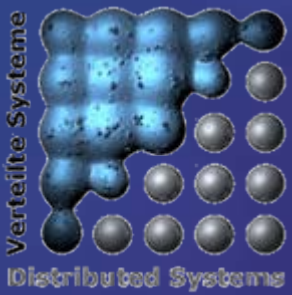
Virtualization Security Infrastructure

Matthew Smith
Christian Schridde
Bernd Freisleben



GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Vertraulichkeit

Die Vertraulichkeit von Information und Wissen (Confidentiality) ist eine elementare Grundlage für die Zusammenarbeit gerade in Private/Public Partnerships. Dies setzt voraus, dass der Besitzer von Information und Wissen die uneingeschränkte Kontrolle über sein intellektuelles Eigentum behält und das Wissen nicht von Dritten missbraucht werden kann.

- Daten dürfen nicht von der Konkurrenz lesbar sein
- Programme dürfen nicht für die Konkurrenz nutzbar sein
- Das es Daten und Programme gibt darf nicht für die Konkurrenz sichtbar sein!
- Wie die Daten und Programme genutzt werden (Prozesse und Workflows) darf für die Konkurrenz nicht sichtbar sein!

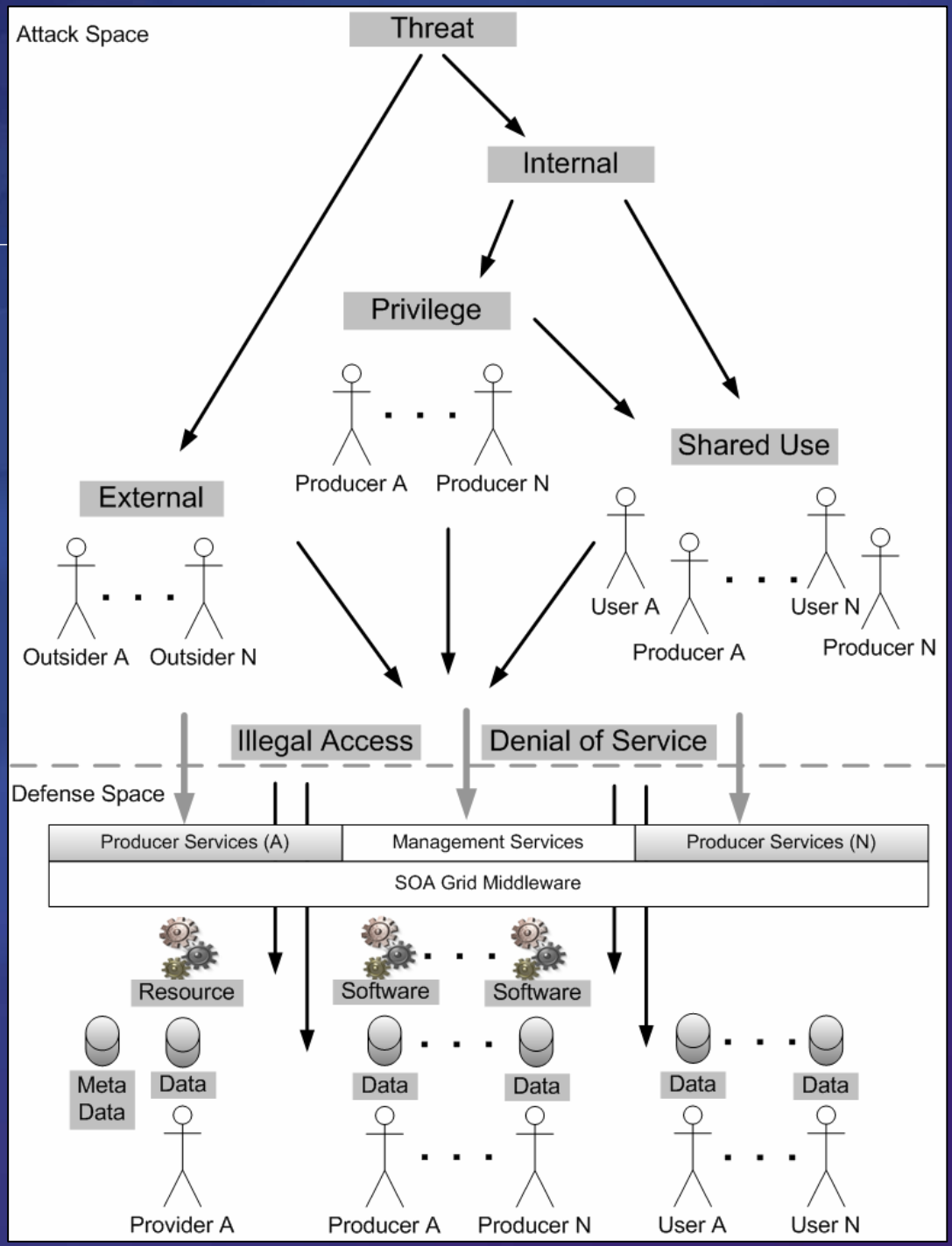
Geistiges Eigentum und der Stand der Entwicklung muss gesichert werden.

