D-Grid

InGrid

Innovative Grid-Entwicklungen für Ingenieurwissenschaftliche Anwendungen

AP 4.3: Sicherheits- und Vertrauensmodelle

D 4.3.1
Anforderungsanalyse existierender Sicherheitsmechanismen, Erarbeitung von Spezifikationen

Table of Contents

1. Übersicht

Das Projekt InGrid beschäftigt sich mit gridbasierten IT-Szenarien für die Ingenieurwissenschaften. Diese bilden die Grundlage für Zusammenarbeitsmodelle für Forschung und Entwicklung in der Fertigungsindustrie. Typischerweise arbeiten hier Firmen, Zulieferer, Ingenieurbüros und öffentliche Forschungseinrichtungen sehr eng zusammen. Grundlage dieser Zusammenarbeit sind gegenseitiges Vertrauen und adäquate Sicherheitsmassnahmen.

Sollen solche Zusammenarbeitsmodelle mit Hilfe der Gridtechnologie auf Systeme der Informations- und Kommunikationstechnik abgebildet werden, so müssen diese IT-Umgebungen auch die Themen Sicherheit und Vertrauen in entsprechender Weise abbilden.

Dieser Bericht gibt einen Überblick über die relevanten Themen und zu treffenden Maßnahmen um die notwendigen Voraussetzungen für die Grid-Nutzung in den Ingenieurwissenschaften zu schaffen.

2. Basisdienste

2.1 Authentifizierung

Das Thema Authentifizierung wird im Integrationsprojekt DGI bearbeitet. Die spezifischen Anforderungen aus der Engineering-Community wurden kommuniziert und verwertet. Der aufgesetzte AAI-Service des DFN erfüllt alle gestellten Anforderungen.

2.2 Autorisierung

Das Thema Autorisierung wird im Integrationsprojekt DGI bearbeitet. Die spezifischen Anforderungen aus der Engineering-Community wurden kommuniziert und verwertet. Das geplante Identity-Management des DFN auf der Basis von Shibboleth erfüllt die Anforderungen aus der Engineering-Community in funktionaler Hinsicht.

Hierbei ist anzumerken, dass Software-Pakete in der Größe von Shibboleth ein eigenes Risiko darstellen, da davon auszugehen ist, dass sie unbekannte Schwachstellen enthalten. Diese Risiken betreffen den Betreiber direkt, da sie zu Kompromittierung oder Missbrauch der von ihm zur Verfügung gestellten Ressourcen führen können. Für die Anwender können mittelbar Risiken entstehen, wenn die Schwachstellen zu in ihrem Namen oder mit ihren Rechten erfolgenden, unautorisierten Zugriff auf Ressourcen führen. Außerdem schützt Identity-Management nicht gegen Manipulationen seitens des Betreibers. Deswegen, und weil die Gegenmaßnahmen gegen die Risiken der eingesetzten Software bei dem Betreiber liegen, nimmt er technisch und organisatorisch eine besondere Vertrauensstellung ein.

2.3 PKI

Das Thema PKI wird im Integrationsprojekt DGI bearbeitet. Die spezifischen Anforderungen aus der Engineering-Community wurden kommuniziert und verwertet. Der aufgesetzte AAI-Service des DFN erfüllt alle gestellten Anforderungen.

2.4 Auditability

Die Auditability, d.h. das Reporting über alle eingesetzten IT-Systeme nach erfolgter Verarbeitung spielt in den Ingenieurwissenschaften in erster Linie in sicherheitskritischen Bereichen, bei Kundenreviews und bei Produkthaftungsthemen eine Rolle. Da im medizinischen Bereich die diesbezüglichen Anforderungen noch sehr viel härter sind, wird dieses Thema, unter Berücksichtigung der Anforderungen aus den Ingenieurwissenschaften, im CP MediGrid bearbeitet.

2.5 Trackability

In den Ingenieurwissenschaften muss natürlich ausgeschlossen werden, dass Servicekomponenten von nicht vertrauenswürdigen Sites angezogen werden, eine Trackability, d.h. ein Nachweis, welche IT-Systeme verwendet werden, vor dem eigentlichen Verarbeitungsschritt spielt jedoch in den ingenieurwissenschaften keine Rolle. In der Medizin ist dies aufrund der gesetzlichen Rahmenbedingungen anders. Deshalb wird dieses Thema im CP MediGrid bearbeitet.

