

**TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ**

**XX - IAM B2B Klientsky komponent**

**Manuál pre administrátorov**

Projekt je spolufinancovaný Európskou úniou  
 Európsky fond regionálneho rozvoja

d

dd

Európsky fon

**Elektronické služby zdravotníctva**

kód ITMS projektu: **2110120009**

www.informatizacia.sk  
 www.opis.gov.sk

Základné informácie o dokumente

|  |  |
| --- | --- |
| **Názov dokumentu** | IAM\_B2B\_Klientsky\_komponent\_Manual-pre-administratorov\_v1\_1 |
| **Aktuálna verzia** | 1.3 |
| **Vlastník dokumentu** | BSP |

História dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzia** | **Dátum** | **Autor** | **Popis verzie a zmien oproti predchádzajúcej verzii** |
| 1.1 | 7. február 2018 | BSP | Úvodná verzia dokumentu. |
| 1.2 | 15. marec 2018 | BSP | Doplnená informácia o spôsobe inštalácie certifikátu |
| 1.3 | 25. November 2021 | NCZI | Úprava špecifikácie typu HSM |

Akceptačné riadenie

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Odberateľ** | | | **Dodávateľ** | | |
| **Dátum** | **Meno (Rola)** | **Podpis** | **Dátum** | **Meno (Rola)** | **Podpis** |
|  | Marian Šimegh |  |  | Štefan Gordian |  |

Súvisiace produkty a referenčné materiály

|  |  |
| --- | --- |
| **ID** | **Názov dokumentu a referencia** |
|  |  |

**Charakteristika dokumentu**

Cieľom dokumentu je popísať integráciu na servisné rozhrania systému NZIS, konkrétne subsystému IAM pre Business to Business komunikáciu.

Dokument popisuje vzorové postupy pri inštalácii a konfigurácii hardvérových šifrovacích moduloch ako aj základný postup generovania kľúčov a vytvárania žiadostí o certifikáty.

Dokument je určený:

* Administrátorom IS PZS

[1. Úvod 4](#_Toc505760158)

[1.1 Interné a sieťové HSM 4](#_Toc505760159)

[1.2 Typografické konvencie 4](#_Toc505760160)

[1.3 Základné pojmy 6](#_Toc505760161)

[2. Inštalácia a konfigurácia interného HSM (PCI karta) 7](#_Toc505760162)

[2.1 Inštalácia nCSS 7](#_Toc505760163)

[2.2 Vytvorenie nového Security World a administrator card set, konfigurácia CNG nCipher KSP 10](#_Toc505760164)

[2.3 Konfigurácia CAPI (32bit a 64bit) nCipher CSP 15](#_Toc505760165)

[3. Inštalácia a konfigurácia sieťového HSM 17](#_Toc505760166)

[3.1 Inštalácia nCSS na Windows servery 17](#_Toc505760167)

[3.2 Konfigurácia sieťového subsystému HSM 20](#_Toc505760168)

[3.3 Vytvorenie RFS na Windows servery 20](#_Toc505760169)

[3.4 Konfigurácia RFS na HSM 22](#_Toc505760170)

[3.5 Vytvorenie nového „Security World“ a administrator card set na HSM 22](#_Toc505760171)

[3.6 Definovanie klienta na HSM 23](#_Toc505760172)

[3.7 Pripojenie servera k HSM 23](#_Toc505760173)

[3.8 Konfigurácia CNG nCipher KSP na Windows servery 24](#_Toc505760174)

[3.9 Konfigurácia CAPI (32bit a 64bit) nCipher CSP na servery 26](#_Toc505760175)

[4. Overenie funkčnosti HSM 28](#_Toc505760176)

[5. Generovanie kľúčov a CSR v HSM 30](#_Toc505760177)

# Úvod

Tento dokument v stručnosti opisuje postupy spojené s inštaláciou a konfiguráciou hardvérových šifrovacích modulov (HSM) **Entrust nShield**. Tento dokument nenahrádza informácie ani dokumentáciu dodávateľa HSM a nie je normatívny.

