Sichere Autorisierungen im Internet

DAS SHIBBOLETH-VERFAHREN SCHAFFT DIE VORAUSSETZUNG FÜR EINE BENUTZERFREUNDLICHE UNIVERSITÄTSÜBERGREIFENDE FORSCHUNG

Das so genannte Shibboleth-Verfahren ermöglicht eine verteilte Authentifizierung und Autorisierung für Anwendungen sowie Dienstleistungen im World Wide Web und kommt besonders im Bereich Forschung und Lehre zum Einsatz. Damit bietet es seinen Nutzern den Vorteil, sich nur einmal bei einer Heimateinrichtung zu authentisieren und danach ortsunabhängig auf Dienste anderer Anbieter zugreifen zu können. Ein Wissenschaftler des Instituts für Verteilte Systeme zeigt auf, wie dieses Verfahren im Bereich des Grid Computing eingesetzt werden kann.

Grid-Computing

Grid-Computing ist eine Form des verteilten Rechnens, bei der organisatorisch und geographisch verteilte Ressourcen lose gekoppelt werden. Bei diesen Ressourcen handelt es sich in erster Linie um Hochleistungsrechner und Speichersysteme, aber auch beispielsweise um Sensoren von wissenschaftlichen Experimenten. Durch die Kopplung dieser Systeme ist ein organisationsübergreifender Zugriff möglich. Somit können Forscher auf eine Infrastruktur zugreifen, die weit über das lokale Angebot ihrer Universität hinausgeht. Um den Zugriff über das Internet zu ermöglichen und Zugriffskontrollen durchführen zu können, ist eine spezielle Software auf den Ressourcen notwendig, die so genannte Grid Middleware.

Autorisierung im Grid

Im vom Bundesministerium für Bildung und Forschung geförderten Projekt »D-Grid« arbeiten Forschercommunities aus unterschiedlichsten Bereichen zusammen, um eine gemeinsame Gridcomputing-Infrastruktur aufzubauen. Eines der wichtigsten Ziele ist es, die existierenden IT- Infrastrukturen für wissenschaftliches Rechnen zu integrieren und interoperabel zu machen.

Parallel dazu wird in Deutschland zurzeit eine Shibboleth-Föderation aufgebaut, welche es Universitäten und Forschungseinrichtungen erlaubt, Attribute ihrer Mitarbeiter anderen Einrichtungen für Autorisierungszwecke auf sicherem Wege zur Verfügung zu stellen. Diese Föderation heißt »DFN-AAI«, wobei AAI für »Authentifizierungs- und Autorisierungsinfrastruktur« steht. Ein Mitarbeiter der Universität kann sich über dieses System beispielsweise ein Buch in der Bibliothek einer anderen Universität ausleihen, ohne dort einen separaten Benutzeraccount mit eigenem Benutzernamen und Passwort anlegen zu müssen. Dieses als »Single Sign-On« bezeichnete Konzept erleichtert den Benutzern die Verwaltung ihrer Logindaten erheblich, weil sie nicht mehr für jede Ressource einen separaten Benutzernamen verwalten müssen.

Für die Benutzung des D-Grids bietet es sich an, diese Infrastruktur insbesondere für Gelegenheitsnutzer einzusetzen. Durch die Verwendung der Shibboleth-Föderation wird aber nicht nur der Zugriff auf die dafür notwendigen digitalen Ausweise (Zertifikate) deutlich benutzerfreundlicher. Zusätzlich zu der reinen Authentifizierungsinformation kann nämlich noch eine Reihe von Nutzerattributen bereitgestellt werden. Klassische Beispiele hierfür wären »professor@uni-hannover.de« oder »student@uni-hannover.de«. Hierbei handelt es sich nicht um E-Mailadressen, sondern um Attribute. Das erste Beispiel heißt somit: »Der Nutzer hat das Attribut Professor an der Institution Leibniz Universität Hannover«. Diese Art von Attributen wird »Campus Attribute« genannt.

