SEE-GRID CA self Audit

In general

- We do operations well

- Our policy documents need work (mostly to make the text clearer in a few sections)

Brief history

- SEE-GRID CA was first presented and accredited in 2004

- Major update on 2010 to include the EGI catch-all service

Audit results

- Audit guidelines used: GFD.169 April 19, 2010

- In policy:
  - B: 9
  - C: 7
  - D: 0
  - X: 2
- But in practice 8 “B” and 3 “C” are “A” as well as 2 “C” are “B”

"B": 1/9

- Is there a single CA organization per country, large region or international organization? (CA item 2)
  - Stated correctly but only in section 1.3.3 Subscribers instead of 1.3.1 Certification Authorities
  - Practically an A ☺

"B": 2/9

- The CP/CPS documents should be structured as defined in RFC 3647 (CA item 6)
  - It is not stated anywhere
  - Practically an A ☺

"B": 3/9

- The CA computer where the signing of the certificates will take place must be a dedicated machine, running no other services than those needed for the CA signing operations (CA item 7)
  - Needs: rewording
  - Practically an A ☺

"B": 4/9

- The CA system must be located in a secure environment where access is controlled, limited to specific trained personnel (CA item 8)
  - Building number changed
  - Doesn't explicitly mention the CA system
  - Practically an A ☺

"B": 5/9

- Every CA must issue a new CRL immediately after a revocation (CA item 30)
  - Stated only in 4.10.1 Operational Characteristics (not 4.9.9 On-line revocation/status checking availability which is suggested)
  - Practically an A ☺

"B": 6/9

- The repository must be run at least on best-effort basis, with an intended availability of 24x7 (CA item 49)
  - Stated only in 2.4 Access Control for Repositories instead of 2.1 Repositories
  - Practically an A ☺

"B": 7/9

- Accredited CAs must define a privacy and data release policy compliant with the relevant national legislation. The CA is responsible for recording, at the time of validation, sufficient information regarding the subscribers to identify the subscriber. The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that CA (CA item 55)
  - Needs: rewording

"B": 8/9

- An RA must validate the association of the certificate signing request (RA item 5)
  - Needs: rewording
  - Practically an A ☺

"B": 9/9

- The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate. (CA item 8)
  - Needs: rewording
  - Practically an A ☺

"C": 1/7

- Whenever there is a change in the CP/CPS the O.I.D. of the document must change and the major changes must be announced to the responsible PMA and approved before signing any certificates under the new CP/CPS (CA item 4)
  - Partly stated in 1.5
  - Practically an A ☺

"C": 2/7

- The profiles of the CA certificates must comply with the Open Grid Forum GFD.125 (CA item 22)
  - CA's certificate profile is not mentioned in CP/CPS
  - Practically a B 😐, AuthorityKeyIdentifier includes Dirname and serial number

"C": 3/7

- The CRLs must be compliant with RFC5280 (CA item 32)
  - Not mentioned explicitly in the CP/CPS
  - Use of unspecified reason code
  - Practically is a C ☹

"C": 4/7

- No user certificates may be shared (probably keys) (CA item 35)
  - Partly mentioned in 6.1.1 Key Pair Generation
  - Practically, (hopefully) an A ☺

"C": 5/7

- The end-entity certificates must comply with Grid Certificate Profile as defined by the Open Grid Forum GFD.125…. (CA item 38)
  - Neither nsKeytype nor ExtendedKeyUsage is mentioned
  - Practically is a B 😐, nsKeytype is used

"C": 6/7

- Over the entire lifetime of the CA it must not be linked to any other entity. (RA item 6)
  - Needs: rewording
  - Practically is an A ☺

"C": 7/7

- The CA is responsible for maintaining an archive of these records: (all requests and confirmations) in an auditable form. (RA item 10)
  - Not documented
  - Practically is a C ☹, this information is archived to the internal ticketing system.

"X": 1/2

- The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates and signed revocation lists (CA item 16)
  - Not an online CA

"X": 2/2

- For host and service certificate requests, an RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate (RA item 4)
  - Due to the nature of SEE-GRID CA, the procedure to achieve this has been delegated to the RAs

What next?

- A new CP/CPS will be distributed for review
  - Will fix all the fixable issues
  - We are not going to re-issue the CA certificate to fix CA item 22
    - CA expires in 2014

Thank you

- Please stop reading emails and volunteer for the peer audit review ☺
  - We need at least 2 of you