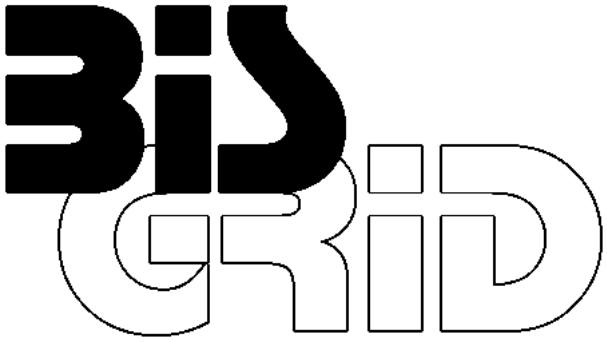


Betriebliche Informationssysteme:
Grid-basierte Integration und Orchestrierung

Deliverable 2.5

Arbeitspaket 2

Spezifikation der Anforderungen an Sicherheit und Service Level Agreements im Zusammenhang mit WS-BPEL

19 März, 2009

GEFÖRDERT VOM

Förderkennzeichen: 01IG07005

Autoren:

Holger Nitsche, **Dirk Meister**
Universität Paderborn
Paderborn Center for Parallel Computing

Stefan Gudenkauf, **Guido Scherp**
OFFIS Institute for Information Technology
R&D-Division Energy

André Höing
Technische Universität Berlin
Faculty of Information Technologies
Complex and Distributed IT Systems

Diese Arbeit wird vom Bundesministerium für Bildung und Forschung (BMBF) und dem Förderkennzeichen 01IG07005 als Teil der D-Grid Initiative gefördert.

Dieses Dokument repräsentiert Deliverable 2.5 “Spezifikation der Anforderungen an Sicherheit und Service Level Agreements im Zusammenhang mit WS-BPEL” des Arbeitspaketes 2 des Projekts BIS-Grid[1], einem vom BMBF geförderten Projekt der deutschen D-Grid[2] Initiative. Inhalt des Dokuments ist die Beschreibung der Sicherheitsanforderungen an die Grid-basierte Integration von betrieblichen Informationssystemen, sowie die Beschreibung der notwendigen Service Level Agreements (SLA). Bitte beachten Sie, das das Dokument als Gegenstand laufender Arbeit durch höhere Dokumentversionen ersetzt oder erweitert werden kann.

[1] http://www.bisgrid.de
[2] http://www.d-grid.de

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument repräsentiert Deliverable 2.5 “Spezifikation der Anforderungen an Sicherheit und Service Level Agreements im Zusammenhang mit WS-BPEL” des Arbeitspaketes 2 des Projekts BIS-Grid[3], einem vom BMBF geförderten Projekt der deutschen D-Grid[4] Initiative. Inhalt des Dokuments ist die Beschreibung der Sicherheitsanforderungen an die Grid-basierte Integration von betrieblichen Informationssystemen, sowie die Beschreibung der notwendigen Service Level Agreements (SLA).

1.1 Das BIS-Grid-Projekt

Typischerweise betreiben Unternehmen verschiedene Informationssysteme mit dem Ziel, die Verwaltung von und den Zugriff auf Informationen über die Ressourcen des Unternehmens, seinen Kunden und seinen Produkten zu ermöglichen. Dabei sind die betreffenden Informationen in den einzelnen Informationssystemen oftmals redundant, was deren Pflege zu einer aufwändigen und teuren Aufgabe macht. Die so genannte Enterprise Application Integration (EAI) zeigt Wege auf, solche heterogenen Informationssysteme zu integrieren [CHKT05] – oftmals durch Dienstorchestrierung in dienstorientierten Architekturen (Service-oriented Architecture, SOA). Geschäftsprozesse werden hier als Workflows auf die technische Ausführungsebene abgebildet. Dabei wird die unterliegende technische Infrastruktur durch so genannte Web Services verborgen, die häufig überhaupt erst die Grundlage für eine Dienstorchestrierung darstellen. Üblicherweise sind Unternehmen in Abteilungen unterteilt, die häufig jeweils eigene IT-Infrastrukturen betreiben (z. B. Server und Storage-Lösungen). Sobald solche Unternehmen wachsen, tendieren ihre Abteilungen dazu, sich zu IT-Ressourcen-“Silos” zu entwickeln. Enterprise Grids sind ein Ansatz, die festen Abteilungsgrenzen zu überschreiten, um Arbeitslastspitzen zu verteilen und den Ressourcenbedarf ansonsten isolierter Abteilungen zu reduzieren [MT]. Beide Technologien, EAI und Enterprise Grids, stellen wohlerprobte Mittel dar, um die Herausforderungen der Integration von betrieblichen Informationssystemen und gemeinsamer Ressourcennutzung zu begegnen. Dennoch werden diese Herausforderungen nur individuell und auch nur unternehmensspezifisch adressiert, und beide Aspekte – die Integration betrieblicher Informationssysteme und die gemeinschaftliche Ressourcennutzung – sind wenig integriert.

Grid-Technologien wie die Grid-Middlewares UNICORE 6[5] und Globus Toolkit 4[6] basieren auf dem Web Service Resource Framework (WSRF) [Ban06], einem Standard, der ansonsten zustandslose Web Services mit Zuständen versieht. Zustandsbehaftete, WSRF-basierte Web Services – auch Grid Services genannt – stellen eine Basis dar, dienstorientierte Architekturen mit Hilfe von Grid-Technologien zu realisieren. Dabei haben Grid-Technologien und EAI viel gemeinsam, da beide Integrationsprobleme innerhalb eines heterogenen Umfelds adressieren – Grid-Technologien auf der Ressourcen-Ebene

[3] http://www.bisgrid.de
[4] http://www.d-grid.de
[5] http://www.unicore.eu
[6] http://www.globus.org/toolkit/

und EAI auf der Anwendungsebene.

BIS-Grid beabsichtigt, eine horizontale Dienstschicht für betriebliche Informationssysteme zu realisieren. Das Ziel ist dabei, die Machbarkeit der Integration von unternehmensinternen und -externen Informationssystemen mit Hilfe von Grid-Technologien unter Beweis zu stellen, um die Kluft zwischen der Informationssystemintegration und der effizienten Ressourcennutzung zu überbrücken und der EAI zu ermöglichen, dynamisch organisationsspezifische Grenzen zu überschreiten ohne unternehmensspezifische Sicherheitsanforderungen abzuschwächen. Diese Idee geht weit über die Idee des Enterprise Grid hinaus, da letzteres lediglich einzelne Technologien und Konzepte der Grid-Welt für den Einsatz im existierenden Unternehmenskontext adaptiert. BIS-Grid beabsichtigt dagegen die Erschließung des Grids für die Industrie durch neue Kollaborations- und Geschäftsmodelle.

Vornehmlich adressiert BIS-Grid kleine und mittelständische Unternehmen (KMU). Diese sollen befähigt werden, ihre Geschäftsprozesse als Orchestrationen von Web Services und Grid Services zu realisieren, um dynamische Lösungen für die Informationssystemintegration und der effizienten Ressourcennutzung anbieten zu können. Hierbei steht der Gedanke im Vordergrund, im Sinne der Inanspruchnahme der Dienste vertrauenswürdiger Grid-Provider keine eigenen Großanlagen (z. B. Computing oder Storage-Lösungen) betreiben zu müssen. Auf der technischen Seite des Projekts wird hierzu eine Grid-basierte Workflow-Middleware entwickelt, die in der Lage ist, mit Hilfe des industriellen de facto-Standards WS-BPEL sowohl herkömmliche Web Services als auch Grid Services zu orchestrieren.

2 Grundlagen

In diesem Abschnitt werden Konzepte, Standards und Technologien vorgestellt, die im weiteren Verlauf dieses Dokuments verwendet oder als bekannt vorausgesetzt werden.

2.1 BIS-Grid-Engine

Ein Ziel in BIS-Grid ist, die Machbarkeit der Integration betrieblicher Informationssysteme mit Hilfe von Grid-Technologien zu belegen. KMU sollen befähigt werden, ohne übermäßigen Aufwand heterogene Informationssysteme zu integrieren und gleichzeitig Grid-Ressourcen nutzen zu können. Hierzu entwickeln wir eine Workflow-Middleware, die auf dem industriellen de facto-Standard für Dienstorchestration, WS-BPEL, basiert und in der Lage ist, sowohl herkömmliche Web Services als auch Grid Services zu orchestrieren. Diese Middleware, die BIS-Grid-Engine, basiert maßgeblich auf Diensterweiterungen der Grid-Middleware UNICORE 6 und einer frei wählbaren, herkömmlichen WS-BPEL-Engine. Dienstorchestrierungen werden dabei von der BIS-Grid-Engine als (zustandsbehaftete) Grid Services angeboten.

Die BIS-Grid-Engine besteht aus zwei Komponenten: Der Grid-Middleware UNICORE 6 und einer frei wählbaren WS-BPEL-Engine im Backend, die nur über die UNICORE 6-Middleware zu erreichen ist (cp. [GHH+08]). Dabei überbrückt die UNICORE-Schicht die technische Kluft zwischen Grid-Umgebungen und WS-BPEL. Jede Nachricht, die zwischen der WS-BPEL-Egine und einem externen Dienst oder Endklienten ausgetauscht wird, muss die UNICORE-Schicht passieren. Dort werden z. B. Nachrichten um Sicherheitszeugnisse (sog. *credentials*) wie etwa SAML Assertions ergänzt[7]. Durch die Auslagerung von WS-BPEL außerhalb der UNICORE-Middleware als Frontend kann diese separat deployt werden, um beispielsweise Lastbalancierung zu unterstützen[8].
Die UNICORE-Schicht der BIS-Grid-Engine basiert auf Diensterweiterungen für den Service-Container von UNICORE 6 (vgl. Abbildung 1). Diese bestehen im Wesentlichen aus einem *Workflow Management Service* und einem generischen *Workflow Service*. Der Workflow Management Service stellt Funktionalitäten wie Prozess-Deployment, -Redeployment und -Undeployment bereit. Während des Deployments eines Prozesses erstellt der Workflow Management Service eine neue spezielle Instanz des Workflow Service für den betreffenden Prozess. Unter anderem bietet dieser Workflow Service dann die vollständige Web Service-Schnittstelle des originalen WS-BPEL-Prozesses an. Somit besitzt jeder über die UNICORE-Schicht in der WS-BPEL-Engine deployter WS-BPEL-Prozess eine zugehörige Instanz des Workflow Service. Ein *Proxy Service* fängt dabei alle Nachrichten ab, die von einer Prozessinstanz in der WS-BPEL-Engine gesendet werden und übermittelt sie an die zugehörige Workflow Service-Instanz zur weiteren Bearbeitung, bevor sie an den eigentlichen Empfänger versendet wird. Die Nutzungsszenarien der beiden Dienste Workflow Management Service und Workflow Service werden in Abbildung 2 dargestellt. Weitere Informationen zur BIS-Grid Engine finden Sie in

