



Fachgebiet 3.2
AAI/VO

Generische VO-Strukturen für das D-Grid

Autoren

Christian Grimm (RRZN, Leibniz Universität Hannover)

Benjamin Henne (RRZN, Leibniz Universität Hannover)

Stefan Piger (RRZN, Leibniz Universität Hannover)

Michael Schiffers (LMU München/LRZ Garching)

Wolfgang Ziegler (Fraunhofer SCAI St. Augustin)

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	PRÄAMBEL	4
2	MANAGEMENT SUMMARY.....	4
3	ZIEL DIESES DOKUMENTS	4
4	GRUNDBEGRIFFE.....	5
4.1	Virtuelle Organisation.....	5
4.2	Virtuelle Ressource und virtueller Dienst.....	6
4.3	Mitglied.....	6
4.4	Gruppe	6
4.5	Rolle	6
4.6	Capability.....	6
5	ANFORDERUNGEN AN GENERISCHE VO-STRUKTUREN	6
5.1	Bestehende VO-Strukturen im D-Grid	6
5.2	VO-Managementprozesse im D-Grid.....	7
6	ABLEITUNG EINER GENERISCHEN VO-STRUKTUR.....	8
6.1	Allgemeine Einordnung.....	8
6.2	Interne VO-Struktur	9
6.2.1	Gruppenstruktur	9
6.2.2	Rollenstruktur.....	10
6.2.3	Capability-Struktur	11
6.3	Umsetzung	11
7	GENERISCHE VO-PROZESSE	11
7.1	Prozesse zum Aufbau und Abbau einer Virtuellen Organisation.....	12
7.1.1	Gründung einer VO (<i>createVO</i>).....	13
7.1.2	Einrichten einer VO (<i>initVO</i>)	13
7.1.3	Terminierung einer VO (<i>terminateVO</i>).....	14
7.2	Prozesse zum Betrieb einer Virtuellen Organisation	14
7.2.1	Aufnahme von Mitgliedern (<i>addMember</i>)	14
7.2.2	Änderung der Mitgliedschaft (<i>changeMember</i>)	15
7.2.3	Sperren, Freigeben und Ausscheiden von Mitgliedern (<i>suspendMember</i> , <i>releaseMember</i> , <i>deleteMember</i>).....	15
7.2.4	Management von Ressourcen (<i>addResource</i> , <i>modifyResource</i> , <i>lockResource</i> , <i>unlockResource</i> , <i>removeResource</i> , <i>logResourceUsage</i>)	15
7.2.5	Management von Rollen (<i>createRole</i> , <i>modifyRole</i> , <i>deleteRole</i>)	16
7.2.6	Management von Gruppen (<i>createGroup</i> , <i>modifyGroup</i> , <i>deleteGroup</i>).....	16
8	INSTANZIIERUNG IM KONKRETEN FALL	16

1 Präambel

Dieses Dokument baut an verschiedenen Stellen auf Arbeiten anderer Fachgebiete auf, die sich zum Teil noch im Entwicklungsstadium befinden. Die Ergebnisse dieser Arbeiten liegen daher in einigen Bereichen vollständig vor, in anderen Teilen nur partiell und in wieder anderen sind sie erst skizziert. Werden Resultate der letzten beiden Kategorien verwendet, werden die entsprechenden Textpassagen durch die Symbole „►“ und „◄“ eingerahmt und farbig hinterlegt. Sie werden in späteren Versionen dieses Dokumentes vervollständigt werden.

2 Management Summary

VOs werden in der Regel von den D-Grid-Communities im Rahmen von Projekten gebildet. Dies geschieht typischerweise Community-intern. Zunehmend werden aber auch Community-übergreifende und Community-unabhängige VO-Gründungen gewünscht. Dazu ist ein Rahmenwerk erforderlich, das einerseits die bisher schon spezifizierten VO-Rahmen- und Betriebskonzepte integriert, andererseits aber auch zukünftigen VOs ein generisches Struktur- und Prozessgerüst bereitstellt, das für deren spezifische Anforderungen instanziiert werden kann.

In diesem Dokument, das als Teilergebnis der Teilaufgabe 1.2. des Fachgebietes 3.2 des DGI-2 zu sehen ist, wird eine generische VO-Struktur und ein dazu passendes Rahmenwerk für VO-Management-Prozesse dargestellt. Der Bericht orientiert sich dabei wesentlich an den Vorarbeiten und Ergebnissen früherer D-Grid-Projekte. Das finale Dokument wird zum Meilenstein 9 (Dezember 2009) geliefert.

Nach einer kurzen begrifflichen Einordnung werden die Anforderungen an eine generische VO-Struktur und die damit zusammenhängenden Managementprozesse spezifiziert, bevor diese selbst dargestellt werden. Die vorgeschlagene VO-Struktur orientiert sich an den D-Grid *best practices* und dem Prinzip des *separation of concern*. Insofern induziert die hier vorgeschlagene VO-Struktur eine (hierarchische) Gruppenstruktur mit einer Rollenstruktur.

Als generische Ausprägungen von Gruppen werden eine Mitgliedergruppe, eine Gastgruppe, eine Administratorgruppe und eine Supportgruppe vorgeschlagen.

Als generische Ausprägung von Rollen werden Gruppen-Manager, VO-Administratoren, Software-Administratoren, Datenmanagement-Administratoren, VO-Repräsentanten, Datenschutz-Kontakte, Accounting Manager und Support-Kontakte vorgeschlagen. Spezielle Rollen bilden der Datenschutzkontakt, der für die Einhaltung von Richtlinien und Policies verantwortlich zeichnet und für Entwicklungsarbeiten Software-Entwickler und –Tester. Die generischen Gruppen und Rollen werden als Fully Qualified Attribute Name (FQAN)¹ dargestellt.

Die für VOs relevanten generischen Management-Prozesse orientieren sich am Lebenszyklus der VO. Insofern werden in diesem Dokument Prozesse zum Aufbau und Abbau einer Virtuellen Organisation sowie zum Betrieb einer VO vorgeschlagen. Die Betriebsprozesse beinhalten die Aufnahme von Mitgliedern, die Änderung von Mitgliedschaften, das Sperren, Freigeben und Ausscheiden von Mitgliedern, das Management von Ressourcen während der Lebenszeit einer VO sowie das Management von Gruppen und Rollen.