3. Zugriffsrechte und Zugriffskontrolle

3.1 Feingranulare Zugriffsrechte

Eine Steuerung von Zugriffsrechten unterhalb der Dokumenten- oder Dateiebene wird in den Ingenieurwissenschaften nicht benötigt. Dieses Thema wird deshalb im CP MediGrid bearbeitet.

3.2 Verteilte Zugriffskontrolle ohne Zentralinstanz

Gefordert wird hierbei eine gesicherte Anmeldung über die lokale Domänengrenze hinweg. Für die Verwaltung der Zugangsdaten für die im Grid zur Verfügung stehenden Ressourcen wird verlangt, dass diese ohne zentrale Instanz und Kontrolle betrieben werden kann. Die Autorisation der Grid-Benutzer an der lokalen Ressource soll nach wie vor in der Hand von befugten Administratoren bleiben. Das Ziel ist somit das dynamische Auffinden eines Autorisationspfades.

Zur Umsetzung bieten sich die Techniken moderner P2P-Systeme z.B. Pastry oder Chord an. Durch den dezentralen und redundanten Charakter dieser Verfahren bieten sie eine erprobte Umgebung zur Speicherung von Zugangs- bzw. Auffindungstabellen. Die Planung einer entsprechenden Architektur wäre das Ziel der nächsten Monate.

4. Vertraulichkeit

4.1 Daten: Dokumentenebene

Die Vertraulichkeit auf der Dokumentenebene soll Datensicherheit sowie die Integrität der Daten gewährleisten. Neben der Bereitstellung von Kryptographie-Algorithmen zur Datenverschlüsselung war gewünscht, das Sicherheitsproblem der gleichzeitigen Mehrfachnutzung eines Grid-Knotens zu beseitigen.

Durch die Methode der Virtualisierung ist es möglich, diesen Grad an Sicherheit/Vertraulichkeit zu erreichen. Durch die Verwaltung mehrerer, gleichzeitig laufender Betriebssystem-Instanzen auf einem physikalischen Rechner ist es möglich, das Konzept des exklusiven Zugangs auf einen Multiuser-Grid-Knoten zu übernehmen und somit die Benutzer eines Knotens sicher und anonym voneinander abzuschirmen (siehe Abbildung 1).

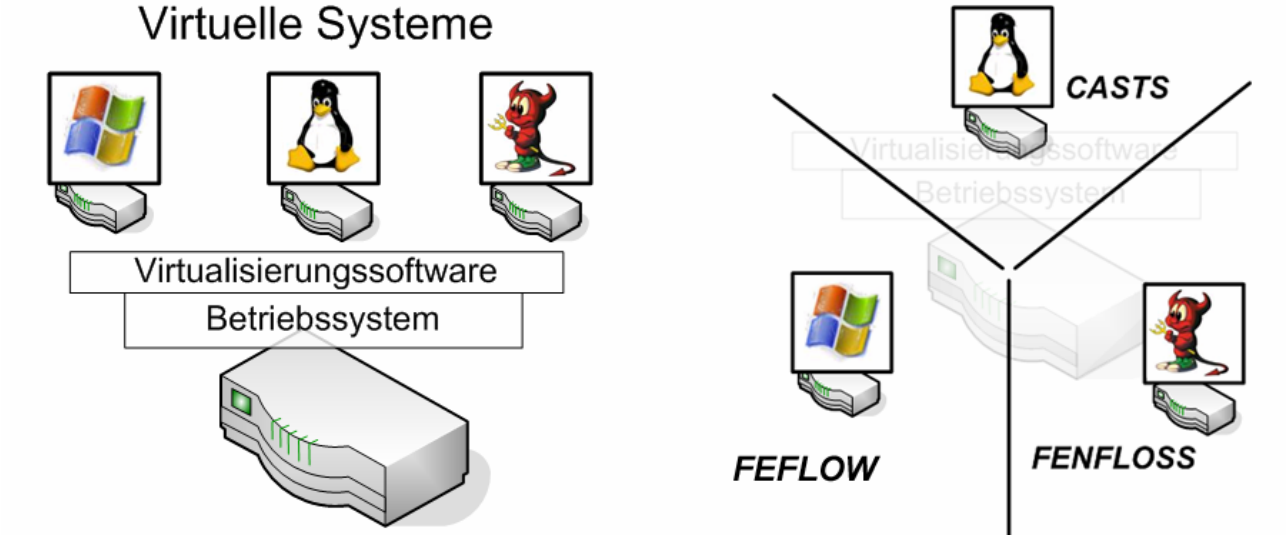

Abbildung 1 - Virtualisierte Systeme auf einer physikalischen Hardware (links). Symbolisierte Trennung der einzelnen Systeme und der sich darin befindenden Programme (rechts).

