CA-OPS Collaborative Minutes OGF36

http://bit.ly/OGF36CAOPS

Agenda

- Minutes
- Actions
    - DG will make first pass in migrating Documents CA-OPS Gridforge -> Redmine, importing documents into documents. Does it support versioning? DONE
    - MJ email Andre about Changes to CA-OPS Chairs DONE
    - JJ will send slides and Mike will post them here. ONGOING
- GFD.125 bis
    - We have version 6 which consolidates all comments and track changes
    - Has been through WG last call
    - We will now send to JJ (Area Director) as part of the document process -> public comments P-REC.
- OCSP [MS]
    - Client is ready but not published.
    - Operation Recommendation for OCSP Responder: Profile of OCSP for deployment in IGTF CA services: Document in OGF CA-OPS WG -- P-REC. Editors will be MS and SHOULD also include Scott Rea.
    - Need to think about formalising and requiring Caching service - “guideline on the retrieval and processing of revocation information by relying parties” within the scope of IGTF: EU-GridPMA perhaps.
- Redmine
    - Six wg members now signed up
    - All docs now available via redmine
    - history preserved in RAR files.
- SHA.nn
    - SHA.2 Timeline (see also https://www.eugridpma.org/meetings/2012-09/eugridpma-26-lyon-summary.txt)
        - Jan 1st will be too early for EGI, WLCG, OSG
        - Some SHA2 certs have been issued
        - Rec to not issue SHA2 for general use until 2013/08/01
        - If SHA.1 is broken certificates will be revoked
        - SHA1 EECs should have a valid beyond 2014/09/01
        - CA’s who issue SHA1 certificate which are valid beyond 2014/09/01
    - SHA.256 SHA.512 are the only recommended SHA2 flavours
    - Thou shalt not introduce SHA-3 until after SHA-2
- Private Key Protection
    - Some changes since Ljubljana PMA meeting
    - Revision here: https://grid.ie/eugridpma/wiki/GuidelineOnPrivateKeyProtection2
    - This version is the “refactoring” - follows the lifecycle of the key more.
    -
- LoA
    - see http://kantarainitiative.org/idassurance/
    - Communities now getting re-interested in LoA
    - IGTF have info in many documents
    - NIST has been *de facto* to date but perhaps not suitable

    - Perhaps define IGTF CAs comparable to the above levels
    - LoA Registry IANA
- CA Cert retirement
    - IGTF has changed its policy for withdrawing CA certificates.

IGTF Business:

- Require consensus on document “Private Key Protection” (URL above)
- Jens to present document
- General principles should not use Normative Caps SHOULD, MUST,...
- Clear when applied to user keys and not
- Jim asks: IGTF agreed that CILogon Silver could generate private keys for subscribers. Does this document still allow it?
- Need to explicitly define “Subscriber” or change the value
- Need to do full matrix of all variables for PKP.

Need Glosary
Need to revise the document to have clear consistent terms throughout.

Rewrite to comments above, submit as CA-OPS doc.
IGTF then refer to this to write IGTF policy documents

Alan, David expressed wish to write:

- “Guidance on the operation of keystores” e.g. keystore operator compromised; how to manage access to those keys when data may be locked/encrypted with only these keys for access

AOB

- eugrid pma wiki is going to move [no more edits please]