3 Ziel dieses Dokuments

Ziel dieses Dokuments ist die Festlegung generischer Strukturen Virtueller Organisationen (VO) im D-Grid. VOs werden in der Regel von den D-Grid-Communities im Rahmen von Projekten gebildet, in der Vergangenheit eher Community-intern, in Zukunft zunehmend auch Community-übergreifend und

¹ Im Sinne [voms]

Community-unabhängig. VOs manifestieren sich dabei in den Abbildungen von Individuen (in der Regel Community-Mitglieder) auf VO-Mitgliedschaften, die wiederum die Grundlage für Autorisierungsmechanismen innerhalb der D-Grid-Infrastruktur bilden.

Die von den bestehenden² Communities geforderte generische VO-Struktur und ein dazu passendes Rahmenwerk für VO-Management-Prozesse sind Gegenstand dieses Berichts.

Der Bericht orientiert sich wesentlich an den Ergebnissen früherer D-Grid-Projekte, insbesondere [vorahmenkonzept], [betriebskonzept] und [ivom].

4 Grundbegriffe

4.1 Virtuelle Organisation

Das Konzept der *Virtuellen Organisation* ist in Grids von zentraler Bedeutung und ausführlich in der Literatur behandelt. Die für diesen Bericht gültige Auffassung orientiert sich an der Definition des VO-Rahmenwerks [vorahmenkonzept] nach der VOs aus Personen und/oder technischen Ressourcen autonomer realer Organisationen (*legal entities*) mit dem Ziel rekrutiert werden, kooperativ und koordiniert zur Lösung eines (oder mehrerer) Probleme -- dem eigentlichen Zweck der VO -- beizutragen. Im Folgenden wird daher unter einer Virtuellen Organisation

„ein permanentes oder zeitlich begrenztes Konsortium geographisch verteilter Individuen, Gruppen, Organisationseinheiten oder ganzer Organisationen“ verstanden, *„die Teile ihrer physischen oder logischen Ressourcen und Dienste, ihre Kenntnisse und Fähigkeiten sowie Teile ihrer Informationsbasis derart zusammenlegen, dass die gemeinsamen Ziele erreicht werden können.“*

Die wesentlichen Konzepte und deren Zusammenhänge sind in Abbildung 1 schematisch dargestellt.

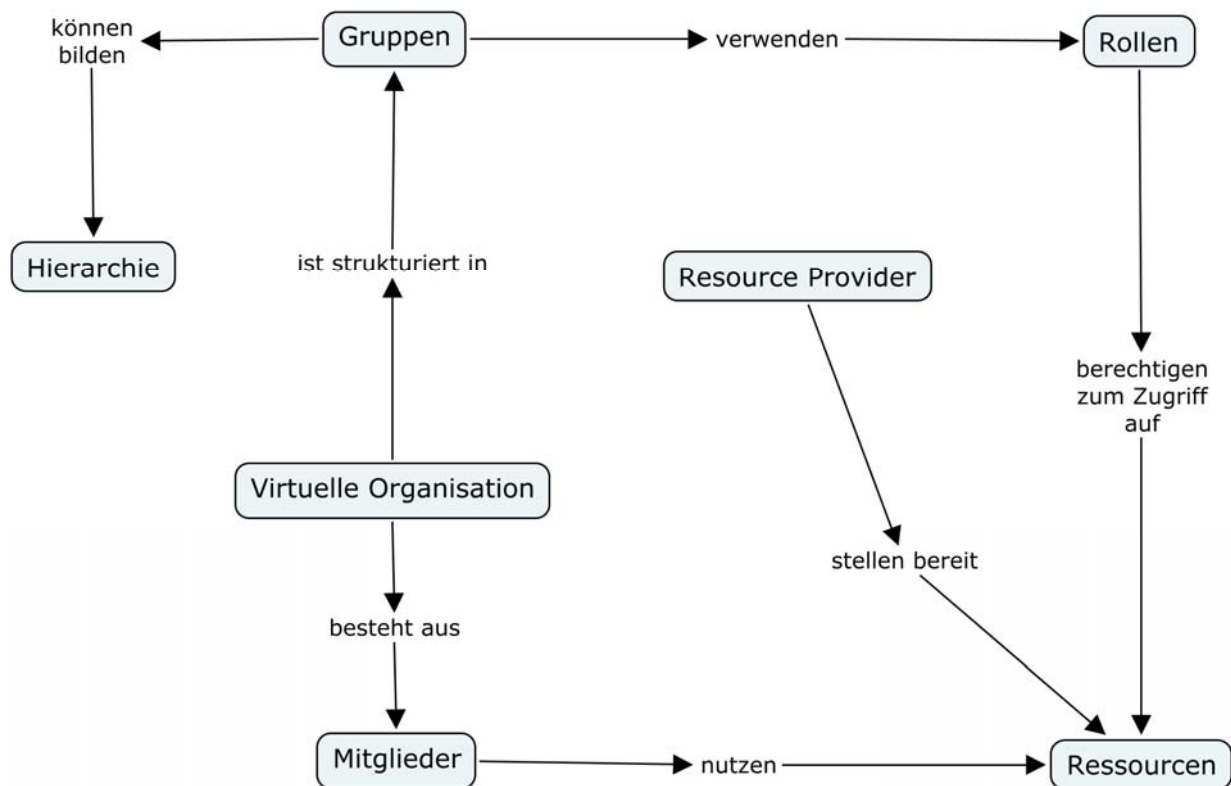


Abbildung 1: Allgemeine VO-Konzepte

² per 24. Juni 2008

4.2 Virtuelle Ressource und virtueller Dienst

Eine VO stellt *virtuelle Ressourcen* und *virtuelle Dienste* bereit. Eine Ressource ist virtuell relativ zu einer VO wenn auf sie aus der VO zugegriffen werden kann. Ebenso ist ein Dienst virtuell relativ zu einer VO wenn er aus der VO benutzt werden kann. Virtuelle Dienste und virtuelle Ressourcen werden in dieser Nomenklatur von einer VO *bereitgestellt*.

4.3 Mitglied

Ein Individuum ist *Mitglied* einer VO wenn es autorisiert ist, die von der VO bereitgestellten virtuellen Ressourcen und virtuellen Dienste zu nutzen oder einer Rolle in der VO zugeordnet werden kann. Eine Gruppe von Individuen ist Mitglied einer VO wenn jedes Gruppenmitglied auch Mitglied der VO ist, eine Organisation ist Mitglied einer VO, wenn mindestens ein Organisationsmitglied auch Mitglied der VO ist oder wenn die Organisation eine Ressource bzw. einen Dienst bereitstellt, auf die VO-Mitglieder zugreifen können.

