Kurzlebige Zertifikate in einem Gridportal-Szenario

Stefan Pinkernell, Bernadette Fritzsch
Alfred Wegener Institut für Polar- und Meeresforschung, Bremerhaven, Deutschland
stefan.pinkernell@awi.de, bernadette.fritzsch@awi.de

Abstract

Der Zugang zu D-Grid-Ressourcen ist derzeit auf eine zertifikatbasierte Authentifizierungs- und Autorisierungsinfrastruktur beschränkt, in der nur EUGridPMA akkreditierte X.509 Zertifikate akzeptiert werden. Es hat sich aber gezeigt, dass dies für weite Nutzerkreise eine sehr hohe Einstiegsschwelle bedeutet. Um diese herabzusenken, kann in portalbasierten Grids der Bezug und die Handhabung von Zertifikaten vom Portal im Namen des Nutzers übernommen werden. Dazu wird ein Portal Delegation Verfahren eingesetzt, bei dem auf Knopfdruck ein kurzlebiges Zertifikat von einer Online CA bezogen werden kann, das dann sofort im Portal zur Verfügung steht.

Für eine differenzierte und feingranulare Autorisierung auf den Grid-Ressourcen können zusätzliche Attribute genutzt werden. Als Attribut-Quellen kommen Campus Attribute aus der Shibboleth Umgebung und Rollen aus einer virtuellen Organisation in Frage. Diese Attribute werden am Portal gesammelt und automatisch als SAML Assertion in ein Proxy-Zertifikat eingebettet. In dem Beitrag wird das Konzept vorgestellt und die Implementierung gezeigt.

1 Einleitung

Der Zugang zu Grid-Ressourcen über die bereits etablierte zertifikatbasierte Authentifizierungs- und Autorisierungsinfrastruktur gestaltet sich für weite Nutzergruppen als schwierig. Die Motivation für die hier vorgestellten Entwicklungen war die Suche nach einem für den Nutzer möglichst einfachen Weg ins Grid, der eine gute Integration in Grid-Portale ermöglicht und den Nutzer weitgehend von der Beantragung und der Handhabung von Zertifikaten entlastet.

Die diskutierte Lösung verbindet zwei Ansätze: Zum einen soll der Nutzer von den Problemen im Zusammenhang mit der Beantragung, sicheren Speicherung und Handhabung des Zertifikats weitgehend entbunden werden, indem das Portal diese Aufgaben im Auftrag und Namen des Nutzers übernimmt. Zum anderen sollen kurzlebige Zertifikate genutzt werden, da für ihre Beantragung eine Authentifizierung innerhalb einer Shibboleth Föderation ausreicht, was relativ einfach in das Portal integriert werden kann. Die Zertifikate können jeweils bei Bedarf schnell bezogen und für die Absicherung des folgenden Gridjobs genutzt werden. Damit entfällt die Notwendigkeit, die Zertifikate über einen längeren Zeitraum sicher zu verwahren.

Für die feingranulare Autorisierung der Nutzer bei den Ressourcenprovidern kann das Konzept erweitert werden. Die Erfahrung zeigt, dass zum einen Informationen aus der Heimateinrichtung benötigt werden: So könnte etwa der Status eines Mitarbeiters (z.B. Praktikant) von Interesse sein, wenn eine Autorisierungsentscheidung für den Zugriff auf einen Datensatz getroffen werden soll. Zum anderen ist aber auch die Funktion eines Mitarbeiters innerhalb eines Projektes von Bedeutung, die über ein zentrales Rollenkonzept in einer virtuellen Organisation repräsentiert werden kann. Das Portal sammelt dazu die verfügbaren Informationen aus verschiedenen Autorisierungsquellen und bettet sie in Form einer SAML Assertion in das Proxy-Zertifikat ein. Damit stehen sie an der Grid-Ressource zur Auswertung bereit.

