

Grid Mean Business: Security Management in Grids – A new challenge?

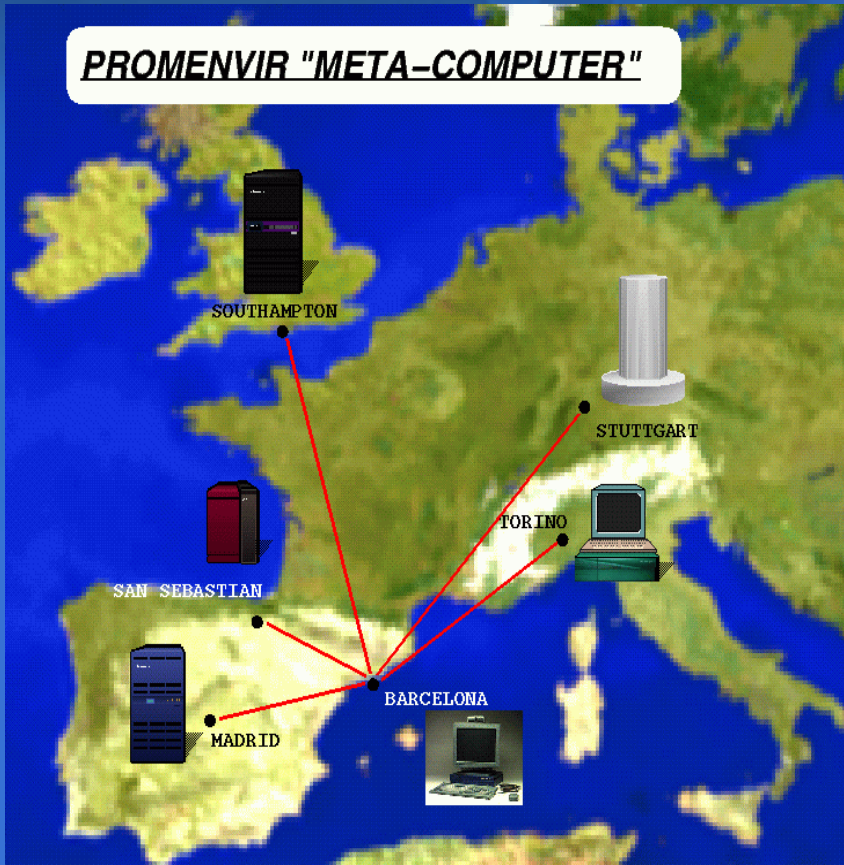
Mike Boniface
(mjb@it-innovation.soton.ac.uk)

OGF20, Manchester
Wednesday 9 May 2007

IT Innovation

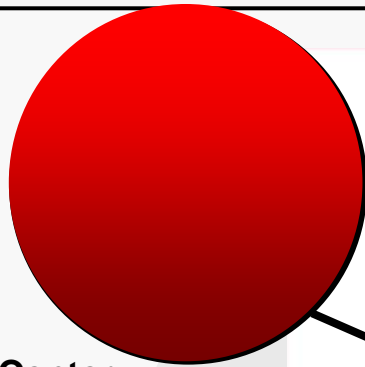
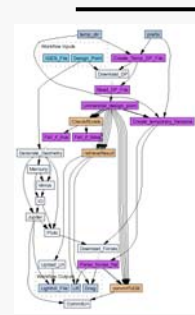
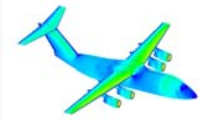
- An applied research centre, complementing the academic research groups in the School of Electronics and Computer Science
- Our objective is the innovative application of IT
- We carry out applied research and development with and for industry and commerce
 - collaborative research (supported by EC and UK programmes)
 - client-funded research, development and consulting
- We deliver proofs-of-concept, demonstrators and novel operational systems

Do You Remember...

