GridPP36 Security Report

Ian Neilson
GridPP Security Officer

Security Report

- Operational Security
- Policy Updates
- Collaborations & Projects
- Future Work
- ARGUS Ban Tests

Operational Security (1)

- EGI CSIRT : WLCG & EGI Incident Response Team
  - EGI-Engage (30 months from March 2015)
  - EGI Security Officer: Sven Gabriel, Nikhef
  - IRTF Coordination: Vincent Brillault, CERN
    - 7 NGI reps. core team, weekly on duty rota
    - ~450 tickets to sites (5 UK) in last 12 months
    - 5 “critical” vulnerability campaigns --> ~20 sites suspended (0 UK)
    - 5 incidents
      - 1 Asia | 2 reported by CESNET | 2 from UK
  - Monitoring Tools: Daniel Kouril, CESNET
    - Pakiti, Nagios, EGI Dashboard integration
      - Correlation across tools still labour intensive --> ? Dashboard
    - VMI scanning – FedCloud/AppDB
  - Security Co-ordination: Dave Kelsey
    - Policy and Vulnerability Groups
    - Monthly and F2F meetings

Operational Security (2)

- UK NGI Security Team
  - Generic reporting address for UK NGI
  - Support and cover for GridPP Security Officer
    - David Crooks replaced Ewan MacMahon
    - Jeremy Coles, Ian Collier, David Crooks, Linda Cornwall, Alessandra Forti, Rob Harper, Dave Kelsey
  - ~Twice monthly phone conferences
    - Site patching follow-ups
    - EGI procedures feed-back (pakiti & RT tickets)
    - ARGUS, proxy length, glexec ….

Policy & Procedure Updates (1)

- AUP
  - Generalise to include all EGI service offerings
    - Grids, Clouds, Long Tail of Science, etc.
- Policy on VM Endorsement and Operations
  - Responsibilities and requirements for VMs in EGI AppDB
  - Roles: Endorser, Operator, Consumer
    - https://documents.egi.eu/secure/ShowDocument?docid=2729&version=3
- Data Protection Policy
  - Processing of Personal Data based on “Binding Corporate Rules”
  - International Transfers & looking forward to GDPR in 2018
    - http://indico.cern.ch/event/394776/
- LToS Platform Security Policy
    - https://documents.egi.eu/public/ShowDocument?docid=2734

Policy & Procedure Updates (2)

- SVG Security Threat RA - with cloud focus
  - Lead: Linda Cornwall
  - Likelihood x Impact assigned to 103 threats in 19 categories
    - https://documents.egi.eu/secure/ShowDocument?docid=2653
      * *Security incidents and incident handling in the EGI federated cloud, ...*
      * *The proliferation of software and technology in use in the infrastructure ...*
      * *Whether there is sufficient manpower to carry out security activities ...*
      * *Compliance with policy ...*
- Updates to:
  - SVG Vulnerability Assessment Process
  - CSIRT Critical Vulnerability Handling Procedure
  - CSIRT Incident Handling Procedure (ongoing)

Projects (1)

