



Fachgebiet 3.2  
AAI/VO

# **Definition von Attributen für die Autorisierung auf D-Grid Res- ourcen**

Version 1.0, 21. Juli 2008

1	MANAGEMENT SUMMARY .....	4
2	ZIEL DIESES DOKUMENTS .....	4
3	AUTORISIERUNG IM D-GRID (STATUS QUO) .....	4
4	AUTORISIERUNG AUF BASIS VON VO-ATTRIBUTEN IN DER D-GRID INFRASTRUKTUR .....	4
4.1	Unterstützung von VO-Attributen in der D-Grid-Infrastruktur .....	5
4.1.1	Attribute für die Zugriffskontrolle auf allen D-Grid Ressourcen .....	5
4.1.2	Attribute für die Zugriffskontrolle auf D-Grid Compute-Ressourcen .....	5
4.1.3	Attribute für die Zugriffskontrolle auf Storage-Ressource .....	5
4.1.4	Zukünftige Erweiterungen .....	5
4.2	Einbindung von VO-Attributen in Proxy-Zertifikate .....	6
4.3	Autorisierung mittels VO-Attributen auf Compute Ressourcen .....	6
4.3.1	Zusätzliche Nutzer-Accounts .....	6
4.3.2	Umsetzung im gLite 3.0 LCG Compute Element .....	6
4.3.3	Umsetzung im Globus Toolkit 4.0 .....	7
4.3.4	Umsetzung in UNICORE 5 .....	8
4.4	Autorisierung mittels VO-Attributen auf Storage Ressourcen .....	9
5	FAZIT .....	10

# D-Grid Integrationsprojekt 2 (DGI-2)

## **Autoren:**

Christian Grimm (RRZN, Leibniz Universität Hannover)

Benjamin Henne (RRZN, Leibniz Universität Hannover)

Stefan Piger (RRZN, Leibniz Universität Hannover)

Michael Schiffers (LMU/LRZ)

Wolfgang Ziegler (Fraunhofer SCAI)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IG07014 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

## 1 Management Summary

In diesem Bericht werden Vorschläge für die Einführung einer auf VO-Attributen basierenden Autorisierung in die D-Grid Infrastruktur dargelegt. Durch deren Umsetzung sollen sowohl neue Funktionalitäten für Nutzer<sup>1</sup> der D-Grid Infrastruktur bereitgestellt werden als auch Perspektiven zur Vereinfachung des Managements von Ressourcen aufgezeigt werden. Dieser Bericht stellt eine erste Fassung dar, auf deren Basis die Referenzinstallation [referenzinstallation] weiterentwickelt werden kann. Er soll auch dazu dienen, eine Basis für weitergehende Diskussionen zwischen Communities und DGI-2 im Bereich der Authentifizierungs- und Autorisierungsinfrastrukturen und des VO-Managements zu legen.

## 2 Ziel dieses Dokuments

Dieses Dokument diskutiert Vorschläge, wie eine im D-Grid umsetzbare Autorisierungsinfrastruktur bereitgestellt werden kann, die eine vereinfachte Administration von Nutzerrechten und eine feingranulare Abbildung von Rollen- und Aufgaben der jeweiligen VO auf konkrete Rechte innerhalb der Ressourcen der Grid-Infrastruktur ermöglicht.

Die Vergabe der Attribute wird auf Basis der im D-Grid eingesetzten „Virtual Organization Membership Service“, (VOMS) Instanzen erfolgen, um die Kompatibilität zum etablierten VO-Management zu wahren. Auch soll die erweiterte Autorisierungsinfrastruktur parallel zu den bestehenden Verfahren aufgebaut werden, das mittels Auswertung des Subjekt-DN im (Proxy-)Zertifikat des Nutzers auf dedizierte Accounts für jeden Nutzer abbildet.

Gegenstand der Betrachtungen sind die Vergabe sowie die Durchsetzung von Rechten für die Nutzung der etablierten Ressourcenarten im D-Grid, wie Compute- und Storage-Ressourcen. Eine zukünftige Erweiterung der in diesem Bericht vorgeschlagenen Autorisierungsverfahren ist möglich.

