Participants 26th EUGridPMA meeting

Meeting Information | Registration

	Name	Affiliation	Membership
1	David Groep	Nikhef	DutchGrid and EGI
2	Valentin Pocotilenco	RENAM	MD-Grid CA
3	GUEZOU Jean-François	RENATER	GRID2-FR
4	Armenuhi Abramyan	Armenian e-Science Foundation (ArmeSFo)	ArmeSFo CA
5	Narine Manukyan	Armenian e-Science Foundation (ArmeSFo)	ArmeSFo CA
6	Adeel-ur-Rehman Zafar	National Centre for Physics, Islamabad, Pakistan.	PK-GRID-CA
7	Jules Wolfrat	SARA	PRACE
8	Oleksandr Rokovyi	NTUU KPI	UGRID CA
9	Sergii Stirenko	NTUU KPI	UGRID CA
10	Vincent Ribaillier	CNRS/IDRIS	PRACE
11	Urpo Kaila	CSC - IT Center for Science	CSC - IT Center for Science
12	Maarten Litmaath	CERN	CERN TCA
13	David Kelsey	STFC-RAL	WLCG
14	Keith Chadwick	Fermilab	Fermilab
15	Paolo Tedesco	CERN	CERN CA
16	Alessandro Usai	SWITCH	SWITCH
17	Hardi Teder	EENet	Baltic Grid CA
18	Roberto Cecchini	INFN	INFN CA
19	David O'Callaghan	Trinity College Dublin	Grid-Ireland CA
20	Eric YEN	ASGC	ASGCCA
21	Dobrisa Dobrenic	SRCE	SRCE CA
22	Milan Sova	CESNET	CESNET CA
23	Thijs Kinkhorst	Tilburg U./TERENA	TCS Personal
24	Cosmin Nistor	Romanian Space Agency (ROSA)	RomanianGRID CA
25	Alexandru Bobe	Romanian Space Agency (ROSA)	RomanianGRID CA
26	Nuno Dias	LIP	LIPCA

Comments to David Groep.

participants remote: Vincent R. (CIDRIS/PRACE).

Eric Yen no changes to membership in AP.
ASGC → looking for new provider, ~100 certs.

Dave K./Derek TAGPMA update.
(AGC) *TACC retirement. (caused by other XSEDE CA)
*IGTF registration practices.
*SHA-2 variants.
*OCSP + IPv6. no issue in US: no interest.

S/P. ✓ Hellas + SEE: needs to be done still
Dutch Grid: DONE ✓
IUCC: now to TCS.
• HR Grid: ongoing.
✓ TR-Grid: ongoing.
• BG: org.
ROSA: waiting for review Ursula.
(AGC) . BG: : ping?
HPACI: : done.
Baltic: : redo S/A.
(AGC) . UK: : on initial. → must do S/A and update CP/CPS.
(AGC) pkIRIS: : ongoing.
IRELAND: : done.
Ireland: : done.

11:45
SHA 1→2. jGlobus: Keith: Globus team moving to new jGlobus 10 but that's not started yet.

! * also CP risk w/SHA-1 is ok but CA runs risk of being locked out once SHA-1 is broken.
especially QuoVadis, maybe also Comodo affected.
but CAB forum may suddenly mandate move to SHA-2 ...

(2).

by Apr 2013 aim to have no unsupported s/w. → CMD2 by 30 apr.
so at the end of 2013 (CMD3) all "should" bg ok.

also address software by vos communities (esp. LCG experiments).
that should be tested. but no firm commitments from them.

TAGPMA.

end-of-life. means valid Until date ≤ 31 march 2014.
other mitigation option: longer eecl but withdraw CA in case of breaking SHA-1.

* if algo is broken in a way you can brute force any content, then s/w should disable algo.
then it's a s/w vulnerability and that has a different process (and not an IGTF process).
→ prefer OS and common library :-)

* new CA exits in 2014 SHA-2 ?! rediscuss.
↳ what happens if s/w disables the algo? will all fail.
but also MD5 has never been removed.

* What about attribute authorities like VOMS? Testing needed
assume algo remains, this issue is not coupled.
but to be secure also VOMS should be SHA-2, but today both need to be ok (also identity) to be secure.
should be checked, but there are more implementations (OSG, uses the globus XACML library).
FNAL has a SHA-2 VOMS server for testing.

* multiple algo's support in same chain needed.

* new roots (existing compromised not) should be SHA-2? difference between roots and inter mediates.

* CA's themselves use SHA-512, and SHA 256 for EEC's? K

* CRL's: different dates, some issue both.
switch to SHA-2 only after everything known to work.

SHA-2 capable CA's. as of now

non-acc: CERN TCA. CILogon,

acc : DutchGrid, DigiCert, GridCanada.

by 1 oct '12: BalticGrid, RDSA, INFN?, CESNET.

IDAT discussed. → keep categorization. needs IGTF CA inputs for proper remediation.

- because of new software problems like the move to NSS by Redhat and impact on libcurl &c

move to EC crypto in 2013? not now.

(AG) * Remember move to 2048 bit EEC by end of 2012.

—

Alessandro. SLCS OCSP (as per Karlsruhe) is that needed?

for sites it's less relevant, so make it optional?

