

minutes: Usula on Monday.

Intro: Usula: 12000 issued, 20000 valid of which 50% was 50% hits

Sens: 25000 issued, ~3500 valid. 30% was.

DavidG: moving to TCS! (~6000 issued, ~1000 valid).

Reimer: 1200 valid cents and 105 RP's. SACS is not a lot yet!

Alice: 800 valid was + 800 sewer = 1600 valid.
catch-all stopped.

Emir +
Dobri: 430 issued, 117 active (50/50%).
self-audit issues fixed.

ChristosT: 2500 issued / 500 valid. SEE-GRID is new catch-all for EGI

Milan: going to switch off the current CA and migrate to the new one.

Nuno: new CP/CPS sent last week.

Roberto: 2400 valid cents. & 85 RP's of which 15 are international.
moving users to TCS. (with a QRQR hot).

Time:

Eric: ~~ABE~~

Daniel: phIRIS

DavidCC: TCS has run into local .ie policy issues and is on hold.

Thys: still <100 active.

DaveK:

Remote: Panel, Sales.

Miroslav: 150 valid (of ~700 issued). 8 RP's

Cosmin: >400 issued, 150 valid.

AlexanderB:

Valentini

Tamas:

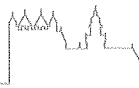
Jan Jona Javorek:

10⁰⁹ Eric: APGridPMA

- NGO withdrawal withdrawn - and now looking for new CA in Singapore.
- new Zealand will deploy a new CA, but for now supported by PARS.
- 1404 users, 2677 hosts in total for APGridPMA.
- JP, TW: considering federated CAs.

10¹² TAG (Time/DaveK):

- remote proofing is most contentious issue in TAGPMA. NIST 800-63 allows remote proofing, based on e.g. utility bills and postal address.
- TAGPMA in Texas in 2 weeks, then Colombia.
- PKP guidelines for SACS/NICS working.

10²² RAT (Jens).

- no real incidents.
 - SHA1-2.
 - what about 1024 → 2048 for EEC's?
 - CRT expiration.
 - communication tests: ① of 10 responded within 18 hrs, 4 within 60 min!
- Current system works reasonably well.

M/N communication: need to demonstrate things that are broken.

where is the responsibility? CA → cannot know where to test but needs it to work.

RP → communications needed.

Subca. → are clueless.

As use a test CA.

- RP's need a test certificate from the CA's
- OSQ/EEC can then do the software validation.
- through GIN? not unproductive anymore. → raise at OGF30.

↳ set up page with test CA & certs on the PMA page.

- DFN has a "CA in half-a-day" package.

Task force: SHA-2
Jens, Mine,
DG, Milan?

- after 2012: not all CA's should migrate at the same time.
- date "Jan 2012" now an educated guess based on SHA1 attacks and RP agility

- UK training CA can be used to test generate test certs - as long as Open SSL supports it.

Test Cases: → SHA2 (EEC; CSR; intermediate CAs; DPs) + mixed chains.

→ 2048 performance should now be less of an issue

- 1024 NIST recommendation → why obsolete?

2048 is already commonly in use already by many CA's.

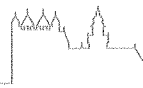
- 768 now routinely breakable with enough shortcuts or PEP's.

- 2048 is default for Firefox already.

was NCSA did some tests. → Jens talks to Jim B. (next test are on public key and is thus faster with a 'simple' public key with a few bits set)

already 2048 bits used frequently. - no test needed

switch is not get requirement, but it's not forbidden. Recommendation to change was already there.



CRL download

still download issues in OSF, also.

then complain about expired CRLs and download issues. Many of these are network issues, esp. with Jambofarm.

~

Chair: re-elected David G.

Self/An ? NCC: no news from Avyph. Denis & Charles K.

(since Berlin)

Christos T to John etc.

g LIP: complete.

~ ULES: new CP/CPS upcoming.

? PHIDAS: no updates yet.

g ARMSTO: live audit completed July 2009. detailed reviews done. update from Area sent to list and was thorough. only mitprods left.

g SRCE: done and completed with v1.2.

X AEGIS: nothing heard from Jason

g SWITCH: OK.

g ^{NHIF} BalticGrid: OK.

