

Benutzerfreundliche und sichere Zugänge zu Grid Ressourcen

Anette Weisbecker¹, Jürgen Falkner²

¹Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO)

Nobelstraße 12

70569 Stuttgart

Anette.Weisbecker@iao.fraunhofer.de

²Institut für Arbeitswissenschaft und Technologiemanagement (IAT)

Universität Stuttgart

Nobelstraße 12

70569 Stuttgart

Juergen.Falkner@iat.uni-stuttgart.de

Abstract: Ziel der wissenschaftlichen Nutzung von Grid-Technologien ist es, Wissenschaftlern, deren primäre Aufgabe und Ausbildung meist nicht im IT-Bereich liegen, einen einfachen und sicheren Zugang zu einer leistungsfähigen IT-Infrastruktur zu bieten. Hierdurch soll die Zusammenarbeit zwischen Wissenschaftlern unterstützt und sie in die Lage versetzt werden, ihre oftmals sehr ressourcenintensiven wissenschaftlichen Aufgaben überhaupt, oder erstmals in einer leistungsfähigen Umgebung umsetzen zu können. Ein Beispiel hierfür bietet der Bereich der biomedizinischen Forschung, in dem zahlreiche Anwendungen mit unmittelbarem Nutzen für die alltägliche Anwendung in der Patientenversorgung aufgrund fehlender Anbindung an ausreichende IT-Ressourcen sowie aufgrund der technischen Hemmschwellen bezüglich der Nutzung solcher Ressourcen bisher nicht in nennenswertem Umfang zum Einsatz kamen. Im Rahmen der D-Grid Initiative wird im Community-Projekt MediGRID ein nutzerfreundlicher portalbasierter Zugang zu umfangreichen Rechen- und Storage-Ressourcen sowie medizinischen Anwendungen und Daten realisiert [Weis06]. Nicht zuletzt aufgrund der gesetzlichen Bestimmungen zum Umgang mit personenbezogenen medizinischen Daten liegt ein Schwerpunkt der Arbeiten in der Umsetzung eines sicheren zertifikatsbasierten Zugangsverfahrens, das auf der anderen Seite dennoch ausreichend einfach in der Nutzung ist, um die Handhabbarkeit und Akzeptanz unter den Anwendern der biomedizinischen Community zu gewährleisten.

1 Einleitung

Grid-Technologien ermöglichen sowohl in Wissenschaft und Forschung als auch zunehmend im wirtschaftlichen Einsatz die Nutzung verteilter Rechenleistung, Speicherkapazitäten, Anwendungen sowie Dienste und Daten. Während in der Anfangsphase der Entwicklung von Grid-Technologien der primäre Fokus auf der Bereitstellung grundlegender Dienste zur entsprechenden Vernetzung dieser Ressourcen lag, rückt mit zunehmender Reife der so genannten Grid-Middleware die einfache Bedienbarkeit und vor allem auch die sichere Nutzung von Grid-Systemen in den Vordergrund. Neben die „Early Adopters“, vor allem aus dem Umfeld des klassischen High-Performance Computing, sind in der Zwischenzeit viele weitere Nutzergruppen getreten, denen ebenfalls durch die Nutzung von Grid-Technologien völlig neue Möglichkeiten zur Steigerung ihrer Leistungsfähigkeit und vor allem auch zur Zusammenarbeit und dem Austausch von Anwendungen in ihren Communities offen stehen. Im Unterschied zu den Pionieren des Grid Computings, ist in diesen aktuellen, und noch viel mehr in den zukünftigen Nutzergruppen von Grid-Technologien der Schulungsgrad im Bezug auf die Nutzung komplexer IT-Systeme deutlich weniger stark ausgeprägt. Aus diesem Grunde ist es erforderlich, dass den Nutzern einfach zu bedienende Benutzungsschnittstellen zur Verfügung gestellt werden, die keine detaillierten Kenntnisse über die verwendeten Grid-Systeme und deren Ressourcen sowie besonderes IT-Fachwissen im Bezug auf die Bedienung von Grid-Middleware erfordern.

Neben dem Bedürfnis nach einfacher Nutzbarkeit tritt zunehmend auch die Anforderung nach belastbaren Sicherheitsmechanismen in den Vordergrund, wie dies beispielsweise im Bereich der Medizin, Biomedizin und Lebenswissenschaften, aber auch bei der industriellen Nutzung von Grids der Fall ist. Dabei gilt es, eine Balance zwischen diesen beiden Bedürfnissen zu finden, da stärkere Sicherheitsmechanismen meist zu Lasten der Bedienbarkeit gehen, wie am Beispiel der Nutzung von Zertifikaten zur Benutzerauthentifizierung leicht ersichtlich ist. Im Folgenden werden verschiedene Arten von Benutzerzugängen und deren Vor- und Nachteile erläutert um daran anschließend die Umsetzung in der zur D-Grid Initiative gehörenden MediGRID Community zu beschreiben. Dabei wird auf die Problematik der praktischen Sicherung von Nutzerzugängen eingegangen. Weiterhin wird die Umsetzung von Virtualisierungskonzepten beschrieben, die es dem Nutzer weitgehend ersparen sollen, Spezialwissen über die genutzten Grid-Infrastrukturen aufzubauen, das mit seiner eigentlichen wissenschaftlichen oder beruflichen Aufgabe nichts zu tun hat.