4.4 Gruppe

Gruppen dienen innerhalb einer VO der administrativen Ordnung von VO-Mitgliedern. Sie geben alleine keine Auskunft über die Aufgabe ihrer Mitglieder und werden nur zusammen mit den in ihnen möglicherweise definierten Untergruppen sowie Rollen zur Autorisierung herangezogen. Konzeptionell fungiert die VO selbst als Wurzel-Gruppe einer Gruppenhierarchie. Insofern ist jedes VO-Mitglied immer mindestens einer Gruppe zugeordnet. Gruppen partitionieren VOs allerdings nicht im strengen Sinn, da sich Gruppen überlappen können.

Bei Bedarf können zusätzlich zu den Gruppen *Untergruppen* definiert werden, um VO-Mitglieder mit gemeinsamen Merkmalen zusammenzufassen. Dies kann beispielsweise die Zugehörigkeit zu einer gemeinsamen Disziplin sein oder die Tätigkeit in der gleichen Einrichtung.

4.5 Rolle

Rollen von VO-Mitgliedern geben Auskunft über deren Aufgabengebiete, die über die mit der einfachen Mitgliedschaft verbundenen hinausgehen. Diese können beispielsweise reflektieren, dass ein Mitglied spezielle Aufgaben in der Administration der VO ausübt. Rollen sind nur in Gruppen gültig.

Jedes Individuum X, das einer VO Y beitrifft, ist damit a priori auch der (Wurzel)Gruppe Y zugeordnet mit der Rolle „NULL“, allerdings wird dieser Spezialfall selten explizit dargestellt.

4.6 Capability

Capabilities dienen der direkten Berechtigungsvergabe an Rollen. Damit werden explizit Nutzungsberechtigungen vergeben, die über die eigentlichen Rollenberechtigungen hinausgehen (bzw. diese einschränken). Dies kann beispielsweise die Nutzung von Software-Lizenzen betreffen. Capabilities werden allerdings von aktuellen Grid-Middleware-Konzepten nicht mehr unterstützt, sie sind deshalb als Konzept in Abbildung 1 auch nicht aufgeführt. Der Vollständigkeit halber seien sie hier jedoch noch kurz erwähnt.

5 Anforderungen an generische VO-Strukturen

5.1 Bestehende VO-Strukturen im D-Grid

In [vorahmenkonzept] und [betriebskonzept] wurden die im D-Grid verwendeten VO-Konzepte auf der Basis der oben formulierten Definitionen ausführlich dargestellt. Dort wurde gezeigt, welches Rollenmodell einer D-Grid-VO zu Grunde liegt, welche Prozesse den Lebenszyklus einer VO bestimmen und welche Prozesse die operative Phase einer VO (z.B. Management von Mitgliedschaften) ausmachen.

Außerdem wurde diskutiert, welche unterschiedlichen VO-Konzepte die einzelnen Communities³ verfolgen und mit welchen Werkzeugen deren Sichten auf VOs unterstützt werden. Diese Vorarbeiten können wie folgt zusammengefasst werden:

VOs sind immer einer Community zugeordnet. Die Gründung einer VO im D-Grid muss vom Sprecher dieser „Home Community“ genehmigt werden.

- ► Grundsätzlich können VOs zwar auch ohne übergeordnete Community gegründet werden können (siehe auch [workflow]), dieser Fall wird jedoch aktuell im D-Grid noch nicht unterstützt. ◀

VOs können sich überlappen (partiell und komplett), indem sich Mitglieder bei mehreren VOs (mit demselben Grid-User-Zertifikat) anmelden.

Im Kontext des VO Managements treten verschiedene Rollen auf, die in der Realität allerdings in den einzelnen Communities mehr oder weniger stark ausgeprägt sind und zum Teil in den Communities unterschiedliche Semantiken besitzen:

- Resource und Service Provider,
- Community Sprecher,
- Community VO-Manager (VO-Repräsentant),
- D-Grid VO-Manager,
- VO-Administrator,
- Gruppen-Manager,
- VO-Mitglied.

VOs werden auf der Basis von D-Grid-spezifischen Richtlinien für VOs gegründet und betrieben. Diese regeln, wie VO-Mitglieder identifiziert, aufgenommen, abgelehnt, gesperrt oder entfernt werden:

- VOs erlassen *VO-AUPs*⁴ für ihre Mitglieder, die die Nutzung des D-Grid und dessen Ressourcen regeln.
- Provider erlassen *Resource-AUPs*, die die Nutzung der für das D-Grid bereitgestellten Ressourcen regeln.

VOs benötigen einen Ansprechpartner für Support- und Sicherheitsfragen.

VOs können eine hierarchische Gruppenstruktur besitzen.

Gruppen können eine (nicht-hierarchische) Rollenstruktur besitzen.

5.2 VO-Managementprozesse im D-Grid

Die im D-Grid erforderlichen VO-Managementprozesse sind ausführlich in [vorahmenkonzept] und [betriebskonzept] diskutiert. Für eine generische Betrachtung virtueller Organisationen sind die folgenden Prozesse von Bedeutung:

Gründung einer VO

Einrichten einer VO

Terminierung einer VO

Betrieb einer VO, hier insbesondere die Teil-Prozesse

- Mitgliedsmanagement

³ Genauer: Die zu dem damaligen Zeitpunkt am D-Grid teilnehmenden Communities

⁴ AUP: Acceptable Use Policy

- Aufnahme von Mitgliedern
- Ändern des Mitgliedstatus
- Sperren und Freigeben von Mitgliedern
- Ausscheiden von Mitgliedern
- Ressourcen/Service-Management
 - Aufnahme von Ressourcen/Services
 - Ändern von Ressourcen/Services
 - Sperren und Freigeben von Ressourcen/Services
 - Entfernen von Ressourcen/Services
 - Logging von Ressourcen/Service-Nutzung
 - Abrechnen der Ressourcen/Service-Nutzung
- Gruppenmanagement
 - Bildung von Gruppen
 - Ändern von Gruppen
 - Löschen von Gruppen
- Rollenmanagement
 - Bildung von Rollen
 - Ändern von Rollen
 - Entfernen von Rollen

6 Ableitung einer generischen VO-Struktur

Aus diesen Vorarbeiten lässt sich eine generische VO-Struktur für das D-Grid ableiten, die sich einerseits auf bestehende VO-Strukturen in den bisherigen Communities abbilden lässt (*best practices*), die andererseits aber auch flexibel genug ist, auch zukünftigen VO-Anforderungen gerecht zu werden.

