

# **First results in setting up a CERT Infrastructure in D-Grid**

**or:**

# **How Grids can use existing CERT Infrastructures**

3rd TERENA NREN-Grids Workshop

Paris, 27th April 2006

Gerti Foest, DFN-Verein

**For more than two years (start of EGEE) we know:**

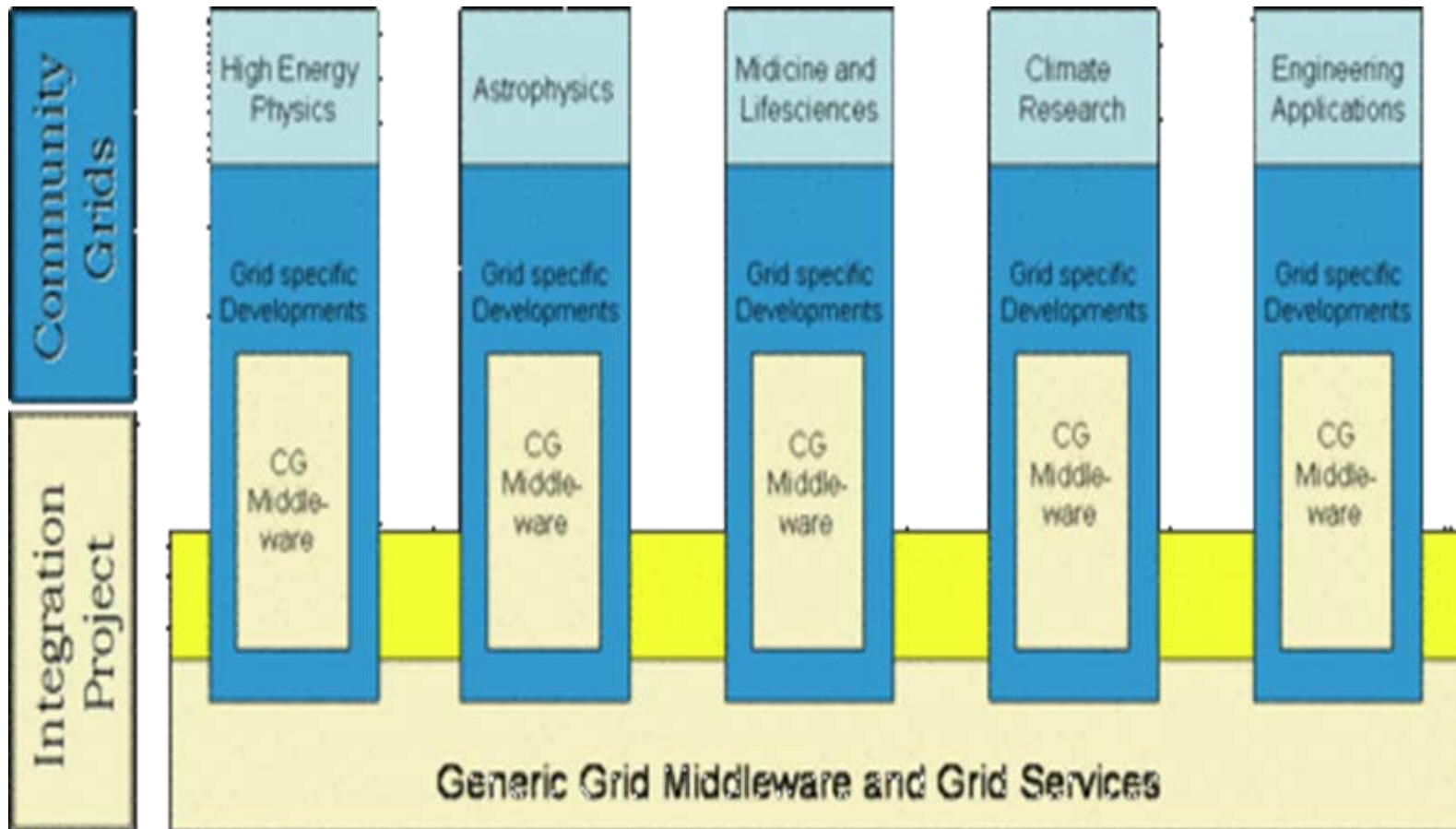
- **Grids need CERT services, but**
  - **Grids didn't know about CERTs**
  - **CERTs didn't know about Grids**
  - **“Come together” was a problem**
- **DFN started activities in D-Grid**
  - **Build organisational basis to develop**
  - **technical services**

