GSI – die Grid Security Infrastructure

Safer Grid

Die systemimmanente globale Verteilung beim Grid Computing und der Datenaustausch per Internet erfordern zwingend eine sichere Authentifizierungsmethode für alle Beteiligten. Die Grid Security Infrastructure des Globus-Toolkits benutzt dafür asymmetrische Kryptographie. Ursula Epting

Das World Wide Grid taugt leider auch als Spielplatz für Skript-Kiddies. Als Lohn winkt der Zugang zu weltweit verteilten Clustern mit zehntausenden CPUs. Grid-Betreiber brauchen daher eine Methode zur sicheren, automatischen Authentifizierung von berechtigten Benutzern und Endgeräten. Beim Globus-Toolkit zeichnet hierfür die GSI-Komponente verantwortlich.

Die Grid Security Infrastructure (GSI, [1]) bedient sich der Public-Key-Kryptographie (siehe Kasten „Verschlüsselung und Signatur"). Während das Verschlüsseln von Daten in der Public-Key-Kryptographie mit dem öffentlichen Schlüssel sehr simpel abläuft, ist es fast unmöglich, sie ohne Zusatzinformationen wieder zu entschlüsseln. Diese Informationen stecken im korrespondierenden privaten Schlüssel, der nur dem Besitzer bekannt ist [2], [3].

Zertifizierung bestätigt die korrekte Schlüsselherkunft

Das Konzept des Zertifikats stellt sicher, dass ein öffentlicher Schlüssel wirklich zu einer bestimmten Person – oder im Grid Computing zu einem Server einer Anwendung oder einem Service – gehört [4]. Ein Zertifikat enthält einen weltweit eindeutigen Namen, den so genannten Distinguished Name (DN), außerdem den öffentlichen Schlüssel der Person. Es speichert zudem Gültigkeitsdauer, Ausstellungsdatum, verwendete Algorithmen, Schlüssellängen, den Namen der zuständigen Zertifizierungsstelle sowie ihre Signatur über die im Zertifikat enthaltenen Informationen.

Die Zertifizierungsstelle (Certification Authority, CA) als vertrauenswürdig angenommene Instanz beglaubigt mit ihrer unabhängigen Unterschrift die Identität mit ihrem öffentlichen Schlüssel. Die Art und Weise, wie eine Zertifizierungsstelle die Identität eines Benutzers, Servers oder Service überprüft und welche Sicherheitsvorkehrungen sie rund um die Zertifizierungsstelle trifft um Missbrauch zu verhindern, bestimmen eine Certification Policy (CP) und das so genannte Certification Practice Statement (CPS).

Die Certification Policy ist frei zugänglich und jede Institution, die Ressourcen für das Grid zur Verfügung stellt, kann selbst entscheiden, ob sie die Zertifizierungsstelle akzeptiert oder nicht. Sie vertraut nur Zertifikaten, die von einer bekannten und akzeptierten Stelle stammen. Da es in jedem System ein Maß an Missbrauch gibt, veröffentlichen Zertifizierungsstellen Widerrufslisten. Auf diesem Weg erklärt die CA Zertifikate für ungültig, zum Beispiel wenn ein privater Schlüssel gestohlen wird. Über den Mechanismus bleibt ein Zertifikat auf seine Aktualität hin überprüfbar.

Mapping zwischen DN und Unix-Name per Datei

Die Autorisierung eines Benutzers für den Zugang zu einer Ressource erfolgt bei Unix und Linux über eine Verknüpfung des global eindeutigen Distinguished Name mit einer lokalen Unix-ID. Dieses Mapping ist im Grid-Mapfile (siehe Listing 2) festgehalten, die Berechtigungen des Unix-Accounts legt der lokale Administrator fest. Der für das Mapfile notwendige Distinguished Name lässt sich aus der »Subject«-Zeile des Zertifikats (siehe Listing 1) entnehmen. Der DN steht dann in Anführungszeichen links, nach etwas Whitespace folgt der Unix-Name.