**V prípade akýchkoľvek rozporov medzi touto dokumentáciou a dokumentáciou dodávateľa HSM, má prednosť dokumentácia dodávateľa HSM.**

## Interné a sieťové HSM

HSM Entrust nShieldsa dodávajú v dvoch najčastejších verziách:

* sieťové appliance,
* interný HSM modul / PCI karta.

Od konkrétneho vyhotovenia HSM závisí:

* spôsob inštalácie a konfigurácie (tak fyzickej: montáž do servera / racku, ako aj logickej),
* možnosti podpory virtuálnych serverov (podporované len v sieťovej verzii HSM),
* možnosti pripojenia viacerých klientov k HSM (možno len v sieťovej verzii HSM),
* cena HSM a pod.

Celkové porovnanie jednotlivých typov HSM prináša:

* interné HSM:
  + https://www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-solo
* sieťové HSM:

https://www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-connect

Inštalácii a konfigurácii interných HSM nShield Solo sa venuje kapitola 2. Inštalácii a konfigurácii sieťových HSM nShield Connect sa venuje kapitola 3.

## Typografické konvencie

**Piktogramy:**

|  |  |
| --- | --- |
|  | Poznámky |
|  | Dôležité informácie |
|  | **Dôležité upozornenia na potenciálne problémové časti, ktoré môžu spôsobiť závažné problémy pri funkčnosti systému.** |

sKurzíva:

* Internetové adresy, URL, URI, mená serverov, IP adresy, napr.:
  + *127.0.0.1*
* Cesty v súborovom systéme, napr.:
  + *C:\Windows\System32*
* Skupiny, napr.:
  + *Domain Admins*
* Iné hodnoty parametrov

|  |  |
| --- | --- |
|  | V prípade **ak hodnota parametrov nie je definovaná** použije sa prednastavená (***default***) hodnota. |

Kurzíva:

* Postupnosť krokov v používateľskom rozhraní oddelené pomocou >, napr.:

*Configuration Initialization > Initialize Configuration*

**Courier:**

* Listing programov a skriptov, ktoré musia byť prepísané od slova / do slova, napr.:

|  |
| --- |
| **"c:\Program Files (x86)\nCipher\nfast\bin\nopclearfail.exe" --clear --all** |

<Courier>:

* Listing programov a skriptov, ktoré musia byť parametrizované, napr.:

|  |
| --- |
| nethsmenroll.exe --force <IP adresa HSM> <HSM ESN> <HSM KNETI hash> |

## Základné pojmy

| ***Pojem/skratka*** | **Vysvetlenie** |
| --- | --- |
| *Certificate Signing Request (CSR)* | Žiadosť o certifikát v elektronickom tvare. Táto žiadosť nenahrádza papierovú žiadosť ani zmluvu medzi CA resp. RA a žiadateľom. Slúži iba ako technický prostriedok pomocou ktorého žiadateľ poskytuje svoj verejný kľúč CA. Žiadosť obsahuje informácie (predovšetkým verejný kľúč) ktoré by mali byť súčasťou certifikátu a je podpísaná príslušným súkromným kľúčom.  Formát CSR upravuje viacero štandardov, medzi inými [PKCS#10](http://www.rsa.com/rsalabs/node.asp?id=2132), [PKCS#7 resp. CMC](http://www.rsa.com/rsalabs/node.asp?id=2129). |
| *Cryptographic service provider (CSP)* | Knižnica implementujúca CAPI rozhrania. Táto knižnica môže byť dodávaná inou spoločnosťou ako Microsoft, napr. spoločnosťou ktorá sa zaoberá výrobou HSM alebo čipových kariet. |
| *Federal Information Processing Standards (FIPS)* | Súprava štandardov vyvinutá Spojenými štátmi americkými, záväzná v USA a bežne využívaná aj v iných krajinách. |
| *Hardware Security Module (HSM)* | HSM je špecializovaný hardvér, ktorý slúži na ochranu kryptografických kľúčov a bezpečné vykonávanie kryptografických operácií. |
| *Key storage provider (KSP)* | Knižnica implementujúca CNG rozhrania. Táto knižnica môže byť dodávaná inou spoločnosťou ako Microsoft, napr. spoločnosťou ktorá sa zaoberá výrobou HSM alebo čipových kariet. |
| *Microsoft Crypto API Next Generation (CNG)* | Rozhranie poskytujúce kryptografické operácie na nízkej úrovni vyvinuté spoločnosťou Microsoft dostupné od Windows Vista. |
| *Microsoft Crypto API (CAPI)* | Rozhranie poskytujúce kryptografické operácie na nízkej úrovni vyvinuté spoločnosťou Microsoft. |
| *nCipher Support Software (nCSS)* | Middleware / ovládače, ktoré sprostredkujú služby HSM (nCipher) operačnému systému a aplikáciám. |
| *Pravidlá na výkon certifikačných činností (CPS)* | Dokument ktorý popisuje procesné postupy spojené so správou CA, najmä s vydávaním, rušením platnosti, spravovaním a opätovným vydávaním certifikátov. Tento dokument slúži ako smernica pre správcov CA pri vykonávaní ich povinností. |
| *Registračná autorita (RA)* | CA má vytvorený vzťah s jednou alebo viac RA ktoré sprostredkúvajú najmä komunikáciu medzi CA a koncovým používateľom. RA je zodpovedná najmä za overenie údajov, ktoré vyžaduje CA pri vydávaní a rušení certifikátov, za prijímanie žiadostí o vydanie, obnovu a zrušenie certifikátov a pod. |
| *Remote file system (RFS)* | Špecifické úložisko informácií pre sieťové nShield HSM. Toto úložisko informácií slúži na perzistovanie konfigurácie HSM a ukladanie kryptografických kľúčov v šifrovanej forme. |

