5TH TAGPMA F2F MEETING
16-18 JULY 2007
BANFF, ALBERTA, CA

Minutes respectfully submitted by Marg Murray, TAGPMA Secretary.
Comments and corrections are welcome. Please send to tagpma list.

Monday 16Jul07 Day One	
Local Participants	***Remote Participants***
Bob Cowles, OSG, SLAC, US	Israel Becerril, UNAM, MX
Irwin Gaines, FNAL, US	Duncan Brown, Chicago
David Groep, NIKHEF, NL	Shreyas Cholia, NERSC
Vanessa Hamar, ULAGrid, VE	Nuno Dias, LIP, PT
Mike Helm, DOEGrid, ESnet, US	Guangshun Huang, Norman, OK
Jens Jensen, Rutherford Lab, UK	Lia Molinari, UNLP, AR
Marg Murray, TACC, US	Doug Olson, DOEgrids,ESnet, US
Darcy Quesnel, CANARIE, CA	Dhiva Muruganantham DOEgrids,ESnet, US
Vinod Rebello, UFF, BR	
Scott Rea, Dartmouth, HEBCA, US	
Alan Sill, TTU, HEPnet, US	
Milan Sova, CESnet, CZ	

TAGPMA CHARTER REVISIONS

Current charter V2 dated Dec 2005. Tony Genovese started making changes in the May 2006 timeframe.

Proposed changes:

- Fix date.
- Remove people names; replace with org names.
- Section 12.2 Chartering Procedure: Bring process up to date.
- 12.3.4: TAGPMA needs somebody to be a "trusted introducer" for TACAR, The chair should have a means to present a necessary position (e.g., Security Officer, archivist) and then select/delegate/recruit for it.
- 12.3.5: New or renewing membership process. We should have our own process. Define membership vs. accreditation vs. relying parties vs. CA operators.
- 12.3.6: We need an organized way to hand over responsibility/authority. What to do when people change jobs? We need to address procedures for membership transitions and ownerships. Who is the member? (person or institution) Original charter was based on members as people. Change to: members are organizations represented by people.

ACTION: Alan will update/edit Charter and will send it out to the list. After some discussion period (1 month) there can be a vote.

ACTION: Alan offered to setup the svn repository within 2 weeks. Marg can assist.

TAGPMA REVIEW PROCESS AND TIMELINE

Discussion of Jim Marsteller's 20Jun07 document occurred.

A TAGPMA community applicant needs opportunity to decide the organization's membership role: CA Operator or Relying Party. Newcomers need a mentor first . If they pursue CP/CPS accreditation then they also need reviewers. Community members serve as reviewers or mentors on some regular basis. Clarify that more than one in-person attendance at a F2F meeting is required to meet accreditation and community service parts of TAGPMA process.

Although it would be timely to do the operational review at the same time as the CP/CPS accreditation, the vote only applies to accreditation. Passing operational review must occur before accredited CA gets into IGTF distribution. A CA can go operational within local context prior to operational review for IGTF distribution. It is up to Relying Parties (and not the TAGPMA) to decide whether or not a site will accept certificates from an accredited CA.

It would be useful to consider the re-accreditation process in the diagram and to encourage RFC3647 CP/CPS format. TAGPMA-provided templates and tutorials can promote self-consistency within candidate CP/CPS documents and facilitate accreditation.

ACTION: Alan and Scott will revise the process diagram and present to group.

IGTF UPDATE

Yoshio Tanaka is the current IGTF Chair.

Notes from Yoshio Tanaka's slides:

- There are compliance problems between old CAs and evolving APs.
- It is instructive to have CAs do self-audit using Yoshio's audit document.
    - Failing a self-audit can yield a remediation plan.
    - What are grounds for removal of a CA from the distribution? Failure of audit? Failure to remediate? What do Relying Parties say?
    - Some CAs had to be removed from the IGTF distribution for cause (e.g., bad CRL download, trailing space(s),
- No progress to date on portal-based credential services.
- It is up to individual CA / RA to decide how they will handle identity documents. The obligation is to provide auditable traceability.
- Don't put OIDs in Root certificate. For subordinate CA certificates, include the OID of the policy under which it was signed.
- Existing Authentication Profiles can work. It might be better to register, rather than accredit, CAs for which current APs are a barrier.
- Related IGTF work available on: https://forge.gridforum.org/projects/caops-wg

EUGrid PMA Update

40 accredited CAs (39 Classic and 1 SLCS)! Currents applications: Romania, Morocco, Ukraine, Latvia, Iran, FYROM. Byelorus is problematic due to travel restrictions. Only Luxembourg, Malta and Moldavia are missing from EUGrid PMA!

