

BMBF Hardware



Dr. Helmut Heller
LRZ, DGI FGI.2: Globus

15.11.2006



Overview



1. BMBF Hardware

- Astrogrid Resources at LRZ
- Operational Concept

2. MPICH-G2 vs. Security

3. Globus and VOMS



Astrogrid Resources at LRZ



- Already available at LRZ: Linux Cluster
 - ~230 compute nodes, 32 bit and 64 bit
 - ~25 TB disk space
 - details at
<http://www.lrz-muenchen.de/services/compute/linux-cluster/overview/overview.html>
- > 5% reserved for Astro Community!!



New BMBF Hardware



- New hardware from BMBF for Astro, HEP, DGI, ...
- Attended housing at LRZ desired because...



BMBF Requirements



- Usable by all communities
- Usable with all middleware systems (Globus, Unicore, gLite)
- Usable by others if not used within D-Grid
- Combine resources from different communities at one site
- Guarantee operation for lifetime of systems
- LRZ can **only** do this if new HW is integrated into existing Linux cluster



Astro Requirements



- Assessed at meeting at LRZ on 26. Oct. 06
- Large pseudo-temporary scratch space
- High bandwidth access for reading
- Huge background storage on tapes
- “Raw” disk space for data bank
- Lustre parallel file system is best suited