# Inštalácia a konfigurácia interného HSM (PCI karta)

## Inštalácia nCSS

|  |  |
| --- | --- |
|  | **POZOR! Verzia nCipher Support Software musí byt adekvátna k dodanému HSM zariadeniu. Pri staršom HSM zariadení musí byt nainštalovaná staršia verzia ovládačov**  **Napríklad pri HSM rade XC.od Entrustu by mal byt nainštalovaný ovládač 12.50.** |

1. Vložiť CD, spustí sa inštalácia „nCipher Support Software“, pokračovať *Next*
2. Potvrdiť licenčnú zmluvu, pokračovať *Yes*  
   
3. Vybrať komponenty podľa obrázka, pokračovať *Next*  
   
4. Pokračovať v inštalácii SNMP agenta *Next*  
   
5. Ukončiť inštaláciu  
   

## Vytvorenie nového Security World a administrator card set, konfigurácia CNG nCipher KSP

|  |  |
| --- | --- |
| **Nevyhnutné právomoci:** | člen lokálnej skupiny *Administrators* |
| **Prerekvizity:** | Server musí spĺňať štandardné podmienky inštalácie a musí byť podporovaný softvérom nCipher Support Tools  Na servery musia byť inštalované prerekvizity (**nCSS**) |

Opis inštalácie:

1. PCI karta musí byť inicializačnom stave[[1]](#footnote-1)



1. Spustiť sprievodcu inicializáciou CNG "*C:\Program Files (x86)\nCipher\nfast\bin\capingwizard64.exe"*
2. Zvoliť *Create a new security world*



1. Ak systém nedetegoval modul, overiť že je v inicializačnom stave a spustiť:

|  |
| --- |
| "c:\Program Files (x86)\nCipher\nfast\bin\nopclearfail.exe" --clear --all |

1. Pokračovať s vopred nastavenými hodnotami, zvoliť parametre administrátorských kariet (napr. 1/3):

|  |  |
| --- | --- |
|  | **POZOR! Nevytvárajte FIPS 140-2 Level 3 compliant security world, pokiaľ neexistuje vo Vašej organizácii explicitná požiadavka. Takto vytvorený Security World výrazne sťažuje prevádzku HSM.** |



1. Povoliť *Remote share target*



1. Zadať administrátorské karty (neodporúča sa používať PIN)

|  |  |
| --- | --- |
|  | **POZOR! Administrátorské karty (a prípadné PIN na ich ochranu) starostlivo uschovajte. Sú nevyhnutné pre prípadnú obnovu HSM v prípade poruchy.** |

