Verschlüsselung und Authentifizierung als Basis internationalen Vertrauens

U. Epting, IWR

Einleitung

Grid Computing gibt seinen Nutzern die Möglichkeit zum Zugang zu weltweit verteilten Rechenressourcen mit potentiell zehntausenden von CPUs. Ausgefeilte Sicherheitsmechanismen müssen deshalb für die Einhaltung vorgegebener Sicherheitskriterien sorgen. Wird über das Grid etwa ein Programm auf einen Cluster in Italien oder Taiwan geschickt, so wird der Benutzer dort in aller Regel nicht persönlich bekannt sein. Umgekehrt möchten Wissenschaftler sicher sein, ihre neuesten Forschungsergebnisse auf dem richtigen Datenserver abzulegen – und nicht etwa bei einem Hacker. Es wird also eine Methode zur sicheren, automatischen Authentifizierung von Benutzern und Servern benötigt. Das Globus-Toolkit [1], das in der GridKa-Umgebung des IWR eingesetzt wird, stellt ein Sicherheitsmodell bereit – die Grid Security Infrastructure (GSI) [2].

Die Grid Security Infrastruktur (GSI)

Public Key Kryptographie und RSA-Algorithmus

Die Sicherheitsinfrastruktur GSI des Globus Toolkits dient hauptsächlich der sicheren Authentifizierung von Benutzern oder Endgeräten. Sie bedient sich dazu der Public-Key-Kryptographie. Dieses 1976 durch Whitfield Diffie und Martin Hellman entwickelte Konzept, auch als asymmetrische Kryptographie bekannt, beruht auf mathematischen Algorithmen, mit deren Hilfe man sehr einfach Daten mit einem öffentlich bekannten Schlüssel verschlüsseln kann, wohingegen es fast unmöglich ist, sie ohne zusätzliche Informationen wieder zu entschlüsseln. Diese zusätzlichen Informationen bezeichnet man als privaten Schlüssel, der nur dem jeweiligen Besitzer bekannt ist [3] [4]. Öffentlicher und privater Schlüssel bilden zusammen ein Paar.

Der bekannteste in der Public-Key-Kryptographie verwendete Algorithmus ist der 1977 nach seinen Erfindern – Ron Rivest, Adi Shamir und Leonard Adleman – benannte RSA-Algorithmus. Die Sicherheit dieses Verfahrens beruht auf der Schwierigkeit, große Zahlen zu faktorisieren, d.h. in ihre Primfaktoren zu zerlegen. Zur Herstellung des Schlüsselpaares werden zwei sehr große Primzahlen p und q – mit 150-200 Dezimalstellen oder mehr – verwendet. Bei jeweils etwa 150 Dezimalstellen ergibt sich für das Produkt N = p x q ein Wert mit etwa 300 Dezimalstellen, was einer Schlüssellänge von 1024 Bits entspricht. Zusätzlich wird eine zufällige Zahl e so gewählt, das e und (p – 1) x (q – 1) keinen gemeinsamen Teiler haben. Die beiden Zahlen N und e sind der öffentliche Schlüssel. Der private Schlüssel d wird mit Hilfe des sogenannten erweiterten Euklidischen Algorithmus berechnet und geheim gehalten. Der Klartext M wird über die ASCII-Tabelle zunächst in Binär- und dann in Dezimalzahlen verwandelt und blockweise mit der in Abb.1 dargestellten Formel berechnet. Es ergibt sich der verschlüsselte Text C – der so genannte Cipher-text. Der Empfänger kann ihn nur dann mit der Umkehrfunktion, die in der zweiten Formel von Abb. 1 dargestellt ist, wieder entschlüsseln, wenn er d kennt oder berechnen kann.

