Gap-SLC

Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids

Konzeption für die Nutzung spezifischer Anwendungen durch anonyme Nutzer unter Berücksichtigung der Anforderungen aus den Communities

– Task 5, Deliverable D5-1 –

– Förderkennzeichen 01IG09003B –

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

Fraunhofer IAO

AWI

UNIVERSITÄTSMEDIZIN GÖTTINGEN : UMG

DAASI International

Date	**30.09.2009**
Version	**1.0**
Type	**Deliverable**
Status	**Internal Review**
Authors	**J. Falkner, A. Weisbecker, Martin Haase, Peter Gietz, Stefan Funk, Frank Dickmann, Bernadette Fritzsch**

Inhaltsverzeichnis

1 Ausgangssituation

Es gibt in D-Grid eine wachsende Zahl an Anwendungen, die für eine sehr breite Nutzerschaft schnell und unkompliziert zur Verfügung stehen sollen. Sichere Authentifizierungsverfahren wie GridShib und PKI sind hierbei aufgrund des nutzerseitigen Aufwands bzw. des Aufwands bei der Nutzerorganisation, ein massives Hindernis. Der Aufwand entsteht dabei zum einen durch den Beantragungsprozess für PKI-Zertifikate, durch erforderliche Zertifikatskonvertierungen, die Erzeugung und Verwaltung von Proxy-Zertifikaten sowie zum anderen durch den Betrieb von Registration Authorities (bei PKI) oder Identity Providern (IdP, bei Shibboleth).

Umfragen in den D-Grid Communities TextGrid und MediGRID/Services@MediGRID haben ergeben, dass sich Anwendungsentwickler und Endnutzer einfachere Methoden der Zugangssicherung wünschen, die den Endnutzer, bzw. dessen Heimatorganisation, vom Registrierungs- und Betriebsaufwand in Verbindung mit den im Moment gängigen Authentifizierungssystemen entlasten. Gegenwärtig werden viele Grid-Anwendungen im D-Grid als Software-as-a-Service zur Verfügung gestellt. Die produktiven Endnutzer bleiben jedoch oftmals aus, da die Registrierung und Authentifizierung für diese Endnutzer zu aufwändig und zu schwierig ist.

Eine Abstufung von Sicherheitsbereichen im D-Grid wäre daher sinnvoll, um für Anwendungen mit geringeren Sicherheits- und Datenschutzanforderungen eine Möglichkeit zu bieten, die Einstiegsschwelle für Endnutzer auf ein Minimum zu reduzieren.

Insofern sind Verfahren nötig, die sowohl die anonyme ad-hoc Nutzung von Anwendungen als auch die Verwendung schwacher Authentifizierungsmechanismen für nicht sicherheitskritische Anwendungen ermöglichen.

Diese Verfahren müssen dabei berücksichtigen, dass die gegenwärtig verwendeten D-Grid Middlewares in jedem Fall eine PKI-basierte Authentifizierung und Autorisierung erfordern.

Beispiele für den Bedarf nach solchen Verfahren findet man unter anderem in folgenden Bereichen:

- der Zugriff auf frei zugängliche biomedizinische Ontologien und die zugrundeliegenden Datenbanken. Diese Ontologien unterstützen die Fachnutzer bei der Klärung von Begrifflichkeiten und Abhängigkeiten zwischen Begriffen (MediGRID)
- die Bereitstellung von Anwendungen zur Sequenzanalyse von Tiergenomen (MediGRID)
- der Zugriff auf veröffentlichte Dokumente (TextGrid)
- der Zugriff auf frei zugängliche Klimadaten (C3Grid)

2 Randbedingungen und Anforderungen

Technisch ist ein Konzept zu entwickeln, das die Nutzung solcher Anwendungen in den auf PKI-Zertifikaten aufbauenden D-Grid Middlewaresystemen unterstützt, ohne mit den gültigen Policies in D-Grid zu kollidieren. Ebenso muss auf technisch-konzeptioneller Ebene geklärt werden, wie solche Anwendungen gegenüber Anwendungen und Ressourcen mit höheren Sicherheitsanforderungen separiert werden können. Durch die Unterstützung schwacher Authentifizierung oder anonymer Nutzung soll das Sicherheitsniveau bestehender Ressourcen, Dienste und Daten nicht abgesenkt werden.

2.1 Authentifizierung und Autorisierung in D-Grid Middlewares

Da serverseitig im Grid aufgrund der Implementierung der verschiedenen Middlewares die Authentifizierung und Autorisierung gegenwärtig ausschließlich über Zertifikate erfolgen muss, wird auch bei einer Nutzung von Anwendungen durch mehr oder weniger anonyme Nutzer die Nutzung von Zertifikaten für die Ausführung von Grid-Jobs oder den Zugriff auf Daten im Grid erforderlich sein.

Einen Lösungsansatz bieten hier die Regelungen zu Robot-Zertifikaten, wie sie von einigen durch die EUGridPMA akkreditierten Grid CAs angewendet werden und von der EUGridPMA explizit vorgesehen sind. Nach entsprechender Prüfung und Anpassung könnten diese Regelungen in die Policies der deutschen D-Grid-Stammzertifizierungsstellen (DFN und GridKa) übernommen werden. Diese Robot-Zertifikate werden analog zum Konzept der Maschinen- oder Server-Zertifikate für bestimmte Grid-Anwendungen bzw. Grid Services ausgestellt. Wie auch bei den Maschinenzertifikaten wird ein Administrator für die Anwendung bzw. den Service registriert und zuvor anhand seines PKI-Zertifikats authentifiziert. Er übernimmt die juristische Verantwortung für die Verwendung dieses Robot-Zertifikats und trägt somit letztlich die Verantwortung für die Endnutzer, denen er die Nutzung dieses Zertifikats über eine entsprechend abgesicherte Grid-Anwendung zur Verfügung stellt. Dabei empfiehlt es sich für den Servicebetreiber, den Funktionsumfang dieser Anwendung sowie den Zugriff auf Ressourcen, Services und Daten im Grid durch diese Anwendung soweit wie möglich auf die tatsächlich notwendigen Ressourcen, Services und Daten einzugrenzen.

2.2 Schwache Authentifizierung

Bei der Ausarbeitung dieses Konzepts gilt es zu klären, wie viel bei unterschiedlichen Typen und Sicherheitseinstufungen von Anwendungen an überprüfbaren Nutzerinformationen bei der Registrierung für eine schwach authentifizierte Nutzung von Grid Anwendungen und entsprechend dafür zur Verfügung gestellten Ressourcen erhoben werden kann bzw. erhoben werden muss und wie diese Informationen auch als Job Parameter mit dem einzelnen Grid Job transportiert werden können.

Bei der Verwendung schwächerer Authentifizierungsmechanismen ist es nicht unbedingt das Ziel, eine vollständig anonyme Nutzung des Grids zu ermöglichen, sondern ein Verfahren zu etablieren, bei dem der Endnutzer einerseits möglichst weitgehend von Registrierungsaufwänden und komplexer Bedienung von Authentifizierungsmechanismen entbunden wird und andererseits aber ein Mindestmaß an Sicherheit und rechtlicher Absicherung für die Betreiber von Ressourcen, Anwendungen und Services sichergestellt wird.

