Notes prepared by Lauri Anton. I will still edit these as I promised Lauri, but I did not have the time yet. Will follow sometime this week, before the end of October. Sorry. DavidG.

Sept 28. 2005
EUGridPMA

Coffee

IGTF Federation Document and related messages

Comments on structure:
Tony: TagPMA will be restructured into 3 sections:
1 federation –
2 administration –
3 governance – how you decside, more legal section, voting rules etc.

David Groep: do not see practiocal reason for that

Tony: eduroam service level agreements can be used for operations, good example.
Who runs the infrastructure?

Tony: doc should contain: IGTF may create additional controlling documents as needed.
Ian:
David:
Tony: doc should contain: all the documents should be stored in repository

... plain english .. :)

DG: can we use this document
Tony: It is very mature

DavidK: is it regional or continental PMA?

Willy: .. members?

Ian: first section: asserts?
DG: --> ensures

Tony: Where is the namespace uniqueness clause
DavidK: all the namespace changes must be approved??
DG: yes

DK: announcement mailing list? do we do that?
Tony: announcements to who?
DG: as wide audience as possible
Ian: whoever wants to subscribe

DG: announcements list is outbound only

Tony: should we have OID registry?
DG: ITU can generate OID – *ugly*

Tony: we offered a branch from our OID space for IGTF.

Christos: what are the terms of using DoE OID branch
Tony: it's free; we can write a document with terms
IANA OID branch is experimental and it should not actually used for enterprises, CA-s

Willy: should we move to DoE branch of OIDs
Milan: I would like to stick with my own OID branch
DG: remain [with your OID] where you are.
Tony: so you would like the IGTF branch?
DG: yes

DK: 7. liable?
..: no liability
...: subsume?
DK: lets take sentence out and leave „unless stated otherwise...“

8. Financial responsibilities
9. Auditing
Tony: can a CA run under 2 different profiles?

... intellectual property – new section

lets take GGF Copyright notice :)

Tony: we need to add this to TagPMA and profiles also

11. compromise and disaster recovery
concerns@*PMA*
Maybe security@*PMA*

12.2 rotation of the Earth
remove the „earth rotation“ and just dictate the order.

Ian: we do not have the definitoon of „board“
DG: replaced by „PMA chairs“

--
DG: IGTF document is almost ready: asiapma approves, EUGRIDPMA approves, hopefully tagpma
On GGF we plan a small party
I made a draft press release (who will we mention)
No specific CAs are mentioned

__________IGTF press release________

Willy: should we put X.509 PKI infra?
No, too technical

DK: „Once the English sites“ --> „Once the British sites and Fermilab..“
DK: it very boring, should put better title „30,000 scientists can use grid worldwide...“

Tony: change the title „TITLE HERE“ --> DoE chair.

Anders: add NorduGrid as relaying party

When will the document published? next tuesday?

You should use mobile phone number as contact.

DG: is the gorup genereally happy with text?
Tony, DK: we need better title!

Lunch.

Jens's presentation
[-- missing a bit --]
Tony: is it about proxy?
Jens: No, about secret keyprotection

Willy: I do not like linking ID service with banking card

Jens: in many softer sciences, there is attitude, that using grid is hard and „take my cert and use"

Jens:
[-- missing a bit --]

Milan:
One Statement Certificate Policy

Coffee

Asli Zengin
Thanks to reviewers. (also to Christos for missing review :-)
[presentation]
TUBITAK-ULAKBIM

www.grid.org.tr/ca

Milan: in the EE certificate the CA:false is not good
...: it is required by Minimum Requirements 4.1.4

Jens: also the question about requests send by e-mail, as Estonia?
Asli: they should use the secure web form.

Ara: why we use the requirement „CA must issue a new 7 days before expiration"
Milan: lets discuss this tomorrow, i think it's crap

Tamas: What software do you use?
aOpenSSL commands and scripts, right now do not use packaged CA software like OpenCA; plan to write their own web interface

Javi Masa
applause for designing the logo

Ursula: What does the CN of the personal ceritificate mean?
Javi: it easier to write that way..
Ursula: I am not confident that it would not cause problems
DG: the email address is not in printableString

DG: has this configuration tested in wild?
Javi: it has tested with globus
Jens: should be tested also with browsers

Jens: it seems that there is two ways to encode the name of the person
Javi: some

Milan, etc: why there is the organization in the CN of the personal certificate?
Javi: we thought that we use DC, CN,
Javi: names can be duplicated,
Milan: but there can be two names in the same organization
Javi: but names can be written multiple ways
Milan: we are back to the pseudonym discussion in the morning. Some RPs definitely do not like the pseudonymes.

Ara: what means that the CA can request the revocation?
Willy: its for documentation of the revocation
Milan:
....
Ursula: if the CA gets to know that the key is compromised, then the CA should revoke the cert

Tony: How do you encode the CSR in XML?
Javi:
Ara: what logs do you store?
Javi: all kinds of the changes.

Milan: how can you search for the certificate from LDAP?
Javi:

Tony: how can i find rubens cerificate?
Javi: you cannot find that from LDAP, you have to use PKIrisGRID web interface.

Ara: does this XML with OpenSSL? How dows it work?

Tony: will the CP have all the namespaces, what you will sign certs for?
Javi: no
Tony: what about O?

Willy: how do you generate the keypair?
Javi: keys are generated in browser.

17:58
Ara
Short presentation of our status.

Jens: whatabout the digital signature law? will the users of the CA be legally binding?
Ara: do not now. usually the armenians are compatible with laws of other (european) countries.

DG: 8pm at Ratusz.

2nd day

Roberto Cecchini
INFN CA:
- lots of RA-s, number causes problems
- the renewals are done without te intervention of the RA
- using RT for ticketing system
- do not allow the Safari browser (do not encrypt the key?)
RA went to US and left the certificate to collegue

Milan: do you have legal connection to RAs?
RC: right now not
Milan: maybe you should have contracts with RAs
Tony: our RAs are on the board of directors (?)
Tony:
DK: do you have training
RC: we meet face-to-face, authenticate and explain the
DK: would you do auditing of the RAs?
Milan: punish one very hard for example to others
RC: often the RAs are researchers, not administrative persons. i do not want to be a policeman
----
Ursula Epting
Ursula: Are those RA-models OK?
DK: the first one is definitely OK..

Tamas: do you have contracts with RA hosting organizations?
Ursula: no, it is based on personal trust; have personal connetions couple times a year. formal contract maybe would be nice.
RC: Milan, you have the contract in preparation?
Milan: I can send it to you, butit in ceck
Milan: with such document, you can stop the service
Tony:

Lauri: relations between DFN and your CA?
Ursula: not resolved yet, maybe in a year
Anders: both CAs are getting more RAs. the one with more RAs wins ;-)
Tony: i do not see big problems with multiple CAs within country
Ursula: inside country there will not be big problems, because we can divide the userbase (HEP, others). the problem will be here (in EUGridPMA)

Sajjad Asghar
PK-Grid
OK :)

Jules Wolfrat
UNICRE Security

technologies deployes
- batch system
- global file system GPFS, dedicated network 1Gbps, want to upgrade to 10Gbps
- AFS, if GPFS is not available
- UNICORE for uniform submission
UNICORE

DEISA is really deploying the middleware, we do not develope

UNICORE architecture
Client -> Gateway -> NJS -> UUDB (gridmapfile of Globus)

UNICORE Security
keypair is saved in password-protected keystore in client machine

Milan: what if the certificate is changed?
Jules: excactly, we have insisted that they use only DN in UUDB

Ian: does it allow multiple mappings on DN?
Jules: every site has the UUDB. we have LDAP service for distributing user information into UUDBs.

Jules: we have to have same users and groups for every users because of GPFS user rights
DK: are the users real persons or institutions?
Jules: real persons only
Jules: all the communications and AJOs are encrypted; we plan to have gridftp for large file transfers

Ian: how far this kind of architecture wold scale?
Jules: problems are with administering of users

Jules: we have DEISA primer to describe of the configuration of the client

Ian: how many users do you have?
Jules: number of ten's

Mic: middlewares need lots of open ports
Bob: is there coordination between EGEE and ..?
DG, Mic: i think there is coordination

Mic: UNICORE is starting to do proxies because of interoperability initiative between Globus and UNICORE

Coffee

Kyruacos Neocleous
CyGridCA
web site has changed
CPCPS has new version
new root cert was issued – they use new alias CyGridCA; validity for 3 years
Current status: 5 user, 7host certs
one RA, additional RA planned
plans: updates to cpcps, create RA web application,

DG:
Namespace constraints expression
Lets change the format of the namespace constraints
Only globus uses signing_policy file, no other middleware uses that
when tried to define signing_policy for Switch CA, got some problems
middleware cannot handle c=ch/ O=!cern system

Can we come up with more requirements

Anders: why we do it is because we now authenticate based on DN only
Robert Cowles: CA to gridmap file?
[missing a bit]
Rob:
DG: Namespace will be unique
DG: We do not reassing the namespace from one CA to another
Rob: namespace constraints apply on

Milan: lots of problems would disappear if the software would allow longer paths (now EE -> CA)

DG: we guarantee that DNs are unique

Tony:
DG: the document is for middleware developers
DK:

Rob: what about Christos note about SEE-GRID
thats irrelevant because SEE-GRID

Milan: DN is format, subjest is the instance

should be plossible to send cert along with job. ..(?)

