Meeting Minutes 30th EuGridPMA Meeting, Jan 2014, Abingdon, UK

(Taken by Ursula)

Monday, 13th January 2014

Welcome

Agenda

Events see slides

You can find all slides here: http://agenda.nikhef.nl/conferenceDisplay.py?confId=2694

For notes within discussions: Q=Question, A=Answer

Round Table (postboned)

APGridPMA update - David Groep (David)

see slides

No questions

TAGPMA update -Alan Sill

see slides

Officer elections tue

New position: Co-char for Latin America (… at minimum fluency in Spanish)

sub meetings to be organized by co-chair and held in spanish as english was/is a problem for some CA-managers from South America

Currently cleaning up membership list

Join OGF-meeting! Grid profile could become a recommendation.

TAGPMA19 May 26-28 Cancun Mexico

TAGPMA 20 Dated TBD Fall 2014 Salt Lake City, Utah USA

Everyone should attendend OGF!

CAOPS contracts for Higher level CA's

HLCA ever granted, checklist, Policy 0.10

Grid certificate profile update

Privat Key Protection update 1.4

Update self audit status - Kaspars Krampis

see https://wiki.eugridpma.org/Members/SelfAuditStatus

Q: Belnet? → TCS problems with some institutions → create a catch all for those?

Suspension of Jordan CA - David

CA was removed from IGTF release after several warnings

if they want to be in IGTF-release again – go to the initial accreditation process.?

Decision: Hear their reasons and then decide

HIAST CA - David

– Syria has many times problems with crl – but we will keep them in the release as their situation with the civil war in Syria is very difficult.

-----coffee break----

Self Audits (in changed order)

CA update II: MREN - Lidija Milosavljevic

see slides
Questions:
CA does not rekey? User has to revet every time (small ca only a few users)
Copy of id's still legal?
1024 bit keys → **please change to 2048**
peer reviewer: Krisots Kanellopoulus. David Groep

Round Table
Do we have alist with all attendees, wasn't able to catch all names

----Lunch----

wLCG identity management requirements and development - Dave Kelsey (Dave)
Identity Federation – slides from Romain Wartel, presented by Dave Kelsey
see slides

Q: ssh to portal? (see later)
Discussion about moonshot (webbased) Focus of above is to be usable from cli
Discussion during presentation
Q: Alan Sill does not scale with mass-job-deployment (if shib is used for each submission)
[…] dnssec would be a solution (but is not available everywhere)
concept of 'user account' expires (probably) – cloud service/virtualization- > user are root everywhere → containers
rebuild the token to have something highly available
Jules Wolfrath: sites do not trust portals want to have log information about users
----
David problem: with iota-based igtf-release – then you serve all vo's in there – and you might not want to do that.

What could IGTF do to help with ideas for a solution?

Different discussions about STS/Moonshot/ECP, Pilots, cilogon and so on
More discussion later

AAI federations and LoA: stepping up, not down - Thijs Kinkhorst
see slides
Yubikey one time password (otp), selfregistration.
This could be used for the TCS Administrators at the moment.

scenario: malicious process on laptop – yubikey otp– could be fished – then own authorisation would not work
Server Software? Several implementations.
Yubikey – appears as usb keyboard, if touched then prints out characters.
(only some points of the interesting discussion have been noted)

IOTA AP endorsement - David Groep
see slides, work on the document, for the outcome see document:
https://wiki.eugridpma.org/Main/IOTASecuredInfraAP
discussion 'direct contact to the user' and mail address in SubJectAlternativeName
Big discussion here but then:
The document in it's newest version 1.1 has been accepted from the people present in the meeting.

Tuesday, 14th January 2014

CA update IV: LIP CA, Nuno Dias
see slides
Q: Willy – renewal - how is it guaranteed that's the same person?
Nuno: by some technical means + visit at the ra
Q: remainig lifetime ca certificate double?
A:... for short lived ca certs minimum lifetime, for long lived the remaining time must be as long as end entity
sha2 certs issued
new cp/cps possibly at the end of april
Reviewers: Anders Wäanenen, David Groep

CA update III: UK eScience CA - Jens Jensen
see slides
Q:. Jules: internal users can use internal cert for their internal cluster/single sign on and escience cert if they need grid non-local –
A:yes
Q: Anders – use cases for tar.gz / vdt packages?
A:-yes, bsd or other, has been just useful
vdt dead since 2 years …
Q: Jules – whats the difference between 2a and 2b?
A: 2a is online, 2b only wakes up to synchronize. 2B was thought to be used together with local idm
Q: dave what does the advisory group
A: Not much (missed something ;)
WLCG not ready for sha2 – dcache versions issues, vomrs-admin interface not ready, first time registration with sha2 cert not possible (adding later is possible) and some sources in the US were also not ready.
Have a look at the full review table on the wiki
New CP (not CPS!) nearly ready for production, each CA has it's own CPS
Interested Parties to read the CP: Willy Weiss, Ursula Epting

