Serving a variety of users
with differentiated security levels

evolving the VO Portal Policy

David Groep, Nikhef and the Dutch National e-Infrastructure coordinated by SURFsara
for EGI Security Central Task
This work is supported by EGI-InSPIRE under NA2

e-infrastructure

Distributed Trust

It’s all about risk

Requirements to ponder

Privacy and data protection

- important 'unalienable right' for research
- correlation of PII among service providers could allow profiling
- exchange of PII often fraught with issues

Regulatory compliance

- need to know who you let in beforehand

Incident Response

- long-term* traceable
- independent from short-lived community
- must be revocable
- correlate with other information sources
- banning and containment handle

Access Control Attribute handle

- unique binding
- never re-assigned

Measurement and Accounting

- publication metrics
- usage metering, billing
- auditing and compliance monitoring

identity lives
in a policy ecosystem
to protect all participants

commensurate to their risk level

Risk

‘risk envelope’

Subject (ID/LoA) based

- Defined **identity assurance level**
- **Includes Community-given LoA**
- For given actions, resources, and acceptable residual risk, required ID assurance is a given

Action (app) based

- More constraint actions can lower need for identity LoA
- **(J)SPG VO Portal policy** does that: 4 levels of actions

Resource (value) based

- e.g. access to wireless network does not pose huge risks, so can live with a lower identity LoA (eduroam)

Residual Risk:

Determine the risk envelope

- What are you willing to accept
  - Cost of monitoring to assess/retain systems integrity
  - Cost of recovery in case of incidents (time, money, consultancy costs)
  - Benefits of having more (paying) users
  - Benefits of appearing ‘low-barrier’

- Considerations
  - Your ‘outside’ risk envelope should stay the same – determined by local regulation,
    by the AUPs of your network peers,
    and by your (media) exposure and reputation status

Within the ‘usual’ envelope

VO portal policy

https://documents.egi.eu/document/80

- off-set lower (identity) assurance by limiting actions
- differentiates levels of ‘impact’ on the infrastructure

- Aims to retain *critical traceability elements* across all service and sites – incidents must not be allowed to flow from low impact > high impact services
- Mixing risk levels in the same system (e.g. in a single batch compute cluster, shared storage): *not* a good idea!

Service stratification

1. **Web Rendering** (“Closed Self-Contained Simple One-Click”)
   use a Robot certificate, but no identification of end user. Portal must keep list of source IPs
   Infrastructure use must be stateless and rate-limited
2. **Parameter sweeping**
   User provide verified email address or pseudonym (must be human)
   Robot cert for portal or user’s real credential
   Infrastructure use rate limited and stateless (copy data back to portal)
3. **Data Processing portals**
   Identified users (well-verified email address, known domains) or better
   … e.g. anyone with an IdP in eduGAIN, or people ‘known’ to the service
   Portal may use robot or user credential
   Use rate-limited, and store output only in pre-agreed locations on the infrastructure
4. **Job Management portals**
   use strong named user credentials via, e.g. SLCS, MICS (TCS), Classic

Current VO Portal Service

Portal Classes today in DocID#80			
Portal Class	**Executable**	**Parameters**	**Input**
Simple one-click	provided by portal	provided by portal	provided by portal
Parameter	provided by portal	chosen from enumerable and limited set	chosen from repository vetted by the portal
Data processing	provided by portal	chosen from enumerable and limited set	provided by user *(and output to designated resources)*
Job management	provided by user	provided by user	provided by user

Next steps

We need to evolve the VO portal policy

- It's not actually about portals, but about services
- The classification per risk provides a starting point
- Outside the current risk envelope there is a wider world
  - but these should *not be mixed inadvertently* to prevent incidents from spreading like worms

- **The aim to have available, useful services!**
  - So Keep a close watch on traceability
  - or you will not know what bit you
    … and worse it makes consistent recovery impossible