WissGrid

Deliverable 2.3.2

Arbeitspaket 2: Blaupausen und Beratung

Betrachtungen zur akademischen Sicherheitsinfrastruktur im D-Grid[1]

Deliverable	2.3.2 Sicherheitsinfrastruktur im D-Grid
Autoren	Arbeitspaket 2: Blaupausen und Beratung
Editoren	C. Grimme, H.Enke
Datum	09-11-2011
Dokument Version	1.0.0

A: Status des Dokuments

Deliverable 2.3.2, Version 1.0.0, freigegeben zur Publikation durch das Projekt

B: Bezug zum Projektplan

Dieses Dokument fasst zusätzlich zu den im Projektplan vorgesehenen Blaupausen den Stand der Sicherheitsinfrastruktur im D-Grid zusammen und stellt Konzepte für den Aufbau einer solchen Infrastruktur zur Verfügung.

C: Abstract

Siehe Summary/Einleitung

[1]This work is created by the WissGrid project. The project is funded by the German Federal Ministry of Education and Research (BMBF).

D: Änderungen

Version	Date	Name	Brief summary
0.0.1	18.02.2011	C. Grimme	Erstellung des Arbeitsdokumentes
0.0.2	21.02.2011	C. Grimme	Struktur des Arbeitsdokuments (Draft)
0.0.3	31.03.2011	G. Stöckle	Sicherheitsinfrastruktur in AstroGrid-D
0.0.4	07.04.2011	C. Grimme	Sicherheitsinfrastruktur in C3Grid, Konzepte offen
0.0.5	03.05.2011	C. Grimme	Sicherheitsinfrastruktur in C3Grid fertiggestellt, Zusammenfassung der übrigen Projekte zusammengestellt und Konzepte aus Material dokumentiert
0.0.6	12.05.2011	C. Grimme	Klassifikation (erster Teil)
0.0.7	03.06.2011	C. Grimme	Klassifikation draft fertig
0.0.8	16.06.2011	C. Grimme	Technische Konzepte, Authentifizierung
0.0.9	17.06.2011	C. Grimme	Technische Konzepte, Autorisierung
0.1.0	24.06.2011	C. Grimme	Technische Umsetzung, Deliv. als Draft fertig
0.1.1	07.07.2011	B. Fritzsch	Korrekturen und Anmerkungen eingearbeitet
0.1.2	08.07.2011	B. Fritzsch	kleinere Anmerkungen
0.1.3	27.07.2011	T. Rathmann	Druckfehlerkorrektur, Formulierungen
0.1.4	27.07.2011	C. Grimme	Summary
0.1.5	28.07.2011	F. Viezens, C.Grimme	Ergänzungen zur Materialsammlung MediGrid
1.0.0	29.07.2011	C. Grimme	Public Comment
	12.12.2011	H. Enke	Publication

Inhaltsverzeichnis

Summary

This document offers a summary and technological overview on security aspects in virtual research environments like community grid infrastructures. Based on conceptual and technical expertise from the first phase of academic D-Grid projects, this document classifies accessibility to such infrastructures as well as security use cases from the users', service providers', and resource providers' points of view. In its final part, this deliverable provides additional information on technological concepts for authentication, authorization, and already available the technical realization of both aspects in the grid infrastructure context.

Overall, this document is an entry point for all interested communities to get an impression of use cases, challenges, and already available solutions regarding security aspects in virtual research environments.

How to read this document:

For a high-level view:	digest the introduction to each chapter, chapter 2 and the first two conceptual sections in chapter 3.
For a detailed view:	include also the technical part of chapter 3.
For a complete/detailed view:	review also chapter 1 to get a complete impression of realizations in all academic D-Grid projects.

Einleitung

Betrachtet man die akademischen Infrastrukturen der ersten Projektphase des D-Grid Projektes, so stellt man fest, dass die Einbeziehung von Sicherheitsaspekten nicht in jedem Projekt eine zentrale Rolle gespielt hat und die vorliegenden Lösungen durchaus prototypischen Charakter haben. Die Diversität und die Unterschiede im jeweiligen Konzeptions- und Entwicklungsstand sind insbesondere durch zwei Gegebenheiten in der frühen Phase der Grid-Infrastrukturentwicklung zu erklären:

Prototypische Infrastruktur: Da in der ersten Konzeptions- und Entwicklungsphase der akademischen Infrastrukturen der Fokus vielfach auf der grundsätzlichen Erprobung von Gridtechnologie und der Umsetzung prototypischer Anwendungen lag, wurde bereits vielfach während der Antragsphasen auf eine konkrete Betrachtung der Sicherheitsproblematik im Grid verzichtet. Grundsätzlich gab es im D-Grid eine Vereinbarung zum Sicherheitskonzept auf Ebene der Middleware, die übergreifend zum Einsatz von persönlichen Nutzerzertifikaten führte. Spätere Anforderungen an die Sicherheit der Grid-Infrastruktur mussten somit in das vorhandene Konzept eingepasst werden. Gleichzeitig trat aber vielerorts die Sicherheitsproblematik erneut zugunsten der Fertigstellung eines funktionsfähigen Prototyps der Grid-Infrastruktur in den Hintergrund. Dies führte zum Ende der ersten Förderphase zu einem breiten Bedarf an Lösungen für einzelne Grid-Infrastrukturen, der gegenwärtig noch nicht abschließend gedeckt ist.

Unterschiedliche Anforderungen: Zusätzlich zu der zögerlichen Aufnahme der Sicherheitsproblematik in die Realisierungen der jeweiligen akademischen Community-Grids verfügen die Communities über sehr unterschiedliche Sicherheitsanforderungen, die eine D-Grid-weite Vereinheitlichung eines einzelnen Konzeptes erschweren. Außer der initialen Festlegung auf zer-

tifikatsbasierte Authentifizierung gab und gibt es sehr unterschiedliche Umsetzungen und einen sehr diversen Umgang mit diesem Mechanismus. Dies ist begründet in sehr unterschiedlichen Ansprüchen der Nutzer, Dienstebetreiber und Ressourcenanbieter in den jeweiligen Community-Grids. Stehen einerseits öffentlich geförderte und damit auch weitgehend öffentliche Daten zur Verfügung, existieren etwa im medizinischen Anwendungsbereich hoch sensible Datensätze, die nur ausgewählten Nutzern zugänglich sein dürfen. Daneben gibt es Mischformen des Datenschutzes. Zugleich bestehen sehr unterschiedliche Anforderungen an die Nutzbarkeit der Sicherheitsinfrastruktur und die Nachvollziehbarkeit der Nutzung von Daten (Auditing).

Dieser Bericht stellt nun einen Ansatz dar, die vorliegenden Konzepte und prototypischen Umsetzungen zusammenzustellen, zu untersuchen und zu klassifizieren. Dabei wird aufbauend auf den infrastrukturellen Ergebnissen der fünf akademischen Community-Grids eine Analyse der Unterschiede in den Anforderungen durchgeführt und diese in entsprechende Klassen von Konzepten, Methoden und Lösungsansetzen eingeordnet. Diese Einordnung soll dann abschließend dazu dienen, offene Punkte in Sicherheitskonzepten aufzuzeigen und Synergiepotentiale zu identifizieren. Gleichzeitig, und dies ist die vorrangige Aufgabe dieses Berichtes, steht damit eine Sammlung von Erfahrungen und Konzepten bei der Etablierung einer Grid-Sicherheitsinfrastruktur zur Verfügung, die beim Aufbau neuer Community-Grids oder virtueller Forschungsumgebungen als Richtschnur und Blaupause verwendet werden kann.

Kapitel 1

Auswertung der Sicherheitskonzepte akademischer Community-Grids

1.1 Sicherheitsanforderungen und Konzepte im AstroGrid-D

1.1.1 Kurze Projektdarstellung

Ziel des Projektes AstroGrid-D ist die Anpassung, Erweiterung und Neuerstellung von Grid-Diensten für astrophysikalische Zwecke. Dies betrifft insbesondere die koordinierte Durchführung von astrophysikalischen Analysen und Verwaltung von verteilten Daten in der Grid-Infrastuktur. Dabei werden nicht nur konventionelle Rechenressourcen und Datenbanken, sondern auch spezialisierte Instrumente (Virtual Observatory) in die Infrastruktur einbezogen.

1.1.2 Sicherheitsanforderungen

Die folgenden Anforderungen sind jeweils strikt aus dem Blickwinkel des jeweiligen Akteurs formuliert. Es ist natürlich die Aufgabe der Infrastruktur-Provider (aka CG), z.B. die Integrität der CA, der RA-Infrastruktur und des VO-Management zu garantieren.

Nutzer: Das Schutzbedürfnis der Nutzer in AstroGrid-D betrifft vorrangig die Sicherheit und den nachvollziehbaren Zugriff auf Daten, Methoden und Ergebnisse. Die Astrophysiker sind grundsätzlich technikaffin und sind das Arbeiten mit der Commandline gewohnt. Zertifikate werden teilweise bereits in anderen Kontexten benutzt. Für HPC-Cluster sind auch Kerberos-Systeme, Smart-Cards und andere zusätzliche Sicherungen durchaus im Einsatz. Sicherlich gibt es nicht eine einzige Bedienungsstruktur, die alle Nutzer zufrieden stellt. Weiterhin gibt es folgende Anforderungen aus Sicht der Nutzer:

- Individuell einstellbare Zugriffsrechte auf Daten (Unix ugw)
- Vereinfachte Gruppenbildung für kollaborative Projekte
- Uniformer Zugang zu Grid-konnektierten Ressourcen (Grid Certificate/Proxy und nicht noch IP-Adressen-Registrierung etc.)
- Respektierung geistiger Eigentumsvorbehalte

Datenprovider: Die Datenanbieter in AstroGrid-D haben insbesondere datenschutzrechtliche Anforderungen. Dabei müssen Nutzungsbedingungen für Daten (auch mit kommerzielle Interessen) eingehalten sowie Nutzungseinschränkungen und Nachvollziehbarkeit der Nutzung sichergestellt werden. Detaillierter sind folgende Anforderungen zu nennen:

- Individuell einstellbare Zugriffsrechte auf Daten (Unix ugw)
- Zeitliche Begrenzungen für Datenzugriff von verschiedenen Gruppen
- Projekt-/gruppenbezogener Datenzugriff
- Geringer kommerzieller Wert von astronomischen Daten, daher sind keine wirtschaftlichen Interessen zu berücksichtigen
- Nachvollziehbarkeit der Zugriffe auf Datensätze, die nicht schon als „public access“ markiert sind

Rechenprovider: Auch die Rechenanbieter wollen Zugriffsbeschränkungen und Rechte von Nutzern wahren, die Sicherheitsanforderungen an auszuführende Programme und die Nachvollziehbarkeit der Ressourcennutzung sicherstellen. Genauer betrifft dies folgende Aspekte:

- Individuelle Zugriffsrechte, keine rollenbasierten Zugriffe
- Nachvollziehbarer Gebrauch limitierter Ressourcen
- Durch VO oder Administrator installierte Bibliotheken, normale Executables (d.h. mit Nutzerrechten ausführbar)
- Zertifikats-basierte Dienste

Im Folgenden sind im Kontext von AstroGrid-D bedeutsame Anwendungsfälle aufgeführt, die die oben erarbeiteten Anforderungen in fünf Szenarien (Use Cases, UC) verdeutlichen.

UC1 „atomic jobs“: Jobs, in denen das gleiche Executable (ggf. mit Compilierung) mit verschiedenen Start-Dateien ausgeführt wird. Keine speziellen Anforderungen, Commandline-basierte Job-Submission, Submission durch zertifizierte User (Globus-Job-Sumission)

UC2 „BOINC jobs“: (hier EinsteinHome): Deployment einer Infrastruktur (BOINC) auf den Grid-Ressourcen, Extra-Ports für Logging Jobcontrol und Monitoring, Deployment durch Admin und/oder AEI, Submission durch zertifizierte AEI-User (eigene Infrastruktur)

UC3 „Compute Servcies“: wie UC1. Public Web-Interface für Parameter-Wahl, dann Ausführung über Zertifikat des Nutzers (der als Service-Anbieter fungiert). Deployment einiger Libs und Installierung des Programms auf ausgewählten Ressourcen. Kann auch als atomarer Job ohne Deployment auskommen. (Globus-Job-Submission) Ggf. wird hier auch OGSA/DAI benötigt, manchmal auch SVN-Client Zugriff auf das Source-Repository für die Erzeugung des Executables.

UC4 „Cluster jobs“: Jobs, in denen das gleiche Executable mit verschiedenen Start-Dateien ausgeführt wird. Jedoch wird ein interaktiver Zugriff benötigt, um das Executable mit verschiedenen Compile-Time Settings zu kompilieren und die Submission ins Batch-System zu testen. GSISSH-basierter Zugriff auf Ressourcen und Job-Submission, Submission durch zertifizierte User

UC5 „GridWay jobs“: Jobs, die über den Metascheduler Gridway (Globus) verwaltet werden, der die Submission auf freie Ressourcen verwaltet. Dies wird insbesondere bei der Kooperation mit spezieller Hardware (GRAPE und GPU) eingesetzt. Benötigt zusätzliche Monitoring Information (ganglia). Submission wie UC1. Installation von Globus 4.03 oder später erforderlich.

Insgesamt sind noch folgende Anmerkungen zur allgemeinen Nutzung der Infrastruktur wichtig: Die Zertifizierungs-Infrastruktur ist international noch nicht so gut ausgebaut, so dass gerade internationale Kollaborationen noch sehr schwer diese Security annehmen. Die RA-Struktur in den nationalen Astronomie-Instituten ist ganz gut ausgebaut, d.h. in nahezu jedem Institut gibt es DFN- oder GridKA-Repräsentanten, die Zertifikatsrequests signieren können.

Eine transparente Nutzung der Authentifizierungs-Prozeduren der verschiedenen Grid-Middlewares wäre sehr hilfreich und erwünscht. Beispiel: Ein DEISA-Account sollte sowohl mit Globus als mit Unicore funktionieren.

