
# CESNET CA Self-audit EUGridPMA meeting Tartu, Estonia 2014

Jan Chvojka
CESNET PKI
ca@cesnet.cz

# About CESNET CA

CESNET CA

- is signed by self-signed CESNET Root CA
- SW: EjbCA + JBoss AS on Linux, HW: dedicated server, nCipher HSM module (FIPS Level 3)
- is running on dedicated machine in locked room, access allowed to CA operators only, logged and monitored.
- Subject: cn=CESNET CA 3, o=CESNET CA, dc=cesnet-ca, dc=cz

CESNET Root CA

- is offline and stored in safe

# CESNET CA CP/CPS

http://pki.cesnet.cz/en/ch-cp-cps.html

CESNET CA CP/CPS

- OID 1.3.6.1.4.1.8057.1.2.2.3.1
- Version: 3.1

CESNET Root CA CP/CPS

- OID: 1.3.6.1.4.1.8057.1.2.3.1.1
- Version: 1.1

# CESNET CA - what's new

CESNET CA Root is offline in safe, once a year is CRL generated. In 2013 we realized, that CCA3 USB stick is broken – we proved our disaster recovery procedure is working.

Changed the old PIX firewall to ASA firewall / IDS – first step to be able to operate on IPV6.

Since december 2013 we are offering also SHA2 certificates.
CESNET CA CPS: The CESNET CA SHOULD use the following cryptographic algorithms: … SHA1
Change in our CPS is needed ASAP.

Plan: migrate hardware token to NetHSM.

# CESNET CA – audit results

B: 0
C: 0
D: 3
X: 2
Not sure: 1

# D – must be changed

**(34) No user certificates may be shared.**

Users are already signing that, but it is not in CP/CPS.

# D – must be changed

**(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 must be adequately protected by system methods.**

Users are already signing that, but it is not in CP/CPS.

# D – must be changed

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

RA operational audit is done usually once per 2 years. Audit is not mentioned in the CP/CPS. Also results of RA audit is not auditable.

# Not sure

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

CESNET CA CP/CPS:

The Registration Authority verifies the application. If the application is accepted, the RA issues a one-time authentication token to the requester.

The token MUST be passed during a face-to-face meeting with the requester or using a message encrypted using the requester's valid personal certificate.

The requester requests the certificate from the CA's enrollment application using the one-time authentication token for authentication.