55th EUGridPMA+ meeting, with GN43 EnCo, AARC, IGTF, and EOSC ISM

Monday May 23rd – Wednesday May 25th, 2022 – Garching bei München, DE, hosted by LRZ

Present: Jens, Adeel, Mirvat, Miroslav D, Paul Mantilla, Jule(P), DaveK(P), Maarten(P), DavidG(P), Cosmin, Feyza, Eric, Nicolas, Mischa, IanN(P), JanC, KyriakosG, Nuno, RalphN, Lidija

Round table updates ()

Self-audit review (Cosmin)

Only LIP and KENET are currently in the review schedule. The table is rather empty at the moment.

For LIP, there has been no feedback from Ronald yet, so a second reviewer is called for. DavidG will have a look and act as a substitute.

The self-assessment process seems stuck – TAGPMA has annual reconfirmation letters, which at least shows that they are alive and well. We see them at other events (EGI Council etc.) , but that does not help here. BYGRID is the oldest one. With now coming out of the pandemic, it's time to start that up again, even if its remote particiaption for extended periods of time.
Most of the reason for being is is WLCG, so us thorwing them out will need the backing from the RPs.
Will WLCG scream if we kick out a T2 site country?
In due course this may go away?

Alternative process: assing a reviewer/mentor to puh the assessment outside of the meetings? GO throuh the process in a couple of hours side of a meeting, but dirng a dedicated time slot. Two meetings, two weeks apart to comleete the entire thing. Arrange meetings at more convenient times.
Iyt may mostly be reviewing the CPS and comparing that to current practice (after a few years to may have changed a bit, but not the doc updated).

Requirements:

- delegate trust to dedicated reviewers
- they do the 'assisted registry check'

Volunteers to act as assistants: DaveK, IanN, Jens, JanC, Feyza.

Cosmin will try and choose two to start the process with >7yrs (BYGRID, PK-GRID, NIIF, MREN, PolishGrid, TSU GRENA).

RCauth HA (Jens, et al.)

Three-site-four-instances setup is now working, see slides on the agenda! And besides the four production instances there are o course also acceptance and dev instances.

The HA proxy sends you to the closest DS, except fo rthe Nikhef one which prrefers STFC.

Anycast is apparently perceived as ‘complex’, whereas in fact its trivial. GBP failover is anyway becomng really standard.

APGridPMA updates (Eric)

(see slides)

Are other research communities also moving to tokens in AP? NII JP is doing that also for HPC, in TW also for the general eScience community. So this is a general movement.

There is a role for IGTF in the policy/assurance/trust issues remain for tokens, and these need to be taken into account. Surely! Interop on tech+ assurance (AAOPS+REFEDS RAF) Thi smimics the IGTF assurance levels + PKI Tech Profile

Do this for ISGC2023 as a session for IGTF meeting! Do that as F2F in Taipei for a meeting there, and how NII & co are doing in this area. Use that as a focal point for the assurance discussion about the token assurance. And use the rest of ISGC for the related topics. Timescale is right for that. And make it an IGTF all hands meeting.

WLCG kind-of works since CERN HR does the heavy-lifting. But that does not scale to other communities. And needs to be documented for the WLCG use case as well.
That generalisation would also be appropriate for EnCo GN5 work!

How to add value to the REFEDS work there (since REFEDS is more standardization, but not quite policy). Tokens and eScience stuff is a better match for IGTF, with help of EnCo. REFEDS remains a bit too much oriented on enterprise campus bits.

Also for the token world, keepthe same assurnce profiles/named (so Cappucine and Espresso)

For APGridPMA, prepare this one during the autumn meeting?

BCDR planning and trust (all)

- CRL distribution

- CRL issaucen

- certificate creation/issuance

- trust restablishment after failure

challenge forsmall calssic CAs. Short vs. long-term effect?
Have a long CRL is escrow to keep the service available? Existing certs will cotnue to work, but revocation cannot be done.

Need to distinguish between **internal** to the CA, and across CAs to other peers and relying parties.

CRL expiration may cause to flag sites down. Resiliance for the whole trust network is IGTF buisiness, internal to the CA is more local.

Escrow works for the bases where the operational integrity is OK and operators are fine, but there are technical issues in isuing the CRL technically (i.e. CA safe is bombed). This is the same as for a decommissioning CA.

But the risk is higher since you cannot revoke certs any more. So this works as long as the trust in the operators remains and they are not under duress.

Is the protocol to re-establish trust of sufficient urgency to the IGTF? The warm and fuzzy feeling got chilled. After severance, re-establishment would need to be done as per initial procedures, unless there is a pre-agreed protocol in place.

Ultimately, if a APT national state takes over one of the CAs, that is hard to recognise. But we know them not by identifier, but by baseline behavior. That personal trust is essential.