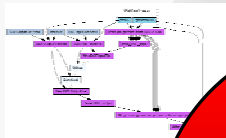


- Probabilistic design environment
- Sensitivity to uncertainties
 - manufacturing tolerances
 - modeling assumptions
- Example applications
 - satellite antennae deployment
 - crash modeling
- Distributed resources
 - 7 sites (3 with firewalls)
 - over 100 processors

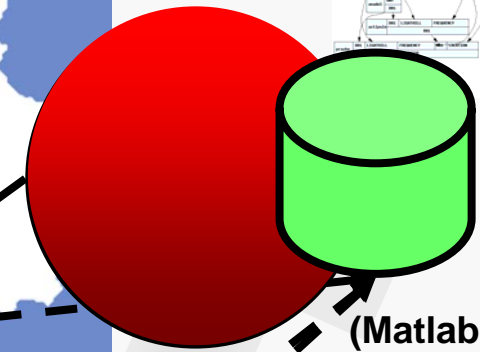
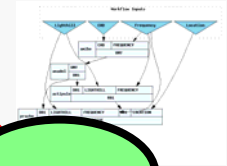
Where are we today?



(Model Center,
SunGridEngine, GRIA)



(iSightFD,
Torque, GRIA)



(Matlab, OGSA-DAI,
Condor, GRIA)

