Alternative AAI auf Basis von kurzlebigen Zertifikaten

Stefan Pinkernell[1], Bernadette Fritzsch[1],
Stefan Funk[2], Martin Haase[2], Peter Gietz[2]
1.)Alfred-Wegener-Institut für Polar- und Meeresforschung 2.)DAASI International GmbH

Wie kommen die SLCs ins Portal / Grid ?

SLC - Steckbrief
- Short lived credentials (SLC)
- Digitale X509 - Zertifikate
- Lebenszeit: max. 1 Million Sekunden (~11,5 Tage)
- DFN-SLCS (http://www.pki.dfn.de/slcs)
- Verwendet werden Proxy-Zertifikate
- Bezug per Java WebStart –Anwendung: CredentialRetriever
- Keine Browser-Integration
- Akkreditierte und nicht akkreditierte Version
- Authentifizierung per Shibboleth

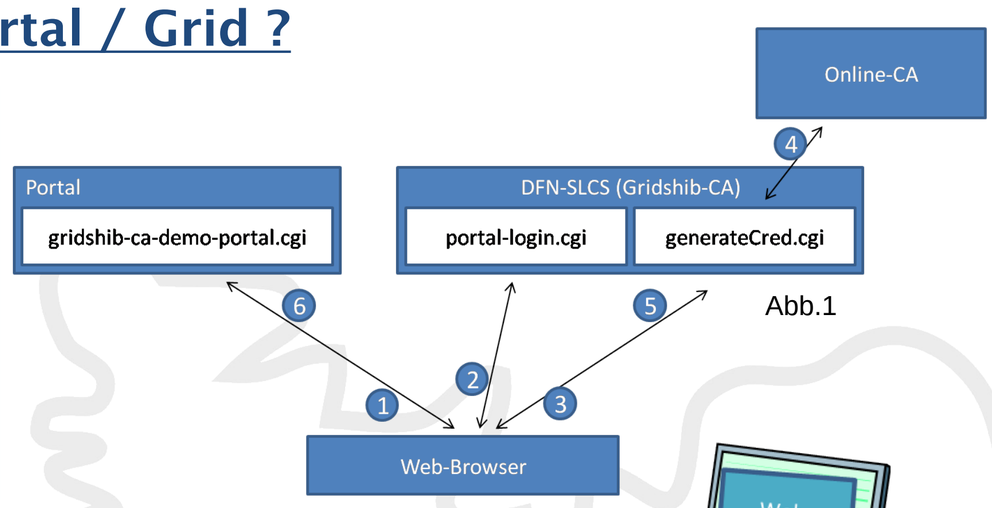


Abb.1

Abb.1: Portal Delegation
1. Portal-Aufruf generiert Schlüsselpaar und Cert-Request
2. Cert-Request wird gesendet, spätestens hier: Shibboleth-Auth.
3. Zustimmung zu PortalDelgation (Token)
4. Zertifikat wird ausgestellt
5. Zertifikat wird an Web-Browser gesendet
6. Zertifikat wird an Portal weitergeleitet

Abb.2: Portal Delegation

1. Nutzer Login am shibbolisierten Portal
   a) Portalaufruf
   b) Weiterleitung an den WAYF zur Auswahl der Heimateinrichtung
   c) Weiterleitung an den Shib-IdP der Heimateinrichtung zur Authentifizierung
   d) Weiterleitung des authentifizierten Nutzers an das Portal
2. a) Portal generiert Schlüsselpaar sowie Zertifikat-Request und kontaktiert den DFN-SLCS
   b) Kurzlebiges Zertifikat (SLC) wird durch Online CA ausgestellt
3. Bezug der am VOMS hinterlegten VO-Attribute (Authentifizierung über das SLC)
4. Am Portal: Ausstellung einer neuen SAML Assertion mit den gesammelten Campus- und VO-Attributen, die in das vom SLC abgeleitete Proxy-Zertifikat eingebettet wird
5. Über das Portal können Grid-Jobs abgeschickt werden (abgesichert durch das Proxy Zertifikat)

Achtung: Unverschlüsseltes Abspeichern von privaten Schlüsseln der Nutzer am Portal nicht erlaubt. Diese werden während der Browser-Session im Speicher des Portals gehalten.