1. Prepnúť modul do prevádzkového stavu (prepínač na zadnej časti karty) a spustiť

|  |
| --- |
| **"c:\Program Files (x86)\nCipher\nfast\bin\nopclearfail.exe" --clear --all** |

1. Pokračovať ďalej, zvoliť ochranu privátnych kľúčov pomocou module key:



1. Pokračovať *Next*  
   
2. Ukončiť inštaláciu *Finish*  
   
3. PCI kartu možno vrátiť späť do prevádzkového stavu



## Konfigurácia CAPI (32bit a 64bit) nCipher CSP

|  |  |
| --- | --- |
| **Nevyhnutné právomoci:** | člen lokálnej skupiny *Administrators* |
| **Prerekvizity:** | Server musí spĺňať štandardné podmienky inštalácie.  Na servery musia byť inštalované prerekvizity (**nCSS**).  Na servery je vytvorený Security World, ACS. |

Opis inštalácie:

1. Spustiť sprievodcu inicializáciou 64 bit CSP "*C:\Program Files (x86)\nCipher\nfast\bin\domesticwizard64.exe*"
2. Pokračovať k nahraniu *Security World*, zvoliť existujúcu konfiguráciu



1. Zvoliť ochranu pomocou *module key*



1. Vypnúť *nCipher CSP* ako *default SChannel CSP*



1. Opakovať predošlé kroky pre 32 bit CSP "*C:\Program Files (x86)\nCipher\nfast\bin\domesticwizard.exe*"

# Inštalácia a konfigurácia sieťového HSM

## Inštalácia nCSS na Windows servery

**Zodpovedný:** lokálny a**dministrátor** na serveri

**Umiestnenie:** Windows Server

**Postup:**

1. Vložiť CD, spustí sa inštalácia „*nCipher Support Software*“, pokračovať *Next*
2. Potvrdiť licenčnú zmluvu, pokračovať *Yes*  
   
3. Vybrať komponenty podľa obrázka, pokračovať *Next*  
   
4. Pokračovať v inštalácii SNMP agenta *Next*  
   
5. Ukončiť inštaláciu  
   

## Konfigurácia sieťového subsystému HSM

**Zodpovedný:** **HSM administrator**

**Umiestnenie:** HSM

**Postup:**

1. Priradiť IP adresu na prvé sieťové rozhranie HSM: *System > System configuration > Network config > Set interface #1*
   1. Zadať IP adresu HSM modulu
   2. Zadať sieťovú masku stlačiť *Next*
   3. Select desired link speed „*auto*“ stlačiť *Next*
2. *Finish* *Confirm* reboot, HSM sa reštartuje

## Vytvorenie RFS na Windows servery

**Zodpovedný:** lokálny **Administrator** na serveri

**Umiestnenie:** Windows Server

**Postup:**

1. Spustiť command prompt: Start > Run > cmd.exe
2. Zmeniť adresár na nfast\bin:   
   **cd %NFAST\_HOME%\bin**  
   
3. Zistiť HSM ESN („electronic serial number“) a HSM KNETI hash:   
   *anonkneti.exe <IP adresa HSM modulu>*

**anonkneti.exe 10.10.10.1**

|  |  |
| --- | --- |
|  | **POZOR! Keď nie je nainštalovaná adekvátna verzia ovládačov nebude príkaz fungovať.**  **Môže vypísať hlášku:** „Error from ANonymousKnetHash command: UnknownParameter“. |

1. Vložiť do clipboardu výstup predchádzajúceho príkazu   
   
2. Zadať príkaz na vytvorenie RFS:   
   *rfs-setup.exe –-force <IP adresa HSM modulu> <HSM ESN> <HSM KNETI hash>*

napríklad  
  
**rfs-setup.exe –-force 10.10.10.1 7AAE-4704-119A 0f75b9767f7efc091b4f07f833a6aa028c83eb53**  
  


|  |  |
| --- | --- |
|  | **POZOR! Služba RFS musí byť pre sieťové HSM dostupná, tzn. je potrebné zabezpečiť výnimku na Windows Firewall (by default port 9004 TCP).** |