1.1.3 Konzepte und Lösungsansätze

Entwicklungsstand des Sicherheitskonzeptes

- Die wesentlichen Anforderungen des Sicherheitskonzepts können durch Abbildung auf Unix-Permissions bewältigt werden. Die VO-Accounts werden auf Grid-Accounts abgebildet, wobei eine VO-Id das konsistente Mapping bei verschiedenen Providern garantiert. Darüber hinaus werden Gruppen durch das VO-Management geschaffen (via VOMRS), die auf Gruppen in den Ressourcen abgebildet werden. Das Mapping (einschließlich Einrichtung neuer User) kann durch das vom AstroGrid entwickelte ManageLocalGridUser System lokal automatisiert werden. Zusätzlich werden die AstroGrid-Ressourcen durch fail2ban geschützt vor Password-Cracker und anderen Attacken. Die CRL-Listen werden auf jeder AstroGrid-Ressource täglich erneuert. Das AstroGrid-D betreibt den VOMRS-Service in eigener Regie und hat neben dem DGrid-VOMRS-Interface noch ein eigenes VO-List Applet, mit dem jederzeit die VO-Accounts abgefragt werden können. Der Service ist Passwort-geschützt.
- Die meisten Anforderungen können mit dem gegenwärtigen System realisiert werden. Es ist allerdings „Handarbeit“ erforderlich, wenn Accounts in mehreren Gruppen organisiert sind, da das derzeitige System hierfür noch angepasst werden muss. Es wäre an dieser Stelle sinnvoll und hilfreich, wenn Globus-Gridmap durch eine weitere Spalte das Mapping zu verschiedenen Gruppen integrieren würde.

Technische Realisierung sowie Tools und Technologien

- Für Grid-Accounts ist nur ein zertifikatsbasierter Zugang vorgesehen, da nicht auf vorhandene lokale Accounts gemappt wird, und das Passwort eine automatisch generierte Zeichenfolge ist. Konzeptuell soll auch die Änderung des Passworts durch den Grid-Nutzer nicht möglich sein.
- Zur technischen Umsetzung des Konzeptes werden hauptsächlich GSISSH, GSIFTP und globus-job-submit in verschiedenen Varianten und die damit vorhandenen Sicherheitskonzepte genutzt. Es werden neben GridWay auch OGSA-DAI, der Replika-Service durch ADM und (eventuell) für das GridSphere-Portal des CactusToolskit auch Globus-Myproxy eingesetzt.

- Es werden externe Dienste und Eigenentwicklungen genutzt: An verschiedenen Stellen wird Stellaris als Informations- und Job-Monitoring und Job-Metadaten Server eingesetzt. Einige Spezial-Interfaces (Robotic Telecopes) speichern auch die Instrument-Profile, die zur Job-Submission erforderlich sind. Zugang zu den dort gespeicherten Informationen sind i.a. durch htpassword und ähnliche Mechanismen geschützt. Weiterhin gibt es einen DataStream-Service, der eine P2P-Superstruktur auf der Middleware aufbaut. Dieser ist jedoch v.a. im experimentellen Einsatz.
- Verwaltung der Nutzer und der Nutzerrechte, und damit das VO-Management liegt beim AIP. Neue VO-Mitglieder müssen vor Aufnahme in die VO durch trusted User/VO/Mitglieder des jeweiligen Instituts bestätigt werden.
- Sicherheitspolitik bei verschiedenen Partnern und die organisatorische Einbettung aller Prozesse in ein gemeinsames Sicherheitskonzept. Policy für „shared ressources“ wie D-Grid, jedoch teilweise auf Gruppen beschränkt.
- Nutzung technischer Hilfsmittel (VOMS/VOMRS) VOMRS + ManageLocalGridUser

1.2 Sicherheitsanforderungen und Konzepte im C3Grid

1.2.1 Kurze Projektdarstellung und Anwendungsfälle

Das Collaborative Climate Community Data and Processing Grid (C3Grid) stellt Klimawissenschaftlern im Kontext der Klimafolgenforschung (IPCC AR5) eine virtuelle Forschungsumgebung zur Verarbeitung und Analyse von Klimadaten zur Verfügung. Dabei werden national verteilt vorhandene Datenbestände über ein zentrales Portal und durch Middlewaredienste such- und zugreifbar. Weitere Dienste stellen dann zugleich eine Abstraktion von Rechenleistung zur Verfügung und ermöglichen die Nutzung der Daten in standardisierten Weiterverarbeitungsschritten, sogenannten Workflows. Diese umfassen die automatische Aquisition der Daten, ihre Vor- und Aufbereitung, Analysen sowie Visualisierung entsprechend den Einstellungen eines Forschers.

Durch die zwei Schwerpunkte der Datenvereinheitlichung/Datenmanagement und der Nutzung verschiedener Rechenressourcen ergeben sich ebenfalls zwei Sichtweisen auf die Sicherheit im C3Grid. Die Klimadatenbestände im C3Grid verfügen über unterschiedliche Sensibilität, während die Nutzer unter Umständen individuelle Ansprüche an den Schutz ihrer Ergebnisdaten haben. Zugleich verfügt das C3Grid über Rechenressourcen, die unter dezentraler Verwaltung stehen und damit unterschiedliche Sicherheitsanforderungen mitbringen. Insbesondere wird hier eine individuelle Nachvollziehbarkeit der Nutzung der Ressourcen als grundlegend vorausgesetzt.

Für den Zugriff auf die C3Grid-Infrastruktur und die damit verbundene Sicherheitsinfrastruktur können für das C3Grid insgesamt drei mögliche Nutzungsszenarien betrachtet werden, die im Folgenden kurz dargestellt werden. Die Nutzungskonzepte gehen dabei dabei bereits von impliziten technischen Voraussetzungen aus, die im Lösungskonzept von C3Grid erneut betrachtet werden. So ist die Nutzung von Zertifikaten – wie im gesamten D-Grid, aber auch im Umfeld der internationalen Klimaforschung – oder die spätere Anbindung an eine Single-Sign-On Infrastruktur ein zentraler Bestandteil in C3Grid:

UC1 (Nutzung persönlicher Zertifikate): Ein Nutzer der C3Grid-Community verfügt über ein persönli-

ches (langlebiges) Zertifikat und greift über ein Portal auf die Dienste von C3Grid zu. Dabei soll eine Rechtedelegation an das Portal stattfinden. Durch die Übermittlung des DN kann dann beim Ressourcenanbieter ein personalisierter Zugriff des Nutzers auf persönliche Daten und Tools ermöglicht werden. Dieser Use-Case umfasst insbesondere den feingranularen Zugriff auf spezielle Funktionen bei Daten- und Rechenprovidern, die eine gesonderte Autorisierung benötigen.

UC2 (kurzlebiges Zertifikat, ggf. Passwort): Alternativ zum konventionellen langlebigen Zertifikat, das sich der Nutzer jeweils bei seiner RA holt, können auch kurzlebige Zertifikate eingesetzt werden. Dabei nutzt der Anwender den SLC-Dienst des DFN und wird an den Identity-Provider seiner Heimateinrichtung verwiesen, wo er sich wie gewohnt per username/password anmeldet. Voraussetzung ist allerdings, dass die Einrichtung Mitglied der Shibboleth-basierten DFN-AAI ist. Durch die Föderation wird eine Vertrauensbasis aufgebaut, die Voraussetzung für die Akkreditierung des SLCS ist. Damit aber sind die kurzlebigen Zertifikate gleichwertig zu den bisher genutzten Zertifikaten und werden von den Ressourcenanbietern ebenfalls akzeptiert. UC2 ist daher nach der Erhalt eines SLC identisch mit UC1. Danach erfolgt wieder Rechtedelegation zwischen den einzelnen Komponenten im C3Grid bis zur endgültigen Autorisierungsentscheidung beim Ressourcen-Provider.

UC3 (anonyme Nutzung): Dabei werden nur spezielle Dienste angesprochen, die auf öffentliche Daten zugreifen und keine persönliche Autorisierung benötigen. Diese Funktionalität wird zu Demonstrations- und Schulungszwecken genutzt, Daten- und Rechenprovider verzichten an dieser Stelle auf eine feingranulare Nachvollziehbarkeit der Nutzung. Das Portal kapselt Nutzeraufträge vollständig.

1.2.2 Sicherheitsanforderungen

Unterschiedliche Teilnehmer am C3Grid (Forscher, Datenprovider, Rechenprovider) haben aus ihrer Sicht sehr unterschiedliche Anforderungen an die Sicherheitsinfrastruktur. Im Folgenden werden die zentralen Aspekte der jeweiligen Rollen dargestellt.

Nutzer: Die Nutzer von C3Grid haben ein Interesse an der einfachen Nutzbarkeit der Sicherheitsinfrastruktur. Da die gesamte Forschungsumgebung über ein Portal bedient wird, soll die Nutzung nicht durch komplizierte technische Sicherungsvorgänge erschwert werden (weitgehende Transparenz technischer Aspekte). Insbesondere wenn der Nutzer ein Zertifikat besitzt, soll der Aufwand des Authentifizierungsprozesses nicht größer sein als bei Eingabe eines Passworts. Zusätzlich ist anzumerken, dass die Nutzer von C3Grid es zwar grundsätzlich gewöhnt sind, algorithmische Probleme für die Auswertung von Klimadaten zu lösen und entsprechende Programme zu implementieren, eine umfangreiche Beschäftigung mit Sicherheitstechnologien ist jedoch nicht gewünscht und im Anwendungsbereich nicht zielführend. Deshalb sollte die Nutzung der Forschungsumgebung auf Ebene des Portals nicht mehr als die Identifikation über ein Passwort, im Spezialfall über ein persönliches Zertifikat erfordern.

Bezüglich der Sicherheitsanforderungen an die Datenhaltung von Ergebnissen und Produkten einer durchgeführten Auswertung beschränkt sich das Nutzerinteresse weitgehend auf eine Personalisierung und Kontrolle der Zugriffsrechte. Ein Nutzer möchte selbst entscheiden, ob und in welcher Form Daten von Außenstehenden zugegriffen werden können. Grundsätzlich sollen Ergebnisse nur dem Nutzer zur Verfügung stehen. Eine Freigabe für andere Nutzer

und damit die Aufnahme der Ergebnisse in den Datenbestand von C3Grid muss vom Nutzer autorisiert werden. Das Gleiche gilt für individuelle Skripte und Programme, die von einem Nutzer persönlich erstellt wurden.

Insgesamt sind die Daten der Nutzer jedoch nicht sehr sensibel. Neben dem Schutzbedürfnis der Produktionsskripte und Ergebnisse bestehen weitgehend keine datenschutzrechtliche Anforderungen.

Datenprovider: Die Datenprovider stellen im C3Grid insgesamt eine Menge an Klimadaten aus unterschiedlichen Quellen und mit unterschiedlichen Lizenzvorgaben zur Verfügung. Neben weitgehend frei verfügbaren Daten, die ggf. nur eine Authentifizierung eines Nutzers oder die Protokollierung der Zugriffe erfordern (um nachzuvollziehen, wer die Daten genutzt hat), verfügen einige Daten über strengere Zugriffsbeschränkungen, da sie für einen gewissen Zeitraum auch kommerziell genutzt werden. Für solche Fälle ist eine entsprechende Authentifizierung und feiner abgestufte Autorisierung notwendig, um sie individuellen Nutzern mit speziellen Zugriffsrechten (Autorisierungsmechanismen) zur Verfügung zu stellen.

Weiterhin ist durch die Einbindung des C3Grids in den Kontext internationaler Forschung des IPCC eine Anbindung an die entsprechenden weltweiten Datensätze erwünscht. Einige Datenprovider im C3Grid treten zugleich als Datenzentrum für die Erstellung des Weltklimaberichtes auf. Hier ist eine entsprechende Homogenisierung der Sicherheitsinfrastruktur und die Verfügbarmachung der entsprechenden Daten notwendig. Es ist anzumerken, dass sich einige dieser Anforderungen verstärkt erst in der Fortsetzungsphase C3Grid-INAD des ursprünglichen C3Grids ergeben haben.

Rechenprovider: Die Rechenprovider bieten im C3Grid fast ausschließlich Rechenleistung für die Ausführung von Teilaufgaben eines Analyseworkflows an. Dabei bestehen nur sehr grundsätzliche Anforderungen an die Sicherheitsinfrastruktur. Da alle Rechenprovider verschiedenen Institutionen zugeordnet sind und unter der Verwaltung einer lokalen Domäne stehen, ist aus ihrer Sicht eine Authentifizierung der Nutzer notwendig. Zugleich ergibt sich aus der Anforderung der Nutzer eine Auftrennung der Userspaces, die nur noch jeweils einem Nutzer zugänglich sein dürfen. Dies muss auf der Ebene der Rechenprovider ebenfalls umgesetzt werden.

1.2.3 Konzepte und Lösungsansätze

Das C3Grid hat die Nutzer-, Datenprovider- und Rechenprovideranforderungen in verschiedenen Phasen der Projektrealisierung auf unterschiedliche Art und mit unterschiedlicher Granularität prototypisch erfüllt. Abbildung 1.1 stellt dies schematisch dar. Die beiden Ansätze werden im Folgenden kurz zusammengefasst.

Das C3Grid versucht bisher eine weitgehende Vereinheitlichung der Sicherheitsinfrastruktur umzusetzen,. Dabei wird vom Vorliegen eines Zertifikats bei der Einreichung eines Jobs ausgegangen. Dies bedeutet, dass das Portal bei der Einreichung des Jobs ein Zertifikat vorzulegen hat. Dies kann das Nutzerzertifikat, ein SLC oder ein Robot-Zertifikat sein. Für die Weiterverarbeitung der Nutzerinformationen (im Falle der anonymen Nutzung die Portalidentität) wird die Nutzeridentität zwischen den beteiligten höherwertigen Diensten delegiert. Damit tritt jeder beteiligte Dienst unter der Identität des Nutzers auf, der damit bei jedem Schritt im System identifizierbar ist. Damit werden weitgehend alle Anforderungen an die Authentifizierung der Nutzer abgedeckt.

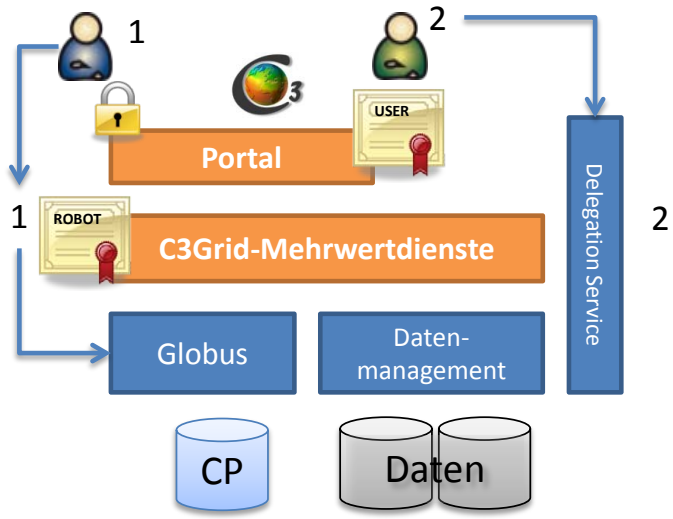

Abbildung 1.1: Schematische Darstellung der C3Grid-Infrastruktur inklusive der zwei umgesetzten Lösungswege zur Authentifizierung in der ersten Generation (1) und der zweiten Generation (2).