Neben dieser neueren Art von Attributen gibt es im Grid Computing auch bereits eine eigene Attributverwaltung in den sogenannten Virtuellen Organisationen (VO). Eine Virtuelle Organisation ist im Gegensatz zur Heimateinrichtung eines Nutzers keine real existierende Einrichtung, sondern ein virtueller Zusammenschluss von Forschern verschiedener Einrichtungen, die ein gemeinsames Forschungsziel verfolgen. Im D-Grid ist hierfür die Virtual Organization Management Service (VOMS) Technologie im Einsatz. Als benutzerfreundliches Webfrontend dient VOMRS (Virtual Organization Management and Registration Service). Hier kann ein Nutzer beispielsweise das Attribut »softwareadministrator@GDI-Grid« ausgestellt bekommen. Dies weist ihn als Softwareadministrator der Virtuellen Organisation GDI-Grid aus. Die größte Herausforderung liegt hierbei in der Hetero-

genität der existierenden Implementierungen: Drei Grid Middlewares und verschiedene Ansätze für die Nutzer- und Rechteverwaltung müssen orchestriert werden, um die beabsichtigte Interoperabilität zu gewährleisten.

Kodierung von Attributen

Damit die vorgestellten Attributtypen im Grid auf den eigentlichen Ressourcen für Zugriffskontrollentscheidungen zur Verfügung stehen, müssen sie in einer geeigneten Art und Weise kodiert und elektronisch übermittelt werden. Der Nutzer bezieht für ihn gültige Attribute von den jeweiligen Attribut-Autoritäten. Diese sind digital signiert, so dass ein potenziell bösartiger Nutzer sich nicht selber beliebige Attribute ausstellen kann, um ungerechtfertigten Zugriff zu erlangen. Durch die digitale Signatur kann aber auch die Kodierung nicht einfach geändert werden, da hierdurch die Signatur ungültig würde.

Die vorgestellten Quellen für Attribute, Shibboleth und VOMS verwenden unterschiedliche Kodierungen, mit denen die Attribute übertragen werden. Während Shibboleth auf den XML-basierten Standard »Security Assertion Markup Language« (SAML) setzt, verwendet der VOMS bisher sogenannte Attributzertifikate. Neuere Versionen des VOMS können bereits zusätzlich SAML-Assertions ausstellen. Semantisch sind diese Kodierungen (in diesem Kontext) äquivalent, aber sie unterscheiden sich deutlich in der verwendeten Syntax.

Die Konsumenten der Attribute sind im D-Grid drei verschiedene Middleware-Systeme, welche den Zugriff auf die Grid Ressourcen bereitstellen. Sie basieren ihre Zugriffsentscheidungen auf diesen Attributen. Diese Systeme unterscheiden sich in ihren Standardversionen stark in Bezug auf die unterstützten Kodierungen für Nutzerattribute, wie in Tabelle 1 dargestellt ist. Wie man einfach erkennen kann, gibt es keine Kodierung für die Attribute, welche von allen Komponenten unterstützt wird.

Middleware	Attributzertifikate	SAML-Assertion
Globus Toolkit 4 (pre-WS)	Keine Unterstützung	Keine Unterstützung
Globus Toolkit 4 (WS)	Unterstützung durch Plug-In (VOMS-PDP)	Unterstützung durch Plugin (GridShib)
UNICORE 5	Unterstützung durch Plug-In (in IVOM entwickelt)	Unterstützung durch Plug-In (in IVOM entwickelt)
gLite	Native Unterstützung	Keine Unterstützung

Tabelle 1
Attributbasierte Autorisierung in Grid Middlewares

Basierend auf diesen Erkenntnissen wurde im IVOM-Projekt eine Roadmap erstellt, um eine attributbasierte Autorisierung im D-Grid langfristig umsetzen zu können.

Eine Roadmap für Attributbasierte Autorisierung im D-Grid

Aufgrund der fehlenden gemeinsamen Unterstützung für die Kodierung der Attribute ist es derzeit nicht möglich, eine interoperable Grid Infrastruktur bereitzustellen, die

- Campus- und VO-Attribute zu den Grid Ressourcen überträgt,
- die drei Middlewares unterstützt,
- Vertrauensprobleme durch das Benutzen von »Trust Proxying«[1] vermeidet und
- keine potenziell nicht mehr gültigen Attribute bereitstellt.