## Konfigurácia RFS na HSM

**Zodpovedný:** **HSM administrator**

**Umiestnenie:** HSM

**Postup:**

1. Zadať adresu RFS servera do HSM: *System > System configuration > Remote file system*
2. Zadať IP adresu RFS servera, ponechať „*default port 9004*“
3. Systém odpovie: „*Remote file setup completed OK*“
4. *System > System configuration > Config file options > Allow auto push*
   1. Klávesnicovými šípkami vybrať voľbu „*Off*“
5. *System > System configuration > Log config* (1-1-7)
   1. Šípkami zvoliť „*Append*“
   2. Na otázku „*Append Log files to netHSM ... mins*“ zadať „*60*“
   3. Systém odpovie „*Log configuration successful*“
6. *System > System configuration > Date/time setting*
   1. Zadať systémový dátum a čas
   2. Na otázku „Reboot required“ potvrdiť reštart HSM

## Vytvorenie nového „Security World“ a administrator card set na HSM

**Zodpovedný:** **HSM administrator**

**Umiestnenie:** HSM

**Postup:**

1. Vytvoriť Security World: Security World Mgmt > Module initialization > New security world
   1. Zvoliť „Admin cardset quorum“ na 1/3, nastaviť „Specify all quorums“ na „No“
   2. Nastaviť typ kľúča modulu na „*AES*“, na otázku „*Select security world module key type*“ zvoliť „*AES*“
   3. Na otázku „*Do you want your world to run in FIPS 140-2 level 3 compatibility mode (does not improve security)?*“ odpovedať „*No*“
   4. Na otázku „*Do you want to make module 1 a valid target for remote shares*“ odpovedať „*Yes*“
2. Vložiť do modulu potrebný počet kariet

|  |  |
| --- | --- |
|  | **POZOR! Administrátorské karty (a prípadné PIN na ich ochranu) starostlivo uschovajte. Sú nevyhnutné pre prípadnú obnovu HSM v prípade poruchy.** |

## Definovanie klienta na HSM

**Zodpovedný:** **HSM administrator**

**Umiestnenie:** HSM

**Postup:**

1. Zvoliť *System > System configuration > Client config > New client*
   1. Zadať IP adresu servera
   2. Šípkami zvoliť „*Unprivileged*“
   3. Na otázku „*Do you wish to enroll with nToken*?“ zvoliť šípkami „*No*“ a potvrdiť
   4. Potvrdiť port „*9004*“
   5. Porovnať „*Client ESN*“ a „*key hash*“ (alfanumerické reťazce zobrazené na obrazovke HSM) s nToken ESN a nToken KNETI hash, ktoré prislúchajú pridávanému klientovi (KNETI hash a nToken ESN možno zistiť pomocou utility *anonkneti.exe* na príslušnom klientovi pričom ako parameter je potrebné uviesť jeho IP adresu.), ak sú zhodné šípkami vybrať „*Yes*“
2. Systém odpovie „*Client configuration completed OK*“

## Pripojenie servera k HSM

**Zodpovedný:** lokálny **Administrator** na serveri

**Umiestnenie:** server RFS

**Postup:**

1. *Start > Run >* ***cmd.exe***

|  |
| --- |
| **cd % NFAST\_HOME%\bin**  *nethsmenroll.exe --force <IP adresa HSM> <HSM ESN> <HSM KNETI hash>* |

napríklad

|  |
| --- |
| **nethsmenroll.exe --force 10.10.10.1 7AAE-4704-119A 0f75b9767f7efc091b4f07f833a6aa028c83eb53** |

## Konfigurácia CNG nCipher KSP na Windows servery

1. Spustiť sprievodcu inštaláciou nCipher CSP (*Start > All Programs > nCipher > CNG Configuration Wizard*)
2. Pokračovať   
   
3. Vybrať „*Use the existing security world*“   
   
4. Vybrať správny modul   
   
5. Vybrať „*Module protection*“  
   
6. Pokračovať   
   
7. Ukončiť inštaláciu   
   

## Konfigurácia CAPI (32bit a 64bit) nCipher CSP na servery

|  |  |
| --- | --- |
| **Nevyhnutné právomoci:** | člen lokálnej skupiny *Administrators* |
| **Prerekvizity:** | Server musí spĺňať štandardné podmienky inštalácie.  Na servery musia byť inštalované prerekvizity (**nCSS**). |

Opis inštalácie:

1. Spustiť sprievodcu inicalizáciou 64 bit CSP "*C:\Program Files (x86)\nCipher\nfast\bin\domesticwizard64.exe*"
2. Pokračovať k nahraniu Security World, zvoliť existujúcu konfiguráciu



1. Zvoliť ochranu pomocou module key



1. Vypnúť nCipher CSP ako default SChannel



1. Opakovať predošlé kroky pre 32 bit CSP "*C:\Program Files (x86)\nCipher\nfast\bin\domesticwizard.exe*"

# Overenie funkčnosti HSM

Správnosť inštalácie možno overiť nasledovne:

|  |
| --- |
| C:\Program Files (x86)\nCipher\nfast\bin\enquiry.exe |

Overiť hodnotu

* + *mode*

mala by sa rovnať

* + operational

ako ilustruje nasledovný listing:

|  |
| --- |
| Server:  enquiry reply flags none  enquiry reply level Six  serial number C06F-149B-D545  mode operational  version 2.92.1  speed index 440  rec. queue 422..622  level one flags Hardware HasTokens  version string 2.92.1cam17, 2.33.60cam1 built on Jul 17 2007 16:17:38, 2.41.2cam2  checked in 00000000487debd5 Wed Jul 16 14:38:45 2008  level two flags none  max. write size 8192  level three flags KeyStorage  level four flags OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient  module type code 0  product name nFast server  device name  EnquirySix version 4  impath kx groups  feature ctrl flags none  features enabled none  version serial 0  remote server port 9004  Module #1:  enquiry reply flags UnprivOnly  enquiry reply level Six  serial number C06F-149B-D545  mode operational  version 2.33.60  speed index 440  rec. queue 19..152  level one flags Hardware HasTokens  version string 2.33.60cam1 built on Jul 17 2007 16:17:38, 2.41.2cam2  checked in 00000000469cdb9c Tue Jul 17 17:09:16 2007  level two flags none  max. write size 8192  level three flags KeyStorage  level four flags OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard ServerHasCreateClient  module type code 7  product name nC1003P/nC3023P/nC3033P  device name Rt1  EnquirySix version 5  impath kx groups DHPrime1024  feature ctrl flags LongTerm  features enabled StandardKM  version serial 24  connection status OK  connection info esn = C06F-149B-D545; addr = INET/10.10.10.1/9004; ku hash = 12c8b409f56ae6095cca13a07c5665f2e3584428, mech = Any; time-limit = 24h; data-limit = 8MB  max exported modules 6  rec. LongJobs queue 18  SEE machine type PowerPCSXF |

# Generovanie kľúčov a CSR v HSM

|  |  |
| --- | --- |
|  | **POZOR! Pre zabezpečenie úplnosti konfigurácie HSM je v príručke uvedený postup konfigurácie KSP/CNG. Súčasná verzia IAM B2B klientskeho komponentu podporuje výlučne certifikáty generované pomocou nCipher Microsoft CAPI CSP implementácie.**  **Ak sa pri generovaní kľúčov použije KSP (nCipher Security World Key Storage Provider) kľúče ani certifikáty NEBUDÚ použiteľné s IAM B2B klientskym komponentom.** |

Generovanie kľúčov resp. CSR do vysokej miery závisí od samotnej aplikácie najmä od toho či aplikácia očakáva kľúče a certifikáty v úložisku

* Používateľa/servisného účtu (Cert:\CurrentUser\My)

Alebo

* Systémovom úložisku (Cert:\LocalMachine\My)

|  |  |
| --- | --- |
|  | **POZOR! IAM B2B klientsky component očakáva kľúče a certifikáty v úložisku “Cert:\LocalMachine\My”.**  **Zároveň je potrebné zabezpečiť, aby k daným privátnym kľúčom mal prístup aplikačný účet, v kontexte ktorého bude komponent bežať.** |

Na generovanie CSR možno využiť skript GenerateCSR uvedený na konci kapitoly.

