

9³⁰

Note takers: David OC, Christos K.

Muno, Serge, Reimer, David OC, Natal, Dolores, Jimmy, Alessandro,
Yury, Jens, Milan, Roberto C, Daniel Ganeira, Kasper, Harri,
Christos T, Christos K, Jeroen B, Doull, James, Alice.

Dionys

LISQC: 20-24 Apr 2009]

Sim's TAGMIA:

QFD 25 →

check before acc.

Jens: what about the not-yet accredited RAs?

what's their time scale? some members are very slow.

Sim: RAT:

Milan: what's the address from RAT? Sim: you also have to react to
suggestions, and these don't have a fixed address

Sim: add log to the subject line

Jens: send challenge to individuals only, not 197-general.

Doull: should also be private.

Reimer/Milan: "please reply" → SPAM. Bcc → SPAM.

Sim: signed message? this one was signed...

③ Frequency: 6 mo; better: twice per year.

Control info? not a core risk task, but very useful.

Christos: keep RAT focussed, don't also try to solve everything

+ Doull: assess global risk/risk analysis.

④ CONTACT INFO.

Milan: who has access to private contacts?

Jens: escalation path; only to very specific individuals

CP/CS should be primary? this resp. for that...

emerging control path for all CAs shared with RAT

every CA free to define "escalation process"

collect within 1 mo.

send around email? encryption required.

RAT to describe process also collect info. Jim → ... email how ...



* RPT: Home page to state public cert & RPT keys of all members.

(ACT)

PMA chair to request the escalation path from the CA's

private for PMA chairs and RPT

each CA can put in "special instructions"

////// COFFEE //////////

- CALG: Jens + Hardi; Jens: problems not get fix. Updated again Friday.

next: review that.

Hardi: deadline for them was July 2008.

Jens: there is progress.

A: probably complete by email.

- MID: Christos doc looks fine, but web site inaccessible so no operational review.

and download uncertain and impossible to test.

A: over email is likely OK.

- ZA: Jens in contact based on template should not delay the process.

- Senegal: reviewers: (pending) Jens tentatively.

Roberto: INFN internal audit.

4 robot certs (last month).

→ RFC 3647: ignore, as all do

→ #15/#16: key changeover? Milan: user can see the impact.

→ CRL v2: not critical but will change (but no deason certs)

*! single network entity / FQDN.

cf. etohn → renewal: VPN cisco boxes affected. now corrected.

*! → RA audits over 200 people, virtually impossible. cf. ukesc.

added check a few years ago for authorization by RA

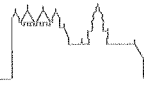
on travel speed to verify F2F meeting. Users travelling

over 1000 miles/hr found → revoked :-).

* → authorized orgs admin: checking is ill defined.

location independent URL (no "afi.")

* → PMA for INFN is now only Roberto C.



CP15 @ rest

R. P. Perlas de S.A. #50

Alessandro U: slide 6/7 re us out in consistency.

* how flexible is profile? (for robots, more CIDs) → no problem

ACT: web

* Reviewers: Reimer, Jens.

CRL: Milan: yes

Reimer: caveat: holiday period. may affect system downtime?

Milan: IP is not a requirement. If CA can guarantee 24/7, why not a 3-day CRL? should be OK.

CERN's 2 days is not seen causing actual problems.

Jim: the problem ends up at the RP, as the user's job start failing.

Jim: re-issue 3 days before next update. acceptable.

web cachability

Classic AP update (4.2)

4.2 approved

Milan: Geant3. start Q3 2009.

in Milan's words: "no proposal exists are expected to be used"

"some kind of policy is needed", for which you need a PMA.

People: Milano - stack leader, (SAB leader from DISC)

but proposal purpose: "more accessible to end-users"

subject AltName URI cannot directly be a urn → not def. in standard.

that's why there's the "resolver" URL instead.

participants to SAB. V1 is CESNET & DFN (DFN to run catch-all)

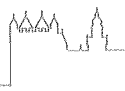
expect managers from NREN CAs to participate in QN3-PMA.

catch-all: numbers: ~20-40 per country.

SURF/Fede/* CA: how to care for Robots?!

when using SES* for hosts....

} outsource entire link to federation to say, Phowels? Joint with SURF



Yury/Belarusstan CA: CP/CPS minor version / OID change pending.