Um diese Zielsetzung bereits bei der Planung und beim Aufbau neuer nutzergruppenspezifischer Grid-Umgebungen umsetzen zu können ist hierbei ein Vorgehen nach den Prinzipien des User-Centered Design Prozesses empfehlenswert. User-Centered Design basiert auf der Modellierung des Verhaltens bzw. der Interaktion zwischen (Computer-) Systemen und den Nutzern – dem so genannten Interaction Design [PRS02]. Der grundlegende Ansatz ist dabei, das System aus der Nutzerperspektive zu modellieren und den Fokus auf die Nutzbarkeit des Softwaresystems zu setzen, mit dem der Nutzer interagiert.

Wie in Abbildung 1 dargestellt beginnt der User-Centered Design Prozess mit der Analyse der Bedürfnisse des Nutzers sowie der funktionellen Anforderungen. In weiteren Schritten folgt dann eine Konzeptions- und Spezifikationsphase, gefolgt von einer Umsetzung und Erprobung. Durch die Erprobungsphase wird der Prozess iterativ, indem die Ergebnisse der Evaluation und das Feedback der Nutzer wieder nach den eingangs beschriebenen Gesichtspunkten analysiert werden und in eine verbesserte Konzeption und Umsetzung münden.

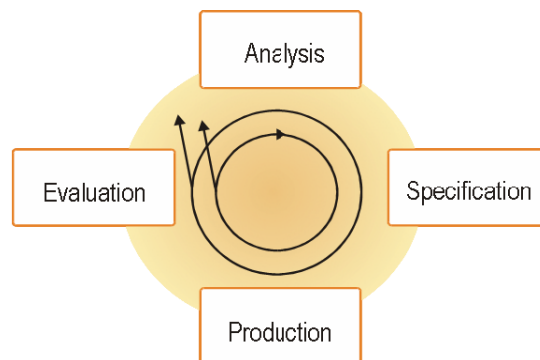


Abbildung 1: User-Centered Design Prozess

Auch im Bereich des Requirements Engineering [Adam06]] werden nützliche Praktiken und Methoden bereitgestellt um das systematische Design und den Aufbau komplexer Softwaresysteme, wie beispielsweise eines Grids, zu unterstützen.

2 Nutzerzugänge zum Grid

Rückt man den Nutzer in das Zentrum des Interesses, so spielt vor allem die Benutzungsschnittstelle, die die (einzige) Verbindung des Nutzers mit dem Grid darstellt, eine wesentliche Rolle. Dabei gilt es zunächst zwei grundsätzlich unterschiedliche Voraussetzungen beim Zugriff auf Grid-Systeme zu unterscheiden. Im ersten Fall hat der Nutzer einen direkten Zugriff auf einen Rechner der Teil der Grid-Infrastruktur ist und somit die softwaretechnischen Voraussetzungen und notwendigen Konfigurationen zur Interaktion mit den anderen Bestandteilen des Grids bereits mitbringt. Im zweiten Fall greift der Nutzer von außerhalb der Grid-Infrastruktur auf das Grid sowie seine Anwendungen und Dienste zu.

Befindet sich der Nutzer (bzw. sein Rechner), wie im zweiten Fall beschrieben, nicht innerhalb des Grids ist eine Schnittstelle zwischen Grid und Außenwelt erforderlich, die in der Regel über ein Gateway (meist in Verbindung mit einer Client-Software) oder ein Portal bereitgestellt wird. Neben Grid-Clients und Portallösungen steht als dritte Benutzungsschnittstelle, die in den Grid-Middleware-Lösungen integrierte Kommandozeilenoption zur Verfügung. Letztere erfordert aber den direkten Zugriff auf die Grid-Middleware und somit einen ins Grid integrierten Rechner und den gesamten damit verbundenen Installationsaufwand.