[7] SAML Assertions werden derzeit nicht in WS-BPEL unterstützt
[8] Weitere Details zum Thema Lastbalancierung mit der BIS-Grid-Engine finden sich in [GHH+08]

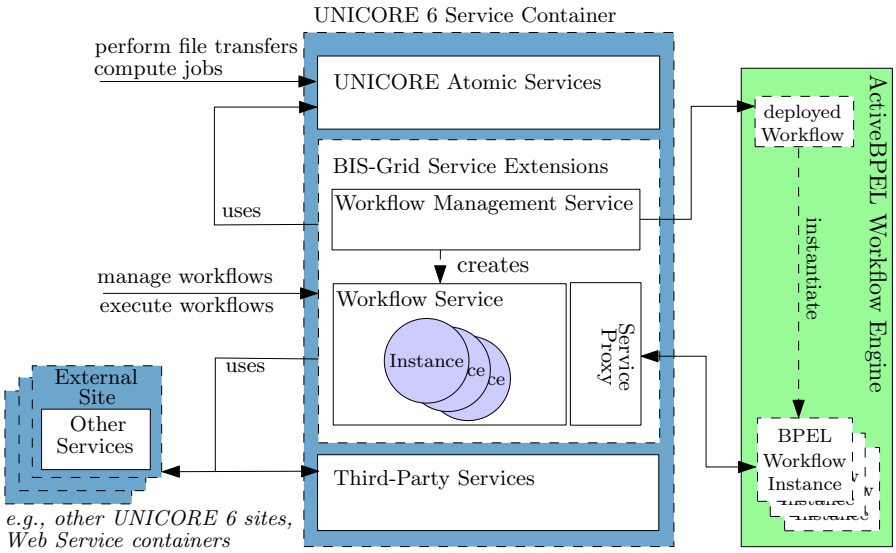
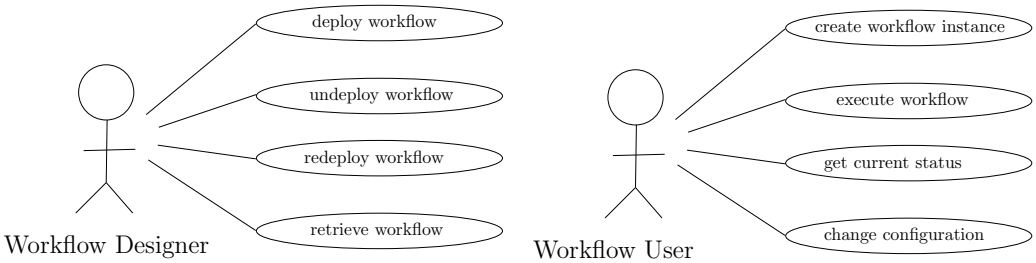


Abbildung 1: Architektur der BIS-Grid-Engine

Deliverable 3.1, der Spezifikation der BIS-Grid-Engine [HHG+07] und Deliverable 3.2, der zugehörigen Dokumentation [HGS08].



(a) Workflow-Management-Service (b) Workflow-Service

Abbildung 2: Nutzungsszenarien der BIS-Grid-Diensterweiterungen für UNICORE 6

2.2 Security Assertion Markup Language (SAML)

Die Security Assertion Markup Language (SAML) ist in der Version 2.0 von der OASIS als Standard angenommen worden und wurde von der Liberty Alliance, einem Zusammenschluss von über 130 Firmen, übernommen. SAML ist ein auf XML aufsetzender Standard zum Austausch von Autorisierung-, Authentisierungs- und Attributinformationen zwischen verschiedenen Sicherheitsbereichen (*Security Domains*), z. B. verschiedenen Firmen. Dabei werden Sicherheitsinformationen über einen Nutzer (*Principle*) in Form von *Assertions* zwischen einem *Identity Provider* (IdP , Aussteller von "Assertions") und einem *Service Provider* (SP, Nutzer von Assertions) über Web Service-Schnittstellen aus-

getauscht. Das SAML-Protokoll und die SAML-*Bindings* definieren, wie einzelne SAML-Elemente in Anfragen (*request*) und Antworten (*response*) verpackt werden.

Der SAML-Standard beinhaltet SAML-Profile für bestimmte Anwendungsszenarien, wie z. B. für die einmalige Anmeldung über einen Web Browser (Single-Sign-On, *Web Browser SSO Profile*). In diesen SAML-Profilen ist detailliert das Zusammenspiel zwischen Identity Provider, Service Provider und Principle, sowie den benötigten Teilen des SAML Standards beschrieben. Es gibt einige Annahmen die dem SAML Standard zu Grunde liegen.

- Es existiert ein Vertrauensverhältnis zwischen dem (einem oder mehreren) Identity Provider und allen Service Provider. Dieses Vertrauensverhältnis wird meist technisch durch eine Public-Key-Infrastruktur (PKI) umgesetzt, in der über Zertifikate Nachrichten signiert und/oder verschlüsselt werden.

- Ein Principle ist bei mindestens einem Identity Provider registriert und der Identity Provider garantiert die Identität eines Principle. Bei einem menschlichen Principle (Nutzer) wird dessen Identität vor der Registrierung mittels des Lichtbildausweises überprüft.

- Der Identity Provider bietet dem Principle eine Schnittstelle zur Authentifizierung, wobei der SAML-Standard die Art der Authentifizierung nicht vorschreibt. Diese kann über Zertifikate, Username/Passwort, eToken, usw. erfolgen.

- Der Service Provider trifft seine Zugriffsentscheidung für eine Resource/Dienstleistung aufgrund einer SAML-Assertion, die durch den Principle beim Identity Provider veranlasst wird.

2.3 eXtensible Access Control Markup Language (XACML)

Die eXtensible Access Control Markup Language (XACML) liegt ebenfalls in der Version 2.0 vor und ist auch durch die OASIS standardisiert. XACML ist ein feingranulares Zugriffskontrollsystem für Subjekte, die ihre Identität in XML ausdrücken. Dabei können die Subjekte sehr unterschiedlich sein, z. B. so genannte *Principles* wie sie in SAML definiert sind. Der XACML-Standard beschreibt ein XML-Schema und einen Namensraum, mit dem die Zugriffsrechte als *Policies* modelliert werden können. Alle Policies sind nach dem folgenden Muster modelliert: ein Subjekt möchte eine Aktion auf einer Ressource unter bestimmten Bedingungen durchführen. Um solche Policies durchzusetzen benötigt man zwei Komponenten, einen *Policy Enforcement Point* (PEP) und einen *Policy Decison Point* (PDP).

Die beiden Standards XACML V2.0 und SAML V2.0 wurden dahingehend entwickelt, sich gegenseitig zu ergänzen. XACML-basierte Attribute können z. B. in SAML beschrieben werden. So ist es möglich, dass mittels XACML-Policies spezifiziert wird, was beim Eintreffen einer SAML-Assertion bei einem Provider geschehen soll.

2.4 Shibboleth

Das Shibboleth-Projekt ist eine Initiative des Internet2-Konsortiums[9]. Ziel des Projekts ist die Entwicklung Policy-basierter Open-Source-Systeme zur Kontrolle des Zugriffs auf Online-Ressourcen. Dabei fokussiert das Shibboleth-Projekt die Bedürfnisse höherer Bildungseinrichtungen und deren Partner. Das im Projekt entwickelte Shibboleth-System ist eine standardbasierte Open-Source-Software für das Web-basierte Single-Sign-On über organisatorische Grenzen hinweg. Das Shibboleth-System ermöglicht, automatisiert Autorisationsenscheidungen für anfragende Individuen zu treffen, ohne die Datensicherheit der betreffenden Online-Ressource (z. B. ein Internetportal) zu gefährden. Shibboleth sieht dabei die Unterstützung des SAML-Standards als Anforderung an, so dass die Unterstützung von SAML V2.0 als Nahziel auf der Entwicklungs-Roadmap von Shibboleth angekündigt ist.

2.5 GridShib

GridShib ist ein System, um eine verteilte Authorisierungsinfrastruktur auf Basis des Shibboleth-Systems mit Grid-Technologien wie dem Globus Toolkit zu integrieren. Das GridShib-System fungiert in einem Shibboleth-System als Service-Provider und führt so eine Authentifizierung/Autorisierung auf Basis des Shibboleth-Systems durch. Nach erfolgreicher Authentifizierung wird ein maximal 27 Tage gültiges (kurzlebiges) Zertifikat generiert, durch das ein Zugriff auf Grid-Resourcen möglich ist. Das GridShib-Projekt ist eine Kooperation zwischen NCSA und der Universität von Chicago und wird durch die NSF gefördert.

[9] http://www.internet2.edu/

3 Sicherheitskonzept

In diesem Abschnitt werden die Überlegungen für ein BIS-Grid Sicherheitskonzept für die Orchestrierung betrieblicher Informationssysteme in heterogenen Umgebungen, insbesondere Unternehmens- und Grid-Umgebungen, dargestellt. In den Abschnitten 3.1 und 3.2 wird hierzu eine kurze Übersicht über das BIS-Grid Szenario und die verschiedenen Sicherheitsebenen gegeben. Danach werden in Abschnitt 3.3 die generellen Partnerrollen aus Kollaborationssicht, und in Abschnitt 3.4 die Rollen der Beteiligten, die speziell an der Entwicklung und Ausführung automatisierter Geschäftsprozesse mit WS-BPEL beteiligt sind, vorgestellt. Im Anschluss wird in Abschnitt 3.5 die Sicherheitsinfrastruktur von BIS-Grid diskutiert.

3.1 Übersicht

Das Projekt BIS-Grid kann aufgrund seiner Einbettung in die vom D-Grid bereitgestellte Infrastruktur auf eine vorhandene Sicherheitsinfrastruktur zurückgreifen. In D-Grid ist ein Public-Key-Infrastruktur (PKI) etabliert, die mittels X.509-Zertifikaten die Absicherung von Netzwerkverbindungen (SSL/TSL) sowie die Authentifizierung von Nutzern ermöglicht. Des weiteren werden virtuelle Organisationen unterstützt, so dass Nutzer in verschiedene Kontexte gesetzt werden können und mit unterschiedlichen Rechten ausgestattet werden. Diese unterschiedlichen Rechte werden auf den meisten Ressourcen im D-Grid über verschiedene Nutzerkennungen direkt abgebildet. Im betrieblichen Umfeld ist diese Art der Umsetzung von Nutzerrechten wenig praktikabel, da für eine natürliche Person verschiedene Nutzerkennungen existieren können. Dies wird bereits bei der Betrachtung des Ausscheidens eines Nutzers aus einer Organisation ersichtlich, da mehrere Nutzerkennungen gesperrt oder gelöscht werden müssten.

