

3. D-Grid Security-Workshop Göttingen 1. und 2. April 2008



Tagesordnung 2. April 2008

09:00 - 09:15	V21	Vorstellung Schwerpunkte 2. Tag
09:15 - 10:00	V22	Keynote: Secure Hypervisor Thomas Rueter, IBM Northeast Europe
10:00 - 10:15	V23	Diskussion
10:15 - 10:45		Kaffee- und Kommunikationspause
10:45 - 11:15	V24	Service-Zertifikate und Portal Security Ulrich Sax, Jürgen Falkner, UMG, FhG IAO - MediGRID
11:15 - 11:45	V25	Data Management and Security Andreas Landhäußer - T-Systems SfR - InGrid
11:45 - 12:15	V26	SAML – Create and Exchange Security Information in Grids Morris Riedel, FZ Jülich – OMI I Europe
12:15 - 12:45	V27	Diskussionspanel Zusammenfassung und Abschluss des Workshops

Keynote: Secure Hypervisor



Thomas Rueter

IBM Sales leader STG Infrastructure Solutions Northeast Europe

Thomas Rüter hat Physik in Heidelberg studiert bevor er 1995 zu IBM kam. Er war mehrere Jahre als Senior IT Architect im IT-Service tätig. Als Business-Development Manager hat er Infrastruktur-Lösungen entwickelt und vertrieben. Er leitete die IBM Grid Computing Aktivitäten in der Region Central (DACH).

Seit 2005 verantwortet er den Infrastruktur Lösungsvertrieb für Europa. Dabei liegt ein Focus auf Grids, Virtualizations Engine, Cell Computing und Infrastruktur-Lösungen.

http://www.research.ibm.com/secure_systems_department/projects/hypervisor/

3. D-Grid Security-Workshop Göttingen 1. und 2. April 2008

Tagesordnung 2. April 2008

09:00 - 09:15	V21	Vorstellung Schwerpunkte 2. Tag
09:15 - 10:00	V22	Keynote: Secure Hypervisor Thomas Rueter, IBM Northeast Europe
10:00 - 10:15	V23	Diskussion
10:15 - 10:45		Kaffee- und Kommunikationspause
10:45 - 11:15	V24	Service-Zertifikate und Portal Security Ulrich Sax, Jürgen Falkner, UMG, FhG IAO - MediGRID
11:15 - 11:45	V25	Data Management and Security Andreas Landhäußer - T-Systems SfR - InGrid
11:45 - 12:15	V26	SAML – Create and Exchange Security Information in Grids Morris Riedel, FZ Jülich – OMI I Europe
12:15 - 12:45	V27	Diskussionspanel Zusammenfassung und Abschluss des Workshops

