


|   |         |       |
|---|---------|-------|
|  NFQES | Verzia: | 1.0   |
| "Interné"   | Strana: | 1 z 3 |

## Záznam z generovania asymetrického kľúčového páru a elektronickej žiadosti vo formáte PKCS#10 pre systém na poskytovanie kvalifikovaných služieb (OCSP 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: ocsf\_nfqes.csr
- Algoritmus: RSA
- Veľkosť kľúča: 3072

### PEM formát žiadosti:

-----BEGIN CERTIFICATE REQUEST-----

```
MIIDtzCCA8CAQAwcjkEMCIGA1UEAwwbQ0EgT0NTUCBTAwduaw5nIENlcnpZmljYXRIRSwGQQYDVQKDBJicmFpbm10LnNrLCBzLnIuby4xCzAJBgNVBAYTAINLMRAW DgYDVQQHDAFFvWlsaw5hMQ4wDAYDVQQQLDAVORlFFUzCCAaIwDQYJKoZIhvcNAQEB BQADggGPADCCAYoCggGBALiANlph4BdGoDPqJlNeQwW6MepqOym7ntKsTwpArxdi rpuA5Qap9uhhjV5D7HzQ12cv0Jt7moVRIDgcQidJ0y25SxyuddyCOd8jqJMPetd8 9gEHIQ9ksnLnD1LaPr1jH9cjCFHSRF07S1w5R6W6kvPXytfKgnOXXsI0tNKruR4u cQaUFGpBTpfokF/7pUcu+2z3EvUDUVsQUa18ZrVfsUGuzYiSH/My/1Bpv6w5Ctk3 9imNbeS4TERSEpEAxzTVPDSHCPWR1IBOE224ryrKlBQ9z1ZX0qI66Y83UAdaAU9H JyidhqgM0v36zFe0eNrEHphyFKIMFOFX90W9unXZvPhIkJ+BxPwi0VwfH3fw/MIi uZonyDKa1/r6D8AHqJurPo5ILrZAPS3FGyy0+jb+iCOXbpx6C00dNqjNadbthww2 y5+nix5QEI7wr9Br1PB+IIqsHz1YHjpyZec0kiVYkY1lbtYqUPkizJXhk7KUggSV 2bJYGKXhRyyFpBK++0yR8QIDAQABoAAwDQYJKoZIhvcNAQELBQADggGBACaHgJnx 0beHvetp2MjbuAuJ0FSis/ufuoN7ZsL+gkeItHEB/1wmJKLbnexJSV/4p7H82kIy oJh4NH0gH3cUm4CbWLErXcFp560xR1L27Abt3hVeIXfMYdFdMgu8W0g7YWHIAqeg GzFt6Qt81Ev0mFnLtt86419VpjIFjz/Kd7wWbcF3AHnhuIco8SHxo/jwqhP19EUm Nq4x2Kh5pnNeua2JGzkDZxERZzsPtFwWJ68XFEUJuI5FEyYyCSChTcIkWBKwz3o uuXas2X42CnCb9nIc/Xn1e6tT0mqOyJRL9GU+BL0pVs74n78Xu2iopZgWt6U9CvW wFSMnNBqqEBArCZrksL/V4fAWzhQ1vRA+nVpAqb00X0izo5MZMI5pwndNXbok6zL 842CCna4f0GXZMZFkM15gNnppIh1iB2A7fGf/UaqPeyMyGqeq25wVHMWxmDBgJ1 XypyIich2wurqarDDPjrxBjHgBcdqF2zOCg8Rowyi4o1Dzq2yf9DUZz/Ew==
```

|   |         |       |
|---|---------|-------|
|  NFQES | Verzia: | 1.0   |
| "Interné"   | Strana: | 2 z 3 |

-----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 OCSP 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 (3184 bit)
      0011000010000010000000001100010100000001010000010000000011000000100000...
    SEQUENCE (2 elem)
      INTEGER (3072 bit)
      418702001723099448465526387289843722641116660153539040212222054379834...
      INTEGER 65537
    [0] (0 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
    NULL
  BIT STRING (3072 bit)
  001001101000011110000000100110011111000111010001101101111000011110111...

```

**Zoznam prítomných osôb:****Dátum: 16.12.2020**

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