Virtuelle Organisationen in Grids: Charakterisierung und Management

Jens-Michael Milke
Forschungszentrum Karlsruhe
Institut für Wissenschaftliches Rechnen
jens.milke@iwr.fzk.de

Michael Schiffers
Munich Network Management Team
Institut für Informatik
Ludwig-Maximilians-Universität München
michael.schiffers@mnm-team.org

Wolfgang Ziegler
Fraunhofer Institut SCAI
Abteilung Bioinformatik
Sankt Augustin
wolfgang.ziegler@scai.fraunhofer.de

Überblick

In diesem Beitrag werden Virtuelle Organisationen (VO) in Grids charakterisiert und zwei unterschiedliche Sichtweisen des VO-Managements adressiert: Das Management von Mitgliedschaften im Rahmen von Authentifizierungen und Autorisierungen (VO-interne Prozesse) und das Management von VO-Lebenszyklen. Für die erste Fragestellung haben sich mit VOMS und Shibboleth Technologien etabliert, die in diesem Beitrag betrachtet werden. Für die zweite Fragestellung, die durch die zunehmende Dynamisierung von Grids an Bedeutung gewinnt, wird der Entwurf eines Rahmenwerkes vorgestellt.

Schlüsselwörter: Virtuelle Organisation, Shibboleth, VO-Membership, VOMS, Globus Toolkit, UNICORE

1 Einleitung

Die stetigen Fortschritte in IT- und Kommunikationstechnologien [14] eröffnen Industrie und Wissenschaft Möglichkeiten, kollaborative Netzwerke als neues Organisationsparadigma zu etablieren. Im kommerziellen Bereich bilden hoch integrierte Lieferketten (*supply chain*) und Virtuelle Unternehmen nur einige Beispiele organisationsübergreifender Wertschöpfungskonstellationen [3]. In der Wissenschaft führen analoge Überlegungen zurzeit zu diversen e-Science Initiativen auf der Basis von Grid-Infrastrukturen [13, 15] zur Adressierung so genannter „Grand Challenges“ [26].
Seit Mitte der 1990er Jahre wird unter dem Grid-Problem allgemein das „*koordinierte Problemlösen und die gemeinschaftliche Nutzung von Ressourcen in dynamischen, multi-institutionellen, virtuellen Organisationen*“ verstanden [12]. Lag der Forschungsschwerpunkt anfänglich noch auf speziellen, auf konkrete Anwendungsfälle zugeschnittene Mechanismen zur Kopplung geographisch verteilter Supercomputer (Metacomputing), so hat sich der Fokus in den letzten Jahren auf die Sicherstellung von Interoperabilität, Integrierbarkeit und organisationsübergreifende Aggregation von Grid-Diensten sowie die Erfüllung komplexer Dienstgüteanforderungen verlagert. Der aktuell festzustellende Boom von Grid-Projekten in Wissenschaft und Industrie deutet zudem darauf hin, dass - zumindest was den Teilbereich des Resource Sharings im oben genannten Grid-Problem angeht - auf eine mittlerweile akzeptabel stabile und robuste Grid-Middleware zurückgegriffen werden kann.
Das Konzept Virtueller Organisationen (VO) ist für Grids von zentraler Bedeutung, da diese den organisatorischen Rahmen für die angestrebten, organisationsübergreifenden, Kollaborationen bereitstel-

Teile dieser Arbeit wurden mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01AK800B im Rahmen der D-Grid-Initiative gefördert.

len. Der sich aus der begrenzten Lebensdauer von VOs ergebende typische Lebenszyklus impliziert zahlreiche - zum Teil neue – Anforderungen, nicht nur an die Bereitstellung von Grid-Ressourcen und -Diensten, sondern insbesondere auch an das Management von VOs selbst [17]. Fragen nach einem IT-gestützten Lebenszyklusmanagement von VOs, nach adäquaten Policy-Mechanismen und deren Durchsetzbarkeit oder nach organisationsübergreifenden Workflow-Kompositionen und deren Einbettung in konfliktfreie Co-Management-Lösungen rücken mehr und mehr in den Vordergrund [27]. Für Ad-Hoc-Grids [36], für Grids mit hohen nicht-funktionalen Anforderungen (Dependable Grids [28]) und für nachhaltige Grid-Infrastrukturen, wie sie in der D-Grid Initiative angestrebt werden [15], sind diese Fragen sogar kritisch.
Trotz der drängenden Notwendigkeit eines auch gerade VOs als *managed objects* umfassenden, integrierten Grid-Management-Ansatzes im Sinne von [16], sind die dazu erforderlichen begrifflichen Einordnungen und die technischen Architekturansätze, Plattformen, Betriebskonzepte und Maßnahmen noch weitgehend ungeklärt oder liegen bestenfalls konzeptionell vor, wie die Aktivitäten der Enterprise Grid Alliance (EGA) [8] oder die noch vagen Ansätze der Open Grid Services Architecture (OGSA) [19] zeigen. Welche konkreten Mechanismen jedoch für ein effizientes und effektives VO-Management notwendig sind und welche Routineaufgaben wie und unter welchen Randbedingungen automatisierbar sind, stellen nach wie vor offene Fragen dar, die zum Teil im Rahmen des VO-Management-Arbeitsgebietes der D-Grid Initiative [15] adressiert werden. Eine kritische Fragestellung betrifft insbesondere das Management von Mitgliedschaften zu VOs und dem damit einhergehenden Problem des Managements von Identitäten und Zugriffsrechten, da VOs nicht immer eigene Ressourcen „besitzen“, sondern häufig auf Ressourcen und Dienste von nicht der VO angehörigen Providern angewiesen sind.
In diesem Beitrag werden zunächst im Kapitel 2 charakteristische Eigenschaften Virtueller Organisationen diskutiert bevor im Kapitel 3 der VO-Managementaspekt in den Vordergrund gestellt wird. Dies geschieht unter den Gesichtspunkten „Mitgliedschaftsmanagement“ und „Lebenszyklusmanagement“.