Unter einer *generischen* VO-Struktur ist dabei die Struktur einer abstrakten VO zu verstehen, die für konkrete VOs instanziiert werden kann und dabei deren Komponenten und Konzepte „erbt“ (im Sinne objektorientierter Konstruktion).

6.1 Allgemeine Einordnung

Für die allgemeine Einordnung einer virtuellen Organisation orientiert sich dieser Bericht an den *best practices* des Rahmenkonzeptes [vorahmenkonzept] und des Betriebskonzeptes [betriebskonzept]. Diese setzen für jede VO eine Heimat-Community voraus und auf der Community-Ebene einen VO-Repräsentanten für jede VO -- typischerweise⁵ der Gründer der VO (manchmal auch *Principal Investigator* genannt).

► Grundsätzlich stellt dies zwar eine Einschränkung dar, da VOs ohne übergeordnete Communities nicht gegründet werden können (siehe auch [workflow]), konzeptionell kann jedoch eine Default-Community definiert werden, die VOs ohne konkrete Heimat-Community aufnimmt. ◀

⁵ Aber nicht notwendigerweise.

6.2 Interne VO-Struktur

Um den Anforderungen nach Gruppenstrukturen und Rollenverständnissen (Abschnitt 5) gerecht zu werden, besitzen VOs im D-Grid inhärent eine hierarchische Gruppenstruktur. In den einzelnen Gruppen werden spezifische Rollen zusammengefasst. Der Grundgedanke einer solchen VO-Struktur orientiert sich am Prinzip des „*separation of concern*“.

6.2.1 Gruppenstruktur

Gruppen dienen innerhalb einer VO der *administrativen* Ordnung von *Personen*, die einer VO zugeordnet werden können. Insofern besitzt jede D-Grid-VO standardmäßig die folgenden Gruppen (siehe Abbildung 2):

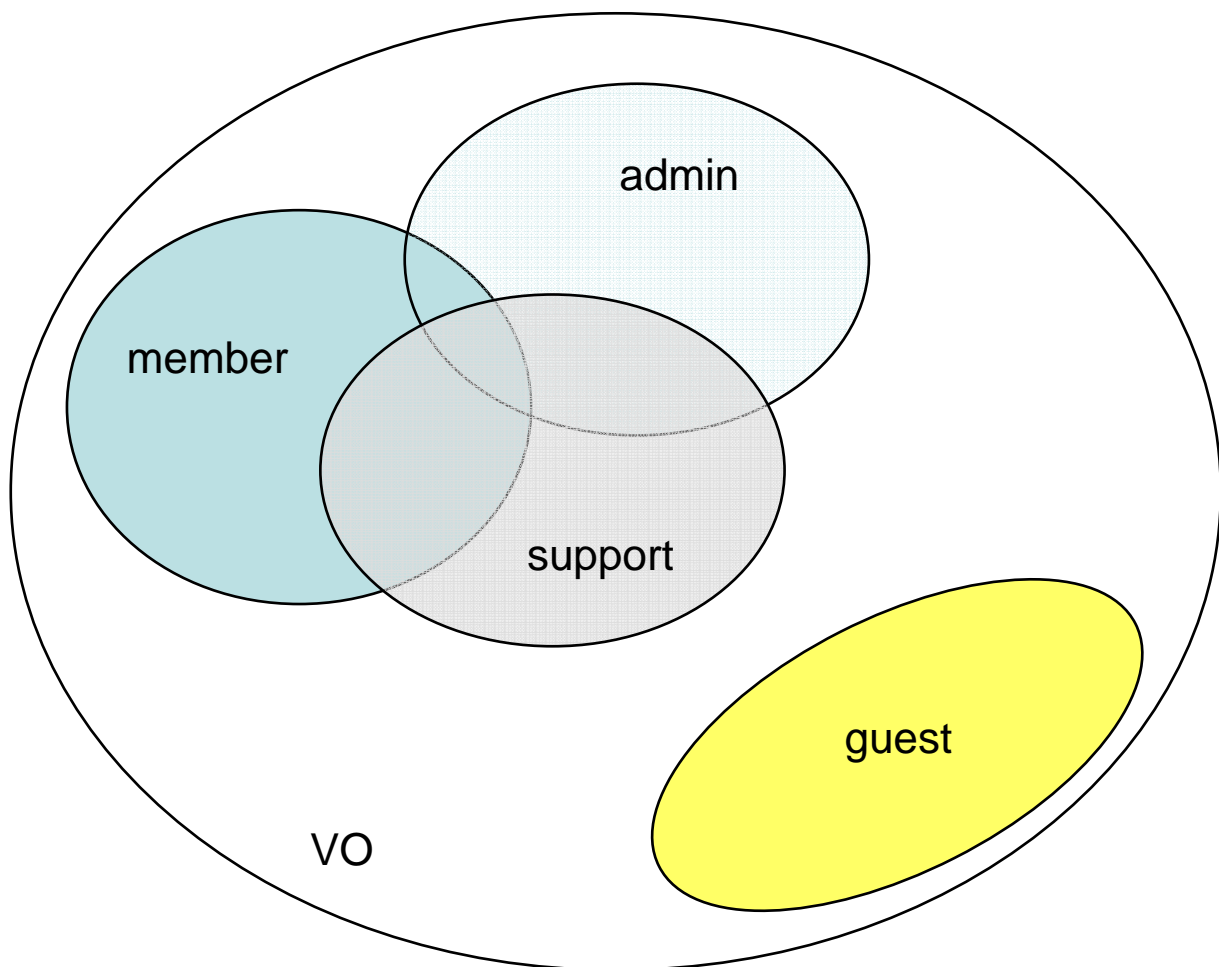


Abbildung 2: Generische Gruppenstruktur

member: Die *Mitgliedergruppe* umfasst alle Mitglieder-spezifischen Rollen. Sie kann VO-spezifisch weiter in Untergruppen unterteilt werden wie beispielsweise Gruppen mit speziellen Ressourcen-Kenntnissen oder Gruppen in speziellen geographischen Lokationen.

guest: Während die Mitgliedergruppe alle „akkreditierten“ Mitglieder einer VO umfasst, werden in der *Guestgruppe* alle VO-Gäste zusammengefasst. Gäste können weder Support- noch Administratorrollen übernehmen, noch können sie zur *member*-Gruppe gehören. Die präzise Definition eines „Gastes“ ist VO-spezifisch.

admin: Die *Administratorgruppe* (oder *Managementgruppe*) umfasst alle Rollen, die dem operativen Betrieb einer VO zuzuordnen sind. Typische Rollen in dieser Gruppe sind der VO-Administrator und die oben erwähnten Gruppen-Manager.

support: Die *Supportgruppe* umfasst die Rollen, die im Rahmen von VO-spezifischen Supportprozessen relevant sind.

