen Sich hier der Einrichtung zu, gegenüber der Sie sich authentifizieren möchten. Sie werden auf die Anmeldeseite dieser Einrichtung weitergeleitet, dort erfolgt die Anmeldung mit Ihrer persönlichen Benutzerkennung.

Über AAI : Über DFN

DFN-AAI-Test: Heimateinrichtung auswählen

Um auf Resourcen auf dem Rechner `'slcs.pca.dfn.de'` zuzugreifen ist eine gültige Benutzerauthentifizierung nötig.

Wählen Sie Ihre Heimateinrichtung ...

Auswählen

☑ Auswahl für die laufende Browsersession speichern.

☐ Auswahl permanent speichern und den WAYF von jetzt an umgehen.

▶ Der DFN-Verein empfiehlt, das 'DFN-PKI Root CA Certificate' in den Webbrowser zu importieren.

Fertig wayf.aai.dfn.de Proxy: None

DFN-AAI-Test: Auswahl der Heimateinrichtung - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://wayf.aai.dfn.de/DFN-AAI-Test/wayf/?shire=https%3A%2F%2Fslcs.pca.dfn.de%2FShibboleth.sso%2FSAML%2FPOST&time=

DFN Deutsches Forschungsnetz

Wählen Sie Ihre Heimateinrichtung ...
Alfred-Wegener-Institut für Polar- und Meeresforschung in der Helmholtz-Gemeinschaft
Alfred-Wegener-Institut für Polar- und Meeresforschung in der Helmholtz-Gemeinschaft (IAM Suite)
C3 Grid DKRZ Hamburg
C3Grid Projekt am PIK
DAASI IdP
DFN Berlin IdP
DFN Test-IdP
DFN-CERT Services GmbH
DLR - Deutsches Zentrum für Luft- und Raumfahrt e.V.
DWD
Demo AAR
FZJ-Zentralbibliothek
GKSS
HS-Harz
IFM-GEOMAR
Ludwig-Maximilians-Universität München
RWTH Aachen
RWTH Aachen Test
TU Chemnitz

Wählen Sie Ihre Heimateinrichtung ...

