Gap-SLC

Nutzung von kurzlebigen Zertifikaten in portalbasierten Grids

Prototypische Umsetzung des Konzepts für die Nutzung von Robot-Zertifikaten

– Task 5, Deliverable D5-2 –

– Förderkennzeichen 01IG09003B –

„Service Grids für Forschung und Entwicklung“
des Bundesministeriums für Bildung und Entwicklung (BMBF)

Fraunhofer IAO

AWI

UNIVERSITÄTSMEDIZIN GÖTTINGEN UMG

DAASI International

Date	**28.02.2011**
Version	**1.0**
Type	**Draft**
Status	**Final**
Authors	**J. Falkner, O. Strauß, A. Weisbecker, S. E. Funk, P. Gietz, M. Haase**

Inhaltsverzeichnis

1 Einleitung

Mit der Anpassung der DFN Grid Zertifizierungsrichtlinien und der damit einhergehenden Erweiterung hinsichtlich der Nutzung von Robot-Zertifikaten wurde im Juni 2010 die Basis für eine Nutzung von Dienstezertifikaten im D-Grid gelegt. Die sogenannten Robot-Zertifikate werden dabei nicht für eine Person oder einen Rechner im Grid ausgestellt, sondern für eine bestimmte Anwendung. Ähnlich wie bei Server-Zertifikaten ist auch hier eine Person oder eine Personengruppe für das Schlüsselpaar, das Zertifikat und deren Verwendung verantwortlich und haftbar.

Hiermit wird erstmals ermöglicht, dass Endanwender Grid-Anwendungen nutzen, die auf Rechnern ausgeführt werden, die eine Authentifizierung mittels PKI erfordern, ohne dass der Endanwender hierfür selbst ein Zertifikat benötigt. Damit wird dem Endanwender der Aufwand für die Erlangung, Verwaltung und Nutzung von PKI vollständig abgenommen und die Eintrittsschwelle für die PKI-basierte Grid-Nutzung massiv gesenkt.

Gleichzeitig erhöht sich der Aufwand (moderat) für die Betreiber von solchen Grid-Anwendungen, die für Endanwender ohne eigenes PKI-Zertifikat zur Verfügung stehen sollen und es ergeben sich rechtliche und organisatorische Implikationen für die Betreiber von Infrastrukturkomponenten und von Grid-Anwendungen.

Insbesondere die Erlangung und Verwaltung von Robot-Zertifikaten sowie der Zugriff auf die für die Ausführung im Grid erforderlichen Proxies durch die Robot-Anwendungen soll im Folgenden im Detail beschrieben werden. Hierbei wird insbesondere auch auf den speziellen Fall eingegangen, dass mehrere Robot-Anwendungen den Endanwendern über ein Grid-Portal zur Verfügung gestellt werden sollen. Im Grid-Portal gibt es somit für jeden Robot-Grid-Service ein eigenes Portlet, das aus einem MyProxy Robot Credential Store (MPRCS) über die bekannten Mechanismen eines MyProxy Credential Services ein Job-Credential beziehen kann, das den Job bei den Grid-Ressourcen, auf denen die eigentlichen Grid-Anwendungen installiert sind, als Robot-Service identifiziert und authentisiert.

Wie bereits in Deliverable D5-1 [1] ausführlich konzipiert, soll für die Ausführung von Robot-Diensten ausschließlich ein von den normalen D-Grid-Ressourcen getrennter Ressourcenpool verwendet werden, der explizit für die Verwendung von Robot-Diensten vorgesehen und gekennzeichnet ist. Es ist hierbei zusätzlich wünschenswert, dass die Betreiber von Grid-Ressourcen, auf denen Robot-Jobs akzeptiert werden, ihre Autorisierungssysteme so konfigurieren, dass bestimmte Robot-User ausschließlich Zugriff auf diejenigen auf der Grid-Ressource installierten Anwendungen erhalten, die für die Ausführung des Robot-Services erforderlich sind.

Um eine prototypische Umsetzung der Nutzung von Robot-Zertifikaten erreichen zu können sind folgende Punkte zu berücksichtigen:

- Rechtliche Grundlagen für die Verwendung von Robot-Zertifikaten
- Ausstellung von Robot-Zertifikaten
- Aufbewahrung von Robot-Zertifikaten
- Nutzung von Robot-Zertifikaten
- Akzeptanz von Robot-Zertifikaten und Robot-Jobs auf D-Grid Ressourcen

In den folgenden Kapiteln werden die einzelnen Punkte ausführlicher beschrieben.

2 Rechtliche Grundlagen

Die rechtlichen Grundlagen der Nutzung von Robot-Zertifikaten in D-Grid sind durch die entsprechenden Regularien der EUGridPMA hinsichtlich der Verwendung von Robot-Zertifikaten [2][3] sowie in der DFN Grid PKI Robot-Policy [4][5] dargelegt und im Detail beschrieben. Die Implikationen hinisichtlich der Ausstellung, Aufbewahrung und Nutzung von Robot-Zertifikaten werden in den folgenden Kapiteln beschrieben.

3 Ausstellung von Robot-Zertifikaten

Die Ausstellung von Robot-Zertifikaten erfolgt durch die DFN PKI ([6]), erreichbar über das Webfrontend unter https://pki.pca.dfn.de/grid-root-ca/cgi-bin/pub/pki

Hierbei ist wie z.B. auch bei Server-Zertifikaten oder Codesigning-Zertifikaten ein PKCS#10-Zertifikatantrag (PEM-formatierte Datei) hochzuladen. Dieser Zertifikatantrag (oder auch Certificate Signing Request, d.h. eine „.csr“-Datei) ist vom Antragsteller auf einem in geeigneter Weise gesicherten System (siehe dazu auch Kapitel 4) selbst zu erzeugen. Das Verfahren zur Erzeugung eines PKCS#10 Zertifikatsrequests ist ebenfalls auf den Webseiten der DFN PKI nachzulesen [7].