3. D-Grid Security-Workshop

D i s k u s s i o n s p a n e l

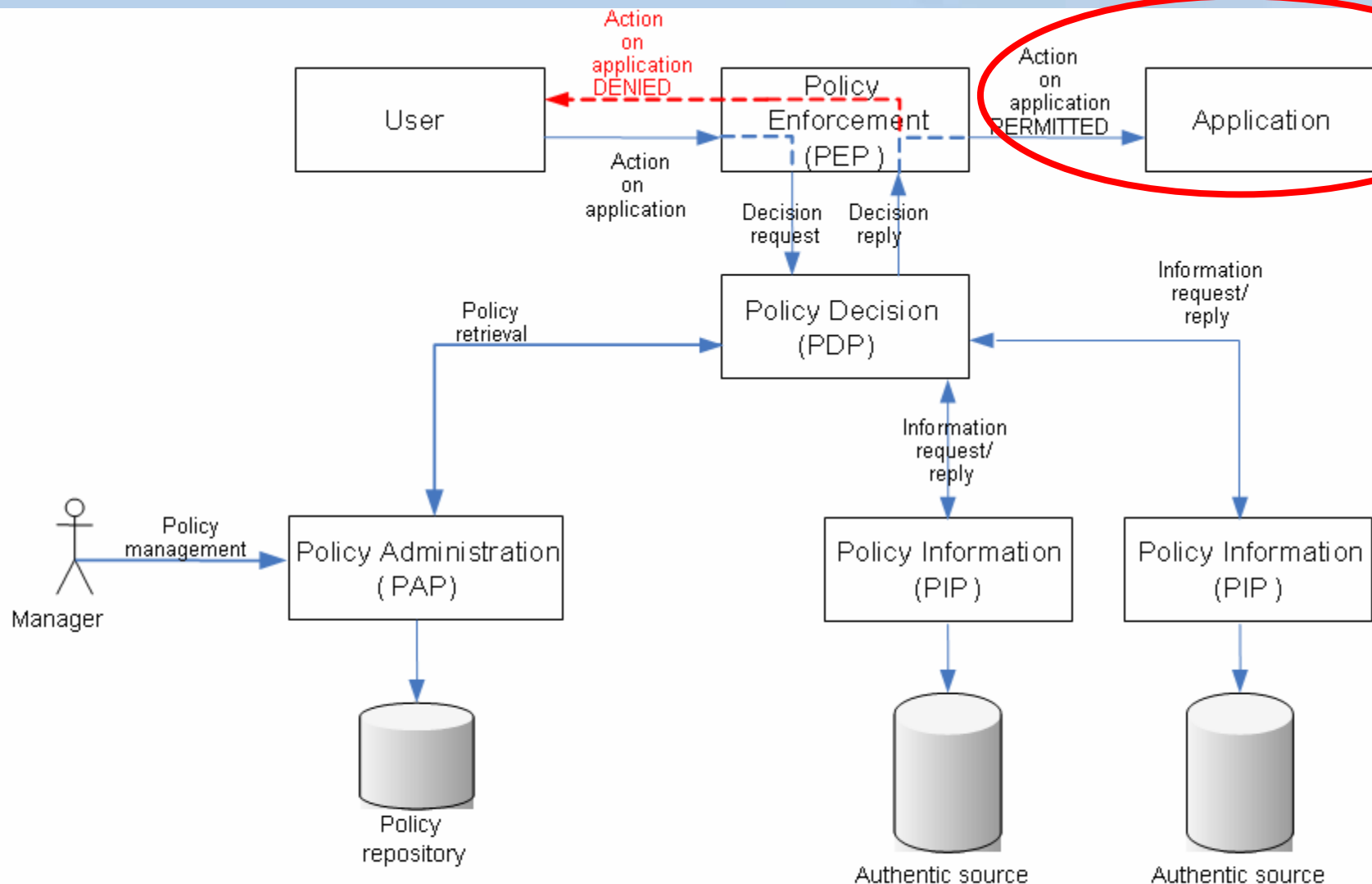
„Enhanced Security“ AP InGrid/MediGRID/DGI

- **Audit:** a posteriori Logs. Data provenance und data annotation (Prozessschritte).
- **Trackability:** a priori Kenntnisse bzw. Richtlinien wo Datentransport, Transaktionen, Berechnungen und Speicherung von personen- bzw. patientenbezogenen Daten stattfinden.
- **feingranulare Zugriffsrechte:** Zugriffsrechte und Zugriffskontrolle sollen nicht nur auf Fileebene erfolgen, sondern auch innerhalb eines Formulars bzw. Datensatzes.
- **Vertraulichkeit:** parallel den Anforderungen bei den Zugriffsrechten muss auch Vertraulichkeit entsprechend feingranular erfolgen können.
- **Trust und Trust Delegation:** nicht nur für Software-Instanzen, sondern auch auf Ebene von Personen und Organisationen ist erforderlich.
- **Safety:** Physikalische Absicherung von Daten in Grid-Umgebungen und dynamischen Grid-Umgebungen (Policy-based storage, Querbezug zu Daten- und Informationsmanagement)

„Hausaufgaben“ der bisherigen Security-Workshops

2005	Getting Started (Zertifikate, Firewalls etc.)
2006	Authentifizierung
2007	Shortcomings → Autorisierung, feingranular
2008+	?