Serial number: latest guidance is to make it long and unique
only less software that had problems with long integers (over
20 octets) had OCSPD writing to syslog.

version uses an obfuscation hash for SN to make the number of issued certs.

[add Classic AP OID (anc) to policyIdentifiers]

CA cert on web site still needs to be replaced.

→ citizens vs residents? → residents.

(VACT) send new version, two week review final (DQ+SS), → accreditation ok.

2K. key length? 1024 bits keys are usable only until 2010
↳ change to 2048 bit now

* increase min in Classic AP to 2048 bit.?

* drop 1024 3-year for renewal on HW/token.?

impact on performance, given that CA's are already 2048 & proxied S/R.
verification takes 4x longer (1ms/fin total)?

that about 1536.?

Needs checking for Jens' storage systems.

rotation is always possible. This is not the bigger risk!

Still ask other PTIA's.

RAT can assess if it happens.

Symms. Yury, Alice
↓ new ↓ next time.

Jens: use of cuts in real-life medical situations.

does this need certificates with a "Special Status" (life critical, VOMS, etc)

Milan: CA does not 'know' about usage.

Christo: cuts are equal?!

Dowell: auth2 / VOMS cuts are not equal.

Christo: "package" to users.



AA profile discussion

Christos: title is too generic for content

Dimitry: Scope "Grid VO" or "VO" or "community"?

x

Alessandro: VPSH support for VONS.

Dimitry: scaling will require distr. (natl) accreditation.

Christos: it should be about the infrastructure to run on.

DI: do we need to define "long term commitment" as a requirement.

CA/SS: "a single logical AA service per VO"

on database consistency: Cons: should be done securely.

"Attribute" definition → long discussion on semantics, but in the end revisit of scope.

life time? given that ~~the~~ assertion cannot be revoked...

generally, it ought to have depended on the actual attribute assertion...

24hrs?

DI: defining this is actually a VO policy, not a policy on running/operating the actual trust infrastructure.

LLUNCH1

Op req (sec 4).

* min key length 2048

not sure if the actual VO's domain (port 15xxx) must be a host name.

* advantageous to have assertion signed by a special cert.

this cert is issued by an authority (to allow revocation), once a service is accredited.

* policy OID for special "aa" cert. Issued based on (statement of) accreditation.

- separate key pair for each VO (separate certificates for same key is
↳ or certificate be different || something you cannot prevent)

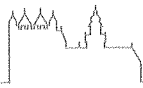
↳ or even one cert with all VO names (good idea? -).

currently all VO's instances can see everything (all run in same account).

a Vincenzo willing to change according to a (sensible:-) policy we draft.

- Checking if the service manager is actually authorized by the VO manager to request a cert (so: stronger than current host certs!). Should then be strongly documented.

CK: imposing this on the VO's might be too heavy..



Trust repository: - how to recognize the "proper" VO? What is even the "proper" VO?
(following discussion)

tendency now for a keypair per server, since there are problems in?
assigning responsibility and on getting into VO management.

assumed level for host/service certs is too low for some CA's.

clw: general statement from CA should focus on strengths/level; not application.

Hille's issue: get signature on a fake AAA cert by making it the challenge
in the SSL handshake.



Therefore, AAA signing cert must be different from any cert
used for SSL/TLS.

Jens: AAA signing cert should not have TLS Server Auth set.

"VOMS profile"?

DK: cert per host may be first stage, at least a different one for SSL and AAA.

light-weight proxies must remain possible, current low-security host cert
should remain possible.

SS: "VOMS profile" looks like a Robot

clw: not "VOMS", but just a higher level, like "gold".

clw/SS: define levels of assurance for hosts

DK: can we work with Vincenzo to actually try it? Progress should be made.

MS: LOPA is the distinguishing characteristic, rest is between VO & infra.

maybe as ISCP.

or is listing in a trust repository the definitive decision (not a cert per-se).

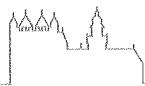
DK: Try before January, on Christelle:...

14⁴⁵

Jens: CP/CPS generation by DocBook.

next steps: {
- contribute text (all)
- Jens: style sheet. (using xslt)
- editor for new CA managers.

with blessed text by next OGF.



