MaGrid CA Self audit and update

Nabil Talhaoui
MaGrid - CNRST
Mob.: +212 6 00 01 94 42
Mail: talhaoui@cnrst.ma

Tartu 2014

Overview

- General information
- Some statistics
- Self-auditing report
- Policy Updates
- Robot certificates

General information

- Established by CNRST in October, 2006 and accredited in September 2007.
- Single CA in the Moroccan academic field (No subordinate certification authorities).
- It provides X509 certificates for academic research and educational activities in Morocco (essentially for e-science and grid).
- Managed by CNRST-MaGrid team.
- CP/CPS Document follows RFC 3647.
- Web site: http://www.magrid.ma/ca.
- Current OID for CP/CPS: 1.3.6.1.4.1.26529.10.1.2.0
- Current version: 2.0

Some Statistics

Certificates	Number	Valid	Expired	Revoked
Users	323	**79**	219	25
Servers	114	**24**	81	9

- In 2014 :
  - 29 valid certificates (27 for users and 2 for servers)
  - 2 revoked certificates (2 for users and 0 for servers)

Self Audit

- Self audit was performed using the audit document GFD 169.
- We used the scoring system provided in the document:
  - A: Good
  - B: Recommendation (minor change)
  - C: Recommendation (major change)
  - D: Advice (must change)
  - X: Could not evaluate (N/A)

Self Audit

- 50 items with score A (good)
- 11 items with score B (minor change)
- 2 items with score C (major change)
- 2 items with score D (must change)
- 2 item with score X (N/A)

Self Audit

D (must change):

- **TRUE** but not in CP/CPS
  - (3.1.7 - 34) No user certificates may be shared.
  - **Must be added in section 4.5.1**

Self Audit

D (must change):

- **TRUE** but not in CP/CPS
  - (3.1.7 - 37) The end-entity certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125. In the certificate extensions :
    - 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

C (major change):

- **TRUE** but no evidence in CP/CPS
  - (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of he/she lost or compromised the private key pertaining to the certificate or the data in the certificate are no longer valid.
  - **Should be in Section 4.9.1.**

Self Audit

C (major change):

- **TRUE** but no evidence in CP/CPS
  - (3.1.9 - 46) Every CA should perform operational audits of the CA/RA staff at least once per year.
  - **Described in Section 8. Should be in Section 5.4.**
  - But it is not done every year. Partial audits are done

Self Audit

B (minor change):

- **TRUE** but to be clearer in CP/CPS
  - (3.1.2 - 7) The CA system must be located in secure environment where access is controlled, limited to specific trained personnel.
  - **Should be more clarified in Section 5.1.2.**

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (3.1.3 - 12) 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. Should be in 6.2.8.**

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (3.1.3 - 14) 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 in 6.2.4, 6.2.5 .**

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (3.1.6 – 27) The CRL lifetime must be no more than 30 days.
  - Located in Section 2.3. Should be 4.9.9
  - (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.
  - Located in Section 4.9.7. and Section 2.3. Should be 4.9.9
  - (3.1.6 – 29) Every CA must issue a new CRL immediately after a revocation.
  - Located in Section 2.3. Should be 4.9.9

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (3.1.7 – 33) The lifetime of subscriber certificates must be no longer than 395 days (13 months).
  - **Located in Section 6.3.2. and referred in Section 5.6.**
  - **But should be described in this section?**

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (3.1.7 - 36) 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. and 9.6.3 Should be in 6.2.8.**

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (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.
  - **Located in Section 4.7.3, and referred to this section in section 4.6 (Should be also added in section 3.3.1 and 5.6 ?)**

Self Audit

B (minor change):

- **TRUE** but to be clearer in CP/CPS
  - (3.1.8 - 44) These records must be kept for at least three years, where the identity validation records must be kept at least as long as there are valid certificates based on such a validation.
  - **Should be more clarified in Section 5.5.2.**

Self Audit

B (minor change):

- **TRUE** but in different section in CP/CPS
  - (3.1.10 – 48) 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

- Issues identified by self-audit:
  - Not all downtimes were announced to the relying parties.
  - Some CRLs were issued less than 7 days before the stated next update time in the latest-issued CRL.
    - Though there was no expired CRLs.
  - Power failures due to the external raisons (Electric provider).
  - All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.
    - Not all users know how to use the signed e-mail, so they prefer to come with there laptops directly to the RA/CA.

