UGRID CA

Self-audit report

Sergii Stirenko
stirenko@ugrid.org

Overview

- Self-audit was done in accordance with the GFD.169
- Audit date: Jan 15, 2011
- Summary:
  - A : 52
  - B : 1
  - C : 8
  - D : 4
  - X : 3

3.1 Certification Authority
3.1.1 CP/CPS

- (1) Every CA must have a CP/CPS

https://ca.ugrid.org/ca.php

- (2) Is there a single CA organization per country, large region or international organization?

UGRID CA is the country-wide CA.

- (3) Every CA must assign its CP/CPS an O.I.D.

OID 1.2.840.113612.5.4.2.6.1.1.1.4

- (4) Whenever there is a change in the CP/CPS the O.I.D. of the document must change…

(C) Sergiy Velichkevych the a person determining CPS suitability for the policy

3.1 Certification Authority
3.1.1 CP/CPS

- (5) All the CP/CPS under which valid certificates are issued must be available on the web.

YES, all versions of CP/CPS are available on the web

https://ca.ugrid.org/ca.php

- (6) The CP/CPS documents should be structured as defined in RFC 3647.

YES

- (7) The CA computer where the signing of the certificates will take place must be a dedicated machine ...

The signing machine is a dedicated machine, completely offline and powered down between uses.

3.1 Certification Authority
3.1.2 CA System

- (7) The CA system must be located in a secure environment ...

CA is located in High Performance Computing Center of the National Technical University of Ukraine "Kyiv Polytechnic Institute". HPCC's rooms are guarded with local security personnel. The signing machine locked in the safe with controlled access.

- (8) The CA system must be completely off-line or on-line. On-line CAs must use at least a FIPS 140-2 ...

CA is completely offline

- (9) The secure environment must be documented and approved by the PMA ...

(C) Secure environment not documented

3.1 Certification Authority
3.1.3 CA Key

- (10) The CA key must have a minimum length of 2048 bits

CA key is 2048 bits

- (11) The CA key must be configured for long term use

5 years, current Expiration date: Jan 19, 2013

- (12) If the private key of the CA is software-based, it must be protected with a pass phrase …

Yes, the private key is software-based. Protected with strong pass phrase known only to CA personnel.

- (13) Copies of the encrypted private key must be kept on offline media in a secure location where access is controlled.

A copy of the encrypted private key is kept on offline media in secure location in the sealed box.

3.1 Certification Authority
3.1.3 CA Key

- (14) The pass phrase of the encrypted private key must also be kept on offline media, separated from the encrypted private keys …

YES

- (15) The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates and signed revocation lists.

(X) Not applicable, offline CA

- (16) When the CA's cryptographic data needs to be changed, such a transition shall be managed …

(C) Not documented

- (17) The overlap of the old and new key must be at least the longest time an end-entity certificate can be valid …

(X) We haven't changed CA crypto data yet

3.1 Certification Authority
3.1.4 CA Certificate

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

Yes, published in EUGridPMA repository, available on the Web

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

Lifetime of the CA certificate is 5 years

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

YES, maximum lifetime of the end entity certificates is 1 year

- (21) The profile of the CA certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

YES

3.1 Certification Authority
3.1.5 Certificate Revocation

- (22) Certificate revocation can be requested by end-entities, registration authorities, and the CA. Others can request …

Usually, revocation can be requested by end-entity, RA or CA. Others can request revocation if they prove compromise of the private key.

- (23) The CA must react as soon as possible, but within one working day, to any revocation request received.

Revocation requests are processed within one hour in working time and on a best effort basis on holidays.

- (24) Subscribers must request revocation of its certificate as soon as possible, but within one working day …

Our clients are bound to it by our CP/CPS and the document they are signing for each request

- (25) Revocation requests must be properly authenticated.

Encrypted and signed emails in most cases. Photo ID in case if private key was lost.

3.1 Certification Authority
3.1.6 Certificate Revocation List

- (26) Every CA must generate and publish CRLs.

YES, http://ca.ugrid.org/cacrl.der

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

YES, 30 days

- (28) Every CA must issue a new CRL at least 7 days …

YES, 10 days before nextUpdate field

- (29) Every CA must issue a new CRL immediately after a revocation.

YES

- (30) The signed CRL must be published in a repository at least accessible via the World Wide Web, as soon as issued.

YES, CRL is published as soon as issued

- (31) The CRLs must be compliant with RFC5280.

YES

3.1 Certification Authority
3.1.7 End Entity Certificates and Keys

- (32) The user key and the host key must have a minimum length of 1024 bits.

YES

- (33) Lifetime of user certificates and host certificates must be no longer than 13 months.

User and host certificated have lifetime not more than 12 months

- (34) No user certificates may be shared.

