



Remote: Savi, Lidija, Miroslav, Roberto, Vladimir, ~~Jan C.~~

Local: Anders, David G, Wino, Marc, Davek, Jan N, Christos K, Bob C, Feyza.
Cosmin, Jens, Bozidar, Emir

Notes: Christos K,

⑥ Voting.

⑦ Distribution format (apt+rpm, yum2). Single package.

* Anders / Welcome.

* TAG PMA / Davek. using Carpi slides
next TAG PMA at end of May 28-29.

AP / David G. -

Christos K / SEESRID. affected ESI catch-all will start serving Switzerland.
after the demise of SWITCH.

E-GI: ~ 100 users and hosts.

David G / Robots in TCS now.

* Cosmin / self-analyst status: not yet aggressive enough :-). See page.

- TCS: 8 - CERTN IT/IS: 8

- PKGrid: pending progress.

- BG ACAD: progressing

- Austrian Grid: no CP/CPS yet

- IRAN: no progress.

⑧
YCT

- MaGrid Review

- PLGrid: did robots get fixed?

- UK eSC: nothing.

- LIP: declare success!

- CALG: updated, just wait for a bit. (status 2015-05-11)

- phIRISgrid: declare success.

- NIF: assumed success.

Cosmin: more nagging is needed.

Belnut: move to TCS

11⁵⁰ Jens / UK esc. (see slides)

Service cents not needed, normally requested by 'mistake'.

JISC Assent. status

Davek: how much disruption expected around July 1st when a bunch of contract ends?
migration might cause issues - transient but emerging, e.g. for OSG.

Process / Next / final transition?

key is primary concern. - will use transitional CP.

target: done distr. introduction.

Dec/Jan: - discontinuum old work.

For SHA: use Sha-256

4096 RSA.

transitional CP just technical review.

CPs to the list of 2 lists of reviews.

SHA-2 timeline / Downig.

similar ok.

^{one} ~~before~~ uses sha-2 CRT yet, apart from VCS G3 + error in AP.

some intermediates are surely SHA-1.

test ~~done~~ and done.

14⁰⁰ Eric Yen / AP. status update.

14²⁰ Emix / SRCE S/A.

need new self-audit guidelines to align with Classic 4.4.

2048 bits in practice ok, but not yet in CP/CPs + SHA-256.

Reviewers: Feyza, Jan N.

14⁴⁰ Jens / QFD.225

- "Required" in colored box to be fixed.

- on CN in server certs: duplicate 'service/'; "contain" → "consist of"

- remove "." from 'x-example.com' =

(4.3.3 WTFP also new).

- CIA → ISSN.

- page #16 "find" formatting bug.

- Street Address & postal Code SHOULD NOT be used.

link to mailing list. Deadline. ~~undefined~~ → Jens to ask the QFD Editors



Sep. 2015 - Amsterdam.

May 2016 - Istanbul or Ankara.

later Jan 2016 - ? Danzig? ?

Jan 2016. → central Europe (Vienna, Bratislava).

16⁰⁰ RIS. SP + ST done w/ track changes

TUESDAY

09³⁰ Borizar / MARGIT CA. (see presentation)

→ SHIA-2: 256 or 384 8

* availability of subscribers → should be recorded. in serial + signature.

* old CRL's must not be on-line.

Recommended SHIA-256 given NISS discussion.

REVIEWERS: Emir, David G.

need CR v 1.1 online

10¹⁵ Jens / HLCA

packaging issues → dynamic, more complex due to generation signing-policy.

namespaces distinct

no HLCA meta-package yet.

ready for review.

- shadow cr file + "enabled" / "available" debien like packaging

- signing policy engine needs dynamic generation.

- monitoring? more complex.

Ⓛ because of sorted "just" installing additional policies like 1079 or EXP.

policy meta-packages w/ scripting post-installation.

11⁴⁵ BobC / NIST LOA.

factorizing components main thrust of new NIST process?

fear of it being overly complex and thus may be unused.

EIDAS awareness levels: 3 levels, but e.g. hardware token specifies up to the member states.

communication on LOA as important as LOA itself.

↳ LOA gets stamped at

trust marks "SicTFEi" ← ID assurance/authenticator.

then PEP as attribs

useful debug messages for end-users: "why was I denied access?"

'leave' the country.

PHH 3

(6)

gets too complex for awhile - RP's unclear. - depends also on 'sensitivity of access'.

STORL: 4 levels in deliverable.

- organisational factor / quality of IP, of issuer.
 - technical / security features of issuer, et al
- combined in level 1-4, where 'substantial' assurance seems ill-useable.
(only "government" involved distinguishes it).

Christos: linking education and STORL in a project ongoing.

no policy agreement, but technical communication progressing on attrib. Xchge.

SPML MD trust marks - Entity categories for issuer.

- per assertion LOA can be same or lower than the trust in the issuer.

for IGTF: our RP's will need LOA on end-to-end assurance, so also

consider processes in other authorities / community enrolment / etc.

The LOA levels now: consolidate levels (A, B, C) and (D).

maybe Eppon, Birch, CEDon, like EUDAT did.

⁴⁵
12: cons / VM certs

relocation after VM deinitializes? or periodic renewal.

DNS FQDN ownership challenge / DCV.

Because of long CRLs → use shorter life time of the cert.

+ automated renewal from within the VM.

⁴⁰
RAT + CRL

include an expired CRL in the distro? to auto-disable a CIA even on fresh installation.

- install requires fetch-crl.

(AET) - a dedicated pkg of expired CRL's for use by RP's. optional package.
w/ files as "config(=)" to not override.

RAT = CC

what about recurrent failures? → discuss, not automatic.

communications is most important thing anyway.

(S) 30 days, also if distro is ~ 30 days.

distro release on a case-by-case basis up per urgency, RP's opinion.



RAT/Docing.

for nonEU, involve chairs
also build needs list of persons updated.

Q's: simple like SHB-2 if there's also the option to just react and deliver
the answer.

#2 certainly too complex.
separate RPT CC from Q's.

LOA -> do RPs care about differences SICS/MICS/Classic?

compensatory control.

RPs might want specific life times if they cannot handle reconnection.

"ASPEN, BIRCH, CEDAR" are close to equivalent

use LOA marks in conjunction.

new doc -> netting section

done for (BIRCH, CEDAR) and (ASPEN).

in §5 added the req to ASPEN/BIRCH -> this increases to MICS/SICS.
min. req.

audit §2 del 1 -> §3.2

Done. Now towards a single 'PRX' profile for IOTA, SICS, MICS, Classic.

16⁴⁵ Jens' Soapbox on cast.

Wed. 13

09³⁰ PARC. / Douvry -> Deepnes

10¹⁵ non-rob + tech RPT "

11¹⁵ tea

11⁴⁵ Round table: disc. on Near shot.

Tech draft: - Yarn 2 eol ole.
- apt-rpm. eol ole.

nic RTable.

⊕ RRLs SHB-2 at least for long lived off-line CR Books.

- big push by govt to federations to boost employment for young people - to get things working
- our terminology and work is still too complex for normal use ---

PHASE

(6)