Um diese Balance herzustellen, werden Nutzer aus dem Umfeld der Universitätsmedizin Göttingen und aus TextGrid im Vorfeld befragt und werden in Zukunft auch in die Evaluation und Praxis-Tests einbezogen. Diese Nutzergruppen waren bisher nicht mit der Nutzung von Grid-Infrastrukturen vertraut. Auf diese Weise kann die Einstiegshürde für die Nutzer deutlich gesenkt werden und die Nutzerbasis wesentlich verbreitert werden, ohne einen vollständig anonymen Zugriff auf die der Anwendung zugrundeliegenden Ressourcen zu gewähren.

Um im Grid öffentliche und rechtlich nicht im Zugriff eingeschränkte Daten auch vollständig ohne vorherige Registrierung zugänglich machen zu können, wird über dies hinaus auch eine anonyme Nutzung – z.B. Lesezugriff auf öffentliche Datenbanken – angestrebt. Als Vorbild kann hier der Zugriff auf Informationsbestände wie Wikipedia dienen, die im Internet ohne jegliche Anmeldung frei zugänglich sind. Beispiele für eine solche anonyme Nutzung von Anwendungen und Datenbeständen im D-Grid sind:

- der Zugriff auf frei zugängliche biomedizinische Ontologien und die zugrundeliegenden Datenbanken. Diese Ontologien unterstützen die Fachnutzer bei der Klärung von Begrifflichkeiten und Abhängigkeiten zwischen Begriffen (MediGRID)
- der Zugriff auf veröffentlichte Dokumente (TextGrid)
- der Zugriff auf frei zugängliche Klimadaten (C3Grid)

Für den anonymen Zugriff auf Ressourcen sollten auf Seite der Ressourcenprovider diese Ressourcen in einer geeigneten Weise als anonym gekennzeichnet werden. Der Zugriff kann dann über die erwähnten Robot-Zertifikate oder andere besonders gekennzeichnete "Zertifikate" erfolgen.

2.3 Unterscheidung von Sicherheitsstufen

Zusammen mit der Berücksichtigung der Nutzung schwacher Authentifizierungsmethoden, auch über Shibboleth-basierte Mechanismen mit Online-Registrierung ergibt sich letztlich eine größere Flexibilität der Zugänge zum Grid und seinen Datenbeständen und Anwendungen. Somit kann in den Policies für den Zugriff auf Grid-Ressourcen von verschiedenen Autorisierungsgraden ausgegangen werden: persönliche Zertifikate, SLCs, schwache Authentifizierungsmethoden wie beispielsweise die Selbstregistrierung mit Verifizierung der E-Mail-Adresse und schließlich auch vollständig anonym.

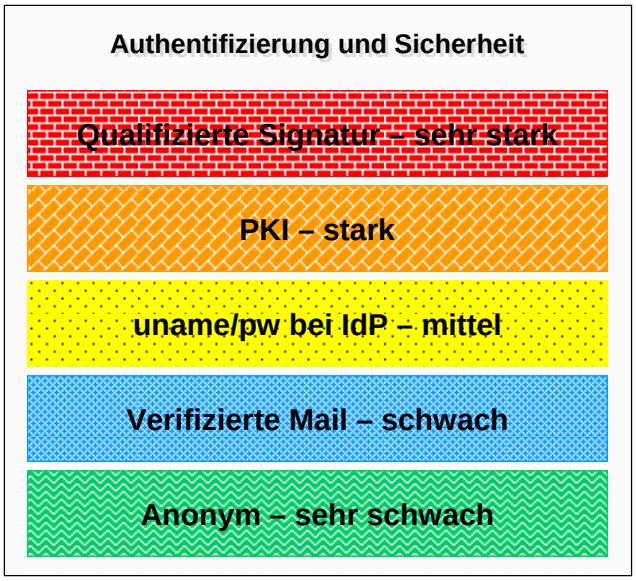

Abbildung 1: Mögliche Unterteilung von Sicherheitsstufen

Abbildung 1 zeigt eine mögliche Unterteilung von Sicherheitsstufen entsprechend der jeweils verwendeten Authentifizierungsmethoden beim Single Sign On ins Grid. Die oberste Sicherheitsstufe wird erreicht, wenn sich der Nutzer mittels einer qualifizierten elektronischen Signatur am Zugangspunkt ins Grid ausweist. Eine normale PKI-basierte Authentifizierung mit den in D-Grid üblichen Nutzerzertifikaten, die von Zertifizierungsstellen der EUGridPMA ausgestellt werden, bildet die zweithöchste Stufe. Authentifizierungsmethoden wie beispielsweise ein Shibboleth-Login, falls dabei nur die Eingabe von Usernamen und Passwort verwendet wird[1], sind schwächer einzustufen als die PKI-basierte Authentifizierung, da Passwörter in der Regel leichter zu knacken sind als PKI-Zertifikate. Werden Gastnutzeraccounts eingerichtet, die zwar auch Usernamen und Passwörter erfordern, bei denen aber die Überprüfung der Identität weniger gewissenhaft erfolgt, als dies beispielsweise einer Shibboleth-Authentifizierung bei der Heimatorganisation vorausgeht, so ist nur noch von einer schwachen Authentifizierung auszugehen und die Sicherheit entsprechend einzustufen. Die Selbstregistrierung als Gastnutzer mit Verifikation der bei der Registrierung angegeben E-Mail-Adresse würde z.B. in diese Kategorie fallen. Erfolgt hingegen ein völlig anonymer Zugriff auf Daten, Dienste oder Ressourcen, ist das niedrigste Sicherheitsniveau erreicht.

Die Verwendung von Service-Zertifikaten an sich stellt also noch keine Einschränkung des Sicherheitsniveaus dar, sofern die Authentifizierung am Service bzw. an dem Portal, in dem der Service läuft, ein ausreichendes Sicherheitsniveau erreicht und gleichzeitig bei der weiteren Nutzung von Grid-Ressourcen durch den Service die Information auf geeignete Weise weitergereicht wird, in wessen Auftrag der Service gerade agiert. Die Weiterreichung

[1] Shibboleth unterstützt auch weitere Authentifizierungsformen (Login Handler), wie z.b. X.509-Zertifikate oder InfoCard, wenngleich die Benutzernamen-Passwort-Methode die gebräuchlichste ist.

der Nutzerinformationen sollte zum einen möglichst nicht abstreitbar sein, um eine sichere Re-Identifikation des Endnutzers zu erlauben. Auf der anderen Seite sollten die hierfür weitergereichten Nutzerinformationen je nach Bedarf pseudonymisiert werden, um ggf. Datenschutzanforderungen zu erfüllen. Diese Information ist auch für eine mögliche Abrechnung von Leistungen zwischen Service-Betreiber und den Endnutzern relevant. Ein entsprechender Ansatz für die Erweiterung des D-Grid Accounting Dienstes DGAS liegt bereits vor [1][2].

