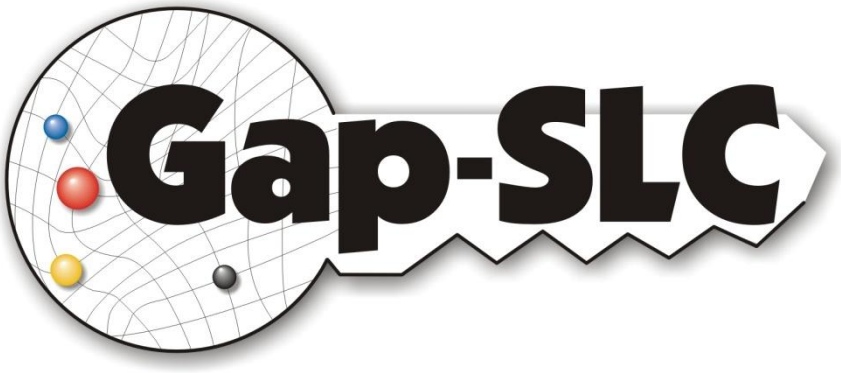
Gap-SLC

Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids



Supportkonzept

– Task 7, Deliverable D7-3 –

– Förderkennzeichen 01IG09003A-D –

„Service Grids für Forschung und Entwicklung“
des Bundesministeriums für Bildung und Entwicklung (BMBF)

Date	**27.05.2011**
Version	**0.3**
Type	**Draft**
Status	**In Progress**
Authors	**B.Fritzsch, S. Pinkernell, M. Pattloch, O. Strauss, P. Gietz,**

Inhaltsverzeichnis

1 Einleitung

Im Rahmen des Projekts „Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids – GapSLC“ wurden unterschiedliche Nutzungsszenarien betrachtet, für die jeweils Lösungen implementiert wurden, um den Anwendern den Zugang zum Grid zu erleichtern. Die Anforderungen stammten zwar primär aus den Grid-Communities, die dieses Gap-Projekt initiiert hatten, jedoch wurden im ersten Workshop auch Anforderungen aus anderen Communities aufgenommen und danach in die Arbeit integriert.

Für die Nachnutzung der entwickelten Softwarepakete wurden jeweils separate Dokumentationen geschrieben, um die Handhabung zu erleichtern. Im Sinne der Nachhaltigkeit sollen hier Überlegungen für ein Supportkonzept dargelegt werden.

2 Überblick über die entwickelten Software-Komponenten

2.1 gPUT

Für die Nutzung von D-Grid-Ressourcen werden klassischerweise sogenannte Proxies der eigentlichen Nutzerzertifikate benutzt. Diese Proxies werden im Rahmen von Grid-Jobs delegiert (Trust Delegation) um den Nutzer gegenüber Ressourcen und Anwendungen im Grid zu authentifizieren. Die Schwierigkeit hierbei ist, dass der Nutzer das Proxy lokal erzeugen, auf sichere Weise ins Grid hochladen und schließlich dafür sorgen muss, dass die Grid-Infrastruktur Zugriff auf dieses Proxy erhält. Die bisher verfügbaren Lösungen erforderten in diesem Prozess Formatkonvertierungen der Zertifikate mit Hilfe entsprechender Software, die auf dem Nutzerrechner installiert sein musste und letztlich mit einem hohen nutzerseitigen Konfigurationsaufwand verbunden war.

Durch das im Gap-SLC-Projekt entwickelte „Grid Proxy Upload Tool“ (gPUT) wurde dieser Prozess für die Nutzer wesentlich vereinfacht. gPUT ist als Java-Applet realisiert und braucht daher nicht als Anwendung installiert zu werden. Der Nutzer kann das gewünschte Zertifikat aus verschiedenen Quellen (PEM-Dateien, P12-Datei, Firefox Keystore, Internet Explorer Keystore, Windows Keystore) laden. Das aus diesem Zertifikat erzeugt Proxy-Zertifikat wird nach Angabe eines optionalen Usernamens und eines Passworts zur Zwischenspeicherung zu einem MyProxy-Server im Grid hochgeladen. Der Upload erfolgt mit Hilfe eines zwischengeschalteten Java-Servlets über den Standard-SSL-Port 443 und ist daher auch in Umgebungen mit restriktiven Firewalls nutzbar. Alle anderen Schritte laufen automatisch und für den Nutzer transparent ab. gPUT ermöglicht dem Nutzer darüber hinaus das Setzen der Proxy- und Credential-Lifetimes und somit eine flexible und an seine Anforderungen angepasste Eingrenzung des mit den Proxies verbundenen Sicherheitsrisikos.

2.2 TextGrid-Lösung

Im Zusammenhang mit der Integration von SLCs in die Textgrid-Infrastruktur wurden folgende produktiv einsetzbare Software-Komponenten entwickelt:

1. Erweiterung der Web-basierten Authentifizierungskomponente um eine Komponente, die sich auf Grundlage einer Shibboleth-Authentifizierung beim DFN-SLCS ein SLC bezieht, sowie um eine Komponente, die neue Benutzer automatisch im VOMRS registriert.
2. Erweiterung des auf OpenRBAC beruhenden Middleware TG-Auth um die Generierung von Schlüsseln und Zertifikatsanträgen, sowie zur Speicherung der SLCs
3. Entwicklung eines Daemons, der die beantragten Schlüssel verwaltet, wobei die privaten Schlüssel und deren Schutzpasswörter aus Sicherheitsgründen nur im flüchtigen Arbeitsspeicher vorgehalten werden.
4. Entwicklung eines über Cronjob angestoßenen Skripts zur Umsetzung der in OpenRBAC festgelegten Zugriffspolicies auf einem Unix-File-System des Grid-Rechners über Posix ACLS
5. Entwicklung eines Programms, welches Benutzer aus dem VOMRS bezieht und deren Zertifikats-Subject-DNs in ein Grid-Map-File einfügt, sowie dazugehörige Accounts auf einem Globus-Rechner im Unix-System anlegt,.

2.3 SLC mit Portal Delegation

Kurzlebige Zertifikate, die erst bei Bedarf bezogen werden, bieten in einem Grid-Portal eine einfach zu bedienende Alternative zu „normalen“ Grid-Zertifikaten. Dazu wurde eine Portlet-Anwendung entwickelt, mit der in einem Portal Delegation Szenario mit wenigen Mausklicks ein kurzlebiges Zertifikat bezogen und im Grid-Portal verfügbar gemacht wird.

2.4 Komponenten für SAML-Lösungen

Als SAML Assertion kodierte Nutzerattribute bieten an einer Grid-Resource eine Basis, auf der eine feingranulare Autorisierungsentscheidung getroffen werden kann. Dazu wurden zwei Komponenten entwickelt: Zum einen wurde das Portal Delegation Portlet um eine Variante erweitert, bei der Attribute aus mehreren Quellen in einer neuen, vom Portal signierten SAML Assertion zusammengefasst werden. Derzeit werden als Quellen sowohl die Shibboleth-Umgebung für Campus Attribute als auch ein VOMS Server für Informationen zu einer virtuellen Organisation genutzt. Die Assertion mit den gesammelten Attributen wird in das Proxy-Zertifikat eingebettet und steht damit an der Grid-Resource zur Verfügung. Dort wird die Software Gridshib for Globus Toolkit eingesetzt, um die SAML-Assertions mit den enthaltenen Nutzerattributen auswerten zu können. Diese Software deckt den hier angewandten Anwendungsfall allerdings nicht komplett ab, so dass hier eine Erweiterung notwendig war. Bei der zweiten Komponente handelt es sich um eine modifizierte Klasse (SAMLUtil.java) in der Bibliothek gridshib-common-0_5_0.jar, die zur Auswertung der neu erzeugten SAML Assertion notwendig ist. Damit kann auch eine eingebettete Assertion

ausgewertet werden, die, wie in diesem Fall, eine andere Zertifikatkette als das Proxy-Zertifikat hat, in das die Assertion eingebettet ist.

2.5 Shibboleth Auto Login Hook für Liferay

Soll das beschriebene Portal Delegation Verfahren in einem Portal angewendet werden, so ist neben dem Portal-Login zusätzlich auch ein Shibboleth-Login notwendig. Für Liferay gab es bisher noch keine Komponente für einen shibbolisierten Login.

Mit dem Shibboleth Auto Login Hook wurde eine solche Komponente entwickelt, über die sich ein Nutzer per Shibboleth an einem Liferay Portal anmelden kann. Die dabei erzeugte Shibboleth Session kann ohne erneuten Login auch für das Portal Delegation verfahren weitergenutzt werden.

3 Support

3.1 Grundsätzliche Maßnahmen

- Die entwickelte Software ist über die GapSLC-Webseiten direkt oder über einen Link an die Entwicklereinrichtung verfügbar.
- Um den Support auch nach personellen Fluktuationen in den Entwicklerteams weiter zu gewährleisten, wurden jeweils nicht personengebundene E-Mail-Adresse für Supportanfragen eingerichtet. Dies sind:

    - AWI: grid-development@awi.de
    - DAASI: gap-slc@daasi.de
    - IAO: srv-mput@medigrid.de

3.2 Spezifische Maßnahmen

3.2.1 SLCS

Der DFN-Verein stellt kurzlebige Grid-Zertifikate (SLC) im Rahmen seines Dienstes DFN-SLCS aus. Um diese Zertifikate auch weltweit in Grid-Umgebungen nutzen zu können, hat der DFN-Verein einen Akkreditierungsprozess der zugrunde liegenden Policy bei der EUGridPMA durchgeführt, der im Februar 2009 erfolgreich abgeschlossen wurde.

DFN-SLCS kann von allen Anwendern im Rahmen der DFN-PKI ohne zusätzliches Entgelt genutzt werden.

3.2.2 gPUT

Die entwickelte Software wird zum Projektende samt dem Quellcode unter einer noch zu bestimmenden Open Source Lizenz über die Projekt-Website veröffentlicht und zur Unterstützung der Nachnutzung und Weiterentwicklung durch eine Entwickler- und Nutzerdokumentationen ergänzt.

3.2.3 TextGrid-Lösung für SLC und SAML

Alle von DAASI erbrachten oben unter **Fehler! Verweisquelle konnte nicht gefunden werden.** beschriebenen Ergebnisse werden als Open Source Software lizensiert und können von der gesamten D-Grid-Community, als auch von weiteren Stellen nachgenutzt werden.

Grundsätzlich ist DAASI bemüht, alle in Forschungsprojekten erbrachten Ergebnisse in Kundenprojekten kommerziell nachzunutzen. Die von DAASI erbrachten Leistungen können sehr gut für wissenschaftliche Grid-Projekte, insbesondere TextGrid nachgenutzt werden. Dies gilt sowohl für die Integration von Shibboleth basierter AAI und SLCs, als auch für den auf OpenRBAC basierenden Policy Decision Point.

Insofern kann wenigstens mittelfristig davon ausgegangen werden, dass ein aktiver Support für die entwickelte Software geleistet werden kann. Dies gilt insbesondere für alle entsprechenden Ergänzungen von OpenRBAC, da diese von DAASI entwickelte Software als strategisch wichtigen Asset angesehen wird, wofür nachhaltige Support-Dienste angeboten werden.

Gegenwärtig gibt es Bestrebungen, die TextGrid-Infrastruktur im Rahmen einer nachhaltigen Organisationsform zu verstetigen. Hierzu wurden zunächst unterschiedliche Organisationsformen evaluiert, wobei die Gründung eines Vereins mit der Option aus dem Verein eine gemeinnützige GmbH zu gründen als günstigste mittelfristige Option angesehen wurde. Langfristig sollen diese Nachhaltigkeitsbemühungen mit existierenden Bestrebungen für die Errichtung einer nachhaltigen IT-Infrastruktur für Geisteswissenschaften in Deutschland („Digital Humanities“) korreliert werden. Parallel hierzu wird der Produktiv-Betrieb der TextGrid-Software (Client-Komponente und TextGrid-Infrastruktur) vorbereitet, wobei auch organisatorische Aspekte, wie die Formulierung einer Nutzungsordnung berücksichtigt werden.

3.2.4 Portal Delegation-Portlet für SLC

Die entwickelte Software wird samt Quellcode unter einer Open Source Lizenz über die Projekt-Website veröffentlicht. Neben den Deliverables zu den einzelnen Projekt-Tasks, in denen die zugehörigen Entwicklungsarbeiten beschrieben sind, ist für die Nachnutzung ein zusammenfassendes Dokument erstellt worden[1]. Um Weiterentwicklungen und eventuelle Anpassungen an neue Software-Environments zu unterstützen, wurde für Techniker ein weiteres Dokument mit Softwaredokumentation bereitgestellt.

[1]S. Pinkernell, B. Fritzsch: Einsatz von Portal Delegation und SAML Assertions bei der Authentifizierung und Autorisierung, verfügbar unter gap-slc.awi.de/documents/portalDelegation-1.0.pdf

4 Zusammenfassung

Die im Projekt entwickelte Software steht der gesamten D-Grid Community zur Verfügung und führt für die im Antrag genannten Use cases zu einer Vereinfachung der Authentifizierungsmechanismen im Grid.