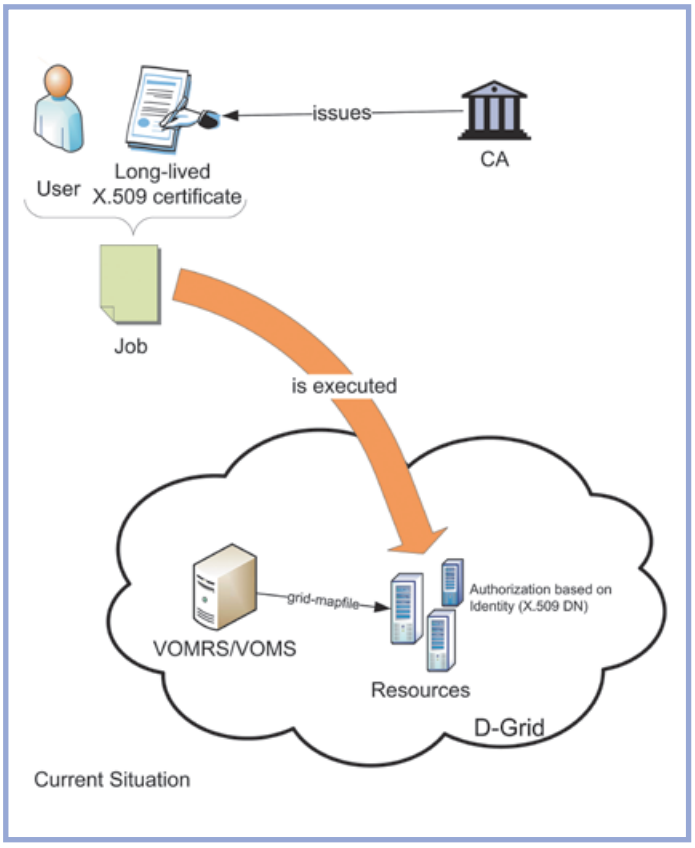

Abbildung 1
Ausgangssituation im D-Grid
Quelle: [1]

Ausgangslage
Identitätsbasierte Autorisierung im D-Grid

Die Ausgangssituation im D-Grid ermöglicht keine attributbasierte Autorisierung, sondern eine ausschließlich identitätsbasierte Autorisierung, das heißt jeder Nutzer muss persönlich namentlich

1 Trust Proxying bezeichnet das Neuausstellen von Attribute Assertions durch Dritte. Dadurch kann die Ressource nicht mehr explizit die Validität der Attribute prüfen, sondern die Ressource muss implizit darauf vertrauen, dass der Dritte die Attribute korrekt weitergeleitet hat.

bei jeder Grid-Ressource bekannt sein und kann nicht anhand einer Eigenschaft oder Rollenzugehörigkeit autorisiert werden. Dies skaliert nicht für die große Nutzerschaft und die große Anzahl von Ressourcen im Grid. Im Einzelnen funktioniert das wie in Abbildung 1 dargestellt: Eine CA stellt dem Nutzer ein mal im Jahr einen ebenso lang gültigen digitalen Ausweis (ein klassisches X.509 Zertifikat) aus, mit dem er sich auf Grid-Ressourcen ausweisen kann. Zusätzlich registriert der Nutzer sich einmal im Jahr auf einem VOMRS/VOMS-System, wo ein VO-Administrator seine Berechtigung prüft und den Nutzer im positiven Fall freischaltet. Von diesem VOMRS/VOMS-System werden täglich Listen mit den Namen aller autorisierten Personen (sogenannte grid-mapfiles) an alle Grid Ressourcen verteilt. Wenn nun ein Nutzer einen Job an eine dieser Ressourcen sendet, weist er sich mit seinem Namen aus und die Ressource überprüft anhand des grid-mapfiles, ob der Nutzer autorisiert ist.