Trennung von Daten verschiedener pseudonymer Nutzer

Während mit einer PKI-basierten Authentifizierung (z.B. auch mittels Short Lived Credentials) die Identität des Benutzers am Zertifikat selbst zu erkennen ist, ist dies bei der Verwendung von Robot-Zertifikaten nicht mehr möglich, bzw. jegliche Verwendung ist zunächst dem Service-Betreiber zugeordnet. Dies ist kein Problem bei anonymer Nutzung (unterstes Sicherheitsniveau in Abbildung 1). Bei pseudonymer Nutzung (das darüber befindliche Sicherheitsniveau, z.B. E-Mail-Verifikation) muss jedoch klar unter den eigentlichen Nutzern bzw. Auftraggebern unterschieden werden, damit beispielsweise Daten eindeutig zugeordnet werden können. Dies muss demzufolge mit weiteren Methoden erfolgen, die nicht Gegenstand dieses Dokuments sind, sondern durch den jeweiligen Service-Betreiber sichergestellt werden müssen, der einen Robot-Service anbietet. In TextGrid kann hierzu beispielsweise eine eindeutige SessionID verwendet werden, die als Resultat einer Authentifizierung, z.B. über Shibboleth, entstanden ist. Dies gewährleistet der TextGrid-eigene Policy Decision Point TG-auth*, der eine rollenbasierte Zugriffskontrolle (openRBAC) ermöglicht.

2.4 Mandatory Access Control

Die Autorisierunsgssysteme in D-Grid müssen dann so angepasst werden, dass sie ihre Autorisierungsentscheidungen je nach Sicherheitsbedarf und den bei der Authentifizierung des Endnutzers verwendeten Sicherheitsstufen treffen. Sie müssen so angepasst werden, dass Ressourcen, Dienste und Daten höherer Sicherheitsstufen nicht von Nutzern erreicht werden können, die aufgrund der von ihnen verwendeten Authentifizierungsmethoden in eine niedrigere Sicherheitsstufe eingruppiert werden müssen. In MediGRID und TextGrid wird dies im Rahmen dieses Projekts zunächst als Proof-Of-Concept erfolgen.

Eine Konsequenz aus der Zulassung schwächerer Authentifizierungsmethoden ist somit die Einführung der Mandatory Access Control zur Autorisierung in D-Grid sowie die Einstufung von Ressourcen, Diensten, Daten, Nutzern und Authentifizierungsmethoden in verschiedene Sicherheitslevel. Mandatory Access Control bedeutet, dass die Autorisierungsentscheidung für ein Objekt (Daten, Anwendungen, Ressourcen) nicht (nur) auf Basis der Einstufung durch den jeweiligen Besitzer des Objekts erfolgt, sondern durch das System. Dessen Entscheidung erfolgt auf Basis der Einstufung von Nutzer, Objekt und ggf. auch von Kommunikationswegen in verschiedene Sicherheitslevel. Auf Objekte höherer Sicherheitseinstufungen kann dabei nicht von Subjekten niedrigerer Sicherheitseinstufungen zugegriffen werden. Wenn die Kommunikationswege mit berücksichtigt werden, bedeutet

das, dass ein Subjekt mit hoher Einstufung auf ein Objekt mit gleicher Einstufung oder niedrigerer Einstufung nur zugreifen kann, wenn die genutzten Kommunikationswege eine ebenso hohe (oder höhere) Einstufung wie das Objekt besitzen. Ein Beispiel hierfür wäre, dass ein privilegierter Nutzer mit hoher Sicherheitseinstufung, der sich mit einer qualifizierten elektronischen Signatur authentisiert, nicht auf einen Datensatz mittlerer Sicherheitsstufe zugreifen kann, weil er eine unverschlüsselte Verbindung nutzt und der Datensatz aufgrund seiner Sicherheitseinstufung nicht für eine unverschlüsselte Übertragung zugelassen ist.

Ein pragmatischer Ansatz für D-Grid wäre zunächst eine Aufspaltung in eine hohe Sicherheitsstufe, für die weiterhin die bisherigen Zugriffsregeln in D-Grid gelten, und eine zusätzliche niedrige Sicherheitsstufe, die alle anderen Authentifizierungsmechanismen abdeckt. Für letztere Gruppe ist die Nutzung von separaten Ressourcen erforderlich, die keinerlei ungeschützte Verbindung zu den Ressourcen der höheren Sicherheitsstufe haben.

Nach Umsetzung einer technischen Lösung und erfolgreichen Tests mit zwei Sicherheitsstufen kann dann ohne größeren Aufwand eine weitere Aufspaltung der Sicherheitsstufen erfolgen.

2.5 Technische Randbedingungen

Die Regularien der EUGridPMA sehen für die Verwendung von Robot-Zertifikaten zurzeit zwingend die Verwendung von Crypto-Tokens für die Speicherung der Schlüsselpaare vor. Die Verwendung von Robot-Zertifikaten betrifft vor allem Grid-Service Clients, die z.B. in Community-Portalen als Portlets implementiert sind oder direkt über Service-Schnittstellen auf weitere Grid-Dienste zugreifen.

Es ist nun davon auszugehen, dass auf den verschiedenen Portal-Servern im Grid jeweils eine Vielzahl von Anwendungsdiensten bzw. deren Clients installiert sein wird. Insofern ist die Auslieferung von Robot-Zertifikaten auf Hardware-Tokens problematisch und aus praktischen Gründen nicht wünschenswert.

Eine Anpassung der Regeln der EUGridPMA wird daher angestrebt. Gap-SLC wird entsprechend mit Vertretern der EUGridPMA in Kontakt treten, um die Möglichkeiten zu eruieren.

Sollte dies nicht möglich sein, wird die Anzahl der maximal über einen Portalserver bereitzustellenden Grid-Service-Clients aus technischen Gründen auf 127 begrenzt sein, da dies die technisch maximal mögliche Anzahl von USB-Geräten ist, die an einen Server angeschlossen werden kann. In der Praxis dürfte aber auch diese Zahl nicht realistisch zu erreichen sein. Zudem wird es erforderlich sein, eine Unterstützung für die Erzeugung von Proxy-Zertifikaten für Schlüsselpaare, die auf Hardware-Tokens gespeichert sind, bereitzustellen.

3 Bedarf und Akzeptanz

3.1 Bioinformatik und Medizin

In einigen Bereichen der biomedizinischen Community wurde eine Umfrage durchgeführt, mit der ermittelt werden sollte, inwiefern ein Bedarf nach einer anonymen oder pseudonymen Nutzung von Grid-Ressourcen mit vereinfachten Authentifizierungsmechanismen besteht und inwiefern bestimmte Lösungsansätze auf Akzeptanz stoßen.

An der Umfrage beteiligt waren sechs Vertreter der Communities MediGRID/Services@MediGRID, MedInfoGrid, PneumoGrid sowie eines für 2013 geplanten Graduiertenkollegs aus der epidemiologischen Forschung in Göttingen, welches Grid-Ressourcen verwenden möchte.

Zusammenfassung der Ergebnisse:

In den Bereichen Medizin und Bioinformatik besteht ein Bedarf, die Registrierung und Authentifizierung für bestimmte Nutzergruppen zu vereinfachen. Robot-Zertifikate stellen hierfür nach Einschätzung der Communities ein geeignetes Mittel dar. Die potenziellen Betreiber von Robot-Services sind in diesem Zusammenhang grundsätzlich auch bereit, die mit der pseudonymen oder anonymen Nutzung von Grid-Ressourcen verbundenen Haftungsrisiken zu tragen. Hierbei werden jedoch diejenigen schwachen Registrierungs- und Authentifizierungsverfahren bevorzugt, die eine gewisse Re-Identifizierung der Nutzer erlauben. Die völlig anonyme Nutzung von Ressourcen, Services und Daten wird eher kritisch gesehen, von Teilen der Befragten aber dennoch befürwortet. Insofern sollte nach einer Testphase ein mehr als zweistufiges Sicherheitskonzept umgesetzt werden.