Für Robot Zertifikate sind dabei einige Besonderheiten zu beachten:

- **Begriffserklärung Zertifikatnehmer:**

  Zertifikatnehmer eines Robot Zertifikats ist entweder

  - eine Einzelperson, die für alle Aktivitäten des automatisierten Client (Robot) verantwortlich ist, oder
  - eine dauerhaft etablierte Gruppe von Administratoren, die für alle Aktivitäten des automatisierten Client (Robot) verantwortlich ist.

- **Schlüsselerzeugung, -speicherung und -transport (DFN-PKI Grid CPS [5] 6.1.1, CP [4] 4.5.1):**

  Private Schlüssel für Robot Zertifikate müssen entweder in einem Hardware-Krypto-Gerät (z.B. Smartcard) erzeugt und gespeichert werden oder auf einem entsprechend gesichertem System, zu dem nur der verantwortliche Zertifikatnehmer (s. Begrifferklärung Zertifikatnehmer) Zugang hat. Private Schlüssel von Robot Zertifikaten sollten weder während einer längeren Inaktivität unverschlüsselt abgelegt, noch unverschlüsselt im Netz übertragen werden. Private Schlüssel und Passwörter von Robot Zertifikaten dürfen grundsätzlich nie im Klartext über irgend eine Art von Netzwerk übertragen werden.

- **Zertifikatname (DFN-PKI Grid CPS [5] 3.1.2c):**

  Das CN-Attribut im Zertifikatnamen von Robot Zertifikaten muss mit dem Schlüsselwort "Robot" direkt gefolgt von einem Doppelpunkt oder Minuszeichen und einem Leerzeichen beginnen. Darauf folgen eine verständliche, bedeutungsvolle Beschreibung des automatisierten Clients, der Name des Zertifikatnehmers (s. Begrifferklärung Zertifikatnehmer) und deren (Gruppen-)E-Mail-Adresse. Die im Robot Zertifikat enthaltenen E-Mail-Adressen müssen dem Zertifikatnehmer gehören. Die Gesamtlänge des CN darf 64 Zeichen nicht überschreiten. Beispiele für das CN-Attribut:

  - **Zertifikatnehmer ist eine Einzelperson:**

    CN=*Robot- Job Upload Robot - Martin Mustermann*

  - **Zertifikatnehmer ist eine Gruppe:**

    CN=*Robot: Sample Grid Portal - HRZ Portal Ops - portal-ops@dfn.de*
    oder
    CN=*Robot: Job Performance Mon - Monitoring Group - grid-ops@dfn.de*
    oder
    CN=*Robot- Job Performance Mon - Monitoring Group - grid-ops@dfn.de*

  Hierbei ist zu beachten, dass zwischen *Robot* und dem folgenden ":" bzw "-" kein Leerzeichen stehen darf.

- **Alternativer Zertifikatname (DFN-PKI Grid CPS 7.1.2):**

  Robot Zertifikate müssen immer mindestens einen alternativen Zertifikatnamen (SubjectAlternativeName, SaN) vom Typ "email" beinhalten, in dem eine E-Mail-Adresse des Zertifikatnehmers aufgeführt wird. Wenn das CN-Attribut bereits eine E-Mail-Adresse enthält, sollte genau diese als E-Mail-Adresse im SaN übernommen werden.
  In der DFN-PKI kann der SaN vom Typ "email" erzeugt werden, indem im PKCS#10-Zertifikatrequest (CSR) beim Zertifikatnamen (subjectDN) das Attribut "emailAddress" entsprechend angegeben wird.

- **Zertifikatnutzung (DFN-PKI Grid CP 4.5.1) und Betrieb der automatisierten Komponente (DFN-PKI Grid CPS 7.1.2):**

  Auf E-Mails an die im Robot Zertifikat enthaltenen E-Mail-Adressen muss innerhalb eines Werktages reagiert werden. Computersysteme, auf denen private Schlüssel von Robot Zertifikaten gespeichert sind, müssen entsprechend gesichert sein und aktiv im Hinblick auf sicherheitsrelevante Vorkommnisse überwacht werden. Diese Computersysteme müssen in einem gesicherten Raum mit Zugangskontrolle untergebracht sein. Zugang darf nur autorisiertem Personal gewährt werden.

4 Aufbewahrung von Robot-Zertifikaten

Die Aufbewahrung von Robot-Zertifikaten bzw. den entsprechenden Schlüsselpaaren obliegt gemäß der Policy des DFN [4][5] den jeweils für die Robot-Services verantwortlichen Personen. Dies kann eine natürliche Person sein, die für einen bestimmten Robot-Service verantwortlich ist bzw. ein entsprechender Personenkreis. Bei der Bereitstellung mehrerer Robot-Services von unterschiedlichen Anbietern über ein einziges Grid-Portal kommt noch die Besonderheit hinzu, dass die Schlüsselpaare für mehrere Robot-Dienste in einem gemeinsamen MyProxy Robot Credential Store (MPRCS) aufbewahrt werden können und sich der Kreis der verantwortlichen Personen dann um den oder die Administratoren des MPRCS erweitern kann.

Hieraus ergeben sich zwei grundsätzlich unterschiedliche Methoden, die Aufbewahrung von Robot-Zertifikaten umzusetzen. Diese werden in den nächsten beiden Abschnitten erläutert.

