TÜBİTAK
ULAKBİM

TR-Grid CA Updates
September 24th, 2024

Feyza Eryol
Chief Researcher

OVERVIEW

- General Information
- Statistics
- Self-Auditing Report
- CA Root Certificate Update

GENERAL INFORMATION

- Accredited in September 2005.
- Single CA in Türkiye for academic field.
- It provides X509 certificates for academic research and educational activities in Türkiye
- Managed by TÜBİTAK ULAKBİM.
- http://www.truba.gov.tr/index.php/en/certification-authority/
- CP/CPS:
  - Follows RFC3647.
  - Current version 2.4 since October 2021.
  - Plan to update CP/CPS to version 2.5 after signing new root certificate or using TCS.

STATISTICS

2021

Certificates	Number	Valid	Expired	Revoked
Users	2547	17	2066	464
Servers	492	26	380	86

2024

Certificates	Number	Valid	Expired	Revoked
Users	2571	7	2096	468
Servers	601	23	429	149

LAST SELF AUDIT RESULTS

- Performed by GFD.169 every year.
- No need to be updated until root certificate changes
- Scores:
- 5 item with score X (N/A) X (N/A)
  - 3.1.2(9) Online CA
  - 3.1.2(10) Secure Environment
  - 3.1.2(16) Online CA
  - 3.1.3(40) Hardware Token
  - 3.1.6(41) Hardware Token

PROBLEMS ABOUT SHA1

- CA certificate will be expired within a 378 day.
- CA certificate key is 2048 bit, but signature algorithm is SHA1
- Services which are running for EGI infrastructure are running on the EL9 or similar.
  - Problems on Tier-2 Centre tests: Suggested mitigation

NEXT STEPS – RENEW CA CERTIFICATE

- Update CA root certificate with SHA2:
  - CA certificate will be expired at October 5th, 2025,
  - 7 personal certificates,
  - 23 service certificates (all ULAKBIM & METU services)
- All EEC is needed to be renewed with new CA certificate to be sure that there is no needed to be manage the SHA-1 root certificate.
- Necessary updates will be applied to CP/CPS as soon as possible.
- There is a need to change the CRL path of the TR-Grid CA:

  from www.grid.org.tr to www.truba.gov.tr
- Submit CP/CPS for approval to PMA members.

NEXT STEPS – BEGIN TO USE TCS

- Join TCS as a new member:
  - Not sure it is possible in a short time.
  - Not know the cost of an EEC. (It is needed to be approved by the management.)
- If TUBITAK ULAKBIM is able to join to TCS:
  - All EEC is needed to be renewed by TCS.
  - Necessary updates will be applied to CP/CPS as soon as possible:

    Is it needed?
- Submit CP/CPS for approval to PMA members.

Thanks, questions and suggestions?

TÜBİTAK
ULAKBİM