If any org/state wants to apply sanctions, that an AuthZ, not a AuthN issue. That is an IGTF principle, as we have done before.

The suspension review committee was kind-of a closed list but the full list has all kinds of people on in, including both parties.
The plenary meeting here agrees that the smaller (suspension-review) was the appropriate choice – then bring it back the plenary meeting for discussion. Do the others feel involved? No strong opinions.

Nuno to join the suspension-review list.

The suspension review committee can take emergency action, but it is to be reconfirmed at the next plenary meeting. This is both for emergencies, as well as from complete non-response by an CA member.

There is also an IGTF keybase channel for secure communication, which is instant.

Links are: https://keybase.io/team/igtf and keybase://team-page/igtf

Redundant CRL hosting: with local caching it is maybe less critical, except for new systems. Cross-hosting may be helpful, but not that urgent.
For the RCauth setup, each sites in producing CRLs and they are cross-downloaded by the other sites. But there is one distribution point (one web site), but that is independent from its production. That can even be an independent vhost config. Having separate subdomain name for the CRL is useful.

WISE SCI v2 How-To (IanN)

(see also the slides on the agenda)

More guidance is needed when completing the spreadsheet, since the bullet lists do not give sufficient context. Uros and Ian crafted guidance document, and the assessment chart B is both simpler and more abstract since it explains the items in more details (e.g. for OS3).

The result of the exercise is a set of tables per section, with a What-Why-How+Checklist for each of the elements (the checks are for the fundamental criteria).

Now we have two difference matrices, and we need to find out by trying which of the two (or both) are the most relevant. And even the cost of maintaining both is not too much. The "B" sheet may be more resource intensive.

One the challenging questions is about the "Security Plan". That is a large and potentially heavy-weight question – and the self-assessment is challenging. There is some general texts and questions – which try to specialise it enough without requiring a structured security plan. This is certainly to be considered in SCIv3 to reconsider that 'security plan'.

SCIv2 assessment was attempted on the UK-IRIS infrastructure. Some personal observations on that process (slide#12):

- trying to require an overall score, when it's partially true, determining the overall score is hard. Minimum, average, weighted?
- Interdependence between checks
- creep of implicit requirements that were not actually in SCIv2. Not put in specific approaches that are not mandatory, even if oft seen as good practice?

The fact that the FAQ is now on the Wiki, it is easier to edit, and we need some management and contributions to make it a live document.

The "B" spreadsheet that goes with it, will need a bit of review (like in PRC1 and PRC2 where there are suggestions that are not matched by the actual SCIv2 framework.

The IRIS assessment took a couple of meetings, ~ 3x1hr meetings. Then preferably *once a year*, and on significant changes (like the CSI process, and the rest of an SMS).

The coincidental advantage of measurement against SCI (or any SMS), is to clarify which specific areas need improvement, and getting resources to do an improvement is easier if it's more specific.

Now has any org that has gone through ISO 20k1 certification also gone through SCI, i.e. is SCI highlighting elements that are not in ISO27k? That would highlight unique elements.

The NIST cybersecurityrisk framework (a policy mapping) did have lots of mappings, but not all elements there appear in all standrds (there are things in the framewor that are then not in 800-53, or not in ISO27k2, Does that also hold for SCIv2? SCI is much more suitable for our distributed research infrastructures.

Now we just have to train auditors in auditing SCI (and not only ITIL or 20k). Otherwise the auditing costs are getting too expensive over-all. The STFC auditor did go through SCI. just like we has the internal auditor at NWO go through this in the Nikhef research infra. The NWO auditor did a mix of both, but the recommendations were not very SCI specific. (DavidG went through the NWOI Nikhef audit results from Francis as an exercise). There have been not that many others that have tried to use SCI as a formal mechanism (or use SCI to keep auditors from using ISO27k for multi-domain infra). It would ne nice for

more people to use it to identify the blind sports from SCI. The AEGIS communities might be good, since Christos is monitoring adherence to the specifications passed there. SCI is not an AEGIS document (even though all infra endorsed in in 2017). We need a few detached people to try it and proide feed-back.

The downside of ISO27k10 multi-domain framework, while looking nice, still also tied you to 27k2 controls, so it needs both.

Also Snctfi (as in the mail by Tom Barton) is relevant in this context – the SP proxies generally follow this, but there is not formal assessment against it. Some SP proxies will not go through AARC-G071/AAOPS, which does give trust.

From SCIv1 came Srtfi and Snctfi, and both Sirtfi has now gone to v2, and there is now SCIv2 – so time for SCIv3 to bring it back together? SCIv3 as an umbrella over SirtfiV2, Snctfi+ and the new guidance document?