4.1 Aufbewahrung von einzelnen Robot-Zertifikaten

Wenn im Grid jeder Robot-Service über einen eigenen Client oder ein eigenes Portal zur Verfügung gestellt wird, nur ein einziger Robot-Service angeboten werden soll oder der Zugriff auf alle Grid-Services über einen einzigen Autorisierungsdienst gesteuert wird, der seinerseits als Robot-Service implementiert ist so ist die oben angedeutete Einrichtung eines MyProxy Robot Credential Stores nicht erforderlich. Beispielhaft werden die Aufgaben der Aufbewahrung für diesen einfacheren Fall anhand der Umsetzung in der TextGrid-Middleware dargestellt. Dort werden alle Zugriffe auf den Grid-Storage durch den Web Service basierten Dienst TG-crud (der TextGrid-Service für Create-, Retrieve-, Update- und Delete-Operationen) durchgeführt.

Das TextGrid-Robot-Zertifikat für TG-crud und sein privater Schlüssel werden auf einem virtuellen Rechner gespeichert. Zum Aufstellungsort des zugehörigen Wirts haben nur berechtigte Administratoren Zugang. Ein Login zu Gast- und Wirtsrechner besitzen nur TextGrid-Administratoren über je einen individuellen Nutzer-Account. Der root-Zugriff ist nur per „sudo“ möglich, das direkte Login mit dem root-Account selbst ist abgeschaltet. Eine Firewall für Wirts- und Gastrechner ist konfiguriert, die nur die absolut nötigen Ports freigibt, nach Möglichkeit beschränkt für ein bestimmtes Teilnetz.

Intrusion Detection stellt sicher, dass unautorisierte Zugriffe zeitnah bemerkt werden können und schützt vor Brute-Force-Attacken auf Nutzernamen/Passwörter.

Der Schlüssel zum Robot-Zertifikat wird im lokalen Dateisystem des Rechners gespeichert und ist mit einem Passwort gesichert. Das Passwort ist zu keiner Zeit und in keiner Form im Dateisystem des Rechners gespeichert.

Die alternativ mögliche Nutzung eines Krypto-Tokens für die Speicherung des privaten Schlüssels wird gegenwärtig ebvaluiert.

Nur eine kleine Gruppe von Personen hat Zugriff auf den virtuellen bzw. physikalischen Wirt des Robot-Schlüsselpaares. Diese Personen sind zu einer Gruppe zusammengefasst, deren E-Mail-Adresse sich im Distinguished Name des Robot-Zertifikats wiederfindet.

4.2 Aufbewahrung von Robot-Zertifikaten im Fall der portalbasierten Nutzung mehrerer Robot-Services

Für die Aufbewahrung von Robot-Zertifikaten im Fall der portalbasierten Nutzung mehrerer Robot-Services werden im Folgenden die Betriebsanforderungen für einen MyProxy Robot Credential Store (MPRCS) beschrieben, der erforderlich ist um für mehrere Robot-Services gleichzeitig die erforderlichen Robot-Credentials bereitstellen zu können und gleichzeitig die rechtlichen Rahmenbedingungen zu erfüllen, die gemäß der DFN-Policy für die Aufbewahrung von Robot-Schlüsselpaaren gelten.

4.2.1 Was ist unter einem MPRCS zu verstehen?

Der MyProxy Robot Credential Store (MPRCS) ist ein dedizierter Server, der ausschließlich für die Erzeugung und Speicherung von Robot Zertifikaten durch berechtigte Personen sowie für die Bereitstellung eines MyProxy Credential Services dient, über den Service-Client-Portlets zu Grid-Anwendungen Robot-Credentials beziehen können. Diese Robot-Credentials werden dann mit den Grid-Jobs zur Authentifizierung im Grid weitergegeben, wie dies auch mit herkömmlichen Grid-Nutzer-Credentials der Fall wäre.

Dieser Server dient ausschließlich dem oben beschriebenen Zweck. Insofern sind alle Anwendungen, die nicht diesem Zweck dienen, zu deinstallieren. Der Server ist sowohl physikalisch als auch hinsichtlich der Software angemessen zu schützen. Eine physikalische Zugangsbeschränkung zum Serverraum und ein aktueller Patch-Stand für das Betriebssystem und die eingesetzten Anwendungen werden somit ebenso vorausgesetzt wie die Beschränkung der offenen Firewall-Ports auf ein absolutes Minimum.

4.2.2 Wer darf den MPRCS administrieren?

Es soll nur ein kleiner Kreis von Administratoren Zugang zum MPRCS haben. Ihre Aufgabe ist die Erzeugung von Robot-Schlüsseln und Zertifizierungsrequests sowie die Beantragung von Robot-Zertifikaten für alle Robot-Services ihrer Community. Der Kreis dieser Administratoren soll möglichst klein gehalten werden, die Sicherstellung der oben genannten Anforderungen und Aufgaben aber trotzdem gewährleisten.

4.2.3 Welche Rechte hat der Administrator und wer hat sonst noch Rechte auf dem System?

Die Administratoren haben Vollzugriff auf den MPRCS.

Ansonsten hat niemand direkten Zugriff. Es wird nur eine API zum Bezug von Robot-Credentials zur Verfügung gestellt (siehe Abschnitt 4.2.4).

4.2.4 Welche APIs werden für die sonstigen Nutzer zur Verfügung gestellt und wie müssen die sich authentifizieren und autorisieren?

Außer den Administratoren haben ausschließlich die Client-Portlets zu den Robot-Services einen Zugriff auf das System. Dieser beschränkt sich darauf, über den MyProxy Credential Service auf dem MPRCS Robot-Credentials nach vorheriger Authentifizierung zu beziehen.

Die Entwickler und Bereitsteller von Robot-Services haben dafür Sorge zu tragen, dass der Bezug von Credentials ausschließlich im Rahmen der von ihnen beabsichtigten Nutzungsmöglichkeiten der Robot-Services durch den Endnutzer erfolgt und keine direkten Zugriffsmöglichkeiten an den Endnutzer weitergegeben werden.

