EUGridpma Day #2 – 12 May 2009

Milan Sova – CESNET – TCS

Terena Certificate Service – presentation

Originated in SCS – TERENA certificate reselling / buying cooperative

Pretty successful – large growth & adoption

New SCS:

- New provider – Comodo
- Model is roughly the same for host cer
- Adding personal & codesigning
- Changing brand name to TCS

Comodo is testing profiles we sent them,

Writing CPS

Test set up may be up in about a week

Server cert service will commence in June

Operational model

Stakeholder roles:

Comodo hosts infrastructure – CA, physical security

TERENA contractual party

NRENs – provide RAs

Organizations (NREN subscribers) – Subscribers, approvers (agents)

- IE at national level, there will be no need to touch request

"BigOrg" model

Pre-registers with its NREN

BIGORG identity – names, address, proof of legal existence

Registers its domain names

Then typical delegated practice

SmallOrg model

Similar, except NREN RA verifies & approves request

However, NRENs would prefer the "bigorg" model for all (ie delegate as much as feasible)

Server profile – subject names

C, ST*, L*, O, OU*, CN, unstructurename* (* optional)

Review of various parameters

Supporting OCSP

eScience (=GRID) server profile

dc=org/dc=terena/dc=scs C,O,OU*,CN

2 AIAs

OCSP

http://crl.tcs.terena.org/eScience_server.crt

These terena.org FQDNs are outsourced to Comodo

"The CN will contain a reasonable representation of the real name"

Requirement to IDP – users cannot modify (what – email attribute I think)

COMODO insists on having different issuers for certain combinations of attributes/keys so these will be 2 difft issuers.

Q: Do the "bigorg" models provide a CPS of their own?

A: NO

Q: How can relying party trust them? How do you assert the trust?

Q: about server certs

A: We must start the conventional server certs first – in June

Q: Bigorg vs small org model

A: Not that much different – just a question of what is pre-registered

TN: How does COMODO keep its accreditation

Choose auditor

Issue a random set of common names

Ask the registrars from customers to prove that these certificates were issued appropriately

You the registrar come up with signatures showing you checked items

We do not know yet how the personal certs are managed

RKM: How do bigorgs register a new domain name?

A: Register & wait for nren approval

NREN level RA holds this list of approved documents as a signed document –

NREGN registrar resets /rewrites this as domain ownership shifts. Then system is configured to accept this domain.

Can't issue certs in unregistered domains

DK: What profiles

A: Classic servers ; MICS personal

Separate accreditations for each

Q: How do you make sure domain is still managed by registered org?

A: Perhaps we can check the cached whois entry for changes

Q: What about subdomains (delegated to other legal orgs)

A: If the org doesn't tell us it's changed, well… it's the 2nd level that is important for commercial providers

Q: Is document in RFC 3647 format

A: No

Q: Wait – then what are we doing – maybe we are undermining our rationale here

A: It's an existing document – we do not always require people ot completely update their documentation & change to something else. There are also documents in the appropriate format but the complexity due to the style of writing it can be overwhelming.

SIGNET – update on NAGIOS

Been around since 2004 –

Also Asia version

6 hour cycle, checks CRLs, distribution consistency

Recent changes

Auto-update – For 2 years the distribution hcekc starts a configuration update handel

Check if you change distribution – it's likely that changes will cause monitor to become confused

Portability – due to Vinod R – downloadable as of this afternoon

Operational setup – now it's very simple – NAGIOS 2/3 installation

Local network definitions file

3 custom checking ploug ins – CRL/Cert/Distro

One handle that does autoconfigure

Issues –

Supposed to be an early warning system – starts warning early

What is the right model for CRL warnings (different types of CRLs &c)

More frequent checking? How about

CRL once an hour

EUGRidPMA availability every 15 mins

Possibilities

Show trending

Cache CRLs (because they are retrieved as part of the service)

More email? Leads to authN issues

Give administrators access

Could do more checking

What about saving mailing list warning messages?

Problems

AP – can't find it? Seems to be running today

TAGPMA blocked because slow response to Vinod R

http://signet-ca.ijs.si/nagios

Good moment to ponder CRL fail-over service

Q: Where is the download?
A: It has a bug – I will fix it tout de suite.

A: problems – embedded perl in NAGIOS is strange – tries to parse things, took me a while to fix this so it would be portable

Change your email address

Change your local host – and look at network connectivity attribute

5 lines to edit

Comments about multiple CRL access points

DG/MH/DO'C = CRL_URL file supports multiple urls

Not sure about the info file; DG thinks it might allow comma-delimited ones

Need to check

Alexey Tselishchev – CERN CA audit results

Certs used not just for grids but for authentication to machines & other purposes

Review of process & procedures

Review of Website & UI

You can map an existing certificate to your CERN account

CERN CA has about 2000 valid users, 4000 host certs (from remarks during presentation)

Looking for 2 audit reviewers.

