Deutsches Forschungsnetz

DFN
Deutsches Forschungsnetz

DFN-PKI GridGermany Accreditation of DFN-SLCS-CA

15th EUGridPMA meeting

Nicosia, January 26th 2009

Reimer Karlsen-Masur

Overview

- DFN-SLCS-CA with Shibboleth-based DFN-AAI
- DFN-SLCS-CA
  - basic details
  - architecture
- A user's run to get a SLC
- CP/CPS review status

DFN-SLCS-CA
with
Shibboleth-based DFN-AAI

SLCS-CA w/ Shibboleth-based DFN-AAI federation

DFN Deutsches Forschungsnetz

- DFN operates an online CA for short-lived certificates (SLC) (valid for max. 1Mio secs)
- CA is a service provider (SP) within the Shibboleth-based DFN-AAI federation
- Distributed RAs at the user's home org implemented as Identity Providers (IdP) in the DFN-AAI
- CA uses authN decisions of users' home orgs' IdPs to authN users
- CA uses attributes of users' home orgs' IdPs to base authZ decision on and to construct unique sDN for the SLC

DFN-AAI federation background

- DFN-AAI federation started in 2007
- Shibboleth-based federation of DFN orgs
- 30+ participating orgs
- DFN-AAI policy, covers
  - Identity Management System (IDMS) issues, attributes, processes within the org
- Contracts between AAI-participants and DFN
- additional SLCS-participant agreement between org and DFN if org wants to provide SLCs to its users

DFN-AAI basics

- Defined set of compulsory attributes
- Rules to define and document processes in the IDMS
- Rules to update IDMS data
- Rules for the ID vetting of the users

DFN-SLCS-CA
basic details

CA basics: Root Certificate

```
Version: 3 (0x2)
Serial Number: <number>
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN SLCS-CA
Validity
    Not Before: <date>
    Not After : <date - validity is 10 years>
Subject: C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN SLCS-CA
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
        Modulus (2048 bit): <key modulus>
        Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier: <hash>
  X509v3 Authority Key Identifier: keyid:<hash>
  X509v3 Basic Constraints: critical
    CA:TRUE
  X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
Signature Algorithm: sha1WithRSAEncryption
<dig sig>
```

CA basics: Sample CRL

- CRLs valid for 30 days
- re-issued 5 days before expiry

```
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /C=DE/O=DFN-Verein/OU=DFN-PKI/CN=DFN SLCS-CA
  Last Update: <date>
  Next Update: <date - validity is 30 days>
  CRL extensions:
    X509v3 CRL Number:
     <number>
No Revoked Certificates.
    Signature Algorithm: sha1WithRSAEncryption
<dig sig>
```

CA basics: Namespace for SLCs

/C=DE

/O=GridGermany

/OU=SLCS

/OU=<assigned org name>

[/OU=<assigned org unit name>]

