

Security through Virtualization



inGRID

DGI



Philipps



Universität
Marburg

Matthew Smith
Niels Fallenbeck
Matthias Schmidt

Distributed Systems Group
Philipps-University Marburg

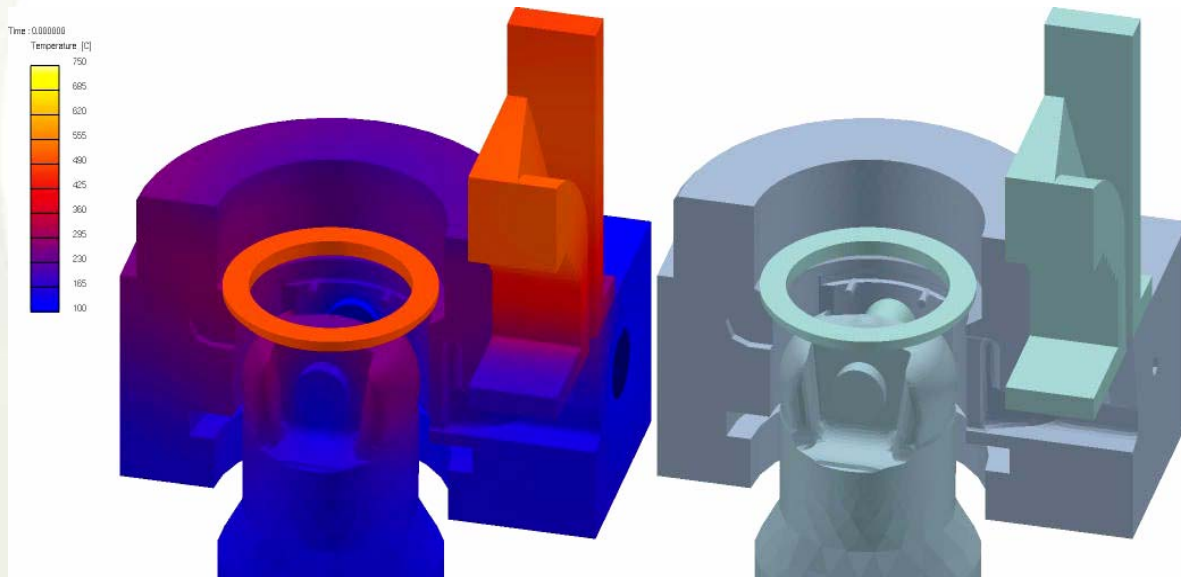
Outline

- ▶ Current Grid security issues
- ▶ Customized Image Creation
- ▶ Virtualization within the D-Grid
- ▶ Xen Grid Engine

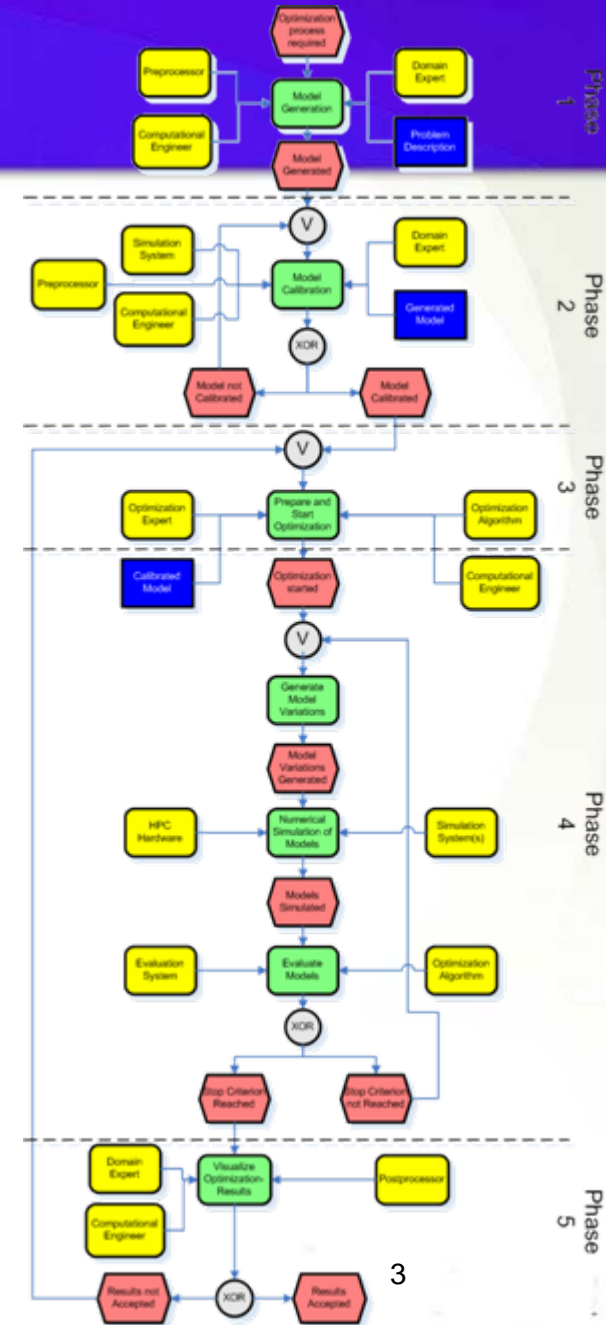
Sample Application (InGrid)

