14th EU Grid PMA meeting - 6-8 October 2008 - Lisbon, Portugal

Minutes by David O'Callaghan david.ocallaghan@cs.tcd.ie

Many speakers have attached presentation materials to the agenda for the meeting. For this reason, these minutes do not contain summaries of material presented.

Attendees are indicated by their initials after their first mention.

APGridPMA Updates – Jinny Chien

JC presented updates from the APGridPMA and the IGTF meeting in Singapore (see agenda).

The Netrust CA was having problems with heavy CRL traffic so the CRL has been mirrored to AIST.

Jens Jensen commented that two accreditations by APGridPMA have raised questions so it may be necessary to review the accreditation process. David Groep suggested that automated tests before accreditation may help.

TAGPMA Updates – Jim Basney

JB presented updates from the TAGPMA (see agenda).

JJ commented that some TAGPMA CAs awaiting accreditation haven't been heard from for a while.

IGTF Risk Assessment Team – Jim Basney

JB discussed the http://tagpma.es.net/wiki/bin/view/IGTF-RAT.

There was discussion of the RAT communications test. It was decided to perform such tests twice a year and without advance warning. There was discussion of how to make the test messages appear less like spam.

JB asked for suggestions of what else the RAT should do. Christos Kanellopoulos said that it should "assess risks". Dave Kelsey and others said that in effect it is an incident response team.

DG raised the issue of improving reliability of contact information for CAs. He proposed that each CA should provide an escalation process including contact information to be used if there is no response from the primary contact point.

JB will establish a PGP-secured email list service for the RAT members.

Latvian CA Update

JJ stated that he had received an update to the Latvian CA's CP/CPS within the last month that was lacking some required changes. Another version has been sent that is yet to be reviewed. JJ has done an operational review and the state is not too bad. The accreditation process will be completed by email.

RENAM Update

CK reported that the RENAM web page is not available. The CP/CPS document is fine but it is necessary to check that everything is as described.

African CAs

South Africa and Senegal are planning to establish CAs.

INFN CA Internal Audit – Roberto Cecchini

RC presented an internal audit of the INFN CA using the proposed Audit Guidelines (see agenda).

INFN CA will develop a disaster recovery plan based on NIST 800-53.

RA auditing is a key issue. RC noted that it would be very difficult to audit all 103 RAs (with more than 200 staff).

Other issues relate to authentication of requests for host certificates. The meaning of a "single network entity" in relation to sharing of certificates between hosts is unclear.

QuoVadis CA for Switch – Alessandro Usai

AU presented the planned QuoVadis Grid CA commissioned by Switch (see agenda).

AU stated that the security procedures of the CA are very good and any problems are likely to be in relation to grid compatibility.

DG asked how easy it would be to add certificate profiles. Kaspar Brand said that the CA is running Unicert which supports policies and currently these are updated every few days so the only question is how many they want to have.

Reimer Karlsen-Masur asked if the Data Encipherment Key Usage flag will be set for compatibility. Milan Sova said he does not do this and DG agreed that it is not necessary (it only affects message-level security with XML signatures in particular software).

CRL issuance for SLCS CAs

Discussion of lifetime of CRLs issued by SLCS CAs. JB and others have a requirement for one-business-day response to revocation requests.

It was suggested that CRL issuance should be bound to the lifetime of certificates issued: if the lifetime of the cert is short then the revocation process may not need to be started before the cert has expired.

CRL nextUpdate

The Classic AP required CAs to issue a CRL 7 days before reaching the nextUpdate date of the previous CRL. There was a proposal to relax this requirement and reduce the interval to 3 days before reaching the nextUpdate date.

JB brought up the OSG requirement to have a CRL with several days “validity” so that network problems, etc. can be dealt with before the CRL “expires” (i.e. reaches the nextUpdate date).

It was agreed to require online CAs to issue certificates 3 days before nextUpdate while off-line CAs must still issue certificates 7 days before nextUpdate.

The Classic AP was modified to include these changes.

Classic AP Changes

DG presented some uncontroversial changes to the Classic AP and the document was modified live.

An issue was raised in relation to Section 3.1: should the RA document how identity of end-entities is maintained? JJ stated that RAs may validate the identity differently and it may not be done in an auditable way.

JJ pointed out that FQDN ownership for host certificates may be checked using records internal to an organization so additional records are not kept. An RA should document the validation of external DNS names.

