1 EDG CA managers meeting – 12-13 Dec 2002

Present:

```
Dave Kelsey (RAL)
Brian Coghlan (TCD/IE)
Jens Jensen (RAL/GridPP-UK)
Milan Sova (CESNET/CZ)
Tony Genovese (DoEGrids/US)
Matthias Gug (CERN)
Mike Helm (DoEGrids/US)
Lev Shamardin (Russia)
Wei Xing  (UCY) …  (Cyprus) (xing at ucy.ac.cy)
Ingrid Schäffner (Karlsruhe/DE))
Sophie Nicoud (CNRS/FR)
Ursula Epting (FZK/DE)
Jan Astalos (Slovakia)
Pawel Wolniewicz (Poland)
Robert Cowles, SLAC/US
Darcy Quesnel (Canarie/Grid Canada)
[Plus Andy Hanushevsky, SLAC and a few others not on roll]
```

Introduction

Regrets from

David Groen (Nikhef), Anders Wanaanen (Nordugrid), Christos Kanellopoulos (Greece)

Minutes

Mike Helm

Attendance: 16

Abbreviations:

Q: Question ; A: Answer; C: Comment; usually Q: comes from EDG audience but not always. [] enclose note taker's editorial comments: interpolation, abbreviation expansion, &c.

Minutes Review: June 2001 meeting

See

http://hepwww.rl.ac.uk/edgwp6ca/Jun02/CA-coordination-20020627.txt for the itemized list

6.1 OpenCA alternatives

1.1.1 CSP – Christos; PICA, Jens; other: mike

Mike hasn't done his, no news on Christos', Jens has done his or will update

6.2 Renewing Certificates with same DN, different key

Mike – but discussion deferred until later [we did not cover this]

6.3 CA directory configuration to be put in CVS

Roberto has put info into CVS directory, not sure how much has been looked at, is ready for questions.

6.4 Update of CNRS

Pending Sophie's arrival [see below, "catch-all" service part of presentation]

6.5 NorduGrid new CP/CPS

[continued]

6.6 Subject Alt Name

Will talk about tomorrow [came up repeatedly]

6.7 Cross Grid links

done

6.8 Pre-screening of cross grid CPS

[BC has done this]

6.9 New CERN CA

TBD [discussed below]

6.10 CA scaling graphs

[See statistics discussion below]

6.11 Renewal

Will take that up later today

6.12 HSMs

Mike will discuss tomorrow [very quickly]

6.13 Authentication procedures for RA's

Levels? Meaning?

Do we want to map on to one of those levels?

6.14 Basic rule set for auto evaluation

6.15 Explanation of auto rule set evaluation

Both to Brian – will cover

6.16 German RPM

Anders; done

6.17 Cross Grid CA/CP's

done, but limited discussion to date

6.18 RPM's as required

pending, 6.17 dependency?

6.19 CA publishing directory

[How to do this – Mike hasn't done it]

6.20 X.509 extensions

Brian; but comes up in Mike's doc

6.21 New CA's recipe

There is an immediate need; this is a Euro deliverable; DK and others.

6.22 Date of next meeting

before Oct 15; we failed! See below for next meeting

6.23 CA Key Sizes

No news that people know of, for key size issues with CA's, EE's; no further info to date.

PAG standard

Discussion last time about CP/CPS; anyone looked at?

Recommend self-audit against it?

Revocation

We need to add this to agenda

What does it mean? An important case for managers &c is:
Someone has left, & we *know* they have left….

Statistics

Said we'd collect quarterlies
What statistics would be meaningful?
How about – the number of current, unexpired certificates;
Revocation numbers – [noted as small, fairly constant numbers]
"Certificate accounting problem"
Dave K: will send email asking for quarterly statistics, basic accounting.

Round Table

CERN

Matthias Gug presented an update on current CERN CA practices.
Workflow of CA's EE signing:
User sends request to "team leader", who approves, then CA Manager signs certificate. CA defines three roles:

Roles

User

Generates keys via openssl from afs node

Team Leader

Approval done by application running on afs nodes

CA Managers

Req2floppy – floppy2net applications on AFS node
CA/sign on offline CA
Some discussion on the level of identity assurance took place – can the name of a subscriber be guessed and allow an identity theft attack? CERN "team leaders" must verify the EE requestor personally. There is no project related information in these certificates. It is not clear whether these certs are generally usable in other projects (ATLAS, CMS) -- check? A new architecture will appear in the spring, openCA based, probably; CP/CPS coming..