AA Operations Guidelines implementation plan Keith Chadwick (*FNAL)*
see slides
questions
Q:Dave – voms signing key – seperate keys – fully supported?
A:Keith: two different keys, configuration item at server start up
Q:David: document not clear enough, wanted: key for signing of users is another than the normal hostkey
A:Keith (didn't get that)
David –> revise documentary
Dave: Lifetime of assertions – end user can extend lifetime
A: normally done at the client side, but can be set at the voms-server side
Dave: was something missing in the operations document?
A Keith: no
Dave: Talk from Keith could be a template
David : As service provider it's easy to describe this, but not for communities
Keith:...
David : what does OSG have compared with VO-ID cards?
Keith: didn't understand

Q: Dave terminology 'AA' ~ Authentication/Authorization here used as Attribute Assertion – could/should/might be changed to make it clearer
A: Jens 'AA' is also used in RFC 5028
Jules comment: in Prace review of ldap based system ~ attribute releasing system, this assessment will be/was also used.

----Coffee----or----Tea-----

IGTF communication test –Ursula Epting
Rechallenge will be done during the next 2-3 weeks by Ursula for all those CA's which didn't respond to the regular challenge. Couldn't be done earlier as some contact information had to be updated first.

Private Key Protection guidelines I Jens Jensen
see slides
discussion - result see in the new document
https://wiki.eugridpma.org/Main/PrivateKeyProtectionLifeCycle

----Lunch----

New NIIF CA, Tamas Maray
see slides

Anders has concerns with Fedora 18 on the RA maschine, cause that's not supported anymore, esp. no security updates!!
Tamas: will check
Q: Kevin how many RA's do you have
A: Tamas: only two, maybe more in the future
Q: Kaspar: Spear Rasperies?
A: Tamas: Pub webinterface is a virtual maschine
Q: Kristos: how are machines interconnected?
Discussion (again) don't use Fedora for RA-maschine, cause constant updates are needed.
Q: Power?
A:Tamas:: UPS connection
Q: Anders: how many modifications on OpenCA?
A: Tamas: not to many
Q: Anders: general question move to sha2 difficult??
A: configuration is in openssl, not directly openCA
Q: Willy: online CA? Root?
A: - still selfsigned,, no offline ca issuing crls needed by
David: root key was generated outside and uploaded to the hsm
Discussion about softwares looking at crl
and more discussion about hsm level 3
Q: Jens: which hsm token ist it
A: T: Gemalto IDPrime MD FIPS 140-2-Level 3 certificate
more discussion
Reviewers: Anders Wäanenen, Jens Jensen

Online CA architectures - David Groep
see slides
~ requirements document for online ca (classic profile)
new req: key should be manually activated on boot, not automatically

Q: back to Willy: how is it really done on NIIF CA, token does the signing or encryption only?
David is going to draft a document for online CA's (finally after 11 years this happens)

Private Key protection guidelines II Jens Jensen
results see document
Q: Willy: difference creation/import into level 3 for ca's and users → see document.

Presentation of the next 31st meeting in Tartu, Estonia – Piiu Pitt
Problems with vidyo - postboned

Jens Soap Box – Jens Jensen
see Document (relevant parts of document will be uploaded later)
Disaster recovery, thorough analysis on services and dependencies
availability versus integrity eg for ca private key

Q. Jules 'network' means everything, higher level like firewall...?
A. Jens: everything, each component

Some problems with secret splitting, two out of three, one is leaving and giving the secret part to the other so one person has already two parts of the secret.
How can we do this kind of things in a good way?
Put it on key-token […]
Most problems unsolved, do the best you can – don't make it too complicated as this may bring more problems into life.

Soapbox - Jens Jensen
see slides
feel well :-)
critical points: change process not perfect
Discussion/talk about the stuff Jens mentions

Q: Alan: Extending use of our cretificates eg to clouds?
small discussion, no decisions

Now again
Presentation of the next 31st meeting in Tartu, Estonia – Piiu Pitt
see slides
DATES: Wed-Thu 14-15 May 2014 in Tartu, Estonia
Detailed information will then come, but already a lot of information in the slides!

Wednesday, 15th Jan 2014 could not be covered by me :(