Dear IGTF, EnCo, EOSC ISM, EUGridPMA and AARC community members!

Thanks to all those that joined the sessions of the 55th EUGridPMA+ joint meeting in Garching bei München. We warmly thank Jule Ziegler and the Leinbiz Rechenzentrum LRZ that made this in-person meeting possible! And we of course appreciate the perseverance of all of you who joined virtually and partook in the day-long discussions. Thanks for joining!

In this 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 at https://eugridpma.org/agenda/55 or linked therefrom. In this summary:

- Updates from the Americas and the Asia Pacific
- RCauth.eu distributed CA, IP Anycast on the Internet, and HAproxy
- Attribute Authority Operations deployment and implementation monitoring
- Business Continuity and Disaster Recovery – on mutual support, resilience, and CDNs
- OpenID Connect Federation
- Assurance requirements and FIM4R
- WISE SCI - adding data protection to the PDK policy development kit
- Enabling Communities with GEANT's eScience Engagement in the GÉANT 4 and 5 projects.
- Communications and Security Service Challenges
- Privacy and data protection - in the EOSC DPMS, EGI and WLCG, and the WISE SCI working group
- WLCG and public cloud hybrid trust models for server credentials
- Laws of Software - and the progress of development tools
- Operational matters, self assessment process, and mentorship
- Attendance

The next 56th EUGridPMA+ meeting is scheduled for **October 4 – 6, Tuesday morning till noon on Thursday, and will be in-person** in a central place,yet to be announced, that is easy to get to. Virtual participation will of course still be possible, although must of the trust building and innovation happens more naturally and productively in a face-to-face setting.

Hope to see you soon at TNC22 in Trieste, one of the many security meetings, and of course in October!

Best, DavidG.

Table of Contents

Updates from the Americas and the Asia Pacific

Eric Yen presented the developments in the Asia Pacific region. The composition of the APGridPMA remains the same (with Eric as chair and Eisaku Sakane-san as co-chair), although both the CNIC and SDG credential providers may cease operation and are long-since due for a self-assessment. The IHEP CA, also part of the mainland Chinese Academy of Sciences, remains in full operation.

The move to token-based authentication is also in swing in the AP region, with the NII in Japan ding that for HPC access (in Gakunin), and in Taiwan the general eScience community is following the developments in WLCG as well. This is certainly a general movement. The role for the IGTF in policy/assurance/trust issues remains the same for tokens, and the need for assurance and policy (and not just nice software) need to be taken into account during the transition. This will mimick the differentiation between assurance (AAOPS+REFEDS RAF) and the implementation profiles (like we have for PKIX and SAML, but these will need to be there also for OIDC) This thus mimics the IGTF assurance levels + PKI Tech Profile.

We foresee a dedicated session at ISGC2023, with a F2F meeting in Taipei during the SecrityWorkshop and during the conference, and use that as a focal point for the assurance discussion. This will match the assurance discussion from FIM4R, also to complete around that timeframe. This **should be an IGTF All Hands meeting in Taipei in March 2023**.

For WLCG assurance is managed mostly by virtual of having CERN HR doall the heavy lifting (including ID checks), but this process does not scale to other, or smaller, communities. There assurance will need to come (also) from the home orgs. Generalising that would be a very appropriate work item for GN5 EnCo (Jan2023 and beyond). This augments and complements the work in REFEDS (where the assurance profiles are standardised, but no implementation monitoring and support is scheduled) and the IGTF+ is a good place to do that. Also REFEDS remain a bit (much) focused on the campus enterprise IT side, and is no the best place to make giant steps forward. We will of course re-use the same assurance profiles (Cappuccino/BIRCH, Espresso, &c). The APGridPMA in autumn this year could prepare for this to happen.

In the Americas, TAGPMA will hold the next token workshop (WoTBAn&Az 2022) during the NSF Cybersecurity Summit in Bloomington (Oct 18-20, 2022). The next F2F meeting will be during I2 TechEx in Denver (CO) in early December 2022. If you go to only one meeting, pick TechEx …

The XSEDE project will close, and is being replaced with the ACCESS scheme starting on October 1st. It's 5th track was not awarded, and ACCESS only gets half the money compared to XSEDE (but is of course expected to deliver the same). The front office is going to be jointly operated also from to Ohio. Meanwhile, some catch-all services like the IdP and the specific CAs for GSISSH access will be decommissioned, as is the central jumphost – this is the best time to publicly 'kill' things that the users use, since now they cannot complain that much.

