



DZ e-Science CA Self audit and update

36th EUGridPMA meeting, IISAS, Bratislava, Slovakia,
18-20 Jan 2016

Hassina Ladour - Aouaouche El-Maouhab

19 Jan 2016



- 1 Overview
- 2 Self-Audit
- 3 Summary



1 Overview

2 Self-Audit

3 Summary



- Is part of the Algerian Research Network ARN services operated by DZ e-Science GRID Team, Networks Division at CERIST.
- Established in 2010 and accredited in 2011.
- Provides X.509 version 3 certificates for scientific community through ARN.
- Single CA in the Algerian Academic and Research field (No subordinate certification authorities).
- CP/CPS structured according to RFC 3647.
- Current CP/CPS version: 1.1
- OID assigned: 1.3.6.1.4.1.24881.1.1.1.1
- <http://ca.grid.arn.dz>
- CA operators: 2
- RA operators: 2



■ Implementation:

- **Offline server: (CA signing)** Redhat Enterprise Linux with OpenCA-offline version 1.1.0.
- **Online virtual Machine: (CA repository)** Redhat Enterprise Linux with OpenCA-online version 1.1.0.



- **Version:** 3 (0x2)
- **Serial Number:** 1 (0x1)
- **Signature Algorithm:** sha1WithRSAEncryption
- **Issuer:** CN=DZ e-Science CA,O=DZ e-Science GRID,DC=ARN,DC=DZ
- **Validity:**
 - **Not Before:** Jun 20 10:42:29 2011 GMT
 - **Not After :** Jun 16 10:42:29 2026 GMT
- **Subject:** CN=DZ e-Science CA,O=DZ e-Science GRID,DC=ARN,DC=DZ



- Issued certificates since 2011: **238**
 - Personal: **148**
 - Service/Server: **90**
- Revoked certificates since 2011: **11**
- In 2015:

Certificates	Valid	Expired	Re- voked
Personal	12	9	1
Server/Service	19	14	1



1 Overview

2 Self-Audit

3 Summary



GFD-I.169

The current Self-audit was done in accordance with the GFD-I.169 document version 1.0

- Audit dates: 3-7 Jan 2016
- Reviewers: CA Operators
- We used the scoring system provided in the document: **A**, **B**, **C**, **D**, **X**



Self-Audit

Pre-Examination



- CP/CPS: Available in repository
- Relevant IGTF Authentication Profile(s): yes
- Manuals for subscribers: Available in repository
- Operational manuals: Available for the CA Operators
- CA Repository: <http://ca.grid.arn.dz>
- CA Certificate: Available in repository
- End entity certificates: Available in repository
- HSM manual: N/A, offline signing machine
- Any other document described as published in the repository in the CP/CPS: N/A
- Any other document available for the auditors: N/A



Self-Audit

Main examination (1)



- CA room for Online CA Server: located in the main DATA Center of Network Division-CERIST. Restricted access with RFID card and key, 24/7 surveillance, fire alarm system.
- CA room for Offline CA signing machine: Located in a Self dedicated room near the CA operator office. Access Restricted only for CA Operator with RFID card and key, 24/7 surveillance, fire alarm system.
- HSM: N/A
- Backup media of the CA private key: yes, on two separated USB and burned in a CD-R and locked separately in dedicated safe boxes on separated rooms.
- Offline media (sealed envelope) which contains a passphrase of the CA private key: Yes, sealed envelope locked in dedicated safe box.



Self-Audit

Main examination (2)



- Media storage of archived logs and other documents and their place: Yes, logs of The OffLine and the Online machines are included in A full Backup of the two machines on a dedicated separated storage
- End entity certificates (if not available for the pre-examination), including issuance activities: yes, in repository
- Logs of the CA/RA servers: Yes, logs of The Offline and the Online machines are included in a full regular Backup of the two machines on a dedicated separated storage
- Logs of the CA repository (e.g. Web server): Yes, on the Online server and included in the regular backups on a dedicated separated storage
- Records of operation of the CA private key (including accesses to the HSM): N/A
- Access log to the CA room: N/A
- Any other documents (e.g. daily report of the CA operators): N/A



Only the scores above A are described next.

