12th EUGridPMA meeting, Day 1

Monday 14 January 2008
NIKHEF, Amsterdam, Netherlands

CA updates

- Milan Sova (MS) (CESNET):
  - planning to rebuild the whole infrastructure and provide Shibboleth interface.

- Jens Jensen (JJ) (UK eScience):
  - security incident

- David O'Callaghan (DC) (Ireland):
  - activities within Grid Ireland, SLCS, but in few months or years

- Reimer Karlsen-Masur (RKM) (DFN-PCA):
  - starting to prepare roll-over, try to get rid of user and service CA and let the root CA issue certificates in the same time, requires small CP/CPS changes
  - preparing SLCS CA, will be ready for presentation in Kopenhagen, searching for reviewers, SWITCH already accepted (Mike volunteered)

- Spain:
  - old CA expired in September

- Willy Weisz (WW) (Austrian Grid CA):
  - no changes, problems with funding in 2007

- SWITCH CA:
  - upgraded infrastructure in September

- Roberto Cecchini (RC) :
  - robot certificates
  - problem with sites downloading dead CRLs, action should be taken (Italy will send a list of IPs to David, Jens, ...)

- CERN:
  - solved problem for Vista users,
  - mid-term goal: issuing certificates on smart cards, testing how it will be compatible

- SRCE, Emir Imamagic (EI):
  - self audit, moving to new RFC
  - MICS or SLCS in half of year hopefully

- Arsen Hayrapetyan (AH) (Armenia):
  - selfaudit will be presented

- LIP:
  - no news

- CNRS:
  - change of a machine, doesn't require approval of CP/CPS update

TAGPMA, Vinod Rebelo (VR)

- 19 members (CA, US, MX, Latin America)
- in contact with developer of OpenCA (anyone interest can send feedback)

- SLCS profile revision in two stage:
  - language update, HSM level issue (v2 or v3)
  - policy update (do we need CRL?)

  Q: Jürgen Brauckmann (JB): what kind of security incidents related to need of CRLs?
  A: David Groepp (DG) Kerberos keyfile for multiple of users (1000) got compromised
  Mike Help (MH) There was no solution how to invalidate these certificates, other than disabling whole CA for period of time
  - Agenda

Accreditation: U-GRID (Ukraine), Sergiy Velichkevych

- DG: **accepted**

Accreditation: MARGI CA, Aleksandar Dimieski

- CA machine is kept in 1. safe, CA key is in 2. safe, CA passphrase is in 3. safe
- presented web site

- Christos Kanellopoulos (CK): problem with usage of official name of country of Macedonia

  Q (AH): which software is used?
  A: CSP (set of perl scripts wrapping openssl)
  Q AH: is the problem solved with CRL v2?
  A: it has been solved by Greece and AEGIS

Continuous Audit Process II: BEgrid, Christian Van Heurck (CVH)

- were using home made scripts, but are planning to use complete PKI solution
- complete solution will demand revision of CP/CPS document
- CP/CPS doesn't have OID, it will be added (not too bad since CP/CPS hasn't changed since 2004

- they made quick review of tools, weren't happy with OpenCA (will check OpenCA NG with VR), had interesting presentation from OpenTrust (http://www.opentrust.com/)

Q Jules Wolfrat (JW): in October it was noticed that CP/CPS wasn't on the web?
A: everything will be fixed

DoEGrids CA and PKI Architecture, Mike Helm

Presentation order:
- ESnet-CA-Stats-Presentation.ppt
- DOEGridsCAOverview.ppt
- ESnetResume.ppt
- IGTF-Reviews-DOEGrids-CA-Operations.ppt
- UnixSecurity_JohnW_atf-1.ppt
- physical-security-atf-1.ppt

Discussion:
Q (Ian Neilson, IN): (related to NIST) do auditor look at each assertion?
A: yes, every 3 years; there are many people from both institute and auditing side

Issues:
- renewal is performed automatically (without re-authentication every 5 years) (MS, IN commented, will be discussed later)
- new RFC - no (waste of time and energy)

Q (David Kelsey, DK): were RAs audited as well?
A (Doug Olson, DO): picked random user and service certificates and traced back identity verification records at RAs

Q (RKM): renewal is a political issue?
A: No, it is a customer issue, agents are used to do stuff in certain way, and otherwise they might leave. Identity validation is political issue.
Q (RKM): how to other TAGPMA members solve these issues?
A: there are no US members that couldn't get certificate from DOEGrids.
Q (JJ): (~) rekey or renewal?
A: renewal service was not done good i the first place, so users used rekey interface. Now the renewal interface is disabled completely.
Q (MS): how do you do encryption?

A: they don't do it that much, mainly for emails

Conclusion (DG): for all of these audits we should get couple of reviewers?
Volunteers: ??

Comment (CK): what is the impact of audit - how to respond to aspects which are not compliant and won't be changed because of whatever reason?
Comment (MH): some problems are just documentation issues which will be fixed, change of profile needs to be gently introduced due to the community reponse and habits
Q (Szabolcs Hernath SH): will there be a 2. round after reviewers review audit
A: no

Identity in US Science Environments, Doug Olson

Comment (CK): what are the consequences of not changing non-compliant CP/CPS?

DG: ~ in general issues should be resolved and update should be done within 6 months; after a year CA is kicked out, unless enough arguments are provided for not changing the CP/CPS

12th EUGridPMA meeting, Day 2

Tuesday 15 January 2008
NIKHEF, Amsterdam, Netherlands

Effect of the Grid Cert Profile on the Classic AP, David Groep

DG: general idea: throw out parts from AP in favor of Grid Certificate Profile (GCP) to avoid inconsistencies

Q (MS): what about other profiles?
A: other will be changed as well

RC: should IGTF use OGF profile? What happens if OGF decide to change?
A: reference will be make to exact version of document which is frozen
DK: these are the same group of people

WW: but then we must comply to other body which we don't have influence on?
CK: instead of having IGTF as a single body doing everything, it is better to make parts standard within community like OGF; also this doesn't limit us to drop OGF document
MS: would it help if AP would have reference to exact version?
DK: we decided to adopt frozen document
MS: isn't that another obstacle, because it takes ~9 months to change it; are we happy with this period

JJ: problem with MUST in C attribute (described in GCP)

Kaspar Brand (KP):
- there should be room for exception which can solve problem of slow OGF process.
- welcomes removing redundancies

RC: if the GCP document is in final form, how do you solve Jen's problem? If the GCP is not in final form what are we approving?
DK: we won't have new version of AP before GCP is in final version

MS:
- is there a need to give the text to other body? (and risk problems with updates) is it worth it

DK: it's a bit late, document already went to
JJ: it's not a question whether it should be published, it will be published, question is weather we won't to put must comply in AP?

WW: if we adopt OGF why should RPs come to us?

EI: what is the difference between accepting other external documents like RFC?
WW: RFC is widely accepted within Internet (and other) community

JJ:
- there should be a contact person in case of issues
- there should be defined update process

CK: you can only publish document in OGF, but not update

DK: (regarding contact) all the authors are from this group, so you can contact them

Q (JP): how many questions have been asked by RPs in the past?
A: several notorious (e.g. uid)

DG: only issue is "red" paragraph (on slides).

Q WW: deeper problem: we cannot say it must comply, because the GCP says it is pure information and not technical recommendation
A MH: but we can interpret the document any way we want
A CK: this is why we say must
WW: how can we say that correctly if the document is only informational

DK & WW: maybe is good to use expression like "adopts content of OGF document .." (?)
JJ: maybe to use "has written by IGTF and published by OGF"

Conclusion:
"adopts the contents of GFD-C.XXX as published by the OGF and based on the IGTF operational experience .... should comply therewith"
(http://www.eugridpma.org/agenda/askArchive.php?base=agenda&categ=a073&id=a073s1t1/text)

SLCS Profile updates and endorsement, Mike Helm

- 3 Identity
"not sharing private key" should be somewhere else
... discussion related to private key sharing and grid portals which enable users to store their private keys ...

- 3.1 Identity translation rules
- accountability - heavy request "any time in future", is the year enough?

- 4 Operational Requirements
- is it necessary to have "FIPS 140-2 level 3", suggests downgrading level 2

Jürgen Brauckmann (JB): planning to set up all inclusive CA machine, can this machine have other services (e.g. timestamping), but still accessible only by CA staff. Does that comply with profile?
MH: are these virtual hosts or applications vissible to each other?
JB: could be virtual machine
DG/MH: it is possible for a machine to serve both MICS and SLCS CA

MH: CRL is necessary in distributed environment, would like to hear experiences from existing SLCS CA...

CAs in the NATO Partner and Mediterranean Dialogue Contries, Arsen Hayrapetyan

Q RKM: you're pushing OpenCA and some of them don't have experience with ICT, OpenCA is quite complex?
A JJ: it will be made easier

Anders Wäänänen (AW): what about OpenXPKI?
DG: technical discussion postponed...

Establishing a sustainable PKI in the NATO Silk Highway countries, CEENET, and the CEENET-EUGridPMA relationships, Jacek Gajewski

comment DG: experiences from SEE-GRID will be useful

Q MH: what are other applications besides grid for PKI?
A:
- first grid in Georgia, first groups in Uzbekistan; due to the lack of contact with western science community and connectivity issues they were out
- they're interested in cooperation
- there are some things on network level...

CVH: it is good to have CERT and PKI people together from the very beginning

comment CK: they faced similar situation in 2004; things don't move with same speed in all countries/phases
JG: it would be nice to have a mother CA from this group for countries
AH:
- there is a big difference between SEE region and these countries because of their political situations - some countries might object being child to certain mother
- it is better to enforce establishing national CAS (emphasizing importance of certificates)
- there are 4 established CAs in this case (Morocco, Israel, Armenia, Ukraine), maybe they should be responsible for their regions
- problem of national legislation - when the crime is committed, who is responsible for prosecution

DG: **group in this community for monitoring activities**: **Christos Kanellopoulos, Baiba Kaskina (Latvia)**

Updates from the APGridPMA, Yoshio Tanaka (YT)

Q JJ: NAREGI has a CP template which is interesting to others

Continuous Audit Process III: HellasGrid, Christos Kanellopoulos

... discussion related to missing identity validation records ...

