11 May 2009

EUGridPMA minutes

Welcome & Agenda overview

Notetakers

Announcement about election

Roundtable – about 30 people

Eric Yen from Taiwan – new chair of APGridPMA this summer

Eric Y Gives update for APGridPMA

(Yoshio cannot make it due to travel restrictions)

APGrid PMA F2F last month at ISGC, Taiwan Grid meeting

4 big topics:

NGO/Netrust extend CRL lifetime

HKU approved as a classic type CA

ASGC – major fire incident – long report later

And the F2F itself. Next meeting – second half of year

Updates from 10 national CAs

Approved classic profile ver 4.2

Approved Australian federation document (w/ SLCS CA as a service/ IGTF

Proposed joint meeting w/ TAGPMA – Banff CA, Hawaii , ?

Vinod isn't connected so David Groep will put up his slides, & Jim Basney will show

Membership issues – most interesting topic was TAGPMA charter update and how TAGPMA deals with membership status changes

CANARIE officially hands over management of CA CA to NRC,

New owner Roger Impey was in attendance

And CANARIE moves to TAGPMA

PSC hosted federated workshop- separate set of indico pages & presentations

- Incommon & us shibboleth federations
- Verizon (now large scale commercial CA service vendor too)
- Safenet

TAGPMA approves namespace management

Minor change to SLCS profile – language update & references

MICS – approved 1.1 – does not contain some language that is missing from slide deck, but is about traceability

What constitutes "traceability" – from eg MICS to backend IDP or federating IDPs

End of discussion is - we don't understand traceability

What the goal is

What the end results are

We ask for a discussion on this in IGTF

We voted in the other changes to MICS profile

Jens "Kihon" presentation – is the deep meaning of our requirements being lost?

Reviving Bridge WG

4 BF – a US initiative on 4 Bridge CAs agreeing to interoperate

How to use bridge CAs in our environment – technical interop issues

Jim Basney's SHA-2 presentation

TAGPMA will accept DOEGrids CA as accredited member

New accreditations nearing: FNAL, NCSA Fed, TACC MICS

Maybe a joint APGRIDPMA / TAGPMA in CA? in Oct – maybe interact with IGTF sessions

Banff is a busy location – need to set up quickly

See slides for video contact info – fortnitely (biweekly) conference call/video call – all welcome.

IGTF Risk Assessment team (RAT) report – Jim Basney

Team is open – please join

Chartered to assess risks that mite affect IGTF ops –

See slides for addresses

MD5

All the CA certs have been updated

A few are still issuing crls in md5

Opened bug w/ globus project –

They have commited change to CVS – latest code will use hash in EE cert

ECDSA

Found a few of these keys (CERN) valid til August; not widely used (CA can support wide range of keys in CSRs by default)

Q: Are they ECC or just DSA?

A: Not sure

Various sanity checking issues:

- ECDSA
- RSA exp < 65537
- Md5
- Debian exposed keys

Sent out survey – essentially audited the IGTF infrastructure for these issues

See slide for timeline

15 Jan start

11 Feb sent survey

23 Feb 57/80

28 Apr 78/80 responded

Survey method

Idea of web survey is to avoid email response & work needed to fold/organize the responses

1 CA objected to using surveymonkey.com, so used email

Disclosing private info to this company

Perhaps need to stand up own collection/survey site

- Jens may have service – will investigate
- Most web CMS have plugins for this

Saved JB a lot of time doing this way

How to encourage CAs to respond more quickly

Publish response times?

WW: Objection: Not all the CA operators are entitled to answer such surveys

Also the hi level management may not be available, even tho the operator may be doing what he is supposed to do

A: But it's a serious problem for our infrastructure if CA cannot respond to a problem in 4 weeks

A1: CA operator is instructed to respond to risks; but not necessarily to respond to queries

Publishing the time then is misleading (or damaging to reputation).

The operator should acknowledge requests even if they cannot answer all of them. -> Previous agreement was that response should be 1 business day

Justify not answering or not answering in detail.

Does response mean anything if the range is I received your mail to here is my complete analysis

A: concern that there are a few CAs that don't seem to read their email

Discussion about fire drills, complexity of questions, and making information publick

- Make firedrills, and make results discussable in meetings for benefit of group/RPs, not public
- Aggregate info is ok
- No consensus yet on making complete results public

SHA-2

NIST advises to replace SHA 1 by 2010

Understand software support for SHA-2 – when can relying parties begin handling SHA-2?

MH – I think this is not a big problem, it is good to identify these issues and be ready

TN – sha1 collisions will happen – the new NIST hash function support will probably be better than sha-2 anyway; let's be cautious

WW – this is dangerous, we must move to a better standard like sha2, sound the alarm, otherwise there will be yet more software dependent on poor algorithms

MS – We should ask for versions of openssl that can use sha-2

Will not be multiple hash signing &c by 2010

Q: How long will we accept RSA 1024 modulus?