4.2.5 Welche Netzwerkverbindungen sind erlaubt, welche Ports dürfen geöffnet sein und für wen?

Der MPRCS ist über eine Internetverbindung mit dem Portal-Server verbunden, der die Robot-Service-Client-Portlets beherbergt. Diese Internetverbindung beschränkt sich auf den Port 7512, der für das Credential-Retrieval erforderlich ist und auf die IP-Adresse des Portal-Servers. Ansonsten ist eine Fernwartungsmöglichkeit für die Administratoren des MPRCS über Port 22 (SSH) erlaubt, die ebenfalls auf die IP-Adressen der Client-Rechner der Administratoren beschränkt sein sollte.

4.2.6 Welche Betriebssysteme sind erlaubt?

Keine Einschränkungen, außer dass der Betrieb eines MyProxy Servers vom Betriebssystem unterstützt werden muss.

4.2.7 Welche Best Practices zum Security Patch Management sind minimal erforderlich?

1. Der MPRCS ist sowohl bezüglich seines Betriebssystems als auch bezüglich seiner installierten Anwendungen und Services ständig auf einem aktuellen Security-Patch-Level zu halten.

2. Die Dienste des DFN-CERT zu Benachrichtigungen über Sicherheitslücken sind zu nutzen und deren Empfehlungen umzusetzen.

3. Sicherheitsrelevante Log-Files sind in regelmäßigen Abständen von max. 1 Werktag auszuwerten und ggf. geeignete Maßnahmen zu ergreifen. Zu den sicherheitsrelevanten Log-Daten zählen z.B.:

a. die Liste der ausgegeben Proxy-Zertifikate, d.h. sDN, iDN des zugehörigen Robot-Zertifikats

b. Gültigkeit, Seriennummer und Name/ID des anfordernden Portlets

c. die Zuordnung von am Portal angemeldeten Nutzern (Nutzer-Kennungen) und den jeweils für diese angeforderten Proxy-Zertifikate der Robot-Zertifikate

Dieser Prozess kann z.B. durch Intrusion Detection Systeme unterstützt werden.

4.2.8 Zusammenspiel von Grid-Portal, MPRCS und MPCS

Grundsätzlich sind zwei Arten der Nutzung von Grid-Services möglich, die auch in Abbildung 1 wiedergegeben werden. Zum einen können zur Trust Delegation im Grid Credentials verwendet werden, die vom eigenen Nutzerzertifikat abgeleitet sind und zum anderen können Robot-Credentials zu Einsatz kommen. Der erstere Fall ist in Abbildung 1 durch den Certified Grid User dargestellt, der letztere Fall durch den Guest User.

Auf administrativer Seite sind der Administrator des MPRCS (MPRCS Admin) sowie der Administrator der eigentlichen Robot-Services und des zugehörigen Client Portlets (Robot Service Admin) zu unterscheiden.

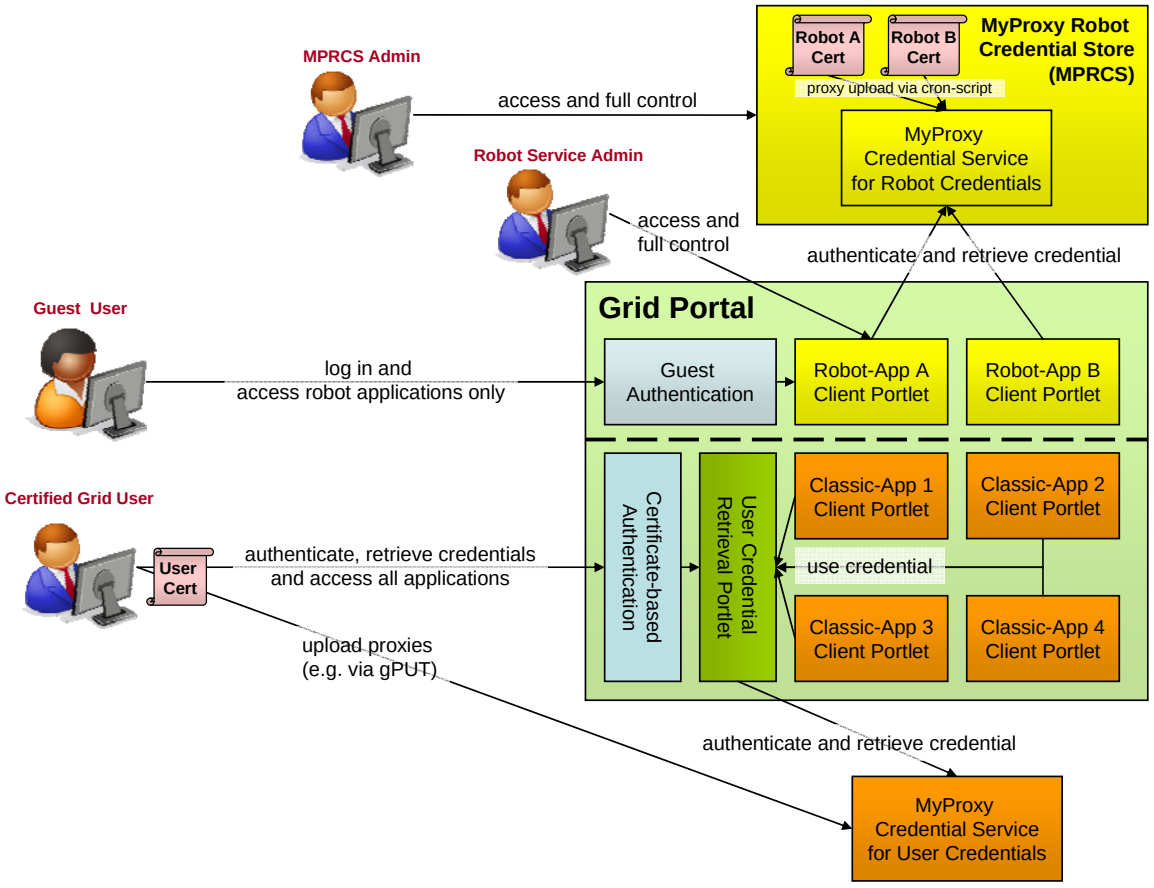

Abbildung 1: MyProxy Robot Credential Store für die portal-basierte Nutzung von Robot-Services