Metal Casting:

Numerical simulations are performed to substitute the expensive and time-consuming building processes for physical tools and prototypes

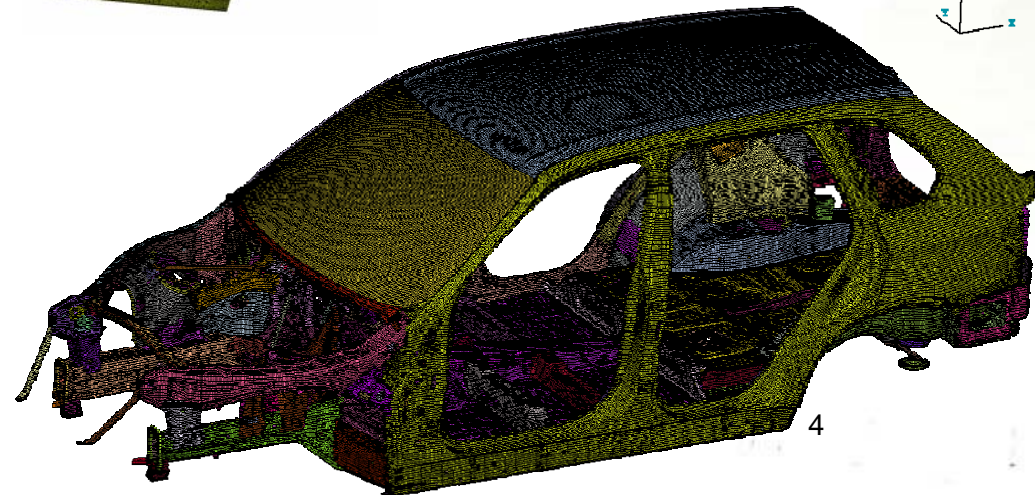
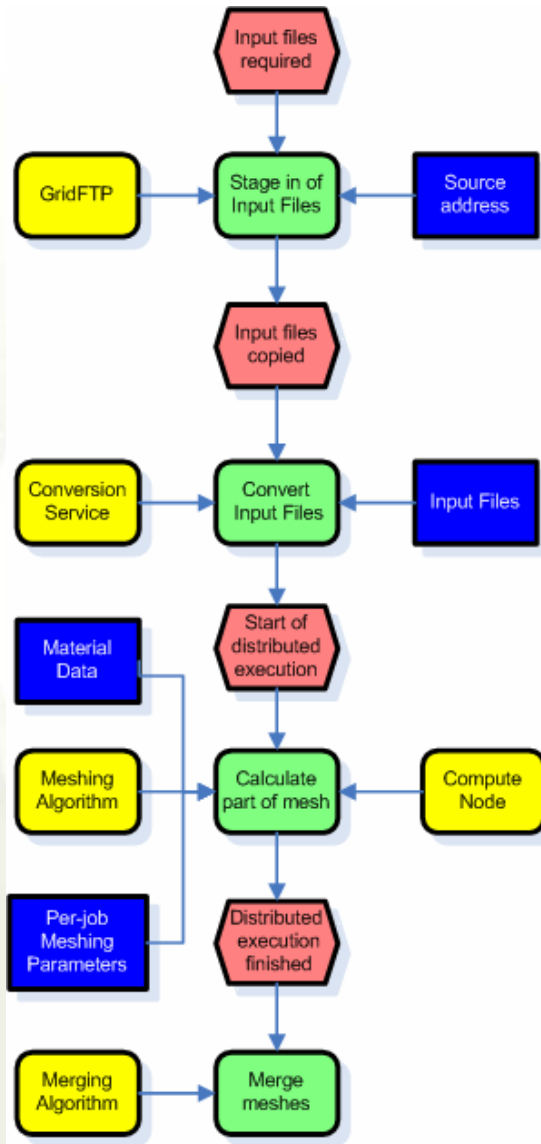