Needs a commitment by the infrastructures to follow SCIv3+/Snctfi+ - this can be done through AEGIS? Like with AARC-G071, do that also for the Snctfi2+ - assign besides the IGTF guideline ID also an AARC number and then push there. Would InCommon it then find useful? Would proxies do the (self)assessment? Or add the SCI requirement to it (SCIv3), and do it all in one go? The latter seems the most effective … also since Snctfi was based on SCIv1. A bit like the ISO27k series with inter-document links.

And get the input from Tom on what InCommon was looking for in term of trust (also from feedback during the ACAMP sessions).

Privacy notices and WISE in distributed communities (DaveK)

The EGI/WLCG policy on sharing data was to enable sharing for accounting (and incident response) in a distributed environment – it was approved finally in 2017 (mostly), but predates GDPR. The model was inspired by the BCR model for data sharing – and that was the best that could be done there. But since EGI/WLCG was not a single corporate group, demonstrating due diligence was the best we could do.

Given the lack of CoCo approval even under GDPR by the AP (or any other DPA) today, this remains true even today… although we can use REFEDS CoCo best practice guidance as a basis now.

And CNIL kind-of confirmed (as found by Uros) that the kind of data we process is low-risk anyway.

The EOSC Future project put together guidance as well – using “multiple controllers” as a principle, but not being definitive guidance (https://wiki.eoscfuture.eu/display/DPMS/EOSC+Data+Protection+Policy)

Still that does no solve the Exchange issue – which WP29 and the EDPB also acknowledges.
Now the question to a lawyer should always be asked “what is the risk”, not “are we allowed to do this” … they are not there to make executive decisions!

Enabling Communities within (and outside) GN43 (Maarten Kremers)

The Enabling Communities within the GN project encompasses both specific targeted activities (InAcademia, eduTEAMS) as well as the key cross-domain elements. This is always in collaboration with communities outside the project (AARC, FIM4R, AEGIS, WISE, IGTF, REFEDS, &c).

For example, the assurance framework is driven via REFEDS (Jule), with both assurance and the authentication profiles adopted around 2018, and the RAF and MFA are now evolving to version 2 (or an update for MFA). The paper on assurance in PoS/ISGC has now been officially published!

Sirtfi v2 is almost done, alongside the eduGAIN security handbook.

WISE SCI aligns very well with EnCo, and cross-infrastructure security risks get special attention. The SCI trust framework assessment tool (Ian and Uros) is now almost done (see the discussion yesterday). There is now an **active hunt for infrastructures** willing to do a self-assessment against the new SCI framework using the tool/FAQ and we need feed-back.

Policy Dev Kit PDK is evolved in WISE SCI as well. The top-level policy in the kit is there now. The other elements (Service operations security guideline) are almost done, but not yet published. This needs to be pubished by DaveK.

AAOPS guideline is now done, and endorsed by AEGIS (as AARC-G071)! This will drive also the AAI proxies in AARC/AEGIS/EOSC. The structure (based on the one from SCI) allows for easy identification of the criteria and assessment.

FIM4R is about to be revitalised after the lockdowns!

Updated from GN43 were presented at ISGC22, there is an accepted talk at TNC22, and abstracts have been submitted at I2 (and to be submitted to EGI).

GN5-1 has been submitted last week (1st Jan 2023 – 31 Dec 2024, i.e. 2 years) EnCo structure and collaboration will remain roughly the same. Thanks to Maarten!

Participation and help is very very welcome.

FIM4R requirements update and participation

Trying to revive FIM4R, with a three pronged approach:

- general updates to cross-present on AAI and developments in the communities

- planning a F2F in person again

- get the fresh assurance requirements from FIM4R, through a 4th lightweight paper on getting the assurance requirements out. Maybe it needs a clear expression of need by FIM4R to get the IdPs to implement and release it. But as long as the RPs don't require it, there will be no pressure on the IdPs to release assurance values.

We expect assurance to be a key element for an AAI, and we need to clarify and elicit the use cases from the communities, and put that combined 'pressure' on the table.

Is implementing RAF considered more complex than reduing everything locally incl. Even identity vetting – like SURF did for SURFdomeinen, which did not want to use RAF and insisted on re-doing the lot. :(((

Are there more experience stories on trying to get SPs to get to require RAF? Not that many SPs talk in the calls. But for example DFN is implementing RAF and plans to go into production this year (switching from a national profile to REFEDS, so there was already something there). But they start from a existing baseline.

So if FIM4R is to collect the requirements, do enough communities sign up? The LSAAI seems the obvious use case (with Mikael there), but at the moment it seems not yet required (or consumed). But it should be on board in the requirements group to make it a convincing use case.

The pressure from national goverments may help? Or could be detrimental and push for more national IDs that don't work globally.