Policy Updates

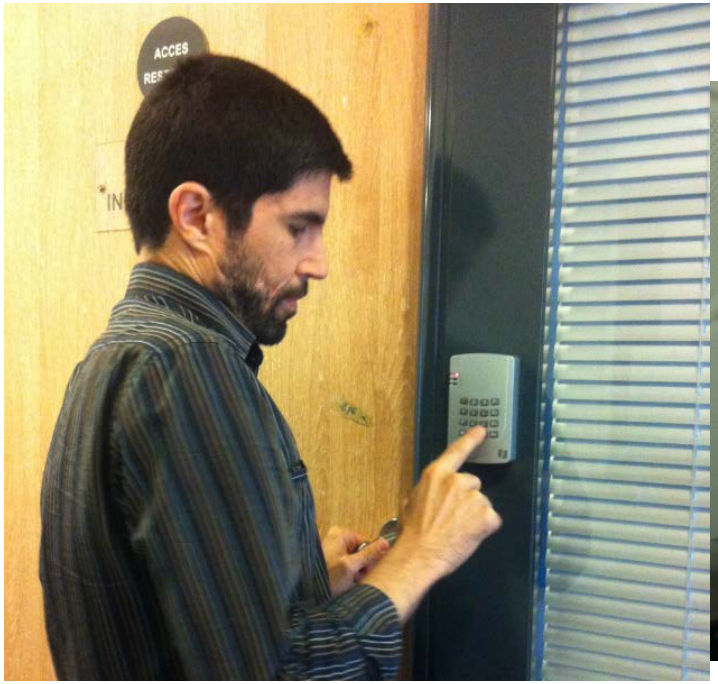
❑ Address and phone changes

- CNRST (hosting CA) has moved to a new location
- CNRST Address , the Manager CA Address , Phone and Fax have changed:
  - They are updated in the version 1.3.0 (Red color)
- No change in Email, web, and technical requirements.
  - Is it possible to change the URL of online-RA? the old one still valid but it's just a link redirection to the real machine.

Policy Updates

❑ Physical Security

- Physical security meets Classic AP and CP/CPS requirements
  - No changes in CP/CPS



Policy Updates

- Physical Security

Robot certificates

- Would like to introduce these for grid purposes “Grid portals , Science Gateways ...”
- Will follow “Guidelines on IGTF Approved Robots”

Robot certificate policy text

3.2.3 Authentication of individual identity

1. The certificate must be requested from the MaGrid RA in person, or be authenticated with a valid personal MaGrid CA certificate;
2. The certificate request must be preceded by a secure online submission to the MaGrid CA Public Server;
3. The identity of the Robot certificate owner must be authenticated as for a personal certificate;
4. The RA must retain a record to allow a Robot certificate to be traced to its owner.

Robot certificate DN

- **Illustration of a full subject distinguished name for a robot:**
  - **C=MA,**
  - **O=MaGrid,**
  - **OU=CNRST,**
  - **CN=**Robot **:** <Robot purpose> **-** <owner>
- Robot purpose expresses some intended purpose, e.g. "**MaGrid Science Gateway** "
- Owner is natural person responsible for robot, e.g. "**Nabil Talhaoui**"

Robot certificate DN

Extension	Attribute
Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	keyid, DirName, serial
Key Usage	critical, digitalSignature, KeyEncipherment, dataEncipherment
Extended Key Usage	serverAuth, clientAuth
Netscape Comment	STRING
CRL Distribution Points	URI
Certificate Policies	OID *
Subject alternative name	Subscriber's E-mail address

*** OID :**

- CP/CPS : 1.3.6.1.4.1.26529.10.1.3.0
- IGTF Classic Authentication Profile : 1.2.840.113612.5.2.2.1
- Robots : 1.2.840.113612.5.2.3.3.1

Conclusion

- CP/CPS needs to be approved
  - All corrections/clarifications have been done in CP/CPS (Version 1.3.0).
  - The highlighted version has been published :
    - (Changes due to self audit in red)
    - (Changes due to the introduction of robot certificate in green)
- Next steps:
  - Upgrading the online RA from OpenCA 0.9.3 to OpenCA version 1.1.1
  - Implementation of the approved changes in the technical materials
  - Update the user manual in MaGrid Wiki page

Thank you

Any questions?