(Simulation of a motor piston)



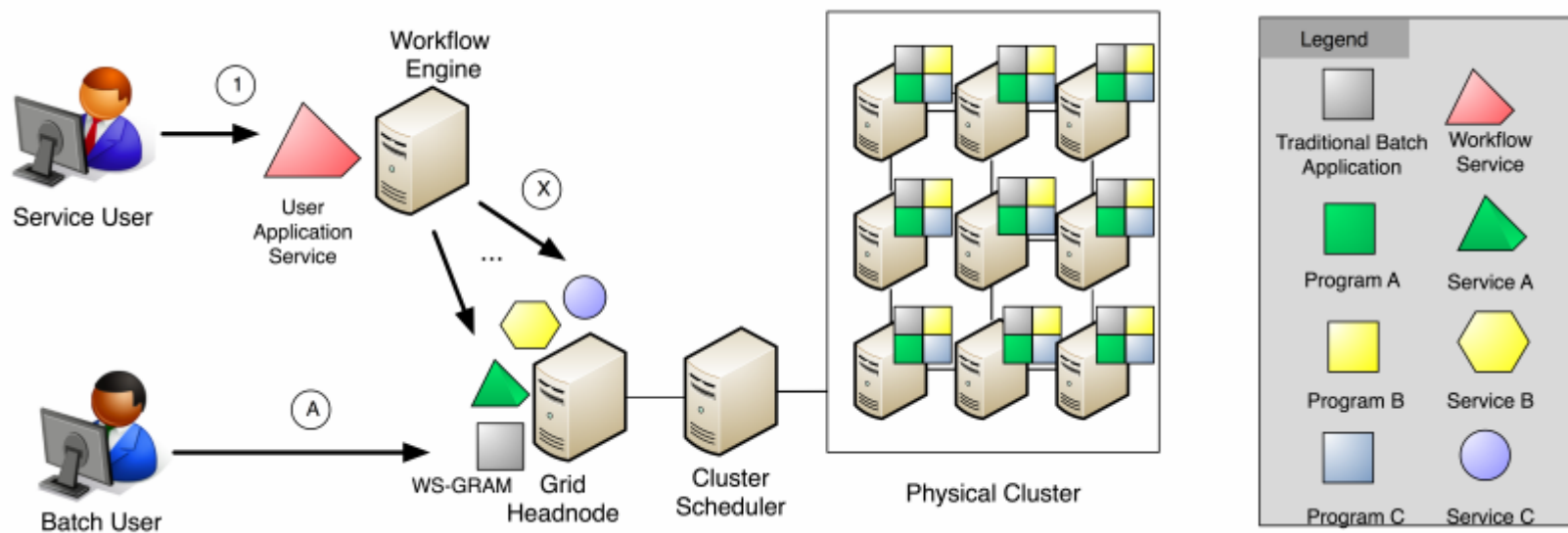
Sample Application (Biz2Grid)

