

Present

Notes: Jan Jona; Jens; Javi

①

(Emir
Dassan
Jan N.)

David.

Alessandro

Majid.

Jan Jona

Bernt.

Dave.

Christos K. / SEEGrid will live for Georgia & Albania;

Bosnia coming up.

Pavel. new EA standing for all sciences.

Willy

Anders. (12+2+10 involved); SLCS (-)

Anders (from NQGF).

Dave K.

Roberto C (10)

* Prilkipovich. (HREN)

Lidija (HREN).

Usman.

Alice.

Jim B.

Niño

Szabolcs → Nechnology presentation. ^{KP&S} ^{RPM&S}

Cosmin.

Sergen

Reimer.

Dika

Yoshio

Ursula

Milan

Jens

Javi

+ Valentin Pocat ; Luka, Lidija

APCGrid PMA.

new members: CDAC, India

refreshed: Univ of Hong Kong.

UHG PMA.

New issues: - CRL's for SLCS.

- FIPS 140: level 2

next meeting July in Venezuela

2nd wk. November in Argentina.

BE, D&E

ArmeSto

Hallas

DutchGrid.

CyGrid

Slovak.

IUC

19³⁰

Rest. Romagna

Nöfvebraga de 51

15¹⁵

John Renner
Hansen

LatGrid / SIGMA net (Dane). - Jens + Harci

- * 120 valid certs today in Baltic Grid in Latvia.
- * will migrate to 3697 format. → but not now!

comments from dane: - CRL lifetime.

- Proof of possession? dealt with by having requester print out the request.

RIA should then look at the logs?
no describe this in CPKPS.

process: update CD/CPS

Jens to catch +

2 weeks

acceleration

OK. after that.

Willy: would be change procedures to have user generate keys in the web browser. using Bouncy Castle. with Java 1.6+ (as that one can set access rights on Unix Is that OK?

DIFFN uses that already. - it's OK.

Mike → Randomness is general problem, partially addressed by FIPS.

Code. will be available. when ready. (Jens also).

Valentin P (TID). → Cosmin + Christos K.

no- OI/IANA. only last week.

→ C= naming? Why not DC? S → in CIA cert there should not be an OI for the policy. will change to DC.

- using Brazilian Notary protocol :-).

- TREN? ⇒ NREN.

no- solve all of TID? S.

- where is private key? safe? S: in cage inside controlled room, 3-persons have access

Lidya (TREN). → Christos K.

C= naming. → DC naming I.

DN-ordering. S.

→ proc like LatGrid S.

Lunch

14⁰⁰ Milan.

Andrius: IACC comprehensive response to Jens OK? Not meeting in req or CRL's. Since by May 30th? needs larger. Jens to follow up.

G Grid - Christoffel.

Slovak -> David G.

Hellas Grid -> done, new version w/ Robots in the making.

BE Grid -> verdu proc completed.

John Dennis H.

- delay response
 - concerns response.
 - response time.
 - risk analysis.
 - OCAP. (Robets)
 - suspension.
 - ROBAB / holidays.

-> dec. committee/rota.
 -> need challenges.
 -> dedicated list for request.
 -> response by CP more important than actual reaction.
 -> IETF-wide response needed.

VONS new type of cert.
 -> ticket proc ~ 1/3 people

- communicate very early to RP's (for public vulnerabilities)
 - > initially on web site.
 - > announce list. + URL for info
- assessment and agreed time line. inside PMA.
 - > ded. mailing list.
 - > to "mail" in .info file tag with label in subject.
 - and define expected response with time line.
 - signed emails, not encrypted.
- ACK. next business day. for CA's

-> involve RP Risk Assessment teams. (CA's all have access to NREN CERTs that are globally coordinated.)
 -> incident team mailing list

-> CA's must update email in .info file. (not personal)
 -> CA can ask for extension by asking risk assessment team.

① on expiry of decline for response start suspension process:

- call ca on designated phone number! or fax. (private to pma)
 - > non-response starts suspension: small team to decide, mail out decision and ask for response < 24 hrs.
 - > includes announcement to ietf-general as always. (interruptable).
 - > push out after ~ 6 hrs at any day.
 - > CC TACAR removes IETF flag.

⊕ restoration also within a day!

RPT	Jim	Coret.
	Jens.	David.
	Nilly	dg.
	dg.	Ursula.
	Josho.	Jan.
		ROBAB procedure
		Andrew.

list on eys.dyn.org

SAM
SAM-on-demand.
(CAMP/CHUB)

2nd. should data output
with comm.

Panel: RPT
0427 53BF 4790 A659 EA 01 A729 C5F4 16D8 D8F742E8

Jens: "project naming" in Robots.

"policy components" (Jens).

"protection"

other are for by jurisdiction.

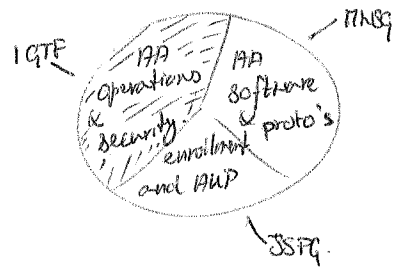
- NSF
- classic
- trusted org (DB / Sub). "go between the IdP"
- not public.

in 3.2.3.
ref in 3.3.1 / 3.3.2.

PCT fix up section distr.
for 1SCP's. (2/3 left).

f2f → also govt only papers? not yet

Auth2



Auth2 web site → mandate
presentations
doc. drafts
membership.

"one" AA authority per NQI
more already that way.
↳ relevant for EQI-DS.

What kind of cuts
where in VOTS &
VOTS Admin

not same host cut
everywhere

→ [present to EQEE/SP]

SLCS.

Oil. → SWITCH to get Coak w/ time line.
→ record who activated the signing key (as compensation for lowering to level 2).
+ reason...

2nd auth. component (FICS). will stay.
email box ownership check also ok.
(send mail w/ one-time web link)

REKI

- exceptional cases
- document
- sign off

} useful to describe existence of this as a process in CP/CPS.

IRAN

ordering? Open CA

Self/Prolets

Sep'08

- Ursula German Grid
- Roberto INFU.
- (Revised) →
- Slovak Grid.
- Baltic Grid.

- CatchAll CA's → Jan'08
- CNRS
- SEE
- DOE LCG-RA.
- PK-Grid (already done).
- NIF

Large session on catch-alls.

Jens'

3.1.1 de naming example.

operational security is a "red" bit that a CA should fully fill in.