

# Hardware Security Modules

## Základy administrácie



# Rozsah a program

## Úvod

- Základy šifrovej ochrany
- Správa a ochrana kryptografických kľúčov
- API a frameworky pre šifrovanie / dešifrovanie údajov (pomocou HSM)
- Architektonický prehľad nCipher HSM

## DEMO / Jednoduchý set-up sieťového HSM

- HSM: Konfigurácia/factory reset
- SRV: Inštalácia middleware nCSS
- SRV: Vytvorenie Remote Filesystem (RFS)
- HSM: Vytvorenie Security World / Inicializácia
- SRV: Enrollment HSM
- SRV: Inštalácia / konfigurácia nCipher CSP/KSP
- SRV: generovanie žiadosti o certifikát
- PREPROD: vydanie certifikátu
- SRV: inštalácia certifikátu

# Základy šifrovej ochrany a problém správy a ochrany klíčův



# Načo je dobrá kryptografia I.?

- Dôvernosť
  - Šifrovanie údajov a dokumentov (ochrana pred krádežou údajov/zariadenia, DATA-AT-REST)
  - Šifrovanie sieťovej komunikácie (ochrana pred odpočúvaním, DATA-IN-TRANSIT)
  - Dlhodobá / krátkodobá ochrana
- Príklady citlivých údajov
  - Heslá
  - Osobné údaje
  - Finančné údaje

# Načo je dobrá kryptografia II.?

- Integrita
  - Údaje neboli zmenené
  - Checksum súborov pri sťahovaní
- Autenticita
  - Pôvod informácií je garantovaný, údaje neboli zmenené
  - Checksum súborov pri sťahovaní, overený voči **dôveryhodnému** zdroju
  - Digitálny podpis údajov (sieťové protokoly, autentifikácia)
  - Pôvodnosť dokumentov (DATA-AT-REST + DATA-IN-TRANSIT)
- Nepopierateľnosť
  - Tvorca nedokáže spochybniť autorstvo / vytvorenie podpisu
  - Digitálny podpis údajov (elektronický podpis)

# Načo je dobrá kryptografia III.?

- Autentifikácia
  - Ochrana hesiel (skôr patrí k ochrane citlivých údajov), dobré spomenúť že nie vždy je potrebné údaje aj dešifrovať
  - Bezpečné protokoly na využitie hesla / autentifikáciu pomocou hesla
    - Replay útoky
    - Challenge response protokoly
  - Nahradenie hesiel inými formami autentifikácie
  - Viac-faktorová autentifikácia