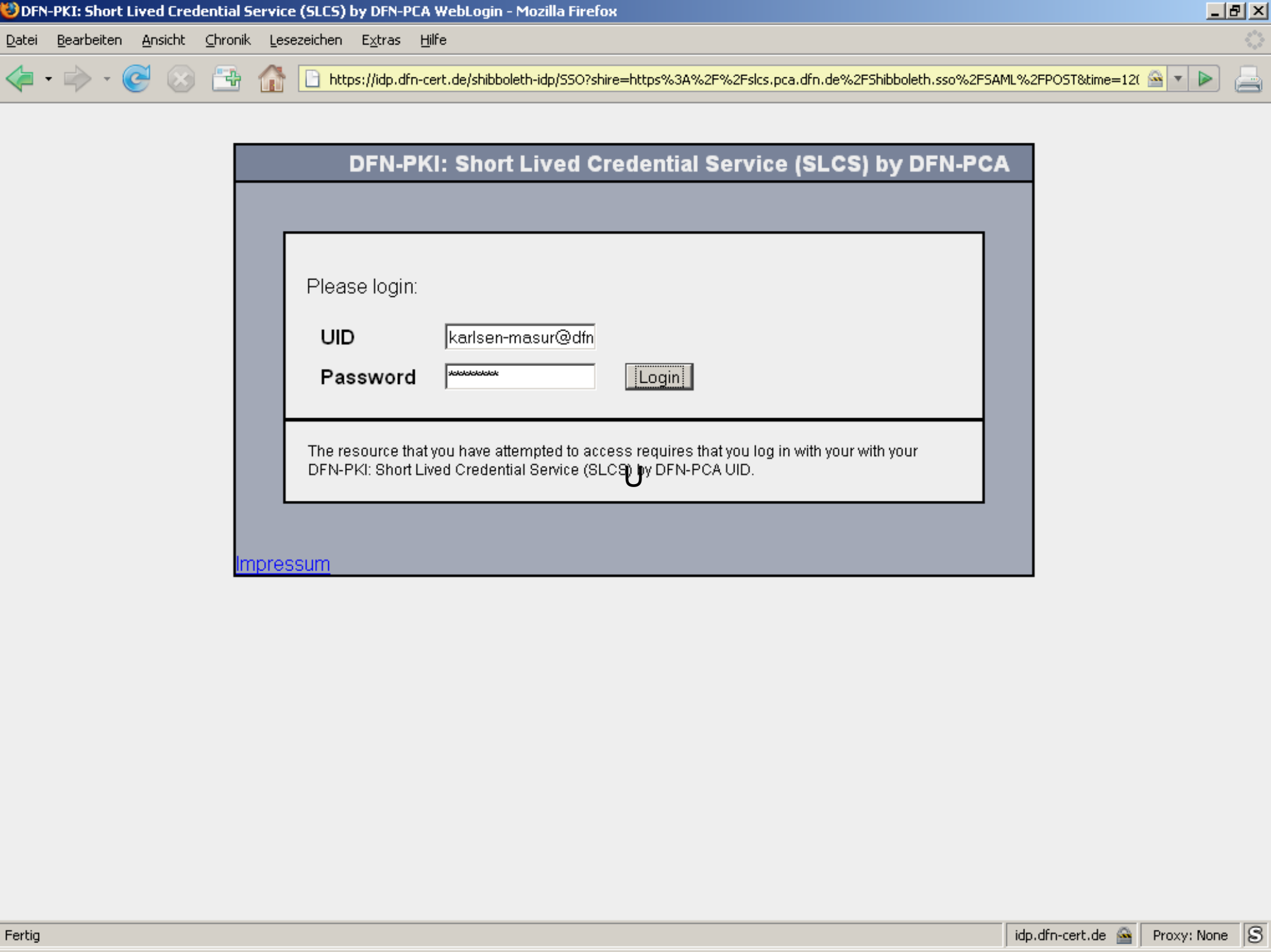
Auswählen

☑ Auswahl für die laufende Browsersession speichern.

☐ Auswahl permanent speichern und den WAYF von jetzt an umgehen.

▶ Der DFN-Verein empfiehlt, das 'DFN-PKI Root CA Certificate' in den Webbrowser zu importieren.

Fertig wayf.aai.dfn.de Proxy: None


DFN-PKI: Short Lived Credential Service (SLCS) by DFN-PCA WebLogin - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://idp.dfn-cert.de/shibboleth-idp/SSO?shire=https%3A%2F%2Fslcs.pca.dfn.de%2FShibboleth.sso%2FSAML%2FPOST&time=12(
DFN-PKI: Short Lived Credential Service (SLCS) by DFN-PCA
Please login:
UID
karlsen-masur@dfn
Password
Login
The resource that you have attempted to access requires that you log in with your with your DFN-PKI: Short Lived Credential Service (SLCS) by DFN-PCA UID.
Impressum
Fertig
idp.dfn-cert.de
Proxy: None

GridShib CA

(Version 0.4.0)
GridShib Home Page

Welcome karlsen-masur@dfn-cert.de

Your GridShib-CA X.509 identity from this CA will be:

Globus Grid-Mapfile Format:
/C=DE/O=DFN-Verein/OU=DFN-PKI/OU=SLCS/OU=DFN-CERT Services GmbH/CN=karlsen-masur@dfn-cert.de

Standard RFC 2253 Format:
CN=karlsen-masur@dfn-cert.de,OU=DFN-CERT Services GmbH,OU=SLCS,OU=DFN-PKI,O=DFN-Verein,C=DE

Get your Grid Credential

Credential Lifetime: (•) Default (12 hours) ( ) Other: 12 Hours (277 max)

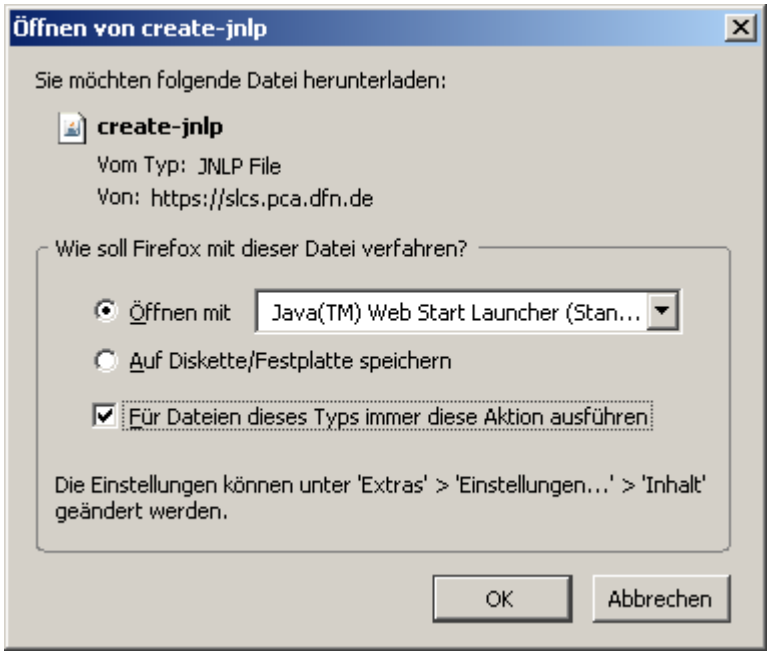
[Press here to generate and download Grid credential.]