3.2 Textwissenschaften

Ähnlich wie in der Bioinformatik und Medizin wurde auch in der TextGrid-Community eine Umfrage durchgeführt. Im Gegensatz zu der vorhergehenden Umfrage wurde diese Umfrage auf Middleware-Entwickler zugeschnitten und nicht auf „normale“ TextGrid-Benutzer, die mit Authentifizierungsfragen kaum vertraut sind. Entsprechend ging der Fragebogen an zwei Entwickler, die die entsprechenden Kompetenzen in diesem Bereich hatten.

Zusammenfassung der Ergebnisse:

Von der bisherigen Nutzerschaft würde gegenwärtig nur ein Bruchteil (die Teilnehmer an der DFN-AAI) mit SLCs versorgt werden können, was zunächst eine besondere Berücksichtigung dieses pseudonymen Sicherheitsniveaus, zusätzlich zu anonymer Nutzung, erforderlich macht. Es ist anzunehmen, dass zukünftig weitere Forschungseinrichtungen entweder zur DFN-AAI oder anderen international vernetzten SAML-basierten Föderationen hinzukommen, so dass tendenziell ein höherer Anteil von Benutzern mit SLCs versorgt werden kann.

3.3 Weitere Communities

Die Befragung bzgl. des Bedarfs nach einer anonymen oder pseudonymen Nutzung von Grid-Ressourcen mit vereinfachten Authentifizierungsmechanismen wurde zunächst nur in den am Projekt Gap-SLC direkt beteiligten Communities durchgeführt. Im Rahmen des von Gap-SLC durchgeführten D-Grid Workshops „Sicherheitsanforderungen“ am 21.09.09 in Göttingen wurde von weiteren anwesenden Community-Vertretern ein ähnlicher Bedarf zum Ausdruck gebracht.

4 Konzeptentwurf

4.1 Robot-Zertifikate

Die Zugangspunkte, über die schwach authentifizierte Nutzer oder anonyme Nutzer den Zugriff auf bestimmte (eingeschränkte) Grid Anwendungen und Services erhalten, werden mit Robot-Zertifikaten ausgestattet, um sich gegenüber den D-Grid Ressourcen, Services und Anwendungen authentisieren zu können. Diese Service-Zertifikate werden aus praktischen Gründen (siehe auch Abschnitt 2.5) als Software-Zertifikate ausgestellt.

Auf ausgewählten Hardware-Ressourcen im Grid und gegenüber ausgewählten Grid-Diensten werden diese Robot-Zertifikate äquivalent zu normalen Nutzerzertifikaten behandelt. Diese Ressourcen und Dienste müssen von ihren Betreibern explizit für die Nutzung durch Services mit Robotzertifikaten freigegeben sein.

4.2 Identity und Usermanagement

Dienste (d.h. Endnutzer-Clients zu Grid-Anwendungen und Grid-Workflows, z.B. Application-Portlets in Grid-Portalen), die mit Robot-Zertifikaten ausgestattet sind, treten in der Praxis im D-Grid wie normale D-Grid-Nutzer auf. Insofern müssen die Dienste samt den zugehörigen DNs ihrer Robot-Zertifikate auch in den User- und VO-Managementsystemen bekannt gemacht werden. Der Betreiber eines Dienstes muss also seinen Dienst auch an den entsprechenden User- und VO-Managementsystemen anmelden. Über die in D-Grid üblichen Verfahren werden dann die „Robot-User“ auch den Ressourcen- und Service-Betreibern in D-Grid bekannt gemacht. Dabei ist es erforderlich, diese Robot-User auch als solche zu kennzeichnen, um es den Betreibern zu ermöglichen, diese Nutzer auf ihren Ressourcen / Diensten abzulehnen (siehe auch 4.4). Dies kann beispielsweise über Attribute im VOM(R)S erfolgen. In diesem Zusammenhang ist es sinnvoll, die dgridmap-Skripte, mit denen lokal die Einrichtung von Nutzeraccounts und das Mapping von DNs/Nutzern auf lokale Accounts abgewickelt wird, entsprechend anzupassen und als Minimallösung zwei verschiedene Skripte anzubieten – eines, das Robot-User akzeptiert und eines, das sie ablehnt.

Vor der Einstellung von Robot-Usern in die User- und VO-Management-Systeme muss daher gewährleistet werden, dass entweder alle Ressourcen- und Servicebetreiber das ihnen entsprechende Skript implementiert haben oder dass die Verwendung von Robot-Zertifikaten nur innerhalb einer speziellen VO erfolgt, zu der ausschließlich solche Ressourcen und Dienste gehören, die Robot-Zertifikate ausdrücklich akzeptieren. Die testweise Erprobung der technischen Infrastruktur für die Verwendung von Robot-Zertifikaten wird auf letzterem Ansatz beruhen. Die hierfür verwendete D-Grid VO wird die VO „gapslc“ sein. Die Ressourcen, die von der VO „gapslc“ genutzt werden, sind ausschließlich Testrechner, die von den Projektpartnern explizit zu diesem Zweck bereitgestellt werden. Es werden hierfür keine bestehenden D-Grid Ressourcen verwendet.

4.3 Schwache Authentifizierung und anonyme Nutzung

Die Verwendung von Robot-Zertifikaten ist in zwei Fällen sinnvoll:

- Wenn Nutzern eine anonyme Nutzung von Grid-Diensten ohne jegliche Registrierung ermöglicht werden soll
- Wenn Nutzern eine Nutzung von Grid-Diensten ermöglicht werden soll, die lediglich einen einfachen und kurzen Registrierungsprozess voraussetzen, der gemäß Abbildung 1 in die unteren beiden Sicherheitsstufen einzusortieren wäre.

In letzterem Fall ist ein Verfahren möglich, das dem Nutzer eine einmalige Selbst-Registrierung an einem D-Grid-Community-Portal oder einem zentralen D-Grid-Portal ermöglicht und abverlangt. Im Zuge dieser Registrierung werden Basisdaten des Nutzers erhoben, wie beispielsweise sein Vor- und Nachname, sowie seine E-Mail-Adresse. Der Nutzer wählt eine Kombination von Nutzername und Passwort, die fortan zur Authentifizierung – z.B. an einem Grid-Portal – verwendet werden. Um ein Minimum an Nachvollziehbarkeit der Angaben zu gewährleisten, erhält der Anwärter im Registrierungsprozess einen Registrierungslink an die von ihm angegebene E-Mail-Adresse, sodass zumindest die Existenz der E-Mail-Adresse zum Registrierungszeitpunkt gewährleistet ist und überprüft werden kann. Zusätzliche Sicherheit könnte erreicht werden, indem die sich registrierenden Nutzer gezwungen würden, von der angegebenen E-Mail-Adresse aus eine E-Mail an das zur Registrierung verwendete System zu schicken, da dadurch zusätzlich „Instant Mail"-Adressen[2] ausgeschlossen werden könnten. Auf diese Weise besteht selbst bei falschen Angaben des Nutzers eine eingeschränkte Möglichkeit der Rückauflösung seiner Identität, sofern die IP-Adresse des Rechners, von dem aus der Nutzer seine Registrierung durchführt, mitgeloggt wird. In schweren Missbrauchsfällen kann so unter Einschaltung von Strafverfolgungsbehörden über die Logging-Daten des Internet-Service-Providers des Nutzers seine Identität zumindest bis an den von ihm bei der Registrierung genutzten Rechner zurückverfolgt werden – sofern der Zeitraum zwischen Registrierung und Missbrauch nicht den Zeitraum der gesetzlich vorgeschriebenen Vorratsdatenspeicherung bei ISPs überschreitet. Insofern könnten eine zeitliche Begrenzung solcher Gastnutzeraccounts und die Forderung der Re-Registrierung nach Ablauf dieser Frist sinnvoll sein.

