

**Minutes of 10<sup>th</sup> TAGPMA Face-to-Face / 1<sup>st</sup> IGTF All Hands Meeting,  
16-17 Oct. 2009  
Banff, Alberta, Canada**

11 Jan 2010

Note takers – Dave Kelsey, Doug Olson

Agenda with slides is at <http://indico.rnp.br/conferenceOtherViews.py?view=standard&confId=66>.

## **16 Oct. 2009**

Attendance list posted at

<http://indico.rnp.br/materialDisplay.py?sessionId=3&materialId=0&confId=66>

plus Andres Holquin on the phone, Irwin Gaines on streaming.

### **1. Welcome from Roger Impey and Scott Rea**

- today will be more IGTF focused and tomorrow will be more TAGPMA specific

### **2. Quick round of introductions.**

Adjustments to agenda and list of IGTF topics are:

- Private key protection
- Signing policy files to allow non-IGTF CAs
- Naming for robot certificates
- Incident response
- an IGTF document (private key protection?)

### **3. TAGPMA Update – Scott Rea**

- see slides
- First F2F meeting since election of new officers
- 2 classic CAs are pending accreditation
- 23 members, 2 in suspension status, have had discussion with Jim Jokl (UVA) who expects to become active but no news from Greg Barnes (Purdue)
- next F2F planned for Lima, Peru, May 2010

### **4. EUGridPMA update – David Groep**

See slides.

23 of 25 EU member states (all but LU, MT) + AM, CH, HR, IL, IS, MA, ME, MK, NO, PK, ... (map should include South Africa)

Talks about Federation developments in the EU - Switch, Germany and new TERENA SCS. TERENA SCS will be expanding to more countries also starting 2010.

Robot certificates implementations on hardware tokens. Why hardware tokens since proxies are used?

Naming for robots.

Have started doing compliance update sessions and post-mortems following operational disruptions.

3-4 CAs/meeting provide self audits.

Next meetings are Jan2010 – Dublin, April 2010 Riga, LV (future ones listed in slides)

## **5. APGridPMA update – Eric Yen**

See slides.

14 accredited CAs. New members are ThaiGrid and Mongolia. 877 user certs, 1729 hosts. (across all CAs).

More than half have completed inclusion of the OID (of profile).

Room for improvement in IGTF RAT response.

New SLCS and federations CAs are happening.

Issues with CRL updating. CA auditing happening. Next F2F meeting could be at ISGC (Taipei) in March 2010 – to be decided in next video conf.

## ***Break***

## **6. IGTF History - David Groep**

See slides.

GFD I.030

1999 EC rule to establish national PKIs – didn't work, Grid CAs were set up.

First meeting of EDG CA Coord Group in December 2000.

2003 Tokyo Accord lead to EUGridPMA, APGridPMA.

2005 IGTF was formed. Many interesting details in the slides.

Alan S asks whether the PMA charters are sufficiently technology independent. David G thinks so, and points out the other federation activities have a problem including relying parties as there are so many of them.

## **7. IGTF All Hands open meeting - issues**

### **7a. Private Key Protection issues.**

Neil W shows slides from Australian Access Federation (ARCS) SLCS CA. (shown yesterday in CAOPS-WG). A use case has emerged where a web portal (authN by Shibboleth) needs to generate a certificate with users who want to know nothing about certs. How/where does the web portal generate the key pair for the Grid cert?

They have two possible solutions:

1. Allow web portal to create a key pair and request a cert under DN of the user. (SLCS delegation)
2. SLCS proxy. SLCS proxy service creates a certificate then stored in MyProxy and issues a proxy to the web portal.

Neil asks is one better than the other? In case 1 the relying party cannot distinguish between the web portal or direct from a users own laptop.

David G. shows document, draft EUGridPMA guidelines on key protection.

These were first drafted in OGF26 in Chapel Hill. The current AuthN profiles say the user must generate the key pair. This is often not the case because they are generated on shared machines managed by others.