Systemseitig gibt es drei Systeme:

1 das Grid Portal selbst, das die Endnutzer Authentifizierung übernimmt, ggf. beim Upload von persönlichen User-Credentials ins Grid behilflich ist und vor allem die Client Portlets zu allen über das Portal verfügbaren Grid-Services beinhaltet. Hierzu zählen sowohl Client Portlets zu Robot-Services als auch zu klassischen Grid-Services.

2 der MyProxy Credential Service für die Verwendung von normalen User-Credentials

3 der MyProxy Credential Service für die Verwendung von Robot-Credentials

Abbildung 1 beschreibt die Abläufe sowohl der Nutzung von Robot-Credentials als auch der Nutzung von User-Credentials. In ersterem Falle meldet sich der Endnutzer als Gast am Portal an und erhält Zugriff auf verschiedene Robot-Service Client Portlets, über die er Robot-Services im Grid ausführen kann. Bei der Ausführung werden für den Nutzer transparent vom jeweiligen Portlet Robot-Credentials aus dem MPRCS über die vorgesehene API angefordert. Im MPRCS sind die Original-Schlüsselpaare zu den Robot-Services gespeichert, aus denen die Robot-Credentials abgeleitet werden und dem Robot-Client-Portlet zur Verfügung gestellt werden. Der Zugriff auf die Original-Schlüsselpaare ist ausschließlich den Administratoren des MPRCS vorbehalten, obwohl auch die Robot-Service-Admins für deren Verwendung mit verantwortlich sind. Dies sichert einerseits die entsprechend den Policies zur Verwendung von Robotzertifikaten geforderte weitestgehende Beschränkung des Zugriffs, trägt aber andererseits auch der Tatsache Rechnung, dass die Implementierungen der Robot-Service Clients, aber auch der Robot-Services selbst, ein nicht völlig zu eliminierendes Risiko in sich tragen, so dass auch deren Verantwortliche (Robot-Service-Admins) die Haftung mittragen.

Im herkömmlichen Fall der Nutzung von User-Credentials kommen ebenfalls Implementierungen von Grid-Services und Grid-Service-Clients zum Einsatz, auf die der Nutzer keinen Einfluss hat. Wenn sich der Nutzer beispielsweise am MediGRID Portal einträgt und einen Dienst zur Bildverarbeitung nutzt übergibt er diesem seine Credentials zur Ausführung einer Bildverarbeitung. Wenn der Service nun aber Schwachstellen aufweist und nicht das tut was er soll läuft rechtlich trotzdem alles im Namen des Endnutzers und er trägt zunächst auch die Verantwortung für die Handlungen des Services selbst, da er aufgrund der Zustimmungen zu den Nutzungsbedingungen des Grids rechtlich die alleinige Verantwortung für die Verwendung seiner Credentials übernimmt – auch wenn er eigentlich nicht für das haften kann was der Service für ihn tut.

5 Erlangung von Robot-Zertifikaten

Nachdem in den vorangegangenen Abschnitten geklärt wurde, welche Bedingungen an Robot-Zertifikate zu stellen sind und wie diese aufzubewahren sind, wird im folgenden beschrieben, wie man Robot-Zertifikate in der Praxis erlangen kann.

5.1 Variante 1: einzelner Robot-Service

5.1.1 Robot-Schlüssel-Generierung

1. Es wird jeweils eine für einen Robot-Anwendungsdienst spezifische Mailingliste eingerichtet <anwendung>@<institution>, z.B. tgcrud@daasi.de (im Folgenden „Anwendungs-Listen-Adresse“ genannt).
2. Auf dieser Mailingliste sind der oder die verantwortliche(n) Entwickler bzw. Administrator (Im Folgenden „Entwickler“ genannt) einzutragen.
3. Einer dieser Entwickler erzeugt auf einem nur für ihn zugänglichen Rechner einen Private Key und einen zugehörigen Certificate Signing Request (CSR) für einen Robot-Anwendungsdienst.
4. Dieser CSR enthält als Common Name (CN) "Robot: <Community> - <Robot-Anwendungsdienstname> - <Anwendungs-Listen-Adresse>"
5. Als SubjectAlternativeName hat der CSR einen Eintrag email:<Anwendungs-Listen-Adresse>
6. Der Entwickler stellt von seinem Rechner aus über das DFN-Portal den Zertifizierungsantrag.
7. Die DFN-Grid-PKI schickt das Zertifikat an den ausführenden Entwickler.
8. Auf das Robot-Zertifikat und den zugehörigen Private Key erhalten ausschließlich die Entwickler Zugriff.

5.1.2 Erzeugung und Nutzung eines Robot-Proxies

Ein Daemon erzeugt alle 24 Stunden ein Proxy-Zertifikat mit einer Lebensdauer von 25 Stunden. Das Passwort des privaten Schlüssels wird dann nur beim Start des Daemons manuell von einem Entwickler eingegeben und wird ausschließlich im Hauptspeicher des Rechners gespeichert. Die Begrenzung auf diese Lebensdauer ist nur dann möglich, wenn nur entsprechend kurz laufende Jobs bzw. nur Dateizugriffe auf der Grid-Ressource ausgeführt werden sollen, wie es gegenwärtig bei TextGrid der Fall ist.