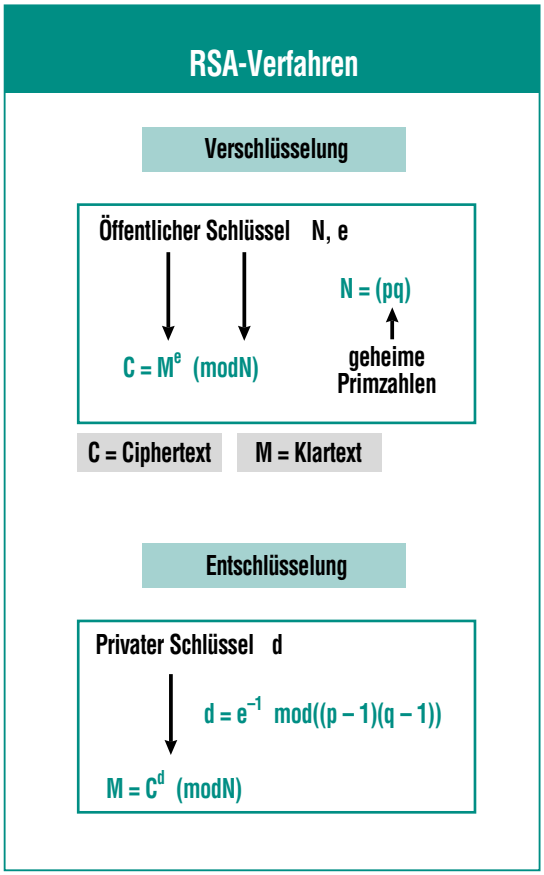

Abb.1: Der RSA-Algorithmus zur Kryptographie mit öffentlichem Schlüssel beruht auf der Schwierigkeit, sehr große Zahlen N zu faktorisieren, d.h. in ihre (geheimgehaltenen) Primfaktoren p und q zu zerlegen. Die beiden Zahlen N und e sind der „öffentliche Schlüssel". Der Klartext M wird über die ASCII-Tabelle zunächst in Binär- und dann in Dezimalzahlen verwandelt und mit der dargestellten Formel in den verschlüsselten Text C umgerechnet. Ein Empfänger kann C nur dann mit der Umkehrfunktion entschlüsseln, wenn er den geheimgehaltenen „privaten Schlüssel" d kennt (oder bei gelungener Faktorisierung von N berechnen kann!)

Die verwendete Modularithmetik untersucht endliche Gruppen von Zahlen. Sie ist als „Uhrenarithmetik“ jedem aus dem Alltag bekannt: Wenn Ihnen abends um 23.00 Uhr gesagt wird, dass in 5 Stunden ein Treffen stattfindet, wissen Sie, dass das Treffen nicht um 28.00 Uhr, sondern um 4.00 Uhr nachts stattfindet. Sie berechnen dies folgendermaßen: 23 + 5 = 28, 28 geteilt durch 24 = 1 Rest 4. Mathematisch dargestellt: 23 + 5 = 4 mod 24, also (Rest) modulus (Teiler). Dieser Ausdruck ist aber offenbar nicht eindeutig, sondern könnte auch 23 + 29 bedeuten. Modulfunktionen werden wegen ihrer Eigenschaften als Einwegfunktionen geschätzt. Es ist sehr schwer, zu einer gegebenen Funktion die Umkehrung zu finden. [5]

Im Fall von RSA müsste man die Zahl N faktorisieren. Dies ist zwar im Prinzip möglich, aber bei entsprechend großem N sehr zeitaufwändig. Man schätzt, dass man für die Faktorisierung einer 1024-Bit langen Zahl $3*10^{11}$ MIPS-Jahre braucht. (Ein MIPS-Jahr erfordert einen Rechner, der z. B. 1 Million Instruktionen pro Sekunde durchführen kann und ein Jahr läuft.) [6]

Das Verfahren eignet sich auch dafür, die Herkunft von Daten oder eines Textes durch eine Unterschrift (Signatur) zu bestätigen. Hierbei wird über die Daten oder den Text mit einer Einwegfunktion eine eindeutige Prüfsumme (Hashwert) ermittelt. Dieser wird sodann mit dem privaten Schlüssel des Absenders verschlüsselt und ebenfalls übermittelt. Der Empfänger entschlüsselt nun mit dem öffentlichen Schlüssel des Absenders den gesendeten Wert und vergleicht ihn mit dem von ihm selbst berechneten Wert. Stimmen beide überein, so ist die Herkunft der Daten oder des Textes bestätigt, da keine andere Person den zum verwendeten öffentlichen Schlüssel gehörigen privaten Schlüssel besitzt.