The Three Problem Pillars of In-Grid Security

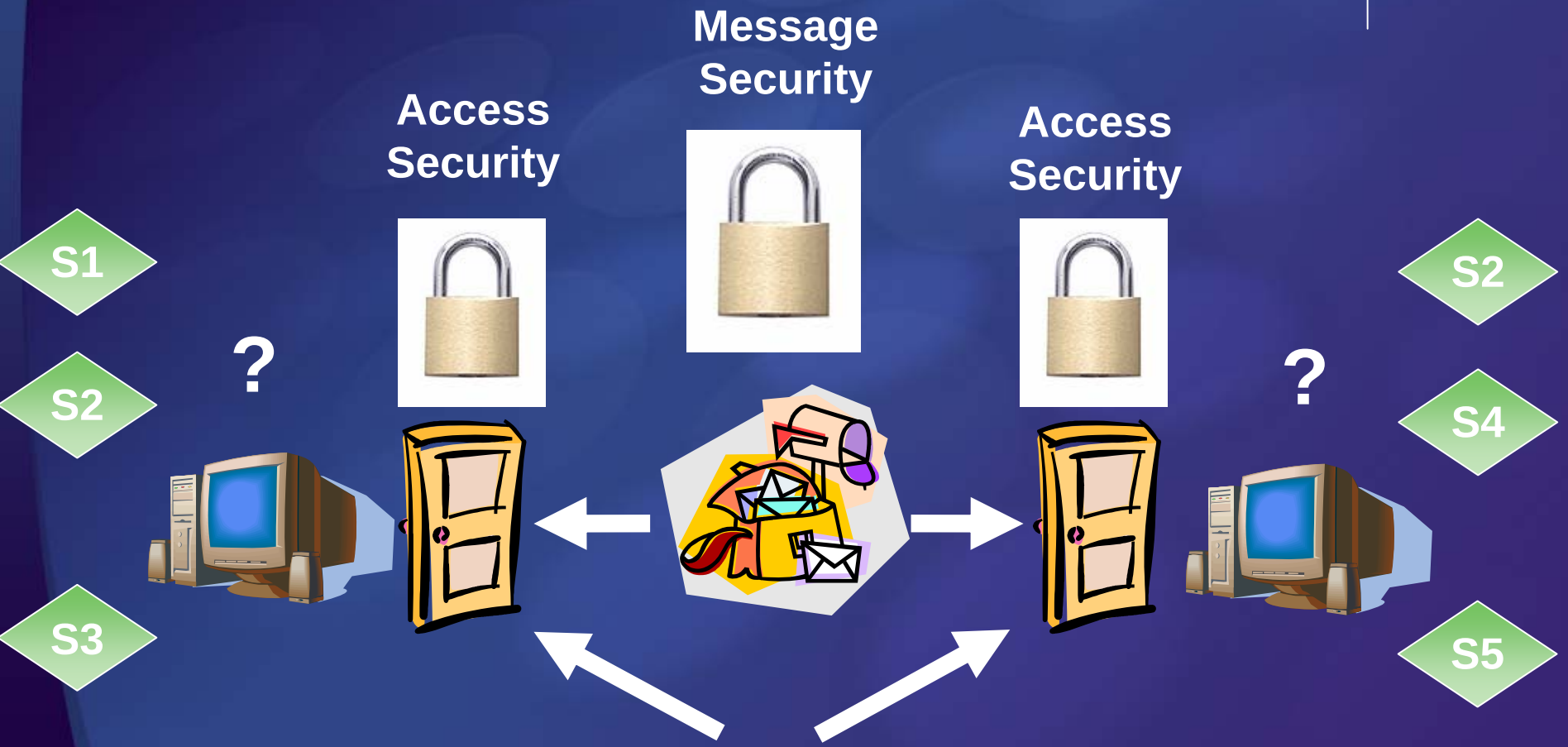
- Multiple Users / Producers operate on the same Node at the same time (Shared Use)
- Producer can install Software on Producers Node (Privilege)
- Number of Users / Producers is large and fluctuates over time (Shared use, Scale and Dynamics)

