

TAGPMA F2F Meeting at PSC

30 April 2009

Welcome from D. Moses (PSC)

Presentation by Cheryl Begandy from PSC EOT

Updates from EUGridPMA, APGridPMA, CAOPS and OGF25

STATUS ROUNDTABLE:

- Jim Marsteller: Working on a SAMP project for TeraGrid to pass attributes for users through Science Gateways to resource providers. CMU is looking at joining InCommon. NCSA is the TG Service Provider accepting InCommon identity. JimB: The GridShib CA is totally separate from the SAML project.
- Alan Sill: Pursuing SURAGrid bridged CA. Hoping to move to OpenCA.
- Irwin Gaines: FNAL SLCS CA still in operational review. Working with JimB to make final changes.
- Scott Sakai: Brought SDSC's TAGPMA Membership letter. He has cleaned up the SDSC CA CNs. Not quite ready to present a CP/CPS. Still looking around for an HSM. Darren Bennett: Here to get some face time – SDSC plans to be more active with TAGPMA.
- Roger Impey: This is his first F2F meeting.
- Doug Olson: Currently doing CA contingency planning: what if there was an earthquake in Berkeley.
- David Kelsey: Consulted with LCG about names and name persistence. They want in-person vetting and status quo. Also interested in disaster planning. Is there something that IGTF as a body can do? Guidelines? Best practices? Consider the fire at the location of the APGrid CA – they were only down for 48 hrs. ScottR: We need to discuss CRL generation if a CA goes down. MikeH: DOEGrids makes the NextUpdate = 30days. Scott: Relying Parties can continue to work. MikeH: OR: have an OCSP provider. Another idea: Fix openssl to allow an alternate CRL issuer. Milan notes that if the CA is down, the code never looks through the list of CRL distribution points.
- Javier Diaz: Working mostly with Europe on HEP projects. Just starting a grid in the country – not clear yet how this will develop.
- Mike Helm: Would like to talk about DNSSEC. He expects this to be very disruptive to CA operation – not sure if this will be good or bad... 1.5 months ago they moved their CRL publishing point. OSG audit motivated them to look at their logfiles. 75% of the CRL downloaders had moved in 1 month. 25% have not yet moved. Have asked the IGTF RAT to think about it.
- Richard Miguel: Ready for 1st review of CP/CPS. Using Spanish CA SW.
- Ruben Aquino: Runs UNAM Grid CA. Mostly used by biologists and economists. Will finish the TACAR registration. He is also concerned with continuity of ops. So far, 50-60 certs issued.

- ScottR: Earlier this week, he launched 4BF “4 Bridges Forum” that deals mostly with US federal space to enable cross-certification. Right now, HEBCA is supported by Dartmouth instead of EDUCAUSE. He is in the process of moving HEBCA to a commercial vendor (by the end of 2009) and is also focusing on NIST 800-63 Lvl 1 & 2. He heard KenK comment “SAML will be the LoA ‘currency’”. But he believes that trading assertions across federations will require some kind of underlying PKI.
- Herve Guy: Here to formalize the transition of management of the Grid Canada CA.
- Jens Jensen: UK federations are sending mixed messages about signing SAML assertions and related metadata. There are anti-PKI sentiments in the UK as well. ScottR: Australians are more pro-PKI but there, the same organization runs both Shib and PKI. Most large-scale orgs employ both PKI and attributes. We have tools to leverage attribute-based federations. In the US, Higher Ed for most IdPs are at the lower end of the NIST LoA scale, so Shib is easier to do. Even Dartmouth is interested in Shib because it’s “easier to do” than PKI. DaveK: Australia is putting up a SLCS CA based on SAML.
- Vinod Rebello: Plans to completely overhaul the Brazilian Classic CA. BrGrid will now be a production service under the national PKI infrastructure. (They will submit a Root CA to TACAR for accreditation.) He also intends to bring up a SLCS Federated CA (for a new educational org with no previous PKI). Started looking at self-audit. Audited LA catch-all. Found an external reviewer, but needs to tell him what to do. Has a Portuguese doc of best practices/template – wants to work with Jens on the IGTF template. ScottR: we have a PhD student at Dartmouth working on RFC3647 bits. Vinod: CA staff need to understand the CP/CPS. It would be nice to speed up the accreditation process. Jens]: we also find that writing the CP/CPS is a very time consuming part of the accreditation process.

ABOUT SELECTING THE TAGPMA LOGO:

- Vinod: TAGPMA logo as on T-shirt (with fatter letters). T-shirt key with thicker letters accepted with rest of T-shirt logo. Accepted. Done. No more votes on this ;)
- ACTION[JimM]: Put logo in various sizes on the website where members can get it.

TAGPMA OFFICER ELECTIONS:

- Term of office ends in July 2009. Elections will be held sometime between May and June. Existing officers will not be running again.

WEB SITES AND MAILING LISTS:

- IGTF Website <http://www.igtf.net>
- <http://www.tagpma.org>: Hosts static, public info
- tagpma-general mailing list subscription seems to be working now.

- PSC manages the closed tagpma-private list: JimM asks if we can allow postings from other IGTF members. Use it only for sensitive things. Leave the review as open and transparent as possible. The final review goes to the public list. Intermediate reviews can go to the private list.
- SLCS version 'c' is missing from the website. Add profile discussion to MICS profile discussion.
- Classic Profile is in 6 months (from 20Apr09) period where existing CAs need to conform to this profile!