## 3 Autorisierung im D-Grid (Status Quo)

Der Zugang zu den Ressourcen der D-Grid Infrastruktur wird bisher generell identitätsbasiert autorisiert. Zu diesem Zweck werden die „Distinguished Names“ (DN) der Nutzerzertifikate aus den Datenbanken der für die Verwaltung der Virtuellen Organisationen (VO) eingesetzten „Virtual Organization Management Registration Service“ (VOMRS) Instanzen ausgelesen und im „Grid Resource Registry Service“ (GRRS) gespeichert [betriebskonzept].

Der GRRS liefert diese Daten als grid-mapfiles, bzw. im Fall von dCache-Systemen als kpwd-files, an die angemeldeten Ressourcen aus. In diesen Dateien wird eine Zuordnung vorgenommen von DN des Nutzerzertifikats auf einen für jeden Nutzer individuellen Account. Aktuell wird somit eine statische Zuweisung von Rechten zu einzelnen Nutzer durchgeführt.

## 4 Autorisierung auf Basis von VO-Attributen in der D-Grid Infrastruktur

Während der aktuell realisierte Autorisierungsansatz für die Bedürfnisse der im D-Grid arbeitenden Nutzer in den meisten Einsatzszenarien ausreichend zu sein scheint, ist eine Flexibilisierung in einigen Fällen wünschenswert und sinnvoll. Dabei soll es dem Nutzer ermöglicht werden, ihm zur Verfügung stehende Privilegien dynamisch zu aktivieren, um die für die gewünschte Aktion im Grid benötigten Berechtigungen zu erhalten.

Im D-Grid werden die Dienste VOMRS sowie VOMS zur Verwaltung von Virtuellen Organisationen eingesetzt. Diese bieten den Administratoren der VOs Mechanismen zur Zuweisung von Gruppen- und Rollenmitgliedschaften zu Mitgliedern der VO. Darüber hinaus können Mitgliedern auch generische Attribut/Wert-Paare zugewiesen werden.

Für eine auf VO-Attributen basierende Zugriffskontrolle auf Grid-Ressourcen ist eine Übertragung dieser Attribute zu den Ressourcen während des initialen Nutzerzugriffs erforderlich. Diese muss der-

---

<sup>1</sup> Nutzer der D-Grid Infrastruktur sind immer auch Mitglieder mindestens einer unterstützten VO.

art gesichert erfolgen, dass die ausstellende Entität zweifelsfrei nachvollzogen werden kann und eine nachträgliche Änderung der ausgestellten Attribute nicht spurlos möglich ist. Beide Forderungen werden durch die vom VOMS verwendeten digital signierten Attributzertifikate (bzw. die im SAML-VOMS von OMII-Europe [omii-europe] verwendeten SAML-Assertions) erfüllt. Zum Transport zu den Ressourcen im Push-Verfahren werden Attributzertifikate in Proxy-Zertifikate eingebunden, die SAML-Assertions können auch im SOAP-Header (WS-Security extensions) transportiert werden.

#### 4.1 Unterstützung von VO-Attributen in der D-Grid-Infrastruktur

Die Autorisierung von Ressourcenzugriffen soll unter Verwendung von Attributen aus dem D-Grid VO-Management erfolgen. Die Struktur von Virtuellen Organisationen und die daraus abgeleiteten Attribute werden im DGI-2 FG3-2 Milestone-Bericht „Generische VO-Struktur für D-Grid“ beschrieben [vo-struktur], ihre Bedeutung für die Zugriffskontrolle auf D-Grid-Ressourcen wird wie folgt vorgeschlagen:

##### 4.1.1 Attribute für die Zugriffskontrolle auf allen D-Grid Ressourcen

- **`/<voname>/member/<group>/[Role=<role>]`**

Die Einrichtung von Gruppenhierarchien innerhalb der Mitgliedergruppe einer VO dient dazu, VOs mit großen Mitgliederzahlen oder Mitgliedern unterschiedlicher Herkunft übersichtlich strukturieren zu können. Damit ist es beispielsweise möglich, lediglich eine Untermenge der Mitglieder einer VO auf Ressourcen zuzulassen.