These new guidelines address this issue. David G presents these. If this gets accepted then all AuthN profiles will need to be updated to refer to it. Christos K reports that ESFRI projects in EU require easier AuthN without having to manage certs. Important for IGTF to support these types of use. Jim B says TeraGrid also have very similar user requirements. Collective editing of the document starts. Text was agreed. TAGPMA will vote on this at its next video conference. See email from DG 16-Oct-09.

**7b. Jens advertises a document grid CAs.**

This will be based on his various soapbox talks. He shows a draft. Probably to be an IGTF document aimed at everyone interested in these topics. We agree that this is a good idea. Alan S proposes that we need more information for the public, e.g. wikipedia articles.

----- *lunch* -----

**7c. IGTF Globus signing policy for HLCA - Jens**

Jens describes a use case (UK NGS) where a CA hierarchy exists with a non-IGTF accredited CA signed by an IGTF-trusted root CA. He proposes to permit Trusted CAs (i.e. HLCAs in the IGTF distribution which do not themselves issue EE certificates) to have more permissive signing policy files in the IGTF distribution. Otherwise relying parties wishing to trust IGTF CAs and the non-accredited CA would have to modify the signing policy of the root CA.

Extensive discussion follows! Several people are very concerned and feel that non-IGTF CAs should not appear in the IGTF-distributed signing policies. If needed, projects should create modified distributions for their RPs use.

**8. Review anomaly in the MICS profile.**

Section 3.1 paragraphs 1 and 2. Marg summarizes how MICS is supposed to work. See email from Mike H. 30Sep2009. Defers to an authoritative source for identity. If it works for their payroll needs, for example, then it should work for us. The profile does not require re-vetting every 5 years. David G points out that the Classic profile does not actually require face to face identity re-check at the 5 year point, either. We agree that nothing needs to be changed.

**9. PSC SLCS CA presentation - Derek Simmel.**

MyProxy CA replacing an ageing KCA. See slides. A partner in TeraGrid.

This CA is a backup for the accredited NCSA SLCS CA, in case network connectivity is lost to NCSA. Shows CA hierarchy. Same RA as NCSA-SLCS and same user database. Separate but similar namespaces. CN is same in both cases. All cert requests are authenticated via Kerberos 5. TeraGrid users will get both NCSA and PSC DNs into the DB.

Describes the HSMs. Scott asks who will be the TAGPMA representative for this CA? A: Derek Simmel. Letter has been given to Doug. (This is different from Jim Marsteller being the TeraGrid RP member).

TAGPMA vote to accept PSC as a member. Nobody objects. Membership accepted.

Jim B is the mentor. Scott calls for two reviewers - Doug and Marg appointed.

--- *coffee* ----

**10. Jim B - IGTF Risk Assessment Team**

See slides. Shows RAT responsibilities. Membership open to all IGTF members.

Shows recent RAT activities and shows timeline of Audit 2009-01.

Second test (Aug09) was a communications test. New web mailer will send individual mails to CAs to avoid SPAM filters.

Move from SHA-1 to SHA-2 could start early 2011. Null prefix vulnerability, PureTLS in Java Cog. Please announce service disruptions on igtf-general.

EUGridPMA plenary meetings will have an agenda slot to discuss operational issues. Scott (TAGPMA) and Eric (APGrids) agree that their PMA's will also do this. Post mortem should go to the mail list. Can also be covered at fortnightly meetings.

Jim proposes an IGTF RAT person or persons. Jim B wants to reduce his efforts in this area. Jens has volunteered. More are welcome. Still operates by consensus. We all agree to the need for a chair.

Jens J. has volunteered to chair. Applause to endorse him

Enough RAT members present to approve JJ as chair.

See [Tagpma.es.net/wiki/bin/view/IGTF-RAT](http://tagpma.es.net/wiki/bin/view/IGTF-RAT)

### **11. Jim B - CILogon CA**

See slides. A new CA funded by a new award from NSF. Facilitates campus login to NSF CI (cyber infrastructure - new word for Grids). Bridge from InCommon to X.509 PKI for the CI. InCommon is large and growing (160+ univ., 3.6M users). InCommon Silver Identity Assurance Profile defines common standards. Silver satisfies SLCS requirements. Will run two CAs - Basic and Silver/IGTF. There is a Silver pilot project with 3 institutes right now and then add 10 large institutes. Compares new CA with the NCSA GridShib CA. Latter was serving only TeraGrid users. Need to rely on id vetting of institutes according to Silver accreditation.