6.2.2 Rollenstruktur

Rollen von VO-Mitgliedern geben Auskunft über deren Aufgabengebiete, die über einfache Gruppenzugehörigkeiten hinausgehen. Rollen sind daher mit Gruppen assoziiert und auf Personen abbildbar. Jede D-Grid-VO besitzt standardmäßig die folgenden Rollen:

groupmanager: Der *Gruppen-Manager* regelt die Zugehörigkeit von VO-Mitgliedern zu den von ihm verwalteten Gruppen, indem er diese bestätigt, ablehnt oder modifiziert. Der Gruppen-Manager ist Mitglied der Administratorgruppe.

VOAdmin: Der *VO-Administrator* ist für die administrativen Belange während der Lebenszeit einer VO verantwortlich. Dazu gehören das Einrichten von Gruppen und Untergruppen, das Einrichten von Rollen, die Registrierung von Mitgliedern, die Aufnahme von Ressourcen, die Überwachung von Policies oder das Management von Audit-Daten. Der VO-Administrator ist Mitglied der Administratorgruppe.

softwareadmin und dataadmin: Spezifische Rollen der Administratorgruppe sind der *Software-Administrator* und der *Datenmanagement-Administrator*. Während der Software-Administrator für die Installation Community-spezifischer Software auf den D-Grid Compute-Ressourcen verantwortlich zeichnet, unterstützt der Datenmanagement-Administrator die strukturierte Datenhaltung auf den Speicher-Ressourcen der VO. Beide Rollen werden separat gefordert, um den Belangen virtueller Ressourcen gerecht zu werden.

vorepresentative: Der *VO-Repräsentant* ist als Gründer oder erster Ansprechpartner der VO per constructionem Mitglied der Administratorgruppe. Er repräsentiert die VO auf der Community-Ebene.

privacy: Ein *Datenschutz-Kontakt* ist für die Einhaltung von Richtlinien zum Schutz personenbezogener und VO-bezogener Informationen verantwortlich. Diese Rolle gewinnt im Kontext nachhaltiger Grid-Infrastrukturen zunehmend an Bedeutung. Der Datenschutz-Kontakt ist Mitglied der Administratorgruppe.

Eine spezielle Funktion besitzt der Administrator, der die Einhaltung von Richtlinien und Policies überwacht. Ihm wird die Rolle **abuse** zugeordnet.

accountingbilling: Der *Accounting Manager* ist für das Accounting und Billing innerhalb der VO verantwortlich. Er ist Mitglied der Administratorgruppe.

developer und tester: Die Mitglieder einer VO (genauer: die Mitglieder der Gruppe *member*) können unterschiedliche Rollen besitzen. Da in vielen Fällen spezielle Entwicklungs- und Testaktivitäten durchzuführen sind, sind diese Rollen speziell ausgewiesen.

supportcontact: Der *Support-Kontakt* ist für das Management der Supportprozesse verantwortlich. Gleichzeitig ist er der Ansprechpartner für alle Support-relevanten Fragen. Er ist Mitglied der Supportgruppe.

6.2.3 Capability-Struktur

Konzeptionell können Rollen spezifische Berechtigungen in der Form von Capabilities (siehe [ivom]) zugeordnet werden. Da diese Zuordnungen jedoch sehr Szenario-spezifisch sind und von aktuellen Grid-Middleware-Technologien nicht (mehr) unterstützt werden, werden sie hier nicht weiter skizziert.

6.3 Umsetzung

Gruppenzugehörigkeiten und Rollenzuteilungen werden im D-Grid über die aus den VOMS/VOMRS-Systemen bekannten Fully Qualified Attribute Names (FQAN) spezifiziert [voms]. Die allgemeine Struktur eines FQAN ist durch das folgende Konstrukt gegeben:

```
/VO[ /group[ /subgroup(s) ] ]/Role=<role>/Capability=<cap>6
```

Ist keine Rollenzuordnung vorgesehen, wird der Rollenparameter mit dem Wert „NULL“ initialisiert.

Für die interne generische VO-Struktur ergibt sich daraus ein Attribut-Baum wie er in Abbildung 3 dargestellt ist. Weitere VO-spezifische Untergliederungen und Verfeinerungen sind zulässig (siehe auch [voms]) und können im Rahmen einer VO-spezifischen Instanziierung erfolgen.

Die komplette Umsetzung der hier vorgeschlagenen Strukturen ist Szenario-spezifisch und kann deshalb ebenso wenig antizipiert werden wie eine weitergehende mögliche Attributierung. Werden allerdings Attribute für Gruppen und Rollen vorgesehen, so erfolgt deren Management über entsprechende Rollen der Administratorgruppe. In [vorahmenkonzept], [betriebskonzept] und [ivom] ist näher beschrieben worden, welche Werkzeuge zur Realisierung zurzeit mit welchen Einschränkungen genutzt werden können.

Für eine weitergehende Diskussion der Umsetzung wird auf [attribute] verwiesen.

7 Generische VO-Prozesse

► Die nachfolgenden Diskussionen beziehen die Darstellungen in [betriebskonzept] und [workflow] wesentlich mit ein. Da jedoch zum Zeitpunkt der Erstellung des hier vorliegenden Dokumentes [workflow] noch nicht öffentlich zugänglich ist, werden einige Ergebnisse aus [workflow] hier antizipiert. Eine spätere Version dieses Dokumentes wird den dann aktuellen Stand aller referenzierten Dokumente reflektieren. ◀

Aus der Übersicht im Abschnitt 5.2 lassen sich die generischen VO-Prozesse für das D-Grid ableiten, die sich einerseits auf bestehende VO-Prozesse in den bisherigen Communities und im Kern-D-Grid abbilden lassen (*best practices*), die andererseits aber auch zukünftige VO-Anforderungen unterstützen müssen. Im Betriebskonzept [Betriebskonzept]) sind diese Prozesse für bestehende Communities detailliert dargestellt.

Unter *generischen* VO-Prozessen sind hier die Prozesse einer abstrakten VO zu verstehen, die für konkrete VOs instanziiert werden und damit die generischen Konzepte und Prozesse „erben“ (im Sinne objektorientierter Vererbung von Methoden).