In Textgrid verwendet TG-crud dieses Proxy-Zertifikat, um über JavaGAT auf den Grid-Speicher des TextGrid Repository zuzugreifen, wobei die dafür vorgesehenen Bibliotheken des Globus Toolkit verwendet werden. Es werden niemals private Schlüssel über das Netz geschickt, sondern – falls Delegation benötigt wird – die Standard Challenge-Response-Prozedur genutzt, die auch in SSL verwendet wird.

5.2 Variante 2: Portal-basierte Nutzung mehrerer Robot-Services

5.2.1 Robot-Schlüssel-Generierung (à la MediGRID)

1. Es wird jeweils eine für einen Robot-Anwendungsdienst spezifische Mailingliste eingerichtet <anwendung>-robot@<Community.de>.

1. Auf dieser Mailingliste sind der oder die verantwortliche(n) Entwickler sowie die MPRCS-Administratoren einzutragen.

2. Die MPRCS-Admins erzeugen auf dem MPRCS-Rechner einen Robot Private Key und einen zugehörigen Certificate Signing Request (CSR) für einen Robot-Anwendungsdienst.

3. Dieser CSR enthält als Common Name (CN) "Robot: <Robot-Anwendungsdienst>@<Community>.de"

4. Dieser CSR wird vom ausführenden Administrator per SSH auf seinen eigenen Rechner übertragen.

5. Der MPRCS-Administrator stellt von seinem eigenen Rechner aus über das DFN-Portal den Zertifizierungsantrag.

6. Die DFN-Grid-PKI schickt das Zertifikat an den ausführenden MPRCS-Admin.

7. Dieser überträgt das Zertifikat auf den MPRCS.

8. Auf das Robot-Zertifikat und den zugehörigen Private Key erhalten ausschließlich die MPRCS-Admins Zugriff.

5.2.2 Erzeugung von Robot-Proxies am MPRCS und Upload in den MyProxy Credential Service

Damit die Robot-Zertifikate auch tatsächlich von den Robot-Anwendungen genutzt werden können, müssen im MyProxy Credential Service des MPRCS Proxies diese Robot-Zertifikate zur Verfügung gestellt werden. Da der Zugriff auf die Schlüsselpaare auf die Administratoren des MPRCS begrenzt ist und eine dauerhafte Verfügbarkeit der Robot-Anwendungen gewährleistet werden soll, werden die Robot-Zertifikate vom Administrator direkt in den MyProxy Credential Service hochgeladen. Auf diese Weise können die Robot-Portlets während der gesamten Laufzeit der Robot-Zertifikate von diesen Credentials ableiten.

Für jedes Robot-Credential wird eine eindeutige Kombination aus Username und Passwort vergeben, über die mittels der üblichen MyProxy-Methoden Credentials von den Proxies bezogen werden können. Diese Username/Passwort-Kombinationen werden ausschließlich den jeweiligen Betreibern der Robot-Services zur Verfügung gestellt. Je nach Implementierung der Credential Retrieval Funktionen der Robot-Service-Client-Portlets können unterschiedliche Credential Lebenszeiten realisiert werden.

6 Nutzung von Robot-Zertifikaten in der Praxis

6.1 Über Web Service

Im Beispiel von TextGrid, bei dem nur ein Robot-Zertifikat zum Einsatz kommt, wird das Robot-Zertifikat für den Web-Service TG-crud verwendet. Dieser Dienst ermöglicht TextGrid-Nutzern ohne persönliche Zertifikate die Durchführung von Dateioperationen im Grid. Anonyme Nutzer dürfen hierbei nur Leseoperationen auf veröffentlichten Dateiressourcen durchführen. Schwach authentifizierten Nutzern (E-Mail-Verifikation mit Login über TG-auth*, die Authentifizierungs-und Autorisierungskomponente von TextGrid) stehen sämtliche CRUD-Operationen auf den ihnen per Robot-Zertifikat zugänglichen Ressourcen offen. Für stärker authentifizierte Benutzer (Zertifikat oder Shibboleth) kann statt des Robot-Zertifikats ein persönliches Zertifikat (User-Zertifikat oder Short Lived Credential) verwendet werden, um den Zugang zu Ressourcen mit höherer Sicherheitsstufe zu ermöglichen.

6.2 Portalbasierte Nutzung von Robot-Zertifikaten

Für den Fall der Bereitstellung mehrerer Robot-Dienste über ein Grid-Portal wird im Folgenden die Erzeugung von Robot-Proxies am MPRCS, der Upload in den MyProxy Credential Service und das Retrieval von Credentials durch den Robot-Service bzw. durch das zugehörige Robot-Service-Client Portlet beschrieben.

Bei der Nutzung eines Robot-Service-Client Portlets am Portal wird vor der Job-Submission an den eigentlichen Robot-Service (auf verteilten Ressourcen im Grid) ein Robot-Credential bezogen. Das jeweilige Robot-Service-Client Portlet implementiert zu diesem Zweck eine Methode, mit der ein Robot-Credential vom MyProxy Credential Service des MPRCS geladen wird. Die Authentisierung erfolgt über die für den jeweiligen Robot-Service spezifische Kombination aus Username und Passwort (siehe Abschnitt 5.2.2).

Der Entwickler des Robot-Service-Client Portlets hat dafür Sorge zu tragen, dass diese Methode angemessen gesichert und getestet ist.

Der Endnutzer der Robot-Anwendung loggt sich mit seinem Gastnutzer-Zugang am Portal an und erhält ausschließlich Zugriff auf Robot-Anwendungen, die für die Nutzung durch schwach authentifizierte Nutzer vorgesehen sind.

