EUGridPMA Zurich

13 May 2009 (Wed)

Day 3

The list of volunteers for large/secure credential stores:

MikeH

Jim B

David G

Christos T

JensJ

Reimer – Next meeting preview

We invite you to Sept meeting in Berlin

You must reserve by the end of August for the hotel (Ibis) – 15 mins/2 stops from office

So book by 3 Aug

Ring the doorbell – DFN – Verein – see the web site instructions !

Not returning to items of yesterday

Majid Arbol – Upgrade RFC 2527 -> 3647 (Iran CA)

Approved in May 2008 (based on RFC 2527 framework); we promised to upgrade to 3647

Used several community examples as basis for this upgrade.

Created a kind of mapping table – used this to move/translate text from one context to another.

Some things obviously translate into multiple locations, or multiple old locations move to a single rfc 3647 spot

Also many common “No stipulations”

Many new items such as

Anonymity

Revocation requirements (timeliness)

Q: How much time

A: 36hours

A: No it took longer than that!

Process for 4 months between the 2 of us.

Q: Which of the models were the most influential?

Brazilian for guide, Marko's for completeness/recentness

DG: Please attach your mapping to the agenda, ppl will want to see it.

DOEGrids cloning

Will it work

What about EU sites?

Christos K joins remotely – national virtual smart card proposal

Users do NOT want to deal with certificates!

But PKI is essential for distributed computing services

We have a general trend to move "standard operations " to the web, and

Using national "AAI" infrastructures as a more user-friendly identity service for users

Myproxy has advantage of being able to manage the important certificates to the users beter tha other things.

Pattern:

Users want to make long-term proxy, upload it to myproxy, & then stop dealing with their true long-term CA-issued cert

More patterns:

Everybody uses the browser to generate key pairs, & then export

Myproxy as a concept becomes focus of work, result is users upload long-term proxies to multiple services & have to trust these infrastructures.

Common problems – the level of incompatibility/process change from browser to browser rev to rev regarding certificate & key pair handling

Common problems - losing passphrases or private keys

Hellas Grid –

AAI to provide on demand certs

MyProxy service as the online CA to generate & store key pairs

Use the production myproxy service to use for proxy storage & delegation

Can we proceed on this?

This is a complete automation solution – user logs in, keys are generated, signed, & then storied. Possibly, the next step, proxy creation, is not automated.

JJ – has many comments

SLAC virtual smart card proposal

Also have AAI like thing in UK that does this – but we are not trying to accredit it

CK: Want to investigate a profile around this

JJ: Some of this difficulty is because the software is bad – perhaps if we drop the browsers & focus on java that will be better.

DG: Fundamental issue is generation & management of keys - how do we move this into our trust fabric.

JJ: About private key protection

Perhaps our policy is more of an implementation issue rather than a natural policy issue.

We are trying to ensure only the EE holds the private key in its use, so far the best way of ensuring this is by the user generation … interaction with users sharing name/password

Use MICS like arch based on federation account that you don't share as the basis

CK: I will provide a 2-level services. For most, access to proxy is enough. For others, they can download private key.

Discussion on limiting lifespan of proxy certs in myproxy – limiataiton on uploaded certs didn't happen until Dec 2008.

JJ: UK we have central one for NGS & GridPP – why don't you have one?

CK: For browsers we have one. But many have been brought up by communities (by randomness, design, need to have own infrastructures, &c); lots of credentials stored in various services of various qualities.

How can we control or regulate this phenomenon?

Would users take advantage of a secure service?

CK: Bring the myproxy infrastructure closer to the CAs

Q: How do you deal with potential liability if you as CA / myproxy owner manage or even generate long-lived keys?

JJ: Not accrediting these, so less concern

JB: Teragrid – we feel we can lock down & monitor more closely these infrastructure

The myproxy server helps us address security responsibility

CK: The fact that the keys are generated on myproxy doesn't mean we own it ….

The policies have to reflect it.

WW: We are now discussing secure tokens for key pairs, this (here) is a real step back, it's a single point of failure too – if there is a problem accessing it or an attack that destroys it or takes it

JB: But you can back it up or give it to user

WW: Then you have the problems of attacks on these stores

Will normal end users use (eg hardware) tokens? Not clear

DK: WG about this; the need for this credential store; the usage of tokens

JJ: Another option – more & better software to deal with this

How can you as a CA say, the CA is not owning, escrowing this key?

DK: there is a 3rd model where the portal owner or the credential store owner is separate & manages the key.

DG: WG should describe how the store is run.

MH: How does the proposed large scale cert backend interface to this/? Does the provider have issues

AU: what about various liability cases

What to do - defer to WG? Should there be a profile(-ing) of this

Once we write this down, will RPs rely on this?

Some will trust their OWN key generation schemes, but it's less clear about things that cross various organizational/national boundaries

MH: Worth thinking about OIDS and filtering profiles

JJ: How to restrict/identity secure servers

DG: Thanks for generating 47'50" of discussion!

… gap…

DG is talking about warm spares for EU Grid PMA distribution point

Possibly in relation to move at NIKHEF mentioned earlier? Yes.