Die Virtualisierungssysteme XEN (http://www.cl.cam.ac.uk/Research/SRG/netos/xen) und OpenVZ/VIRTUOZZO (http://openvz.org/documentation/tech/virtuozzo) wurden bereits von Marburg erfolgreich für den Einsatz im Grid getestet.

Neben den genannten kompletten Virtualisierungstechniken wurden für UNIX BSD-Systeme SysTrace und Jailing, zwei Techniken zur Prozessabschirmung, für den Einsatz im Grid getestet. Beide sind allerdings auf Grund ihres hohen Konfigurationsaufwand nur bedingt in dynamischen Gridumgebungen einsetzbar. Für reine Java-Implementierungen wurde eine native Java-Sandboxumgebung getestet, die eine hohe und flexible Sicherheit gewährleistet, jedoch auf Grund der Java-Restriktion nicht als generelle Lösung vorgeschlagen werden kann. Abbildung 2 zeigt eine detaillierte Architektur, in der alle drei Techniken parallel laufen können.

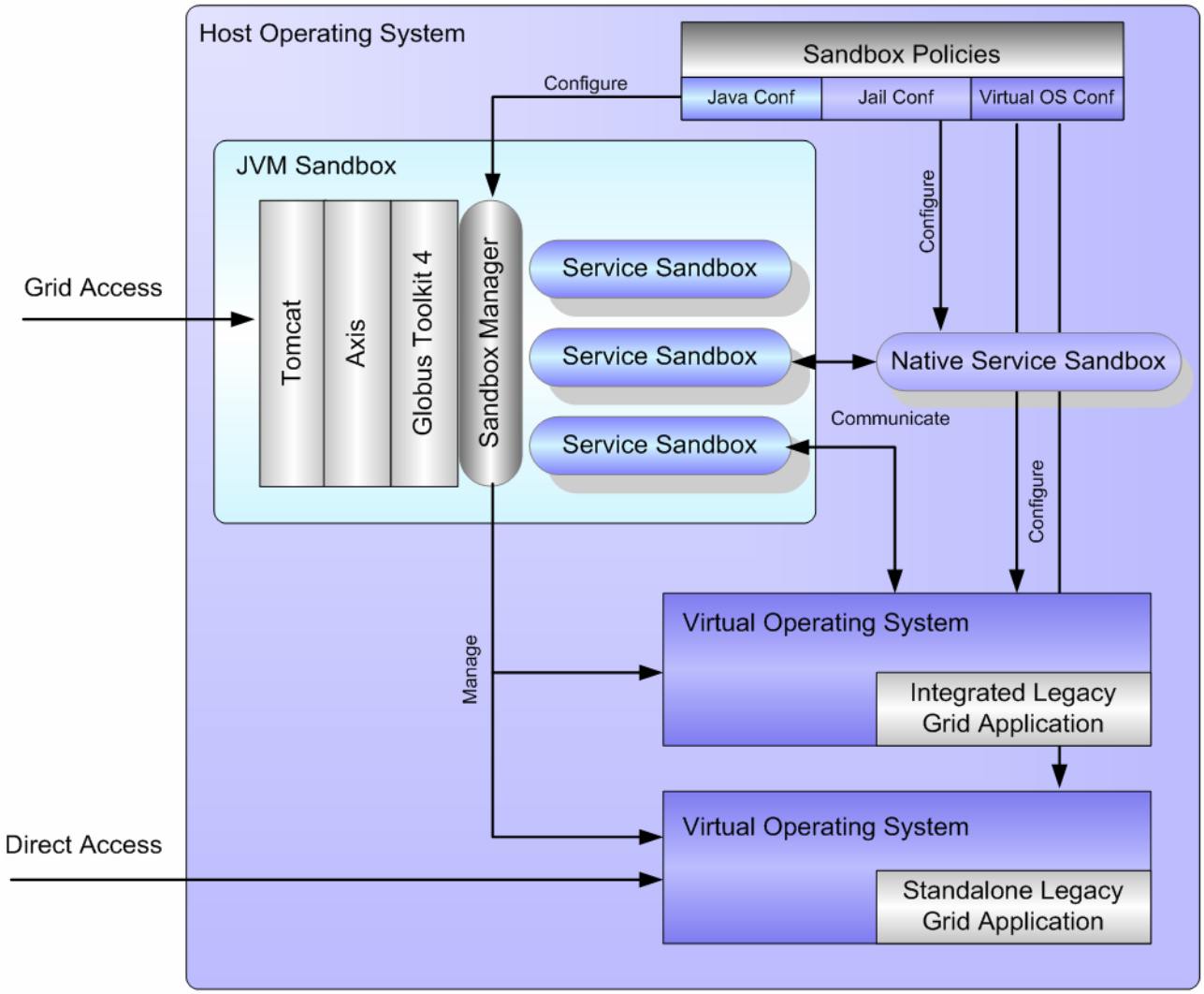

Abbildung 2 – Eine Grid-Knoten Architektur mit Verwendung von Betriebssystem-Virtualisierung, Native Service Sandboxes (Systrace, Jail) und Java Sandboxes.

4.2 Daten: Feingranular

Prozesse und Werkzeuge zur Sicherstellung der Vertraulichkeit unterhalb der Dokumenten- oder Dateiebene werden in den Ingenieurwissenschaften nicht benötigt. Dieses Thema wird deshalb im CP MediGrid bearbeitet.

4.3 Prozesse/Workflows

Der Schutz von Prozessen und Workflows umfasst alle Probleme, die auch beim Schutz von Dateien behandelt werden müssen, da die Programme, die den Workflow ausführen und aus denen die Prozesse gestartet werden, oft lokal gespeichert werden. Zusätzlich müssen Meta-Informationen über aktuelle Workflows und deren Prozesse, die über das Betriebssystem oder über die Grid-Middleware abgefragt werden können, geschützt werden. Die Virtualisierungstechniken, die für die Datenvertraulichkeit auf Dokumentenebene entwickelt werden, können gleichzeitig genutzt werden, um Prozess- und Workflowwissen zu schützen. Die Abschirmung der Nutzer auf Betriebssystemebene gewährleistet auch hier den Schutz vor anderen Grid-Nutzern. In der Grid-Middleware müssen analog dazu Sandbox-Umgebungen gebaut werden, die auf der Serviceebene Schutz bieten, um das in Services gespeicherte Prozess- und Workflow-wissen zu schützen. Ferner können die Methoden für den Schutz von IPRs auch eingesetzt werden, um Prozess- und Workflowwissen zu schützen.