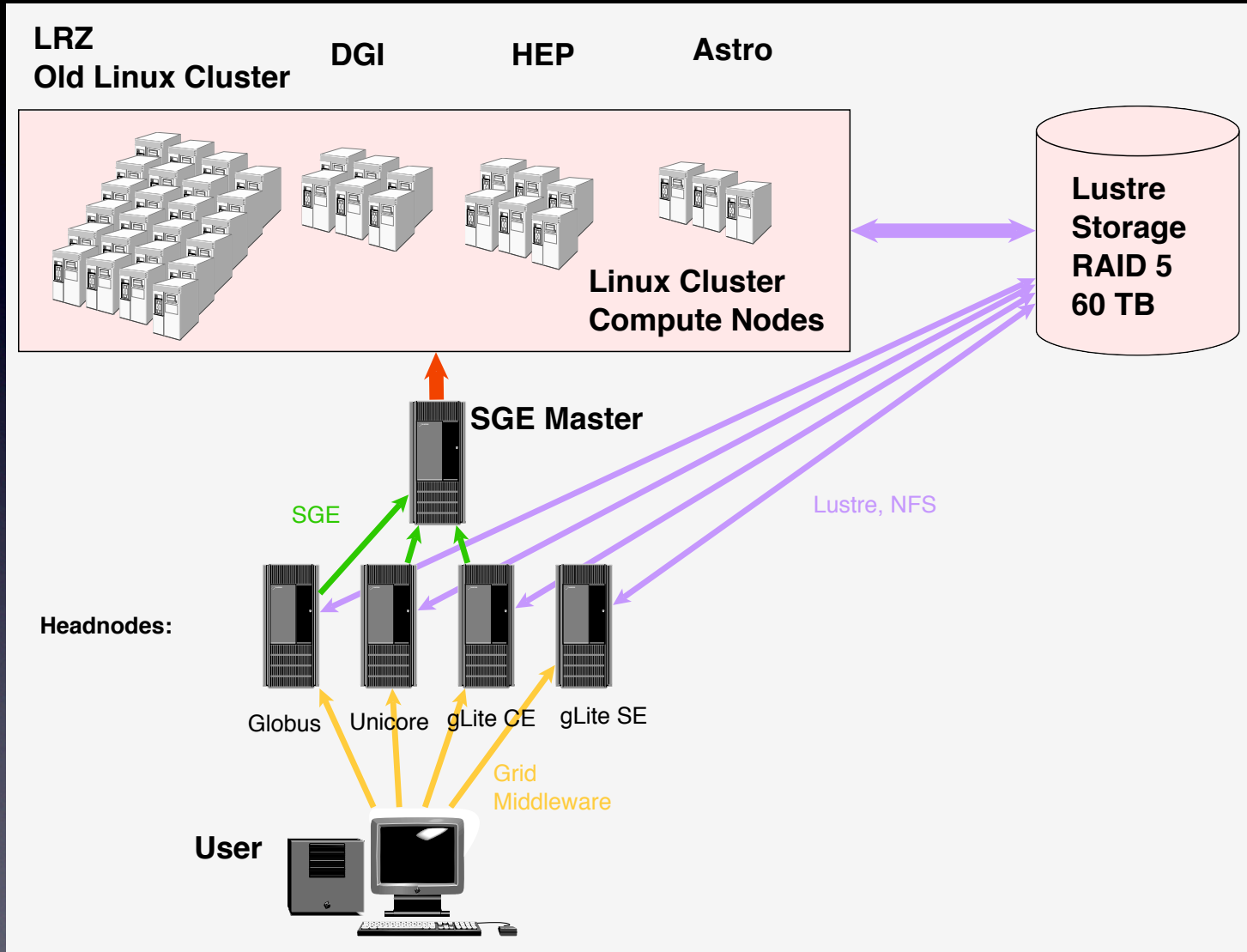
New BMBF Hardware @ LRZ

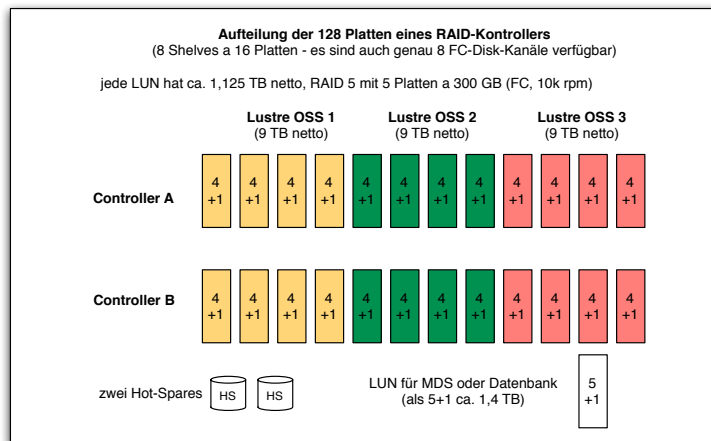
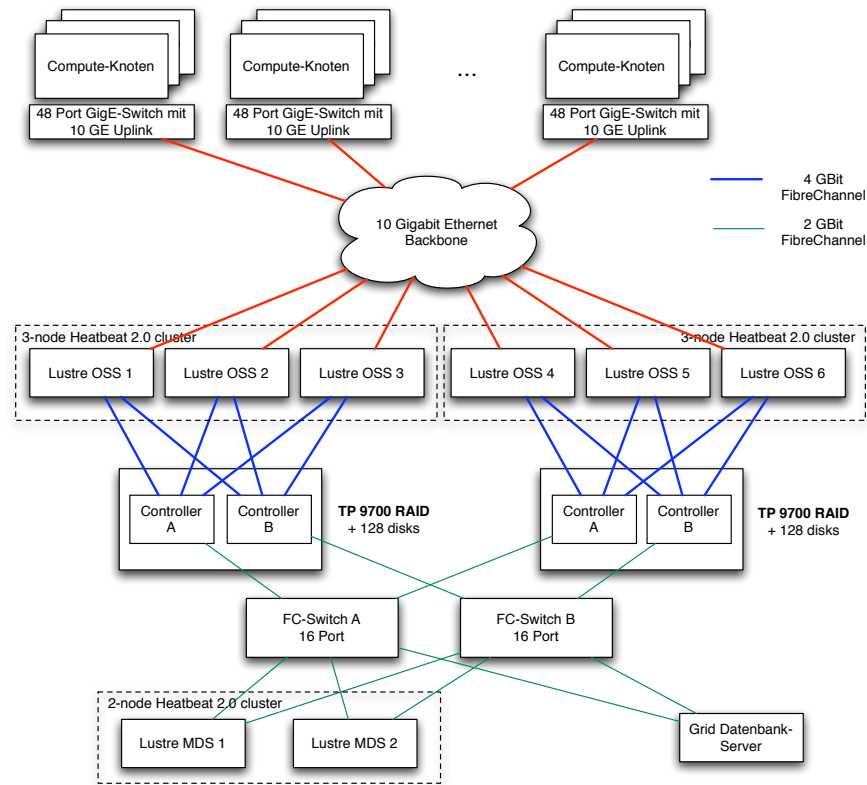


	Cores	Disk/TB
DGI	20+3+8	46
HEP	20	
ASTRO	8	29



Operating Concept







Concept for Other Sites



preliminary

- Principle: freedom!