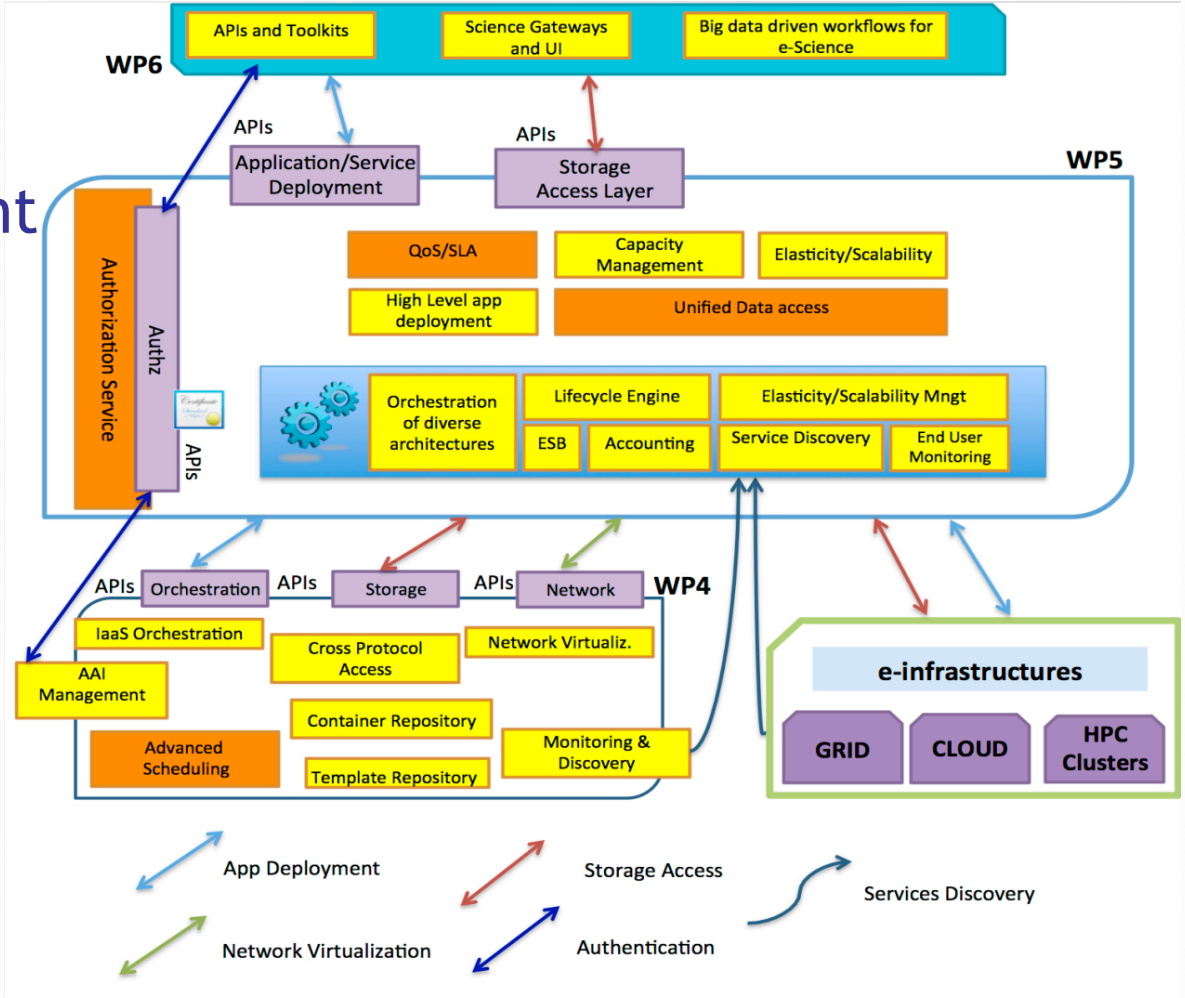
- Executive Summary: Lots of work on Federation
- AARC: Authentication & Authorisation for Research & Collaboration
  - Started May 2015 (2 yr): https://aarc-project.eu/
  - *".. integrated cross-discipline AAI framework, built on production and existing federated access services."*
  - *PoC End-to-end AAI pilots built on existing services*
  - *Policy and best practice harmonisation - LoA, Data Protection, Incident Response ….*
  - *Training and outreach for IdPs and Service Providers*
- SIRTFI: Security Incident Response Trust Framework for Federated Identity
  - https://refeds.org/sirtfi
  - *".. enable the coordination of incident response across federated organisations."*
  - *".. defines a set of capabilities and roles associated with security incident response that an IdP or SP organisation self-asserts."*

Projects (2)

- WISE: Information Security for collaborating E-infrastructures
  - Workshop Oct 2015: https://wise-community.org/
  - GEANT SIG-ISM (NRENS) and SCI (Infrastructures – EGI, OSG, PRACE, EUDAT, XSEDE)
  - How to share best practice, risk assessment, establish trust, ….
    - *https://www.terena.org/activities/ism/wise-ws/agenda.html*
  - *Working Groups: SCI2; Training; Risk Assessment; Audit; Big Data*
- INDIGO-DataCloud:
    - https://www.indigo-datacloud.eu/the_project
  - ".. software to simplify the execution of applications on Cloud and Grid based infrastructures .. HTC & HPC .."

