

Present: Dave U, Jens, Sam C, Feyza, Bob C, Tamas, Reimer, Marc, Jan N,
Cosmin, Jules, Walter, David G, Scott R., Simon Cooper

Remote: Anders, Savi, Roberto, Vladimir, Miroslav, Ara Gregorian, Narine Manukyan,
Nuno (Misha), Armenuhi Abramyan.

09³⁰ Intro, and apologies to Feyza.

09⁵⁵ Round Table: - Scott Rea still TAG PMA, but now moved to Don't Matter and no longer Digi Cert

- Maber de Jong: PRACE security forum rep. (background in DENSA).

- Sales will retire in a few months - last meeting.

- Tamas: NIF status will "change ^{this} year" and future uncertain ??

very change things around end of all of the NREN.

CERN DG → ask Fabiola (also for Wigner).

for moving the CA → document + audit.

closure → takes 2-3 mo.

- Anders N → moving to TCS

- Savi → moving to TCS

; Roberto → also moving, but very slowly: ((

(ACT) withdraw
old NG CA

10¹⁰ TAG PMA, Scott Rea / < see presentations >

"no officers left" (formally).

OSG is actually Classic (contrary to presentation slides #5 and #6)

"OGF → OSG" (slide #6).

10⁴⁵ Cosmin / Self-audit.

[note: for self audit 1 response is enough]

Belnet → should stop RNN (ACT) → ends 1/1/2017.

Arme S Fo → tomorrow.

Ullsc → new CP/CPS there.

TARAN → prod reviewers

Austrian Grid → moving to TCS.

✓ MARGI → success!

✓ TR → success!

RDIG → pending CP/CPS.

DZESC → pending reviewers

11³⁰ TCS Update / DLG

- logging entire SAML assertion.
- make daily backup of eduGPIV.

→ RAuth! VACT

12¹⁵ Simon Cooper / 818C on 8CS

12³⁰ [lunch]

14⁰⁰ Jens S / Ullerschlag

service quality of RA's (e.g. for PRPCE) is variable, as experienced by Jules. CP/CPS needs extension; LB will ~~always~~ still be needed and will remain.

need major changes if moved to federated auth. → new reviewers and prod in September '16

14³⁰ RAuth / DLG

describe all

Reimer & Ursula said OK → accept.

Reimer modules. → accredited by acclamation!

ACCREDITED!

16³⁰ IOTA Upd / DG

v1.1a approved as errata. → OK

16⁴⁰ TCredStores

similar effort in USFPIA (for DirectTrust). The result is that the requirements there for a credstore online that should be at one level above the protected credential (see always use on HSM). for technical

also has draft comment version of SP800-63-3 with a VoT like approach

The NARE works is considering both decomposition and ISO 29115-style this could help company what the LoA increment could be. We could apply the 'principle' by adding controls.

see 4 → see result. align w/ PUP.

see 4, 01. →

09²⁰ Sales N / HPC Trust.

09⁵⁰ Norman Piliygan / AmesFO. <see slides> Selfaudit.

recent new CP/CPS Apr 11 2016

- doc structure 2527: this is A or B, not C :-)

Reviewers: Jan C, Jens S.

10⁰⁵ Dark Matter / Scott Rea. <see slides>

dealing covered. Reviewers: Feyzer, David G, Jens.

big investment in Research - still eqi resources there as well.

target: end of Q2.

CPS document: in partnership. hardware now hosted in bn but will come to ac.
public trust CIA, inspired by existing accredited CIA by provider.

10⁵⁰ Chair: DLG re-elected.

there is a need for more participative agenda building
and roles (vice-chair? secretary?)

11³⁰ Eric Jen / APG and PMA

the major changes to IOTB + Classic will be disc. by email before APMA.

circulate new APs to all PMA's after this meeting.

11⁵⁰ Disaster Recovery: Jens S, Jan C,

Jens: - "operators are not to try and fix things".

- dual-redundant people, all material on same site.

DEA forced similar distribution of Root → settled on 2 people: 1 fragment.

CESNET DR Case study / Jan C: <see doc>

- 5 parts are on CD-ROM.

- when needed, CD's are securely destroyed by protocol.

Scott: cheap 2-person controls with lockboxes and paper stuff.

Revitalise working group: write guidelines taken from existing s.8 CPS

* Jens, Jan C, Scott R, } but ~~these~~ sharing needs to be limited.

Reimer, David. } most examples are private...

start as Wiki page → then move to guideline. (Members Wiki stand)

14⁰⁰ Vetting model

- presentation..

(in SP000-03-3 LoA2 are no longer collecting copies, just file number.)

- making it clear it's a real passport even video should be checked.
- LoA should not be any, but meet or exceed CEDAR, BIRCH, those are the only relevant LoA's in this context. Marginal increments do not matter (for our AP or RP's).
- RAs should be specifically trained (central) like changing viewing angle to show that it's a real passport.
- ~~The RAs~~ but also notary publics are not tasked to do these checks, they just auth a copy.
- appropriate compensating controls.
- what are we protecting? same person continuity & traceability
- smartphone app to scan NFC passport data

Is it within the current CEDAR/BIRCH boundaries. w/ compensatory controls.

"duty of care", for the RA/TA.

Score the compensatory controls when approving a CPS

discuss on list (Feyza) for endorsing it → target later this year.

See Wiki

15³⁰ Tea

16⁴⁵ OGF: GFD 225 OK.

