33rd EUGridPMA Berlin meeting.

mo 09:40

Remote : Vladimir, Miroslav., Davi, JohnMcEwan.

Present : MarkT, Reimer, Heike, Paolo, Daniel, Tomas, Jules, Urpo, Temur, Mikael, Cosmin, Roberto, Scott, Willy. Nabil, Adeel, Eric, Jens

Agenda

✓ IGTF All Hands content.

* RAT.

* SHA-2 impl.

=> * Self-audit Officer.

Round Table update.

10:00 TAGPMA / Scott Rea.

- website still to be done. (waiting for CPS creds)
- NCAR/SDSC - not even in bundle yet.

SDSC-TRAGPMA has also been discontinued.

10:15 Self-audit.

BG - CPS sent., reviewers will have a look

Austrian Grid - new root in classic renewed. S/D pending.

- with SHA-512 signatures, EEC have SHA-2 as well.
- online CA is not ready yet.

IDRAN Grid - pending,

Paolo - to review in place of Haspars.

MaGrid. - working on comments Pawel.

PLGrid - pending robot.

UK eSc. - started review.

LIP - pending

33 EUGridPMA . (2).

3/A HREN : - declare success.

CALG : - pending.

pkIRISGrid : - waiting for David to review.

NIIF : - document to reflect RPi done.

- send, or declare success tomorrow.

SlovakGrid : - declare success.

"

MARGI : impossible to contact / elicit reply.

before suspending : ① - phone call to address/no in CP/CPS + reception.

② - letter to CPS address

HIAST because the CRL not updated. - suspend from distro for operational reasons.

for RP consistency & new software.

We understand the difficulties, but there are new operational issues at the RP's.

General Guidance

suspend operationally after ~~90~~ ~~(90)~~ N days without CRL.

must react to RAT CC ; after ~~90~~ ~~60~~ N days?

} ⇒ All Hands.

RAT CC every 6 mo?

clock to start ticking after last test, then a 30 day timer starts. (Sales Vol.).

discussion goes between 30 to 90 days.

rough consensus on 30 day. (so next one after 30 days).

Replacement at Vlospous: Cosmin.

~~absorbation~~

non-response nagger: David G.

Nagios no longer works reliably, removed from public pages.

Adeel / PKGrid : see slides

- some identity level to go in 2.2.1 and in relying/renewal sections.

- Update GFD.169 (also w/RPS).
- update to 5280 (or not, c.f. IntDN).
  new 6818 : - paths, - Policies, - path val, IDN
  - sec. considerations.

Reviewers: Tomur & Nabil.
within 1 mo.

Paolo/CERN IT/IS : (Reclassify as HICS).

- DoB Question is no longer needed for HICS ("second factor" also) ✓
- for SSO trigger session expiration for this SP. → strongly recommended.
  "ForceAuthn=true" in AuthnRequest.: good → also for internal security! ✓
- host certs : in internal process change, so fine. ✓

Auto-enrollment for short-lived VM's.

Krb cred based on IP address. (beware of secondary SAN DNS names).

- CN/FQDN based on? name restricted to IP address, and the naming is registered in NetDB. (do you cannot request a VM named "account" :-)
- is the naming reviewed? VM creation has quota. (personal & group).
- re-use of names? scoped to .cern.ch, so that's safer.
  but CERN is large that name use may change. → needs a policy on NetDB.
- sensitive hostname list? blacklist (for paypal-nl.web.cern.ch ?:-).
- the auto-enrollment admins should be added manually/authenticated, as RA's.
- list NetDB process in CPS? including that NetDB users are UserSSC w/class B, C, E access certificates

⊛ Will need new CPS with a more detailed discription, also of NetDB.
(RPs needs to know that uniqueness is in place).

(update to HICS profile might be needed.)

Paolo Self audit CERN IT/IS: see slides.

new CP/CPS forthcoming.

CRL issued normally once a day.

Reviewers: DavidS, Robert, +Scott on auto-enrollment.

14[00] Eric Y / ASCG / APGrid.

IGTF F2F: limited.

+remote attendance.

4[30] DavidG - Robot 0.3 (v1 rev3): removal naming section (as it's not 1-scp).

endorsed! ✓

- On-line CA guidelines: endorsed ✓

1[45] ScottR / RPS: see attachment.

Naming discussion - being able to keep the name for EECs depends on whether RA owns all process and documentation.

section §1 done. ✓.

6[00] focus on §§ §3.x and §9.x.

17[30] made it till 3.4

09:15 Ursula. Wildcard certs.

slides for motivation / FTS.

mixed use of * and ? as not-left-hand-only subdomain name.

CAB forum guidance allows only LH-only, and this gets implemented in e.g. Firefox.

do *.ftsnodes.gridka.de 'would' work.

then validation based on DNS/whois. is also clearer.

Classic RP does not say anything about it.

since 'fts-*.bla' does not actually works, ought to be in GFD.225 or so.

cert with the wildcard has to be on the same host.

- so each node must have its own cert, but with the same name
- only allow '*' in left-hand subdomain name, on it's own. (GFD.225)
- it's recommended to have a specific subdomain with a responsible person assigned.

09:50 TCS G3 / DavidG.

Reviewers: Jules, Reimer, Dane K, Urpo.

for TCS: education for end-users → FAQ
for institutions → to be done by TCS / Alessandra

done by February release.

Scott: tech + operation presentation (confidential).

33rd EU GridPMA Berlin TAG meeting

12:45 Ullesc / Jens.

collaboration - output is open as to what comes out. Timelines mentioned are tentative.

14:15 Dogwood. - see live doc.

⇒ include inc. resp. section in CP/CPS, SLCS. (§ 5.1 from IOTA.)
INCIDENT RESPONSE should be there!

be. LoA §5 well-documented and maintained. → for SLCS/MICS+Classic

new versions attached to Niki's.

16:05 Seifenkasten / Jens

risk inventorisation & sharing.

WEDNESDAY.

09:20 SHA2. HAIGI: must present in CPH, may be over video but must stay connected for longer time.
(ACT).

SHA-2. done in EUGridPMA RPS are still SHA-2.

Google's agressive timeline might suggest Google's knows something we don't get know? Or is Google just FUDing, because of market share they have.

So SHA-1 must be gone before 1 jan 2016 ... publicly.

The 'should' may be interpreted to permit exceptional SHA-1 at discretion of CP

SHA2 for the CRL, it might be at SHA1 for as long as the CP can issue SHA-1 certs.

Many CRL's are still SHA-1

* roll-over of SHA-1 Intermediate ICA's. : do it with new serial.
* a few CP's (AEGIS,) almost switched, but had technical issues. (old Open CA)

all AP on SHA2, TAG OK.

Ursula to run RAT CC with the SHA-2 questions

① - "do you now issue SHA-2 by default?"

② (- "when will your last 'default SHA-1' cert expire?")

⊗ get ACK.

① should be answerable. within one working day.

② might take longer...

For CSR's it is less relevant as they live longer shorter, and there are other compensatory controls (digest of key in validation, or secure channels).

updated Leab.org web. URL.

RIS/Scott. section 5g in detail. done (

So latest version has sec 1, 5, and 9 done.

Latest attached to agenda

11:50 SIR-T-FI /DaveK.

for IdM training: train IdM folk to interact with (local + TE-CSIRT) CERT's.

12:15 end