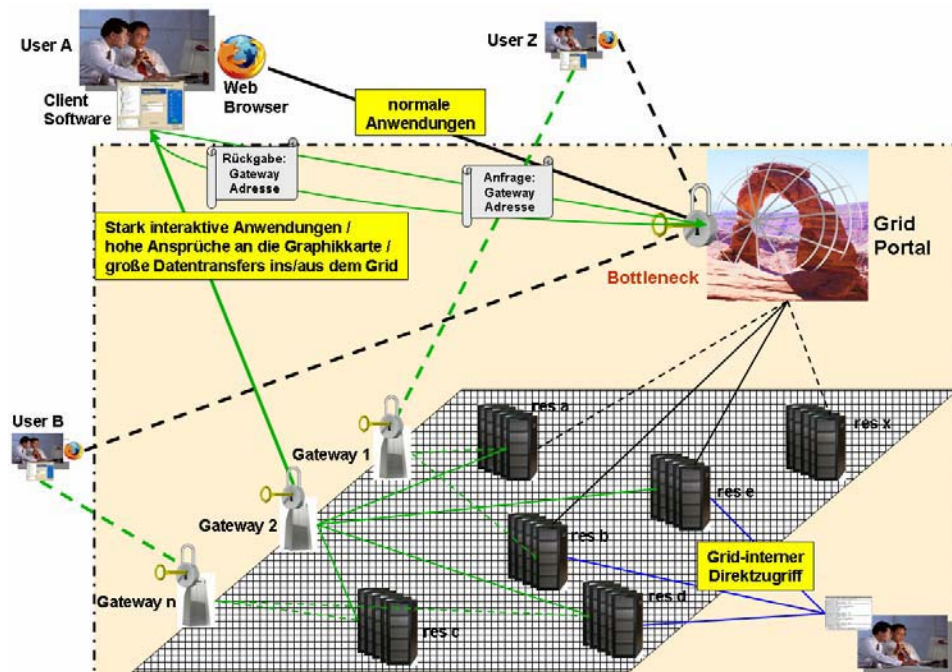


Abbildung 2: Zugriff auf Grid-Ressourcen von außerhalb einer Grid-Infrastruktur

Alle drei Zugangsarten haben ihre Vor- und Nachteile und bilden je nach Nutzergruppe und Anwendungszweck eine geeignete Lösung. Die Vorteile des Direktzugriffs per Kommandozeile liegen zweifellos in der Vermeidung von Flaschenhälsen beim Zugriff auf Grid-Ressourcen sowie im vollen Funktionsumfang, der auf diese Weise bereitgestellt wird. Dem gegenüber steht der nicht unerhebliche Installations- und Konfigurationsaufwand, der einem ungeübten Nutzer nicht ohne weiteres zumutbar ist. Darüber hinaus erfordert auch die Bedienung einen hohen Einarbeitungsaufwand während die fehlende graphische Unterstützung gleichzeitig wenig Übersicht über notwendige Informationen vermittelt. Das konträre Konzept hierzu stellt das Grid-Portal dar, das graphische Anwendungsschnittstellen über intuitiv nutzbare Webseiten bereitstellt. Hierbei reduziert sich der Installationsaufwand seitens des Nutzers auf ein Minimum, da der Nutzer nur einen herkömmlichen Webbrowser und in der Regel ein aktuelles Java Runtime Environment benötigt. Durch Portlet-Standards [JSR168] wird ein modularer Aufbau der Portale ermöglicht und ein Austausch der Anwendungsinterfaces zwischen verschiedenen Portal-Frameworks grundsätzlich ermöglicht. Die Nachteile dieser Lösung liegen im Zusatzaufwand, den die Bereitstellung von Anwendungsportlets – wenn auch nur auf Seiten des Entwicklers und nicht auf Seiten des Nutzers – darstellt, sowie in der Flaschenhalsproblematik, wie sie in Abbildung 2 anschaulich dargestellt wird. Darüber hinaus bieten Webanwendungen nur schlechte Unterstützung für graphisch sehr aufwändige Darstellungen, wie sie in hoch-

interaktiven Anwendungen, beispielsweise im Computer Aided Design (CAD) vorkommen. Die dritte Variante – der Grid-Client – stellt eine Desktop-Anwendung dar, die lokal auf dem Nutzerrechner installiert werden muss, dafür aber auch graphisch anspruchsvolle Darstellungen bewältigen kann. Durch Client-Plugins können ähnlich wie bei Portalen spezifische Anwendungsmodul entwickelt werden. Der Installationsaufwand hält sich hier zwar in Grenzen kann aber bei manchen Nutzergruppen auch schon ein Hindernis darstellen. Insgesamt liegen in diesem Bereich sehr große Potenziale, die aber vor allem im Hinblick auf die Virtualisierung von Ressourcen [Fost04] noch nicht voll genutzt werden, wie ein Blick auf den Unicore-Client [Uni] zeigt. Durch die enge Bindung an die Unicore Middleware besteht nicht wie bei Grid-Portalen die Möglichkeit, Dienste außerhalb der Middleware-Features einzubinden, die beispielsweise eine automatische und dynamische Verteilung von Anwendungen und Anwendungs-Workflows auf die vorhandenen Grid-Ressourcen ermöglichen (siehe Kapitel 4). Ebenso wie bei Portalen erfordert auch bei Grid-Clients die Erstellung von Anwendungsinterfaces einen zusätzlichen Aufwand bei der Entwicklung.