Threat Tree

- External: standard threats of any distributed system
- Privilege: threats posed by the administrative rights needed by the Producers
- Shared Use: threats posed by multiple Users or Producers using the same resource at the same time



Standard Grid Security

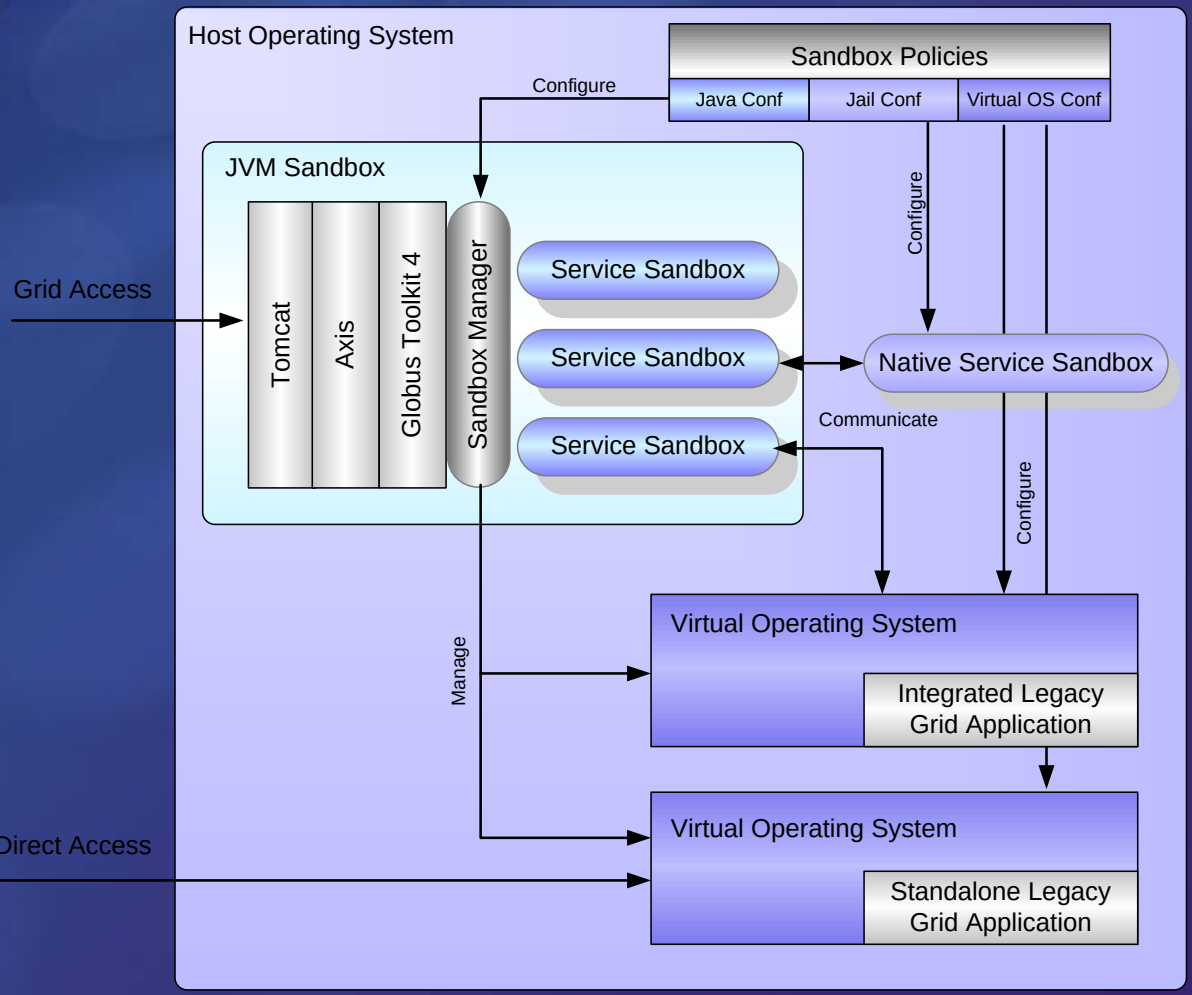


What happens behind these doors is hardly regulated!

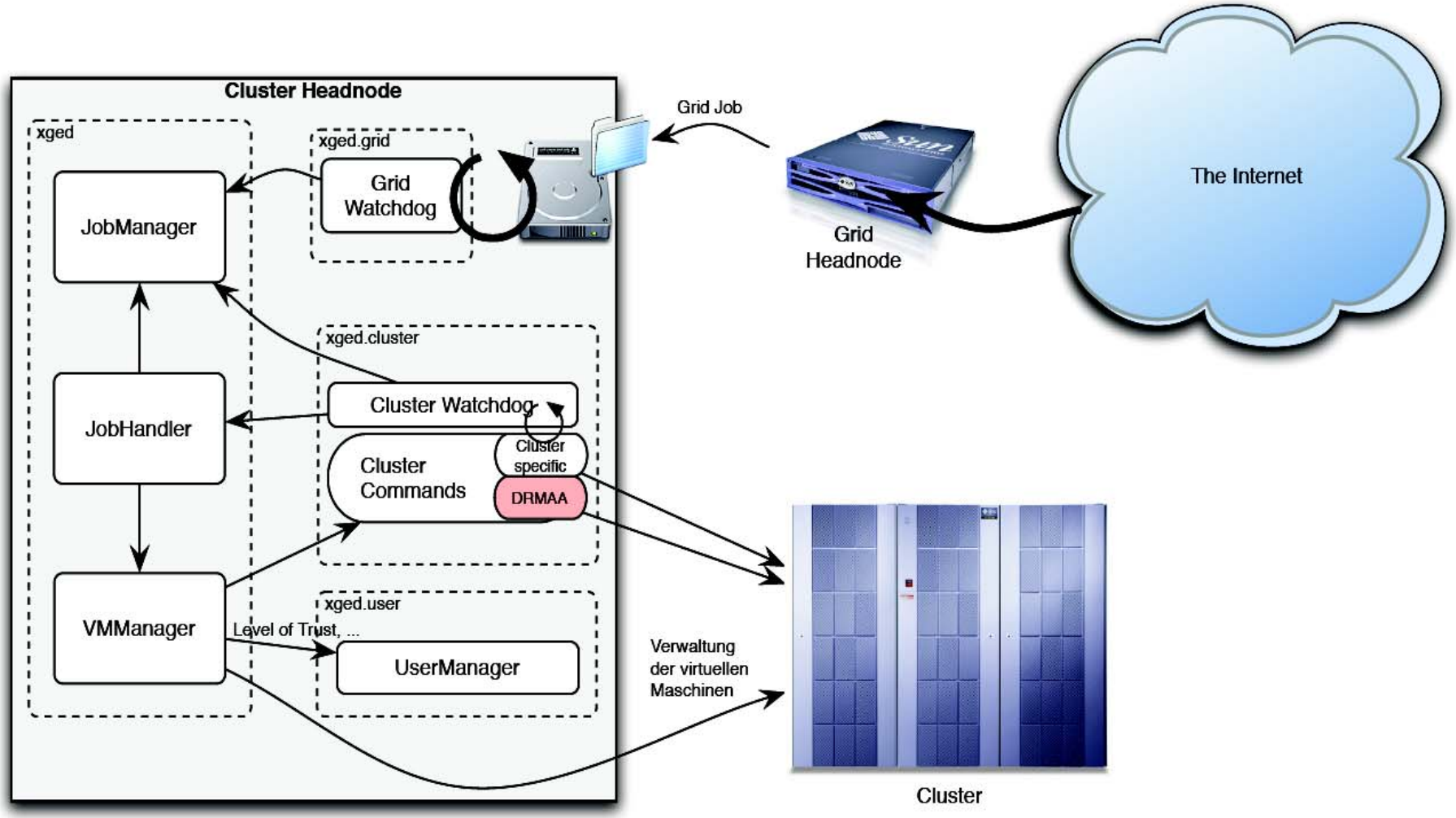
Just like in a beehive.
Once you have passed the outer defences you are free to do what you like.