##### 4.1.2 Attribute für die Zugriffskontrolle auf D-Grid Compute-Ressourcen

- **`/<voname>/admin/Role=softwareadmin`**

Dieses Attribut kennzeichnet ein VO-Mitglied in der Rolle eines Software-Administrators. Damit verbunden sind Schreibrechte in den VO-Verzeichnissen auf Compute-Clustern. Die VO-Verzeichnisse dienen der Installation von Community-spezifischer Software auf den D-Grid Compute-Ressourcen.

- **`/<voname>/member[/subgroup(s)]/Role=developer`**

Dieses Attribut kennzeichnet ein VO-Mitglied in der Rolle eines Entwicklers. Mitgliedern einer VO soll die temporäre Aktivierung dieser Rolle die Nutzung spezieller Batch-Queues auf Compute-Ressourcen gestatten, die nicht für die Produktivnutzung zugelassen sind und daher eine zügige Abarbeitung von Rechenaufträgen garantieren. In diesen Rollen sollen keine umfangreichen Rechenaufträge bearbeitet werden, sondern lediglich Softwaretests und Übersetzungsläufe durchgeführt werden.

##### 4.1.3 Attribute für die Zugriffskontrolle auf Storage-Ressource

- **`/<voname>/admin/Role=dataadmin`**

Dieses Attribut kennzeichnet ein VO-Mitglied in der Rolle eines Administrators auf Storage-Ressourcen. Die Einrichtung von Storage-Administratoren innerhalb von VOs soll dazu dienen, eine strukturierte Datenhaltung auf den entsprechenden Ressourcen zu etablieren. Dazu benötigen die Storage-Administratoren besondere Schreib- als auch Löschrechte für Dateien und Verzeichnisse auf Storage-Ressourcen (dCache oder OGSA/DAI) unterhalb des der entsprechenden VO zugeordneten Verzeichnisses. Die spezifische Ausgestaltung der Berechtigungen ist abhängig von den jeweiligen Bedürfnissen der VOs.

##### 4.1.4 Zukünftige Erweiterungen

Die in diesem Bericht vorgeschlagene Unterstützung von VO-Attributen für die Zugriffskontrolle auf D-Grid Ressourcen stellt einen ersten Schritt dar. Abhängig vom Bedarf und zukünftigen Anforderungen der D-Grid Communities werden weitere Funktionalitäten in spätere Fassungen aufgenommen.

## 4.2 Einbindung von VO-Attributen in Proxy-Zertifikate

Die Ausgabe von VO-Attributen und ihre Einbindung in die zur Authentifizierung verwendeten Proxy-Zertifikate erfolgt in Form von Attributzertifikaten. Ihr Abruf vom VOMS-Server erfolgt entweder mittels der durch das gLite User Interface Paket bereitgestellten Werkzeuge oder durch webbasierte Nutzerportale.

Eine Unterstützung für VO-Attribute in Form von SAML-Assertions, wie sie durch den SAML-VOMS des Projekts OMII-Europe erstellt werden, ist zu einem späteren Zeitpunkt geplant. Dafür müssen jedoch die beteiligten Komponenten der Grid-Middlewares durchgängig SAML-Assertions für die Autorisierung unterstützen und durch das DGI ausgetestet worden sein.

## 4.3 Autorisierung mittels VO-Attributen auf Compute Ressourcen

Die Zugriffskontrolle auf D-Grid Compute Ressourcen erfolgt, wie bereits in Kapitel 3 dargelegt, auf Basis der Subjekt-DNs der zugreifenden Nutzer. Die Vergabe der Rechte auf der jeweiligen Ressource erfolgt durch Zuordnung der Nutzer zu individuellen Accounts. Dieses Verfahren bietet einige Vorteile sowohl für den Betrieb der D-Grid Ressourcen als auch für die Nutzer. Dazu gehört das vereinfachte Auditing für Ressourcenbetreiber, d. h. die einfache Zuordnung von Aktivitäten zu Verursachern, wie auch die Möglichkeit für die Nutzer, sich ihren Account entsprechend den eigenen Bedürfnissen einzurichten. Daher soll dieses Verfahren auch zukünftig so weit wie möglich beibehalten werden und durch die neuen Funktionalitäten lediglich ergänzt werden.