Zertifizierung

Um sicherzustellen, dass ein öffentlicher Schlüssel wirklich zu einer bestimmten Person gehört, wurde das Konzept der Zertifizierung entwickelt. Eine dritte, vertrauenswürdige Instanz – eine Zertifizierungsstelle (Certification Authority, CA) – beglaubigt mit ihrer unabhängigen Unterschrift die Verbindung einer Identität mit einem öffentlichen Schlüssel. Ein Zertifikat enthält einen weltweit eindeutigen Namen, den so genannten Distinguished Name (DN), den öffentlichen Schlüssel der Person und zusätzliche Informationen wie Gültigkeitsdauer, Ausstellungsdatum, verwendete Algorithmen und Schlüssellängen. Ferner finden sich darin der Name der Zertifizierungsstelle sowie ihre Unterschrift, die bestätigt, dass die im Zertifikat enthaltenen Informationen korrekt sind.

Die Art und Weise, wie eine Zertifizierungsstelle die Identität der Benutzer oder Endgeräte überprüft und welche Sicherheitsvorkehrungen sie rund um die Zertifizierungsstelle trifft sind in der Certification Policy (CP)/Certification Practice Statement (CPS) festgelegt und veröffentlicht. Jede Institution, die Ressourcen für das Grid zur Verfügung stellt, kann entscheiden, ob sie der Zertifizierungsstelle vertraut. Über veröffentlichte Widerrufslisten kann ein Zertifikat schnell für ungültig erklärt werden, wenn zum Beispiel der private Schlüssel gestohlen wurde.

Die Zertifikate, die von der GSI verwendet werden, folgen in ihrem Datenformat dem X.509-Standard, der von der Internet Engineering Task Force (IETF) für das Internet standardisiert wurde und auch von anderer Software, etwa den üblichen Webbrowsern (Konqueror, Opera, Netscape, Internet Explorer), eingesetzt wird.

Zertifizierungsstelle GridKa-CA

Das Institut für wissenschaftliches Rechnen (IWR) betreibt seit Dezember 2001 die Zertifizierungsstelle GridKa-CA [7]. Hier erhalten Wissenschaftler aus 22 verschiedenen deutschen Institutionen Zertifikate, die von mehr als 65 Institutionen in insgesamt 24 Ländern akzeptiert werden. Die stetige Zunahme an Benutzern zeigt deutlich die Akzeptanz der GridKa-CA Zertifizierungsstelle des Forschungszentrums Karlsruhe. Der Betrieb einer Zertifizierungsstelle stellt besonders hohe Ansprüche an den Betrieb des zur Zertifizierung verwendeten Computers sowie den Schutz der darauf gespeicherten Daten (Abb. 2).

Die praktische Arbeit in großen, nationale Grenzen überschreitenden Projekten führte zu einem Zusammenschluss von CA-Betreibern aus verschiedenen Ländern. Diese in vielen internationalen Grid-Projekten tätige „Euro-