/CN=<unique persistent common name (eduPersonPrincipalName attritube from IdP)>

CA basics: Sample SLC

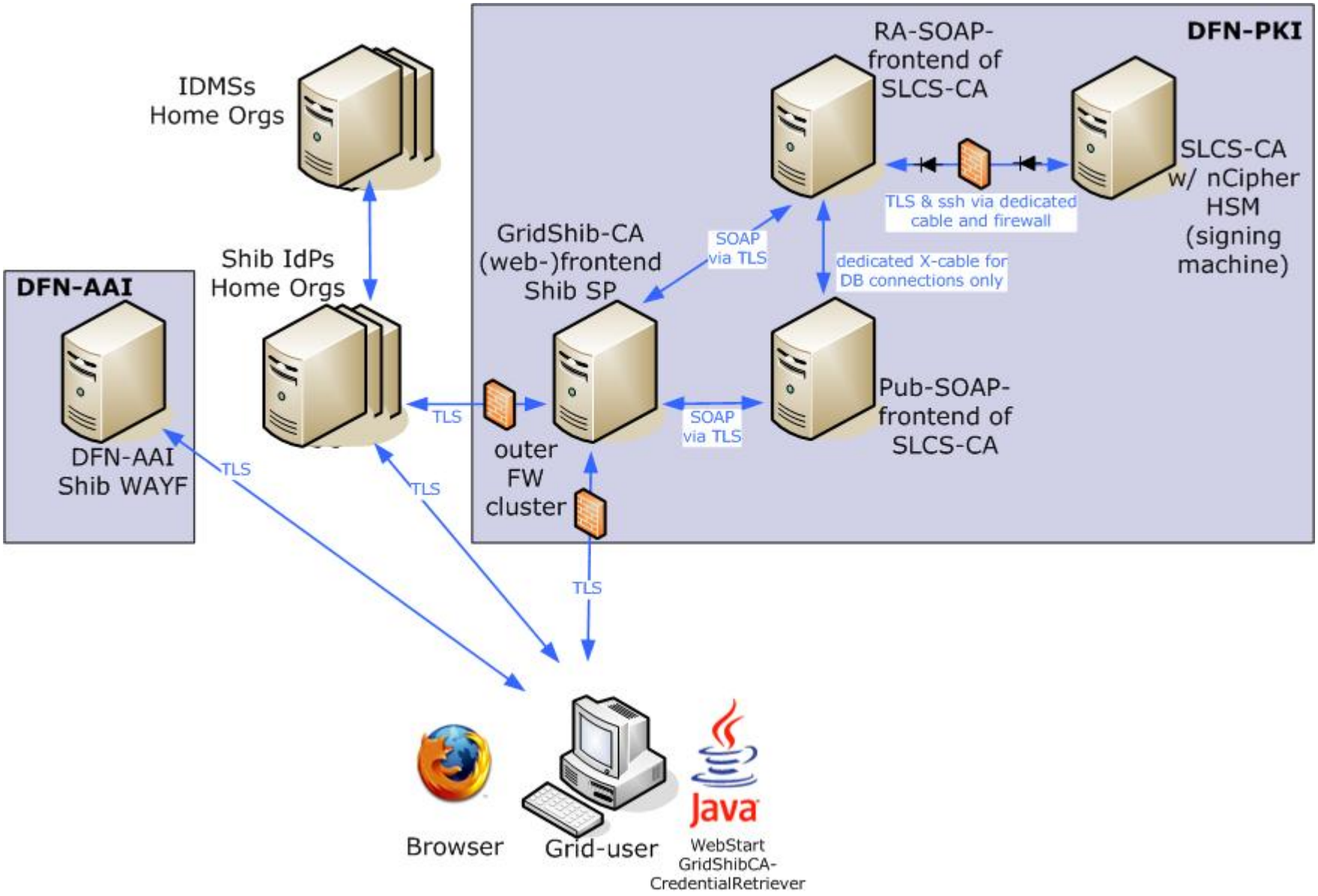
```
Version: 3 (0x2)
Serial Number: <number>
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN SLCS-CA
Validity
  Not Before: <date>
  Not After : <date - validity is max. 1000000 seconds>
Subject: C=DE, O=GridGermany, OU=SLCS, OU=DFN-CERT Services GmbH,
         CN=karlsen-masur@dfn-cert.de
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit): <key modulus>
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment, Data Encipherment
  X509v3 Extended Key Usage: TLS Web Client Authentication
  X509v3 Subject Key Identifier: <hash>
  X509v3 Authority Key Identifier: keyid:<hash>
  X509v3 Subject Alternative Name: email:karlsen-masur@dfn-cert.de
  X509v3 Certificate Policies:
    Policy: 1.3.6.1.4.1.22177.300.3.1.6.1.1 (CPCPS OID)
    Policy: 1.2.840.113612.5.2.2.3 (IGTF AP SLCS 1SCP)
  X509v3 CRL Distribution Points:
    URI:http://cdp1.pca.dfn.de/slcs-ca/pub/crl/cacrl.crl
  Authority Information Access:
    CA Issuers - URI:http://cdp1.pca.dfn.de/slcs-ca/pub/cacert/cacert.crt
Signature Algorithm: sha1WithRSAEncryption
<dig sig>
```