Die aktuelle Infrastruktur der zweiten Generation ist über die Dienstekette Portal, Workflowmanagement, Datenmanagement, Rechenprovider und Datenprovider über Delegation von Zertifikaten abgesichert, siehe Abbildung 1.1. Während in der ersten Generation noch ein Robot-Zertifikat genutzt wurde und alle Zugriffe mit einer zentralen Identität durchgeführt wurden, wird in der zweiten Generation nun die Nutzeridentität auf allen Ebenen der Infrastruktur verwendet.

Autorisierungsinformationen werden bisher nicht zentral verarbeitet. Einem Nutzer sind also auf Dienstebene bisher keine Rechte zuzuordnen. Die Rechteverwaltung findet momentan lokal bei den Rechen- und Datenprovidern statt.

1.2.4 Technische Umsetzung

Die C3Grid-Infrastruktur inklusive der Sicherheitsinfrastruktur basieren in ihrer technischen Realisierung weitgehend auf Globus. Grundsätzlich wird die Existenz eines Zertifikates zur Nutzung des Systems vorausgesetzt.

- Im C3Grid wird verbreitet auf die Verwendung von Nutzerzertifikaten gesetzt, inzwischen gibt es einen ersten Prototyp, der ebenfalls im Portal erzeugte Short Lived Certificates (SLC) nutzt.
- Als zentraler Dienst zur Rechtedelegation wird der Globus Delegation Service (Bestandteil der Standard-Globus-Installation GT 4.0.x) genutzt. Mit diesem Dienst können Nutzer ihre Proxy-Zertifikate in den Globus-Container eines Dienstes delegieren. Der Dienst innerhalb des Containers ist dann in der Lage, auf die Informationen zuzugreifen und mit der Identität des Nutzers aufzutreten.
- Nutzung des Globus Delegation Service stellt aufgrund unzureichender Dokumentation ein technisches Hindernis dar. Weiterhin erscheint die Abhängigkeit vom Globus-Stack ein mittelfristiges Problem für die nachhaltige Nutzung der Technologie zu sein, da Globus 4.0.x ab

Ende 2010 nicht mehr gepflegt wird. Perspektivisch erwägt C3Grid für die Umsetzung der nächsten Generation der Infrastruktur den Einsatz von MyProxy für die Delegation.

1.3 Sicherheitsanforderungen und Konzepte im HEP-CG

1.3.1 Kurze Projektdarstellung

Das High Energy Physics Community Grid (HEP-CG) stellt im Kontext des LHC Experiments am CERN eine nationale Plattform für die Analyse der gewonnenen Daten zur Verfügung. Gleichzeitig zu den geringen Anforderungen an die Sicherheitsinfrastruktur in diesem Projekt sollen die Anforderungen der PhotonScience Community betrachtet werden. Deren Anforderungen sind erheblich weitgehender.

Die Sicherheitsanforderungen von Nutzern, Datenprovidern und Rechenprovidern sind im Falle von HEP-CG sehr grundlegend. Durch die Vorgaben des LHC-Projektes ist die Nutzung der Grid-Middleware und der darin enthaltenen Sicherheitsmechanismen vorgegeben. Dabei wird nur eine rudimentäre Zugriffskontrolle auf die grundsätzlich öffentlichen Daten und im Konsortium übergreifend nutzbaren Ressourcen möglich. Die einzige Anforderung zum Schutz von Ressourcen beschränkt sich auf die Nutzung von Zertifikaten und Passwörtern. Dies ist jedoch für die weitgehend technikaffine Nutzerschaft kein Problem.

Bei der PhotonScience stellt sich das Nutzungsszenario anders da. Die Nutzer sind gewöhnlicherweise nicht besonders technikaffin und nicht bereit viel Zeit in die Nutzung von Sicherheitstechnologien zu investieren. Zugleich werden zwei Sicherheitsanforderungen der Nutzer erhoben:

- Schutz von Daten (Ergebniss und Eingabedaten).
- Auditing des Zugriffs, also Nachvollziehbarkeit der Nutzung von Daten und Programmen.

Dabei ist die Nutzerschaft weitgehend heterogen, jedoch oftmals auf die Nutzung der Infrastruktur über Windows angewiesen. Ebenfalls sollte eine Nutzung über ein Portal möglich sein.

1.3.2 Konzepte und Lösungsansätze

Hier werden kurz die bisherigen Lösungen von HEP-CG und der PhotonScience-Community aufgezeigt. Dabei ist zu beachten, dass die PhotonScience noch keine Infrastruktur betreibt. Alle aufgeführten Punkte betreffen erste Konzepte.

HEP-CG: Die Community baut auf der von der Middleware gLite bereitgestellten Infrastruktur auf und nutzt zusätzlich PKI und die VO Management Infrastruktur.

PhotonScience: Insgesamt existiert noch keine tatsächliche Struktur für die PhotonScience Community. Bisher klar sind einige Randbedingungen, nämlich dass es anders als bei HEP keine direkte Interaktion mit der Middleware (gLite/Globus) geben kann. Hier muss eine Portallösung angestrebt werden, die ebenfalls die wichtigen und recht strikten Sicherheitsanforderungen integriert. Zudem zeichnet sich ab, dass dieses Portal eine Nutzung von Zertifikaten ggf. stark abstrahieren muss, um es für die Nutzerschaft der Community zugänglich zu machen.

1.4 Sicherheitsanforderungen und Konzepte im MediGRID

1.4.1 Kurze Projektdarstellung

Das MediGRID-Projekt bietet eine auf Grid-Technologie basierende Forschungsplattform für die Verarbeitung von medizinischen Datenbeständen. Dabei konzentrieren sich die Anwendungen auf klinische, biomedizinische und bildverarbeitende Arbeitsprozesse der Forschung. Besonders sensibel ist in diesem Kontext der Umgang mit Patientendatenbeständen. Hier liegt daher ein starker Fokus der Bestrebungen für eine gute Sicherheitsinfrastruktur.

1.4.2 Sicherheitsanforderungen

Obwohl die Nutzungsszenarien (Use Cases) ähnlich wie bei dem C3Grid-Projekt sind, können teilweise andere Nutzeranforderungen festgestellt werden. Diese werden im Folgenden aufgelistet.

Nutzer: Da auch im Kontext von MediGRID nicht von sehr technikaffinen Nutzern ausgegangen werden kann, müssen die folgenden Aspekte insbesondere unter dem Aspekt der Einfachheit der Benutzung betrachtet werden.

- Datenschutz: Insbesondere bei dem Umgang mit Patientendaten gelten höhere Sicherheitsanforderungen. Hier ist eine Anonymisierung, Pseudonymisierung oder Komplettverschlüsselung der Patientendaten bei Speicherung, Transfer und Weiterverarbeitung im Grid erforderlich.
- Schutz der Daten vor Zugriff durch Personen ohne berechtigtes Interesse: Ein unberechtigter Zugriff muss verhindert sein.
- (Industrielle) Nutzer haben weiterhin ein Interesse daran, dass bspw. Mitbewerber kein Nutzungsprofil (z.B. höherer Nutzung aufgrund von Produkttests) erstellen können, um somit an Betriebsinterna zu gelangen.
- Eine (Re-)Identifizierung durch Personen ohne berechtigtes Interesse darf nicht möglich sein.
- Die Datenhoheit muss weiterhin bei dem Patienten liegen. Hierzu gehört zu wissen, was wo mit den Daten passiert (Trackability).
- „Robustness“ muss durch die Grid-Infrastruktur bereitgestellt sein. Insbesondere bei langen Jobs muss die Verfügbarkeit von Ressourcen und Diensten und somit die Integrität der Ergebnisse und Teilergebnisse von Grid-Jobs sichergestellt sein (Beispiel: Bildverarbeitungsapplikation mit MRT-Daten dauert mehrere Tage und produziert Zwischenergebnisse sowie Daten die nachfolgende Prozesse innerhalb der Jobausführung benötigen).
- Optimieren der Einstiegsschwellen in Bezug auf die Authentifizierung bzw. Zertifikatsbeantragung. Für die Evaluierung der Nutzerfähigkeiten und zur Verfikation der Anforderung werden hier die Ergebnisse eines Nutzertest im Rahmen des GAP-SLC Projektes erwähnt, bei dem gPUT im Portlet und der DFN-IdP für die Beschaffung von SLCs benutzt wurden (20 Teilnehmer):

Nr.	Frage	Typ	Ergebnis (Mittelwert)
F1	Wie IT-affin schätzen Sie sich ein?	sehr hoch:5 - sehr niedrig:1	4,20
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	3,90
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	3,79
F4.2	Mit PEM-Datei	sehr hoch:5 - sehr niedrig:1	3,16
F4.3	Mit P12-Datei	sehr hoch:5 - sehr niedrig:1	3,28
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	4,50
F5.2	Gegenüber gPUT	sehr hoch:5 - sehr niedrig:1	3,80
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	4,37
F6.2	Gegenüber gPUT	sehr hoch:5 - sehr niedrig:1	3,53
F6.3	Gegenüber SLCS	sehr hoch:5 - sehr niedrig:1	3,37
7	Welche weiteren Verbesserungen würden Sie sich wünschen?	Freitext	

Eine graphische Aufbereitung der Befragung findet sich zusätzlich in Abbildung 1.2. Teilnehmer der Studie waren das Rechenzentrum, die Abteilungen Medizinische Informatik, Medizinische Statistik, Genetische Epidemiologie, Hämatologie und Onkologie, Herzzentrum, IASTE-Student der Universitätsmedizin Göttingen.

Insgesamt bringt die Nutzerschaft wenig Erfahrung im Umgang mit fortgeschrittenen Sicherheitskonzepten mit. So kann eine gewisse Vertrautheit mit der Anmeldung per Nutzername und Passwort vorausgesetzt werden. Die Nutzung von Zertifikaten ist wenig verbreitet. Im

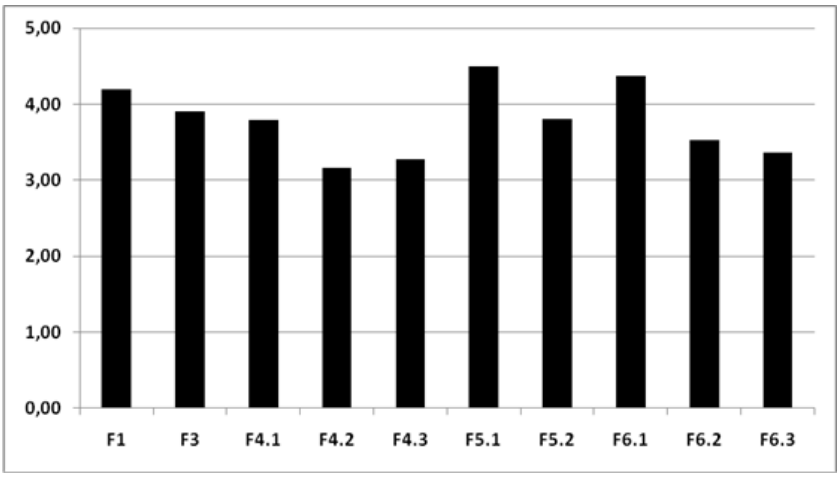

Abbildung 1.2: Graphische Darstellung der Befragung. Jeder Balken gibt den ermittelten Durchschnittswert bezüglich der jeweiligen Frage an (20 Teilnehmer).

Bereich der medizinischen Anwendung sind teilweise technikaffine Nutzer anzutreffen, die überwiegende Nutzergruppe benötigt jedoch erhebliche Hilfestellung bei der Benutzung eines Systems, etwa durch eine geeignete graphische Oberfläche oder ein Portal.

Datenprovider: Da die zur Vefügung gestellten Daten starken Datenschutzrichtlinien unterliegen existieren auch von Seiten der Datenprovider starke Anforderungen an die Infrastruktur.

- Audit-Trail zur Nachvollziehbarkeit von Nutzeraktivitäten - auch notwendig als Grundlage für Etablierung von Service Level Agreements.
- Datenschutz: s.o.
- Anbindung an das Accounting als Grundlage für die Service Level Agreements.
- Umsetzen der Berechtigung(sstrukturen).
- Sicherheit der Ressourcen muss gewährleistet sein (OS-Patches etc.)

1.4.3 Konzepte und Lösungsansätze

Im folgenden werden kurz der Entwicklungsstand, die technische Realisierung und einige organisatorsche Aspekte des Projektes dargestellt.

Entwicklungsstand des Sicherheitskonzeptes

Es wird vom Vorliegen eines Zertifikats bei der Einreichung eines Jobs ausgegangen. Die bisherige Infrastruktur ist über die Dienstefolge Portal, Workflowmanagement, Datenmanagement, Rechenprovider und Datenprovider über Delegation von Rechten abgesichert.

Autorisierungsinformationen werden bisher nicht zentral verarbeitet. Einem Nutzer sind also auf Dienstebene bisher keine Rechte zuzuordnen. Die Rechteverwaltung findet momentan lokal bei den Rechen- und Datenprovidern statt - über das Gridmap-File werden die Berechtigungen übergreifend verteilt (analog zu anderen Communities).

Das Datenschutzkonzept im PneumoGrid basiert insbesondere auf zweifacher Pseudonymisierung, um den Schutzbedarf der zu verarbeitenden Daten zu verringern.

Weiterhin ist kein eigenes zentrales Zertifikats-Management etabliert. Stattdessen existieren RAs zur DFN-Grid-CA z.T. bei den Einzelinstitutionen, etwa bei der Charit'e in Berlin[1].

Technische Realisierung sowie Tools, Technologien und Prozesse

- Bisher verbreitet sind die Nutzerzertifikate, vereinzelt auch Robot-Zertifikate (GWES)
- Grid Proxy Upload Tool (gPUT) für Proxy und Credential Management via LifeRay-Portal mit den Optionen (a) userkey.pem und cert.pm, (b) p12-Zertifikat und (c) Browser-integrierte Zertifikate (IE, Firefox).
- Als zentraler Dienst zur Rechtedelegation wird der Globus Delegation Service (Bestandteil der Standard-Globus-Installation GT4.0.x) genutzt.
- Secure-DICOM zur Pseudonymisierung von medizinischen Bilddaten wird eingesetzt.
- Ein myproxy-Server wird zur Verwaltung mittelfristiger Proxyzertifikate verwendet.
- Aufbau einer VO „medigrid“, sowie Untergruppen (z.B. Bioinformatik, Bildverarbeitung, Ontologie) in VOMS, die Untergruppen werden aber derzeit von der Middleware nicht unterstützt. Zusätzlich wurde eine VO für PneumoGrid (aufgrund indistrieller Nutzung und Datensicherheit) eingerichtet.

