



# Services und Unterstützung für die D-Grid Communities

DGI FG3: „Netze und Sicherheit“

Workshop „Service Grids in F&E“

Kassel, 24. Oktober 2006

Marcus Pattloch, DFN-Verein

- **FG3 „Netze und Sicherheit“**
  - FG 3-2: Erweiterung der Netzplattform um D-Grid spezifische Elemente
  - FG 3-3: Alternative Transportprotokolle
  - FG 3-4: Aufbau einer AA-Infrastruktur für das D-Grid
  - FG 3-5: Entwicklung und Einsatz von Firewallkonzepten in Grid-Umgebungen
  - FG 3-6: Grid-spezifische CERT-Dienste
- **Teilnehmende Einrichtungen**
  - FH Aachen, RWTH Aachen, DFN-Verein Berlin, FhG SIT Darmstadt, Leibniz Uni Hannover, FZ Jülich, TU Kaiserslautern, FZ Karlsruhe, Uni Karlsruhe

- **FG 3-2: Erweiterung der Netzplattform um D-Grid spezifische Elemente**
  - Wissenschaftsnetz (X-WiN) als allgemeine Netzplattform
  - zusätzlich Bedarf an speziellen Netzlösungen (VPN)
  - Konzepte und Umsetzung auf Basis der Anforderungen im D-Grid (Communities, Virtuelle Organisationen)

- **Bisherige Arbeiten**

- Aufnahme Netzbedarfe aller Communities
- Zusammenfassung dazu im Halbjahresbericht

- **Nächste Schritte**

- Konkretisierung der VPN-Bedarfe mit C3, InGrid und AstroGrid (ab 10.2006)
- Planung des HEP-T2/T3-Netzes
- Entwurf eines HEP-VPN mit Anbindung an GridKA
- Konkretisierung der Bedarfe von MediGrid, TextGrid, WISENT nach Konsolidierung der Planung in den Communities (ab 12.2006)

- **FG 3-3: Alternative Transportprotokolle**

- Bewertung existierender alternativer Transportprotokolle hinsichtlich Performance und Stabilität
  - Betrachtung bis 10 Gigabit Ethernet
- Empfehlungen für den effizienten Einsatz von Transportprotokollen im D-Grid
  - Auswahl der Transportprotokolle
  - Geeignete Wahl von Parametern in Betriebssystemen und Applikationen

- **Bisherige Arbeiten**

- Analyse von TCP-Varianten und UDP-basierten Transportprotokollen
- Analyse der Fairness alternativer Transportprotokolle in High-Performance-Netzen
- Empfehlungen zur Konfiguration von Betriebssystemparametern in High-Performance-Netzen

- **Nächste Schritte**

- Untersuchung des Einsatzes UDP-basierter Transportprotokolle in Grid-FTP

- **FG 3-4: Aufbau einer AA-Infrastruktur für das D-Grid**
- Authentifizierung (A1) vs. Autorisierung (A2)
  - A1: globale (!) Bestätigung der Identität, z.B. von Nutzern, Rechnern, Diensten, Daten
  - A2 : lokale (!) Steuerung der Zugriffsmöglichkeit auf Ressourcen

- **Ausstellung von Zertifikaten für das D-Grid**
  - fast alle Grid-Anwendungen benötigen Zertifikate
  - Grid-Zertifikate im Rahmen der EUGridPMA
  - in Deutschland zwei „Dienstleister“ (FZK, DFN)
  - Aufsetzen von Grid-RAs
  - die (Pilot)Dienstleistung ist etabliert
- **Kontakt**
  - entweder direkt zu FZK oder DFN
  - oder per E-Mail an: **zertifikate@d-grid.de**

- **Bericht: Analyse von AA-Infrastrukturen in Grid Middleware**
  - Globus Toolkit 4
  - LCG/gLite
  - UNICORE
- **Bericht: Use Cases for Authorization in Grid-Middleware**
  - Ansätze für übergreifende Autorisierung in Grids

- **Interviewbogen für die Gespräche mit den D-Grid Communities**
  - verwendete Middleware
  - VO-Konzept
  - Authentifizierung
  - Autorisierung
    - Use Cases: compute / data / information services
- **Status: Interviews wurden durchgeführt oder Termine sind vereinbart**

- **FG 3-5: Entwicklung und Einsatz von Firewallkonzepten in Grid-Umgebungen**
  - Firewalls in Hochgeschwindigkeitsnetzen (Durchsatzraten im Bereich mehrerer Gbit/s)
  - Analyse der Kommunikationseigenschaften typischer D-Grid Anwendungen
  - Empfehlungen für statische Firewall-Konfigurationen
  - Untersuchung Ansätze zur dynamischen Konfiguration von Firewalls.

- **Bisherige Arbeiten**

- Empfehlungen zur statischen Konfigurationen von Firewalls für Globus Toolkit 2, Globus Toolkit 4 und Unicore
- Untersuchung von aktuellen Implementierungen dynamischer Firewalls
- Firewall-freundliche Einsatzmodelle für Globus Toolkit 4

- **Internationale Aktivitäten**

- Teilnahme in OGF (Open Grid Forum) Firewall Issues Research Group

- **FG 3-6: Grid-spezifische CERT-Dienste**
  - Computer Notfallteams im „klassischen“ Internet seit Jahren etabliert
  - Aber: neue Themen in Grids, z.B. spezielle Grid-Anwendungen und Grid-Middleware (Globus, UNICORE, ...)
  - Pilotierung von CERT-Diensten in Grid-Umgebungen
  - CERT-Ansprechpartner für Prävention und Reaktion im Bereich Grid-Sicherheit

- **Etablierung des Themas Grid-CERT in wichtigen Arbeitsgruppen**
  - europäische TERENA Task Force CSIRT
  - deutscher CERT-Verbund
- **Erweiterung existierender Informationsinfrastrukturen**
  - Nutzung „klassischer“ CERT-Strukturen
    - Grid-Advisory auf Bugtraq (20. 10. 2006)
  - Kontakt zu Herstellern

- **Untersuchung Grid-Software**
  - (vorher abgesprochene) Pentests gegen Grid-Testbed der Leibniz Uni Hannover
  - div. Scans und DDOS-Angriffe
- **Nächste Schritte**
  - (Grid) Sicherheitstutorium
  - Pilot-Hotline für Grid-relevante Vorfälle

- **DGI FG3: Unterstützung der Communities in den Bereichen Netz und Sicherheit**
- **Ansprechpartner: Christian Grimm (LUH)**
  - Transportprotokolle
  - Firewalls
  - AAI - Autorisierung
- **Ansprechpartner: Marcus Pattloch (DFN)**
  - Netzplattform / VPNs
  - Grid-CERT
  - AAI - Authentisierung / Zertifikate