UPDATE FROM EUGRIDPMA (VINOD FOR DAVID G.):

- Proposed TERENA SLCS CA and TERENA MICS CA: Federated CAs in EU SWITCH May 2007, TERENA May 2009? CESNET May 2009?
- AlanS: Was the SLCS LoA intended to be different from MICS LoA? SLCS is not for throw-away certs. But it expires in a week so has limited liability. SLCS was created for Kerberos. Milan: there are different reqs on the IdP and the CAs. SLCS are **easier** to implement. Many folks think that MICS is too hard. JimB: the phrase face-to-face does not appear in the SLCS profile. Group: Yes they are different. We need to discuss LoA.
- Audits are going on. 3-5 presentations at each EUGridPMA meeting. Self-audits are typically quite thorough and critical. Peer-reviews are going slowly.
- Robots: we have an OID but no profile. Looking towards UK e-science to move this project along. Existing robots need to be able to comply. EUGridPMA has already implemented robots in 3 CAs (run by Jens and David Groep and Milan). MikeH: US is balking because of use of HW tokens. Which PMA should be responsible for the profile? Probably EUGridPMA. Who is author? Jens is happy to accept. Who is editor? There are plenty of volunteers from TAGPMA (Jens, Alan, Doug, Marg). ACTION[Jens]: Define a draft profile.
- Credential Repositories: 'virtual smart card' concept is back. Andy Anushevsky gave a talk years ago: private key is only held in a repository. MyProxy is an implementation of this. MikeH: EnTrust CA includes something like this. Commercial repositories deliver the private key to your desktop. On agenda for EUGridPMA meeting in Zurich.
- Reference: Jim Basney, William Yurcik, Rafael Bonilla, and Adam Slagell, "The Credential Wallet: A Classification of Credential Repositories Highlighting MyProxy," 31st Research Conference on Communication, Information and Internet Policy (TPRC 2003), Arlington, Virginia, September 19-21, 2003.
- <http://www.ncsa.uiuc.edu/~jbasney/credentialwalletTPRC.doc>
- <http://www.ncsa.uiuc.edu/~jbasney/credentialwalletTPRC.pdf>
- That paper references: R. Sandhu, M. Ballere and R. Ganesan, "Password-Enabled PKI: Virtual Smartcards versus Virtual Soft Tokens", Proceedings of

the 1st Annual PKI Research Workshop, 2002.

<http://www.cs.dartmouth.edu/~pki02/>

- November version of MyProxy can limit the lifetime of the private key in the MyProxy repository. MikeH knows of a community that would be interested in this (who previously left IGTF table) and will contact them. ScottR: Dartmouth is playing with Aladdin's software SmartCards. You put the tokens wherever. MikeH: once this is allowed, then there is no CA control. JimB: Folks have been using MyProxy since 2001. There needs to be a best practices guidelines to help folks implement this correctly.
- IGTF Release – new mirror
- <https://dist.eugridpma.info/distribution>
- <https://www.apgridpma.org/distribution>
- Mike and Vinod offered to also put up mirrors.
- Jan Jona Javorsek (jan.javorsek@ijs.si) is working on the nagios monitoring

APGRIDPMA SUMMARY (VINOD FOR YOSHIO)

(SLIDES ON APGRIDPMA WEB SITE):

- Approved new Classic AP version 4.2
- New chair: Eric Yen from Academia Sinica as of 1Jun09.
- 13 accredited CAs, 1 under review
- ASGC had a fire in Taipei in Feb 2009. 25Feb: email broadcast notification of downtime. Later that day they were able to get access to their machines and move them. There was smoke damage and much manual labor required.
Lessons learned:
 - Have a notification plan.
 - Check CA functions regularly.
 - Backup regularly and archive at the safe place.
 - Document, document!
- Australian Access Federation is both PKI/SLCS with Shibboleth: Only one of the two online CAs will be IGTF accredited.

TAGPMA CHARTER UPDATE (ALAN SILL):

- Now V2.6, pdf copy with full changes posted on agenda
- Added Caribbean region
- Member cp/cps repository – agreed that we should have a link to the cp/cps
- Membership Definitions:
 - Inactive – we hadn't heard from a member. Transitioning back to Active only requires action but not a vote. Irwin: Inactive state moves members into a non-voting role so that officers can check with them prior to voting them into a suspended state. Then, at least they don't count against quorum.

- Suspended: TAGPMA votes after 6 months of Inactive state. If the member has not taken active steps, that member loses their membership and any accredited CAs lose their accreditation. Restoration to Active status from Suspended status has the same requirements that are incumbent on a new member.
- Alan will post the new version. Folks can look at it and a vote will happen.
- ACTION[Marg]: Add a link to all TAGPMA accredited CP/CPS documents to the website

SCOTT REA: BRIDGE WG STATUS UPDATE:

It all started @ F2F6 in November 2007:

- Policy mapping between Basic and old Classic AP “failed” – lots of nos; some exceeds
- Policy mapping between C4 and old Classic AP (both directions) worked better – but still some nos
- Lost all mapping docs at Banff due to hard drive failure.
- ACTION[Vinod]: Generate an RFC3647 CP/CPS doc that is consistent with our Classic AP; Get agreement among all 3 PMAs (because there is variation in Section 8)
- Audit is the one glaring item to solve in order to achieve relevance with other federations
- If Bridging is in place; how to build and validate certificate paths?
- JimB: the issue with SHA-2 support is not with Globus but rather with openssl
- AlanS: Don’t assume that Globus won’t make changes we need.
- Need to discuss different LoAs
- Need a more efficient way to distribute Trust Anchors
- ACTION: We need revive a mailing list. Tagpma-bridge@tagpma.org ???
- Former E-Auth initiative is defunct. Replace with NIST 800-63. Peter Alterman is leading the NIST LoA activities
- FPKI High; Medium/HW and Medium/HW-cbp; FPKI Medium & Medium-cbp; FPKI Basic; FPKI Rudimentary; C4. Peter Alterman runs it. HEBCA and FPKI use the same LoAs. Expect that myproxy with SAML will allow access to level 3.
- 4BF: uber-federation is HEBCA, FNCA, CertiPath, SAFE
- Jim Jokl wants to cross-certify UVA CA
- IDTrust: InCommon wants to engage us, but they want to control the agenda. Shibboleth/SAML2. JimB: If Shib could provide a non web-browser interface, then we can engage with them. Grids do things a bit differently.
- AlanS: SURA: most resource providers are 2-tiered AuthN infrastructure. There are problems with bridge SW & tools.
- ScottR: Federations are a hot topic. InCommon is focused on assertion-based technology. HEBCA can’t go production until they can establish separation of