Der Anbieter der Robot-Anwendung und des Robot-Service-Client Portlets trägt die volle juristische Verantwortung für alle Aktionen, die mithilfe seines Robot-Credentials auf Ressourcen im Grid ausgeführt werden. Dementsprechend obliegt ihm eine Sorgfaltspflicht hinsichtlich der Programmierung seiner Robot-Anwendung und seines Robot-Service-Client Portlets.

7 Akzeptanz von Robot-Zertifikaten und Robot-Jobs auf D-Grid Ressourcen

Um Befürchtungen entgegenzutreten, dass mit der Nutzung von Robot-Zertifikaten im Grid Schwachstellen in der Authentifizierung und Autorisierung erzeugt werden, von denen alle Ressourcen und somit auch alle anderen Services sowie die voll zertifizierten Nutzer betroffen wären, wird empfohlen, einen gesonderten Ressourcenpool in D-Grid zu betreiben, der explizit für die Nutzung von Robot-Services vorgesehen ist. Dieser Ressourcenpool kann für alle Arten von D-Grid Zertifikaten bzw. deren Nutzer zugänglich sein.

Ressourcen, die diesem Pool angehören sollen, werden durch ein zusätzliches Attribut, welches beispielsweise über den Grid Resource Registration Service (GRRS) verwaltet werden könnte, als solche gekennzeichnet (Abbildung 2, Schritt 0). Als Vorschlag für den Attributnamen wird **respool** vorgeschlagen. Das Attribut *respool* könnte beispielsweise die Werte **robot** oder **standard** einnehmen. Mit dem Attribut *standard* könnten alle anderen Ressourcen gekennzeichnet werden, die nicht für die Nutzung durch Robot-Services vorgesehen sind. Durch das Hinzufügen weiterer Attributwerte besteht zukünftig die Option, weitere Ressourcenpools zu unterscheiden, beispielsweise entlang der für diese Ressourcen vorgesehenen Sicherheitsanforderungen.

Die Kennzeichnung von Ressourcen als Robot-Ressourcen hat den Vorteil, dass Workload-Management-Dienste (wie in Abbildung 2, Schritt 5 dargestellt) bei Anfragen von Robot-Services automatisch nur für diese Services zugelassene Ressourcen berücksichtigen können oder umgekehrt bei Anfragen von Services mit hohen Sicherheitsanforderungen diese Ressourcen meiden können.

Eine weitere Methode zum Ausschluss der Ressourcennutzung durch Robot-Services bietet sich im Autorisierungssystem (Abbildung 2, Schritt 1). Hier können die Anfragen durch Robot-Services grundsätzlich gefiltert und abgelehnt werden. Die Möglichkeit hierzu bietet das Namensschema für DNs in Robot-Zertifikaten (siehe auch Kapitel 3).

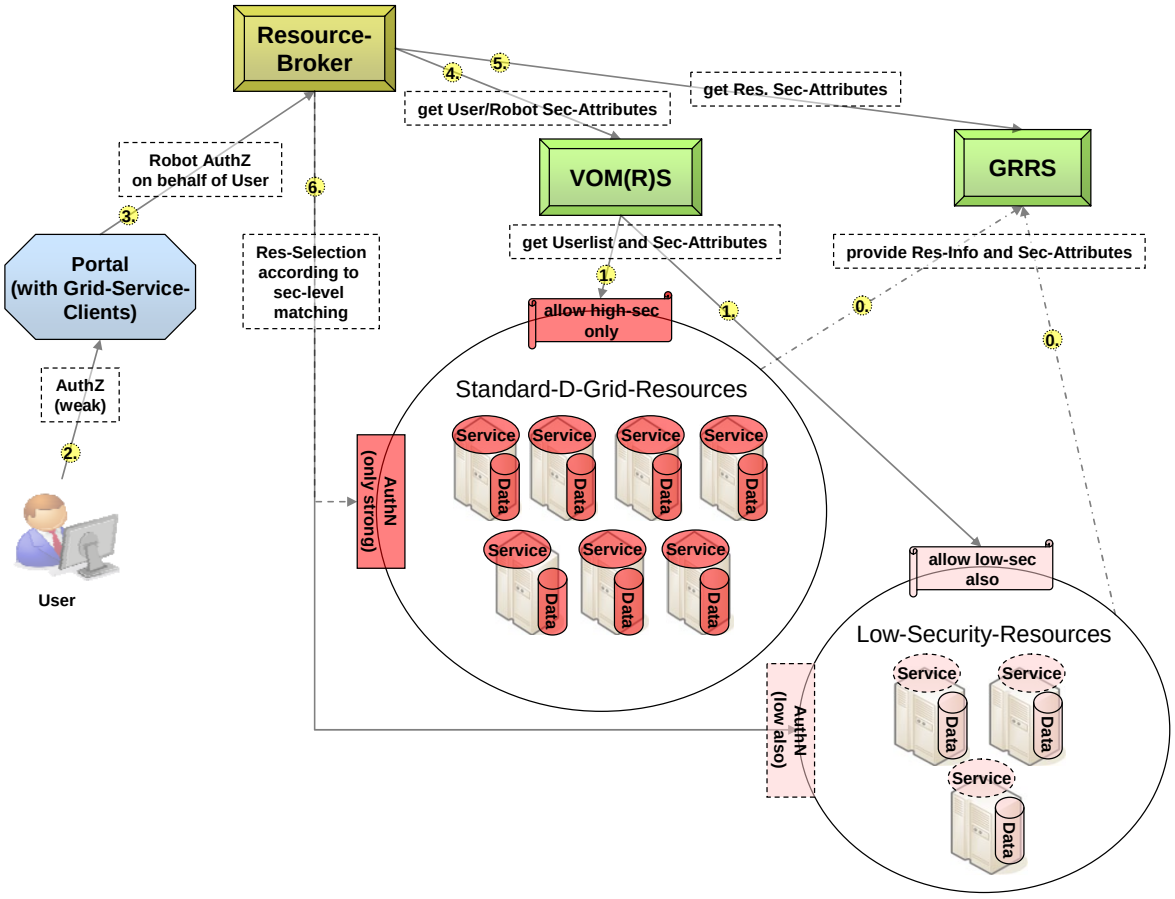

Abbildung 2: Architektur zur Verwendung von Robot-Zertifikaten

Robot-Zertifikate und die zugehörigen Robot-Nutzer – d.h. die für die Robot-Services und zugehörigen Zertifikate verantwortlichen Administratoren – können somit gefahrlos über das D-Grid VOMS bzw. VOMRS registriert werden, sofern im Vorfeld alle Ressourcenbetreiber rechtzeitig darüber informiert wurden und ihre Autorisierungssysteme entsprechend anpassen können.