We require 2048b for CAs, & we know we can move to that size for EE certs

Identifying software that employs hash & what problems exist

Openssl < 0.9.8

Nss

Pure tls

Bouncy castle

&c – lots of derived software using openssl 096 like things

Lots of things have sha-2 support, some have version issues, some are unknown status

WW: Set up a roadmap in order to get some discussion – pushback

MS: be careful formulating roadmp – what if we don't do sha-2 – bad effect on future roadmap

JJ: We can file bugs against software distros that don't support sha-2

JB: Roadmap would say, we would like to move to sha-2 by 2010 ….

DOEGrids CRL discovery – 25% of RP's still using old CRL URL – is this a risk

What do we do with this info?

- Should not publish – don't know what to do with information
- Why did we agree not to do anything about it?

Problems with updating the certificates

Comment – back to SHA-2 – dcache for whatever you have in Java, so not a problem

Encourage other sites that change significant URLs like CRL URL to keep statistics

Send data to RAT or perhaps use the TLD info to route to CAs.

DG: Is there anyone who wants to take up position of chair person?

Requirements:

Member

Accredited CA – no RP's

Workload is not so bad

I will be happy to continue (general acclamation)

But I don't want to be SPF - operations outsourced to Anders, also have 4 distro-builders

Agreed – DG will continue for another year.

--------------- coffee ---------------------

WW – talking about need for a codesigning cert for java ….

Need to sign jar files

Self audits

Peer review of self-audits has never actually started

Started a list which is at

Eugridpma.org/review/selfaudit-review

Has CAs, assigned peer reviewers

Need list & tracker to follow this up – keep track of large list of CAs

JJ: it's much the same as doing operational review; need 2-3 reviewers

- Should keep list
- Test reviewers to complete work
- Need wider base of peer review
- Problem is get Jens + 1 other volunteer from small set

Could assign reviewers based

Could save things in the wiki

Need both open & closed part of wiki

DO'C – can use the internal ACLs to manage access to close some parts, and leave the rest open to anyone with a cert

- Agree that we will have "ABCD" audit status on wiki will be private –
- RW to members only
- Reviewers will work w/ CA for updates/status changes
- Chair will manage the reviewers
- PMA site will only have global/generic status (pending/reviewers)

JJ: Need for agreement about schedule for change w/ CA manager –

- Changes should be done ASAP, but reasonable time – w/I 6 months, but by agreement with reviewer

---

New Austrian Grid CA – Willi Weisz

Hope to complete by end of June

Still some software & hardware issues to resolve

Essential changes

Online CA – safenet – protectserver gold 200

New name space = dc=at/dc=austriangridca

This domain owned by Austrian CA

Hardware security provisioning

Software – 3-4 Virtual machines – using XEN 3.1

1 VM for running CA

2 VM for development

1 VM for XP – access control system

We have had some problems with some of these services which caused outages, some things like fingerprint reader not working on VM (USB interop issue probably)

Online CA + online signing server – separate machines

User interfaces

Keys & CSR generated by Java applet

Support for Windows only

Java 1.6 – needs setting of file access rights

- Policy: private key restrictions set so only user has access, and can't destroy it inadvertently

Improvement to UI to improve vulnerability checking & rekeying / renaming for new infrastructure

What about the CRL for the old CA, need to extend
Need a root CA – offline CA – what about CRL for that?
RA – more delegation to RA
Going to use secure tokens somehow
Documented in certificate (1SCP) ; or perhaps additional subordinate CA;

JJ: Not necessary to have root CRL limited to 30 days. Could make it 1 yr
DG: Classic profile – only issuing CAs issue CRLs on the 30 day clock
JJ: We have accredited root CAs under this profile – 1st TACC root CA in TAGPMA

DG: No distribution for root CAs as-such – and some relying parties wouldn't accept these root CAs if they change profile! So EGEE & LCG must change their policies before we can use it.

- Need separate CP/CPS for root

JJ: There are many people out there who do strange things
(Comment about where does info about CAs come from)

Tangential digression:
HLCA profile –
Needs some text
Relying parties need to accept

Discussion on scripts -there is a page on euridpma wiki w/ links to useful scripts

TN: hardware signer is separate server
CA is on one site + other VMs
Is that collection of VMs presentation of add'l security risk?

A: HSM is on its own CA
Front end transfers CSR to signing machine
A': CA VM is just web front end

Whole creation of certificate will be on special signer

Want to avoid user / local crypto problems – java applet does the work with bouncycastle crypto

How long do you have to provide CRLs after CAceases operation?
While you have valid certs – as normal
1 more after all expire?
Until last cert expires, keep re-issuing on 30 day cycle
Then issue one more for a long period, or revoke the signer

Q: Which of the online CA models are you in? A/B?
A: Model A

Grid Ireland update – David O'Callaghan
Very difficult to update the CA software
This summer we will really update
2x server certs as ppl – about 140 certs in use – level usage

Review of audit requirements and compliance steps in progress or completed
Should we issue a sha-2 ca cert
DG: Perhaps we should go for a dedicated CA to use as a demonstration

Moving to DC – based name space – grid.ie dc=ie/dc=grid
Going to use support robot certs & naming

Recommend … some naming change which I didn't quite get
Upgrading to OpenCA 1.0.2
    Needs help in various ways with openCA
Asking about different LoA – configured – no response from group
Going to assign random – 64 bit serial numbers
Implement sanity checks of certs + requests

Do robots need to go on hardware tokens?
DG: All current CAs do this

Timeline
By Sep 2009 – new system & policy ready (Berlin EUGridPMA)
Do I need to re-accredit or audit or ?

DG: The general review of this seems adequate + the 2 week review period as usual

Update on checkcerts.pl

Updated Crypt::openSSL::X509 is on github
Github.com/dsully/perly-crypt-openssl-x509
Will do some more work on this for GFD 125 compliance

JJ: what cauases re- review of CA?
DG: identity vetting changes; major process changes
Perhaps other things just send out to list
Don't want to block improvements because reviewers' time / availability

JJ: wrong to unaccredit CA just because it makes changes
JJ: precedent of introduction of robot certs

-------------------------Lunch---------------------------

TERENA Grid CA pilot project

At Nicosia was known as Nether-Nordic; now upgraded to TERENA

Countries collected in this are the ones that have well-established federations but didn't feel like standing up a service like this CA on their own.

Can scale to 10ks of users
Will issue personal certificates
TERENA SCS will take care of host requests

Why – takes too long to get a certificate – inhibits trial use
Scaling - easier to scale the pki equipment infrastructure than grow the base of PKI experts to run separate services

TERENA wil be the legal entity controlling/host service

Workflow
User connects to service – a portal like thing – cert backend does the issuing & crls
1st thought – make own backend, multiple CRL servers
Problem with Redhat is the pricing model – if the service is successful we would be bankrupt
Also egba
TERENA has recently a new provider – unlimited supply of personal & server certificates
Issued from separate sub CA
TERENA controls issuing process & writes CPS (Milan Sova)
So perhaps we will use this TERENA back end

Need clear policy distinction between grid use and other personal certs

MS: Currently SLCS is not on the table, just MICS
The profile is not covered – need to issue more certs, more often -> negotiation with provider
MICS cert will be trusted in email clients – even in the WII & iphone!

We will avoid setting up our own physical infrastructure if we can avoid it.

1st step is to make server certs – grid server certs might be available at same time.
Perhaps done by next meeting, Sep 2009.

We have a draft CPS
https://ow.feide.no/terenagcs:start

We spent a lot of time on "will this work with you" with federations
Figuring out end user portal

Now focus on identity vetting & other things in id profile

We see this
A federation signs up to TERENA grid certificate service
A direct legally binding relationship between service & home institution

Why have the bilateral agreements?
Need to show we meet PMA requirements
DFN has a participation agreement somewhat like this

Federation is going to administer the subscription contracts

There are multiple paths of relationships in this and the reasons for this are derived from the need to meet the identity verification requirements in IGTF profiles –
The federation cannot provide this assurance
The IDP can

Q: how do you assure the IDP will do this – you will need audits

Entitlement – another area of discussion
What is the definition/scope of this entitlement?
DK: who is entitled to get this service?
A: Anyone from the institution who has been properly identified.

SCS created an environment where there is no longer a reason not to have a browser-valid cert.

This new contract will do the same for personal certs.

We do not want a contract on a per-cert basis.

DK: Is TERENA committing to longer than the contract length (3 years)?
DG/JM: It will be run with business sense in mind – if it is viable, we will keep it, if not, we will kill it.

Most of work for this project is aligning PMA requirements to federation

We don't want any contact at all with end user

JJ: How does traceability work?
Need an incident response model

AW: Same as Eduroam?
Eduroam operated by NRENs had own policy

UK will not interoperate with this due to UK rules

Which attribute will be used for naming – something will be used that is released ot the service, and used to build the cert name.

We will require revocation from IDP if AAI account is compromised.