Im Folgenden werden die generischen VO-Prozesse konzeptionell beschrieben. Eine Implementierung der Prozesse setzt eine Reihe von Grundannahmen und Designentscheidungen voraus, die nicht nur die in der VO verwendeten VO-Managementsysteme berücksichtigen muss, sondern auch die eingesetzten Middleware-Technologien und die Community-spezifischen Gegebenheiten. Insofern sind Implementierungen die hier vorgeschlagenen VO-Prozesse immer fallspezifisch. Eine konkrete

⁶ Der Capability-Zweig wird von bestehenden VO Management-Systemen wie VOMS nicht mehr unterstützt und kann daher entfallen.

Prozessbeschreibung unter Berücksichtigung des jeweiligen Kontextes wird Gegenstand einer späteren Version dieses Dokumentes sein. Auf eine weitergehende Darstellung des für die Prozesse erforderlichen Attributmanagements wird ausdrücklich hingewiesen [attribute].

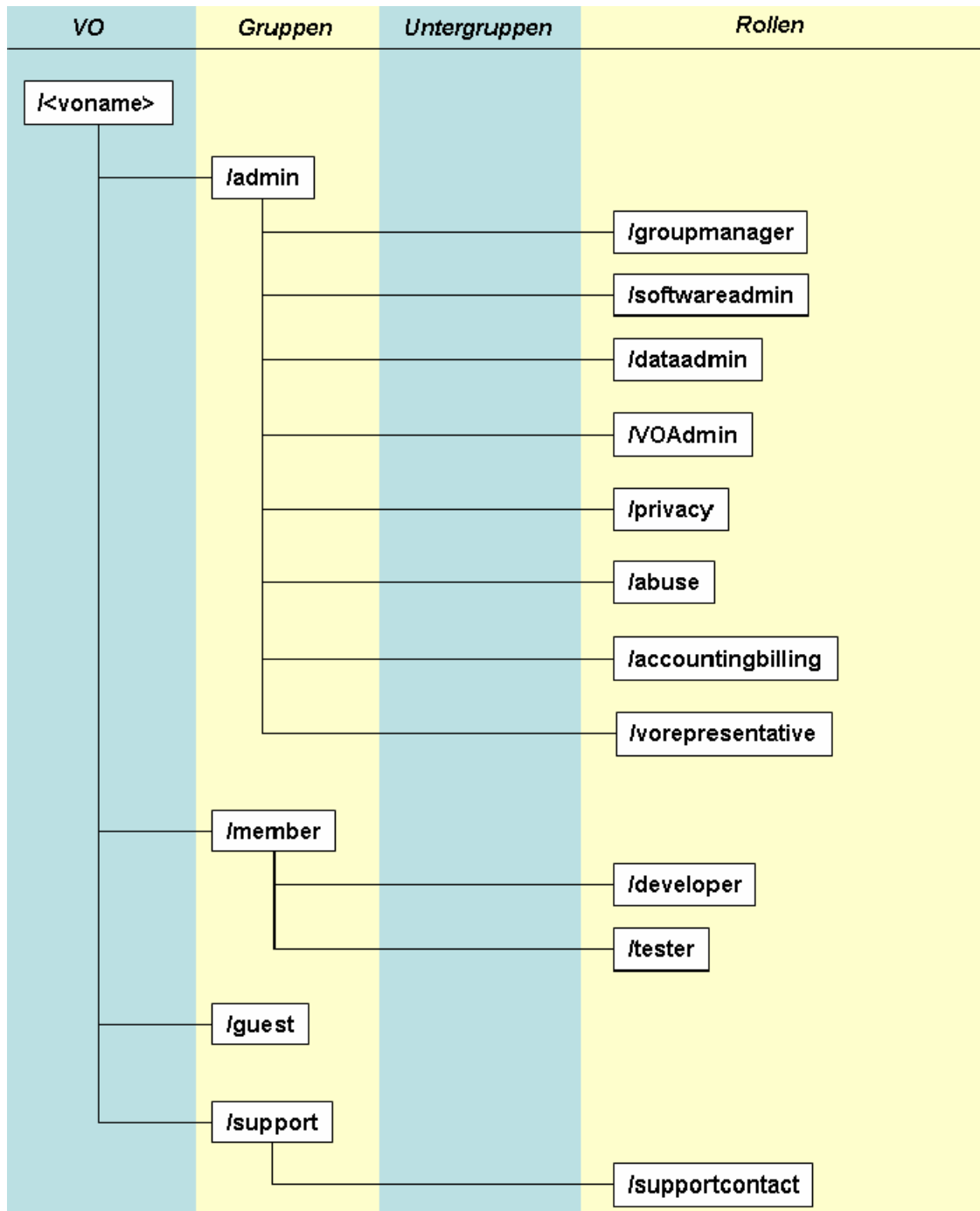


Abbildung 3: Generische VO-Struktur (FQAN-Darstellung)

7.1 Prozesse zum Aufbau und Abbau einer Virtuellen Organisation

Mit dieser Gruppe von Prozessen wird der Lebenszyklus einer VO auf der Community-Ebene gestartet und beendet.

7.1.1 Gründung einer VO (*createVO*)

Der Prozess der Gründung einer VO ist in [vorahmenkonzept], [betriebskonzept] und [workflow] hinreichend detailliert beschrieben. Der Leser wird daher auf diese D-Grid-Dokumente verwiesen. Für den VO-Gründungsprozess können die folgenden Aktivitäten aus diesen Dokumenten extrahiert werden:

Da die Gründung einer neuen VO im D-Grid in der Regel über eine bestehende Community erfolgen wird, ist auch deren Einwilligung (über den identifizierten Community-Sprecher) nötig (vergleiche aber auch die Ausführungen im Abschnitt 6.1).

Soll eine neue VO gegründet werden obwohl keine zugehörige Community identifiziert werden kann, wird über noch zu definierende Eskalationsprozeduren eine Community etabliert [workflow].

Der Community-Sprecher veranlasst die Gründung einer VO und benennt den (oder die) VO-Repräsentanten.

Der VO-Repräsentant akzeptiert die grundlegenden VO-Richtlinien im D-Grid [betriebskonzept] und er formuliert damit kompatible VO-AUPs.

Sollen die Mitglieder der neuen VO auch auf Community-interne Ressourcen⁷ zugreifen können, sind entsprechende Vereinbarungen und Zugangskriterien zwischen den Betreibern dieser Ressourcen und der Community bzw. der VO erforderlich.

Der Zugang zu den Ressourcen durch VO-Mitglieder setzt voraus, dass die VO die jeweiligen Ressourcen-AUPs der Provider akzeptiert [betriebskonzept].

