51st EUGridPMA meeting (virtual)

Monday, 8 February, 2021 09:20

Dear all:

Thanks to all those that joined today's session of the 51st EUGridPMA PMA meeting!
I'm glad that the some of the spontaneity and sparkle of the in-person trust building remained also for the video-participants. Your stamina is to be commended, and I hope to see you all tomorrow morning as well - we start at 09.30 CET (08.30 UTC) in the same virtual room:

https://eugridpma.org/z/51

In this running summary, I'll try to give an impression of the main discussions and results. As usual, much is also contained in the slides and ancillary materials and documents that are attached to the agenda pages at https://eugridpma.org/agenda/51 or linked therefrom.

Here are some of the highlights of today.

APGridPMA meeting

Everyone is welcome to join the upcoming virtual 27th APGridPMA Meeting:

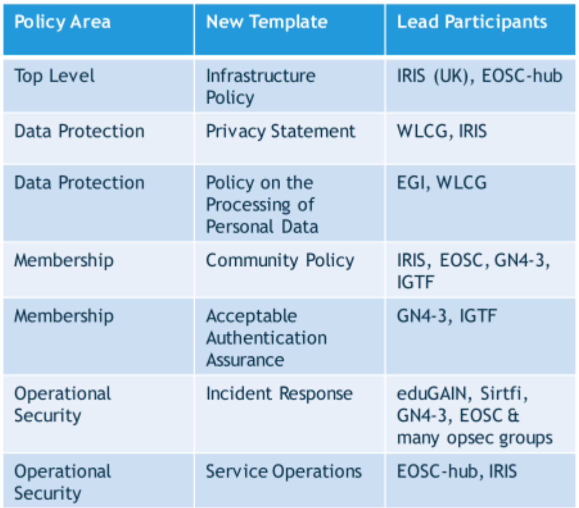
- 11am - 3pm CET on 23 March - co-located with ISGC 2021
- the ISGC Security Workshop is scheduled on 22 March (2 sessions)

Certificates for container-based and self-service entities

Hannah Short presented the updated CERN CP/CPS that aims to better accommodate container-based services that are not really 'machines' (real or virtual), but rather containers that get spun up in an OpenShift container management service. Such containers, like an Indigo IAM instance as 'wlcg-iam.web.cern.ch' have a proper domain name, but would appear to fall outside the host definition since they do not appear in the local (CERN) network database.
This is actually common, and the DCV process for example does not distinguish it, as long as the domain names used of course are properly controlled - so for a web-service based container like wlcg-iam.web.cern.ch, the owner of web.cern.ch (and/or cern.ch) would have to allow that.
If so, the term used for these can be many things - industry still revers to Server SSL certificates even if things are not servers, nor using SSL (but TLS). And the discussion on what a subordinate or an intermediate CA is, is equally muddled (as seen on the LAMPS list).
All CERN container names will be domain-name based (so not use the legacy Kerberism *service/hostname*), and this is perfectly fine.
The changes proposed throughout the CERN CP/CPS (as attached to the agenda) are approved as-is, and the new CERN CP/CPS can take effect immediately.

WISE SCI and the AUP

Various groups jointly work on the aspects of SCI, and the alignment between AARC, IGTF, IRIS, GN43, EGI, EOSC, WLCG, and others is very close - addressing the whole range of SCI issues:



Policy Area	New Template	Lead Participants
Top Level	Infrastructure Policy	IRIS (UK), EOSC-hub
Data Protection	Privacy Statement	WLCG, IRIS
Data Protection	Policy on the Processing of Personal Data	EGI, WLCG
Membership	Community Policy	IRIS, EOSC, GN4-3, IGTF
Membership	Acceptable Authentication Assurance	GN4-3, IGTF
Operational Security	Incident Response	eduGAIN, Sirtfi, GN4-3, EOSC & many opsec groups
Operational Security	Service Operations	EOSC-hub, IRIS

The AUP version 1 is no longer a draft, and is now available from the WISE web site - the version from Feb 2019 is materially unchanged. It is not directly uploaded (for technical issues with the WordPress site) but the WISE web points to the proper version on the GEANT wiki.
There is a slight discrepancy with the TrustedCI template, which would need reconciliation in order to be fully compatible (specifically the clause 10, using "responsible" instead of "liable" which maybe has a specific legal US meaning to some readers there, although Fermilab was fine with the WISE version?) - work is ongoing in this area. The US is still discussing, updated in the coming time.

WISE SCI implementation guide

The WISE SCI v2 was endorsed by many, which is one of its strong points - although not everyone may remember. It defined five areas with specific requirements, and each of them can have a maturity level associated with it (0..4) that can be used for self-assessment. The self-assessment can also be used an inspiration for peer infrastructures if these are shared within the (trusted) group, extending on the Policy Development Kit, in a Google document (attached to the agenda).
While terms are re-used if relevant from similar frameworks (NIST, ISO), but SCI does not specifically redefine terms (using more their dictionary meeting), and does aim to be a self-contained document. The ISO/NIST frameworks does target single administrative domains, where SCI also specifically tries to address federated environment. The collaborative environments does not make a good match and, say, accrediting the EGI federation to ISO27k will never be a good match. SCI does aim to address to those issues.
So for example, information sharing for incident response does make an important element for SCI in the 'collaborating' ("C") sense.
But of course SCI should not be confusing terms with respect to their NIST/ISO definitions.

The document was revised and improved during the meeting, starting with section IR1 (Incident Response contact information). Anyone with the link can comment!
The document should not turn into the ultimate reference guide, so for some more detailed guidance (like on how to do incident response, IR2) it need not contain a comprehensive procedure nor a complete set of references. If needed, readers can either look themselves for courses like TRANSITS, talk to SCI, etc. "Talk to your local security team" (if it exists) does not quite help since the audience for the SCI document is (also) the local team. The same applies also to some of the OS requirements like the security plan - so an introductory comment ("what does this document help you with") at the top may clarify this scope.
For IR3, since people are not likely to converge on a single tool for collaboration, the text is necessarily a bit generic. Some of the mechanisms are actually in place and tested (like for the Sirtfi exercises), but most of that is either related to eduGAIN or (on a smaller scale) the IGTF RATCCs. But adding those may well be too detailed, and the Sirtfi one is specifically scoped to eduGAIN as well. We could add endless links here, but is that really helpful? In the "how", the main aim is "To be consistent with the SCI framework should be able and willing to collaborate with others", with "able" means having both the

tools/resources and the mandate to act, but also specifically including 'willingness'. So "authority, resources, and sufficient priority".
And you cannot have IR3 without IR4 on information sharing, and you need to explain how to then share information - which is what all the wording there provides (including "TLP").

Operational matters

- the MD-Grid self-audit was completed successfully and can be closed
- for the RDIG CA, Eygene really should send the new CP/CPS (and make that update persistently available), and ensure that practice (good) and document (outdated) align
- the TR-Grid self-audit review was presented - peers are X and Y

We thank the following people for the extended attendance and stamina for sitting through the virtual meeting: Eric Yen, Eisaku Sakane, David Kelsey, Anders Wäänänen, Ian Collier, Cosmin Nistor, David Crooks, Daniel Kouřil, Hannah Short, Jana Zrakova, Jule Ziegler, Lidija Milosavljevic, Maarten Kremers, Marcus Hardt, Miroslav Dobrucky, Mirvat Aljogami, Mischa Sallé, Ian Neilson, Paul Mantilla, Reimer Karlsen-Masur, Scott Rea, Uros Stevanovic, Jens Jensen, Sven Gabriel, Adeel-ur-Rehman, Nuno Dias, John Kewley, David Groep.