Difficulty with "warm spares"

So the distribution committers will notice ssh server changes

There will be some other technical updates to committers

There should not be an outage pertaining to this, there will be an orchestrated management of changes;

Scheduled roughly mid-July.

David O'Callaghan

Checkcerts.pl

This is in EUGRidPMA distribution

Also look in EUGridPMA wiki for links

http://github.com/dsully/perl-crypt-openssl-x509

Others are welcome to work on GFD125 test suites

Proposed a summer student job to work on checkcerts.pl & test suite

---

DG: One document from 1SCP series – the others are on the agenda page

http://agenda.nikhef.nl/conferenceDisplay.py?confId=644

I am a Host certificate – the original 1SCP use case justifying this mini-CP approach

The interesting bit is 1.4.2 – statement about usage.

Forbidding client usage to some extent

JB: The GSPG pilot infrastructure permits pilot jobs to be submitted by a service certificate

The VOs wanted it to be service.

DG: You will have no assurance about who submitted that job.

AW: host certs are convenient, on the file system, & not encrypted

DG: This text came from Dutch Grid CPS where host certs should only be used to identify endpoints not as clients.

jJ: we should express the idea that the validation is typically only checked when used as server cert

subjectaltname content should be checked against the host name used

MS: Usage as server or client is expressed already by server/client KU bits

Idea about expression of trust is related to SAM cases (& perhaps VOMS AAs too)

Oops – this came up – putting in a statement that signatures from these host certs are not reliable indicator of identity or the validty of signature for some purpose (this is getting at the VOMS AA trust question).

Side note – some PKIs have hosts that can rekey themselves (but apparently RA is part of the approval process)

Discussion of various edge security cases that reduce the trust quality of these certificates.

Changing text in 3.1 to say “host or service” instead of something else

Intention here is the common name can contain anything (but you have to have at least one CN)

The SAN must have 1 or more FQDNs

JB: Only recent versions of globus look at SAN, so forbidding wildcards is not good

MS: Too many requirements in 1SCP – put them in profile

Keep to naming & appropriate use

But wait – the naming is in the profile.

So all this is left with is “I am a host?”

Are ANYCAST addresses hosts (yes & no – probably mostly yes)

Adding a section 3.2 for identity validation (of owner)

The entity MUST be a host

JJ: distinction here is we are identifying the EE not the subscriber, & the EE is in fact a host

Some concern about removing naming ; perhaps just reference 5280?

Decided to drop 3.1 entirely

3.2

The end-entity MUST be a network end-point ie a host or service

(There are various associated meanings involving services and endpoints but this should be clear enough – yes?)

MS: Now everyone can include the OID in certs

What's left;

Abstract; cert usage; "I am a host"

KB: How is this approved?

DG: Taken to OGF @ NC for approval

Review of OIDS and 1SCPs – see eugridpma.org oid tree

http://Eugridpma.org/objecteid/?oid=1.2.840.113612.5.2.3 &c

DG: I have been updating the OIDS in this branch in the OID-INFO registry (not everything , assignments to certain things).

Eric Yen on Asia Grid and federation CA projects

Looking at TERENA project

Review of motivation & background problems/requirements

Same problems as CK mentioned – users have problems with managing PKI; choose convenience over security

In Asia, national AAI infrastructure not there, nor national CAs &c

Interesting table of Grid programs in Asia (slide #3) – "Landscape of Grid in Asia"

A lot of Glite infrastructure

14 accredited CAs in APGridPMA – about 1000 users, 2000 hosts registered

Large range of applications

Objective for federations – slide 10

Ease of use; resource sharing – break down islands; reliability ; flexlbility; sustainability

What is path forward?

User POV: based on application

Do use case analysis within VOs from TW & EUAsiaGrid

Q: Could have been written about US – can you describe your requirements process?
A: Not yet – just getting this started!

General need to do requirements gathering & user requirements research…..

Q: Expect this to be used for other things?
A: Not sure yet

Q: Who is doing federation things – could they come to REFEDS? We at REFEDS should know – who is the contact person?
A: TBD

RPDNC – OGF document

Relying party defined name space constraints

Can we get it published in whatever state it is in now?

Has readable defs of what namespace is, and has examples

How to distinguish different types of names based on namespace – basically syntax and topo-graphy? Of names.

So read it at your leisure in the next week and then comment, or don't comment

Except for those who physically appear at Chapel Hill, who MUST say yes, and then it will be submitted.

Audit framework – Waiting for Yoshio to consolidate comments & complete (Jinny will be there)

Discussion of some comments –

Need for other profiles to be equivalently done

DK: What about more public wiki access?

DG: Don't have to register with David, now it will do this automatically

MS: What is going to happen if OGF disappears - attendance is low

DG: Chapel Hill is not expected tobe big, designed to be a small meeting

MS: Still….

DG: Impact on IGTF – nil. Need to organize a venue, to cohost with PMA meetings.

MH: Is Banff in Oct the first of those?

DG: It's a special circumstance

We need a publishing venue for certain things

What about Chapel Hill?
Discuss traceability

May 28 workshop dates for CAOPS – OGF

Thanks to Alessandro and the rest of the team at SWITCH for hosting us!