Distributed Meshing in Computer Aided Engineering



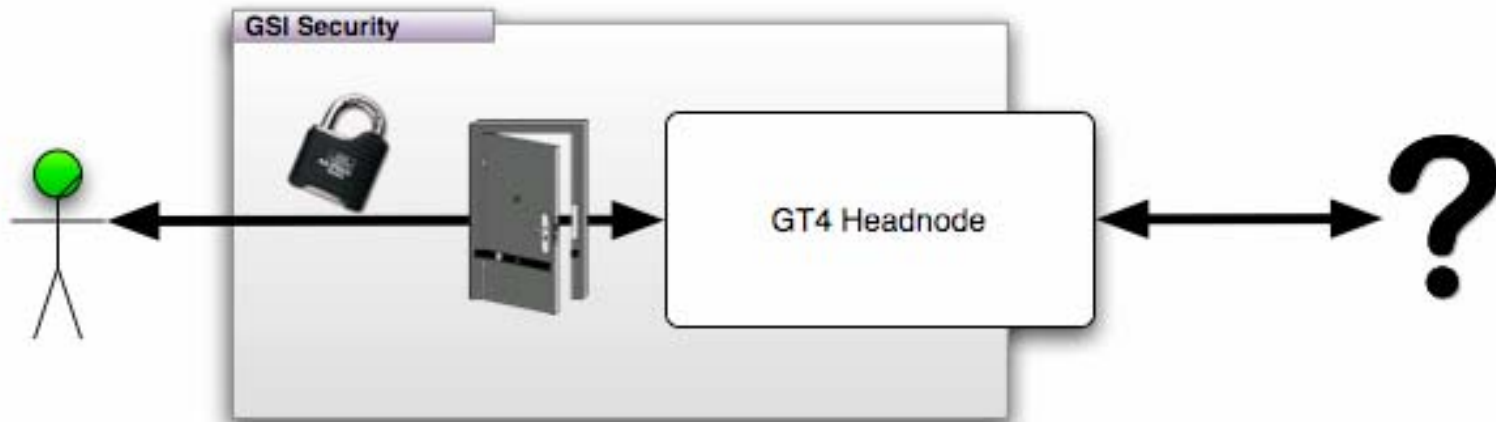
Services vs Jobs

- ▶ Install Globus on all Workernodes?



Security issues in Grid environments

- ▶ In a trusted environment, GSI covers nearly all security aspects to protect the Grid from outside threats.



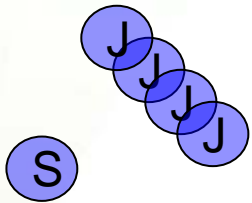
- ▶ This traditional view suffers from several security issues, especially if users may install software autonomously.

Security issues in Grid environments

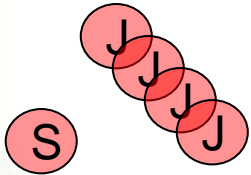
- ▶ Customers need to install their own software
 - Installation via the local admin is expensive and potentially opens the door for malicious users (rootkits, manipulated software packages, etc)
 - Manual installation way to complex for most users (GridFTP, GSIssh or GRAM remote Make)
- ▶ Different customers work on the same resources
 - Disclosure of sensitive data is possible
- ▶ Meta-Data information can be disclosed
 - Information about the used software can be gained
 - Workflow of other users can be traced
- ▶ These issues prevent commercial adoption of shared Grid technologies