RC initially objected to the requirement in section 4.3 that all certificates must comply with the Grid Certificate Profile as defined by the OGF document GFD.125. CK explained that GFD.125 is “frozen” and will not be changed. If requirements change we can override the Grid Cert. Profile in the AP or by drafting a new OGF document.

DK suggested some changes in order to better accommodate robot certificates.

GÉANT3 PKI & PMA – Milan Sova

MS presented the GÉANT3 tasks related to PKI and establishment of a PMA (see agenda). MS will be the leader of the GÉANT3 task SA3/T1.

CA managers from NRENs will participate in a PMA and DFN will run a catch-all CA for NRENs without a CA. The PKI will provide host certificates and will not be visible to users but rather be used between services, in a similar fashion to Edugain.

DG noted that an objective of the proposal is “increasing use of PKI by end users” and expressed concern. MS answered that it is not a requirement for any deliverables.

DG was also concerned about having two similar bodies (EUGridPMA and the GÉANT3 PMA) making representations to eIRG. MS said that it may be possible to make some arrangement where the set of CAs overlap, but there may be political problems.

RKM and CK noted that this PKI will be distinct from the grid PKI. However, since the profile differences will be minor, it might be possible to define a new profile for GÉANT3 within EUGridPMA. DG suggested that EUGridPMA could act as a repository for such profiles. RKM noted that this is a planned extension to TACAR, but MS said that it is not defined in the task.

MS said that NRENs may be asked to run a new PKI for GÉANT3. JJ commented that JANET is responsible for the SCS in UK. DG noted that proliferation may cause problems if it filters up to eIRG.

DG reiterated that he would like to remove the objective of exposing end users to PKI as it contradicts the federated approach. MS noted that there are no use cases for end users. DG noted that if end users do need to access PKI they could do so under one of the existing EUGridPMA profiles.

SLCS CA for Northern Europe – David Groep

DG presented plans for a SLCS CA for Northern Europe covering the Netherlands, Norway, Denmark and possibly Sweden and Finland. The plan is to have the CA in the Netherlands and the SP in Norway.

Currently the federated identity system in the Netherlands covers universities but not all the smaller research organizations where the grid users are. It is not possible to give a time-frame for the SLCS CA to be in place.

MS asked how robot certificates could be provided if SLCS CA is used for users and SCS for servers. DG replied that a classic CA may be needed, or it might be possible to use SLCS in some way.

AU noted that users may need to import SLCS certs into a browser to contact VOMS and other web-based services. DG said that the CA may be MICS style (issuing ˜1 year certs) but noted that the current federation policies are not strong enough to support SLCS or MICS. MS commented that every federation will need additional policies and gave the example of the CESNET SLCS SP which will require another contract with the Czech IdPs.

RKM asked if the SLCS will have an SP in a joint federation or if there will be an SP for each federation. DG replied that it will be a single CA dealing directly with the federations rather than through Edugain.

DK asked if the Distinguished Names of certificates will be persistent. DG replied that the CA will need a persistent unique identifier. RKM suggested that IdPs could be contracted to provide the Principal Name and MS similarly suggested to require a non-reusable targeted ID.

AU asked if a commercial CA had been considered for this service. DG commented that commercial CAs tend to provide a signing interface but not a way of interacting with the federation.

Belarusian Grid CA – Yury Ziamtsou

YZ presented the Belarusian Grid CA for accreditation (see agenda).

There was discussion of certificate serial numbers. KB had previously noted that the CA certificate should not have 0 as its serial number. MS noted that some software has problems writing writing large serial numbers to syslog.

It was noted that O rather than OU should be used in certificate subject distinguished names to identify the Organization. There had been a problem with RDN ordering due to EJBCA configuration but the latest version is correct.

MS asked if the CRL Distribution Point URL pointed directly to EJBCA as this might cause performance problems. YZ replied that it does not as the CA is off-line.

DG asked how visitors to Belarus can be handled as the CP/CPS required a Belarusian passport. YZ agreed to accept other passports for non-Belarusian residents.

YZ requested a quick accreditation and DG agreed that the PMA could complete the accreditation by email within two weeks.

2048 bit key length

MS said that US Government requirements for key length require that more than 1024 bits be used after 2010. This would require certificates issued in 2009 to comply. As we are at the end of 2008 we need to prepare.

MS asked if the PMA and the other PMAs agree. The proposal was to require every CA to stop issuing certificates for 1024 bit keys before the end of 2009.