roles – this is part of the process of getting a commercial CA bus to run it. But there are a lot of issues with sharing metadata. InCommon wasn't interested. USHER/HEBCA should run in the same infrastructure (but I2 took USHER away when they brought it into their InCommon infrastructure.) USHER is truly a Lvl 1, so not appropriate for grids. But they have policies for higher Lvl. Have tried to sell to Internet2 about issues with metadata distributions that PKI could help.

- AlanS: What HEBCA CAs are equiv or stronger than IGTF? ScottR: it's not simple to answer. Dartmouth has 2 policies; 1 is low assurance & 1 was higher. AlanS: We can go up easier than we can go down because our trust mechanisms are CA based. ScottR: We need to find a way to support this. Jens: there is a namespace issue but we can work with it.
- MikeH: At RSA last week, Dan Kaminsky advocated DNSSEC. (basically a trusted key system for DNS zones). Kaminsky considers PKI to be a failed technology. DNSSEC could be another bridging mechanism to help find trust anchors. ESnet will sign its zones, but it is not clear whether this approach will propagate. .gov is in the process of being signed. .com may be signed within 2 years. Analogy: DNS is a house with no locks. DNSSEC is a brand new house with good locks and doesn't know about anything else. ScottR: IETF DNSSEC folks have engaged with Max Pala.
- ScottR: Issues are that base tools don't do hierarchical PKIs or cross-bridging. PRQP and TAMP can overcome some of these issues. There is interest in these tools from edu, gov and commercial sectors.
- ACTION[Marg]: give ScottR admin access to the tagpma.org website – to create a section on tools and protocols.
- AlanS: Valerio wants to circulate a VOMS attribute certificate format. Is essentially the AuthN included within the X.509 wrapper. Addresses extended attributes. DaveK: It's been around for a long time, but hasn't been published.
- DougO: What's the value of bridging to the grid community? ScottR: Many federations use PKI but you will never get them under the same administration. Policy mapping is the advantage to understand how to interoperate without dealing with seeking multiple individual accreditations. AlanS: People want a scalable trust infrastructure. Prediction: APs for bridges and we operate with the bridge. DougO: My concern is that the host & service authorities that have no monetary value. When the trust anchors DO start showing up in web browsers – we become a target. ScottR: I agree but this is an advantage for bridging – it doesn't have to be a 2-way certification.

A PUBLIC HEALTH MESSAGE:

Anita Barkin, Director CMU Student Health Services CMU, stopped in re swine flu vigilance:

They are trying to reach folks who have traveled where there was a case, and how they need to communicate with us. Sudden onset of fever accompanied by body

aches; can include nausea, vomit, diarrhea. Contagious 1 day before symptoms and 7 days after. You may not have a healthcare provider in Pittsburgh. CMU wants to be aware of anybody who might become ill. Can direct folks to medical support. Get Tamiflu or Relenza. Social distancing is considered 6 ft. We're in close proximity. 72hrs is the incubation period. If you don't feel well, take your temp. Fever > 100 degrees + other symptoms. She will leave business cards. JimM and Ray Scott. If somebody becomes ill in this mtg, do we offer Tamiflu or Relenza as a prophylactic? No cases in Allegheny County. 2 folks who traveled back from MX thought they were exposed. USA 1% mortality. MX 5-6% mortality. Virus stays live on in-animate.

JIM BASNEY: MAPPING BETWEEN IGTF SLCS AP AND INCOMMON'S BRONZE/SILVER IAP

- David Wasley was waiting for confirmation from ScottR.
- Currently there are no InCommon providers who meet either Bronze or Silver profile – mostly due to lack of audit.
- Initial ID validation in person followed by validation. Bronze has NO ID proofing. Don't get hung up on this – I don't think anybody will certify at Bronze. They will do Silver instead. Silver is very closely in line with the Classic CA profile.
- Technical environment
- InCommon: 7 years and 3 months – comes from audit world? (???)
- InCommon: 72 hrs (because of weekend) SLCS: 24 hrs. (???)
- For Silver, we don't have to ask for audit info, because they have to do it every 24 months. Or they get dropped. So CA should check meta-data to see whether that org has been dropped. CA needs an error page: There's a problem at your home inst. Call your helpdesk, not us. Common InCommon practice is to update the meta-data daily.
- ScottR: 4BF is publishing an audit standard that will not be WebTrust. JimB: This will probably be the University's internal audit staff. There is nothing in Silver that enables peer audit. ScottR: In Fed space, PMA investigates the report and asks questions. Irwin: term 'professional auditor' not highly held.
- Marg: Most Univ auditors don't deal with IT, but rather finances. JimB will look up the specifics. Irwin: CA can't be audited down to the penny, so you end up with checklists. ScottR: With WebTrust, that's also what you get. 4BF: at least one auditor who is trained in IdM practices. ScottR: many of today's metadata DNs do not resolve; many certs have expired?
- Assertions of name uniqueness in IdP – tough to do. InCommon may not provide identity but rather things like "isStudent" i.e., attributes that don't require persistence and MAY provide uniqueness. UK Fed does not guarantee uniqueness.
- For Silver - IdP shall assign a unique identifier, this identifier "may" be included in the identity assertions that require a specific identifier for this Subject. This identifier must be unique among all such identifiers previously issued by the IdP operator and never be reassigned to a different person.