RCauth.eu distributed CA and HAproxy

The four instances of RCauth.eu are now working, and the production end-points for the signing (DS) and discovery (WAYF) components will be switched to the HA proxy shortly. And besides the four production instances there are of course also acceptance and development instances.

Each HA proxy sends you to the closest delegation service (DS), except for the one at Nikhef which prrefers STFC (since STFC has the better HSM).

For unknown reasons, IP anycast – the technology used for this highly available setup across multiple countries and autonomous systems - is apparently perceived as 'complex', whereas in fact it is rather trivial. And BGP based failover is anyway quickly becoming a standard feature also in cloud deployments. We hereby note that also for stateful services, using IP anycast, even across multiple AS'es and without using specific anycast-designated IPv4 space, is working perfectly and is not hard. See e.g. https://www.nikhef.nl/~davidg/p/Building-stateful-HA-services-for-RCauth.eu-20220404.pdf.

Attribute Authority Operations: deployment & implementation

The Attribute Authority Operations (security) guideline is now ready and published as AARC-G071 (https://aarc-community.org/guidelines/aarc-g071/, https://doi.org/10.5281/zenodo.5927799). Now how to we help the infrastructures implement it? For this, it has been submitted to the AARC Engagement Group for E-infrastructures (AEGIS), where the major operators of AAI proxies have committed to implement it within a reasonable timeframe. The AEGIS group is also tracking its implementation status. One of the first to do the assessment is likely UK-IRIS, so how can we help IRIS to

do the AAOPS assessment? Some of the key people are present around the table - and some not here (e.g. Tom Dack).

We **propose to develop a simple AAOPS assessment spreadsheet** (similar to SCIv2 and the CA profiles), and do some assessment in the same way we do with the SCI FAQ sheet. There should preferably be some form of encouragement, e.g. a trust badge for compliant proxies and authorities. The other option is for *Snctfi* to require AAOPS compliance as a prerequisite. Running a proxy is more than just 'apt-get install', and requires several types of policy to be in place and monitored.

Depending on the level of support in EOSC, this could for example be a badge (or baseline) for the EOSC AAI federation proxies. Or having the AAOPS/G071 badge will get you more attributes from the IdPs in eduGAIN? These are then the 'flagships' – and based on these we can ask the federations (IdPs) to then release at least R&S to those proxies. Tom Barton *et al*. may enlighten us in this respect. Or does it also need Snctfi? A Snctfi v2 should align with and refer to AAOPS/G071, although Snctfi itself has a bit more elements concerning community management: *how* the community manages its own life cycle is described in Snctfi, and not in AAOPS/G071 (since it is not a technical element).

Other proxies with which to do the initial assessment are eduTEAMS (Dick Visser, maybe?), EGI Checkin (Nicolas, Kyriakos), and the IAM instance at CERN (Hannah, and/or Francesdo Giacomini). Around October 2022 also the ACCESS programme (the successor to XSEDE in the US) will start, and they may have a (new) proxy there which Jim Basney can discuss and present in TAGPMA. The best time to discuss these seems to be around October this year (2022).

For the moment, we need to confirm a location for the October meeting (waiting to **discuss with Hannah at TNC22**), **DavidG will discuss with the AEGIS proxy operators** on their plans and time availability at TNC during the breaks there, and then **have a dedicated one-day AAOPS operator session during the October meeting** to do a live interactive evaluation for a few operators, where they can also discuss with each other, and both discuss their own operations as well as provide feedback on G071 (so we can improve that document if it does not meet the needs or we find blocking issues).

Business Continuity/Disaster Recovery: support, resilience & CDNs

"BCDR" affects credential providers in various ways. The one most visible to the outside world is the availability of (fresh) revocation status information (CRLs, OCSP endpoints) – in itself comprised of two components (the ability to issue fresh signed information, and the ability to distributed tha through the internet). The other elements is the ability to provide service to its customer base (subscribers), i.e. issuing new credentials.

