Minutes: Meeting on Monday

Introduction: 12,000 issued, 2,000 valid of which 50% were 50% loss
Sulan: 2,500 issued, 98% invalid, 2% seen.
Davido: nearing to TCS (!) (~6,000 issued, ~1,000 invalid).
Ramone: 1,200 valid cards and 105 CP's. SLCS is not a lot yet!
Alice: 800 valid users + 800 server = 1,600 valid.
Catch-all stopped.

Emir: 4,397 issued, 117 active (30/50%).
Debra: self-issued issues fixed.

Christina: 2,500 issued / 700 valid. SEE GRID is main catch-all for EG.
Cleon: going to switch off the current CP and migrate to the new one.
Nino: new CP/CPS and fixed issues.
Roberto: 2,100 valid cards & 850 CP's of which is an international.
Moving users to TCS (with a QMEX box).

Tima:

Eric: 150

Daniel: ph/DRIS

David: TCS has run into local, i.e., policy issues and is on hold.

They: still <100 active.

Dave:

Hiromitsu: 150 valid (of 700 issued). 50% CP's
Conrad: >1,000 issued, 150 invalid.

Alexander:


10:03 Eric: APPGridPM,
- AGM met and discussed for new CP in Singapore.
- UK leads on a new CP, but not supported by APES.
- 1,482 users, 2677 tests (in total for APPGridPM).
- OP: TH; considering federated CPs.

10:07 TGQ (Ture Durali):
- Remote上网 is most contentious issue in APPGrid. Most CP's like
  allow remote probing, based on e.g., identity, bills, and postal address.
- TGCQ in times, in 2 weeks, than Colombia.
- P3P guidelines for SLCS/ITICS working.
RAT (Juno)

- No real incidents.
- SW31-2.
- What about 1024 → 2048 for EBC's?
- CR1 expiration.
- Communication tests: 6 of 10 responded within 18 hrs, 4 within 60 mins.
  Current system works reasonably well.

R/W communication: need to demonstrate things that are broken.
  Who is the responsibility? CR → I cannot know when to test
  but needs to work.
  RPs → communications needed.
  SSOs → are clueless.

- Raised a tool CR.
  - RPs need a test certificate from the CR's.
  - OSG/ESG can then do the software validation.

- Set up page with test CR & outs on the RPA page.
  - GSS has a "get half a day" package.

- After 2012: not all CR's should migrate at the same time.
- Date "Jan 2012" too on educated guess based on SSh attacks and RP
  agility

- We training CR can be used to test generate test outs - as long as
  - Open SSL supports it.
  - Test Cases: - SSH92 (ESG, CSE, Intermediate CRs, DPs) + mixed chains

- Due to performance should now be less of an issue
  - 1024: MIT recommendation -> why different?
  - 2048 is already common in use already by many CR's.
  - 768 now routinely breakable with enough weaknesses on CRPs.
  - 2048 is default for Firefox already.

- NASA did some tests. -> Dana talks to Jim B. (not tool on any platform)
  - Closer faster with "same public key with a few trits"
  - SSOs don't bits used frequently. - no test needed
  - switch is not yet requirement, but it's not forbidden. Recommendation to change
  - has already thus.
CRL download
still download issues in AS: 2010.
there could be expired CRLs and download issues. FIrst of
these are Network issues, e.g. with dnload.pls.

Chair: re-elected David G.

(since Berlin)
ChristoT to join CRL.

# Lip: complete.
N ilAE: news CP/ES Upcoming.
? polIB: no updates yet.

# ArmSt: live audit completed July 2019. Detailed reviews done.
system from then sent to UK and too heavy.
only mid-prod left.

# SRC: done and compiled with v1.2.
X REGIS: nothing heard from driven

# Switch: OK.

# BalticGrid: still awaiting approval.

# BalticGrid: OK.

# RDG: self-audit run and auditors reviewed and commented.
showed that there are some known items not listed and
not yet fully answered.

Technically it should not be terribly wrong. Response is good, CPE/OK.
not approved for 2019. Requires that there is nobody but Eugene.

