Zusammenfassender Abschlussbericht

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

Förderkennzeichen 01IG09003 A-D

B. Fritzsch, J. Falkner, P. Gietz, S. Pinkernell, M. Haase, F. Dickmann, M. Quade, F. Viezens

---

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 01IG09003 A-D gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

And I believe if we learn from the past
We'd find keys to unlock every door
Dark would turn into light
We'd be strong
We'd be right

Styx, “Haven't We Been Here Before?”
aus dem Album “Kilroy Was Here” [1983]

1 Einleitung

Zum Zeitpunkt der Beantragung des Projektes GapSLC waren durch die beiden ersten Calls der D-Grid-Initiative neben dem Integrationsprojekt DGI und den fünf akademischen Projekten auch noch ein GapProjekt (D-MON), drei Serviceprojekte sowie neun kommerzielle Projekte aktiv. Durch die Sonderinvestitionen des BMBF wurde dazu die Installation bedeutender Rechen- und Speicherkapazitäten ermöglicht. Trotzdem blieben die Nutzerzahlen in D-Grid hinter den ursprünglichen Erwartungen zurück.

Einer der Gründe dafür wurde in der für viele potentielle Nutzer schwer handhabbaren Sicherheitsinfrastruktur identifiziert. GapSLC hat aus den Erfahrungen der beteiligten Projekte gelernt und drei Anwendungsfälle definiert, für die alternative Lösungen erarbeitet werden sollten. Das Ziel bestand dabei darin, die Hürden für neue Nutzer beim Einstieg in das Grid zu senken und damit einen Beitrag zur weiteren Verbreitung der Gridtechnologie zu leisten.

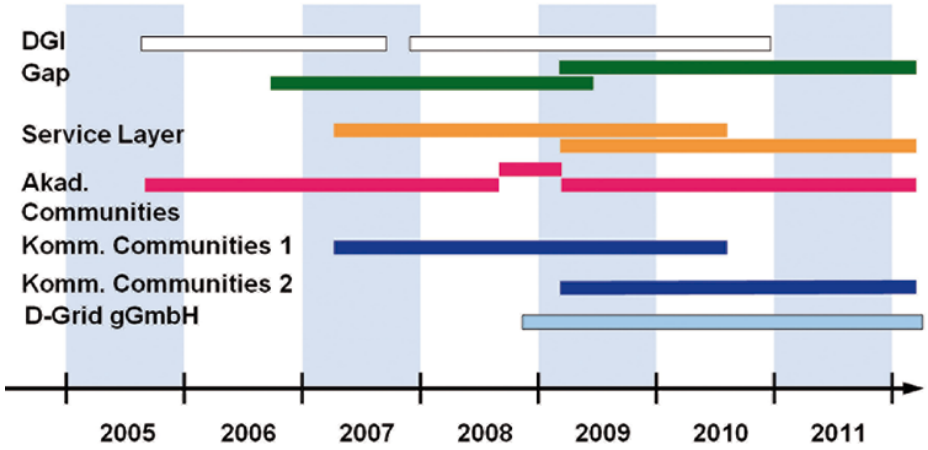

Abbildung 1: Entwicklung von D-Grid. Mit den drei Calls (2005, 2007 und 2009) wurden jeweils neue Projekte mit unterschiedlichen Ausrichtungen initiiert. (Quelle: U. Schwiegelshohn in „D-Grid. Die Deutsche Grid-Initiative. Vorstellung der Projekte zum All Hands Meeting 2009. http://www.d-grid-ggmbh.de/downloads/BroschuereAHM2009.pdf)

1.1 Aufgabenstellung und Statusbestimmung

Das Projekt „Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids (GapSLC)“ ist ein Gap-Projekt im dritten Call der vom BMBF geförderten D-Grid-Initiative. Bei der Arbeit in Projekten der vorhergehenden Calls tauchte immer wieder das Problem auf, dass die in D-Grid etablierte Sicherheitsinfrastruktur für einige Nutzer nicht komfortabel genug handhabbar

ist und sie daher vor der Nutzung von Gridtechnologie insgesamt zurückschrecken. Dies trifft vor allem auf technikfernere Nutzergruppen zu.

Daher fanden sich Vertreter aus C3Grid, TextGrid, MediGRID und Services@Medigrid zusammen, um über alternative Konzepte nachzudenken und deren Umsetzung in D-Grid zu evaluieren. Bei der Erstellung des Antrags (1) wurden die Erfahrungen aus diesen Communities eingebracht, um drei typische Anwendungsfälle zu definieren, die die unterschiedlichen Nutzungsprofile der beteiligten Nutzergruppen widerspiegeln. Ziel des Projekts war es, für diese Anwendungsfälle einfachere Zugangsmechanismen zum Grid zu finden. Die Anwendungsfälle beschreiben eine breite Spanne von Szenarien:

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

Dabei war GapSLC als ein sehr schlankes Projekt konzipiert, in dem keine grundlegend neuen Entwicklungen stattfinden sollten, sondern die bereits vorhandenen Ansätze verschiedener nationaler und internationaler Projekte miteinander verknüpft und eine funktionierende Lösung implementiert sollte. Dieser Ansatz ist auch hinsichtlich der weiteren Pflege der entwickelten Software von Bedeutung. Im Folgenden wird kurz dargelegt, an welche Vorarbeiten GapSLC für die betrachteten Anwendungsfälle jeweils anknüpfen konnte.

Use Case A. Nutzer ohne persönliches Zertifikat mit Portalzugang zum Grid

Um die Nutzer von der Beantragung von traditionellen langlebigen Zertifikaten und deren komplizierter Handhabung zu entlasten, wird das Portal Delegation Verfahren (2) eingesetzt. Dabei bezieht das Portal im Auftrag des Nutzers jeweils vor dem Starten der Gridanwendung ein „frisches“ kurzlebiges Zertifikat und sichert damit den Gridjob ab. Vorarbeiten hierzu wurden im Projekt IVOM (3), (4) (Integration und Interoperabilität der VO-Management-Technologien im D-Grid, 10/2006 bis 03/2008) geleistet. Es wurden Lösungsansätze auf der Basis von Shibboleth (5) diskutiert, jedoch konnte im Rahmen von IVOM keine Umsetzung der Vorschläge erfolgen. Diese Lücke wurde mit GapSLC dann geschlossen und eine funktionierende Implementierung erarbeitet. Bei der Implementierung wurde auf die Entwicklungen des GridShib-Projekts zurückgegriffen (6). Für die Autorisierung bei den Ressourcenprovidern wird die Security Assertion Markup Language SAML (7) eingesetzt. Sie spezifiziert einen Rahmen, in dem vertrauenswürdige Aussagen zu Identitäten dargestellt und ausgetauscht werden können.

Use Case B. 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 gezogen werden. Vorarbeiten dazu gab es mit dem „MyProxy Upload Tool“ des CCLRC (UK), das sich jedoch in der Anwendung als zu kompliziert erwies und dessen Sourcen für die Weiterentwicklung nicht verfügbar gemacht werden konnten. Aus diesem Grunde wurde im Rahmen von MediGRID ein ähnliches Tool entwickelt, welches die Konfiguration weitgehend vorwegnimmt und somit für den Nutzer deutlich einfacher zu bedienen ist. Das Tool diente als Ausgangspunkt für die Entwicklungen in GapSLC.

Das myproxy-Upload-Tool in der ersten Version erlaubte das Uploaden der Credentials aus den Keypair (privater und öffentlicher Schlüssel) im pem-Dateiformat mit drei Arbeitsschritten. Später kam in der zweiten Stufe in der gPUT-Applikation (s. Pkt.2.2) die Möglichkeit des Uploadens von Credentials aus einer einzigen, passwortgeschützten p12-

Datei mit zwei Arbeitsschritten dazu. Aktuell war es dem Anwender möglich, das im Browser integrierte Zertifikat über den jeweiligen Keystore in einem Schritt zu uploaden. Die aus Usersicht einfachste Lösung wurde mit dem SLCs-Generator über den DFN IdP vorgestellt.

Use Case C. 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. Dafür gab es zum Zeitpunkt der Antragstellung international bereits Robot-Zertifikate (siehe z.B. in (8)). Für die DFN-Grid-Policy sollte die Anforderungen aus den Communities eingebracht werden, um eine EUGridPMA akkreditierte Grid CA zu etablieren.

1.2 Planung und Ablauf des Vorhabens

Das Projekt ist in sieben Tasks unterteilt. Die Use Cases B und C werden in den Tasks 5 und 6 behandelt. Für den Use Case A erfolgte eine Aufteilung von Teilthemen: Integration des SLC-Bezugs in das Portal (Task 2), Vereinfachung der Handhabung von SLCs (Task 1) und die Autorisierung per SAML (Task 3 und 4). Um eine enge Zusammenarbeit mit anderen Projekten zu erreichen, war der Dissemination ein eigener Task gewidmet, der auch das Projektmanagement enthielt.

Die Arbeiten in den einzelnen Tasks wurden im Wesentlichen entsprechend der Planung durchgeführt. Nur in Task 2 gab es eine inhaltliche Änderung und Erweiterung: Zwar wurde zunächst mit GridSphere gearbeitet und gemeinsam mit dem AEI eine shibbolisierte Version erstellt. Jedoch ist die Weiterentwicklung von GridSphere wegen des Weggangs des Hauptentwicklers unsicher, und viele Communities in D-Grid haben inzwischen auf Liferay umgestellt. Daher wurde zunächst eine Evaluierung von Liferay bzgl der Shibbolisierung erarbeitet (9) und später ein Shibboleth-Hook (10) entwickelt, der der Liferay Community zur Verfügung gestellt wurde.

Zum Start des Projekts wurden in einem Workshop Anforderungen weiterer D-Grid-Projekte aufgenommen (11) und in einem Abschlussworkshop (12) den interessierten Communities vorgestellt und ausführlich diskutiert.

Eine konkrete Evaluation der Verwendung von SLCs, der DFN-AAI, des gPUT sowie der Robot-Zertifikate wurde in der biomedizinischen Community durchgeführt. Hierzu wurden im Herbst 2009 sowie im Frühjahr 2011 Umfragen auf Basis eines standardisierten Fragebogens durchgeführt.

- Nutzerstruktur: woher, wie viele? Die Nutzer setzten sich aus Studenten, studentischen Hilfskräften, Technikern und wissenschaftlichen Mitarbeitern zusammen. Die Teilnehmer des Nutzertests kamen dabei aus dem Geschäftsbereich IT der UMG, der Abteilung Medizinische Informatik, der Abteilung Hämatologie/ Onkologie, der Kardiologie, der genetischen Epidemiologie und Statistik und der medizinischen Statistik.

- Fragestellungen: Die Testteilnehmer haben nach einer theoretischen Einführung (Zertifikatsgrundlagen, Authentisierung) mit der gPUT-Applikation innerhalb des MediGRID-Liferay-Portals die verschieden Schritte aus dem Fragebogen (s. Anhang) abgearbeitet. Begonnen wurde mit den beiden Key-Pairs im pem-Format, über das passwortgeschützte p12-Zertifikat bis zum integrierten Zertifikat im jeweiligen Keystore des Browsers. Zusätzlich wurde der IdP des DFN für die Funktionsdarstellung von SLC genutzt. Die vollständigen Fragebögen finden sich im Anhang.

1.3 Zusammenarbeit

Bei der Zusammenstellung der Anforderungen wurden nicht nur die Projekte berücksichtigt, die dieses Gap-Projekt initiiert hatten. Vielmehr hat GapSLC von Anfang an eine offene Kommunikation und Zusammenarbeit auch mit weiteren Projekten gesucht, damit die entwickelten Lösungen möglichst vielen Nutzern zugutekommen können.

Besonders intensiv war die Zusammenarbeit mit dem DFN, der als assoziierter Partner direkt an den Projektarbeiten beteiligt war. Die Diskussionen zu SLCS und Robot-Zertifikaten fanden dann Niederschlag in den offiziellen Policies (13), (14).

Umfangreiche Kooperationen gab es auch mit den DGI Fachgebieten sowie mit weiteren D-Grid Communities. Insbesondere sei hier WissGrid erwähnt, wo umfangreiche Zuarbeiten zu einer Blaupause im Arbeitspaket 2 zum Thema Sicherheit gemacht wurden (15). Damit wird neuen Communities ein Dokument bereitgestellt, in dem sie sich über vorhandene Sicherheitsinfrastrukturen im Grid informieren können, um eine an ihre konkreten Anforderungen angepasste Lösung auszuwählen.

Daneben wurden Kontakte zu inner- und außer-europäischen Projekten und Gruppen wie z.B. den Entwicklerteams von VOMS/VOMRS, Shibboleth, Globus Toolkit und GridShib aufgebaut und intensiv genutzt.

2 Ergebnisse

Die Gliederung dieses Kapitels orientiert sich nicht an den Arbeitspaketen, sondern primär an den definierten Anwendungsfällen[1]. Damit kann verdeutlicht werden, welche konkreten Ergebnisse erreicht werden und wie sich die Situation des jeweils angesprochenen Nutzers durch die Resultate aus GapSLC verbessert hat.

2.1 UseCase A: Nutzer ohne konventionelles persönliches Zertifikat

2.1.1 Allgemeines

Für die Absicherung von Gridjobs sind zwingend Zertifikate notwendig. Bei konventionellen Zertifikaten ist bereits deren Beantragung relativ kompliziert und langwierig (persönliches Erscheinen bei der Grid-CA mit Authentifizierung per Personalausweis). Außerdem erfordert die Handhabung der Zertifikate ein nicht zu vernachlässigendes Maß an technischem Verständnis der Problematik, wovon zwei Probleme exemplarisch aufgezählt werden sollen. So darf der private Schlüssel nur dem Inhaber des Zertifikats zugänglich sein (Beachtung der korrekten Rechte auf dem Nutzerrechner). Zudem verlangen unterschiedliche Anwendungen evtl. unterschiedliche Formate der Zertifikate.

Die in GapSLC diskutierte Lösung verbindet daher zwei Ansätze: Zum einen soll der Nutzer von den Problemen im Zusammenhang mit der Beantragung, sicheren Speicherung und Handhabung des Zertifikats weitgehend entbunden werden, indem das Portal diese Aufgaben im Auftrag und Namen des Nutzers übernimmt. Zum anderen sollen kurzlebige Zertifikate genutzt werden, da für ihre Beantragung eine Authentifizierung innerhalb einer Shibboleth Föderation ausreicht, was relativ einfach in das Portal integriert werden kann. Die Zertifikate können jeweils bei Bedarf schnell bezogen und für die Absicherung des folgenden Gridjobs genutzt werden. Damit entfällt die Notwendigkeit, die Zertifikate über einen längeren Zeitraum sicher zu verwahren.

[1] Zur Zuordnung der Arbeitspakete zu den Anwendungsfällen sei auf den Projektantrag (1) verwiesen

Zur Erzeugung kurzlebiger X.509 Zertifikate wird vom DFN der Short Lived Credential Service (DFN-SLCS) betrieben. Dieser Service existiert in zwei baugleichen Ausführungen:

Der produktive DFN-SLCS stellt EuGridPMA-akkreditierte kurzlebige Zertifikate aus, die eine ähnliche Vertrauensbasis gewährleisten wie persönliche Grid Zertifikate. Allerdings erfordert der DFN-SLCS, neben der Mitgliedschaft in der DFN-AAI (16), eine explizite Teilnahmeerklärung für diesen Dienst, die weitere, teils sehr strenge Anforderungen (z.B. Audits) mit sich bringt (14).

Der DFN-Test-SLCS dagegen läuft in der DFN-Test-AAI und stellt nicht akkreditierte kurzlebige Zertifikate aus, die jedoch ein deutlich niedrigeres Sicherheitslevel als die akkreditierten Zertifikate besitzen. In diesem Projekt wurde durchgehend der DFN-Test-SLCS verwendet. Die Ergebnisse sind aufgrund der Baugleichheit der beiden Systeme aber direkt übertragbar.

Für die feingranulare Autorisierung der Nutzer bei den Ressourcenprovidern kann das Konzept erweitert werden. Das Portal sammelt dazu die verfügbaren Informationen aus verschiedenen Autorisierungsquellen und bettet sie in Form einer SAML Assertion in das Proxy Zertifikat ein, so dass sie an der Grid-Ressource zur Auswertung bereitstehen.

Mit einem abgestimmten Fragebogen wurde ein Nutzertest durchgeführt, der alle momentan im Grid-Umfeld verfügbaren Authentifizierungsmechanismen abbildet. In dem Nutzertest wurden für jede Frage eine Punktzahl von 1 bis 5 vergeben (1=sehr niedrig bis 5=sehr hoch). Nach dem Test wurden die Bewertungen pro Frage aufgenommen. Das Ergebnis des Tests ist nachfolgender Abbildung 2 zu entnehmen.

Teilnehmerzahl: 18

Nr.	Frage	Typ	Ergebnis (Mittelwert)
F1	Wie IT-affin schätzen Sie sich ein?	sehr hoch:5 - sehr niedrig:1	4,28
F2	In welchem Bereich sind Sie tätig?	Freitext	
F3	Wie hoch schätzen Sie den Aufwand für den allgemeinen Arbeitsprozess bei der Verwendung von Zertifikaten und Proxy-Zertifikaten in Grid-Umgebungen ein?	sehr hoch:5 - sehr niedrig:1	3,83
F4	Wie hoch schätzen Sie den Nutzen von gPUT zur Vereinfachung der Verwendung von Zertifikaten und Proxy-Zertifikaten in Grid-Umgebungen ein?		
F4.1	Mit Browser-Zertifikat (IE/Firefox)	sehr hoch:5 - sehr niedrig:1	3,82
F4.2	Mit PEM-Datei	sehr hoch:5 - sehr niedrig:1	3,35
F4.3	Mit P12-Datei	sehr hoch:5 - sehr niedrig:1	3,38
F5	Wie hoch schätzen Sie den Vorteil der Nutzung von Short Lived Credential Services unter Verwendung der Authentifizierung und Autorisierung über die Heimatorganisation ein?		
F5.1	Gegenüber Nutzerzertifikaten ohne Tools	sehr hoch:5 - sehr niedrig:1	4,44
F5.2	Gegenüber gPUT	sehr hoch:5 - sehr niedrig:1	3,78
F6	Wie hoch schätzen Sie den Vorteil der Nutzung von Robot-Zertifikaten ein?		
F6.1	Gegenüber Nutzerzertifikaten ohne Tools	sehr hoch:5 - sehr niedrig:1	4,35
F6.2	Gegenüber gPUT	sehr hoch:5 - sehr niedrig:1	3,47
F6.3	Gegenüber SLCS	sehr hoch:5 - sehr niedrig:1	3,29
7	Welche weiteren Verbesserungen würden Sie sich wünschen?	Freitext	

Anmerkungen (Frage 7)

Refreshzeit im Portal/in gPUT zu kurz, das irritiert die Nutzer	mündliche Rückmeldungen
Assistent wäre sinnvoll (Avatar-Projekt aus Ulm)	2 x genannt

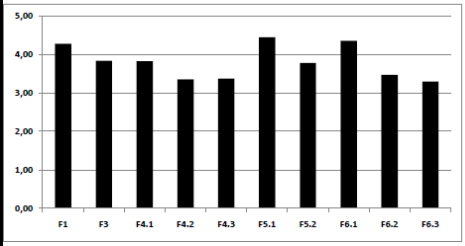

Abbildung 2: Fragenkatalog mit den Wichtungen als Übersicht und statistisches Diagramm

In der Auswertung ist der hohe Grad an Nutzerakzeptanz der Keystore-Lösung und der SLCs deutlich zu ersehen, abgesehen von den automatischen Roboter-Zertifikaten. In dem

biomedizinischen Use Case werden alle Möglichkeiten vorgestellt, was aber nicht über die Hindernisse beim Einsatz im Gesundheitswesen mit Versorgung und Forschung hinwegtäuschen kann und soll. Daher gibt es in den biomedizinischen Grid-Portalen die unterschiedlichen Möglichkeiten je nach Stufe der zu schützenden Daten.

2.1.2 Umsetzung für C3Grid

Am AWI wurde ein Test-System mit Shibboleth Komponenten und Test Grid Ressourcen aufgesetzt: Neben dem Shibboleth Identity Provider existiert ein per Shibboleth Service Provider geschütztes Test Portal, von dem aus die kurzlebigen Zertifikate per Portal Delegation bezogen werden. Zudem wurde eine Test Grid Ressource mit Globus Toolkit 4.0.8 (17) aufgesetzt, auf der die erstellten Credentials getestet werden können.

Die Portal Delegation Software wurde im Gridshib Projekt entwickelt und besteht aus zwei zueinander passenden Komponenten: Der eine Teil bildet den Short Lived Credential Service und ist am DFN installiert. Die andere Komponente, die dazu dient, die kurzlebigen Zertifikate vom Portal aus zu beziehen, besteht aus einem Perl-CGI-Skript und wurde zunächst für erste Tests und Evaluierung des SLCS verwendet. Zur besseren Integration in ein Portal wurde die Software als Portlet neu implementiert.

Diese portierte Portal Delegation Software läuft im Portal und enthält auf der graphischen Oberfläche nur einen Button. Durch ein Klick auf diesen Button wird automatisch zunächst ein neues Schlüsselpaar und anschließend aus dem öffentlichen Schlüssel ein PKCS#10 Certificate Request generiert. Anschließend wird der Nutzer automatisch per Browser Redirect an den (Test-)SLCS weitergeleitet und der Certificate Request im Hintergrund an diesen Dienst übergeben. War die vorherige Authentifizierung und Autorisierung per Shibboleth erfolgreich, wird ein kurzlebiges Zertifikat ausgestellt, das per Browser Redirect wiederum an das Portal übergeben und von der Portal Delegation Software in Empfang genommen wird. Abschließend wird vom kurzlebigen Zertifikat ein Proxy Zertifikat abgeleitet, das damit für die Arbeit im Grid am Portal zur Verfügung steht.

Zur Absicherung des Portals wird Shibboleth verwendet. Um dem Nutzer das Login am Portal zu vereinfachen, muss das entsprechende Portalframework über eine Anbindung an die Shibboleth Infrastruktur verfügen. Hier wurden im Rahmen von GapSLC zwei Lösungen erarbeitet. Das AWI hatte daher schon im Vorfeld des Projekts eine Kooperation mit dem AEI als Entwickler des Portalframeworks GridSphere zu dessen Shibbolisierung. Im Rahmen von GapSLC wurde eine shibbolisierte Version von GridSphere vom AEI bereitgestellt und am AWI ausgiebig getestet. Da während der Projektlaufzeit GridSphere jedoch aus dem offiziell unterstützten D-Grid Software Stack fiel, wurden die Arbeiten nach der Evaluierung eines alternativen Portalframeworks dann für Liferay durchgeführt. Leider bietet Liferay noch keine Unterstützung für einen Shibboleth basierten Login, aber zumindest die Möglichkeit über sogenannte Hooks eigene Funktionalität zu integrieren. Ein shibbolisierter Login am Liferay Portal konnte über die Implementierung eines Auto Login Hooks durch das AWI umgesetzt werden. Über diese Software wird ein Shibboleth Account auf einen Liferay Account gemapped, der für einen automatischen Login genutzt wird. Für den Fall, dass noch kein Liferay Account besteht, wird anhand der Shibboleth Campus Attribute automatisch ein neuer Liferay Account erstellt. Die Software und die Dokumentation ist über die Projekt-Website zum Download verlinkt (18).

An der Grid Ressource sollen, zusätzlich zur Authentifizierung mittels Zertifikat und der damit verbundenen Autorisierung des Nutzers über Gridmap-Files, auch Nutzer-Attribute für eine feingranularer Autorisierung eingesetzt werden. In einem ersten Schritt werden dazu Campus Attribute aus der Shibboleth Umgebung verwendet, die in Form einer SAML 2 Assertion von Shibboleth bereitgestellt werden. Die Nutzer-Attribute sollen dann, als SAML Assertion codiert, in das von der Portal Delegation Software erzeugte Proxy Zertifikat mit eingebettet werden.

An der Grid Ressouce wird die Middleware Globus Toolkit 4.0.8 und, um die Informationen aus der SAML Assertion auswerten zu können, zusätzlich die Software Gridshib for Globus Toolkit 0.6 (19) verwendet. Damit können allerdings nur SAML 1 Assertions verarbeitet werden, und auch nur jeweils eine Assertion pro Proxy Zertifikat.

Zunächst wurde die zu Task 1 entwickelte Software erweitert, um die SAML 2 Assertion mit den Campus Attributen zu beziehen und die enthaltenen Attribute in eine neu ausgestellte SAML 1 Assertion einfließen zu lassen. Um das Vertrauensverhältnis aufrecht zu erhalten wird diese neu erstellte Assertion zudem durch das Portal signiert. Das Design der Software berücksichtigt dabei schon, dass mehrere Attribut-Quellen einfließen können.

An der Grid Ressource wird diese SAML Assertion ausgewertet und die darin enthaltenen Attribute werden in die Entscheidungskette zur Autorisierung aufgenommen. In der Software GridShib ist dieser Anwendungsfall, bei dem das kurzlebige Zertifikat (bzw. das davon abgeleitete Proxy) und das Zertifikat, mit dem die eingebettete SAML Assertion signiert wurde, nicht auf denselben Aussteller zurückgehen, zwar konzeptionell vorgesehen, aber noch nicht implementiert. Die Originalversion von Gridshib kann die neu ausgestellte Assertion aus diesem Grunde nicht auswerten. Daher wurde eine Erweiterung der in Gridshib enthaltenen Bibliothek vorgenommen, um zunächst die üblichen Prüfungen des Zertifikats und der Zertifikatskette durchzuführen und ggf. die Nutzung der Attribute der eingebetteten SAML Assertion zu erlauben.

Nach einem Austausch der Original-Version der Bibliothek gegen die modifizierte Version ist lediglich ein Neustart des Globus-Containers notwendig. Am Ressource Provider wird eine Liste aller vertrauenswürdigen Aussteller von SAML Assertions gepflegt. Über die Grid Shib Software können zur Autorisierung notwendige Attribute konfiguriert werden. Danach werden Jobs mit falschem Attribut oder einer nicht verifizierten Signatur abgewiesen, Jobs mit gültigem Proxy Zertifikat und den erforderlichen Attributen in der SAML Assertion werden ausgeführt. Die modifizierte Bibliothek ist auf der Projekt-Website zum Download verlinkt. Eine detaillierte Anleitung findet sich im Dokument (20)

Der Virtual Organisation Membershib Service (VOMS) (21) dient dazu, virtuelle Organisationen (VO) über Institutsgrenzen hinweg zu verwalten. Benutzer melden sich einmalig am VOMS-Server mit ihrem Zertifikat für eine VO an und bekommen vom VO-Representative ihre Rollen und ggf. Attribute zugewiesen. Der VO-Representative ist ein Teilnehmer der VO, der die nötigen Rechte zur Verwaltung der VO besitzt.

Am Forschungszentrum Jülich wird der offizielle D-Grid VOMS betrieben, der allerdings nur die akkreditierten kurzlebigen Zertifikate vom DFN-SLCS akzeptiert, die in diesem Projekt verwendeten kurzlebigen Zertifikate jedoch nicht. Aus diesem Grunde wurde am AWI ein eigener VOMS Server aufgesetzt, der in der Konfiguration dem offiziellen D-Grid VOMS entspricht. Dabei ist vor allem der VOMS SAML Service, der seit der Version 2.0.18 Bestandteil der Software VOMS Admin ist, von großer Bedeutung.

Über den VOMS SAML Service können die am VOMS konfigurierten VO-Rollen und -Attribute eines VO-Teilnehmers über eine Axis2-Webschnittstelle (22) programmatisch als SAML 2 Assertion abgerufen werden. Die Client Software basiert auf einer Implementierung eines bestehenden Test-Clients aus dem SAML VOMS Paket, die zur Integration in die entwickelte Portal Delegation Software angepasst worden ist.

Der Nutzer muss sich mit seinem kurzlebigen Zertifikat einmalig am VOMS Server für eine VO registrieren und vom VO-Representative freigeschaltet werden. Von der Portal Delegation Software wird im Namen des Nutzers am Portal ein kurzlebiges Zertifikat vom DFN (Test-) SLCS bezogen und mit diesem Zertifikat dann automatisch eine SAML 2 Assertion vom VOMS SAML Service abgerufen. Die in dieser SAML Assertion enthaltenen Attribute werden dann von der in Task 3 beschriebenen Software ausgewertet und fließen in die neu ausgestellte SAML Assertion mit ein. Damit sind auch die Attribute und Rollen aus

der VO an der Grid-Ressource für eine feingranulare Autorisierung nutzbar. Zusammenfassend ist der schematische Ablauf in Abbildung 3 dargestellt.

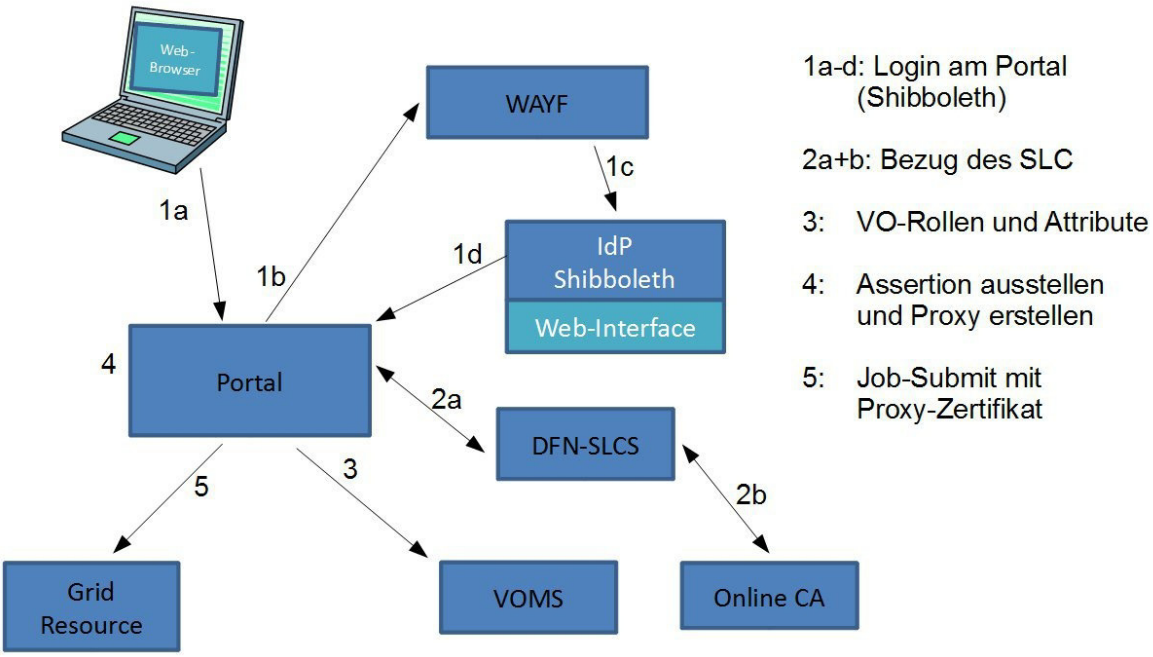

Abbildung 3: Schematische Darstellung der einzelnen Schritte beim implementierten PortalDelegation Verfahren mit kurzlebigen Zertifikaten.

Die Software und Dokumentation ist über die Projekt-Website zum Download verlinkt.

2.1.3 Umsetzung für TextGrid

Die Umsetzung des Konzepts für TextGrid wurde vom Partner DAASI vorgenommen. Auch hier wurde das Portal Delegation Szenario implementiert. Dabei agiert die TextGrid-Middleware als Portal. Es wird ein 12 Stunden gültiges SLC bezogen, welches in der Middleware und nicht auf dem Rechner des Benutzers generiert und verwaltet wird. Wie bei der C3Grid-Lösung werden privater Schlüssel und Zertifikatsrequest im Portal generiert und über die Web-Service-Schnittstelle des DFN SLCS von diesem signiert. Auch hier wurde auf der Perl-basierten Software vom GridShib-Projekt aufgebaut, diese jedoch dahingehend modifiziert, dass die Speicherung von SLC-Passphrases nur im Hauptspeicher erfolgt, damit die Bestimmungen der EuGridPMA für die Sicherheit von Schlüsselinformationen erfüllt werden können.

Außerdem wurde die Middleware erweitert, damit alle in D-Grid geforderten Benutzerattribute abgefragt und gespeichert werden. Dies ist als dynamisch konfigurierbare Attributliste ermöglicht.

Bisher unbekannte, über Shibboleth authentifizierte Benutzer werden zudem automatisch und sicher sofort im VOMRS registriert, zusammen mit den gleichzeitig erhobenen Benutzerattributen und dem zeitnah erzeugten SLC. Hier wurde auf Software vom VOMRS-Projekt aufgebaut.

Diese Erweiterungen sind als konfigurierbare und zuschaltbare Option in die aktuelle Entwicklungslinie der TextGrid-Middleware (TG-auth*) integriert. Der Dienst für Dateioperationen (TG-crud) wurde ebenfalls um den sicheren Bezug von SLCs von TG-auth* erweitert, damit deren Verwendung im Grid gewährleistet ist.

Bei den Ressourcenprovidern kann die Autorisierung alternativ zu einer reinen SAML-Anfrage an den PDP auch mittels Attributen geschehen, die in einem PDP vorliegen. Hier können für ein lokales Enforcement die Attribute direkt vom PDP geholt werden. Als naheliegende Option zum Schutz durch das Dateisystem wurden POSIX-ACLs auf dem Grid-Rechner verwendet. Eine Synchronisierung der Autorisierungsattribute vom PDP in ACLs geschieht durch ein Mapping. Die Attribute von „Projekten“ und „Objekten“ in TextGrid / TG-auth* werden zu Verzeichnis- und Dateiattributen. Zur Synchronisierung dieser Attribute wurde ein Skript implementiert, das diese in regelmäßigen kurzen Intervallen durchführt.

2.1.4 Anforderungen an SAML-Attribute aus MediGRID

Um SAML für die Autorisierung auf Gridressourcen einsetzen zu können, müssen für die jeweilige Community die notwendigen Attribute definiert werden. Für MediGRID wurde daher eine Untersuchung durchgeführt, bei der der Fokus auf der Erhebung von Anforderungen aus dem Bereich der klinischen Studien lag. In diesem Anwendungsfeld wird schon derzeit maßgeblich mit IT-Systemen gearbeitet. Es gibt mehrjährige Erfahrung am Standort Göttingen im Betrieb und Einrichtung von derartigen Systemen.

Wichtig erscheint eine Unterscheidung von mindestens sechs Rollen (vergleiche Abbildung 4) mit unterschiedlichen Zugriffsrechten auf ein derartiges System. Diese Unterscheidung lässt sich zweckmäßigerweise mit SAML-Attributen in Form einer Rollenbeschreibung abbilden.

AdminTool: All roles (7 roles)

◀ Page 1 of 1 ▶

ID	Name	Internal name	Type	Messages	Review	Freeze	Patient	Search	Export	Project setup
4	Clinical Investigator	Clinical Investigator WP1	Participant	Read, Send	no	no	yes	yes	no	no
41	Clinical Investigator	Clinical Investigator WP2	Participant	Read, Send	no	no	yes	yes	no	no
6	Data Manager	Data Manager	Participant	Read, Send	Review B	yes	no	yes	yes	no
8	Formular Builder	Formular Builder	Participant	no	no	no	yes	yes	yes	no
5	Monitor	Monitor	Participant	Read, Send	Review A	no	no	yes	no	no
3	Observer	Observer	Participant	no	no	no	no	no	no	no
7	Principal Investigator	Principal Investigator	Participant	Read, Send	Review B, Revoke A	no	no	yes	no	no

New participant role

top

Abbildung 4: Rollen innerhalb einer klinischen Studie.

a) Clinical Investigator: Ein Prüfarzt ist für die GCP-konforme Durchführung der klinischen Studie verantwortlich. D.h. er muss aus medizinischer und ethischer Sicht die Sicherheit der Studienteilnehmer gewährleisten.

b) Data Manager: Ist zuständig für die Koordinierung der Datenerfassung gemäß Studienprotokoll und für die Kommunikation mit Biometrikern. Diese Rolle exportiert die erfassten Daten und leitet sie zur statistischen Auswertung weiter. Als identifizierendes Merkmal stehen nur die Pseudonyme in der Studiendatenbank zur Verfügung.

c) Formular Builder: Implementiert die Fragebögen (eCRF) mit der dahinterliegenden Logik wie z.B. Plausibilitätschecks, Prüfung auf Inkonsistenzen und auf Vollständigkeit gemäß Studienprotokoll.

d) Monitor: Prüft kontinuierlich die studienprotokoll- und gesetzeskonforme Durchführung der Studie. Dazu gehört die Quelldatenkontrolle, die Prüfung der Dokumentation und der Dokumentationsbögen auf Vollständigkeit und Aktualität sowie die Überprüfung der Einverständniserklärungen. Der Monitor ist somit für die Qualitätskontrolle im Prüfzentrum verantwortlich.

e) Principal Investigator: Der leitende Prüfarzt und Projektverantwortliche in einer klinischen Studie.

Bezüglich der ausgeübten Rollen kann zwischen fachlichen Rollen und technischen Rollen unterschieden werden. Die Gematik sowie auch HL7 (health level 7) beschreiben unterschiedliche Berufsgruppen, welche im Behandlungszusammenhang differenzierte Rechte und Pflichten an Patientendaten inne haben. In Tabelle 2 sind die im FuE-Projekt „ePA gemäß § 291a“ berücksichtigten Rollen aufgeführt. Diese Einteilung ist an die Empfehlungen und Vorschläge der Gematik angelehnt.

Tabelle 2: Fachliche Rollen

Personenkreis gemäß §291a SGB V	**Potentieller Personenkreis für eine Rolle (strukturelle Rolle)**	**Rolle (funktionale Rolle)**	
Versicherte	Versicherte	Versicherter	
Ärzte	Ärzte	Mitarbeiter des Studienarztes	Studienarzt / mitbehandelnder Arzt
Zahnärzte	Zahnärzte		
Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten	Apotheker	autorisierter Apotheker	
Berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätige Personen unter Aufsicht eines Arztes	Mitarbeiter in einer Praxis	Mitarbeiter des behandelnden Arztes	Mitarbeiter des Studienarztes
Berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätige Personen unter Aufsicht eines Zahnarztes	Mitarbeiter einer zahnärztlichen Praxis		
Berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätige Personen in einem Krankenhaus	Mitarbeiter eines Krankenhauses		
Berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätige Personen unter Aufsicht eines Apothekers	Mitarbeiter einer Apotheke	Mitarbeiter des autorisierten Apothekers	
Psychologische Psychotherapeuten	Niedergelassene Psychotherapeuten	Behandelnder Psychotherapeut	

Die technischen Rollen unterscheiden Personen, welche mit den Daten aus administrativer Sicht in Berührung kommen. Dies sind insbesondere Datenbankadministratoren, Backup-Beauftragte und Personen, die an der Überprüfung des Audit-Trails beteiligt sind.

Die benötigten SAML-Attribute für eine Grid-Infrastruktur müssen daher insbesondere die fachlichen Rollen beschreiben können. Dies muss feingranular und lückenlos geschehen können. SAML-Attribute bieten hierfür ausreichendes Potential.

2.2 UseCase B: Nutzer mit persönlichen Zertifikaten

Ein wesentliches Problem bei der Verwendung PKI-basierter Authentifizierung war bei Beginn des Projekts die Bedienbarkeit der Authentifizierungslösungen. Um Grid-Anwendungen über ein Portal nutzen zu können, ohne auf dem Endgerät des Nutzers vorher aufwändige Installationen von Grid-Middleware-Komponenten durchzuführen, ist es erforderlich, auf dem Endgerät eine leichtgewichtige Anwendung bereitzustellen, mit der die Erzeugung von Proxies der persönlichen D-Grid-Nutzerzertifikate und der Upload auf einen sicheren MyProxy-Server im Grid ermöglicht wird.

Die Ausgangssituation des Projekts war, dass viele potenzielle Nutzerkreise nur geringe Erfahrungen bei der Verwendung von persönlichen Zertifikaten aufwiesen und insofern eine hohe Einstiegsschwelle ins Grid vorhanden war. Gleichzeitig war die Nutzung von persönlichen Zertifikaten im Grid aufwändig und komplex während eine Reduzierung der

Sicherheitsanforderungen, z.B. im Medizinbereich, aufgrund hoher Anforderungen an Datenschutz und Sicherheit nicht möglich war – und auch heute noch ist.

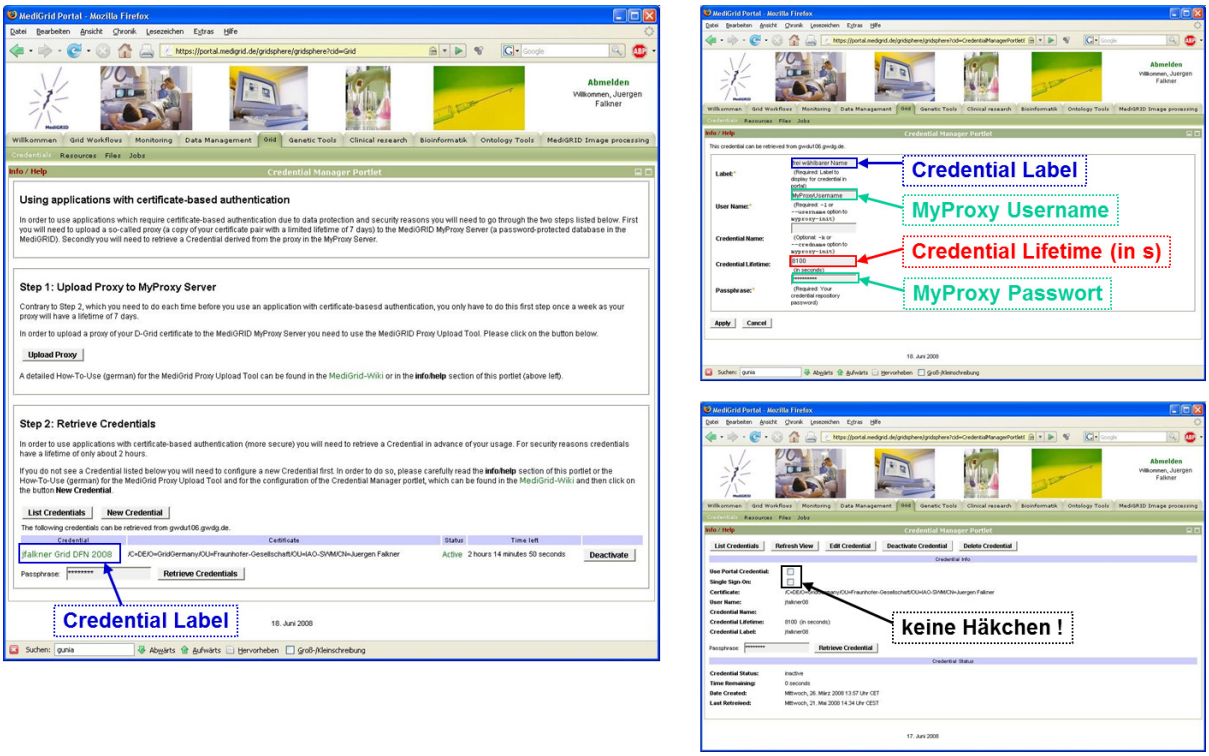

Abbildung 5: Erforderliche Konfigurationseinstellung im GridSphere Portal vor Beginn des Projekts – die Konfiguration ersteckte sich über drei verschiedene Seiten im Portal

Das Fraunhofer IAO hat aus diesem Grunde das zu diesem Zeitpunkt bereits für das MediGRID entwickelte Proxy Upload Tool weiterentwickelt, um die für die Nutzung erforderliche Nutzerinteraktion auf das absolute Minimum zu reduzieren und somit die Bedienbarkeit des Tools und die Akzeptanz bei den Endnutzern zu maximieren. Tests mit Endnutzern aus dem Bereich der Medizin und Bioinformatik hatten zuvor gezeigt, dass das Tool in seiner damaligen Form zwar in der Lage ist, eine technisch gangbare Lösung zu bieten, dass allerdings die Bedienung für die Zielgruppe noch eine hohe Hürde darstellte, was an den umfangreichen Konfigurationsmöglichkeiten im Tool und dem damals verwendeten Grid-Portal auf Basis des Portalframeworks GridSphere lag.

Eine weitere Problemstellung war, dass die für die Kommunikation zwischen Endnutzer und dem MyProxy-Server im Grid verwendeten Ports eine Nutzung in restriktiven Firewall-Umgebungen, wie sie z.B. in Kliniken üblich sind, nicht erlaubte. Aus diesem Grunde wurde über die Verbesserung der Bedienbarkeit hinaus ein komplett neuer Ansatz zur Realisierung des Proxy Uploads gewählt. Es wurde eine Applet-/Servlet-Variante umgesetzt. Sie erlaubt auch in äußerst restriktiven Firewall-Umgebungen ohne nutzerseitigen Installations- oder Konfigurationsaufwand, dass Proxys auf einen MyProxy Server geladen und über ein Portal die für einen Grid-Job notwendigen Credentials bezogen werden können.

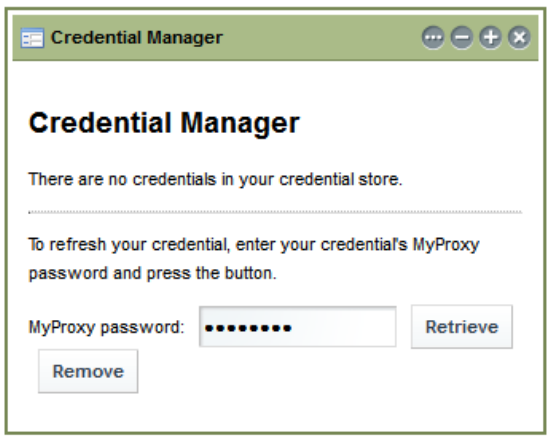

Abbildung 6: Die Eingabeerfordernisse des in Gap-SLC entwickelten Credential Manager Portlets im Vergleich zu den Erfordernissen in Abbildung 5 - hier reicht die Eingabe des MyProxy Kennworts zur Aktivierung eines Credentials und die anschließende Nutzung von Grid-Anwendungen

Zusammenfassend sollen im Folgenden nochmal alle zu lösenden Probleme und deren jeweilige Lösungen kurz dargestellt werden.

Firewall-Problematik:

- Das für die ursprüngliche Realisierung des Proxy Upload Tools verwendete Java Webstart sowie auch Applets laufen auf dem Nutzerrechner
- Die für den Proxy Upload Tool (Webstart/Applet) aufgebaute Verbindung verlief somit direkt vom Nutzerrechner zum MyProxy Server im Grid, der wiederum nur über Port 7512 kommuniziert.
- Restriktive Firewalls (z.B. klinische) erlauben jedoch ausschließlich Kommunikation mit Port 80 (HTTP) und 443 (HTTPS)

Lösung

- Implementierung als Applet / Servlet Konstrukt
- Das Applet läuft auch weiterhin lokal beim Nutzer
  - Proxyerzeugung weiterhin lokal (dies stellt eine sicherheitstechnische Voraussetzung dar)
  - Der Private Key des persönlichen Schlüsselpaars verlässt den Rechner nicht
- Der Upload des Proxies erfolgt zunächst an ein Servlet im Grid-Portal über Port 443 (HTTPS)
- Dort erfolgt serverseitig am Grid-Portal ein Redirect an den MyProxy Server
- Der Nutzer kommuniziert somit ausschließlich über HTTPS während alle Sicherheits-Anforderungen an die Proxy-Erzeugung erfüllt bleiben

Bedienbarkeit:

- Diverse Eingaben erfolgten bisher doppelt, sowohl im Proxy Upload Tool als auch im Portal bei der Verwaltung von Credentials, die für die Verwendung von Grid-Anwendungen erforderlich sind.
- Wenn diese Eingaben differieren erfolgen Fehler, die den Nutzer verwirren

Lösung:

  - engere Integration von gPUT mit Credential Portlets und Login Portlets

Format-Wirrwarr:

- Der Nutzer erhält sein Zertifikat in der Regel im Format PKCS12 (Dateiendung „.p12“)
- Um aber im Grid Credentials zu erzeugen, die dann an weitere Grid-Rechner weitergegeben und dort interpretiert werden können sind Proxys im PEM Format (Dateiendung „.pem“) erforderlich
- Ein (automatischer) Konvertierungsmechanismus ist erforderlich. Die Konvertierung muss auf dem Endgerät des Nutzers erfolgen.
- Problem: der Nutzer muss die Java Cryptography Extension installiert haben – diese ist aufgrund rechtlicher Beschränkungen in US-Ausfuhrbestimmungen NICHT Bestandteil der Standard Java Runtime Environments und insofern im Normalfall nicht auf den Nutzerrechnern installiert

Lösung:

  - One-Click-Installation der JCE durch gPUT

Festschreibung von Proxy und Credential Lebenszeiten:

- Die Credential Lifetime, also die Lebenszeit des zwischen den Grid-Ressourcen im Rahmen eines Grid-Jobs zur Trust Delegation weitergereichten Proxies muss größer sein als die voraussichtliche (und vor allem als die tatsächliche) Job-Lifetime
- In GridSphere-Portalen musste die Credential Lifetime fest im Credential Manager konfiguriert werden. Die Konfiguration überforderte meist die Endanwender
- Die Proxy Lifetime muss größer sein als die gewünschte Credential Lifetime, d.h. bei einer Änderung der Credential Lifetime kann es sein, dass auch die Einstellungen für das Proxy verändert werden müssen
- Die Proxy Lifetime war in der Regel nur über Kommandozeilen-Clients frei wählbar. Hierzu war die Installation von Grid-Middleware-Komponenten auf dem Endgerät des Nutzers erforderlich.

Lösung:

  - Sowohl die Proxy Lifetime als auch die Credential Lifetime können bei jedem Proxy Upload im Grid Proxy Upload Tool auf einfache Weise gesetzt werden. Nimmt der Nutzer keine Änderungen vor so werden automatisch die Standardlebenszeiten von 7 Tagen für Proxies und von 12 Stunden für davon abgeleitete Credentials verwendet.

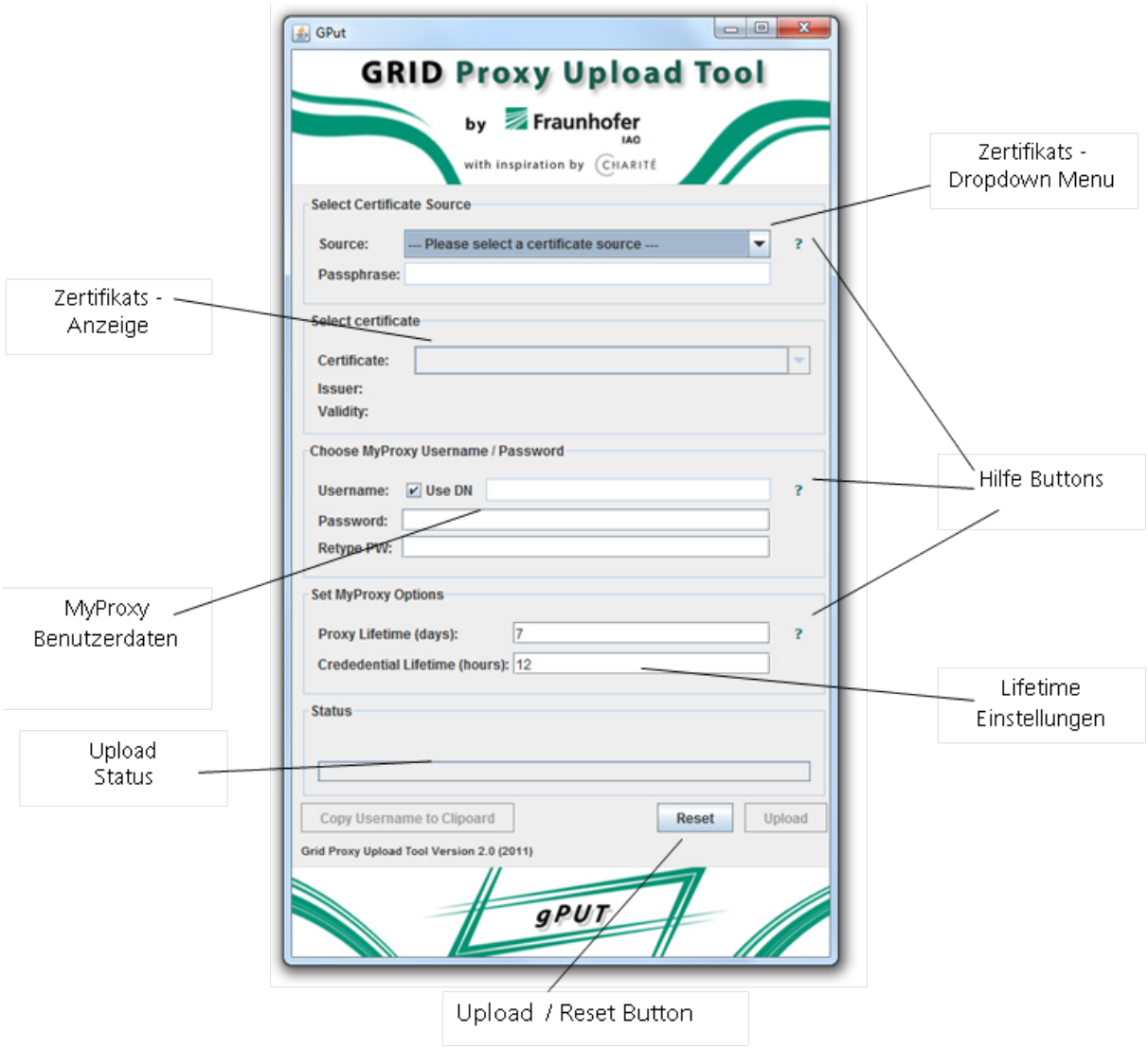

Abbildung 7: Grid Proxy Upload Tool (gPUT)

Abbildung 7 zeigt die finale Version des Grid Proxy Upload Tools. Der Nutzer kann zunächst im Zertifikats-Dropdown Menü seinen gewünschten Zertifikatspeicher wählen. Dabei hat er die Möglichkeit sowohl Dateipfade zu Zertifikatsdateien im PKCS12- und im PEM-Format anzugeben als auch die Zertifikatspeicher der Browser Mozilla Firefox und Microsoft Internet Explorer zu verwenden. Die ggf. erforderliche Konvertierung ins PEM-Format läuft im Hintergrund und für den Nutzer unsichtbar ab.

Wenn das Zertifikat aus dem entsprechenden Speicher ausgewählt wurde werden die Zertifikatinformationen im Bereich der Zertifikatanzeige zur Überprüfung dargestellt. Der Nutzer muss nur noch ein Passwort für den MyProxy Server im Grid setzen und die Eingabe wiederholen um Fehleingaben auszuschließen.

Erst wenn alle erforderlichen Angaben eingegeben wurden wird der Upload Button rechts unten aktiviert und anklickbar. Beim folgenden Upload erfolgt eine Fortschrittsanzeige und eine Erfolgsmeldung.

Das noch in 2009 bereits in erster Instanz fertig gestellte Grid Proxy Upload Tool (gPUT) wurde in der Folge weiteren Funktionstests seitens der Universitätsmedizin Göttingen und

der DAASI GmbH unterzogen. Die Feedbacks wurden zu Überarbeitungen und Verbesserungen der Software genutzt.

Die finale Version 4 des Tools wurde in Verbindung mit einigen im Projekt entwickelten Liferay-Portalerweiterungen auf der Gap-SLC Projektwebseite veröffentlicht und zum freien Download bereitgestellt. Die Liferay-Erweiterungen ermöglichen beispielsweise den zertifikatbasierten Login in Liferay-Portalen und die Verwaltung von Credentials (siehe auch Abbildung 6) zur weiteren Nutzung in Verbindung mit portalbasierten Grid-Anwendungen.

2.3 UseCaseC: Nutzer, die bestimmte Anwendungen im Grid ad-hoc und quasi anonym nutzen möchten

Die Ausgangssituation zu Projektbeginn stellte sich so dar, dass in einigen Nutzungsszenarien aus bestehenden D-Grid Communities der Zugriff auf Grid-Dienste auch ohne Zertifikat gewünscht wurde, zu diesem Zeitpunkt aber nicht möglich war. Da im Grid selbst zwischen den Ressourcen die Verwendung von Zertifikaten zwingend erforderlich war und auch heute noch ist, muss für derartige Szenarien ein Anbieter von Anwendungen im Grid – inzwischen würde man diesen als Software-as-a-Service-Provider bezeichnen – sein Grid-Zertifikat für seine Nutzer zur Verfügung stellen. In diesem Szenario erhält also nicht mehr jeder Nutzer ein persönliches Zertifikat, sondern der Betreiber des Grid-Services erhält ein Service-Zertifikat, das er für alle Grid-Jobs sämtlicher Nutzer zur Verfügung stellt (sogenannte Robot-Zertifikate).

Da zu Projektbeginn Service-Zertifikate im D-Grid nicht vorgesehen waren, gab es keine Möglichkeit, ein solches Szenario umzusetzen, ohne die Sicherheitspolicies zu verletzen, die im Zusammenhang mit der Verwendung von Zertifikaten im D-Grid gegeben waren. Jedoch gab es klare Anforderungen dafür von der Nutzerseite. Der Bedarf entstand in Szenarien, die ausschließlich unkritische Daten verwenden, wie z.B. die Folgenden:

- Analyse von Verwandtschaftsbeziehungen zwischen Tier-Genomen (MediGRID)
- Zugriff auf freie biomedizinische Ontologien (MediGRID)
- Zugriff auf veröffentlichte Dokumente (TextGrid)
- Zugriff auf frei zugängliche Klimadaten (C3Grid)

Es sollte ein Zugriff auf Grid Anwendungen über Portale (z.B. in MediGRID oder C3Grid) oder Rich Client Plattformen (z.B. in TextGrid) ermöglicht werden, die vom Nutzer weder eine Authentifizierung über Shibboleth, Short-Lived-Credentials noch über persönliche Zertifikate erforderte.

Insofern war eine Absenkung des Sicherheitsniveaus zu Gunsten der Bedienbarkeit gewünscht. Die Herausforderung des Projekts war nun, ein Konzept zu erstellen und prototypisch umzusetzen, das die Nutzung von Service-Zertifikaten ermöglichte, ohne dabei das Sicherheitsniveau anderer Anwendungen und Ressourcen zu gefährden oder abzusenken.

Zunächst wurde hierzu ein erster Entwurf für eine Konzeption zur Nutzung von Robot-Zertifikaten in D-Grid am Fraunhofer IAO erarbeitet und im Projekt mit den Partnern diskutiert. Dieser umfasste eine Schilderung der Ausgangssituation und Motivation für die Verwendung von Robot-Zertifikaten bzw. Service-Zertifikaten sowie eine Zusammenstellung von Randbedingungen und Anforderungen an den Dienst. Der Konzeptionsentwurf befasste sich neben der eigentlichen Verwendung von Robot-Zertifikaten darüber hinaus mit dem Zusammenspiel mit Identity- und Usermanagementsystemen sowie mit den Notwendigkeiten

einer Unterscheidung verschiedener Sicherheitslevel auf Ressourcenseite. Der Konzeptionsentwurf wurde zeitnah mit den Betreibern von Ressourcen und Diensten in D-Grid diskutiert und iteriert.

Eine erste Version einer Konzeption zur Nutzung von Robot-Zertifikaten in D-Grid wurde als Delieverable D1 in Task 5 fristgerecht erstellt. Diese Konzeption diente ebenfalls als Grundlage für die Diskussion mit dem Europäischen Dachverband der Grid-Zertifizierungsstellen (EUGridPMA) um die Zulassung von Robot-Zertifikaten und eine Ausgestaltung der damit verbundenen Umsetzungsrichtlinien.

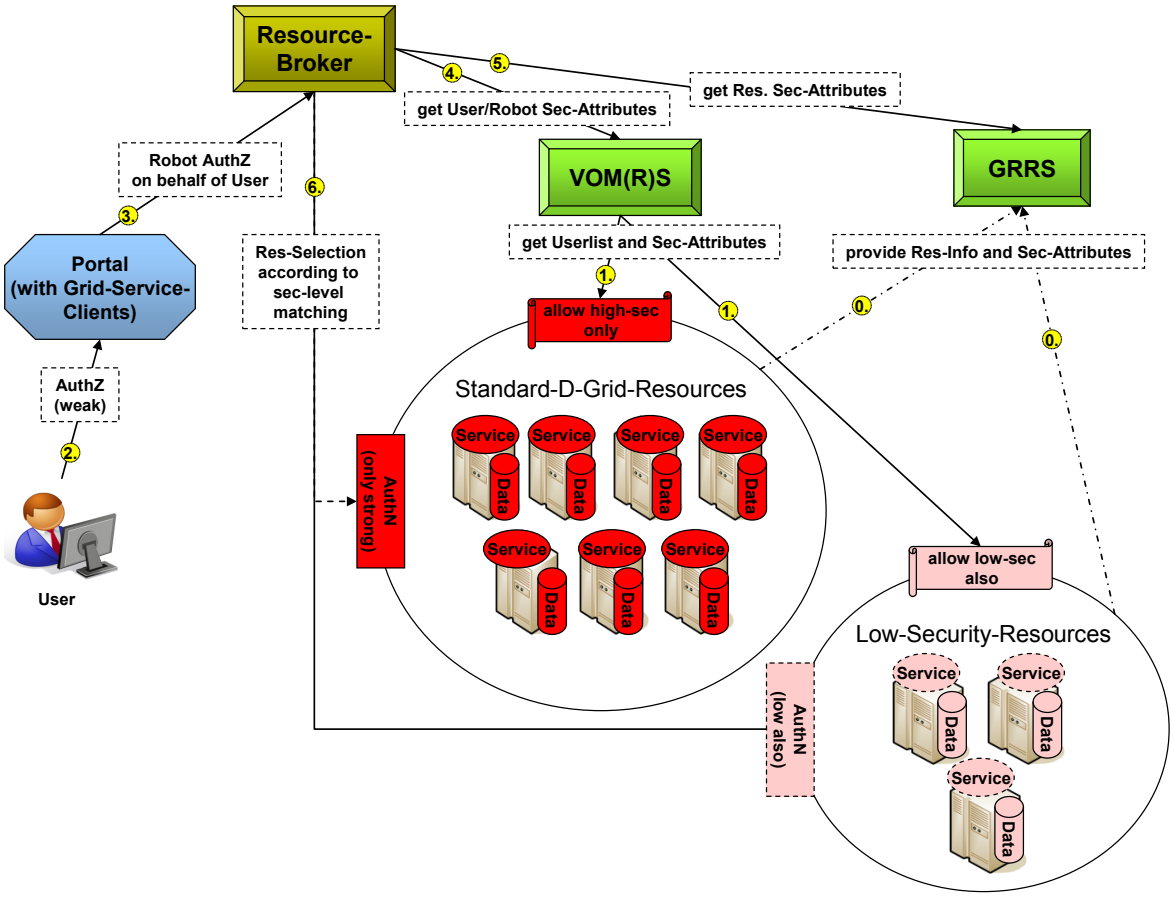

Abbildung 8: Architektur zur Verwendung von Robot-Zertifikaten

Abbildung 8 zeigt ein Ergebnis dieser Konzeption, in dem der gesamte Prozessablauf der möglichen Nutzung von Robot-Zertifikaten sowie das Zusammenspiel der verschiedenen D-Grid Dienste und Ressourcen dargestellt sind.

Nach der ersten Konzeption zur Nutzung von Robot-Zertifikaten in D-Grid erfolgte eine Diskussion und Abstimmung von Vorschlägen zur Umsetzung von Robot-Zertifikaten zusammen mit der DFN-PKI. Das Ergebnis dieser Diskussionen wurde auf Europäischer Ebene bei einem Treffen der EUGridPMA im April 2010 eingebracht und beeinflusste die Verabschiedung der „Guidelines on Approved Robots“ sowie der „Guidelines on Private Key Protection“.

Im Anschluss an diese Vorlage auf Europäischer Ebene wurde die Grid-Policy der DFN-PKI entsprechend angepasst und um Regeln für die Nutzung von Robot-Zertifikaten in D-Grid erweitert. Es erfolgte eine enge Abstimmung zwischen dem DFN und dem Projekt Gap-SLC. Die neue Policy wurde im Juni 2010 in Kraft gesetzt.

Ausgehend von dieser nun rechtlich abgesicherten Möglichkeit zur Verwendung von Robot-Zertifikaten in D-Grid wurde im Projekt Gap-SLC mit der Entwicklung eines Verfahrens zur praktischen Umsetzung der Richtlinien des DFN begonnen. Dieses schließt insbesondere den Fall der portalbasierten Bereitstellung von mehreren Robot-Services mit ein. Die Herausforderungen lagen hier in der sicheren Aufbewahrung von Robot-Zertifikaten und in der Beschränkung des Zugriffs auf die zugehörigen Schlüsselpaare entsprechend der DFN-Policy. Abbildung 9 zeigt den im Projekt erarbeiteten Vorschlag für die sichere Verwaltung von Robot-Credentials.

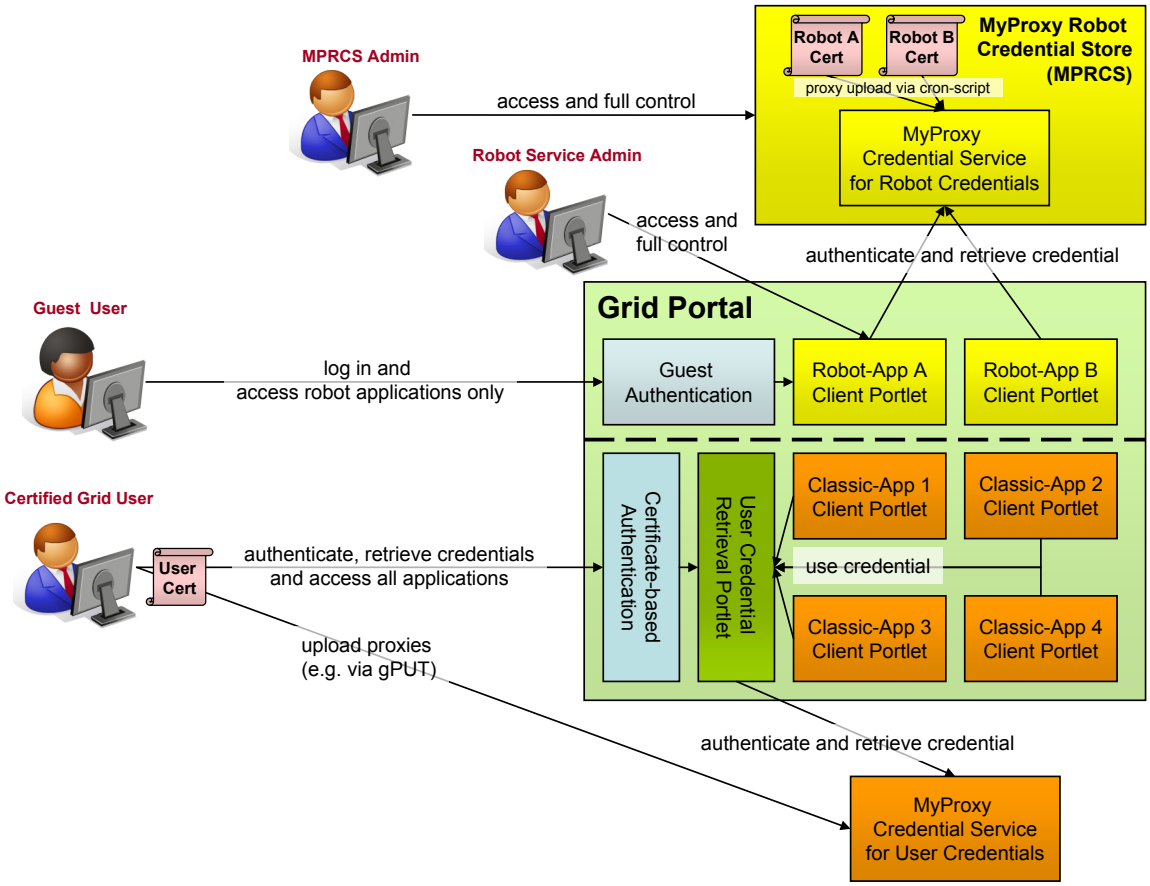

Abbildung 9: MyProxy Robot Credential Store für die Portal-basierte Nutzung von Robot-Services

Nachdem mittels Anpassung der entsprechenden Policies die rechtlichen Grundlagen für die Verwendung von Robot-Zertifikaten sowohl auf Europäischer Ebene durch die EUGridPMA als auch auf nationaler Ebene durch die DFN-PKI gesetzt wurden, konnte anschließend mit der prototypischen Realisierung geeigneter Verfahrensweisen und praktischer Implementierungen begonnen werden. Hierzu wurde in Zusammenarbeit mit der DFN-PKI ein Verfahren entwickelt, wie Robotzertifikate beantragt, erlangt, aufbewahrt und genutzt werden können. In Deliverable D5.2 mit dem Titel „Prototypische Umsetzung des Konzepts für die Nutzung von Robot-Zertifikaten“ wurden sämtliche Verfahrensschritte im Detail beschrieben. Hierbei wurde zudem zwischen zwei Fällen unterschieden, die in der Praxis vor allem Unterschiede hinsichtlich der Aufbewahrung und Nutzung von Robot-Zertifikaten aufweisen:

Zum einen ist dies der Fall der Nutzung von einzelnen Robot-Services und zum anderen ist dies der Fall der Nutzung mehrerer Robot-Services über ein gemeinsames Portal. In

letzterem Fall müssen die Schlüsselpaare verschiedener Service-Betreiber in einem gemeinsamen Robot Credential Store aufbewahrt und verwaltet werden um eine Nutzung über das Portal zu ermöglichen. Dies fügt dem Prozess eine weitere Komplexität hinzu, die gemeinsam mit der DFN PKI bewältigt und für den Nutzer transparent gestaltet werden konnte.

