

09<sup>30</sup> Present: DG, Manikantan, Danek, Sen S, Inez, Andrian, Liam,  
Tom D, Maarten, Nisha, Davide, Sen S, Harmoh.

Remote: Adeel, Scott R, Eric, Miroslav, Casper D, Ann Cugula, Bayraktar  
Nicolas.

09<sup>45</sup> ~~UK~~ UK impact is growing through the DRT activity and coherent T&I  
in the UK. Lots of attendance reflects that.

Collaborative notes // DG reconfirmed as chair.

09<sup>57</sup> Eric / APGRAPPA.

move to SH2-2 Pacts for ASQC, KEK, IHEP by end of 2023.

next meeting now ~~is~~ moved to June to get et al. in.

IPv6 access is targeted to CRL download. 2024 will likely see 50% v6

\* mapping CPs and federations need mapping. Eg Gchq has not done  
Sirtfi yet!

\* Token transition in HP just starting.

10<sup>15</sup> Sen + Nisha // RAuth.

\* EOSC always tries to claim RAuth, but got "HA-" RAuth.

\* PMA is good as an independent assessment on the operations.

but now the PMA is a bit too slow, → use e.g. to check against the  
EOSC security baseline.

\* HA for EOSC does require monitoring.

~ monitoring based on end-to-end type needs a 'test service' account.

- issuing to 'robots' is actually against the RAuth policy.

- disabling test ends (key usage == none) may work but then this  
needs specific handling. Any arb. out extension should be fine

\* frequency of monitoring? → now ~ 1 minute. But not all aspects need

\* eduGAIN tagging of service accounts? Not distinguishable now <sup>some</sup> frequency

\* Write up HA experience as a paper.

\* most communities want ASPEN / Cppnetno. And there is existing service.

in Denmark to elevate assurance. Cppnetno / RAF is necessary, but still slow.

\* for success, Cppnetno is needed.



11<sup>37</sup> // TCS, David.  
CPS change: OK!

12<sup>10</sup> // Scott, eMiddha.

\* does AATL via video! :) more "like DigiCert", then test users on RP agent  
- see details. 2PA also has biometrics (face, FP, Iris scan).

[formally applied to APQ and APD.]

↳ new ICA for joint-trust offering for hosts.

12<sup>45</sup> // SHB-1

dual-blob solution partially tested by Misha → BC is too mixed.

\* Brian B should test!!!

otherwise flags for OSSL in source code.

\* migration encouraged but not enforced.

\* post-process trust store? → tool.

14<sup>02</sup> // David C / Resource evolution.

FINAL now fixed, but now "a bit sketchy".

The solution with the U.S. Science CA would include (C=UK) in it.

but now cheerily resolved, prepare for next question!

\* Swiss situation as DT.

one-time CRL ok → pre-generate CRLs to have no policy change.

removal of the CA "quickly" (days) will work.

UBern can be an RA for Sens, Sens will offer. ✓

- then replace all certs "quickly"

- subsequently remove DT asap.

↳ later to new retail CA — Modica

Beyond Fermilab

splitting trust stores needs "too much effort" during token migration.

risk assessment for tokens is also still lacking → not enough "bodies"  
even if the effort is there "money-wise".



14<sup>39</sup>// Start of experiments first? Based on CMS SSC discussion. But are the experiments coherent? And likes to opsec tend to get lost over time. ATLAS (Mario) is at least interested. But the work takes (in an SSC) a lot of time.

For the "cloud" use cases, there may be larger issues than just cost provisioning for provisioning assets to the cloud, automation is needed (KOME U more), mostly an NLCG thing → think also ISO 27k compliance & auditing.

↑ "Acceptable assurance" policy evolution to mandate ISO 9001 + assurance setting level.

That might also be an IGF role → to alleviate SP worries about committees.  
 ⊕ Write down lessons in some papers [Scott R]

15<sup>01</sup>// Hbörnsh // Cern CA.

→ see slides. pin next time to remove one month ahead, might be good for the Wiki.

15<sup>45</sup>// Davidf - EOSC.

- updates on 2 sec. events + one ongoing from EGI → EOSC
- risk assessment out two sp's (cai, marketplea).

EOSC core-IAAI: how much testing? worked fine with Pinja, but since CERN is a black hole.

