Tagesordnung für den
2. D-Grid Security Workshop

27.-28. März 2007, Göttingen

Dienstag, 27. März 2007 (Moderation 1. Tag: Grimm)

ab 13:00 Kaffee

14:00 - 14:30 V11: Begrüßung, Darstellung der Ziele des Workshops u. Vorstellung Schwerpunkte 1. Tag

14:30 - 15:00 V12: *Towards More Flexible and Increased Security and Privacy in Grids*
(Herr Weisz - Universität Wien - Austrian Grid)

15:00 - 15:20 V13: Wo stehen wir – AAI, VO, Sonderinvestitionen (Herr Piger - RRZN Hannover - DGI)

15:20 - 15:50 Kaffee- und Kommunikationspause

15:50 - 16:10 V14: Der Einsatz von Shibboleth als Single-SignOn-System in wissenschaftlichen Bibliotheken
(Herr Ruppert - UB Freiburg - Vascoda)

16:10 - 16:30 V15: Aktuelle Entwicklungen zu GridShib (Herr Gröper - RRZN Hannover - IVOM)

16:30 - 16:50 V16: Aufbau einer Shibboleth-basierten Autorisierung im C3-Grid
(Herr Herr Makedanz - AWI Bremerhaven - C3)

16:50 - 17:10 V17: Status Einsatz von Firewalls in Grid-Umgebungen (Herr Volpato - RRZN Hannover - DGI)

17:10 - 17:30 V18: Application-Level-Gateway für das Globus Toolkit (Herr Metsch - DLR SISTEC)

17:30 - 17:50 V19: Shortcommings aktueller Grid-Middelwares bzgl. Datenschutz und Datensicherheit
(Herr Mohammed - Uni Göttingen - MediGRID)

17:50 - 18:10 V110:Zusammenfassung und Abschlussdiskussion

ab 19:00 gemeinsames Abendessen (Kartoffelhaus, Göttingen)

Mittwoch, 28. März 2007 (Moderation 2. Tag: Sax)

ab 08:30 Kaffee

09:00 - 09:15 V21: Vorstellung Schwerpunkte 2. Tag

09:15 - 09:45 V22: WS-Federation in TrustCoM und BREIN (Herr Geuer-Pollmann – EMIC - Microsoft)

09:45 - 10:05 V23: Virtualisierungstechniken (Herr Smith - Uni Marburg - InGrid)

10:05 - 10:25 V24: Aktueller Stand der CERT-Dienste im D-Grid (Herr Kossakowski - DFN-Cert Hamburg - DGI)

10:25 - 10:40 V25: VO-Management im AstroGrid mit VOMRS (Herr Enke - AIP - AstroGrid)

10:40 - 11:00 Kaffee- und Kommunikationspause

11:00 - 11:20 V26: Anforderungen an Zertifikate und Rechtemanagement (Herr Sax - Uni Göttingen - MediGRID)

11:20 - 11:40 V27: Security-Management bei OGSA-DAI und SRB (Frau Kottha - TU Dresden - MediGRID)

11:40 - 12:00 V28: SRM-dCache (Herr Synge - DESY - DGI)

12:00 - 12:20 V29: Anmerkungen/Wünsche/Fragen der neuen Communities

12:20 - 12:40 V210: Diskussionspanel

12:40 - 13:00 V211: Zusammenfassung und Abschluss des Workshops

anschließend Imbiss

Organisatorische Hinweise

Anmeldung bitte per Mail an:
medigrid@med.uni-goettingen.de , Betreff: [D-Grid] Security WS - Anmeldung

Veranstaltungsort: Hörsaal 04 der Georg-August-Universität Göttingen • Bereich Humanmedizin

Eine Anfahrtskizze finden Sie hier:
http://www.med.uni-goettingen.de/content/3115.html

und innerhalb des Gebäudes
http://www.med.uni-goettingen.de/content/3118.html

Der Hörsaal 04 befindet sich beim Aufzug D3 (Plan links oben)

Übernachtung:
Hotel am Papenberg
liegt genau gegenüber vom Klinikum

Sondertarif Klinikum = €80 mit Buchung bis zum 12.03.2007
(30 Zimmer geblockt)

Buchung: Kennwort MediGRID
Hermann-Rein-Strasse 2, Goettingen, 37075, DE
Phone: 49-551-30 550
Fax: 49-551-305 5400
book.bestwestern.com/bestwestern/productInfo.do

Alternativ:
Hotel Astoria

10 min Fußweg vom Klinikum, Bus zum Bahnhof

Sondertarif Klinikum = €70 incl. Frühstück mit Buchung bis zum 12.03.2006 (20 Zimmer geblockt)