Sandbox Options

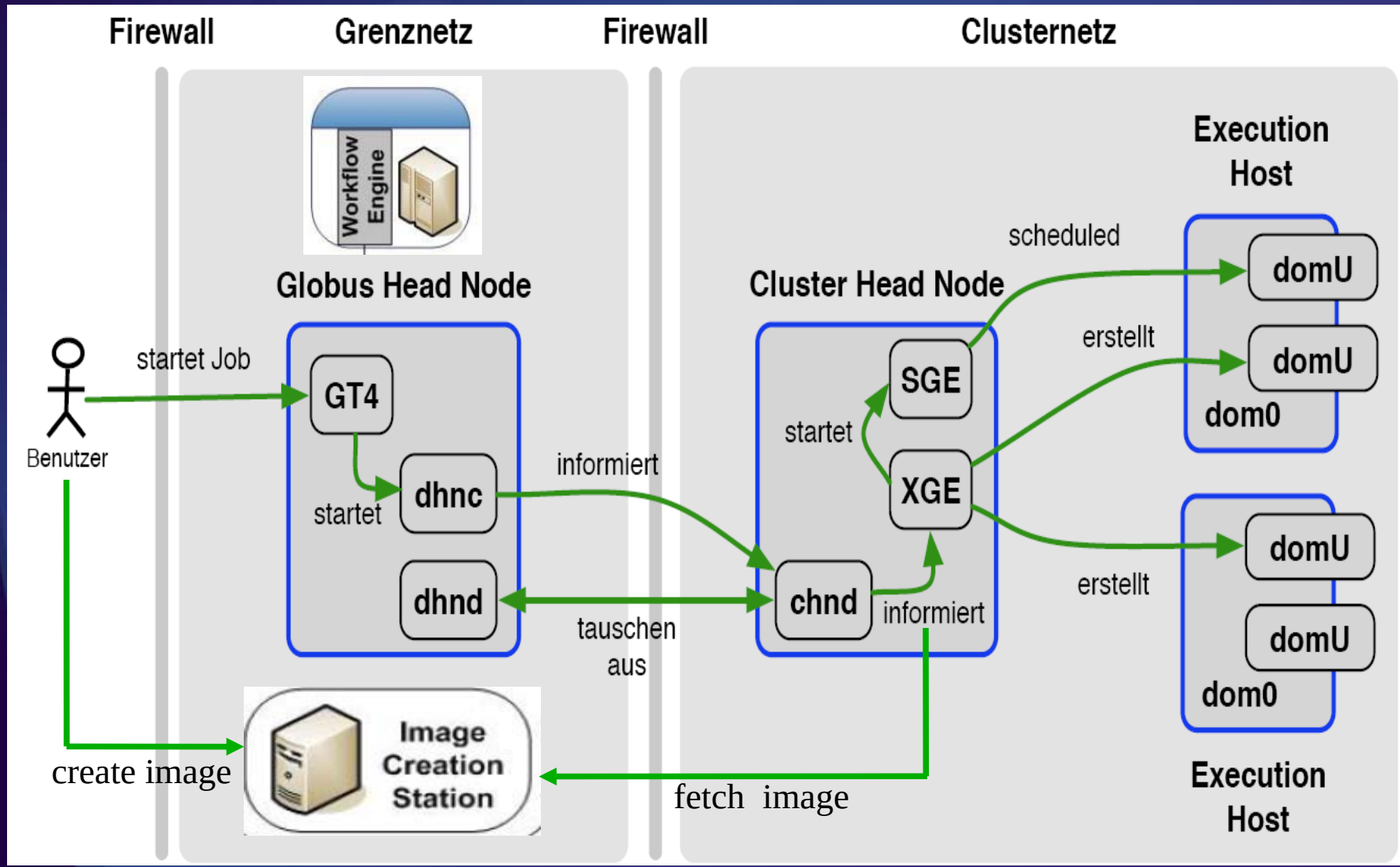
- Java Sandboxes
  - Secure Service ClassLoaders
- Process Sandboxes
  - Jails
  - Systrace
- OS Sandboxes
  - Xen
  - OpenVZ
  - Virtuozzo
  - Virtual PC
  - VMWare



