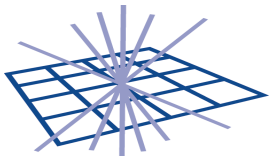
Security Update

WLCG GDB

CERN, 12 June 2013

David Kelsey

STFC/RAL



GridPP

UK Computing for Particle Physics

Overview

- A VERY long time since I gave a Security Update
  - Much to talk about (this will be rushed!)
- IGTF news
  - SHA2 etc
- Revised Security Policies
  - Service Operations
  - AUP
- Security for Collaborating Infrastructures (SCI)
- Security operations

IGTF news

- I attend EUGridPMA and TAGPMA meetings
  - Representing WLCG as a "Relying Party"
- Many recent developments
  - But today just report on some!
- TAGPMA meeting 6-7 May 2013
- EUGridPMA meeting 13-15 May 2013
- Thanks to David Groep for the following slides
  - Shown to the EGI OMB
- Summary of EUGridPMA meeting at: https://www.eugridpma.org/meetings/2013-05/eugridpma-kyiv-summary-20130515.txt

SHA-2 time line agreed

- **Now**
  - CA certificates in the IGTF distribution and CRLs at official distribution points should use SHA-1
  - CAs should issue SHA-1 end entity certificates by default
  - CAs may issue SHA-2 (SHA-256 or SHA-512) end entity certificates on request. CAs may publish SHA-2 (SHA-256 or SHA-512) CRLs at alternate distribution point URLs
- **1st October 2013**
  - CAs should begin to phase out issuance of SHA-1 end entity certificates
  - CAs should issue SHA-2 (SHA-256 or SHA-512) end entity certificates by default
- **1st April 2014**
  - New CA certificates should use SHA-2 (SHA-512)
  - Existing intermediate CA certificates should be re-issued using SHA-2 (SHA-512)
  - Existing root CA certificates may continue to use SHA-1
- **1st October 2014**
  - CAs may begin to publish SHA-2 (SHA-256 or SHA-512) CRLs at their official distribution points.
- **1st December 2014 ('sunset date')**
  - All issued SHA-1 end entity certificates should be expired or revoked.

In case of new SHA-1 vulnerabilities, the above schedule may be revised.

SHA-2 readiness

For SHA-2 there are still a few CAs not ready

- a few can do either SHA-2 OR SHA-1 but not both
  - so they need to wait for software to be SHA-2-ready and then change everything at once
- A select few can do SHA-2 but their time line is not driven solely by us (i.e. some commercials)
  - Their time line is driven by the largest customer base
  - All can do SHA-2 already – some do on request (since non-grid customers do request SHA-2-only PKIs)
  - it is because of these that RPs have to be ready, because when directives come from CABF they will change, and do it quite irrespective of our time table!
- Keep in mind issues for HSMs (robot tokens)

Other work items

- IPv6 deployment
  http://www.particle.cz/farm/admin/IPv6EuGridPMACrlChecker/
  - expect RPs with v6-only systems to setup 6-to-4 NAT/proxy
- IGTF 'Test Suite' for software providers
- Guidelines on operation trusted credential stores (draft)
  http://wiki.eugridpma.org/Main/CredStoreOperationsGuideline
  - matches with the Private Key Protection guidelines
  - guidance for MyProxy setups, portals, credential mngt systems
  - intended to be 'good advice' for RPs – things to consider
- Progress on move towards differentiated ID assurance
  http://wiki.eugridpma.org/Main/IOTASecuredInfraAP
  - provides *only* unique opaque identifier: no identity, no tracability
  - needs tuning of LoA with our RPs, current version may be too much XSEDE and does not even work yet for PRACE-T1s…

IGTF IOTA profile

- Input TAGPMA, CI Logon Basic, and UK SARoNGS
- RP requirements from XSEDE and PRACE
- New authentication profile
  - Identifier-Only Trust Assurance
  - Persistent unique identifiers
  - Light-weight identity vetting
- Appropriate in cases where VO does robust ID vetting, e.g. LHC VOs

IOTA (2)

- If a commonName is included
  - it must contain either an opaque unique identifier
  - or a name chosen by the requestor and obtained from (a list proposed by) the IdP on which the issuer will enforce uniqueness
- Full details at
- http://wiki.eugridpma.org/Main/IOTASecuredInfraAP

Revised Security Policies

- EGI Security Policy Group
- Old Grid Site Operations Security Policy
  - Replaced by **Service Operations Security Policy**
    - As it is not just sites who run services
  - And a recent new bullet on the policy requirement for deployment of Security Emergency Suspension
- https://documents.egi.eu/document/1475
- *You must implement automated procedures to download the security emergency suspension lists defined centrally by Security Operations and should take appropriate actions based on these lists, to be effective within the specified time period.*

Service Operations Security Policy (2)

- Other changes:
  - addresses end of security support for software
    - *… software patches, updates or configuration changes required for security or end of security support …*
  - removes the IPR statement (covered elsewhere)
  - addresses the retirement of a service
    - *Upon retirement of a service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for the retention period specified in the Traceability and Logging Policy*
- Has been adopted by EGI from 1st June 2013
- **I propose that WLCG adopts this revised policy**
  - **At an upcoming WLCG MB meeting**

Revision to Grid AUP

- EGI Council decided to require its users to acknowledge support and resources used
  - And requested change to the User AUP
- EGI SPG considered
  - Not easy as Users usually register with VOs not sites or infrastructures
- https://documents.egi.eu/document/1779
- This is one document where common wording between all VOs, communities etc is very useful!
- The following new wording has been added
  - Next page

New AUP(2)

- *Acknowledgement of support or of your use of the resources or services provided to you by Infrastructure Providers, Infrastructure Organisations and/or Resource Centres may be required by the body or bodies granting you access. You shall comply with all such requirements by adding the specified citations or acknowledgements to all published papers, preprints, conference papers and talks and any other published material, whether or not these are subject to copyright.*

- Additional procedures are required to specify what acknowledgements are required and by whom

Security for Collaborating Infrastructures

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, …
- Developed out of EGEE and WLCG
- We are developing a *Trust framework*
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies

SCI (2)

- A draft version (V0.95) may be found at http://www.eugridpma.org/sci/
- The document defines a series of numbered requirements in 6 areas
  - Each infrastructure should address these
  - Part of promoting trust between us all
- Version 1 has been produced
  - And is being tidied
- No time to look at details today
- But this is a useful way of building trust within WLCG
  - And for identifying areas that need more work
- Once V1 is finalised we will share with GDB and MB

Security Operations

- You are all very aware that WLCG uses resources from several computing infrastructures:
  - EGI, OSG, NDGF/NeIC, …
- Today security operations in WLCG relies on strong collaboration between
  - Romain Wartel as WLCG Security Officer
  - CERN security team
  - The CSIRTs from EGI and NGIs, OSG, NDGF/NeIC
- In recent weeks there has been much activity by the EGI CSIRT monitoring and handling the vulnerability CVE-2013-2094
  - Several people have been very busy for some weeks!
- EGI CSIRT is now accredited by TF-CSIRT/Trusted Introducer

Security Operations after end of EGI-InSPIRE?

- The study made by EGI as to which global tasks need to continue beyond May 2014 identified "Security", including a strengthened core expert incident response team as of "critical" importance
- As we move into an ever-changing world
  - Agile computing, Clouds, Virtualisation etc
  - Security risks and threats will change
  - Competent security teams will be needed!
- We confidently expect EGI.eu sustainable funding for this important activity to continue
  - And we may be able to bid for additional funds
    - E.g. Horizon 2020
- I don't currently see any plan B for WLCG and its members to take over the funding of this

Discussion?