The baseline for eduGAIN is pretty low (with respect to the RAF levels), but using this argument to push for more assurance may be blunt and rather inappropriate narrative. RAF does have 'local enterprise' as a level that would also work, but it is not used very often.
Who is included in the 'local enterprise' definition? That is not yet formally defined. REFEDS RAF WG is planning to work on making local-enterprise more prominent: not processed-based vetting, but it is a risk-based vetting where the entry-barrier to asserting it for IdPs seems to be lower.

A new aarc-like project (preceded by a AAA study style pilot) might be appropriate for assurance? Also there FIM4R (v1) was the instigator

Planning:

- FIM4R v3 paper on assurance, as an early success for GN5

- the open call should target real individuals (Hannah might hopefully be interested! Maarten can help out but not quite drive it). Jule is also willing to help ofcourse.

- target the authors of FIM4Rv2, asking them

- the IGTF BIRCH/Cappuccino level is providing medium assurance, which many of the research infra depend on. Where now move to tokens, we should either kept that form the IdPs, or all communities have to implement step-up. There is more in it (and likely more needed) than just the identifier (which you could get from Google).

- Aim for publication by TNC23

- Maarten will find all the authors from FIM4Rv2

- include also MyAcademicID (via ChristosK)

- the 'no single solution' from FIM4Rv2 was very much taken on board.

- the EOSC AAI federation does no (yet) require assurance. That would be a big driver…
Christos did ask the ESFRI clusters in the context of the EOSC AAI federation to investigate which ones

were ready to connect via a proxy. The results of that (a rather fixed result!) should be re-used to not ask the same people twice the same question?

Communications Challenges (Jouke)

The security challenge this year is targeting the WLCG CMS experiment. This is one of the more in-depth challenge types, including a mock incident and limited forensics capability testing. And with the changing underlying infrastructure (like the move to tokens rather than certificates), driving that will need updates as well. There are requirements for renewal and credential delegation that will be very different.
There is also a need for logging on what is going n during the challenge. For example, some sites my decide to just re-install rather than try to contain and mitigate the incident. This is useless during a challenge, and actually harmful during a real incident. And a re-install may just re-install the same vulnerabilities again.

The framework for driving these challenges has been upgrades, and now uses a standard (open source) C2 solution "Mythic" (https://kalilinuxtutorials.com/mythic/) – and that provides a cross-platform agents that can communicate through various protocols, write out logs, and which can be weaponised as needed. The Mythic framework is sufficiently fit for purpose. The same systems can also be used for kill-chains to worm and fix vulnerabilities in a controlled way …
There is overlap between operational trust and policy-based trust – for which a common vocabulary would be useful.

There is also a set of response challenges – there are some for TI/TF-CSIRT. Some use bulk mailers, but with the increased spam filtering is becomes more complex to get it delivered. The basic idea is simple, but the devil is in the details to get it right.

More complex comms challanges run with a more complex open source standard platform.

OpenID Connect Federation (Jouke)

RolandH is moving towards finalising the standard – fix it at TNC including a showcase with a presentation by GARR. Also at the NorduNET conference in a few weeks. The standard is now moving to a more stable state, with less crazy features, and more polishing. This looks Good(TM).

Now time to look at security aspects of the OIDCFed. The framework is open, but the specifics now need to be defined.

GARR has made various micro service implementations and provided APIs to provide drop-in replacements to replace existing static config setups with almost zero changes.

If that is working, implementation might be rather fast. With proxies, and many science services using OIDC by default this already has a rather large user base.

The path construction and delegation of authority to orgs has been retained in the final spec! :) The meta-data can be places in a 'trust ancor' (MDSS), so the web of nodes is still there. The biggest changes are in the policy verifiability that is controlled by the RP – to make sure that the OP/RP is compliant with the meta-data for the service. That part has been changed extensively.

The GARR implementation will nail the operational details.

Looking forward to TNC.

Trust construction is not exactly defined (path building vs. graph traversal)? There are some security concerns about loop prevention using random identifiers. But finding a root of trust is up to the implementation. There are some rules about roots of trust, but not specific enough to determine it – and you can trust multiple federation. It is mostly tree-like. The effective policy – dependent on the route taken – has implementations on the effective policy, and thus e.g. for he contact points.

OpenID Connect session at TNC22 is on Tuesday (during the same session with CoCo)

For the TNC on-line session: SIGN UP (for free), since the links are individual.

AAOPS (DavidG)

How to help the Infrastructures to implement G071/AAOPS?
UK-IRIS is part of AEGIS, so how can we help IRIS to do the AAOPS assessment? People around the table (and some not here, Tom Dack and DavidC)

To assist, maybe create the spreadsheet first, like for the CAs. Lightweight assistance like wit SCI to help the infrastructures along? Creating meetings is actually away of making things move forward. Sine it is coming also from IGTF, can we help from here. Can we do e.g. an assessment from the IGTF, and ask two infrastructures to present the results of the assessment at the iGTF meeting, to identify common complications.