There are also significant threats that are non-technical. A specific hard challenge is to (re)establish trust with CA operators where communication has been disrupted, and continuity of trust potentially lost. This can be because the CA and its staff is compromised, staff has been arrested and broken, forced to act under duress, or killed and replaced with the substitutes claiming authority that they do not have, even if they have taken and forced access to the CA materials.

In this context, the remit of the IGTF is to ensure trusts in the global fabric, not the internal security of the issuing CAs, and in case there are (confirmed) doubts as to the integrity of a member that re-emerges **after a (suspected) compromise, the trust re-establishment will need to be re-done as per the**

initial procedures. We note that the personal trust established prior is extremely important, since it allows out-of-band verification and checking if a person is acting "in accordance with expectations" and we might be able to infer if somebody is acting under duress. Pre-agreed protocol would be preferable, but are hard to establish ad-hoc (e.g. arranging duress 'canarie' words, etc).

The technical BCDR for availability is most easily supported: the CRL can be distributed over a CDN (CloudFlare is free, and Jim Basney is doing that for the CILogon CAs for instance), it can be mirrored and the mirror CRL URL included in the distribution, or even in the CRL CDP URIs in the end-endity certs (this is done for ArmeSFo at KIT, and the former – with the support and endorsement of the UGRID CA operators – also at the EUGridPMA main mirror server (*.mirrors.eugridpma.org). Cross-mirroring between peers is encouraged, as long as the URI are stable (and the distribution supports multiple URLs for the CRL).

In case of issuance problems, it is possible to pre-generate a long-lived CRL – at the risk of not being able to do new revocations. This can be a temporary work-around, and the risks need to be assessed. If no new CRL can be generated, and the escrow model is impossible or unreliable, then a CA would need to be temporarily suspended from the IGTF distribution until the situation can be remedied. Luckily this has not happened in this case. And we commend and have deep respect for our UGRID colleagues who kept their operations in Kyiv fully going during the invasion, with a lot of – well justified – trust in their country's and their own strength!

We also reconfirmed that any (inter)national sanctions and organizational policies must be applied at the authorization (AuthZ) stage, and that the identity certificates and the issuing CAs are inappropriate and ineffective places to attempt to implement and enforce sanctions. This has been true for the past decades, and continues to be true today.

For the moment, we conclude that the standing subcommittee on suspension review is the most appropriate body to discuss urgent and sensitive issues. The conclusions reached there will be submitted for reconfirmation (or reversal) by the full membership at the next plenary EUGridPMA meeting. The subcommittee is in principle open to anyway, although in case of conflict of interest the party involved will of course be temporarily suspended from the committee. **Nuno Dias agreed to join the subcommittee**, so that is now consists of: Jens Jensen, David Kelsey, Jan Jona Javorsek, Nuno Dias, and David Groep.

We point out there is an IGTF keybase channel for secure communication as well. Links are: https://keybase.io/team/igtf and keybase://team-page/igtf

OpenID Connect Federation

Roland Hedberg is moving towards finalising the standard, which should be 'fixed' at TNC 22, including a showcase presentation by GARR (it will also be presented at the NorduNET conference in Reykjavik in a few weeks time). The standard is thus moving to a more stable state, with less 'experimental, complex' features, and gets a more polished stablity. This looks Good™. And it's now time to look at the security aspects of the OIDCFed: the framework is rather open, but the specifics need to be defined. This we may get from the GARR implementation: GARR has made various micro service implementations, and has provided APIs to provide 'drop-in replacements' to replace existing static config setups with almost zero

changes. If that is working, broad implementation might be going 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 – based onpath traversal (not graph construction, apparently). The meta-data can be placed in the 'trust anchor' (MDSS), so the 'web of nodes' is still there. The biggest changes are in the policy verifiability controlled by the RP – to make sure that the OP/RP is compliant with the meta-data for the service. That part has changed extensively. The GARR implementation will nail the operational details.

