Minutes 20th EUGridPMA Meeting, 20th September 2010

Round Table
Attendees
Ursula Epting, 12500z, 2400v half u/h, Jens Jensen 25000z 3000v, David Groep 6000 z, 800 v, Reimer Karlsen-Masur, 4400z, 1200v, slcs/robots rarely; Alice de Bignicourt CNRS, 800v u 800 vh, Emir Imamagic, 438 z, 117v half u/h, selfaudit; Dobrisa Dobrenic SRCE CA
Kristos Hellas, 2500 z 500v; Valentin Pocofilenco, Milan Sova Cesnet, new CA PCS(?), Nuno Dias LIPCA, CPS update; Robert Cecchini INFN 3400 v, 85 RA's, Mine Altunay OSG, RP, Erik Yen Taiwan/AP;
Daniel Garcia Franco RedIris 1100 v 500 u, David O'callaghan GridIreland, move to TCS; Thijs Kinkhorst, Surfnet
Dave Kelsey RP, Miroslav 700z,150 v; Alexandru Bobe/Cosmin Nistor Romanian CA 400z 150v;

Attendees:22, +Tamas MarayNIIF/Hungarnet

Erik Yen, Status of APGridPMA
see slides
19th March 2011 IGTF All-hands meeting collocated

Mine Altunay, Status TAGPMA
New CA's using Sibboleth, new questions regarding remote identiy proofing, NIST guidelines are allowing remote id proof, but how to do for CA's
Dave comment TAGPMA issues also updates to MICS/SLCS; priv. Key protection guidelines
next F2F Dublin, (?)

Jens update about Risk Assessment Team
No real incidents since last time; technical issues: switch to longer keys more than 2048 and sha1/2; Can middleware support this?
CRL get to close to their expiry-date – concerns about it, what to do
communication test: 10 member 8 responses within the first day, 2 members never responded
summary no more effort put into this communication stuff
short discussion how to contact MW groups and who has to do test that certificates are working:
collaboration between sw developers and ca management is needed!

Q Dave Build a ca with sha2 stuff and show on website, look how they will look like from 2012 on.
Reimer or Jens built up a ca with sha2 sign
Prerequisites: sha2 signature should work, also mixes of algs in the chain,
second issue: key size 2048 – signature checking is an issue to performance

Task Force: Jens Jensen, (Milan Sova), Mine, David G.

Q Reimer: how many 1024 bit long keys are out there

Jens: DPM gets performance problems with 2048
Conclusion NCSA should be asked about the results of performance tests 1024/2048 keys

For CRL – please look at Nagios

Mine: publications and retrieval of crls sometimes difficult for sides, expired or network problems.
a) central distriution point
b) crl longer lifetime

No

Chair election: David was reelected as chair for another year!!!

Reviews:
IUCC – Jens and Kristos Kanelopoulous – no updates on this
LIPCA – Alice and Daniel – kompleted
UK-CA – review completed, but new updates on CP (see presentation)
missed David O'callaghan
Armenia – Jens and David, review at Armenia ok, new updates not rereviewed now,
... Emir , Kristos
AegisCa – Alice? no updates on the list
Switch – Riga, Allesandro – David G. Edgar – OK
RDIG-CA – Jens, Kristos K. - Eygene R. - audit overdue, audit not ok (format), they didn't show up for more than 3,5 years, Jens has sent his comments back, technically good feeling
D.G. is supension an option? write a letter to the management of RDIG? showing up is a must – 3,5 years is to long. D.K. follow up via WLCG management board,
Decision: somebody from RDIG has to show up at the next meeting in Utrecht otherwise they will be suspended (->worthless)

End self audit

Milan Status update Terena EScience CA
Personal Ca no problem, server – hope that many certificates can be issued soon
Life demo: Tacar website has changed, easy
COMPLAINTS about sha1sum of a signed certificate (converts into der and then calculates the checksum which is not the same as of taking it from the pem-file.

<u>Tacar – Milan Sova</u>
Demo of new Webinterface for users/ca-admins
Prop. K. selection of CA's cert download

<u>Downtime notification – how to bring this the best way to RP's?</u>
EuGridPMA, Website? GOCDB? Distinguish between crl and other things
Mine: nice to have a table with scheduled downtimes
Suggestion TAGPMA/EuGridPMA wiki page (with RSS feed?)
Create table template
Discussion
Conclusion – requirements: CA's enter their own notifications after authentification, should support RSS and/or email, list formatted output on some website public, service for RP's/consumers of IGTF , information should expire, subscribe for changes
Who? – David O'C
Recommendation to announce downtimes 1 week before (if possible)

<u>High-level CA Profile and technical implementation and acceptance by the RPs – Jens Jensen</u>
Discussion where to put "trusted" CA's with accredited subordinates.

IGTF Policy for high-level certification authority v 0.10
Q. impklcit trust for intermediate CA's?
Fortsetzung.
Comments semantic i ssue (which one?), Namespace contstraints file (see David G. notes ☺

- ➔ New edit cycle new pick up again next TAGPMA meeting or/and at OGF

Update from Authorization (Non-)Working Group – Dave Kelsey
See document
X509 – SAML, stick to VOMS generalize the rest ?☺
No substitute voms with attribute authority, no no.
Editing the document…