Die Einführung der neuen Funktionalitäten wird durch Abbildung von VO-Attributen auf spezielle Accounts bzw. Gruppen von Accounts erfolgen. Die folgenden Abschnitte beschreiben für die eingesetzten Middlewares mögliche Vorgehensweisen zur Implementierung der gewünschten Funktionalität, d. h. die erforderliche Konfiguration und die dafür notwendigen Software-Pakete.

### 4.3.1 Zusätzliche Nutzer-Accounts

Auf den Frontend-Systemen [referenzinstallation] sowie auf allen Worker-Nodes werden Accounts zur Implementierung der erwünschten Funktionalitäten benötigt. Dies umfasst einen Account pro VO für den Software-Administrator sowie je nach Bedarf der betreffenden VO einen Pool gleichberechtigter Accounts für die Rolle „developer“.

Der Account für den Software-Administrator muss auf den Worker-Nodes über Schreibrechte im VO-Verzeichnis verfügen, auch ist er üblicherweise dessen Besitzer (owner). Die Accounts für die Rolle „developer“ müssen zu einer Gruppe gehören, die zur Abgabe von Rechenaufträgen in Batch-Queues berechtigen, die nicht für die Produktivnutzung vorgesehen sind und für die mindestens ein Worker-Node reserviert wird. Um wertvolle Produktionsressourcen zu sparen, kann hierfür auch der interaktive Knoten [referenzinstallation] verwendet werden.

### 4.3.2 Umsetzung im gLite 3.0 LCG Compute Element

Das LCG-CE benötigt keine zusätzliche Software für die Unterstützung der Autorisierung mittels VOMS-Attributzertifikaten. Die gebotene Funktionalität umfasst sowohl die Zugriffskontrolle anhand des Subject-DN des Nutzerzertifikats bzw. von VO-Attributen als auch die Abbildung von Subject-DN und VO-Attributen auf Accounts bzw. Account-Gruppen. Die Konfiguration erfolgt am Beispiel der VO „dgtest“, die am Forschungszentrum Karlsruhe verwaltet wird.

## Konfiguration des Grid-mapfile

Im Grid-mapfile (Standardinstallation erfolgt im Verzeichnis /etc/grid-security/) werden die Abbildungen von „Fully Qualified Attribute Name“ (FQAN) im VOMS-Attributzertifikat auf lokale Accounts festgelegt.

Diese werden zusätzlich vor den bestehenden Zuordnungen von Subject-DN auf Account eingefügt. Notwendig sind für jede unterstützte VO auf den Ressourcen Einträge nach folgendem Muster:

```
"/dgtest/admin/Role=softwareadmin/*" dgtestsgm
"/dgtest/member/Role=developer/*" .dgtest
```

Der erste Eintrag legt die Abbildung der Rolle „softwareadmin“ auf den einzelnen Account „dgtestsgm“ fest, der zweite Eintrag bildet die Rolle „developer“ auf die Accounts der Gruppe „dgtest“ ab.

### Konfiguration des Groupmapfile

Das Groupmapfile (Standardinstallation erfolgt im Verzeichnis /etc/grid-security/) hat eine ähnliche Funktion wie das Grid-mapfile, es bildet FQAN-Einträge auf Unix-Gruppen ab. Die für die erweiterten Funktionalitäten benötigten Einträge lauten:

```
"/dgtest/admin/Role=softwareadmin/*" dgtest
"/dgtest/member/Role=developer/*" dgtest
```

### Dateien im Gridmapdir

Für jeden Account im Pool, der für die Rolle „developer“ vorgesehenen ist, muss eine Datei mit dem Namen des Accounts im Verzeichnis gridmapdir (Standardinstallation erfolgt im Verzeichnis /etc/grid-security/) existieren:

```
-rw-r--r-- 1 root root 0 May 29 16:42 dgtest01
-rw-r--r-- 1 root root 0 May 29 16:42 dgtest02
-rw-r--r-- 1 root root 0 May 29 16:42 dgtest03
[...]
```

Diese dienen dazu, mittels eines Hard-Links vom DN des Nutzers auf die entsprechende Datei, reservierte (leased) Accounts zu kennzeichnen. Die Freigabe des entsprechenden Accounts erfolgt durch Löschen des Links.