1.5 Sicherheitsanforderungen und Konzepte im TextGRID

1.5.1 Kurze Projektdarstellung

Das Projekt TextGrid stellt die Infrastruktur für eine Virtuelle Forschungsumgebung in den Geistes- und Kulturwissenschaften zur Verfügung. Den Einstiegspunkt in die Virtuelle Forschungsumgebung bildet das TextGrid Laboratory mit zahlreichen Werkzeugen und Services zur Bearbeitung geisteswissenschaftlicher Forschungsdaten, deren langfristige Verfügbarkeit und Zugänglichkeit das TextGrid Repository garantiert.

In diesem Kontext werden aktuell nur Grid-Speicher-Ressourcen verwendet. Von den Zielen des Projekts vorgegeben, ist eine langfristige Verfügbarkeit (mehrere Jahre) der gespeicherten Daten unabdingbar. Die produktiven Daten beschränken sich aktuell auf einen Grid-Rechner aus den Sonderinvestitionsmitteln an der SUB Göttingen. Weitere Grid-Speicherknoten sind mittelfristig in Planung; langfristig sollen auch Compute-Ressourcen einbezogen werden.

1.5.2 Sicherheitsanforderungen

Nutzer: Benutzer müssen zu ihren Daten eindeutig zugeordnet werden können. Trotzdem soll ein Benutzer auch bestimmte Rechte auf den von ihm verwalteten Daten anderen Benutzern

[1] `http://www.charite.de/medinfo/Userpages/Mitarbeiter/Krefting/home/?page_id=61`

oder Gruppen einräumen können. Eine detaillierte Aufstellung der Anforderung folgt in diesem Abschnitt.

- Die Nutzer stellen hohe Anforderungen an den zuverlässigen Zugang zu ihren Daten und deren Schutz vor unautorisierten Zugriffen. Dazu wurde frühzeitig aus der Community die Forderung nach rollenbasierter Zugriffskontrolle laut: die Daten sollen "Projekten" zugeordnet werden können und in jedem Projekt soll eine Anzahl von Rollen den Zugriff darauf regeln, z.B. Projektleiter, Administrator, Bearbeiter und Beobachter. Diese besitzen jeweils verschiedene Rechte an den einzelnen Datenobjekten innerhalb der Projekte. Dennoch sollte es einfach möglich sein, anderen Mitgliedern der Community bestimmte Rechte an den Objekten zu erteilen. Außerdem soll es möglich sein, einzelne Objekte zu "publizieren", d.h. sie irreversibel in einem Nur-Lese-Modus der Öffentlichkeit zugänglich zu machen, u.A. ohne Authentifizierung im WWW.
- Erwünscht ist aber auch eine möglichst transparente AAI: Login-Vorgänge sollen möglichst nicht bemerkt werden (z.B. existieren einzelne Forderungen nach dem "Merken" des Logins auf einem Arbeitsplatzrechner) und nicht länger als wenige Sekunden dauern. Hier gilt es im Einzelfall Einfachheit und Sicherheit gegeneinander abzuwiegen.

Die TextGrid-Nutzer sind zum einen vertraut mit der Authentifizierung per Nutzername und Passwort, ebenso mit der Authentifizierung per Shibboleth (was im Prinzip ebenfalls unter Nutzername/Passwort fallen dürfte). Mit Nutzerzertifikaten sind die Nutzer nicht vertraut, sie werden jedoch auch nicht benötigt (da dies alles durch TG-crud und sein ROBOT-Zertifikat gekapselt wird). Zur Nutzung von SLCs siehe unten.

Als Überforderung kann angesehen werden, wenn der Benutzer – etwa zum Setzen einer umask für den Web Browser – die Kommandozeile verwenden muss. Ebenso sollte nicht vorausgesetzt werden, dass der Benutzer sich Dateipfade merkt, etwa zu temporären Proxys. Will ein Nutzer die Shibboleth-Infrastruktur zum Beziehen eines SLC benutzen, (um mit den High-Security Ressourcen arbeiten zu können), so kann mit einigen Klicks die Delegation des SLCs an das Portal (in dem Fall TextGrid) erlauben. Nach einer Wartezeit von wenigen Minuten ist das SLC erstellt und ggf. beim VOMRS (einmalig) angemeldet. Dieser Vorgang wiederholt sich jeden Tag. Sehr wünschenswert und nötig für eine Akzeptanz der SLCs wäre eine Beschleunigung und Vereinfachung der SLC-Erstellung.

Datenprovider: Daten müssen langfristig verfügbar sein und zuverlässig gespeichert werden. Besonders hohe Sicherheitsanforderungen bezüglich des Schutzbedürfnisses der Daten vor unberechtigtem Zugriff bestehen nicht. Detailliert ergeben sich folgende Forderungen:

- Ein Benutzer muss einer bestimmten Organisation angehören, um auf eine Ressource zugreifen zu können.
- Ein Benutzer muss sich an einem bestimmten Ort aufhalten, z.B. dem Forschungsinstitut oder einem Land, um auf eine Ressource zugreifen zu können.
- Ein Benutzer muss erst einen Lizenzvertrag bestätigen, um auf eine Ressource zugreifen zu können.
- Ein Benutzer darf erst nach einem bestimmten Datum auf eine Ressource zugreifen, z.B. 75 Jahre nach dem Tod des Autors.
- Ein Benutzer darf erst nach einer bestimmten Zeitspanne (z.b. 6 Monate) nachdem die Ressource erzeugt wurde, auf diese Ressource zugreifen.

- Eine beliebige Kombination der oben genannten Bedingungen

Ressourcenprovider: Der Ressourcenprovider muss im Missbrauchsfall nachvollziehen können, welche Daten welcher Person gehören. Weitere Anforderungen gibt es bislang nicht.

Insgesamt sind für TextGrid etliche Anwendungsfälle (Use Cases) identifizierbar. Einige sind im Folgenden aufgeführt. Hier wird insbesondere auf die sicherheitsrelevanten Vorgänge eingegangen:

- Arbeit mit dem Rich Client (TextGridLab) ohne Login (Nur-Lese-Zugriff auf publizierte Daten) oder mit Login (Vollzugriff)
- Login entweder über (schwächeren, weil ohne echte Identifizierung der Person) Community-LDAP-Server oder über (sichere, weil im Campus persönlich identifiziert) DFN-AAI
- Nutzer verwendet seine Daten allein.
- Nutzer teilt seine Daten zum Lesen/Bearbeiten/... mit anderen Forschern.
- Nutzer publiziert seine Daten für die Öffentlichkeit.
- Nutzer legt neues Projekt an und wird somit zum Projektleiter.
- Projektleiter entscheidet entsprechend über die Projektdaten.
- Institution liefert Daten frei (s. Nutzer publiziert....).
- Institution liefert Daten unter bestimmter Lizenz (gebunden an Attribute des Nutzers/der Daten/andere Faktoren), der zugestimmt werden muss.

1.5.3 Konzepte und Lösungsansätze

Als Grid Middleware in TextGrid wird Globus Toolkit verwendet. Weiter wird eine rollenbasierte Zugriffskontrolle (PDP) mit eigenem Benutzer- und Projektmanagement sowie ein CRUD-Dienst für Dateioperationen, der als PEP fungiert. Für die technische Umsetzung der Konzepte wird Globus Toolkit 4.2.1 und GAT eingesetzt. Im Produktivsystem wird über einen Dienste-Account (ROBOT) hierauf zugegriffen. Als Benutzer- und Projektmanagement und zur Zugriffskontrolle / als PDP wird die Eigenentwicklung openRBAC eingesetzt (PEP ist die Eigenentwicklung TG-crud).

Im Folgenden wird auf das allgemeine Konzept und die Umsetzung in TextGrid detaillierter eingegangen. Dabei wird auch die organisatorische Struktur näher betrachtet.

Allgemeines Sicherheitskonzept

Der Zugang zu TextGrid kann einerseits per Shibboleth über einen existierenden Zugang an einer deutschen Hochschule als Mitglied des DFN-AAI erfolgen. Durch die Föderation wird eine Vertrauensbasis aufgebaut, die zusätzlich zu noch strengeren Anforderungen[2] Voraussetzung für die

[2]Die Akkreditierung eines SLCS stellt scharfe Anforderungen an den Betreiber, etwa das Vorhandensein von automatischen Prozessen zur Accountauflösung, eine starke Absicherung der Zugriffskontrolle und das Erlauben von Auditings.

Akkreditierung des SLCS ist. Damit sind die kurzlebigen Zertifikate gleichwertig zu den bisher genutzten Zertifkaten und werden von den Ressourcenanbietern ebenfalls akzeptiert. Andererseits funktioniert der Zugang über einen Account im TextGrid-LDAP, der über ein Formular auf der TextGrid-Homepage beantragt werden kann. Dieser wird nach einer Prüfung durch TextGrid angelegt. So können auch interessierte Privatpersonen oder Personen aus dem Ausland TextGrid nutzen, können jedoch nicht auf evtl. High-Security-Ressourcen zugreifen.

Auf Grid-Infrastruktur-Ebene beschränkt sich die Authentifizierung auf zwei Szenarien. Nach einer Authentifizierung durch den TextGrid-Dienst TG-auth* per TextGrid-LDAP oder Shibboleth wird hier entweder ein ROBOT-Zertifikat oder ein kurzlebiges Zertifikat (SLC) für die Grid-Authentifizierung genutzt. Für die Nutzung eines SLC ist die Anmeldung über Shibboleth erforderlich. Mit dem ROBOT-Zertifikat des TextGrid-Services TG-crud (Create/Retrieve/Update/Delete) wird per JavaGAT auf die Grid-Infrastruktur über ein Globus Toolkit zugegriffen. Hier wird zunächst nur auf die TextGrid-eigenen Ressourcen zugegriffen, denkbar ist eine Erweiterung auf andere D-Grid-Ressourcen, sofern sie ROBOT-Zertifikate zulassen (so genannte Low-Security Ressourcen).

Technische Realisierung, Technologien und Prozesse

Die Sicherheitsanforderungen wurden durch die Komponente TG-auth* realisiert (Eigenentwickung, Kombination aus optionalem Shibboleth-Login und openRBAC-Autorisierungs-Framework). Zur Transparenz: Es wird dem Benutzer nicht zwingend vorgeschrieben, dass er mit einem Zertifikat/SLC arbeiten muss, da bei der aktuellen Dauer eines SLC-Login-Vorgangs die bisherige hohe Akzeptanz dadurch deutlich leiden würde. Stattdessen ist über die direkte LDAP- bzw. DFN-AAI-Authentifizierung per Shibboleth die Verwendung des ROBOT-Zertifikats möglich. Sowohl das ROBOT-Zertifikat sowie auch die Nutzung des SLC werden vom TextGrid-Dienst TG-crud für einen Zugriff auf die Grid-Ressourcen genutzt. TG-crud nutzt JavaGAT für die Zugriffe, wobei entweder ein Proxy-Zertifikat oder das SLC selbst für die Authentifizierung genutzt werden (GSIFTP).

Ein TextGrid-Nutzer weist sich durch Nutzername und Passwort aus, entweder im TextGrid-LDAP oder per Shibboleth. Die Nutzung des ROBOT-Zertifikats wird seit einigen Wochen produktiv in TextGrid genutzt, die Nutzung von SLCs ist bisher prototypisch auf einem Test-System implementiert. Produktiv nutzt TextGrid die GSIFTP-Schnittstelle des eingesetzten Globus Toolkit (momentan Version 4.0.8, bald 4.2.1) über JavaGAT.

Organisatorische Aspekte und Prozesse

- Die Nutzer von TextGrid werden auf zwei Ebenen verwaltet. Zum einen im TextGrid-internen LDAP (mit Selbstregistrierung und manueller Überprüfung) und zum anderen über Shibboleth (automatische Registrierung). Mitglieder aus beiden Ebenen können Projekte erstellen und Objekte erstellen und importieren. Die Verwaltung der Rechte geschieht mit openRBAC, das Teil der Komponente TG-auth* ist.
- Nutzung technischer Hilfsmittel (VOMS/VOMRS): VOMS-Synchronisation von SLCs wird im Rahmen von SLC-Gap implementiert. Weitere Hilfsmittel sind der Rich Client TextGridLab (Eclipse, mit eingebettetem Browser), Apache2 für das Portal, Tomcat6 für TG-crud, etc.

Kapitel 2

Klassifikation von Zugangswegen und Anforderungen

2.1 Zugangswege zur Forschungsplattform

Die vorherige Betrachtung der sicherheitsbezogenen Anwendungsfälle für die Grid-Infrastrukturen der akademischen Communities zeigt, dass es ein zentrales Problem der Zugangswege zu einer solchen Forschungsumgebung gibt. Betrachtet man die Architektur eines jeden Grids, so lassen sich mehrere Schichten der Abstraktion feststellen (siehe Abbildung 2.1 und auch die WissGrid-Blaupause zu den Architekturkonzepten [2]). Neben der Zugangsschicht kann man bei grober Unterteilung insbesondere die Middlewareschicht (inkl. der höherwertigen Dienste) und die Ressourcenanbieter (Daten und Rechenprovider) identifizieren. Diese Schichten weisen eine hohe technische Komplexität auf und werden in der Regel von erfahrenen Technikern betreut. Innerhalb dieser Schichten haben die meisten Communities relativ geringe Probleme, die geforderten Sicherheitsaspekte und Anforderungen der Nutzer umzusetzen[1]. Durch das VO-Management und die zugehörigen Dienste auf Middlewareebene ist der Umgang mit Zertifikaten und Nutzerzuordnungen weitgehend abgedeckt. Während höchstens die Autorisierung an einigen Stellen noch technologische und vor allem organisatorische Probleme darstellt, ist die Handhabbarkeit der Sicherheitstechnologien auf Ebene der Nutzerschnittstellen sicher nicht ausreichend entwickelt und auch konzeptionell schwer.

Nahezu alle Projekte verfügen zwar über eine technische Sicherheitsinfrastruktur, jedoch nicht über eine ausreichende Abstraktion der Konzepte, um eine einfache Nutzung der gesicherten Infrastruktur durch technisch wenig erfahrene Nutzer sicherzustellen.

Um eine Grundlage für die weitere, vielleicht strukturierte Beschäftigung mit diesem Thema zu schaffen, sollen im Folgenden die unterschiedlichen Zugangswege zu einer Grid-Umgebung herausgearbeitet und klassifiziert werden. Dies kann dann ggf. von neuen Communities oder etablierten akademischen Community-Grids als Startpunkt für fokussierte Überlegungen bezüglich einer einzelnen Klasse von Zugängen genutzt werden. Im nächsten Kapitel wird dann zusätzlich auf die technischen Lösungsmöglichkeiten eingegangen.