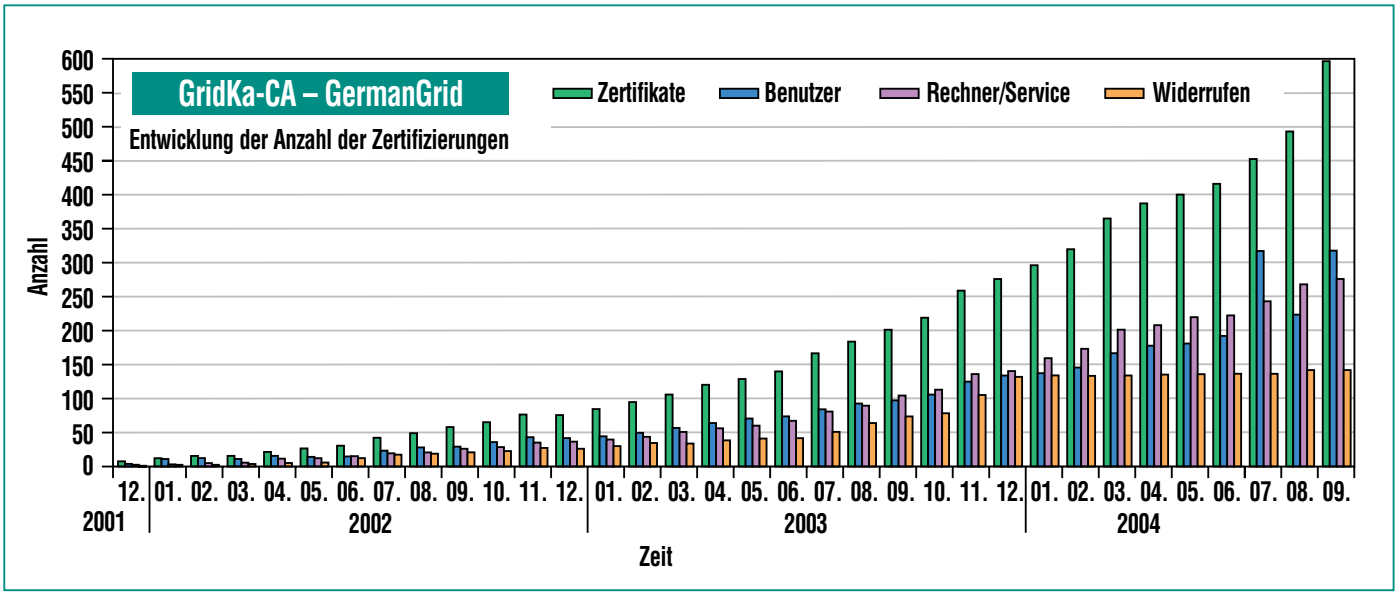

Abb. 2: Das IWR betreibt seit Dezember 2001 eine Zertifizierungsstelle. Das kontinuierliche Ansteigen der ausgegebenen Zertifikate zeigt das wachsende Interesse an Grid-Projekten in Deutschland.

pean Policy Management Authority Group for Grid-Authentication in e-science“ (EuGridPMA)[8] entwickelt für Zertifizierungsstellen Mindestanforderungen und Verfahren zur gegenseitigen Überprüfung, um eine gemeinsame Vertrauens-Domäne herzustellen. Auf diese Weise wird (projektabhängig und demokratisch) eine „Liste“ [9] [10] von vertrauenswürdigen Partner-CA’s erstellt. So ist ein Netz des Vertrauens entstanden, das die meisten europäischen Staaten, Amerika [11] und Teile Asiens [12] umfasst. Das IWR ist in dieser Gruppe seit ihrer Gründung vertreten.

Authentifizierung versus Autorisierung

Ein Zertifikat ist mit einem Personalausweis oder einem Reisepass vergleichbar. Ein Reisepass bescheinigt zwar die Identität des Besitzers, berechtigt aber nicht automatisch zur Einreise in jedes Land, sondern oft wird zusätzlich ein Visum benötigt. Ähnlich verhält es sich mit dem Besitz eines Zertifikats: um Zugang zu Grid-Ressourcen zu erhalten muss nach der Authentifizierung die Autorisierung erfolgen. Es muss festgelegt sein, welche Rechte der Benutzer hat – z.B. wie viel Rechenzeit er in Anspruch nehmen darf, welche Dateien er schreiben oder lesen darf. Die Rechte eines Benutzers werden über die Mitgliedschaft in einer virtuellen Organisation (VO) festgelegt. (Siehe Artikel „Grid Computing – Basis of multi-institutional Virtual Organizations“ im gleichen Heft.) Durch eine Abbildung (mapping) des eindeutigen DN („Distinguished Name“) auf ein lokales Userkonto bewahrt die GSI den lokalen Administratoren die Lufthoheit über ihre Ressourcen und macht sie von einem zentral verwalteten Sicherheitssystem unabhängig.