Die Globus-Sicherheitsinfrastruktur bewahrt auf diese Weise den lokalen Administratoren die Lufthoheit über ihren Ressourcen und macht sie von einem zentral verwalteten Sicherheitssystem unabhängig. Das Datenformat der GSI-Zertifikate folgt dem X.509-Standard, der von ISO/IEC und CCITT entwickelt wurde. Das bei GSI benutzte X.509-Profil hat die Internet Engineering Task Force (IETF) bestimmt. Es ist das gleiche, das

auch Konqueror, Opera sowie Netscape & Co. akzeptieren und einsetzen.

Ein nicht-hierarchisches Modell

In der praktischen internationalen Arbeit der großen Projekte vereinigten sich die Grid-CA-Betreiber zur „European Policy Management Authority Group for Grid-Authentication in e-science“ (EugridPMA, [5]). Sie entwickelt für die Zertifizierungsstellen Mindestanforderungen und Verfahren zur gegenseitigen Überprüfung, um eine gemeinsame Vertrauensdomäne aufzubauen. Die EugridPMA beheimatet nicht nur die Betreuer der Zertifizierungsstellen, sondern auch Vertreter jener Institutionen, die ihre Ressourcen in Grid-Projekten zur Verfügung stellen.

Anders als bei hierarchischen Modellen bestehen diese CAs meist nur aus einer Root-CA, die Zertifikate für Benutzer, Server und Services ausstellt. Jede CA hat ihre eigene, RFC-2527-orientierte Certification Policy (CP). Die Mitglieder begutachten und bewerten die CP. So entsteht projektabhängig und demokratisch eine Liste ([6], [7]) vertrauenswürdiger Partner-CAs. Eine Koordination mit diversen amerikanischen und asiatischen CA-Betreibern vermeidet, dass sich Namensräume überschneiden.

Ein besonderes Globus-Verzeichnis enthält – zentral über RPMs verteilt – für jede akzeptierte CA deren Root-Zertifikat, die URL der Widerrufsliste und die »signing-policy.conf«-Datei, die den Namen der CA enthält und den Namensraum festlegt, den die CA signieren darf. Im Beispiel sieht sie so aus:

```
access_id_CA  X509   '/C=DE/O=Linux-World/➥
CN=Linux-CA'
pos_rights    globus CA:sign
cond_subjects globus ➥
'"/C=DE/O=Linux-World/*" ➥
"/O=Linux-World/OU=*"'
```

Derzeit bauen die beteiligten CA-Betreiber eine Instanz auf, in der man die Fingerprints der Root-Zertifikate unabhängig vergleichen kann.

Stummes Vertrauen per SSL und Zertifikat

Die Grid Security Infrastructure benutzt das im Internet gängige SSL/TLS-Protokoll für eine stumme Zwei-Wege-Authentifizierung, bei der die Benutzer Passwörter eintippen müssen. Zwei Parteien beweisen einander mittels asymmetrischer Kryptographie, dass sie diejenigen sind, die sie vorgeben zu sein. Voraussetzung ist, dass beide Parteien ein Zertifikat besitzen und dass den jeweiligen Zertifizierungsstellen zu vertrauen ist [8], [9].

Das Prinzip zeigt Abbildung 2: Partei A nimmt Verbindung zu Partei B auf und sendet ihr das eigene Zertifikat »CertA«. B entnimmt »CertA«, wer A ist und überprüft dessen Gültigkeit und die Richtigkeit der Signatur der Zertifizierungsstelle. Das geschieht mit dem öffentlichen Schlüssel der CA, der in einem Globus-Verzeichnis hinterlegt ist. Hierbei unterstellt B zunächst, dass der Zertifizierungsstelle zu vertrauen ist.

Ein Blick in die Widerrufsliste klärt, ob das verwendete Zertifikat zwischenzeitlich widerrufen wurde. Ist alles in Ordnung, sendet B eine Nachricht zufälligen Inhalts an A. Diese Nachricht verschlüsselt A mit ihrem privaten Schlüssel und sendet sie an B zurück. Dort angekommen entschlüsselt B die Nachricht mit dem öffentlichen Schlüssel von A und vergleicht das Ergebnis mit der zuvor gesendeten Nachricht. Stimmen beide überein, dann ist die Partei A wirklich die Besitzerin des privaten Schlüssels, der zum beglaubigten öffentlichen Schlüssel gehört.