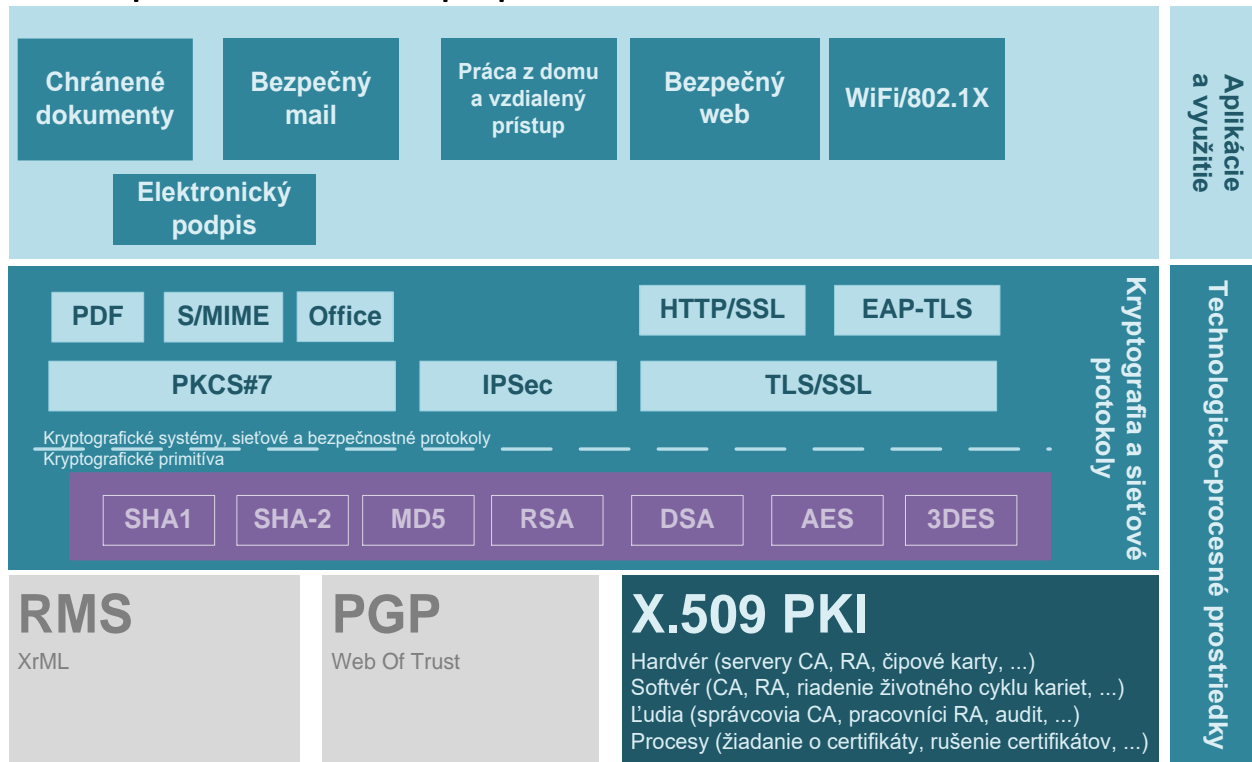
# Možnosti a Use Case šifrovej ochrany

## Využitie šifrovania a X.509 certifikátov

- Silná autentifikácia
- Šifrovanie a ochrana údajov
- Podpisovanie a nepopierateľnosť

## Najčastejšie aplikácie

- SSL/TLS (HTTPS, SMTP, LDAP)
- Kerberos (PKINIT), Smart-card logon (AD, Citrix, etc.), VPN
- S/MIME, Microsoft EFS



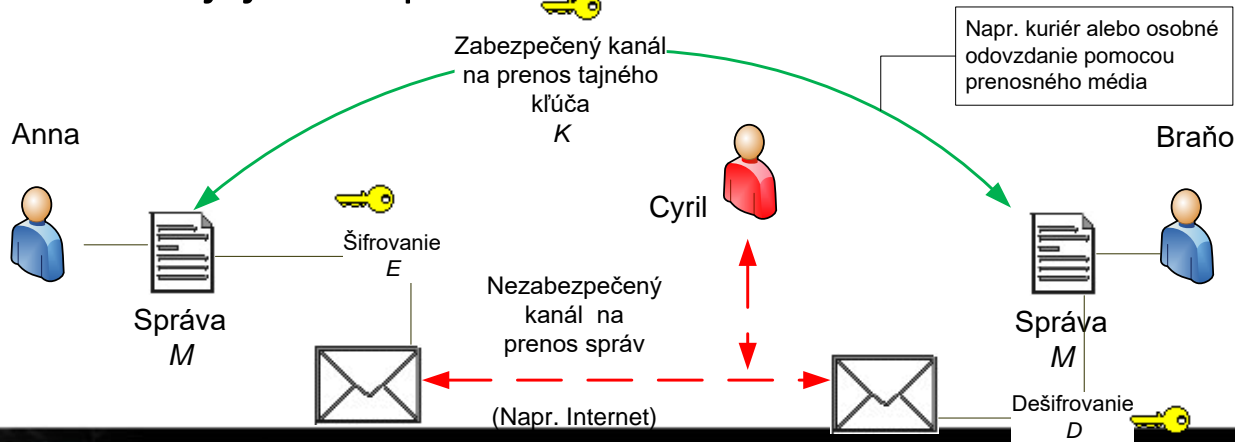
# Symetrické šifrovacie algoritmy

- Na základe rozličného pochopenia kryptografického kľúča možno rozdeliť šifrovacie algoritmy na symetrické a asymetrické
- Symetrické algoritmy využívajú kľúč ktorý je známy len oprávneným subjektom v rámci komunikácii
- Na základe znalosti kľúča sa informácie šifrujú a dešifrujú
- Ak útočník získa šifrovací kľúč ochrana je prelomená
- Kvalita ochrany informácie teda závisí od kvality šifrovacieho algoritmu a ochrany a jednoduchosti distribúcie šifrovacieho kľúča