Für Ressourcen, die die Nutzung durch Robot-Services ausschließen möchten, ist hierfür die oben angesprochene Filterroutine beim Abruf der gridmapfiles aus dem VOMS einzurichten, die alle durch ihren DN als Robots gekennzeichneten Nutzer aussortiert. Anpassungen des Ressourcen-Eintrags am GRRS sind für die Ablehnung von Robot-Nutzern nicht zwingend erforderlich. Ein Setzen des oben vorgeschlagenen *respool* Attributs auf den Wert *standard* hätte aber den Vorteil, dass diese Ressourcen von Workload Management Systemen von vornherein nicht mit Anfragen von Robot-Services versorgt würden.

Für Ressourcen, die Robot-Services akzeptieren möchten, wäre hingegen keine Anpassung am Autorisierungssystem erforderlich. Stattdessen müsste für die jeweilige Ressource beim GRRS das *respool* Attribut auf den Wert *robot* gesetzt werden.

Für weitergehende Differenzierungen hinsichtlich der Akzeptanz von Robot-Usern auf D-Grid Ressourcen, beispielsweise zur Unterscheidung der Zugriffsrechte innerhalb von Ressourcen für verschiedene Services, wäre eine Erweiterung der Unterscheidungsfähigkeiten der Autorisierungssysteme erforderlich. Es wäre z.B. denkbar, Robot-Usern nur Zugriff auf bestimmte Services einer Ressource zu gewähren. Solchen Differenzierungen sind grundsätzlich keine Grenzen gesetzt, sie erfordern aber jeweils Anpassungen in der Logik der Autorisierungssysteme selbst. Außerdem wäre ebenfalls eine Kennzeichnung der jeweiligen Differenzierungstiefe über weitere *respool* Attributwerte im GRRS zu empfehlen, um anderen Ressourcenbetreibern die Möglichkeit zu geben, sich demgegenüber abzugrenzen.

In jedem Fall bedarf die Zulassung von Robot-Services in D-Grid einer Zulassung durch den D-Grid Beirat. Diese wiederum erfordert die rechtzeitige Information und Mitwirkung der D-Grid Ressourcenbetreiber.

8 Zusammenfassung

Mit der Erweiterung der Policies zur Zertifikatnutzung seitens der EUgridPMA und der DFN Grid PKI wurde die Basis für die Nutzung von Robot-Zertifikaten und somit auch von Robot-Services in D-Grid gelegt. Um auch für die Nutzung von Robot-Services möglichst hohe Sicherheitsstandards zu gewährleisten, wurden umfassende Anforderungen an die Kennzeichnung und Aufbewahrung sowie an die Verwendung von Robot-Zertifikaten definiert. Diese wurden in den Kapiteln 2 bis 6 im Detail erläutert.

Für einen produktiven Einsatz in D-Grid ist jedoch zusätzlich die Akzeptanz der Nutzung von Robot-Zertifikaten erforderlich. Um diese sowohl auf Seiten der Ressourcenbetreiber, als auch auf Seiten der Nutzer mit persönlichen Zertifikaten etablieren zu können, wird eine Trennung der Ressourcen für Robot-Services und für alle bisher existierenden Services empfohlen. Die Einrichtung unterschiedlicher Ressourcenpools erfordert aus praktischen Gründen des Workload Management geringfügige Anpassungen am Grid Resource Registration Service (GRRS) sowie geringfügige Anpassungen der Autorisierungsmechanismen an den Ressourcen.

Ob und wie weit eine Nutzung von Robot-Zertifikaten in D-Grid in der Praxis gewünscht und akzeptabel ist, muss vom dafür zuständigen Gremium, dem D-Grid Beirat, geklärt werden.

9 Literatur

[1] Falkner et al.: Gap-SLC – Task 5, Deliverable 5-1, Version 1.0, http://gap-slc.awi.de/documents/Gap-SLC_D5-1_v1.0.pdf

[2] EUGridPMA : Guideline on Approved Robots, Version 1.0, 09 Feb 2010, http://www.eugridpma.org/guidelines/robot/approved-robots-20100119.pdf

[3] EUGridPMA: Protection of private key data for end-users in local and remote systems, Version 1.1, 21 Sep 2010, http://www.eugridpma.org/guidelines/pkp/pk-protection-1.1-20100921.pdf

[4] DFN PKI: Certificate Policy of the Public Key Infrastructure in the Deutsche Forschungsnetz – Grid – V1.5, May 2010, https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_grid-cp_v15.pdf

[5] DFN PKI: Certification Practice Statement of the Public Key Infrastructure in the Deutsche Forschungsnetz – Grid – V1.5, May 2010, https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_grid-cps_v15.pdf

[6] DFN Grid PKI Webportal, https://www.pki.dfn.de/grid/

[7] DFN PKI FAQ: Wie erzeuge ich einen PKCS#10 Zertifikatrequest (CSR - Certificate Signing Request)?, https://www.pki.dfn.de/faqpki/faqpki-allgemein/#c13011