The CESNET CA 3 is (almost) dead, long live the CESNET CA 4!

Jan Chvojka
CESNET

EUGridPMA, May 2018
Karlsruhe

CESNET CA 3 vs. CA 4

	CESNET CA 3	CESNET CA 4
DN	CESNET CA 3, O=CESNET CA, DC=cesnet-ca, DC=cz	CESNET CA 4, O=CESNET CA, DC=cesnet-ca, DC=cz
Issuer DN	CESNET CA Root, O=CESNET CA, DC=cesnet-ca, DC=cz	CESNET CA Root, O=CESNET CA, DC=cesnet-ca, DC=cz
Valid from	15th of December, 2009	20th of May, 2018
Valid to	18th of December, 2019	20th of May, 2028
Signing algorithm	SHA1	SHA256
Key lenghth (bits)	2048	4096

What remained unchanged

Unchanged from CA 3:

Private key generated in HSM (nShield Connect)

Software: EjbCA on Linux

HSM in secure room with monitored access (24x7 surveillance)

Only CA admins have access to CA room

RA officers: IP address restricted, access keys on HSM tokens

End users: no direct access to CA, only via CESNET portal

CP/CPS proposed changes:

Supported only SHA256 certificates

Minimal key length: 2048 bits

External CA for authentication: added Czech qualified CAs

Dropped *Security Trustee* role

Other:

In end-user form added link to CESNET's GDPR page

We would like to know…

Topics to discuss:

Lots of EUGridPMA CP/CPS has minimal key length 2048b. What about EC certificates?

Should be possible to check end-user identity via ANY European qualified CA? Can I get your certificate using PostSignum?


cesnet
THANK YOU!
ANY QUESTIONS?