



Fachgebiet 3.2  
AAI/VO

# **Beratung weiterer Communities im D-Grid**

## **Autoren**

Christian Grimm (RRZN, Leibniz Universität Hannover)

Benjamin Henne (RRZN, Leibniz Universität Hannover)

Stefan Piger (RRZN, Leibniz Universität Hannover)

Michael Schiffers (LMU/LRZ)

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.

**Inhalt**

1	MANAGEMENT SUMMARY .....	4
2	AKZEPTANZ DER BESTEHENDEN AAI .....	4
2.1	Weiterentwicklung der AAI.....	4
3	SCHULUNGEN, WORKSHOPS UND VORTRÄGE .....	4
4	INDIVIDUELLE BERATUNGSLEISTUNGEN FÜR RESSOURCEN- UND SERVICE-ANBIETER ..	4
5	REALISIERUNG ATTRIBUT-BASIERTER AUTORISIERUNG DER ROLLE „VO-SOFTWARE-ADMINISTRATOR“ MIT GLITE UND BEISPIELUMSETZUNG FÜR DIE HEP-VO .....	5
6	BERATUNG VON GDI-GRID.....	5
7	STATUS UND AUSBLICK .....	5

## **1 Management Summary**

Die Beratung von bestehenden und neuen Communities in D-Grid durch FG-3.2 dient dazu, die existierenden und geplanten Funktionen der Authentifizierungs- und Autorisierungsinfrastruktur (AAI) möglichst optimal durch die Communities nutzen zu lassen. Die Communities werden über die Möglichkeiten der aktuellen D-Grid-Infrastruktur informiert und wo nötig geschult. Basierend auf den Anforderungen der Communities werden Möglichkeiten der Verbesserung der existierenden Infrastruktur identifiziert und auf eine mögliche Umsetzung im Rahmen der D-Grid-Infrastruktur hin untersucht. Im zweiten Halbjahr 2008 wurden diese Ziele durch entsprechende individuelle Schulungen und Beratungsleistungen verfolgt.

## **2 Akzeptanz der bestehenden AAI**

Die momentan fast rein Identitäts-basierte Autorisierung innerhalb der D-Grid-Infrastruktur scheint die Mitglieder der Communities zufrieden zu stellen. Eine feingranulare Autorisierung basierend auf Nutzer-Attributen, wie schon im Rahmen des IVOM-Projektes erarbeitet, wurde den Communities bei verschiedenen Veranstaltungen vorgestellt, doch daraufhin bei DGI-2 FG-3.2 gering nachgefragt. Für die zukünftige Entwicklung verschiedener Community-Projekte zeichnet sich jedoch die Notwendigkeit feingranularer Autorisierung ab (vgl. Abschnitte 5 und 6).

### **2.1 Weiterentwicklung der AAI**

Die bestehende AAI soll in 2009 weiterentwickelt werden und auf den D-Grid-Ressourcen im Rahmen eines aktualisierten Betriebskonzeptes und einer neuen Referenzinstallation etabliert werden. Die bisher Identitäts-basierte Autorisierung soll um Funktionen der VO-Attribut-basierten Autorisierung erweitert werden. Hierzu kooperiert FG-3.2 mit den entsprechenden Fachgebieten am FZK, FZJ und RRZN. Über die Neuerungen werden die Communities beim All-Hands-Meeting 2009 informiert.

## **3 Schulungen, Workshops und Vorträge**

In H2/08 wurden keine allgemeinen Schulungen und Workshops für den Bereich AAI/VO veranstaltet. Die Beratung fand individuell aufgrund einzelner Anfragen statt. Im Rahmen des „Grid Security Workshop for Administrators and Developers“ der GridKa School 2008 wurde mit dem Vortrag [futureconcepts] über die aktuelle AAI des D-Grids sowie zukünftige Entwicklungsmöglichkeiten und Ziele informiert.