Steps: need for tomorrow.
- Don 2011 update is difficult
- otherwise suspend automatic key.
- Double follow-up via m Ble.

(19:41)
- money still not human should know about this last change.

12:35 Milan: State TCS & TACAR.
- TCS: SSL in next distribution.
- TACAR: new website and process - live demo.

with CENET, CP-2-
the SIRP-1 PP at the CP and is of the DER are, so use openst - sorry.
- Letters should be fixed documented by Chris


**downtimes (de)**
- the website has a notification area
  - mailing list? different from announce list, so most AP's won't notice brief
  - integrating with projects?
  - differentiate between DOW or DS RMS?

  what do we communicate? CRU unavoidably, see can survive, or? All
  of them! Messages should be differentiated for users, directory, sites.
  Sites only care about CRU & IP web.

1. Announcements of downtime at least a week before!
- on a wiki (web) page
- wiki table: on P110 with RSS feed

  Recommendation: link

  > So it allows subscription to the page!

  RSS feed is only useful if you have a cleaned-up
  or new page

  anyone editing the wiki - design should be RSS friendly + email.

  > other options include RT & cc.

**Requirements:**
- CRU's enter their own at least 3x, authenticated.
- email, (+ RSS or any nice) subscription.
- web-based list output.
- one category at least.
- expiring of old messages (and timely).

Tech investigations by:

- Christo
- Milan
- David CC

(0) Downtime announcement: preferably 7 days in advance. (and not
too much earlier!)

NCFA profile. in distribution.

structure is not usually re-purposed locally.

build combination packages with proper dependencies.

> then provide checksum files for big data in the distribution?
downloads of tarballs requires admins to think.

CPP packages are also intended to be re-purposed downstream.

1: who owns the profiles separately!? 2: once, everyone looks at CPP's

when real CPP comes in, we will face the issue now seen with the
worthless training CPP's like in the past case.
I discussed CP 20677, but since then:

- My aim is to complete this today, and then have it approved by all PRSs, so that we can then build a draft distribution.

3.3.3 #3: Single private key for "CP or Trust Anchor"? Definition is: "CP" from definition.

Confusion on terminology in document text (e.g., publishing by pre-paste).
Both CP and RHCP or object CP. Terminology is not 100% consistent yet.

- The organisational body should be defined in the glossary.
- It is still unclear who is supposed to be responsible. Require 'persistence and long-term commitment'.

[In the W3C's case, W3C also operates the issuing CP, so had to show up.]

- Name space must be provided, but actual writing is usually by IG TF CP.

- Must ensure that there is enough information to write the RSPNC and any policy files.

- Is support for dynamic hierarchies ('implicit') really needed?
- This is not supported in middleware anyway.
- So let's clean it up and take it out.

New version by OGF 30 with all changes, to be made by Jens.
- Other PRS should comment before 3rd Nov, send 1 week before OGF.
- Then EU GreenPMA shall own the profile.
- Make document consistent.

—

Davide Retzel Hög.

Putting requirements on the operation of other authority types. Alive existing of the NCI.

- This document does not actually define accreditation, but use it for self-assessment (and maybe later to have NCI's do the accreditation).
- The thing accredited would be, say, 1998, hosting one or more AP's.
- Extend scope to deal with any kind of exception, but still limit to OGC.
- Try to do without the OGC words, and see how we get... and common sense authority...
Eugene - Self-audit of RDG. [Refer also to Jan's discussion yesterday]

Eugene presents all "hard" issues from the audit.

Slide 5: "designated personnel"?

Slide 13: not deleting anything...

Report is consistent with assessment by Jan, except that the self-audit was too hard on the CS itself.

How many operators: 2 persons.

All reservations come in by phone, which is one of the reasons why ARE is being... works with 60 far fewer people. Also, the personal union with security incident response means that reservations are known early.

The PMG commented that this can be done with fewer people...

Roll-over plan circulated to PMG to resolve the "5".

Otherwise audit looks ok.