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

Assurance requirements and FIM4R

The FIM4R group has been rather quiet recently. Following the (widely downloaded and quoted) VIM4R v2 paper and its EOSC specific position paper (10.5281/zenodo.3727545), there has been limited engagement by the FIM4R community at large. The ambition to reinvigorate the group may be implemented by a three-pronged approach: (i) develop a general update to the v2 paper to cross-present the developments in AAI in each of the communities to the group as a whole, (ii) running an interactive F2F workshop, and (iii) use the need to get assurance assertions from the identity and attribute providers into the (community) proxies and services by way of having a 4th, assurance specific, FIM4R requirements paper.

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 do not actually 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.

But maybe: is implementing RAF on the side of the service providers considered 'more complex' than just re-doing all assurance and even identity vetting locally yet again? Even if the IdP already does it, and is even willing to convey it in REFEDS RAF standard attributes? Like SURF did for its 'SURFdomeinen' service step-up assurance, where SURF did *not* use RAF, and even for those IdPs which *did* do RAF completely still insisted on re-doing it on a per-user basis yet again – including some videoconf-based identity vetting, as DavidG experienced? If even a well-organised service provider like SURF cannot do RAF and wants to annoy the users of its services instead of doing RAF, is that representative of more relying parties? ☹

Are there more experience stories on trying to get SPs to get to require RAF? Not that many SPs speak up publicly. But there are also very good and forward-thinking examples, such as DFN which is implementing RAF (replacing a previous national scheme) and who plans to go into production this year. So, if FIM4R is to collect the assurance requirements, will enough communities sign up? The LSAAI seems the obvious use case (with Mikael present). Getting a broader engagement from the FIM4R communities in the requirements group would make a more convincing use case. Pressure from national governments might be a mixed blessing: lots of need for assurance, but then only their own definitions and requirements (and usage tracking by them, maybe). Or it could mean a push for more use of national IDs that don't work globally (like eIDAS and other European eID schemes, which are rather useless for global use cases since a need for a catch-all will then always remain).

Following all deliberations, we defined the **following actions on FIM4R and assurance**:

- There will be a push for a FIM4R v3 paper (if the FIM4R group agrees, of course), as an early output of the GN5-1 activities
- An open call for input should target real individuals (Hannah might hopefully be interested, Maarten can help out but not quite drive it). Jule is also willing to help of course.
- Primary target are the authors of FIM4Rv2 – Maarten will collect the list and prepare for asking them (who does the asking remains open: DaveK, Hannah, PeterG, …)
- Include also input from MyAcademicID (via Christos Kanellopoulos)
- Aim for publication by TNC23

The IGTF BIRCH/RAF Cappuccino level is today providing medium assurance, which many of the research infra depend on. Where we now move to tokens, we should either ensure we get that from 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 even Google). The "no single solution" statement from FIM4R v2 was indeed taken to heart, which is good. 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 mixed result) might be used here again, so as not to ask the same people twice the same question?

REFEDS RAF v2 working group status

Presented by Jule, who chairs the REFEDS WG

The REFEDS RAF version 2 document is under active discussion (including the more general discussion on how to express "v2" versus "v1", which remains an open item). The document for RAF 2.0 is at https://docs.google.com/document/d/13tfexdOafnSEXidJ6fbcT0a5qo0wrsu_fqLk856AaTA/

A key change is that the assurance requirements are now also in-lined in the document (as an option next to Kantara, IGTF, or eIDAS), for those not following one of the existing frameworks. That makes it more comprehensive and self-explanatory. Also adding more 'FAQ'-like text should help in this regard. For example, "local enterprise includes those anyone vetted to a same or better process", makes it clearer that local-enterprise can also be asserted for user who are merely equivalent to local enterprise service users. Care may need to be taken with terms that are also in GDPR (like "vital").

The interdependencies between the requirements will need to be defined sufficiently clearly so that 'time shifted' identity vetting is obviously allowed (like we have for BIRCH, or in eIDAS). For example in IE1: it is sufficiently clear that this does *not* preclude leveraging existing business relationships, where 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. Wording like "information derived from an ongoing business relationship with the credential provider" may help.

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.