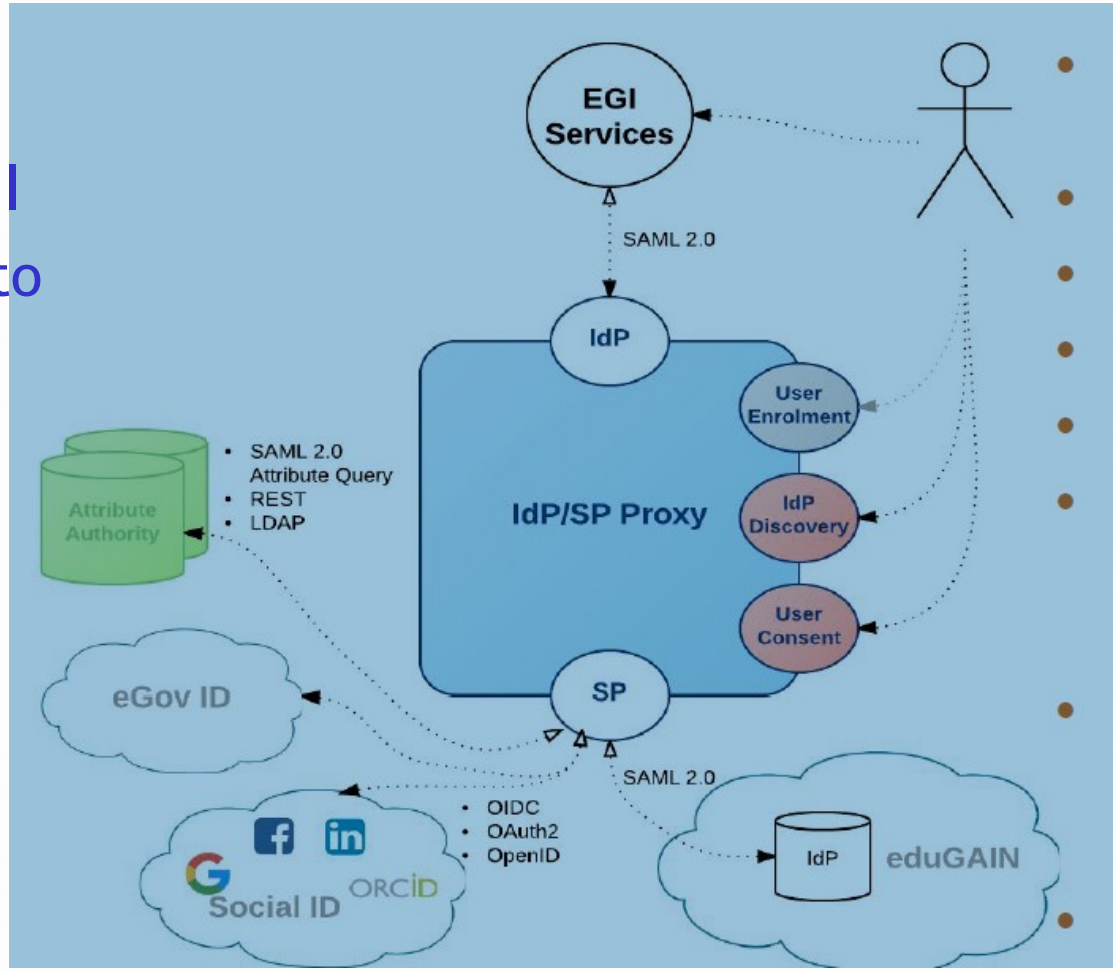
Projects (3)

- Indigo-DataCloud
- AAI – Identity and Access Management
  - Login service
  - Groups service
  - Authz service
- Token translation
  - OIDC base token
  - S3, ssh, X.509



Projects (4)

- EGI AAI
- SP/IdP Proxy
  - 1 for whole EGI
  - Acts as Service to an Identity Provider
  - Acts as Identity Provider to a Service
  - Attribute Aggregation



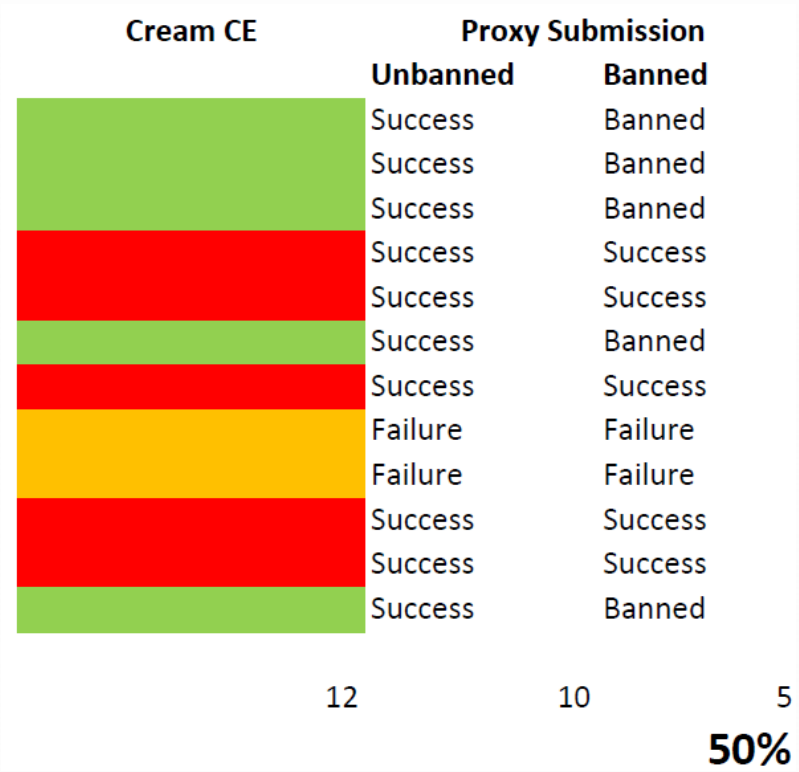
Projects (5)