DG noted that in the Class AP there is an explicit minimum of 1024 bits and mention of allowing 1024 bit keys on tokens. JJ noted that some hardware tokens can only support 1024 bit keys. Furthermore, he noted that such an increase will add processing load to software.

JB stated that some experiments he had carried out showed that RSA signing with 2048 bit keys takes 5 times as long as with 1024 bit keys. Verification takes 4 times as long.

Special Certificates – Jens Jensen on the Soapbox

JJ raised the issue of certificates whose continued validity requires special attention of the CA. For example, grid certs are in use on hosts used for time-dependent analysis of medical scans. If a certificate were to expire it could possibly put lives at risk and the user or organization might blame the CA.

JJ proposed that enhanced mechanisms are need for notifying subscribers of some expiry for some certificates. Another example is VOMS server certificates whose expiry would cause widespread authorization failure. The key point is that “some certs are not equal”.

MS asked how a CA can know what the cert will be used for. DK said that subscribers might know. AU noted that with commercial CAs importance is attached to the lifetime of a certificate and CAs could consider issuing longer lifetime certs for such cases.

JB commented that IGTF currently does not consider quality of service of CAs, except response time for revocation requests. JJ suggested an escalation procedure for upcoming renewals and CK suggested that CAs could offer a service to give extra notification of expiry if requested.

Authorization Working Group – David Kelsey

DK presented the draft document from the Authorization Working Group (see agenda).

DK noted that JSPG is developing a related but distinct document describing requirements for VO membership management and that the document under discussion is currently focussed on VOMS as it is currently deployed rather than on Attribute Authorities in general.

There was discussion of the title of the document, whether it should mention VOMS and whether it is an "Authorization Profile" or an "Authorization Operations Profile".

The document uses the term "PMA" to loosely mean the body that accredits an attribute authority service operator. It was agreed that EUGridPMA cannot accredit these directly and suggested that a national body could do it.

CK suggested that the document should be about how to manage the infrastructure, not the attributes. It was suggested that the document should specifically mention VOMS groups, roles, etc.

There was some discussion of attribute lifetime, which is seen to depend on the attribute. However it was mentioned that a maximum lifetime would be useful as there is no revocation mechanism.

Operational Requirements

It was agreed to increase the minimum key length for the signing key to 2048 bits.

There followed a discussion about using a specific certificate for signing attributes rather than the current practice of using the host certificate.

DG noted that it is currently possible for the VOMS software to use a different cert for the web interface and signing, but this key is also used for the SSL VOMS service itself.

DK raised the possibility of using an uncertified or self-certified key for signing but acknowledged that it would make validation difficult.

DK said he could see the advantage of having a different cert that indicated that it had passed accreditation. It was mentioned that the certified name should be the name of the VO.

CK liked having different key pairs for different VOs. This would require VOMS to support individual signing keys per VO. MS suggested having multiple certificates, one per VO, but with the same key, or a single cert that covers multiple VOs. However, AU and DG pointed out that adding a new VO would affect existing VOs.

DK raised the issue of a VO-specific cert allowing a private key to be shared on replicated VOMS servers. JB indicated that private keys should be isolated between VOs to allow functionality to be split and DG said it would allow migration of a VO from one service to another. CK noted that since all VOMS instances run as root there is no difference in having multiple key pairs in case of a compromise, however he suggested that a future version of VOMS could support services running as distinct non-privileged users.

AU raised the issue of how accreditation would be conveyed to the CA. A CA must do a strict check that a subscriber is responsible for a VO.

JJ commented that the assumption that each VO has a cert doesn't apply to dynamic VOs but DK noted that the intention was to make it clear which VOs are accredited.

There was further discussion on whether the VO or the service operator should be accredited and what should be indicated in a signing key-pair certificate.

JJ noted that we might want to have a different certificate profile for signing key certificates, for example, removing the SSL Host flag. MS said that such certs are like robot certs. CK suggested including a policy OID for the AA profile.

DK asked if accreditation should be tied to a server but MS indicated that this would involve, for example, hardware checks. Instead we want to give a person an accreditation to run a VOMS server with a unique name, but that it would be difficult for a CA to do this.

David O'Callaghan suggested that the operator should be accredited, the accreditation should be brought to the CA in some form and the operator would then be able to request and have signed a signing certificate. DOC and AU noted that we should allow less secure VOMS services to exist alongside accredited services. JJ suggested that there are different levels of VO such as site VO, national VO, international VO; the latter might be required to use HSMs and have PIs send a signed document to the CA.

