SLCS der DFN-PKI

September 2009

Jürgen Brauckmann
dfnpca@dfn-cert.de

Überblick

- Aktuelle Informationen zur DFN-PKI
- SLCS der DFN-PKI

Aktuelle Informationen zur DFN-PKI

Aktuelles (1)

- Mehr als 240 Einrichtungen nutzen DFN-PKI
- Mehrere CAs mit >10.000 Zertifikaten
  - Keine Grid-Zertifikate, Policy aber vergleichbar
  - Anbindung in Hochschul-IDM
  - Zertifizierung über SOAP-Schnittstelle
  - Nutzung auf Chipkarten
- Grid-Zertifikate kontinuierlich genutzt, ca. 1.000 Zertifikatnehmer

Aktuelles (2)

- Integration Telekom Root in Mozilla ist erfolgt (DFN-PKI Global, **nicht** Grid)

- Zeitstempeldienst: Stetige Nutzung (200-300 pro Monat)

  Bei Interesse:
  www.pki.dfn.de/zeitstempel
- Java RA-Oberfläche wird genutzt
- OCSP Test-System ist verfügbar

Root-Integration

DFN Deutsches Forschungsnetz

Status der Integration Telekom Root CA2

- **Windows**: alle aktuellen Desktop Versionen
- **Apple**: seit Juni 2008 (Mac OS X, iPod, iPhone)
- **Opera**: in aktueller Version
- **Mozilla**: Firefox >= 3.0.12
  Thunderbird >= 2.0.0.23
- **Sun Java**: Integration ab V6u11 erfolgt (11.08)
- **Google Chrome**: OK, da abhängig vom OS

DFN-PKI Global, **nicht** Grid!

Alle Informationen zur Integration unter

www.pki.dfn.de/integration

SLCS der DFN-PKI

- Überblick
- Rahmenbedingungen
- Technik
- Tour

Überblick

Überblick SLCS

- Bezug von Zertifikaten auf der Basis von Shibboleth und der DFN-AAI

- Für Einrichtungen, die identifizierte Nutzer im IdP eintragen
- Keine Browserintegration
- Zwei Varianten:
  - SLCS der DFN-PKI: EUGridPMA Akkreditierung
  - Zweiter SLCS ohne Akkreditierung als Test-System in der Test-AAI verfügbar

Rahmenbedingungen

Rahmenbedingungen

Sinn der Vorgaben:

- Sicherer/kontrollierter Zugriff auf Ressourcen (Anforderung der Ressourceprovider)

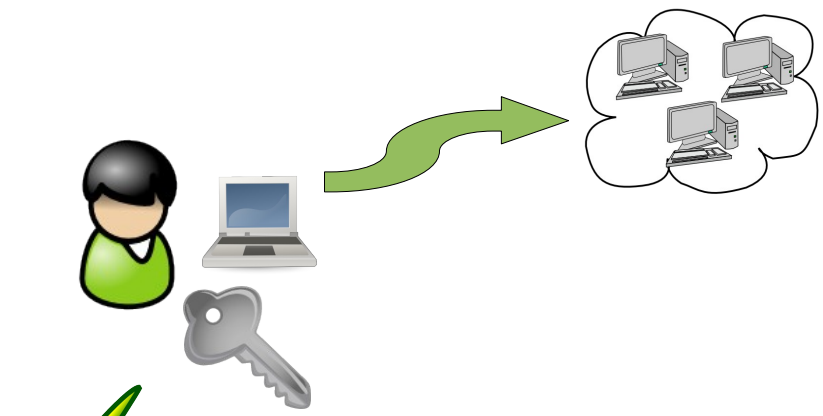
EUGridPMA Akkreditierung:

- Persönliche Identifizierung
- Schnelle Reaktionszeit bei IdP-Pflege
- Audits bei IdPs möglich
- Eindeutigkeit von Namen (eduPersonPrincipalName...)
- Nutzer hat direkte Kontrolle über privaten Schlüssel (kein Portal!)