Those who know how to set up the new systems, can do it their way (if BMBF requirements are met).

- For those, who don't know what to do DGI will provide a suggestion:
 - Head nodes with GT4, Unicore, gLite with VOMS



Concept for Other Sites



preliminary

- Compute nodes with
 - TORQUE
 - SciLinux 4.4 (32bit or 64 bit)
 - dCache for storage
 - SRM or OGSA-DAI
- Meeting 23.11.2006 in Hamburg (all hands meeting) for further discussions
- Communities should send suggestions to Uwe Schwiegelshohn



MPICH-G2 vs. Security



- Astro announced need for MPICH-G2
- Problem: all compute nodes (Linux cluster, HLRB-2, etc.) are - for security reasons - in an internal network, which is not routed to the internet!
- ⚡ No MPICH-G2 possible now!
- How real is the need for MPICH-G2?

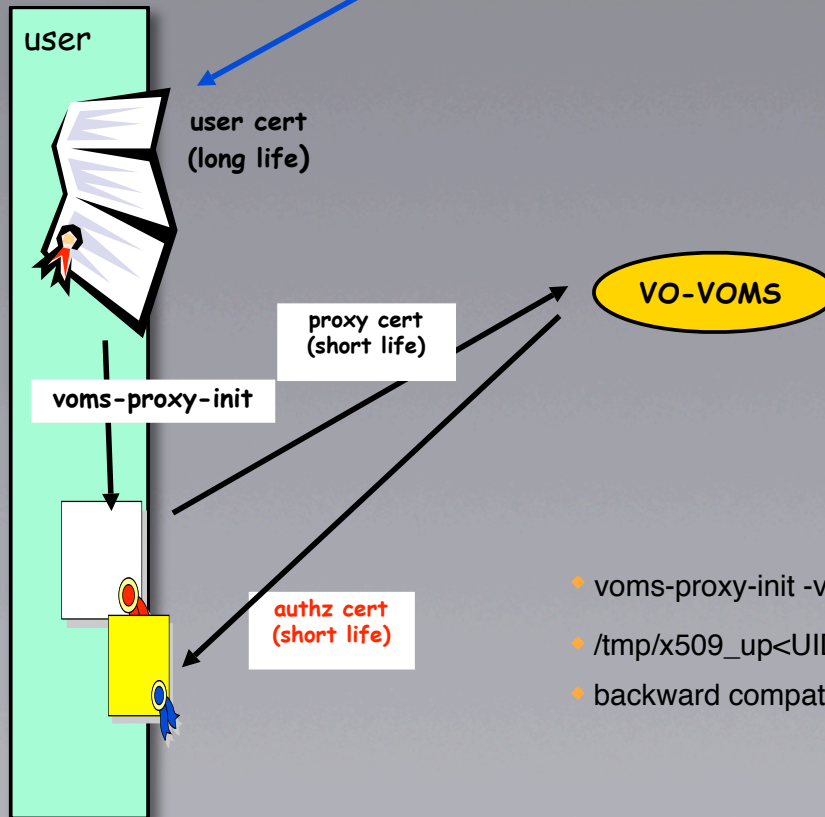
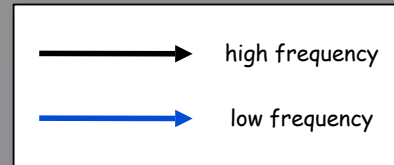


