Nutzung von kurzlebigen Zertifikaten in portal-basierten Grids

Stefan Pinkernell[1], Bernadette Fritzsch[1], Stefan Funk[2],
Martin Haase[2], Peter Gietz[2], Sinan Mece[3] , Andreas Schreiber[3]
1.)Alfred-Wegener-Institut für Polar- und Meeresforschung 2.)DAASI International GmbH 3.) Deutsches Zentrum für Luft- und Raumfahrt e.V.

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

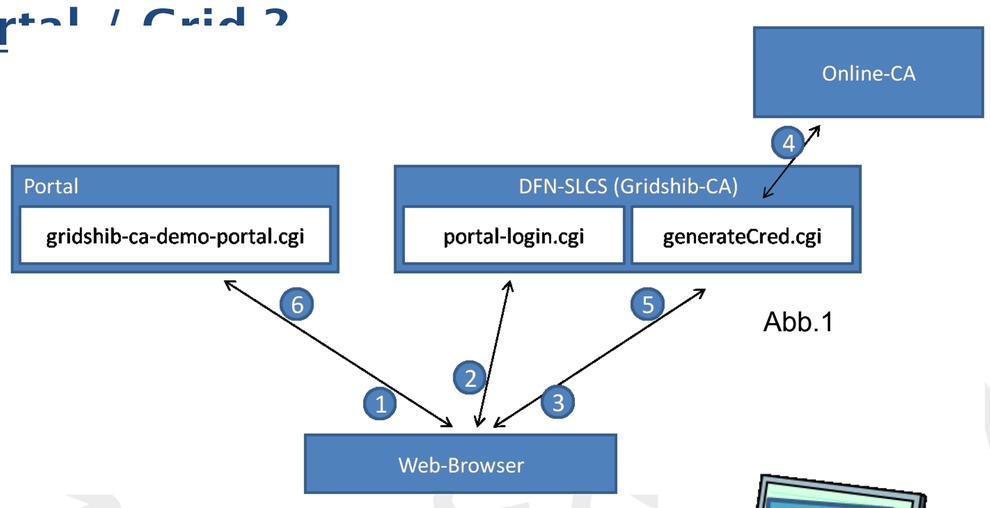


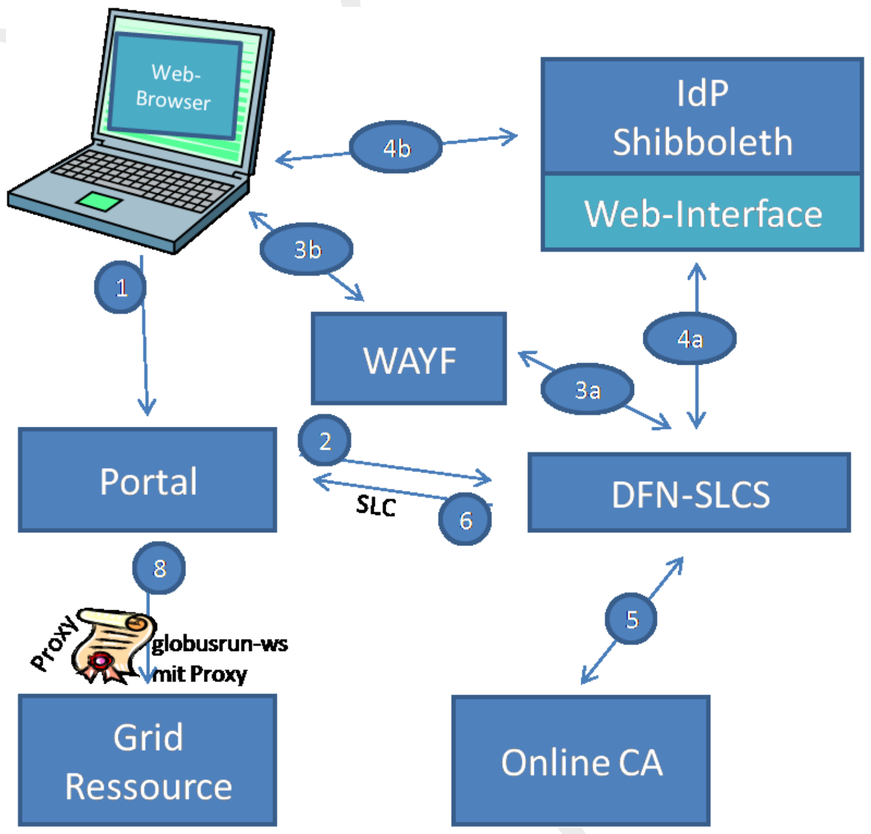
Abb.1

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. Aufruf des Portals durch den Nutzer
   (optional: Ist das Portal shibbolisiert werden die Schritte 3 und 4 vorgezogen)
