Projekt „Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids (GapSLC)“

1 Einleitung

GapSLC resultiert aus den Erfahrungen früherer Projekte, dass die in D-Grid etablierte Sicherheitsinfrastruktur für einige Nutzer wenig komfortabel ist und vor allem technikferne Gruppen daher vor dem Einstieg in das Grid zurückschrecken. Das Projekt vereinte Vertreter aus C3Grid, TextGrid, MediGRID und Services@Medigrid und zielte auf Vereinfachung in drei definierten Anwendungsfällen:

- Nutzer, die möglichst weitgehend von allen Prozessen im Zusammenhang mit persönlichen Zertifikaten (Beantragung, Verwahrung, Nutzung im Grid) entbunden werden sollen
- Nutzer, die zwar ein konventionelles persönliches Zertifikat besitzen, aber mit dessen Handhabung überfordert sind
- quasi-anonyme Nutzung des Grids für abgegrenzte Dienste und Ressourcen

Während der Projektlaufzeit 05/2009 bis 06/2011 wurden bereits vorhandene Ansätze verschiedener nationaler und internationaler Projekte zu funktionierenden Lösungen verknüpft, die D-Grid-weit bereitgestellt wurden.

2 Nutzung von kurzlebigen Zertifikaten

Im Portal Delegation Verfahren bezieht das Portal im Auftrag des Nutzers jeweils vor dem Starten der Gridanwendung ein „frisches“ kurzlebiges Zertifikat (SLC), sichert damit den Gridjob ab und entlastet dadurch den Nutzer von der Beantragung und Handhabung von Zertifikaten.

Zur Erzeugung kurzlebiger X.509 Zertifikate wird vom DFN der EuGridPMA akkreditierte Short Lived Credential Service (DFN-SLCS) betrieben mit einer Authentifizierung der Nutzer bei ihren Heimateinrichtungen über Shibboleth. Zur Wahrung der Vertrauensbasis müssen die Einrichtungen die Teilnamebedingungen für die DFN-AAI Föderation und für den DFN-SLCS akzeptieren.

Für das C3Grid wurde prototypisch ein Portlet implementiert, mit dem im Portal nach nur wenigen Mausklicks neben dem SLC auch ein abgeleitetes Proxy-Zertifikat zur Verfügung steht, mit dem Jobs im Grid abgesichert werden können. Für eine feingranulare Autorisierung bei den Ressourcenprovidern können automatisch auch ausgewählte Campus-Attribute vom Shibboleth Identity Provider sowie Attribute aus einer virtuellen Organisation (VO) in Form einer SAML Assertion (Security Assertion Markup Language) eingebettet werden. Ein neu implementierter Auto Login Hook ermöglicht den bisher fehlenden Shibboleth-basierten Logins für das in vielen D-Grid-Projekten eingesetzte Liferay. Abbildung 1 zeigt schematisch den Ablauf des Gesamtprozesses.

Für TextGrid wurden die entsprechenden Erweiterungen der Middleware als zuschaltbare Option in die TextGrid-Authentifizierungskomponente integriert**.** Von dort bezieht der Dienst für Grid-Dateioperationen die SLCs auf sicherem Wege. Autorisierungsrelevante Rolleninformationen werden dabei auf Dateiberechtigungen auf der Gridressource abgebildet. Über Shibboleth authentifizierte Benutzer werden zudem automatisch und sicher sofort im VOMRS registriert, zusammen mit den gleichzeitig erhobenen D-Grid-konformen Benutzerattributen und dem zeitnah erzeugten SLC. Eine manuelle Bestätigung durch VO-Repräsentanten entfällt somit.

3 Vereinfachung der Nutzung von persönlichen Zertifikaten

Für Nutzer, die auf das Grid über ein Portal zugreifen, können mittels eines Credential-Management Portlets die notwendigen Credentials aus einem MyProxy Server bezogen werden. Vom Fraunhofer IAO wurde ein Proxy Upload Tool entwickelt (siehe Abbildung 2), das eine leichtgewichtige Anwendung zur Erzeugung von Proxies der persönlichen D-Grid-Nutzerzertifikate und dem Upload auf einen sicheren MyProxy-Server im Grid darstellt, gleichzeitig aber die hohen Sicherheitsanforderungen insbesondere in der Medizin berücksichtigt. Da im klinischen Umfeld meist sehr restriktive Firewall-Umgebungen vorliegen, musste die Kommunikation zwischen Endnutzer und dem MyProxy-Server im Grid über Applet-/Servlet umgesetzt werden.