### Dateien im Vomsdir

Im Vomsdir (Standardinstallation erfolgt im Verzeichnis /etc/grid-security/) müssen die Serverzertifikate der unterstützten VOMS-Server vorhanden sein, um die Überprüfung der Signaturen der durch diese erstellten Attributzertifikate zu ermöglichen. Weiterhin müssen im Verzeichnis „/etc/grid-security/certificates“ regelmäßig aktualisierte „Certificate Revocation Lists“ (CRL) der unterstützten „Certificate Authorities“ (CA) vorliegen.

### 4.3.3 Umsetzung im Globus Toolkit 4.0

Das VOMS-Autorisierungs-Plugin<sup>2</sup> für das Globus Toolkit 4.0 ermöglicht das Auslesen von VO-Attributen aus in Proxy-Zertifikaten integrierten Attribut-Zertifikaten. Die ausgelesenen Attribute können für die Autorisierung und eine Grid-mapfile-äquivalente Abbildung von VO-Attributen auf Accounts verwendet werden. Der folgende beispielhafte Eintrag in der entsprechenden Mapping-Datei bildet die Rolle „softwareadmin“ auf den einzelnen Account „dgtestsgm“ ab.

```
"/dgtest/admin/Role=softwareadmin/Capability=NULL" dgtestsgm
```

<sup>2</sup><http://dev.globus.org/wiki/VOMS>

Der „Dynamic Accounts“ (DA) Service<sup>3</sup> (Globus Incubator Projekt, Technical Preview 6) ermöglicht aufbauend auf der Java VOMS Parsing-Bibliothek die dynamische Zuweisung von Pool-Accounts basierend auf DN und VO-Attributen. Über die DA Factory wird ein dynamischer Account mit einer festgelegten Laufzeit instanziiert und einem Nutzer zugewiesen (Leasing). Die Laufzeit kann verlängert sowie Zuweisungen vor dem Ablauf gelöst werden. Der Zugriff auf die DA Factory wird über DN- und Attribut-basierte ACL und Bannlisten geregelt. Für die Abbildung der DN/VO-Attribute auf Accounts existieren momentan drei System Backends:

- Adduser

Bei der Erstellung eines dynamischen Accounts wird ein neuer Account im System angelegt. Bei Ablauf eines Leases wird der entsprechende Account gelöscht und nicht für andere Nutzer wieder verwendet. (keine Dokumentation zur Konfiguration vorhanden)

- LCMAPS

Die Zuweisung von Accounts aus vordefinierten Pools wird durch LCMAPS<sup>4</sup> getätigt. Sie wird durch Einträge in der Grid-mapfile und der Groupmapfile gesteuert.

Beispiel: Mitgliedern der Gruppe „member“ der VO „dgttest“ mit der Rolle „developer“ werden Accounts aus dem Pool „dgttest“ zugewiesen.

```
"/dgttest/member/Role=developer" .dgttest
```

- Database Pool Accounts

Die Zuweisung von Accounts aus vordefinierten Pools wird Datenbank-basiert verwaltet. Sie wird durch Einträge im Grid-mapfile (Abbildung von DN) und einem Attribut-mapfile gesteuert und entspricht der Konfiguration von LCMAPS mit einer Trennung von DN- und Attribut-Mapping in die zwei Dateien. Account-Leases für DN können persistent vergeben werden. Dabei werden die entsprechenden Accounts bei Lease-Ablauf inaktiv geschaltet, bis selbiger DN wieder einen dynamischen Account benötigt.

