27th EUGridPMA Rome meeting

from **Monday 14 January 2013 (09:15)**
to **Wednesday 16 January 2013 (17:00)**
Europe/Amsterdam
at **CASPUR (GARR)**
chaired by: ***David Groep (Nikhef)***

Monday 14 January 2013 | Tuesday 15 January 2013 | Wednesday 16 January 2013 |

Monday 14 January 2013

09:30	Welcome (10') (Slides)	
	introductions information from our local hosts agenda, minutes of last meeting, selection of note taker	
09:40	Eulogy Milan Sova (15')	
09:55	Round-table update (05')	
10:00	Updates from the APGridPMA (20')	Eric Yen
10:20	IGTF Risk Assessment Teams actions and future (20')	Jens Jensen
10:40	Report-out from the self-audit review (20') (Slides)	David Groep
11:00	Coffee (30')	
11:30	CA Update I: SlovakGrid (30')	Miroslav Dobrucky
12:00	SHA-2 availability status and issues (1h00')	
13:00	Lunch (1h30')	
14:30	CAOPS/IGTF Joint Sessions: OCSP Profile for CAs (1h00')	David Groep
15:30	Tea (30')	
16:00	CAOPS/IGTF Joint Sessions: OCPS Recommendations for Relying Parties (1h00')	David Groep
17:00	Closing and location dinner (10')	

Tuesday 15 January 2013

09:15	CA update II: MD-Grid (30')	Valentin Pocotilenco
09:45	CA update III: NIIF Hungarnet (30')	Tamas Maray
10:15	Documenting suitability of Kantara/NIST LoA-2 (45')	unknown
	For the Classic and MICS profiles Documenting suitability of Kantara/NIST LoA-2 ("CILogon style") (with govt. involvement where relevant) as meeting Classic and MICS AP guidelines. This is relevant for our Nordic countries.	
11:00	Coffee (30')	
11:30	Private Key Protection Guidelines and Guidance for the operation of key stores (1h30')	Jens Jensen
	"how to manage access to those keys when data may be locked/encrypted with only these keys for access" (from IGTF session on private key protection guidelines) Private Key Protection (Jens Jensen et al).	
13:00	Lunch (1h30')	
14:30	Generalisation of the SLCS profile – "STS" profile (1h00')	
15:30	Tea (30')	
16:00	Presentation of the next 28th meeting in Kyiv (15')	Sergii Stirenko
16:15	Jens' Soap Box (1h00')	Jens Jensen
17:15	Closing and location dinner (10')	

lower loa? new audiences?

Wednesday 16 January 2013

09:15	CA update IV: NorduGrid CA and transition (30')	Anders Waananen
09:45	CA update V: (reserved) (30')	
10:15	TechWednesday (45')	group discussion
	how to build a 'will it work with the IGTF CAs' suite of test certs for software providers to validate against? How to prevent these having to request a cert from each of us?	
11:00	Coffee (30')	
11:30	TechWednesday (1h00')	
	Open Forum (e.g. OCSP implementations)	
12:30	Lunch (1h30')	
14:00	SCI meeting (3h00')	David Kelsey

EUGridPMA 27. (1).

RAT * communication challenges. Ursula to coordinate. (for CAs)
- we know of no PKI (/Fed) specific trust groups yet.
Maybe Scott or Derek.
* which crypto circles we move in to gain advance warning.

S/A * UK eSc update on Wednesday.
* Baltic: Reimer to contact to see if they want to update/stay. (ACT)
* Prod: MARGI, BY, TR, (ACT)
* Nordic: sent on Friday. Due to review, looks good.
* ROSA completed.
* CALG on hot list (ACT)

RoundTable * ETSI audit passed by DFN. (not grid-specific policies, but physical setup is the same). ETSI does the technical bit, CABForum does the policy bit.

[coffee].

SlovakGrid CA (Mirasbru). Full self audit.
* do not change CN / Subject name wantonly, mainly for storage ownership
* Reviewers: Pawel, Emir

SHA2: * since the TAG/PMA time line is materially the same as the Lyon text (modulo Sept/Oct 2014) this is OK
- "MUST" when sha-1 is broken., really don't.
- end of SHA-1 CRLs allowed per Sept. 2014.