Im Gridshib Projekt [1] wurde schon ein ähnliches Konzept umgesetzt, bei dem allerdings nur Informationen aus einer einzelnen Quelle verwendet wurden. Für die hier vorgestellten Arbeiten mussten einige Anpassungen und Neuentwicklungen vorgenommen werden, um mehrere Attributquellen zu erlauben.

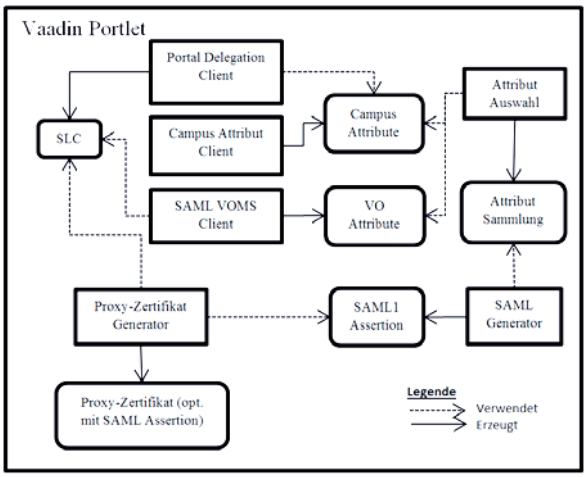

Abbildung 1: Schematischer Aufbau des entwickelten Portlets. Gezeigt wird das Zusammenspiel zwischen den einzelnen Klienten. Das für den Gridjob erstellte Proxy-Zertifikat enthält optional die am Portal gesammelten Attribute aus den unterschiedlichen Quellen als eingebettete SAML1 Assertion.

Die zentrale Software ist ein neu entwickeltes Portlet auf Basis des Java Frameworks Vaadin [2] (vgl. Abb.1). Es enthält neben einer Komponente zum Bezug der kurzlebigen Zertifikate aus dem Portal heraus auch einen Klienten für den VOMS SAML Service, der die Rolleninformation aus der virtuellen Organisation

abrufen kann, sowie ein Modul, das die Campus Attribute abruft. Zudem kann dieses Portlet eine neue SAML Assertion ausstellen, die eine Auswahl aus den gesammelten Attributen enthält. Auch die an der Grid-Ressource eingesetzte Software wurde für diesen neuen Anwendungsfall angepasst, was über Modifikationen an einer Bibliothek umgesetzt wurde.

In den folgenden Kapiteln werden zunächst die zugrunde liegenden Technologien vorgestellt und dann die entwickelte Software näher erläutert.

Die vorgestellten Arbeiten sind im Rahmen des vom BMBF geförderten Projekts „Nutzung von kurzlebigen Zertifikaten in portal-basierten Grids (GapSLC)“ entstanden.

2 Verwendete Technologien

2.1 Shibboleth

Shibboleth [3] bietet ein Verfahren zur verteilten Authentifizierung und Autorisierung im Umfeld der Webservices und Webanwendungen. Die grundlegende Idee sind dezentrale Nutzerverwaltungen, die in einer Föderation zusammengeschlossen sind und damit ein Vertrauensverhältnis untereinander aufbauen. Damit kann ein Nutzer nach erfolgter Anmeldung bei seiner Heimateinrichtung auch auf Dienste anderer Anbieter zugreifen, ohne sich nochmals authentifizieren zu müssen (Single Sign On). Shibboleth wird vor allem im Bereich der Lehre genutzt. Es gibt bereits eine Reihe von nationalen Föderationen (Bsp. DFN-AAI [4], SWITCHaai [5]).

2.2 SLCS

Kurzlebige Zertifikate (Short Lived Certificates, SLC) sind spezielle X.509 Credentials mit einer Gültigkeitsdauer von maximal 1.000.000 Sekunden, was ca.11,5 Tagen entspricht. Sie wurden bereits ursprünglich als eine Option zur Authentifizierung im Web diskutiert [6]. Im Rahmen von EGEE wurde dann gezeigt, wie sie in Grid-Umgebungen mit gLite als Grid Middleware eingesetzt werden können [7]. Dazu wurde ein spezieller Dienst (Short Lived Credential Service, SLCS) in der Shibboleth-Föderation entworfen und installiert.

