2020.09.07. EUGridPMA 50 / EnCo / ISM.

PMA 50 09[20] intro.

0 DavidG, Sara, Mischa, JensJ, Jouke, JanChvojka, Matt Viljoen
Baptiste, Cosmin, David C, Eric Yen, Feyza, Hannah, Nuno,
Ian C, Ian N, Jan Jona Savorsek, Lidija, Maarten K,
Nicolas, Miroslav, Mirvat, Scott, Reimer, Jens, Daniel K, Dennis K,
Adeel, Bill Yau (HK), AndersN, Dennis., Urpo S, ScottR, Gerben V
John Kewley

09[40] APGridPMA / Eric → updates, more self-audits done
BC/DR is working out pretty well for remote ops.
~~remote~~ vetting for more CA's, like HPCI-CA.
next F2F will be at ~~I~~SGC 2021 in march 21[st]

09[50] Cosmin // Self
Moldovan Grid CA: Valentin confirmed on Friday,
CRL extensions are OK, but the updated CP/CPS
is not online yet.
Slight progress, looking good.
RDIG : Evgeny received the mails,
reviewers will look on the web for updated CP/CPS.

What to do with extremely overdue CA's?
~~next~~ candidates: TR-Grid.

10[10] TCS;
keygen moving JS also works,
but mobile, IE &c makes PKCS#12 more compatible.
There is CSR now, and that might be used to develop
a credential manager à la Master Portal + RCauth.
CESNET has its own portal, but personal IGTF unknown status
due to nameform.
Jens / UKeSc. has done JS experience. // Jan is building CESNET portal
but: IGTF certs via API does not work :(
due to lack of ASCIIfication

10[30] coffee

11[00] EOSC ~~DavidG~~.

Sectigo is putting accented chars back in
Locality even in a ~~independent~~ Org!

11^{00} = EOSC / Davidf. see slides.

Mccarden: eduGAIN also as to up its own baseline

EOSC as a carrot for baseline.

how to validate the baseline → assessment & trust marks.

in partial. with seals.

needs AI

output to RoP WG and TF-*.

Matt: onboading service providers will be limited to ~~facts~~ light weight rules (CTRL)+ * contacts)

- order process, contact, "incidents" mngt.

min: contact details. + keeping confidential data confidential.

[lunch] * will it scale?

13^{30} / Uros - SCI [see slides] [introduction] [see doc]

sci is more a framework that should be implemented with concrete text by the "users", incl. assessment of security.

*needs mabye targeted meetings of the SCI WG, but at least start now (starting at the end of the doc)

(1hr / 2wks)

Specific topics: OSS security plan?

- in fact, nobody actully has one!

"security plan" is coming mainly from ISO27k → documented but this level of formality is over done? since nobody has one apart from ISO audited orgs.

less documentation and more examples.

you need answers to questions more than documents

there is a diffference between a plan and a "shared direction" in the guidance, maybe give examples of plans more than guidance.

* peer reviewed assessment can compensate for documentation maturity assessment by peers.

PR*: the difference between PRU* en PRC* is in the scope and who is responsible. Aim as explained by Uros

SCIv2 // on PRC/PRU: if SCI itself is confused, the infra's will also be!

* in the guidance, be explicit and direct: "you must ...".
for the AUP, see AARC guidance I-Φ44.
eg. maybe PRU2 guideline on AUP was too restrictive by requiring a registration process. that belongs better in PRC2 :)

Actually all of PRU is about the AUP, but all directed at the infrastructures and communities (not the end-users :)

* ultimate goal is to help people fill the assessment spreadsheet *
(how to meet the requirements is better addressed by the PDK)

in the sheet, people need to write down what process they have chosen
link to the spreadsheet as clickable guidance next to the row?
so slightly more than adoc → linking them closer together.

"is it documented" "is it published". (→ 3 levels like in TI.)

* but keep it more lightweight than those long ISO lists...
if you have a doc, point do it, otherwise, describe the process here.
(the "how" column in the spreadsheet). → "methods of enforcement" column.
explicit questions are easier to answer, either as a separate row or as a "hover-infobox".
AUP is the simplest one in this category.

* For data protection: clarify that it is about personal data collected "as a result of accessing the infrastructure" as per DPCoCo.
For questions, then come to AARC/EnCo/IGTF/CoCo for help.

* At the end, the benefit is a shared understanding of what SCI is bringing about amongst the infrastructures.
(*) the discussion is the benefit for everybody. (*)
There is a slight risk that a marking spreadsheet gives the wrong signal -- but the peer review discussion in WISE is the real value.

[For the EOSC, start with a (much lower) baseline of coded info.]

PMA SO Mon 7, 2020 (4)

15:25 Derek // TAGPMA update. → America's particularly hard hit.
NERSC stays up - unexpectedly. Some CRL issues, though.
TAGPMA Slack channel comms. (tagpma.slack.com)

for the tokens, avoid the WLCG Authz WG session hackathon in September. → Hannah could report to the US workshop. (OK).