BalticGrid: still awaiting replies.

X RDIG: self-audit was sent and Jens reviewed and commented. ~~mentioned~~ there are some locking items not listed, and not get fully answered.

Technically it should not be terribly wrong. Response is good, CRL OK. not approved for 3/2. worrisome that there is nobody but Eugene.

Steps: - wait for tomorrow.

- Jan 2011 Utrecht is DELIST

- otherwise suspend automatically.

- David - follow-up via WLCG.

(ACT) - management should know about this last check

12³⁵ Milan Sova TCS & TACAR.

- TCS SSL in next distribution.

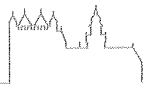
- TACAR: new website and process -> live demo.

with CERNET CA 3.

The SHIP-1 FP of the CA cert is of the DER one, so we openid - forger.

-> this should be fixed / documented by Chris

-> Request: Sova key store as a format.



downtimes (Dn).

- the website has a notification area
- mailing list? different from announce list, as most AP's won't notice brief
- integrating with projects? downtimes.
- differentiate between DOWN or AT RISK?

what do we communicate? CRL unavailability, no user aware, or? All of them! Messages should be differentiated for users: security teams; sites. Sites only care about CRL & CA web.

① Announcements of downtime at least a week before!

on a table (web) pages Wiki table! on PMD with RSS feed.

Recommendation: 1 wk

↳ as 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 etc.

Requirements:

- CA's enter their own notifications, authenticated.
- ~~email~~ email. (+ RSS as very nice) subscription.
- web-based list output.
- one category at least.
- expiring of old messages. (archiving).

Tech investigations by:

- Christos T
- Milan.
- David OC.

② REC Downtime announcement: preferably 7 days in advance. (and not too much earlier!)

NLCA profile. & distribution.

structure is not usually re-packaged locally.

build compilation packages with proper dependencies.

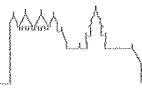
→ then provide checksum files for key data in the distribution?

downloads of tarballs requires admin to think.

RPM packages are also intended to be repackaged downstream.

! who uses the 'profiles separately'? now, everyone takes all AP's.

when real LOP comes in, we will face the issue now seen with the worthless training CA's like in the UK case.



HLCR / Sens :

a last discussed OGF 2d/2g, but since 2000.

* aim is to complete this today, and then have it approved by all PMA's, so that we can then build a test distribution.

§3.3 #3: single private key for "CA" or "Trust Anchor"? definition is == from definition. confusion on semantics in document text (e.g. on publishing by piece of data).
 both CA and HLCR or subject CA. Terminology is not work consistent yet.

① The organisational body should be defined in the glossary.

it is still unclear who is supposed to be responsible. Require "persistent and long term commitment" - like language?

[in the @Vack's case, @V also operated the issuing CA, so had to show up.]

② - name space must be provided, but actual writing is usually by IETF

CA MUST ensure that there is enough information to write the RPSPNC and signing policy files.

③ - is support for dynamic hierarchies ("implicit") really needed?

but this is not supported in middleware anyway!

↳ so clean up and take it out.

New version by OGF 30 with all changes, to be made by Sens.

- other PMA's should comment before start, send 1 week before OGF

- then EU and PMA shall own the profile.

- make document consistent.

~

Devlet. Auth2 NG.

putting requirements on the operation of other authority types. Live editing of the Niki.

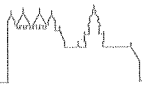
- This document does not actually defines accreditation, but use it for self-assessment (and maybe later to have NIKI's do the accreditation)

- The thing accredited would be an RPSP, hosting one or more AP's.

- extend scope to deal with any kind of assertion, but still limit to VORS?

- try to do without the VORS word, and see how far we get... incl. common SPAN authorities

< live editing onces >



09:30

* Eugene - Self-audit of RDIG. [Refer also to Jens' discussion yesterday]

Eugene presents all "hard" issues from the audit.

→ Slide 5: "degraded personnel"?

Slide 13: not deleting any logs...

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

How many operators: 2 persons.

all Revocations come in by phone, which is one of the reasons why CRT issuing works with so few people. Also, the personal union with security incident response means that revocations are handled early.