New developments: UK, NL and CZ plan to issue certificates for robots or automated clients; CRLs for compromised CA;, non-repudiation bit in keyUsage; meaning of Locality; LoA and management of hardware tokens. More contentious issues include object signing bit usage; frequency of self-audit. What if CA gets accredited and then the AP changes?

RECOMMENDATION: Plenary meeting attendance once every 1-2 years would help CA operators to stay current with issues. Upcoming meeting Nov 29-30 in Malaga will focus on attributes.

Operational Review

We need a reviewer's guide in addition to the Operational Review spreadsheet initiated by Mike Helm. How to facilitate OpeReview? (OpReview requires checks of CP/CPS.)

- List commands used. (How reviewer checked something.
- Evolve this document as reviewers perform operational reviews.
- Promote consistency and best practices. Provide more comprehensive checklist and technical details.
- Cause of some problems may be the length of time between CP/CPS approval and Operational Review
- Automated checks? (e.g. nagios checks)
- Reviewers not at site can not verify physical procedures.
- Must rely on self-audit and provide guidance to CA operators.

TAGPMA Tutorials

ACTION: Marg will solicit "tutorial wishlist" information useful to CA operators:

- Survey of specific implementations (HW/SW used.)
- How to setup a CA using openssl.
- How NOT to use default OpenCA.
- Sample config files for different software:
    - Microsoft CA
    - RedHat CA
    - Baltimore (Unitrust)
    - EnTrust
    - Use of commercial CA services
- NIKHEF key token tutorial at http://ca.dutchgrid.nl/info/etokens
- Information on HSM config.
- DOEGrids GridAdmin interface
- Scott Rea has some materials.

ACTION: Dhiva will setup a TAGPMA wiki by the first week of August. Wiki will be a place to host and manage tutorial development and document best practices.

If TAGPMA solves the problem of key registration and management (What is authentication type? What is the trust anchor? Contact detail?) this could be beneficial to the larger community. There was a discussion about TAGPMA CA vs. Thawte certificates vs. signed PGP keys vs. authentication tokens. Note: TACAR V2 policy currently requires PGP (or attend meeting). If TAGPMA writes up a draft policy change for TACAR V3.0 that includes S/MIME (or video-conferencing?), TACAR would be open to discussion. Milan offered to facilitate communication with other leaders. He plans to present something at the Sept. TACAR meeting. Would it be possible to have the same TAGPMA ID for the INDICO server, the wiki and the Drupal part of the website?

AUTHENTICATION PROFILE UPDATES

SLCS

Discussion occurred concerning HSM as a barrier.
SUGGESTION: Use a USB Alladin etoken for the HSM.

SLCS Profile language hasn't yet been upgraded to language in Classic and MICS.

ACTION: Mike Helm: Revise SLCS AP to be consistent with other APs and allow compatibility with e.g., Shibboleth. He has a list. Originally was aiming for Manchester mtg. Next OGF is in Oct. Jim Basney is 'helper'. Targeting completion within a few weeks.

MICS

EUGrid PMA wanted one word change ("must" to "should") in section 3.1.
APGrid PMA suggested additional "must" to "should" change of criticality in keyUsage to cover case where a commercial CA service is used.

ACTION: OGF 20 Manchester attendees! There was a discussion at OGF 20 Manchester during the CAOPS session about eligibility of entities for certificates. Could anybody who has concerns or suggestions please forward these to the editor (Marg) or to the tagpma list?

ACTION: Marg make changes: Use all caps to indicate that meaning is not common language. 'MUST' and "MUST NOT" "SHOULD" "SHOULD NOT" "MAY" "RECOMMENDED" "SHALL" "SHALL NOT"

CLASSIC

URL should report the DER-encoded (not PEM-encoded) form of CRL.
Discussion ensued about caching with squid proxy caching, OSCP and CRLs.

TAGPMA STATUS MATRIIX

Green is misleading. We need additional colors to show:

- Conditional acceptance
- Reviewers have approved.
- TAGPMA voted to accredit.
- Status process needs to match workflow process.