Abschließend befasst sich das Deliverable auch mit den äußeren Rahmenbedingungen, die für eine Akzeptanz von Robot-Services auf D-Grid Ressourcen erforderlich sind und unterbreitet Vorschläge wie diese Akzeptanz durch eine Erweiterung des D-Grid Ressourcenverwaltungsmodells zu erreichen ist.

Parallel wurden sowohl in TextGrid als auch in MediGRID prototypische Realisierungen von Robot-Services und den zugehörigen Robot Credential Stores umgesetzt, so dass auch Praxiserfahrungen mit den vorgeschlagenen Verfahren vorliegen. Das D-Grid-weit erste ROBOT-Zertifikat wurde für den TextGrid-Dienst TG-crud erstellt, das entsprechend öffentliche Daten aus dem TextGrid-Repository als Dienst an anonyme Nutzer ausgibt, wobei der externe Policy Decision Point (PDP) gefragt wird (TG-auth*).

Die erarbeiteten Konzepte und Erfahrungsberichte stehen über die Gap-SLC Projektwebseite zur weiteren Diskussion und Verwendung in D-Grid bereit.

3 Disseminierung und Verwertbarkeit der Ergebnisse

Die Mitarbeiter von GapSLC haben während der Projektlaufzeit einerseits nachnutzbare Software implementiert, andererseits Konzepte entwickelt, deren Umsetzung über das Projekt hinausweisen. Beide Kategorien stehen D-Grid-weit zur Verfügung und können nachgenutzt werden.

Konzeptionelle Arbeiten wurden zu folgenden Themen abgeliefert:

- Konzepte zur Integration von SLCs in verschiedenen Nutzungsszenarien
- Konzeption von verschiedenen Security-Levels für ROBOT-Zertifikate

Evaluierungen zu verschiedenen Technologien wurden durchgeführt:

- Shibboleth-Integration in Liferay
- VOMRS und VOMS
- XACML-SAML-Callout von Globus Toolkit an einen externen Policy Decision Point

Zu den direkt nachnutzbaren Ergebnissen gehören:

- Software zur Nutzung von SLCs mittels PortalDelegation für Liferay mit und ohne Integration von Autorisierungsinformationen mittels SAML
- Shibboleth Hook für Liferay
- OpenRBAC mit Passphrase Daemon, SLC-Bezug und –Speicherung
- pdp2acl – Synchronisation von externen Policies in POSIX ACLs im Dateisystem
- vomrs2gridmap – Bezug eines GT4 GridMap-Files
- gPUT zum Upload von persönlichen Zertifikaten

Die Software sind sämtlich unter OpenSource Lizenz verfügbar. Aufgrund seiner Ausrichtung als Gap-Projekt, zur Schließung technologischer Lücken in D-Grid erfolgt die primäre Verwertung der Projektergebnisse durch die Bereitstellung der Ergebnisse für die D-Grid Communities sowie das D-Grid Integrationsprojekt. Jedoch stehen die Ergebnisse darüber hinaus auch weiteren Anwendern zur Verfügung.

Im Projekt wurde bereits bei der Beantragung darauf geachtet, einen möglichst breiten Nutzerkreis anzusprechen. Daher wurden zwei Workshops geplant und durchgeführt, um einerseits die Anforderungen auch aus anderen Communities zu erfassen und andererseits die Ergebnisse darzustellen und zur Nachnutzung anzubieten. Der erste Workshop zu Sicherheitsanforderungen in D-Grid fand am 21.09.2009 in Göttingen statt und lieferte wertvolle Hinweise auf weitere Anforderungen aus den Projekten DGI-II, GDI-Grid, BauVOGrid, PneumoGrid, medInfoGRID, AeroGrid, WissGrid und GIDS. Interessierte konnten einen Newsletter abonnieren, der über den Fortschritt der Entwicklungen informiert. Auf dem Abschlussworkshop am 09.06.2011 in Tübingen konnten die entwickelten Lösungen vorgeführt und mit den Nutzern diskutiert werden. Die Rückmeldungen zeigten, dass die von GapSLC geleisteten Arbeiten als wertvoller Beitrag wahrgenommen werden.

GapSLC nutzte auch zwischendurch die Möglichkeit, seine Ergebnisse einem breiteren Publikum vorzustellen, indem es 2010 auf dem All Hands Meeting eine OpenIssue Session initiierte und in Kooperation mit DGI-II, WissGrid und Services@MediGRID durchführte. Begleitend dazu wurden Poster und Demos zu den entwickelten Lösungen vorgestellt. Ein weiterer Meilenstein bei der Verbreitung der Ergebnisse war der fünfte D-Grid Security Workshop am 29./30.09.2010 in Göttingen (23), wo GapSLC die Planung und Ausrichtung übernahm. Der Workshop bot Gelegenheit, die vorläufigen Ergebnisse aus GapSLC darzustellen und die weiteren Schritte mit anderen Projekten und Playern in D-Grid (Ressourceprovider) abzustimmen. Vor allem die Paneldiskussion zeigte die Relevanz des Themas Robot-Zertifikate für die weitere Entwicklung.

Durch die Zusammenarbeit des Fraunhofer IAO mit dem Institut für Arbeitswissenschaft und Technologiemanagement (IAT) der Universität Stuttgart wurde und werden die Arbeiten aus dem Projekt Gap-SLC während des Projekts und auch in Zukunft in die Lehre integriert.

4 Veranstaltungen und Publikationen/Vorträge

Projektinterne Meetings

- 03.06.2009 Gap-SLC Kickoff, Bremen
- 08.02.2010 Gap-SLC Konsortialtreffen, Bremen
- Monatliche Videokonferenzen

Teilnahme an D-Grid Workshops

23.-25.03.2009	D-Grid All-Hands-Meeting
06.05.2009	D-Grid Workshop zu Betriebskonzepten, Jülich
07.-08.05.2009	D-Grid Monitoring Workshop, Jülich
25.06.2009	D-Grid Geschäftsmodelle, Dortmund
03.09.2009	SLA4D-Grid Workshop, Bonn
21.09.2009	D-Grid Workshop Sicherheits-Anforderungen, Göttingen (Organisation und Durchführung)

15.-16.10.2009	D-Grid Security Workshop, Göttingen
21.01.2010	D-Grid Workshop zu Betriebsmodellen, Dortmund
22.-24.03.2010	D-Grid All-Hands-Meeting, Dresden
07.04.2010	D-Grid Workshop VO Management als VC
29./30.09.2010	5. D-Grid Security Workshop, Göttingen (Organisation und Durchführung)

Tabelle 3: D-Grid Workshops

Publikationen

- Deliverables siehe http://gap-slc.awi.de/dokumente.html

Vorträge

2009

- J. Falkner: Anforderungen ans Monitoring, D-Grid Monitoring Workshop, Jülich, 07.05.2009
- J. Falkner: Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids - GapSLC. D-Grid Workshop zu Sicherheits-Anforderungen, Göttingen, 21.09.2009
- B. Fritzsch: Alternative AAI-Lösungen: Das Projekt GapSLC. D-Grid Workshop Sicherheits-Anforderungen, Göttingen, 21.09.2009
- S. Pinkernell: Erfahrungen mit dem DFN-SLCS. D-Grid Workshop Sicherheits-Anforderungen, Göttingen, 21.09.2009
- B. Fritzsch: Alternative AAI – Lösungsansätze in GapSLC. 4. D-Grid Security Workshop, 15.10.2009, Göttingen
- J. Falkner: Trust Delegation im Grid – Proxies als Generalvollmacht. 4. D-Grid Security Workshop, Göttingen, 16.10.2009, Göttingen.
- S. Funk: Grundprobleme Nutzer-basierter Autorisierung in TextGrid. 4. D-Grid Security-Workshop, 15.10.2009, Göttingen

2010

- P. Gietz: Nutzung von SLCs und ROBOT-Zertifikaten in Textgrid. D-Grid All Hands-Meeting 2010, 22.-24.03.2010, Dresden (Open Issues Session)
- B. Fritzsch: Der einfache Weg ins Grid – SLC und Robots. D-Grid All Hands-Meeting 2010, 22.-24.03.2010, Dresden (Open Issues Session)
- J. Falkner: Einfache Nutzung von D-Grid Zertifikaten. 5. D-Grid Security Workshop, 29.09.2010, Göttingen.
- B. Fritzsch: Robot Zertifikate – Policy und erste Erfahrungen. 5. D-Grid Security Workshop, 29.-30.09.2010, Göttingen.

- P. Gietz: Einbindung eines externen PDP in die TextGrid-Infrastruktur über SAML/XACML. 5. D-Grid Security Workshop, 29.-30.09.2010, Göttingen.

2011

- B. Fritzsch: Einführungsvortrag, Abschlussworkshop GapSLC09.06.2011, Tübingen
- J. Falkner: Einfache Nutzung von Zertifikaten – Grid Proxy Upload Tool (gPUT), Abschlussworkshop GapSLC09.06.2011, Tübingen
- J. Brauckmann: Robot-Zertifikate, Abschlussworkshop GapSLC09.06.2011, Tübingen
- S. Pinkernell: Portal Delegation in einem Grid-Portal Szenario. Abschlussworkshop GapSLC09.06.2011, Tübingen
- P. Gietz, M. Haase, S. Funke: Kurzlebige Zertifikate in TextGrid. Abschlussworkshop GapSLC09.06.2011, Tübingen
- S. Pinkernell, B. Fritzsch: Kurzlebige Zertifikate in einem Gridportal-Szenario. 4. Workshop Grid- und Cloud-Technologie für den Entwurf technischer Systeme. 21.-22.09.2011, Dresden

Poster

- S. Pinkernell, B. Fritzsch, S. Funk, M. Haase, P. Gietz, S. Mece , A. Schreiber: Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids. D-Grid All Hands-Meeting 2010, 22.-24. März 2010, Dresden.
- J. Falkner, B. Fritzsch, M. Haase, P. Gietz: Nutzung von ROBOT-Zertifikaten, D-Grid All Hands-Meeting 2010, 22.-24. März 2010, Dresden.
- J. Falkner, O. Strauß, D. Berberovic: Einfachere Nutzung von D-Grid Zertifikaten. D-Grid All Hands-Meeting 2010, 22.-24. März 2010, Dresden.
- B. Fritzsch, S. Pinkernell, M. Pattloch: Short Lived Certificates in a Community Grid – Use Case Climate Research. TERENA Networking Conference 2010, 31.05.-04.06.2010, Vilnius.

5 Literaturverzeichnis

1. *Projektantrag: Nutzung von kurzlebigen Zertifikaten in portal-basierten Grids (GapSLC), Gap-Projekt im Rahmen des 3. Call D-Grid.* 2008.

2. GridShib-CA Administration Documentation. *Chapter 7. GridShib-CA Portal Delegation.* [Online] http://gridshib.globus.org/docs/gridshib-ca-1.0.0/admin/portal-delegation.html.

3. **Gietz, P., Grimm, C., Makedanz, S., Pattloch, M., Schiffers, M., Ziegler, W.,.** *Interoperabilität und Integration der VO–Management Technologien im D–Grid (IVOM).* 2006.

4. Website des Projektes IVOM. [Online] http://www.d-grid.de/index.php?id=314.

5. Shibboleth. [Online] http://shibboleth.internet2.edu.

6. GridShib: Bridging SAML/Shibboleth and X.509 PKI for campus and grid interoperability. [Online] 2009. http://gridshib.globus.org.

7. **E. Maler, P. Mishra, and R. Philpott.** Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. *OASIS Standard.* [Online] 2003. http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf .

8. **Barbera, R., et al.** The GENIUS Grid Portal and robot certificates: a new tool for e-Science. 2009, Vol. 10, 6, p. 21. http://www.biomedcentral.com/1471-2105/10/S6/S21.

9. **Haase, M. and Gietz, P.** Evaluierung der Shibboleth-Integration der Portalsoftware Liferay. [Online] 2010. http://gap-slc.awi.de/documents/Evaluierung_Liferay_v0.05.pdf.

10. **Pinkernell, S.** Shibboleth Auto Login Modul für die Portalsoftware Liferay. [Online] http://gap-slc.awi.de/documents/shibAutoLogin-1.0.pdf.

11. Workshop Sicherheitsanforderungen 21.09.2010 Göttingen. [Online] http://gap-slc.awi.de/workshop.html.

12. GapSLC-Abschlussworkshop 09.06.2011 Tübingen. [Online] http://gap-slc.awi.de/abschlws.html.

13. Certificate Policy of the Public Key Infrastructure in the Deutsche Forschungsnetz - Grid – DFN-Verein Grid-CP V1.5. *https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_grid-cp_v15.pdf.* [Online] May 2010.

14. Certificate Policy and Certification Practice Statement of the Public Key Infrastructure in the Deutsche Forschungsnetz - SLCS. [Online] 2010. https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_SLCS-CPCPS_v11.pdf.

15. **Grimme, C and Enke, H. (Eds).** WissGrid Deliverable 2.3.2: Betrachtungen zur akademischen Sicherheitsinfrastruktur im D-Grid1. [Online] http://www.wissgrid.de/publikationen/deliverables/wp2.html.

16. [Online] http://www.dfn.de/dienstleistungen/dfnaai/.

17. Globus. [Online] http://globus.org/toolkit.

18. Software Repository. [Online] http://aforge.awi.de/gf/project/gapslc/frs/.

19. Gridshib SAML Tools. [Online] http://gridshib.globus.org/docs/gridshib-saml-tools-0.5.0/readme.html.

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

21. VOMS. [Online] http://www.globus.org/grid_software/ security/voms.php.

22. Apache wiki. *http://wiki.apache.org/ws/FrontPage/Axis/DynamicSSLConfig.* [Online]

23. 5. D-Grid Security Workshop. *http://www.d-grid-ggmbh.de/index.php?id=149.* [Online]

Anhang: Fragebogen

Fragebogen zur Evaluation von gPUT und SLC-Services im Grid

Rahmenbedingungen

Im Rahmen des Grid Computing wird gegenwärtig eine Public Key Infrastructure (PKI) eingesetzt. Dabei werden persönliche Zertifikate der Nutzer verwendet, um diese in der gesamten D-Grid-Infrastruktur einheitlich zu authentifizieren. Die Autorisierung des Zugriffs erfolgt je nach Umfang, den der jeweilige Betreiber von D-Grid-Ressourcen für die Nutzer einer Virtual Organization (VO) zugänglich macht.

Um ein persönliches Zertifikat für das Grid zu erhalten, sind folgende Schritte für den Nutzer notwendig:

1. Ein entsprechendes Web-Formular des DFN (Deutsches Forschungsnetz) ausfüllen, welches zu seiner lokalen Zertifizierungsstelle gehört. Hier den richtigen Link zu finden ist nicht trivial, da diese nicht einheitlich veröffentlicht sind.
2. Zu einer lokalen Zertifizierungsstelle gehen und sich dort mit seinem Personalausweis authentifizieren.
3. Ist keine lokale Zertifizierungsstelle vorhanden, kann auf das Post-Ident-Verfahren zurückgegriffen werden.
4. Auf das Zertifikat warten, was ggf. mehrere Tage in Anspruch nehmen kann.
5. Nach Erhalt des Zertifikats ist dieses nicht im passenden Format vorhanden und muss entsprechend konvertiert werden.
6. Nach einem Jahr müssen die Schritte erneut durchlaufen werden, um das Zertifikat zu verlängern. Eine persönliche Authentifizierung ist dabei immer notwendig.

Anschließend muss sich ein Nutzer bei der entsprechenden VO anmelden, um die darin angebotenen Daten und Dienste nutzen zu können. Hierfür ist eine Registrierung bei dem VOMS (VO Management System) notwendig.

1. Zur Registrierung muss in MediGRID die jeweils aktuelle Resource Usage Policy akzeptiert werden.
2. Des Weiteren muss ein Representative der VO ausgewählt werden, der dem Antrag auf Aufnahme in die VO zustimmt.

Zur Nutzung von Grid-Diensten ist anschließend ein Proxy Upload Tool notwendig, welches temporäre Zertifikate von dem persönlichen Zertifikat des Nutzers ableitet.

1. Das Proxy Upload Tool muss heruntergeladen oder über den Browser installiert werden.

2. Zur Verwendung des Grid muss mittels des Proxy Upload Tools nach Ablauf der Laufzeit der temporären Zertifikate jeweils ein neues Proxy Zertifikat erzeugt werden.

3. Für die Nutzung des Proxy Upload Tools muss der TCP-Port 7512 zugänglich sein, was in Sicherheitsumgebungen, wie z.B. Universitätskliniken, nicht zutrifft. Hierfür ist eine Lösung in Arbeit.

4. Alternativ kann auch eine Kommandozeilenversion verwendet werden, die den **ursprünglichen Arbeitsfluss** darstellt:

   a.) grid-proxy-init → Erzeugen des Grid-Proxys

```
medigrid-srv ~ >grid-proxy-init -valid 168:00
Enter GRID pass phrase for this identity:
Your identity: /C=DE/O=GridGermany/OU=Gesellschaft fuer wissenschaftliche Datenv
erarbeitung mbH/CN=Dietmar Sommerfeld
Creating proxy ............................ Done
Your proxy is valid until: Sun Jun 21 21:41:26 2009
```

   b.) grid-proxy-info → Verifizieren der Erstellung des Grid-Proxys

```
medigrid-srv ~ >grid-proxy-info
subject  : /C=DE/O=GridGermany/OU=Gesellschaft fuer wissenschaftliche Datenverar
beitung mbH/CN=Dietmar Sommerfeld/CN=1511290626
issuer   : /C=DE/O=GridGermany/OU=Gesellschaft fuer wissenschaftliche Datenverar
beitung mbH/CN=Dietmar Sommerfeld
identity : /C=DE/O=GridGermany/OU=Gesellschaft fuer wissenschaftliche Datenverar
beitung mbH/CN=Dietmar Sommerfeld
type     : Proxy draft (pre-RFC) compliant impersonation proxy
strength : 512 bits
path     : /tmp/x509up_u10010
timeleft : 167:54:10  (7.0 days)
```

   c.) myproxy-init → Hochladen des Proxys auf den zentralen MyProxy-Server

```
medigrid-srv ~ >myproxy-init -t 24 -c 168 -l dsommer -s gridmon.gwdg.de
Enter GRID pass phrase for this identity:
Your identity: /C=DE/O=GridGermany/OU=Gesellschaft fuer wissenschaftliche Datenv
erarbeitung mbH/CN=Dietmar Sommerfeld
Creating proxy ..........................................................
......... Done
Proxy Verify OK
Your proxy is valid until: Sun Jun 21 21:56:46 2009
Enter MyProxy pass phrase:
Verifying - Enter MyProxy pass phrase:
A proxy valid for 168 hours (7.0 days) for user dsommer now exists on gridmon.gw
dg.de.
```

   d.) myproxy-logon → Erzeugen eines Credentials

```
medigrid-srv ~ >myproxy-logon -t 20 -l dsommer -s gridmon.gwdg.de
Enter MyProxy pass phrase:
A credential has been received for user dsommer in /tmp/x509up_u10010.
```

Teststellung/Evaluation

Damit nicht jeder Anwender ein eigenes Zertifikat beantragen muss und den damit verbundenen Aufwand umgehen kann, können entweder so genannte Robot-Zertifikate oder Short-Lived-Credentials die entsprechende Lösung darstellen. Mit gPUT kann die Nutzung der Zertifikate vereinfacht werden.

Daher ist die Teststellung wie folgt aufgebaut:

1. Nutzung eines (Test-)Zertifikats mit gPUT
2. Nutzung eines (Test-)SLC mit DFN-SLC

Die Evaluation eines Robot-Zertifikats erfolgt auf Basis folgender Beschreibung:

> Eine Grid-Anwendung mit Robot-Zertifikat verwendet intern ein auf eine Person eines Unternehmens oder einer Institution zugelassenes Zertifikat zur Authentifizierung der Anwendung im Grid. Der Nutzer der Grid-Anwendung wird hingegen gegen eine Authentifizierungslösung der Anwendung authentifiziert. Der Betreiber einer Grid-Anwendung muss daher Sorge für die Sicherheit der Authentifizierung tragen. Der Vorteil von Robot-Zertifikaten liegt darin, dass der Betreiber einer Grid-Anwendung selber Benutzeraccounts anlegen/verwalten, und damit für die Nutzer schneller verfügbar machen kann. Zudem entfällt für Nutzer der Authentifizierungsprozess für das persönliche Zertifikat.

Fragen

Nr.	Frage	Antwort				
		sehr hoch	hoch	normal	niedrig	sehr niedrig
1	Wie IT-affin schätzen Sie sich ein?	( )	( )	( )	( )	( )
2	In welchem Bereich sind Sie tätig? (Antwort als Freitext)					
		sehr hoch	hoch	normal	niedrig	sehr niedrig
3	Wie hoch schätzen Sie den Aufwand für den allgemeinen Arbeitsprozess bei der Verwendung von Zertifikaten und Proxy-Zertifikaten in Grid-Umgebungen ein?	( )	( )	( )	( )	( )
4	Wie hoch schätzen Sie den Nutzen von gPUT zur Vereinfachung der Verwendung von Zertifikaten und Proxy-Zertifikaten in Grid-Umgebungen ein?					
		sehr hoch	hoch	normal	niedrig	sehr niedrig
4.1	Mit Browser-Zertifikat (IE/Firefox)	( )	( )	( )	( )	( )
4.2	Mit PEM-Datei	( )	( )	( )	( )	( )
4.3	Mit P12-Datei	( )	( )	( )	( )	( )
5	Wie hoch schätzen Sie den Vorteil der Nutzung von Short Lived Credential Services unter Verwendung der Authentifizierung und Autorisierung über die Heimatorganisation ein?					
		sehr hoch	hoch	normal	niedrig	sehr niedrig
5.1	Gegenüber Nutzerzertifikaten ohne Tools	( )	( )	( )	( )	( )
5.2	Gegenüber gPUT	( )	( )	( )	( )	( )
6	Wie hoch schätzen Sie den Vorteil der Nutzung von Robot-Zertifikaten ein?					
		sehr hoch	hoch	normal	niedrig	sehr niedrig
6.1	Gegenüber Nutzerzertifikaten ohne Tools	( )	( )	( )	( )	( )
6.2	Gegenüber gPUT	( )	( )	( )	( )	( )
6.3	Gegenüber SLCS	( )	( )	( )	( )	( )
7	Welche weiteren Verbesserungen würden Sie sich wünschen? (Antwort als Freitext)					