PMA47 2019-09 Karlsruhe (1)

Participants: Maarten, Ian, Melanie, Bozidar, Mirvat, David, Jule, Scott
Uros, Ingrid, David G.

Remote: MiroslavD, Vladimir D., Roberto G., Cosmin, Nuno,
John Hewley., Hannah, Adeel.

Monday

10^α intro

agend adds: (1). @ANPL meeting on combined assurance models.
silver CE logon based on community assertions
what could/should TA do (RCauth. or Pathfinder).

GN4-3. SCI:/Uros → Push to add Trusted CI to the SCI list. (likely Susan S)
is now with TrustedCI but no updates.

review of the NSF Cybersecurity Summit where Susan
will be - also at CERN next week.
(OSG can now support travel to Europe)
hopefully somebody looked for Trusted CI.

Assurance
Jule → IANA. OZH

logo's for assurance (combined w/ other things that need a logo)
with Nicole H. → GEANT has designers.
maybe register? since it gives assurance.
publish so that it becomes known.

Sirtfi lots of discussion. → see folder Google drive.
(view-only).
response guide under development.

AARC ops
also Andrea Ceccanti for WLCG, DOMA & ESCAPE

what about WebAuthN? (Uros). (see REFEDS TNC19 presentation).
from Norway folks).

through both ID bump eIDAS in tchus → also UAR @ swtr. or hrpt.

AA VOMS moving to newer platforms? → move to IAM?
there is an (older) library from Manchester to just create VOMS AC's. link that to newer org mngt systems like COManage / eduTEAMS?

This need VOMS-Admin, which is used by Uros for eduTEAMS!

PDK people still don't really know what to use, esp. if you only consume – at which point you need to describe user management.
Used at HDF and in GridPP.

At bootstrap time of a community not everything is available all of the same time, – so it has to be swallowed whole or modularized → create steps.

↳ "Implementation guide".

FIM4R blog on fim4r.org. targeted at HEP & DUNE collaboration.
combined assurance, or CI logon Silver via RAF Cappuccino.
natl. ID checking is @FNAL. → is authZ
several US HEP people from e.g. BNL & BrionB.
next: @TIIME.
see combined assurance slide from AARC2 review "boxes" ⇒ -

(11[20] Coffee) 11[35] // IanN – diff Assurance

Access to services (in this context GOCDB) for "trusted" user takes "had to be" accepted. Eg. with the linked draft procedure.
Issue is generic for non-EGI infra's (UK IRIS for instance) as well.

two options. → BIRCH, or do assessment?
and what about Google. [see DLG's mail to SPG].
Risk assessment!
google names can be intentionally confusing. so gb needs vetting: remote vetting?

non R&S: remote vetting for non R&S.
e.g. through NFC checking of passports with apps.
With a good phone.
needs a biometric passport.

risk → lower assurance requirements (like read-only goodb access).
Unique & actual person. → individuals.

for most R&E federation that actual person is pretty well guaranteed.
and in many cases DFN is probably internally BIRAH quality.

Need for a good reference process for communities.

Remote vetting via a passport distribute the RA. Hierachical.
implicit RA via a secret communicating through agents.

Catch-all by the Infra's is costly (but needs to be there)
address of record based on professional affiliation & address.

This is essentially an RA infrastructure.

Needed:
- risk assessment, (based on examples) e.g. like in BDK).
- vetting process choices (e.g. points system for options) (phone not from public registry).
- catch-all functions for EGI & Infra's, RA & maybe more.
- link to a 'bumped' SSO Account at DOGWOOD. (R&S+Sirtfi).

for citizen scientists need something else.

—

12[20] Cosmin // 3-A.
Ulles/Sens: sent the doc again. → pending.
CESNET: declare success! OK ✓
MA-Grid: pending on some op changes.
ND-Grid: pending.
RDIG: pending.

Austrian Grid: gone in next 1.102 release.
&.

14[15] David/RAFCC. [see slides]

-do send the heads-up. both to Lost and contacts.

-after 8 days start the review process (30 + days).
and re-test repeatedly until compliace (no suspension).

to prevent overload, actual contacts used should be shared?
so actual addresses? NISE known people did not quite like that
do classify by 'level' (with EGI SSC's being almost highest level.)

post to the wiki → ~~how-do~~ prevent by information. no blocking.

For the challenge QB.

scope: all auth.