# Šifrovanie a výmena kľúčov

- Šifrovanie  $C = E_K(M)$
- Dešifrovanie  $M = D_K(C)$
- Princípy výmeny kľúčov určených pre symetrické šifrovacie systémy
  - Kľúč, ktorý budú oprávnení účastníci zdieľať, nesmie byť prenášaný pomocou nezabezpečenej komunikácie, ku ktorej by mohol mať útočník prístup. V žiadnom prípade nesmie byť ohrozená **integrita** a **dôvernosť** prenosu kľúča.
  - Bezpečnosť výmeny kľúčov a ochrana samotnej komunikácie sa **nesmie** spoliehať na utajenie algoritmov a formátu komunikácie, ktoré sa v jej rámci používajú.

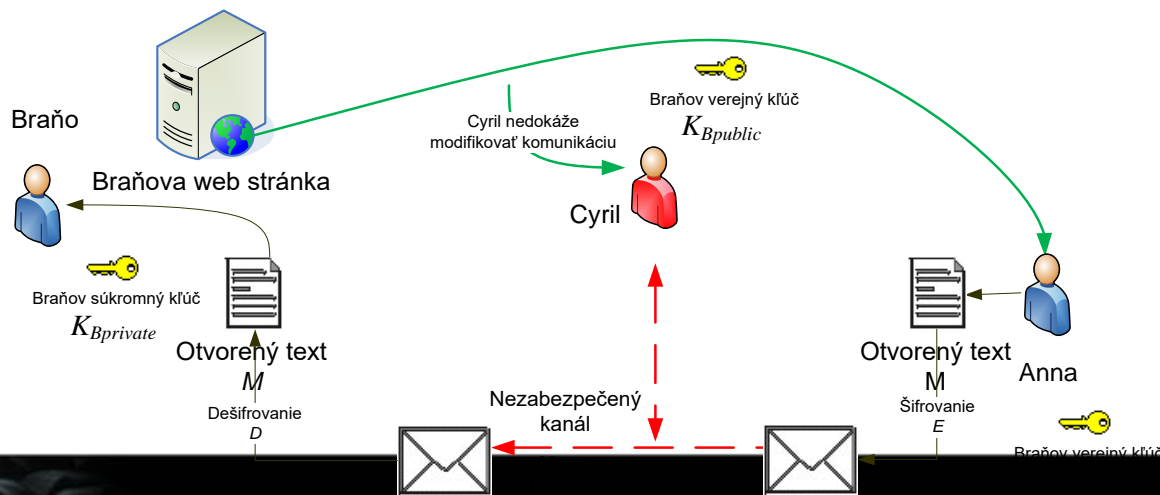


# Asymetrické šifrovacie algoritmy

- Asymetrické algoritmy využívajú dvojicu kľúčov (verejný a súkromný)
  - Verejný kľúč slúži na šifrovanie a je známy všetkým
  - Súkromný (privátny) kľúč slúži na dešifrovanie a pozná ho len jeho vlastník
- Ak útočník získa súkromný kľúč ochrana je prelomená
- Kvalita ochrany informácie teda závisí od kvality šifrovacieho algoritmu a ochrany súkromného a distribúcie verejného kľúča

# Šifrovanie a výmena kľúčov

- Asymetrické algoritmy zjednodušujú proces distribúcie šifrovacích kľúčov
- Šifrovanie  $C = E_{K_{Bpublic}}(M)$
- Dešifrovanie  $M = D_{K_{Bprivate}}(C)$
- Princípy výmeny kľúčov určených pre asymetrické šifrovacie algoritmy
  - Kľúč, ktorý budú oprávnení účastníci komunikácie zdieľať, môže byť prenášaný pomocou nezabezpečenej komunikácie, ku ktorej má útočník prístup, no **integrita a autenticita prenosu kľúča nesmie byť ohrozená**.
  - Bezpečnosť výmeny kľúčov a ochrana samotnej komunikácie sa **nesmie** spoliehať na utajenie algoritmov a formátu komunikácie, ktoré sa v jej rámci používajú.