Virtual Organization Membership Service



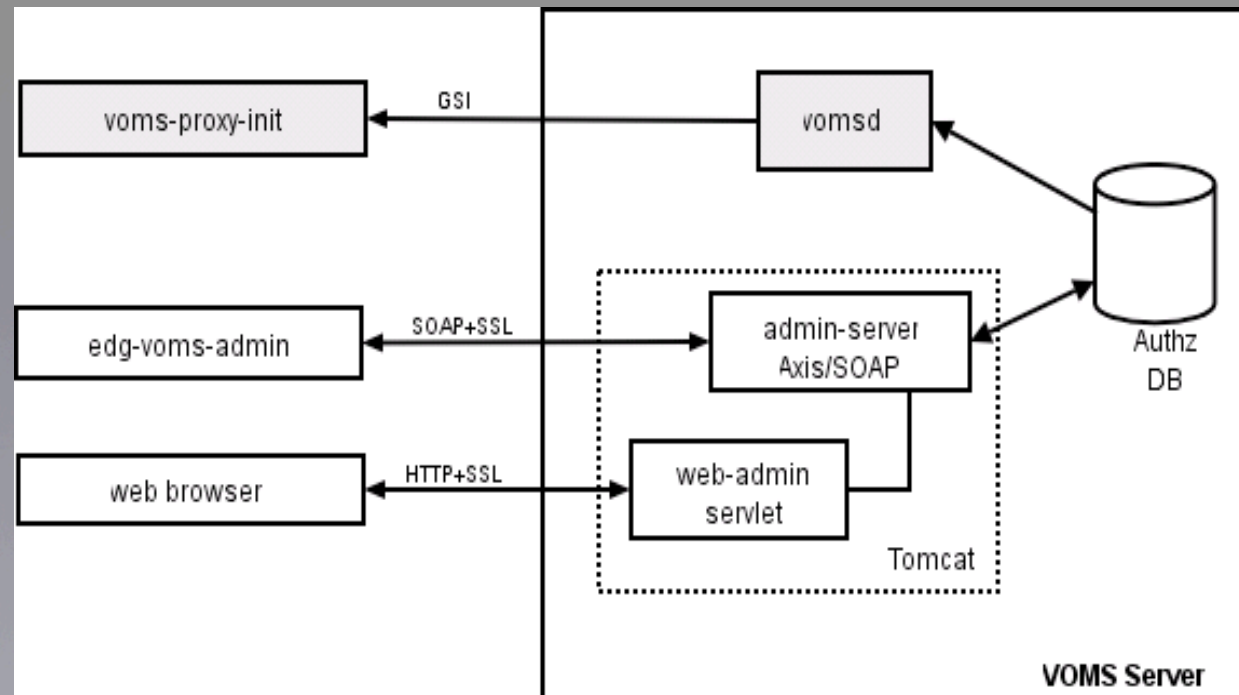
- Provides authorization information (User \leftrightarrow VO)
 - X509 authentication, backwards compatible
 - Single sign-on
 - Multiple **VOs** per user
 - **(Sub)groups** in VOs
 - Finer grained authz, multiple **roles** in VO, capabilities
 - compatible X509 extensions
 - signed by VOMS server
 - Web admin interface

How does it work?



- voms-proxy-init -voms dgtest
- /tmp/x509_up<UID> (normal proxy location)
- backward compatible proxy format

The Architecture



- Authz DB
- VOMS
 - vomsd
 - clients, voms-proxy-init
- VOMS admin
 - java server app
 - UI servlet
 - voms admin client
- Get data: edg-mkgridmap

