CHANGELOG of TSU CA

Changelog from CP/CPS 0.0.0 to CP/CPS 1.0.1 – May 12, 2014

- We modified the filename
- We modified the CP/CPS document version and date
- 1.2 We changed the CP/CPS document version, date and inserted IANA Enterprise number.
- 1.5.1 and 2.1 We replaced the CP/CPS email grid-ca@grena.ge by grid-ca@tsu.ge
- 2.2 We replaced the CP/CPS website grid-ca.grena.ge by grid-ca.tsu.ge
- 4.1.2, 4.2.1, 4.3.2, 4.4.1, 4.7.3, 5.1.3, We removed information about the web portal, because of its lack
- 4.2.2 We replaced private key size 1024 bit by 2048 bit
- 4.9.3 We removed information about revocation via web site because of its lack.
- 4.9.7 We replaced minimum CRL lifetime 7 day by 30 day
- 5.1.6 We removed "magnetic tape cartridges" and "floppies" and inserted external HDD drive and changed "CD-ROM" by "DVD-ROM"
- 6.1.5 We changed the minimum key length for an End Entity certificate 1024 bit by 2048 bit and for the TSU CA private key 2048 bit by 4096 bit.
- 6.3.2 We changed the maximum lifetime for certificates issued by TSU CA 1 year by 13 month.
- 7.1.3 We changed the hash function "id-sha1 1.3.14.3.2.26" by "sha256 2.16.840.1.101.3.4.2.1" and the signature algorithm "sha1WithRSAEncryption 1.2.840.113549.1.1.5" by "sha256 with RSA Encryption 1.2.840.113549.1.1.11"
- 7.1.4 We inserted some paragraph at the beginning:

  "The subject name is of the X.500 name type. It has one of the following forms:"

  and at the end :

  "The Distinguished Name must be unique for each subject certified by the TSU CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the commonName to ensure uniqueness.

  The canonical name in the certificate subject must be able to be obtained from the real subject name.

  Certificates must apply to unique individuals or resources. Subjects may not share certificates." .

  We changed structure by list of user, host and service certificate and replaced in name forms: Issuer: C=GE by Issuer (TSU CA), CN=TSU-CA by

O=TSU GRID, CN=SUBJECT NAME by CN=commonName and removed Subject: C=GE and O=INSTITUTE. We explained commonName for all three types of certificates.

Changelog from CP/CPS 1.0.1 to CP/CPS 1.1.0 – May 30, 2014

- We modified the filename
- We modified the CP/CPS document version and date
- 1.2 We changed the CP/CPS document version, date and inserted IANA Enterprise number.
- 4.4.1 We replaced the sentence:

  "The subscriber must send an e-mail within 5 working days from the day that his/herSubscriber receives certificate was issued and complete theinstructions by mail, according to that mail he/she automatically agrees certificate acceptance procedure in which (s)he will be stating that (s)he:"

  by

  "Subscriber receives certificate and instructions by mail, according to that mail he/she automatically agrees certificate acceptance procedure in which (s)he will be stating that (s)he:"

- 7.1.4 We replaced "C=GE, O=TSU, CN= TSU GRID" by "DC=GE, DC=TSU, CN=TSU Root CA" and "C=GE, O=TSU GRID, O=Organization Name, CN=commonName" by "DC=GE, DC=TSU, O=People, O=Organization Name, CN= commonName ".

  We replaced for Services certificates the sentence:

  "where the commonName must be the DNS FQDN."

  by

  "where the commonName must include the service name and DNS FQDN separated by a / in the commonName component."

- 7.1.5 We shortened this point by sentence:

  "There are no other name constraints than those that are to be derived from the stipulations in 7.1.4 and 3.1.1."

Changelog from CP/CPS 1.1.0 to CP/CPS 1.1.1 – June 10, 2014

- We modified the filename
- We modified the CP/CPS document version and date
- 1.6.1 We inserted in definitions table FQDN
- 3.1 We inserted sentences at the end:

  "The common names must be encoded as Printable Strings according with RFC 1778 and

  RFC 2252. The characters allowed in the common names of personal certificates are as

  follows:

  • ' ' (space), '(', ')' and '-';

  • '0' – '9';

  • 'a' – 'z' and 'A' – 'Z'.

  In addition, the characters '.' (period) and '/' (slash) are allowed in host and service certificates. The period must be used to separate the DNS host name components and the slash must be used to separate the service name or the keyword "host" from the DNS host name."

- 3.2.3 We inserted photo for user personal identification
- 4.1.2 We inserted sentence at the beginning:

  "The requesting party generates the key pair with a size of at least 2048 bits on their system through the instruction provided at the TSU CA web site."

- 4.2.3 We replaced sentence:

  "Each certificate application will take no more than 2 working days to be processed."

  by

  "After that, subscriber will complete correctly all necessary procedures of certificate request, each certificate application will take no more than 3 working days to be processed."

- 4.7.3 We corrected some syntax mistakes: "re key" by "re-key" and "beforeexpiration" by "before expiration". We inserted more explanation:

  "Expiration warnings will be issued to subscribers 30 days before expiration and 7 days before expiration if not renewed yet. Re-key before expiration can be accomplished by sending a digitally signed e-mail to the RA serving their organization."

- 5.1.6 We replaced the sentence:
  "The backup of TSU CA private key will be stored on external HDD that are directly attached on server and DVD-ROMs."

  by

  "Backup of CA (CRLs, Certificates and CSRs) are performed after every change, backups are recorded into USB flash drive."
- 5.6 We changed overlap time of old and new private key 12 year by 13 months

Changelog from CP/CPS 1.1.1 to CP/CPS 1.1.2 – June 10, 2014

- We modified the filename
- We modified the CP/CPS document version and date
- 4.1.2 We added ID number as required detail for user registration
- 4.1.2, 4.2.1, 4.3.2, 4.4.1, 4.7.3, 5.1.3 We returned the information about web portal
- 4.3.2 We removed sentence: "In the same e-mail the subscriber will be requested to acknowledge his/her adherence to this policy."
- 5.7.1 We replaced all by:
  "If the CA private key is compromised or destroyed the TSU CA will:
  - Inform the EuGridPMA;
  - Inform all the nodes, RAs and other relying parties
  - Conclude the issuance and distribution of certificates and CRLs
  - Generate a new CA certificate with a new key pair that will be soon available on the website."

- 9.4 We had "TSU CA does not collect any confidential or private information"
  and we added exception: "except for the case when CA or RA archives copies of ID documents for identity validation of a user certificate request. TSU CA guarantees that this personal information will not be used for any other purposes."

Changelog from CP/CPS 1.1.2 to CP/CPS 1.1.3 – November 3, 2014

- We modified the filename
- We modified the CP/CPS document version and date
- 3.1.1 We added surname for subject name"
- 7.1.2 For "End Entity certificates" We removed sentense "Authority key identifier", added sentences "extended key usage" and "Certificate Policies"