When the Credential Retriever application completes, you may click on the following button to return to the main GridShib CA page or simply close this browser window.

[Return to GridShib CA main page]

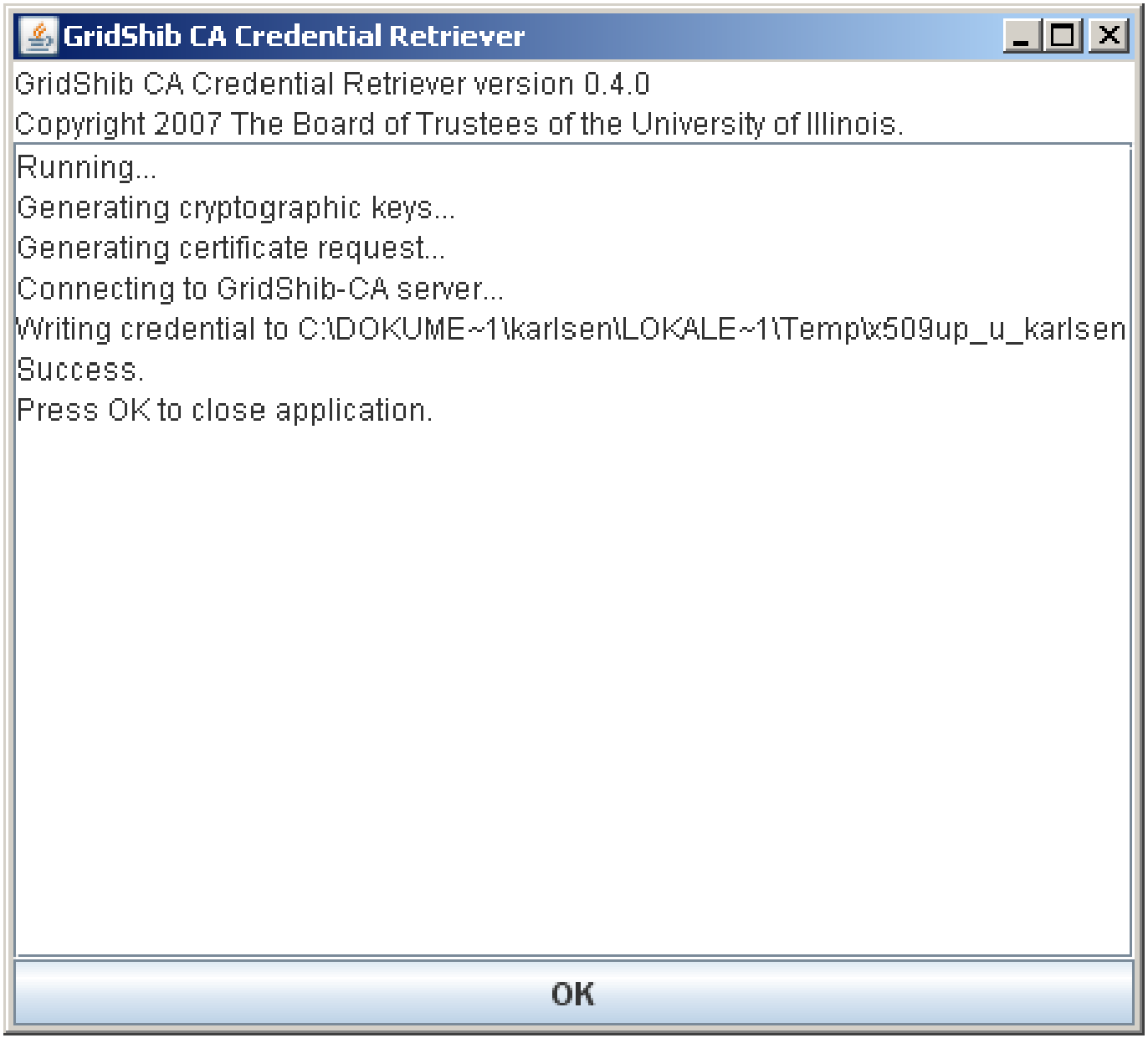
Java WebStart (JWS)