4.4 Intellectual Property Rights an Programmen und Methoden

Die vom Betriebssystem angebotene Funktionalität zum „User Rights Management“ wird zurzeit genutzt, um Software und Prozesswissen zu schützen. Weiterhin werden Kernel-Modifikationen und Beschränkungen auf exklusiven Knotenzugang genutzt, um Prozessmetainformationen zu verbergen.

Auch für den Schutz der „Intellectual Property Rights (IPR)“ lassen sich die Techniken der Virtualisierung erfolgreich einsetzten. Durch die Separation einzelner Benutzer/Applikationen untereinander, werden sämtliche Informationen und auch Metainformationen gegenüber Dritten verborgen. Als weiterer Schritt lassen sich die Techniken der „Trusted Computing Group“ (TCG) (www.trustedcomputinggroup.org) sinnvoll zum Schutz der IPRs einsetzen. Gerade auf dem Teilgebiet des „Digital Right Managements“ versprechen die TPM Spezifikationen einen geeigneten Schutz. TCG sieht die Verwendung von zusätzlicher Hardware vor, um Systeme gegen bekannte Angriffe abzusichern (siehe Seite 10, *SoftwareInstanzen*).

Ein durch TPM gesichertes Betriebssystem auf Basis eines modifizierten Fedora Core IV wurde zu Testzwecken in Marburg bereits installiert. Das Systemimage kann den Projektpartnern zur Verfügung gestellt werden.

Digital Watermarking ist eine weitere Technik, die helfen kann, den Missbrauch von fremdem geistigen Eigentum zu sichern. Dieses dient nicht zur direkten Sicherung, sondern zur möglichen Zurückverfolgung und kann somit abschreckende Wirkung erzielen.

Weiterhin kann die Verschleierung („Obfuscation“) von Quellcode als Schutz vor Plagiaten dienen und ist einfach realisierbar. Es wäre möglich, „Digital Watermarking“ und auch „Obfuscation“ als Dienste durch die Middleware-Systeme zur Verfügung zu stellen.

5. Trust und Trust-Delegation

5.1 Personen

Die Delegation von Vertrauensstellungen an Personen spielt in den Ingenieurwissenschaften eine deutlich geringere Rolle als beispielsweise in der Medizin. Deshalb wird dieses Thema im CP MediGrid bearbeitet. Spezifische Anforderungen aus den Ingenieurwissenschaften wurden eingebracht.