3 Grid-Nutzung in den Lebenswissenschaften

Der typische Nutzerkreis in der Medizin und der biomedizinischen Forschung setzt sich aus Ärzten, medizinisch-technischen Assistenten, Radiologen, Biologen, Biomediziner und ähnlichen Berufsgruppen zusammen, die in der Regel eines gemeinsam haben: sie sind keine ausgewiesenen Computerexperten oder gar Grid-Experten. Dennoch sind Grid-Infrastrukturen in der Lage für sie einen erstrebenswerten Mehrwert zu bieten. Über Grid-Portale kann einer großen Anzahl weltweit verteilter Nutzer Zugriff auf Anwendungen geboten werden, die im Moment meist ausschließlich lokal zugreifbar sind und für größere Nutzerzahlen mit herkömmlichen Infrastrukturen (z.B. einzelne Server) nicht skalieren würden. Durch Grid-Technologien und die damit verbundene Möglichkeit, dynamisch auf weitere Ressourcen an anderen Standorten zuzugreifen und je nach Bedarf wechselseitig zusätzliche fremde Ressourcen zu integrieren, wird es möglich, auch verhältnismäßig rechenintensive, lokal vorhandene Spezialanwendungen einer breiten Zahl an Interessenten zugänglich zu machen. Nutzeranalysen aus dem D-Grid Community-Projekt MediGRID [EFPSW06] zeigen, dass hier großes Interesse besteht.

Unabhängig von der Erschließung neuer Nutzergruppen besteht aber auch in zahlreichen computergestützten Anwendungen im Bereich der Medizin und Lebenswissenschaften ein erheblicher Bedarf an Rechenleistung und Datenspeicherkapazitäten, wie dies z.B. in der medizinischen Bildverarbeitung der Fall ist. Als Beispiele seien hier die Verarbeitung von Mammographien und von dreidimensionalen Ultraschallaufnahmen (im Zuge von Prostatabiopsien) genannt, bei denen jeweils für sehr große Zahlen an Patientinnen und Patienten große Bilddatensätze erfasst und verarbeitet werden müssen.

Die besonderen Herausforderungen bei Aufbau einer Grid-Infrastruktur für die Medizin und Lebenswissenschaften bestehen zum Einen – aufgrund der heterogenen Nutzerstruktur – in der Schaffung einfach zu bedienender Benutzungsschnittstellen und

zum anderen – aufgrund der sensiblen (Patienten-) Daten – in der Sicherung der Daten und der Zugriffsmöglichkeiten auf diese Daten. Daran schließt sich unmittelbar das Benutzermanagement an, das mit beiden Bereichen verknüpft ist.

Um den Anforderungen der Community gerecht zu werden muss der Nutzer in das Zentrum der Betrachtungen gerückt werden. Dieser wiederum möchte sich der Ressourcen eines Grids (Rechenknoten, Datenspeichersysteme, Sensoren, technische Geräte, Daten, etc.) ausschließlich über Anwendungen bedienen, die ihm die Durchführung seiner eigentlichen fachlichen Arbeiten erlauben und technische Feinheiten wie die Auswahl von geeigneten Ressourcen für bestimmte Jobs im Grid oder die Adressierung bestimmter Speicherorte für den Abruf benötigter Daten vor ihm verbergen. Abbildung 3 illustriert dieses Prinzip, das der Virtualisierung im Grid zugrunde liegt.

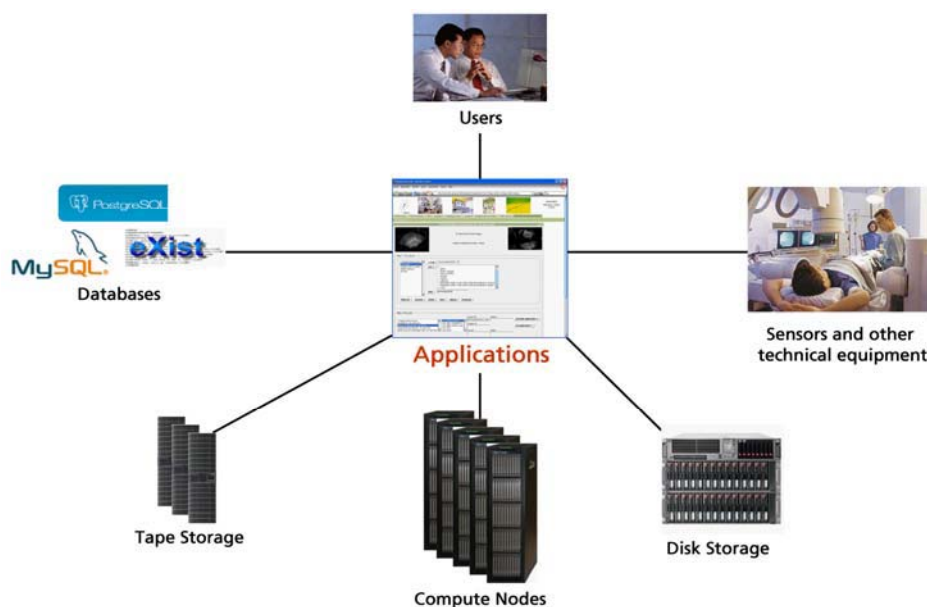


Abbildung 3: Anwendungszentrierte Nutzung von Grid-Ressourcen

4 Benutzerfreundlichkeit durch Virtualisierung

Als Konsequenz aus einer wie in Kapitel 3 beschriebenen anwendungszentrierten Nutzung von Grid-Ressourcen ist es erforderlich, den gesamten Ablauf der Ressourcenauswahl, Job- und Workflowausführung sowie des Datentransfers im Grid durch den Einsatz von Grid-Informationssystemen, Resource Brokern, Worklow- und Datenmanagementsystemen weitestgehend zu automatisieren, wie dies im MediGRID Projekt gegenwärtig umgesetzt wird.