2. Portal generiert Schlüsselpaar sowie Zertifikat-Request und kontaktiert den DFN-SLCS
3. a) Weiterleitung an den WAYF
   b) Auswahl der Heimateinrichtung durch den Nutzer
4. a) Weiterleitung an den IdP der Heimateinrichtung des Nutzers
   b)Authentifizierung am IdP
5. Kurzlebiges Zertifikat (SLC) wird durch Online CA ausgestellt
6. SLC wird an das Portal zurückgesende
7. Am Portal wird vom SLC ein Proxy-Zertifikat abgeleitet
8. Über das Portal können Grid-Jobs abgeschickt werden

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

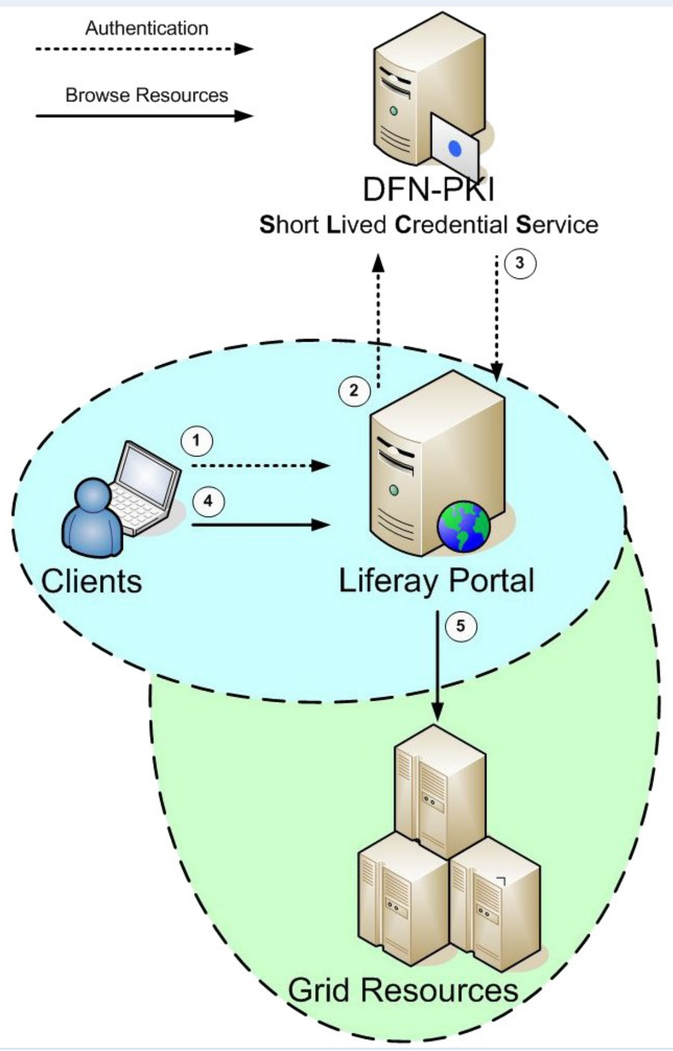


Wie werden SLCs bei den Communities verwendet? Use Cases.

