EGI Security – Introduction, Security Policies & Trust Frameworks

EGI/INDIGO conference/summit, Catania
10 May 2017

David Kelsey (STFC/RAL)

Security Coordination Group (SCG)

Security operations, including monitoring and training (CSIRT)

Incident Response (IRTF)
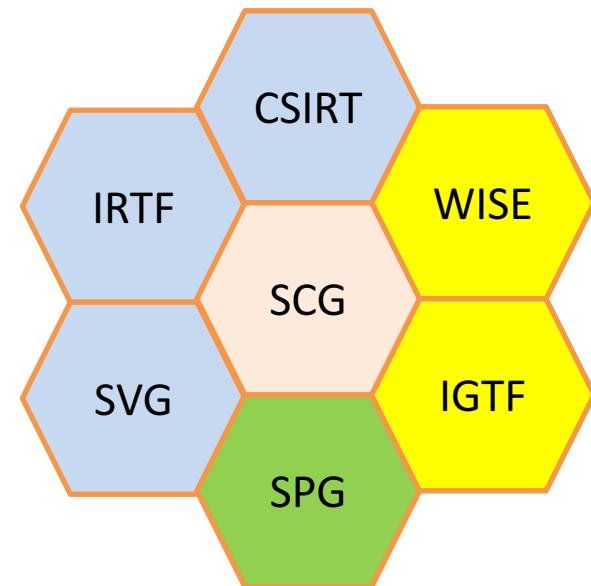
Software Vulnerabilities (SVG)

Security Policy (SPG)

Interoperable Global Trust
        Federation (IGTF)

Wise Information Security for
        Collaborating
        e-Infrastructures (WISE)

EGI-Engage security evolution

EGI-Engage – WP5 task SA1.2

- *Develop security operations, including policies, procedures and best practices, to meet the requirements of new trust models, new developments and new usage scenarios as these evolve*

- Five activities
  - *security requirements and risk assessment*
  - *evolution of operational security procedures, incl. forensics*
  - *new trust frameworks and new policies*
  - *develop the security challenge framework*
  - *develop the software vulnerability handling processes*

- More details
  - EGI-Engage deliverable D5.3 - *https://documents.egi.eu/document/3027*
  - Paper submitted to the proceedings of the ISGC2017 conference, Taipei
    - "**Coordinating Operational Security in evolving distributed IT-Infrastructures**"

Agenda – today's session

Introduction	*David KELSEY*
Room: F1	*16:30 - 16:35*
Security policy and Trust frameworks	*David KELSEY*
Room: F1	*16:35 - 16:50*
Software Vulnerability Group	*Linda CORNWALL*
Room: F1	*16:50 - 17:05*
Security Monitoring in EGI	*Daniel KOURIL*
Room: F1	*17:05 - 17:20*
Incident prevention & resolution	*Vincent BRILLAULT*
Room: F1	*17:20 - 17:35*
EGI CSIRT: Keeping the Infrastructure Secure	*Dr. Sven GABRIEL*
Room: F1	*17:35 - 17:50*
Questions and Discussion	
Room: F1	*17:50 - 18:00*

Security Policy and Trust Frameworks

Aims of EGI Security Policy Group

- Develop and maintain security policy for use by the EGI Community

- Provide policy advice

- Work with other infrastructures and activities
  - Make policies simple and general

Currently adopted policy available at:

https://wiki.egi.eu/wiki/Policies_and_Procedures

https://wiki.egi.eu/wiki/SPG:Documents

EGI security policies

1 EGI Approved Security Policies

1.1 Top-level EGI Security Policy:

- e-Infrastructure Security Policy 🔒 (Updated 1 Feb 2017)

1.2 For all Users:

- Acceptable Use Policy and Conditions of Use 🔒 (Updated 10 Oct 2016)

1.3 For all Sites:

- Service Operations Security Policy 🔒 (Updated 1 June 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images 🔒 (Updated 10 Oct 2016)

1.4 For all VOs:

- VO Operations Policy 🔒
- Virtual Organisation Registration Security Policy 🔒
- Virtual Organisation Membership Management Policy 🔒
- VO Portal Policy 🔒 (Updated 14 Nov 2016)
- Service Operations Security Policy 🔒 (Updated 1 June 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images 🔒 (Updated 10 Oct 2016)

1.5 General policies

- Security Traceability and Logging Policy 🔒 (Updated 14 Nov 2016)
- Security Incident Response Policy 🔒 (Updated 14 Nov 2016)
- Policy on the Processing of Personal Data 🔒 (New policy from 1 Feb 2017)
- Policy on Acceptable Authentication Assurance 🔒 (Updated 1 Feb 2017)
- Policy on e-Infrastructure Multi-User Pilot Jobs 🔒 (Updated 14 Nov 2016)
- Grid Policy on the Handling of User-Level Job Accounting Data 🔒

1.6 Policies with specific scope

- EGI Access Platform Security Policy 🔒 (aka. Platform for the long tail of science)
- Access Platform AUP and Conditions of Use 🔒 (aka. Platform for the long tail of science)

1.7 Glossary of terms used in SPG policy documents:

- EGI Glossary V2 🔒
- Security Policy Glossary of Terms 🔒

Why have we updated the policies?

- To generalise beyond classic HTC use cases

- To cover new and evolving EGI services
  - EGI FedCloud service, LToS (applications on demand), etc.
  - Work with FedCloud on deployment (AppDB)

- To address data protection issues in more general way

- To address new IGTF work (Levels of Assurance)

- Update references and glossary terms used

New & revised policies

- Adopted in 2016
  - Acceptable Use Policy and Conditions of Use
  - Endorsement and operation of virtual machine images
  - VO Portal Policy
  - Traceability and logging
  - Security incident response
  - Multi-user pilot jobs
  - EGI Access platform - Applications on demand (LToS)
  - EGI Access platform – AUP and Conditions of Use (LToS)

- Adopted in 2017
  - Top-level Security Policy
  - Policy on the processing of personal data
  - Acceptable Authentication Assurance

Future revision of policies

- Before end of EGI-Engage (31 Aug 2017)

- Revise old VO security policies
  - VO Registration policy
  - VO Membership management
  - VO Operations

- Will aim for 2 policies
  - One to control interface between Infrastructures and Communities
  - One to control interface between Communities and Users

- SPG role in assessment of VO identity proofing
  - For IGTF DOGWOOD assurance (IOTA CA)

Other policy and trust activities

AAI and Identity Trust Frameworks

- In collaboration with EGI-Engage JRA1.1
  - Also with IGTF, FIM4R, REFEDS and EU H2020 AARC project
- Much of this covered in other sessions this week
- IGTF – new levels of assurance - evolving trust anchors
  - Pilot with WLCG IOTA CA
  - Identifier-only trust services
- Input to REFEDS Sirtfi and AARC Snctfi trust frameworks

- Wise Information Security for e-Infrastructures
  - SCI & GEANT SIG-ISM together – first meeting Oct 2015
  - Excellent way of collaborating with other Infrastructures
    - EGI, EUDAT, PRACE, GEANT, NRENs, WLCG, XSEDE, OSG, HBP, …
  - EGI people on WISE steering committee
  - Leading the SCIV2 working group
    - Security for Collaborating Infrastructures
    - Include more stakeholders (GEANT and NRENs)
    - SCI version 2
      - published before and endorsed at TNC17 Linz (1 June)

Thank you for your attention.

Questions?