"What's in it for me?" to encourage participation. Marketing or promo stamp. "Approved Proxy" just like Snctfi. Maybe Snctfi should require G071.

From an IdP point of view, if the proxy has a trust mark label thing that makes an easier case to release attributes. More than just apt-get install for the proxy – and that is better to mesh with the federations.

Going through the list is not too complex – the effort is in fixing those elements that are not yet aligned to requiremetns. So the assessment is easy, the implications can be larger.

But once you *have* done it, then what does it bring you? What are the benefits? E.g. only then you get into the EOSC AAI fedeeation, or get attributes from IdPs.

So start with multi-community large-scale IdPs – so CheckIn, eduTEAMS, IRIS-IAM to begin with.

These are the 'flagships' – and then ask the federations/IdPs to then release at least R&S to those proxies. Tom Barton et al. may enlighten us. Or does it also need Snctfi. A Snctfi v2 should align with and

refer to AAOPS/G071. Snctfi has a bit more on community management. How to community manages its own life cycle is in Snctfi, and not in AAOPS/G071 itself (since it is not technical).

The number of proxies that represent entire structured communities (ESFRIs in Europe) is still rathe rlimited. Naturity is varying (e.g LSAAI is very mature and far long, some specific communities have their inidvidual ones (like WLCG), but far from all of them have such a single proxy.

Can we invite the major proxies to the next IGTF meeting. You can get the trust mark there. Invite a few to the next meeting (at CERN in early October? :) to present. Should be the 'tech' people.
Why should they show up? Learn from each other. CO-develop guidance and evolve requirements. Have a discussion with the proxy operator people to see what *they* find useful.
For maybe Dick for eduTEAMS, and Kyriakos for Checkin, and Tom for IRIS-IAM? "Learn from eachother and evaluate the usefulness from this document – and how to improve both the doc and the AA operations". And WLCG IAM instance, of course! So also get Hannah and FrancescoG there.

Discuss with Hannah at TNC. - with Four of them there it is worthwhile!

Add some assurance in addition to AAOPS as well?

A that time (round October) the successor to XSEDE ("ACCESS") should be starting, so Jim might be good to have there as well.

Since the meeting is in October, there should be some resilience against lockdowns, and since CERN takes the AND of all possible measures, it is a more high-risk area. (backup in Ferner?)

Actions items:

- wait to chat with Hannah first at TNC and decide there and then (to get it at CERN)

- DavidG will talk to the ones present in AEGIS through a coffee meeting at TNC (Monday)

- decide a date (weeks of Oct 3, or Oct 10)

Meeting: October 4-6, probably CERN

Chair election:

DavidG willing to do it – two weeks on mailing list process:

- Propose Ralph to be the voting committee (since he is RP only)

- candidates withtin 2 weeks

- if no counter candidates, it defaults back to DavidG

- otherwise, Ralph will collect the votes.

TAGPMA updates (Derek Simmel)

Chairs remain Derek (PSC) and Paula Venosa (UNLP) – also the others remains the same

TAGPMA Members

Organization	Country	Representative	Member Type
FNAL	U.S.A.	Jeny Teheran	Relying Party
OGF	U.S.A.	Alan Sill	Relying Party
OSG	U.S.A.	Mike Stanfield	Relying Party
REBCA	U.S.A.	Scott Rea	Relying Party
SDSC	U.S.A.	Scott Sakai	Relying Party
UFF	Brazil	Vinod Rebello	Relying Party
ULAGrid	Venezuela	Ale Stolk	Relying Party
UNIANDES	Colombia	Andres Holguin	Relying Party
WLCG	Switzerland	David Kelsey	Relying Party
XSEDE	U.S.A.	Derek Simmel	Relying Party
DigiCert	U.S.A.	Tomofumi Okubo	Authentication Provider
GridCanada	Canada	Lixin Liu	Authentication Provider
IBDS ANSP	Brazil	Angelo de Souza Santos	Authentication Provider
InCommon	U.S.A.	Jim Basney	Authentication Provider
NCSA	U.S.A.	Jim Basney	Authentication Provider
PSC	U.S.A.	Derek Simmel	Authentication Provider
REUNA	Chile	Alejandro Lara	Authentication Provider
UNAM	Mexico	Jhonatan Lopez	Authentication Provider
UNLP	Argentina	Paula Venosa	Authentication Provider