~~scope~~ aim: just response.

send to every address. (unique addresses).

for GDPR compliance? - do not ask for name but for something other 'human'.
('1+1' = 2 v "11" v 106.)

- use it for follow-up, mails will be deleted afterwards.
check against membership database.

(NISE SCCCSHQ - 15 Oct meeting)

e.g. RCauth testing RCS+Sirtfi will find overlap w/ eduGAIN.
an overview as a first start.

Run ocon → Oct 23 2019.

Tea 15[20] - 15[40]//

25[42] // David (SlateCI.io) -- guidance on registration for communities @SCI/NISE
per risk. (not by what is affordable).

give categories for AUPs and tagged a level alongside it
and then how to manage the community.

the AUP service provides should be the ones stating and
promoting the processes. Implementation guide needed.

SLATE.CI - trust model changes - are looking for (security/policy) input
- distributed SLATE.CI also in UK → CVMFS caches.
- WT #16 → curated canned apps. VO Portal #3.
- risk concerns well-identified in slide deck

PHA47

SlateCI.10 (contd) working group formed Sept 10th for WLCG. (Rob Gardner, Romain N) (5)
see the problem statement written @ Fermilab) as it includes security & trust.
wrap-up by May 31st 2020.

openness of WLCG to be discussed.

16[30] // Derek - TAGPMA Update. Jeny Teheran is now TAGPMA Secretary.
Derek is now also ½ of Sim Mandeller → co-lead
for XSEDE security (and Sim moved to Penn State).
and Derek now doubles for XSEDE as well (and is paid!).
OSG is now an RP member.

Move to "service_hostname" with <underscore> violated BR!

16[40] Jens // RCauth.dotr. to better support also EOSC hub.
randomness exchanged with STFC, but not yet with GRNET.

MariaDB does need low-latency for multi master. → takes lots of time.
needs low latency (now 40-50 ms still).

for assurance @ BIRCH via Pathfinder.
suggest linking to RAF Cappuccino (via IdP-SP-Proxy maybe?).

user access to creds (e.g. for DIRAC) should go through a trusted credrepo
like the moonshot portal or MyTTS. (there are >4 now).

17[00] End of today.

09[37] // [after vidyo mess] Bozidar. MARGI CA S/A.
update embed address needed. → incl. domain name.
still on original version. 1.1 was reviewed but was delayed
→ add policy oid for classic to EEC's.

quick fix and approval → then done. should be quick. Bozidar will send.

Reviewers: Tom N, David G.

09[53] // SCI v2. do it live for one example (EGI Fed)
Uros has the spreadsheet and is editing live.
Hand at SP.

SCIv2 @ EGI // Ursula Duvell.

example on data protection: EGI has published policies, but auditing esp. the communities of users is not effectively done (e.g. we do not exclude any of the current LHC communities).

privacy notice changes and update → may need to re-present to user periodically (e.g. yearly review).

* in SCI → no way to distinguish "documented" vs. "self-asserted enforced".
→ for training also record traing taken.

add column to describe enforcement ~~to~~ not influencing score but at least make people think about it.

Incident response contacts &c was externally reviewed by TI "certified team"!
↳ added column to sheet.

with the participation in TI / TF-CSIRT comes external collaboration.

colors are important as well. better would be a bronze-silver-gold scale.

11:[illegible] // Scott Rea - DigitalTrust update.

new hierarchy with new name. And wallet for different public trust hierarchy.
since that was the only thing G+ and MSFT claims against. (who would do the DCV)
new model would be WebTrust RA under another CA.
trust anchors by a jan 2020. for the public trust ones.

For the IGTF specific branch is ready now - new infra, but just new hierarchy and namespace change. to DigitalTrustGrid/*

new one is an exact clone, same processes, same net controls, same personnel. (just new HSM's).

(V). New hierarchy is approved by acclamation.

Anubis should start to actually use their certs in EGI &c.
also for IGTF → eduGAIN bridge.

Generally: ENISA trust store ~2025 as a plugin for browser (to break their monopoly) "future trust". in eIDAS context.

otherwise choice is google or Apple.

11^50 // Davide - OIDC. see presentation.
test RP's / OP's. maybe WATTS as RP!
OP's maybe IdP-SP-Proxies.
other use cases at STFC (Sens)

and there is a relation w/ OAuth2 authz from WLCG.

this is not trying to boil the federation ocean. only limited. OP's and RP's need Sirtfi and are thus hierarchically controlled.

it is IGTF wide.

