OpenCA
Research & Development Labs

Shibboleth.

OpenCA & Shibboleth

Universität Konstanz, Rechenzentrum

Gruppe Kommunikationsinfrastruktur

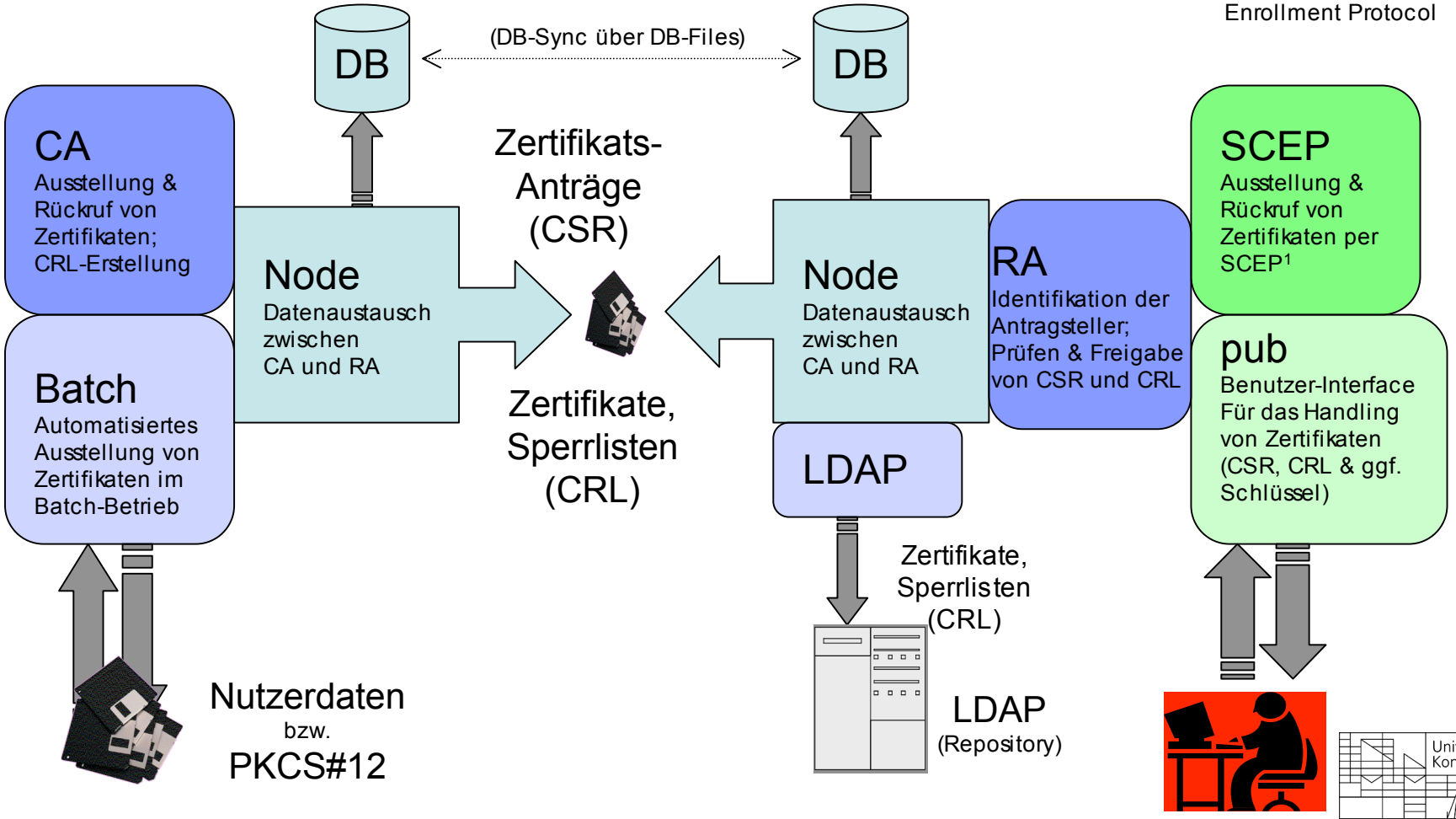
Markus Grandpré

Andreas Merkel

Giovanna Ratini

- Freie Software zum Aufbau einer Public Key Infrastruktur (PKI)
- Basiert auf den kryptografischen Funktionen von OpenSSL, OpenLDAP (öffentliches Repository), DBI (SQL-DB-Anbindung) und dem Apache-Web-Server
- Produktiver Einsatz in mehreren Organisationen