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 for hub-n-spoke federations)? It's a bit of a pity that SAML MD does not allow embedding of signed and validated programmatic XSLTs inside it, that can be used by SPs to automatically infer attributes based on meta-data :)
- RAF adoption is rather mixed. DFN is deploying is widely now, but SURFcontext has just one IdP that does it, and even then the federation proxy cannot process it further. And SURF's own SPs still insist on doing their own assurance step-up, ignoring incoming RAF assurance even if it is available. A tear for its SURFdomeinen service ☹.
- When CERN required Sirtfi, that did work! Spectacularly! Now what about a major SP requiring RAF – and see what happens? :) But then, remember that Scott Koranda kind-of gave up on getting attributes at all, having tried for five years to get anything reasonable from IdPs in terms of attributes. But then, scaring the IdPs too much may cause them to give up entirely as well – and that would be the end of federation usefulness.

WISE SCI - adding data protection to the PDK policy development kit

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! With this caveat, DaveK then proceeded …

The data protection statement for WLCG/EGI is sufficiently old now that – although materially it is remains a perfectly good match for GDPR – it does not reference GDPR itself but the 46/95.EC directive. The intent is to updae the AARC PDK privacy guidance, and the notice 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 (Thomas Schaaf, LRZ) has provided the DPMS "Data Protection Management System" for itself, but that is used specifically for EOSC processing and – although having quite good, if rather tabular, templates – does not solve the scalability issue of multilateral agreements. That was the basis for the WLCG/EGI/AARC model: "Pretty-binding not-quite-corporate Roles" (BCR-like, as in the AARC guidelines).

The AARC guidance needs to be updated now as well, referencing GDPR: it will *still* have to be based on the BCR-like model, given that the risk is limited to the R&S attribute set which researchers anyway want

to make public, and that there is no binding CoCo. Lawyers will probably continue to claim that it's 'not legal', but then lawyers should be in this wol to point out risks, not to make decisions.

The disclaimer at the top of the EOSC DPMS is worthwhile to be copied. We (WISE) provide 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, so even if we are no complete, it is still useful. 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"

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. And, frankly, the end-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.

We note that there are (at least) *two* good templates for privacy notices. The one that is actually understandable by users is – of course – on the JISC web site. It is readable, and – by paraphrasing the legal bases rather than giving article numbers – makes the users understand what is happening. We surmise that of course Andrew Cormack is behind this really nice and readable notice (unfortunately, the entire JISC website is CC-BY-NC-ND, so you cannot derive from it, but you can be inspired!). It's at https://www.jisc.ac.uk/website/privacy-notice

Then REFEDS CoCo, and also the EOSC DPMS, have the tabular form. It is also complete, and makes for simple completion by the processor, but is less readable by the user: https://wiki.eoscfuture.eu/pages/viewpage.action?pageId=24514251 has the text.

The WISE guidance can point to both versions, state a preference (of course), but both are in the end fine. And both are better than concocting a dubious one from scratch!

Enabling Communities with GEANT's eScience Engagement

The Enabling Communities task within the GN4-3 project encompasses both specific targeted activities (InAcademia, eduTEAMS) as well as the key cross-domain elements ("enabling communities"). The latter is always done in close collaboration with existing 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). Of note: the paper on assurance in PoS/ISGC has now been officially published. Also Sirtfiv2 is almost complete now.

WISE SCI similarly aligns very well with EnCo, and cross-infrastructure security risks get special attention. 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 (volunteers welcome, besides just UK-IRIS).

Many of the activities discussed in this meeting are co-supported by GN43 EnCo (just as the meeting itself is sponsored by it, as it is also an officient GN43 EnCo Workshop).

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

Communications and Security Service Challenges

There are several types of security challenges. The 'complex' one, with in-depth probing and the possibility for forensics training, is performed by EGI again using the CERN CMS experiment framework as a deployment strategy (thanks to CMS!). 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 may 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 upgraded, 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.