TAGPMA Members

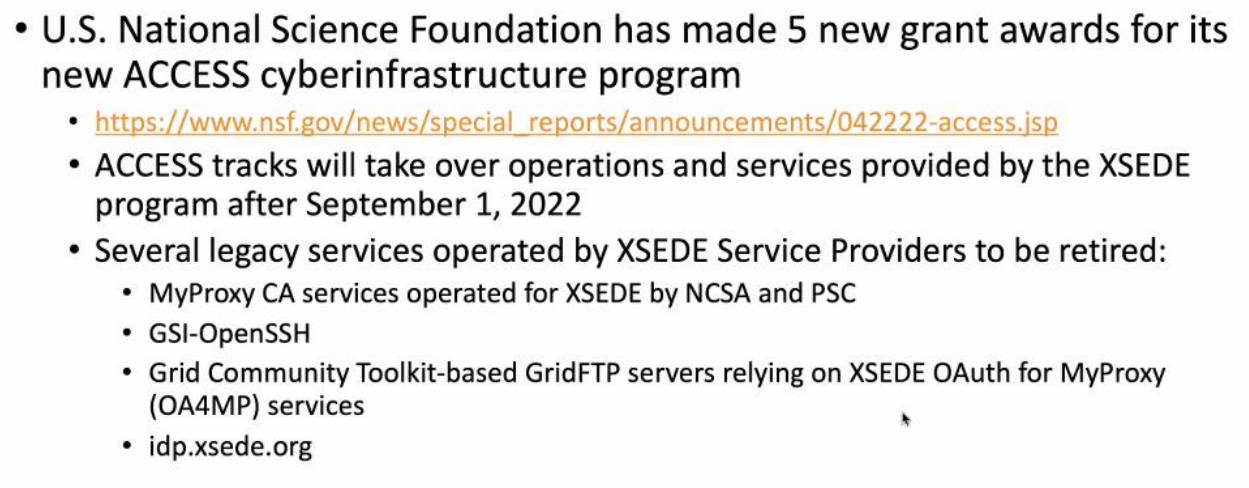
- **19** Members (9 APs, 10 RPs) from the North, Central and South American countries + Switzerland
  - Including Argentina, Brazil, Canada, Chile, Colombia, Mexico, U.S.A and Venezuela, + WLCG (RP) in Switzerland
- **17** IGTF-Accredited CAs (as of distribution v.1.116, March 2022)
  - 13 Classic CAs
    - Argentina: UNLPGrid
    - Brazil: ANSPGrid
    - Canada: GridCanada
    - Chile: REUNA
    - Mexico: UNAM (2)
    - U.S.A.: DigiCert(6), InCommon (IGTF Server CA)
  - **2** Short Lived Credential Service (SLCS) CAs
    - U.S.A.: NCSA SLCS-2013, PSC MyProxy CA
  - 1 Member-Integrated Credential Service (MICS) CA
    - U.S.A.: NCSA (CILogon-Silver)
  - 1 Identifier-Only Trust Assurance (IOTA) CA
    - U.S.A.: NCSA (CILogon-Basic)

- CILogon CA infrastructure migration completed March 21, 2022
  - CILogon web front-end moved from NCSA to AWS US East (Ohio)
    - Higher availability of web services (SAML, OIDC, OAuth, SciTokens)
  - CA back-end and HSMs remain at NCSA machine room at uiuc.edu
    - Amazon CloudHSM remains prohibitively expensive at over $1K/month
  - Communications between front- and back-ends to be secured via TLS with mutual authentication
  - Updated CP/CPS documents at:
    - https://ca.cilogon.org/policy/silver (v.14 2021-03-16)
    - https://ca.cilogon.org/policy/basic (v.6 2021-03-16)
  - Contact: Jim Basney - jbasney@illinois.edu

TAGPMA Activities

- Temporary DigiCert Intermediate CA established under existing accredited CA
  - Contact: **Tomofumi Okubo** tomofumi.okubo@digicert.com
- New DigiCert Grid Classic CA TAGPMA review for accreditation ***on hold***
  - Awaiting further development and response from DigiCert…
- DigiCert Certificate Policy (CP) v.5.10 2022-02-07
  - https://www.digicert.com/content/dam/digicert/pdfs/legal/digicert-cp-v5-10.pdf
- DigiCert Certification Practices Statement v.5.10 2022-02-07
  - https://www.digicert.com/content/dam/digicert/pdfs/legal/digicert-cps-v-5-10.pdf
- Assigned primary reviewers
  - Paula Venosa, UNLP, Argentina
  - Jeny Teheran, Fermi Lab, U.S.A.
  - Derek Simmel, PSC, U.S.A.

- TAGPMA-related Face-to-Face meetings planned for late 2022;
  - Workshop on Token-Based Authentication and Authorization (WoTBAn&Az 2022) planned for U.S. NSF CyberSecurity Summit (Oct. 18-20, 2022)
  - TAGPMA F2F possible for Internet2 Technical Exchange (Dec. 5-8, 2022)
    - Tech Ex Panel proposal submitted regarding Token-Based Authentication & Authorization



The 5th track was not awarded, since probably NSF wanted to change its content. And ACCESS only gets half the money compares to XSEDE (but of course expected to deliver the same).The front office is going jointly to Ohio (for friendly access) and another partner.