Buchung: Kennwort MediGRID
Hannoversche Straße 51-53, 37075 Göttingen
Phone: 0551-30500
http://www.stadtplandienst.de/spd20/Map.aspx?sid=01ba00c9cb5e689328779b00b1b6eea4

Ggf. gibt es noch einzelne Zimmer zu €72,- im InterCity-Hotel Göttingen (ist voll)

Intercity Hotel Göttingen
Bahnhofsallee 1a
D-37081 Göttingen
Tel: 551/5 21 10
goettingen@intercityhotel.de
www.intercityhotel.de/intercityhotel/view/hotelinformationen/eng_goettingen.shtml

Abendveranstaltung

Ein gemütliches Abendessen ist im Kartoffelhaus, Goetheallee 8, Göttingen (Nähe Bahnhof) geplant.

http://www.stadtplandienst.de/spd20/Map.aspx?sid=01ba00c9cb5e689328779b00b1b6eea4

Ort: Obere Ebene

Menüvorschlag wird am Veranstaltungstag ausgereicht.

14:30 - 15:00 V12: Towards More Flexible and Increased Security and Privacy in Grids (Herr Weisz – Universität Wien – Austrian Grid)

Ausgehend vom Verständnis von Funktionen und daraus abgeleiteten Rechten werden die entsprechenden Konzepte und die Sicherung ihrer Einhaltung für virtuelle Organisationen im Grid vorgestellt. Besonderer Wert wird dabei auf die in VOs besonders wichtige Nachvollziehbarkeit der häufiger wechselnden Teilnehmer und ihrer Rollen. Dabei muss die Sicherheit immer auf dem höchstmöglichen Stand bleiben, soll Grid-Computing in Bereichen wie den der Biomedizin in Zukunft einsetzbar sein. Schon vorhandene Lösungsansätze und deren Aussichten werden besprochen.

15:00 - 15:20 V13: Wo stehen wir – AAI, VO, Sonderinvestitionen (Herr Piger - RRZN Hannover - DGI)

Der Vortrag gibt einen Überblick über den technischen Aufbau der aus den Sonderinvestitionen beschafften D-Grid Infrastruktur. Schwerpunkt ist der Bereich AAI und VO-Management. Weiterhin wird ein Ausblick auf mögliche Weiterentwicklungen der Infrastruktur gegeben.

Folgende Ziele sollen erreicht werden:

- Information über die beschaffte D-Grid Infrastruktur
- Konfiguration der AAI Komponenten für die drei eingesetzten Middlewares
- Struktur der Virtuellen Organisationen und technische Umsetzung
- Ausblick auf mögliche Erweiterungen der implementierten AA-Mechanismen

15:50 - 16:10 V14: Der Einsatz von Shibboleth als Single-SignOn-System in wissenschaftlichen Bibliotheken (Herr Ruppert - UB Freiburg - Vascoda)

Gerade im Bibliotheksbereich ist heute die Vernetzung der Angebote untereinander sehr hoch: Bibliographische Datenbanken verweisen auf elektronische Zeitschriften und diese wiederum über Zitate auf weitere Quellen. Die Nutzer erwarten in zunehmendem Maße den ortunabhängigen Zugang zu allen lizenzierten Ressourcen im Internet mit möglichst wenigen Barrieren. Da insbesondere auch internationale Verlage das Verfahren Shibboleth unterstützen lag es nahe, in diesem Bereich eine flächendeckende Implementierung von Shibboleth zu initiieren. Zum Aufbau und vor allem zum nachhaltigen Betrieb der für Shibboleth notwendigen Föderation konnte der DFN-Verein gewonnen werden. Diese Föderation steht allen Einrichtungen offen.
Der Vortrag stellt die Sicht der Bibliotheken auf Shibboleth dar und berichtet auch über den aktuellen Stand der Gründungsarbeiten zur deutschen Föderation DFN-AAI. Sowohl der DFN-Verein als auch das Projekt AAR stellen Testumgebungen zum Aufbau einer eigenen Shibboleth-Infrastruktur zur Verfügung.

16:10 - 16:30 V15: Aktuelle Entwicklungen zu GridShib (Herr Gröper - RRZN Hannover - IVOM)

Zukünftige Grid-AAIs sollten nutzerspezifische Attribute von bestehenden oder zurzeit im Aufbau befindlichen Shibboleth Föderationen verwenden können. Insbesondere Attribute wie die Nationalität oder Mitgliedschaft in einer organisatorischen Einheit sollten für die Verwaltung von Virtuellen Organisationen nicht neu erhoben und verwaltet werden müssen. Die vier im Rahmen des Globus Projektes entwickelten GridShib Komponenten sind das Bindeglied zwischen der SAML-basierten Shibboleth Welt und der Grid Security Infrastructure mit ihren X.509 Zertifikaten:

- GridShib CA: Online CA für die Ausstellung von „Short Lived Certificates“
- SAML Tools: Abfragen von SAML Assertions und Einbinden in X.509 Zertifikate
- GridShib for Globus: PDP für webservicebasierte Globuskomponenten
- GridShib for Shibboleth: Zusatzmodul für Shibboleth IdPs für Attribute Query durch GS for Globus.