Schritt 1
Verwendung von VO-Attributen für die Autorisierung im D-Grid

Der erste Schritt in Richtung attributbasierter Autorisierung ist in Abbildung 2 (links) dargestellt. Im Vergleich mit der Ausgangssituation können Nutzer nun ihre VO-Attribute vom VOMS/VOMRS-System mit entsprechenden Programmen abfragen und in ihre Jobbeschreibung einbinden. Da die Attribute vom VOMRS/VOMS digital signiert sind, ist es nicht möglich, dass Nutzer sich zusätzliche Attribute erschleichen. Aufgrund der bereits beschriebenen fehlenden Unterstützung für SAML-Assertions in den Middlewares muss dieses Verfahren zuerst mit Attributzertifikaten umgesetzt werden.

Im Einzelnen sind die zusätzlich notwendigen Komponenten:

- gLite unterstützt Attributzertifikate, somit sind keine zusätzlichen Komponenten notwendig.
- Globus Toolkit: Der VOMS-PDP (Policy Decision Point) muss in den Web Service-basierten Diensten installiert werden. Die nicht Webservice-basierten Komponenten werden nicht unterstützt.
- UNICORE 5: Unterstützung für Attributzertifikate und SAML-Assertions wurde in IVOM entwickelt und muss entsprechend installiert werden.

