4:30 Note takers. David CC, Christos K.

Nuno, Jorge, Reimer, David CC, Natnil, Dolors, Jimmy, Alessandro, Yury, Jens, Milan, RobertoC, Daniel Gomez, Kaspar, Hardi, ChristosT, ChristosK, JimB, DaveK, James, Alice.

Jimmy. [ISGC 20-24 Apr 2009]

Jim's TAGPMA:

GFD 125 → check before acc.

Jens: what about the not-yet accredited CAs.
what's their time scale? some members are very slow.

Jim: RAT:

Milan: whitelist address from RAT? Jim: you also have to react to revocations, and these don't have a fixed address
Jim: add tag to the subject line
Jens: send challenge to individuals only, not off-general.
DaveK: should also be private.
Reimer/Milan: "please reply" → SPAM. Bcc → SPAM.
Jim: signed message? this one was signed...

⑤ Frequency: 6 mo; Scotts: twice per year.

Contact info? not a core risk task, but very useful.
Christos: keep RAT focussed, don't also try to solve everything.
*DaveK: assess global risk/risk analysis.

*CONTACT INFO.

Milan: who has access to private contacts?
Jens: escalation path.; only to very specific individuals
CP/CPS should be primary? resp. for that....
emerging contact path for all CA's shared with RAT
every CA free to define "escalation process"
collect with 1 mo.
send around email? encryption required.
RAT to describe process to collect info. Jim → secure email how Jens

* RAT: home page to store public certs & PGP keys of all members.

(ACT) PMA chair to request the escalation path from the CA's

private for PMA chairs and RAT
each CA can put in "special instructions"

//// COFFEE ////

- CALG: Sens + Hardi; Sens: problems not get fix. Updated again Friday.
next: review that.
Hardi: deadline for them was July 2008.
Sens: there is progress.
A: probably complete by email.
- MD: Christos doc looks fine, but web site inaccessible so no operational review.
crl download uncertain and impossible to test.
A: over email is likely ok.
- ZA: Sens in contact based on template. should not delay the process.
- Senegal: reviewers: (pending) Sens tentatively.

Roberto: INFN internal audit.
4 robot certs (last month).
→ RFC 3647: ignore, as all do
→ #15/#16: key changeover? Milan: user cannot see the impact.
→ CRL v2: not critical but will change (but no reason code)

* single network entity / FQDN.
cf. eToken → 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 :-).
* → authorised sys admin: checking is ill defined.
location independent URL (no ".it.")
** → PMA for INFN is now only Roberto C.

Alessandro U: slide 6/7 DE vs OU in consistency.
* how flexible is profile? (for robots, more OIDs) → no problem
(ACT: Heb) * Reviewers: Reimer, Sans.

CRL: Milan: yes
Reimer: caveat: holiday period. may affect system downtime?
Milan: if 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 nextUpdate. acceptable.

Classic AP update (4.2)
4.2 approved.

Milan: Geant3. start Q3 2009.
in Milan's words: "no personal certs are expected to be used"
"some kind of policy is needed", for which you need a PMA.
People: Milan - task leader, (SA3 leader from DISC)
but proposal purpose: "more accessible to end-users"

subjectAltName URI cannot directly be a urn → not def. in standard.
that's why there's the "resolver" URL instead.

participants to SA3. T1 is CESNET & DFN (DFN to run catch-all)
expect managers from NREN CAs to participate in GN3-PDP.

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

SURF/Feide/* CA: how to care for Robots?!
when using SCS* for hosts...

} absence entire link to federation to, say, the world? Joint with Switch

R. Perlos de S.A. #58

(15' @ rest)

web cachability

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

Serial number: loosest guidance is to make it long and unique only been software that had problems with long integers (over 20 octets) was OCSP not writing to syslog.

Verisign uses an obfuscation hash for S/N to make the number of issued certs.

[add Classic AP OID (arc) to policyIdentifiers]

CP and on web site still needs to be replaced.

→ Citizen's vs residents? → residents.

(RACT). send new version, two week review final (DG + 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-years for renewal on HW/token.?

impact on performance. Given that CA's are already 2048 & proxies 512.

verification token 4x longer (1ms/in total)?

what about 1536?

Needs checking for Dens' storage systems.

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

Still ask other PMA's.

RAT can assess if it happens.

Signing. Yury, Alice

↓ ↓

new next time.

Dens: use of certs in real-life medical situations.

does this need certificates with a "special status" (life critical, loans, etc)

Milan: CA does not 'know' about usage.

Christos: certs are equal ?!

David: authZ / VOMS certs are not equal.

Christos: "package" to users.

AA profile discussion

Christos: title is too generic for content

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

Alessandro: VASH support for VOMS. DavidL: scaling will require distr. (not L) accreditation.

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

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

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

on database consistency: Sens: should be done securely.

"Attribute" definition → long discussion on semantics. Out in the end risk out of scope.

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

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

24hrs?

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

[LUNCH]

Op req (sec 4).