Continuous Audit Process IV: CyGrid, Andreas Kekkou

DG: no reviewers were assigned so far

volunteers: **Jens Jensen, Mike Helm, Christos Triantafyllidis**

comment MH: it is difficult to comment since both reviews didn't present any artefacts

... long discussion related to operation reviews / audits and its purpose and concequences ...

more volunteers for selfaudits: **David O Callaghan, Emir Imamagic**

DG: **6 months after the selfaudit there should be update of CP/CPS and after 1 year you get kicked out**

TACAR Policy updates, Licia Florio (LF)

- three representatives: Mike Helm, David Groepp & Yoshio Tanaka
- TACAR interface: (it works!), room for improvement & would like to get some requirements (example: is registering CA accredited by IGTF?)

SCS accreditation, Milan Sova

- there is not going to be accreditation this year
- provider of the service is not responsible enough to make necessary changes

comment LF: any changes of cert profile will affect all customers

EI: will it be possible to make any progress before contract with provider expires?
LF: possible, there are some things TACAR is not happy with, contract with provider expires in 2010

Authorization Working Party report, Dave Kelsey

WW: problem of accrediting VO; we should accredit certificate for VO service

- no-one generally disagree with working on this; DG: no need to change charter

- group of people volunteered to join the group

New CA presentation: SigmaNet and the Latvian CA, Baiba Kaskina

Hardi Teder (HT): Baltic Grid doesn't object

JJ: we can't say no to new user
CK: agrees with Jens; would like to see transition plan to being accredited
HT: some of the BalticGrid users have CERN certificates

reviewers: **Jens Jensen, Hardi Teder**

AEGIS CA, Dusan Radovanovic

CAOPS-WG, Christos Kanellopoulos

JJ: suggestions for CAOPS meeting:
- there should be discussion about robot certificates
- proxy certificates + service certificates...
- OpenCA
- High level certificates
- how to support renewal

people coming to Boston: DG, MH, VR, JJ, YT

Establishing a Repository of Known Good and Known Bad CP/CPS Texts, Jens Jensen

- (bad example: several CA machines being on N-th floor because of flood protection)

comment MS: provide new CAs with standard policy CP and let them define CPS
comment MS: if we accept that part will simply be written then CA won't actually define policy
... more discussion ...

- group of people volunteered to participate in activity of defining template CP/CPS

The Next Meeting in Copenhagen

- decided: May 26-28, 2008

12th EUGridPMA meeting, Day 3

Wednesday 17 January 2008
NIKHEF, Amsterdam, Netherlands

Accreditation: IR-GRID, Majid Arabgol (MA)

Q MH: CA looks finished, repository is there; what pieces are missing?
A MA: missing pieces will be implemented as soon as possible

Q IN: should they upgrade to new RFC format?
A MA: we would like to keep it
JJ: it is not required
DG: not needed

IN: CERN supports the CA at very highest level
DK: LCG too

MH: repository needs a little bit of work

Asli Zengin (AS): suggest checking compliance with AP and GCP

reviewers: Asli Zangin, Arsen Hayrapetyan

DG: **if IANA doesn't deliver OID, they can get IGTF one**

DG:
- **they don't need to do any more personal presentation for accreditation**
- **further discussion will go through email**

The CERN Grid CA and Identity in LCG: Lessons Learned, Ian Neilson

comment MH: similar problems with DN change and VOs + users
comment JJ: their problem was different, change occured only to Issuer DN, but still had problems due to the VOMS architecture
comment AW: additional problems with storage manager where DN is associated with file ownerships

Definition of the 1SCP OID Hierarchy, Milan Sova

... discussion ...

Continuous Audit Process V: SlovakGrid, Miroslav Dobrucky

... some discussion about OIDs, ...

EI: typo nonRepudation -> nonRepudiation (also in GCP)

- reviewers: Emir Imamagic

Continuous Audit Process VI: IUCC, Yan Benhammou

... discussion related to sustainability ...

CK: there are sites that don't upgrade software, is this problem?
MH:
- how is software patching managed?
- this is not addressed in IGTF audits (useful points in NIST)

Q CK: regarding identity vetting, confusing description. Is there F2F?
A: yes

DG:
- there are two reviewers: Jens Jensen, CK
- results should be presented in Kopenhagen

Status and plans of the TR-GRID CA, Asli Zengin

Status and autonomous self-audit of the ArmeSFO CA, Arsen Hayrapetyan

... discussion ...

reviewer: David O Callaghan

OID discussion

DG: adding AP OID to EE certificates

- OID should be listed after CP/CPS OID

Survey of CA implementations and software, Ursula Epting

... discussion about sw features ...

Closure

volunteers for next round of selfaudits: Poland, Ireland (2nd update)

WW: will have CA update/HSM documentation ready for the 2. meeting
RC: planning to perform self audit but cannot promise

EI: can we just submit results to the list
DG: yes

Comment AW: possible reason for dead CRL issue might be standalone user interfaces which are not updated