In dem Vortrag soll der GridShib Ansatz und die vier Komponenten kurz vorgestellt werden und anschließend mögliche Architekturansätze für eine GridShib basierte AAI im D-Grid diskutiert werden.

16:30 - 16:50 V16: Aufbau einer Shibboleth-basierten Autorisierung im C3-Grid (Herr Herr Makedanz - AWI Bremerhaven - C3)

Das Community Projekt C3-Grid plant im Laufe dieses Jahres den Aufbau einer Grid-Testumgebung mit Shibboleth-basierter Authentifizierung und Autorisierung. Diese Testumgebung wird neben GridSphere, dem Globus Toolkit und den C3-Grid-spezifischen Metadaten-Mechanismen auf dem GridShib-Anwendungsfall für ein Teragrid Science Gateway basieren. Es soll gezeigt werden, dass auf einem zentralen Portal generierte Proxy-Zertifikate mit integrierten SAML Assertions in einem Produtions-Grid zur Autorisierung auf den Ressourcen genutzt werden können. Die Bausteine und die Roadmap für diesen Ansatz werden vorgestellt.

16:50 - 17:10 V17: Status Einsatz von Firewalls in Grid-Umgebungen (Herr Volpato - RRZN Hannover - DGI)

Dieser Vortrag präsentiert zwei unterschiedliche Themenbereiche im FG 3-5 des DGI:

- eine Empfehlung für den Einsatz von Firewalls in Grid Umgebungen am Beispiel der D-Grid Sonderinvestitionen, die Problematik mit GridFTP Verbindungen zu den Worker Nodes (hochladen/unterladen von input/output Dateien) und eine mögliche Lösung für dieses Problem;
- die Anforderungen der Ressourcen-Anbieter und Nutzer über Hochleistungsfirewalls und die gewonnen Erfahrungen während der ersten Tests.

17:10 - 17:30 V18: Application-Level-Gateway für das Globus Toolkit (Herr Metsch - DLR SISTEC)

Zum sicheren Zugriff auf Grid-Ressourcen, die nur durch eine Firewall hindurch erreichbar sind, wird bei DLR SISTEC ein Security Proxy für Grid Services entwickelt. Dieser Proxy überprüft und verifiziert alle eingehenden Service-Anfragen von außenstehenden Grid-Clients (aus dem Internet) und leitet die gültigen Anfragen weiter an die Grid Services im internen Netzwerk (durch Firewall geschütztes Intranet). Der Proxy wertet die einzelnen Anfragen (SOAP Requests) auf Applikations-Ebene aus und er agiert wie ein Grid ("Proxy Grid") gegenüber Clients im Internet und entsprechend wie ein Grid-Client gegenüber den Ressourcen im Intranet.

17:30 - 17:50 V19: Shortcomings aktueller Grid-Middlewares bezüglich Datenschutz und Datensicherheit (Herr Mohammed – Georg-August-Universität Göttingen – MediGRID)

Die Analyse des Grid Security Infrastructure (GSI) in Globus Middleware bzw. die Analyse zusätzliche Plugins (z.B. OGSA-DAI, SRB) zeigt Mängel in der Erfüllung einiger Sicherheitsanforderungen. Ziele dieses Vortrages sind,

- die Anforderungen aus Sicht des Datenschutzes und der Datensicherheit kurz zu erläutern,
- was GSI und die zusätzliche Plugins bieten und welche Anforderungen noch zu erfüllen sind, zu diskutieren, sowie
- einen Ausblick und Lösungsmöglichkeiten zu formulieren.

09:15 - 09:45 V22: WS-Federation in TrustCoM und BREIN (Herr Geuer-Pollmann – EMIC - Microsoft)

In diesem Vortrag wird ein Überblick über die "web services security"-Mechanismen gegeben, die im FP6 Projekt TrustCoM verwendet werden sowie über geplante Erweiterungen, die im Rahmen des FP6 Projektes BREIN Einzug halten sollen. Dieser Überblick beinhaltet das Setup der Web Services

Federations, d.h. der Sicherheitskonfiguration für Virtuelle Organisationen, die Interaktion zwischen den Sicherheitskomponenten, sowie den Aufbau des "Security Token Service" (STS), dessen Entwicklung das European Microsoft Innovation Center (EMIC) im Rahmen von TrustCoM begonnen hat.