Die im D-Grid genutzte Art der Rechtevergabe für Nutzer ist für die bisher vorwiegend wissenschaftliche Nutzung der Ressourcen ausreichend. Im Projekt BIS-Grid reicht diese Art der Rechtevergabe aber nicht aus, da verschiedene Nutzer mit unterschiedlichen Kontexten (Rollen) auf den selben Vorgang (Workflow) auf eine Ressource zugreifen. Daher wird eine rollenbasierte Zugriffskontrolle (*role-based access control* RBAC) benötigt. Diese wird aber im D-Grid nicht unterstützt. Ein weiterer wichtiger Punkt für die BIS-Grid-Nutzer, die Mitarbeiter von Firmen sind, ist die Nutzung der D-Grid PKI. Erstens muss eine natürliche Person bei einer PKI-Registrierungsstelle (*Registration Authority*, RA) persönlich vorstellig werden, um ihren Antrag für ein Nutzerzertifikat abzugeben, da mittels Lichtbildausweis die Identität überprüft wird. Zweitens kann eine Firma nur PKI-Registrierungsstelle werden, wenn sie in ein Vertragsverhältniss zum DFN e.V. tritt, der die D-Grid PKI betreibt.

Daher wurde für BIS-Grid die Idee formuliert, eine verteilte Authentifizierung- und Autorisierungsinfrastruktur (AAI) einzusetzen, an das die Firmen ihre bestehenden Identitätsmanagementsysteme (IdM-Systeme) bzw. bestehenden Verzeichnisdienste (Active Directory/LDAP) anbinden. Das DFN hat eine solche AAI bereits aufgesetzt. Die unentgeltliche Nutzung der DFN-AAI durch industrielle Partner im Rahmen des Projektes BIS-Grid ist durch das DFN schriftlich bestätigt worden. Basis der AAI-Nutzung ist

aber ein Vertrag zwischen den Firmen im BIS-Grid Projekt und dem DFN e.V., in dem Nutzungsbedingungen und Policies geregelt sind (siehe auch 3.2). Generell können DFN-Dienste nur von Mitgliedern des DFN Verein genutzt werden. Firmen können prinzipiell gegen Entgeld Mitglieder werden.

3.2 Sicherheitsebenen

Grundlegende Fragen bei der Sicherheit von Computersystemen sind: was ist abzusichern, womit wird Sicherheit geschaffen, wie hoch ist der Schutzbedarf, wie viel kostest die Sicherheit und wie wird von Menschen die Sicherheit gelebt (Sicherheitskultur)? Für die Sicherheit werden in BIS-Grid drei verschiedene Ebenen betrachtet:

- Vertragliche Ebene
- Organisatorische Ebene
- Technische Ebene

Die *Vertragsebene* ist die oberste Schicht. Hier sind Verträge zwischen Hersteller und Anwender von Sicherheitslösungen angesiedelt, aber auch Verträge zwischen Anbietern und Anwendern von Ressourcen, die den Zugang über eine gemeinsame, verteilte AAI einsetzen. Allgemeiner gesagt werden auf der Vertragsebene sämtliche Qualitätsanforderungen aller Beteiligten sowie die technischen Schnittstellen und das Vorgehen bei Verstößen geregelt. Auf der *organisatorischen Ebene* ist von den Anbietern und Anwendern sicher zu stellen, dass die vertraglich getroffenen Vereinbarungen umgesetzt werden. Das kann von der Dokumentations- und Reportverpflichtung, über personelle Maßnahmen, bis hin zu baulichen Umsetzungen reichen. Verallgemeinert kann man sagen, dass hier die Qualität der betrieblichen Organisation in Hinblick auf Verlässlichkeit, Aktualität und Ausfallsicherheit der Systeme zusammengefasst ist. Auf der *technischen Ebene* sind sämtliche Aspekte angesiedelt, die die Computer- und Softwaresysteme betreffen. Dazu zählen z. B. auch Firewall-Konfigurationen und das Klimaanlagen-Management. Die Systeme der technische Ebene müssen die Qualitätsanforderungen der vertraglichen Ebene wiederspiegeln.

Für eine verteilte AAI im BIS-Grid-Projekt bedeuten diese Überlegungen, dass die Anforderungen definiert und zumindest informell schriftlich fixiert werden. Formale Verträge für eine AAI sind im Rahmen der in BIS-Grid betrachteten exemplarischen Anwendungsszenarien nicht als realistisch anzusehen.

3.3 Kollaborationsrollenmodell

Teil der Planung einer verteilten AAI ist die Betrachtung der verschiedenen Teilnehmerrollen. Im dem angestrebten Szenario einer verteilen AAI betrachten wir derzeit drei primäre Kollaborationsrollen.

Der *Anbieter* einer Ressource oder Dienstleistung, häufig auch *Service Provider* (SP) genannt, möchte seine Ressourcen mit möglichst geringem Aufwand vor unberechtigtem Zugriff schützen. Der Service Provider hat keine aktuelle Information darüber, ob ein

bestimmter Nutzer noch Teil der Organisation eines kooperierenden Anwenders ist. Dazu müsste er seinen Informationsstand regelmäßig mit dem Anwender abgleichen. Da er aber üblicherweise mehreren Anwendern den Zugriff auf seine Dienste oder Ressourcen ermöglicht, wäre ein solcher Abgleich mit allen Anwendern mit einem hohem Aufwand verbunden. Der *Anwender* möchte seinen Nutzern mit möglichst geringem Aufwand den Zugriff auf eine Ressource/Dienst ermöglichen. Es liegt häufig im Interesse des Anwenders, zeitnah seinen Nutzern den Zugang zu den Ressourcen eines Anbieters zu gewähren, oder zu entziehen. Falls der Anwender dafür auf die Mitarbeit des Anbieters angewiesen ist, z. B. durch einen regelmäßigen Datenabgleich oder die Einschaltung einer telefonischen Hotline, ist der Aufwand hoch. Im BIS-Grid Projekt besteht der Wunsch, dass die Anwender selber festlegen, welche Nutzer mit welchen Rechten (Rollen) auf Dienstleistungen (z. B. Workflows) beim Anbieter zugreifen können. Die *Nutzer* wiederum möchten sich möglichst ortsunabhängig und selten authentifizieren. Als idealtypisch wird hier die Idee des *Single-Sign-On* (SSO) angesehen. Das SSO soll dabei sowohl für die Angebote die direkt vom Anwender den Nutzern zur Verfügung gestellt werden, als auch für den Zugriff auf die Ressourcen und Dienstleistungen eines Anbieters gelten.

Auf BIS-Grid übertragen sind die *Nutzer* Mitarbeiter der Industriepartner CeWe Color, KIESELSTEIN und CADsys. Die Industriepartner sind somit die *Anwender* in dem Szenario. OFFIS und die Universität Paderborn (PC^2) stellen die *Anbieter* dar.

3.4 Rollenmodell der Workflow-Beteiligten

In diesem Abschnitt werden die an der Erstellung und Ausführung von automatisierbaren Geschäftsprozessen (*workflows*) beteiligten Rollen beschrieben. Dabei wird zwischen primitiven Basisrollen und zusammengesetzten Rollen unterschieden. Der Fokus der nachfolgenden Rollenbeschreibung liegt dabei auf den Basisrollen, da zusammengesetzte Rollen szenariospezifisch erstellt werden können. Aus Gründen der technischen Dokumentation und Wiederverwendbarkeit sind die Rollenbeschreibungen in Englisch verfasst (siehe auch Del. 3.1).

3.4.1 Basisrollen von Workflow-Beteiligten

	Business Analyst	*Process Designer*	*Process Deployer*	*Process Undeployer*	*Process Initiator*	*Process Owner*	*Process Instance Owner*	*Process Instance Stakeholder*	*Business Process Administrator*	*Execution Environment Administrator*	
provide design-specific information	X	(X)				X			X	X	
design process		X	(X)			(X)			X	X	
deploy			X			X			X	X	Deployment
re-deploy			X			X			X	X	
undeploy				X		X			X	X	
instantiate					X	X			X	X	Factory
destroy						X	X		X	X	
provide information						X	X	X	X	X	Workflow
is notifiable						X	X	X	X	X	
assign/unassign						X[10]	X[11]		X[12]	X[13]	

Tabelle 1: Übersicht der Basisrollen von Workflow-Beteiligten

Business Analyst

- Design level authorisations: provide business process design-relevant information (must pass information to process designers)
- Process level authorisations: *none*
- Instance level authorisations: *none*
- Management level authorisations: *none*

[10] Process Instance Owners, Process Instance Stakeholders, other Process Owners
[11] Process Instance Stakeholders
[12] Process Initiators, Process Owners, Process Instance Owners, Process Instance Stakeholders, other Business Process Administrators
[13] Process Initiators, Process Owners, Process Instance Owners, Process Instance Stakeholders, Business Process Administrators, other Execution Environment Administrator

Process Designer

- Design level authorisations: provide business process design-relevant information (may pass feedback information to business analysts), design processes (must pass processes to process deployer)
- Process level authorisations: *none*
- Instance level authorisations: *none*
- Management level authorisations: *none*

Process Deployer

- Design level authorisations: may pass design-specific feedback information to process designer
- Process level authorisations: deploy and re-deploy processes
- Instance level authorisations: *none*
- Management level authorisations: *none*

Process Undeployer

- Design level authorisations: *none*
- Process level authorisations: undeploy processes
- Instance level authorisations: *none*
- Management level authorisations: *none*

Process Initiator

- Design level authorisations: *none*
- Process level authorisations: instantiate processes
- Instance level authorisations: *none*
- Management level authorisations: *none*

Process Owner is a Process Designer, Process Deployer, Process Initiator, Process Instance Owner, and Process Instance Stakeholder. There must be at least one Process Owner per process.

- Design level authorisations: provide business process design-relevant information (may pass feedback information to business analysts), may pass design-specific feedback information to process designer

- Process level authorisations: deploy, undeploy, and re-deploy processes, instantiate processes
- Instance level authorisations: destroy process instances, provide information to process instances, is notifiable by process instances
- Management level authorisations: assign/ unassign Process Instance Owners, Process Instance Sakeholders, and other Process Owners

Process Instance Owner is a Process Instance Stakeholder.

- Design level authorisations: *none*
- Process level authorisations: *none*
- Instance level authorisations: destroy process instances, provide information to process instances, is notifiable by process instances
- Management level authorisations: assign/ unassign Process Instance Sakeholders

Process Instance Stakeholder

- Design level authorisations: *none*
- Process level authorisations:*none*
- Instance level authorisations: provide information to process instances, is notifiable by process instances
- Management level authorisations: *none*

Business Process Administrator is a Process Owner (Owner of a set of Processes and Process Instances).

- Design level authorisations: provide business process design-relevant information (may pass feedback information to business analysts), may pass design-specific feedback information to process designer
- Process level authorisations: deploy, re-deploy and undeploy processes, instantiate processes
- Instance level authorisations: destroy process instances, provide information to process instances, is notifiable by process instances
- Management level authorisations: assign/ unassign Process Initiators, Process Owners, Process Instance Owners, Process Instance Stakeholders, and other Business Process Administrators

Execution Environment Administrator is a Process Owner and Process Instance Owner (Owner of all Process and Process Instance in the Execution Environment). There must be at least one Execution Environment Administrator per Execution Environment.