Disadvantages: leaks activity of client to responder/cache (unless you use stapling)

advantages: more timely, use next to CRLs, TLS stapling.

"OCSP stability at many CA's may not be good enough. and therefore threatens infra stability."

early on do OCSP on CA's to allow development. Not all CA's get. use trusted (not authorized) responder.

From TAG,PMA: not all CA's needed.

but all RP sites would need a cache service.

Stapling is hard for client-auth.

Recent from Karlsruhe, taking Panama into account:

(AG) Not needed for SLCS.

defer date for those that cannot do production-Level. If you can: do it!

consider jointly running anycast OCSP?

16 Florence ok.

b Abu Dhabi ok.

cg 44 EG-GRID ok for reviewers. Accredited by acclamation. (ACT)

Armenuhi cg 48 Armenia CA.

good review. → reset date of S/A. (ACT).

reviewers should be more active.

PL-Grid (10^00) (Adeel) Self audit presentation. by Adeel ur Rehman.

Slide 6: in practice ok? (cf #8) yes, in practice ok.

#9 → is ok :-) like #10

record archival partially is not D but A.

Reviewers: Milan, David G.

Valerdin did not show.

either show or suggest resignation. (ACT).

(DECIS) review membership guidelines → allow video to replace F2F do some extend (2 out of 3 drops a year for F2F)

(ACT) ask OSG rep for Kim Branley.

(ACT) Send warnings to MREN

NIIF + S/A

Anders. → MUST come or face removal.

RDIG.

IRAN16

(ACT). DoE Grids → move to TAG/PMA.

S/A

IRAN, NIIF, SiGNet, SlovakGrid, UlleSc.

FIM4R. differentiating LoA in IGTF
look at EUDAT? not active in policy based Stuff yet.
↳ ask as RP?

[lunch]

Hardi S/A BalticGrid CA.
↳ Self audit done, maybe re-use RP network also for LV TCS service.
new CP/CPS by end of the week. (16 Sep)
Rev: Dave K., Oleksandr.

Uambua (Milan). → general feeling about LoA-2 is not pessimistic.
- everyone to read Uambua doc (esp. RP's).

[lunch]

[STS]. based on Christoph's presentation.
+Reimer +Valery.
STS development at 80% done of SAML → X509. based on IdP's F/S extension. (Hannu)
demo next week at EGITF Prague. → beta in december 2012.
target EMI-3., support afterwards unclear.
generalised SLCS focus on SAML → X509.
only unicore has operational use case: submit jobs from Unicore to VOMS-CREAM CE.
also WLCG service access is a use case (RomainW), & Fed Cloud?

START with usecases. for STS discussion.
- reschedule for Jan. 2013 once usecases identified.
-
* maybe original IdP should be identifiable in final cert.
* where does the incoming SAML assertion coming from?
in client-ig device A is portal or unicore device.
↳ unicore makes internal SAML assertion, maybe from X509 again :-).

* STS demo next week!

(5) 26th EUGridPMA. 12-09-2008.

Paolo SHA-2. @CERN.
- same namespace for new CA.
code signing → not really useful, but users seem to insist on them
- 2 years is a problem:
→ put code signing on different (non-accredited) ICA under the same root. (and make it the typical 3 years)
→ look at meaningful "O" attributes to get sensible displayname in browser warnings.
remains classic, just add new root+ICA in distribution.

Robot · colon has issues in httpsvd. found for "UID:" and "Robot:". FNAL did testing for "uid:" 3 years ago, and lots of other things did not work.

Until may have a s/w solution to still use a colon in httpsvd.
↳ see mail.
use of "/" for robot in use for "service" certs. DFN uses "--".
→ use a non-alpha, (non-whitespace), Printable char after Robot.

"=" is bad, "/" is confusing, ":" is broken, recommend "Robot␣-␣".

Next gen of BC + apache.
* New CAs should prefer the new convention, but existing CA's do not have to change.
* prefer the last RDN, so it shows up more in logs.

OCSP RFC 5019 only in PHP+Apache
- needs only the index.txt file for OpenSSL based CA's.
Validity of responses:
. start with 30-day pregen response life time to stress the test.
do at least have something there and RP's can start to test.
it should be easy on the CA's to generate them

OCSP
- hit on CA may be higher (more requests than CRL's). "DDoS"-like.
- not mandatory yet. (and RP's don't use it yet).
- OCSP responses are smaller (and scaling behaviour different wrt load of CAs)

S/W expected by end of Sept 2012.

(YAT). doc and guidance → OSOPS-WG in OGF36 (Chicago). → Milan.

Miscoc. (DK) don't let EECs live until the very end of the CA life time.
allow a few months different.

DECISION: allow 2 month.
not in RP, but in distribution process guideline.

in release doc: "CA must be valid for entire period until the new release at the last Monday of the month".

→ document the release process.

x bert: roll over earlier (14-16 mo in advance).
(YAT). send warning on distro build 16 mo. in advance and.
don't trust the CD's.

(YAT). Cyprus has an issue on Feb 3.

GridIreland THANKS to David OC!
decisions in next month on if and how to continue for e.g. PRACE.
- is relevant for prace! Rules to raise awareness in PRACE in .ie.
- maybe TCS solution. Or hand take it over.

12:15 closing: thanks to Jean-François and Hélène.