Je nach Sicherheitsanforderungen der Hardware- und Service-Betreiber in D-Grid können dann für unterschiedliche Arten der Registrierung die Zugriffsrechte unterschieden werden.

[2] Hier sind Dienste gemeint, bei denen man sich überhaupt nicht registrieren muss. Ein Benutzer kann sich eine beliebige Wegwerf-E-Mail-Adresse in deren Domain ausdenken, z.B. xyz123@mailinator.com oder abc456@instant-mail.de. Die dort eintreffenden Mails können für einige Stunden ohne ein Passwort abgerufen werden. Es ist nur reines Lesen, aber kein Versenden von Mails möglich.

Dies setzt voraus, dass die Betreiber die Information über die Art der für die Nutzung eines Dienstes erforderlichen Registrierung nachvollziehen können – z.B. über Attribute zu den Robot-Services im VO-Management-System.

Hierfür muss der Betreiber eines D-Grid-Dienstes, der Robot-Zertifikate verwendet, durch geeignete Policies und Nutzungsbedingungen verpflichtet werden, dass er bei der Registrierung in den User- und VO-Managementsystemen wahrheitsgemäß angibt, welche Art(en) der Registrierung er seinen Endnutzern ermöglicht.

4.4 Akzeptanzbereich von Robot-Zertifikaten

Da Robot-Zertifikate eingesetzt werden, um Endnutzern schwache oder anonyme Authentisierung/Authentifizierung zu ermöglichen, muss es den Betreibern von Hardware, Anwendungen und Diensten in D-Grid freigestellt bleiben, solche Zertifikate – und somit pseudonyme[3] oder anonyme Nutzer – zu akzeptieren oder abzulehnen.

Ein pragmatisches Vorgehen wäre, unterschiedliche Ressourcenbereiche für unterschiedlich starke Authentifizierungsgrade zu definieren. Es könnte einen Standard-D-Grid-Ressourcenpool geben, der nur die bisher übliche starke Authentifizierung erlaubt und somit Robot-Zertifikate ablehnt. Darüber hinaus könnte man einen oder mehrere weitere Ressourcenpools definieren, die Robot-Zertifikate akzeptieren und ihren Nutzern im Gegenzug in den Nutzungsbedingungen aber nicht (mehr) die volle Sicherheit und Verfügbarkeit des Systems sowie die Datensicherheit garantieren. Die Service-Levels hinsichtlich Security wären für diesen Ressourcenpool, der Robot-Zertifikate akzeptiert, gegenüber den Standard-Ressourcen eingeschränkt. Auf diese Weise wäre der Normal-Betrieb durch die Aufweichung der Authentifizierungsanforderungen nicht berührt.

Eine weitere Unterteilung der eingeschränkten Ressourcenpools wäre beispielsweise noch möglich, indem man zwischen Diensten differenziert, die eine völlig anonyme Nutzung ermöglichen und solchen, die zumindest Basisdaten des Nutzers erheben, beispielsweise über eine Selbst-Registrierung des Nutzers mit Überprüfung der E-Mail-Adresse durch einen Verifikationslink im Anmeldeprozess (siehe 4.3).

Um letztlich auch den Endnutzern in D-Grid eine Möglichkeit zu geben, die Verwendung von Ressourcen auszuschließen, welche die Nutzung von Robot-Zertifikaten akzeptieren und somit nur eingeschränkte Security-Service-Levels anbieten, muss gewährleistet werden,

[3] Pseudonym bedeutet in diesem Zusammenhang, dass dem Ressourcenbetreiber die Identität nicht bekannt ist, dass diese aber grundsätzlich rückauflösbar ist. Dies kann der Fall sein, wenn dem Betreiber des Services, welcher das Robot-Zertifikat nutzt, die Identität des Nutzers bekannt ist und ein Kundenpseudonym als Jobparameter mitprotokolliert wird. Einen Grenzbereich zwischen anonym und pseudonym stellt die Selbstregistrierung des Endnutzers beim Servicebetreiber dar, wenn ausschließlich die Existenz der angegebenen E-Mail-Adresse verifiziert wird. Im Zweifelsfall ist der vom Nutzer zur Registrierung verwendete Rechner hier über Logging-Daten seines Internet Service Providers zurückverfolgbar – hier besteht allerdings keine Garantie der Rückauflösbarkeit.

dass die Ressourcen- und Service-Betreiber ihre Ressourcen und Services entsprechend in den Grid-Informationssystemen (z.B. GRRS) kennzeichnen – z.B. durch Attribute – wenn sie nicht die vollen Security-Service-Levels unterstützen.

Der Nutzer bekommt dann beispielsweise über Brokering-Dienste[4] die Möglichkeit, Ressourcen mit niedrigem Sicherheitslevel bei der Job-Submission von vornherein auszuschließen. Der Brokering-Dienst kann hierfür die entsprechenden Security-Attribute zu Ressourcen aus den Grid-Informationssystemen berücksichtigen. Auf diese Weise würde auch das sogenannte „Tracking" ermöglicht – die a priori Auswahl von Ressourcen nach ihrer Sicherheitseinstufung für die Grid-Job-Ausführung. Zusätzlich wird sichergestellt, dass dem Nutzer keine Ressourcen vermittelt werden, für die er keine Zugriffsrechte besitzt.

Datenmigration zwischen Domänen mit unterschiedlichen Sicherheitsleveln

Bei einer Trennung zwischen Ressourcen-Bereichen mit unterschiedlichen Sicherheitsleveln wird auch der Fall eintreten, dass Daten von einem Bereich niedriger Sicherheitsstufe in einen Bereich höherer Sicherheitsstufe transferiert werden sollen. Dies kann nur durch Nutzer erfolgen, die selbst eine ausreichende Sicherheitseinstufung für den höheren Sicherheitslevel besitzen und zum Zeitpunkt des Transfers entsprechend an den Ressourcen höherer Sicherheitslevel authentifiziert und autorisiert sind.

Nutzung von Daten auf low-security Ressourcen durch Anwendungen auf high-security Ressourcen

Eine offene Fragestellung ist, inwiefern und unter welchen Umständen Anwendungen auf Ressourcen höherer Sicherheitslevel Lesezugriff auf Daten erhalten, die auf Ressourcen niedrigerer Sicherheitslevel gespeichert sind, ohne diese zuvor zu migrieren.