In Deutschland stellt der DFN einen solchen Dienst mit seinem DFN-SLCS [8] zur Verfügung, über den EUGridPMA akkreditierte kurzlebige Zertifikate ausgestellt werden können. Der SLCS enthält neben einer Online Zertifizierungsstelle für die automatische Ausstellung der SLCs auch Schnittstellen, über die der Zertifikat-Request eingereicht und das fertige SLC ausgeliefert werden kann. Um diesen Dienst nutzen zu können, ist eine Reihe von Voraussetzungen zu erfüllen. Die jeweilige Einrichtung muss der DFN-AAI angehören. Im zugehörigen Shibboleth Identity Provider (IdP) muss für den Nutzer im Attribut „eduPersonEntitlement“ der URN „urn:geant:dfn.de:dfn-pki:slcs“ gesetzt sein. Für die Einrichtung und den Betrieb der SLCS-RA werden strenge Anforderungen gestellt [9].

Um für die kurzlebigen Zertifikate eine gleichwertiges „Level of Assurance“ LoA wie bei den konventionellen langlebigen Zertifikaten zu erreichen, gelten ähnlich restriktive Anforderungen bei der Handhabung der Zertifikate. Dies musste bei der Kombination mit Portal Delegation berücksichtigt werden. So dürfen beispielsweise die privaten Schlüssel der SLC nicht ungeschützt persistent auf dem Portalrechner abgelegt werden.

2.3 VOMS

Mit dem Virtual Organisation Membership Service (VOMS) kann eine Gruppe von Personen, die auch aus unterschiedlichen Organisationen stammen können, zu einer virtuellen Arbeitsgruppe verbunden werden. Den Mitgliedern dieser Arbeitsgruppe können dann zentral über ein Rollen-Konzept bestimmte Attribute zugeordnet werden, die für die Autorisierung bei den Ressourcen genutzt werden können [10].

In der Software *VomsAdmin* ist seit der Version 2.0.18 auch der sog. VOMS SAML Service enthalten. Damit können die VO-Attribute automatisiert über einen Web-Service abgerufen werden.

2.4 SAML

SAML ist ein ab 2001 von OASIS entwickeltes XML Framework zur Authentifizierung und Autorisierung [11]. Hauptanwendungsgebiet neben Single-Sign-On Systemen sind Autorisierungsdienste.

Das Framework existiert in zwei Versionen. Eine wachsende Zahl von Identity Providern verwendet SAML2 und stellt damit die Campus-Attribute zur Verfügung. Auch der VOMS SAML Service liefert die Nutzer-Attribute und -Rollen im SAML2 Format. Jedoch verwendet die an der Grid-Ressource genutzte Software *Gridshib for Globus Toolkit* noch SAML1 Assertions.

3 Portal Delegation

Beim Portal Delegation Verfahren [12] wird aus dem Portal heraus ein kurzlebiges Zertifikat am DFN-SLCS beantragt. Dabei werden das Schlüsselpaar und der davon abgeleitete Zertifikat-Request am Portal erstellt, welcher wiederum per Browser Redirect an den SLCS übergeben wird. All dies passiert im Namen des Nutzers auf Knopfdruck, die technischen Details sind dabei weitestgehend verborgen. Anschließend wird der Nutzer wieder an das Portal zurückgeleitet, wo das SLC für die weitere Prozessierung zur Verfügung steht.

Dieses Verfahren bietet den Vorteil, dass „frische“ kurzlebige Zertifikate auf Knopfdruck angefordert werden können und innerhalb kürzester Zeit am Portal bereitstehen. Für den Nutzer reduziert sich das gesamte technische Verfahren im Hintergrund auf drei Button-Klicks: Zunächst am Portal, um das Portal Delegation

Verfahren anzustoßen. Dann noch einmal am SLCS, wo dem Portal Delegation Verfahren explizit zugestimmt werden muss und noch ein letztes Mal, um – samt Zertifikat – wieder an das Portal zurückgeleitet zu werden.

