# HellasGrid 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

- HellasGrid CA was first presented and accredited in 2002
- Major update on 2006
- Minor updates until 2010

# Audit results

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

- In policy:
  - B: 10
  - C: 5
  - D: 1
  - X: 2
- But in practice 8 "B" are "A"

# “B”: 1/10

- Is there a single CA organization per country, large region or international organization? (CA item 2)
  - Stated correctly but only in section 1.1 Overview instead of 1.3.1 Certification Authorities
  - Practically an A ☺

# "B": 2/10

- Is the CA system a dedicated system? (CA item 7)
  - Should be written more clearly
  - Practically an A ☺

# "B": 3/10

- Is the CA system located in a secure environment where access is controlled? (CA item 8)
  - The building id has a typo… It should be 22b instead of 22d…
  - Practically an A ☺

# "B": 4/10

- Does the CPS describe the protection of the CA private key? (CA item 13)
  - Yes, but under 6.4.1 Activation data generation and installation (not 6.2.8 Method for activating private key which is suggested)
  - Practically an A ☺

# "B": 5/10

- Is a new CRL issued immediately after a revocation? (CA item 30)
  - Yes, but this is described in 4.10.1 Operational Characteristics (not 4.9.9 On-line revocation/ status checking  availability which is suggested)
  - Practically an A ☺

# "B": 6/10

- Is the protection of private keys described as an end entity obligation? (CA item 37)
  - Yes, but this is described so in sections 4.1.1 Who can submit a certificate application and 6.4.1 Activation data generation and installation (not in 6.2.8 Method of activating private key which is suggested)
  - Practically an A ☺

# "B": 7/10

- How does the CA perform operational audits? (CA item 47)
  - This is described in section 5.3.4 Retraining frequency and requirements (not in 5.4 Audit logging procedures which is suggested)
  - Practically an A ☺

# "B": 8/10

- Is the web repository available 24x7 on a best? (CA item 49)
  - This is stated in section 2.4 Access control on repositories and not in section 2.1 Repositories which is suggested
  - Practically an A ☺

# "B": 9/10

- How are privacy and confidentiality described? (CA item 55)
  - In general well enough but some further development of sections 9.3 Confidentiality of Business Information and 9.4 Privacy of personal information is suggested

# "B": 10/10

- How is the CA or the RA informed of changes? (RA item 8)
  - In general well enough but some further development of sections 4.8 Certificate modification and 4.9 Certificate revocation and suspension could be done

# "C": 1/5

- Does the CP/CPS describe the CP/CPS change procedures, publication and notification policies, and approval procedures? (CA item 4)

  – These are mentioned and described in section 1.5 Policy Administration. It is suggested that the relevant content is moved to section 9.12 Amendments and be further developed.

# "C": 2/5

- Is the CRL compliant with RFC 5280? (CA item 32)

  – Reason Code for all revoked certificates is:

    *Unspecified*.

    - According to RFC 5280: “reason code CRL entry extension SHOULD be absent instead of using the unspecified (0) reasonCode value”

# "C": 3/5

- No user keys may be shared. Is this described as an end-entity obligation? (CA item 35)
  - This is partly discussed in section 6.1.1 Key Pair Generation. It is suggested that the text is refined and moved to section 4.5.1 Subscriber Private Key and Certificate Usage.

# "C": 4/5

- Over the entire lifetime of the CA it must not be linked to any other entity. How does the CA guarantee this requirement? (RA item 6)
  - This is discussed but we suggest making the procedure more clear in section 3.1.5 Uniqueness of names.

# "C": 5/5

- Does the RA maintain the archive of records in auditable form? (RA item 10)
  - This is not made clear in CP/CPS. Re-wording and refinement of the text in section 5.5.1 Types of Records Archived is suggested.

# “D”: 1/1

- The end entity certificated must comply with the Grid Certificate Profile…? (CA item 38)
  - Section 7.1 of CP/CPS should be updated
  - In practice (after inspection):
    - In **subscribers** certificates usage of Non-repudiation should be removed from keyUsage
    - In **host/service** certificates extendedKeyUsage should be included in the extensions.

# "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 online CA

# "X": 2/2

- The RA must record and archive all requests and confirmations. Does the RA record and archive all requests and confirmations? (RA item 9)
  - Aside application data other relevant information is archived via the HellasGrid user portal