23rd EUGridPMA Meeting

RomanianGRID CA Self-Audit

Marrakesh, Morocco
12-14.09.2011

Cosmin Nistor; Alexandru Bobe
Romanian Space Agency (ROSA)

RomanianGRID CA

- RomanianGRID CA was established and is operated by the Romanian Space Agency (ROSA), a public institution supervised by the National Authority for Scientific Research – Ministry of Education and Research in Romania.
- Purpose: A top level Certification Authority to provide PKI services for the GRID activities of the Research and Academic communities in Romania

RomanianGRID CA

- RomanianGRID CA reached the “Production” status on the 9th of October 2007, when the CA was included in the IGTF Distribution of Authority Root Certificates

- Since January 2008 RomanianGRID CA is listed in TACAR (TERENA Academic CA Repository)

RomanianGRID CA

- **Website / Public Repository:**

  http://www.romaniangrid.ro

- **CP/CPS structure: RFC 3647**

Facts & Figures

Registration Authorities:

- **Nov 2007 – 6**
- **Dec 2008 – 12**
- **Dec 2009 – 12**
- **Dec 2010 – 13**
- **Sept 2011 – 15**

IFIN-HH – Bucuresti
ISS – Bucuresti
UPB – Bucuresti
ICI – Bucuresti
UTC-N – Cluj-Napoca
ROEDUNET-IASI – Iasi
ITIM – Cluj-Napoca
UVT – Timisoara
UB – Bucuresti
UCv – Craiova
CSA-INCAS – Bucuresti
INCDMTM – Bucuresti
SIS – Bucuresti
UMF – Bucuresti
UTCB – Bucuresti

Facts & Figures

Certificates

Root certificate (CA certificate) validity:

Saturday, September 30, 2017 7:56:22 PM GMT+03:00

User / Server valid certificates

77 / 95 (172)

All certificates (2007 – p)

601 total / 172 valid / 47 revoked / 382 expired

Operational Issues

- Technical:
  - CA Root cert caused VOMS authentication problems due to incorrectly used AuthorityKeyIdentifier extension. The CA Root cert was reissued with correct extensions and different serial number.
  - Added clientAuth extension in extendedKeyUsage in server certs

Operational Issues

- Downtime:
  - Internet connection failures. Solved by implementing a BGP connection.
  - Power failures. Too long for the UPS-s to handle. Forced to buy a generator.

Self-Audit

- Document used:

  GFD.169 v1.1 (Oct.28, 2010)

- Overview:
  - 45 As
  - 11 Bs
  - 5 Cs
  - 4 Ds
  - 2 Xs

Self-Audit

- D (must change):
  - (3.1.7-34) *Lifetime of user certificates and host certificates must be no longer than 13 months.*
  - True, but not in CP/CPS. (Section 5.6)

Self-Audit

- D (must change):
  - (3.1.7-35) *No user certificates may be shared.*
  - True, but not in CP/CPS. (Section 4.5.1)

Self-Audit

- D (must change):
  - (3.1.7-38) *The end-entity certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125. In the certificate extensions:*
    - *ii. the policyIdentifier must include the OID or Authentication Profile under which the Certification Authority has been accredited. For Classic AP, OID is 1.2.840.113612.5.2.2.1.*
  - We have to include the OID for Classic AP. (Section 7.1)

Self-Audit

- D (must change):
  - (3.1.7-42) *Certificates must not be renewed or re-keyed consecutively for more than 5 years without a form of auditable identity and eligibility verification, and this procedure must be described in the CP/CPS.*
  - Not in CP/CPS. (Sections 3.3.1, 4.6, 4.7, 5.6)

Self-Audit

- C (major change):
  - TRUE but no evidence in CP/CPS
    - (3.1.1 – 2*) Is there a single CA organisation per country, large region or international organization?*
    - Should be in Section 1.3.1.
    - *(3.1.1 – 4) 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.*
    - Should be in Section 9.12.

Self-Audit

- C (major change):
  - TRUE but no evidence in CP/CPS
    - (3.1.2 – 7) *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.*
    - Should be in Section 6.5.1.
    - *(3.1.2 – 10) The secure environment must be documented and approved by the PMA, and that document or an approved audit thereof must be available to the PMA.*
    - Should be in Section 6.5.1.

Self-Audit

- C (major change):
  - TRUE but no evidence in CP/CPS
    - (3.1.5 – 25) *Subscribers must request revocation of its certificate as soon as possible, but within one working day after detection of he/she lost or compromised the private key pertaining to the certificate or the data in the certificate are no longer valid.*
    - Should be in Section 4.9.1.

Self-Audit

- B (minor change):
  - TRUE but in different section in CP/CPS
    - (3.1.3 – 13) *If the private key of the CA is software-based, it must be protected with a pass phrase of at least 15 elements and it must be known only to designated personnel of the CA.*
    - Located in Section 6.4.1. Should be 6.2.8
    - (3.1.3 – 15) *The pass phrase of the encrypted private key must also be kept on offline media, separated from the encrypted private keys and guarded in a secure location where only the authorized personnel of the CA have access. Alternatively, another documented procedure that is equally secure may be used.*
    - Located in Section 6.4.2. Should be 6.2.4, 6.2.5

Self-Audit

- B (minor change):
  - TRUE but in different section in CP/CPS
    - (3.1.4 – 20*) Lifetime of the CA certificate must be no longer than 20 years.*
    - Located in Section 6.3.2. Should be 5.6
    - (3.1.4 – 21*) Lifetime of the CA certificate must be no less than two times of the maximum life time of an end entity certificate.*
    - Located in Section 6.3.2. Should be 5.6

Self-Audit

- B (minor change):
  - TRUE but in different section in CP/CPS
    - (3.1.6 – 28*) The CRL lifetime must be no more than 30 days.*
    - Located in Section 4.9.7. Should be 4.9.9
    - (3.1.6 – 29*) Every CA must issue a new CRL at least 7 days before the time stated in the nextUpdate field for off-line CAs*
    - Located in Section 4.9.7. Should be 4.9.9

Self-Audit

- B (minor change):
  - TRUE but in different section in CP/CPS
    - (3.1.6 – 30*) Every CA must issue a new CRL immediately after a revocation.*
    - Located in Section 4.9.7. Should be 4.9.9
    - (3.1.7 – 37*) Every CA should make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data. When using software tokens, the private key must be protected with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords. Private keys pertaining to host and service certificate may be stored without a passphrase, but may be adequately protected by system methods.*
    - Located in Section 4.1.1. Should be 6.2.8

Self-Audit

- B (minor change):
  - TRUE but in different section in CP/CPS
    - (3.1.10 – 49) *The repository must be run at least on a best-effort basis, with an intended availability of 24x7.*
    - Located in Section 4.10.2. Should be 2.1

Self-Audit

- B (minor change):
  - TRUE but could be clearer
    - (3.2.1 – 6*) The CA or RA should have documented evidence on retaining the same identity over time. In all cases, the certificate request submitted for certification must be bound to the act of identity vetting.*
    - Located in Section 5.5.1.
    - (3.2.3 – 9) *All communications between the CA and the RA regarding certificate issurance or changes in the status of a certificate must be by secure and auditable methods.*
    - Located in Section 4.1, 4.2.

RomanianGRID CA

Thank you!