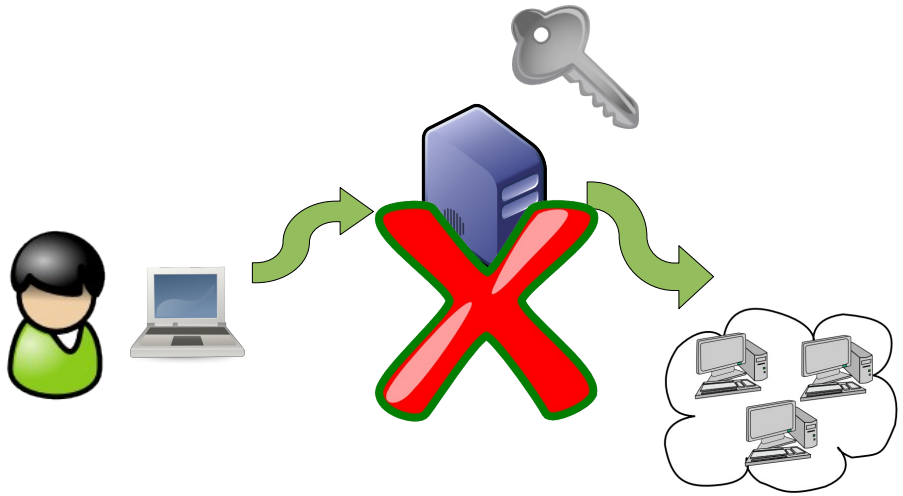
Kontrolle des Schlüssels (1)

Schlüsselerzeugung und Besitz, klassisch:

- Nur durch/beim Nutzer!
- Keine Nutzer-Zertifikate im Portal!
- Problem: Portale können dann kein Grid nutzen...



Schlüssel beim Nutzer



Schlüssel beim Portal

Kontrolle des Schlüssels (2)

Lösungsmöglichkeiten für Portale:

- Proxy-Zertifikate und Abläufe zur Verteilung derselben
- ROBOT-Zertifikate:
  - Client-Zertifikat für das Portal, verwendet „im Auftrag eines Nutzers“, ein Zertifikat für alle Nutzer
  - Nur auf Crypto Token
  - Spezieller DN:
    `/C=DE/O=GridGermany/OU=DFN-CERT Services GmbH`
    `/CN=ROBOT: Test-Portal: Juergen Brauckmann`
- Aktuelle Diskussion EUGridPMA:
  - Zert.- und Schlüsselverwaltung durch Portale erlauben?
    => Nur unter engen Voraussetzungen

Formales

- Resultat der EUGridPMA Vorgaben:
  - SLCS-Teilnahmeerklärung
  - Teilnahmeerklärung geht über AAI hinaus: Strengere Vorgaben für IdP-Pflege, Audits
- SLCS Policy:
  http://www.pki.dfn.de/slcs

Technik

Technik (1)

- SLCS ist eingebunden in die DFN-AAI
- Identity Provider müssen Attribute zur Verfügung stellen:
  - eduPersonPrincipalName
  - surName
  - givenName
  - email
  - eduPersonEntitlement mit Wert `urn:geant:dfn.de:dfn-pki:slcs`

Technik (2)

Ablauf:

1) Nutzer wählt SLCS Web-Seite
2) Loggt sich über seinen IdP ein
3) Bekommt eine Java Webstart Applikation
4) Java WS erzeugt Zertifikat und legt es auf Nutzer-Rechner ab

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://slcs.pca.dfn.de/gridshib-ca/slcs_2.html

DFN
Deutsches Forschungsnetz

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

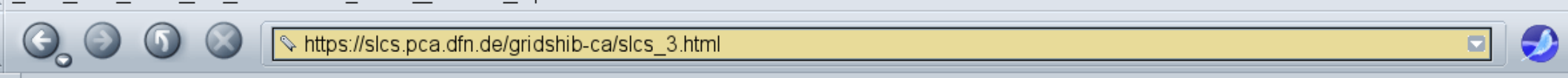
Willkommen zum SLCS der DFN-PKI

Hier können Sie das CA-Zertifikat und die Signing-Policy-Datei des SLCS der DFN-PKI herunterladen

- Das CA-Zertifikat finden Sie hier: CA-Zertifikat
- Die Signing Policy Datei finden Sie hier: Signing Policy

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"

Impressum



DFN
Deutsches Forschungsnetz

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

Willkommen zum SLCS der DFN-PKI
Hier finden Sie die Policy des SLCS der DFN-PKI.

- Policy des SLCS der DFN-PKI zum Download

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

Fazit

- DFN-PKI Betrieb erfolgreich
- SLCS steht mit EUGridPMA Akkreditierung zur Verfügung

pki@dfn.de

http://www.pki.dfn.de