- Design level authorisations: provide business process design-relevant information (may pass feedback information to business analysts), may pass design-specific feedback information to process designer
- Process level authorisations: deploy, re-deploy and undeploy processes, instantiate processes
- Instance level authorisations: destroy process instances, provide information to process instances, is notifiable by process instances
- Management level authorisations: assign/ unassign Process Initiators, Process Owners, Process Instance Owners, Process Instance Stakeholders, Business Process Administrators, and other Execution Environment Administrators

Domänenspezifische Rollen

Domain-specific roles are specialisations of basic roles, for example: **Escalation Recipient** is a Process Instance Stakeholder. An Escalation Recipient has to be informed when events occur that are regarded as critical, for example, when a deadline is exceeded.

- Design level authorisations: *none*
- Process level authorisations: *none*
- Instance level authorisations: provide information to process instances, is notifiable by process instances
- Management level authorisations: *none*

3.5 BIS-Grid Sicherheitsinfrastruktur

In diesem Abschnitt werden verschiedene Alternativen für die Architektur und Umsetzung einer BIS-Grid-Sicherheitsinfrastruktur vorgestellt.

3.5.1 Anforderung an die BIS-Grid Sicherheitinfratsruktur

Die Anforderungen aus der in Abschnitt 3.1 formulierten Idee einer AAI können in folgenden Merkmale unterteilt werden:

- Verteiltes Identity Management
- Abbildung von Nutzern auf Rollen
- Kein Einsatz von Nutzerzertifikaten
- Geringer Verwaltungsaufwand

Neben den funktionalen Anforderungen gibt es durch den Einsatz von UNICORE 6 noch technische Anforderungen an eine AAI, um die Ideen und Anforderungen vom BIS-Grid-Projekt an eine AAI umzusetzen:

- SAML Support für Abbildung der Nutzer auf Rollen
- XACML Support für Abbildung der Rollen auf Rechte
- PKI mit X.509-Zertifikaten

3.5.2 Alternative auf Basis von GridShib

Eine Alternative, die Anforderungen an die Sicherheitsarchitektur der BIS-Grid-Lösungen umsetzen, basiert auf der Anwendung des Shibboleth-Systems zur verteilten Authentifizierung und Autorisierung sowie kurzlebigen Zertifikaten (engl.: Short-Lived Certificates, SLC). Diese Alternative wird im folgenden Abschnitt ausführlich dargelegt. In dem Ansatz existieren vier Komponenten, die im Zusammenspiel die Authentifizierung und Autorisierung ermöglichen:

Service Provider: Der Service Provider stellt Ressourcen durch die BIS-Grid-Engine zur Verfügung. Der Service Provider kommuniziert ausschließlich mit dem lokalen Anwender.

Lokale Nutzer: Der lokale Nutzer möchte Ressourcen eines Service Providers nutzen und kann sich bei einem Mitglied eines BIS-Grid-Systems authentifizieren. Ein typischer lokaler Anwender ist Mitarbeiter eines Unternehmens oder einer Organisation, das BIS-Grid-Workflows zur Erledigung ihrer Geschäftsprozesse nutzt. Ein lokaler Nutzer kommuniziert im Verlauf des Authentifizierungs-/Autorisierungsprozesses mit dem Service Provider und der Online-CA.

Online-CA: Die Online-Certificate-Authority (Online-CA) konvertiert mit Hilfe des GridShib-CA-Systems SAML-Resourcen zu kurzlebigen Zertifikaten. Außerdem übernimmt die Online-CA die Koordination der verschiedenen Komponenten und kommuniziert mit dem lokalen Anwender und dem lokalen Identitätsprovider (IdP) der Anwender.

WAYF-Dienst: Der WAYF-Dienst (Where Are You From) dient der Zuordnung von Benutzern zu ihren lokalen Identitätsprovidern. Ein WAYF-Dienst beinhaltet eine Liste aller vertrauenswürdigen Organisationen, woraus ein lokaler Nutzer seine zugehörige Organisation auswählen kann.

Lokaler Identitätsprovider: Der Lokale Identitätsprovider (IdP) stellt auf Basis des Shibboleth-Systems einen Authentifizierung/Autorisierungs-Mechanismus einer Organisation zur Verfügung, indem existierende Identitätsmanagementsysteme der Organisation wie Active Directory oder OpenLDAP durch eine einheitliche Schnittstelle angesprochen werden können. Die gesamte Nutzerverwaltung und Rollenzuweisung, die im Rahmen dieser Infrastrukturalternative anfällt, erfolgt durch die Administratoren einer Organisation in existierenden, lokalen Systemen. Jede Organisation, die auf durch BIS-Grid verwaltete Ressourcen zugreifen will, muss einen lokalen Identitätsprovider betreiben.

Der Ablauf der Authentifizierung/Autorisierung eines Benutzers ist in Abbildung 3 vereinfacht dargestellt. Die Bedeutung der einzelnen Schnitte sind im Folgenden erläutert:

1. Ein lokaler Anwender startet eine Authentizierungsanfrage, indem er auf ein Webinterface der Online-CA geht.

2. Sollte kein gültiges kurzlebiges Zertifikat vorliegen, wird der Anwender per *HTTP Redirect* zum Webinterface des WAYF-Dienstes weitergeleitet.

3. Im WAYF-Webinterface wählt der Anwender aus allen verfügbaren Organisationen seine Organisation aus, bei der sich der Anwender authentifizieren möchte.

4. Der WAYF-Dienst wird den Anwender nun zum Webinterface des Shibboleth-Dienstes des lokalen Identitätsproviders weiterleiten.

5. Der Anwender authentifiziert sich i.d.R. Regel mit Benutzername und Passwort beim lokalen Identitätsprovider.

6. Der lokale Identitätsprovider prüft im lokal administrierten Identitätsmanagementsystem die Daten und die Berechtigungen.

7. Die Rollen des Benutzers werden als *SAML Response* an den Webbrowser des Anwenders gesendet.

8. Der Webbrowser leitet den SAML Response an die Online-CA weiter.

9. Die Online-CA erstellt auf Basis der Authentifikations- und Rolleninformationen der SAML Response ein kurzlebiges Zertifikat (SLC).

10. Dieses SLC wird an den Anwender zurückgegeben, der mit Hilfe dieses Zertifikats auf Grid-Resourcen z. B. durch die BIS-Grid Engine zugreifen kann.

Der Kernaspekt dieser Lösung ist, dass keine langlebigen Zertifikate für jeden Benutzer notwendig sind und die Benutzerdaten und Rolleninformationen nicht redundant verwaltet werden müssen.
Diese Architektur wird im D-Grid-Projekt entwickelt. Der DFN-Verein testete seit März 2007 mit dem DFN-SLCS eine Online-CA auf Basis von GridShib und einer OpenSSL-basierten CA. Seit März 2009 ist auch eine Produktionsinstallation verfügbar. Mit der DFN-AAI betreibt der DFN-Verein ebenfalls ein Shibboleth-System mit zahlreichen vertrauenswürdigen lokalen Identitätsprovidern und einem WAYF-Dienst. Das D-Grid-Projekt IVOM beschäftigte sich mit der Interoperabilität und der Integration von VO-Management-Technologien im D-Grid und entwickelte im Rahmen dieser Anstrengungen auch eine Erweiterung für UNICORE 5, um GridShib-SLC mit der UNICORE 5-Grid-Technologie zu verbinden.

Es bestehen jedoch Zweifel, ob diese Architektur im Rahmen der Anwendungsszenarien in BIS-Grid umsetzbar ist. Die Gründe hierfür sind wie folgt.

Integration mit UNICORE 6: GridShib wurde ursprünglich für das Globus-Toolkit entwickelt und ist auch Teil des Globus-Projektes. Im Rahmen des D-Grid-Projektes IVOM wurde ein Plugin für UNICORE 5 entwickelt. Nach Aussage von Wolfgang Ziegler aus dem IVOM-Projekt wird derzeit an der Integration von GridShib in UNICORE 6 gearbeitet.

Jeweils ein Shibboleth-System pro Organisation notwendig: Jede Organisation muss ihr lokales Identitätsmanagementsystem durch eine Shibboleth-Instanz verfügbar machen. Durch Tests im PC^2 und bestätigt durch persönliche Kommunikation mit Reimer Karlsen-Masur vom DFN-PCA wurde festgestellt, dass der Betrieb eine Shibboleth-Systems äußerst komplex und fehleranfällig ist. Der Betrieb eines Shibboleth-Systems für die Zielgruppe von BIS-Grid, kleinen und mittelständischen Unternehmen (KMU), ist sorgsam abzuwägen.

Rückgriff auf DFN-Installationen möglich, aber problembehaftet: Grundsätzlich erlaubt der DFN- Verein für die Laufzeit des BIS-Grid-Projektes die Aufnahme lokaler Identitätsprovider der Unternehmen in das Shibboleth-System DFN-AAI. Hiermit ist eine notwendige Voraussetzung erfüllt, um die DFN-Online CA nutzen zu können. Notwendig für die Aufnahme in die DFN-AAI ist zudem der Abschluß eines Vertrages mit dem DFN-Verein sowie die Akzeptanz dessen Nutzungsbedingungen und Policies. Die Nutzungsmöglichkeit bestünde dann allerdings zunächst nur im Rahmen des BIS-Grid-Projektes. Eine weitergehende Nutzung nach Beendigung des Projektes ist nach Aussage von Marcus Pattloch vom DFN-Verein nur möglich, wenn die Firmen zahlende Mitglieder würden.

Eine Variante besteht darin, einen lokalen Identitätsprovider beispielsweise bei PC^2 aufzusetzen und diesen in die DFN-Systeme einzubinden. Alle BIS-Grid-Nutzer müssten hierzu ihre Nutzerdaten in diesen zentralen Bis-Grid-Identitätsprovider pflegen. Der Nachteil dieser Lösung ist, dass die nichtredundante Pflege der Nutzer- und Rollendaten durch die Unternehmen in ihren existieren Systemen verloren geht.

BIS-Grid eigener Online-CA/WAYF-Service schwierig: Eine weitere Alternative zur Nutzung der DFN-Installationen ist der Betrieb eines eigenen GridShib/Shibboleth-Stack für das BIS-Grid-Projekt bei PC^2. Die Erfahrungen aus dem Testbetrieb der DFN-Online CA fasst Reimer Karlsen-Masur wie folgt zusammen [KM08]:

> "Ein SLCS für den Regelbetrieb ist nicht mal so eben aufzusetzen."

Es ist daher zu diskutieren, ob der Betrieb eines eigenen GridShib-Stacks im Rahmen der Anwendungsszenarien in Bis-Grid sinnvoll ist.