Das Secure Socket Layer (SSL) Protokoll

Das im Internet zur Sicherung der Kommunikation häufig verwendete Secure Socket Layer Protokoll – auch unter dem neuem Namen Transport Layer (TLS) Protokoll bekannt – ist auch in der GSI implementiert und ermöglicht eine Zwei-Wege-Authentifizierung. Zwei Parteien können mittels asymmetrischer Kryptographie beweisen, dass sie diejenigen sind, die sie vorgeben zu sein. Voraussetzung ist, dass beide Parteien ein Zertifikat besitzen und dass den jeweiligen Zertifizierungsstellen vertraut wird (Abb. 3).

Dies geschieht folgendermaßen: Partei A sendet B das Zertifikat (ZertA) zu. B entnimmt ZertA, wer A ist, und überprüft zunächst die Gültigkeit des Zertifikats und die Richtigkeit der Signatur der Zertifizierungsstelle. Dies geschieht mittels des öffentlichen Schlüs-

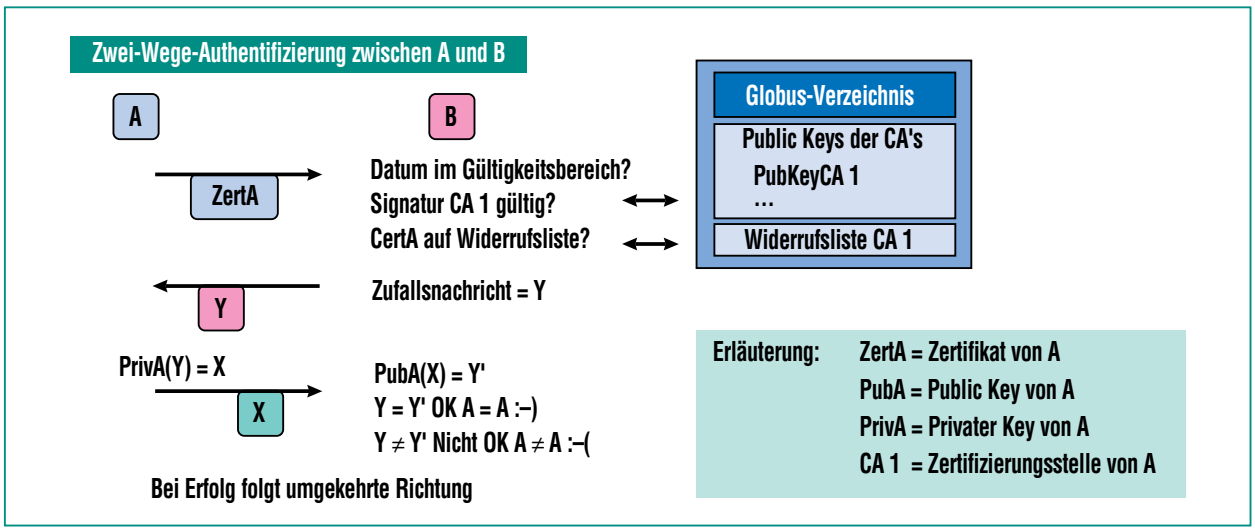

Abb. 3: Die 2-Wege-Authentifizierung zwischen den Parteien A und B erfolgt ohne direkte Absprache („stumm"): A sendet B das Zertifikat (ZertA) zu, dem B entnimmt, wer A ist. B überprüft die Gültigkeit des Zertifikats und die Richtigkeit der Signatur der Zertifizierungsstelle. Dann sendet B eine zufällige Nachricht an A. Diese wird von A mit seinem privaten Schlüssel verschlüsselt und an B zurückgesendet. B entschlüsselt die Nachricht mit dem öffentlichen Schlüssel von A und vergleicht das Ergebnis mit seiner ursprünglichen Nachricht. Stimmen beide überein, ist A der Besitzer des privaten Schlüssels, der zum beglaubigten öffentlichen Schlüssel gehört. Seine Identität ist somit bewiesen und es folgt in umgekehrter Richtung die Identifizierung von B.