[1] Eine Umsetzung ist hier nicht im technischen Sinne durchaus nicht einfach, es gibt jedoch verschiedene technisch gut erprobte Möglichkeiten die Verbindung der Ressourcen auf unterster Ebene sicher zu gestalten.

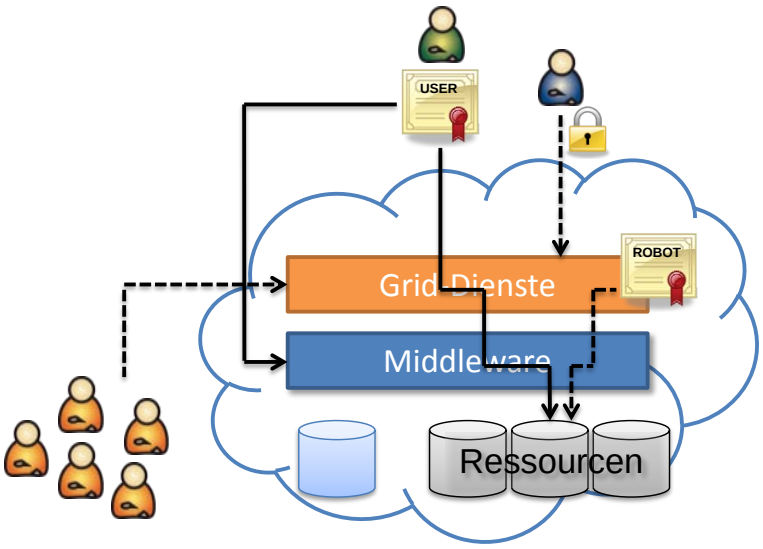

Abbildung 2.1: Schematische Darstellung aller drei Zugangswege zur Gridinfrastruktur betrachtet unter dem Sicherheitsaspekt. Neben der offenen Nutzung (links) findet sich die Nutzung von Dienstzertifikaten (rechts) und die personalisierte Nutzung über Nutzerzertifikate (mitte).

2.1.1 Offene Nutzung

Die offene Nutzung einer Grid-Infrastruktur spielt in einigen Communities dann eine Rolle, wenn bezüglich der allgemeinen Verwendung unkritische Daten jedem zur Verfügung gestellt oder für öffentlichkeitswirksame Demonstrationszwecke genutzt werden sollen. In diesem Fall darf jeder ohne weitere Identitätsprüfung auf die Infrastruktur zugreifen und mit der Infrastruktur arbeiten.

Generell tritt dieser Fall nur ein, wenn keine sensiblen Daten oder Programmaufrufe in der Gridinfrastruktur genutzt werden. Grundsätzlich sind dabei Nutzer anonym und nicht mit den jeweiligen Aktionen in Verbindung zu bringen. Ein Auditing dieser Nutzung ist damit auf keiner Ebene der Architektur möglich.

Aus Sicht der Nutzung ist dies das einfachste, aber mit Abstand unflexibelste Konzept. Ein Nutzer benötigt keinerlei Zugangsberechtigung und es kann von der gesamten Sicherheitsproblematik abstrahiert werden. Nicht anwendbar ist dieses Konzept aber für die alltägliche Arbeit des Forschers, der auf spezielle Daten zugreifen und diese ggf. mit seinen eigenen Programmen analysieren will. Ein Schutz von Ergebnissen und Eingabedaten ist nicht gegeben, eine Individualisierung der Zugriffsrechte nicht vorgesehen.

2.1.2 Dienstezertifikate

Ein Zwischenweg zur relativ einfachen Nutzung von Diensten im Grid-Umfeld stellen die Dienstezertifikate (oder Robot Certificates) dar. Dabei wird auf technischer Ebene von einer durch Zertifikate abgesicherten Infrastruktur ausgegangen. Jedoch ist nicht jeder Nutzer mit einem Zertifikat ausgestattet. Vielmehr können sich die Dienste untereinander ausweisen und damit als Stellvertreter für

den Nutzer agieren. Jeder Dienst wird dazu mit einem Robot-Zertifikat ausgestattet und agiert als zentraler Nutzer innerhalb der Infrastruktur. Dieses Vorgehen setzt für einen einigermaßen sicheren Betrieb des Konzeptes zwei grundlegende Annahmen voraus:

1. Service-Vertrauen: Die miteinander interagierenden Dienste müssen sich uneingeschränkt vertrauen. Insbesondere müssen die Ressourcen-Provider bereit sein, den Zugriff auf die Daten über einen einzigen Nutzer zuzulassen. Dazu wurde in GapSLC-Projekt ein Konzept entwickelt, das mehrstufige Sicherheitslevel bei den Ressourcen-Providern vorsieht, so dass nur in unkritischen Bereichen die Dienstezertifikate genutzt werden, siehe [3]. Dennoch ergeben sich rechtliche Probleme durch die einfache Abstraktion der Nutzeridentität. Da unterhalb der Middleware (der Dienste) nicht sichergestellt werden kann, dass der Nutzer der Dienste einer befugten Nutzergruppe angehört, können oftmals verschiedene rechtliche Vorgaben bei dieser Nutzungsart nicht eingehalten werden[2]. Mechanismen, die dies auf der Dienstebene sicherstellen, sind bisher nicht entwickelt.

2. Auditing durch jeden Dienst: Da der einzelne Nutzer aufgrund der Nutzung eines einzigen Zertifikats für alle Anfragen unterhalb der Nutzerschnittstelle nicht mehr eindeutig zu identifizieren ist, muss diese Schnittstelle ein Auditing der Nutzung und eine Kontrolle der Aktionen des Nutzers erlauben. Meldet sich der Nutzer per Name und Passwort an der Benutzerschnittstelle (Portal, Client) an, so muss jede Aktion verfolgt werden, um später eine lückenlose (und durchaus aufwändige) Zuordnung auf allen Ebenen der Infrastruktur sicher stellen zu können. Bei der gewöhnlich parallelen Nutzung der Infrastruktur wird eine Nachvollziehbarkeit und eindeutige Zuordnung oft unmöglich.

Insgesamt ist dieses Konzept ein erster Ansatz zur sicheren Nutzung von Ressourcen. Viele Community-Grids haben deshalb dieses Konzept in einer ersten Generation der Infrastruktur umgesetzt. Für den prototypischen Einsatz oder die Nutzung im Rahmen wenig sensibler Daten und Anwendungen ist dieses Konzept durchaus handhabbar. Für den produktiven Betrieb in einer Forschungsumgebung mit feingranularen Zugriffsrechten und hohen Datenschutz- und Sicherheitsanforderungen ist es jedoch zu eingeschränkt.

2.1.3 Personalisierte Nutzung

Im Kontext der bisherigen Umsetzung von Grid-Infrastrukturen hat sich die zertifikatsorientierte und personalisierte Umsetzung des Zugangsweges für stärker abgesicherte Datenbestände und Rechenressourcen durchgesetzt. Dies ist nicht zuletzt dadurch begründet, dass viele Middlewares ihre Dienstnutzung durch personalisierte Zertifikate absichern. Dieses Konzept bietet als einziges der hier vorgestellten eine durchgehende Identifikation des Benutzers auf allen Ebenen der Grid-Infrastruktur, wenn die Zertifikate bei jeder Aktion vorgezeigt werden müssen. Anders als bei den vorherigen Konzepten fungiert das Zertifikat in seiner ursprünglichen Funktion als Ausweis des Nutzers. So kann an jedem Dienst die Identität des Nutzers sichergestellt werden. Kombiniert mit Mechanismen der Rechtedelegation erlaubt die Zertifikatsnutzung eine feingranulare Zugriffskontrolle

[2] Aufgrund von Nationalität, lizenzrechtlichen Regelungen und ähnlichen Randbedingungen kann die Nutzung von Ressourcen über ein allen Nutzern gemeinsamen Zugang unerwünscht oder rechtlich problematisch sein. Als Beispiel seien hier die Vertragsbedingungen beim Kauf von US-amerikanischer Hardware genannt, die den Käufer verpflichten zuzusichern, dass keine Nutzer spezieller Nationalitäten auf diesen Ressourcen rechnen. Durch die Abstraktion der Nutzer durch ein einziges Zertifikat ist eine solche Vorgabe nur schwer einzuhalten.

auf verschiedene Funktionalitäten oder Daten. Dazu sind jedoch zusätzliche Informationen notwendig, die gewöhnlich nicht vom Ressourcen-Provider selbst, sondern mit dem Zertifikat verbunden von zentraler Stelle geliefert werden (etwa der Heimeinrichtung des Nutzers, siehe Abschnitt 3.2).

Grundsätzlich ist die personalisierte Nutzung aber auch das am technisch aufwändigsten umzusetzende Konzept. Zugleich stellt es für die Nutzer eine Handhabungshürde dar, da ohne ein entsprechendes Zertifikat keine Aktivitäten im Grid durchgeführt werden können. Die zugehörige Beantragungsphase und der richtige Umgang mit Zertifikaten setzt eine gewisse technische Kenntnis oder Bereitschaft zum Erlernen neuer technischer Konzepte voraus. Bereits die Analyse der Nutzeranforderungen hat gezeigt, dass dies nicht bei jeder Nutzergruppe angenommen werden kann.

Die technische Umsetzung erfolgt gewöhnlicherweise über verschiedene Ansätze der Delegation der Identität. Ein Benutzer stellt dabei eine kurzlebige Kopie seines Zertifikats einem Dienst zur Verfügung, der anschließend im Namen des Nutzers agiert. So kann ein Dienst die Identität erneut an weitere Dienste in der Forschungsumgebung weitergeben. Damit wird ein lückenloses Auditing und die Möglichkeit der Autorisierung ermöglicht.

2.2 Zusammenfassende Klassifikation von Sicherheitsanforderungen

Aus den in Kapitel 1 dargestellten Anforderungen der einzelnen akademischen Community-Grids wird hier eine Übersicht erstellt, die zwei grundlegende Zielsetzungen hat. Einerseits kann anhand mehrerer Communities auf drei verschiedene zentrale Aspekte der Sicherheitsanfordeungen eingegangen werden. Andererseits werden die einzelnen Aspekte qualitativ bezüglich ihrer Wichtigkeit für die verschiedenen Communities dargestellt, siehe Abbildung 2.2. Aus dieser Bandbreite heraus kann sich für neu aufzubauende Community-Grids eine Einordnung der eigenen Sicherheitsinteressen in den Kontext bestehender Realisierungen ergeben. Dies ermöglicht dann die zielgenauere Untersuchung bisheriger Konzepte und Umsetzung zur Adaption in der eigenen Infrastruktur.

Interessanterweise ergibt sich bei der Auswertung der akademischen Infrastrukturen im D-Grid eine große Bandbreite in allen angesprochenen Aspekten: Nutzbarkeit, Rechtemanagement/Datenschutz und Nachvollziehbarkeit der Nutzung.

2.2.1 Nutzung

Bereits die Klassifikation der Zugangswege zu Forschungsinfrastrukturen im vorherigen Abschnitt zeigte, dass es grundsätzlich drei Arten gibt, diese zu nutzen. Dennoch beeinflussen nicht nur die Sicherheitsanforderungen an eine Infrastruktur den technischen und konzeptionellen Aufwand zur Umsetzung. Vielmehr spielt auch die Affinität der Nutzergemeinschaft zu technischen Systemen eine zentrale Rolle. Sind Nutzer den Umgang mit Kommandozeilen-Tools gewöhnt, ist auch die Einstiegsschwelle in stark abgesicherte Systeme geringer. Zudem kann oftmals bei solchen Nutzern ein grundlegendes technisches Verständnis und eine Bereitschaft zur Adaption an neue Technologien vorausgesetzt werden. Umgekehrt verhält es sich bei Nutzern, die ausschließlich als Anwender spezieller Software arbeiten und in ähnlicher Weise ebenfalls in der Forschungsumgebung agieren wollen. Solche Nutzer sind zumeist nur mit grundlegenden Authentifizierungsmaßnahmen wie dem Eingeben eines Nutzernamens und eines Passworts vertraut. Die Beantragung und das sichere Management von Zertifikaten ist für diese Nutzer schwer zu bewältigen und sicherlich ein Grund,

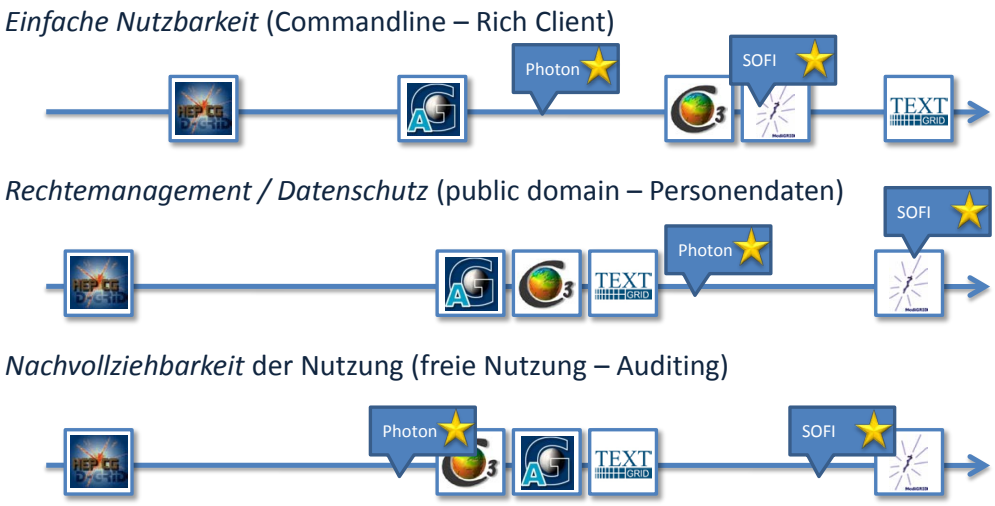

Abbildung 2.2: Übersicht über die Sicherheitsanforderungen der existierenden akademischen Community-Grids und ausgewählter neuer Communities anhand der in diesem Abschnitt aufgezeigten Kriterien.

existierende Infrastrukturen, die solche Vorgänge verlangen, nicht zu nutzen.

Beispielsweise ist die Nutzung von Zertifikaten für technikaffine Hochenergiephysiker im HEP-CG keine Hürde für den Einstieg in und die Nutzung von Grid-Infrastrukturen. Das Arbeiten auf Ebene der Kommandozeile gehört zum täglichen Geschäft. Daher ist auch eine Beschäftigung mit entsprechenden Sicherheitsmechanismen kein Problem.