CNRS

Sophie Nicoud – slides
Highlights: There are some 49 "units" or RA's, including 21 other institutes all over the world, including India; a China unit soon. This CA has supported 4 EDG tutorials. Question was raised on Slovakia, whether the new Slovakia national CA will replace the service for Slovakia listed; this will happen soon according to both parties.
Criteria for signing by CNRS:
Need a tie to an application, like CMS.
They may be institutes in covered countries not part of the national structure (eg non-INFN institute in Italy, or non-CERN Swiss site).
Usually these are sites with a small number of users (but possibly many server or hosts certs required).
Q: Remind us about the namespace: not just in French NS?

A: Some examples
/C=CH/O=SIB/OU=Lausanne/CN=tota/Email=toto@si
Q: does the CP reflect this?
A: CP says we issue certs for all people in datagrid project.
Q: does it need to be in CP? [Should the namespace description be in CPS?]
A: We have a structured name.
The name collision issue was raised – it is possible in this kind of CPS for a person to request certification from 2 different CA's with same structured name. Should a name unique to the CA be in the subject name of cert?
Q: Eg a name unique to the CA in the cert…

Renewal

Customer receives email from CA 2 months before expiration; RA also receives a verification request on customer renewal; key pair is replaced on certificate renewal.

Browser

CNRS supports netscape browsers, 4.6 and up, and some IE (some problems).

CNRS CA PKI software

The organization's CA software, UI code and CA management are available; see Sophie for access; crypto functions based on openssl, other functions require *perl*. 3 machines used to support CA: Web server, RA, and CA host.

Karlsruhe

New project supported: GridLAB. CPS update to appear Jan or Feb 2003. 75 certs issued, 25 revoked, stats on web site.

INFN

Not much news. Waiting for progress on RA delegation from management. There is a need to issue certs for other institutions. Implemented DNS name in subject alt name – this lead to a discussion resulted about the difficulties involved in getting *subjectaltname* data into signed certificates; discuss on how to do [perhaps should publish the recipe for openssl].
CNR -- discussion about jurisdiction between INFN, CNRS. INFN doesn't have the ambition to be the CA manager for Italy, perhaps this Italian organization (CNR) will have to have its own CA eventually.

Russia

New business: a biology application. Have new LDAP directory for CA – cert publishing, and have added RA's outside of Moscow.

CZ

CA survived the flood. Trying to provide the service for the rest of the country.

Acceptance Matrix

Brian Coghlan

Cross Grid

DOE Science Grid and Canada just added, to be added: Poland, Greece, Slovakia, soon Cyprus ; maybe Austria? But Austria not in Cross grid list.

Auto evaluation

New work:

New worker will replace / augment existing compiler

X and Y axes are swapped compared to current display.

The new version will appear in about 3 months, but during this period we can discuss the rule set and associated modifications.

There was some interest expressed in adding local rules or VO based rule-sets. Can we agree on a default rule set or sets? It was proposed to put up as an experimental work page; and find or define a way to submit rule sets.

Another useful quality would be to extract CA or PKI features directly from certificates issued.

Q: Recourse? How to improve one's rating, or appeal a bad rating?

Presentations from CA's

Greece –n/h

Poland

Pawel Wolniewicz

Plgrid-ca is at man.plsnan.pl

EE qualifications & scope

Natural persons & computer entities; scope is Polish distributed computer applications. Non-commercial use.

CA Specifications

CA signing cert has a validity of 5 yrs; the EE certificates, one year.

15 character pass phrases for certificates are required.

CA extensions

Many netscape extensions in certificates.

Name structure

C=PL, O=GRID, O=organization, CN=subject-name

"Organization" from small set of institutions, kept in the following list

http://www.man.poznan.pl/plgrid-ca/ra-list.html

The list is expected to grow. [This explicit file, in the CA web pages, seems like a very good idea, as most EDG CA's are developing an RA model.]

Workflow

[Must see slides & CPS]

Mostly standard or best practices features. Transactions are sent by email; would like to add more authentication mechanisms for certificate signing. The RA may also verify the subscriber by personal contact. The signed cert. is sent to the RA to deliver to the subscriber.

Q: if mail bounces, should a certificate be revoked?

A by Audience: if for example the email address in the certificate is no longer usable, then it is ipso facto a false statement in the cert & so certificate should be revoked.

Q: Section 317b- “should”?

A: We require a personal contact (change to **must**)

Host certificates discussion (this section of the presentation launched a philosophical discussion about host certificates)

Presentation: System administrators make host certificate requests.

Q: how do you know who asys adm is?

Comment: Perhaps need something more….

C: Need auditable trail

C: I don’t want to re-issue certificates!

[C: Somewhere in here Mike & Tony mentioned how DOEGrids issues host certs; multiple certs are allowed; our service is too dispersed and our ties to “sites” too shallow to enable us to figure out who an authorized system administrator is with any great confidence. This led to the following caveat:]

C: GDMP uses host certificates as user certificates, and makes multiple certificates used by a host a danger.

C: Argument was made that multiple certificates issued for the same DN for a host could make an attack easy.

C: Dave circulated, “A Rough Guide to Grid Security”, how an attacker would get a certificate in someone else’s name, but that person would be the holder of the private key.

[Discussion about what SSL intends to provide the “client” in the server check; what the host name checks provided by a) the de facto standard check in SSL web servers and b) Globus servers actually do, and what the limitations are; and more about *subjectaltname*.]

C : [based on dependencies of SSL] You can co-opt DNS AND get one of these rival host name certificates. Then you can capture these transactions.

[Seems like the DNS cache issue is the essential one, not the number of certificates for a given host.]

C: The relying party should be able to trust that the CA has done the right thing in order to issue a certificate to hosts.

C: We don’t have papers [“contracts” that state a person is entitled to request/use a host certificate].

C: Most people required signed requests ie from a certified user

The issue of host certificates is difficult! [It seems like there should be some action items in here, but I missed them. I think Milan made a comment that the *subjectaltname* extension really was needed for certain flavors of openldap client code to function properly, and so this policy should be continued at least for certificates intended for usage by LDAP clients. Perhaps there should be some clarification from Globus about some of this matter; Mike will do this anyway.]

Discussion now returned to the Polish CA configuration.

The CA is in a restricted location, no net connection, powered off (meets standard requirements). There are about 20 certificates issued so far and 3 revocations.

Some discussion about private key protecting pass phrases followed. It would be helpful if *voms-proxy-init* could check length, quality. Of course it is difficult to do a crack-like test since this could take many minutes.

C: One could hack openssl to put in pass phrase rules….

C: [From Bob Cowles]: I pushed for a 15 character passphrase, not for password strength, but to limit liability of system manager.

Slovakia

Jan Astalos

Applicability: IISAS & CrossGrid

Applications – related to flood events; flood forecasting; some HEP.

There are some other VO's which may require certificates.

CA is based on openssl, restricted physical access, off-net. The CA cert is 2048-bit, 5 year lifetime, with a 15-character password, backed up in a sealed envelope.

Issuing policy:

Slovakia organizations involved in research. EE certificates are valid for 1 year, 1024 bit keys.

Naming:

C=SK, O=<org>, OU=<orgunit>, CN=common name

RA checking of requests:

Valid official ID card (or RA's personal knowledge)

RA checks relation of applicant to organization specified in CSR.

Server / service cert signed on request of valid system administrator.

[Other details: see CP/CPS and slides]

Q: Do you intend to issue certs to all of Slovakia?

A: Yes, but need to discuss a few issues here before doing this; for example potential clash in namespace with CNRS

Q: Section 3.1.6: email address must be from your home domain; in our environment people have addresses in other domains, but this is ok isn't it?

A: We want them to show by email address that they are linked to their research organization.

CyGrid CA

Wei Xing

Cross Grid member ; support researchers who need X.509 certificates for grid. The CyGrid CA is independent of other organizations on Cyprus.

There is minimal information in the certificate: {name, organization element, base name}

Work flow

Name, email address, contact, info -> RA
RA verifies, using personal contact with valid ID
CA sign cert & sends to [?] by email

CA configuration

There is one, at the High Performance Computing Lab at the University of Cyprus, Nicosia. Namespace – see CPS. Web page: http://www.cs.ucy.ac.cy/cygrid-ca

The CA is located in a secure room, meets standard requirements. 3 user and 6 host certificates have been issued for test bed as of Dec 2002. No directory publishing yet.

Future

Move to OpenCA ; add directory services; web site update

Q (to Cyprus): What do you want of us [at EDG]? Do you want approval now, or readying for future use?

C: It's an early stage, perhaps should allow a few months of settling, perhaps resolve use of openCA.

Q: Do we need to wait approval for another face-to-face?

C: No, but of course we have to have the right keys from Cyprus in order to generate the RPM's &c.

C: It's a large step to switch to openCA; perhaps should stick with openssl for a while.

Q: Is it a requirement to use openCA here?

A: No – use what you are happy with.

Assignment for review: Tony, Jens, will read and comment by end of Jan 2003.

Approval of Cyprus CA will probably take place shortly thereafter.

Canada

Darcy Quesnel, Grid Canada, employed by CANARIE

Grid Canad

Formed by MOU between CANARIE (operates research backbone), NRC (federal labs) and C3.ca (high performance computing sites in Canada);

Project drivers

NRC: Multi-scale modeling – 5 –50 users

Atlas Canada: 10-30 users?

Challenges:

No federal agency has identified grids as "strategic direction".

My position is the only funded position related to grids in Canada, but expect explicit grid component will emerge in projects, and agencies will move to support grids.

CA Specifications

Built in April; CA signing cert lifetime 5 yrs ; issued 13 user certificates, 18 host, 2 revocations so far. Based on *simple_ca_bundle.* This CA is limited to supporting grid work only.

Namespace

/c=ca/ou=grid/ou=domainname/cn=fullname

We insist on these domain names being recognized organizations which exist in DNS eg phys.uvic.ca.
See the website:
http://www.gridcanada.ca/ca
No directory (or other certificate) publishing yet.
Some differences from standard EDG model
This is a small community – I know everybody; no separate RA's spread across the country.   Host requests are not signed by a user cert (no need yet, small community).

Future work

Scaleable RA infrastructure (when existing community grows)
North America PMA
C: North American PMA is too new; don't put in your critical path; Atlas has work to do!
XML schema for CP/CPS [Probably a good IETF project]

Questions by Darcy for EDG:

Are there any problems with our service? How about host / service request not signed?
Q: what about publishing XML source of CP/CPS in LDAP for online access / analysis?
Q: Did any of you look at the "trust European" project – automatic way of assigning trust to a certificate authority, from Chadwick
A: Host certs are to be verified by any appropriate means [personal knowledge], so you are ok.
Q: how to do cross-org RA's with no money?
A: Volunteer fire department model – volunteers committed to making their projects work.
EDG questions:
Q: Section 1.1 Lifetime of certificates limited to 48 months
A: Will look into that.
Q: 3.1.9 Refers to empty section specification
A: Will fix section referencing
Q: About means of identification: fax of identity cards is not so trustworthy.
A: Well what about using fax in the interim before RA appears?
C: [strong insistence on personal appearance by some EDG members]
C: This is a demanding requirement for a large country like Canada, and the trustworthy people [RA's or their agents] should have reasonable means for identifying people.

Summary:

Who do we approve today, and how do we go ahead?
DK: Move to approve Poland, Greece, Slovakia without delay.
We do know at least 3 people in Cross Grid say they have read these CPs, and documents have been available for extended period. These three CA's were approved. .

Cyprus to be considered by end of January

Canada

This CA has been operational for some time; Atlas is pushing us; identity vouching questions raised seem like they will be met properly via personal knowledge; seems to meet minimum requirements, CP/CPS has been read by some participants..

Canada approved.

CA Updates

[13 Dec]

IRL

Brian C.

This is 2nd gen Grid-Ireland, change openssl -> openCA.

Workflow:

Browser based, and everything based on openCA. Email notifications to user about cert issuance. It's up to user to pick up.

Host requests use custom grid-cert-request

Naming

EE: C=ie, o=Grid-Ireland, ou=<VO>, L=<RA>, cn=<common name>

CA: … cn=grid-ireland certification authority

Generation:

User: user

Host: grid-cert-request

New CP/CPS to come…

UK e-Science CA

Jens Jensen

Very similar to IRL (close cooperation). 3 differences from IRL:

- Email workflow
- host CSR pages
- certificates are published

About 170 certs in new CA (all kinds; 40% machine). Have 25 RA's ; 3 new per week. There is a formal RA approval mechanism. RA's check a photo id to approve EE certificates.

Server certificate issuance is somewhat restricted.

Expect to top out ~500 personal certs; openCA dbms may not scale well above 1000.

Naming

/C=UK/O=eScience/OU=…/L=../CN=name

Where ou & l AVAs describe the RA

CP/CPS changes

New CPS took effect 30 Nov; effects from UK law included. One more update to finish.

Scope is to accept UK Grid users – expanding scope outside of eScience.

Some updates may take place, including a policy oid, and dns name in *subjectaltname*. Intend to move to RFC 3280 compliance.

Future

Poor IE explorer support currently – want to support IE better

RA's forced to use NS 4.7 ; need to fix this.

Use java to generate PKCS#10 requests?

[Discussion with Sophie, Darcy, Brian; common problem – future work?]

DOEGrids/US update

Tony Genovese

Name change: doesciencegrid -> doegrids (appears in various places, including domain names of servers, base name of issued certificates).

PMA approved new CP (see for details).

Developing a new root certificate policy (the original root CA had no policy document).

Changed PMA charter to fit GGF model.

CA products

Iplanet CMS 4.1 root -> 4.7 Real Soon

Iplanet CMS 4.7 community (doegrids) CA

Need to coordinate insertion of CA certificates – introduction of new community CA depends on EDG and other relying parties' distribution of new certificate chain.

Other

We introduce a "naming convention" document here, which was used in our new CA's and CPS.

A few CDs containing the new certs were distributed.

The CP/CPS of the older community CA, doesciencegrid.org, needs to be returned to the appropriate web site, since certificates were issued under this CPS, and the new CP/CPS is different.

Q: Your CA mentions certain VO's; what about "non VO'd" people? Another site mentioned having set up a "solo" VO, for people who are independent.

A: While this problem was anticipated in the original proposal, we haven't had the problem – yet. Perhaps we haven't noticed it.

Note that we have a few deviations from the EDG core requirements, mostly discussed and allowed before.

Physical security and network security components are being built.

Europe – North America – World

3 inter-related issues to consider here:

What is our relationship with the rest of world?

EDG as a project ends next yr, but –LHC not on the air until some years from now.

"This body" has a life outside the funding project.

PMA

Limitations of GGF – does not seem like the place where a worldwide PMA will be sponsored, at least for now.

Will the countries set up CA's of wider scope?

Will the academic area [TERENA, CREN] just set one up?

Does it make sense to spin up / regionalize PMA bodies?

Should we set up a charter for ourselves?

What is the way forward here?

LCG needs something to go forward – A: should be in LCG board

Comments from EDG:

This group should carry on; not just die with EDG & Cross Grid.

Cost of starting this kind of thing again for every experiment is high; so getting continued funding should be easy

C: From a recent TERENA meeting: PKI not the future?

[Not clear what the implication of this is; could be that no alternative coordinated PKI will appear in European research and higher education, or maybe that's jumping to a conclusion.]

Particle physics:

LCG

EGI – large infrastructure

If we can avoid these project setting up 2 independent infrastructures, management bodies &c, we should benefit these communities.

Propose: draft a European PMA charter for next meeting. Dave Kelsey will draft charter with help from others. The charter will focus on identified customers and community, allowing expansion later.

Date of next meeting

Next Data Grid meeting is mid May 2003.

Dave Kelsey will investigate setting up a "private" meeting, convenient to CA managers attending this Data Grid meeting. Other alternatives include a CERN location in spring. Details on the mailing list.

GGF Update

Tony Genovese

6.1 CA OPS

Refocused GRID CP document onto operational areas of interest.

Last call documents:

- Trust model
- PMA charter
- Grid CP

Now with editor -> "Best Practices" documents in 60 days?

We have some other things we need to cover (see web site).

North American PMA

Good support from US Federal agencies; we are identifying charter members, and web site will be set up soon. May ask for EDG liaison.

Directory, naming, cert extensions, HSM

Mike Helm

[Reconstruction from memory – note taker was presenting, and slides he used are unavailable at the moment.]

Due to time considerations these were only briefly introduced.

Directory – we need to specify completely how certificates are published. The idea is to support VOMS properly. We have run into operational problems with the VOMS users. This is not a Grid standard (maybe someday), but if we publish as a best practice at GGF other CA managers will align. Little work has been done to date; almost all the material needed is in the mailing list. Roberto Cecchini said he would contribute a "use-case" which should help with the query specification. Andy Hanushevsky will contribute some security considerations to the directory paper.

Certificate Extensions – the PKIX profile, EDG practice, and grid requirements are not completely clear on what extensions should be used when. In particular there are extensions related to OCSP, CRL, and policy handling that could be used to support grid infrastructure better. But there is also a need to provide the minimal amount of complexity and information in a certificate. Mike Helm has collected data on the use of certificate extensions. A best practices document is proposed for GGF, and participation by this community is solicited. This may also support some of the automatic evaluation work mentioned earlier.

Naming practices – DOE Grids re-naming, and the counter pressure to minimize the certificate information payload, led to a naming convention expanding into a naming practices document. Perhaps this is a DOE Grids-only specification, but the author feels it should be useful in EDG. Provide a standard set of naming practices for all CA related protocols and services, but frame as *recommendations* ("should") rather than *mandates* ("must"). Allow alternative naming. The principle is that a relying party or customer should be able to derive and locate all useful features of a CA – documents, certificate copies, web sites, email addresses, CRL's, &c – by knowing something basic about the CA, like its organizational owner or the organization's DNS name. See paper (will appear in www.doegrids.org & on mailing list).

HSM paper – this is important for our relationship with EDG. Hardware Security Modules secure our CA's private keys, and do the signing. We want to make sure the EDG community understands what we are doing and why. Pictures of the hardware were shown and a short description was made. A paper will appear shortly, perhaps to a private audience due to licensing and security issues. Details early next year.

Brian Coghlan:

There is an opportunity to write an academic paper about our experiences… looking for contributors.

Afternoon video conference

FNAL KCA

Matt Crawford & Dane Skow, remote from FNAL, presented their Kerberos -> KX.509 [KCA] certificate authority. This has been in operation most of the year on "revision 1", will rebuilt.

Workflow for client:

TGT -> Service ticket -> Key generation -> CSR + Kerb authentication ->signing -> cert
Comparison with KDC:
KCA change involves sites' help
KDC change doesn't involve everyone
KCA is simpler, and same net profile, than KDC
KDC not compromised, expertise widely available
[Not clear to note taker exactly what is meant by the above]
Advantages:
Users don't have to learn PKI discipline
Certificates can be obtained automatically
PK-World advantage
Short lifetimes for certificates – no revocation
Update of profile
[By this is meant, user does not ask for extensions, we at KCA do this]
Compromise is easier to deal with
Some other comments from presenter:
Credentials are just like original grid credentials.
We don't like signed email or non-repudiation.
We don't protect the KCA or KDC with a firewall. Several years' experience shows that these can be protected adequately without requiring a firewall.

CPS discussion

[CPS is complex; at least 3 different CA's are described: a root CA to protect the PKI, an SSL host CA, and the KX509 [KCA] CA. See CPS]
Q: What is the 1st step in the authentication
A: Kerberos; password to unlock credential; we impose password control
Comment: You need 4 CP's:
1 KDC
2 Long term service CA
3 Kerberos CA
4 Root CA
A: It reads better this way
Q: Each CA needs its own policy document and OID.
Q: How do people get Kerberos token in 1st place.
A: You mean like an RA function [for the KDC]? This is done by external reference.
Q: Most of the CP's document how they check identification.
A: Ok [presumably an action item]
Q: How do you protect your online CA?
A: We have 2 questions we want to discuss:
We are putting up an infrastructure similar to DOE Science Grid
We are proposing to be a peer, because subordindate CA doesn't work in Globus