sels der CA, der in einem Globus-Verzeichnis hinterlegt ist. Einem Check der Widerrufsliste wird entnommen, ob das verwendete Zertifikat zwischenzeitlich widerrufen wurde. Ist alles in Ordnung, so sendet B eine zufällige Nachricht zu A. Diese wird nun von A mit dem privaten Schlüssel verschlüsselt und zu B zurückgesendet. B entschlüsselt die Nachricht mit dem öffentlichen Schlüssel von A und vergleicht das Ergebnis mit der ursprünglichen Nachricht. Stimmen beide überein, so besitzt A den passenden privaten Schlüssel – seine Identität ist somit bewiesen.

Der Vorgang wird wiederholt, wobei nun B sein Zertifikat an A sendet. Sollte gewünscht sein, dass die gesamte Kommunikation verschlüsselt wird, werden anschließend die Algorithmen festgelegt und ein symmetrischer Sitzungsschlüssel erzeugt, mit dem die Daten verschlüsselt werden. Aus Performancegründen (Übertragung etlicher GBits pro Sekunde) wird im Grid-Umfeld darauf jedoch verzichtet.

Schlussbemerkung

Dieses Jahr konnte ein Team der Universität Bonn mit Unterstützung des Instituts für Experimentelle Mathematik in Essen und des Bundesamts für Sicherheit (BSI) erstmals eine 576 Bit lange Zahl – das sind 174 Dezimalstellen – faktorisieren [13]. Dennoch schätzen Experten, dass Schlüssel mit einer Länge von 1024 Bit – die im Grid-Umfeld als Mindestlänge betrachtet wird – noch bis zum Jahre 2020 sicher sein werden.

Jedoch hängt die Sicherheit von RSA zum einen von der Entwicklung der Mathematik ab: Bisher ist es nicht gelungen zu beweisen, dass es keinen Algorithmus für die Primfaktorzerlegung gibt, wenn auch Mathematiker seit 2000 Jahren verbissen danach suchen. Fände aber morgen ein Mathematiker solch einen Algorithmus, so wäre RSA für alle Zeit unbrauchbar geworden. Andererseits ermöglicht auch der Fortschritt in der Computertechnik immer kürzere Berechnungszeiten. So könnte man auch das Grid mit seinen riesigen Ressourcen zur Faktorisierung großer Zahlen verwenden und so die sichere Basis, auf der es jetzt ruht, zerstören, frei nach dem Motto:

„Die Revolution ist wie Saturn, sie frisst ihre eigenen Kinder." [14]

Literaturverzeichnis und weiterführende Informationen

[1] *Globus Software,*
http://www.globus.org

[2] *GSI,*
http://www.globus.org/security/overview.html

[3] Bruce Schneier,
Angewandte Kryptographie, Protokolle, Algorithmen und Sourcecode in C, Addison-Wesley, 1996, S. 525 - 540

[4] *Simon Singh,*
Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet,
Carl Hanser Verlag, München Wien, 2000

[5] Bruce Schneier,
ibid. S. 288 – 290

[6] Bruce Schneier,
ibid. S. 187

[7] http://grid.fzk.de/ca

[8] *EuGridPMA,*
http://www.eugridpma.org

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

[10] *CrossGrid Projekt,*
http://www.crossgrid.org

[11] www.gridpma.org *bzw.*
http://www.doegrids.org/pages/doegridspma.html

[12] http://www.apgridpma.org/

[13] http://www.proka.de/start.htm?/ipool/inform/krypto/rsa576.htm

[14] Georg Büchner,
Dantons Tod, Reclam Verlag, Ditzingen, 1989, S. 22