In der hier vorgestellten Lösung ist der Nutzer per Shibboleth am Portal angemeldet. Die Campus-Daten, die für den Shibboleth-Login verwendet werden, stammen von der Heimateinrichtung des Nutzers und werden z.T. schon für die Erzeugung des Zertifikat-Requests verwendet. So werden beispielsweise der Vor- und Nachname, die E-Mail Adresse und die Heimateinrichtung aus den Campus Attributen übernommen. Das Zertifikat wird zwar aus dem Portal heraus angefordert und auch direkt an das Portal ausgeliefert, ausgestellt ist es aber auf den Nutzer!

Die Portal Delegation Software besteht aus zwei Teilen: Dem (DFN-) SLCS zum Ausstellen des kurzlebigen Zertifikats einerseits und einem Klienten zum Anfordern und Entgegennehmen andererseits. Letzterer Teil wurde zur Integration in das Portal neu implementiert und mit weiteren Funktionen versehen.

Eine bereits existierende Klient-Anwendung aus dem Gridshib Projekt in Form eines Perl CGI-Scripts erwies sich für eine Integration in das Grid-Portal als nicht brauchbar, da dort beispielsweise das Schlüsselmaterial ungeschützt auf der Festplatte abgespeichert wurde. Der Klient wurde daher für das Liferay Portal Framework komplett neu implementiert. Die Portal Delegation Komponente des Portlets erstellt das Schlüsselpaar und den Zertifikat Request, der dann an die Online CA gesendet wird, und nimmt auch das fertige kurzlebige Zertifikat in Empfang. Im Gegensatz zur ursprünglichen Implementierung wird das Schlüsselmaterial hier lediglich innerhalb der Session flüchtig im Arbeitsspeicher gehalten, womit diese Implementierung zu den SLC-Policies konform ist.

Damit werden in diesem Szenario die Zertifikate nun nicht mehr auf dem Rechner des Nutzers in dessen Eigenverantwortung gehalten. Stattdessen werden die kurzlebigen Zertifikate erst bei Bedarf aus dem Portal heraus im Namen des Nutzers automatisch bezogen und stehen dort zur weiteren Verwendung direkt zur Verfügung.

In weiteren Ausbaustufen wurden dem Portlet zusätzlich zur eigentlichen Portal Delegation Funktion noch weitere Features zur Attribut-basierten Autorisierung hinzugefügt.

4 Attribut-basierte Autorisierung

Am Portal werden mehrere Quellen für Nutzerattribute verwendet: Neben Campus Attributen aus der Shibboleth Umgebung werden auch Rollen-Informationen aus einer virtuellen Organisation benutzt. Das in Kapitel 3 vorgestellte Portlet dient neben der Funktion als Portal Delegation Klient auch dazu, die für die Autorisierung notwendigen Attribute aus diesen beiden Quellen zu laden.

Das Portal ist über einen Shibboleth Service Provider geschützt. Daher kann an dieser Stelle schon direkt auf die vom Identity Provider gelieferten Campus-Attribute des angemeldeten Shibboleth-Nutzers zugegriffen werden. Alle vom Shibboleth Identity-Provider für diesen Service Provider freigegebenen Attribute werden über den jeweiligen Service Provider zum Download bereitgestellt. Die Attribute sind schon in einer SAML Assertion zusammengefasst, deren Adresse über die Shibboleth-Session verfügbar ist. Nur innerhalb dieser Session ist der Zugriff auf die Assertion möglich.

Zusätzlich können noch die Rollen-Informationen aus der virtuellen Organisation über den VOMS SAML Service in Form einer SAML Assertion abgerufen werden. Dazu wurde ein Client in das Portlet integriert, der über eine Axis 2 Schnittstelle die Assertion vom SAML VOMS Server herunterlädt.