[1] = Cisco Simple Certificate Enrollment Protocol



Zugriffskontrolle auf die Module erfolgt dreistufig:

- Zugriffskanal (Channel: http/https)
- Login per UserID/Passwort oder Nutzer-Zertifikat
- Rolle

Module bzw. Interfaces	Gewählte Login Art	Rolle	Zugriffschutz mit Schibboleth
CA (Certification Authority)	UserID/Passwort (interne DB)	CA Operator	**Nein**
RA (Registration Authority)	UserID/Passwort (interne DB)	RA Operator	**JA**
NODE	UserID/Passwort (interne DB)	RA Operator	**JA**
LDAP	UserID/Passwort (interne DB)	RA Operator	**JA**
SCEP	UserID/Passwort (interne DB)	RA Operator	**JA**
PUB	Ohne UserID/Passwort	User	**JA**

Mit Shibboleth	Ohne Shibboleth
Sichere Authentifizierung gegen einen zentralen IdP Wahlweise mit UserID/Passwort oder mit X509 Nutzer-Zertifikaten	**Lokale Benutzerverwaltung** Mehraufwand für die Programmierung zur sicheren Authentifizierung gegen eine externe Benutzerdatenbank
Sichere Datenquelle Benutzerdaten werden direkt aus unserer Benutzerdatenbank in das Repository des IdP übertragen	**Unsichere Datenquelle** Anwender gibt seine persönlichen Daten selbst über das Web-Frontend (Browser) ein
OpenCA Teil eines uni-weiten SSO-Service User braucht sich nur einmal an einem Service-Portal anmelden	**Dedizierte UserID/Passwort Paare** Nutzer muss sich für jede Anwendung eigene Zugangskennungen mit (hoffentlich) unterschiedlichen Passworten merken

- **Keine Code Änderungen in Shibboleth erforderlich ☺**
- **‚OpenCA Rolle' wurde in das Schema-Attribut <Description> abgebildet**
- **Anpassungen nur in der Anwendung 'OpenCA' selbst:**

  - Definition eines neuen *Login-Typs <Shibboleth>* *(node.xml)*
  - Abbildung der entsprechenden OpenCA-Rolle *(z.B. RA Operator)* in das Schema-Attribut <Description>
  - Änderungen im Source Code zur Implementierung des neuen *Login-Typs <Shibboleth>*
  - Änderungen im Source Code zur Implementierung des neuen IO-Moduls zur Datenübernahme aus dem IdP-Repository

- **Programmierung erfolgte unter der Anleitung von Giovanna Ratini von Markus Grandprè vorgenommen und mit einem der OpenCA Entwickler (Michael Bell) abgestimmt;**
- **die o.g. Funktionen wurden der OpenCA Entwicklergemeinde zur Verfügung gestellt.**

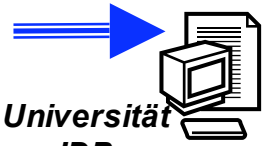
1 User zu OpenCA

Remote/lokaler Nutzer
WWW-Browser (IE, Mozilla, etc.)
PC (>= W2K); MAC (OS X)

2 Shib -> zu WAYF

Shibboleth Service Provider
OpenCA (DFN? Uni Konstanz)

Shibboleth WAYF



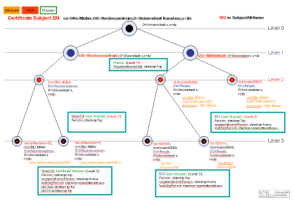
Shibboleth Identity Provider
Uni-Konstanz

3 User sagt welche Universität
4 WAYF meldet sich zu IDP

7 Shib. shickt Auth & Attribute zu Service Provider

5 IDP macht Authent
durch Zert oder Login PW
gegenüber OpenLDAP

OpenLDAP



6 Shibboleth Verhandlungen