+ min key length 2048

not sure if the actual VOMS common (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 (bad idea :-).

currently all VOMS instances can see everything (all run in same account).

+ 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.
CIL: General statement from CA should focus on strengths/level; not application.

Mike's issue: get signature on a fake AA cert by making it the challenge in the SSL handshake.
Therefor, AA signing cert must be different from any cert used for SSL/TLS.

Jens: AA 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 AA.
light-weight process must remain possible, current low-security host cert should remain possible.

JJ: "VOMS profile" looks like a Robot
CIL: not "VOMS", but just a higher level, like "gold".
CE/JJ: define levels of assurance for hosts

- DK: can we work with Vincenzo to actually try it? Progress should be made.
MS: LoA 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 Christos U: ...

14:45
Jens: CP/CPS generation by DocBook.
next steps:
- contribute text (all)
- Jens: style sheets (using xslt)
- editor for new CA managers.

with blessed text by next OGF.

CH: 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 AA.

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 SWITCH AAI is very formal and correct / CH: guest fed. as well

but DFN-AAI will be loose as well, since not managed by DFN-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. CH: so interoperation is impossible!

Sens: it's similar in the UK, there are hardly any requirements.

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

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

CH: change title & look for feedback based on "AP profile" now being developed.

Reimer: would a GridShib (or v.v.) AP make sense? Sim: all things still needs certs.

ie. define this on top of a pure Shib implementation.

Sim: it should be a SAML (not Shib) profile Milan: SAML 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: 88: this is the requirements on how to write a requirements document :-)

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

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

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

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

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

- 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

IGTF CP → Sens to add examples, then WG 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 RA's.
as a CA, it is impossible to define the procedure in the CP/CPS.
CK: check this when you audit the RA's? RC: as not feasible with >100 RA's.
Milan: value is in the fact that the RA's feel that they may be audited.
CK: random checks of a few ou? 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 wanted 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 consistencies. 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" as "lighter" items in the min. req.
SS: 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?
DK: it is useful as it is. Value is in section 2. and the table is your 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 doc editor.

→ Next meetings Berlin? Mo-Wed Sept 14-16
(eGrid is Sep 21-25 in BCN).

[8:15 @ restaurant]

⟸ [2008-10-08]

Jens. - robots
- cert mngt s/w
} Cyprus

DG: - web cacheability.

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

Jim: - the policy OID must appear in all certs in the chain? No: one is enough.
matching logic in OpenSSL is « OR ».

proposal: start issuing profile OIDs in Everyone! (ACT)

old must be opaque.

no-one sees issues with adding policy OIDs

updated Classic AP. TAG to do this for SLCS / NICS.

Robots ISCP: "client but not human"

orthogonal to vetting or private key protection.

Host cert ISCP: ?"

Robot: - profile must not have server extension. Key
- individual person is responsible.
- say what they are, not what they do.
} agreed on OIDs (ACT)

Klaus

(ACT) Agreed to add these OIDs to robot certs. → send message to cas

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

Christos: may have problem with h/w tokens. Dave M: security people want H/W.

DG: having robots without h/w will actually lower security level, as current h/w is Myproxy

DG: HW 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 key by user: 3x - revocation, rekeying, VOMS registration.
since there are in SEE very (11 mo) long lived proxies there, why not store the original proxy keypair there? (and kill the longterm keypair)
Necessitates a policy on secured credential store. - and could do that for robots as well?

Positive feedback on presentation with regards to managing the private key
Alessandro interested. Darrell: even the CP can say 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. JS: do the RP accept proxies that live that long.
DG: Site AA requirements doc states that non-revocable credentials should live longer than 1 Ms. But no associated policy.
CK: longterm proxies are (11 mo) already there.
revocation of long proxies is anyway a problem. If compromise of a MyProxy 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.
JS: different (4) players of user, VO, CA, ~~credstore~~ RP?
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 is proof.
So user using a credential store knows 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 min. req. For RP recommend banning? Today,
stopping can be done by revoking a non-compromised cert

~D Ck: good step forward: profile can help to run a trusted store.

Milan: in the end only the RP can do banning. Not 'our' problem (Sens: Ack)

Ck: for those with UI's and MyProxies: see how long the proxies are →

↳ DG: might be useful for a VCS like idea again (thanks Bob!) to store keypair for long-lived cert.

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

MSM? → centralized key mngt.

Ck: incremental improvement, as it should remain feasible.

Ck: ① write down risk
② present solutions
③ circulate to RPs.
→ WG: Ck, DoC, RKM (in context of SLCS store)

GFD 125 requirement check

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

DoC has a list.

- key length.

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

- exponent check (≠ 3, 5, 2, 1, large enough and prime).

- life time of EE cert

CRL: - 'expires' HTTP headers.

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

<perl>

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

Language: perl.

Jens: template CPCPS: if you encode cert profile in XML as well the automated tool can parse to automatically check the actual certs.

dinner: 8 people.