09:45 - 10:05 V23: Virtualisierungstechniken
(Herr Smith – Universität Marburg - inGrid)

In diesem Vortrag wird der Erfahrungsbericht zur Integration von Virtualisierungstechniken in Globus Toolkit 4 und der Sun Grid Engine, aus dem InGrid Projekt, vorgestellt. Basierend auf dem X509 Benutzerzertifikat werden die Grid Job Daten aus einer DMZ in das geschütze Cluster Netz übertragen. Dort wird eine benutzerspezifische Virtuelle Maschine gestartet um die Daten zu empfangen und den Grid Job zu berechnen. Die Rechte der Virtuellen Maschine werden benutzerspezifisch gesetzt. Nach Beendigung des Jobs werden die Daten aus der Virtuellen Umgebung zurück in die DMZ übertragen und die Virtuelle Maschine zerstört und sicher gelöscht.

10:05 - 10:25 V24: Aktueller Stand der CERT-Dienste im D-Grid
(Herr Kossakowski - DFN-Cert Hamburg - DGI)

Die etablierten Dienste und Strukturen des DFN-CERT wurden im Rahmen des DGI Fachgebiets 3 auf Grid-spezifische Anforderungen erweitert. Dies bezieht sich u.a. auf die nationale und internationale Koordination und Kooperation in Gremien wie CERT-Verbund (Deutschland), TF-CSIRT (Europa) und FIRST (Welt).
Ein weiterer Aspekt ist, Vorfälle frühzeitig zu erkennen. Dazu werden etablierte Frühwarnsysteme/Intrusion-Detection Systeme zu Grid-Sensornetzwerken ausgebaut.
Eine Hotline für Grid-spezifische Meldungen nimmt nicht nur Vorfallsmeldungen entgegen sondern beantwortet auch Sicherheitsfragen aus den Communities.
Im Sommer 2007 wird ein Grid-CERT Tutorium angeboten. Vorgesehen sind Themen wie die Grundabsicherung von Unix-Diensten, PKI-Grundlagen für Grids und Vorfallsbearbeitung in Grids. Auf der Basis der Untersuchungen von Grid- Software werden außerdem Sicherheits-Besonderheiten in Grid-Software behandelt.

10:25 - 10:40 V25: VO-Management im AstroGrid mit VOMRS
(Herr Enke - AIP - AstroGrid)

Im AstroGrid-D ist ein auf VO-Management entwickelt worden, welches aus drei Komponenten besteht:

- VOMRS-Server für das Zertifikats-Management
- Query-Interface für das Update der lokalen GridMaps
- LocalGridMap-Management inklusive des User-Managements

Diese Lösung gestattet es, flexible Abbildung der VOs auf lokale Gruppen einzurichten, und so Anforderungen zu erfüllen, die zB den Zugriff auf spezielle Hardware über VOs zu steuern.

11:00 - 11:20 V26: Anforderungen an Zertifikate und Rechtemanagement
(Herr Sax – Georg-August-Universität Göttingen - MediGRID)

Seitens der medizinischen Community werden besondere Anforderungen an Authentifizierung und Autorisierung gestellt. Bezüglich der zertifikatsbasierten Authentifizierung wird derzeit in Deutschland eine Infrastruktur mit Heilberufsausweisen für Ärzte, Apotheker und weitere Personengruppen ausgerollt, die mit in die biomedizinische Gridwelt einbezogen werden muss.
Bezüglich der Autorisierung liegen datenschutzseits Anforderungen vor, dass die Zugriffsrechte bezogen auf einzelne Datensätze und Dokumente (a) erteilt und (b) überwacht werden müssen. Perspektivisch werden auch Zugriffsrechte innerhalb strukturierter XML-Dokumente benötigt.

11:20 - 11:40 V27: Security-Management bei OGSA-DAI und SRB (Frau Kottha – TU Dresden - MediGRID)

Providing security and authorizations for data, which is stored either in relational databases or in flat file systems in a distributed computing environment like Grid, is a quite challenging issue. In this presentation, how the security and authorizations are provided by important Grid data management tools such as OGSA-DAI and SRB, will be discussed. The security holes that need to be closed to ensure the data integrity will be discussed as well.

11:40 - 12:00 V28: SRM-dCache - dCache and its Security models development (Herr Synge - DESY - DGI)

dCache was initially used as a single site disk cache for Mass Storage Systems for Unix computing farms. Dcache has since been developed as a mass deploy able solution for the LHC computing grid, transforming the requirements in the areas of authentication, authorization, auditing and accounting. This talk focuses upon the previous and current developments of dCache in these areas and illustrates the evolving nature of security. Authentication has transformed from rsh and GSI to VOMS/SAML and AuthZ. Authorization is changing from from Unix permissions to NFSv4 ACL's. Auditing and accounting has changed from log files to an RDBMS databases. These transformations are required as grid services allow storage to be served globally while organization responsibility remains local in a Grid environment.