2 Charakterisierung Virtueller Organisationen

Trotz der Bedeutung Virtueller Organisationen für Grids sind viele grundlegende VO-Konzepte noch immer im Fluss und eine allgemein akzeptierte VO-Definition ist nicht zu finden, wie eine Analyse der Literatur zeigt.
Intuitiv werden VOs aus Personen und/oder technischen Ressourcen autonomer realer Organisationen mit dem Ziel gebildet, kooperativ und koordiniert zur Lösung eines (oder mehrerer) Probleme - dem eigentlichen Zweck der VO - beizutragen. VOs sind daher zweckorientiert und einer gemeinsamen Interessenslage verpflichtet, die die „Geschäftsgrundlage“ der VO bildet. Anders als reale Organisationen sind sie jedoch a priori zeitlich befristet angelegt mit einer hohen Dynamik sowohl in ihrer Struktur als auch in den internen und externen Prozessen. Die wohl gängigste und am häufigsten zitierte Definition ist in [12] zu finden („*A Set of individuals and/or institutions defined by resource sharing rules*“). Diese Definition impliziert allerdings, dass eine VO die ihr zugeordneten Ressourcen auch „besitzt“, oder zumindest den Zugriff darauf autonom regeln kann. Weiterhin impliziert diese VO-Sicht eine gewisse, a priori vorgegebene Statik der Mitgliedschaft. Der dynamische VO-Charakter wird deshalb in [10] eingeführt, während [41] und [39] zusätzlich den Aspekt der gemeinsamen Interessenslage und die dafür erforderlichen Koordinationsmechanismen unterstreichen. Eine weitergehende Diskussion der Definitionsproblematik ist in [25] zu finden.
Eine umfassende VO-Charakterisierung hängt von der jeweiligen Perspektive des Betrachters ab, der jedoch unterschiedliche Merkmale in den Vordergrund stellt. Eine Analyse aktueller Grid-Projekte [5, 9, 15, 23] zeigt, dass aus der Managementsicht die in Abbildung 1 dargestellten Dimensionen von Bedeutung sind.
So besitzen VOs wie Grid-Ressourcen [4] einen Lebenszyklus, der sich an klassischen Lebenszyklusmodellen [6] orientiert. Die Lebensdauer einer VO kann variieren von kurzfristig (wie bei Ad-Hoc-Grids) bis langfristig (wie im Large Hadron Collider Grid [23]). Die Frage, ob VOs im Rahmen von Projekten geplant gegründet werden oder eher bei Bedarf oder gar spontan (wie im FireGrid-Projekt [2]), betrifft den Gründungsprozess selbst. Ob es sich bei einer VO um eine geschlossene Gruppe [5] oder eher um eine offene handelt, kennzeichnet die der VO zu Grunde liegende Gruppenstruktur. Unabhängig davon sind die eigentlichen Mitgliedschaftsmodelle zu betrachten, die – je nach VO-

Definition – User und Ressourcen umfassen und einen statischen oder dynamischen Ansatz verfolgen. Kooperationen innerhalb einer VO, aber auch zwischen VOs, können unterschiedlich strukturiert sein. Beispiele sind sequentielle Lieferkettenmuster (*supply chains*), Sternstrukturen mit einem zentralen Mittelpunkt (*hub-and-spoke*) oder Peer-to-Peer-Kooperationen. Aus der Sicht des VO-Managements sind zusätzliche Aspekte wie die Administrationsmechanismen (manuell, automatisiert) und der eigentliche Managementfokus (stehen VO-interne Prozesse oder Prozesse zwischen VOs im Vordergrund) von Bedeutung.

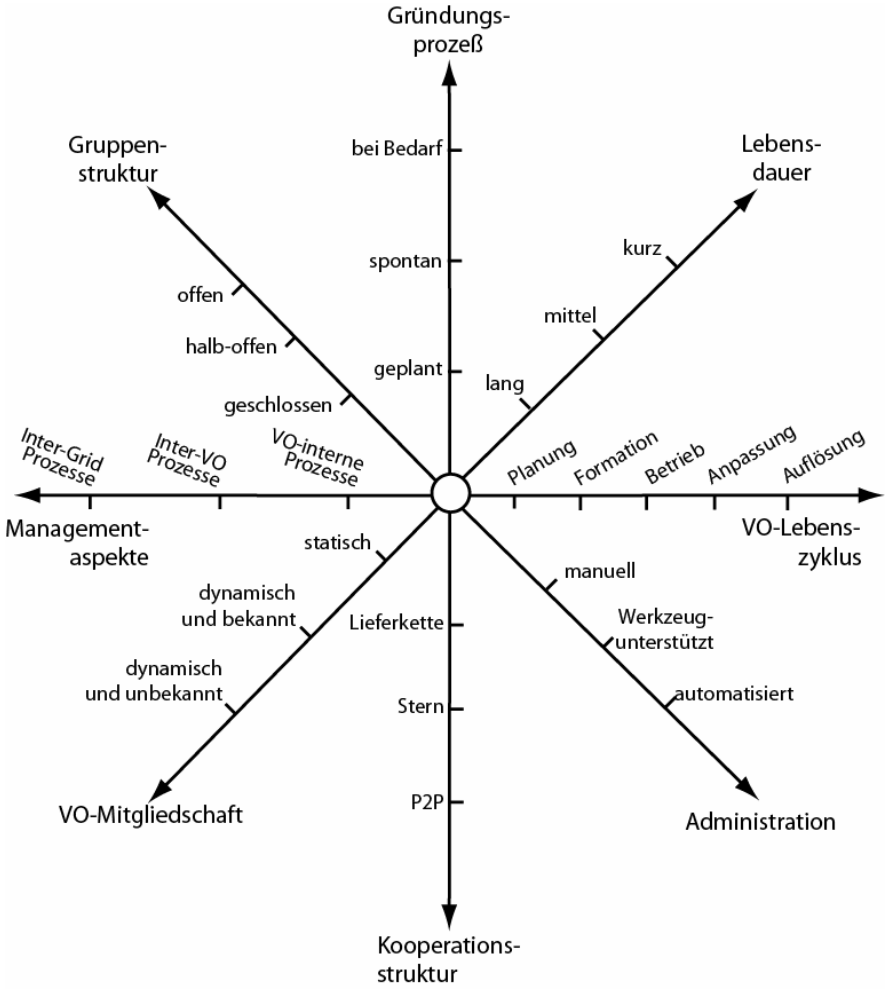

Abbildung 1: Charakterisierung Virtueller Organisationen

Aus diesen Überlegungen leitet sich eine Reihe allgemeiner VO-Merkmale ab. VOs repräsentieren dynamische, organisationsübergreifende Gruppen von Benutzern und/oder Ressourcen, sie implizieren eine definierbare Mitgliedschaft (ist Mitglied, ist nicht Mitglied oder ist Mitglied mit eingeschränkten Rechten), aus der der Zugang zu Grid-Ressourcen abgeleitet werden kann. Eine VO „besitzt“ selbst jedoch nicht immer Ressourcen und stellt im Allgemeinen auch keine Identitäten zur Verfügung, sie verlassen sich stattdessen auf extern gelieferte Authentifizierungsdaten (ein Grund warum Authentifizierungen typischerweise nicht in VOs durchgeführt werden).