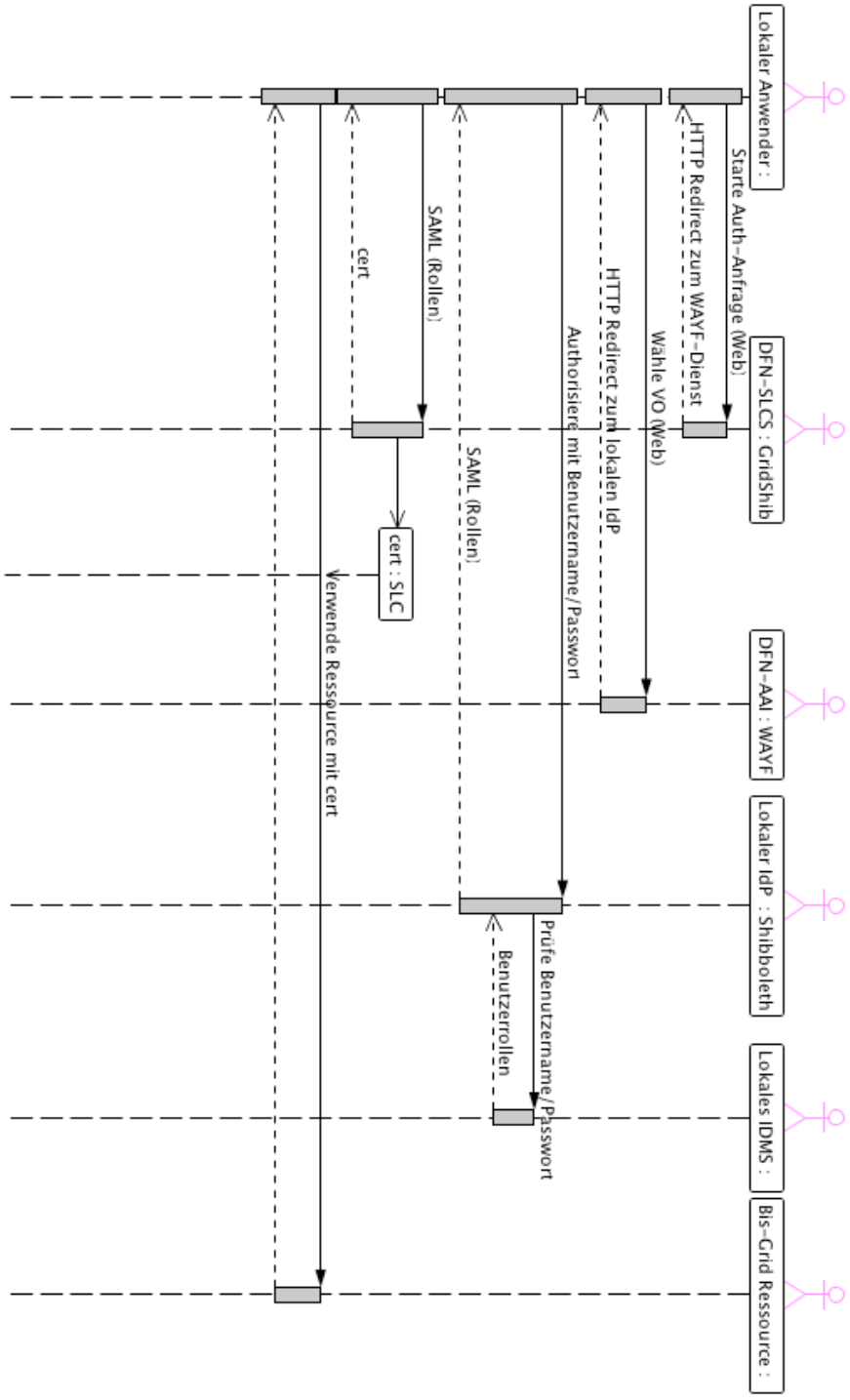


Abbildung 3: Architektur der Sicherheitsarchitektur auf Basis des Shibboleth-Systems

3.5.3 Alternative auf Basis von UVOS

Als Alternative zu der GridShib-basierten Lösung bietet sich für das Projekt BIS-Grid die Software *Unicore VO System (UVOS)*[14] an. Die VO-Lösung ist im Rahmen des von der EU geförderten Projektes Chemomentum[15] entwickelt worden und setzt wie BIS-Grid auf UNICORE 6 auf. Grundsätzliche Funktion von UVOS ist die Verwaltung von Nutzeridentitäten, die hierarchische Organisation der Informationen in Gruppen und die Anreicherung der Nutzerinformationen um zusätzliche Attribute. Die im UVOS enthaltenen Informationen können von SAML2-konformen Anwendungen abgefragt werden. Dazu sind die folgenden SAML Profile implementiert [Ben07]:

- SAML Attribute Query Deployment Profile for X.509 Subjects
- SAML Attribute Self-Query Deployment Profile for X.509 Subjects
- OGSA Attribute Exchange Profile Version 1.2
- XACML Attribute Profile

Die Authentifizierung der Nutzer bei UVOS kann über verschiedene Mechanismen erfolgen. Allen gemein ist aber, dass abhängig vom Authentifizierungsmechansimus und dem Authentifizierungsprotokoll, die Authentifizierungsinformationen auf eine Identität abgebildet werden. Jede Anfrage an das UVOS-System muss authentifiziert werden. Es gibt drei verschiedene Kombinationen aus Authentifizierungsmechanismus und -protokoll [Ben07]:

- X.509 TLS authenticated TLS session peer is mapped to an identity of X509 certificate type.
- DN TLS authenticated TLS session peer is mapped to an identity of DN type.
- Login HTTP an email type identity is created as obtained from HTTP BASIC authentication header and verified using a password, which is also set in the header.

UVOS unterstützt zur Abfrage der gespeicherten Informationen die beiden Methoden *PULL* und *PUSH*. Die PULL-Methode findet Verwendung wenn ein Service, z. B. UNICORE/X, die Informationen für einen Nutzer beim UVOS abfragt. Die dann vom UVOS mitgeteilten Informationen können von UNICORE/X zur Entscheidung über die Autorisierung herangezogen werden. Abbildung 4 beschreibt den Vorgang[16]:

[14] http://uvos.chemomentum.org/
[15] http://www.chemomentum.org/
[16] UVOS Dokumentation: http://uvos.chemomentum.org/documentation.html

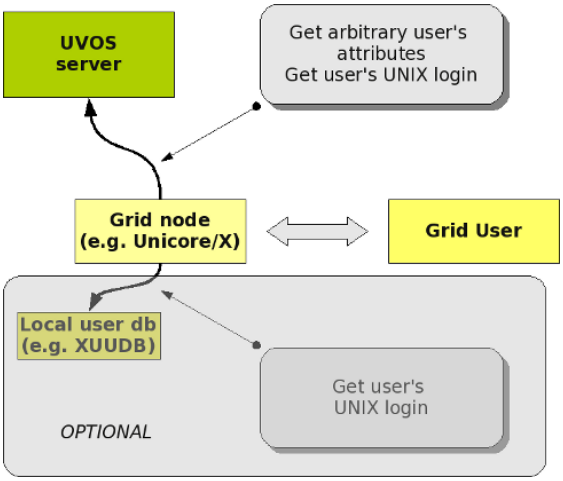


Abbildung 4: Schematische Darstellung UVOS mit PULL-Methode

Bei der PUSH-Methode kontaktiert der Nutzer direkt den UVOS-Server und erhält die Liste seiner Attribute als *Signed Assertion*. Diese Liste kann dann an den Aufruf eines Grid Service angehängt und damit dem Service bekannt gemacht werden. Es muss eine Vertrauensstellung zwischen UVOS-Server und Grid-Service geben, damit der Grid Service der Signatur von UVOS auch vertraut. Der Vorteil für den Nutzer liegt darin, dass er nur einen Teil seiner Attribute, die im UVOS hinterlegt sind, dem Grid Service bekannt geben kann. Eine Übersicht über die PUSH-Methode beschreibt Abbildung 5[17]:

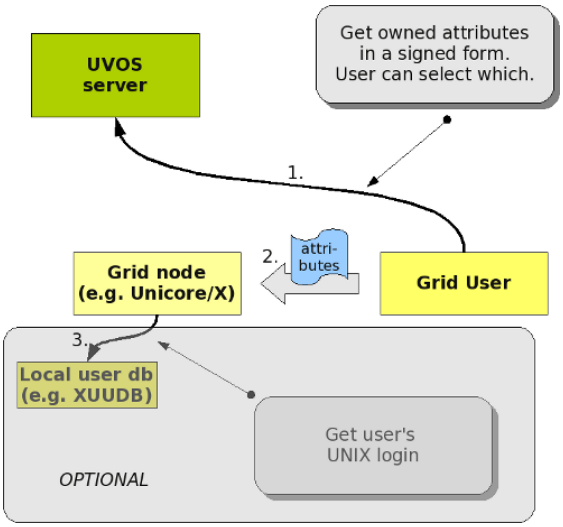


Abbildung 5: Schematische Darstellung UVOS mit PUSH-Methode

[17]UVOS Dokumentation: http://uvos.chemomentum.org/documentation.html

Für das BIS-Grid-Projekt bietet UVOS Mechanismen, die zur Abbildung der verschiedenen Rollen und die Nutzung von SAML notwendig sind. Die verschiedenen Workflow-Rollen können über Attribute im UVOS abgebildet werden. Es gibt im Gegensatz zu GridShib einen entscheidenen Nachteil: Bei UVOS handelt es sich nicht um eine verteilte AAI. Der Vorteil von UVOS liegt aber in der Einfachheit und die gute Interoperabilität mit UNICORE 6. Dennoch kann ein Großteil der unter 3.5.1 beschriebenen Anforderungen an eine AAI abgedeckt werden.

In der Praxis würde der UVOS-Service bei einem der Anbieter in BIS-Grid als Service installiert werden. Für die Verwaltung der Nutzer gibt es zwei Möglichkeiten. Entweder die Anwender stellen die Informationen ihrer Nutzer zu Verfügung, oder der Anbieter installiert die zum UVOS gehörende *VO Registration*-Anwendung und lässt die Anwender die Informationen ihrer Nutzer selber verwalten. Die Anbindung zu UNICORE 6 ist auf den Webseiten des UNICORE-Projektes unter "VO Support for UNICORE/X"[18] beschrieben.