Als Benutzungsschnittstelle kommt hierbei aus Gründen der Akzeptanz und Bedienbarkeit sowie der Minimierung des nutzerseitigen Installationsaufwands ein Grid-Portal zum Einsatz, das sowohl für Nutzer als auch Anwendungsentwickler und Ressourcenbetreiber den zentralen Zugang zu allen Diensten und Informationen im Grid darstellt und wie ein herkömmliches Webportal zu bedienen ist. Die darin integrierten Anwendungsportlets bieten dem Nutzer die Möglichkeit zur Eingabe und zum Upload der für seine Zwecke nötigen Parameter und greifen – für den Nutzer transparent – auf Broker und Daten- bzw. Workflowmanagementdienste zu, die eine Virtualisierungsschicht oberhalb der eigentlichen Grid-Middleware etablieren. Nicht zuletzt bieten die Anwendungsportlets, wie in Abbildung 4 dargestellt auch die Möglichkeit die Ergebnisse der Grid-Anwendungen direkt über das Portal abzurufen bzw. herunterzuladen.

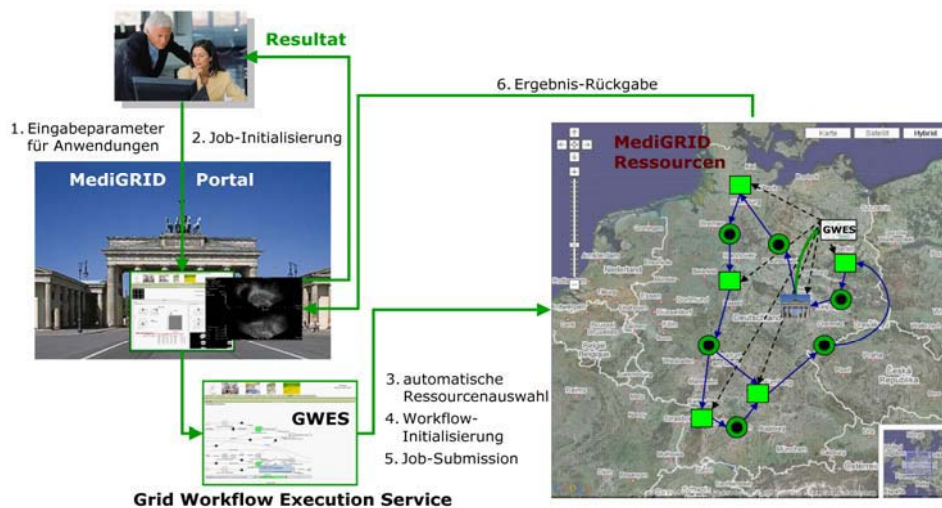


Abbildung 4: Virtualisierung mittels Workflow Management und Resource Brokerage

Die im Portal integrierten Anwendungsportlets rufen nach Eingabe der Anwendungsparameter durch den Nutzer abstrakte Anwendungsworkflows auf, die durch den Anwendungsentwickler definiert wurden. Diese Workflows sind insofern abstrakt, als noch keine konkreten Ressourcen und keine konkreten Instanzen von Anwendungen oder Diensten definiert sind, sondern nur die jeweils benötigte Klasse von Ressourcen, etc. Mit der Initialisierung eines Workflows – die in der Regel vom Nutzer durch Klicken eines Start-Buttons im Webinterface angestoßen wird – beginnt der Grid Workflow Execution Service [NHG06] die in der Workflowbeschreibung definierten Anforderungen zu interpretieren und mit den Informationen aus verschiedenen Grid-Informationssystemen abzugleichen. Als Ergebnis dieses Abgleichs erfolgt die automatische Auswahl der im Moment (nach verschiedenen Kriterien) am besten

geeigneten Ressourcen im Grid. In einem weiteren Schritt werden notwendige Datentransfers im Grid und die Ausführung der einzelnen Bestandteile (Atomic Jobs) des Workflows angestoßen. Der Workflow Service kann auf beliebigen Ressourcen im Grid laufen und auch in mehreren Instanzen vorkommen um Ausfallsicherheit und Lastverteilung zu gewährleisten. Im MediGRID-Projekt wurde auch eine enge Kopplung zwischen Workflow- und dem Datenmanagementsystemen SRB (Storage Resource Broker) [BMRW06] erreicht um eine Anbindung an die Datenvirtualisierungsschicht zu ermöglichen.