Anders stellt sich die Situation bereits bei Nutzern der Photonenphysik oder der Klimaforscher dar. Obwohl auch hier vereinzelt technikaffine Nutzer zu finden sind, ist die Mehrzahl auf die einfache Nutzung von Funktionen der Forschungsumgebung über eine graphische Oberfläche eines Internetportals angewiesen. Dabei ist ein Nutzer oftmals nicht bereit, sich in unterliegende Konzepte der Grid-Infrastruktur einzuarbeiten und spezielle Zertifikate für die Nutzung zu beantragen oder zu verwalten (konvertieren, sicher ablegen usw.). Ebenso richtet sich die durch einen Rich-Client erreichbare Forschungsinfrastruktur von TextGrid und die konzipierte Umgebung für SOFI an Nutzer, deren Hauptinteresse die technische Abstraktion von der Infrastruktur und damit auch von der eingesetzten Sicherheitstechnik ist.

Es ergibt sich also eine große Spannbreite von Nutzungsanforderungen an die Sicherheitsinfrastruktur, auf die, abhängig von den durch die Forschungsumgebung angesprochenen Nutzern, eine technische Antwort gefunden werden muss. Dabei ist eine vorherige Aufnahme der Anforderungen an die Sicherheit wichtig. Insgesamt ist aber festzustellen, dass die Vertrautheit mit Technologien zur Sicherung von Infrastrukturen und sicheren Verwaltung von Daten nicht notwendigerweise mit den Sicherheitsanforderungen steigt. Manchmal legen gerade die technisch erfahrenen Nutzergemeinschaften geringen Wert auf Sicherheit, während jene, die viel Unterstützung bei der Handhabung benötigen, auch die höchsten Sicherheitsanforderungen stellen. Damit kann die Komplexität der Umsetzung sicherer technischer Infrastrukturen leicht überproportional steigen.

2.2.2 Rechtemanagement und Datenschutz

Auch im Bereich des Rechtemanagements und des Datenschutzes sind starke Unterschiede festzustellen. Während in einigen Communities Daten, Programme oder sogar Ergebnisse keiner Zugriffsbeschränkung (etwa HEP-CG) unterliegen, benötigen andere Communities zumindest einen rudimentären Zugriffsschutz auf Daten. Im C3Grid werden Daten teilweise frei zur Verfügung gestellt, es ist jedoch oftmals eine Registrierung zur Nutzung der Daten erforderlich. Der Zugriff auf Ergebnisse wird dabei unter Umständen restriktiver gesehen. So sollen dort Ergebnisse für einen Nutzer personalisiert abgelegt werden, ohne Zugriffsmöglichkeit von anderen Nutzern. Dennoch ist es dort etwa möglich, dass ein Nutzer seine Daten und Ergebnisse der Allgemeinheit zur Verfügung stellt. Ähnliche Anforderungen ergeben sich auch bei AstroGrid-D und TextGrid. In der Forschungsumgebung von MediGrid hingegen stellt der Datenschutz und das Rechtemanagement eine sehr zentrale und wichtige Anforderung dar. Da dort abgelegte Daten meist patientenbezogen sind, muss Datenschutz mit höchster Priorität betrieben werden. Dies setzt unter anderem Möglichkeiten zur Anonymisierung, Pseudonymisierung und zur Verschlüsselung voraus, die jeder Speicherung, Bearbeitung und jedem Transfer vorausgehen müssen. So ergeben sich Anforderungen oft auch automatisch aus gesetzlichen Regelungen, die bei der Ablage von personenbezogenen Daten (medizinischer oder statistischer Art) grundsätzlich eingehalten werden müssen.

2.2.3 Nachverfolgbarkeit

Im Gegensatz zu den Anforderungen der Nutzung einer Grid-Infrastruktur, hängen die Anforderungen der Nachvollziehbarkeit weitgehend mit den Anforderungen zum Datenschutz und Rechtemanagement zusammen. Communities, in denen der Datenschutz eine große Rolle spielt, legen konsequenter Weise auch auf die Nachverfolgbarkeit der Nutzung großen Wert.

So gehen bei HEP-CG die Anforderungen bezüglich der Nachvollziehbarkeit nicht über das Logging des Zugriffs auf Datensätze und der Nutzung von Ressourcen hinaus. Oftmals bestehen bei den frei verfügbaren Daten nicht einmal diese Anforderungen. Bei den Projekten AstroGrid-D, C3Grid und TextGrid bestehen die Anforderungen, dass jeder Ressourcenanbieter die Nutzung seiner Ressourcen nachvollziehen kann. Bei MediGrid hingegen erfordern die stark ausgeprägten Datenschutzrichtlinien ein regelmäßiges Auditing der Sicherheitsrichtlinien und der durchgeführten Datennutzung.

Kapitel 3

Einordnung der Lösungsansätze

An die vorherige Betrachtung von Zugangswegen in und Anforderungen an Grid-Infrastrukturen und virtuellen Forschungsumgebungen schließt hier nun ein Überblick und eine Klassifizierung der in den akademischen Community-Grids eingesetzten technologischen Konzepte an. Dabei wird strukturell zwischen Authentifizierung, Autorisierung und technischer Umsetzung unterschieden. Im ersten Abschnitt werden Konzepte dargestellt, die eine Feststellung der Nutzeridentität erlauben. Danach wird die Umsetzung von Nutzerberechtigungen im Grid betrachtet. Schließlich soll kurz auf einige Technologien eingegangen werden, die im Grid Verwendung finden.

3.1 Konzepte zur Authentifizierung

Die Grid-Infrastrukturen der akademischen Community-Grids wurden in ihrer ersten Phase grundsätzlich auf dem Konzept der zertifikatsbasierten Authentifizierung aufgebaut. Diese Festlegung liegt in den zur Projektgründung vorherrschenden drei Grid-Middlewarerealisierungen Globus, Unicore und gLite begründet. Alle drei Middlewares gehen von einer Identifizierung der Nutzer über Zertifikate aus. Dabei fungiert ein Zertifikat, ausgestellt von einer vertrauenswürdigen Organisation (im Kontext von D-Grid der DFN Verein und die GridKa CA), als ein digitaler, den Nutzer eindeutig identifizierender Ausweis. Ein solches Zertifikat muss bei der entsprechenden Autorität beantragt werden und gilt daraufhin ein Jahr lang. Eine Verlängerung ist durch Vorzeigen des alten Zertifikats innerhalb der Frist jederzeit möglich. Die Erstellung der Zertifikate und die anschließende Nutzung als digitales Ausweisdokument basiert auf dem Public Key Verfahren. Ausgestattet mit einem solchen Zertifikat kann der Nutzer an Middlewaredienste der drei eingesetzten Middlewares herantreten, sich ihnen gegenüber eindeutig identifizieren und sie nutzen. Die Identifizierung des Nutzers gegenüber der CA erfolgt über eine Verifikation des vorgelegten Zertifikats durch die ausstellende Einrichtung (Certificate Authority, CA), siehe Abbildung 3.1.

Die Nutzung von Zertifikaten kann technisch in zwei Klassen unterteilt werden, die auch zuvor in Kapitel 2 bereits dargestellt wurden. Im ersten Fall muss der Nutzer direkt mit einem Zertifikat ausgestattet sein. Im zweiten Falle wird im Namen des Nutzers ein Zertifikat verwaltet oder sogar erstellt oder auf ein gemeinsames Zertifikat für alle Nutzer zurückgegriffen.

Direkte Zertifikatsnutzung: In dieser Variante verwaltet der Nutzer sein Zertifikat persönlich in seiner Domäne und ist für den Schutz verantwortlich. Im Grid-Kontext ist dies aufgrund

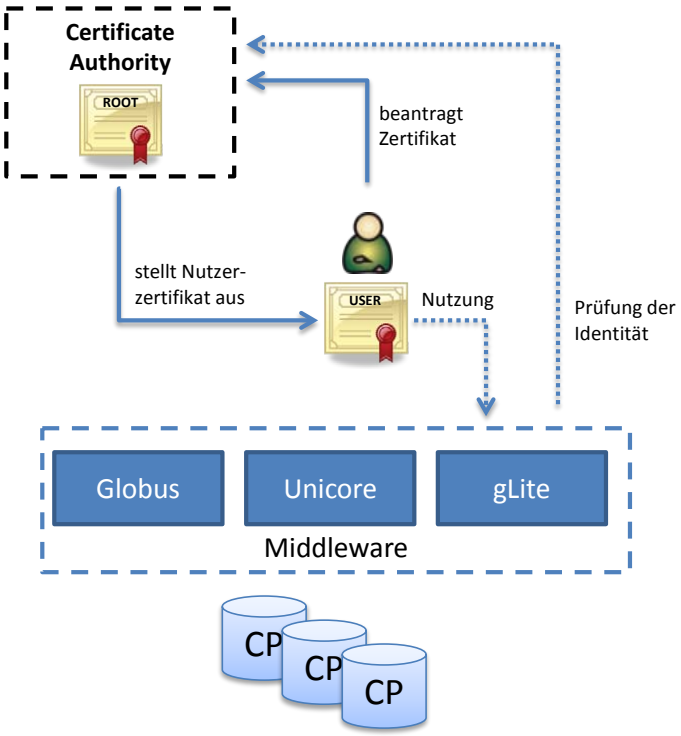

Abbildung 3.1: Schematische Darstellung der Public Key Infrastructure (PKI) und ihrer Nutzung in der Grid-Infrastruktur.

rechtlicher Gegebenheiten die verbreitete Variante. Entsprechend der Richtlinien der meisten Certificate Authorities muss er für die sichere Aufbewahrung seines Zertifikates und des zugeordneten privaten Schlüssels selbst sorgen. Insbesondere ist der Nutzer nicht befugt, diesen Schlüssel anderen zugänglich zu machen, da andernfalls jeder die Identität des Nutzers annehmen kann.

Da eine Grid-Infrastruktur gewöhnlich einer Service-orientierten Architektur folgt, also verschiedene Dienste an vielen Orten und weit verteilt ausgeführt werden, ist der Nutzer gewöhnlich verpflichtet, sein Zertifikat bei allen von ihm genutzten Diensten vorzuzeigen, um dort identifiziert werden zu können. Da dies für den Nutzer extrem aufwändig ist, implementieren alle Middlewares und auch viele Forschungsumgebungen mit höherwertigen Dienstangeboten den Mechanismus einer Identitätsdelegation. Bei dieser Delegation kann der Nutzer einem Mehrwertdienst erlauben, die Nutzeridentität anzunehmen und damit in seinem Namen einen weiteren Dienst zu nutzen. Dafür ist es jedoch notwendig, dass der Mehrwertdienst ebenso wie der Nutzer über ein Zertifikat und den privaten Schlüssel des Nutzers verfügt. Da die Herausgabe des Originalzertifikats problematisch ist, wurde das Konzept der Vertreter-Zertifikate (oder Proxy-Zertifikate) entwickelt. Hier wird vom Nutzer ein nur für kurze Zeit gültiges Zertifikat vom Originalzertifikat abgeleitet und an den Mehrwertdienst weitergegeben, der damit, für begrenzte Zeit die Identität des Nutzers übernehmen kann.

Die Nutzung dieses Konzeptes setzt ein gewisses Verständnis der zugrunde liegenden Prozesse durch den Nutzer voraus und stellt diesen vor die Aufgabe, sein originales Zertifikat sicher aufzubewahren. Aus technischer Sicht kommt oftmals noch die Notwendigkeit hinzu, ein solches Zertifikat vor der Nutzung durch Konvertierung in das von der Middleware oder der

Forschungsumgebung vorausgesetzte Format zu bringen. Dies stellt für viele nicht Technik-affine Benutzer eine relativ große Hürde dar.

Technisch betrachtet ist dieses Konzept in allen Middlewares integriert und weitgehend umgesetzt. Bei der Entwicklung entsprechender Dienste oberhalb der Middleware sind entsprechende Anpassungen vorzunehmen, die einen gewissen Aufwand zur Einarbeitung in die Problematik der Zertifikatsdelegation erfordern. Jedoch werden bereits einige Standardwege angeboten, die dieses Problem lösen und in die Realisierung eines Dienstes einbezogen werden können.

Kapselung der Zertifikatsnutzung: Ein anderes Konzept zur Nutzerauthentifizierung in Grid-Infrastrukturen baut auf dem vorherigen Prinzip auf, verringert aber die Einstiegshürde für den Nutzer. Dafür sind jedoch gewisse Einschränkungen der Anforderungen auf Seiten der Betreiber der Infrastruktur notwendig. Alternativ kann auch ein entsprechendes Vetrauensverhältnis zwischen Nutzern und Betreibern von Ressourcen und Diensten innerhalb der Forschungsumgebung die Voraussetzung schaffen.

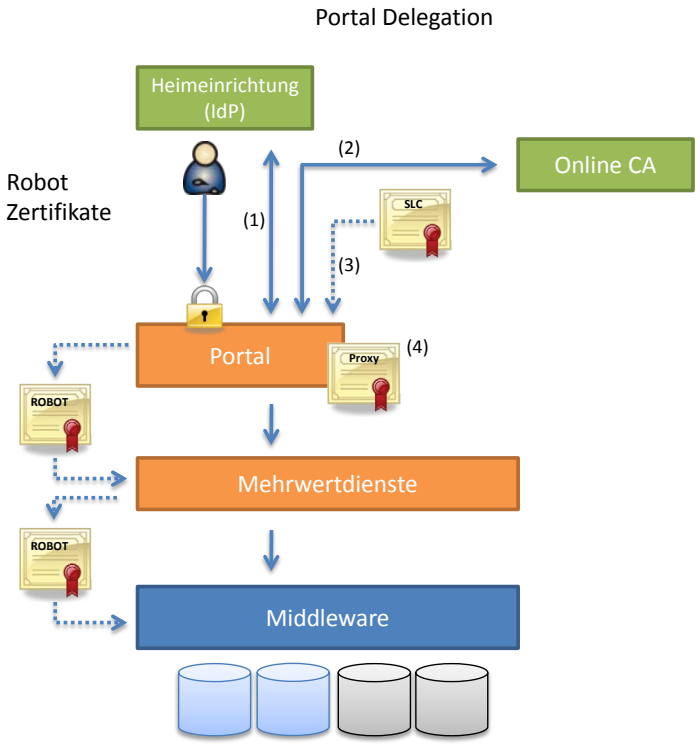

Abbildung 3.2: Schematische Darstellung der Nutzung von Robot-Zertifikaten und Portal Delegation in Grid-Infrastrukturen.

Die einfachste Variante ist die Nutzung eines einzigen Zertifikats auf Dienstebene, ein sogenanntes Robot-Zertifikat, siehe Abbildung 3.2. Damit ist der Nutzer von der Verwendung von Zertifikaten befreit. Er meldet sich per Nutzername und Passwort bei einer Applikation, einem Dienst oder meistens einem Portal an. Diese Softwarekomponente gilt als Einstiegspunkt in die Nutzung der weiteren Griddienste und übernimmt die Überwachung der Nutzeraktivität. Anschließend führt sie im Auftrag des Nutzers, aber mit einem eigenen, für alle Nutzer gleichen Zertifikat, Aufrufe anderer Dienste durch. Dabei geht für nachfolgende Dienste die Zuordnung zu einem speziellen Nutzer verloren. Es muss ein vollständiges Vertrauensverhältnis zwischen den kommunizierenden Diensten herrschen. Weitere Nutzungen anderer Dienste

führt der aufgerufene Dienst wiederum mit seinem eigenen Zertifikat aus. So reißt auch die Kette zur Nachvollziehbarkeit zum Einstiegsdienst ab. Technisch ist das Konzept der Robot-Zertifikate einfacher zu realisieren als das Konzept der Delegation einer Nutzeridentität. Das Vorgehen bringt allerdings auch einige Nachteile und rechtliche Unklarheiten mit sich, die bisher nicht abschließend gelöst werden konnten. Wie bereits in Kapitel 2 dargestellt, kann durch die Einschränkung der Nachvollziehbarkeit keine sichere Aussage über die Identität des Nutzers und dessen Berechtigung zur Verwendung von Ressourcen gemacht werden. Bisherige Umsetzungen haben in prototypischem Status (z.B. C3Grid, TextGrid) auf Nutzerzertifikate zurückgegriffen. Dabei setzt sich aber der Eigentümer des Zertifikats dem persönlichen Risiko des Missbrauchs aus. Zudem trägt er allein die gesamte Verantwortung für die Nutzung des Zertifikats. Inzwischen gibt es vom DFN-Verein eine offizielle Policy zum Einsatz von Robot-Zertifikaten und auch eine Möglichkeit, solche Zertifikate Ausstellen zu lassen[1]. Ein solches Zertifikat ist nicht mehr an eine Person gebunden und kann laut DFN für die „Automatisierung von Aufgaben im Grid“ eingesetzt werden. Trotzdem wird die Policy in D-Grid im Allgemeinen bisher nicht anerkannt, da Rechenprovider grundsätzlich den oben angesprochenen gesetzlichen Vorgaben folgen müssen. So ist ein Einsatz von Robot-Zertifikaten nur in sehr eingeschränkten und abgeschlossenen Umgebungen erfolgt.

Eine weitere konzeptionelle Möglichkeit zur einfacheren Nutzung von Zertifikaten durch den Nutzer besteht in der sogenannten *Portal Delegation*, siehe auch Abbildung 3.2. Dabei übernimmt das Portal stellvertretend für den Nutzer die Zertifikatsbeantragung von einer Online Certificate Authority sowie das Ableiten eines Proxyzertifikats für die Nutzung im Grid. Der Nutzer meldet sich dabei wie üblich per Nutzername beim Portal an und wird von diesem zu seiner Heimateinrichtung zur Authentifikation weitergeleitet (1). Nach erfolgreicher Identifikation des Nutzers, erzeugt das Portal ein Schlüsselpaar und eine zugehörige Zertifikatsanforderung an eine Online-CA (2). Wenn diese von dem Nutzer freigegeben ist, bezieht das Portal im Namen des Nutzers ein kurzlebiges Zertifikat (3), das temporär gehalten und zur Ableitung eines Proxy-Zertifikats (4) genutzt wird. Mit diesem arbeitet das Portal im Auftrag des Nutzers weiter. Ein langfristiges Abspeichern des Schlüsselmaterials zum beantragten SLC ist dem Portal nicht erlaubt. Damit ist für den Nutzer die Verwendung des Zertifikats weitgehend transparent. Der Mechanismus setzt jedoch voraus, dass Ressourcen und Dienste einerseits der Online-CA und andererseits dem Portal vertrauen. Eine ausführliche Darstellung, auch bezüglich technischer Konzepte und Umsetzungen, findet sich in einem Überblick des GapSLC-Projekts [4].

3.2 Konzepte zur Autorisierung

Unter der Autorisierung eines Nutzers wird die Festlegung der Rechte dieses Nutzers innerhalb der Infrastruktur verstanden. Dies spielt insbesondere dann eine Rolle, wenn hohe Datenschutzanforderungen gestellt werden.

In vielen Realisierungen der akademischen Community-Grids spielt eine sehr feingranulare Unterscheidung der Nutzerrechte auf Daten- und Rechenressourcen eine nachgeordnete Rolle. Hier reicht es meist aus, die Nutzer einzeln zu identifizieren und auf eine lokale Nutzerkennung auf den jeweiligen Ressourcen innerhalb der Infrastruktur abzubilden (z.B. C3Grid, AstroGrid-D, HEP-CG, TextGrid). Für andere Communities spielt jedoch, wie in den Kapiteln 1 und 2 dargestellt, der

[1] `https://www.pki.dfn.de/grid/robot-zertifikate/`

Datenschutz und die feingranulare Unterscheidung der Zugriffsrechte eine vordringliche Rolle. Deshalb werden in diesem Abschnitt einige Varianten zur konzeptionellen Umsetzung von Autorisierungsmöglichkeiten dargestellt, die beide Fälle abdecken. Bereits hier ist anzumerken, dass bisher keine Community den zweiten Fall durchgängig realisiert hat.

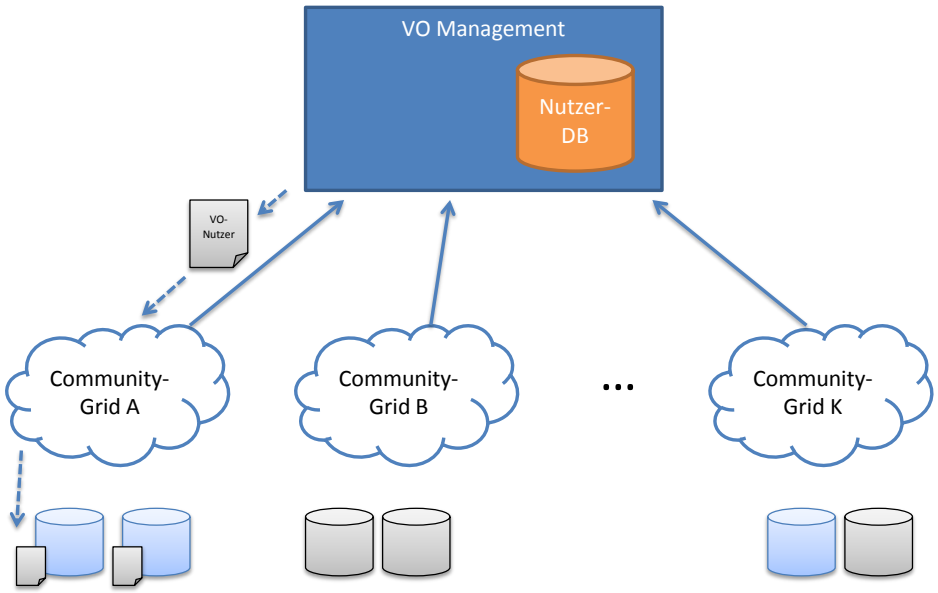

Abbildung 3.3: Schematische Darstellung eines VO-Managementdienstes mit verschiedenen verwalteten Community-Grids.

Globales VO Management: Im Kontext des Hochleistungsrechnens auf Clustern ist es üblich, dass jeder Nutzer im lokalen Umfeld einen individuellen Zugang besitzt, der auf der genutzten Ressource auf eine individuelle Umgebung (Home-Verzeichnis) abgebildet wird. In dieser Umgebung kann der Nutzer entsprechend den ihm zugewiesenen Rechten Programme ausführen, Daten ablegen und verarbeiten. Je nach Rechtevergabe kann kein anderer Benutzer die Daten oder Programme dieses Bereiches einsehen. Ebenso verhält es sich mit vielen Datenspeichern. Dort kann ein Nutzer, durch individuelle Rechte ausgestattet, auf eine Untermenge der verfügbaren Daten zugreifen.

Die Einbindung solcher Ressourcen in eine Grid-Infrastruktur mit der Anforderung, dass jeder Nutzer auf jeder Ressource eine individuelle Umgebung besitzen soll, bringt die Schwierigkeit der gleichzeitigen Verwaltung der Nutzeraccounts auf den verteilten Ressourcen mit sich. Jedoch kann mit diesem Verfahren sehr einfach eine individualisierte Nutzung verschiedener Ressourcen und Daten sowie die nutzerbezogene Berechtigungsverwaltung auf Ressourcenebene sichergestellt werden.

Um dies umzusetzen, wurde in vielen Realisierungen der Community-Grids das Konzept der *Virtuellen Organisationen* (VOs) sowie die zentrale Verwaltung und automatische Abbildung von Nutzern auf die in der Infrastruktur vorhandenen Ressourcen adaptiert, siehe Abbildung 3.3. In einer VO werden die Nutzer einer Community zusammengefasst. Ihnen wird ein Nutzername zugeordnet und dieser mit dem Identifikationsnamen (Distinguished Name - DN) des persönlichen Zertifikats verbunden. Die VO-bezogenen Daten werden in einer zentralen Datenbank abgelegt und regelmäßig von den Ressourcen abgerufen, die Dienste für

die betreffende VO betreiben. Auf Ressourcenebene werden daraus Nutzeraccounts angelegt. Tritt nun ein Nutzer mit seinem (delegierten) Zertifikat an die spezielle Ressource heran, kann auf Basis des DN und des vorhandenen Nutzeraccount eine individuelle Umgebung mit festgelegten Rechten für den Nutzer zur Verfügung gestellt werden.

Beschreibung und Durchsetzung individueller Rechte: Während der vorherige Ansatz zwar grundsätzlich eine individuelle Festlegung der Rechte eines Nutzers auf jeder Ressource erlaubt, gibt es keinerlei Regelung und auch keinen Mechanismus, dies einheitlich umzusetzen. Durch die verschiedenen lokalen administrativen Domänen der Ressourcen ist es faktisch jedem Administrator einer Ressource überlassen, welche Rechte ein Nutzer erhält und welche nicht. Zwar kann man sich Community-intern auf einheitliche Regeln einigen, dennoch erfordert dies an jeder Stelle Konfigurationsaufwand.

Um eine projektweite und feingranulare Unterscheidung zwischen Gruppen und Personenrechten innerhalb der gesamten Community durchzuführen, kann man Rechte direkt an die Authentifizierungsinformationen binden und damit durch eine automatische Entscheidung über Rechte eines Nutzers und eine damit verbundene Umsetzung auf Ebene der Ressource sicherstellen. Dies setzt lediglich eine externe Verwaltung der Nutzerrechte (zentral oder auch dezentral, etwa in der Heimateinrichtung des Nutzer) voraus und die Möglichkeit die Nutzerrechte zu beschreiben. Dafür ist vom OASIS Security Services Technical Committee die sogenannte Security Assertion Markup Language (SAML) entwickelt worden, die eine Beschreibung von Attributen und Autorisierungskriterien zusätzlich zu einer Identität (etwa gegeben durch ein Zertifikat) erlaubt. Hier können dann in einem XML-Dialekt sehr feingranulare Zugriffsrechte auf Funktionen, Schnittstellen, Programmteile oder Daten formuliert werden.

Eng verbunden mit der Frage der Autorisierung des Zugriffs auf verschiedene Dienstleistungen in Grid-Infrastrukturen ist die Frage der Nutzung lizensierter Inhalte. So wird im Kontext der allermeisten akademischen Forschungsumgebungen von einer freien Nutzung aller Software und Daten ausgegangen. Bereits die Anforderungen in Kapitel 1 und die Klassifikation der Nutzung in Kapitel 2 haben jedoch gezeigt, dass es durchaus einen Bedarf für den Schutz und nur lizensierten Zugang zu Inhalten gibt. Leider sind in diesem Zusammenhang noch keine ausgereiften Konzepte im Kontext der betrachteten Projekte entstanden.

3.3 Technische Umsetzung

Technisch verwirklicht sind in den akademischen Community-Grids Authentifizierungsmechanismen. Wie bereits zuvor dargestellt reichen diese Ansätze für sehr viele Anwendungsfälle – in Kombination mit VO-Management und Autorisierung auf Ressourcenebene – aus, um eine sichere Nutzung zu gewährleisten. Da man sich im D-Grid initial für die Nutzung von Zertifikaten entschieden hat, sind Lösungen entwickelt und genutzt worden, die vor allem die in Abschnitt 3.1 dargestellten Konzepte der Zertifikatsdelegation umsetzen.

Die Zertifikatsdelegation kann jedoch aus zwei unterschiedlichen Blickwinkeln betrachtet werden. Einerseits stellt sich die Frage der Delegation von Identitäten innerhalb einer technischen Umgebung. Hier können recht komplexe Mechanismen eingesetzt werden, da eine Benutzeroberfläche oftmals technische Details vor dem Benutzer verbirgt. Andererseits besteht die Notwendigkeit der Zertifikatsverwaltung durch den Nutzer. Selbst die Nutzung einer weitgehend abstrahierenden Oberfläche

(Portal oder User Interface, UI) erfordert die Identifikation des Nutzers gegenüber dem Portal bzw. UI und schließlich eine Delegation der Nutzeridentität an die vom Nutzer verwendete Applikation.

Beide Aspekte werden mit einigen technischen Konzepten in diesem Abschnitt besprochen. Neben zwei Mechanismen zur Delegation von Zertifikaten (MyProxy und Globus Toolkit Delegation Service) wird in einem zweiten Abschnitt auf die Anmeldung und den Zugang zu Grid-Portalen eingegangen.

3.3.1 Delegation von Zertifikaten

Die Globus Middleware in der (inzwischen nicht mehr unterstützten) Version 4.x ist Bestandteil aller Projekte (nur im HEP-CG wird die gLite Middleware eingesetzt) und stellt mit dem Delegation Service und MyProxy zwei Möglichkeiten zur Delegation von Zertifikaten zur Verfügung. MyProxy kann jedoch unabhängig von Globus verwendet werden, ersetzt in der neuen Version Globus 5 den Delegation Service vollständig. Im Folgenden werden beide Konzepte erläutert.