Policy enforcement model



Zusammenfassung feingranulare Zugriffsrechte

bislang unterstützte Granularität: eine Datei

→ RBAC-Ansatz, OS-Niveau (rwx), Storage-MW [SRB]: rwxnn

MediGRID-Anwendungen jetzt: physikalische Trennung von Daten (Bild) von Metadaten (Patientendaten)

gesucht: Unterstützung einer feingranularen Zugriffskontrolle für strukturierte Dokumente

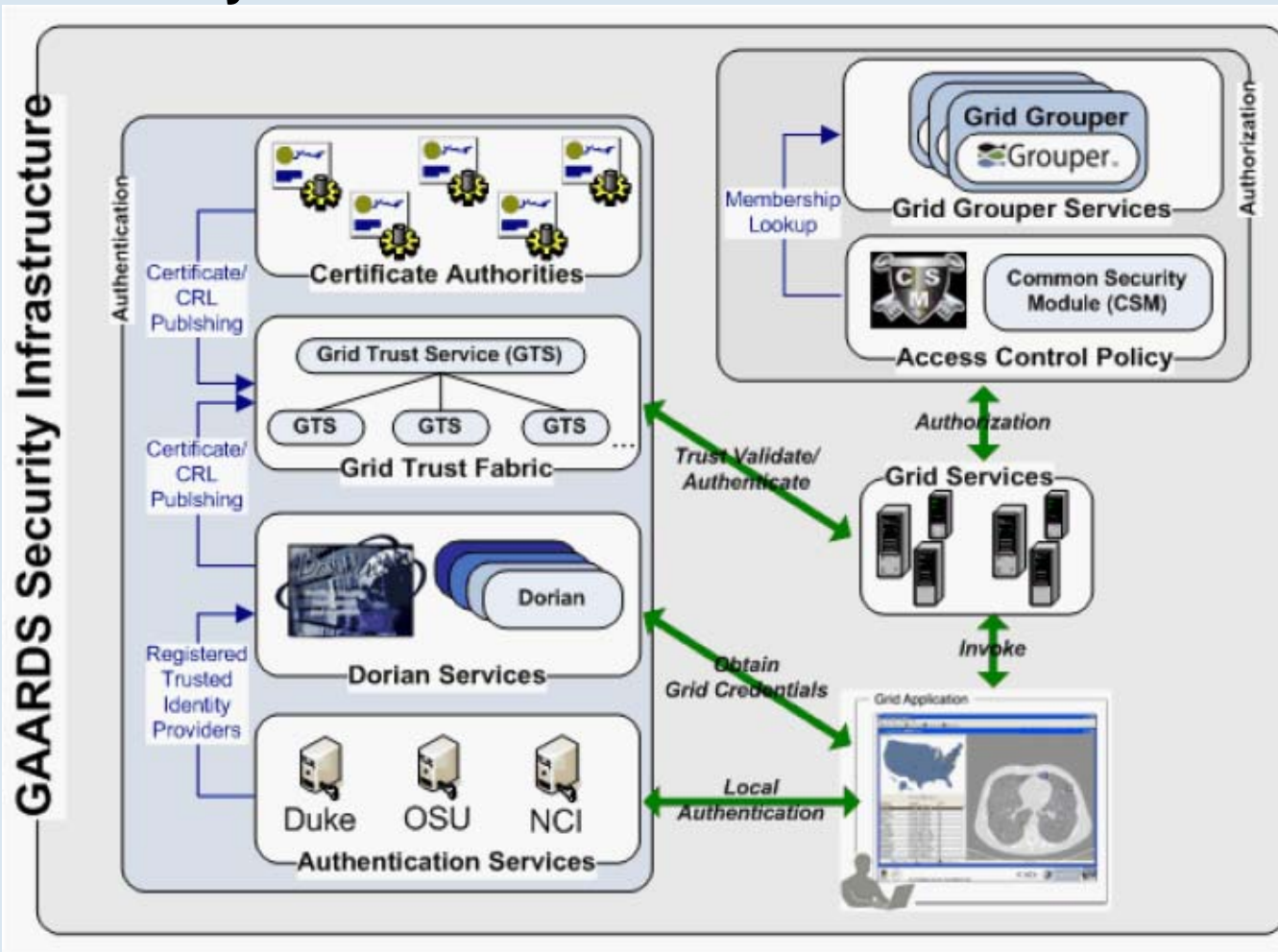
beachten: "Allmacht" der Administratoren