4.5 Architektur zur Verwendung von Robot-Zertifikaten

Um das oben beschriebene Konzept umsetzen zu können, bedarf es in D-Grid zunächst der Unterscheidung (mindestens) zweier Arten von Ressourcen:

- High Security Ressourcen (D-Grid Standard)
- Low Security Ressourcen (nicht Standard!)

Der Unterschied zwischen den beiden Arten von Ressourcen ist folgender:

- High Security Ressourcen erfordern eine PKI-basierte Authentifizierung des Endnutzers mittels Proxies von Nutzerzertifikaten und der Endnutzer muss

[4] Brokering-Dienste dienen dazu, für eine bestimmte Job-Anfrage zunächst die technisch in Frage kommenden Ressourcen anhand von Grid-Ressourceninformationssystemen zu ermitteln. Anschließend werden über Meta-Scheduling-Dienste diejenigen Ressourcen unter den in Frage kommenden ermittelt, die am wenigsten ausgelastet sind. Für den Nutzer hat dies den Vorteil, dass er die Ressourcen und Ressourcenzustände im Grid nicht selbst kennen und mitverfolgen muss.

sich beim Single-Sign-On ins D-Grid (z.B. via Portal) auf sichere Art und Weise am ersten Zugangspunkt authentifizieren (PKI oder Shibboleth)

– Low Security Ressourcen erfordern ebenfalls eine PKI-basierte Authentifizierung. Sie erlauben aber zusätzlich zu den Proxies von Endnutzerzertifikaten den Zugriff über die Proxies von Robot-Zertifikaten, die im Auftrag von anonymen oder pseudonymen Endnutzern agieren und von ihren Endnutzern nur eine schwache Authentifizierung erfordern – z.B. einen Gastnutzerzugang mittels Username/Passwort mit vorheriger Verifikation der E-Mail-Adresse des Nutzers

Wie in Abbildung 2 dargestellt, melden sich zunächst beide Arten von Ressourcen am Grid Resource Registration Service in D-Grid an (Schritt 0). Bei der Registrierung geben sie an, welchen Security-Level sie anbieten möchten (high oder low). Der GRRS speichert diese Information als Attribut zur jeweiligen Ressource. In der ersten Testphase wird eine Auswertung von Ressourcen-Attributen im GRRS noch nicht erforderlich sein, da ein explizit getrennter Ressourcenpool verwendet wird (siehe Abschnitt 4.2).

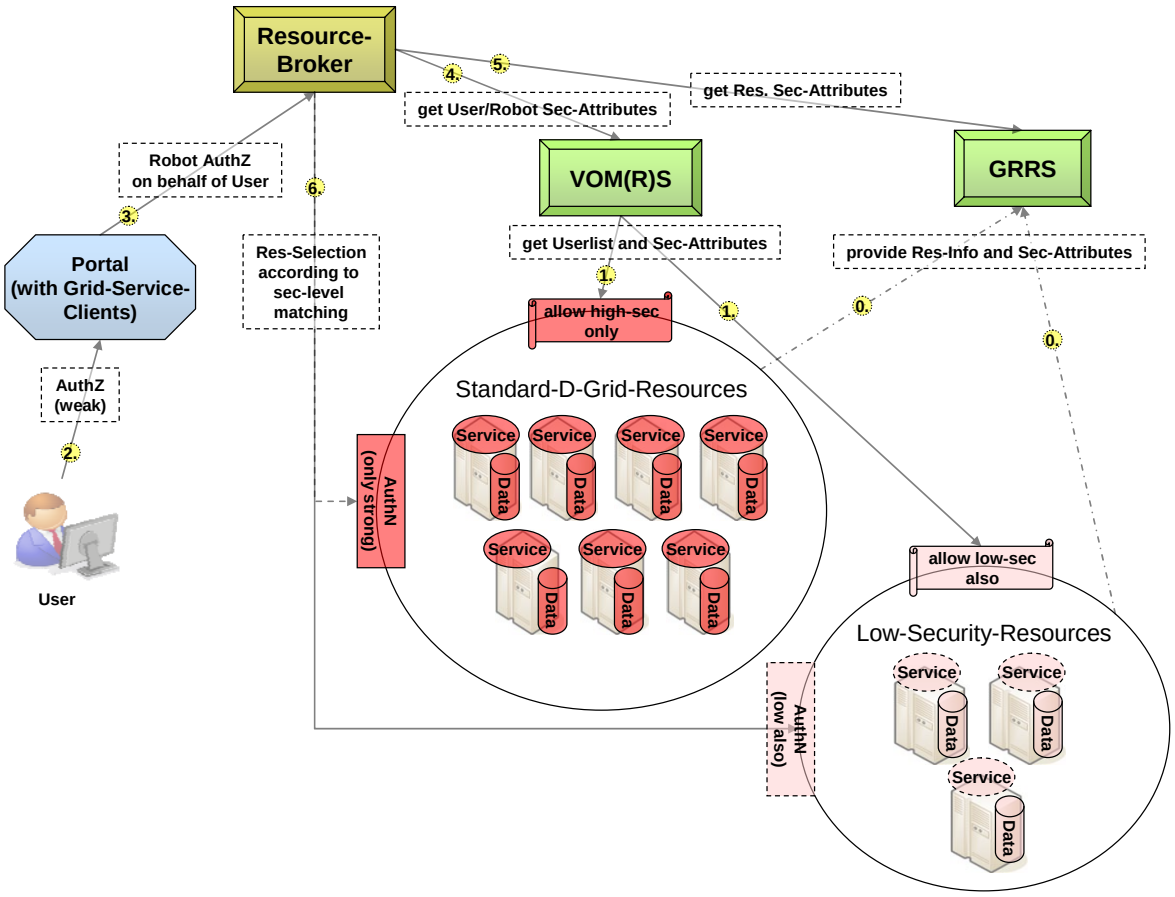

Abbildung 2: Architektur zur Verwendung von Robot-Zertifikaten

Anschließend beziehen beide Arten von Ressourcen die Nutzerinformationen zu den VOs, für die sie ihre Ressourcen zur Verfügung stellen wollen, aus dem VO Management System (Schritt 1). Je nachdem, welches Sicherheitslevel sie von ihren Nutzern fordern, lassen sie

entweder alle Nutzer der jeweiligen VOs auf ihrem System zu (dies ist der Fall für Low Security Ressourcen) oder nur diejenigen Nutzer, für die im VOMS das Attribut „high security“ hinterlegt ist. Robot-Nutzer erhalten dieses Attribut grundsätzlich nicht. Um sicherzustellen, dass eine Ressource nicht aus Versehen alle Nutzer zulässt, obwohl sie das nicht möchte, könnte der Abruf von Nutzerdaten aus dem VOMS so gestaltet werden, dass zum Abruf von Nutzern mit niedriger Sicherheitseinstufung (d.h. von Robot-Nutzern) ein gesondertes dgridmap-Skript erforderlich ist, während das normale und zurzeit im Einsatz befindliche Skript diese Nutzer nicht ausgibt.