Xen Grid Engine



Sonderinvestitionen Setup



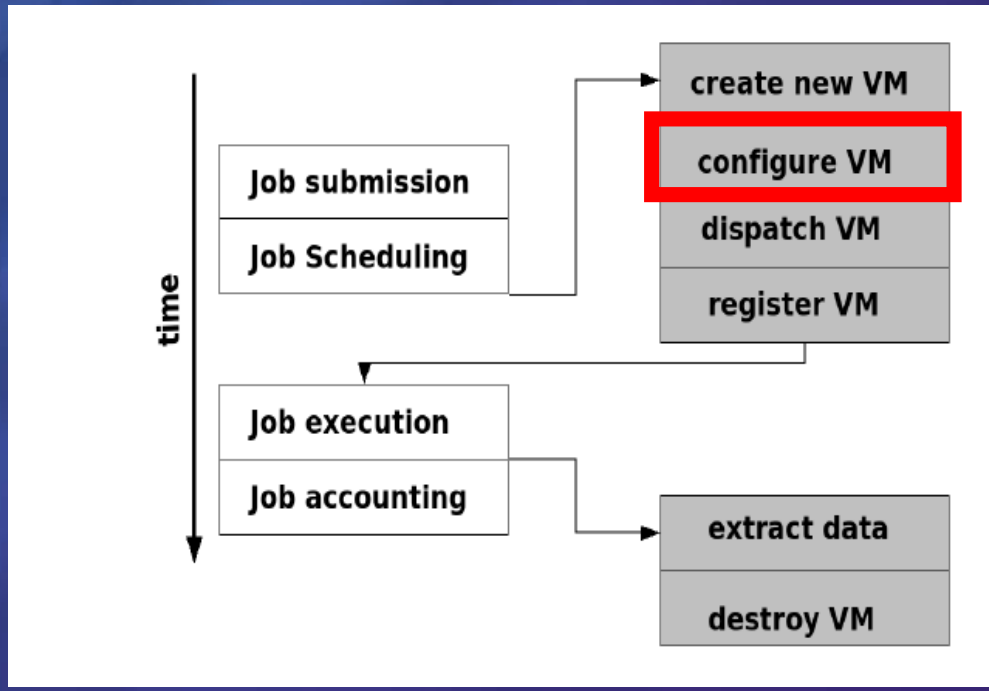
Next Steps

Finished:

- DMZ configuration
- Simple User/VM mapping
- Rough VM configuration

Todo:

- Data separtion on DMZ Headnode
- VO based User/VM mapping
- SLA based VM configuration
- TPM protection of VMs



Publications

- M. Smith, M. Engel, T. Friese, B. Freisleben, G. Koenig and W. Yurcik:
Security Issues in On-Demand Grid and Cluster Computing
Cluster Security (Cluster-Sec), Workshop at the 6th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid), 2006.

- *M. Smith, T. Friese, M. Engel, B. Freisleben*
Countering Security Threats in Service-Oriented On-Demand Grid Computing Using Sandboxing and Trusted Computing Techniques
Journal of Parallel and Distributed Computing (Elsevier)

- N. Fallenbeck, H. Picht, M. Smith, B. Freisleben:
Xen and the Art of Cluster Scheduling
In: *First IEEE/ACM International Workshop on Virtualization Technology in Distributed Computing (held in conjunction with SC06,) Tampa, Florida, IEEE Press, 2006*

- *T. Friese, M. Smith, B. Freisleben:*
Native Code Security for Grid Services
In: Proceedings of 8. Internationale Tagung Wirtschaftsinformatik, (accepted for publication), 2007

- *C. Schridde, M. Smith, H. Picht, M. Heidt, B. Freisleben:*
Secure Integration of Desktop Grids and Compute Clusters Based on Virtualization and Meta-Scheduling
In: Proceedings of the German eScience Conference (accepted for publication), 2007