Auditing Scoring

- **A**: 57 Good.
- **B**: 9 Recommendation (minor change)
- **C**: 1 Recommendation (major change)
- **D**: 0 Advice (must change)
- **X**: 1 Could not evaluate (N/A)



C score (major change)

3.1.7 (46) Every CA should perform operational audits of the CA/RA staff at least once per year.

- Operational audits are not made every year, partial audits are done . Described in section 8 on CP/CPS.
- Should be also added in section 5.4



B score (minor change)

3.1.4 (18) CA must provide and allow distribution of an X.509 certificate to enable validation of end-entity certificates.

- True, described in section 7.1.1 on CP/CPS.
- Should also mention (X.509 version 3) in section 2.2



B score (minor change)

3.1.4 (19) Lifetime of the CA certificate must be no longer than 20 years.

- True, described in section 6.3.2 on CP/CPS.
- Should be also added in section 5.6



B score (minor change)

3.1.4 (20) Lifetime of the CA certificate must be no less than two times of the maximum life time of an end entity certificate.

- True, described in section 6.3.2 on CP/CPS.
- Should be also added in section 5.6



B score (minor change)

3.1.5 (22) Certificate revocation can be requested by end-entities, registration authorities, and the CA. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.

- True, described in section 4.9.2 on CP/CPS.
- Should be also added in section 4.8.2



B score (minor change)

3.1.5 (24) 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.

- True, described in section 4.9.4 on CP/CPS.
- Should be also added in section 4.9.1



B score (minor change)

3.1.6 (27) The CRL lifetime must be no more than 30 days.

- True, described in section 4.9.7 on CP/CPS.
- Should be also added in section 4.9.9



B score (minor change)

3.1.6 (28) Every CA must issue a new CRL at least 7 days before the time stated in the nextUpdate field for off-line CAs, at least 3 days before the time stated in the nextUpdate field for automatically issued CRLs by on-line CAs.

- True, described in section 4.9.7 on CP/CPS.
- Should be also added in section 4.9.9



B score (minor change)

3.1.7 (41) 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.

- True, described in section 4.7.3 and referred in section 4.6.1 on CP/CPS.
- may be added in sections 3.3.1 and 5.6



B score (minor change)

3.2 (2) In order for an RA to validate the identity of a person, the subject should contact the RA face-to-face and present photo-id and/or valid official documents showing that the subject is an acceptable end entity as defined in the CP/CPS document of the CA.

- True, described in sections 4.2, 4.6, 4.7 on CP/CPS.
- Should be more clarified in section 4.1



B score (minor change)

3.2 (3) In case of non-personal certificate requests, an RA should validate the identity and eligibility of the person in charge of the specific entities using a secure method.

- True, described in sections 4.2, 4.6, 4.7 on CP/CPS.
- Should be more clarified in section 4.1



X score (could not evaluate)

3.1.7 (40) Certificates associated with a private key residing solely on hardware token may be renewed for a validity period of up to 5 years (for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits).

- No, our keys are stored in software.



1 Overview

2 Self-Audit

3 Summery



- CP/CPS needs to be approved
 - All corrections/clarifications will be done in CP/CPS (new version)

- Next Steps
 - Upgrading the CA Online machine (repository) and the CA Offline machine to the new version of OpenCa.
 - Will introduce Robot Certificates for grid purposes "Grid portals , Science Gateways ...", so any advices from CAs who already completed such a procedure, are welcome.
 - Expired and future certificates must be generated and hashed with sha2.



Questions ?

Hassina LADOUR
Aouaouche EL-MAOUHAB

ca@grid.arn.dz