5.2 Organisationen

Die Trust-Delegation an Firmen, staatliche Stellen und Virtuelle Organisationen wird ebenfalls im CP MediGrid bearbeitet, da hier vor allem die rechtlichen Vorgaben wesentlich stärker sind. Spezifische Anforderungen aus den Ingenieurwissenschaften wurden eingebracht. Die Überprüfung der Authenzität dieser Stellen ist durch (Grid-)Zertifikate, wie vom DGI bereitgestellt, ausreichend gesichert.

5.3 Software-Instanzen

Um das Vertrauen in Softwareinstanzen zu erhöhen, muss deren Integrität und die Integrität der Hersteller überprüft werden können. Die Integrität/Authenzität der Hersteller lässt sich durch den Gebrauch von (Grid-)Zertifikaten feststellen, wie sie beispielsweise vom DGI zur Verfügung gestellt werden. Für Software gibt es das Konzept der *Software-Publishing-Zertifikate.* Dieses erlaubt es, die Integrität von Software von unabhängigen Stellen überprüfen zu lassen.

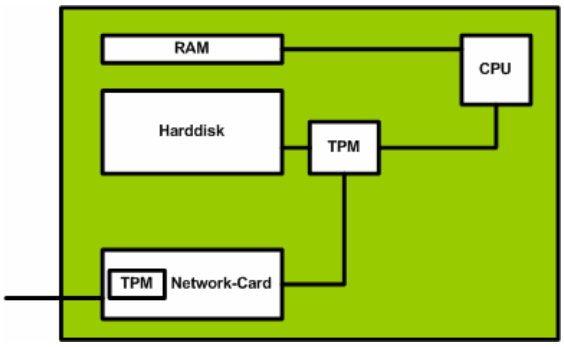

Abbildung 3 - Vereinfachte Abbildung. Der TPM-Chip befindet sich auf der Platine und sichert das System durch zusätzliche Methoden ab.

Neben diesen zentralen Lösungen bieten auch hier die Konzepte der TrustedComputingGroup (TCG) eine weitere Lösung für Integritätsprüfung von Software und kompletten Systemen. Durch den Einsatz von Hardware (TPM-Chip) am Anfang jeder lokalen Integritätsprüfung lässt sich die Integrität einer/s Applikation/Betriebssystem auf die Vertraulichkeit der verwendeten Hardware zurückführen. Ebenso kann durch den Einsatz von TPM geschützten Kommunikationskanälen die entfernte Integritätsüberprüfung von Applikationen und Systemen realisiert werden.

Durch die starke Unterstützung der TrustedComputingGroup in den letzten Monaten sind bereits viele dieser gesicherten Systeme ausgeliefert worden, und eine einsetzbare Unterstützung dieser Technik wird in Rahmen der In-Grid Laufzeit mit hoher Wahrscheinlichkeit erwartet.

5.4 Trust-Infrastrukturen zur Vertrauensbewertung

Zur sicheren und evtl. verteilten Speicherung von den bisher lokal gespeicherten Trustwerten lassen sich die P2P-Techniken aus 1.1 einsetzen.

Die bisherige Nutzung von manuell gepflegten Vertrauenstabellen könnte durch automatische Trust-Metriken ausgetauscht werden. Mögliche Datenquellen für die Trust-Metriken sind Accounting- und Billing-Daten.

6. Safety

6.1 Physikalische Absicherung von Daten in Grid-Umgebungen und dynamischen Grid-Umgebungen

Die Mitarbeit innerhalb der InGrid Gemeinschaft ist abhängig von der Nutzung gemeinsamer Datenbestände. Daten müssen für InGrid Benutzer zur Verfügung gestellt werden, um ihnen eine schnelle und zuverlässige Technikforschung zu ermöglichen.

Die Anforderungen an "Daten-Sicherheit" bei InGrid Daten hängen davon ab, wie Daten in den ingenieurwissenschaflichen Arbeitsprozessen verwendet werden.

Dieses Kapitel beschreibt die einzusetzenden Mittel, um den Verlust von Daten zu verhindern. Der Aspekt der Datensicherheit und der Zugriffssteuerung wird in anderen Teilen dieses Reports beschrieben.

6.1.1 Datenfluss

Die grundlegende Annahme ist, daß alle Daten, die in InGrid verarbeitet werden, auf zuverlässigen Speichersystemen abgelegt sind.