DK how does user revoke a cert?
Thru the same admin interface as above

RKM – how do you identify certificates held by a compromised user?
A: a unique identifier – the attribute not agreed on – will help you find these certs to revoke

It's difficult to keep the customers from contacting you - there needs to be an issue management model

More discussion about the relationship map

Trying to make it an issue of fraud if idp does things wrong, rather than try to guarantee everything is done right.

Example of cert issuance

Get entitlement set tht includes assertion of F2F meeting
EPPN
& of course other attributes

We do NOT want to use 2nd identification method – effectively unimplementable
Why isn't it necessary? – An argument of the beard about SLCS.
Any compromise of idm account contractually obliges all the issued certs to that account to be revoked.

JJ: this is not equivalent to 36 SLCS – only in compromise case

Dk: possession of this account entitles you to get a certificate. How valuable is this account?
2nd factor was give some level of assurance that the account was still in operation by the right person.
What we are doing now is lowering the LOA somewhat.

Discussion about whether IDPs would actually cause a revocation, & how this would be done.

Gamble is that eliminating barriers to grid use will cause an increase.
Revocation issues will just have to be worked.

TN: my worry is … suppose the software works & the legal things are ok. Most idps are bad at deprovisioning ("exit rules").

DK: there are cases where Shibboleth accounts exist for convenience – certain use cases but not SSO or not widely used – they could become compromised w/o users knowledge …. How do you deal with this?
A: We only want to deal with federations & IDPs that have their house in order.

RKM: the profile says "MAY" about the 2nd factor – why did we impose this on the CERN MICS? If there is a reason for this , do it everywhere , if not , withdraw it.

Perception here is that portals are making accounts more valuable, and there is an assertion by David Groep that the IDMs are doing a better job with id assurance.

Why impose the 2nd factor – make sure account is not used by non-valid user.

DG: Processes for managing id in CERN IDM is more rigorous

JJ: Agreements with IDPs – it belongs in the CP/CPS because it is fundamental to the nature of the way this works.

The services are dependent on email addresses – for event notification - how do we manage the change of email addresses to ensure safety.

JM: How do we drop the 2nd identification step
JJ: Timeliness of the account – activitiy. Proactive strength of password.

What constitutes a valuable service? Your organizational email? What about the impact of cloud services like gmail?

I don't want to have a conversation with every IDP to decide they are doing a "valuable service".

A high quality IDP can have low quality users (eg users that don't use the idp account for much).

More discussion on how to get the 2nd factor.

Problem is, idp has 20 grid users out of 20k local customers – not going to get traction with IDP.

Summarize = we have MAY in text so we don't have to do 2nd factor
Only UK objections to quality of IDM

Will be mailing out certificates

Would be interesting to see agreement

JJ: Would the secret certificate use case be allowed (eg the use case where CA or service holds the whole credential, not the user).

There do not appear to be blocking factors.

Polish Grid CA – audit report

Review of CA – origin in 2002, validity extended to 2007
Starting a new PKI for Poland as of 01 May 2009
Issued about 2k certificates over 7 years, about 1:1 people : hosts, people slightly ahead
Different communities have different issuing patterns.

Review of audit findings – agreement, deviation, partial deviation

Is host subjectaltname (SAN) required or not? DNSNAME
This is derived from an RFC ….

"The CA should provide a means to validate the integrity of its root of trust"
This really means, submit your CA to TACAR & go thru their registration process.

Summary:
Update point of contact for CA
Update numerous minor issues in CPS
Major issues:

Update cert profile
Record keeping and audit of CA/RA personnel
Manage the right to use FQDN
These will be addressed in the new version of Polish Grid CA – 2.0

JJ: how many certificates are valid? The record keeping makes things a little brittle.
We don't have permission from govt to record ids.

You could collect actual signatures (hand written)

DG: the one thing our RPs really wanted, was the same identity was issued to the same person.

JJ/DK: would prefer issues were addressed now & not wait until future CA.
Identity verification & records management are fundamental

DG: Need 2 peer reviewers – perhaps RP given interest?
David O'Callaghan & 1 other

Eric Yen - CA recovery from dramatic incidents

Incident caused by burnout of UPS battery

Shutdown all services; crl was not published in time.
Restored operation at a different location approx 31 hours after the fire.

Recovery activities
Should be verified by audit guideline

Discussion of various risks and impacts on community as a result
Suppose CA could not be recovered in 2 days – could another CA take over CA services
What is maximum allowed time of CA restoration?
Could some kind of federation help?

Lessons learned
Many roads to failure
Decide what to backup and how to minimize downtime
Duplicate CA services

Discusssion of battery failure

What would backup support mean?

Can we partner up and backup key material – either in HSM devices that support download, or in secure storage + key splitting techniques

CRL download issues
Sign 2 CRLs – one with 30 day lifetime, one with a very long lifetime

We will discuss CRL hosting at dinner