It is seen as essential that RDG shows up in January 2011. In-person appearance is essential. The least least-bit effort level historically has not been enough. Non-appearance would affect the accreditation status.

PMG sees this as important. It has now been much longer.

Consequences for the Russian Federation and who is severe.

If help from PMG or NLO is needed, we can give that!

PMG thanks Eugene for presenting and the thorough self-audit.

[Dave V. to take notes]

David CC - Grid.Ireland self-audit - see presentation on-line.

- proceed as on slides, with this document.

- changes held off as a new CS was planned, but this has started to materialize.

- Reviews: Nano and Jan - additional data is available.

IST 800-68 and Remote Validation (Mike)

The pending requirement of 88 require the RP to have read access to the aging issues databases!

Actually - all students in a class will share 155, since they share addresses and mailers! Email address is also enough.
at h2 security is based on email, so dependance level of portal/email is highly variable in countries.

In existing ICPE remote has not any publics, e.g. for classic.

May a level NIST 2/2/3 new profile? No (ICPE) do not need to match NIST, see just in Common is using NIST.
CHS with NIST 2/2/3 can go into level 2/2 bucket.
Is would RPs pick only NICE, or always pick all anyway?

LCRS already fits for NIST 2/2!

Can CI Login + In Common may use Comodo as a back-end.

Historically In Common was slightly different from NIST 2/2/3.

The In Common, Id vetting, adds the student ID as valid, which may result in a circular proofing possibility, as per 4.2.2.3.3.

So maybe NICE is not really the right. InCommon is moving to NICE, though.

In Common: also email is enough.

Address: In Common: what about the avoid steal? Is left to WHO, CA only records issuing WHO.

RCS retained R2F!

Is remote vetting really critical, does it add much to the business case.
Submit it do only R2F? RCS can do that; do why not in US?

In LCS: probably not interested in remote students, as mainly religion staff and PhD students, and they would show up in person anyway.

Should RPs accept a new profile as they are NICE today? So that these would not be an effective difference.

Ask CI Login for the use cases where remote vetting is critical, for RPs.

We want CI Login in, but based on R2F, so IdPs should differentiate like the RCS does, or CERN.

SICS would match remote now.

Also: RCS level has effective high level that needs to be conserved.

Need to understand RP use case!
Use the subject namespace to differentiate between remote and T2F, and only advertise the T2F namespace under NICS. A CPS would be better. (policy could not be processed).

Many people feel that records of remote should already indicate in the BGP records whether it was in-person or remote.

Reliance on national info like postal system is incommensurate and complex between countries. The nationalized document of Brazil is at least as reliable.

- Ask C1 Logon for RP use cases for remote.
- Split in 2 CPs (pat via namespace).
- New profile is also good solution, but differentiation is better, or RP's with NICS will lose out on T2F vetted people.

VRP/MP may view it as equivalent, given the operational background.

and why is InCommon Lower than NICE? !

**Conclusion:** EUQPMP NOT happy to include InCommon Remote as-is.

**New coffee run**

License and OS distribution.

- Debian (Rattus) is regarded as important.
- Yorke redistributes under Mozilla Public License 1.1.
  - Lots of AS Blah in it, as not reviewed.

Meta-data CC-BY = OK.

- Trust on behalf of these present = OK.
- @V: OK.

- What about use of DPF IP in derived works, is misuse thus illegal or immoral? b) last sentence should present it
- We license only the trust metadata and metadata, NOT our document and the PPs's.
- CC-BY should be OK. Misuse from Canada accepted.
- We trust "our" CPS to be happy, and we don't need explicit statements.
Encourage downstream maintainers to make timely (security) updates.

Recommend update within 24 hours.

- Meaning of RP's on our name, NOT GPF -
- More peculiar on your may have RP's on name.

install in separate (e.g. /etc/grid-security) and not in browser or
default system default locations?

- Has impact on trust for web shops, etc. everywhere.
- Do you trust the grid RP's for on-line banking?

