Baltic Grid Certification Authority

Self-audit

Hardi Teder
EENet

Overview

- Baltic Grid CA
- Statistics
- Self-audit
  - Minor
  - Medium
  - Major
- Future plans
- Conclusions

Baltic Grid CA

- Baltic Grid CA gives certificates to end entities which are located in Estonia, Latvia or Lithuania and have interest in grid computing.
- Accredited: November 2005
  - replaced Estonian Grid CA (accredited 2004)
- Run by EENet and funded by „Estonian Scientific Computing Infrastructure project“ for now
  - Location: Tartu, Estonia
- Opetated by:
  - Hardi Teder
  - Tõnu Raitviir

Statistics

- 2079 issued certificates
  - 1403 user, 657 host, 19 service
  - 105 revoked
  - 930 LT, 401 LV, 740 EE
- 295 valid
  - 189 user, 104 host, 2 service
  - 6 revoked (during last year)
  - 105 LT, 11 LV, 178 EE
- 18 RAs
  - 9 LT
  - 3 LV
  - 6 EE

Recent changes

- BGCA CP/CPS changes v1.1->v1.2 are available at CA web page
  - Certificate lifetime extended to 395 days instead of 1 year
  - Certificate request must be at least 2048 bits
  - Removed „Knoppix“ from CA requirements (6.5.1)
  - MD5 signatures are not used in certificates
  - CRL version number updated to X.509 v2

Scores

- Based on GFD.169 for the CP/CPS review
  - Classic AP version 4.3
- Scores:
  - A. OK
  - B. Recommendation (minor change) 7
  - C. Recommendation (major change) 2
  - D. Advice (must change) 1
  - X. Could not evaluate (N/A) 1

B. Recommendation (minor change)

- **GDF.169#2** Is there single CA organisation per country?
  - CP/CPS update: move text from 1.3.3 to 1.3.1
- **GDF.169#6** The CP/CPS should be structured as defined in RFC3647
  - CP/CPS is still structured as RFC 2527 defines
- **GDF.169#13** CA certificate password length is not mentioned in CP/CPS
  - CP/CPS update: add to 6.2.7 the “15 character pass phrase” length requirement

B. Recommendation (minor change)

- **GDF.169#20** Lifetime of the CA Certificate must be no longer than 20 years.
  - CP/CPS update: add CA certificate lifetime (10 years)
- **GDF.169#24** CA must react within one working days
  - CP/CPS update: add the “one working day“ requirement
- **GDF.169#38ii** the policyIdentifier must include the OID or authentication profile under which the CA has been accredited
  - Update CP/CPS: Add the PolicyIdentifier
- **GDF.169#43** Every CA must record … login/logout/reboot information
  - CP/CPS update: add the text about „login/logout/reboot“

C. Recommendation (major change)

- **GDF.169#42** Certificates must not be re-keyed for more than 5 years without person verification
  - CP/CPS update: add the „5 years“ requirement
- **GDF.169#47** Every CA must perform operational audits ot the CA/RA stuff at least once per year
  - After the end of BalticGrid project the meetings with RAs are rare
  - The meeting with RAs have to be organized in 2013

D. Advice (must change)

- The pass phrase of the encrypted private key must be kept also on an offline medium, separated from the encrypted private keys and guarded in a safe place where only the authorized personnel of the CA have access.
  - Had everything in one safe accessible only for the Director of EENet
  - Already have a separate safe for CA backups

X. Could not evaluate

- **GDF.169#41** about harware tokens
  - No hardware tokens in use

Future plans

- SHA-2 actions
  - Need to update offline CA OpenSSL version
    - Currently in use: OpenSSL 0.9.7c 30 Sep 2003
    - Need to write new CA's liveCD
  - Update script with signuser-sha2 and signhost-sha2 options
- Add IPv6 support for CA web
  - Done
- EENet joined witn TCS
  - Since September 2012
  - Server and user certificates
  - Federated AAI – TAAT (http://taat.ee)

Conclusions

- CP/CPS needs several updates
- RA archiving and auditing procedures should be updated
- Backups

- Reviewers will get the updated CP/CPS at the end of this week.

Thank you

Q&A

hardi.teder@eenet.ee
http://ca.balticgrid.org