Milan: would you have an agreement with InCommon? A: yes. Will be a SP and have a process for getting back to the individual.

Shows demo of <https://go.teragrid.org> Java software available from gridshib.globus.org. Jim agrees that he needs to work with CI projects to address ease of use for non-expert end users. Shows timelines - prototypes by April 2010 and operational in Sep 2010. Would like to have accreditation about April 2010. Need to identify reviewers (after next topic).

### **12. Jens - Robot Key protection issues**

See slides. Issues discussed at recent EUGridPMA meeting. Private key protections for robots, first. (Mainly how it is stored).

2 use cases - Automated clients and Shared certs.

Current requirement - on hardware token. Pros – holds > 1 key, can renew cert, can have IGTF robot.

Cons – costs money, needs software, RA has to witness key generation.

Reimer has described an attack – generate enough proxies to last full life of the cert. Token gives you no extra security. Discussion on attack methods. Classic profile currently requires a robot cert to be on a token. Keith notes that the FNAL SLCS CA can get robot certs. General feeling is that this is another form of personal cert (even though it has ou=robot).

Options: ignore proxies, allow soft keytokens, consider restricting the lifetime of the robot cert (short lived). If hardware token key is activated there is little increased security of unencrypted key on local disk. Jim B says it gives us no extra security and is actually impeding community take-up of robot certs.

Conclusions of very lengthy discussion: There are some security benefits in use of a hardware token.

Appropriate robot naming allows restriction of activity (via authorisation). Several are pushing for dropping the requirement to use a hardware token. We agree to investigate whether the new Private Key Protection guidelines can help. We need to come back to the naming issue later too.

**17 Oct. 2009**

<http://indico.rnp.br/materialDisplay.py?sessionId=4&materialId=2&confId=66>

plus Irwin G. on streaming.

**1. Review of today's agenda.**

Still some items left over from yesterday. Shuffle topics to allow remote participation.

**2. Keith Chadwick - Experiences for CRLs as a Relying Party.**

See slides. Shows details of FermiGrid. Update of CRLs on many systems every hour using a Squid-HA cache. Cache hit rate in excess of 95%. >2M downloads through the squid server per day with actual download of just over 100k per day.

Roger asks why his CA sees many download request from the same nodes every few seconds (e.g. CERN does this). Shows details of http headers in the 94 CRLs. Conclusion - most CAs not publish squid-friendly CRLs.

Jim B questions whether CAs should set a CRL next update as they may wish to revoke a cert and get this downloaded quickly. But, revocation procedures often take hours or a day or two.

Keith reports that when CA is down he receives 1000's of failure messages. Shows CRL download incidents. #2 is not an IGTF CAs.

Shows list of requests to CA operators.

- a. Add the appropriate http headers to specify your CRL modification time, expiration time and maximum cache age.
  - Don't specify "no-cache" on your http header.
- b. Don't shut your CA down without establishing an "alternate" location for the CRL downloads;
  - Especially when you may be / are having a security incident.
- c. Verify the changes to your CA infrastructure;
  - Especially immediately after publishing new CRLs.
- d. Monitor your CA infrastructure overnight and the weekend.
- e. Have a disaster recovery plan;
  - And test it periodically.

Milan is concerned that he cannot satisfy all customers at the same time. Others disagree as processes are known to be long.

David G refers to his earlier analysis on this; some sites have all worker nodes individually downloading, some sites have wrongly configured squid caches.

Christos reports they had big problems in August when they thought they were under a DOS attack because of a badly configured site.

David G points out that fetch\_crl has a configuration option for tolerance to intermittent faults.

Agreed: ACTION ion Keith to prepare web-page recommendations on this issue. (also including David G's La Plata presentation)

**3. David G - TERENA TCS Grid CA**

See slides. First 9 slides rushed through. Many different federation technologies in EU - interoperation through SAML 2.0. Shows the methods to meet the requirements of MICS; persistent unique names and reasonable representation of person's name. There will be O(200) IDPs in the initial cross-federation.

This is the first MICS federation CA. Shows details of TERENA's certificate services including the "TERENA eScience Personal CA". EUGridPMA accreditation is well underway. CP/CPS near to completion. Scott asks about WebTrust audits- has to go all the way down the chain. A: the personal cert service is different and is not required for WebTrust. Scott disagrees. The vendor will take care of the audit section of the CPS.

Marg asks what the Confusa portal is. Open source see confusa.org.

Back to the WebTrust audit question - Milan points out that the TERENA SCS service has been in operation for several years.

Scott suggests that additional documentation may be required describing processes at the host institute. May all change when TAMP comes out.

#### **4. Scott - back to Jim's CILogon CA.**

We need a mentor and reviewers. Reviewers: Scott and Roger (apprentice!).

No volunteer as mentor right now. (Jim M could be asked, perhaps).

#### **5. Yoshio - Audit Guidelines document**

As discussed in CAOPS-WG this week. Public comments period is over, several comments received. This will be addressed by Yoshio by end of November. It was also agreed that a separate spreadsheet checklist will be produced (with help from Alan S).

Scott asks what the EUGridPMA position is on external audits, given that APGrids PMA requires annual audits. A: would be nice but there are costs. Really a matter for relying parties to say whether they require it.

---- *coffee* ----

#### **6. Andres - UNIANDDES (Columbia) CA presentation**

Introduces the University. CA will be hosted in one of the two Tier-3 data centres. Part of EELA, ROC\_LA, CMS/CERN. Users in HEP, Comp. Science, Biology, Chemistry, Bio-medics. Requests from external users are there with more expected. 1st draft of CP/CPS has been prepared - Classic profile. Legal office is reviewing then will be sent to TAGPMA. This should happen in December. Implementation by May 2010. Scott: once CP/CPS is available TAGPMA would then like a presentation on the details of the processes. Mentor is Vinod. Reviewers are Alejandra and Jens. Can they get access to the draft CP/CPS now to start the work in parallel. The only problem is that the original is in Spanish and translation still has to happen. Both languages will need to be published. IGTF will require operations to be consistent with the version in English. The English version is the official version.

#### **7. Doug - OSG-ESnet IdM workshop**

See slides. This will happen in 3 weeks. Reviewing technologies and OSG stakeholder requirements.

Survey of all VO requirements too. ~15 are already in.

Scott points out that Liberty is missing - A: they are not looking to invite more at this stage. Suggestions welcome.

----- *lunch* -----

#### **8. Jens - Robot naming**

See slides. Cert should name the end entity. For robots they currently also name the owner (no standards here) - the person responsible for the certificate, may also be responsible for the robot using it. Shows the CERN proposal to EUGridPMA. They do not want to name the responsible person. This is "cold and clear" (opposite to warm and fuzzy!). CA may be unwilling to divulge ownership details. Keith: as a RP I need to get the contact info from the CA. A: But not all CAs are able to do this (if not allowed by the CP/CPS and/or laws). VO registration data should maintain the contact info and Grid operations should have access to this. EUGridPMA was very concerned that the name should be there. Jim B would like to adopt robots but EUGridPMA keeps changing the specs so he will wait until it has settled down.

Agreement: EUGridPMA should produce a Guideline document on Robots, including naming and key storage. The question of warm and fuzzy DNs containing a name of real person is still not clear - there are conflicting views. Needs to be continue to be discussed as part of producing the guidelines.

### **9. Jens - Host certificate validation**

No slides. Some UK RAs do things differently when validating the ownership of a host, prior to issuing the certificate. Jens asks if we can do better. Milan has no RAs at institutes so a representative at the institution has to approve the request for a host cert. Scott describes the procedures they use at Dartmouth. Jens: audit of the UK RAs tends to concentrate on the personal certs and not host/service certs. All agree that the IGTF policies are fine and correctly specify the RA obligations for host certs. The issue is more related to the processes used by particular RAs and how does the CA satisfy themselves that the procedures are sufficient. Jens says he will review his RA guidance documents.

### **10. Dhiva - DOEGrids CA update and new projects**

See slides. DOEGrids CA with High Availability (continuity of operations). Includes a distributed netHSM. Already in operation with local deployment. Within next few weeks will start to implement remote operators and locations. Shows results of Cert Profile compliance tests.

New projects - Shibboleth and OpenID. Working on a shib CA to issue short-term certs. Dhiva shows the roadmap for their Shibboleth project and gives a demo. Then shows the shib twiki.

Next, moves on to their OpenID project. OpenID is an authN protocol allowing single sign-on.

Decentralised - user can choose their IdP. They plan to implement an OpenID IdP and create a CA using this and a Twiki.

Gives a demo. The OpenID plugin for twiki is limited in functionality. Does not support groups or registration. Describes some problems with OpenID; phishing (but cert-based authN solves this); can OpenID be used with non-web applications? (answer not really but maybe if modify the legacy application); OpenID exposes user info (but could give user ability to control release); OpenID ids are persistent and global and behaviour can be studied (could give users a dynamic identifier).

Looks at differences between OpenID and Shibboleth. First is open Trust model, second is federated trust. For OpenID there is no "club" to join and there are therefore no rules. US Federal government is trying to "standardize" OpenID Operators (ICAM and TFAP) to adopt OpenID 2.0 for low-risk transactions. Dhiva shows their future plans.

----- *coffee and key exchange* -----

### **11. Vinod - reviews the membership list.**

Members can request alternates be defined. Also shows the CA spreadsheet. Vinod will generate PDF versions and make them available. David G describes how he manipulates CA data with PHP for display. Vinod will do the work.

Continue to review the membership.

Purdue has been inactive and not responded to attempts to contact them. Vote to drop them. Agreed. Looked at the 6 CAs working towards accreditation. We need a volunteer to be mentor for San Diego. Perhaps Shreyas will be willing (Scott to check). A number of TAGPMA CAs are missing from TACAR. It seems that the instructions for what has to be done for TACAR is not clearly stated on a web page. Milan says that Geant3 is looking for any future requirements for TACAR. Please send to him, Licia Florio or the list.

#### **12. Scott - Headsup.**

Sometime soon HEBCA is likely to be seeking accreditation.

#### **13. Scott - Computational Framework for Cert Policy operations.**

See slides. Our accreditation procedures are somewhat similar to mapping in bridge environments. Our process is also fairly subjective. Scott and colleagues are working towards automating some of this. They are using TEI-XML. A PKI Policy Builder exists and also a Policy Reporter. This is much faster (at least 60%) than manual processes. Also much better at finding SHALLs, MUSTs etc. The Policy Mapper can transform 2527 format to 3647. Repository is available at <http://pkipolicy.appspot.com>. Scott shows an analysis of how many CAs are making policy documents available over SSL (one third) and only one signs it. Milan notes that TACAR serves policies over SSL. What would you sign the policy with? Could be the cert of the chair of the policy authority. There are still 45 CAs in 2527 format. Scott offers to assist in the translation to 3647. There may be a new RFC to pull together sections on a topic basis. Shows a demo. Comments from Milan on his experience: issues with pdf to text converter and also problems with the handling of sub-sub-sub-sections. It is very good at converting from old to new format. Scott reports that they actually found an error in the RFC!

#### **14. AOB**

Peru will host the next F2F TAGPMA meeting in first week of May.

Offer from Alan Sill, Lubbock, Texas to host Oct 2010 meeting (Oct 3-6), to celebrate the 5th birthday of IGTF.

Next video conf is on 4th Nov.

Big thanks to Roger for all the arrangements at this excellent meeting.

Has this been a useful experience re the first IGTF All Hands? General agreement that it has been a useful experience. In future could be an annual event rotating around the regional PMAs. Could be a way of engaging more relying parties. Scott proposes that we should plan to have one in 12 months time to review how we are progressing with federated CAs. BUT.. a meeting in Europe in September could be difficult with the Lubbock meeting in October. Marg proposes that we should have a specific agenda for All Hands meeting to make sure we address joint issues. Meeting should be joint with a PMA meeting and hopefully in an easy location from travel point of view.

#### **Adjourn**