- Overall status: see presentation and <cloudplugfeats.org>
- from SC30 there are links to SC22 security, to which OGF is allowed to contribute. (but not vote)
- OGF cents: act as a DigiCert reseller and then don't do uplift and so be cheap. (needed for e.g. commercials since there's no public market).
- new docs: e.g. Disaster Recovery structure doc could be an OGF doc.
- move HLCA to IQTF (in a 'tree'?!).

AT LEAST the GFD process should speed up! Jens will take care of it

IOTA + Classic: reference IARE for PUI Tech Guidelines

- Aste + minor update of PUI Tech guidelines on SPAN
- update all to 1.0 for LORA + Tech
- Classic to 1.0
- IOTA to 2.0

endorsed

For EGI: ?
 new acceptable auth
 and ask VO's to
 meet CEDAR/BIRCH/OPEN
 replace acceptable CIA policy

endorsement by other PMAs needed. TAG to update MICS + SLOS.
 LOR doc + PUI Tech managed by EUGridPMA.

16⁴⁰ Jens' Scrapbox!

(mailforward in US to prevent address of record abuse)

17⁴⁰ Next meeting: All Hands @ CERN Sep 19-21
 maybe plan tour on Wed afternoon.

Next

09¹⁵ BobC / Assurance update SP800-63-3: <see slides>

increment level of confidence by asking for additional attributes
 at a different level in one dimension
 inspired by Vot.

input welcome, but no major changes expected.

09³⁰ BobC / Practical Cybersecurity. -> "how to talk to PI's on security"

put in context "we're here to help you":

- your workflow is critical to the project success, isn't it? "yes"
- so we need to protect it! "Ehhh..."
- there are these risks. If you don't protect, you'll sign off on the residual risks, aren't you? Then we'll pick that up. -> "Ehhh"
- now let's talk about what we can do! :-)

This slide deck takes ~1 hr to talk with target audience.

Re-use (also the policy structure).

- keep track of compliance -> will raise awareness.

- use this in EGI/EN* for training / enlightening VO Managers as we move to distributed responsibility.

- PRACE: all the capabilities provided by the Home Sites / centres. no real role for the PI

- Re-use of the CSC work in e.g. NISE (policy templates) and for training in EQI ENGAGE
- providing templates will help communities write their policies.
- for trustworthy science you need integrity of data

10¹⁰ Implementation of generalised LoA.

- Use single sheet for both self-audit & accreditation.
result would be duplicating data from the AP's & from the CR/CPs.
- nice to have hints for RFC section numbers in the AP's so it's always in sync.
- having a check list is also nice & useful
- "white space check": is the same data consistent across all sections in which a statement may appear.
- you'll need to read the whole document anyway.
- in GFD169 → method.

Keep → - hint of where in RFC 3047.

- "annotated AP" with commentary.

first to do review to create the mapping (LDG, Feyza, Seno).
coordinate w/ TAGPPIA.

Equivalence:

- the intent and process were such that they were the same
- no content change in reality.

① - "we can agree and aim that they are identical, because that was the aim and they are meant to be so."

OLD registry is OK! ✓

PR & promotion of IGTF

- the content on the website ~~is~~ (interviews etc) is out of date
< see on OneNote scribbles >

AD - update IGTF entry on REFEDS Wiki!

We have a good story to tell, but we're not telling it. Who can help us tell the story, like the dissemination officers of EGI and GridPP?

But we still have to provide the content.

- What is the target audience? General public, funding agencies, ...
- Write another research paper, maybe as proceedings of the DI4R
- *New journal for OA scientific computing as on-line journal by Elsevier or Springer - "Computing and software for data-intensive physics" representative was at HEPiX.* Same holds for "Journal of Cloud Computing" (with Craigh Lee on the edboard). For internal citation purposes.

What would be the impact of communications?

Add testimonials by VOs and RIs/eInfras: on the IGTF web site with a logo of the endorsing project. Then put on the homepage and e.g. "XXXX says: IGTF invaluable for <blah>".

Generic statement "these projects and infrastructures rely on the IGTF: <list of logos and orgs>" (needs permission from these parties)

For sustainability a "Roadmap" also helps (c.f. the ESFRI one).

Aim might be to expose e.g. assurance levels and get more orgs to provide credentials along those, and more RPs to use them?

We can bridge countries and infrastructures - vibrant community & growing

There is EUGridPMA/IGTF logos present on e.g. the PRACE website and the CERN SSO account page.

Start writing the academic paper for impact on RIs.

Also as an example: Andrew Cormack's content is post-processed by Jisc to result in shiny glossy papers.

Target audience could also be the AARC users and participants.

Create a Wikipedia entry. And some Blogs ... Jens and alter BLog once in a while ;-)

Several blogs in the UK with a target of 8 posts per quarter ;-)"gridpp-storage", there's one for the DFN-PKI, &c

Typically 10-20 reads per day for these blogs, including indexers. (blogging on ZFS has doubled read rates to ~40!)

We can also maybe blog in existing blogs by RPs - so that we get people to get the IGTF message and updates on new work. Blogs should be short (1 screenful, typically), have some graphic, and links in it.

Collection of titles that we want to write something for:

- New assurance levels (and the 'end' of the old names) - Jens
- Onboarding of new CAs. - DarkMatter; RCauth - DavidG/Licia
- New use cases - ...

Contributors:

- Jens and IanN to talk to SaraC on how to present the information (but she'll not have significant effort)
- Jules can contact PRACE-PR, but that won't be a high prio for PRACE
- SURF/SURFsara can be more helpful...

For a whitepaper we first need to generate our own content.