* is it allowed to have both a SHA-1 AND -2 for the same key pair?
- remember to revoke both if priv key compromised
- it's confusing for users, so not recommended. (two keys is clearer)
- but does allow graceful fall-back.
- use two different serial numbers.
- ~~may be~~

PRACE is testing Unicore (should be OK).
jGlobus 2 works., gsiSSHTerm tested by LRZ.
EGI/UCs ____ for dCache still in progress.
Not supported:
old VOMS-Admin tokens.

---

again on dual-issuance:
- may be good for (interm.) CA's to have both hashed certs
- with different serial numbers!

do ALLOW three certs for same keypair and different hashes
IF: serial is different
but should not be a default for confused users. (by CA).

Status: 2048-bit - forced now at AustrianGrid, etc.
- some are not ready! some issues with JE/VB.
SHA-2 : few (MD-Grid, SRCE) not ready.
others can do only either SHA-1 OR SHA2
Server certs also relevant for PRACE! Needs availability by CA's
move to SHA-2 monitored by EGI ops team from Q2 or so? EGI CSIRT.

IPv6

- most important for CRL retrieval and OCSP
- most sites (also BP) mainly preparing or testing only.
Recommend (again) availability for all by January 2014!
and keep v4!
Status tracked by particle.cz: see link on /review/

27th EUGridPMA

Eric Yen – APGridPMA. / see presentation

sha-2 OK after March 2013

* March 22nd (Fri) APGridPMA meeting.
* IHEP emailAddress formally ready but should still migrate!

<on OCSP discussions: see Wiki + notes Jules & Dusan.

—

TUESDAY

Valentin HD-Grid.CA.

upgrade to OpenBSD 5.2 with new OpenSSL for SHA-2.

Reviewers: Cosmin + Miroslav

Tamas NIIF.

TCS also available in Hungary, but not eScience (yet), and only for servers.

TCS personal is also expensive.

maybe run CA off a Raspberry Pi? + LOA-IT HSM @ level 3? → not really HSM?

difficult to generate more demand for TCS Personal.

LoA for MICS Kantara LoA2 is OK. → see text to mailing list / update MICS

new profile @ LoA 1.x : keep unique and persistent, never re-use
"Basic" unique globally across IGTF

but can be anonymous, and RP's do more authN vetting

Tue. 27th EUGridPMA. (4)

Implementation: must be different trust anchor
different OID
different AP profile.

Involvement: RPs(!) Dave V, Sules, David G. +
+ Jens, Jim B.

+ Survey by OSG on site needs.
OSG: user name, email (and VO) needed by Sites [real name]
tracing possible without VO for some sites.

if different LoA, also other (security) requirements may change.
* trust in CA operations remains important (parent hijacking)
important for Sules & PRACE.

Looking at new AP "Light-weight uniqueness-guaranteed AP with secure infrastructure".

— — — —

JUNet has 800 hr problems

Jens PKIPMPG <see slides>.
CA org can run the keystore → see new Wiki text.
approved by EUGridPMA → move to other PMA's.

—

STS: ties in with work for FIM4R. Timeline clearer in a few month since there is no prototype yet.
NEXT STEP: setup wiki with SLCS text. (ACT). People: DaveK, DG, JJ, +Romain
make X.509 bits optional, but needed to integrate SPs with current S/w.

(2) X.509 to SAML - (a) service per country
(b) IGTF IdP

(3) our RA knowledge used as IdP producing also SAML.
again either nationally or IGTF wide.

PERSISTENT UNIQUE NAMING IS ESSENTIAL.

27 EUGridPMA (5)

EIHGR next meeting @ PSI in Filingen (CH) in March
go there, and encourage national federation establishment if
you don't have one yet! Link up through REFEDS and
collaborate.
Too many countries still don't have an operating federation.

Kyiv May 13-15 (Mo → Wed).

<Insert Soapbox>
more focus on outreach / PR / news! → demonstrate use and relevance.

WEDNESDAY.

Andrew / NorduGrid:
rekey needed (now 1024). PMA: some interest in shared certificate mint,
but there is no volunteer to run one and
Milan is no longer.

Test suite: - there is also NIST test suite
- publish test suite also including private keys of EEC
- including expired, revoked etc OCSP
- tar-ball generator → unique keys for security.
properties of test suite: - same number of CRS - subject naming ":"
- similar properties.
generating CA's is simple and known, EEC's unknown.
* CA's to provide EEC's including extreme examples (such as "c" in names).