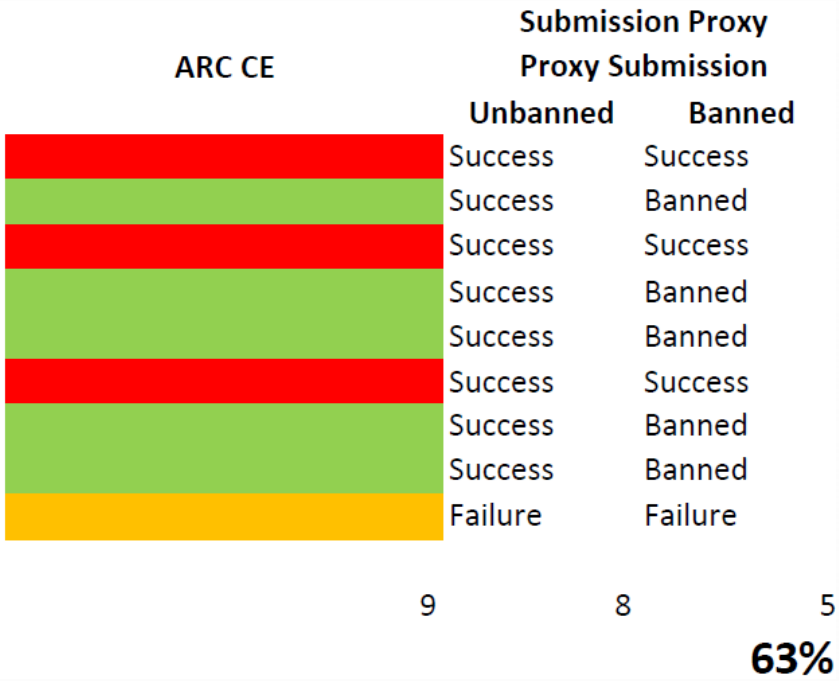
- WLCG
  - Security Sessions at Collaboration Workshop + GDB
  - “Deployment of glexec will be frozen”
    - Does not mean traceability policy requirements have gone away
  - 2 new Security WG’s recognising increased reliance on VOs
    - Traceability tools – V. Brillaut, CERN
      - » VMs/Containers/cgroups
    - Monitoring – D. Crooks, Glasgow
      - » ? Monitoring appliance

UK ARGUS ban testing

- 2 certificate DNs registered in VO gridpp (ops?)
  - /C=UK/O=eScience/OU=CLRC/L=RAL/CN=ian neilson (ukngi sec)
  - /C=UK/O=eScience/OU=CLRC/L=RAL/CN=ian neilson
  - Get one banned (used to test “emergency ban” ☺)
- Generate lists of target resources
  - *e.g. lcg-infosites --vo gridpp se*
- Scripts to run jobs
  - CREAM & ARC CEs: curl a non-existent file from a web server
    - Can see the access in the httpd logs to be sure job ran (or not).
  - SEs: *gfal-copy* local -> remote
    - Job fails to submit with banned cred.

UK ARGUS tests -CEs





UK ARGUS tests - SRM

Summary Stats

Cream CE	50%	12	10	5
ARC CE	63%	9	8	5
SRM	31%	18	16	5

Looking Forward

- All of the above!
- Operations
  - ARGUS clean-up
  - Communications Challenge
  - Security Service Challenge
    - Previously EGI co-ordinated SSCx, now focus is on FedCloud.
    - ? Challenge for the UK ?
- Training
  - HEPSYSMAN – Leif Nixon, pen-test workshop
  - ? EGI Roleplay exercise – run at ISGC

Thank You.