The PMA commends the fact that this can be done with so few people....

Roll-over plan circulate to PMA to resolve the "D".

Otherwise audit looks OK

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

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

Consequences for the Russian Federation and WLCG is severe.

If help from PMA or WLCG is needed, we can give that!

PMA thank Eugene for presenting and the thorough self-audit.

[Dave K to take notes]

David CC - Grid Ireland Self-audit - see presentation on-line

practices are advised better than document.

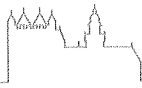
changes held off as a new CA was planned, but this has failed to materialise.

② Reviewers: Nemo and Jens. - additional doc is available.

NIST 800-63 and Remote Validation (Hine)

the primary requirement of LR require the RA to have read access to the agency / issuer databases!

! Actually: all students in a dorm will share IDs, since they share addresses and mailboxes! Email address is also enough.



[NIST] at L2 security is based on email, ~~endorsement~~ level of postal/email is highly variable in countries.

In existing IETF remote has notary publics, e.g. for classic.

new, a level NIST L2/L3 new profile? No (IETF) do not need to match NIST, ~~use~~ Just InCommon is using NIST.

CA's with NIST L2/L3 can go into ~~level~~ new bucket.

↳ would RPs pick only NICS, or always pick all anyway?

SICS already fits for a NIST L2!

~~Can~~ ELogon + InCommon may use Comodo as a back-end.

Historically InCommon was substantially different from NIST L2/L3.

The InCommon 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 NIST is not really the request. InCommon is moving to NIST, though.
InCommon: also email is enough.

Address InCommon: what about the audit trail? Is left to WHO, CA only records issuing WHO.

TCS retained F2F!

Is remote vetting really critical, does it add much to the business case.

limit it to only F2F? YES can do that, so why not in US?

NLCS: probably not interested in remote students, as mainly rely on staff and PhD students, and these would show up in-person anyway.

would RPs accept a new profile as they do NICS today? do that then would not be an effective difference.

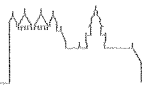
ask ELogon for the use cases where remote vetting is critical for RPs.

We want ELogon in, but based on F2F. So IdP's should differentiate like the TCS does, or CERN

Need to understand RP use case!

SICS would match Remote now

also: TCS level has effective high level that needs to be conserved.



Use the subject namespace to differentiate between remote and FZF, and only account the FZF namespace under MICS. & EP's would be better. (policy OIDs cannot be processed).

anyway, the audit records of Remote should already indicate in the JWP records whether it was in-person or Remote.

Reliance on national infra like postal system is incompatible and complex between countries. The notarized document of Brazil is at least accessible.

no Libbook.

- ask CI Logon for RP use cases for Remote.
- split in 2 CP's (not via namespace)
- new profile is also good solution, but differentiation is better, or RP's with MICS will lose out on FZF vetted people.

EUQ and PMIA may view it as equivalent, ~~given~~ given the national background.

and why is InCommon lower than NISV?!

conclusion: EUQ and PMIA NOT happy to include InCommon Remote as-is.

~ coffee ~

License and OS distribution.

Debian (Mattias) is requesting import.

fontco redistributes certs under Mozilla Public License 1.1

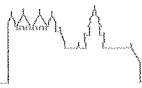
↳ has lots of us blah in it, as not obvious.

Meta-data CC-BY = OK.

trust anchors of those present: OK.

@V: OK.

- what about use of NISV IP in derived works, is misuse then illegal or immoral. 31.5 last sentence should prevent it
- we license only the trust anchors and metadata, NOT our document and the RP's!
- CC BY should be OK, no trouble from Canada accepted.
- we trust "our" EPs to be happy, and we don't need explicit statements.



Encourage downstream maintainers to make timely (security) updates.

Recommend: updates within an hour.

: naming of RP's on proper name, NOT IGF ~ ~

: web pages on groups may have IGF in name.

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

- how impact on trust for web shops, and everything else.

- do you trust the grid CA's for on-line banking?

may we restrict use of certs to application domain? Does that conflict with Debian Free Software Guidelines. - and we do limit use of our certs, e.g. no financial transactions. So for Debian we may end up in non-free.

but: requirements are on the subscribers and RPs, so limitation is not on the data itself.