CU: AuthN service profile → new version of GFD

management of AP's: defined in a profile, need a dedicated section?

DK: why "Authentication" SP? Is also useful for AP.

but see §3 now has "identity".

for (AAI) federations in general, do these items make sense?

Milan: many federations don't care and see policy as an obstacle.

Reimer: the SWATCH AAI is very formal and correct / CU: good fed. as well
but DEN-AAI will be loose as well, since not managed by DEN-PCA.

federation is an appendix to networking contract.

Milan: in CESNET, federation is just the central service, and does not concern itself

with the IdP's. So, any SP with requirements needs specific agreements with each and every IdP. CU: so interpretation is 'impossible'.

Sens: its similar in the UK, there are hardly any requirements.

CU: directed not to individual IdP's, but to a collective.

Reimer: title suggests something very different from content (expect "skibbles" as an AuthN service. Title conveys wrong impression

CU: change title & look for feedback based on "AP profile" now being drafted.

Reimer: would a GridShib (or v.v.)^{AP} make sense? Dim: all things still needs cuts.
i.e. define this on top of a pure Shib implementation.

Dim: it should be a SPARC (not Shib) profile Milan: SAME itself is not unique.

Milan: then these "AP" requirements will be largely on IdP's not on the federation.

Alessandro: main elements such as name uniqueness are generic.

Milan: is it on the IdP or on the service? No SS: this is the requirements or how to write a requirements document :-)

Reimer: wording is confusing. Should be like "—"

the explanatory text suggests a description, whereas the e.g. "Classic AP" writes again requirements there.

Next Steps: - who is going to review and finalize it

OK: compared with current profiles. Those miss liability and finance section.

- impact of DK's AA effort to get a generic template.

→ - title should say "TEMPLATE" (or "framework", like in RFC3647)

- comments are directed to person who is writing the profile.

→★ Christos to revamp and circulate new version. Nov 6th

LPD&CP → Sens to add examples, then HQ last call, Sens: before Nov 6th.

Audit doc & Roberto's questions.

- "Audit of CA staff" unclear what is meant.

"Requestor ownership of FQDN" : is virtually impossible to do with many RD's.

as a CA, it is impossible to define the procedure in the CPKAS.

CK: check this when you audit the RD's? RC: as not feasible with >100 RD's.

Milan: value is in the fact that the RD's feel that they may be audited.

CK: random checks of a few ok? RC: document makes explicit requirements, instead of giving guidance.

RC: doc actually says nothing more than the minimum requirements.

so: - either make it more informative or it just does not add anything.

DG: at some point, Yoshio would provide actual guidance, examples, and reference for rating discrepancies.

RC: questions range from banal to extremely complicated. What is the relative gravity of the respective answers.

Auditor should get guidance on gravity of issues.

CK: ask questions, and not imply the answer.

best auditors should assign severity.

CK: this group should define severity? RC: the doc. should give some guidance here to ensure consistency. The original work by Brian went a long way in doing the proper thing.

DG: we need to be specific on rating levels. We need the guidelines for the individual items. Simple for technical items and more complicated, it's a combination of the importance of the item and the 'amount' of violation.

RC: commercial audit guidelines are far more thorough.

CK: it's not too easy to identify "important" vs "lighter" items in the min. req.

BS: in the end it's humans making a judgement.

CK: ask Yoshio as to how to "rate" each item?

action: - questions should not propose the answer

- it is up to a PMA/reviewer to decide if the answer is sufficient.

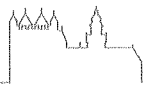
- get back to Yoshio?

DG: it is useful as it is. Value is in section 2. and the table is just an example.

MS: don't expect doc to assign severity, but if you miss an entire feature, then

CK: rephrase where needed, and collect some experience first before assigning severity in a future version.

DG/CK edit the suggestive answers first, then send the editor.



→ Next meetings Berlin? Mo-Wed Sept 14-16
Legesorg 15 Sep 21-25 in BCN.

[8¹⁵ @ restaurant]

[2008-10-08]

Jens. - robots

- cert mngt s/n

iq: - web cacheability.

Cyprus

Milen: demo of OID checking in recent openssl. Code is simple.

Sim: - the policy oid must appear in all certs in the chain? No: one is enough.

matching logic in OpenSSL is $\&OR\&$.

proposed: start issuing profile OIDs in Everyone!