- "make" script for the suite to generate unique keys
- characteristic examples needed

actually compromising a cert to revoke it but not use fresh crl in testing, and you compromise your own cert by sending key to Paul :-)

need sending sample of EEC
- ~~dooer~~
- host
- extreme case (like UTF-8, diacritical chars)

Test needs to be DIFFERENT from real for names. to prevent confusion
(*) and trade mark issues: "ROT 13" all printable characters

Need CA, EEC's + CRL (+OCSP, in real life for original CA, so also RFC5019 and not only openssl ocspd).

(ACT) * each CA:
- send (link to!) sample EEC's
- known trouble EEC's should be included.
- 'parameter space' of subject naming.

To develop test suite: student?
Test suite should include deliberate failures:
- namespace violations
- expired
- revoked
- CRL+OCSP.

Interested CAs looking for disciples: Jens, DavidG, +Paul M.

Open Forum:

online CA project: NATO project modelled in new (PHP) online CA software "phpca".

DogTag, RedHat CM, EJBCA, OpenCA, MyProxyCA, phpCA,
and some training/test CA's that are on-line.

- Why level 3? HSM, and not L2? Inspired by ESNet.
  advantages. - role vs. personal activation
  - tamper-proof vs. evident
  but are these relevant if key is always active?
  Classic: 3, SLCs: 2.

L2: you can import a privkey but not get it out. But you want import with signing ceremony anyway.
*put entire thing in a safe (e.g. Raspberry Pi + HSM token + USB stick)
- Alladin/SAFENet

* compare risks to classic offline.
* better for subscribers and operators

⁉ ⇒ if risk comparable, allow L2 } + compensatory controls. (like a safe)
discuss with TAG+AP. } + operator present on activation. (pin/passphrase)
propose for IGTF All Hands.

Interest by Ursula, Roberto, Dg.

Test Suite.

Participants 27th EUGridPMA meeting

Meeting Information	Registration

		Name	Affiliation	Membership
√	1	David Groep	Nikhef	DutchGrid and EGI
√	2	Jens Jensen	STFC	UK e-Science
√	3	Roberto Cecchini	INFN - GARR	INFN CA
√	4	Miroslav Dobrucky	Institute of Informatics SAS	SlovakGrid CA
N √	5	Jules Wolfrat	SARA	PRACE
√	6	Reimer Karlsen-Masur	DFN-CERT Services GmbH	GridGermany CA
√	7	David Kelsey	STFC-RAL	WLCG
√	8	Jean-Francois GUEZOU	RENATER	Grid2FR
√	9	Valentin Pocotilenco	RENAM	MD-Grid CA
	10	Vincent Ribaillier	CNRS / IDRIS	PRACE
	11	Adeel-ur-Rehman Zafar	National Centre for Physics, Islamabad, Pakistan	PK-GRID-CA
√	12	Ursula Epting	KIT	GridKa-CA
√	13	Willy Weisz	University of Vienna	AustrianGrid CA
	14	Romain Wartel	CERN	CERN
√	15	Emir Imamagic	University Computing Centre (SRCE)	SRCE CA
√	16	Nuno Dias	LIP	LIPCA
√	17	Hardi Teder	EENet	BalticGrid CA
√	18	Eygene Ryabinkin	NRC ""Kurchatov Institute""	RDIG CA
	19	Christos Kanellopoulos	GRNET	HellasGrid/SEE-GRID CA
	~~20~~	Antonio David Pérez Morales	RedIRIS	pkIRISGrid CA
√	21	Cosmin Nistor	Romanian Space Agency (ROSA)	RomanianGRID CA
√	22	Alexandru Bobe	Romanian Space Agency (ROSA)	RomanianGRID CA
√	23	Anders Wäänänen	University of Copenhagen	NorduGrid
√	24	Tamas Maray	NIIF/Hungarnet	NIIF CA
	25	Eric YEN	Academia Sinica Grid Computing Centre	ASGCCA
√	26	Pawe&#32	Wolniewicz	PSNC
N √	27	Dusan Radovanovic	University of Belgrade	AEGIS CA

Comments to David Groep.

Boulder, CO, US. 9-10 May.

Dusan