AeroGrid

Liferay basiertes Portal zum Zugriff auf Grid-Ressourcen über Unicore 6

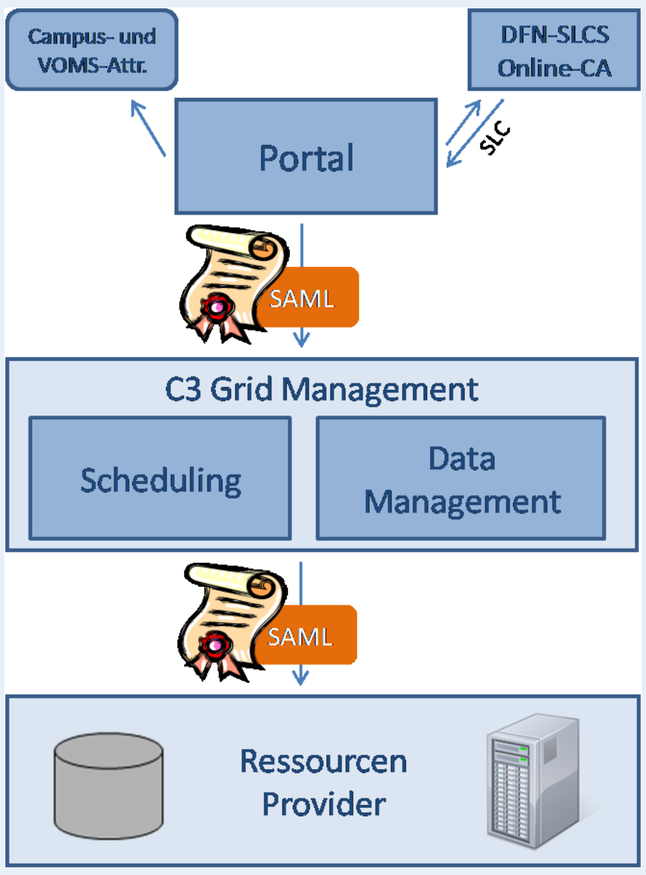
1. Nach Anmeldung am Portal: Anforderung eines SLC über das Short Lived Credential Service - Portlet
2. Portlet erzeugt im Namen des Clients eine Zertifikatsanfrage
3. SLC wird im Portal in einem Keystore gespeichert
4. Per Datafinder - Portlet kann auf die Grid Resourcen zugegriffen werden
5. Zugriff erfolgt über einen Unicore 6 - CLI - Wrapper



C3-Grid

Konzept mit Portal Delegation und Autorisierung anhand SAML Assertions

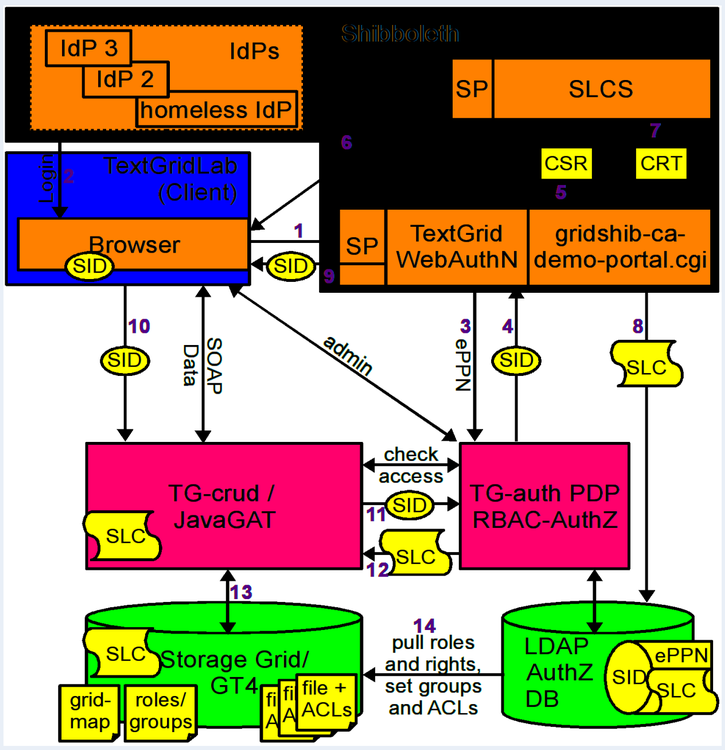
1. Authentifizierung am Portal per Shibboleth.
2. Portal bezieht ein SLC vom DFN-SLCS.
3. Aus Campus- (und VOMS-) Attributen wird eine SAML Assertion zusammengestellt und durch das Portal signiert.
4. Proxy-Zertifikat wird abgeleitet (SAML Assertion wird dabei in Proxy integriert)
5. Proxy (+SAML) werden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



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.



GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung