Záznam z generovania asymetrického kľúčového páru a elektronickej žiadosti vo formáte PKCS#10 pre systém na poskytovanie kvalifikovaných služieb (CA certifikát)

Dňa 10.12.2020 sa v priestoroch dátového centra DC Digitalis, Trnavská cesta 110/B, Bratislava uskutočnilo generovania asymetrického kľúčového páru na zariadení NShield nCipher XC Base+. Následne na to sa v priestoroch Poskytovateľa bezpečným pripojením na diaľku do PKI infraštruktúry dňa 16.12.2020 vytvorila elektronická žiadosť vo formáte PKCS#10.

Dátum a miesto generovania:

10.12.2020

- priestory dátového centra DC Digitalis, Trnavská cesta 110/B, Bratislava

16.12.2020

- priestory poskytovateľa brainit.sk, s.r.o., Veľký diel 3323, 010 08 Žilina

Identifikácia zariadenia, na ktorom bol vygenerovaný kľúčový pár:

- Produkt: nCipher nShield Connect XC Base+
- Výrobca: nCipher
- S/N: 46-XC4002

Elektronická žiadosť vo formáte PKCS#10:

- Názov súboru: csr_nfqes.csr
- Algoritmus: RSA
- Veľkosť kľúča: 4096

PEM formát žiadosti:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEsjCCApoCAQAwbTEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTEb
MBkGA1UECgwSYnJhaW5pdC5zaywgcy5yLm8uMQswCQYDVQQGEwJTSzEQMA4GA1UE
BwwHxb1pbGluYTEOMAwGA1UECwwFTkZRRVMwggIiMA0GCSqGSIb3DQEBAQUAA4IC
DwAwggIKAoICAQCv7GWcIx4WQc+RCz86pyg7A/O/sqN/sLv5RHxn6AXWSlcCd6pC
PiNC8GMsxQfXJEY90X2WxneuJidNG7XGKWxnarY3nkE18Bk1AZ6Ppt455EfBWepW
KFLlvt4BOgFOFyNCIvNnvg47gRNVBw5FqsKsOoKZ0PYewce6u5iKRT23quLcGeE+
btqzDYea61fLPKKBc092QW7xKroVpG9LrDyUZC6IsqjjdzQ36lqK1DVZJIJ3X0Gz
eMvldigSf3s550nSt+A8dLYcaAwxT1+Ebw4W6RuzeGSD1d/6n3+OOtS0AabdTkwZ
fm2p10QbmlwCUYrF2Ogu+I/2XIe090kKvYauQvn3LZZsvss9jd/NSQRF3nzoksim
qgLvCpu+jbNoL/sl5uIVeqlxAuvbjtUcirmml6xgIIiyH3aTmFZiBD8ze2cyNi7L
6P8VBuOa1QRwtZD5sF8qELdVtToRqwn/99QgHj7rrR2wO5p+W84yn8nBXjzzGcLy
nAxeOu0aqX1pNWmrCyHUg51b7fXn/+7JNQlWKOFvDaDehKnqmhbJ9BP4Trzvu3SV
tuYytA1KXbZq/eI9NDzOtFGv8TM8DTcYgJ6lST+PTgKHFOqUGK28dM6FJy38tWdA
Nus36cNTa5G6Rt55v3YN0AI5Yk19fMxX8MnI03zcpk3II4yo59k2NvXmUQIDAQAB
oAAwDQYJKoZIhvcNAQELBQADggIBAH3JVofg3pHM5+n2PEef8uyXRHV1EAGk6Rfz
6uBas8F5bwsetuh/nmVy/5GL/UcRcdjwcBA80qhVZOtGp/KrQ+8JGCczChDhrwff
Csi3asEoArB7VoZLoPwQA+iCVPB2SKt4A5AC1o9pkG3eouVAGYYOyDl6aQ8uazaP
RAePTsC5PsVhm1LP/ETb5ODfMmvWqdldsaOWPldrdaHADCmlLPndWbomqtGp9w7h
cDK120GBvU4Ru2FCvL48yyl94zSjBoMTyiTyEVCQpdUJ9mdS+cQ//0Eulc0bRAK1
vfUs9QB1154+dse3JxShIK9rri50pr9fzPze6xE7rxSt/UGq81dPLX8mMr67RDE6
```

```
3L6IsPT0Tgi99Edui6Z7ntD7whedHHUKt7BaYRSaHciUzDwBRHP9mfaHHzuP19kJ
m2GV+XbujXlfbnGKSGbpZBSWPKG1i33wzLx1/e4b3AU66ql0LpRvox7Q6OGFPUXz
W5S30jQwbHMum0wI4bzdsbn+5MT7At7JxyxdX0WZxlWwK+M+dXmHVZclDgPy+z6r
JWDCqi1Zy65YxZBFwYEZOv2SXe0TzgN2z5OsCQUA12bC0C15FmsGXw6ZPLPdrZXb
PPkZ9lYx20N7Bk1EAHlxBgqDhOb6Q+B5WbNVJ/SuIKcytelE1Q69eXqc7FYwh5ty
PcuWEMxn
-----END CERTIFICATE REQUEST-----
```

ASN.1 formát žiadosti:

```
SEQUENCE (3 elem)
  SEQUENCE (4 elem)
    INTEGER 0
    SEQUENCE (5 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String CA Signing Certificate
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String brainit.sk, s.r.o.
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString SK
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.7 localityName (X.520 DN component)
          UTF8String Žilina
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
          UTF8String NFQES
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (4208 bit)
001100001000001000000010000010100000001010000010000000100000000100000…
        SEQUENCE (2 elem)
          INTEGER (4096 bit)
717704959039196645770337134582108068474134871575727320217974992157478…
          INTEGER 65537
    [0] (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
    NULL
  BIT STRING (4096 bit)
011111011100100101010110100001111110000011011110100100011100110011100…
```

Zoznam prítomných osôb:

Dátum: 16.12.2020

Meno a Priezvisko	Rola	Podpis zúčastnených osôb
Ing. Martin Berzák	CISO	
Ing. Michal Papučík	CIO	
Ing. Branislav Juriš	Administrátor PKI	
Ing. Eduard Baraniak	Konateľ, CEO	
Ing. Ján Kuruc	Konateľ, CEO	