Traditional Grid vs. virtualized Grid

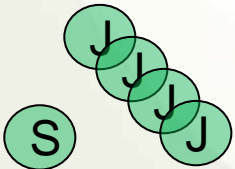
User A



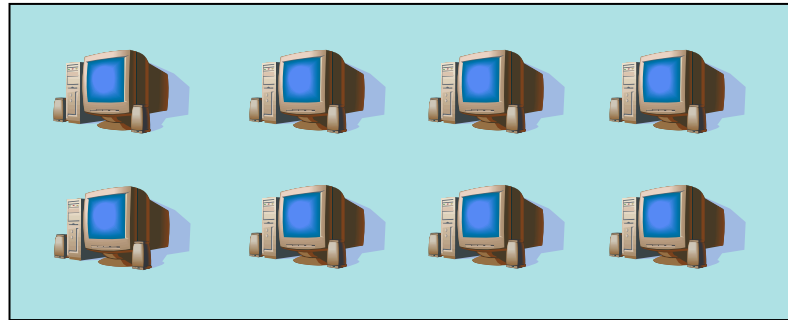
User M



User B

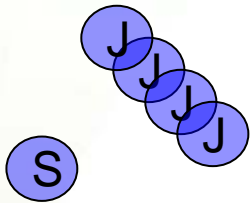


Traditional Grid Resources

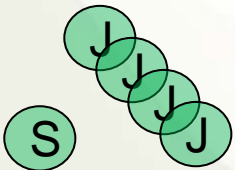


Traditional Grid vs. virtualized Grid

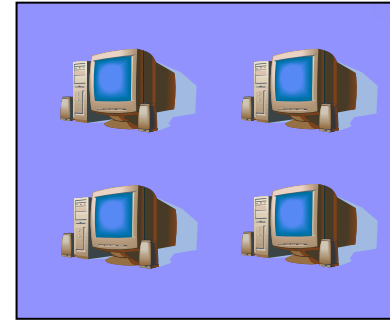
User A



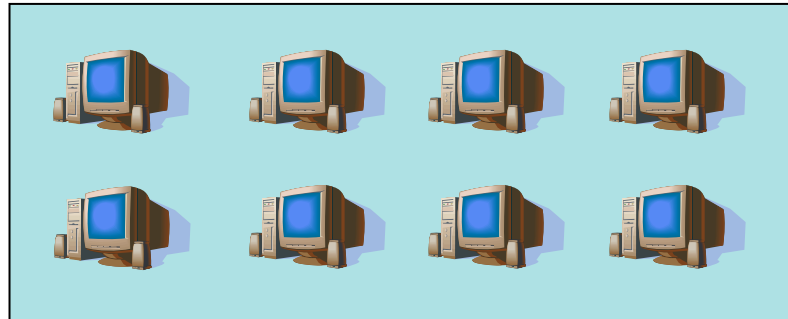
User B



Virtual Grid A



Raw Grid



Virtual Grid B

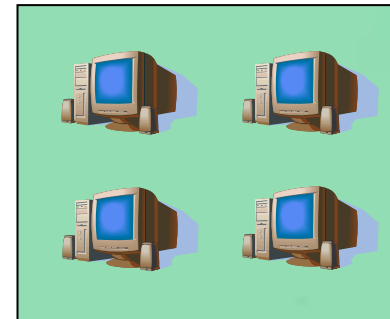


Image Creation Station (ICS)

- ▶ The ICS eases the installation of 3rd party software (root privileges no problem)
- ▶ A user can log in to the VM to install commercial software before the VM is used for job execution
- ▶ After one VM is installed, the remaining VM are cloned
- ▶ A malicious user cannot compromise the system

X.509 Information

Welcome back **Niels Fallenbeck** from **Universitaet Marburg (DE)**
Certificate issued by **DFN-Verein User CA Grid - G01**
Your IP address: **137.248.121.71**