- So have unique identifies but need InCommon policy to release them.
- NCSA is sending email to 80 IdP asking for targetedID, eduPersonPrincipalName
- MikeH: SWITCH didn't go through the Silver reqs. The German CA had a problem with naming.
- Irwin: No blank check. No automatic accreditation. We have the right to reject ID vetting that we don't agree with. ScottR/JimB: Identity vetting practices are not audited for Bronze. AlanS: You must have enough info to traceback to the individual.
- MikeH: It's also a fundamental flaw not to support "directed IDs". We have an opportunity to interoperate with InCommon better than with OpenID.
- DaveK: In Europe Public phone directory is considered private data. IdPs must follow stringent privacy laws.
- Public directories may no longer exist for students? Per JimB. FERPA.
- AlanS: this goes back to LoA – there are cases where we don't need to know the PII. DaveK: You control what they do, not who they are. AlanS: If Silver does everything – then why do you need a CA? JimB: the assertions are short-term and not compatible with non-browser technologies (like Globus).
- JimB: VOMS AuthZ attrib structure – (DaveK: EGEE has no plan to just use attributes to bind to an identity.) Jens: a Portal front-end converts SAML assertions to a cert to run jobs.
- Vinod: what is the next step: DaveK: Somebody proposes putting up a SLCS CA with InCommon behind it. Marg: What about UCGrid in UCLA?
- JimB: The Fed gov wants Silver, not Bronze. ScottR: Several US agencies want Gold (VA, HHS (other than NIH), EPA). NIH wants Silver.

WHITE PAPER BRAINSTORM

- Federations are becoming popular. Can we leverage off of this? What do we need for federated Identity to be acceptable to grids?
- JimB and ScottR: IdP "mapping to profile" process
- Need a document to arrange how to enter into a relationship with the IdPs you choose to federate with.
- Irwin: the world changes when you allow IdPs to federate with each other. It's slicing it a different way. There is a scaling issue: difference between 20 CAs in a hemisphere vs. 2000+ Universities. DougO: TAGPMA and EUGridPMA and APGridPMA are already a federation. As a Relying Party – this leads to gaining some trust.
- ScottR: Maybe we want to change our process? In TAGPMA – what do we have to do to let people trust us.
- AlanS: Any ID federation must have a set of common policies to create a starting point. We might in the future just accept the assertions. A CA must be a point of contact (and CRLs are needed that aren't in InCommon).
- Marg: What is the risk if things scale up?

- Irwin: The gov puts restrictions on me about who has access to the lab.
- DougO: Can InCommon scale up? They will have the problems first – we need to watch.
- Shib is about access to libraries. Silver is about scientist access to resources. LBL will use the UTrust Federation to manage some parts of personnel information. UT-System uses Shib for benefits info - Dartmouth regards anything benefits as very PII.
- DaveK: What is scope of white paper? Just InCommon?
- Marg: but we also talked about technologies and uses of certs.
- As an organization of CAs – the new big issues – are shaping up as...
- MikeH: How to handle directed identity opaqueness. Name representation requirements. DaveK: Feds in EU ARE willing to release the real names. Do higher ed people have the same concept? How can we normalize the path to avoid asking all the IdPs for permission?
- DaveK: SLCS seems to say “Will you release this Display Name to us?” Milan: Fed defines which attributes any member must support (but not necessarily release). If you want the service the user must agree to release the PII. A federation can’t forc and IdP to do anything. If I’m a UK user I have no say about how to release attribs to SAs. Milan: This is a service and these are the rules.
- Irwin: Federated ID changes the paradigm a bit. Federating CAs establishing trust. Now we are breaking out the Identity providers. LoA tokens, mapping.

Friday 1May09 TAGPMA F2F Notes

Members: MikeH; JimBasney; Vinod; Ruben; Richard Miguel; Javier Diaz; Dave Kelsey; Doug Olson; Herve Guy/Roger Impey; Scott Sakai; Irwin Gaines; Alan Sill; Marg Murray; Jim Marsteller; Scott Rea

15 members => quorum is present

Non-members: Jens Jensen, Milan Sova, Michal Prochazka, Darren from SDSC, Dhiva

DAVE KELSEY AUTHZ WG UPDATE

- Our mandate and aims: prepare recommendations on policy and global trust issues related to grid AuthZ
- Min reqs and best practice for operating Grid AuthZ attrib authority
- 2Dec08 mtg at NIKHEF: V Ciaschini, D Groep, O Koeroo, M Helm, Reimer, S Timm, J Wolfrat, D Kelsey
- Access to EUGridPMA wiki requires request to D. Groep or David O'Callaghan – this is an obstacle. Needs to be open instead. But open w/o organization doesn't work.
- Cleaned up AA Profile – need to get to a better draft and assign title and OID.

- Recognize 2 architectures (currently): 1) VOMS push and 2) OSG GUMS pull
- Attrib Authority Service Priority AASP – accredit the AASP, not each VO
- What signing key should be used?
 - Agree not to use host certs (current practice)
 - VOMS developer will allow use of separate key
 - How to prove accreditation?
 - AASP encouraged to consider an HSM
 - How to establish trustworthy VOMS server?
 - Another policy doc – how VOs must operate
 - AlanS strongly wants a key per VO. Then the VO is responsible. DougO: being responsible is not the same as owning the key.
 - FNAL runs a VOMS server that supports multiple VOs.
 - Accreditation scaling & VOMS servers “I run all my VOs the same.”
 - MikeH: this may allow us to extend key lifetimes
- Revocation Issues
 - There is no case for revoking Attrib Certs. (AC) as these are short-lived
 - RP must revoke the entire cert chain
 - March Zurich (OSG/EGEE) mtg: VOMS developer planning a CRL for ACs
- Attribute Practice Statement (APS), should have an OID.
- Experienced VOMS operators: Steve Traylen/CERN Steve Timm FNAL
- Irwin: AA must run securely, but I’m not convinced that putting things in a piece of HW will help this.
- AlanS: Be careful when starting with VOMS paradigm. Policy needs to be technology independent
- Next steps – move forward to first draft, and put it on publically viewable wiki. Welcome additional people to contribute.
- Discussion about need for HSM

VINOD REBELLO (TAGPMA CHAIR): CHANGES TO THE IGTF CHARTER.

Issue: An accredited CA wanted to run a SLCS and MICS. Name uniqueness throughout the IGTF “allocated to each CA”. Would it be nice for an organization to issue multiple certificates in the same namespace?

- Is this good or bad? Both.
- Currently a rollover is like this. An almost expired CA runs at the same time as a new CA.
- German CA wants to issue all sorts of certs in the same namespace.
- Proposal: JimB: replace namespace separation rule to “for PMA member” instead of “for PMA authority”
 - You couldn’t tell from DN which CA issued the cert
 - Considered a win for VOMS

- Should we be handling LoA through the namespace? No. But OID software doesn't work? Except Milan has SW.
- Dartmouth has apps that use OIDs.
- Marg: but Globus middleware only checks DN and expiration
- MikeH: it's easy to issue different kinds. The only way to disallow any kind of cert is to remove the issuer. What about an institution where multiple CAs are folding all types of certs into the same namespace?
- There are OIDs for CP/CPS and AP
- If a Relying Party accepts all APs, then this isn't an issue. DaveK: But this is either/or.
- Motivation: convenience to the user.
- Irwin: Somebody could setup a namespace that forces all IGTF CAs to shut off.
- ScottR: This name space must not overlap with any existing name space
- Motion to approve amendment to IGTF Federation Charter 1.1 (IGTF-Federation-20051005-1.1doc dated 25 June 2008 that is already approved by the EUGridPMA and the APGridPMA
 - 12 in favor
 - 3 against
 - 1 abstain
 - Results: Quorum is present and the motion passes.
- Scott has zero worries about intent – just with wording.
- Timeline: proposed and accepted by EUGridPMA Jan09; Approved at APGridPMA Apr09 Approved at TAGPMA May09. Something will likely happen at Chapel Hill OGF meeting.

JIM BASNEY – IGTF RISK ASSESSMENT TEAM UPDATE

<http://tagpma.es.net/wiki/bin/view/IGTF-RAT>

- Cable Severed in Mediterranean. Affected CRL retrieval
- MD5 hash collisions possible. Should not use MD5
- Globus migrating away from MD5
http://bugzilla.globus.org/globus/show_bug.cgi?6613, proxies will use the same hash algorithm as exits in the parent EE certificate.
- Roger Impey can fix Grid Canada CA when machine moves.
- (EC)DSA EE Key vulnerability in OpenSSL client. RAT requested CAs to audit. 2 CAs found them. 4 certs in total. 2 valid until Aug. Fix is to upgrade openssl client. Nobody should be using DSA, but CSRs may be getting signed without checking the algorithm.
- Sanity Checking Requests:
 - RSA Exponent < 65537
 - Who maintains known-weak keys: blacklist pkg distributed by Debian
 - Dhiva Question 1: What if link is a cluster?

- Dhiva Questions 2: we need bad keys of different sizes to do regression tests to make sure bad keys continue to fail.
- ACTION[Marg] send some bad keys to MikeH and Dhiva.
- Marg: Questions RSA exponent requirement: How can a hardware token have an exponent < 65537 and still get FIPS accreditation unless this was ok? Issue may really be a software config issue rather than a hw token issue.
- Three European CAs still haven't responded.
- TAGPMA has conducted the following audit of known vulnerabilities, and (after our TAGPMA house in order) we request that you request a response from all member CAs and note:
 - Response times: quick/slow/never
 - Hash algorithm: good SHA-1 / still using MD5
 - Issue: Is there a reputation impact / job risk?
 - Issue: Public vs private. TAGPMA has a private mailing list, but there is no private list for EUGridPMA
 - EUGridPMA may want to consider new mechanism of SUSPENDED
 - SHA-1 -> SHA-2
 - NIST advises to replace SHA-1 by 2010
 - SHA-1 Collision search
<http://www.iaik.tugraz.at/content/research/krypto/sha1/>
 - SHA-2 support added in OpenSSL 0.9.8
 - Marg: TeraGrid stack based on OpenSSL 0.9.7 – so globus utilities failed with SHA-2 as a side-effect.
 - JimB surveyed SHA-2 support in OSG/EGEE
 - TAGPMA should construct a request for people to change to SHA-2

JENS JENSEN: CP/CPS TEMPLATE UPDATE

Progress: RFC3647 is currently translated into DocBook, but this isn't very useful.

Jens stepped back to figure out what we need and has a skeleton outline

He wants access to history of what happened with each CA. We need CVS or subversion.

- Discussion:
 - Edit the template to create a derived document.
 - Be able to lock titles and certain text/framework.
 - Doc Structure – maintain RFC3647 format and numbering
 - Sections need popup help description
 - Discussion – many reqs may be met via web docs
 - Must be able to replace canonical text with supplied text
 - Point out to user what is required.
 - Annotations/comments/responses

- Attributions
- What do you do when the framework changes from underneath you?
- Javier: Why didn't you use OpenDocument. It supports internationalization.
- Jens looked at Text-encoding initiative – a framework for annotating text. Jan Javoscek knows about TEI.
- Jens current implementation is in DocBook – it's becoming quite an obstacle.
- AlanS: ICE technology – a set of templates installed into Word or OpenOffice. Backed by a subversion repository. UI can be browser, Word, OpenOffice. Publishes HTML or PDF.
<http://ice.usq.edu.au/introduction/about.htm>
- Milan: Data formats are different from user front-end. UI is paramount. Use a Wiki format
- ACTION: send suggestions to WG (Vinod, Jens) Volunteer CAs will want to re-implement their CAs using this tool.

ROGER IMPEY – GRID CANADA

- History – Formed 8 years ago before EUGridPMA and **Error! Reference source not found.**
- Started at NRC. Moved to CANARIE w Darcy Quesnel in 2004. Now back at NRC.
- NRC is Canadian Federal Lab. \$0.5Billion total. 3500 people, labs in every Canadian province; 18 labs in all.
- Roger works in IMSB – a kind of central IT support
- CA server moved to secure building. Network group running the CA hardware has 5 time zone coverage.
- Roger is Project leader of GridCanada Renewal project
- CP/CPS from Feb 2004
- Perl scripts running Globus version of OpenSSL.
- Back end machines are off-line
- Moving to web interface with backend DB
- HEP community in Canada is small and they know each other. Both NRC and WebGrid keep documents.
- Grid Canada Plan: Moving accreditation to TAGPMA from EUGridPMA. Perform audit within 6 months.
- Formal transfer occurred between Herve Guy and Roger Impey.

MARG MURRAY (TACC): MICS PROFILE UPDATE

- Bring the general language of the profile in line with other profiles
- Change RFC3280 to RFC5280????

- Incl OID for MICS profile into EE certs
- Traceability and revocation
 - mixing eligibility with revocation of existing certs
- change CRL “if you issue” to “MICS must issue CRL”
- remove 1 M sec
- [Action: Marg] generate new MICS profile draft without the traceability paragraph and we can vote on that

JIM BASNEY (NCSA): NCSA GRIDSHIB CA

NCSA GridShib CA supports federated authentication with InCommon institutions of TeraGrid PIs.

- There are now a set of OIDs: available optionally from the EUGridPMA David Groep has talked about this. Recent recommendation. Trusted Third Party (TTP ID Vetting)
- GridShib CA namespace is a NCSA CA.
- IdM is Teragrid allocations process, PI gets allocation and then asserts IDs for grad students
- All TeraGrid users from all TG sites are NCSA users.
- Same DNs as NCSA MyProxy SLCS CA, uses same IdM backend
- Users go to web server, authenticate with their InCommon credential, and authenticate with the NCSA Kerberos credential, which binds the InCommon ID to Kerb ID.
- Binds federated id (eduPersonPrincipalName, eduPersonTargetedId) to NCSA.Teragriud Kerberos principal
- Uses a sequential integer starting from 2 to distinguish name collisions.
- Accounting group creates a Kerberos principal
- Added web server to existing MyProxy – must bind federated identity with CA. Authentication is the binding
- AlanS: PI sends user off a new user to get a portal account. User gets a free TACC portal account. Access in 1 hr. happens. Concern about TG vs TIGRE vs ???
- Irwin: Users can bind their Kerberos principal to one function. One authentication occurs. Subsequent authentication is all Shib authentication.
- GridShib CA adds a level of indirection.
- Not just any Shibboleth dance, just the InCommon Shibboleth dance.
- Uses Kerb authN as an initial registration. Inspired by the Liberty Alliance ?links?
- Federated ID reqs. NCSA asks IDPs how they handle their eduPersonPrincipalnames. ScottR: this is missing from the CP/CPS.
- InCommon Silver doesn't really address name uniqueness
- JimB: we're doing due diligence. But I'm not losing sleep about this. Marg: HR & Shib people worry about this.
- ScottR: you can check whether the Kerb pass is wrong – check once/yr.
- If this isn't more convenient than logging in with Kerb every day.

- <https://go.teragrid.org>
- JimB used Keychain access. Manage associations; creation day; last access; can delete the binding.
- Downloads cred to desktop
- SCOTT REVIEWS: a few things missing from the CP/CPS were in presentation. Concern about how close the backups are being stored. Arrangement with PSC to backup the Kerberos domain. We're swapping our Kerberos principal for an InCommon AuthN. What are limits on mgmt passwords? The InCommon member must have the same or better limits.
- ALAN REVIEWS: This is a full IGTF credential. Is there a dependency on InCommon Silver? I think it does because a user can use their TG credential in a variety of ways. but we need to trust all InCommon operators to provide sufficient evidence that we can trust them. No InCommon members are ready to certify to Bronze.
- MikeH: concern about disaster recovery plan missing. NCSA CAs don't have this?
- JimB: We are working on putting up another myproxy CA at PSC that could serve teragrid users if ncsa is destroyed.
- AlanS: Suggest that GridShib CA operate as an experimental CA and look at accumulated experience over 6 months.
- DougO: we're tainting the process. We're not accrediting InCommon.
- Vinod: What is the state of the CP/CPS? ScottR thinks the talk is within the AP. JimB yesterday said he needs Silver to rely on identity vetting. This CA does NOT rely on the IdM for identity vetting. MikeH: This is linking and this just a convenience. Irwin: anytime somebody gives away a Kerb cred will be recorded. DaveK: so we are issuing X.509 certs based on Shib creds.
- MikeH: thinks it should be accredited.
- Summary: One round of reviews has occurred. JimB responded to MikeH already; just got Scott's review 2 hrs ago.
- JimB will report on how the TAGPMA process works. He got his last review today. Vinod is waiting for the the reviewers to approve the document. Scott is ready to vote after some changes. AlanS raised concerns about a relying on an unvalidated IdP that we know needs to be at Silver before we can have the assurance that we need. A relatively small group of TG users would be affected by using an experimental status. Irwin: experimental is a red herring. This is just two different ways to get the same cert. Let's get away from the experimental format.
- Need to establish a trust relationship with IdP. DaveK: What is different about SWITCH vs. this? Why was I happy with SWITCH?
- What if JimB has a list of InCommon IdPs who I trust, and JimB is the responsible party. Is "members of InCommon in good standing" sufficient?
- 1: gain op experience that we know we haven't opened ourselves up to a risk
2: InCommon gets to Silver. JimB
- AlanS: If you, JimB trust each InCommon IdP – then that would be sufficient. You have a process. (JimB: It's a shame that we're talking about this only today.)