✓

16<sup>15</sup>// Cosmin-

NIIF / → withdrawn in 1.120.

BYG+ → to be send by Cosmin.

KENET → nothing heard. Root CRL now expired, so safe. ✓

ask @TNC23 about-see remove, since Ronald O never reacted.

request for DZ.

16<sup>40</sup>// Derek - TASPMA.

In C RABCA 2 is in the Ine court., met in 1.120. Will boom in Oct '28.



09<sup>05</sup> // EnCo Cooperation

① continued topics: PDK/WISE SCT || completed: Sirtfi  
 Assurance to keep DP CoCo  
 PADS  
 FIM4R

② new: policy for telers, SNCTFI, AppInt

③ Any PADC-TREE work would anyway start in 2024+ (if approved)

ADK → GDPR personal data protection guidance - even if content wise correct - is from before GDPR. But not-quit-BCR did not pass ISM/WISE, although it is the only option (as per Andrew C's<sup>+</sup> discussion)

There is now a community (IRIS/UK) policy available.

↳ [David C/Dave K describe UK-IRIS model] - comparable to HIFES/DE

CI/PDK: new communities (models: loosely or tightly coupled) usually find it useful to have templated. "Augment" existing policy.

SCT: liaison with Trustel CI / BSFCybersec summit.

Assurance: lacking effort now that sale left.

Now: guidance needed for suppliers to encourage adoption./requests.

④ What about assurance on attributes in the BPA/AD's.

has in PADC I and in the FIM4R v2 paper.

but the need from the RI's drives it. Sirtfi w/CERN, HFA w/LUMI

we cases input via FIM4R via EnCo.

How many communities can we get? CERN's Feb'23 meeting was good but a bit small. Townhall education in Stockholm?

education + REFEDS and a small side meeting?

[ in PADC-TREE there is some effort for communities --- ]

less interest because initial login new works? or did that move to the infrastructures or EOSC

Common set of collab services, see SPAM struggle.

ask FIM4R use cases, firm user request.



Enlo - AAOB: toleap is working

- Taken interop → trust model for oisd, esp. towards OP's. Jens is trying to even get Global to change.
- Snetf revisited: what should we do here in the light of TechEx 22 discussions. we could also enrich SCP?

Representative requirements: not always HEP please. More direct influence.  
↳ schedule meetings.

1000 // Mischa OIAC Fed.

fed. spec is quite far. Italy is now (Giuseppe) implementing the almost final stable version. But the OIAC Fed spec is too rich, and we will need an "AAAC profile".

lists will create a single trust domain. The AS proxies today are such things. Draft doc exists that (GOSP) defines AAAC profile.

Take things from the spec if we have to do trust lists for cross-use the RP's need to become a registered client of the other OP. In OIAC Fed that should be with dynamic client registration. So more connected than "just" a policy-bridge list.

MOSS-IQTF.NET can be the policy filter to x-connect federations. can we end up with a single RFE federation? Unlikely! policy & natl. differences will make that unusable. Danger of being subject to a specific country's regulatory env. (see FR issue)

Federations will be relative stable → can be human-based but this will also be an operational (HA) infrastructure for trust.

[See 2019-12-10 Orleans slides]

pathlen constraints (and namepae) part of spec and essential to prevent trust leakage. But RPDNC missing in oisd Fed by default. SHOULD BE VALIDATED <sup>in my implementation</sup> → equiv in local TP at the RP.



11:09 / Bas 2 - AAOPS SRPM.

(DG/Intro) Bas. - see table in google docs.

Community identified as per GDS.

AMS+2.2 → GDPR as well. ✓

Useful. → link to be shared.

12:15 AAFC TREE / dan rdg

12:40 ⊕ Next meeting Need → Thu 5 Oct 2023 in the UK.

12:45 (lunch)

13:24 // Sens - Scapbox

The climate use case is not dissimilar to AmDEX & airline MRO business

14:00 o1defed Ben

14:30 DR1 - Sherry included.

15:30 WISE / Donell.

GDPR: SCI privacy work was suspended since no consensus could be achieved. 'just' changing to GDPR might have worked.

Other work continuing, but contentious bit is "VIII" i.e. the semi-BCR solution.

→ change minimum amount, but keep the doc.

Community: new IRIS policy much clarified! - now approved.

split directives & references. + examples