An dieser Stelle ist dann gewährleistet, dass auf den jeweiligen Ressourcentypen nur für diejenigen Nutzer Accounts und Mappings eingerichtet werden, die auch ausdrücklich erwünscht und zugelassen sind.

Wenn sich ein Endnutzer dann über eine schwache Authentifizierungsmethode an einem Grid-Portal anmeldet (Schritt 2) und dort Zugriff auf Grid-Service-Clients erhält, die mit Robot-Zertifikaten ausgestattet sind, werden von diesen Grid-Service-Clients entweder Low Security Services auf Low Security Ressourcen direkt adressiert (im Bild nicht dargestellt) oder es erfolgt eine dynamische Ressourcenauswahl über einen Broker-Service (Schritt 3). Dieser Broker-Service akzeptiert das Robot-Zertifikat des Grid-Service-Clients und kann diesem Robot-Zertifikat die Identität des verantwortlichen Grid-Service-Client-Administrators entnehmen. Entsprechend der Job-Anfrage ermittelt es über den GRRS die geeigneten Ressourcen (Schritt 5). Ein Kriterium der Eignung ist dabei die Sicherheitseinstufung der Ressource. Da die Anfrage an den Broker mittels Robot-Zertifikat erfolgt ist, kommen für den Job ausschließlich Low Security Ressourcen in Betracht. Bei einer weiteren Unterscheidung von Sicherheitsleveln, wie dies in Abschnitt 2.3 beschrieben ist, erfolgt zusätzlich zunächst eine Anfrage beim VOMS, um zu ermitteln, welcher Sicherheitslevel dem (Robot-) Nutzer zugeordnet ist (Schritt 4).

An dieser Stelle ist sichergestellt, dass der Broker gar nicht erst versucht, die Anfrage des Robot-Nutzers auf eine Ressource zu schicken, die keine Robot-Nutzer zulässt. Falls dies doch geschehen sollte, ist aber durch die Autorisierungssysteme der einzelnen Ressourcen gewährleistet, dass sie eine Job-Anfrage eines Robot-Nutzers zurückweisen würden, da in Schritt 1 nur für echte Endnutzer-Zertifikate Accounts und Mappings eingerichtet wurden. Somit ist auch in Schritt 6, in dem der Broker die Service-Anfrage zusammen mit dem Robot-Zertifikat an die ausgewählte(n) Ressource(n) weiterleitet, gewährleistet, dass kein ungewünschter Zugriff erfolgen kann.

So lange nur zwei Sicherheitslevel unterschieden werden, ist eine Abfrage der Nutzer-Attribute aus dem VOM(R)S streng genommen gar nicht erforderlich – dies betrifft Schritt 1 und Schritt 4. Da Robot-Zertifikate sich in ihrem Distinguished Name unterscheiden, kann man die Autorisierungsmechanismen an den Ressourcen (Schritt 6) auch so einrichten, dass Robot-Zertifikate grundsätzlich zurückgewiesen werden.

5 Zusammenfassung

Die Einrichtung von einfachen Zugangsmethoden zu ausgewählten Ressourcen, Services und Daten in D-Grid ist aufgrund des Bedarfs in mehreren D-Grid Communities erforderlich. Hierfür ist eine Unterscheidung von Sicherheitsleveln sowohl für Ressourcen und Services als auch für Nutzer notwendig. Das in Abschnitt 3 dargestellte Konzept erlaubt eine saubere Trennung von Ressourcen und Nutzern mit unterschiedlichen Sicherheitsanforderungen. Es ist dabei auf einfache Weise möglich, einen Testbetrieb für die Nutzung von Robot-Zertifikaten unter Verwendung zentraler D-Grid Dienste wie VOMRS und GRRS aufzubauen, ohne die bestehende Infrastruktur und deren Sicherheitsanforderungen dabei zu kompromittieren.

Es wird daher empfohlen, mit einer geringen Anzahl an Test-Ressourcen eine Low Security Domäne in D-Grid aufzubauen. Dazu wird eine VO „gapslc“ eingerichtet. Die Nutzungsbedingungen dieser VO sehen vor, dass die Teilnehmer damit einverstanden sind, dass Robot-Nutzer über Robot-Zertifikate auf den VO-Ressourcen zugelassen werden. Die Ressourcen, die der VO über den GRRS zugeordnet werden, sind ausschließlich Test-Ressourcen, deren Betreiber der Verwendung von Robot-Zertifikaten zugestimmt haben.

Um den vollen Nutzen des Konzepts zu entfalten, sind mittelfristig überschaubare Anpassungen im GRRS erforderlich. Mit der bereits erfolgten Einführung des VOMS SAML Service und der Verwaltung von Attributen im VOM(R)S ist eine weitere Voraussetzung für die erfolgreiche Umsetzung des oben beschriebenen Konzepts bereits erfolgt. Bei der (Weiter-) Entwicklung von Broker-Diensten für D-Grid wäre eine Berücksichtigung des Konzepts für die Auswahlentscheidung in solchen Diensten wünschenswert. Für eine testweise Umsetzung eines Proof-of-Concept sind aber bereits alle unbedingt notwendigen Voraussetzungen in D-Grid gegeben.

6 Anhang: Umfragen in den Communities

6.1 MediGRID

Die Ergebnisse der Umfrage waren wie folgt:

1) Besteht Ihrerseits ein Interesse daran, Service-Zertifikate für Grid-Dienste einzusetzen?

   Ja: 5, Nein: 1

   Bewertung: Der Bedarf am Einsatz von Robot-Zertifikaten besteht

2) Bestehen Ihrerseits Bedenken, Service-Zertifikate für Grid-Dienste einzusetzen?

   Ja: 3, Nein: 3

   Bewertung: Die Befragten sind nicht bereit Robot-Zertifikate unter allen Bedingungen zu akzeptieren.

3) Bestehen Ihrerseits weitere Anforderungen an den Einsatz von Service-Zertifikaten?

   Die Antworten zu dieser Frage wurden als Freitext abgefragt.

   Ergebnisse: Es wurde die Trennung von Ressourcen nach Sicherheitsleveln angeregt und die Forderung nach einer Re-Identifizierbarkeit der Nutzer eines Robotservices gestellt. Ein Hintergrund des Interesses an Robot-Zertifikaten ist die leichtere Integration kommerzieller Nutzer.

4) Besteht Ihrerseits ein Interesse daran, anonymen Nutzern Grid-Dienste bereitzustellen?

   Ja: 3, Nein: 3

   Bewertung: Trotz des Bedarfs an einer Nutzung von Robot-Zertifikaten wird die völlig anonyme Nutzung nicht unkritisch gesehen. Insofern ist längerfristig eine Unterscheidung von mehr als zwei Sicherheitsstufen sinnvoll.

5) Besteht Ihrerseits ein Interesse daran, anonymen Nutzern Daten im Grid bereitzustellen?

   Ja: 3, Nein: 3

   Bewertung: Auch hier wird der völlig anonyme Zugang zu Daten kritisch gesehen, was ebenfalls eine Unterscheidung von mehr als zwei Sicherheitsstufen nahelegt.

6) Halten Sie folgende Authentifizierungsmechanismen für praktikabel?

a. Ad hoc Authentifizierung – völlig anonym: der Nutzer erhält Zugriff ohne eigentliche Authentifizierung. Beispiel: Datensätze des EBI können direkt heruntergeladen werden.