Um Attribute vom VOMS Server abrufen zu können, müssen die Nutzer bereits mit einem Zertifikat bei einer virtuellen Organisation registriert sein und zur Abfrage der VO-Informationen ein gültiges Zertifikat vorweisen. Dafür kann das bereits im ersten Schritt bezogene kurzlebige Zertifikat vom Portlet genutzt werden.

Die vom Identity Provider und dem VOMS SAML Service bereitgestellten Assertions liegen beide im SAML2 Format vor. Die Attribute aus diesen beiden Assertions werden zunächst am Portal zusammengestellt. Der Nutzer kann dort über eine graphische Oberfläche nochmals individuell entscheiden, welche Attribute konkret weitergeleitet werden sollen. Damit soll dem Prinzip der Datenvermeidung und Datensparsamkeit (data reduction and data economy) Rechnung getragen werden. Die ausgewählten Attribute werden dann in eine neue, vom Portal signierte SAML1 Assertion mit aufgenommen. Im nächsten Schritt wird diese Assertion in das vom kurzlebigen Zertifikat abgeleitete Proxy Zertifikat eingebettet und steht damit an der Grid-Ressource zur Auswertung bereit [13]. Da die an der Grid-Ressource benutzte Software nur SAML1 Format verarbeiten kann, erfolgt die Neuausstellung der Assertion im SAML1 Format.

Das Portal tritt durch die Sammlung und Zusammenstellung der Attribute nun als Attribute Authority in Erscheinung. Dies hat auch Konsequenzen hinsichtlich der Änderung der Vertrauensbeziehung: die Ressourcen Provider müssen nun auch dem Portal als dem Aussteller der neuen Assertion vertrauen. Die ausgestellte SAML Assertion wird daher mit einem eigenen Zertifikat durch das Portal unterschrieben.

5 Auswertung an der Grid Ressource

An der Grid-Ressource muss zwischen der Auswertung des kurzlebigen Zertifikats und der darin eingebetteten SAML Assertion unterschieden werden.

Zur Auswertung des kurzlebigen Zertifikats werden die gleichen Mechanismen genutzt wie bei auch bei langlebigen persönlichen Grid Zertifikaten. Dazu werden regelmäßig aktuelle Nutzerlisten über ein gridmap-File mit dem VOMS Server abgeglichen.

Da es sich bei den kurzlebigen Zertifikaten um EuGridPMA akkreditierte Zertifikate handelt, hat deren Verwendung gegenüber den konventionellen persönlichen Grid Zertifikaten keine weiteren Konsequenzen.

Anders ist die Lage bei der Auswertung der Nutzer-Attribute aus der SAML Assertion, die optional für eine weitergehende Autorisierung sowohl für die gesamte Ressource als auch für nur einzelne Dienste genutzt werden können. Dazu muss bei den Ressourcenprovidern zusätzlich *Gridshib for Globus Toolkit (GT)* installiert werden. Verwendet wurde hier die Version *Gridshib for Globus Toolkit 0.6.0*, die mit *Globus Toolkit 4.0.8* [14] zusammen arbeitet. Obwohl bereits neuere Versionen von Globus existieren, ist die Verwendung von GT 4.0.8 gerechtfertigt, da einige Communities in D-Grid wegen der fehlenden Webservices in GT5 immer noch auf GT 4.0.x aufbauen. *Gridshib for Globus Toolkit 0.6.*0 erlaubt allerdings nur die Auswertung genau einer SAML1 Assertion pro Proxy-Zertifikat. Wie bereits in Kapitel 3 beschrieben, werden daher die Attribute aus den unterschiedlichen Quell-Assertions im Portal in einer einzigen Assertion gesammelt und im SAML1 Format bereitgestellt.