## **4 Individuelle Beratungsleistungen für Ressourcen- und Service-Anbieter**

Im D-Grid spielen neben den Communities die Ressourcen- und Service-Anbieter sowie die Betriebsorganisation eine nicht unwesentliche Rolle. Der Fokus der individuellen Beratungsleistungen lag daher in H2/08 primär auf der Instruktion dieser Zielgruppen.

Die D-Grid Betriebsorganisation (hier FZJ) wurde nicht nur zu den geplanten Authentifizierungs- und Autorisierungsmechanismen beraten. Es wurde auch vereinbart, die Arbeiten an einem modifizierten Betriebskonzept im Rahmen der entsprechenden FG-Aufträge gemeinsam in 2009 fortzuführen, wie zuvor beschrieben.

Eine entsprechende Beratungsleistung wurde auch bei einzelnen Ressourcen-Anbietern durchgeführt. So wurde beispielsweise am Leibniz-Rechenzentrum (LRZ) damit begonnen, über die Charakteristika Attribut-basierter Autorisierung aufzuklären. Auch hier wurde vereinbart, diese Beratung in 2009 weiterzuführen. Die wesentlichen Fragen, die in diesem Kontext zu klären sind, beziehen sich auf die Umsetzung Rollen-basierter Rechte auf D-Grid-Ressourcen (speziell auf die Umsetzung über heterogener Middleware) und die Auswirkungen bei den Ressourcen-Anbietern (Müssen wir für Attribut-basierte Autorisierung zusätzliche Dienste bereitstellen?).

## 5 Realisierung Attribut-basierter Autorisierung der Rolle „VO-Software-Administrator“ mit gLite und Beispielumsetzung für die HEP-VO

Auf den Ressourcen des Regionalen Rechenzentrums für Niedersachsen (RRZN) wurde für die Middleware gLite die in [attribute] beschriebene Rolle „softwareadmin“ umgesetzt und in der HEP-Community erstmals genutzt. Für gLite muss dazu nur das grid-mapfile erweitert werden, da die Middleware alles Notwendige mitbringt. Vergleichsweise für das Globus Toolkit 4 muss zusätzliche Software (VOMS Policy Information Point und Policy Decision Point) auf jeder Ressource installiert und konfiguriert werden.

Das VO-Attribut „Role=softwareadmin“ kennzeichnet ein VO-Mitglied in der Rolle eines VO-Software-Administrators. Das Einnehmen dieser Rolle ermöglicht dem Benutzer das Schreiben in ein VO-spezifisches (Software-)Verzeichnis, welches von VO-Mitgliedern ohne diese Rolle nur gelesen werden kann. Der Software-Administrator kann auf diese Weise VO-spezifische Software installieren, die von den Mitgliedern der VO im Folgenden verwendet werden kann.

Für die HEP-VO wurde dieser Autorisierungsmechanismus beispielhaft umgesetzt. Das dabei genutzte `grid-mapfile` besitzt folgende Struktur (Auszug):

```
"/hepcg/admin/Role=softwareadmin/Capability=NULL" uhhpsgm
"/C=DE/O=GermanGrid/OU=TU-Dortmund/CN=Beispiel Benutzer" uhhp0816
```

Der einfache Benutzer, wie der im Auszug dargestellte *Beispiel Nutzer*, wird wie bisher auf seinen Einzelaccount `uhhp0816` abgebildet. Dieser ist wie jedes VO-Mitglied in der Unix-Gruppe `uhhp`. Ein Nutzer mit der VO-Rolle `softwareadmin` in seinen Credentials wird hingegen auf den Account des Software-Admins `uhhpsgm` abgebildet.

Unix-Rechte des VO-Verzeichnisses für HEP-VO in `/home/vodirs:`

```
drwxr-x--- 4 uhhpsgm uhhp 3864 24. Okt 11:06 hp
```

Der Unix-Benutzer des Software-Administrator kann auf das VO-Verzeichnis schreibend zugreifen. Alle Benutzer der Gruppe `hp`, also alle Mitglieder der HEP-VO, können die Inhalte des Verzeichnisses lesen.