Predefined options

Kernel: **vmlinuz-2.6.18-4-xen-amd64**
Architecture: **amd64**

Image Options

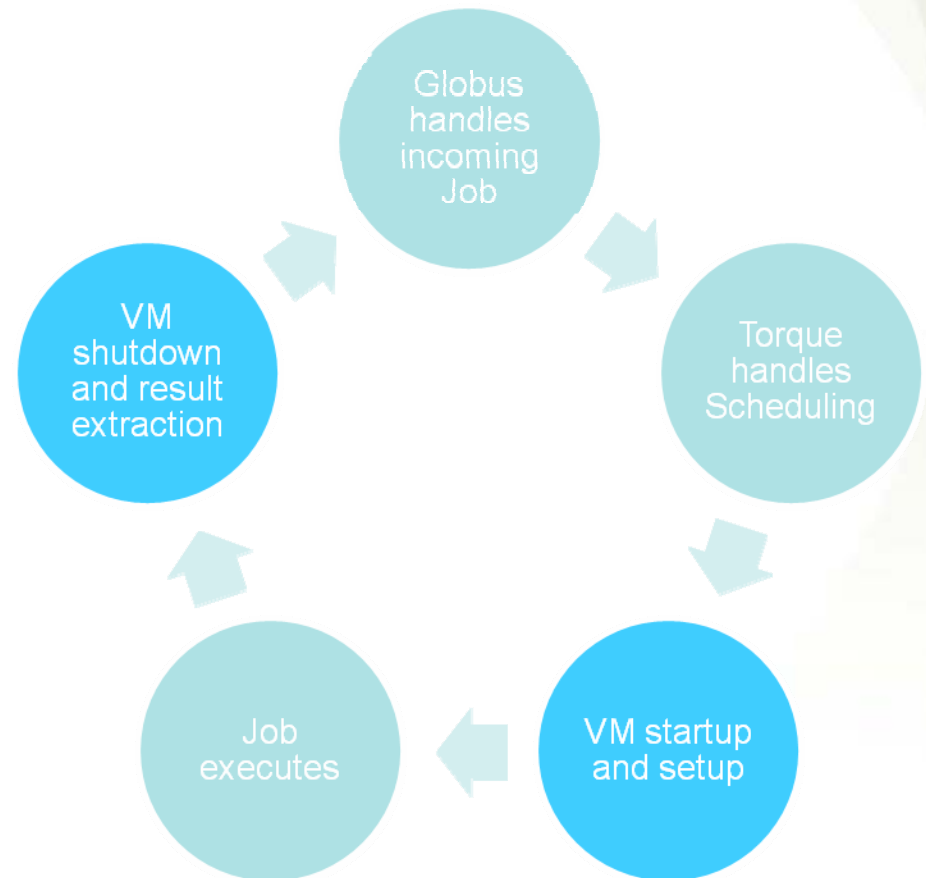
Hostname	<input type="text" value="testimage"/>
Size (MB)	<input type="text" value="1024"/>
Filesystem	<input type="radio"/> ext2 <input checked="" type="radio"/> ext3
Distribution	<input type="radio"/> sarge <input checked="" type="radio"/> etch <input type="radio"/> dapper
Create swap space	<input checked="" type="checkbox"/>
E-Mail Address	<input type="text" value="fallenbe@informatik.uni-marburg.de"/>
SSH key	<pre>ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAIEAwLNHY97mKcWJD3IU/TNtjRsT fallenbeck@dante</pre>
GPG key	<pre>-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.6 (Darwin) mQGIBEDYsbARBADomPr1T4s6mS05TzP523vrKJHQP24DP8Rj23 xd73Yow/8fmeDFJGfR9oSvKe2SwPpU6BI7WQAXotMKChdTOAEg S/oqhjGS3va6Ae1xqdIrJDEhy4MVMF4jHn8EUXZMaOr0QSQaZ5 YItWexr+tDOEh8oCT6rWreUD/1yc1WJ9fFAH1j6S0kROJzVubI 5OxJMuhmSpOE2rrgpb4nxn43EftHAPVOi5bocyht5TalEsgoqN 2n/eD74fCBTxAfUcox02qPXk+x35qdgQaGoiYcDcOYMVKielby puxFBACGLM0uIML75U4nTbbvJuISM+/f8w2i_jpZyDEqTpELnKP</pre>

If you want your notification email encrypted, please submit your public GnuPG key. Note: The key has to match your given email address above!