A: While technically it is a CA, its purpose is not to issue long-lived credentials, so HSM is overkill for this service. Besides, it is too expensive. There is only a remote possibility of someone breaking in to KCA. Basically, this comes down to this:
Intrusion is undetected, or detected.
For the CA signing private key, you have these configuration [sic?] choices.
Long lived, can't be stolen
Short lived, can't be stolen
Short lived, can be stolen
Implications in each case that you have to replace that key.
[This matter of dispute was tabled]
Discussion then moved to hierarchical architecture and the difficulties involved in supporting transitive trust in grids.
FNAL argues that trust of the root CA can be used to enable supporting replacement of the subordinate (KX509) CA when needed. This is true, but other participants point out that this remains a very difficult administrative burden.
Q: Online KCA has network protections; what are these?
A: Its host only accepts a remote management login, and the CSRs.
Q: Where would this service work?
A: Anywhere your users are.
Q: What about using an HSM (Hardware Security Module)?
A: We don't need it. The root CA is offline and non-existent most of the time.
Q: What about the KCA -- it must have HSM or offline? [Ref EDG requirements]
A: Up to this body – we would like to discuss this in context with myproxy, and know for whom objectors are speaking. This is a policy appropriate for issuing long-lived certificates. There is too much money involved in an HSM.
Q: The HSM or off-line CA policy is about trust of the CA, rather than about the certificates it issues. Is it a good CA – is the private key protected or not.
A: The issued certs are very short lifetime. This should be discussed in context with myproxy and VSC.
Q: What about logging?
A: We have extensive logging, and intrustion detection.
Comments from FNAL: We will investigate HSMs. We ask you to define formally CA's and where HSM's are used. If FNAL had an HSM, would our CP be approved?
Response – not ready to do that, need longer review of CP/CPS.

VCS – Virtual Smart Card

Andy Hanushevsky, SLAC
A set of slides goes with this – didn't get url.
Premise: private keys and users don't mix:

Can’t guarantee password protection
Can’t guarantee private key handling

A person can’t mishandle something they don’t have. The VSC acts as a credential repository, integrates into the process of acquiring a long term X.509 credential. The author makes an analogy with a high – quality (FIPS rated) smart card service. Customer makes a request of the service, the service generates key pair & CSR, and the credential is returned to the service. In future operation, the customer uses some acceptable means of authentication to unlock the smart card. The service then generates proxy keys/certs on the customer’s behalf. The keys can be kept encrypted on the store so that local administrators have the least possible access to local credentials (although there is an opportunity during the brief period where the private key is decrypted in order to sign the proxy key pair). A separate password (from whatever you did to authenticate) is required to manage your private key.

We need 3 protocols: dns, ntp, and vsc protocol; don’t need any other network support. A short discussion ensued on possible problems with NTP, and running NTP directly (own the GPS hardware).
Workflow
Ask for cert
Vsc -> generate keys and send cert request to CA (eg remote CA like DOE Science Grid)
Email certificate URL to subscriber
? download cert for CA? [couldn’t read slide]
The rest of the discussion expanded on points made above. The private key of the long term credential never sees the network in any form is the operational implementation of “A person can’t mishandle something they don’t have.”
Q: What about the long running job problem? [For both presenters]
A-vsc: long term techniques: either use a new cert, or leave long-term private key open for expected period.
A-kca: Those jobs invoke a KCA transaction as often as they need to; we are working on a pure – PK world solution with Globus.
Q: How would you authenticate that transaction, from non-Kerberized site?
A: The model we have now assumes batch system has method of getting local -> grid credentials.
A: Who has the responsibility for renewing long running jobs?
Q: Would kca serve as proxy renewal service?
A: We are not proposing that initially; resource provider end; would do so with CONDOR.
Q: What if someone has stolen passphrase from VSC?
A: must steal 2 passwords, one to authenticate, one to decrypt.
Discussion about the analogy with a physical token [a Rainbow USB token was shown] summary from user: a physical token is inconvenient in some respects;

limited ports, access to the token is very slow, can't do encrypted email because it's too slow, &c, so I have given up on it.

Other discussion topics: Performance – AH has some prototypes, haven't explored the performance burden. Sharing – trusting VSC's – the vision is that this is a local site service only and that each site must have one; and SLAC will run one for its users. Comment: What if the University of Manchester ran this, for SLAC? Would SLAC trust it?

Q: What about just an ssl connection to U Manchester

A: the private key never went on the network

Q: SSL is not secure?

A: Not good enough.

Q: If we cant run this generally, we're back to every site running their own.

A: It's up to the VO; there is flexibility of how VSC's are configured, so some change could be made from SLAC's requirements.

Discussion of clashes with existing EDG CP/CPS requirements.

DOEGrids will help enable this for SLAC on a trial / demonstration basis.

[END]