- Consensus seems to be that with addition of CA managers vetting of IdPs that accreditation would be OK.
- Irwin: Avoid fly-by-night U and the U has TeraGrid members. You are checking – add the text.
- Vinod: The CP/CPS needs to be revised. If done by tomorrow – then we can vote

RICHARD MIGUEL – SENAMHI CP/CPS FOR PERU

- Vinod and Javier are the reviewers.
- Using pkIRIS-0.9.55d
 - Easy to install; Spanish SW
 - Used by REUNA
- Richard is checking in with mentor Sandra Jaque about operational practices
- JAVIER REVIEW: Some minor changes in CP/CPS (cert attributes; overall in good shape) Javier received a new version today.
- VINOD REVIEW: good example of somebody who got thrown into PKI and a template would have been good. Some sections are missing requirements.
- CP should reference RFC5280
- Summary: Need one more review.

MARG MURRAY (TACC): TACC MICS CA REVIEW

Jens is ok with CA operation. Made several CP/CPS suggestions that Marg already implemented. Milan didn't have time to review the CP/CPS and won't have time for more than 2 weeks.

Action[Marg]Send fixed CP/CPS to Shreyas and call him next week to see if he can review the TACC MICS CA CP/CPS.

= = = Miscellaneous Notes:

<https://www.eugridpma.org/members/display>

ACTION[Marg]: Ask David Groep for his script that generates ?.info files?

IRWIN GAINES (FNAL): FNAL UPDATE

Irwin: Hopefully will be done within days (or hours) with operational review to make reviewers happy. Maybe an update tomorrow?

Saturday Notes 2May09

Members: MikeH; JimBasney; Vinod; Ruben; Richard Miguel;Javier Diaz; Dave Kelsey; Doug Olson; Roger Impey; Scott Sakai; Irwin Gaines; Alan Sill; Marg Murray; Jim Marsteller

14 members => quorum is present

Non-members: Jens Jensen, Milan Sova, Michal Prochazka, Darren Bennett from SDSC, Dhiva

MIKE HELM – STATUS OF DOEGRIDS AUDIT

- DOEGrids has a PMA
- Alan S. – any efficiencies to be obtained or desired w.r.t. DOEGrids PMA and TAGPMA?
- Marg – perhaps with audit there should be a transfer of accreditation from EUGridPMA to TAGPMA
- reformatted former CP/CPS to RFC3647
- Audit Report Exec Summary
- “Findings” of defects followed by MikeH addition of responses.
 - Consider MICS-type CA
 - Revamp DOEGrids PMA
- Marg: the NIST 800-53 approach (as architected by Dan (drpeterson)) – a web-based tool – is part of what makes this appealing to the audit process. Could this tool be released/shared with the IGTF community?
ACTION[MikeH]
- 2 classes of audit findings:
 - Significant: serious; docs missing; non-conforming
 - Minor deviations: doc errors and omissions
- DOEGrids CPS v3.1 implements DOEGrids Audit
- Marg: pragmatically, it makes sense to give the local org a voice in the process, i.e. a local PMA
- ACTION[Members]: <http://doodle.com/r5cnvskcftf534nz>
- His URLs will be posted to a tagpma mailing list.
- This has turned into a very expensive effort and yet there has been no change to the way in how the DOEGrids CA operated. Significant opportunity cost with limited benefit.
- DOEGrids is constantly challenged about certificates – and does ok.
- The audit does not have its eye on the ball. The cost is extremely high. Watch out.

JENS JENSEN SOAP BOX:

KIHON Part I.A What is an IGTF certificate?

- It’s special: it ties a name to a zero-knowledge secret associated with a LoA.
- Traceability, whatever that means, beyond lifetime of cert by keeping records
- Global name uniqueness
- Timeliness – at issuance and for revocation

- Assertion of eligibility (authZ) – requires judgement
- *Is there a need for a grievance procedure?*
- DougO: You really want accountability in the process.

KIHON Part I.B What certificate purposes are allowed?

- ...as stated in the policy or policy OIDs
- Certificates needing to revoke or rekey themselves
- There's a difference between supported purposes and permitted purposes
- Corollary I: A private key may only be used by the EE and the subscriber
- Corollary II: The SUBJECT names the EE, not the Subscriber. There are cases where the EE and the Subscriber may not be the same. The SUBJECT names the EE, not the Subscriber unless the EE == Subscriber. SO: Be clear that we follow GFD125 before RFC3647 where it says "Subscriber – A subject of a certificate who is issued a certificate."
- Subscriber interacts with CA; EE uses certs for permitted purposes; EE is named in cert.
- Jens advocates for naming EEs correctly. If it's a robot, says so.
- Are service certs still needed? What things don't work without this service?

KIHON Part I.C

- What is an IGTF CA?
 - Is it the trust anchor (a cert)?
 - Is it a cert and a sub-namespace?
 - Is it an issuer DN and a namespace?
 - Is it a collection of certs (rollover) and namespace?
 - Or a collection of issuer DNs
 - Is it a namespace (Relying Party Defined Namespace Constraint (RPDNC))?
 - Is it the issuing authority?
 - Is it the institution (IDP operator) running the issuing authority?
 - Is it a person (le roi, c'est moi)
- How similar are AAs and CAs?