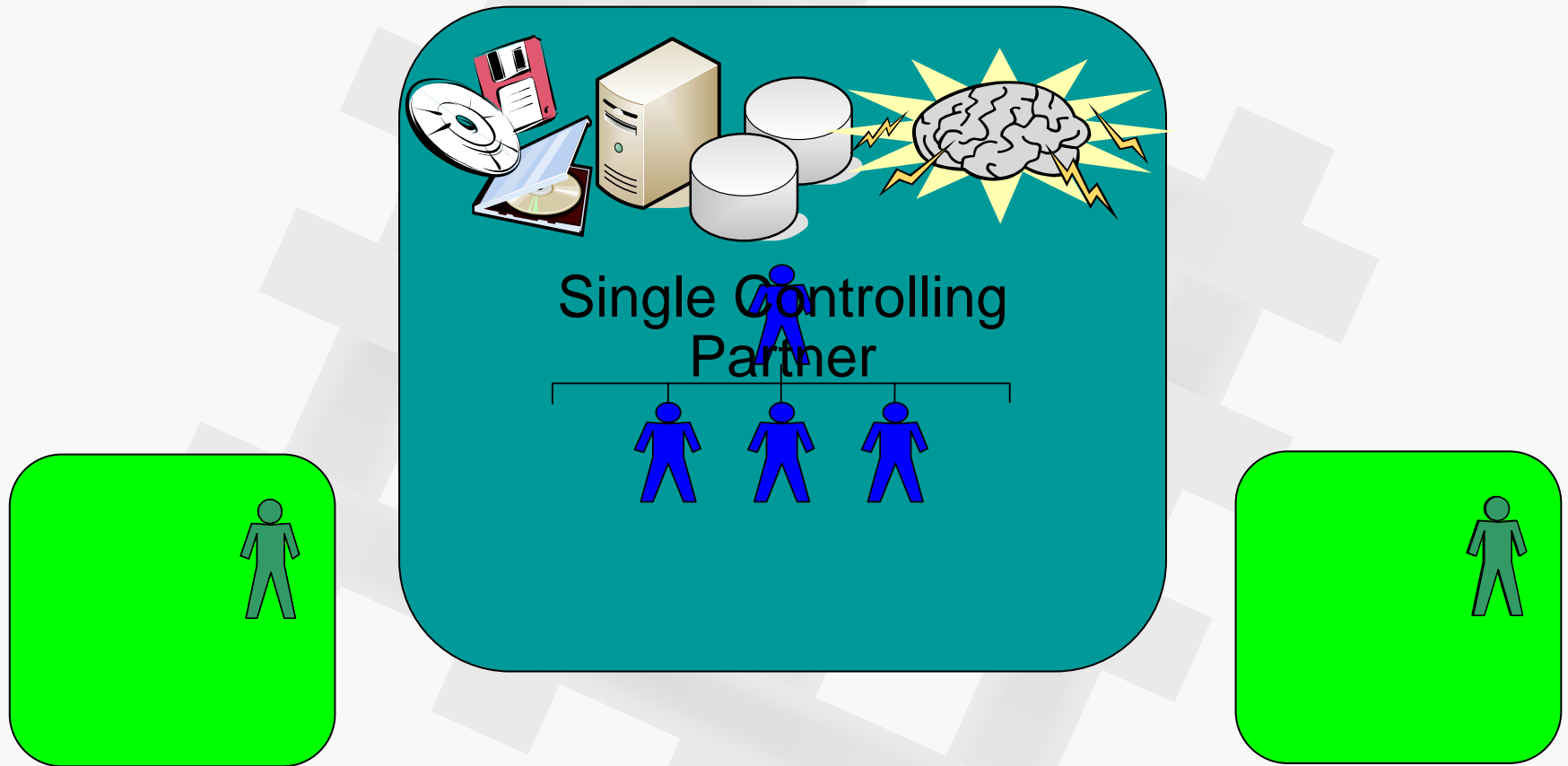


(Patran, GRIA)



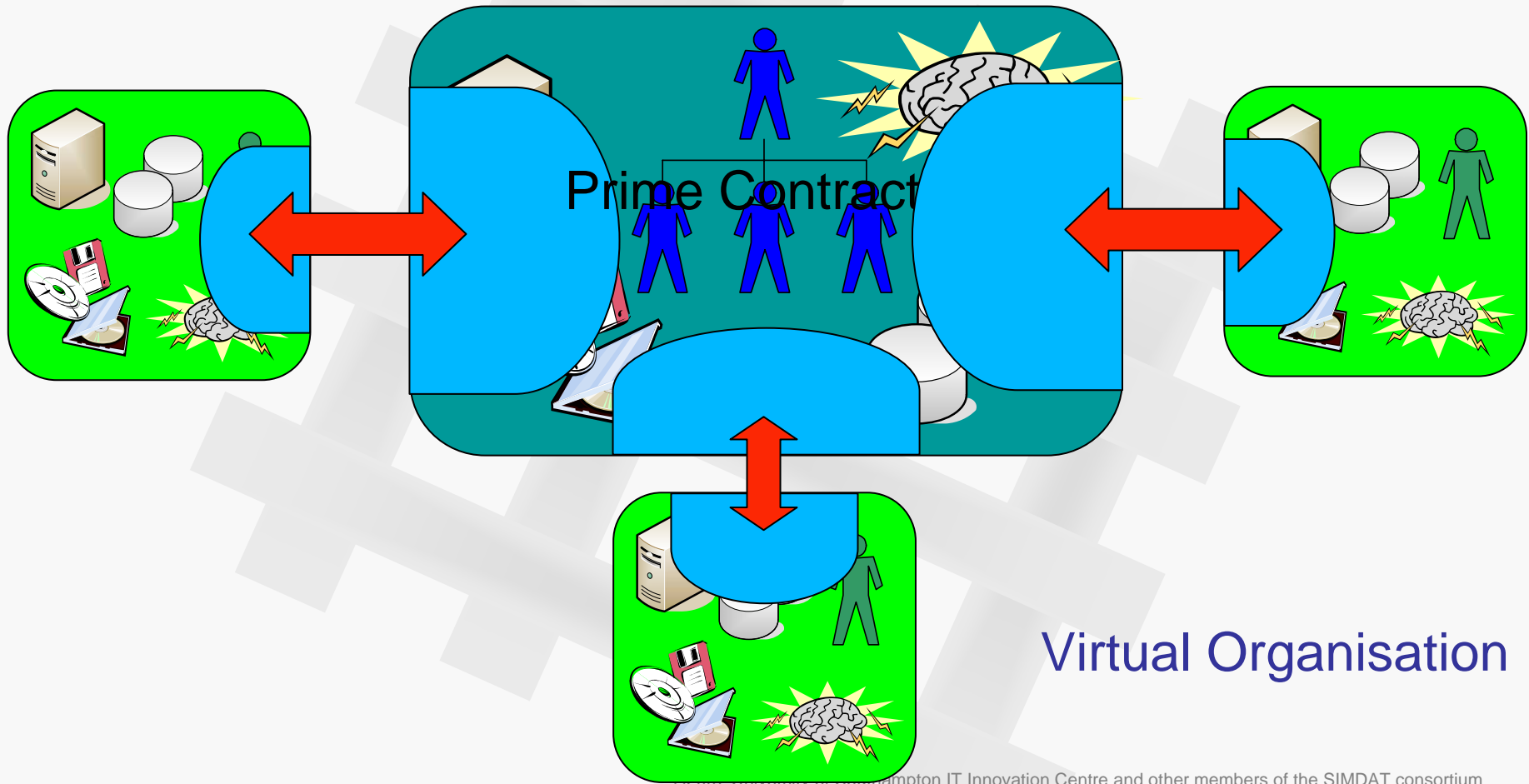
©2007 University of Southampton IT Innovation Centre and other members of the SIMDAT consortium