15:45 // IanN - UKIRIS and the PDK.
* these are comparison between the four main flavours of top-level. the highlighted words & sentences are different among these.

the AARC PDK version still has some substance, although still much leaner then the others (EGI, EOSChub, UK-IRIS).
But indeed too many bread crumbs missing.

Some changes are historic, e.g. the EOSChub is worded as "collaborating infrastructures" instead of a single one. Just like not imposing any kind of requirements on users.

in the next version of the PDK could be modular, e.g. on users. but the top-level policy probably does not need to the same for all, as long as the components are interoperable between infrastructures.

(ACT) Next update PDK along the modular model, based on this analysis.

do other non-SSPG infra's have are that is ~~not cds~~ not just distributing responsibility to all participants? Is PRACE or DIRAC (UK) any different? Compare in NISE?
* UK-IRIS & DIRAC will have to do that mapping anyway.

09[30]// Hcowen-EnCo [see slides]

SCI → will be more active soon w/ STFC joining.

SCCC → provide a challenge kit as a service to federations?
the result is the publishing in and of itself.
Active federations will then act as encouragement to others.
to get this started, invite edu-CAIN SG through Davide V
and have Hannah on board to encourage participation.
with the yearly challenges of SURFconext as example.

(VAC) Also run the IGTF one again after a year.

IAssurance → FAQ in progress.

IAAOps → shortly

OIDCfed → standard needs to stabalize.

Sirtfi → survey coming up on experience of v1.

IAAOps. linking to eduGain Sec Groups? challenge SCCC outside of security sphere: Ind. Marine.

FIM4R → included Helmholtz Data Federation.

10[30] + 11[15] →

DG// AAOps → see doc

13[30]// Scott OIDCfed update.
still a lot of changes in RP & OP spec, with Roland being very open to suggestions so that the spec keeps changing.
So while there is a working / interop set with Henri, "the spec does not improve or deteriorate. It just changes".
e.g. the "loops" that are now possible (ie. you need loop prevention now anyway)..
Many changes in area that is not about validation. It would benefit from simplification (or split). But that appears unlike
A feature freeze ("v1") might be beneficial.
Roland should be looped in here.
Discuss that on the implementer's list, so that new suggestions don't go on changing the spec.

OIDCfed // 13[38]: develops dropping out will not help the spec... it is now several years (!) that it is under development, and version 1.0 was "fine".
Starts to now have all of X.500 (and mimicks SNMP & Corba :).
split spec and create extension mechanism. (and have supplementable section).
Use extensions (and a concept of "critical" which is standard).
and like the OAuth spec family, which are not all required.
Action plan: Sonke to write this to Roland,
maybe in later phase get ~~lets~~ a group action on the list.
[and ask Mike from MS].

Use cases? G052 recommends OIDCfed. (Just like for EOSC??)
(non-web etc.)
we have a few OP's: some singles, some proxies,
(and generically for federation. ~~both~~ OIDC & OAuth actually.)

It needs a few (>2!) entities to have demonstration of scaling, for which OIDCfed is the solution. (so: 3 OPs vs. 3 RPs)

Link in the KIT people & Uros. to implement OIDCfed. in "OIDCAgent"
(ask Gabriel at KIT → Sonke will ping).

14[00] // Sens, RCauth distributed ops [→ see slides]
for load balancing, sessions to the Delegation Servers should be persistent. HA-Linux layer should work if latency is managed.
Anycast would be better, but more involved. But nice.

~~15[20] AA ops.~~ / see docs & comments
(DG)

09[20]// Scott - DigitalTrust → Digital14
rearchitecturing → see slides.
will go into next distro release. (namespaces).
(remove all DM ones now)

as an aside: there is a WPE developed crypto-stack with post-Quantum crypto. By the end of the year.

09[50]// Jens - How to operate beyond the pandemic - what did we learn?
(see slides).
there is a lot of trust in remote working already, and that trust cannot be verified that easily by walking over.
* using multiple ways of ID like we now do for remote vetting actually improves over existing checks of a physical ID. It augment trust if you can correlate.
Different means of comms at various levels. (as seen in slide #12)
* Documentation falls short, and remote ops makes a lack of documentation worse.

a serial link in social network is weakening, whereas parallel channels are strengthening. Social graph structure (#16) is important. And interdependencies may be hidden beneath it...

After the pandemic, we'll never fully go back and somethings will remain remote. Setting the compensatory controls will then be more important, (like not requiring wet-ink signatures:)
(also checks for coercion is important!)
Legislation is changing as well, and we can borrow good practices.

overview of good practices → maybe for a next pma meeting.
maybe: - prepare a per-country view
(ACT) - Christos on eIDAS?

11[00]// Jens' Soapbox! I/O for a computer is exiting. Just think about forking! or threads! It's all beyond past language.