KIHON Part II – Policy – see his talk in Zurich

KIHON Part III – Software – see his talk in Zurich

KIHON Part IV – Scenarios

- What if SHA1 is broken?
- What if RSA is broken? All private keys become suspect.

- RAs are still OK
- Proofs of identity are still OK
- What if your building burns down?
- What if the hash is broken so an attacker can change the cert serial number?
Then CRL checking won't work and verification will pass for a bad cert!
 - Scenario 1 – SHA1 broken
 - Can we still issue certs – using SHA256?
 - Need to rekey CAs as well but can operate both while changing SHA1àSHA2
 - CA rollover – few days, new EE certs – spread over some time
 - Scenario II – hierarchy, certs dodgy, private keys OK
 - Create new CA hierarchy
 - Resign existing CSRs
 - Users download and install new certs
- What if RSA breaks? Life as we know it ends.
- Survival:
 - Separate security question
 - OpenCA PIN
 - Also helps prevent DN reuse
 - RA infrastructure:
 - DB with traceability info
 - Photo ids held offline
 - Must re-vet LRAs
 - Users re-request certs maybe using old CSRs, but re-key
 - Or users re-request but need RA approval
 - Or users just get new certs as normal
- How do you know what a cert did after it was compromised?
 - How do you notify relying parties? LRAs? Subscribers?

VOTE:

TAGPMA Charter

Motion to accept v2.6 as the current version:

Vote: unanimous acceptance:

ACTION[Marg]: post on website

ACTION[JimM]: will take on editor role.

MICS AUTHENTICATION PROFILE 1.1:

Question by Vinod: Should the cert include the AP OID with version or just the base? Discussed at Portugal and Cyprus EUGridPMA meetings where the consensus was to include only the base, but to require compliance within 6 months.

The controversial addition to Section 3.3 has been postponed for additional discussion and revision. Irwin suggests broadening the scope of the traceability issue as it affects all the APs. Don't fix it only for MICS. ACTION[Vinod]: get this on the OGF agenda for Chapel Hill meeting.

VOTE:

Motion to accept the current MICS AP 1.1?

14 AYE: the motion is passed.

ACTION[TAGPMA officers]: We note that the UVA member has been inactive. Vinod will contact Jim Jokl and UVA will be taken out of quorum.

ACTION: Send a note to Greg Barnes + boss and ask for clarification –

JIMB: GRIDSHIB CA UPDATE:

- AlanS: Jim's revisions were responsive to my comments.
- Waiting for ScottR review. Alan notes some changes requested by ScottR that were not yet made.
- After two reviewers are happy and spreadsheets have been posted to tagpma-private, then there can be an accreditation vote.

MARGM: TACC MICS CA UPDATE:

- ACTION[Marg]: Milan and JimBasney found spreadsheets.
- Marg will contact Shreyas to see if he can do the 2nd review promptly.
- After two reviewers are happy and spreadsheets have been posted to tagpma-private, then there can be an accreditation vote.

FNAL CA UPDATE:

- IrwinG: operational review (seems to be OK now)
- Irwin will provide material for IGTF and TACAR electronically now that he has exchanged PGP keys with Mike H.

DOEGRIDS CA UPDATE:

MikeH: wants to transfer his IdP accreditation from EUGridPMA to TAGPMA. Vinod, as a courtesy, will consult with EUGridPMA (David Groep).

== =

AlanS: asked about LogoType RFC

= = =

PLANNING FOR NEXT F2F MEETINGS:

- Joint meeting with APGridPMA
 - Co-locate with OGF in Banf 12Oct09 all week
 - MikeH: would it be useful to setup a Google calendar to keep track of all the IGTF meetings?
 - Alan/Roger: try Canada but in Vancouver. Roger would be happy to host if he can get somebody local to help – maybe at Simon Frazier? If folks are going to Banff – we could have a meeting in Calgary. Notes that the OGF meeting is at Canadian Thanksgiving. **Can we have TAGPMA in Calgary the week before? Say 8-10th October. Thurs-Sat**
- Lima, Peru: 18-20 March 2010. (RSA:1-5Mar2010 IETF21-26Mar2010)
- Hawaii – maybe an all-IGTF meeting? East-West Center???
- San Diego, CA?
- Berkeley, CA?
- DougO: Taipei, adjacent to ISGC conference in April. APGridPMA has meeting there.
- Jens: IGTF is part of OGF – should co-schedule around that.

MIKEH: CA CLONING:

- DOEGrids to be cloned to some other ESnet location
- 5 Essentials
 - Replication and Geographic dispersion of key mgmt
 - Replication and Geographic dispersion of CA interface application (signing initiator, UI, DB)
 - Replication
- CRL publishing: Going to use anycast to provide best-effort services; or Amazon Cloudfront
- Dhiva: we need to solve the problem of keeping the internal LDAP db in sync. Maybe we can keep the 2nd instance off-line as long as the LDAP data is consistent. But maybe we can get to the state where we can keep both on-line transparently.
- Can't need too many HSMs – but HSM DB; LDAP DB; CA interface modules ???
- Linux High Availability: linuxHA <http://www.linuxha.net>
- Mike H. – we would like a technical committee to provide advise and input
- Steve TIMM FNAL Dan Yokum FNAL are knowledgeable about linuxHA.

JENS JENSEN: ROOT CA REVIEW TEMPLATES.

- List of elements / dependenciesS8 Online Server DB
- Showed TACC-ROOT-review spreadsheet.

APPLICATION FOR MAKING A TAGPMA MEMBERSHIP MAP:

<http://backspace.com/mapapp/configure.html>