Tuesday 17Jul07 Day Two	
Local Participants	***Remote Participants***
Bob Cowles, OSG, SLAC, US	Duncan Brown, Chicago
Irwin Gaines, FNAL, US	Shreyas Cholia, NERSC
David Groep, NIKHEF, NL	Nuno Dias, LIP, PT
Vanessa Hamar, ULAGrid, VE	Sandra Jaque, REUNA, CL
Mike Helm, DOEGrid, ESnet, US	Guangshun Huang, Norman, OK
Jens Jensen, Rutherford Lab, UK	Lia Molinari, UNLP, AR
Marg Murray, TACC, US	Doug Olson, DOEgrids,ESnet, US
Darcy Quesnel, CANARIE, CA	Dhiva Muruganantham DOEgrids,ESnet, US
Vinod Rebello, UFF, BR	
Scott Rea, Dartmouth, HEBCA, US	(VRVS problems pm)
Alan Sill, TTU, HEPnet, US	
Milan Sova, CESnet, CZ	

ULAGRID CA UPDATE

Vanessa Hamar made two presentations. The first presentation covers an update of the ULAGrid CA status.

CP/CPS document version number doesn't need to increase until after production certificates have been issued.

Non-repudiation bit should not be set on CA certificate because requirement can not be met. Some harm to the value of the key pair occurs when you use the NR bit . EU qualified cert infrastructures cannot interoperate with digital signature PKIs. (For example: somebody may send you a hash that you sign to authenticate, but this "hash" may actually be a *document* that Mallory wants you to sign for nefarious purposes.

RECOMMENDATION: Key sign and CRL sign are the only keyUsage bits to set on CA certificates. Remove certificate policy OID from Root CA certificate. Drop Netscape extensions. For subordinate-CA and end-entity certificates, only publish the unchanging part of the certificate policy OID. LoA best avoided, if possible (Jens disabled it.) Learn from previous mistakes, improvements in grid security middleware, PKIX profiles and recommendations.

Lessons Learned (CA tricks and troubles).

Vanessa asks whether to use 'make-ssl-cert' with Apache or is there something else? One alternative: create a key-pair on the machine and sign it using an existing CA. Then change the Apache config to use it. It is useless to serve a Root CA certificate over an SSL server that chains to it.

Vanessa presented a description/guide on how to build/install/configure openCA.

There appears to be file management problem with OpenCA-in-a-box. Are there some kind of security measures to discourage copying keys and certificates out of ram?

- Timestamp bit is only for a service that stamps a document with a date and then signs it.
- Object signing bits are problematic.
- dataEncipherment bit is not used in any context we use.

Vanessa's slides will be very useful as basis for a TAGPMA tutorial.

Scott Rea: If there are any specific questions about OpenCA (especially OpenCA-in-a-Boox), please send them to him.

ACTION: Vanessa will make changes to CP/CPS and to her CA. Once her reviewers give the OK, then Vinod will schedule a TAGPMA vote at a conference call.

ACTION: Arrange for secure (authenticated) voting mechanism.

TACC MICS CA UPDATE

TACC CAs intended to meet needs of multiple grid communities. TACC MICS CA addresses short-term certificates so as not to conflict with TX mandates. First candidate IdM is UT-System Shibboleth Federation: a well-organized instance deployed on all UT-System campuses with appropriate governance, policy and technology. There are currently 10 UT service provider applications (SPs) and one commercial SP. The TACC MICS CA is a new SP.

TACC MICS CA CP/CPS describes UT-System Shibboleth IdM in Appendix A. Two additional potential IdMs (Texas A&M, TTU) can be added later via additional Appendixes.

RA handling is split between IdM and TACC. Basically, each campus IdP is authoritative for organizational identity data, while TACC is authoritative for project and grid identity data. The campus IdP sets an LoA attribute that indicates whether a face-to-face meeting occurred where identity documents were validated. A face-to-face meeting with a TACC designated RA is also required to check DN uniqueness, project allocation status and VO membership.

Generating only hort term certificates means no CRL, but implies occasional to frequent renewal. What about long running jobs? It appears that user can fetch job output with renewed certificate because job output is based on DN. Also, short term cert can be used to obtain a proxy certificate (e.g. with VOMS extensions)

RECOMMENDATIONS: Reverse the field order in the TACC Root CA certificate. Simplify namespace, moving all RA-identification data into optional certificate extensions. Use "O=" for TACC MICS CA and UT-System Shibboleth IdM. Use "OU=" for specific campus.

Tomcat 6 / Java2 (SDK 1.5) grid portal development is based on Gridsphere 3 with integrated Shibboleth login (ref: Dr. Aizhong Lin) or direct portal login. Both logins integrate to the same underlying TACC TAS user management database.Portal app can check LoA and can handle hardware tokens (required by HIPAA data users).

CA currently checks for re-use of eduPersonPrincipalName by validating email, address and phone number. If anything changes, re-registration with the RA is required. UT-System IdM is aware of re-use problem, and is developing a guaranteed unique identifier.

SUGGESTION: Store cert and private key in MyProxy. User access to MyProxy mediated by Shibboleth authentication. Put MyProxy on separate server.

PGP / THAWTE SIGNING PARTY

Mike Helm notarized the following people for Thawte and PGP key signing/upload: {alan.sill@ttu.edu, gaines@fnal.gov, marg@tacc.utexas.edu, vinod@ic.uff.br, vanessa@ula.ve }He will add {Milan Sova, Jens Jensen and David Groep} to the TAGPMA keyring soon.

Bob Cowles and Scott Rea also notarized people.

TACAR PROCESS

TACAR constituency is national research (e.g. TERENA) non-profit, academic.
David Groep described process in detail. (See slides.) Process and paperwork allow orderly handover of a CDROM containing Root Certificate; CP/CPS docs in pdf format; TACAR Registration Letter and copy of Accreditation Letter.

Relying parties can benefit from using TACAR repository. In addition, organisations that do not meet the PMA standards, but wish to be deployed in TACAR may fit into the TACAR community (typically NRENs, or national CAs, or at least non-profit academic). Certificates are listed on the same basis along with the rest of the IGTF CAs - this is selected by the clicking procedure. Should be possible to put the selection into the URL, so users automatically get the right ones. Compare this to the browser's root store where CAs somehow have got themselves into the root store (although there is some review somewhere, unlike TACAR which is 'just' a trusted repository, nothing more). Needs an IGTF accredited symbol - or maybe different symbols for Classic, MICS, SLCS. Mike has the icon.

The minutes must include indication of who is the trusted introducer for each organization (TAGPMA, APgridPMA, EUgridPMA).

ACTION: TAGPMA must pick a trusted introducer.
RECOMMENDATION: Ask TACAR to put an "IGTF" logo next to accredited CAs.
ACTION: Perform PGP cross-signing to allow electronic communication of information.

IGTF CA REPOSITORY AND DISTRIBUTION PROCESS

Historically provided by EUGridPMA folks and then mirrored twice/day to the APGridPMA.org mirror. Also redistributed to VDT. https://dist.eugridpma.info provides http/https/rsync from anywhere. This apache server serves static content only – no other services.

Core facility consists of 3 systems, 7 people and various glue software.

Organized according to {Accredited, experimental, worthless}. There is no superset of 'all CAs' so that Relying Parties(RPs) must decide which CAs to install. If a CA becomes "obsolete" it will be automatically removed for the RPs. Expired CAs will not propagate. CRL URLs created automatically from .info files. CA can also generate "EACL file" in preparation for Operational Review.

Signing policies can be difficult to write. Error messages don't propagate well nor are they well-documented. The only documentation about signing policies is the C source in the globus code tree. Std globus parsing only reads first 1024 chars. Most of the Java middleware only parses the string and doesn't check the signing policy. There is an outstanding bug – globus java part has a potential fix… but not C globus. RPM is the only output format that can capture a hierarchical requirements (as needed by DOEGrids and TACC CAs). CRL hits can be high. Wiki/tutorial information is needed. Can we get stuff into XML for automating the signing policy test? David O'Callaghan had built a prototype automated validation system [with a schema-like syntax] - Jens will check status with David.

Five people can put in the core pieces of info (see later) into CVS repository. These trusted committers can change any info. EUGridPMA process for getting into CVS requires supplying info specified at: https://www.eugridpma.org/review/registration. CVS-committer re-checks the information (mini-opreview). See: https://www.eugridpma.org/review/using-cvs

RECOMMENDATION: One repository for all PMAs and multiple mirrors. A TAGPMA mirror site would be useful.

ROBOT CERTIFICATES:

Robot defined as a long-lived **user** certificate whose private key is "unprotected" once activated. (MUST be protected with a passphrase.) Robots authenticate themselves to a third-party. E.g., certificatie signing done by CA.

Robots are different from a service cert in that it is not tied to a network identity. Robots are tied to a specific user but they are used for automated tasks. fRobots MUST have a 1

SCP OID (This doesn't exist. Needs to be defined.) AND must have OID of their CP/CPS. MUST NOT have server extensions. Robots shouldn't be stronger than your personal user cert. Proxies are more limited than user certs.

Discussion: What do Relying Parties want? Could we come up with a common set of robot names? Could a service certificate accomplish the same thing? Could a proxy certificate or an extension of MyProxy work? Use of a hardware token for initial authentication may serve to differentiate robot certificates from other options. How do you distinguish simple from complex robots?

ACTION: Jens. Define use cases. Propose set of names.

Wednesday 18Jul07	
Local Participants	***Remote Participants***
Bob Cowles, OSG, SLAC, US	Israel Becerril, UNAM, MX
Irwin Gaines, FNAL, US	Sandra Jaque, REUNA, CL
David Groep, NIKHEF, NL	Lia Molinari, UNLP, AR
Vanessa Hamar, ULAGrid, VE	
Mike Helm, DOEGrid, ESnet, US	
Jens Jensen, Rutherford Lab, UK	
Darcy Quesnel, CANARIE, CA	
Vinod Rebello, UFF, BR	
Scott Rea, Dartmouth, HEBCA, US	
Alan Sill, TTU, HEPnet, US	
Milan Sova, CESnet, CZ	

VOTING

1) Whether or not create a position to be Trusted Introducer for TACAR. Does this need to be approved by the whole body or can an appointment simply be made by the Chair?

Discussion in the room centered around the topic of whether a vote is required. The consensus is that the Chair can make such appointments or call for votes at his option, and in this case Vinod expressed his desire to have Mike continue the activities he has started and serve as Trusted Introducer for TACAR. Vinod invited comments on this appointment and proposed that if no substantive negative comments are received by the next video/phone meeting, this should take effect.

Venezuela:
Vanessa has agreed to make changes to the CP/CPS based on comments received yesterday. We hope this will be ready within the next one or two video/phone meetings for an accreditation vote. She will simultaneously work on operational issues in preparation for that phase of work.

ACTION: Alan will send out his keyring, which includes most of group.

ACTION: David Groep and Mike Helm with discuss ideas for handling TAGPMA keyring and will bring a proposal back to the group.

PLANNING NEXT F2F MEETINGS

SUGGESTION for Winter 07 F2F date: 06-09 November, where the 6th is an "Open Day" to allow interaction with local researchers.

ACTION: Vinod will consult with Sandra Jaque about hosting this meeting in Chile. If they can't host, he will negotiate with AR or VE. Need to decide during the coming week. Vinod will be on holiday during August.

Feb. 27 - 29 in the SF Bay Area was discussed as the candidate for the meeting after next. Another idea is to have an all-IGTF meeting.

OGSA/AUTHN

OGSA WG (Alan) shutting down AUTHZ, looking at AUTHN via "express authentication profile" interoperability documents. Based on quick and effective rather than the best thing. Beyond X.509, e.g., using username and password, but no evidence of Shibboleth engagement. Language to express policies, e.g. "I require X.509", or "I understand Kerberos". Do they know about Web 2.0 identities, Higgins, OpenID? These are also constructing policy languages.

See theoretical "Express Profile" work at: https://forge.gridforum.org/sf/docman/do/listDocuments/projects.ogsa-wg/docman.root.working_drafts.security_profiles_use_case. This work is being done under the leadership of Andrew Grimshaw. In order to proceed, the group needs 1) a volunteer for co-chair and 2) more work on an identified short set of deliverables. Alan has been monitoring and contributing to the OGSA-WG "express profile" activities. He described the frequency, timing and coordinates of these meetings and the current output of that group, and invited others in TAGPMA and the IGTF to participate.

PROPOSED PAO PROFILE

Bill on PAO profile: accommodate operating CAs which do not fit into any current profile. Nevertheless, they all require some additional modifications to improve their security to match the profile – FNAL might qualify immediately, although is aiming for the SLCS. Lower assurance. What about reuse of identifiers? Profile seems to be required by the CAs, rather than by the RPs. Very few TeraGrid users actually use non-accredited CAs. Some CAs are non-functional – their certificates cannot be loaded into VOMS. Lower assurance may not be worth the PMA's time?

SUGGESTION: Require a request from at least 2 Relying Parties for a new Authentication Profile. Do they currently accept this CA? Will they accept this CA in the future?

SUGGESTION: Follow TACAR model: Register unaccredited CAs rather than accrediting them. Leave it up to Relying Parties whether they accept an unaccredited CA. Work on better specification for LoA of unaccredited CAs.

SQUID PROXY ISSUE

For the next production OSG release, every worker node will need up-to-date copies of CRLs. They intend to accomplish this without killing the CA servers by implementing squid caches on every compute element.

Unfortunately, the following URLs return code 302 indicating that the link is temporary.

The issue: the HTTP standard declares that the 302 page is cachable only if it has an Expires: or Cache-Control: field. If the redirects are supposed to be permanent, it should return a 301 and the crl_url files should be updated (by the CA, I assume). Otherwise, I'd request that they add the Expires: field so that we can cache the redirection page.

ACTION Anybody who has done web caching or who is willing to try web caching: Please post tips and guidelines to the list.