The catch-all IdP operated by XSEDE should just be moved to using the native home IdPs – and put the trust sources there. Research profiles and data will be pushed to ORCID.

Aug 31st is the deadline is hard for the old TACC services (like the registry portal) and they must move to Track 1&2 for getting the new interface there. The other services like IdP will remain with the same people, who may jut keep it for a while unless it takes many resources (or external licensed etc).

ACCESS is also a good reason to publicly kill things. The users are anyway remaining with the HPC sites, and XSEDE/ACCESS is just the reception desk. The real services remain with trusted people.

The jumphost service of XSEDE (which windows users have become dependent on) *will* be decommissioned, and those users will have to learn new ways.

For joint meeting on assurance, TAGPMA, MFA, will be at TechEx/Denver for a working session. I fyou go to one meeting, that ought to be TechEx in December 2022.

Then next year's period is even better for assurance during an all-hands meeting at ISGC/APGrudPMA in March 2023. And do the final presentation at TNC.

And then do the IGTF All Hands meeting in Taipei 2023.

WISE SCI – privacy guidance for research collaboration (DaveK)

Given this is not the official WISE session, we cannot quite adopt the new document here and now, but we can work on it and improve it sufficiently!

Updating the AARC PDK guidance and template to a new version, also taking in the EGI/WLCG version and the LSAAI input. The background documentation and sources are at https://docs.google.com/document/d/11S5UrCytHdeh4mNQc3btvZPW_ox_QgSBx0lII-XhKoI

The LSAAI took the AARC PDK version almost as-is (but fixed the typos), and of course updating the periods (e.g. keep the data for 10 years since that is a requirement for research integrity and ethics in the community).

We had hoped for a binding GDPR CoCo , but that did not happen for the known reasons – so there is now a REFEDS CoCo as best practice. And meanwhile EOSC has provided the DPMS, but that is used for EOSC processing and good templates, but that does not solve the scalability issue of multilateral agreements.

The AARC guidance needs to be updated now as well. It will still have to be based on the BCR-like model, given that the risk is limited to he R&S attribute set which researchers anyway want to make public. Lawyers will probably continue to claim that it's 'not legal', but lawyers should be there to point out risks, not to make decisions.

Ingredients in the WISE Privacy Model:
- use other legal basis – where can consent be used (like in the LSAAI), or performance of contract.

The disclaimers at the top of the EOSC DPMS is worthwhile to be copied. We (WISE) provides templates, but we are not liable for their use):

> **Attention**
> Compliance with the requirements from this policy alone is not necessarily sufficient to meet all applicable legal requirements.

Not giving hints would also not be helpful to user communities.

The reason this work is because the risks are limited, and we use only a few attributes (R&S) that are anyway freely given away in mails and published on the web. This is also for the REFEDS scope:

"[it] relates to the processing of personal data for online access management purposes in the research and education sector"

Also appendix 3 of (https://refeds.org/wp-content/uploads/2022/05/REFEDS-CoCo-Best-Practicev2.pdf) does have the key elements that fall within scope.

The scope has been clarified by simplification now – and the requirement to at least also consider (but out of scope of this document) personal data in data sets is seen as quite reasonable (and ethical even outside of GDPR-regulated jurisdictions).

And frankly the user (data subject) is *not* interested in those privacy notices, controls, and interstitial screens – they will ask to take these out sine they know they are going to the service and want to get there. The reason for those screens are the local DPOs, the DPAs, and lawyers.

Most of the results of the discussion have been incorporated in the text of the document, which is attached to the agenda page including its comments.

The work in WISE SCI on privacy needs to conclude reasonably soon, so as to replace the old 46/95/EC version. That is both a policy, and a pointer to the templates from REFEDS CoCo (or EGI/EOSC-DPMS) and/or the Jisc one as inspiration source (https://www.jisc.ac.uk/website/privacy-notice)

IanN will review the differences – and document that on the WISE Wiki

The next steps will be to include the update in the AARC PDK, but it does not necessarily have to be adopted by AEGIS sine each infra may have its own version. WISE approval is good.

Jens' Soapbox (Jens)

"How do we develop software"? Higher level tools push away the need to worry about comparing two numbers. We have come a long way … ways of 'betterness', on an ascending pattern.

And we don't travel with *all* copies of our software together on floppy disks to a conference … and then loose all of them at the same time.

Software engineering is the inspiration here, not the ultimate message of the Soapbox. That's the state of authentication today, and these are grown to be rather large beasts, all building on top of other many other layers. And all of these are complicated things. WIth enough abstraction layers complexity does not matter that much, as long as the toolchains remain supported. And there are no unexpected kernel panics.