3.5.4 Alternative auf Basis von Cisco Securent Entitelment Solution

Die Firma Securent bezeichnet sich selbst als "The Leader in Entitelment Managment". Securent wurde 2004 von ehemaligen Hewlett-Packard Mitarbeitern in Mountain View (CA) gegründet. Im November 2007 wurde die Firma von Cisco für 100 Millionen Dollar übernommen. Teil des Portfolios ist das kommerzielle Produkt "Entitlement Management Solution" (EMS). Zu den Kunden gehören unter anderem Credit-Suisse, First American und Qualcomm. Auf den Webseiten des Produkts[19] wird die Unterstützung verschiedener Standards, vor allem aber SAML und XACML2.0, hervorgehoben. Auffällig ist die Unterstützung des noch nicht verabschiedeten XACML3.0-Standards. Betont wird die Applikations- und Plattformunabhängigkeit des EMS, was als *ägnostic approach"* beschrieben wird. Das EMS gliedert sich in drei Komponenten auf:

- Centralized policy administration point (PAP)
- Policy decision points (PDPs)
- Policy enforcment points (PEPs)

Das PAP ist eine zentrale Konsole für die Pflege und die Überwachung von Rechten (Policies). Es soll die Rechtevergabe sowohl auf Unternehmensebene als auch auf Applikationsebene möglich sein. Auch das zentrale Audit aller Policies über alle Applikationen ist laut der Beschreibung möglich. Bei dem PDP wird die hohe Geschwindigkeit ("high performance run-time resolution") und die Verwendung von verteilten *decision caches* beworben. Die PDP sollen eine einfache Integration ("snap-on") von Verzeichnisdiensten wie LDAP und Active Directory anbieten. Die PEP werden damit beworben, dass sie *out-of-the-box* für alle führenden kommerziellen Applikationen wie Microsoft SharePoint, BEA WebLogic Portal, IBM WebSphere Portal, JBoss Portal und Documentum erhältlich sind. Als unterstützte Plattformen werden J2EE, Spring-ACEGI, SOAP,

[18] http://www.unicore.eu/documentation/manuals/unicore6/uas-vo/
[19] http://www.securent.com/products/approach/

.Net, C#, C++, VB und COM aufgeführt. Ein wichtiger Punkt scheint die Fähigkeit der PEP zu sein, Entscheidungen des PDP aus Performance-Gründen zu cachen. Eine schematische Darstellung der Securent-Komponenten und ihrem Zusammenwirken zeigt Abbildung 6[20]:

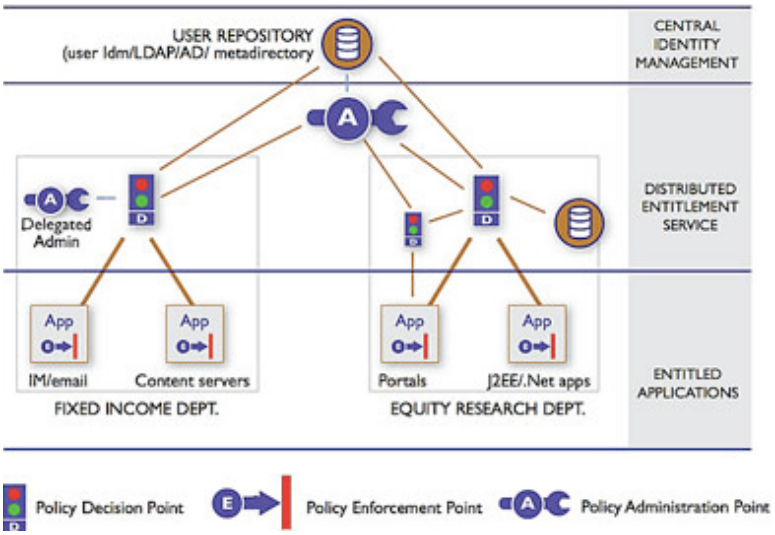


Abbildung 6: Cisco Securent Komponenten Übersicht

[20] siehe http://www.securent.com/products/components/

4 Anforderungen an Service Level Agreements in BIS-Grid

Im Folgenden werden die Überlegungen zum Thema Service Level Agreements (SLAs) in BIS-Grid dargestellt. In Abschnitt 4.1 wird zunächst eine kurze Einführung in Service Level Agreements präsentiert. Danach werden in Abschnitt 4.2 eine Definition für SLA gegeben, Merkmale eines SLA vorgestellt, und SLAs klassifiziert. In Abschnitt 4.3 werden schließlich grundlegende Überlegungen zur Gestaltung von Service Level Agreements in BIS-Grid dargestellt. Die Grundlagen der folgenden Abschnitte beziehen sich dabei maßgeblich auf die Arbeit von Berger [Ber05].

In Anbetracht der laufenden Arbeiten in der Umsetzung der Anwendungsszenarien in BIS-Grid und der Arbeiten bzgl. geeigneter Kollaborations- und Geschäftsmodelle für die Erbringung Grid-basierter Integrationsdienstleistungen ist dieser Abschnitt Gegenstand laufender Arbeiten und kann daher zukünftig entsprechend erweitert werden.

4.1 Einführung

Unternehmen und Organisationen setzen IT-Systeme zur Unterstützung betrieblicher Aufgaben ein. Idealerweise stehen diese dauerhaft und zuverlässig zur Verfügung. Der produktive Betrieb der verschiedenen IT-Systeme stellt sich in der Praxis jedoch als sehr aufwändig dar und wird z. B. durch Systemausfälle, Wartungsarbeiten, Systeminkompatibilitäten und Performance-Engpässen qualitativ beeinträchtigt. Eine mögliche Lösung zur Fokussierung auf die Kernaufgaben einer Organisation stellt die Auslagerung des IT-Infrastrukturbetriebs dar. Ziel ist hierbei oftmals, durch so genanntes Outsourcing höhere Dienstqualitäten nutzen zu können, als die entsprechende Organisation sich mit eigenen Mitteln sinnvoll erbringen könnte. Zur Inanspruchnahme solcher Dienstleistungen ist es jedoch notwendig, die Anforderungen an die zu erbringenden Einzelleistungen zu definieren und Maßnahmen zur Überwachung und Erbringungssicherung zu installieren. Als eine bestimmte Form der Leistungsvereinbarung zwischen einem Dienstleister und einem Leistungsnehmer leisten Service Level Agreements (SLAs) hierzu einen wichtigen Beitrag.

Nachfolgend soll diskutiert werden, in wie weit SLAs im Kontext des BIS-Grid-Projekts betrachtet werden. Insbesondere steht hierbei im Vordergrund, in welchem Rahmen SLAs konzeptionell für einen produktiven Betrieb in einem Integrationsdienstleistungsszenario verwendet werden könnten.

4.2 Definition, Merkmale und Klassifikation von Service Level Agreements

Basierend auf Berger definieren wir in BIS-Grid ein Service Level Agreement als eine *"formale, schriftlich dokumentierte, für einen bestimmten Zeitraum abgeschlossene Vereinbarung zwischen einem Leistungsnehmer (Kunde) und einem Leistungsanbieter (Dienstleister), in der der Leistungsnehmer die Erbringung gewisser inhaltlich und qualitativ definierter Dienstleistungen und der Kunde hierfür die Leistung definierter finanzieller Ausgleichszahlungen zusagt"* [Ber05]. Dabei erfolgt die Festlegung der durch den Dienstleister zu erbringende Qualität der Dienstleistung durch die Vereinbarung

von einzuhaltenden *Service Levels*. Diese werden durch gemeinsam definierte und quantifizierbare Dienstleistungsmerkmale in Form von Kennzahlen definiert. Ferner definiert ein SLA *"Verfahren, die den Nachweis der Einhaltung der Service-Levels regeln, sowie Konsequenzen für den Fall der Abweichung von den vereinbarten Service-Levels"* [Ber05]. Dabei sehen wir die folgenden Merkmale als charakteristisch für SLAs an (vgl. [Ber05]):

- Formalität. Eine SLA ist formal strukturiert und schriftlich dokumentiert.
- Bilateralität. Eine SLA wird zwischen zwei Parteien geschlossen.
- Dienstleistungsbezug. Eine SLA bezieht sich auf eine Dienstleistung als Wirtschaftsgut.
- Verpflichtungsbezug. Eine SLA beinhaltet die Verpflichtung der Erbringung einer Dienstleistung eines Partners (Dienstleister) und die Verpflichtung der Erbringung einer Gegenleistung eines anderen Partners (Kunde).
- Zeitbezug. Eine SLA bezieht sich stehts auf einen bestimmten Zeitraum.
- Inhaltsbezug. Eine SLA beinhaltet die inhaltliche Beschreibung der zu erbringenden Dienstleistung sowie die Beschreibung von Regelprozessen zur Dienstleistungserbringung.
- Qualitätzbezug. Eine SLA definiert die Qualität der zu erbringenden Dienstleistung. Dies geschieht durch die Quantifizierung relevanter Merkmale der Dienstleistung mit Hilfe der Definition von *Kennzahlen*[21] und so genannten *Service Levels*[22]. Abbildung 7 zeigt hierzu ein Entity Relationship-Diagramm zum Zusammenhang zwischen SLA, Kennzahlen und Service Levels.
- Preisbezug. Eine SLA nennt die Verrechnungspreise der Dienstleistung (z. B. auch Kompensationszahlungen) in Bezug auf die definierten Service Levels.
- Abweichungsregelung. Eine SLA enthält Regelungen für Abweichungen von vereinbarten Service Levels (z. B. Konventionalstrafen).

Generell kann zwischen SLAs im engeren Sinne und SLAs im weiteren Sinne unterschieden werden. Erstere definieren ausschließlich die zu erbringende Dienstleistungsqualität, letztere neben der Qualität der Dienstleistung ebenfalls den konkreten Inhalt und die Kosten der Dienstleistung. Eine weitere Klassifizierung kann nach der Art/Beschaffenheit der Beziehungen der beiden Partner eines SLA vorgenommen werden. Bzgl. der rechtlichen wirtschaftlichen Beziehungen kann unterschieden werden, ob Dienstleister und Partner ein und derselben Organisation angehören oder ob sie organisatorisch und

[21] *"Eine Kennzahl bezeichnet eine in numerischer Weise ausgedrückte Information über einen bestimmten quantifizierbaren Tatbestand"* [Ber05].

[22] "Ein Service-Level stellt den Wert einer bestimmten, in einem SLA vereinbarten Kennzahl zur Beurteilung der Qualität einer Dienstleistung dar"[Ber05].

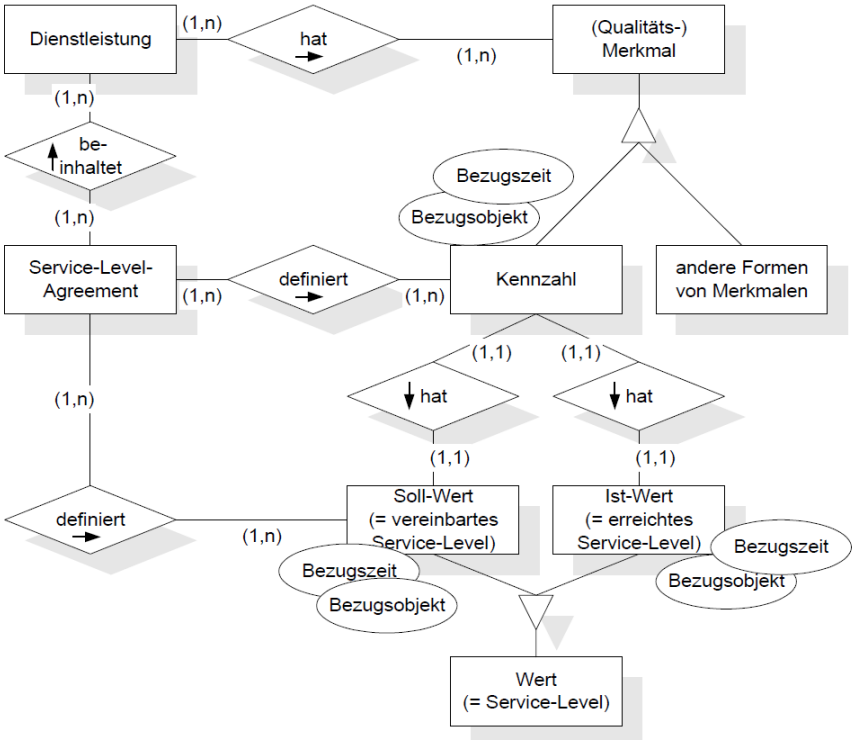


Abbildung 7: Entity Relationship-Diagramm zum Zusammenhang zwischen SLA, Kennzahlen und Service Levels nach [Ber05]

wirtschaftlich unabhängig sind. Im ersten Falle spricht man von *internen SLAs*, in letzterem von *externen SLAs*. Weiterhin können die internen SLAs in *unternehmensinterne und konzerninterne SLAs* unterschieden werden, je nachdem, ob auch innerhalb der Organisationsform bei den internen SLAs wirtschaftliche oder rechtliche Aspekte bestehen. Im Falle von BIS-Grid wird davon ausgegangen, dass zunächst externe SLAs im Vordergrund stehen, obwohl auch interne SLAs (insbesondere konzerninterne SLAs) eine Rolle spielen können. Dies kann z. B. im KIESELSTEIN-Szenario der Fall sein, da mit der KIESELSTEIN Group eine Unternehmensgruppe betrachtet wird, die aus drei rechtlich eigenständigen Unternehmensteilen besteht (vgl. Del. 4.5 bis 4.8).