4 Quasi-anonyme Nutzung des Grids

Für frei zugängliche Daten und eng begrenzte Dienste ist eine Ausweitung der Gridnutzung auch ohne individuelle Authentifizierung von Nutzern vorstellbar und wünschenswert. In Zusammenarbeit mit dem DFN wurden die Anforderungen der Nutzer in die Erarbeitung entsprechender Richtlinien der EUGridPMA eingebracht. Danach wurde die Grid-Policy der DFN-PKI entsprechend angepasst und um Regeln für die Nutzung von Robot-Zertifikaten in D-Grid erweitert.

GapSLC erarbeitete ein Konzept zur Integration von Robot-Zertifikaten in die D-Grid-Policy, das von einer Zweiteilung der Ressourcen ausgeht, wobei jeder Ressourcenprovider selbst entscheiden kann, ob er einen separierten Teil seiner Ressourcen auch für Robot-Zertifikate öffnet. Die entsprechenden Informationen sollten im Ressourcenmanagement vorliegen, so dass die Gridjobs jeweils nur an die dafür vorgesehenen Ressourcen verteilt werden. In TextGrid und MediGRID existieren prototypische Realisierungen von Robot-Services und den zugehörigen Robot Credential Stores.

5 Zusammenfassung

Für die diskutierten Anwendungsfälle konnte durch GapSLC die Handhabung der Sicherheitsinfrastruktur für die Gridnutzer erleichtert werden. Die Software und Dokumentation ist über die Projekt-Website[1] zum Download verlinkt.

[1] http://gap-slc.awi.de/

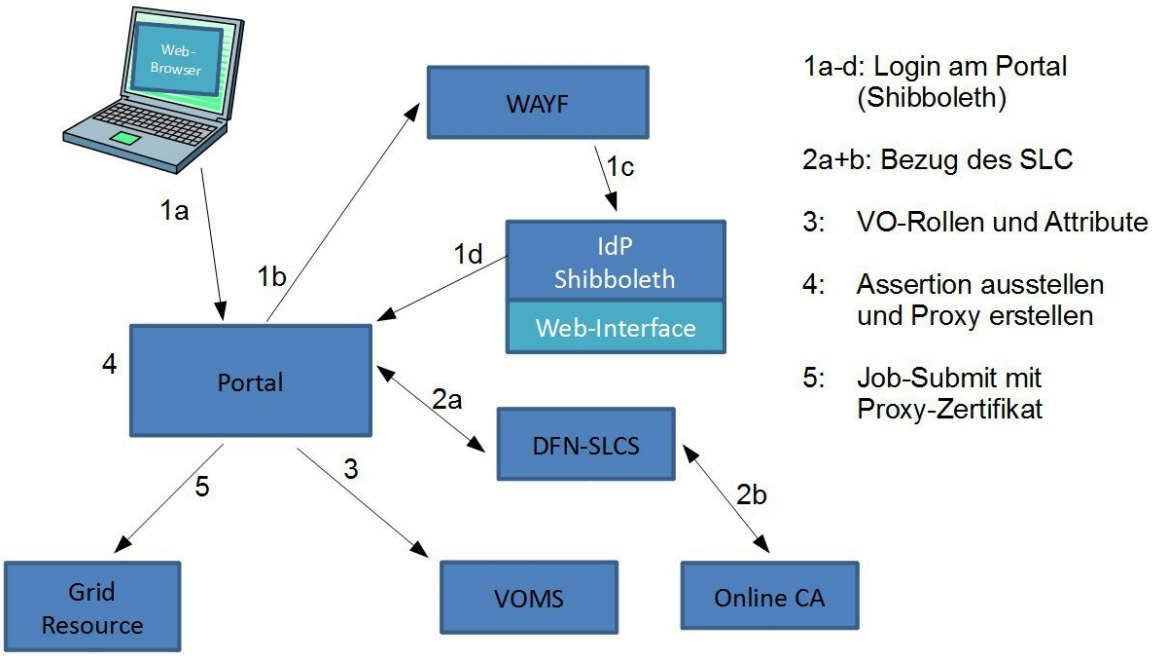

Abbildung 1: Schematische Darstellung der einzelnen Schritte beim implementierten PortalDelegation Verfahren mit kurzlebigen Zertifikaten.