→ Multi-Level-Security-OS, SELinux?

Fazit zu Audit und Tracking

- ➔ Wir benötigen bei kritischen Anwendungen diese Audit-Fähigkeit!
- ➔ Wir benötigen Vorgaben, wie Auditing in solchen Anwendungen in D-Grid auszusehen hat!
- ➔ Einigung auf D-Grid-Standards und Standardverfahren zum Austausch von Audits notwendig
- ➔ Wir benötigen (die Entwicklung von) Audit-Tools für verteilte (Grid-) Systeme
- ➔ Rechtliche Herausforderung:
 - wie schafft man es, dass Grid-weite Audittrails möglich werden?
- ➔ Es sollte möglich sein, WF-Systemen und Resource Brokern in D-Grid Anforderungen bzgl. Tracking über ein Standard-Interface mitzuteilen (z.B. über die Ressourcenbeschreibung)
- ➔ Die Umsetzung und Durchsetzung von Role-based Access und feingranularem Rechtemanagement ist eine Grundvoraussetzung für Tracking

Internationality caBIG security



*Oster S, Foster I, Shanbhag A, Langella S, McConnell P, Hastings S, Wellborn D, Ervin D, Bragg V, Kurc T, Kumar V, Saltz J, Phillips J, Madduri R, Chilukuri R, Gawor J, Akkala S, Siebenlist F, Kher M, Wilde M, Erickson-Hirons W, Kettimuthu R, Manisundaram A, Allcock B, Komatsoulis G. *caGrid 1.0 USER'S GUIDE*

Ziele einiger D-Grid II-Projekte

- **Senken der Eintrittsschwelle zur Nutzung von Grid-Ressourcen** durch neue Communities der Life Sciences und verwandten Gebieten
- **Etablieren von Service-Modellen** für Life Sciences einschließlich Preismodellen, Accounting und Billing unter Berücksichtigung der besonderen Anforderungen an den Datenschutz
- **Einbinden von Service-Providern aus der Industrie**, welche als professionelle Service-Provider und / oder auch selbst als Service-Customer auftreten können
- **Umsetzen von Geschäftsmodellen durch Einbinden von KMU**, um Unabhängigkeit von öffentlicher Förderung zu erreichen

„Hausaufgaben“ der bisherigen Security-Workshops

2005	Getting Started (Zertifikate, Firewalls etc.)
2006	Authentifizierung
2007	Shortcomings → Autorisierung, feingranular
2008+	Virtualisierung + ?

„Hausaufgaben“ der bisherigen Security-Workshops

2005	Getting Started (Zertifikate, Firewalls etc.)
2006	Authentifizierung
2007	Shortcomings → Autorisierung, feingranular
2008+	Virtualisierung + ?
	Offene Punkte:
	<ul style="list-style-type: none"> • „belastbarer“ Betrieb der Sicherheitsinfrastruktur • nachhaltiger Betrieb der Sicherheitsinfrastruktur • verbindlicher Betrieb der Sicherheitsinfrastruktur <ul style="list-style-type: none"> ➤ Accounting (technisch, fachlich) ➤ Audit (intern, extern, Beweiskraft) ➤ Tracking (– Workflow – Broker) ➤ Zertifikate (GridPMA vs. SigG)

3. D-Grid Security-Workshop Göttingen 1. und 2. April 2008