WLCG and public cloud hybrid trust models for server credentials

Contrary to end-user client credentials, there is, today, no model for combined assurance sourcing for host credentials. So, whereas the original 'trigger' (some US-based organisations not being able to find their credential provider, or not procuring the right credential provider, and thus not having access to appropriate IGTF & WebPKI combined accredited providers – but there are of course server/SSL credentials through either InCommon or the renewing DigiCert IGTF ICA available) is not a current issue any more, other use cases remain. These include public-cloud-provisioned K8S clusters of services. And those cases where there is a need for combined IGTF & WebPKI trust, but the (national) CA provider does not offer a profile that supports that (note: both InCommon and GEANT TCS have joint-trust

products in their portfolio). Also, not all CAs have API or ACME access to issuance yet – which is a prerequisite for dynamic (cloud) provisioning of services. Meanwhile, 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 (basically, abusing the host credential as a robot); and for signing assertions (e.g. the VOMS server re-using the host cert for signing the attribute certificates, rather than using a separate signing cert).

And given that the aim of web PKI is an agile ecosystem – regardless of security severity, as per Ryan Sleevi's comment "*The goal of the Web PKI is to ensure an agile ecosystem. The best way to ensure that agility is to ensure that revoking 50,000 certificates is easy, so that it does not matter whether or not there is the security breach […]*", in https://bugzilla.mozilla.org/show_bug.cgi?id=1650910 – i.e. the security of the ecosystem need not be considered as long as it is agile. And the life time is shortening, with WebPKI going to periods shorter than 1 year (90 days in not too long a future), there are elements to be considered here in not using the certificates used for the networked endpoints for anyting but precisely that. And not use the host certs also as clients. Yet of course, many DCV CAs that are 'free' (like Let's Encrypt) do not properly set keyUsage to reflect that, also keep assering also clientAuth in keyUsage. Which makes the proper mechanism to control this unavailable.

Meanwhile getting ACME and/or API access are critical. Most of the larger CAs anyway offer at least API, and some offer ACME for most profiles.

We worked on the comments and clarification in the WLCG WG document, and the next meeting will be on May 31st at 11.00 CEST (0900 UTC). Minutes are at https://docs.google.com/document/d/1Sl0C_q-lGMCifChmFArHjsGzdnd-RM7O7jbpsGa8XRw

Laws of Software - and the progress of development tools

Since the early days of Assembly, ALGOL, COBOL, FORTRAN we evolved now to a world with CI/CD and integration tests. Better tools make for better processes in the past 65 years! Do better tools for authentication today also make for better processes? And a better user experience? Even when taking the four key 'lawsofsoftware' into account?

Wirth's Law: 'Software gets slower faster than hardware gets faster',
Hofstadter's Law: 'It always takes longer than you expect, even when you take into account Hofstadter's Law',
Zawinski's Law: 'Every program attempts to expand until it can read email. Those programs which cannot so expand are replaced by ones that can.' [which implies extensibility (good) and bloat (bad)].
And of course Jens' Law: 'Complexity has to go somewhere (and computers should do the boring stuff)'.

See all of Jens' soapbox to understand the full implication of all this!

Operational matters and self-assessment process

Two authorities are currently in the peer review phase of the self-assessment process, with a mutual review responsibility. In practice, we observe that both the self-assessment as well as the subsequent peer review process take a disproportionate amount of calendar time to initiate and complete. While in

this particular case, **DavidG will complete the peer review for LIP**, there are obvious issues with the process itself. The purpose of the self-assessments is now actually two-fold: first to establish responsiveness and engagement of the (authority) member itself, and secondly to alig documented with operational practices within the AP member's operation. The TAGPMA uses the annual membership reconfirmation letter for the former – which does tend to focus attention. APGridPMA, some members also are more diligent (and engaged) than others.

In practice, there are non-documented trust (re)establishment moments during an EUGridPMA member's life cycle. Many of the members also participate in other European (or global) activities, such as EC programmes, EOSC, WLCG, &c. In those contexts, the members that appear lessactive in EUGridPMA do meet with each other, and with our RP members, and in that way establish trust and working relationships. But such is not visible in a structured way. In addition, with large credential service providers like TCS leading to consolidation of the landscape, some smaller AP members are in a (planned) process of decommissioning, and thus have less of an incentive to perform self-assessments. Meanwhile, most are in regular contact with at least the Chair, and their continued CRL availability does indicate operational continuity. In case of failure, follow-up by the chair does result in (usually timely) communication.