- Java Runtime Environment (JRE) muss auf dem Nutzerrechner installiert sein
- MIME-Type application/x-java-jnlp (Dateiendung .jnlp) für Java WebStart muss ggf. auf dem Browser eingerichtet werden

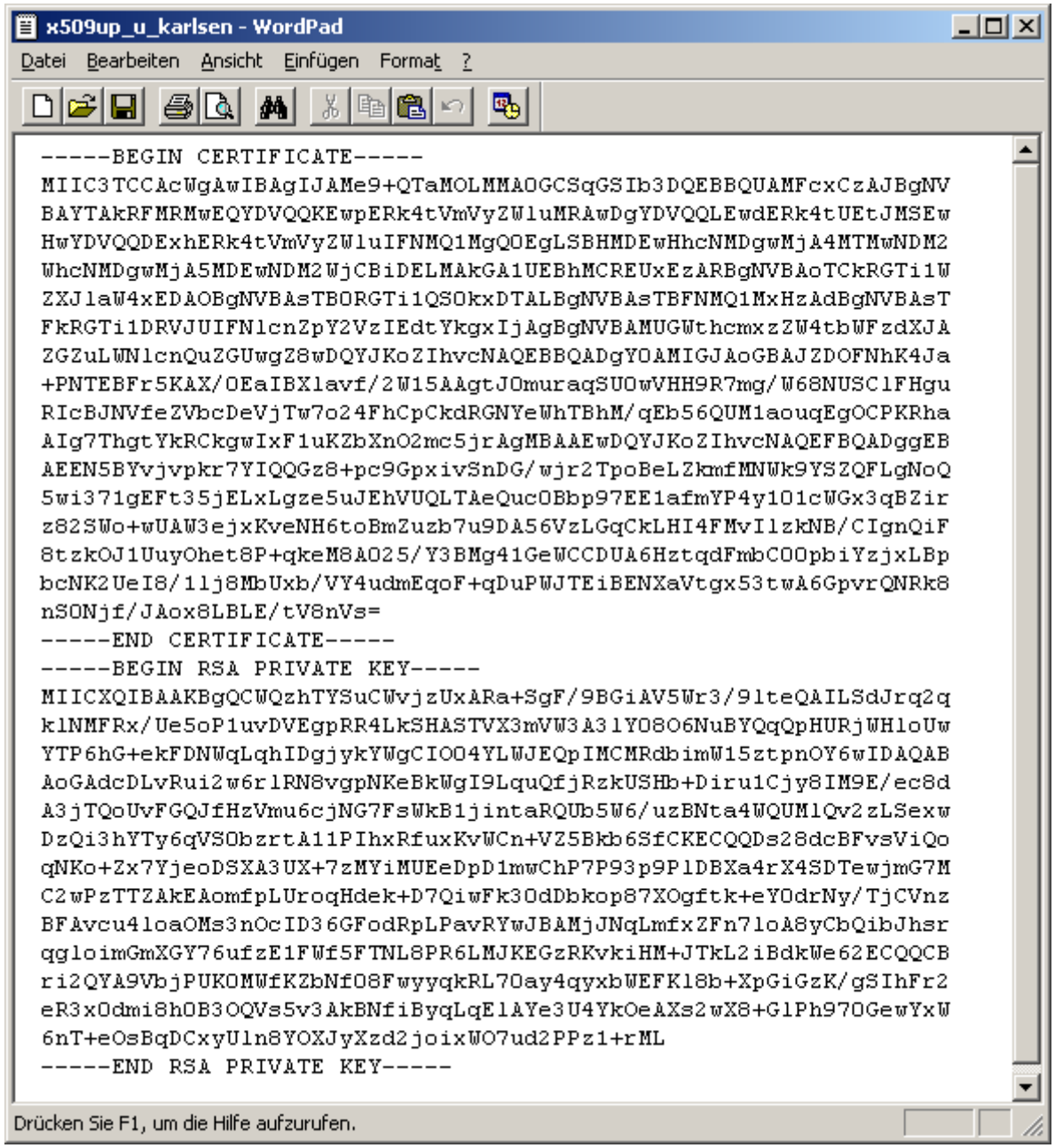


JWS Applikation wird gestartet

GridShib CredentialRetriever



SLC (Zertifikat & Schlüssel)