# Topics

- **The D-Grid Project**
- **Grid-specific CERT Services**
  - **Goals**
  - **What's to be done**
  - **Results**
- **Conclusion**

- Funded by BMBF (Ministry of Education and Research)
- Start: September 2005
- Six Community Projects
  - AstroGrid, C3(Climate)-Grid, HEPGrid, In(Engineering)Grid, MediGrid, (+TextGrid)
- **D-Grid Integration Project (DGI)**

# D-Grid Structure



- D-Grid Core D-Grid Software
- D-Grid Infrastructure
- **Networks and Security**
- Coordination

- **Networks**

- Extending the Network Platform with Grid-specific Elements
- Investigation of alternative Transmission Protocols

- **Security**

- Building an AA-Infrastructure for D-Grid
- Development and Use of Firewall Concepts in Grid Environments
- **Grid-specific CERT Services**

## Basis

- D-Grid projects use the DFN network (this will also be the case for further Grid activities)
- DFN-CERT operates for many years
  - => great experience
  - => established infrastructure

## Objectives

- Make D-Grid Communities aware of classical CERT services
- Develop new services to meet Grid-specific requirements in close collaboration with D-Grid Communities
- Launch pilot version of the new Grid-specific services

To achieve these objectives:

*Use of existing **organisational** and technical CERT infrastructures.*

- **Coordination and cooperation**
  - Set up and maintenance of information structures, cooperation with local, national and international CERT contacts
- **Incident prevention**
  - Advisories, audits, workshops, training courses
- **Incident response**
  - Support by e-mail or phone, coordination of activities, incident analysis
- **Intrusion detection**
  - IDS, Early Warning Systems

- New usergroups (Communities)
- No established CERT-structures
- New software (Grid-Middleware)
- New applications (Data Grids etc.)
- New collaboration techniques (VOs)

## Organisational

- Rise security awareness in Grid communities
- Establish CERT-structures in Grid communities

## Technical

- Investigate Grid middleware, cooperate with middleware developers, provide special advisories
- Develop new intrusion detection techniques to define and recognise Grid incidents in Grid applications
- Protect personal identity credentials

## D-Grid Security Workshop

- About 50 experts from all participating communities
- Communicate „traditional“ CERT services to the Grid communities
- Figure out special security demands from every community
- Find security contact persons in every community to set up an information infrastructure
  - disseminate information
  - communicate community demands

## Organisational structure

- D-Grid CERT approach is very well received
- CERT services are not very well known in Grid communities, but there are people who have been in contact with DFN-CERT
- Security demands are very different in Grid-Communities; some cannot (yet) describe their demands
- Contact points in communities are established, a mailing list **grid-cert@<community>.de** is set up at each contact point

## International Cooperation

- Cooperation with European CERTs and projects
  - Set up of Grid working group within TF-CSIRT (January 2006)
  - Coordination with EGEE security activities

**Goal: Usage of national structures for European Grid-CERTs**

- Global Grid Forum
  - Keep track of developments

## Technical activities

- Collection and publication of existing national and international CERT activities
- Analysis of Grid-systems and protocols used in D-Grid
  - UNICORE, Globus Toolkit, gLite
  - SOAP, Grid-FTP, GSI OpenSSH

Where are potential security lacks?

First results will be published soon

- Grids need CERTs
- Existing organisational CERT structures are suitable for Grid specific technical extensions

=>



Grid CERTs should use established CERT structures on national and international level

**First steps are made!**

- **DGI Grid-CERT**

Gerti Foest, Klaus-Peter Kossakowski, Klaus Möller, Marcus Pattloch

[grid@dfn-cert.de](mailto:grid@dfn-cert.de)

- **TF-CSIRT Grid mailinglist**

[grid-cert@grid-security.net](mailto:grid-cert@grid-security.net)