Anschließend wiederholen beide Parteien den Vorgang, wobei B ihr Zertifikat an A sendet. Sollte gewünscht sein, dass die gesamte Kommunikation verschlüsselt abläuft, legen die Beteiligten die Algorithmen fest und erzeugen einen symmetrischen Sitzungsschlüssel für das Verschlüsseln der Daten. Meist verzich-

Listing 1: Zertifikat (Auszug)

```
01 Certificate:
02   Data:
03     Version: 3 (0x2)
04     Serial Number: 3 (0x3)
05    Signature Algorithm: md5WithRSAEncryption
06    Issuer: C=DE, O=Linux-World, CN=Linux-CA
07     Validity
08         Not Before: Dec  4 13:47:19 2003 GMT
09         Not After : Dec  4 13:47:19 2004 GMT
10     Subject: C=DE, O=Linux-World, CN=Albert Einstein
```

Listing 2: Ein Grid-Mapfile

```
01 "/C=DE/O=Linux-World/OU=Sub-World/CN=Albert Einstein"
   local1
02 "/C=IT/O=TBIN/OU=Personal/L=Catania/CN=Maria Rossario/
   Email=rossario@zb.tbin.it"                    local1
03 "/C=FR/O=LINT/OU=MAM/CN=Claudia Morgan Projekt1/
   Email=morgan@zb.mam.fr"                       local2
04 "/O=Grid/O=PHANT/OU=phant.ch/CN=Hans Julius"  local2
05 "/C=CH/O=FANT/OU=GRID/CN=August Maier 0815"   local2
```

Verschlüsselung und Signatur

Die Public-Key-Kryptographie lässt sich am Beispiel verschlüsselter und signierter E-Mails erläutern: Schreibt ein Kunde eine E-Mail an seine (sehr fortschrittliche) Bank, will er vermeiden, dass ein Dritter ihren Inhalt mitliest. Die Bank ihrerseits möchte nachprüfen können, ob die Mail wirklich von dem angenommenen Absender stammt.

Abbildung 1 zeigt den Vorgang. Der Kunde verschlüsselt zunächst seine Nachricht »KT« (Klartext) mit dem öffentlichen Schlüssel der Bank »PubB« und signiert den verschlüsselten Text »CT« (Ciphertext). Dazu bildet er über den Text eine Prüfsumme »PS« (Hashwert) und verschlüsselt sie (»X«) mit seinem privaten Schlüssel »PrivK«.

Die Bank berechnet nach dem Empfang der Mail ihrerseits die Prüfsumme »CT« und entschlüsselt die mitgesandte Prüfsumme anhand des öffentlichen Schlüssels des Absenders »PubK«. Ein Vergleich der Werte »Y« und »X« zeigt, ob die Nachricht von dem angenommenen Absender stammt. Die Prüfsumme stellt zudem sicher, dass die Nachricht unterwegs nicht verändert wurde. Zuletzt entschlüsselt die Bank die Nachricht mit ihrem privaten Schlüssel »PrivB«. Die Nachricht »KT« ist nun verfügbar.

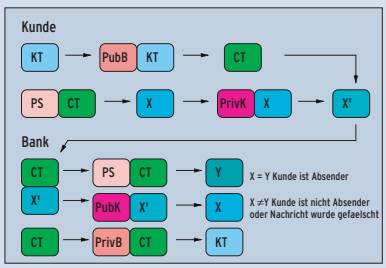

Abbildung 1: Public-Key-Kryptographie erlaubt die Verschlüsselung von Daten und gegenseitige Identifizierung zweier Kommunikationspartner – hier am Beispiel des Austauschs einer E-Mail mit einer Bank erläutert.