These factors combined result in an (apparent) weakening of the trust fabric. Evicting Aps from the distribution might appear a solution, but in practice our largest relying parties (such as WLCG) do depend also on those providers (typically countries with a WLCG 'Tier-2' site). Hence, we do need support from WLCG and EGI before this becomes an effectively implementable mechanism.

To ease timely completion of the process and ease the time requirements – and raise urgency at the same time – we will run with an alternative process for a while, that focusses on short-term insentive communication between the assessing AP member and its peers, through a series of focused interactive videocalls. We will pair reviewers/mentors and AP members, and they will go – outside of the plenary meetings – through the CP/CPS document together, with the member commenting in real-time (voice) to the assessment sheet questions, and the reviewers able to give feedback there and then. After ~ two weeks, a follow-on session based on an updated CP/CPS (or updated procedures) will conclude the process. This allows arranging meetings at more convenient times, and focusses attention fob oh assesse and reviewer. The actual changes needed may even be minimal. In this way, we (i) delegate trust to the reviewers, and (ii) help the AP member in an 'assisted check' mode. This is not unlike the RIPE NCC 'Assisted Registry Check' model that replaced the previous audits of the LIRs.

We decide that our 'Chief Nagging Officer' **Cosmin will start the process** with those authorities tht have the 'oldest' outstanding self-assessments (>7yrs), and that **Dave Kelsey, Ian Neilson, Jens Jensen, Jan Chvojka, and Fayza Eryol will act as mentors** for this first round.

DigitalTrust update

DigitalTrust (part of the Digital14 group in the UAE) continues to provide a range of credential services including the IGTF profiles, both for the UAE (research) constituency. Almost as the only provider – **DigitalTrust makes IGTF profile products available for individual retail** across its global service region. As such, DigitalTrust is currently the only provider in the EUGridPMA to offer this service in countries and to communities that have no other way to access the IGTF credential products -- almost all of the

other providers are either national, or constraint by their membership constituency (TCS), or only offered under a B2B contract model. This is of use e.g. for the EGI federation.

Paul Mantilla (with Aaron Carolan as alternate) will be the new representatives for DigitalTrust, now that Scott Rea has (very recently) left DigitalTrust. The handover has been well coordinated and authenticated.

Keybase channel

We point out there is an IGTF keybase channel for secure communication as well. Links are: https://keybase.io/team/igtf and keybase://team-page/igtf

Chair election

May has the traditional chair election for the EUGridPMA on its anniversary meeting. Since this agenda topic was announced late, and the meeting was not quorate, the process this year – in accordance with both the wording and the spirit of our Charter – will be a two-phase mailing-list based election.

1. The one fully independent RP member, Ralph Niederberger (who is himself not eligible to be elected) will be asked to collect candidates (if these want to remain private for a while), and if necessary to collect votes. **He will be asked by DavidG (done on Wednesday May 25th)**.
2. Candidates can present themselves on the mailing list or to Ralph until June 13th (allowing 3 weeks, given the holidays in between)
3. David Groep is willing to do it for another term again, but that should not stop others
4. If there are **no counter candidates: then DavidG is re-elected** by default without further voting
5. If there are more candidates, the vote collector (Ralph) will collect votes over mail during a 2-week period (until June 27) and announce the result.

Attendance

We thank Jule Ziegler, David Kelsey, Maarten Kremers, Ian Neilson, and David Groep for their in-person attendance in Garching. Jens Jensen, Adeel-ur-Rehman, Mirvat Al-Joghami, Miroslav Dobrucky, Paul Mantilla, Cosmin Nistor, Eric Yen, Nicolas Liampotis, Kyriakos Glinis, Jan Chvojka, Feyza Eryol, Lidija Milosavljevic, Mischa Sallé, Ralph Niederberger, David Crooks, and Nuno Dias all managed to survive the three-day-long videoconference call, for which they are to be highly commended!

(notes by David Groep, consolidated May 26th, 2022 – subject to mistakes and typos)