To see more laws of computing, visit LawsOfSoftware.com

And there are UI errors, where the most prominent element is the one that must note be used (like a login box with username/password, where you actually want users to use institutional login. That is true even on https://iris-iam.stfc.ac.uk/login

We need a better user experience (and both the login box, but also client certs, are not very appropriate)

And role delegation (acting as) during e.g. holidays is hard, and the granularity to do so is not present. You don't want ot replace the low level tools, but there are plenty higher levels tools available tat can be reused and incorporated.

DigitalTrust updates (Paul Mantilla)

(see also the slides from Paul on the agenda)

DigitalTust part of DIgital14 (the group of cybersecurity service companies), also providing sovereign digital services like DTsigning to the Emirates. This is wholly inside the UAE.

(Jens): disaster recovery methodology – for the VMs that is fairly straightforward but for keys, what needs to be done in case of a meteor? This is distributes across both datacenters. They can both sign at the same time, and there is a cluster of HSMs, and all HSMs have a copy of all keys.

Retail options at DigitalTrust continue to be available, for example for EGI. Contact Paul Mantilla for getting this set up. Engagement with (natl.) research is also planned. (Baptiste already promoted contact)

WLCG host trust evolution (David Crooks)

The original trigger – US orgs not having access to accredited providers – is not a current issue any more - since access to certs through either InCommon or the renewing DigiCert IGTF ICA is now available.

The same endpoint can use different certificates on the same endpoint, using SNI for instance. But historically, the host credentials have been used for three things: securing through encryption the already-named networked endpoint; as a client authentication for acting towards other services (like a bad robot); and for signing assertions (the VOMS server re-using the host cert for signing the attribute certificates, rather than using separate certs).

The 'aim of web PKI is agility' according to RS (I.e.: not necessarily security as a goal :(). And the life time is shortening, with WebPKI going to periods shorter than 1 year (90 days in not too long a future). Them ACME and/or API access are critical. Most of the larger CAs anyway offer at least API, and some offer ACME for most profiles.

Next meeting of the WLCG WG on May 31st at 11.00 CEST (0900 UTC). Minutes are at https://docs.google.com/document/d/1Sl0C_q-lGMCifChmFArHjsGzdnd-RM7O7jbpsGa8XRw

More comments are also in that document.

Assurance (Jule Ziegler)

Document RAF 2.0 (link is also on the agenda): https://docs.google.com/document/d/13tfexdOafnSEXidJ6fbcT0a5qo0wrsu_fqLk856AaTA/

A key change is that the assurance requirements, for those not following one of the existing frameworks, are now also in-lined in the document. That makes it more comprehensive. Also adding explanatory text should help in this regard.

E.g. "local enterprise includes those anyone vetted to a same or better process" as local enterprise service users.

Terminology may matter as well. E.g "vital" has a specific life-or-death meaning in GDPR, so is a vital organisational requirement indeed that vital?

For IE1: it is sufficiently clear that this does *not* preclude leveraging existing business relationships, wher e the evidence originally presented was indeed a govt. ID, but then at time of asserting assurance it leverages an existing database (ref. PR3-5) where there is continuity of business relationship ensured by

sufficient strength of binding authentication and vetting. E.g. "information derived from an ongoing business relationship with the credential provider".

Of course Kantara & IGTF APs also remain good options – but then you have to evaluate yourself. Including them would make the document longer (and you have to consider licences) – but then you can also consider one base document and several guidelines targeting specific audiences.

Aim is to complete the RAFv2 this year (and earlier is better) – it's getting close and announce public consultation at TechEx (December 2022). But there is no external pressure to get it done.

To encourage deployment via FIM4R, the opportunities to discuss are TechEx (for US input) and ISGC (AP region input), and then aim for presentation at TNC23. Ad go through the individual communities to get input (bilaterally), starting with the interviews before having a plenary meeting.
We are hopeful that (Jule and Hannah) might contribute to that process. That decision, however, needs to be deferred for a few more weeks.

True assurance and binding – it also protects against social engineering and impersonation attacks (like the 'boss' mails).

Other ideas for increasing assurance statements in real time:

- some federations can already confirm that all assertions for all their IdPs are actually IAP-Low of better, Why not automatically add those attributes then (e.g. in a proxy)? Pity that the SAML MD does not allow programmatic XSLTs inside that that have been signed by the federations and included automatically :)

- RAF adoption is mixed. DFN is deploying is widely now. SURFcontext has just one IdP that does it, but cannot process it further. And SURF SPs still insist on doing their own assurance stepup, and ignore RAF assurance even if it is available. Snif (SURFdomeinen).

- When CERN required Sirtfi, that did work! Now what about requiring RAF – and see what happens? :) But then remember that Scott Koranda kind-of gave up, having tried fo 5 years to get reasonable things and attributes out of the IdPs. But scaring the IdPs too much may cause them to give up – and that's the end of federation.