DK: doest it allow to have two overlapping namespaces?
DG: no

DG: does anybody agree that we need signing policy file?
Yeah

3. it must be possible to support the concept of “subordinate” issuers in a hierarchical chain of issuers, such that a single namespace constraints policy collection (file) support the expression of namespace constraints on any subordinate issuer.

Ursula: is this the case of the CNRS?
DG: no, CRNS is hierachical, their subCAs do not appera and disappear every month

4. the string rendering identifier naming of directoryNames and X.500 distinguished names in the policy expression must comply with RFC2253
-- Order of the components

5. the format must be human readable, in order for relying parties to visibly inspect and assess the namespace constraint policy
human-readable, no XML please :)

6. the policy expression must support Unix-shell glob style wildcard pattern matching. Wildcard matching must be possible anywhere in the pattern.
Tony: what is UNIX glob?
GB: *,?,“ ..;

7. it must be possible to explicitly set a namespace constraints policy for a subordinate issuer, without modifying the policy collection (file) for the up-stream issuer(s). Such a policy on a subordinate issuer must override any policy defined in up-stream policy collections (files).

8. a subordinate authority trust anchor must be able to change (i.e. a subordinate could be compromised and re-keyed) without having to change the namespace constraints policy in any end-system configuration.

Tony: do we have a market for subCAs?
DG: yes. universities, others. now we have working OCSP, now we can do this

Milan: hierarchies?

DG: for example, Nordugrid has 2 O-s (asn1parse)
Swiss has reversed order of components. and in some renderings those components are reordered.
Milan: swiss use email for identifying persons with same names
DG: we have to define the ordering of the components

Deny's will generate a mess

SubCAs namespace files can be found by moveing up by chain

should it be: sequential or DENY over PERMIT?
seems to be that it will be _sequential_

do not allow ANDs, only lists

Milan: such languages should have language versions.

emty file is total deny, if no file, then software does not care

DO'C: comments

Minimum requiremets topics

Tony: CRLv2, how we mix with CRLv1
Willy: HSM migration?
Willy: Should we move to RFC3280 for CP/CPSs.
Ian: pseudonymity
DO'C: certificates on cloned machines
Ian: CRL service levels
Tony: service levels agreements in general?
NAY:-)
...: how CSR should delivered to CA?

DG: topics, which need changes to MinReq
server extensions, certificate profiles
CRL issuance frequency
Pseudonymity

Discussion part:
HSMs

Jens? OK in hotel

Lunch

Minimum requirements

long term -> 10 miljon seconds

DK: 10 miljon is 110 days, should be 1 miljon seconds

Milan: should CA have self-signed cert?
DG: no

Ara: the line „CA should handle... revocations _when necessary_" should be removed.
DG: should leave like it is, textual issue, does not harm

Tony: should we have dossier(?)

Tony: _PKI CA_ must define....
Jules: CA must not run the PKI by default – was problem in Germany. don't mind

Szabolcs: problem with CSR delivery. The procedure should be documented

Milan:

Tony: how to validate to CSR?
Tony: use the secret key to unpack the cerificate

Milan: in your system, the csr is generated in browser?
Tony: yes
Milan: then you got

Christos: when new user asks for the certificate, I do not see the point of SSL encryption

--- tirrrr ----
CA is responsible for the archival of the RA operations
Tony:
Jules: what do you do with the passport number?
Its useful when the policeman shows up and asks for user.

[missing a bit]

Tony: FIPS 140-1 --> FIPS 140-2
Tony: private key protection --> HSMs use short pins, certificates to activate secret key

[missing a bit]

DO'C: if two host share the name, are those different EE or not?
Milan:

Milan:
Ursula: you have to revoke the old and then issue new one, because (OpenSSL) does not oherwise
....: no, its bad software

DG: In the federation document, the EE must be defined.

Roberto Ceccini: Certificates must not be shared among EE-s ---> moved to right place

DG: CRL version --> no stipulation
CRL must be compliant with RFC3280 and v1 or v2.

[missing a bt]

extensions

pseudonym
Ian: the CN should contain close resembling of the name presented on the photo-id

Pawel: could not get openssl with pseudonym
Willy, Milan: use OID and define it by yourself

DG: is RelayingParty happy with this statement?
DK: do not want to see pseudonyms in LHC VO

Willy: i read the RFC ....

DG: okei with pseudonyms.
Christos: I do not agree.

okei, now it is „CN should contain the name“

CRLs –
Pakistan had network breakdown for 10 days
Should stay as it is.

----- Publication and Repository responsibilities -----

---- Privacy and confidentiality ----

--- Termination ---

New CP/CPS's should be structured as defined in RFC 3647.

Tea

Jan Jona Javorsek
Nagios
http://signet-ca.ijs.si/nagios/
... what about multiple distributions etc..

discussion items
CRL validity
CA root certificate validity year + 3 month(15 month)

DG: ...
...
[missing a bit :-]

Jules: Look at the TACAR for information
Anders: the key distribution mechanism is missing
Jules: currently we have to repackage DG's packages
DG: maybe need more alternative packagings
Anders: versioning
DG: have to discuss this with other PMAs
DG: all PMA should have version numbers and version numbers are monolithicly increasing

Jan: how to set up the contact with CAs?
DG: will add contact emails to distribution lists
DG: maybe we shoul have <hash>.info fails instead of file explosion in directory
DG: I will put at least email contact address to <hash>.info

Jan: will send email to contact address with request, where you will be asked to specify the warnings address?
Yes

-- - --
DG: need write a document about descisions
who volunteers?

-- - --
Tony
Eduroam

Grid eduroam Experiment
EAP/TLS

IGTF does not have same comparable service -- ?

Is there interest to join eduroam as IGTF?

Tony: I may put together the pilot. Do you think I should do it?
Tony: they are doing the authorization federation, they could use us as the authentication federation.
Tony: lets discuss it ahead on the list

- - - - - - - - - - - - - -
3rd day
Willy
HSM
What are the reccomendations for moveing to HSM?

Milan: common-sense requirements only --> machine has to be protected by firewall

Willy: it will be protected by FW, allowed connections only to some worknodes
DG: (one system) had connection via serial link
Milan: simplest system: internet --> FW --> WWW machine --> (FW) --> HSM machine->HSM
DG: Log all the traffic going into HSM machine?
Willy: has only local address

Jens: the network cable can be tweaked so that it can transfer data only _out_ of the HSM machine.

DG: lets write down something about (HSMs)

Willy: hope to see you all in January in Vienna. Weather will be cool to cold :-) Flighs to Bratislava may be much cheaper. On tuesday, guided tour by Willy :-) 24.th

- - - - -
Next meeting
Tamas: maybe we can host the meeting in May

Willy: addition to yesterdays last presentation: Austria is joining to the eduroam soon
- - - - - - - - -
Milan
OCSP

OCSP servers should be in certificates you want to be checked by OCSP.

Experimental OCSP policy

(free software is not working... :-)

4.5.2.
4.10.1 Operational characteristics
at least 2 responders

Milan: CRL used by OCSP should not be older than 30 minutes.
Willy: What if the CRL expires?
Willy: should the CRL be the same as written in the certificate
Milan: no

Milan: 6.1.1 key pair generation --> HSM
OCSP keys should be really short-lived (couple hours)

Key must be not backed up or archived – idea: if you lost the responders key, just generate a new one

6.2.7
6.3.2 cert should not be valid for more than one week
6.5.1 dedicated machine, may be shared with online-CA

7.1.2.1 values in EE certificates
7.1.2.2 OCSP responder certificate
7.3 OCSP profile – based on RFC2560

Anders: what are the operational recomendations, when the OCSP responder is down.
Milan:
Willy: it has been defined in RFC: if no answer from OCSP -> then use CRL

Milan: Client --> OCSP (in local machine?) –> OCSP then CRL
Milan: written in collaboration with.... (?)
Willy: Timestamping is needed.

- - - - - - - -
Coffee
- - - - - -
(Some are leaving.)

What should we tell to middleware developers?
Milan: SCS status. Today the tender ends. Will read those tomorrow.
At the end of the next month, will know if the service is usable for grid. Maybe the CA comes here on some next meeting.
Ian: Signing policy is going to overlap?
Milan: no
DG: maybe we can get rid of issuing host certificates :)

Ursula: 2006 sept in Karlsruhe
Asli: 2007 in Turkey?

Jens: certificate suspension and OCSP?
Jens: audited 5 of 50 RAs. some issues. CAs should audit RAs sometimes.

DG: should we use wiki and collect the knowledge from the group
Yes

Jens:

Ian: cold feeling about „should“ in CN in MinReq
Ian: would like the MUST. I deffer
Milan: same names, have to be differentiated

DG: no issues left
Thanks to Pawel

DONE.