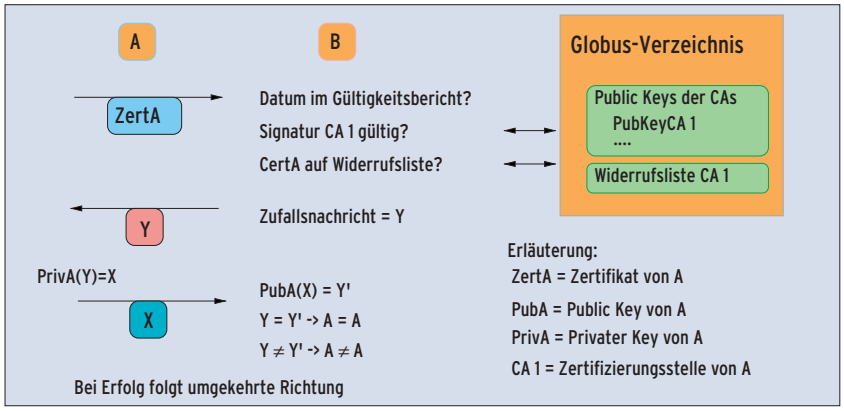

Abbildung 2: Die stumme Authentifizierung der Parteien A und B erbringt den gegenseitigen Identitätsbeweis.

tet man jedoch im Grid Computing darauf – aus Performancegründen .

Delegation

GSI enthält eine Ergänzung des SSL-Protokolls zum Delegieren der Authentifizierung und zum Single-Sign-on. Will eine Applikation auf mehrere Ressourcen und Dienste zugreifen, soll ihr Benutzer sein Passwort zum Schutz des privaten Schlüssels nur einmal pro Session eingeben müssen. Praktisch erledigt das ein Proxy: Der Befehl »grid-proxy-init« erzeugt nach einmaliger Passworteingabe ein Zertifikat mit neuem Schlüsselpaar. Das Zertifikat ist mit dem User-Zertifikat unterschrieben.

Proxy-Zertifikate sind begrenzt gültig, meist nur wenige Stunden. Sie enthalten die Identität des Benutzers sowie den Hinweis, dass es sich um ein Proxy-Zertifikat handelt. Der Prozess der stummen Authentifizierung verläuft nun in leicht abgewandelter Form: Das Proxy-Zertifikat wird mit dem User-Zertifikat überprüft, das ebenfalls mitgesendet wird. Nach gleichem Muster stellt man mittels CA-Zertifikat die Wahrhaftigkeit des User-Zertifikats fest. Hierdurch entsteht eine Kette des Vertrauens, die nirgends unterbrochen sein darf.

Sicherheit durch Geheimhaltung

Die Infrastruktur von Globus kann so lange als sicher angesehen werden, wie die Geheimhaltung des privaten Schlüssels und des Passworts gewährleistet ist. Benutzer und Administratoren müssen dafür Sorge tragen, dass die lokal gespeicherten Dateien über korrekte Dateiberechtigungen geschützt sind. Wer die Sicherheitsvorkehrungen vieler Universitäten kennt, mag zweifeln, ob der Schutz universell und hinreichend ist. Auch im Grid Computing sind also – wie überall im Leben – Zufallsbekanntschaften mit Vorsicht zu genießen. *(jk)* ■

Infos

[1] GSI: [http://www.globus.org/security/overview.html]

[2] Bruce Schneier, „Angewandte Kryptografie, Protokolle, Algorithmen und Sourcecode in C“: Addison-Wesley 1996

[3] Simon Singh, „Geheime Botschaften – Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet“: dtv 2003

[4] Kay Wondollek, „Public Key Infrastructure – Architektur und Software“: Linux-Magazin 02/04, S. 66

[5] EugridPMA: [http://www.eugridpma.org]

[6] European Data Grid Project: [http://marianne.in2p3.fr/datagrid/ca/ca-table-ca.html]

[7] Cross Grid Project: [http://www.crossgrid.org]

[8] Achim Leitner, „Verschlüsselt und authentifiziert kommunizieren mit TLS“: Linux-Magazin 04/02, S. 50

[9] Michael Pramateftakis, „Grundlagen: Authentifizierunsprotokolle“: Linux-Magazin 05/04, S. 50

Die Autorin

Ursula Epting studierte Mathematik, Deutsch und Literatur an der Uni Mannheim. Seit September 2000 arbeitet sie im Bereich Netzwerksicherheit am Forschungszentrum Karlsruhe. Sie leitet die Zertifizierungsstelle German Grid und hat immer ein freundliches Wort für ihre Kollegen parat.