Die Daten werden mit den unterschiedlichsten, für InGrid Benutzer verfügbaren Rechnersystemen verarbeitet. So müssen Daten am Aufstellungsort der Rechner vor der Durchführung von Berechnungsschritten auf örtlichen Zwischenspeichersystemen zugänglich gemacht werden. Daten auf lokalen Speichermedien zur Verfügung zu stellen, ist in der Umgebung von Hochleistungsrechnern besonders notwendig, wenn die Zugriffsgeschwindigkeit auf die Daten den Rechenrozeß nicht verlangsamen darf.

Nach Vollendung der Berechnung müssen diese eben erzeugten Daten in Repositories eingestellt werden und können dann anderen Mitgliedern der InGrid Gemeinschaft und Kooperationspartnern zur Verfügung gestellt werden.

6.1.2 Eigenschaften von Datenobjekten

Ein einzelnes Datenobjekt, das im Datenrepository abgelegt ist, muß für alle rechnenden Prozesse identisch sein. So werden Datenobjekte (bit Dateien) einmal geschrieben und nie geändert. Die Datencharakteristik für alle Daten ist deshalb WORM (write once/ read multiple).

6.1.3 Anforderungen an die physikalische Datensicherheit

Wegen der Tatsache, dass die in den Datenrepositories enthaltenen Daten WORM-Charakteristik haben, brauchen die Daten nur gegen Datenträgerfehler geschützt zu werden. Es ist keine Versionierung von Daten erforderlich.

Die Repositories, die in der InGrid Umgebung benutzt werden, müssen diese Anforderung erfüllen und in Konsequenz Kopien der Datenobjekte auf unterschiedlichen Speichermedien ablegen. Beim Auftauchen einer fehlerhafte Datenkopie, muss diese Kopie durch eine neue ersetzt werden.

6.1.4 Anforderungen an die Datenreplikation

Die Datencharakteristik WORM ermöglicht eine Replikation von Daten ohne potentielle Probleme mit der Datenkohärenz. Einige Daten können als kritisch gelten in Bezug auf Datenübertragungzeiten oder die Zugriffsgeschwindigkeit des Speichersystems. Daten mit diesbezüglich erhöhten Anforderungen können in unabhängigen Repositories repliziert werden. Für jedes Repository gelten wieder die oben angeführten Sicherheitsmaßnahmen.

6.1.5 Zugriff auf Datenobjekte

Datenobjekte können im Umfeld numerischer Simulationen als flache Bitdateien betrachtet werden. Um diese Datenobjekte zu lokalisieren und korrekte Zugriffssteuerung zuzulassen, wird jedes Datenobjekt durch Metadaten beschrieben. Metadaten enthalten Informationen bezogen auf ein einzelnes Datenobjekt wie

- Eigentümer
- Typ der Datei
  Semantische Datenbeschreibung, Speicherort, Objektkennzeichnung, Informationen zu Zugriffsrechten
- Querverweise zwischen Dateien, z.B. Verknüpfungen zwischen Eingabedaten und Simulationsergebnissen
- Mehrere Metadateneinträge können auf das gleiche Datenobjekt zeigen.

Die Metadaten für ein Datenobjekt werden während des Einbuchungsprozesses erzeugt. Einige Metadaten können automatisch erzeugt werden; die meisten Metadaten jedoch müssen von einem einzelnen Benutzer erzeugt werden oder können als Teil des ingenieurwissenschaflichen Arbeitsablauf erzeugt werden.

6.1.6 Sicherheitsanforderungen für Metadaten

Wegen der Tatsache, dass Datenobjekte nur über Metadaten erreicht und zurückgeholt werden können, müssen grosse Anstrengungen unternommen werden, um die Beschädigung oder den Verlust von Metadaten zu verhindern. Eine Beschädigung oder ein Verlust von Metadaten bedeutet in Konsequenz, dass die zugehörigen Datenobjekte als verloren betrachtet werden müssen, obwohl sie physikalisch noch vorhanden sind.

Im Allgemeinen ist es nicht möglich, Metadaten und besonders semantische Informationen, aus den Datenobjekten zu rekonstruieren.

7. Single-Sign-On

Single-Sign-On in Unicore basiert auf der Verwendung von permanenten X.509-Zertifikaten. Diese Zertifikate werden sowohl für Authentisierung als auch für Autorisierung benutzt. Wenn ein Benutzer einen Job auf einer Ressource abgesetzt hat, überprüft der Unicore Gateway, ob sein Zertifikat gültig ist und durch eine vertrauenswürdige Certification Authority ausgegeben wurde. Der Benutzer wird dann nur autorisiert, die Ressource zu nutzen, wenn die sog. Unicore User Database (UUDB) ein Mapping seines Zertifikates auf einen gültigen Account auf der Ressource enthält. Der Accountname und die entsprechende UNIX uid/gid können bei jeder Site unterschiedlich sein. Daher muß sich ein Unicore-User nur ein einziges Paßwort merken, das er nur einmal beim Starten des Clients eingibt, um seine im Keystore enthaltenen Schlüssel für das Signieren seiner Jobs zu entsperren. Der User kann dann seinen Job bei den verschiedenen Unicore Sites submitten. Der Keystore kann ein oder mehrere Schlüsselpaare enthalten, so dass der User, falls er mehr als einen Schlüssel hat, lediglich darauf achten muss, den rechtigen Schlüssel zu wählen.

Unicore in Sites zu integrieren, die Globus als Middlewaresystem verwenden, wie es in heterogenen Grids erforderlich werden kann, oder Globus Services in eine Unicore Site zu integrieren, ist schwierig. Obwohl Security in Globus ebenfalls auf einer Public-Key-Infrastruktur basiert, um User wie Ressourcen zu authentifizieren, werden nicht (wie bei Unicore) signierte Objekte für die Jobübertragung verwendet. Stattdessen wird Proxydelegation verwendet, um Single-Sign-On Zugang zu den Globus Ressourcen zu ermöglichen. Ein sogenanntes "Proxy-Zertifikat" ist ein Standard X.509v3-Zertifikat, das einen unverschlüsselten Private Key, ein selbst-signiertes X.509 Zertifikat plus das von der Certification Authority signierte Zertifikat des Users enthält. Die Verwendung von Proxy-Zertifikaten erlaubt Trust-Delegation, die beispielsweise in Portal-Umgebungen nützlich ist, in denen eine Softwarekomponente Jobs absetzt anstelle des Users, der den ursprünglichen Job submittiert hatte. Um zu vermeiden, daß jemand, der unberechtigterweise im Besitz eines solchen Proxy-Zertifikate ist, permanent Jobs im Namen des Proxy-Zertifikat Inhabers absetzen kann, haben die Proxy-Zertifikate nur kurze Laufzeiten. Dennoch ist das Sicherheitsniveau im Vergleich zu Unicore niedriger.

Abhängig von den jeweiligen Anforderungen sind verschiedene Lösungen entwickelt worden, um Single-Sign-On-Funktionalität in Umgebungen mit Unicore und Globus zur Verfügung zu stellen:

- Die Lösung, die innerhalb des GRIP-Projektes entwickelt wurde, erlaubt das Senden von Jobs von einer Unicore Site (mittels des Unicore Clients) zu den Globus Sites. Hierfür wurde ein Zusatzmodul (Plugin) für den Unicore Client entwickelt, der entsprechende temporäre Globus Proxy-Zertifikate erzeugen kann, basierend auf permanenten Zertifikaten. Der Job wird mittels eines Extended Target System Interfaces vom Unicore Server zur Globus Site transferiert. Es ist nicht möglich, Jobs in der anderen Richtung zu senden, da die Globus Sicherheit niedriger ist als die PKI von Unicore [1].
- Explizite Trust-Delegation: in [2] wird diskutiert, wie das Unicore Sicherheitsmodell modifiziert werden kann, um Single-Sign-On Funktionalität mit erhöhter Flexibilität zur Verfügen zu stellen, indem Trusted Agents wie Server, Portale, Ressource-Broker oder Scheduler erlaubt wird, in einem Grid Jobs im Namen von Benutzern zu erzeugen…
- Das Web-Portal, das derzeit in der Joint Research Activity 2 des HPC Europa Projekts entwickelt wird, erlaubt es Usern, Jobs auf Ressourcen in vielen europäischen Supercomputing-Centren zu submittieren [3]. Ein Job, der in der Portalumgebung erzeugt wird, wird der darunterliegenden Middleware übergeben, die von dem jeweiligen Zentrum, an dem der Job ausgeführt werden soll, verwendet wird. Obwohl die Zentren unterschiedliche Middleware-Systeme verwenden (UNICORE, GRIA and Globus-based systems), soll das Absetzen von Jobs für den User so einheitlich wie möglich sein. Dafür wurden Middleware-Plugins entwickelt, die ein gemeinsames Interface basierend auf Standards wie der Job Submission Description Language JSDL [4] bereitstellen. Um Jobs zu submittieren muß der User ein Proxy-Zertifikat von einem MyProxy Server seiner Wahl

erhalten. Um Single-Sign-On Funktionalität zu ermöglichen, ist dies auch gewährleistet, wenn der User sich für eine Site entscheided, die unter einer Middleware wie Unicore betrieben wird, welche nur Jobs akzeptiert, die mit permanenten Zertifikaten signiert sind. Die aktuelle Implementierung des Portals mappt in diesem Fall die User-Credentials auf den User-Accountnamen der Remote Site. Hierfür wird ein einziges permanentes Schlüsselpaar verwendet, welches auf sichere Weise in dem Portal installiert ist, um Jobs aller User zu signieren. Der Account-Name wird dann dem signierten Unicore Job-Objekt hinzugefügt. Diese Lösung verlangt ein 1:n Mapping des Portal-Zertifikat-Eintrags in der UUDB auf die Account-Namen der Portaluser auf dem Remote Host. Dafür mussten die beteiligten Unicore-Sites die Standard-UUDB durch eine Implementierung des Forschungszentrums Jülich (FZJ-UUDB) ersetzen.
Diese Lösung hat verschiedene Schwächen in Bezug auf Sicherheit, Funktionalität und Skalierbarkeit. Um diese Situation zu verbessern, ist geplant, einen Unicore GSI-Gateway zu entwickeln, der Proxy-Zertifikate handeln kann. Portal-Jobs, die auf einer Unicore-Site laufen sollen, werden dann zum GSI-Gateway an Stelle des Standard-Gateways geschickt.

8. Juristische und Management-Fragestellungen

8.1 Security-Policies

8.1.1 Gesetzliche Regelungen

Die gesetzlichen Regelungen betreffen in der Regel personenbezogene Daten. In den Ingenieurwissenschaften spielen solche Daten nur in ganz seltenen Fällen eine Rolle. Deshalb wird diese Thematik im Projekt MediGrid untersucht, für das sie von zentraler Relevanz ist. InGrid wird im Bedarfsfall auf die dortigen Ergebnisse zugreifen.

8.1.2 Firmen-Policies

Eine kritisch gesetzliche Forderung für die ordentliche Buchführung ist, dass Geschäftsdokumente für 10 Jahre sicher aufgehoben werden müssen. Die technische Schwierigkeit bei elektronischen Dokumenten, wie sie im Grid genutzt werden, liegt darin, dass die digitalen Signaturen, die die Authentizität der Dokumente gewährleisten, auf kryptographischen Verfahren basieren. Kein bisheriges kryptographisches Verfahren hielt länger als 15 Jahre Angriffen stand. Somit ist es nicht möglich, auf ein einzelnes Verfahren zu setzen, um die Unveränderbarkeit über 10 Jahre zu schützen, da zum einen manche Verfahren sehr viel früher als die gemittelten 15 Jahre "geknackt" werden und zum anderen die industriell akzeptierten Verfahren meist schon einige Jahre alt sind. Stattdessen müssen duale Kryptoverfahren mit Signaturrotation entwickelt werden, um über lange Zeiträume den Zustand eines elektronischen Dokumentes zu verifizieren. Hierbei geht es darum, dass verschiedenartige Signaturverfahren kombiniert werden, wie z.B. Primzahlen basierte Verfahren mit Merkle-Signaturen. Immer wenn eine Verfahrensart geknackt wird, kann ein neues Verfahren ausgewählt und dem Dokument zugefügt werden, während die zweite noch bestehende Signatur weiterhin den Zustand des Dokumentes gewährleistet. Diese Signaturrotation sollte von der Middleware und dem Datenhaltungssystem transparent für den Nutzer übernommen werden.

In der Medizin kommen darüber hinaus noch alle Bereiche dazu, die mit Datenschutz und Schutz der Privatsphäre zu tun haben. Die Rahmenbedingungen in den Ingenieurwissenschaften sind somit eine deutlich eingeschränkte Teilmenge der in der Medizin greifenden Regelungen. Deshalb wird diese Thematik im CP MediGrid unter Einbeziehung von Inputs aus InGrid bearbeitet.

9. References

[1] GRIP project, http://www.grid-interoperability.org/

[2] D. Snelling, S. van den Berghe, V. Qian Li, “Explicit Trust Delegation: Security for Dynamic Grids” FUJITSU Sci. Tech. J., **40**,2, p.282-294, December 2004

[3] HPC-Europa project, http://www.hpc-europa.org

[4] Job Specification Description Language WG, https://forge.gridforum.org/projects/jsdl-wg/