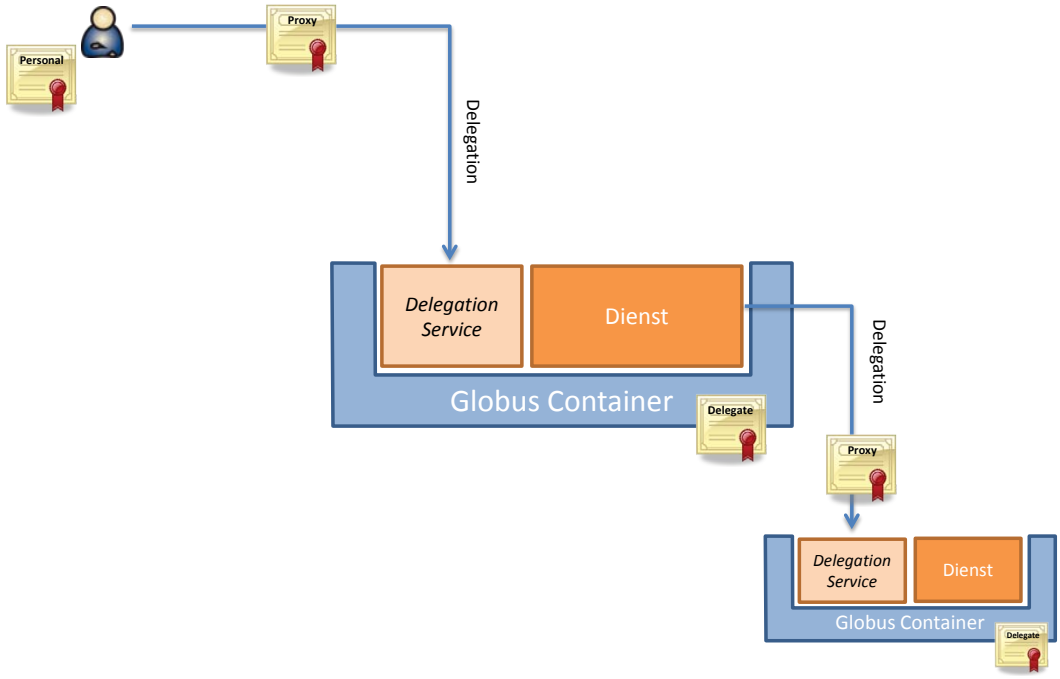

Abbildung 3.4: Schematische Darstellung der Zertifikatsdelegationskette entsprechend der Umsetzung im Globus Toolkit 4.

Globus Delegation: Das Konzept des Globus Delegation Service geht von einer einheitlichen Laufzeitumgebung für die ihn nutzenden Grid-Dienste aus, dem Globus Container. Globus bietet ein dem WSRF-Standard entsprechendes Framework an, um Stateful Web Services für den Container zu implementieren und zu betreiben. Standardmäßig wird der Delegation Service mit dem Globus-Container ausgeliefert. Dieser erlaubt es ein Proxy-Zertifikat (also eine sehr kurzlebige Ableitung des Nutzerzertifikats) an den Globus-Container zu delegieren, siehe Abbildung 3.4. Dabei wird einem delegierten Zertifikat eine Web Service-Instanz des Delegation Services zugeordnet. Diese Instanz verfügt über eine sogenannte Endpunktadresse (EPR

- Endpoint Reference), über die auf Verwaltungsfunktionen zugegriffen werden kann. Diese Funktionen erlauben es, das Zertifikat zu verlängern, zu zerstören oder abzurufen. Ist die EPR einem Dienst im Globus-Container bekannt, so kann dieser das Zertifikat abrufen und damit im Namen des Nutzers auftreten. Wichtig ist zu erwähnen, dass dies nur Diensten innerhalb des Containers erlaubt ist. Externe Dienste haben, selbst bei Kenntnis des EPR, keinen Zugriff auf das delegierte Zertifikat. Um also die Delegation einer Nutzeridentität zwischen mehreren Diensten der Infrastruktur durchzuführen, können mehrere Delegationsschritte nötig sein. Dies gilt insbesondere dann, wenn zwei Dienste nicht in demselben Container, sondern räumlich verteilt betrieben werden. Erfolgreiche Umsetzungen dieses Konzeptes in der Infrastruktur finden sich in MediGrid und C3Grid. Grundsätzlich basiert aber jedes Projekt, das Globus als Middleware einsetzt, auf diesem Delegationsprinzip. Auch der im Globus-Container betriebene WS-GRAM-Dienst zur Einreichung von Aufgaben über die Low-Level-Schnittstelle der Middleware nutzt dieses Prinzip zur Delegation der Nutzeridentität zu den jeweiligen Ressourcen.

MyProxy: Das Konzept von MyProxy lässt sich weitgehend als ein Zertifikatsspeicher mit der Funktion einer Certificate Authority (CA) darstellen. Das eigentliche Einsatzgebiet ist die ortsunabhängige Proxy-Generierung durch den Nutzer und nicht die Delegation von Zertifikaten. Mit einem in MyProxy abgelegten Zertifikat kann der Nutzer überall und jederzeit ein Proxyzertifikat ableiten, um auf Gridressourcen zuzugreifen. Dafür ist standardmäßig vorgesehen, dass der Nutzer sein Zertifikat (Schlüsselpaar) in MyProxy ablegt und dies durch ein Passwort schützt. Mit Hilfe dieses Passwortes kann er jederzeit ein Proxyzertifikat ableiten oder auf das Zertifikat selbst zugreifen.

Diese Funktionalität kann jedoch auch für die Delegation von Zertifikaten innerhalb einer Infrastruktur genutzt werden. Dazu wird ein Proxy-Zertifikat in dem zentralen Speicher abgelegt und mit einem Passwort gesichert. Der Nutzer (oder delegierende Dienst) gibt dazu seine Zugangsdaten für das Ableiten eines neuen Proxy-Zertifikates aus MyProxy an einen Dienst weiter, der dann selbstständig das abgelegte Proxy-Zertifikat bezieht oder ableitet, wenn es für Aufgaben im Namen des Nutzer benötigt wird. Selbstverständlich setzt dies ein Vertrauensverhältnis zwischen dem Nutzer und dem das Zertifikat nutzenden Dienst voraus. Da dafür nur Proxyzertifikate genutzt werden sollen, stellt die geringe Laufzeit des gespeicherten Zertifikates sicher, dass die Identität des Nutzers im schlimmsten Fall nur für eine sehr begrenzte Zeit gestohlen werden kann.

3.3.2 Absicherung der Zugangswege

Die im letzten Abschnitt beschriebene technische Umsetzung von Zertifikatsdelegation setzt natürlich das Vorhandensein und das Management eines Nutzerzertifikats voraus, von dem schließlich ein Proxy-Zertifikat abgeleitet und als kurzlebiger Identitätsnachweis durch die Infrastruktur gereicht werden kann. Dabei ist es gewöhnlich notwendig – und dies bestätigen auch die Ergebnisse des GapSLC-Projektes[2] im D-Grid – den Nutzer zu unterstützen, um eine einfache Handhabung und damit eine gute Nutzbarkeit der Infrastrukturen sicherzustellen. Die Überwindung der Einstiegsschwelle ist daher ein zentraler Punkt der folgenden technischen Betrachtung. Wie gelingt es, Nutzer die Handhabung von persönlichen Zertifikaten im Zusammenhang mit Portalen als Einstiegspunkt zu Grid-Infrastrukturen zu erleichtern?

[2] `http://gap-slc.awi.de/`

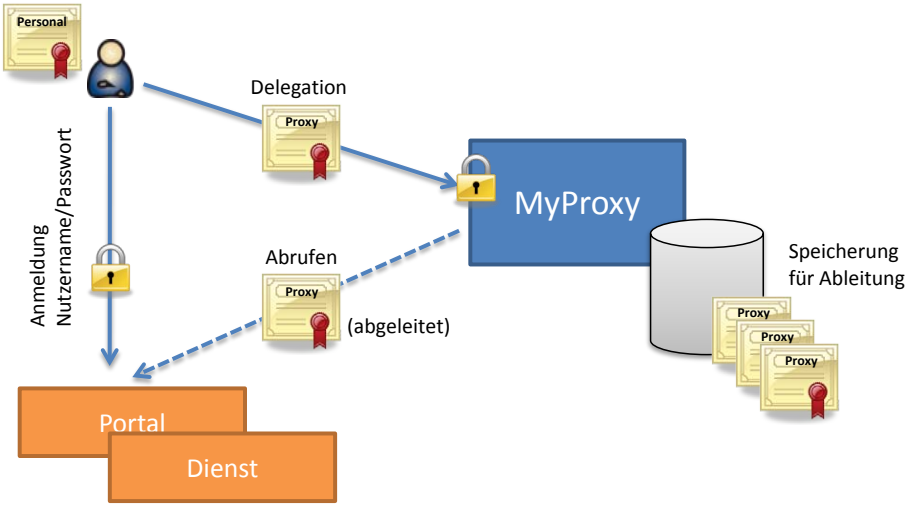

Abbildung 3.5: Schematische Darstellung der technischen Funktionsweise des MyProxy-Dienstes zur Zertifikatsdelegation.

In diesem Kontext soll auf eine Lösung aus dem GapSLC-Projekt aus D-Grid eingegangen werden. Das Tool gPut bietet hier einen sehr einfachen Weg, mit Nutzerzertifikaten über ein Portal im Grid zu arbeiten. Dieses Tool wird verstärkt im MediGRID-Projekt eingesetzt. Abschließend wird noch kurz auf Drittanbieterlösungen eingegangen, die eine dezentrale Authentifizierung und Autorisierung von Nutzern erlauben und gut mit Konzepten zur Kapselung der Zertifikatsnutzung (im Portal) angewendet werden können.

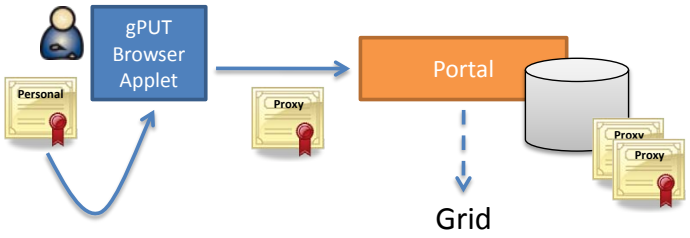

Abbildung 3.6: Schematische Darstellung der Funktionsweise des Grid Proxy Upload Tool gPUT.

Ziel des GapSLC-Ansatzes ist es die Verwaltung und Nutzung von Zertifikaten in Verbindung mit Portalen einfacher zu gestalten. Neben der Beantragung eines Zertifikates sind nämlich zusätzlich vom Nutzer verschiedene Low-Level-Methoden anzuwenden, um sein Zertifikat (1) in das richtige Format zu bringen, (2) die Ableitung eines Grid-Proxy-Zertifikats vorzunehmen und es (3) schließlich zum Portal hochzuladen. All diese Aufgaben übernimmt bei gPUT ein auf Nutzerseite im Browser laufendes Applet, siehe Abbildung 3.6. Nach dem Hochladen eines Grid-Proxy-Zertifikats im richtigen Format, kann im Portal eines der weiter oben beschriebenen Verfahren zur Kapselung der Zertifikatsnutzung angewendet werden. Etwa können die hochgeladenen (und sehr kurzlebigen) Zertifikate in einer Datenbank abgelegt und bei jeder Aufgabe des Nutzers zur Delegation der Nutzeridentität innerhalb der Gridinfrastruktur verwendet werden.

Eine weitere Möglichkeit der Absicherung von Nutzeridentitäten und sogar zum Verzicht auf Nutzer-

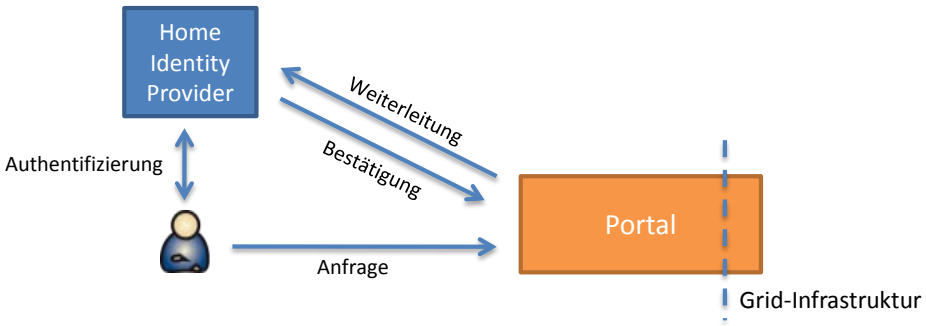

Abbildung 3.7: Grobe Skizze der Funktionsweise eines allgemeinen Single-Sign-On Mechanismus.

zertifikate bieten sogenannte Single-Sign-On-Lösungen. Prominente Vertreter sind etwa OpenID[3] oder Shibboleth[4]. Beide Ansätze basieren auf dem gleichen Grundprinzip, das in Abbildung 3.7 dargestellt ist. Der Nutzer möchte sich dabei am Portal anmelden. Damit er keine Anmeldedaten bei dem Anbieter selbst lagern muss und der Anbieter schließlich die Identität des Nutzers in seinem Auftrage bestätigen kann (single sign on, einmal anmelden), meldet sich der Nutzer lediglich mit seinem Nutzernamen seiner Heimateinrichtung inklusive einem die Einrichtung identifizierenden Bezeichner an. Aufgrund dieses Bezeichners ist das Portal in der Lage, die Anmeldung an den Identity-Provider der Heimateinrichtung weiterzuleiten. Nun meldet sich der Nutzer mit seinem eigenen Passwort bei der Heimateinrichtung an, die daraufhin dem Portal (oder anfragenden Dienst) die Identität des Nutzers bestätigt. Zusätzlich besteht sogar die Möglichkeit Autorisierungsinformationen mitzuliefern. Damit ist der Nutzer gegenüber dem Portal (oder Dienst) identifiziert. Wendet man dieses Prinzip als Einstieg zur Gridinfrastruktur an, so kann nun im Portal ein Zertifikat für den Nutzer generiert werden, mittels dessen die Identität des Nutzers innerhalb der Infrastruktur delegiert werden kann.

[3] http://openid.net/
[4] http://shibboleth.internet2.edu/

Literaturverzeichnis

[1] Rapp A., Grimme, C., Enke, H. (Editoren), Deliverable 2.1.1 Community - Überblick / Report, WissGrid, 2009.

[2] Schlünzen F., Agapov, I. (Editoren), Deliverable 2.1.5 Evaluation und Dokumentation existierender Architekturkonzepte, WissGrid, 2011.

[3] J. Falkner, O. Strauß, A. Weisbecker, S. E. Funk, P. Gietz, M. Haase (Editoren), Prototypische Umsetzung des Konzepts für die Nutzung von Robot-Zertifikaten, 2011, `http://gap-slc.awi.de/documents/GapSLC_D5-2_v1.0.pdf`

[4] Stefan Pinkernell, Einsatz von Portal Delegation und SAML Assertions bei der Authentifizierung und Autorisierung, 2011, `http://gap-slc.awi.de/documents/portalDelegation-1.0.pdf`