Als „kurzlebige“ Objekte unterliegen VOs einem Lebenszyklus, der sich an den *Organisations*zyklusmodellen der Generalized Enterprise Reference Architecture and Methodology (GERAM) [20], dem Lifecycle-Modell für Virtual Enterprises [3] und der Virtual Enterprise Reference Architecture (VERA) des GLOBEMEN-Projektes [37] orientiert und die Phasen *Planung*, *Formation*, *Betrieb* und *Auflösung* [18] unterscheidet. Zusätzlich unterstreicht eine *Anpassungsphase* den dynamischen Charakter einer VO. Abbildung 2 zeigt die Phasen eines VO-Lebenszyklus in ihrem Zusammenspiel mit den ähnlich strukturierten Lebenszyklen der in der VO benutzten Ressourcen. Die Zyklen überlappen sich, da die Betriebsfähigkeit einer VO die Betriebsbereitschaft aller für die VO notwendigen Ressourcen voraussetzt. Die Synchronisation dieser Zyklen stellt gerade in föderierten Umgebungen wie Grids eine erhebliche Managementherausforderung dar. Im Übrigen sei angemerkt, dass aus Sicht einer VO die Lebensdauer der Ressourcen nicht nur die Lebensdauer von Diensten, sondern sogar die der VO selbst überdauern kann.

3 Management Virtueller Organisationen

Dem Management Virtueller Organisationen in Grids liegt prinzipiell der gleiche Managementbegriff zu Grunde wie er auch im klassischen IT-Management Verwendung findet. Er umfasst sämtliche

Maßnahmen für einen effektiven und effizienten Betrieb einer VO und der ihr zugeordneten Ressourcen. Damit werden jedoch zwei unterschiedliche Sichtweisen adressiert. Aus der Sicht einer bestehenden VO stehen die VO-internen Prozesse im Vordergrund (z. B. Management von Mitgliedschaften, Abrechnungsmanagement). Eine andere Perspektive betrachtet VOs als *managed objects* (MO-Sicht) und fokussiert auf den VO-Lebenszyklus selbst. VO-Management aus der MO-Sicht umfasst also nicht nur die Bildung personeller Kollaborationen, sondern strukturiert auch die dynamische Menge der Ressourcen in einen organisatorischen Zusammenhang.
Beispiele VO-interner Geschäftsfälle, die durch einen adäquaten Managementansatz geregelt werden müssen, sind deshalb die dynamische Bildung von Projektgruppen innerhalb einer VO (Anmeldung, Abmeldung etc.), die Festlegung von Rollen und die Benennung von Ansprechpartnern und Verantwortlichkeiten, die Festlegung von Abstimmungsregularien, das Buchen von Ressourcen (z. B. Datenspeicher, Rechner, Softwarelizenzen), der Abschluss von Service Level Agreements (SLA) zur Sicherstellung von Servicequalitäten, das Festlegen von Abrechnungsmodalitäten für die im Grid in Anspruch genommenen Leistungen, die Bereitstellung von Kommunikationsplattformen für die Mitglieder einer VO (virtuelles Büro) oder die Festlegung und das Monitoring von Geschäftsabläufen. Typische Anwendungsfälle der MO-Sicht betreffen die Identifizierung von Providern im Rahmen der Formation von VOs, die Auflösung von VOs (betrifft auch die Verwertung von erworbenen Rechten), die Bereitstellung VO-weiter Policies oder das Konfigurationsmanagement während des Betriebes einer VO. Aus den daraus sich ergebenden Notwendigkeiten von Entscheidungsstrukturen und Verantwortlichkeiten folgt im Übrigen ein enger Zusammenhang mit aktuellen Fragestellungen der IT Governance.

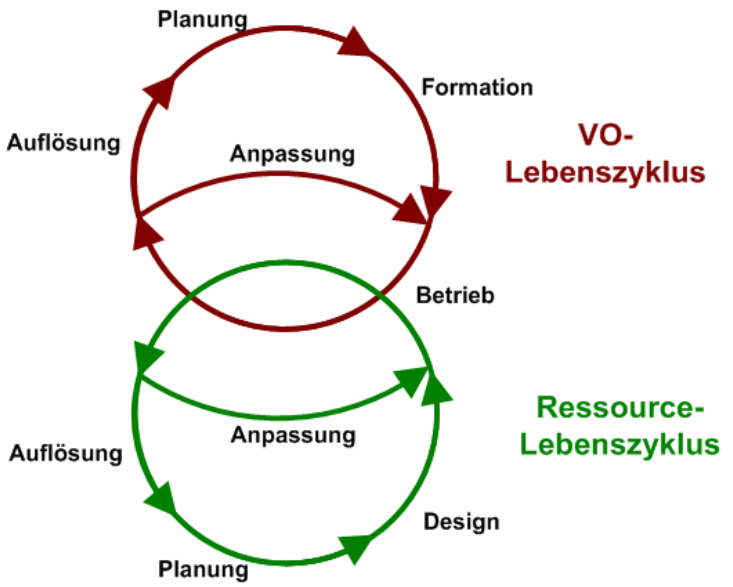

Abbildung 2: Verzahnte Lebenszyklen

Die Synchronisation beider Perspektiven wird über die Kopplung der Lebenszyklen gewährleistet (siehe auch Abbildung 2). Während die MO-Sicht den kompletten Lebenszyklus betrachtet, verfeinert die interne Sicht mit ihrem Fokus auf Dienste und Ressourcen die VO-Betriebsphase. Die eigentliche Managementherausforderung besteht jedoch in der adäquaten Unterstützung der in Abbildung 1 dargestellten Dimensionen im Rahmen eines ganzheitlichen Ansatzes, wie er auch in der D-Grid Initiative langfristig angestrebt wird [15].
Im Folgenden wird im Abschnitt 3.1 auf das Mitgliedschaftsmanagement (die interne Sicht) näher eingegangen, während sich Abschnitt 3.2 Aspekten der MO-Sicht widmet.

