EGI/WLCG Security Policies

David Kelsey (STFC-RAL)

WLCG GDB, CERN, 8 July 2015

www.egi.eu

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Outline

- Some time since last update (GDB June 2013)
  - But there is activity in many different areas!
- Ongoing EGI SPG activities
  - Revised User AUP
  - Revised VM Endorsement & Operations policy
- WLCG policy needs
  - Federated Identity and use of IGTF IOTA
  - Personal Data Protection issues (also for EGI)
- Other topics not discussed today
  - SCI (GDB July 2013) and SIRTFI/AARC (see Romain)

User AUP

AUP revision to address

- Generalise to include all EGI service offerings
  - Grids, Clouds, Long Tail of Science, etc.
- Require: acknowledge support in publications
- Liability issues

https://wiki.egi.eu/wiki/SPG:Drafts:Acceptable_Use_Policy_March_2015

- New version was distributed for public comment
  - A few comments received BUT
- Legal advice: more work needed on handling of data protection and its implications for the AUP

VM Endorsement & Operation

- Modify the policy and trust issues
  - To reflect current use cases
- Important for EGI Federated Cloud Services
  - New trust and responsibilities
- We produced an initial first draft
  - VM Operator – responsible for all security aspects
  - VM Consumer – end user with no privileges
- Worked on during EGI Conference Lisbon (May)
- *https://wiki.egi.eu/wiki/SPG:Drafts:Virtual_Machines_Endorsement_Policy_March_2015*
- Will soon be distributed for public comment

Personal Data Protection

- Currently we have a policy on "User-level Job Accounting Data"
  - Data Protection issues related to User DN in X.509
- Experience in recent months shows we need to generalise this to cover **all** forms of logging
  - Accounting, monitoring, VO monitoring, VO registration data, security audit logs, …
- And user needs to be informed of Policy whenever they register/use a service
- The GEANT Data Protection Code of Conduct

http://www.geant.net/uri/dataprotection-code-of-conduct/Pages/default.aspx

  - Rules for Service Providers on handling personal data so that IDPs will release attributes

Data Protection (2)

- But to transfer data outside of the EU
  - Need to use the "International Code of Conduct"
  - Some way off being finalised
  - And also requires MANY bi-lateral contracts between IDPs and SPs
- Now evaluating the use of a single policy
  - "Policy on the Processing of Personal Data"
  - All EGI/WLCG participants are bound to this
  - And enforcement/sanctions by rules of the Infrastructures
  - "Binding Corporate Rules" for international data transfer

Note on complexities of EU Data Protection

- The European Union is currently moving from the old 1995 Directive on Data Protection to a new Regulation
  - for agreement by end of this year?
  - and adoption in the following two years?
- "…all three components of the European law making process have now produced their proposed texts for a General Data Protection Regulation."
  - Parliament
  - European Commission
  - Council of Ministers
- There are significant differences!

Federated Identity and IGTF IOTA

- WLCG pilot studies – use of Federated Identities
  - Vital part of move away from user managed X.509 certificates
  - Certificates produced by dynamic Security Token Service
- Use new IGTF Profile – "IOTA" (GDB Dec 2013)
  - No requirement for face to face identity vetting
  - The robust identification is done by the LHC VOs
- BUT Trust in CA is per site and not per VO
  - So need mechanisms to restrict certificates to VO members
- A new policy recommendation is being worked on for presentation to the WLCG MB

Thank you for your attention.

Questions?

www.egi.eu

This work by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License.