Zum dynamischen Anlegen von Accounts muss das Adduser-Backend Kommandos mit root-Rechten ausführen. Administratoren müssen einen Teil ihrer Kontrolle über Accounts abgeben. Dies spricht gegen die Nutzung des Backends, auch wenn es sonst einfach realisiert ist und nie mehr Accounts im System existieren müssen als benötigt werden. Die zwei anderen Backends mit vordefinierten Account-Pools sind aus diesem Grund zu bevorzugen. Für die Nutzung des LCMAPS-Backend muss zusätzlich die Software LCMAPS installiert werden. Für eine einfache Installation ist daher das Database-Pool-Accounts-Backend zu empfehlen, da es keine weiteren Software-Abhängigkeiten mit sich bringt. Um konkrete Aussagen über den Betrieb von Pool-Accounts mittels des Dynamic Accounts Services machen zu können, muss das aktuelle Technical Preview des Incubator Projektes noch ausführlich auf seine Stabilität hin getestet werden. Auch sind noch Informationen von den Entwicklern über die Zukunft dieses Projektes in Erfahrung zu bringen.

#### 4.3.4 Umsetzung in UNICORE 5

Die Umsetzung der hier vorgeschlagenen Funktionalitäten ist mit UNICORE Version 5 ohne weitgehende Modifikationen der Referenzinstallation nicht möglich. Die notwendige Unterstützung von VOMS-Attributzertifikaten zur Autorisierung in UNICORE 5 wurde in Form von Erweiterungen bereitgestellt, die im Rahmen des D-Grid GAP-Projekts „IVOM“ [ivom] entwickelt wurden.

Nach Diskussion mit dem DGI FG2 (D-Grid Betrieb) zeichnet sich jedoch ab, dass ein Übergang auf eine neuere Version von UNICORE aus verschiedenen Gründen, wie der Gewährleistung eines langfristigen Support für die Middleware, sinnvoll und daher für die D-Grid Infrastruktur anzustreben ist. Der zu treibende Aufwand für eine Erweiterung der im Einsatz befindlichen Softwarekonfiguration ist daher nicht mehr als nachhaltig anzusehen.

<sup>3</sup>[http://dev.globus.org/wiki/Incubator/Dynamic\\_Accounts](http://dev.globus.org/wiki/Incubator/Dynamic_Accounts)

<sup>4</sup><http://www.nikhef.nl/grid/lcaslcmaps/>

Neuere Versionen von UNICORE bieten bereits Funktionalitäten zur Autorisierung anhand der durch den SAML-VOMS ausgestellten SAML-Assertions. Um einen stabilen Betrieb zu gewährleisten, müssen diese Komponenten (UNICORE Version 6.x sowie der SAML-VOMS) vor einer Übernahme in den D-Grid Regelbetrieb ausführlich ausgetestet werden. Diese Arbeiten werden in enger Abstimmung mit dem D-Grid FG2 nach Veröffentlichung von stabilen Fassungen der genannten Software-Komponenten durchgeführt werden.

#### **4.4 Autorisierung mittels VO-Attributen auf Storage Ressourcen**

Die generische D-Grid VO-Struktur sieht die Einrichtung der Rolle eines Administrators auf Storage-Ressourcen für jede der D-Grid VOs vor. Diese sollen über spezielle Rechte verfügen, um die Datenhaltung im jeweiligen VO-Verzeichnis auf den Storage-Ressourcen zu koordinieren.