Users are obliged through the CP/CPS and the document they are signing for each request

- (35) The authority shall issue X.509 certificates to end entities based on cryptographic data generated by the applicant …

UGRID CA issue certificates to end entities based on cryptographic data generated by the applicant

- (36) Every CA should make a reasonable effort to make sure that subscribers realize the importance of properly protecting…

It is clearly stated in the CP/CPS and in the paper certificate request form

3.1 Certification Authority
3.1.7 End Entity Certificates and Keys

- (37) The end-entity certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

YES

- (38) If a commonName component is used as part of the subject DN, it should contain an appropriate presentation of the actual name of the end-entity.

YES, first and last names in case of user certificate, and FQDN in case of host certificate

- (39) Certificates (and private keys) managed in a software token should only be re-keyed, not renewed.

(D) It is stated in the CP/CPS, but we don't check

- (40) Certificates associated with a private key residing solely on hardware token may be renewed …

(X) Not applicable, don't use hardware tokens

- (41) Certificates must not be renewed or re-keyed consecutively for more than 5 years without a form of ...

YES, the subscriber must go through the procedure equal to the application for a new certificate at least once every 3 years.

3.1 Certification Authority
3.1.8 Records Archival

- (42) Every CA must record and archive all requests for certificates, along with all issued certificates, all requests for revocation, all the issued CRLs and login/logout/reboot information of the issuing machine.

(D) all except login/logout/reboot information of the issuing machine

- (43) These records must be available to external auditors in the course of their work as auditor.

(D)Difficult to make available for auditing

- (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.

YES, all records are kept

3.1 Certification Authority
3.1.9 Audit

- (45) Each CA must accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.

YES, section 8 CP/CPS

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

Internal audits are performed at least once per year

- (47) A list of CA and RA personnel should be maintained and verified at least once per year.

YES, RA list https://ca.ugrid.org/ras.php

verified several times a year

3.1 Certification Authority
3.1.10 Publication and Repository Responsibilities

- (48) The repository must be run at least on a best-effort basis, with an intended availability of 24x7.

(B) YES, but some hours of downtime was in 2010 due to power failures

- (49) The accredited authority must publish their X.509 signing certificate as the root of trust.

Yes, our root is published by EUGridPMA/IGTF

- (50) Each authority must publish the following for their subscribers, relying parties and for the benefit of distribution ***YES, all info published***
- (51) The originating authority must grant to the PMA and the Federation the right of unlimited re-distribution …

No distribution restrictions

- (52) The CA should provide a means to validate the integrity of its root of trust.

YES, SHA1 fingerprint is published by EUGridPMA/IGTF

- (53) The CA shall provide their trust anchor to a trust anchor repository ...

YES, available in the EUGridPMA/IGFT repositories

3.1 Certification Authority
3.1.11 Privacy and Confidentiality

- (54) Accredited CAs must define a privacy and data release policy compliant with the relevant national legislation. The CA is responsible for recording, at the time of validation, sufficient information regarding the subscribers to identify the subscriber. The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that CA.

(C) The legislation has changed at the end of 2010 and it is necessary to modify the policy according to it

3.1 Certification Authority
3.1.11 Compromise and Disaster Recover

- (55) The CA must have an adequate compromise and disaster recovery procedure, and we willing to discuss this procedure in the PMA. The procedure need not be disclosed in the policy and practice statements.

(D) No compromise and disaster recovery plans

3.2 RA
3.2.1 Entity Identification

- (1) A PKI CA must define the role of a registration authority (RA), and these RAs are responsible for the identity vetting of all end entities.

YES, section 1.3.2 of CP/CPS

- (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.

YES, The initial authentication of a person based on government-issued identification documents and physical appearance of the applicant to the RA.

- (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.

encrypted and signed emails

3.2 RA
3.2.1 Entity Identification

- (4) For host and service certificate requests, an RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN …

(C)Host ownership verified by DNS/WHOIS and personal RA knowledge

- (5) An RA must validate the association of the certificate signing request.

RA does it by comparing the personal data and public key modulus at the paper form and incoming request to be processed

- (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.

Checks Photo ID

3.2 RA
3.2.2 Name Uniqueness

- (5) Any single subject distinguished name must be linked to one and only one entity.

YES

- (6) Over the entire lifetime of the CA it must not be linked to any other entity.

YES

3.2 RA
3.2.3 RA to CA Communications

- (7) All communications between the CA and the RA regarding certificate issuance or changes in the status of a certificate must be by secure and auditable methods.

YES, Encrypted and signed emails

- (8) The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.

(C) This procedure isn't well documented

3.2 RA
3.2.4 Records Archival

- (9) The RA must record and archive all requests and confirmations.

(C) only paper personal certificate request forms and photo ID copies

- (10) The CA is responsible for maintaining an archive of these records in an auditable form.

(C) Difficult to make available for auditing

Thank You !