3.1 Management der Mitgliedschaft zu Virtuellen Organisationen

Die einfache und sichere Regelung von Mitgliedschaften in VOs ist von erheblicher Bedeutung für ein erfolgreiches VO-Management, da die Mitgliedschaft zu und die Rolle innerhalb einer VO die Rechte eines Nutzers beim Zugriff auf Ressourcen und Dienste bestimmt. Erforderlich sind damit ein geeignetes organisationsübergreifendes Identitätsmanagement (Authentifizierung und Autorisierung), eine ausgereifte Unterstützung durch die diversen Grid-Middleware-Ansätze und möglichst offene, auf Standards basierende Verfahren.

3.1.1 Identitätsmanagement

Eine wesentliche Komponente für das Identitätsmanagement in Grid-Umgebungen ist eine adäquate Authentifizierungs- und Autorisierungs-Infrastruktur (AAI). Dabei bezeichnet *Authentifizierung* den Nachweis einer Identität. Ein gängiges Verfahren für die Authentifizierung ist die Verwendung von X.509-Zertifikaten. Von der Authentifizierung zu unterscheiden ist der Begriff der *Autorisierung*. Hierbei werden einem zuvor authentifizierten Benutzer bestimmte Rechte auf einer Grid-Ressource gewährt. Die Autorisierung beruht üblicherweise auf einem Benutzer zugeordneten Attributen. Aufgabe des VO-Managements ist es daher, die Attribute ihrer Mitglieder zu verwalten und den Resource Providern (RP) für deren Autorisierungsentscheidungen zur Verfügung zu stellen. Für ausführlichere Informationen zur Thematik „Authentifizierung und Autorisierung“ sei auf den Artikel „Sicherheit in Grids“ (C. Grimm, M. Pattloch, H. Reiser) in dieser Ausgabe verwiesen.

3.1.2 Grid-Middleware und Virtuelle Organisationen

Für das VO-Management werden bei den diversen Grid-Middlewares und deren Erweiterungen unterschiedliche Ansätze verfolgt. Hier sei kurz auf das Globus Toolkit in der Version 4 [11] und speziellen Diensten wie VOMS, auf LCG/gLite [33] und auf UNICORE [40] eingegangen.

- Das *Globus Toolkit* unterstützt VOs im Wesentlichen durch seine Grid Security Infrastructure (GSI), die die Authentifizierung von Benutzern auf der Basis von X.509-Zertifikaten und eine verschlüsselte Kommunikation ermöglicht. Single Sign-On (SSO) und Delegation von Rechten werden durch entsprechende Proxy-Zertifikate umgesetzt (siehe auch den Beitrag von Grimm, Pattloch, Reiser in dieser Ausgabe). GSI-Zertifikate werden von *Certificate Authorities* vergeben, die allgemein als vertrauenswürdig eingestuft werden. GSI induziert jedoch nicht unbedenkliche Skalierbarkeitsprobleme [31] und sieht keine Mechanismen zur Beschreibung von Untergruppen (Sub-VOs) und Rollen vor.

  Um VOs einen flexibleren Zugriff auf Ressourcen, Dienste und Daten zu ermöglichen, wurde der Community Authorization Service (CAS) [22] für das Globus Toolkit entwickelt. CAS setzt auf den GSI-Mechanismen auf und verfolgt einen zentralen Ansatz. Jede VO besitzt einen zentralen CAS-Server, der die Zugriffsrechte der Nutzer in einer Datenbank hält. Ein wesentliches Merkmal des CAS-Ansatzes ist, dass RPs die von einer VO vorgegebenen Policies umsetzen müssen. In CAS-Systemen können keine Attribut-Zertifikate ausgegeben werden, CAS kennt daher weder Gruppen noch Rollen. Da die Rechtevergabe vollständig in der Hand der VO liegt, hat sich CAS konzeptionell vom eigentlichen Grid-Grundsatz „*locality over globality*“ entfernt.

  Um diese Schwierigkeiten zu vermeiden, wurde der Virtual Organisation Membership Service (VOMS) [31] zur Verwaltung von VO-Mitgliedschaften entwickelt. Eine VOMS-VO lässt sich in einer hierarchischen Struktur aus Gruppen und Subgruppen darstellen. Den Mitgliedern lassen sich bestimmte Rollen und frei definierbare so genannte *Capabilities* zuweisen. Ein Benutzer kann in verschiedenen Gruppen mit jeweils unterschiedlichen Rollen und Capabilities Mitglied sein. Die Informationen über einen Angehörigen der VO werden mittels Attribut-Zertifikaten, die von einem zentralen VOMS-Server signiert werden, zur Verfügung gestellt. Diese Zertifikate, bei Bedarf auch mehrere von verschiedenen VOs, werden als Erweiterung in das Proxy-Zertifikat des Benutzers integriert. Dabei kann der Benutzer auch nur eine Submenge seiner Gruppenzugehörigkeiten, Rollen und Capabilities anfordern, um seine Rechte auf die für die aktuelle Aufgabe benötigten zu beschränken. VOMS wurde im Rahmen anderer Projekte um Registrierungsdienste [41], lokale Autorisierungsdienste und Dienste zur Abbildung von Benutzern auf lokale Unix-Accounts (anhand von VOMS-Attributen) erweitert [7].

- Die Middleware LCG-2 wurde ursprünglich für das LHC Computing Grid (LCG), aufbauend auf dem Globus Toolkit Version 2, entwickelt und wird derzeit im Rahmen des Enabling Grids for E-SciencE (EGEE)-Projektes angepasst. LCG-2 wird langfristig durch die ebenfalls im Rahmen des EGEE-Projektes bereit gestellte Middleware *gLite* ersetzt. Während das Globus Toolkit nur Basisdienste anbietet, umfasst LCG/gLite alle Komponenten, die für ein „Pro-

duktionsgrid“ benötigt werden (z.B. Resource Broker, File Catalog, Computing Element, Storage Element). gLite stellt selbst keine weiterführenden Komponenten für das VO-Management zur Verfügung, sondern stützt sich auf VOMS.