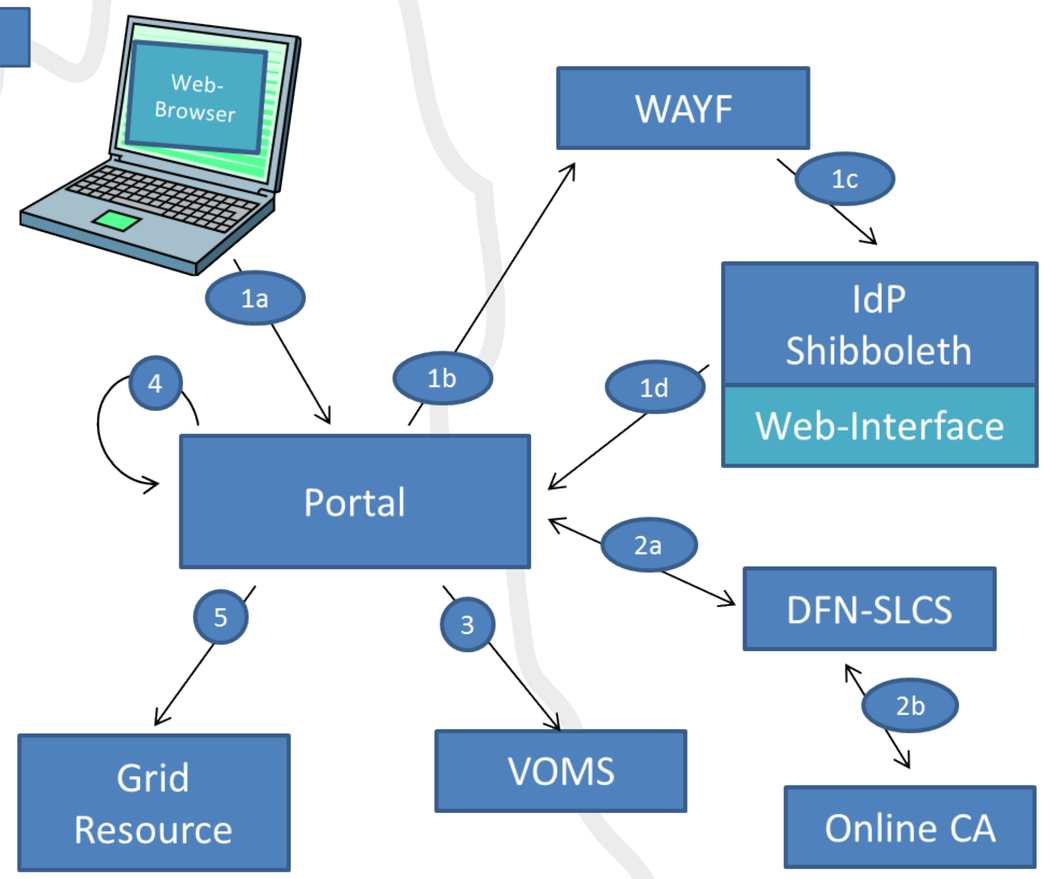


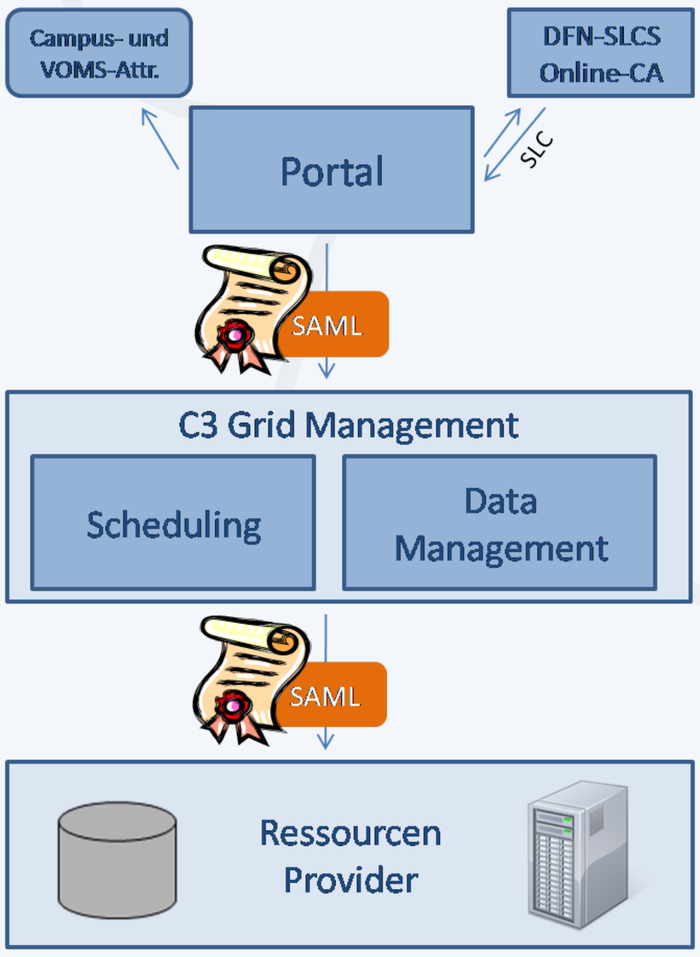
Abb.2

Wie werden SLCs bei den Communities verwendet? Use Cases.

TextGrid

Portal Delegation mit Rechtesynchronisierung auf der Grid-Ressource

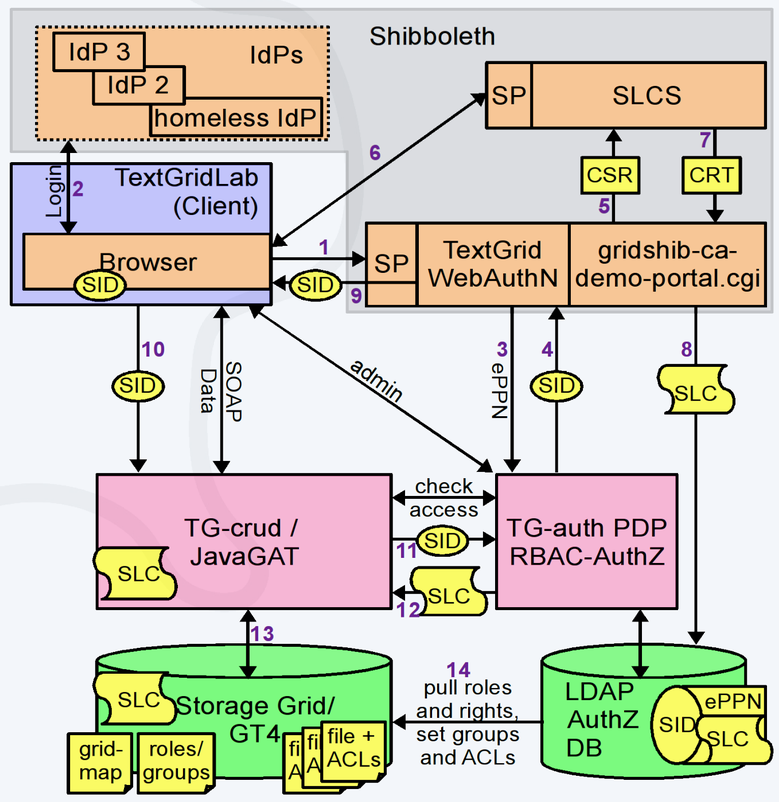
1+2. Authentifizierung über Shibboleth
3+4. Erzeugung der TextGrid SessionID (Security Token)
5-8. Bezug des SLC und Speicherung in der Autorisierungskomponente TG-auth*
9+10. Rückgabe der SID und Anfrage des Rich Clients am zentralen Dateioperations-Dienst TG-crud
11+12. Bezug des SLC von TG-auth* (alternativ MyProxy)
13. Verwendung des SLC durch TG-crud bei Grid-Operationen
14. Rechte- und Rolleninformation aus TG-auth* werden regelmäßig auf Zugriffsrechte auf Dateiebene (POSIX ACLs) und UNIX-Gruppen abgebildet.



C3-Grid

Konzept mit Portal Delegation und Autorisierung anhand SAML Assertions

1. Authentifizierung am Portal per Shibboleth.
2. Portal bezieht ein SLC vom DFN-SLCS.
3. Aus Campus- (und VOMS-) Attributen wird eine SAML Assertion zusammengestellt und durch das Portal signiert.
4. Proxy-Zertifikat wird abgeleitet (SAML Assertion wird dabei in Proxy integriert)
5. Proxy (+SAML) werden durch Scheduling und DMS an die RP weitergereicht.
6. Bei den RP: Autorisierungsentscheidung anhand der Informationen aus der SAML Assertion.



Website:
http://gap- slc.awi.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung