9th EUGridPMA meeting, Day 1

Monday 15 January 2007
Coseners House, Abingdon, Oxfordshire, UK

- Milan Sova (MS): PGP signing key - public keys will be sent to its email that will print & prepare them

Introduction, minutes last meeting, agenda bashing, David Groep

Members and applicants
  23/25 EU member states accepted (MT & LU missing)

eugridpma
  Since Mar01 linear growth
  classic
  38 accredited
  4 applicants
  slcs:
  0 accredited
  1 applicant

tagpma
  active:
    doegrids, gridcanada, brgrid
  recently passed:
    eela catch all
    tacc root and classic
    reuna (chile)
  voted on by email:
    Venezuela & Mexico

apgridpma - Tanaka will give status later...

Round-table brief updates

- CERN - no update on old
    more then 300 certificates issued
    small changes to cp/cps
- Russia - phasing out, more then 300 certs,
    - some new registration authorities
- Slovakia - only 206 certificates (84 are valid)
- Greece - statistics on certificates

- INFN ca - 2000 valid certificates,
    - they issued new CA certificate 10 years validity
    - EUMedgrid EUIndia grid, EUChina grid - after couple of proposals - they became catch-all for EUMedGrid & EUIndia grid
    EU Medgrid - www.eumedgrid.org/
    EUIndia - 3 RAs, no certificate issued -
- Estonia - 350 certificates
- doegrids - no statistics, around 4000 valid certificates,
    - personnel change, Tony Genovese is not working anymore
    - Bob is acting chair person of DOEGrid PMA, looking for officers (meeting in February)
    - DOEGrids are alienated from CA process - new chair would participate in PMA meeting
    - OSG is 80% of certificates
- Croatia - 50 certificate issued
- Spain - 361 certificates, less then 1 year old
- Czech Republic - getting smaller, trying to move everything to other services because they provide services for whole community
    - they got hardware and software - MS will give a talk about details on special session
- SWITCH - no exact statistics,
    - at the end of October they got certified by Swiss (look at web),
    - they'll change key hierarchy to G2 hierarchy,
    - slight modification of CP/CPS because of hierarchy changes - it will be implemented in February
    - SLCS - more details on tomorrow talk
- Portugal - tomorrow
- Germany - new CP/CPS that allow them to run online CA
    - 320 users and 234 server certificates, 40 RAs
- Ireland - over 500 certificates issued
    - planning to upgrade CA software
- Hungary - 300 certificates still valid
    - plan to slightly modify CP/CPS this year (some simplifications
- eScience - few thousands certificates,
    - planning to introduce robot certificates (complicated requirements)
    - training certificates for ?NGS? issued by additional CA
- Dutch - 350 certificates (relatively constant number)
    - Surfnet AAI integration plans - hopefully this year new CA and CP/CPS will be established

Number of certificates small discussion:
- seems that number of user certificates is constant/ doegrids had problems with issuing huge number of certificates for worker nodes
- what will happen when UI nodes start asking for certificates - David Groep (DG): hopefully user's will use user certificates for this

New CA: BG.ACAD, Luchesar Iliev

- changes from the meeting in Karlsruhe
- changes:
  - changes to the CP/CPS
  - operational status of the CA
- CP/CPS change:
  - commonName redefined
  - user 1. version:
    name, last name and initial of father's name followed by period
    problems: period confusing to user's, names are written in Cyrillic, what is father name?
  - user now:
    full name from the document in latin letters
    letters transliterated properly
    if there are three or more part of the names, middle one(s) can be abbreviated without period
    non distinct part separated by hyphens must be written in their completeness
  - for multiple DNs for same user distinctive numbers will be added (e.g. serial number)
  - if user requires email in DN, it will be added as subjectAlternetiveName and not DN
  - host certificates - FQDN must be part of DN - printable string, internationalized FQDN are not approved
- Certificate application process
  - key-pair must be generated by the subscriber
  - the key must be at least 2048
  - private key must be protected by secure passphrase
- Identity verification:
  - face-to-face with RA
  - government-issued ID (not stated in CP/CPS, but: ID card, and/or driver, and/or passport)
  - email is verified with email ping
  - subscriber must prove that it is eligible
  - for host or service
    - posses a valid user certificate or
    - possess a trusted PGP key (signed by BG.ACAD CA or at least two of its current staff members)
    - go through the procedure from the previous slide
  - after successful authentication signs an explicit statement
- RA assigns a 25-character random code to the request
- supplies it to CA ...
- Submission
    - encrypted email or
    - SSL protected web interface
    (in both cases random code is required)
- EE profile:
  - basicConstraints [critical]: CA:false
  - keyUsage [critical]: digitalSignature, keyEnciphrement (other can be included, except
  - extendedKeyUsage: serverAuth, clientAuth

- DN starts with "DC=bg, DC=acad" (new from Karlsruhe), followed by O=class (people|host|service), followed by O=affiliation, CN=
- Re-key request must include the same signed statement (new from Karlsruhe)
- CA can reject the request or postpone its if the overlap of the new and the old would be unjustified
- CRL issued only in v2 format
- CA root certificate:
  - minimum validity is 3 years, maximum validity is 20 years
  - SHA1 message digest
  - DN: "DC=bg, DC=acad, CN=BG.ACAD CA"
  - key length 2048
  - protected by a passphrase at least 30 characters (changed at least twice a year)

- Operational development:
  - single CA at IPP-BAS, no subordinate
  - the RAs: Sofia and Plovdiv
  - url: **www.ca.acad.bg**
  - three access stages:
    - the admission desk at the entrance
    - entranced to CS (RFID controlled lock, video surveillance)
    - cell where CA operates
  - machine:
    - hard disks are locked in strongbox between uses
    - BSD
    - not connected to network
    - using basic openssl
  - technical facilities:
    - double protected power supply
    - fire protection

Discussion:

MS:

Q CN for the host and service certificates should contain only FQDN, service must contain service name

A this was skipped on slide but its in

Q authentication by the PGP - just saying that applicant's key must be sign by staff members is not enough because PGP does not have CP/CPS behinds it

A PGP key could be signed by CA only

Jens Jensen (JJ):

Q PGP key - problem of the PGP key name because PGP key name doesn't have strong form

A it is used only for authentication in case of host/service certificates and it is signed by CA

Q most of the people are happy for EE to have 1024, why 2048?

A in time 1024 will be broken and they would like to avoid re-issuing all certificates

JJ: 2048 makes thing slower and cert is valid an year only

Q why CN 7-ASCII and not printableString?

A CN will be printableString
Q having period in CN is not problem,

Michael Helm (MH):
Q if you are running PGP certification authority you can put stamps in signatures? PGP keys are difficult to rekey
A they will consider this
Reimer Karlsen-Masur (RKM):
Q what happens with token (25-char one) that subscriber gets
A it is verified by RA and used to connect request to user

DG: **new version should be sent and reviewers have two weeks to give their final comments**

New CA introduction: Morocco, Nabil Talhaoui

CNRST (National Center for Scientific and Technical Research)
... (activity list) ...
Connected to GEANT 152MB/s
Moroccan grid infrastructure MaGrid
- 1 cluster per university
- currently have 2 clusters (28 CPUs), planning to grow to 14 sites (400 CPUs) til 2008

EumedGrid project - Mediterranean Region - first non-eu country in it

Single CA for academic research and educational activities
URL: **www.magrid.ma/ca**
participants: CA, RA (univ or institutes), subscribers
CA certificate:
- C=MA, O=MaGrid, CN=MaGrid CA
- self signed
- valid for 5 years
- key length 2048
- passphrase changed every 2 months

EE certificate:
- all available at web site
- C=MA, O=MaGrid, OU=Organization,CN=Name
- keylegth 1024 or 2048
- at least 15 chars passphrase

Requesting:
- S generates key pair and csr with openssl
- submits via webform or email
- ra authenticates and forwards to CA
- CA signs it

Re-key
- procedure is simplified if previous key is valid, otherwise is the same as initial

Revocation request (CA, RA, or any entity holding evidence)

- by email
- by physical presence

CRL
- at least 7 days before expiration and immediately after revocation

Security Controls
- CA:
  - dedicated offline machine in secure environment
- RA:
  - protected by firewall with recorded traffic to it

Repository
- see URL above

Current status
- CP/CPS draft is delivered
- web repository is operational
- signing machine is installed

Discussion:

JJ:

Q how do you check that request came from particular user (OpenCA PIN-like feature)?

A they are planning to use OpenCA

Q why do you change CA key passphrase so often? it is harder to remember it or you have to keep a piece of paper with it

A they are in the test phase now

additional comment from ??: there is no value in changing passphrase, you should do this only when you change personnel

BG: if you change it you increase possible leaks (human errors)

DG: **assigned three reviewers: Jens Jensen, Emir Imamagic and David O'Callaghan (DC)**

Russian DataGrid CA Final Report and RDIG updates, Lev Shamardin

History

It was set up during participation in EU DataGrid

Approved in August 2001

Updated in 2004
- new root key

Decided to replace with RDIG CA with 2005
- broader range of projects
- change of funding of grid activities

Russian Datagrid CA
- approved in May 2005
- not issuing since October 2005
- shutting down - keeping logs til 2009
- currently termination procedure
- not in the latest distribution (1.11)

DG: Russian Datagrid is not obsolete so it is basically still used

LS: problem is that they have to reissue CRLs each month, MH: why not put longer validity period.
LS: they will change validity period and CP/CPS

Update Review: SlovakGrid, Miroslav Dobrucky

IISAS-Grid projects:
- MEDIgRID, Int.eu.grid, DEGREE, L-Wf Grid, EGEE, GILDA
- CA - trying to get national support (using institute or project funding)

Slovak CA
- running 4 years and two months
- based on openssl and custom made scripts
- root expires in December 2007
  - they decided to refresh and not re-key
- 3 RA (Bratislava, Kosice and one in the middle)
  - each applicant should travel less then 200km
- statistics
  - issued 206 certificates
  - valid only 86: 45 user, 39 host
  - revoked 14: 5 user, 9 host
- root CA certificates
  - 2048 bits long
  - will be rekey before 2010
- EE certificates
  - 1024 bits long
  - C=SK, O=SlovakGrid, O=organization, CN=user
  - C=SK, O=SlovakGrid, O=organization, [OU=organization], CN=host/FQDN
  - host can be replaced by service
- ...(Procedure defined in details)...
- new CP/CPS
  - January 2007
  - changes:
    - MD5 -> SHA1
    - validity EE extended with one month
  - minor changes:
    - revoking within 1 day
    - compromise & disaster policy will be included (Q: are there some templates? DG: it seems not)
    - CA private key separate from passphrase
    - policy and data release policy will be included
    - add "user may ask for additional certificate with other DN"
    - add "rekey without F2F at most 5 years"

- Q: 5*(1year + 1month) or 5 years?
- A: JJ: 5 years or 4 rekeying
- Q: how should be OID included in CA and EE certs?
- A:
- Q: should we translate CP/CPS to Slovak language?
- A: JJ: if you do translate you have to say which one is the main! otherwise just translate parts
- Q: may we sign CP/CPS document by CAcert or EEcert?
- A: MS: should not be signed by CAcert.
- Q: should we have LDAP repository?
- A: MS & MH & someone else use it, but majority dont
- Q: what if two users from the same org appear?
- A: add something at the end to make the 2. unite

JJ:

Q: does new certificate has the same serial?
A: yes
Q: Slovak citizens only?
A: it is not stated like that in CP/CPS but it has to work at SlovakGrid organization
Q: firm peronal acq? how do you have a proof (e.g. copy of ID)
A: they don't keep copies of IDs anyway
(DG: DutchGrid CA keeps ID number only)

MH: Problem - different kind of assurance? (this will be further discussed on Wednesday)

9th EUGridPMA meeting, Day 2

Tuesday 16 January 2007
RAL, Abingdon, Oxfordshire, UK

LCG Relying party requirements, David Kelsey

LCG/EGEE policy - accept all IGTF accredited CAs
...(description of LHC & LCG) ...
Requirements
- LCG/EGEE endorse the req expressed by OSG (March 2005)
- additions:
  - naming - EE certificate MUST contain CN in DN and MUST contain actual name of the end-entity
  - identity vetting:
    - the DN assigned to person must be unique.
    - DN assigned to a certain will not be reissued during the lifetime of CA
    - How the CA atest to validity of identity
- RA SHOULD contact subscriber F2F
- if F2F is not possible than CP/CPS MUST:
  - how the CA provides accountability, showing that they have verified enough identity information to get back to physical person any time during the lifetime of the certificate.

IN: why does this definition explicitly applies only when F2F is not possible?
...(didn't catch the answer)...
MH: is this req similar to Thawte notarization (where documents need to be held for 5 years)? does this mean that RA MUST hold copies of documents?
David Kelsey (DK): req is traceability - you have to have a way to trace back to an actual person
DG: how many CAs do keep copies of ID information?
A: about half of CA does and other don't
MS/Robert Cowles (BC): how are you sure that it is the same person when you reneq/rekey the certificate? (for the ppl not storing the info) how do you trace it back?
RKM: it is possible to trace the user by the name
MH: our rule is that if the email address fails EE is not entitled to have the certificate. you want to have something recorder that would enable law enforcement to trace the person...
JJ: I have the copy of ID, if it's held by the institute that could not be accessible to me?
IN: but it is accessible to the law enforcement
DG: it is a good thing to record something because of the renewal? why don't ppl store personal information?
IE: we have string relationship with institute and it is difficult to store personal information so we rely on institute identity data.
MH: same thing is with doegrids
JJ: RAs are keeping copies/ if the RA shut down contract binds them to keep a data for 3 years and then destroys it
DC: should we as IN said make this second req apply to F2F case?

MH: F2F is needless, the context and combination is more important.
The most important part is the requirement to record the data. Should we make this a MUST both all cases?
DG: you have to provide accountability and the renewal.
MH: what's the value of F2F in this context currently?
IN: it is little more difficult than e.g. just sending the email, like you said it is a context
MH: that still doesn't meet the accountability req. e.g. in Cal. there are three MH
DG: should we trust institute issued IDs it is probably good enough?
BC: but that doesn't have to be an employee, e.g. guest?
DK: if the information is good enough for institute or company it should be good for us.
MH: we are not sure that each institute has the same quality of ID
JJ: there is a timing problem - how long does institute keeps the information after the person leaves?
BC: how do you perform a catch-all and meet this requirement?

...(discussion about experimental & training CA)...

RKM: assurance level will be correlated to profiles?
DG: classic Lite profile - rudimental profile with lower identity valid
MH: similar to mozilla foundation - different root for various assurance levels and purposes (e.g. personal, service, etc.)
MH: having different OID will probably not work correctly with existing middleware. it should be done with several root certificates

DG: this will be further discussed on Wednesday LoA

New CA: SWITCH aai, Christoph Witzig

Shibboleth explanation
Replace classic certificate with SLCS one
Hardware:
- frontend - Apache server (DMZ)
  apache with shibboleth module
- SLCS Server (SWITCH Internal network)
  Debian OS ,java tomcat mysql, has only necessary webapp services
- Online SLCS CA (dedicated internal network) with HSM
  Windows MSCS,

Q
MS: protocols?
A: some Tomcat stuff between, both side https auth between SLCS and online CA

For the user:
- from the command line invisible
For the RA:
- can enable or disable individual users

- can obtain log information

SWITCH:

- operates the service
- strict access control
- operates also a second test CA

Q

MS: how does RA enables users to get certificate

A: RA uses admin tool for enabling users or groups to get certificate directly on SLCS server, this is basically authorization information

Registration:

- detailed description...