DK suggested trying to develop the guidelines document and do an accreditation by the next meeting in January. CK volunteered to have his VOMS service accredited. DK noted that the VOMS certificate profile could be developed separately and that VOMS developers should be engaged.

There was some discussion of the name-space of VOMS service certificates. MS suggested that any IGTF robot name would be suitable and it would be up to the VO to decide to use a particular service operator. There could be a specific 1SCP for VOMS services. DK said that there needs to be a mechanism to tie a certificate to an accreditation and JJ said the CA could do it so as not to require RAs to change procedures.

RKM suggested that the PMA could maintain a list of accredited cert DNs and possibly store this in the form of Shibboleth metadata

DK noted that VOMS software would need to be changed to use a second key-pair and to support OID checking. This would also apply to RP software.

IGTF CP/CPS Template Working Party – Jens Jensen

JJ presented work in the CP/CPS template system and displayed some of the DocBook XML (see agenda).

MS and JJ noted that DocBook to WordML conversion is unreliable.

The processing scripts will be written to notice where a modification has been made to the standard text and will bring this to the special attention of reviewers.

JJ plans to get volunteers to write “clean room” text for the template and then review this. It was suggested that copyright could be assigned to OGF.

OGF CAOPS Working Group

Authentication Service Profile – Christos Kanellopoulos

CK presented the Authentication Service Profile, intended as a meta-profile for future Authentication Profiles like the current Classic, SLCS and MICS profiles.

DG suggested that it could be expanded to cover “trust” profiles in general. DK noted that document refers to “identity” but CK argued that this does not only imply authentication. This led to discussion of how identity is managed in a federation such as DFN-AAI. RKM noted that at a general level it is covered in networking contracts between DFN and organizations but extra contracts are needed for IdPs. MS noted that the Czech federation is just an infrastructure and puts only minimal requirements on IdPs (defining semantics and syntax of basic attributes). Each SP must negotiate with IdPs.

RKM commented that if grid middleware were “Shibbolized” we might need a Shib profile. JB suggested an authentication profile for SAML wold be more appropriate. MS noted that requirements would be on IdPs rather than federations as a whole.

CK will develop a new version that makes it clear that it is a template or framework for writing new Authentication Profiles and wait for input from the Authorization Working Group.

Name-space Constraints – David Groep

DG presented relying party defined name-space constraints. JJ and others will provide example use cases and then the document will be sent for its final call.

Audit Guidelines

CK noted that discussion on the qualification of external auditors was intended as a recommendation rather than a requirement.

RC raised some issues resulting from the INFN self audit. RC noted that it is difficult to specify how an RA discovers ownership of a FQDN: it may be an internal procedure. Auditing of RAs is difficult and JJ said RAs may not have an audit trail. CK noted that Yoshio audits random RAs but JJ said that all RAs need to be audited. MS noted that RAs should be aware they might be audited and act accordingly. RC said that the auditing guidelines doesn’t help to perform RA audits.

RC commented that the guidelines do not contain anything more than the authentication profile and said that some guidance is necessary. DG noted that Yoshio had previously promised to provide some information about ratings. CK said the document should be used to ask questions and JJ added that the results could be assessed by the reviewers. CK suggested that the document should be reworded as necessary to avoid leading questions.

Future Meetings

There was some discussion of dates for the Berlin meeting September 2009 and the dates September 14–16 were proposed.

1SCPs and Policy OIDs – Milan Sova

MS demonstrated an OpenSSL command to verify presence of a given policy OID and also a ˜10 line OpenSSL C program that implements basic policy OID checking. MS noted that the current code doesn't support checking for multiple OIDs (e.g. Classic AP with Robot 1SCP) but that it is possible with a little more code.

DG asked if we should insist that Classic AP policy OIDs should appear in certs within 6 months and this was agreed. DG noted that the base OID for the Classic AP should be included to avoid the requirement to include an OID for each version of the AP. JB suggested using an IGTF policy OID as RPs often enable Classic but not SLCS or MICS. DG noted that we don't want to imply equivalence.

DG said that we don't yet have a 1SCP for robots. JJ noted that we may need more than one 1SCP for robots. CK suggested similar 1SCPs for users and hosts.

JJ raised the issued of "non-verified subscriber information" in certs. This could include promises about key protection.

