DFN SLCS

Jürgen Brauckmann
dfnpca@dfn-cert.de

DFN-PKI

- Multiple PKI hierarchies with different security levels and properties
- „DFN-PKI Global“, integrated in all major browsers/operating systems
  - ~500.000 currently valid certificates
  - Secure operating in trustcenter at DFN-CERT in Hamburg
  - Audited according to ETSI TS 102 042 (yearly, auditor TÜViT)
  - No EUGridPMA accreditation!

Grid

Security level „Grid“:

- Since 2005
- Manual registration process
- Currently 700 valid certificates
- 7000 certificates issued since 2005
- 13 months lifetime for subscriber certificates
- 90 registration authorities
- Accredited with EUGridPMA
- Self-audits

SLCS

Security level „SLCS“:

- Since 2009
- 5 registered IdPs (including KIT)
- 870 certificates issued since 2009 for 125 users
- Accredited with EUGridPMA
- Integrated in DFN-AAI
- Test-SLCS available (no policy, Test-AAI)
- Max certificate lifetime: 7 days (policy requirements)

Requirements on secure IdP operations:

DFN-AAI „Advanced“

+ IdP audits

+ requirements on attributes

+ further wording about secure administration

Identity Provider must supply:

- eduPersonPrincipalName
- surName
- givenName
- email
- eduPersonEntitlement with value
  `urn:geant:dfn.de:dfn-pki:slcs`

Workflow:

- User visits DFN-SLCS web site, clicks on button
- Gets a redirect to WAYF/IdP, AAI login dance
- User must confirm certificate request data
- User gets a Java Webstart application („Credential Retriever), which generates the key/CSR, uploads the CSR and downloads the certificate

Implementation:

- Current releases of shibboleth sp package
- gridshib-ca, modified by DFN-PKI for secure trustcenter operations
- gridshib-ca talks to DFN-PKI backend with secure RA system/CA system/HSM
- Turnaround time request->certificate approx. 100 seconds
- No high availability for SP (gridshib-ca)!

Tour

https://slcs.pca.dfn.de/gridshib-ca/

DFN
Deutsches Forschungsnetz

Zertifikate | CA-Zertifikate und Signing Policy Dateien | Policy | Hilfe | Beenden

Willkommen zum Short Lived Credential Service (SLCS) der DFN-PKI
Hier können Sie Zertifikate des SLCS der DFN-PKI beantragen.

- Beantragen Sie hier Ihr SLC:

SLC beantragen

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"

Impressum

https://wayf.aai.dfn.de/DFN-AAI/wayf/?entityID=https%3A%2F%2Fslcs.pca.dfn.de%2Fshibboleth&return=https%3A%2F%2Fsl

DFN
Deutsches Forschungsnetz

DFN-AAI

Heimateinrichtung wählen

Um auf Resourcen auf **'slcs.pca.dfn.de'** zuzugreifen ist eine gültige Benutzerauthentifizierung nötig. 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.

DFN-CERT Services GmbH | Auswählen

- [x] 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, damit der Zugriff auf Ihre Heimateinrichtung problemlos möglich ist.
- Über AAI
- Über DFN

https://idp.dfn-cert.de/idp/Authn/UserPassword

Shibboleth®

Shibboleth Identity Provider Login

Username:

Password:

Login

Done

https://slcs.pca.dfn.de/cgi-bin/login.cgi

GridShib CA

(Version 0.5.1)
GridShib Home Page

Welcome Juergen Brauckmann - brauckmann@dfn-cert.de

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

Globus Grid-Mapfile Format:
/C=DE/O=GridGermany/OU=SLCS/OU=DFN-CERT Services GmbH/CN=Juergen Brauckmann - brauckmann@dfn-cert.de

Standard RFC 2253 Format:
CN=Juergen Brauckmann - brauckmann@dfn-cert.de,OU=DFN-CERT Services GmbH,OU=SLCS,O=GridGermany,C=DE

