44th EUGridPMA Meeting

RomanianGRID CA Self-Audit

Toulouse, France
24-26.09.2018

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 Ministry of Research and Inovation 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:

- **Published on website:**

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

- **Active:**

IFIN-HH – Bucuresti
ISS – Bucuresti
UPB – Bucuresti

ICI – Bucuresti
ROEDUNET-IASI – Iasi
ITIM – Cluj-Napoca

Facts & Figures

Certificates

Root certificate (CA certificate) validity:

Thursday, September 30, 2027 7:56:22 PM GMT+03:00

User / Server valid certificates

41 / 84 (125)

All certificates (2007 – p)

1632 total / 125 valid / 81 revoked / 1426 expired

Changes since 2011 audit

- Subject min Keylength 2048 bits (v 2.0, Feb 2013)
- SHA-256 signing algorithm (Feb 2016)
- Extended CA cert lifetime to 20 years (v 2.1, May 2017)

Self-Audit

- Document used:

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

- Overview:
  - 66 As
  - 4 Bs
  - 0 Cs
  - 0 Ds
  - 12 Xs

Self–Audit

- B (minor change):

- *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. (Ref 3.2.3. - 10)*

- Done in practice – signed emails – not clearly specified in CP/CPS

Self-Audit

- B (minor change):

- *The certificate request submitted for certification* ***must*** *be bound to the act of identity vetting. (Ref 3.2.2. - 7)*

- Done in practice by RAs – not clearly specified in CP/CPS

Self-Audit

- B (minor change):

- *The secure environment **must** be documented and approved by the PMA, and that document or an approved audit thereof **must** be documented and approved by the PMA. (Ref 3.1.2. - 10)*

- Completely offline signing machine in a security certified environment. Not clearly specified in CP/CPS
- Not clear what “Approved by the PMA” means.

Self-Audit

- B (minor change):

- *The records **must** be made available to external auditors in the course of their work as auditor. (Ref 3.1.8. - 44)*

- Not clearly specified in CP/CPS

RomanianGRID CA

Thank you!