Der Prozess zur Gründung einer VO wird typischerweise vom VO-Repräsentanten angestoßen. Er endet mit der Genehmigung verschiedener Entscheidungsgremien (Beirat, Betriebsgesellschaft, Community-Sprecher, etc) und führt über in den Einrichtungsprozess *initVO*.

7.1.2 Einrichten einer VO (*initVO*)

Nachdem die VO gegründet wurde, kann sie eingerichtet werden. Die Einrichtung erfolgt typischerweise durch die zuvor etablierten Rollen des VO-Repräsentanten und des VO-Administrators. Im Verlauf der Einrichtung werden alle Gruppen und die weiteren Rollen gemäß Abschnitt 6.2 generiert. Ebenso werden im Rahmen einer spezifischen Instanziierung auch die nicht-generischen Gruppen, Untergruppen und Rollen eingerichtet.

Unabhängig von diesen organisatorischen Maßnahmen sind unterstützende technische Einrichtungen erforderlich:

Einrichten der(s) VO-Managementsysteme (VO-Server(s) zur Mitgliederverwaltung, z.B. VOMS, VOMRS, ...)

Einrichten möglicher Kommunikationsplattformen für VO-Mitglieder, z.B.

- E-Mail-Verteiler
- Web-Portal
- gemeinsam nutzbarer Speicher für Dateien

Nach der Einrichtung der VO ist diese betriebsbereit. Nun greifen entweder die Betriebsprozesse oder die VO wird beendet.

⁷ Ressourcen, die nicht dem allgemein zugänglichen D-Grid-Ressourcen -Pool zugeordnet werden können.

7.1.3 Terminierung einer VO (*terminateVO*)

Wird die VO nicht weiter für die zur Erreichung des Ziels der Kooperation benötigt, wird sie terminiert. Dabei sind in der Regel folgende Aktivitäten zu durchlaufen, die genaue Spezifikation dieser Teilprozesse ist jedoch noch nicht abgeschlossen und wird in einer späteren Version des Dokumentes vervollständigt:

Die Mitglieder der VO sind rechtzeitig über das bevorstehende Ende der VO zu informieren.

Die Laufzeit von Jobs muss mit dem geplanten Ende der VO – abhängig von den definierten Policies – abgeglichen werden.

Klärung der Notwendigkeit, vorhandene Daten der VO über das Ende der VO hinaus zu speichern und gegebenenfalls für andere VOs der Community verfügbar zu machen. Diese Daten müssen dann in geeigneter Form gespeichert werden.

Festlegung, wie nicht weiter verwendete Daten zu löschen sind (spezifische Sicherheits- und Datenschutzerfordernungen der VO) und diese Daten entsprechend löschen (*VO Garbage Collection*).

Festlegung der Verfügbarkeit der gesicherten Daten im Backup (soweit die Daten der VO in den Backup aufgenommen wurden) und im Backup für die vereinbarte Zeit einfrieren.

Festlegen, welche Informationen über die VO längerfristig zur Verfügung stehen müssen und diese Daten in geeigneter Weise sichern.

Festlegen, welche Verträge und Service Level Agreements (SLA) mit den Ressourcen Providern gekündigt werden müssen und diese Verträge und SLAs kündigen.

Die Abrechnung der Ressourcennutzung muss abgeschlossen werden.

7.2 Prozesse zum Betrieb einer Virtuellen Organisation

Mit dieser Gruppe von Prozessen wird der Betrieb einer VO aufrecht erhalten. Die Gruppe beinhaltet daher generische Prozesse für die Mitgliederverwaltung, die Verwaltung von Ressourcen und Diensten sowie für die Verwaltung von Gruppen und Rollen. Obwohl der Betrieb virtueller Organisationen sehr fallspezifisch ist, sollen dennoch im Folgenden einige Hinweise auf die Funktionalität der Prozesse gegeben werden.

7.2.1 Aufnahme von Mitgliedern (*addMember*)

Die Aufnahme neuer Mitglieder in eine VO erfordert einige Standardaktivitäten (siehe auch [betriebskonzept] und [workflow]), die aus der typischen Einbettung von VOs in Communities resultieren.

Will eine Person Mitglied einer VO werden, wendet sie sich direkt an einen VO-Repräsentanten oder den D-Grid-Support. Sind die allgemeinen Aufnahmekriterien nicht erfüllt oder gelingt keine erfolgreiche Vermittlung durch den D-Grid-Support an eine VO, wird der Aufnahmeantrag an eine nächste Instanz zur Entscheidung auf der Basis noch zu definierender Kriterien eskaliert (ein vom D-Grid Beirat beauftragtes Gremium).

Alternativ wird der Antragsteller gemäß D-Grid Betriebskonzept [betriebskonzept] in die allgemeine VO *kerndgrid* aufgenommen. Der generische Prozess „Aufnahme von Mitgliedern“ kann damit kategorisiert werden in (siehe auch [workflow])

Mitglied in bestehende VO aufnehmen

Mitglied in neue VO aufnehmen

Mitglied in VO *kerndgrid* aufnehmen

Aufnahme in D-Grid ablehnen

Die technisch erforderlichen Maßnahmen zur Unterstützung dieser Teilprozesse hängen von der in der VO verwendeten Middleware und den VO Management-Systemen ab und umfassen neben einem angemessenen Zertifikat-Management (für langlebige und kurzlebige Zertifikate) auch eine Web-Schnittstelle für die Anmeldung (Aufnahmeantrag) und deren Quittierung (Bestätigung des Aufnahmeantrags durch den VO-Repräsentanten) sowie die individuelle Zuweisung VO-spezifischer Autorisierungen an das neue Mitglied.

7.2.2 Änderung der Mitgliedschaft (*changeMember*)

Der Prozess zur Änderung einer Mitgliedschaft wird durch den VO-Administrator angestoßen und umfasst alle Aktivitäten zur Änderung von Berechtigungen, Gruppenzugehörigkeiten, Rollenbelegungen oder ganz allgemein Mitglieds-spezifischen Attributen. Eine konkrete Festlegung der Teilprozesse ist für die Endversion dieses Dokuments vorgesehen.

7.2.3 Sperren, Freigeben und Ausscheiden von Mitgliedern (*suspendMember, releaseMember, deleteMember*)

Für Fälle der missbräuchlichen Nutzung von D-Grid-Ressourcen, des Fristenablauf bei zeitlicher Befristung von Mitgliedschaften, der Ungültigkeit von Nutzer-Zertifikaten oder der Terminierung der VO werden Prozesse vorgesehen, einzelne Mitglieder, ganze Gruppen oder komplette Rollen zu sperren bzw. nach Sperrung wieder freizugeben oder zu entfernen. Der Initiator dieser Prozesse ist in der Regel der VO-Administrator oder – wie im Falle des Ausscheidens eines Mitglieds – das Mitglied selbst.