Vzorové volanie skriptu pre generovanie CSR v kontexte používateľa resp. aplikačného účtu je nasledovné (pozn. predpokladá sa že skript sa spúšťa v kontexte aplikačného účtu):

|  |
| --- |
| GenerateCSR -FirstName "Pavol" -LastName "MIHALOV" -OutputFile C:\Temp\csr01.txt -Store CurrentUser |

Vzorové volanie skriptu pre generovanie CSR v machine kontexte je nasledovné:

|  |
| --- |
| GenerateCSR -FirstName "Pavol" -LastName "MIHALOV" -OutputFile C:\Temp\csr01.txt -Store LocalMachine |

CSR je potrebné odovzdať pracovníkovi registračnej autority v súlade:

* + so zmluvou s NCZI,
  + platným certifikačným poriadkom NCZI.

|  |  |
| --- | --- |
|  | **UPOZORNENIE!** Okrem CSR je nevyhnutné dodať korešpondujúcu žiadosť o certifikát (dokument), ktorý musí obsahovať všetky náležitosti (meno, priezvisko, rodné číslo zdravotníckeho pracovníka, povolanie zdravotníckeho pracovníka a pod.). |

Inštalácia certifikátu prebieha v závislosti od toho či bola žiadosť o certifikát (CSR) generovaná v kontexte aplikačného účtu (Cert:\CurrentUser\My) alebo v systémovom úložisku (Cert:\LocalMachine\My).

Vzorová inštalácia certifikátu v kontexte používateľa resp. aplikačného účtu je nasledovná (pozn. predpokladá sa, že príkaz sa spúšťa v kontexte aplikačného účtu):

|  |
| --- |
| certreq -accept -user C:\Path-To-Certificate\certificate.crt |

Vzorová inštalácia certifikátu v systémovom/machine kontexte je nasledovná:

|  |
| --- |
| certreq -accept C:\Path-To-Certificate\certificate.crt |

|  |
| --- |
| function GenerateCSR  {  param(  [ValidateSet("CurrentUser","LocalMachine")][Parameter(Position=-1,Mandatory=$true)][string]$Store,  [Parameter(Position=-1,Mandatory=$true)][string]$FirstName,  [Parameter(Position=-1,Mandatory=$true)][string]$LastName,  [Parameter(Position=-1,Mandatory=$true)][string]$OutputFile  )  $machineKeySet="FALSE"  if ($Store.ToLower() -eq "localmachine")  {  $machineKeySet="TRUE"  if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]"Administrator"))  {  throw "When generating a CSR in LocalMachine store the command must be run from elevated prompt"  }  }  $req=@"  [NewRequest]  Subject = "CN=$FirstName $LastName"  FriendlyName = "$FirstName $LastName"  MachineKeySet = $machineKeySet  KeyLength=2048  ; 80 - dig sig  ; 20 - key exchange  KeyUsage = 0xa0  ProviderName = "nCipher Enhanced RSA and AES Cryptographic Provider"  ProviderType = 24  ;AT\_KEYEXCHANGE=1  ;AT\_SIGNATURE=2  KeySpec=1  "@  try  {  Write-Host "Checking R/W access to $OutputFile ..."  Write-Output "" > $OutputFile  Write-Host "Creating temp INI file ..."  $tempIni = [System.IO.Path]::GetTempFileName();  $req | Out-File -FilePath $tempIni -Encoding ascii  Write-Host "Preparing request..."    certreq -f -new "$tempIni" "$OutputFile"  if ($lastexitcode -ne 0)  {  rm -Force $tempIni  throw "Error: certreq exited with errorcode: 0x$($lastexitcode.ToString('X8'))!"  }  Write-Host "Removing temp INI file ..."  rm -Force $tempIni | Out-Null  Write-Host "CSR is stored in $OutputFile"  }catch  {  throw $\_.Exception  }  } |

1. Zdroj obrázku „nShield User Guide“ [↑](#footnote-ref-1)