ACT

oid must be opaque.

no-one sees issues with adding policy OIDs

updated Classic IAP. TAG to do this for SLCs / NICS.

Robots 1SCP: "client but not human"

orthogonal to vetting or privacy protection.

Host cert 1SCP: ?

Robot: - profile must not have server extension. Secy

- individual person is responsible.

- say what they are, not what they do.

Max

agreed on OIDs

ACT

ACT Agreed to add these OIDs to robot certs.

→ send message to cci's

Dave: robot request are becoming more acute. Preferably on H/N token.

Chris: may have problem with h/n tokens. Dave: security people want H/N.

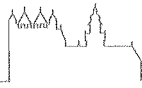
iq: having robots without h/n will actually lower se level, as current b/p is H/N only

iq: HN are easiest policy-wise.

maybe catch-all robot CA needed.

Send important info to CA's

separate guideline recommending that CA's stand on robot certs.



Christos' presentation:

See: <https://access.hellasgrid.gr/>

needs for long-term hy by user: 3x = revocation, relaying, VO/MS registration.
 since there are in SEE very (11 mo) long lived proxies there, why not
 store the original ^{prox} hy pair there? (and kill the long-term hy pair)
 Necessitates a policy on secret credential store. - and could do
 that for robots as well?

Positive feedback on presentation with regards to managing the private keys
 Alessandro interested. Dawell: even the CIA can run this.

[Signing party]

Implication of long lived proxies (without revocation). Christos: solve
 by revoking the higher level user certificate. Milan: this is currently
 not a cause for revocation. JB: do the RP accept proxies that live that long.
 RG: Site AA requirements doc states that non-revocable credentials should
 live longer than 1 Ms. But no associated policy.

CK: long-term proxies are (11 mo) already there.

revocation of long proxies is anyway a problem. P compromise of a HyProxy leaves
 everyone in a quandary.

Reimer: why not accept this as a reason for revocation of the original cert.

CK: 4 options (i) revoke cert (ii) VO's remove cred from VO (iii) should
 be way of banning proxies, or (iv) (ban user until proxy expires?) user
 should be limited by policy - that is not enforceable.

JB: different (4) players { user, VO, CA, ^{RP} ~~certificate~~ }?

Milan: CA cannot rely on third parties. *: banning proxies will not work.

Reimer: CA can always discretionarily revoke a certificate. CP/CPS could
 even state that. >> Jens: how do you prove a proxy is compromised.

So: once anyone sends long-lived credential to CA it's proof.

So user using a credential store ~~triggers~~ repository admin not to trigger such
 a revocation: (....)

Jorge: banning remains scoped to infrastructure, so rest of the world will remain
 at risk.

CK: it's a long-term issue - and for the time being the CA cannot cope in all cases.

Need to look at capacity of all parties in this configuration.

Reimer: when changing CP/CPS will insert something in to cope with this
add likewise to mis. req. For RP recommend banning? Today,
stopping can be done by revoking a non-compromised cert

~D Cl: good step forward: profile on how to run a trusted store.

Milan: in the end only the RP can do banning. Not 'own' problems (Sens: K&K)

Cl: for those with W's and MyProxies: see how long the proxies are →
~D: might be useful for a VCS like idea again (Thanks Bob!) to store keypair
for long-lived cert.

Milan: SCS? → is different as it has keypair with the user.

MSM? → centralized key mgmt.

Cl: incremental improvement, as it should remain feasible.

Cl: write down risk

① present solutions

③ - Circulate to RPs.

→ NQ: Cl, DoC, RKM (in context of SCS store)

CFD 125 requirement check

* can never check if it matches CP/CPS profile section.

DoC has a list.

- key length.

CA/EE: check keypair against (Dobson) blacklist. [CA]

* - exponent check (≠ 3, 5, 7, 11, large enough and prime).

- life time of EE cert

CRL: - 'expired' HTTP headers.

DoC has some of this in Scheme, other elements Ruby by Cl.

< perl >

DoC may stand, but can be pre-empted by anyone standing first.

Language: perl.

Jens: template CP/CPS: if you encode cert profile in X.509 as well the automated tool can parse to automatically check the actual certs.

dinner: 8 people.