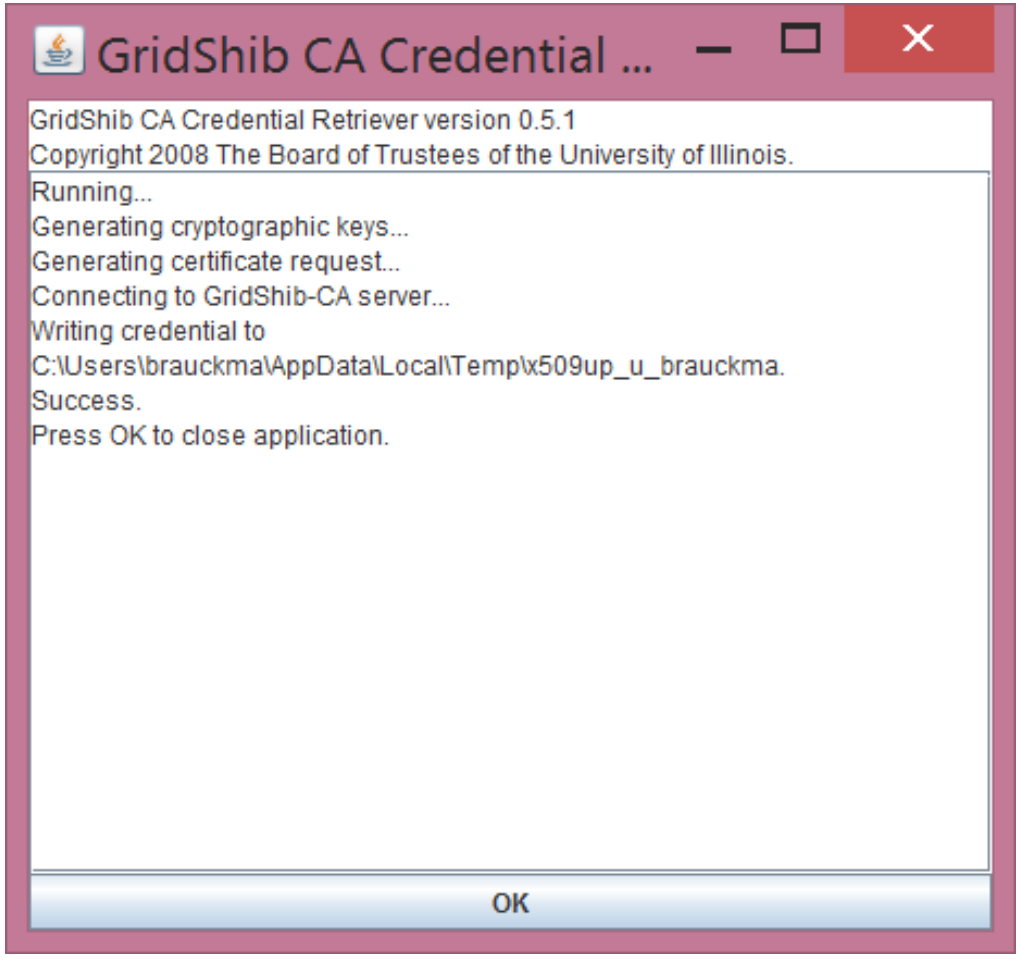
Get your Grid Credential

Credential Lifetime: Default (12 hours) Other: 12 Hours (168 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


GridShib CA Credential ...
GridShib CA Credential Retriever version 0.5.1
Copyright 2008 The Board of Trustees of the University of Illinois.
Running...
Generating cryptographic keys...
Generating certificate request...
Connecting to GridShib-CA server...
Writing credential to
C:\Users\brauckma\AppData\Local\Temp\x509up_u_brauckma.
Success.
Press OK to close application.
OK

Existing alternative for Credential Retriever:
Portal delegation

- Delegation from portal to gridshib-ca with existing AAI login
- User still has to click a button
- Still browser-based

Summary:

- DFN supports grid community and provides certificates
- Grid certificate demand is low
- SLCS even less demand
- SLCS is an expensive service (shib)