5 Sichere Authentifizierung über Grid-Portale

Um den Sicherheitsanforderungen bzgl. des Umgangs mit sensiblen Daten im medizinischen Bereich gerecht zu werden, ist es zunächst erforderlich, eine sichere Authentifizierung der Nutzer im Grid zu gewährleisten. Da im verwendeten Beispiel MediGRID die zentrale Nutzungsschnittstelle das Grid-Portal ist, gilt es also, eine sichere Authentifizierung am Portal und eine entsprechende Weiterleitung dieser Authentifizierungsinformation vom Portal zu den Grid-Ressourcen umzusetzen. Aufgrund des vergleichsweise hohen Risikos der Ausspähung und Überwindung von Passwörtern ist daher in MediGRID die ausschließliche Verwendung von zertifikatsbasierten Authentifizierungsverfahren angestrebt, wenngleich dies im Moment noch nicht für alle Anwendungen durchgesetzt wird.

Zu diesem Zwecke müssen die Nutzer wie in Abbildung 5 beschrieben zunächst ein Grid-Nutzerzertifikat bei einer Grid-Zertifizierungsstelle beantragen. Bereits an dieser Stelle tritt für Teilnehmer kleinerer Organisationen das Problem zu Tage, dass die Beantragung solcher Zertifikate über organisationsgebundene Regional Authorities (RA) erfolgt und es somit erforderlich ist, für seine Organisation bzw. sein Unternehmen eine eigene RA zu betreiben. Der damit verbundene Aufwand stellt ein nicht zu unterschätzendes Hindernis bei der Beantragung von Zertifikaten dar. Sobald der Nutzer im Besitz seines Zertifikats ist tritt das nächste Problem zu Tage: der Nutzer erhält sein Zertifikatspaar (bestehend aus privatem und öffentlichem Schlüssel) nur in einem der beiden Formate PKCS12 und PEM, benötigt aber für die verschiedenen Anwendungen eines portalbasierten Zugriffs beide Formate. Um sich über den Webbrowser zertifikatsbasiert am D-Grid Nutzerverwaltungssystem, dem Virtual Organisations Management and Registry Service (VOMRS), oder am Portal anzumelden, benötigt er ein browser-taugliches Zertifikat (PKCS12) während er für die Delegation von Proxy-Zertifikaten im Grid (zwischen dem Portal und den Grid-Ressourcen) aus technischen Gründen Zertifikate im PEM-Format benötigt. Die erforderliche Konvertierung stellt bei den meisten Nutzern eine erhebliche Hemmschwelle dar und ist für Windows-Nutzer auch nicht ohne die Installation einer speziellen Anwendung lösbar.

Sind diese Hindernisse überwunden, kann man sich am VOMRS unter (zwingender) Nutzung seines D-Grid Zertifikats anmelden. Hierbei wird durch einen automatisch versendeten Registrierungslink zusätzlich die Existenz der angegebenen E-Mail-Adresse überprüft und die Zustimmung zu den Nutzungsbedingungen in D-Grid eingeholt. Anschließend wird der Antrag von einem zuständigen VO-Manager bearbeitet, der im

positiven Falle die Nutzer letztendlich in eine Whitelist einträgt. Die dort gespeicherten Informationen enthalten auch die Zugehörigkeit zu den virtuellen Organisationen (VO) sowie zu Untergruppen dieser VOs und ermöglichen somit in beschränktem Umfang die Verwaltung von Rollen oder Attributen. Diese Whitelist wird von allen Ressourcen im Grid bzw. von deren Administratoren regelmäßig abgerufen und auf den Ressourcen in lokale Benutzerkonten und Mappings [GT4] umgesetzt. Ist dies geschehen, so ist an allen Ressourcen im Grid eine Zuordnung des Nutzerzertifikats bzw. seines Distinguished Names (DN) auf einen lokalen Account mit entsprechender Rechausstattung möglich.