Create image

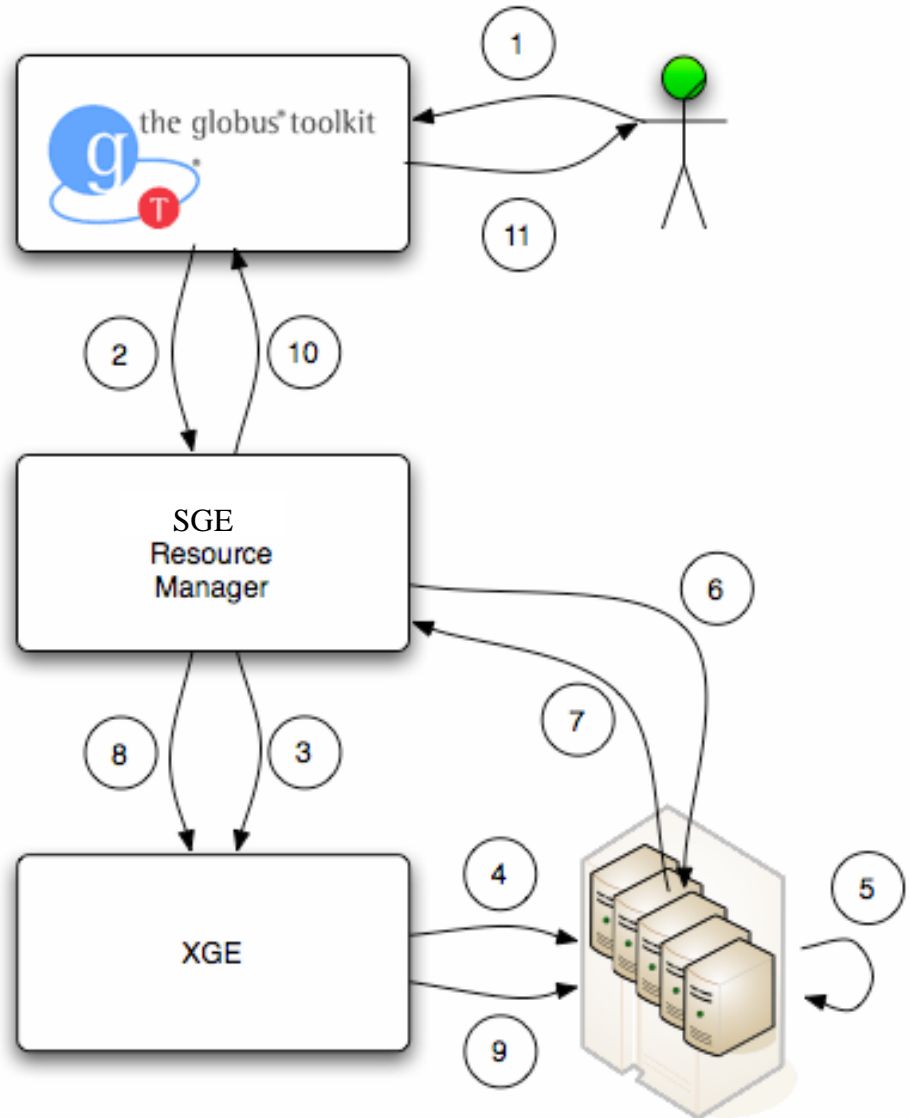
Virtualization within the D-Grid

- ▶ An incoming Job (e.g. via GRAM) is handled by Globus
- ▶ Globus passes the job to the cluster scheduler, (e.g.SGE).
- ▶ The corresponding number of user VMs boot up and are configured
- ▶ The Job is executed inside a VM
- ▶ Cluster scheduler collects all results and the VMs are shut down