14^05 Dave // Assurance. FAQ: RAF, MFA + SFA are known. (see links)
now published, but how to proceed?
That may need a recharter, as discussed in Aug phone conf.
Additions could be: - outreach
- FAQ development (and link to mature MFA ones)
SFA & RAF don't have such a set.
develop here, and ask SP's to start requiring it.

The 'sirtfi adoption model' by CERN was very effective (if not kindly received by some FO's :-).
That may require a risk-based approach by the SP's to request the "right" values.

And some Fed's IdP's may already be OK (like DFN), but not always expressed. So it 'may be simple', but there can also be some variety per user (e.g. for remote students).
employees are much easier (i.e. those are paid)
as contrasted to fee-paying remote users.

"Sirtfi" had the email service → do also for RAF + SMFA.
as higher value services join, proxies can add requirements.

can we give "simple" guidance:? employee? → medium!
student? → check F2F, otherwise low

"high" is much more complex
at Kantara LoA 3.

start with a simple one. So just release "low" for everyone, and then add additional qualifiers.

normally SP's are charged for authentications, which is an incentive not to over-ask higher assurance.

maybe natl. guidance for the auth'N/vetting processes.
the other aspects of RAF are simpler!

Yet you still need an incentive. (service defines the requirements).
error messages should support usability. (not refuse authN).

(transparency in practice may be more confusing on upstream qualities.)

or lead by example? how many IdP's do we control? And Fed's?
push to add this to 'baseline expectations'.

(*). eduGAIN baselining in WP5 / Baseline WG.

non R&E use cases can also help (e.g. finance). Or GDRR to know 'who did it'
'Those who hold the purse strings should see the benefit'.

15[22]/Jen

15[55]/
DPK// Bomb. assurance model: maybe ask community to check compliance with the RPS, just with checkboxes that makes them think.
extract out key elements for vetting + ID binding that are relevant for communities. and that are "checkable"
What they do as large communities is probably OK.
essentially, with ref to RFC section numbers. this is policy mapping.
or "generate" RPS using a web tool.
Do this in IGTF → create template
vetting and acceptance per-RP.
have requirements inspired also by the LIGO questions.

16[19]// SCIv2.
for +R3 → What does that mean? Review in SCIv3.?!
PRU1-AUP → reviewed by NISE, so is "3" (indep. review).
P2C6 → part of NICEPAUP and thus "3" as well.

SCIv2 assessment for EGI example // DPW.

is there actually a Security architecture documented? recent?
we have all the component parts. and all the requirement from D6.4...
those are "2". and fine.
and AARC gave us the BPA for new stuff :)

OS6 → IDS only at site level, not at infra level. So really a ∅

Done! 17:05 ✓

Wed 25th

09[22] // Hannah - OAuth2:

many of the earth libraries rely on publicly trusted certs.
for the connection itself.

for eduOC and the TCS links don't bring trust, just encryption. And
the trust comes from the path constructed through JWKs & the
"authority_hints."

for the OAuth federation you would need something similar.

(*) the one trust "root" JSON must be secure, not just DCV https!
and that one cannot be reached.

Many oauth. SAML federations do out-of-band bootstrap of the root
signing key (e.g. SURFconext asks to call). And that also holds.
for eduGAIN.

(*) separate transport and trust layers.

the hierarchical + X-signing features (also good for dynamic clients).

10[15] Eric Yer // AARC/GN4 updates.
the update meeting @ APAN was barely short (10 min. only -)

ask members on pathway OIDC for eduGAIN Entity.

10:57 // SanC - Future of keygen (see slides)

Since FF 6g, KeyGen is (almost) gone! (2)
does not work everything, legacy Dutch Grid uses JGridstart.
All has Cert Wizard, but both have Java support issues.

Would a "go" application work? to create CSR's.
typically use a local websocket and daemon just like
video conferencing apps. (without Admin, usually?

a shared process needs an aligned issuance process.

keep in touch through mailing list.

11:07 // Sens? - soapbox. on processes and safely moving CD's.
moving and replicating RCauth inspiration from previous move.
classification of service elements for availability.
(like CRLs that can be distributed by CDNs)

share tools and software → modernise elements of the CP's.
* replicate CRLs / anycast.