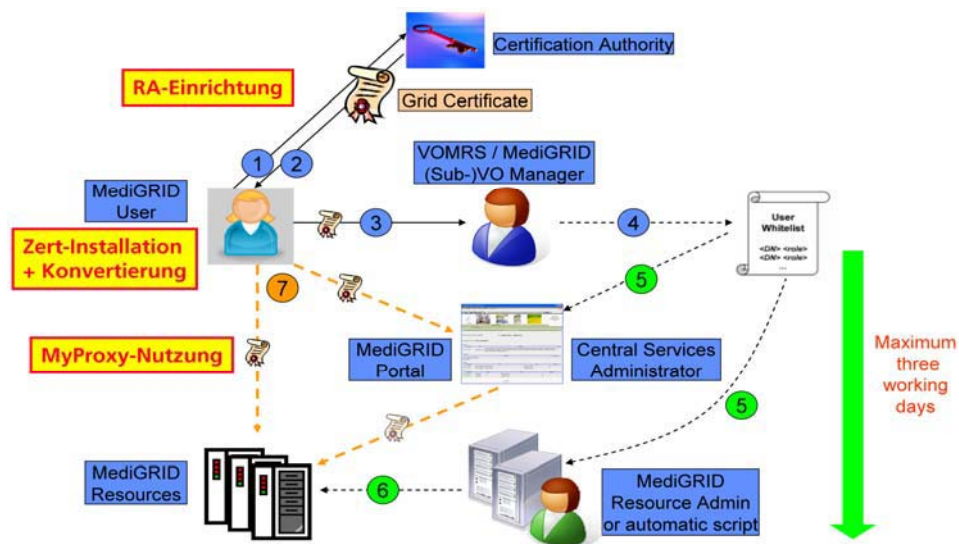


Abbildung 5: Nutzerregistrierung in MediGRID

Damit dies genutzt werden kann ist es aber erforderlich, dass der Nutzer seine Jobaufträge im Grid mit so genannten Proxy-Zertifikaten oder Credentials – also extrem kurzlebigen Kopien seines Schlüsselpaars – signieren kann. Da er selbst in der Regel von außerhalb der Grid-Infrastruktur über das Portal auf die Anwendungen und Ressourcen des Grids zugreift, bedarf es eines Mechanismus, wie der Nutzer Proxy-Zertifikate innerhalb des Grids nutzen kann. Der MyProxy Service [BHW05] bietet hierfür in Verbindung mit dem MyProxy Upload Tool [Drin07] eine Lösung, die in MediGRID auch erfolgreich eingesetzt wird. Das Prinzip ist dabei folgendes:

Der Nutzer lädt einmal eine Kopie seines Schlüsselpaars in einen geschützten Zertifikatsspeicher im Grid – den MyProxy Server. In der Regel wird hierfür eine Zertifikatslebensdauer von einer Woche verwendet. Ist das Schlüsselpaar im Grid bzw.

im MyProxy Server, so kann über eine Grid-Portal-Anwendung – das Credential Management Portlet – auf den geschützten MyProxy Server zugegriffen werden. Der am Portal eingeloggte und über sein im Browser integriertes Nutzerzertifikat authentifizierte Nutzer kann somit unter Verwendung eines Login/Passwort-geschützten Zugangs durch das Credential Management Portlet innerhalb der Grid-Infrastruktur auf den MyProxy Server zugreifen und am Portal ein Grid-Proxy erzeugen. Dieses ist dann für die weitere Verwendung im Grid und die Signierung von Jobaufträgen nutzbar. Somit können Grid-Jobs im Auftrag eines bestimmten Nutzers im Grid verteilt werden und die jeweils ausführenden Grid-Ressourcen können eine zertifikatsbasierte Authentifizierung und Autorisierung vornehmen.

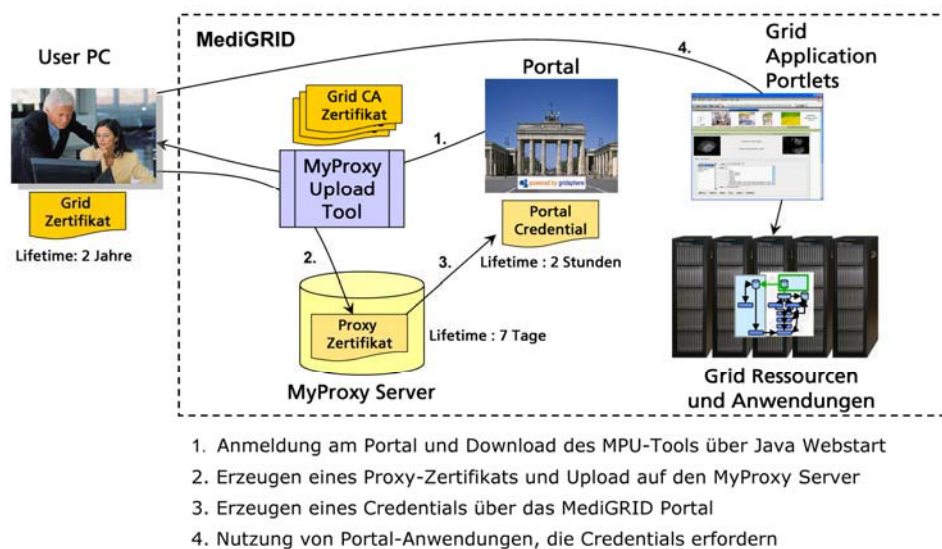


Abbildung 6: Nutzung von Zertifikaten von außerhalb des Grids

Um sein Zertifikat von außerhalb des Grids in den Zertifikatsspeicher hochladen zu können benötigt man aber Security-Funktionen einer Grid-Middleware, die in normalen Betriebssystemen nicht integriert sind. Um es für den Nutzer möglichst einfach zu gestalten, diese Funktionen nachzurüsten, wurde das MyProxy Upload Tool entwickelt, welches Java Webstart nutzt, um einerseits die sichere Kommunikation des Nutzerrechners mit Grid-Ressourcen herzustellen und welches andererseits die Möglichkeit bietet, erforderliche Formatkonvertierungen von Zertifikaten lokal auszuführen. Letzteres ist erforderlich, da der private Schlüssel eines Nutzers nicht an fremde Dienste weitergegeben werden darf. Die oben beschriebene Weitergabe von Proxy-Zertifikaten im Grid widerspricht dieser Vorgabe ganz offensichtlich, wenngleich hier nur sehr kurzlebige Zertifikate aus der Hand gegeben werden. Nichtsdestotrotz wäre es wünschenswert, wenn zukünftige Entwicklungen im Bereich der Authentifizierung und Autorisierung im Grid bessere Verfahren etablieren würden.

Trotz der Lösung des Upload-Problems für Proxy-Zertifikate durch Nutzer außerhalb der Grid-Infrastruktur stellt das in Abbildung 6 dargestellte Verfahren zur Nutzung des MyProxy Upload Tools immer noch eine erhebliche Hemmschwelle für neue Nutzer dar. Unter der Vorgabe einer zertifikatsbasierten Nutzung von Grid-Ressourcen und -Anwendungen ist dies aber gegenwärtig die beste verfügbare Lösung.

6 Zusammenfassung

Die zur Verfügung stehenden Möglichkeiten zur Bereitstellung von Benutzungsschnittstellen bieten grundsätzlich bereits jetzt für jede Nutzercommunity und jeden Einsatzzweck eine geeignete Lösung. Sowohl IT-Experten, die die Einarbeitung in die Detailfunktionen der Grid-Middleware nicht scheuen als auch völlig ungeübte Nutzer können durch die verschiedenen Arten von Nutzerzugängen adäquat bedient werden. Problematisch wird die Nutzung von Grid-Infrastrukturen dann, wenn IT-ferne Benutzergruppen auf ein hohes Sicherheitsbedürfnis treffen und es somit nötig wird, einerseits den einfachen portalbasierten Zugriff von Standardrechnern außerhalb der Grid-Infrastruktur zuzulassen und andererseits eine zertifikatsbasierte Authentifizierung und Autorisierung im Grid erforderlich ist. Die in Kapitel 5 beschriebene Lösung stellt einen gangbaren Weg dar. Der Aufwand bei der Benutzerunterstützung bzgl. der Gewöhnung an das Verfahren und die dafür notwendigen Tools ist allerdings nicht zu unterschätzen. Gleichzeitig besteht noch erheblicher Entwicklungsbedarf in der Umsetzung feingranularer, rollen- oder attributbasierter Rechtekonzepte im Backend der Grid-Ressourcen.

Literaturverzeichnis

- [Adam06] Adam, S., Strauß, O.: Evaluierung der Methodenbaukästen, In: Ehresmann, M., Höß, O., Meier, E., Olsson, T. (Editor): Bausteine zur Optimierung von Software-Entwicklungsprozessen, IRB-Verlag, 2006, S. 157ff
- [BHW05] J. Basney, M. Humphrey, and V. Welch: The MyProxy Online Credential Repository. Software: Practice and Experience, Volume 35, Issue 9, July 2005, pages 801-816
- [BMRW06] Baru Ch, Moore R, Rajasekar A, Wan M: The SDSC Storage Resource Broker. In: CASCON'98 Conference, www.sdsc.edu/srb/, 2006.
- [Drin07] Glen Drinkwater: MyProxy Upload Tool, CCLRS, <http://tiber.dl.ac.uk:8080/myproxy/>
- [EFPSW06] Ernst, T., Falkner, J., Peter, K., Steinke, T., Weisbecker, A.: MediGRID – Analyse der Anwendungen; Deliverable MediGRID Projekt, www.medigrid.de
- [Erns06] Ernst, T., Falkner, J., Peter, K., Steinke, T., Weisbecker, A. (2006): Analyse und Spezifikation der MediGRID-Anwendungen. MediGRID-Deliverable, 31.07.2006
- [Falk06] Falkner, J., Weisbecker, A. (2006): Integration of Applications in MediGRID. To appear in the conference proceedings of the Cracow Grid Workshop 18.10.2006.
- [Fost04] Foster, I., Kesselman, C.: The Grid 2, p.179ff, Morgan Kaufman Publishers (2004)
- [GT4] Globus Alliance: GT 4.0: Security: Authorization Framework;
<http://www.globus.org/toolkit/docs/4.0/security/authzframe/index.pdf>
- [JSR168] Whitepaper, Sun Microsystems: Introduction to JSR 168—The Java Portlet Specification;
http://developers.sun.com/portalserver/reference/techart/jsr168/pb_whitepaper.pdf
- [NHG06] Falk Neubauer, Andreas Hoheisel, Joachim Geiler: Workflow-based Grid Applications. In: Future Generation Computer Systems, Volume 22, Number 1-2, pp. 6-15, © Elsevier, 2006 doi:10.1016/j.future.2005.08.002 (in Druck) (in Englisch)
- [PRS02] J. Preece, Y. Rogers, H. Sharp: Interaction Design, Wiley, 2002
- [Uni] Unicore Client 4.1 User Guide;
http://www.fz-juelich.de/unicoreplus/download/unicore_user_guide.pdf
- [Weis06] Weisbecker, A. (2006): Grid Computing für Medizin und Lebenswissenschaften. Wegweiser (Hrsg.): Jahrbuch Gesundheitswirtschaft 2007: Modernisierung, Prozessoptimierung und Vernetzung im deutschen Gesundheitswesen. Berlin: Wegweiser