Im hier vorliegenden Anwendungsfall werden zwei unterschiedliche Zertifikatketten benutzt: Das kurzlebige Zertifikat des Nutzers geht auf den DFN-SLCS zurück, während das Serverzertifikat des Portals, mit dem die eingebettete SAML Assertion unterschrieben wird, auf einem Zertifikat des Portals basiert. Dieser Fall unterschiedlicher Zertifikatketten war in der originalen Implementierung der *Gridshib SAML Tools* [15] nicht enthalten. Daher wurden entsprechende Anpassungen vorgenommen. Die modifizierte Bibliothek steht zur Nachnutzung bereit und akzeptiert nun auch Assertions mit einer anderen Zertifikatskette als der des umgebenden Zertifikates. Die unterschiedlichen Attribute können für Autorisierungsentscheidungen genutzt werden, in dem sie an entsprechend konfigurierten Policy Decision Points (PDP) ausgewertet werden.

Die Auswertung der SAML Assertion ist optional. Werden die erwähnten Erweiterungen nicht installiert, so wird die eingebettete Assertion ignoriert. Damit kann jeder Ressourcenbetreiber aufgrund seiner lokalen Policy entscheiden, ob er die zusätzlichen Autorisierungsinformationen nutzt.

6 Fazit

Das Konzept zur Nutzung von kurzlebigen Zertifikaten über Portal Delegation bietet eine Möglichkeit für den Einstieg auch wenig technikaffiner Nutzergruppen in das Grid. Für den Anwender sinkt damit der Aufwand für die Beantragung und die Handhabung von Zertifikaten. Erkauft wird dieser Vorteil für den Nutzer durch einen erhöhten Aufwand bei den jeweiligen Heimateinrichtungen, die einen IdP betreiben und die Voraussetzungen für den Beitritt in die Shibboleth-Föderation (DFN-AAI) sowie den Betrieb des SLCS-RA erfüllen müssen. Durch den hier implementierten Lösungsansatz werden die Probleme also von den vielen potentiellen Nutzern hin zu den Rechenzentren verlagert, wo sie wegen der dort vorhandenen Expertise aber leichter und effektiver gelöst werden können.

Die entwickelte Software steht zur Nachnutzung bereit und kann unter der Webseite http://gap-slc.awi.de/dokumente.html heruntergeladen werden.

Verweise

[1] Gridshib: http://gridshib.globus.org/docs/gridshib-gt-0.6.1/readme.html

[2] Vaadin: http://vaadin.com

[3] Shibboleth: http://shibboleth.internet2.edu

[4] DFN-AAI: https://www.aai.dfn.de/

[5] SWITCHaai: http://www.switch.ch/de/aai/index.html

[6] Yung-Kao Hsu, S. P. Seymour, "An Intranet Security Framework Based on Short-Lived Certificates," IEEE Internet Computing, vol. 2, no. 2, pp. 73-79, Mar./Apr. 1998, doi:10.1109/4236.670687

[7] C.Witzig, "Shibboleth Interoperability Through a Short-Lived Credential Service (SLCS)", No EGEE-II-MJRA1.4-770102, SWITCH, Nov 2006. http://www.switch.ch/export/sites/default/uni/projects/grid/download_repository/EGEE-II-MJRA1.4-770102-v0.96.pdf.

[8] DFN-SLCS: https://www.pki.dfn.de/grid/slcs

[9] Certificate Policy and Certification, Practice Statement of the Public Key Infrastructure in the Deutsche Forschungsnetz: https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_SLCS-CPCPS_v11.pdf

[10] VOMS: http://www.globus.org/grid_software/security/voms.php

[11] SAML: http://www.oasis-open.org/committees/security

[12] Portal Delegation: http://gridshib.globus.org/docs/gridshib-ca-0.5.1/portal-delegation.html

[13] S. Pinkernell, B. Fritzsch: Einsatz von Portal Delegation und SAML Assertions bei der Authentifizierung und Autorisierung, 28.02.2011: http://gap-slc.awi.de/documents/shibAutoLogin-1.0.pdf

[14] Globus: http://globus.org/toolkit

[15] Gridshib SAML Tools: http://gridshib.globus.org/docs/gridshib-saml-tools-0.5.0/readme.html