Contextual Collaboration: *Virtual Employee*



©2007 University of Southampton IT Innovation Centre and other members of the SIMDAT consortium

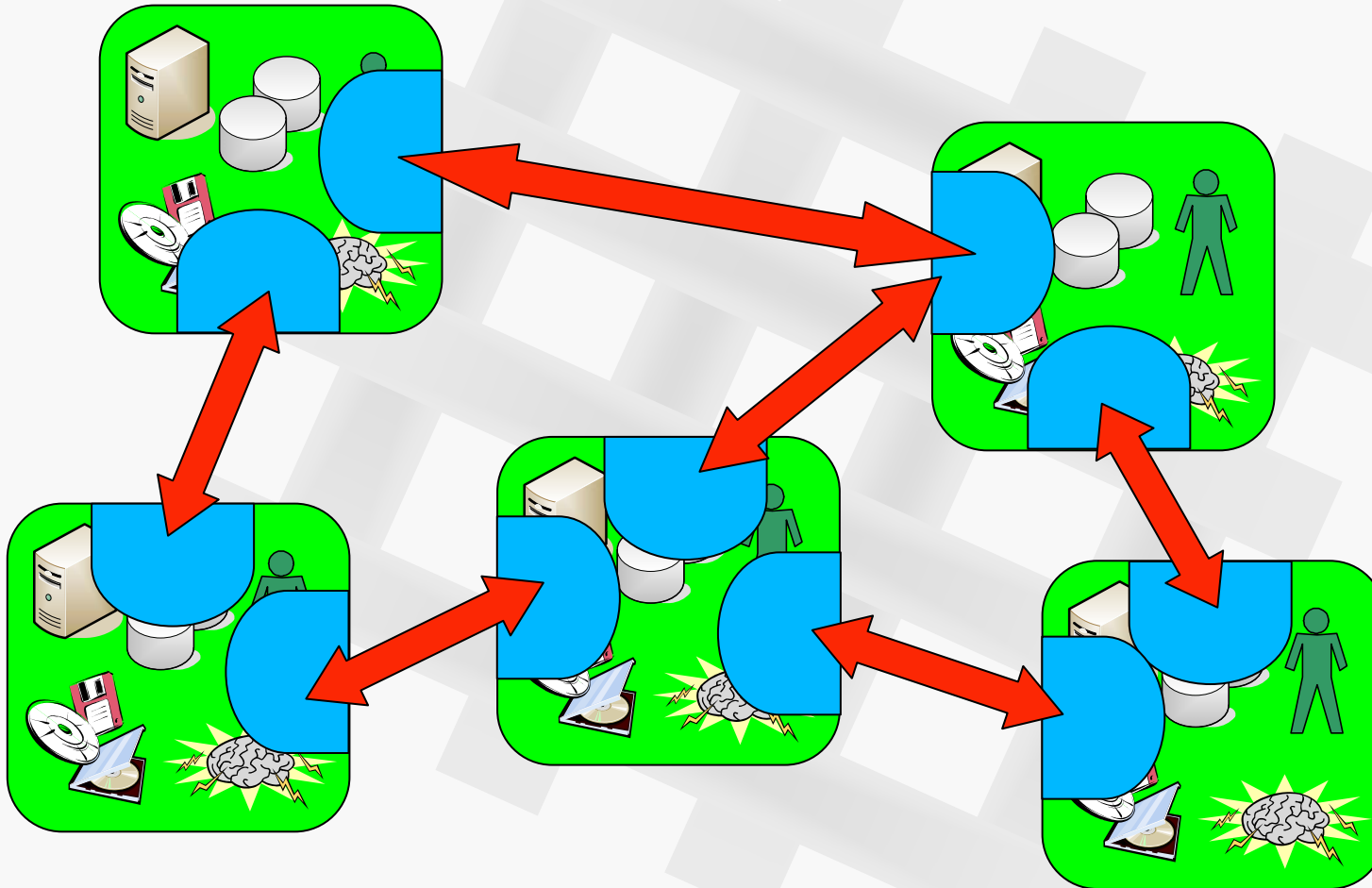
Extended Enterprise: *Business Cooperative*



Virtual Organisation

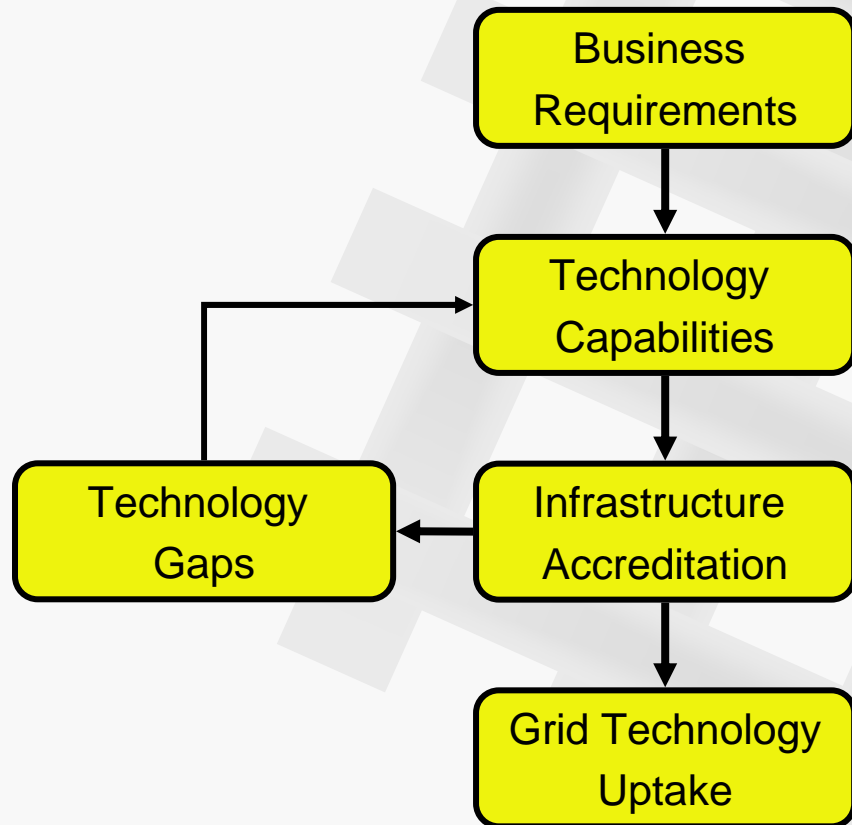
©2004 University of Southampton IT Innovation Centre and other members of the SIMDAT consortium

Extended Enterprise: *Business Partnership*



©2007 University of Southampton IT Innovation Centre and other members of the SIMDAT consortium









Infrastructure Accreditation



- Collaboration patterns
- Operational security policies
- Dynamic trust and security (GRIA)
- SLA management and accounting (GRIA)
- E2E Toolkit (NEC)
- Dynamic Access Control (NEC, IT Innov)
- Transatlantic Secure Collaboration Programme (www.tscp.org)
- Risk analysis

©2007 University of Southampton IT Innovation Centre and other members of the SIMDAT consortium

Operational Security Policies: ISO27001:2005

| Control | Summary of Gap | Procedure update | Existing Technology | Technology Gap |
|---------|--|---|--|--|
| A.6 | Increased complexity of third party risk assessments. |  | | |
| A.7 | Classification of information and labelling across domains |  | | Info Labelling, Monitoring info flows. |
| A.8 | Propagation of user information domains |  | CA's, SLA and Client management services | Monitoring |
| A.10 | Need for secure and trusted audit logs. | | | Auditing, Monitoring, Fault Logging. |
| A. 10 | Shared operational procedures and responsibilities |  | | |
| A.11 | Addition complexity of user management |  | Certificate authorities, PKI, Token services | Integration with existing identity schemes. |
| A.12 | Security in development and support process |  | Grid infrastructure release processes. | Auditing |
| A.12 | Grid vulnerability analysis |  | | Vulnerability analysis tools, Intrusion tolerance |
| A.13 | Reporting of security events in a Grid system. |  | | Monitoring and Reporting tools. |
| A. 15 | Compliance | | | Audit |

©2007 University of Southampton IT Innovation Centre and other members of the SIMDAT consortium

SIMDAT Industrial Grid Profile

- Adoption analysis of key interoperability specifications
- Motivation to
 - ***understand*** adoption of industrial applications (performance)
 - ***recommend*** how the system can be safely adopted by SIMDAT
 - ***publish*** Industrial Grid standards to the community e.g. OGF

©2007 University of



http://www.gria.org/white_papers

SIMDAT

Data Grids for Process and Product Development using Numerical Simulation and Knowledge Discovery

Project no.: 511438

Grid-based Systems for solving complex problems – IST Call 2

Integrated project



D2.2.2 Report on Grid infrastructure interoperability challenges

Start date of project: 1 September 2004

Duration: 48 months

Due date of deliverable: 01/10/2006

Actual submission date: 01/04/2007

Lead contractor for this deliverable: IT Innovation Centre

Revision: 1.0

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Dissemination level

PU

Public

X

16.00 Thursday 10th May
Standards Alignment Report-Out
Charter Suite 5

GRIA: A Grid for business

- Open Source Grid middleware for supporting B2B collaborations based on a service-oriented architecture
- Easy to use yet powerful functionality
 - business-to-business accounting and service level agreements
 - dynamic trust and security
 - distributed file transfer, storage and processing
 - distributed database access using OGSA-DAI
 - distributed inter-domain workflow composition, enactment and publication using Taverna/Freefluo
 - cross-platform, running on Windows XP and various Linux distributions
 - developers kit for new managed application services
- Available free and open source from <http://www.gria.org>

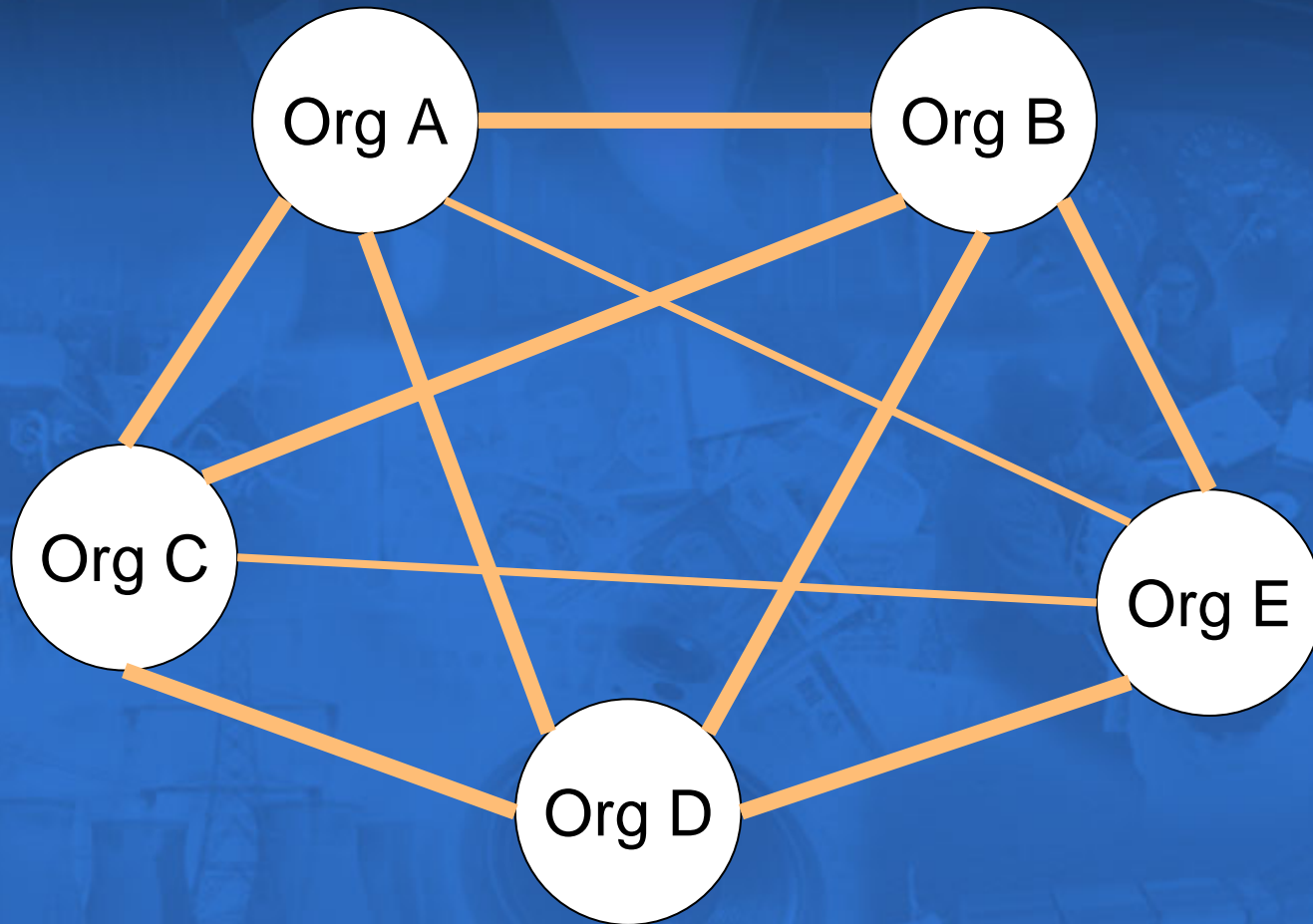
Characteristics of Business Grids

- Customers control which services they consume, how much they are used, and by whom
- Service providers operate independently and maintain control of their own resources
- Service providers operate within the terms of relevant application software licenses
- Services are subject to Service Level Agreements
- Security to commercial standards
- Heterogeneous infrastructures
- Maintenance should be cost-effective

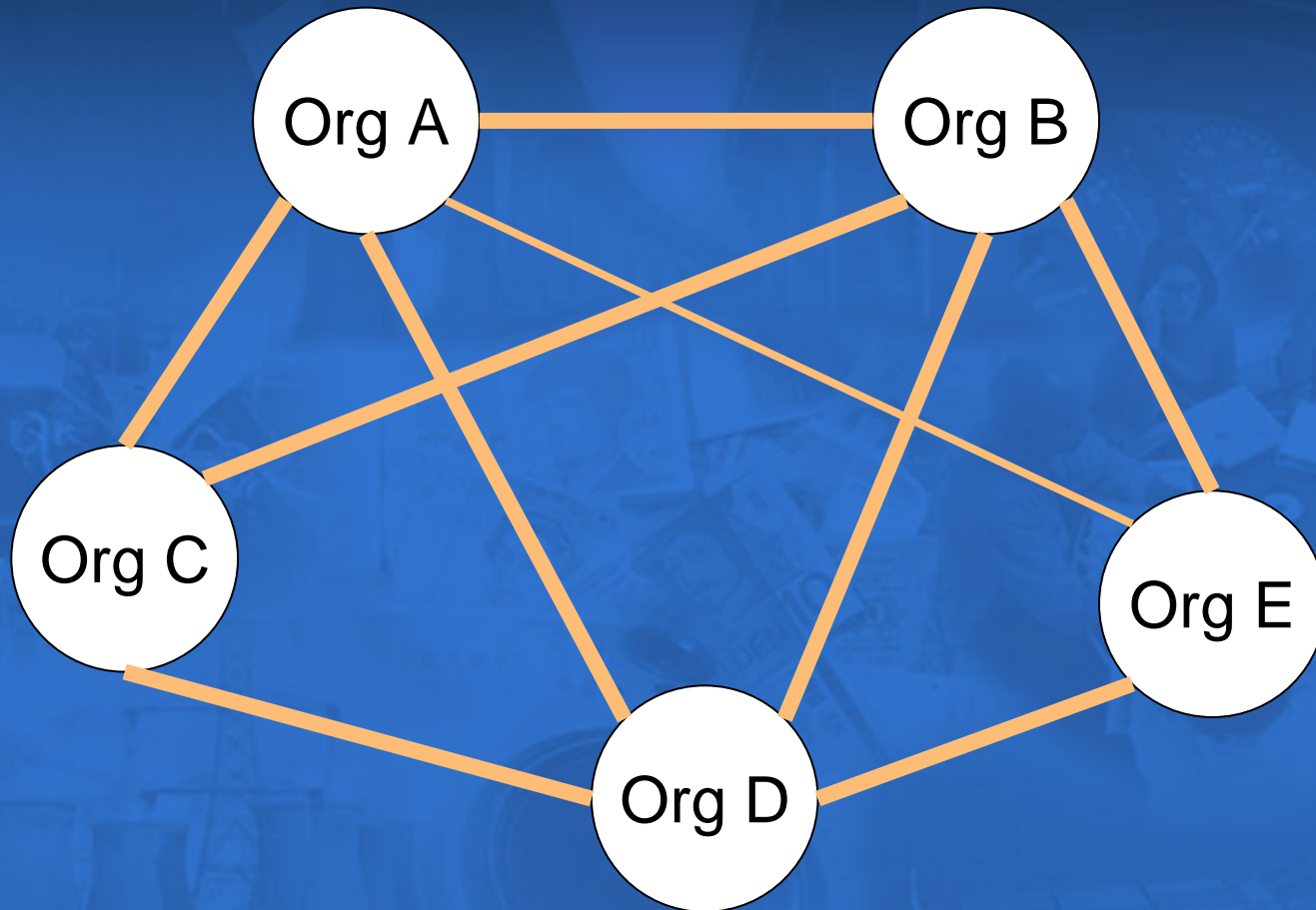
Securing Multi-Organisational SOA

- Traditional systems are “easy” to secure
 - system components are known in advance
 - threats can be anticipated and defences included
 - deployments can be configured to manage threat levels within the system
- Dynamic distributed systems cannot be made secure this way
 - system components and configurations change dynamically
 - system boundaries change as organisations join and leave the application
 - administration is distributed with no overarching threat assessment or management

Trust, Dependency, Intrusion Tolerance



Trust, Security, Intrusion Tolerance



Conclusions

Is security management in Grids a new challenge?

Yes

Thank you for listening



- www.nextgrid.org
- www.simdat.eu
- www.gria.org