- *UNICORE* (Uniform Interface to Computing Resources) wurde mit dem Ziel entwickelt, eine produktionstaugliche Plattform für den sicheren und intuitiven Zugang zu den verteilten Ressourcen der deutschen Hochleistungsrechenzentren zur Verfügung zu stellen. Mit dem Aufkommen des Grid-Paradigmas wurde UNICORE weiterentwickelt und kann heute als vertikal integrierte Grid Umgebung charakterisiert werden. UNICORE stellt zwar umfassende Mechanismen für die Authentifizierung und Autorisierung zur Verfügung, kennt aber keinen expliziten VO-Begriff. Die Authentifizierung in UNICORE basiert auf dauerhaften X.509 Zertifikaten, die für die Authentifizierung von Benutzern, Servern, Software und für die Verschlüsselung der Internetverbindungen verwendet werden. UNICORE bietet die Möglichkeit des Single Sign-On, unterstützt aber aus Sicherheitsgründen keine Proxy-Zertifikate. Das Zertifikat wird nach erfolgreicher Authentifizierung vom Network Job Supervisor (NJS) verwendet, um die Autorisierung des Benutzers durchzuführen. Für diese Autorisierung bildet der NJS die Zertifikate auf lokale (Unix) Benutzerkennungen ab. Damit behält jede Einrichtung die vollständige Kontrolle über die Zulassung von Benutzern und kann – mit den üblichen Unix-Mechanismen - den Zugriff auf Ressourcen des Zielsystems nach eigenen Regeln steuern. Unter UNICORE kann ein Benutzer verschiedene Rollen einnehmen, indem sein Zertifikat auf entsprechende Benutzerkennungen abgebildet wird.

3.1.3 Shibboleth

Shibboleth wird im Rahmen des Shibboleth Projekts des Middleware Architecture Committee for Education (MACE) des Internet2 Konsortiums entwickelt [35]. Shibboleth ist eine auf der Security Assertion Markup Language (SAML) des OASIS-Konsortiums basierende Open Source Middleware, die eine Web-basierte Single Sign-On Lösung innerhalb der Grenzen einer Organisation oder über mehrere Organisationen hinweg implementiert.
SAML selbst setzt auf XML auf und wird seit 2001 vor dem Hintergrund zunehmender Verbreitung lose gekoppelter Web-Services als Technologie für verteilte (IT-)Dienstleistungen entwickelt [29]. SAML erlaubt die Beschreibung von Sicherheits-Modellen und ermöglicht den Austausch sicherheitsrelevanter Informationen zur Authentifizierung und Autorisierung, die so genannten SAML-Assertions: Authentication Assertions bestätigen, dass Benutzer auf Ressourcen zugreifen dürfen, Attribute Assertions bestätigen für einen Benutzer oder einen Web Service bestimmte statische (Rollen, Funktionen) oder dynamische Attribute zugeordnet sind, während Authorization Decision Assertions feststellen, ob und wie auf eine spezifische Ressource zugegriffen werden darf.

SAML wird nicht nur in Shibboleth genutzt, sondern auch im GridShib-Projekt [38], im Globus Toolkit 4 und Liberty [24]. Im Rahmen der OGSA-Roadmap ist ebenfalls geplant, SAML zu Autorisierungszwecken vorzuschlagen.
Zu den zentralen Konzepten von Shibboleth gehören eine föderierte Administration, eine Zugangskontrolle basierend auf Attributen und das aktive Management des Datenschutzes (privacy), da der Benutzer stets mitentscheidet, welche Informationen an wen übermittelt werden. Shibboleth ist generell darauf angewiesen, dass sich die beteiligten Komponenten auf eine gemeinsame Syntax und Semantik der ausgetauschten Attribute einigen. Dafür wird in den meisten produktiven Shibboleth-Umgebungen die LDAP-Objektklasse *eduPerson* [21] verwendet, die jeweils um weitere benötigte Attribute ergänzt werden kann.
Shibboleth erlaubt den beteiligten Einrichtungen, fundierte Autorisierungsentscheidungen auf der Basis zertifizierter Benutzerattribute für den individuellen Zugriff auf Ressourcen zu treffen. Für die Authentifizierung interagieren in Shibboleth zwei Komponenten (siehe Abbildung 3): der Identity Provider (IdP), der sich in der Heimateinrichtung des Benutzers befindet, und der Service Provider, der sich beim Anbieter befindet. Wahlweise kann ein Lokalisierungsdienst oder WAYF (Where Are You From) eingesetzt werden, um die Heimateinrichtung des Benutzers zu identifizieren.

Abbildung 3 gibt einen Überblick über den Ablauf einer Shibboleth-Transaktion beim Browser-basierten Zugriff auf eine Web-Ressource [35]:

1: Ein Nutzer möchte Zugriff auf eine durch Shibboleth geschützte Ressource eines Service Providers (SP) erhalten.

2: Der Nutzer wird zum Where Are You From (WAYF) umgeleitet.

3, 4: Der Nutzer wählt seine Heimat-Institution (IdP) aus.

5: Der Nutzer wird zum Handle Service seines IdP weitergeleitet.

6,7: Der Nutzer authentifiziert sich auf vertrautem Wege gegenüber seinem IdP.

8: Der Handle Service (HS) generiert eine eindeutige ID (Handle) und leitet den Nutzer zurück zum Assertion Consumer Service (ACS) des SP. Der ACS überprüft die mitgelieferte Assertion, generiert eine Session und übergibt an den Attribute Requester (AR).

9, 10: Der AR nutzt das Handle, um Attribute des Nutzers bei der Attribute Authority (AA) des IdP abzufragen. Die AA liefert unter Berücksichtigung der Attribute Release Policy (ARP) eine Attribute Assertion an den AR zurück. Der SP entscheidet anhand der erhaltenen Attribute über die Gewährung und Art des Zugangs.