## 6 Beratung von GDI-Grid

Im Projekt „GDI-Grid“ stehen Nutzern Speicherressourcen zur Verfügung, die über die Zugriffssysteme dCache und OGSA-DAI genutzt werden. Die Speicherressourcen stehen im Projekt einer großen Zahl von Nutzern zur Verfügung und die Daten unterliegen häufig Copyright- und Lizenzbeschränkungen. Somit ist eine Zugriffskontrolle für die gespeicherten Daten von hoher Wichtigkeit. Um eine effektive Zugriffskontrolle zu realisieren soll für die beiden Systeme eine VO-Attribut-basierte Autorisierung realisiert werden [gdi-m18]. Da FG-3.2 schon vorher Untersuchungen bezüglich dCache und Attribut-basierter Autorisierung getätigt hatte, konnte GDI-Grid dazu beraten werden. Die Beratung bezüglich VO-Attribut-basierter Autorisierung für dCache und OGSA-DAI wird in 2009 fortgeführt, wenn diese im Rahmen der in Abschnitt 2.1 beschriebenen Arbeiten weiter untersucht werden.

## 7 Status und Ausblick

Die beschriebenen Beratungsleistungen werden in 2009 fortgeführt. Aufgrund der Entwicklung der Arbeiten in FG-3.2 sind für das Jahr 2009 einige Veränderungen im Bereich der AAI der D-Grid-Infrastruktur zu erwarten. Sobald die für Juli 2009 geplante Referenzinstallation mit VO-Attribut-basierter Autorisierung durch die Ressourcen-Betreiber umgesetzt wird, stehen den Communities neue, feingranulare Methoden der Autorisierung zur Verfügung.

Um die VO-Attribut-basierte Autorisierung im D-Grid umzusetzen, müssen dazu zwei verschiedenen Aufgaben bewältigt werden. Zum einen müssen die Communities aufgeklärt werden, welchen Mehrwert sie durch die neuen Methoden erhalten und auch welche Funktionen damit nicht umgesetzt werden können. Zum anderen muss die Attribut-basierte Autorisierung wie geplant in Betriebskonzept und Referenzinstallation aufgenommen werden und vor allem auch von den Ressourcen-Anbietern auf den Ressourcen umgesetzt werden, um sie den Communities bereitzustellen.

## Abkürzungen

AAI	Authentifizierungs- und Autorisierungsinfrastruktur
LRZ	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
RRZN	Regionales Rechenzentrum für Niedersachsen
VO	Virtuelle Organisation

## Referenzen

- [attribute] Definition von Attributen für die Autorisierung auf D-Grid Ressourcen  
[http://www.rrzn.uni-hannover.de/fileadmin/ful/projekte/DGI-2/DGI-2\\_FG-3.2\\_Definition\\_Attribute\\_Autorisierung\\_D-Grid.pdf](http://www.rrzn.uni-hannover.de/fileadmin/ful/projekte/DGI-2/DGI-2_FG-3.2_Definition_Attribute_Autorisierung_D-Grid.pdf)
- [futureconcepts] Future concepts of authentication and authorization in grid computing – An Outlook by the example of D-Grid, [http://gks08.fzk.de/Talks/2008\\_09\\_12\\_Friday/Future\\_concepts\\_of\\_authentication\\_and\\_authorization\\_in\\_grid\\_computing\\_Benjamin\\_Henne.pdf](http://gks08.fzk.de/Talks/2008_09_12_Friday/Future_concepts_of_authentication_and_authorization_in_grid_computing_Benjamin_Henne.pdf)
- [gdi-m18] GDI-Grid Meilenstein 18 Arbeitspaket 2 Datenmanagement – Autorisierung, Version 0.1, 19.12.2008