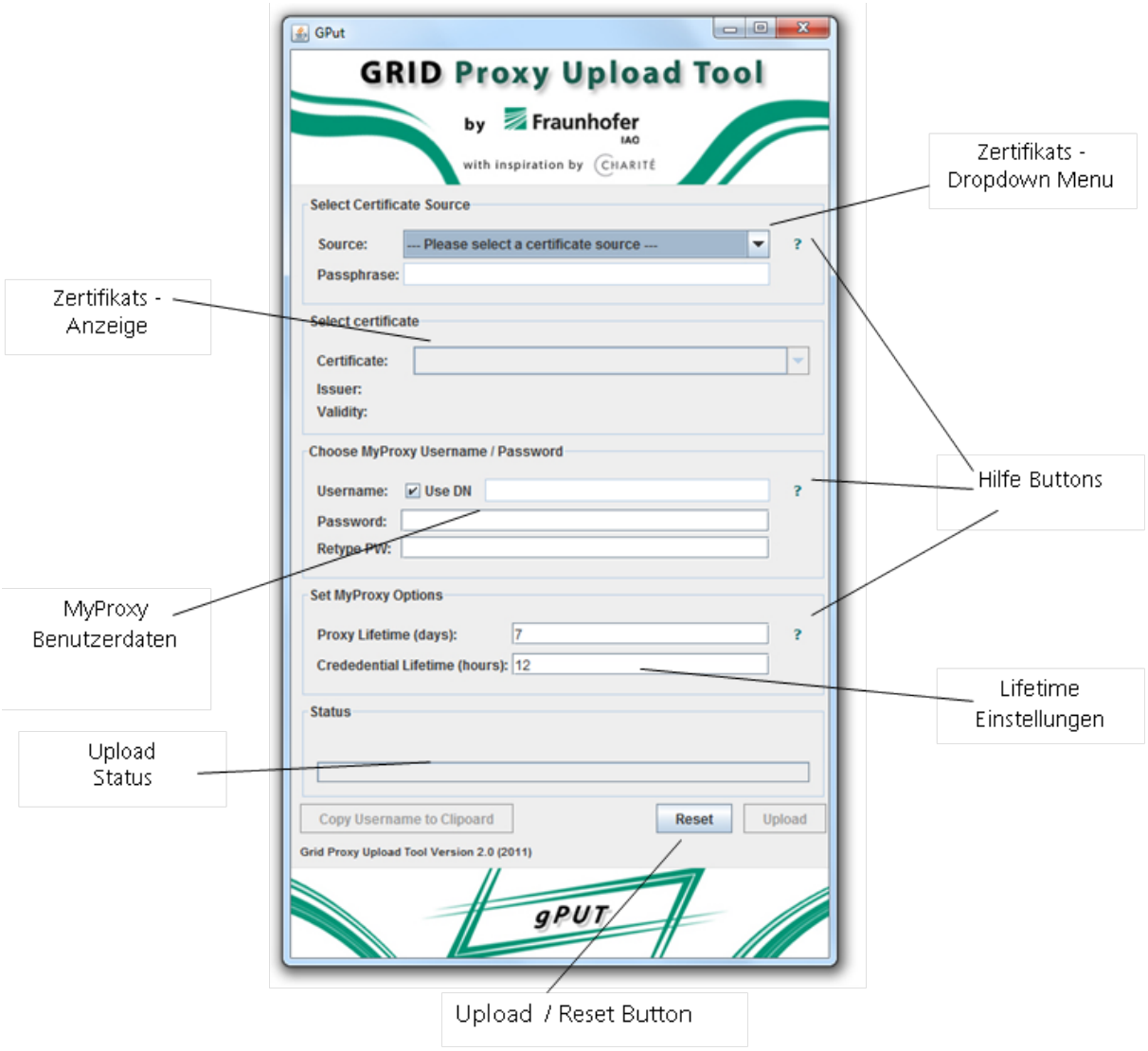

Abbildung 2: Grid Proxy Upload Tool (gPUT)

Projektpartner:
Stiftung Alfred-Wegener-Institut für Polar-. und Meeresforschung Bremerhaven
Fraunhofer Institut für Arbeitswirtschaft und Organisation (IAO)
DAASI International GmbH, Tübingen
Abteilung Medizinische Informatik, Klinikum der Universität Göttingen (UMG)

Kontakt:
Bernadette Fritzsch
Alfred-Wegener-Institut
für Polar- und Meeresforschung Bremerhaven
Am Handelshafen 12
27570 Bremerhaven
Email: Bernadette.Fritzsch@awi.de