Ein weiteres Unterscheidungsmerkmal ist der Grad des Anwendungsbezugs des Leistungsnehmers in der SLA. Danach lassen sich SLAs in anwendungsbezogene SLAs und technische SLAs unterscheiden. *Anwendungsbezogene SLAs* gehen dabei auf die Belange von Endanwendern ein. Diese betrachten Vereinbarungen, die den direkten fachlichen Nutzen der IT-Dienstleistung für deren betriebliche Aufgabe zum Gegenstand haben. *Technische SLAs* beziehen sich dagegen ausschließlich auf spezifische technische Anforderungen und setzen insbesondere auf Seiten des Leistungsnehmers technisches Verständnis voraus. Für die BIS-Grid-Szenarien (Szenario Maschinenkonstruktion und -Vertrieb bei KIESELSTEIN und Call-Center-Support bei CeWe Color) betrachten wir keine kla-

re Unterscheidung zwischen technischen und rein anwenderbezogenen SLAs, sehen aber einen stärkeren Bezug zur technischen Seite. Abbildung 8 zeigt den Fokus auf die in BIS-Grid betrachteten SLAs im Rahmen der hier vorgestellten Klassifikation. Die Gründe für diese Einordnung sind wie folgt.

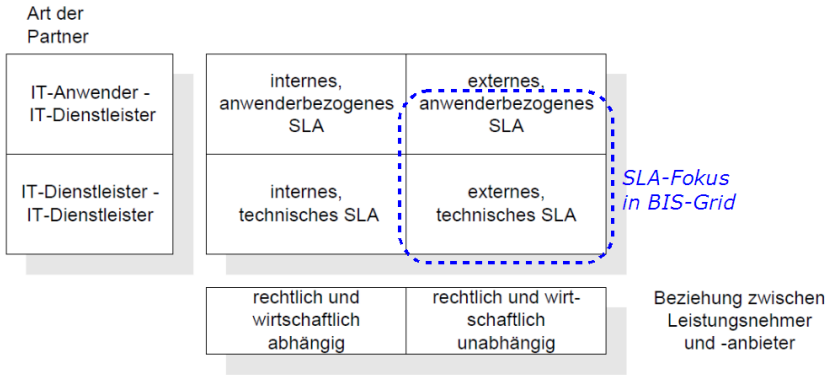


Abbildung 8: Klassifikation von SLAs nach [Ber05] und Einordnung von in BIS-Grid betrachteten SLAs

Seitens CeWe Color und KIESELSTEIN werden hauptsächlich technische Anforderungen in Bezug auf die Nutzung einer externen Ablaufsteuerung zur Dienstorchestrierung genannt. Insbesondere stehen hierbei Sicherheitsvorkehrungen im Vordergrund. Die genannten Aspekte umfassen den kontrollierten und gesicherten Zugriff auf Unternehmensdaten als Teil von Orchestrierungen, und den kontrollierten und gesicherten Zugriff auf die Orchestrierungen selbst. Dies schließt aber auch die Möglichkeit des Monitorings von laufenden Orchestrierungen als technische Repräsentationen von Geschäftsprozessen ein. Insgesamt sind hierbei die unternehmensspezifischen Rollen und Rechte zu berücksichtigen und gegebenenfalls auf ein geeignetes Rollen- und Rechtekonzept für Workflow-Beteiligte abzubilden (vgl. Abschnitt 3.4). Da die betrachteten Prozesse bei KIESELSTEIN zum Teil standortübergreifend (Chemnitz/Dresden) ablaufen, ist auch deswegen die Anforderung an die Datensicherheit als hoch einzuordnen. Weitere wichtige Anforderungen sind eine hohe Ausfallsicherheit der angebotenen Dienste und der zugehörigen entsprechenden Clients, sowie die Gewährleistung vereinbarter Antwortzeiten. Während ersteres ein Kriterium ist, dass für beide Szenarien wichtig ist, ist die Gewährleistung vereinbarter Antwortzeiten insbesondere für das CeWe Color Call-Center-Szenario von großer Bedeutung. Für nähere Details verweisen wir auf Del. 4.9 und Del. 4.10, *Dokument mit Anforderungen an die Grid-basierte Integration und Orchestrierung im Anwendungsszenario CeWe Color/KIESELSTEIN.*

4.3 Gestaltung von Service Level Agreements in BIS-Grid

In diesem Abschnitt sollen die grundlegenden Überlegungen zur Gestaltung von Service Level Agreements in BIS-Grid dargestellt werden. Ziel dieses Abschnittes ist dabei

nicht, ein explizites und detailliertes SLA-Template für sämtliche Anwendungsszenarien bereit zu stellen, die in BIS-Grid bzw. mit der in BIS-Grid betrachteten und prototypisch implementierten *Integration as a Service*-Plattform denkbar wären. Aus unserer Sicht ist ein solches Vorgehen aus Gründen der Generizität der technischen BIS-Grid-Infrastruktur und der Individualität bilateraler SLAs nicht tauglich. Stattdessen sehen wir es als sinnvoll an, einen für die in den BIS-Grid betrachteten Anwendungsszenarien gültigen Anforderungskatalog zu erstellen, in denen die Elemente identifiziert und beschrieben sind, die als unbedingt erforderlich angesehen werden. Hierzu bietet es sich an, eine geeignete Strukturierung zu verwenden. Wir greifen hier die von Berger verwendete Strukturierung in *vereinbarungsbezogene, dienstleistungsbezogene, managementbezogene und dokumentationsbezogene Elemente* auf. Diese werden wie folgt aufgefasst.

- Vereinbarungsbezogene Elemente definieren grundlegende Aspekte der durch das SLA dargestellten Vereinbarung an sich, sowie deren Regelung.
- Dienstleistungsbezogene Elemente beschreiben sämtliche Aspekte, die in direktem Zusammenhang mit der zu erbringenden Dienstleistung stehen. Diese sind in den BIS-Grid-Szenarien hauptsächlich technischer Natur.
- Managementbezogene Elemente beziehen sich auf Aspekte, die die Handhabung des SLA zum Thema haben. Sie bestehen im Wesentlichen aus Definitionen von Regelungen.
- Dokumentbezogene Elemente umfassen sekundäre administrative und redaktionelle Aspekte eines SLAs.

Im Rahmen der Anwendungsszenarien fokussieren wir zunächst vereinbarungsbezogene Grundelemente, dienstleistunsbezogenen Elemente und managementbezogene Elemente, während juristische Elemente, preisbezogene Elemente und dokumentbezogene Elemente in nachfolgenden Schritten betrachtet werden können. Abbildung 9 zeigt einen Überblick über die möglichen Elemente eines SLA und den Betrachtungsfokus in BIS-Grid für die Anwendungsszenarien in erster Iteration. Als zentrale Anforderungen an die exemplarische Definition von SLAs für die Anwendungsszenarien wird dabei die Abdeckung der durch Kennzahlen quantifizierten Anforderungen der Anwendungspartner gesehen, die in den Del. 4.9 und 4.10 genannt werden.

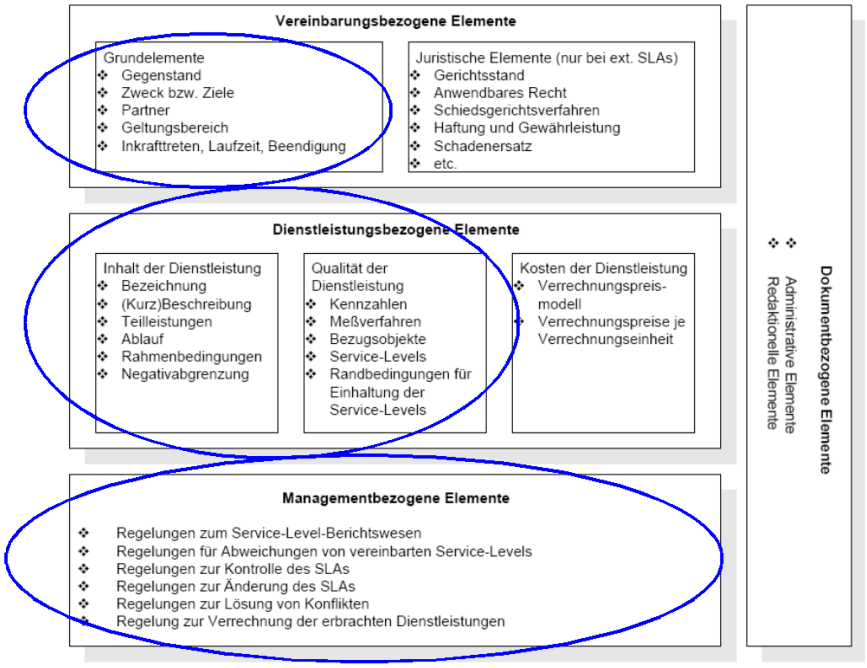


Abbildung 9: Strukturierung und Elemente eines SLA nach [Ber05] und Betrachtungsfokus in BIS-Grid für die Anwendungsszenarien in erster Iteration

5 Fazit

Bei der Bewertung der drei vorher genannten Alternativen gibt es verschiedene Kriterien und Perspektiven, die für eine Bewertung herangezogen werden müssen. Im folgenden werden die vorgestellten Alternativen aus den folgenden Perspektiven betrachtet:

- BIS-Grid-Projekt aus der Entwicklersicht
- BIS-Grid-Projekt aus Anbietersicht
- Anwender und Nutzer der BIS-Grid Lösung
- D-Grid Verbund

Jede dieser Perspektiven hat ihren eigenen Kriterienkatalog, bei dem sich die Kriterien zwischen den Katalogen nur bedingt überschneiden. Daher kann an dieser Stelle keine einfache Kreuzmatrix aufgestellt werden. Die einzelnen Perspektiven werden im Anschluss diskutiert.