DFN-SLCS-CA architecture

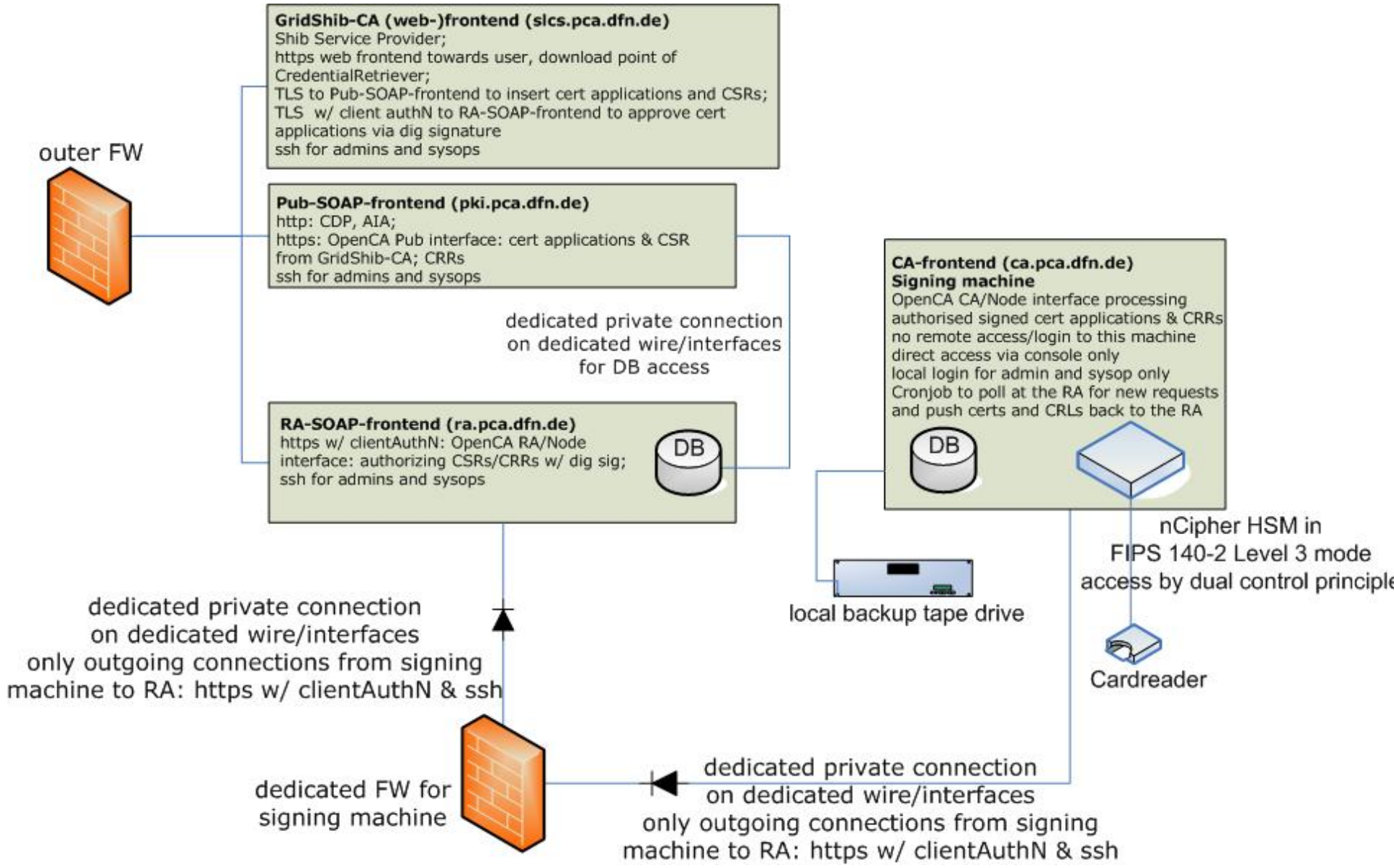
DFN-SLCS-CA architecture (1)

- CA setup is OpenCA-based with GridShib-CA
  - consists of 4 machines:
    - GridShib-CA frontend: Shibbolized user web frontend with Java WebStart application to generate keys on user machine, generates unique sDNs from the users' attributes
    - PUB frontend: gets cert applications & CSRs from GridShib-CA
    - RA frontend: gets digitally signed approval for cert applications from GridShib-CA
    - Signing machine: gets approved cert applications
- Plus Shibboleth federation infrastructure

DFN-SLCS-CA architecture (2)