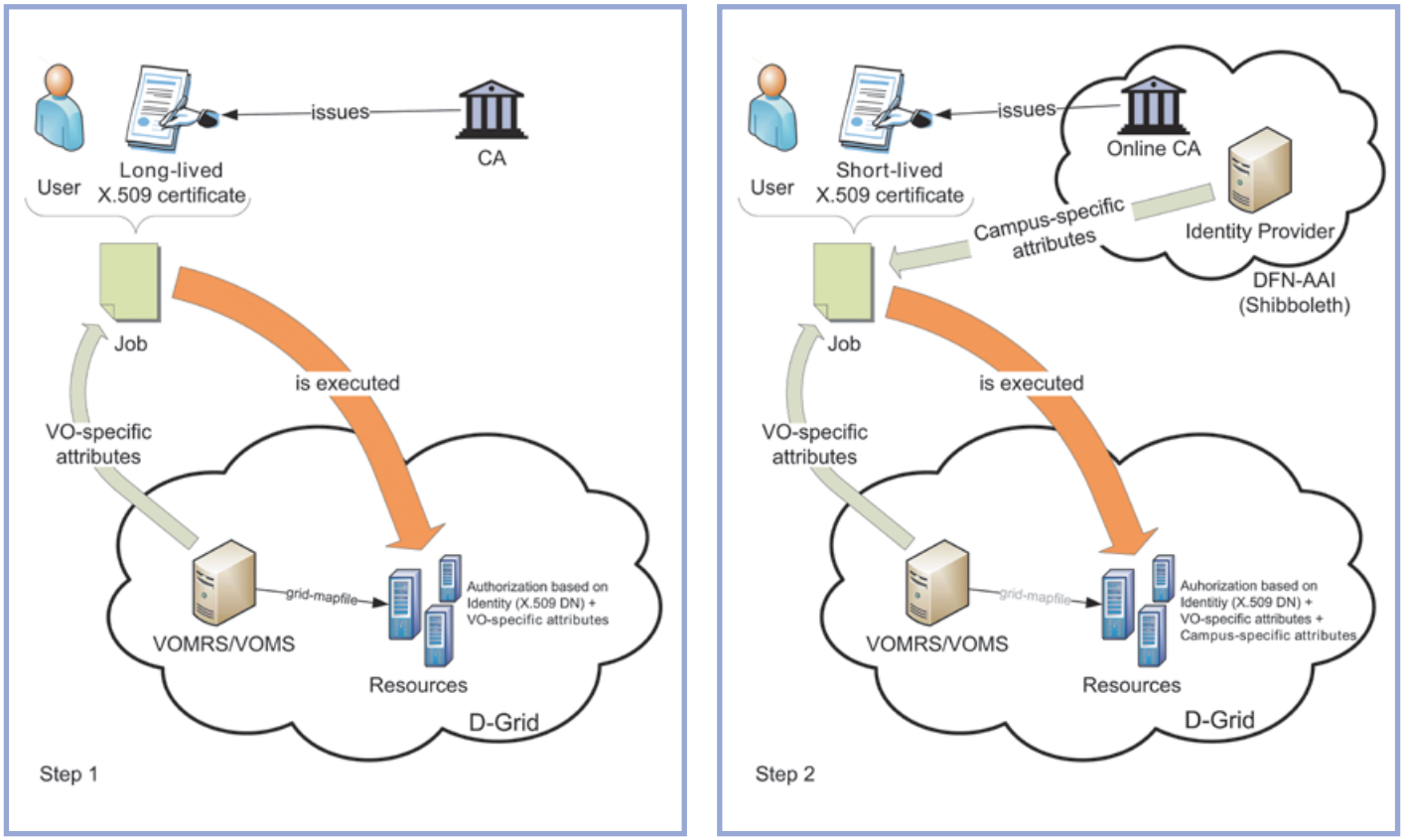

Abbildung 2
Unterstützung von VO- und Campusattributen
Quelle: [1]

Schritt 2
Verwendung von Campusattributen im D-Grid

Zur Unterstützung von Campusattributen werden weitere, momentan nicht verfügbare Komponenten benötigt. Sobald diese verfügbar sind beziehungsweise in D-Grid entwickelt wurden, kann dieser zweite Schritt umgesetzt werden. Hierbei wird die DFN-AAI nicht nur verwendet, um wie beschrieben die Campusattribute zu liefern. Zusätzlich wird der dort vorhandene Login genutzt, um kurzlebige Zertifikate auszustellen. Diese ersetzen die oben beschriebenen digitalen Ausweise, die einmal im Jahr beantragt werden müssen. Das Vorgehen ist in Abbildung 2 (rechts) dargestellt: Zusätzlich zu Schritt 1 werden nun noch Campusattribute in den Job eingebunden. Die Autorisierung auf den Ressourcen hat nun drei mögliche Attributklassen zur Auswahl, welche je nach Anwendungsfall einzeln oder kombiniert verwendet werden können. Diese sind die aus der Ausgangssituation bekannte Identität, die VO- und die Campusattribute.

Diese Ausbaustufe skaliert auch für große Nutzermengen und erlaubt auch Gelegenheitsnutzern den Zugriff auf das Grid, ohne dass sie das herkömmliche aufwändige Verfahren zum Bezug und der Verwaltung von digitalen Ausweisen benötigen.

Fazit

Ausgangspunkt war eine nicht skalierende Grid Sicherheits-Infrastruktur und die nur unzureichend umgesetzte Verfügbarkeit von middlewareübergreifender, attributbasierter Autorisierung. Es konnte gezeigt werden, wie in zwei Schritten das Ziel der auf Campus- und VO-Attributen basierenden Autorisierung erreicht werden kann. Hierbei ist der erste Schritt mit bereits verfügbarer Software umsetzbar, während für den zweiten Schritt die Voraussetzungen erst noch geschaffen werden müssen. Insgesamt ist so eine Roadmap entstanden, nach der die D-Grid Infrastruktur zurzeit erweitert wird.

Literatur

[1] P. Gietz u. a., IVOM Work Package 3 Report: A Concept for Authorization on D-Grid Resources. D-Grid, 2007.

Abbildung 3
Mitarbeiter der Arbeitsgruppe DCSec (Distributed Computing Security) am Institut für Verteilte Systeme

Ralf Gröper
Jahrgang 1978, ist seit 2006 wissenschaftlicher Mitarbeiter in der Distributed Computing Security Group (DCSec) am Institut für Verteilte Systeme an der Leibniz Universität-Hannover. Er forscht an Sicherheitsaspekten für Service-orientierte Architekturen in verteilten Systemen wie dem Grid. Kontakt: groeper@dcsec.uni-hannover.de