There was some discussion on terminology for a hosts 1SCP: "network service", "networked entity". DK asked if we need another classification for VOMS services, e.g. "entity is an attribute authority".

JJ mentioned the use case of issuing certificates with an additional policy to allow security officers to revoke certs without having all the privileges of an RA or CA operator. DG suggested that it should not be implemented with OIDs because if the role changes then the cert must change.

Ensuring Robot Certificate availability in Europe – David Kelsey

DK presented the request that RPs want robot certificates for monitoring, portals and similar purposes. Currently 4 CAs can or will soon be able to provide robot certs: UK, NL, IT, and CZ (soon).

CK said that the requirement for hardware tokens may be unpopular with users. DK suggested using software tokens as an initial step but DG noted that this might actually reduce security from current practice where user certificates are used in conjunction with MyProxy. This led to discussion of using MyProxy for robot certificates either with the certificate stored directly in MyProxy or with a long-term proxy. DK noted that existing policies cover proxies created by users rather than those stored in a credential store. DG said that the policy for using hardware tokens is trivial; after that a policy can be developed for credential stores.

There was some discussion of the existing Classic AP: private key protection for robot and host certificates was not clearly defined. The profile was modified to clarify.

DK said that user communities should approach their local CAs to request robot certificates. It is not clear if support for robot certs is a “must” or “may” for accreditation of the CA.

User Credential Management – Christos Kanellopoulos

CK presented some issues surrounding the difficulty of use of PKI for end users. He demonstrated a Java applet to perform MyProxy-init from the browser. The applet looks for certificates in browser keystores.

The user can request an account on a grid UI and this will be created as a pool account. The user can log in to the UI using a Java GSI-SSH client directly from the browser.

CK stated that many users are storing long-lived (over 100 day) proxies on MyProxy. JB agreed that there is no control of lifetime of proxies going in to the service.

Revocation of User / Proxy Certificates

There was discussion of revocation following compromise of proxy certificates. MS noted that the policy does not give proxy compromise as a reason for revocation. Similarly creation of a long-lived proxy (say 11 months) is not listed as a reason for revocation.

CK noted that a credential store can be configured not to allow export of long lived proxies but others noted that such a proxy could be created outside of a credential store.

CK proposed four options for dealing with exposed proxy keys. The user’s long term certificate could be revoked; the VOs could ban the user’s certificate/subject; the proxy could be banned; the user could be banned until the proxy expires (if the proxy is long-lived, the user may request revocation).

JJ asked how it is possible to know if a proxy is compromised and said that we need more than the proxy key. Jorge Gomes agreed as any site admin could mail a user’s proxy to a CA. DG noted that of the 40000 lxplus users more than 2000 have proxies in their home directories.

RKM suggested changing the APs to give proxy compromise as a reason for revocation and to make some recommendations to RPs. CK suggested a good step forward would be to create a profile for running MyProxy services. JG noted that the issue is not only with MyProxy as proxies can be created on a

UI. MS pointed out that the check for proxy cert lifetime should be done by the RP when checking the chain.

CK raised the issue of using a HSM in a credential store and MS mentioned that a “real” HSM can store thousands of keys.

DG suggested that credential stores which store the primary key must comply with some credential store guidelines. CK, DOC and RKM will draft a document of guidelines for credential stores and circulate to OSCT and JSPG.

Automated Certificate Checking – David Groep

DG raised the issue of automatic checking of CAs and their certificates for GFD.125 compliance. DG gave a presentation that included many of the features to be checked (see agenda).

DG noted a list of extra suggestions for checks, such as the RSA exponent, successful download of the CRL. MS asked if some of these tests could feed in to Nagios.

CK asked how EE certs could be checked and DG said that CAs should provide sample user and host certs before accreditation.

Members of the PMA have already done some work on such tools: DOC has a system written in Kawa Scheme using BouncyCastle. CK has tools written in Ruby (or was it Groovy?). DG suggested a combination of OpenSSL and Perl would be most portable and there was rough consensus on this. DOC and others will work on this.

JJ noted that some features need to be checked against the CP/CPS and this would require clever tools and a machine-readable CP/CPS. This may be possible in relation to the proposed template CP/CPS. DOC mentioned some other research in this area.

HTTP caching of CRLs

There was a brief discussion of improving cachability of CRLs to avoid excessive loads on the CRL servers. DG sent a recipe for Apache to the EU Grid PMA mailing list.