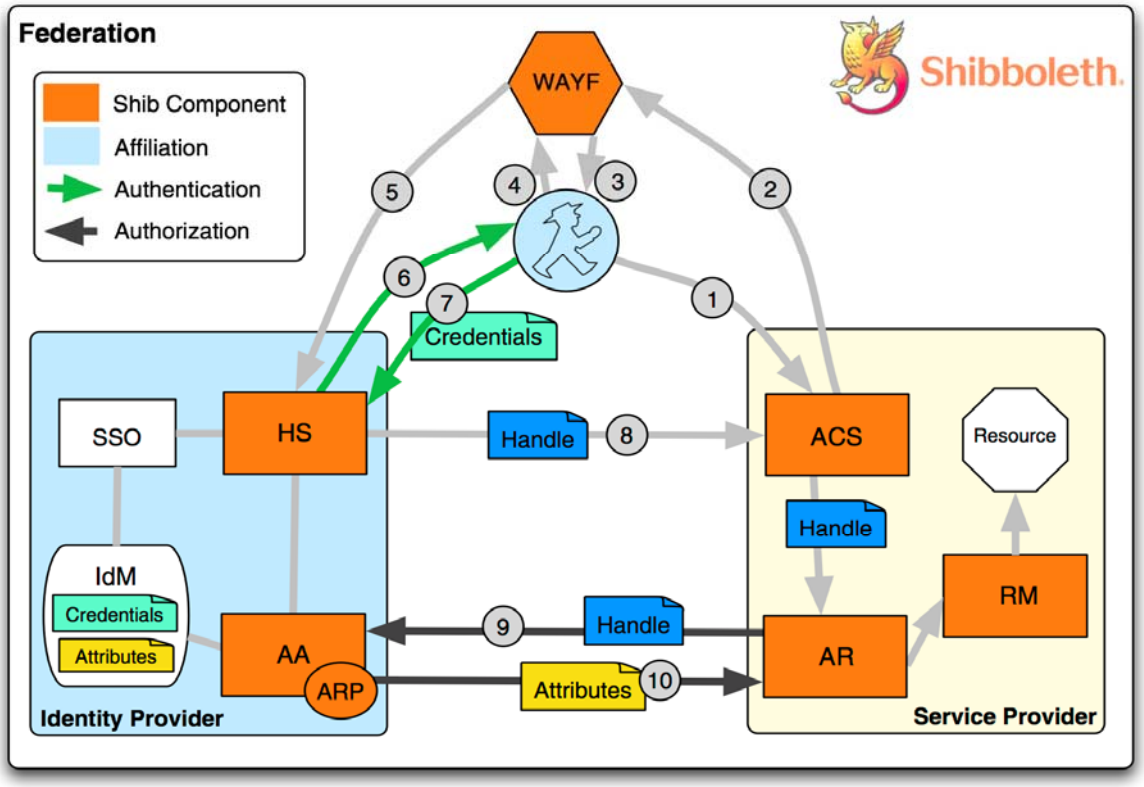

Abbildung 3: Shibboleth-Architektur [35]

3.2 Lebenszyklusmanagement Virtueller Organisationen

Das Lebenszyklusmanagement Virtueller Organisationen betrachtet eine VO als *managed object*. Dies setzt ein adäquates Informationsmodell voraus, in dem VOs für Managementzwecke beschrieben werden können, die Definition von geeigneten VO-Management-Protokollen, ein adäquates Rollenmodell und schließlich im Funktionsmodell eine Spezifikation der erforderlichen Managementfunktionalität mit den entsprechenden Managementdiensten. Keines dieser Modelle ist bisher hinreichend spezifiziert, Ansätze sind jedoch vorhanden [30, 32, 34]. In [18] wird ein Organisations- und Funktionsmodell vorgeschlagen, in dem die Rolle eines so genannten VO-Providers (VOP) als Initiator von VO-Management-Operationen vorgesehen ist. Für das Management des VO-Lebenszyklus wird außerdem eine Reihe von Managementdiensten für die Lebenszyklusphasen angeboten.

In der **Planungsphase** werden ein oder mehrere VO-Profile nach generischen und zielspezifischen Schablonen (*templates*) erstellt. Jedes Profil enthält die Basisanforderungen an das Setup einer VO wie Dienstgüteparameter, Verlässlichkeitskriterien, Listen der Benutzer und deren Abbildung auf Rollen und Dienste, Provider-Präferenzen, VO-spezifische Policies sowie andere Initialwerte.
In der **Formationsphase** wird eine VO vom VOP initialisiert. Zu diesem Zeitpunkt besitzt die VO noch keine Mitglieder. Basierend auf dem in der Planungsphase erstellten Profil startet der VOP nun die SLA-Verhandlungen mit den für das Ziel der VO relevanten Ressourcen- und Dienstanbietern. Die so ausgewählten Provider werden der VO hinzugefügt. Sind „genügend“ viele Provider verfügbar, kann die Betriebsphase eingeleitet werden, in der typischerweise auch der organisatorische Kontext einer VO über die Definition von Rollen hergestellt wird.
In der **Betriebsphase** werden die Lebenszyklen synchronisiert (siehe Abbildung 2). Zu Beginn dieser Phase werden die in der Planungsphase spezifizierten Identitäten eingerichtet und Nutzer/Dienst-Relationen über Task-Assignments erstellt. Nach der Initialisierung werden in der Betriebsphase die klassischen FCAPS-Managementdienste (siehe [16]) bereitgestellt.
Anpassungsphasen sind dann nötig, wenn auf Fehlersituationen reagiert werden muss oder Ressourcen bzw. Provider entfernt, ersetzt oder hinzugefügt werden müssen.
In der **Auflösungsphase** wird die VO zunächst angehalten, um standardisierte oder individuell vereinbarte administrative Prozesse (z. B. Auditing, Rechnungsstellungen, Garbage Collection) durchzuführen. Anschließend kann die VO als *managed object* „zerstört“ werden.
Zusätzliche Funktionalitäten und eine prototypische Implementierung dieses Ansatzes auf der Basis Shibboleth und der vom OASIS-Konsotium definierten Extensible Access Control Markup Language (XACML) sind in [18] beschrieben und werden deshalb hier nicht weiter vertieft.

4 Zusammenfassung und Ausblick

In dem Beitrag wurden zwei unterschiedliche Sichtweisen des VO-Managements adressiert: Das Management von Mitgliedschaften zu VOs im Rahmen von Authentifizierungen und Autorisierungen (VO-interne Prozesse) und das Management von VO-Lebenszyklen.
Für die erste Fragestellung haben sich, bedingt durch unterschiedliche Anforderungen und Infrastrukturen der verschiedenen Grid Communities, mehrere Technologien etabliert, die untereinander nicht interoperabel sind (z. B. VOMS und Shibboleth). Im Rahmen mehrerer Projekte wird zur Zeit an einer Lösung dieses Problems gearbeitet (GridShib, EGEE-2, OMII-Europe, Global Grid Forum). Auch im D-Grid sollen im Rahmen eines im Juni 2006 beim Projektträger eingereichten Antrags für das D-Grid Ergänzungsprojekt „Interoperabilität und Integration der VO-Management Technologien im D-Grid – IVOM“ Konzepte und Software entwickelt werden, die eine VO-übergreifende Authentifizierung und Autorisierung erlauben. Die Lösungen werden dabei jeweils auf den in den VOs verwendeten Technologien und Rahmenbedingungen aufsetzen, diese erweitern und so gewährleisten, dass D-Grid Partner aus ihrer lokalen Arbeitsumgebung heraus organisationsübergreifend D-Grid Ressourcen gemeinsam Nutzen können.
Die zweite Fragestellung (VOs als *managed objects*) steckt noch in den Kinderschuhen, wird allerdings durch die zunehmende Dynamisierung von Grids und Virtuellen Organisationen drängender. Der im Beitrag vorgestellte Ansatz stellt einen ersten Schritt dar, die VO-Management-Problematik ganzheitlich zu betrachten, einem Ziel, dem sich auch das in der D-Grid Initiative zu erstellende Rahmenkonzept zum VO-Management widmet.