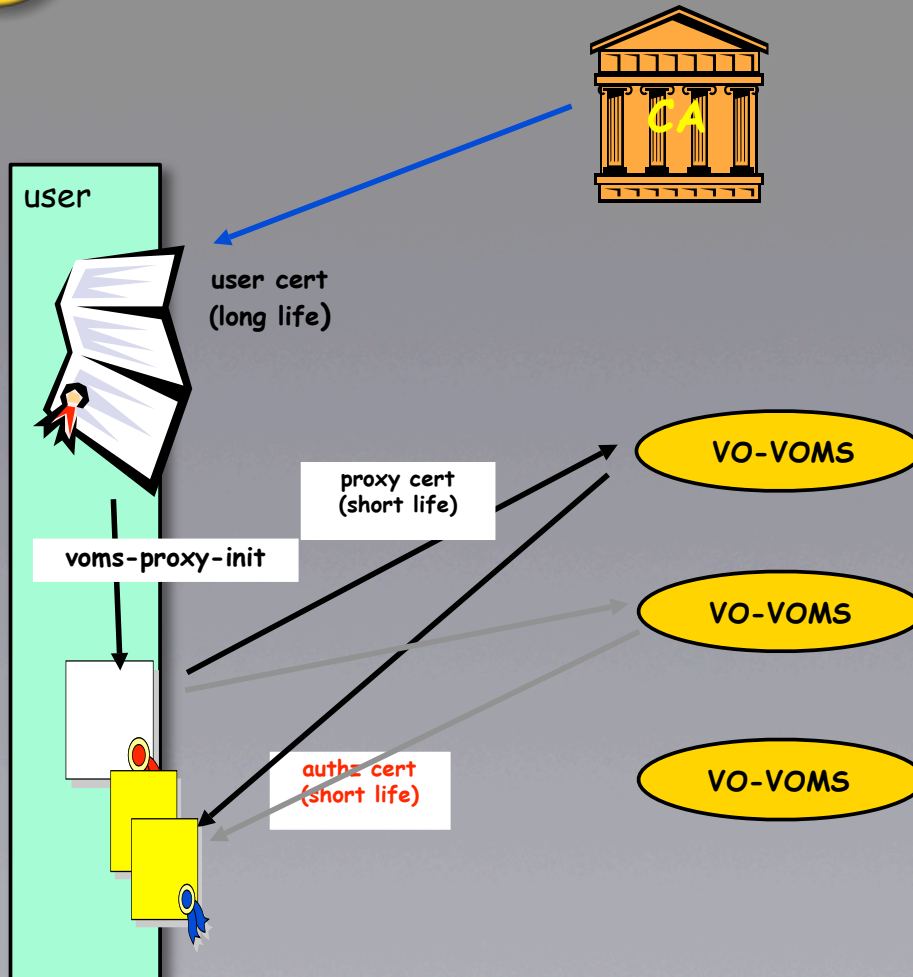


Groups, roles, capabilities



- Members organized in **groups**
 - administration can be delegated (ACLs)
 - hierarchical structure
 - /theVOgroup/subg/subsubg
 - member of subsubg => member of subg
- Members can play **roles**
 - inherited from ancestor groups
 - plays role in group => plays same role in subgroup
 - roles also have ACLs
- Members can have **capabilities**
 - same inheritance as roles
 - free-form strings

Member of several VOs?



- Real problem in vanilla Globus: Your DN can only be mapped to **one** unix account - what if you use your cert in DEISA **and** D-Grid?
- `voms-proxy-init -voms dgtest \ -voms atlas`
- single proxy cert generated
- each VO provides separate VOMS credential
 - **first one is default VO**
- each VOMS credential contains multiple group/role entries
 - **first one is default group**



Who does what?



- VOMS may name groups/roles in order to implement policy
 - user belongs to group **A**, has role **b**
- Up to services to enforce policy
 - allows for local policy
 - resource providers grant access to **VOs, groups** or **roles**
 - LCAS – authz based on cert, attributes, job spec
 - **Sites map VO members/roles to local auth mechanism (unix users)**
 - LCMAPS – provides local credentials for access
 - **mapping to user from pool, and group(s)**
 - **default VO = default UNIX group**
 - **other VO/group/role = other UNIX group(s)**
- Up to resource owner not to override it



Interacting with the server...



- **Users:**
 - web interface
 - requesting membership
 - command line
 - creating voms proxy
- **VO admins**
 - web interface
 - managing users
 - *add, remove, set role(s)*
 - managing groups & roles
 - managing ACLs for groups & roles
- **Services**
 - command line + API
 - fetching VO / role members



How to start



- URL:

<https://dgrid-voms.fzk.de:8443/voms/dgtest/>

- Go to “New User Registration”

<https://dgrid-voms.fzk.de:8443/voms/dgtest/webui/userrequest/create>

Virtual Organization Membership Service - Konqueror
Location: https://dgrid-voms.fzk.de:8443/voms/dgtest/