   Ja: 2, Nein: 4

   Bewertung: Wieder wird der vollständig anonyme Zugang eher kritisch gesehen

b. E-Mail-Verifikation: der Nutzer erhält Zugang nach Bestätigung seiner Identität über eine funktionierende E-Mail-Adresse, die jedoch nicht überprüft wird. Beispiel: Zum Bearbeiten und Einstellen von Inhalten in Wikipedia wird ein Link an die angegebene E-Mail-Adresse geschickt, der durch Aufruf die Funktionsfähigkeit der angegebenen E-Mail-Adresse verifiziert.

   Ja: 2, Nein: 4

   Bewertung: Das bloße Hinterlassen der E-Mail-Adresse reicht offensichtlich nicht, um die Zweifel der Community-Vertreter an einer anonymen Nutzung zu zerstreuen.

c. Integrierte Nutzerverwaltung: Der Nutzer erhält vom Anbieter der Daten/Dienste eine Kombination aus Benutzername und Passwort, wobei die Authentifizierung und Autorisierung in dem Dienst implementiert sind. Der Dienst selbst verwendet im Grid ein Service-Zertifikat.

   Ja: 6, Nein: 0

   Bewertung: Die Verifikation der angegebenen E-Mail-Adresse bei der Registrierung, wodurch eine beschränkte Re-Identifikation des Nutzers möglich wird, reicht den Befragten aus, um einer solchen pseudonymen Nutzung des Grids zuzustimmen.

d. Public Key Infrastructure: Der Nutzer verwendet ein persönliches Zertifikat.

   Ja: 5, Nein: 0, Enthaltung: 1

   Bewertung: Die PKI-basierte Nutzung, wie sie im Moment stattfindet, wird weithin akzeptiert. Aus dieser Akzeptanz lässt sich jedoch nicht ableiten, dass Alternativen unnötig seien.

e. Qualifizierte elektronische Signatur: der Nutzer verwendet ein Zertifikat mit einer qualifizierten elektronischen Signatur. Beispiel: entsprechende Hardware-Lösungen wie die elektronische Gesundheitskarte.

   Ja: 4, Nein: 1, Enthaltung: 1

   Bewertung: Auch die Nutzung von qualifizierten elektronischen Signaturen im Grid wird mehrheitlich positiv gesehen.

7) Würden Sie einer Nutzungsvereinbarung zustimmen, die der obigen Darstellung entsprechend entworfen wurde? (In der „obigen“ Darstellung wurde im wesentlichen erläutert, dass das rechtliche Risiko einer Lösung mit Robot-Zertifikaten beim Service-Anbieter liegt und er somit im Zweifelsfall für seine Endnutzer haftet)

   Ja: 6, Nein: 0

   Bewertung: Die potenziellen Anbieter von Robot-Services sind durchweg bereit das damit verbundene Haftungsrisiko zu übernehmen.

8) Bestehen Ihrerseits Anforderungen an die Nutzungsvereinbarung?

   Als Rückmeldung auf diese Freitextfrage wurde der Bedarf an feingranularer Autorisierung an den Ressourcen und insbesondere an den Datensätzen formuliert.

6.2 TextGrid

Fragebogen zur anonymen Gridnutzung

Version 0.4, September 2009 Peter Gietz, Martin Haase, DAASI International GmbH

Antworten kursiv, Status: September 2009

Zielgruppe

Middleware-Entwickler aus der TextGrid-Community.

Aktuelle Situation

Welche Nutzergruppen gibt es aktuell? (Mehrfachnennung möglich)

- Nutzer besitzen persönliche langlebige (ca. 1Jahr) Gridzertifikate ***4***
- Nutzer beziehen kurzlebige (unter 10 Tagen gültig) Gridzertifikate oder Proxys ***1***
- Nutzer authentifizieren sich über Shibboleth ***2***
- Nutzer sind nur anhand einer gültigen E-Mail-Adresse verifiziert ***ca. 190***
- Völlig anonyme Nutzer a là WWW ***unbekannt***

Möchten Sie einen Punkt der letzten Frage differenzieren oder Punkte hinzufügen? Bitte angeben, wie.

*Zu **unbekannt**: Nutzer können bereits jetzt auch ohne Authentifizierung mit TextGrid arbeiten. Grid-Zugriff erfolgt ausschließlich lesend und nur auf veröffentlichte Ressourcen.*

Schätzen Sie die bisherigen Anteile ihrer authentifizierten Nutzer (in Prozent)

- Mit Account an einer deutschen Hochschule/Einrichtung, die an der DFN-AAI teilnimmt ***ca. 19%***
- Mit Account an einer Hochschule/Einrichtung, die an einer anderen SAML-Föderation teilnimmt ***ca. 17%***
- Mitglied einer anderen Hochschule oder Forschungseinrichtung in Deutschland ***ca. 34%***
- Mitglied einer anderen Hochschule oder Forschungseinrichtung im Ausland ***ca. 11%***
- Mitglied einer Firma ***ca. 6%***
- Privatnutzer ***ca. 12%***
- Andere: ***ca. 1%***

Welche Nutzerdaten werden für eine Nutzung zwingend erhoben? (z.B. bei Verdacht auf rechtswidrige Nutzung oder kostenpflichtigen Angeboten)

E-Mail-Adresse, Insituttionszugehörigkeit, Vor- und Nachname

Welche Ressourcen werden gegenwärtig beschützt? (Mehrfachnennung möglich)

- Grid-Jobs ***nein***
- Datensätze ***ja***
- Grid-Speicher ***nein***
- Services ***ja***
- Sonstiges: ***nein***

Welche Nutzungsszenarien gibt es momentan? (Mehrfachnennung möglich)

- Anonyme Ressourcennutzung ***ja***
- Authentifizierte Nutzer dürfen alles (a là Gridmap-File) ***nein***
- Nutzung eines Policy Decision Point zur Autorisierung
  - zentraler PDP ***ja***
  - eigener PDP bei der Ressource ***nein***

Wenn ein PDP genutzt wird, wo befinden sich die Autorisierungsinformationen?

- Im PDP selbst ***ja***
- Bei der Institution (als Campus-Attribute) ***nein***
- Bei der Virtuellen Organisation (VO-Attribute) ***nein***
- Weitere Quellen:

Wenn ein PDP genutzt wird, auf welcher Technologie baut er auf?

Role-based Access Control mit LDAP-Datenbank

Sind lizenz- oder kostenpflichtige Angebote in der Nutzung enthalten? Welcher Art?

nein

Sind Teile des Angebots sicherheitskritisch (z.B. personenbezogene Daten)?

nein

Zukünftige Anforderungen

Werden sich in der absehbaren Zukunft weitere Anforderungen ergeben, die das aktuelle Bild ergänzen? Welche?

Einsatz von lizensierten Inhalten geplant, Einsatz von SLCs geplant.

7 Literatur

[1] Brenner, M., Wiebelitz, J.: Accounting von vermittelten Grid-Jobs, Version 1.0, DGI-2 Fachgebiet 5.2, 07.11.2008

[2] Wiebelitz, J., Brenner, M.: Konzept für das Accounting im D-Grid, Version 1.0, DGI-2 Fachgebiet 5.2, 01.10.2008