Danksagung

Die Autoren danken dem Arbeitsgebiet 1-10 (VO-Management) des D-Grid-Integrationsprojektes (DGI) und dem Münchner Netzmanagement Team unter Leitung von Prof. Dr. H-G. Hegering für intensive Diskussionen und wertvolle Kommentare zu früheren Versionen dieses Beitrages.

Literatur

[1] Berman, Fran (Hrsg.) ; Fox, Geoffrey (Hrsg.) ; Hey, Tony (Hrsg.): Grid Computing - Making the Global Infrastructure a Reality, J. Wiley & Sons, ISBN 0-470-85319-0, 2003 (Series in Communications Networking & Distributed Systems)

[2] Berry, D. et al.: FireGrid: Integrated Emergency Response and Fire Safety Engineering for the Future Built Environment. In: Cox, Simon J. (Hrsg.) ; Walker, David W. (Hrsg.): Proceedings of the UK e-Science All Hands Meeting (AHM 2005). Nottingham, UK, September 2005, 1034–1041

[3] Camarinha-Matos, L. M. ; Silveri, I. ; Afsarmanesh, H. ; Oliveira, A. I.: Towards a Framework For Creation of Dynamic Virtual Organizations. In: Proceedings of the 6th IFIP Working Conference on Virtual Enterprises (PRO-VE'05). Valencia, Spain, September 2005

[4] Czajkowski, K. ; Ferguson, D. ; Foster, I. ; Frey, J. ; Graham, S. ; Sedukhin, I. ; Snelling, D. ; Tuecke, S. ; Vambenenepe, W.: The WS-Resource Framework. Januar 2005

[5] http://www.deisa.org/. Homepage der Distributed European Infrastructure for Supercomputing Applications (DEISA).

[6] Dreo Rodosek, Gabrijela ; Hegering, Heinz-Gerd ; Stiller, Burkhard: Dynamic Virtual Organizations as Enablers for Managed Invisible Grids. In: Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS 2006), Vancouver, Canada, 2006

[7] Enrico Ferro ; Federica Fanzago ; Vincenzo Fiaschini ; Fabio Spataro: Integration of VOMS + LCAS/LCMAPS. Technical Report INFNGRID20040620-1400 Version: v1.2.0, Februar 2005, http://grid-it.cnaf.infn.it/fileadmin/sysadm/voms-integration/voms-integration.pdf

[8] Enterprise Grid Alliance: EGA Reference Model v1.0, April 2005. http://www.gridalliance.org/en/WorkGroups/ReferenceModel.asp.

[9] Foster, Ian (Hrsg.) ; Carl, Kesselman (Hrsg.): The Grid 2 – Blueprint for a New Computing Infrastructure, Morgan Kaufmann Publishers, ISBN 1-55860-933-4, 2004 (Series in Grid Computing)

[10] Foster, Ian ; Carl, Kesselman ; Nick, Jeffrey M. ; Tuecke, Steven: The Physiology of the Grid. In [1].

[11] Foster, Ian ; Childers, Lisa: Introduction to GT4. Tutorial APAC Conference and Exhibition on Advanced Computing, Grid Applications and eResearch (APAC'05). September 2005,

http://www.globus.org/toolkit/tutorials/BAS/APAC/APACGlobusIntro.pdf.

[12] Foster, Ian ; Kesselman, Carl ; Tuecke, Steven: The Anatomy of the Grid: Enabling Scalable Virtual Organizations. In: International Journal of High Performance Computing Applications 15 (2001), Nr. 3, S. 200–222

[13] Fox, Geoffrey ; Walker, David: e-Science Gap Analysis. Juni 2003. http://www.grid2002.org/ukescience/gapresources/GapAnalysis30June03.pdf.

[14] Garschhammer, M. ; Hegering, H.-G. ; Schiffers, M. ; Broy, M. ; Picot, A.: Kommunikations- und Informationstechnik 2010+3. Bonn: Bundesamt für Sicherheit in der Informationstechnik, ISBN 3–922746–48–9, 2003

[15] Gentzsch, Wolfgang: E-Science-Framework für Deutschland. http://www.d-grid.de. – Homepage der D-Grid Initiative

[16] Hegering, H.-G. ; Abeck, S. ; Neumair, B.: Integrated Management of Networked Systems – Concepts, Architectures and their Operational Application. Morgan Kaufmann Publishers, ISBN 1-55860-571-1, 1999

[17] Hegering, Heinz-Gerd: Management-Herausforderungen bei Grids. In: Wissenschaftsmanagement - Zeitschrift für Innovation (2005), Nr. 1, S. 8–9

[18] Hommel, Wolfgang ; Schiffers, Michael: Supporting Virtual Organization Lifecycle Management by Dynamic Federated User Provisioning. In: Proceedings of the 13th Workshop

of the HP OpenView University Association: HP-OVUA'06. Cote d'Azur, Frankreich, 2006, http://www.nm.ifi.lmu.de/pub/Publikationen/hosc06/

[19] I. Foster ; H. Kishimoto ; A. Savva ; D. Berry ; A. Djaoui ; A. Grimshaw ; B. Horn ; F. Maciel ; F. Siebenlist ; R. Subramaniam ; J. Treadwell ; Reich J. von: The Open Grid Services Architecture, Version 1.5. https://forge.gridforum.org/projects/ogsa-wg/document/draft-ggf-ogsa-spec-1.5/en/8. März 2006

[20] IFIP-IFAC Task Force on Architectures for Enterprise Integration: GERAM: Generalized Enterprise Reference Architecture and Methodology v1.6.3, März 1999. http://www.cit.gu.edu.au/~bernus/taskforce/geram/versions/geram1-6-3/GERAMv1.6.3.pdf.