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

Many, also commercial CAs, will restrict use, e.g. no life-support equipment or nuclear energy.

(ACT) ↳ ask Mattias for OK/statement.

PHA is quite happy with this process!

- also they may be put in the OS default locations, so that some (text-based) browsers etc + servers.

- OS distributors should figure out technical details.

- and ensure that the grid software will work!

(so link or install in /etc/grid-security).

§ Sens: update to PVP - related to XDG/PHA SCS/MCS update

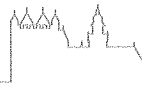
Changes in line 68 and 80 of Wiki are OK.

OLD: ... 1.1.5.2

✓ Approved these changes!

now reviewed.

§ 2.2 - 3g. disallows activated private keys, whereas rest is about de-activated keys



RICP doc. The intent of 2.2.3g was to allow SCS cents to be used exactly like our proxies today.

This doc is only about radical persons. The intent of the doc is thus ok, even though it may be unclear. The footnote explains it.

Jens will come up with a new draft that is clearer, and the PMD can see if it actually helps.

~ LUNCH ~ until 15:00 ~

SCS/MICS updates

version 2.2 SCS: changes agreed by EGP.

MICS? v1.2 last edited July 14th.

- suggest remove "In particular --- 17s" in sec. 3. since it's in the PKPonyway.

- reference to QFD 125 differs between MICS & SCS.

- In 4.4: revocation requirement seems lost. Is that intentional?

only It is correct, but "second part" about revocation in case ID is compromised is missing.

Request update.

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

for the RCS, having connectors have a BEDR plan is enough.

not needed for access/portal services.

EPS 5.1 is enough.

it is not needed for the IdM & IdPs.

with this understanding approved.

Fetch-JERL memo

support for 2.8: goal in OSG, EOL: early 2012 Q2 for 2.7: eol in 2011 Q2.

OSG: tested new distro 1.35⁺ and it works!! Yeah!

BEI: new format for ~~test~~ oct release!

HAAS: part of EUHedGrid II. Roberto gives review update.

Roberto sends review, no feedback yet.

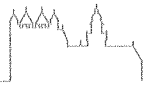
new reviews to use excel sheet: would be handy, but is not there for Classic. Would be nice to have that.

Outstanding critical issues: in current issue of CP/CRS.

- request coupling to identification is unclear ~~is~~.

- QA docs not have separate RA's.

- no working web site, no DC naming, but R=8y. Unexplained.



HHSI Review by Roberto.

- missing info should be discussed in PMA.

Re-accreditation still seems quite a long way away; but it's part of EUMedQnet workplan.

They would have liked to come. Try meet in NT, NL.

~ site visit to SRCE Data Centre ~ ~ ~

Jens: Soapbox on trust and science.

~ ~ ~ WEDNESDAY ~ ~ ~ Not

UKeSc OA new CP/CPS & Software (Jens)

went through a self audit last year. new CP/CPS not yet finished, but direction is new and it will be a complete re-write

new practices will change, just text changing and s/n.

re-write is to make it read better and maybe it shorter. And split CP & CPS.

No re-accreditation needed,

[Tone of presentation]

roll-over expected in fall of the ^{signing} ~~last~~ certificate.

UKeSc → TDG as advisory body.

Replaced software (no longer open CP), but database is compatible.

CertNisard Jens' GUI tool.

Testing possible? Eg for Reimer to test, but the server is not get outside firewall.

<https://svn.esc.rl.ac.uk/trac/cp/wiki/Authentication> for proto info via VPN.

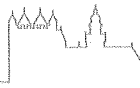
not get open - request info by mail :-)

Jens will send link.

DavidCC - Check Certs

Alan will has some elements to look at, no action yet.

Tech List is useful. - even if it is quiet.



Robot cuts and PKP:

DeC: can the entire robot keypair itself be in a dedicated MyProxy?
(so not a community one, but a dedicated one).

With the PKP guidelines, a MyProxy as a 'virtual HSM' is compliant and OK,
DFN is already using this

SRCE already done S/A → update table.

Next: 2.5 days in Utrecht.