May we restrict use of acts to application domain? Does that conflict
with Debian Free Software Guidelines? - and we do limit use of our acts, e.g.
the financial transactions. So for Debian we may end up in non-free.

But: requirements are on the subscribers and RP's, so limitation is not on
the acts itself.

Is a bit of hairsplitting, but the package you can use anyway you want.
So it should be OK.

Many, also commercial, RP's, will restrict use, e.g. on life-support systems
or nuclear entity.

Act -> ask Mattings for OK/Acknow.

PUP is quite happy with this process!

- Also they may be put in the as default locations, so that some
  (text-based) browsers/etc + services
- As distributors should figure out technical details.
- And ensure that the joint software will work!
  (do link or install in /etc/grid-security).

Sens: update to PUP - related to raffp asics/pics update

Change in line 68 and 69 of raffp in OK.

old: ... 1.1.5.2

✓ Approved these changes!

new version...

9.2.2 - 3g: discusses activated private keys, whereas rest is about de-activated
keys
The intent of 2.2.3g was to allow SICS costs to be used exclusively like user proxies today.

This doc is only about network resources. The intent of the doc is thus still even though it may be unclear. The footwork explains it. Jeps will come up with a new draft that is clearer, and the RNP can see if it actually works.

**LUNCH** until 1540

SICS/RIACS updates

- **version 2.2 SICS:** changes agreed by EQP?
- **RIACS? V1.2** last related 8/14
  - suggest remove "in particular — 17v" in sec 3. since it’s in the p2P
  - reference to GPP-RIACS, changes between RIACS 5 4 and SICS.
  - In 4.4: relocation requirement seems lost. Is that intentional?

- only it is correct, but "second part" about relocation in code 1D is compromised a missing.

Request update.

- in sec 9. de-capitalise "Business Recovery"

for the PCS having Commode have a BDR plan is enough.

not needed for access/portable devices.

CPS $1 is enough.

It is not needed for the ITH & ITPs.

with this understanding approved.

---

Fetch-IRL promo

Support for 2.8. got in Q3, E/E approved 2Q for 2.9. out in 2011 Q2.

CQS: tested new deploy 1.3.1 and it works!! Yeah!

BT: new format for test out release!

---

MASH

part of EVimentGrid. Roberto gives review update.

Roberto sends review, no feedback yet.

New reviews to use excel sheet: would be handy, but is not there for classic. Would be nice to have sheet.

Outstanding critical issues: an current issue of GPR/CRS.

- request complaints to reidentification is unclear.

- 2012 does not have reposition.

- in working web site, one DE missing, but ID = BY. Unexplained.
Hi! Review by Roberto:
- missing info should be discussed in Q&A.
- Re-accreditation still seems quite a long way away; but it’s part of Elitist/Grade book plan.
- They would have liked to come. Try next in 2022.

Site visit to secure data site.

Dunia: Soapbox on trust and science.

~~~ NEDNESDAY ~~~ Not

UKeee. CA new CP/CPS & Software (Jetson)
- went through a self audit last year. New CPS & tool finished. Last direction is run and it will be a complete re-write.
- No process will change but tool changing and split.
- Rewrite is to make it look better and make it shorter. And split CP & CPS.
- No re-re-accreditation needed.

[Notes or presentation]
- rollout expected in 2011 of the new certificate.
- UKeee = TBU as advisory body.
- replaced software (no longer Open CP), but database is compatible.
- Certifiand demo GUI tool.

Testing possible? Eg for Ramesh to test, but the server must not get outside firewall.
- https://svn.essrc.net/tech/cps/AdHocTication for proto info via VPN.
- send out for access to by email.
- Dunia will send link.

DavidCC = Chuck Cotts
- Adam still has some students to look at, no action yet.

Tech list is useful. - even if it is quiet.
Robot uses access PVP.

DC: can the entire robot lay pair itself be in an isolated proxy?

(do not a community one, but a dedicated one)

With the PVP guidelines, a proxy as a 'virtual host' is compliant
and OK.

DFN is already using this

SPICE already done S/P -> separate table.

Next: 2.5 days in Utrecht.