Mike Helm, Feyza Eryol

Q: How does the audit review work?
A: (From CERN) I have a document that reviews the questions & response

Should check with the severity

A: It's like an operational review – initial review intermediate

---

MH on doegrids audit report

Group is happy with this

It's ok to stay in EUGridPMA, or remove to TAGPMA – continued.

MICS 4.4 (D Groep leads) – how do we deal with revocation when traceability is lost

DG vs Marg

Proposal from DG – suspend when traceability is lost

Marg – 10^6 seconds need check

Argument in TAGPMA didn't quite converge, so they approved the text they could agree on.

What are we trying to achive? & the problems understanding are common to most/all profiles.

DK: You have to address the underlying definition/confusion before agreement can be reached.

MS: We cannot expect the IDM managers to prevent authentication to any other service.

JB/JM: This language (what is on slide 3) is not in the current version.

The current doc says the IDM manager must revoke a certificate if the data changes or the traceability to the person is lost.

DG: What "data changes" – what does that mean?

Email? Unique traceability key?

JB: I am not happy with IDM managers revoking certificates – the CA operators control this.

JJ: IDM must request revocation

Legacy text suggesting optional revocation – this should be removed.

AI's : Fix the revocation

Change IDM manager must request revocation, not does revocation

Change "data changes" to something like "data that is basis for certificate issuance"

Change "all valid certificate" to something like "valid certificates issued to the member"

Some more changes - top of section 4.4 – DG

Going thru other changes – to slides

http://indico.rnp.br/materialDisplay.py?contribId=17&materialId=slides&confId=47

Why is there a requirement for 12 character passphrase for private key (ie explicitly 12 char)?

From classic profile

MS: The original IDM may not have this requirement

Move to approve the MICS changes, but add a suggestion to section 4.4?

1.1 is better than 1.0, so let's approve this and give the change to TAGPMA for comment?
1.1 is accepted, but the version with the edited paragraph at the top of 4.4
http://agenda.nikhef.nl/materialDisplay.py?contribId=16&materialId=0&confId=644

Thawte & PGP key siging?
Perhaps Thawte will be obsolete for our purposes in a year …..

Roman Brunner, Quo Vadis
Opportunity to participate in a grid CA program
Zurich financial services -> quovadis
Interest by ZFS in being in digital financial world.

QV team bought out founding company's interest later.

Why born in Bermuda?
ZFS in the re-insurance business was headquartered there.

Not many ppl want to build the PKI infrastructure.
PKI has bad public karma (aura).

QV has critical mass to provide
- Specialized registration systems for user experience
- Securie hosting
- Support for arcane PKI issues
- Audits & accreditations
  - Webtrust/ webtrust ev
  - EU etsi
  - We have main audits every 3 yrs, + annual reviews
    - Prefer the Dutch KPMG team
- Root CA distribution

Switz. has 4 orgs that issue certificates, heavily regulated
For example, electronic invoices

Services offered – managed PKI, signing services (time stamping), hosting

Root distribution
- Working on incliusion Adobe Acrobat, Java
- List is getting long
- Complex process for each application

Only commercial CA that has accreditations in multiple countries
We don't believe that there will be a EU-certificate profile uniform across the continent

Built QuoVadis Grid CA
Available for EUGrid membres' use
- Chained to QV root, simple interface, PKI management issues simplified

QV EUGridPMA accreditation & TACAR enrollment underway

Pre-vetted regirstration, accounts, and automatic issuance for institutions
A delegation model.

Q: Operate only in EU?
No, globally, but no office per se in US.

Jens Jensen soap box (# Nth)

What defines IGTF CAs?
[Explore the "identity" of the CA – what attributes define it ?]

Key, owner &c

Focus first on services: helpdesk, email, front end, back end signer, crl
Notification service – issuance, renewal &c both for subscriber and RA; unusual events
Repository – instructions, documentation
Publications - as per local law & requirement

In the IGTF context we require more
RPDNC - ?
CA manager's PGP key – TACAR
PMA membership/attendance record

PMA reviewer records; emails, spreadsheets
"minreq" and AP implementation

Where does this information go – it's sort of diffused in personal emails as this PMA doesn't want to track in depth the review history.

Also it is networks, DNS both internal & external
Machines & hardware
Note: machine running nCipher card died; they had a "new" machine, but supports old hardware interface, & it worked; so buying machines in the same class as backups.
Physical protection

CA internals
Database – logging & archiving
CA operator interface
Signing interface – hsm
RA database – management of the bureaucracy of this

People-roles
CA manager
RA manager – complex structure – need for an RA manager manager, and other roles to manage the list of RAs &c
Support – a lot of specialized skills and techniques

Auditing

Need people or resource;need training

Need "visitors" to travel to each remote RA O(100)

Manual trust

Photocopies of id

Appointment letters for RAs

Various keying materials

High availability services

Redundancy, monitoring

High integrity serices

Backups

2 kinds of accident

silent data corruption

accidentail deletion of file

High confidentiality services

Encryption, physical protection, release procedures

There are so many things that have to be taken into account running a CA.

Warm & Fuzzy CA (pax Ian Neilson)

Auditing schemes

LoA – level of assurance

Levels of – effort/expertise/inertia

It is hard to change course in a large CA

CA's "age" – the world was different when CA started out.

Catching up to this change

Dealing with decay/obsolescence/loss of materials

Odd age curve effects – if you've existed for a while, you're likely to continue, but if you're a new project, perhaps it is more likely to be knocked off.

Exceptional cases

Case by case problems (eg finding your disk drives are configured RAID 0)

Now to principles

"Render unto Caesar…"

Policy issues

Where is the balance between specification & implementation

The policies or the packages are mashed together and tagged with a single OID, but is inflexible to minor change/improvement

What are the real goals we are trying to achieve?

Eg think about LoA mapping that Scott Rea did against the US government standard, where we came out quite low [< Basic]

How do the APs relate to each other in LoA

Or are we making the problem too complicated – multidimensional things are too complicated.

Does it make sense to do both?

And now about the software

We have a dcache/grid ftp cluster with a thousand nodes to approve – this is hard to deal with – it is error prone because the process is not designed to do this.

As a result, humans are doing a computer/automatable task, and they are not good at this!

"Support" in general is case-by-case and not automatable.

Complexity has to go somewhere.

We are not getting the balance rite between the human / computer choice of work.

Unuseful complexity in the world

Firefox won't import certs from a file? Seems to behave strangely

Renewal for browsers is quite difficult

Signing policy –

Example – root CA that has non IGTF subordinates

Those are good, but not accredited – maintenance headache

See RPDNC document in OGF

Java clients software – STFC will release under some licensing

Conclusion

We don't understand CAs – we don't understand IGTF CAs, which have special rules –

GFD 125 > RFC 5280 > …..

Want feedback on soapbox – want to turn into lecture series

Outstanding incomplete document review

Operational profile for VOMS Attribute Authority – DK &al

    Some progress

Guidelines for operating on-line CAs – cited in classic AP

    Contradiction: those that have one, aren't writing one; those that need this, aren't here to demand it

Guidelines for operating online credential stores

    Christos T has done some work on this

    Need for "national credential stores"

        National/regional virtual smart cards

Various 1SCP's

What is the use case of this credential store, & what is it made of (myproxy, ldap, &c)?

Concern about general myproxy deployments – looking for policy for how to manage these well.

There are 5 people who volunteered to help with this, & this WG should start up a wiki & get started on use cases and policy discussions.

We need OIDs to identify the type of end entity – robots, host, server

DK: Who owns the 1SCP, & what is the process?

DG: Not really

DK: But if you want the pma's to use them DG: should be IGTF wide

DG goes thru the old documents

Personal hardware token

CA should describe how this is done

How can the key be cloned? Aladdin, for example, would have to generate key outside token

(which may involve a technical violation of FIPS 140, but difficult to tell on the face of it in which way the key was used).

WW: Perhaps we should restrict the key generation of these downloaded keys to a very restricted, offline system.

Some language is added to require the CA to describe the issuance process.

JB/MS: This is getting too complicated with all these exceptions – a lot of software crypto can meet this – why bother?

JB wants "the private key may not be transferred"

6.2.6 now reads, the private key must not be transferred into or out of the secure hardware token.

DG: Disqualifies HSMs … so if you're building a portal you cannot use hi quality HSMs.

DG: the only reason for having this 1SCP is to identify robots / portals.

Do robot portals need exportable, "backupable" keys?

A discussion about how to manage keys , portability, HSMs, and application support.

Title: Hardware token with non-exportable keys – new 1SCP

Details: 626/627: The private key must not be transferred into or out of the token, & is used only in the token.

Software based keys

JJ: Do we need this?
DG: it makes the set complete – to make a policy decision later

Seems reasonable

Entity definitions

Policy on automated client entities

Trying to define "robot"

Footnote references old GF draft on automated clients.

The argument about the naming comes down to, the certificate name should be what it "is" not what it "does", in that once the certificate is issued one cannot tell what it is used for (does).

The rationale for a personal name in the robot certificate is that this is what you see in the logfile.

Software doesn't parse OIDs, so must keep "Robot:" in common name

DK: it makes sense to describe the status quo

JB: We need to enumerate the known robot cases

JJ: Could list them in appendix

DG: and assign OIDs to those

Note: in the US we would probably have to have the ability to use a project or other kind of identifier rather than a person.

DG: We are documenting the status quo for now although this could be addressed in the future.

RKM – apache basic auth - the colon in these CNs may be a problem

In a PKI where we had the option to do so, we put a "space dash space" instead

This has something to do with how Apache interprets .htaccess.

JJ: We have a tenuous way of identifying robots across CAs we should not give this up

Discussion of the ":" and alternative character distinguishers

Allow the slash as an alternate separator

DK: Change the title to robot certs

Title changed to something like "Automated client and robot certificate"

You are a human

For completeness

Hosts

Postponed