SLC (Textausgabe)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            c7:bd:f9:04:da:30:e2:d1
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein SLCS CA - G01
        Validity
            Not Before: Feb  8 13:27:12 2008 GMT
            Not After : Feb  9 01:27:12 2008 GMT
        Subject: C=DE, O=DFN-Verein, OU=DFN-PKI, OU=SLCS, OU=DFN-CERT Services
   GmbH, CN=karlsen-masur@dfn-cert.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:86:90:63:8d:81:8b:79:e7:e4:ff:10:c5:33:58:
                    fb:a3:5f:a7:ce:18:1f:93:3f:2b:ea:24:be:da:ab:
                    f5:52:08:20:74:4b:fc:5f:f9:e5:4b:aa:4c:12:ad:
                    47:50:08:9d:40:fe:91:d7:ad:4c:82:bb:1e:25:c4:
                    ac:38:dc:a0:28:e8:20:ee:80:d2:98:65:fd:63:b8:
                    19:ba:a2:e2:4b:5c:e5:85:52:00:08:4a:5e:31:d6:
                    78:4c:bc:80:18:c0:24:6d:a6:3a:0a:6f:70:45:79:
                    30:42:64:f8:80:07:b3:07:0d:94:40:ad:5e:c2:e4:
                    cb:3f:85:30:0a:a4:9d:cc:c7
                Exponent: 65537 (0x10001)
```

GridShibCA

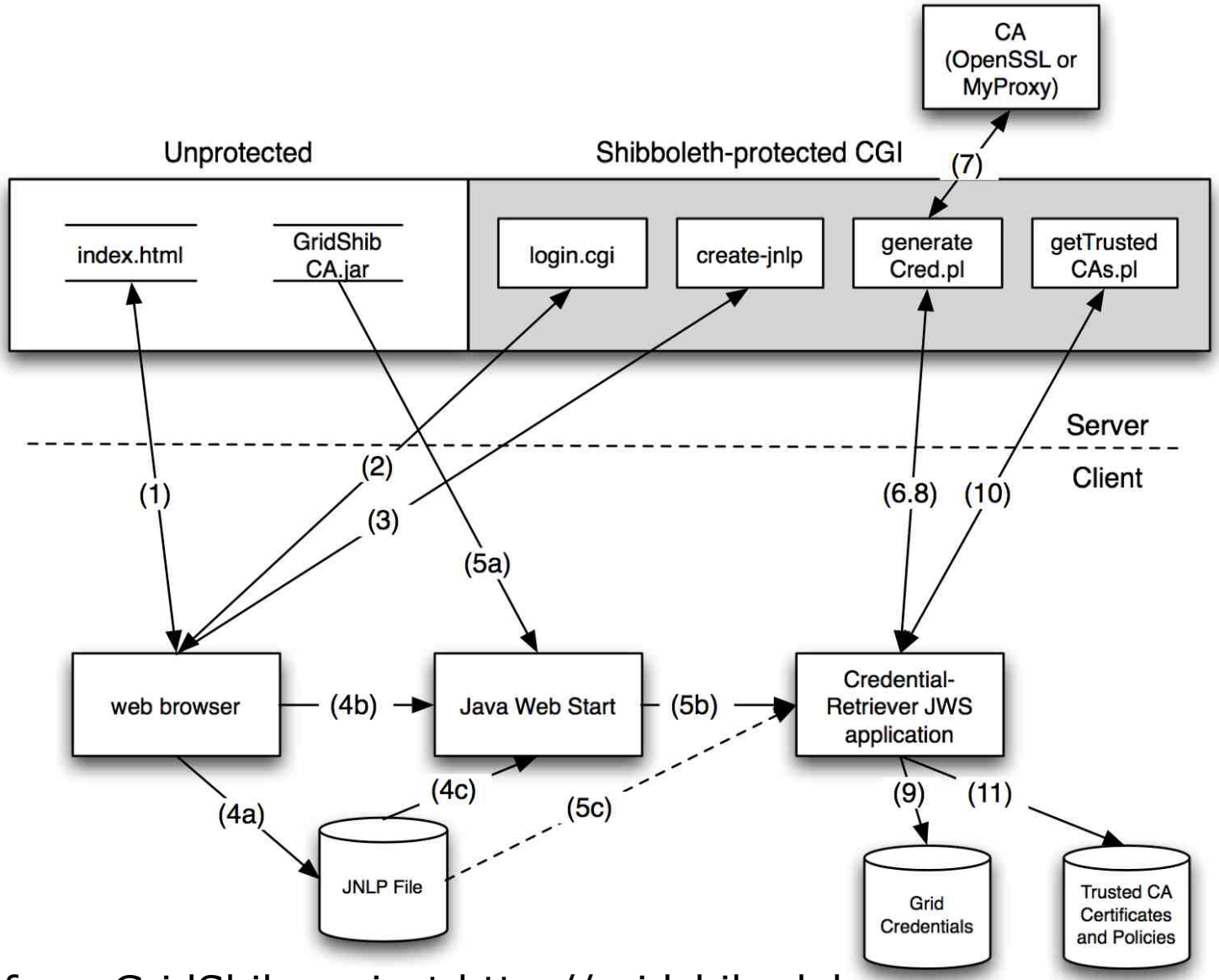


Figure taken from GridShib project http://gridshib.globus.org

Portal Delegation

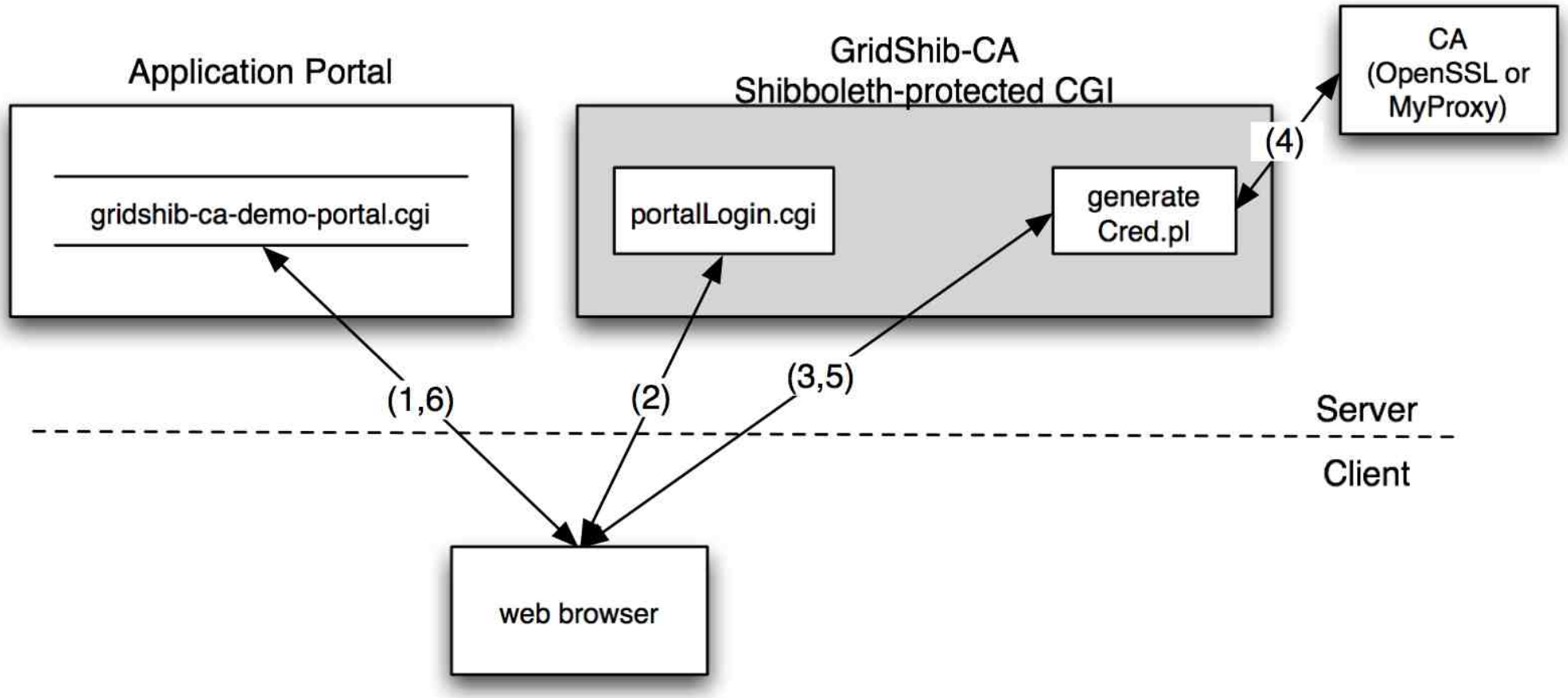


Figure taken from GridShib project http://gridshib.globus.org