5.1 BIS-Grid-Projekt aus Entwicklersicht

Wie schon in Abschnitt 3 vorgestellt, möchten die Entwickler soweit möglich bei der Sicherheitsinfrastruktur auf Standarts wie SAML und XACML setzen. Zum einen besteht die begründete Hoffnung, dass beide Standards sich weiter verbreiten und damit auf eine Lösung mit Perspektive gesetzt wird. Zum anderen sind SAML und XACML auch die Standards, die von UNICORE 6 unterstützt werden. Die Entwicklung eines eigenen Sicherheitsmoduls in UNICORE 6 liegt nicht im Fokus des BIS-Grid-Projektes und ist eine zeitaufwändige, fehlerträchtige Aufgabe. Daher müsste bei einem eigenen Sicherheitsmodul für UNICORE 6 entsprechender Aufwand für Verifikation und Fehlersuche betrieben werden.

Aus Entwicklersicht sollten alle drei beschriebenen Alternativen GridShib, UVOS und Cisco Securent Entitelment Solution gleichwertig sein, da sie jeweils SAML und XACML unterstützen. Bei der momentanen GridShib Lösung, die im Rahmen des DFN-Angebots Önline-CAßur Verfügung steht, muss aber festgestellt werden, dass zum jetzigen Zeitpunkt, Anfang 2009, SAML Assertions noch nicht unterstützt werden.

5.2 BIS-Grid-Projekt aus Anbietersicht

Eine BIS-Grid-Lösung, die für verschiedene Nutzergruppen von einem Anbieter zur Verfügung gestellt wird, läuft in der Regel auf den selben Ressourcen, die auch von anderen virtuellen Organisationen (VO) im Rahmen des D-Grid genutzt werden. Daher sind die Ressourcenanbieter bestrebt, möglichst allgemeine Mechanismen für Authentifizierung und Autorisierung zu nutzen.

Eine spezielle AAI für eine Nutzergruppe ist für einen Ressourcenanbieter nur sinnvoll, wenn der Aufwand in einem vernünftigen Verhältnis zum Ertrag steht. Üblicherweise ist der Ertrag entweder durch eine große Nutzerzahl gegeben. Oder der Aufwand für

die spezielle Lösung für eine kleine Nutzergruppe ist so gering, dass die Lösung in die Supportmatrix aufgenommen werden kann und die kleine Nutzergruppe davon profitiert.

Aus Anbietersicht sind daher die in Abschnitt 3 genannten Alternativen nicht equivalent. Die DFN Online-CA Lösung ist die sicherlich favorisierte Lösung. Denn die Online-CA ist der Grundstock für die zukünftige D-Grid-AAI und somit potenziell die Lösung, mit der ein größerer Nutzerkreis abgedeckt werden kann.

Eine BIS-Grid-interne Online-CA, die bei einem Resourcenanbieter aufgesetzt wird, ist im Gegensatz dazu keine Lösung mit Zukunft. Das bedeutet für einen Resourcenanbieter eine erheblichen Mehraufwand, sowohl bei der Installation als auch bei der Wartung, für einen sehr beschränkten Nutzerkreis.

Wenn für einen kleinen Nutzerkreis, wie BIS-Grid, eine spezielle AAI etabliert werden muss, dann sollte es sich um eine überschaubare, wartbare Lösung handeln. Das UVOS verspricht genau das für BIS-Grid. Es ist optimiert für UNICORE 6, besteht aus einem Service und hat keine weiteren Abhängigkeiten. Der Nachteil einer zentralen Pflege, im Gegensatz zu einem verteilten Ansatz wie GridShib, ist bei der Projektgröße von BIS-Grid und den geplanten Testfällen vernachlässigbar.

Die dritte Alternative in Form von Cisco Securent Entitelment Solution (EMS) ist für einen Resourcenabieter nur dann interessant, wenn die Kostenseite geklärt ist und ein entsprechender Nutzerkreis zur Verfügung steht. Sind diese Punkte befriedigend geklärt, steht einer solchen Lösung nichts im Weg. Denn beim Kauf eines solchen Produktes wird ein Resourcenanbieter den entsprechenden Support automatisch bekommen, bzw. sich bei der Beschaffung dazu kaufen.

5.3 Anwender und Nutzer der BIS-Grid Lösung

Verallgemeinert kann man für die Nutzer einer BIS-Grid Lösung feststellen, dass sie möglichst wenig mit der Verwaltung ihrer Benutzerinformationen oder Zertifikaten zu tun haben wollen. Bei ihnen liegt ausschließlich die einfache Nutzung der Dienste und Ressourcen im Fokus.

Für wissenschaftliche Nutzer der BIS-Grid-Lösung ist die Nutzung der DFN Online-CA unproblematisch, sobald sie sich an der Föderation beteiligt. Bei einer BIS-Grid-spezifischen Online-CA hängt die Möglichkeit der Nutzung sicher sehr stark von der Flexibilität des lokalen Identity Providers und seinen Policies ab. Bei einer UVOS-basierten Lösung sollte es für wissenschaftliche Nutzer keine Hindernisse geben. Dagegen hängt der Einsatz von EMS vom Kostenmodell ab, ob und welche Kosten der Nutzer zu tragen hat.

Kommerzielle Anwender wollen im Hinblick auf den Datenschutz, die Vertraulichkeit und das Vertrauensverhältnis zu Ressourcenanbietern und AAI-Betreibern einige Aspekte geklärt wissen. Hinzu kommt die Frage des Vertrauen der Anwender in die technische Umsetzung der Lösung. Bei kommerziellen Anwendern der BIS-Grid-Lösung gibt es für die Nutzung der Online-CA verschiedene Hürden. Die erste Hürde besteht darin, dass der kommerzielle Anwender mit dem DFN e.V. einen Vertrag schliessen muss, damit er an der Föderation teilnehmen kann. Im Normalfall ist das mit einer Vergütung an das DFN verbunden, im Projekt-Umfeld wird teilweise auch darauf verzichtet. Die nächste

Hürde besteht in der Installation und Konfiguration des IdP auf Seiten des kommerziellen Anwenders, damit das firmeninterne Identity Mangament System in die Föderation integriert wird. Die Integration kann bei falscher Konfiguration den Abfluss von ungewünschten bzw. zu vielen Informationen bedeuten. Jeder kommerzielle Anwender wird für sich auch die Frage nach der Sicherheit, Verifizierbarkeit und sein eigenes Vertrauen in eine komplexe Föderation beantworten müssen.

Der Nutzung der UVOS Lösung stehen für kommerzielle Nutzer keine vertraglichen Gründe entgegen. Auch der Abfluss von sensitiven Informationen ist nicht zu befürchten, da das UVOS getrennt vom Identity Managment System funktioniert. Es gibt aber einen erhöhten Verwaltungsaufwand für die Nutzer, da die Informationen im UVOS zusätzlich gepflegt werden müssen. Da UVOS als Autentifizierungsschema *Login_HTTP* unterstützt, kann auf das Ausrollen von Zertifikaten verzichtet werden.

Für den Einsatz der Cisco Securent Entitelment Solution bei kommerziellen Nutzern sprechen einige Gründe. So hat das EMS gute Referenzen bei Kunden mit sensitiven Geschäftsfeldern, z. B. Banken. Des weiteren gibt es kommerziellen Support für das Produkt so wie Hilfe für die richtige Integration in das firmeninterne Identity Management System. Ein Nachteil dürften die Kosten für ein solches System sein.

5.4 D-Grid Verbund

Aus Sicht des D-Grid kann es für die in Abschnitt 3 genannten Alternativen nur eine Empfehlung geben: der Einsatz der DFN Online-CA. Der Aufbau von parallen Strukturen im Bereich AAI kann nicht gewünscht sein. Auch wird im D-Grid auf absehbare Zeit die gerade im Aufbau befindliche Lösung nicht durch eine andere Lösung, mit gleichen technischen Merkmalen, abgelöst werden. Denn UVOS ist aus Sicht des D-Grid nicht skalierbar und Cisco Securent Entitelment Solution ist aufgrund der Kosten nicht umsetzbar.

5.5 Schlussfolgerung

Bei Abwägung der oben genannten Punkte, und unter Berücksichtigung der in3.5.1 genannten Anforderungen, kann man zum jetzigen Zeitpunkt, Anfang 2009, für das BIS-Grid-Projekt folgende Empfehlung aussprechen: Entweder wird im Rahmen des Projektes eine UVOS-basierte interne AAI etabliert, mit den genannten Einschränkungen. Oder dem DFN kann eine feste Zusage über die Nutzung der Online-CA durch eine genügend große Zahl von Nutzern gemacht werden. Dann würde das DFN die Erweiterung der Online-CA um SAML Assertions auch umsetzen. Jedoch müsste bei der Erweiterung der Online-CA mit dem DFN noch über einen Zeitplan diskutiert werden.

Literatur

[Ban06] Tim Banks. Web Services Resource Framework (WSRF) - Primer v1.2. http://docs.oasis-open.org/wsrf/wsrf-primer-1.2-primer-cd-02.pdf, May 2006.

[Ben07] Krzysztof Benedyczak. Unicore virtual organisations service overview. Technical report, Interdisciplinary Centre for Mathematical and Computational Modelling Warsaw University, Poland, 2007.

[Ber05] Thomas G. Berger. *Konzeption und Management von Service-Level-Agreements für IT-Dienstleistungen.* PhD thesis, Fachbereich Rechts- und Wirtschaftswissenschaften der Technischen Universität Darmstadt, Darmstadt, April 2005.

[CHKT05] S. Conrad, W. Hasselbring, A. Koschel, and R. Tritsch. *Enterprise Application Integration.* Elsevier, 2005.

[GHH+08] Stefan Gudenkauf, Wilhelm Hasselbring, Felix Heine, André Höing, Guido Scherp, and Odej Kao. Bis-Grid: Business Workflows for the Grid. In Marian Bubak, Michal Turala, and Kazimierz Wiatr, editors, *CGW'07 Proceedings*, pages 86–94, Krakow, Poland, 2008. ACC CYFRONET AGH.

[HGS08] Andre Höing, Stefan Gudenkauf, and Guido Scherp. BIS-Grid Deliverable 3.2: Documentation - WS-BPEL Engine. Technical report, BIS-Grid, August 2008.

[HHG+07] Felix Heine, Andre Höing, Stefan Gudenkauf, Guido Scherp, Holger Nitsche, and Jens Lischka. BIS-Grid Deliverable 3.1: Specification. Technical report, BIS-Grid, December 2007.

[KM08] Reimer Karlsen-Masur. Ausstellung kurzlebiger Zertifikate mit der DFN-SLCS-CA. IVOM Workshop, Hannover, February 2008.

[MT] Tapio Niemi Matti Heikkurinen Miika Tuisku, Juho Karppinen. Java Enterprise Grids using JBoss middleware. `http://gridblocks.hip.fi/opencms/export/sites/gridblocks/downloads/J2EE_JEMS_Grid.pdf`. last vistied 17.12.2007.