[21] K. Hazelton (Ed.). EduPerson Object Class Specification. Internet2 Middleware Architecture Committee for Education, Directory Working Group (MACE-Dir), DRAFT Revision, Februar 2006, http://www.educause.edu/eduperson/

[22] L. Pearlman ; V. Welch ; I. Foster ; C. Kesselman ; S. Tuecke: A Community Authorization Service for Group Collaboration. In Proceedings of the 3rd International Workshop on Policies For Distributed Systems and Networks (Policy'02), 2002, IEEE Computer Society, Washington, DC

[23] http://lcg.web.cern.ch/LCG/. Homepage des Large Hadron Collider Grids (LCG).

[24] http://www.projectliberty.org/. Homepage des Liberty Alliance Projects.

[25] Mark Norman**:** What is a VO? -Towards a Definition. http://wiki.oucs.ox.ac.uk/esp-grid/VODefinition

[26] Nelson, David B.: Grand Challenges: Science, Engineering, and Societal Advances Requiring Networking and Information Technology Research and Development. Report of the Interagency Working Group of the National Coordination Office for Information Technology Research and Developmenton (NITRD). März 2004. http://www.nitrd.gov/pubs/200311_grand_challenges.pdf.

[27] NGG2 Expert Group: Next Generation Grid 2: Requirements and Options for European Grids Research 2005-2010 and Beyond. Final Report. Juli 2004. ftp://ftp.cordis.lu/pub/ist/docs/ngg2_eg_final.pdf

[28] Nguyen-Tuong, Anh ; Grimshaw, Andrew S. ; Wasson, Glenn ; Humphrey, Marty ; Knight, John C.: Towards Dependable Grids / University of Virginia, Department of Computer Science. Charlottesville, USA, März 2004 (Technical Report CS-2004-11).

[29] OASIS: Security Assertion Markup Language V1.1 Standard Specification. http://www.oasis-open.org/committees/download.php/3400/oasis-sstc-saml-1.1-pdf-xsd.zip.

[30] Patel, Jigar et al.: Agent-Based Virtual Organisations for the Grid. In: Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS '05). New York, NY, USA: ACM Press, 2005. – ISBN 1–59593–093–0, S. 1151–1152

[31] R. Alfieri ; R. Cecchini ; V. Ciaschini ; F. Spataro ; L. dell'Agnello ; Á. Frohner ; K. Lörentey: From Gridmap-File to VOMS: Managing Authorization in a Grid Environment, 2004

[32] Roel van den Berg ; Matti Hannus ; Jens-Dahl Pedersen ; Martin Tølle ; Arian Zwegers: Evaluation of State of the Art Technologies, Deliverable 411 des EU-GLOBEMEN-Projektes, 2000

[33] Rüdiger Berlich ; Marcel Kunze ; Kilian Schwarz: Grid Computing in Europe: from Research to Deployment. In: Proceedings of the 2005 Australasian Workshop on Grid Computing and e-Research (CRPIT '44), Newcastle, New South Wales, Australien, 2005

[34] Sailer, M.:Towards a Service Management Information Base, In: IBM PhD Student Symposium at ICSOC05, Amsterdam, Niederlande, Dezember, 2005.

[35] Shibboleth Technical Introduction. http://shibboleth.internet2.edu/shib-tech-intro.html

[36] Smith, Matthew ; Friese, Thomas ; Freisleben, Bernd: Towards a Service-Oriented Ad-Hoc Grid. In: Proceedings of the Third International Symposium on Parallel and Distributed Computing/Third International Workshop on Algorithms, Models and Tools for Parallel Computing on Heterogeneous Networks (ISPDC/HeteroPar'04). IEEE Computer Society.

[37] Tølle, Martin ; Zwegers, Arian ; Vesterager, Johan: Virtual Enterprise Reference Architecture and Methodology (VERAM).Joint Deliverable D41/D43 des Arbeitspaketes WP4 des Globemen-Projektes, 2003

[38] Tom Barton et al.: Identity Federation and Attribute-based Authorization Through the Globus Toolkit, Shibboleth, Gridshib, and MyProxy. In: 5th Annual PKI R&D Workshop, April 2006

[39] Treadwell, J.: Open Grid Services Architecture – Glossary of Terms. Version 1.5 vom März 2006. https://forge.gridforum.org/projects/ogsa-wg/document/draft-ggf-ogsa-glossary-1.5-006/en/6.

[40] Unicore Forum: What is Unicore? http://www.unicore.org. Homepage des Unicore Forums.

[41] VOX Project Team: VOMRS User Guide. Chicago, USA: Fermi National Accelerator Laboratory, Computing Division, 2004.

http://www.uscms.org/SoftwareComputing/Grid/VO/vox.pdf

Dr. Jens-Michael Milke, Studium der Physik an der Universität Karlsruhe (TH), Diplom 1998. 2002 Promotion auf dem Gebiet der Teilchen-Astrophysik am Institut für Experimentelle Kernphysik/Universität Karlsruhe (TH). Anschließend wissenschaftlicher Angestellter am Institut für Kernphysik/Forschungszentrum Karlsruhe. Seit Oktober 2005 am Institut für Wissenschaftliches Rechnen/Forschungszentrum Karlsruhe und Mitglied des D-Grid Projektteams. Forschungsgebiete: Grid Computing, VO-Management.

Dipl.-Inform. Michael Schiffers, Studium der Informatik an der Universität Bonn, Diplom 1977. Seit 2002 am Lehrstuhl Kommunikationssysteme und Systemprogrammierung (Prof. Dr. H.-G. Hegering) der Ludwig-Maximilians-Universität München. Davor in verschiedenen Positionen der IT-Industrie. Mitglied des Münchner Netzmanagement Teams. Seit 2005 Mitglied des D-Grid Projektteams. Forschungsgebiete: Grid Computing, VO-Management, Service Management. Mitglied bei GI und ACM.

Wolfgang Ziegler, seit 1987 bei der Gesellschaft für Mathematik und Datenverarbeitung (heute Fraunhofer Gesellschaft) im Institut für Wissenschaftliches Rechnen und Algorithmen (Prof. Dr. U. Trottenberg), Leiter der Grid Middleware Entwicklung in der Abteilung Bioinformatik. Seit 1999 Mitarbeit im Grid Forum und seit 2001 Arbeitsgruppenleiter im Global Grid Forum, seit 2005 Mitglied des D-Grid Projektteams. Forschungsgebiete: Grid Computing, Resource Management und Scheduling, VO-Management, SOA. Mitglied bei IEEE und ACM.