Virtual Organization Membership Service

VOMS

FOR VO USERS

- My membership details
- New user registration
- My requests

FOR VO MANAGERS

- Administer the VO
- Handle requests
- Check audit data

CONFIGURATION

- Configuration information
- List all VOs on this server

© 2004 CERN, ELTE on behalf of the EU EGEE Project



CLI commands



- **voms-proxy-init**

```
$ voms-proxy-init -voms dgtest
```

```
Your identity: /O=GermanGrid/OU=FZK/CN=Ariel Garcia
```

```
Enter GRID pass phrase:
```

```
Creating temporary proxy ..... Done
```

```
Contacting dgrid-voms.fzk.de:15000 [/O=GermanGrid/  
OU=FZK/CN=host/dgrid-voms.fzk.de] "dgtest" Done
```

```
Creating proxy ..... Done
```

```
Your proxy is valid until Thu Oct 13 05:16:33 2005
```

- **voms-proxy-init -voms dgtest -voms atlas**



CLI commands



- **voms-proxy-info**

```
$ voms-proxy-info -all
```

```
subject : /O=GermanGrid/OU=FZK/CN=Ariel Garcia/CN=proxy
```

```
issuer : /O=GermanGrid/OU=FZK/CN=Ariel Garcia
```

```
identity : /O=GermanGrid/OU=FZK/CN=Ariel Garcia
```

```
type : proxy
```

```
strength : 512 bits
```

```
path : /tmp/x509up_u500
```

```
timeleft : 11:59:24
```

```
VO : dgtest
```

```
subject : /O=GermanGrid/OU=FZK/CN=Ariel Garcia
```

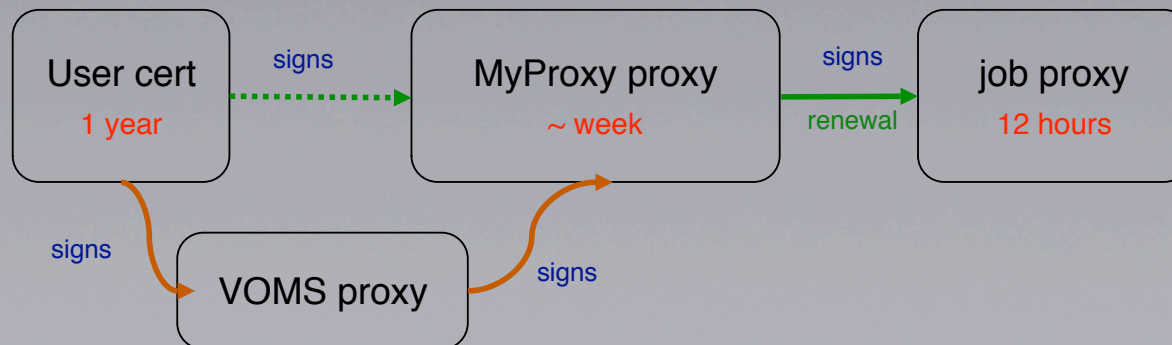
```
issuer : /O=GermanGrid/OU=FZK/CN=host/dgrid-voms.fzk.de
```

```
attribute : /dgtest/Role=NULL/Capability=NULL
```

```
timeleft : 11:59:24
```

- Compatibility with MyProxy
 - voms-proxy-init -voms dgtest
 - export X509_USER_KEY="/tmp/x509up_u`id -u`"
 - export X509_USER_CERT="/tmp/x509up_u`id -u`"
 - myproxy-init
 - (myproxy-get-delegation)

<http://osg.ivdgl.org/twiki/bin/view/Integration/VOMSandMYPROXY>





Installation: Client



- In addition to Globus GT4, also install
voms-client_gcc3_2_2-1.5.4-1_sl3
- No success with SuSE, only with SciLinux!
- For more info (in German) see:
<http://www.nm.ifi.lmu.de/pub/Fopras/czyz06/>
Marcin Czyzewski



Installation: VOMS-Server



- Prerequisites:

- MySQL or Oracle
- Perl 5.8.1 or younger

- Pakets to install:

- glite-security-voms-admin-client-1.0.7-1
- glite-security-voms-admin-interface-1.0.2-1
- glite-security-voms-admin-server-1.1.2-1
- glite-security-voms-api-1.5.9-0
- glite-security-voms-api-c-1.5.9-2
- glite-security-voms-api-cpp-1.5.9-0
- glite-security-voms-clients-1.5.9-0
- glite-security-voms-config-1.5.9-0
- glite-security-voms-mysql-1.0.3-0
- glite-security-voms-server-1.5.9-0
- glite-voms-server-config-2.0.0-3