DFN-SLCS-CA architecture (3)



A user's run to get a SLC

A user's run to get a SLC (1)

- Home org of a user
  - participates in DFN-AAI
  - sets-up its IdP and IDM systems and processes
  - applies for DFN-SLCS participation
    - signs the DFN-SLCS participant agreement which specifically sets strong rules for Shibboleth accounts that are allowed to use the SLCS
    - sets-up the SLCS-RA as part of the IDMS's user registration process

A user's run to get a SLC (2)

- DFN-SLCS-CA
  - checks org's application details
  - assigns IdP specific namespace
    - /C=DE/O=GridGermany/OU=SLCS/OU=<org name>[/OU=<org unit name>]
  - configures the DFN-SLCS-CA GridShib-CA component to accept TLS Shib log-ons from that IdP

A user's run to get a SLC (3)

- User wants to use the SLCS
  - initially registers with his/her SLCS-RA
    - personal ID vetting with official photo ID at SLCS-RA
    - SLCS-RA sets up Shib account for user if not already existing, checks personal account data incl. email address
    - assigns unique persistant eduPersonPrincipal-Name (epPN) attribute e.g. user@domain to user's Shib account
    - sets specific eduPersonEntitlement (epE) attribute value (urn:geant:dfn.de:dfn-pki:slcs) to allow the user to access the SLCS
    - vetting details and epPN attribute are documented & archived by SLCS-RA

A user's run to get a SLC (4)

- User wants to get a SLC
  - uses web-browser to visit the SLCS' GridShib-CA web-site (TLS secured)
  - does the TLS-based Shib log-in dance with DFN-AAI WAYF and user's home org's IdP

A user's run to get a SLC (5)

- GridShib-CA
  - retrieves user's epE, epPN & email-address attributes (signed by IdP) from IdP
  - checks for proper epE attribute (equals urn:geant:dfn.de:dfn-pki:slcs?)
  - builds the sDN for the SLC: /C=DE/O=GridGermany/OU=SLCS /OU=<IdP's org name> [/OU=<org unit name>]/CN=<user's epPN>
  - presents sDN to user

A user's run to get a SLC (6)

DFN Deutsches Forschungsnetz

- User
  - accepts DFN-SLCS CP/CPS and sDN, sets the requested validity time and requests SLC
  - automatic download of Java WebStart application GridShib-CA's Credential-Retriever to user's machine; CredentialRetriever inherits Shib credential for later authN/Z at the GridShib-CA
  - CredentialRetriever generates key pair (1024 bit RSA) & CSR on user's machine, uploads it to GridShib-CA and waits for the SLC to be returned

A user's run to get a SLC (7)

- GridShib-CA
  - uploads CSR, sDN, email-address, requested validity time plus metadata aka „certificate application” into the DB system via Pub-SOAP-frontend (TLS)
  - approves the certificate application with a dig sig on the RA-SOAP-frontend (TLS w/ clientAuthN)

A user's run to get a SLC (8)

- Signing Machine
  - polls for approved cert applications from RA-SOAP-frontend (TLS w/ clientAuth)
  - if found, checks for valid approving dig sig
  - issues SLC
  - delivers it back to the RA-SOAP-frontend (TLS w/ clientAuth)

A user's run to get a SLC (9)

- GridShib-CA
  - polls at the RA-SOAP-frontend for expected SLC (TLS w/ clientAuth)
  - when it arrived it's being passed on to the waiting CredentialRetriever
- User
  - CredentialRetriever puts the SLC into a file
  - can start using his SLC
  - web-browser shows success/info page

CP/CPS review status

CP/CPS review status

- Current version: 0.10 draft
- Compliant to IGTF-AP-SLCS 2.1 w/ CRLs
- It's the result of review process with Mike Helm and Kaspar Brand
- Identified some issues in previous versions which have been sorted out in current version
- This version becomes version 1.1 once the CA is accredited

Thanks to the reviewers

- Special thanks to the CP/CPS reviewers
  - Mike Helm (ESnet)
  - Kaspar Brand (SWITCH)
    - also for the template of a working SLCS-CP/CPS
    - and for paving the Shibboleth path into the EUGridPMA

Questions?

Thanks for your attention!

Questions & Answers