VHO

- virtual home organization - for users that don't have IdP or a home institution is not member of SWITCHaai

How good is and SWITCHaai account

- funding for the universities by the federal gov
- uniq guaranteed by Matrikelnummer

What resources are being accessed with SWITCHaai account

CP/CPS Highlights

- for memeber of an IdP institute:
  - DC=ch, DC=switch, DC=slcs, O=legal name/CN=firstname lastname uniqueId
- for a member of VHO:
  - DC=ch, DC=switch, DC=slcs, O=virtual home org(fixed string)/CN=firstname lastname uniqueId

Initial Identity validation

- Requester must contact RA
- RA enables access if:
  - user has valid AAI account
  - a set of conditions are fulfilled:
    1. issuance of an identity card
    2. has one-to-one mapping to human resource data
    3. F2F meeting with RA
- requester can access SLCS

Q:

MH: is this any different from MICS requirement?

A: two differences: they decided to go with SLCS because MICS might still change and could cause loss of time

eventually they might switch to MICS

MH: when the RA enables user in SLCS is it permanent?

A: yes, but it can be deleted. Also if his account is deleted he cannot get a certificate.

BC: what if someone stops getting salary (related to 2.). how do you check this attribute?

A: RA has to guarantee that requirement and RA should be able to see this attribute.

also this flag is set in IdP and it is checked dynamically each time certificate is issued

DC: what about F2F?
A: information - unique ID is stored in SLCS

BC: is the certificate the same for each of three conditions?
A: yes

JJ: how does a diagram look like for VHO?
A: there is additional IdP ran by SWITCH

...(MH comments I didn't catch)...
MH: some defects in SLCS profile - it was designed for single site and not distributed aai
also there are some obsolete expressions

MH: document doesn't describe signing certificate of SLCS certificate itself.
Root ca should be described somewhere
JJ: it was in the latest update
DG: Subject name of SLCS CA is missing, 2 times issuing name. It should be in the certificate profile section

DG: **apply the latest updates and send around/ after that 2 weeks period for reviewers**
JJ: reviewers need to see CA certificate which is not going to be available until the end of January
CW: this depends on HSM
JJ: two weeks should start after it becomes operational

Update Review: LIP (Portugal), Nuno Dias

history & information about CA
- using OpenCA
- 10 RAs (6 universities & 4 institutes)
- 175 issued - 96 valid certificates, 44 revoked certificates
- future: more CAs

Q
JJ: if you're not happy with OpenCA, what would you use?
A: nothing special at this moment
JJ: what is the problem of OpenCA?
A: split is not very good, changes are demanded for RA operators
JJ: you plan to extend the lifetime and you should keep a serial number because the have auth hash
AW: status of OpenCA?
MV: OpenXPKI (http://www.openca.info/) - complete rewrite the code, released sometime this year
RKM: there was a presentation on CCC kongres in Berlin and slides should be there
http://events.ccc.de/congress/2006/Home
http://events.ccc.de/congress/2006/Fahrplan/events/1596.en.html

Grid Certificate Profile, David Groep

- it is split in 2 parts - CA certificates and EE
- changes to section 2.4.6 to be in accordance to RFC

...(discussion)...

JJ: should we consider Mozilla and Microsoft in this document because most of the users use browsers to access portals?
MS: we should omit nameConstraint in order to avoid problems with any software
MH: the piece of comment 14: "therefore should be avoided in CA certificates..." should be transferred to the section itself

DG: **everyone should look through the document and send comments...**

9th EUGridPMA meeting, Day 3

Wednesday 17 January 2007
Coseners House, Abingdon, Oxfordshire, UK

RomanianGRID CA Status, Cosmin Nistor

Romanian Space Agency (ROSA)

Hardware
Naming
 - CN=firstname.lastname
Authentication
 - natural person: contact personally RA with photo ID or passport
Service
Identification
...
Q
MS: personal certificate has ".", why? can be confused with a hostname
A: it will be dropped because of the confusion with FQDN in service certificates

??: regarding revocation - any entity providing proof can revoke a certificate? is it done through RA?
A: anyone can request revocation?

Signing policy discussion

subordinate CA issue?

DG: Signing policy file - should we say that it is only about a namespace?
 If a client sends subordinate nonaccredited CA it will

IN: if sites want to allow subordinate CAs can do that themselves
DG: it is not easy to modify signing policy
BC: which means that ppl that know what are they doing will be able to do that?
Christos Triantafyllidis (CT) - the namespace will be different?
DG: client could complete a trust change by sending intermediate certificate

MS: if we have 2 subordinate CA signed by the same root they have to have distinguished namespaces?
JJ&DG: yes

DG: we can restrict a namespace of root CA

MH: root CA can create subject issuer no1 that can have its own namespace that can be different
DG: with signing policy we can restrict namespace
MH: only accredited CA should be in signing policy

MH: in the globus - java part doesn't address signing policy at all
DG: it is registered bug (a year ago)

MH: you had to list all trust anchors - otherwise middleware won't work
DG: that's still true

JJ: suggests that we have open signing policy for high level CA and then you enforce it on subordinate policies

MH & DG: we have responsibility for signing policy since we distribute it

DG: HellasGrid should be reviewed and check the root certificate

New CA: AEGIS, Dusan Radovanovic

Dusan Radovanovic (DR): implemented comments from Christos and will send him in few minutes. Then they will send it to Dobrisa and Arsen

DG: final presentation will be in Turkey

SCS, Milan Sova

Server Certificate Service
Project "pop-up free" server certificates
GlobalSign
8 founders and later on 3 new ones joined
C=BE, O=Cybertrust, OU=Educational CA, CN=Cynertrust Educational CA

Issuing procedure
- administrative contact nomination
  - paper, signed by representative of an organization
    - this person is responsible for signing CSR for this org
- host admin posts a CSR
- the administrative contact approved the CSR
  - S/MIME, signed fax, signed email
- The RA cross-checks the CSR and approves it

Q
MH: there is a lot of admins here?
MS: 1. person talking for the organization - kind of an RA at the organization,

but not from the Globalsign perspective, (covered by special contract between NREN and organizations)
2. host administrator and
3. RA - only NREN (defined by special contracts between NREN and GlobalSign, trained by GlobalSign)

IN: what kind of things administrative contact check
MS: binding between requestor and service, that is something that NREN can check from their level, they also check the domain, NREN also
Yoshio Tanaka (YT): which key is used for signing email? (step 3)
GlobalSign defines which CAs can be used (CESNET and SWITCH are fine)

SuerServerTLS mailserver
- no namespace definitions
- lifetimes: 1, 2 or 3 years

GridServer Profile - draft
- profile that they would like to accredit soon
- naming: dc=org, dc=terena, dc=scs, c=CC, o=orgname, cn=host
- lifetime: 13 month (if Globalsign doesn't accept they will stick with 12 months)
- keyUsage,
- subjectAltName dNSName: FQDN,
- Certificate Policies
  - Policy OID?

Roberto Cecchini (RC): what's the purpose of using this certificates?
MS: speaking not only for CESNET: we started CAs for all purposes and I would like to move everything to GlobalSigns
CW: it is natural to use GlobalSign in grid community because NRENs will use it extensively.
it is cheaper to use GlobalSign
DG: if you have SLCS and this we can get rid of long term certificates

RC: does it cover service certificate?
MS: GlobalSign doesn't see a problem with service extension

MH: does this profile cover all usages?

Emanouil Atanassov (EA): is it allowed to ask any service name
JJ: we restrict this with list of services. it shouldn't be in a policy
MS: we can leave this opened and define it locally like

MH: what does a trust chain looks like? is this a root CA?
MS: there are two CAs above SCS root CA. from the signing policy point of view "dc=org,dc=terena,..." would be the namespace
MH: how does this work with a signing policy discussion we had before?
MS: if we use prefixes we can be assure uniqueness
MH: but still we will need to review 2 root CAs

DG: we will do it in a same way as we did for SWITCH CA

RC: what if GlobalSign defines to rise a price?
MS: there will be new negotiation year before 3 years expire
CW: there is a threat for them to loose a lot of customers
RC: but you cannot count on really low prices

MS: **profile agreed with GlobalSign will be presented in Turkey or in worst case in autumn**...

RKM: what happens when commercial company wants to join grid, how do they get service certificate?
MS: commercial grid won't get service certificates (CESNET won't issue them also).
they can get it if they collaborate with some institute. Globalsign agrees with this...

TACAR updates, David Groepp

TACAR aims
- trusted and centralized place for root certificates
- not meant for policy validation
  - no minimum policy or technical requirements
  - but CAs can be grouped (i.e. by IGTF AuthN profile)

TACAR role for IGTF
- authentic source

Getting into it
- has been perceived as "too slow" or "impractical" and "difficult" and "too much work"

Paperwork required
- CD-ROM with bunch of data (see www.tacar.org)

New in 1.4.3 trusted introducer (TI)
- formerly had to be done with a TERENAA Officer
- now you can do that with the TI (who has to do paper work)

Implementation
- latest draft Nov 2006
- with EUGridPMA acceptance almost
- everyone should join until then
- hopefully will be accepted on next meeting in Florence

MH: how is TACAR different from EUGridPMA.
sees convergence, because currently we don't have institutional checking
is being TACAR member mandatory?
DG: I would like to make it MUST because it is easier...
MS: and it is easier for users as well

DG: comments on policy?
MS: is TI defined?

David was appointed as TI for EUGridPMA.

RKM: can David introduce MH as TI for TAGPMA
DG: MH can be meeting with Licia on next

RKM: is there a formal process for making TI? it should be some form for this?
DG: currently there is no, you should ask Licia to do that

SLCS, MICS profiles

SLCS profile comments by MH

MH: one of the problems is that identity has to be based on site's local identity management system. this doesn't fit for federated IdM shibboleth like SWITCH.
...

- agreed to review MICS and then copy changes back to SLCS since MICS is newer...

MICS profile

DG: should the part with SHOULD in section 1 of classic AP be copied to MICS?
SWITCH: it should be the same

- section with SHOULD in section 1 of classic AP was copied to MICS

- 2. section part "and is not ... end-entity", 1. paragraph deleted.

- 2. section, 3. paragraph
SWITCH: in how many details do you have put about the Identity management.
In case of federation do you need to describe for individual organization
MS: does federation has this profiles documented?

- 3. section:
MH: registration doesn't ensure anything so part "To ensure" should be dropped out
...
JJ: how can organization group be DN owner
DG: multiple system administrators
JJ: it is still traced back to a single individual
...
MH: registered owner description - DOEGrids concept to manage cases when single host has multiple certificates owned by different persons and it is not needed in SLCS since it mainly covers users. It should be in classic probably...

registered owner was dropped along with other redundant expressions

- 3.1. section

registered owner is present here so it was re-introduced in section 3.
we go back to section 3. to clarify registration
 - validation defines as binding between EE, registered owner and Subject DN

- 3.2. section

... revocation discussion ...

- 4. section

... technical requirements discussion

- 5. section

... more discussion ...

DG: **he will circulate modified version around ...**

EA: can there be a list of definitions somewhere so that definitions be the same?
DG: there should be a sort of glossary, we currently don't have one we should go through the profiles and see what needs to be defined

Host Certificates and the Meaning of Life, Michael Helm

SAM service Host Certs

SAM - essentially a for of GridFTP app moving data sets for various projects
  - physicists enjoy using it
SAM service
 - names are important
 - sam services are well controlled
 - someone at your site did sign up for this
 - need a dispute resolution
 - it's more trustworthy to organize certification around pre-existing domains

VOMS AA's

accountability - terminates at Grid ID CA
CA identifies hosts or services, we don't identify AA's
how to distribute ID's to AA's
what mechanisms exist to persuade people
low amount of care

is using host certificate as authorization authority a good thing?

MS: I think that we all should agree that using host certification for providing assertions is a not right thing.
IN: can I use service certificate for that?
MS: I would say no again. because host certificates are not good identifiers
MS: using authentication key for signing is simply

JJ: how does it differ from SAML?

MS: VOMS is basically CA that is issuing attribute certificates (AC) (JJ&MH agree)
JJ: you could forbid this in usage in policy

DK: no-one has to sit down and go through VOMS architecture and these problem in details

MV: can we define this as a special service with more strict rules

MH: we need to get together with VOMS ppl
BC: middleware security meeting

DG: there is a significant number of VO servers today

MH: we can help VOMS ppl with distributions

... more discussion between MS and JJ - are these robot certificates ...

conclusion - **discuss more about this on next grid middleware security meeting**