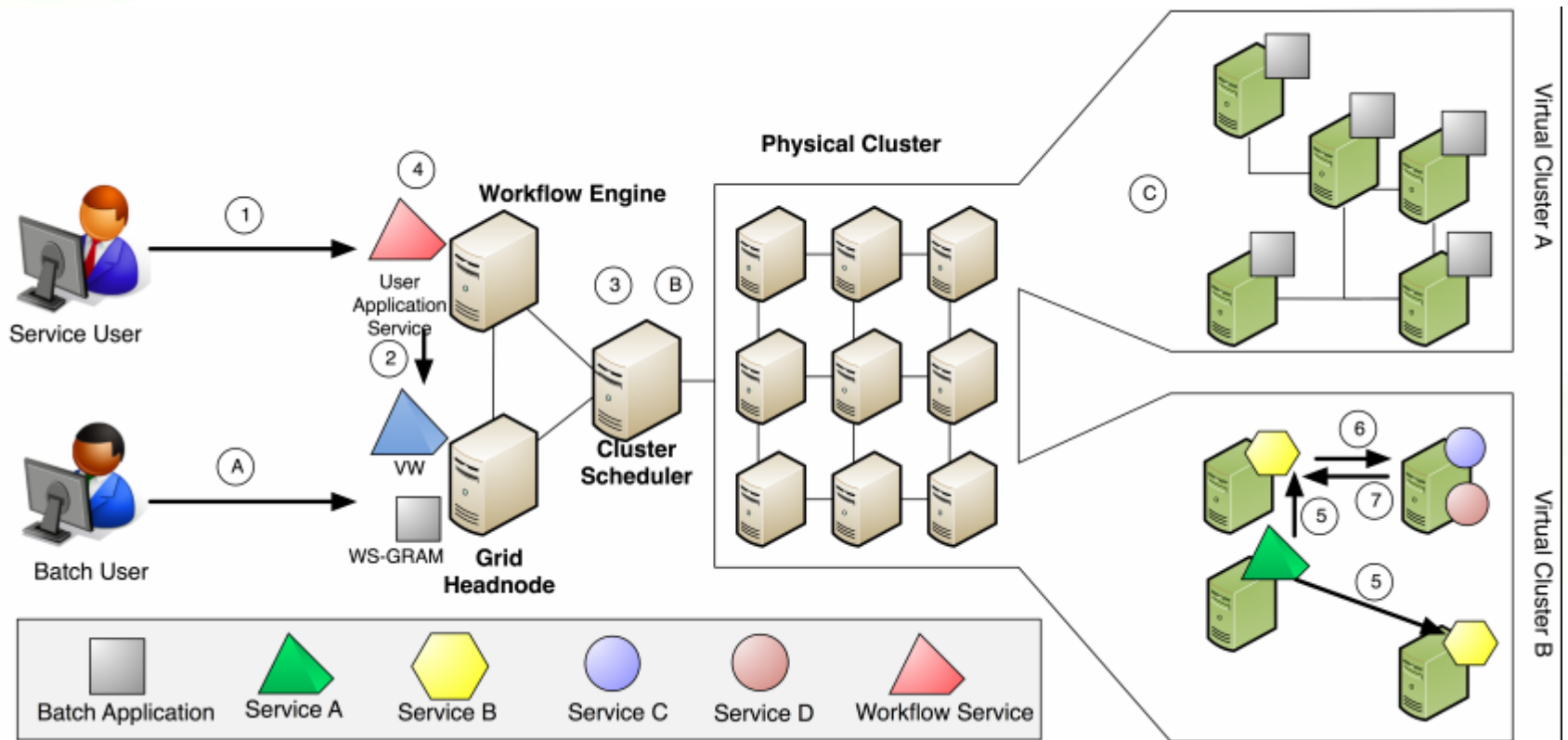


Xen Grid Engine (XGE)

- ▶ Virtualization Management Prototype Software developed at the University of Marburg
- ▶ Transparently coupled to the cluster scheduler (currently Sun Grid Engine)
- ▶ Minimally invasive approach is transparent for Grid middleware and users.
- ▶ Cluster scheduler features are automatically utilized (e.g. Backfilling, advanced reservation, etc.)



Services & Jobs



Demo

- ▶ Video 1) Image Creation
- ▶ Video 2) Job Execution

Roadmap

Marburg Grid Site:

- ▶ ICS - available now
- ▶ XGE - 8 VMs available now
- ▶ Secure Workflow Engine - available now
- ▶ XGE - full installation coming shortly

Installation packages:

- ▶ Secure Workflow Engine - May 2008
- ▶ ICS & XGE - Summer 2008

Questions?

- ▶ Thank you for your attention
- ▶ Contact:
 - Matthew Smith, Niels Fallenbeck, Matthias Schmidt
 - {matthew, fallenbe, schmidtm}@informatik.uni-marburg.de

inGRID

Philipps



Universität
Marburg

DGI



GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung