

GlobalGridForum

Leading the pervasive adoption of grid computing
for research and industry

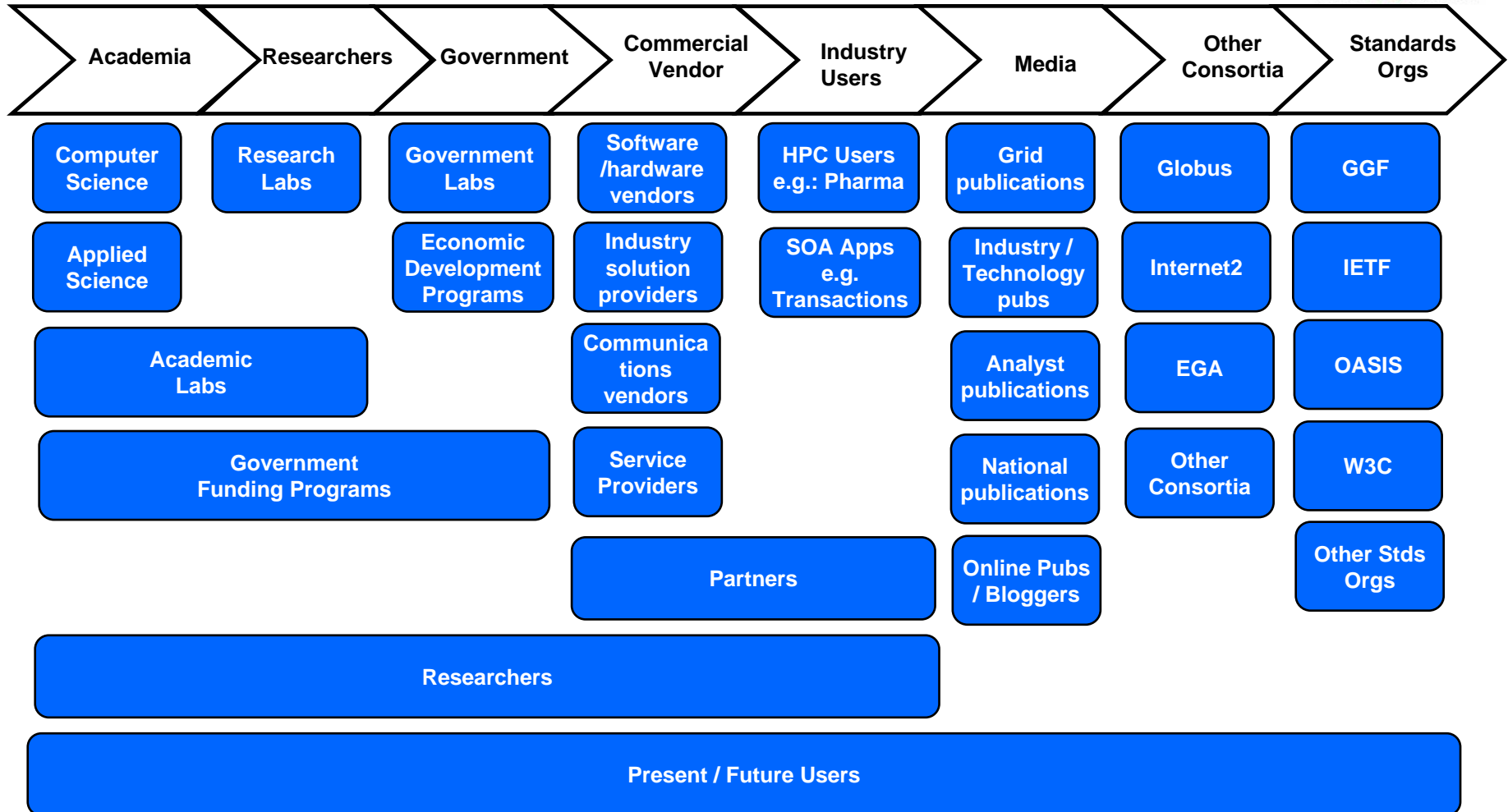
GGF and the Security Area

Olle Mulmo, KTH

GGF Security Area Director & Steering Group Member



Grids: a vibrant ecosystem, many stakeholders



KEY

HPC = High Performance Computing
 SOA = Services Oriented Architecture

Adoption progresses in stages

Scientific/
Technical
Grids



*We are
somewhere
around here*

Commercial/
Enterprise
Grids



Early
Deployments

Momentum Building
(Proven Solutions)

Broad
Adoption

Three Generations of Grid

1

- Local “metacomputers“
 - Distributed file systems
 - Site-wide single sign-on
- "Metacenters" explore inter-organizational integration
- Totally custom-made, top-to-bottom: proofs-of-concept

Three Generations of Grid

1

- Local “metacomputers“
 - Distributed file systems
 - Site-wide single sign-on
- "Metacenters" explore inter-organizational integration
- Totally custom-made, top-to-bottom: proofs-of-concept

2

- Utilize software services and communications protocols developed by grid projects:
 - *Condor, Globus, UNICORE, Legion, etc.*
- Need significant customization to deliver complete solution
- Interoperability is still very difficult!

Three Generations of Grid

1

- Local “metacomputers“
 - Distributed file systems
 - Site-wide single sign-on
- "Metacenters" explore inter-organizational integration
- Totally custom-made, top-to-bottom: proofs-of-concept

2

- Utilize software services and communications protocols developed by grid projects:
 - *Condor, Globus, UNICORE, Legion, etc.*
- Need significant customization to deliver complete solution
- Interoperability is still very difficult!

3

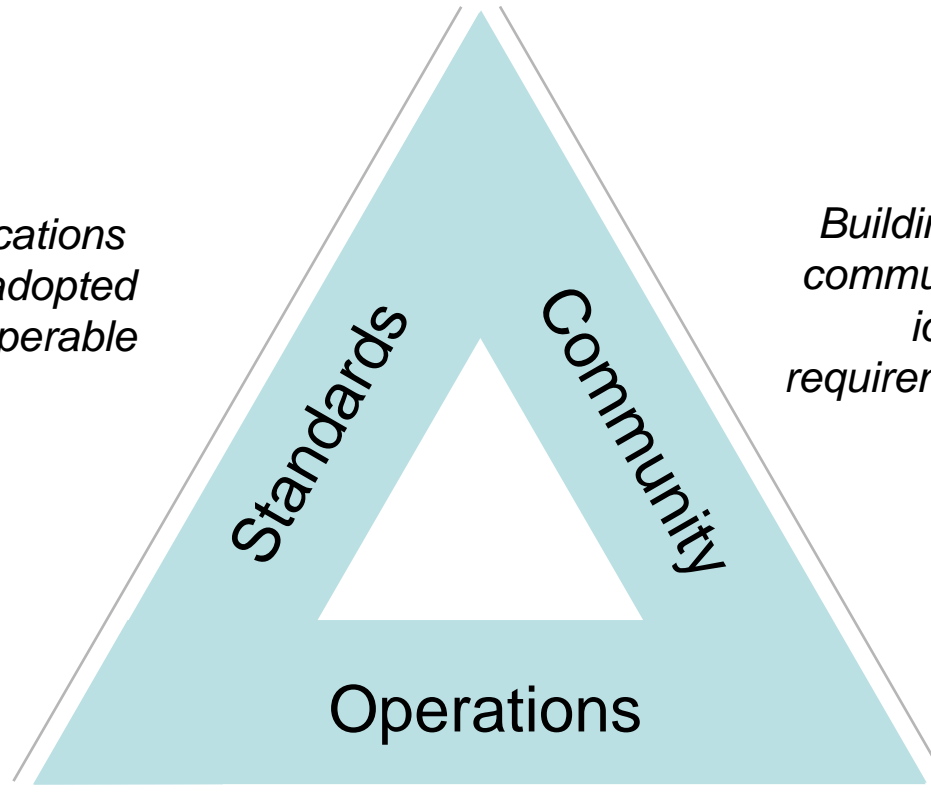
- **Common interface specifications** support interoperability of discrete, independently developed services
- **Competition and interoperability** among **applications, toolkits, *and* implementations of key services**

Standardization is key for third-generation grids!

GGF Mission: Leading the pervasive adoption of grid computing for industry and research



Defining grid specifications that lead to broadly adopted standards and interoperable software



Building a broad international community for the exchange of ideas, experiences, requirements, and best practices

Ensuring ongoing support of our mission and communication of our progress

GGF Activities



Communities/Groups

Research Applications

Industry Applications

Grid Mega-Projects



Technology Innovations

400+ Orgs

50+ Countries

Standards



Best Practices

For Grid

Deployments



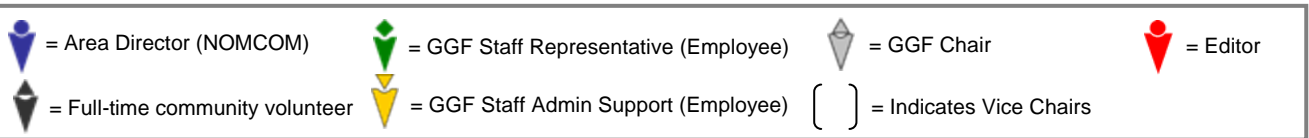
**Interoperable,
standards-based
software**

The GGF organization (evolving)

Still in discussions



Key:

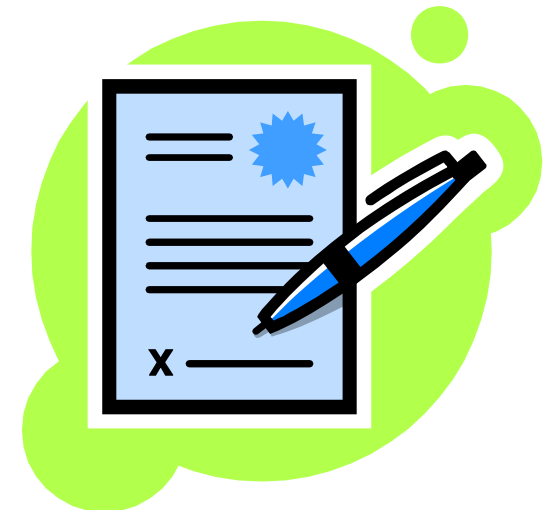


1. Future structure and role TBD

2. Area Directors = 2x number of areas

Recent events

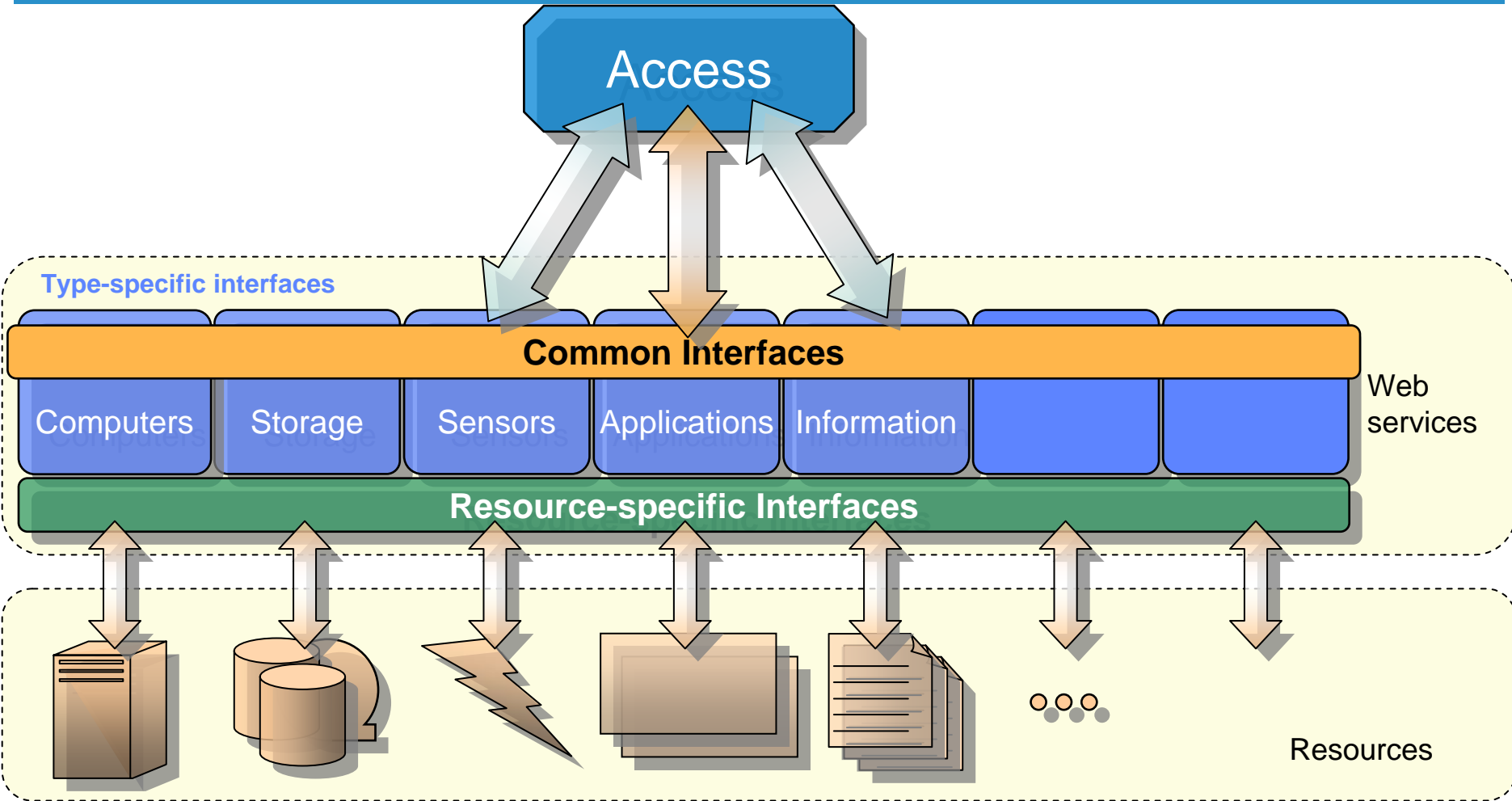
- GGF and EGA recently signed letter of intent to merge
 - For now, business as usual
 - Stay tuned for more information



GGF Groups

- (Standard) Working Groups (WG)
 - Crisp focus on development of a specification, guideline, etc.
 - Clear milestones based on delivery of drafts
- Research Groups (RG)
 - Focus can be broader than WG, but must be clear
 - Organization of workshops
 - Technology exploration
- Community Groups (CG)
 - Explore grid usage and requirement in a particular vertical

Virtualizing Resources



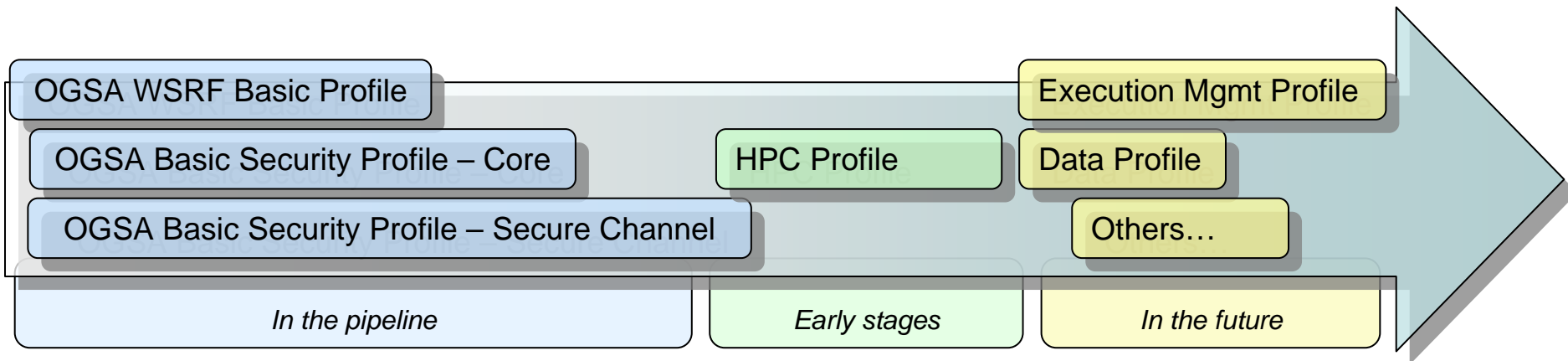


Open Grid Services Architecture, OGSA™

- The “flagship” architecture effort
 - Dynamic service/resource creation and destruction
- “Design Team” Working Model
 - Facilitate cross fertilization within and outside GGF
 - Avoid redundant work applicable efforts
- Profiles
 - OGSA “on top of” WSRF
 - HPC profile of OGSA
 - And so on

OGSA Profiles

- The normative definition of OGSA
 - Styled on WS-I profiles to promote interoperability
 - Define specific usage patterns
 - e.g. execution management
 - Basis for claims of conformance
 - “My scheduler conforms to the OGSA Execution Management Profile...”
- Include specifications developed by GGF **and** by other bodies
 - Issue: How mature and widely adopted?
 - OGSA Profile Definition document provides guidelines



Security activities at GGF

- Certification Authority Operations (CAOPS)
 - Develop operational procedures and guidelines that facilitate the use of X.509 and other technologies for cross grid authentication
 - CP/CPS model
 - Certificate Profile
 - PMA charter
 - OCSP requirements
 - Audit requirements
 - ...
 - Defines documents governing the structure of the regional PMAs (regional collaborating CAs)

International Grid Trust Federation, IGTF (Independent, NOT a part of GGF!)

- Improve trust building through face-to-face contact
- Establish global authentication trust fabric for (academic) production Grids



Security activities at GGF, cont.

- Grid Interoperation Now (GIN)
 - Effort between 18 production Grids to showcase interoperation (not interoperability)
 - Several different middlewares
 - IGTF CAs used for authentication
 - VOMS used for authorization

What about NREN AAls?

- There is no SAML vs PKI war
 - Two complementary technologies
 - One is not a replacement for the other

- Many cross-over efforts underway
 - GridShib, ShibGrid, SHEBANGS, GridShibPermis, MAMS, EGEE, BRIDGES, VOTES, ...
 - inCommon and TAGPMA have discussed common requirements / authentication profile

***See report from Grid and Shib workshop at GGF16
(currently in GGF public comment)***

Security activities at GGF, cont.

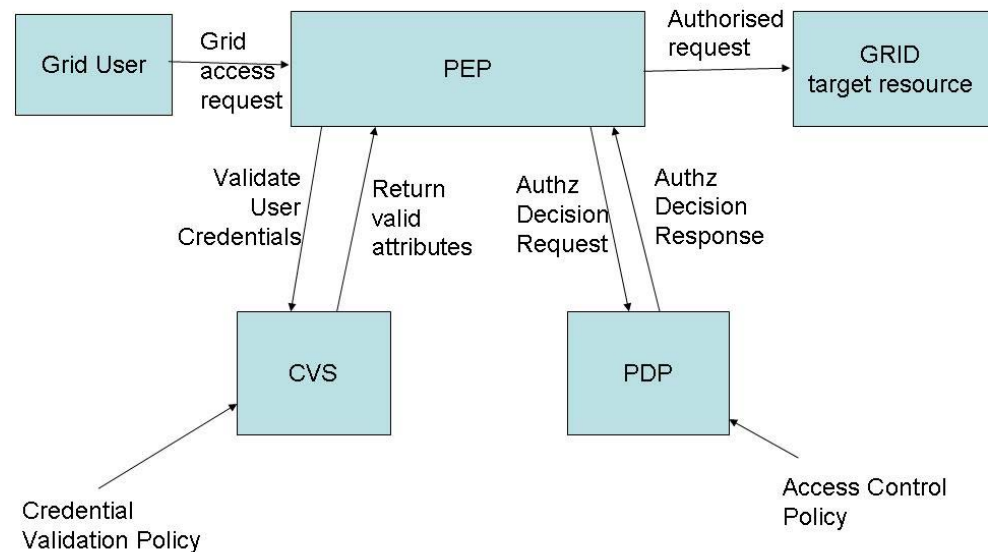
- Firewalls Interest RG (FI-RG)
 - Issues related to Grids and network middleboxes
 - Provide requirements to vendors and IETF middlebox group
 - In particular, emphasis on dynamics

Security activities at GGF, cont.

- Trusted Computing RG (TC-RG)
 - Investigate use of TC technology to improve security
 - Signed executables and run-time environments, credential management, ...

Security activities at GGF, cont.

- OGSA Authorization Group (OGSA-AuthZ)
 - Currently rechartering
 - Authorization protocols, credential formats, and callouts
 - Credential Validation Service
 - Policy propagation





So, what's missing?

... a whole lot!

Security area roadmap

- Sanity check: do we have coverage?
 - Analyze requirements and use cases to find common themes
 - Identify the “blind spots”
- Are we doing the right things?
 - Done lots in AuthN space
 - Done less in AuthZ space
 - Done none in Audit space
- Improve upon the definition of our mission
 - Suggest future work items

GGF Security Roadmap

- GGF is an army of volunteers
 - Lots more to do than we have resources
 - What should we focus on next?
- A first draft is available
- Identifies requirements/themes from “security architecture” efforts
 - EGA requirements
 - EGEE requirements & security architecture
 - GFD.32 : Site-AAA requirements
 - OGSA-Sec arch & roadmap
 - UK e-Science security roadmap
- Use cases from GGF Community function currently being analyzed

“Urgent” results

- A service specification for performing delegation, with profiles for X.509 (proxy) credentials and SAML assertions
- Provisioning / lifecycle management issues (joint with Management area)
- Black-list/white-list service (may also be used as a “Panic-mode button” service)
- Logging: Minimal requirements and operational recommendations

“Moderate” results

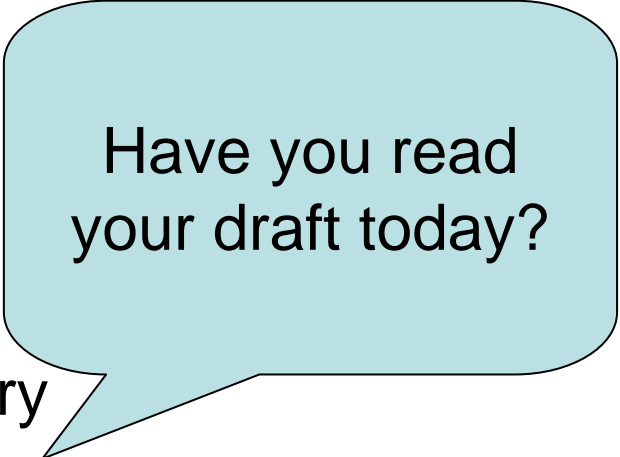
- Auditing: Minimal requirements and operational recommendations
- Credential provisioning
- A simple configuration syntax targeting manual system administration, with clearly defined transformation rules into e.g. XACML
- Mutual authorization
- Simple, initial set of capabilities allowing for constrained delegation

“Other” results

- Policy propagation and combination framework
- Credential validation service

Conclusions

- GGF balances the interest of many stakeholders
- GGF security area is doing lots of interesting stuff
 - This is a huge area, however
 - We could always do more!
 - Would like to see more consumers
- Help kindly solicited
 - Meeting attendance is not necessary
 - Read document drafts, provide input



Have you read
your draft today?

Thank you

**The 17th Global Grid Forum - GGF17
Tokyo, Japan
May 10-12, 2006**



www.ggf.org