

Tagesordnung für den 3. D-Grid Security Workshop



01.-02. April 2008, Göttingen, Universitätsmedizin

Dienstag, 01. April 2008

ab 12:00 Mittag und Kaffee

13:00 - 13:15 V11: Begrüßung, Darstellung der Ziele des Workshops u. Vorstellung Schwerpunkte 1. Tag Überblick über Techniken und Lösungen im Rahmen der ersten D-Grid Projekte - Review

13:15 - 15:00 V12: *Grid Security Tutorial – Ein Tag im Leben eines Grid-Jobs“*
(Herr Grimm/ Herr Weisz – Leibniz Universität Hannover/Universität Wien – DGI/ AustrianGrid)

15:00 - 15:30 Kaffee- und Kommunikationspause

15:30 - 16:15 V13: Sicherheitsanforderungen der neuen Communities
(Moderation und Überblick: Frau Roller - HLRS - InGrid)
mit den Communities *ProGrid* (Horst Schwichtenberg oder Daniel Rubin),
Services@MediGRID (Frank Dickmann) und *MedInfoGrid* (Andreas Thiel)

16:15 - 16:45 Kaffee- und Kommunikationspause

16:45 - 17:45 V14: Bisherige Ergebnisse aus D-Grid I (Herr Pattloch/ Smith – DFN/ Uni Marburg – DGI/ InGrid)
Blockvortrag (Zusammenfassung D-Grid I und Ausblick auf D-Grid II, Inhalt sind Zertifikate, Virtualisierung, u.s.w.), Video (evtl. Live-Demo)

17:45 - 18:00 V15: Zusammenfassung und Abschlussdiskussion

ab 19:00 gemeinsames Abendessen

Mittwoch, 02. April 2008

ab 08:30 Kaffee

09:00 - 09:15 V21: Vorstellung Schwerpunkte 2. Tag Neue Themen und Methodiken für die D-Grid II Projekte

09:15 - 10:00 V22: Keynote: Secure Hypervisor (Herr Rueter, IBM Deutschland)

10:00 - 10:15 V23: Diskussion

10:15 - 10:45 Kaffee- und Kommunikationspause

10:45 - 11:15 V24: Service-Zertifikate (Herr Sax/ Falkner – UMG/ IAO - MediGRID)

11:15 - 11:45 V25: Data Management and Security (Herr Landhaeusser - T-Systems Sfr Goettingen)

11:45 - 12:15 V26: SAML – Create and Exchange Security Information in Grids (Herr Riedel – FZ Jülich)

12:15 - 12:45 V27: 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 Universitätsmedizin Göttingen der Georg-August-Universität

Eine Anfahrtsskizze 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)

Einrichtung und Nutzung des WLAN

<http://www.wlan.med.uni-goettingen.de/>

Übernachtung:

Hotel am Papenberg

liegt genau gegenüber vom Klinikum

Sondertarif Klinikum = €80 mit Buchung bis zum 17.03.2008
(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

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

Intercity Hotel Göttingen

Sondertarif Klinikum = €72 mit Buchung bis zum 17.03.2008
(20 Zimmer geblockt)

Buchung: Kennwort MediGRID

Bahnhofsallee 1a

D-37081 Göttingen

Tel: 551/5 21 10

goettingen@intercityhotel.de

www.intercityhotel.de/intercityhotel/view/hotelinformationen/eng_goettingen.shtml

Abendveranstaltung

La Hazienda, Weender Landstr. 23, 37073 Göttingen

**13:15 - 15:00 V12: Grid Security Tutorial
(Herr Christian Grimm - RRZN - DGI)**

Authentication, authorization and access control are key security functionalities of most Grid middlewares deployed in several international projects. In current Grid environments, authentication of users and services is strictly based on Public Key Infrastructures (PKI) and X.509 end-entity certificates, which replace legacy mechanisms such as resource-local username/password authentication. Authorization instead is based on a variety of mechanisms, ranging from static file mappings to tokens and embedded attributes.

This tutorial illustrates the principles of authentication and authorization for Grid environments, as provided by the Grid Security Infrastructure (GSI) included in the Globus Toolkit. Additionally, we demonstrate by examples of real Grid jobs essential security functionalities like Single Sign-On (SSO) for users and delegation of user rights to Grid services.

**16:45 - 17:45 V14: Bisherige Ergebnisse aus D-Grid I
(Herr Pattloch/ Smith – DFN/ Uni Marburg – DGI/ InGrid)**

The talk gives a general overview of security related activities starting with the results from D-Grid 1 and giving an outlook on D-Grid 2. Some of the activities have led to services within D-Grid, some have given recommendations for D-Grid users and sites and others have laid the foundation in D-Grid 1 that is now extended in D-Grid 2.

To give a concrete example of this process a demonstration of the developed virtualisation security infrastructure will be given. In a practical demonstration a new virtual Grid image will be created, and an application will be installed with root privileges. This image will be deployed onto a Grid site and will be used to create a custom virtual machine. A job will be submitted and executed in this secure Grid environment. The talk closes with a development perspective for the planned security infrastructure for D-Grid 2 business applications.

**11:00 - 11:30 V24: Service-Certificates/ Portal-based Security
(Herr Sax/ Falkner – UMG/ IAO - MediGRID)**

Why do we need service certificates? In D-Grid are existing user and machine certificates. What is however with applications as service? They can be offered to all communities or potential Grid users, however must it be possible to authorize in a legal form at the resource provider themselves. Who determines the safety level of such certificates? A short outline is the describing specification.

Report: Future safety requirements on the base of a concrete use case. The second part is titled "Requirements of dynamic role-based authorization within medicine technology".

**12:00 - 12:30 V26: SAML – Create and Exchange Security Information in Grids
(Herr Morris Riedle – FZ Jülich - ?)**

The Security Assertion Markup Language (SAML) is an XML-based standard issued by OASIS. It serves as a framework for communicating authentication, entitlement and attribute information. This talk indicates the principal features and key components of SAML and illustrates its future role regarding security mechanisms and interoperability in Grids.