Die Umsetzung des VOMS-FQAN „/(<voname>/admin/Role=dataadmin“ auf die damit verbundenen Rechte erfolgt lokal auf den Storage-Ressourcen. Die konkrete Ausgestaltung der mit der Rolle des Administrators auf Storage-Ressourcen verbundenen Rechte ist abhängig von den Bedürfnissen der VOs. Als Standardkonfiguration werden folgende Funktionalitäten empfohlen (vgl. Abbildung 1):

1. Einrichtung eines exklusiven Schreibrechtes für die Rolle „dataadmin“ im VO-Verzeichnis auf den Storage-Ressourcen. Für einfache VO-Mitglieder sollte in diesem Verzeichnis lediglich ein Leserecht existieren.
2. Zusätzlich ist ein Verzeichnis für jedes VO-Mitglied unterhalb des VO-Verzeichnisses einzurichten, in dem für dieses VO-Mitglied Schreibrecht besteht. Abgesehen von Administratoren in der Rolle „dataadmin“ sollen andere VO-Mitglieder dort lediglich über Leserechte verfügen. Wenn von der VO gewünscht, kann der Zugriff auf dieses Verzeichnis auch exklusiv für das entsprechende VO-Mitglied und den Administrator gestaltet werden.
3. Optional können unterhalb des VO-Verzeichnisses noch Verzeichnisse für den gemeinsamen Zugriff aller VO-Mitglieder eingerichtet werden, die beispielsweise dem Datenaustausch zwischen VO-Mitgliedern oder zur Ablage von Experimentdaten dienen. Da diese Konfiguration jedoch VO-spezifisch ist, ist sie nicht Teil der Standardkonfiguration.

Abbildung 1: Verzeichnisstruktur auf Storage-Ressourcen

Die Erarbeitung von Konfigurationsvorschlägen für die in der D-Grid Infrastruktur implementierten Dienste auf Basis von dCache und OGSA/DAI wird in Absprache mit DGI-2 Fachgebiet 4 (vgl. FG4 AP5) erstellt.

## 5 Fazit

Die in diesem Bericht vorgeschlagenen Erweiterungen der bisher ausschließlich identitätsbasierten Autorisierung auf eine sowohl identitäts- als auch attributbasierte Autorisierung ermöglichen eine feingranularere Ausdifferenzierung der Berechtigungen für Ressourcenzugriffe innerhalb des D-Grid.

Die Vorschläge für die in der aktuellen Referenzinstallation einsetzten Middleware-Komponenten für den Zugriff auf Rechenressourcen gLite 3.0 und Globus Toolkit 4.0 sind mit einigen Modifikationen bzw. Erweiterungen der Referenzinstallation umsetzbar. Für die Middleware UNICORE sollten die Vorschläge erst nach der Aktualisierung der Referenzinstallation auf die neuere Version 6.1 oder später umgesetzt werden. Im Bereich der Speicherressourcen sind die Vorschläge noch mit anderen Fachgebieten innerhalb des DGI-2 zu diskutieren und mit den Communities abzustimmen.

Die bisher exklusiv eingesetzten Verfahren der identitätsbasierten Autorisierung innerhalb der AAI werden beibehalten und durch die in diesem Bericht vorgelegten Vorschläge ergänzt. Auf diese Weise wird einerseits auf die Bedürfnisse der Ressourcenbetreiber im Bereich des Auditing (vereinfachtes Auditing durch Benutzer-individuelle Accounts) Rücksicht genommen und andererseits flexiblere Nutzungsmöglichkeiten der Ressourcen (Attribut-Abbildung auf Community- und Pool-Accounts) ermöglicht.

**Abkürzungen**

AUP	Acceptable Use Policy
DN	Distinguished Name
FQAN	Fully Qualified Attribute Name
IVOM	Interoperabilität und Integration der VO-Management Technologien im D-Grid
LCMAPS	Local Credential Mapping Service
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
VO	Virtuelle Organisation
VOMS	VO Membership Service
VOMRS	VO Management Registration Service

## Referenzen

- [betriebskonzept] Betriebskonzept für das D-Grid  
<http://www.d-grid.de/uploads/media/D-Grid-Betriebskonzept.pdf>
- [ivom] Interoperabilität und Integration der VO-Management Technologien im D-Grid <http://www.d-grid.de/index.php?id=314>
- [omii-europe] OMII-Europe Homepage  
<http://omii-europe.org/OMII-Europe/>
- [referenzinstallation] D-Grid Referenz-Installation  
<http://www.d-grid.de/index.php?id=297>
- [vo-struktur] Generische VO-Strukturen für das D-Grid