Für diese Prozesse muss festgelegt werden

- wie das Mitglied über die Sperrung informiert wird,
- welche Instanzen zusätzlich informiert werden müssen,
- welche Maßnahmen für ein nachträgliches Audit eingeleitet werden müssen,
- welche Schritte das Mitglied für die Reaktivierung der Mitgliedschaft unternehmen muss
- und wer eine Sperrung wieder aufheben darf.

Die konkrete Festlegung dieser Aktivitäten ist für die Endversion dieses Dokuments vorgesehen.

7.2.4 Management von Ressourcen (*addResource, modifyResource, lockResource, unlockResource, removeResource, logResourceUsage*)

Während der Lebenszeit einer VO kann sich der Ressourcenbedarf einer VO ändern, so dass Anpassungen notwendig werden. Ausserdem werden Informationen über die Ressourcennutzung erfasst. Für diese Aufgaben sind die folgenden generischen Prozesse definiert:

- Aufnahme von Ressourcen
- Ändern von Ressourcen
- Sperren und Freigeben von Ressourcen
- Entfernen von Ressourcen
- Logging der Ressourcen-Nutzung

Eine genaue Spezifikation der Prozesse wird in einer späteren Version dieses Dokumentes erfolgen.

7.2.5 Management von Rollen (*createRole, modifyRole, deleteRole*)

Autorisierung in VOs, besonders für die Nutzung von Ressourcen gegenüber den Ressourcen-Providern basiert auf Rollen, denen unterschiedliche Rechte zugeordnet werden können. Für das Management von Rollen in einer VO sind die folgenden generischen Prozesse vorgesehen:

- Bildung von Rollen
- Ändern von Rollen
- Entfernen von Rollen

Diese Prozesse schließen Kommunikationsmechanismen mit den Ressourcen-Providern ein, da Änderungen an den Rollen auch an die Ressourcen-Provider übermittelt werden müssen, um dort die Autorisierung entsprechend anpassen zu können.

7.2.6 Management von Gruppen (*createGroup, modifyGroup, deleteGroup*)

Rollen werden in VOs im Kontext von Gruppen definiert (siehe auch Abschnitt 6.3), die wiederum die Struktur einer VO festlegen. Da in vielen Fällen nur die Gruppenstruktur einer VO von Bedeutung sein wird, eine Rollenstruktur aber nicht vorgesehen ist⁸, wird in diesen Fällen auch von einer *Gruppenautorisierung* (statt von einer Rollenautorisierung) gesprochen.

Für das Management von Gruppen in einer VO sind die folgenden generischen Prozesse vorgesehen:

- Bildung von Gruppen
- Ändern von Gruppen
- Löschen von Gruppen

Auch diese Prozesse schließen Kommunikationsmechanismen mit den Ressourcen-Providern ein, da Änderungen in den Gruppenzugehörigkeiten auch für die Ressourcen-Provider von Bedeutung sind, um deren lokale Autorisierungsmechanismen entsprechend anpassen zu können.

8 Instanziierung im konkreten Fall

In diesem Dokument wurden für D-Grid-VOs eine generische Struktur und generische Prozesse im Rahmen des Lebenszyklus einer VO vorgeschlagen. Diese Konzepte sind generisch und erfordern eine Instanziierung im konkreten Fall. Dies bedeutet für die VO-Verantwortlichen:

- die Gruppen gemäß Abschnitt 6.2.1 festzulegen
- die Rollen gemäß Abschnitt 6.2.2 festzulegen
- die Gruppenstruktur VO-spezifisch zu erweitern bzw. zu modifizieren
- die Rollenstruktur VO-spezifisch zu erweitern bzw. zu modifizieren
- die Gruppen- und Rollenstrukturen VO-spezifisch zu implementieren
- die im Abschnitt 7.2 spezifizierten Prozesse zu implementieren

Die bei einer konkreten Instanziierung zu berücksichtigenden Randbedingungen sind nicht nur Community- und VO-spezifisch, sondern müssen sich auch an dem dann gültigen Betriebskonzept [betriebskonzept], den konkreten Workflow-Beschreibungen [workflow] und den konkreten Attributierungen [attribute] orientieren.

⁸ Im FQAN wird dies ausgedrückt durch den Term `Role=NULL`.

Abkürzungen

AUP	Acceptable Use Policy
FQAN	Fully Qualified Attribute Name
IVOM	Interoperabilität und Integration der VO-Management Technologien im D-Grid
SLA	Service Level Agreement
VO	Virtuelle Organisation
VOMS	VO Membership Service
VOMRS	VO Management Registration Service

Referenzen

- [attribute] Ch. Grimm, B. Henne, S. Piger, M. Schiffers, W. Ziegler: *Definition von Attributen für die Autorisierung auf D-Grid-Ressourcen*, Juni 2008. Bericht zur Teilaufgabe 1.3 des D-Grid Integrationsprojektes 2 (DGI-2)
- [betriebskonzept] O. Büchner et al.: *Betriebskonzept für die D-Grid-Infrastruktur*, Version 1.1c, November 2007. http://www.d-grid.de/fileadmin/user_upload/documents/Kern-D-Grid/Betriebskonzept/D-Grid-Betriebskonzept.pdf
- [ivom] Gietz, P., Grimm, C., Gröper, R., Haase, M., Makedanz, S., Pfeiffenberger, H., Schiffers, M., [A Concept for Authorization on D-Grid Resources: Report of Working Package 3 of the D-Grid IVOM-Project](#), D-Grid-Report, D-Grid IVOM, September, 2007
- [voms] EGEE: *EGEE User's Guide, VOMS Core Services*. Oktober 2006, <https://edms.cern.ch/file/571991/1/voms-guide.pdf>
- [vorahmenkonzept] J.-M. Milke, M. Schiffers, W. Ziegler: *Rahmenkonzept für das Management Virtueller Organisationen im D-Grid*, November 2006. http://dgi.d-grid.de/index.php?id=118&no_cache=1&filename=VO_Rahmenkonzept_0.9a.pdf&dir=FG1/VO-Management&task=download&mountpoint=2
- [workflow] Ch. Grimm, M. Schiffers, T. Fieseler, S. Piger, Ch. Dohmen: *Schematische Darstellung von VO-Management-Workflows im D-Grid*. Juni 2008. (wird noch veröffentlicht)