# Infraštruktúra verejných kľúčov

## Centralizovaná infraštruktúra

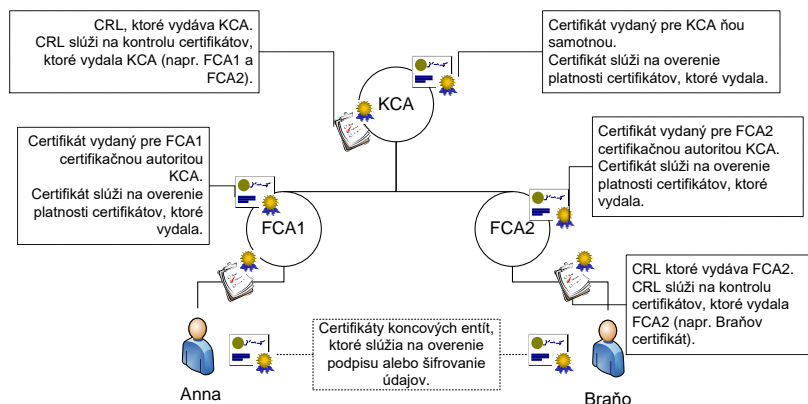
- Centrálna autorita zabezpečuje správu verejných kľúčov (pomocou certifikátov, ktoré podpisuje)
- Distribúcia kľúčov veľkého množstva koncových entít sa redukuje na distribúciu kľúčov malého množstva certifikačných autorít
- Dôveryhodnosť prepojenia kľúčov a identity ich držiteľa určuje autorita
- Platnosť certifikátov býva časovo obmedzená
- Platnosť kľúčov sa overuje na základe periodicky publikovaných blacklistov

## Príklady

- X.509, XrML

## Využitie

- Bezpečný mail, TLS/SSL, 802.1X, IPSec, podpisovanie spustiteľného kódu,



## Decentralizovaná infraštruktúra

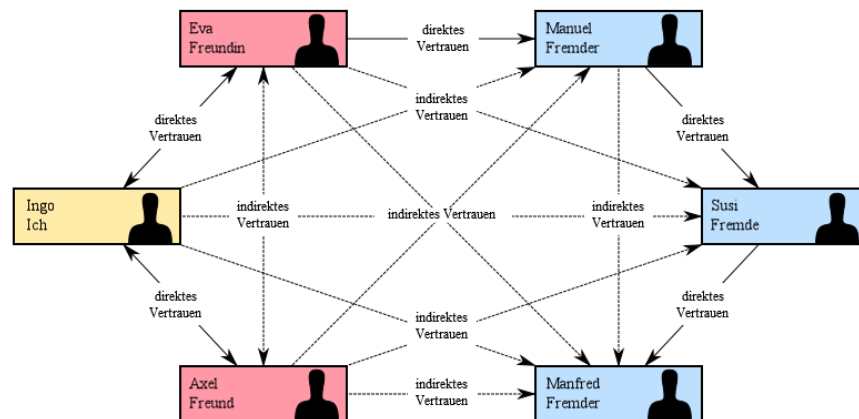
- Správa kľúčov nie je riadená centrálnne, každá entita vydáva svoj vlastný certifikát, ktorý neskôr môže byť podpísaný ďalším účastníkom infraštruktúry
- Distribúcia kľúčov je riadená na základe vzťahov medzi účastníkmi infraštruktúry
- Dôveryhodnosť prepojenia kľúčov a identity ich držiteľa určuje tranzitívny vzťah dôvery
- Platnosť certifikátov nemusí byť časovo obmedzená
- Ďalšia platnosť kľúčov sa prakticky neoveruje

## Príklady

- PGP Web of Trust

## Využitie

- Bezpečný mail, distribúcia softvéru



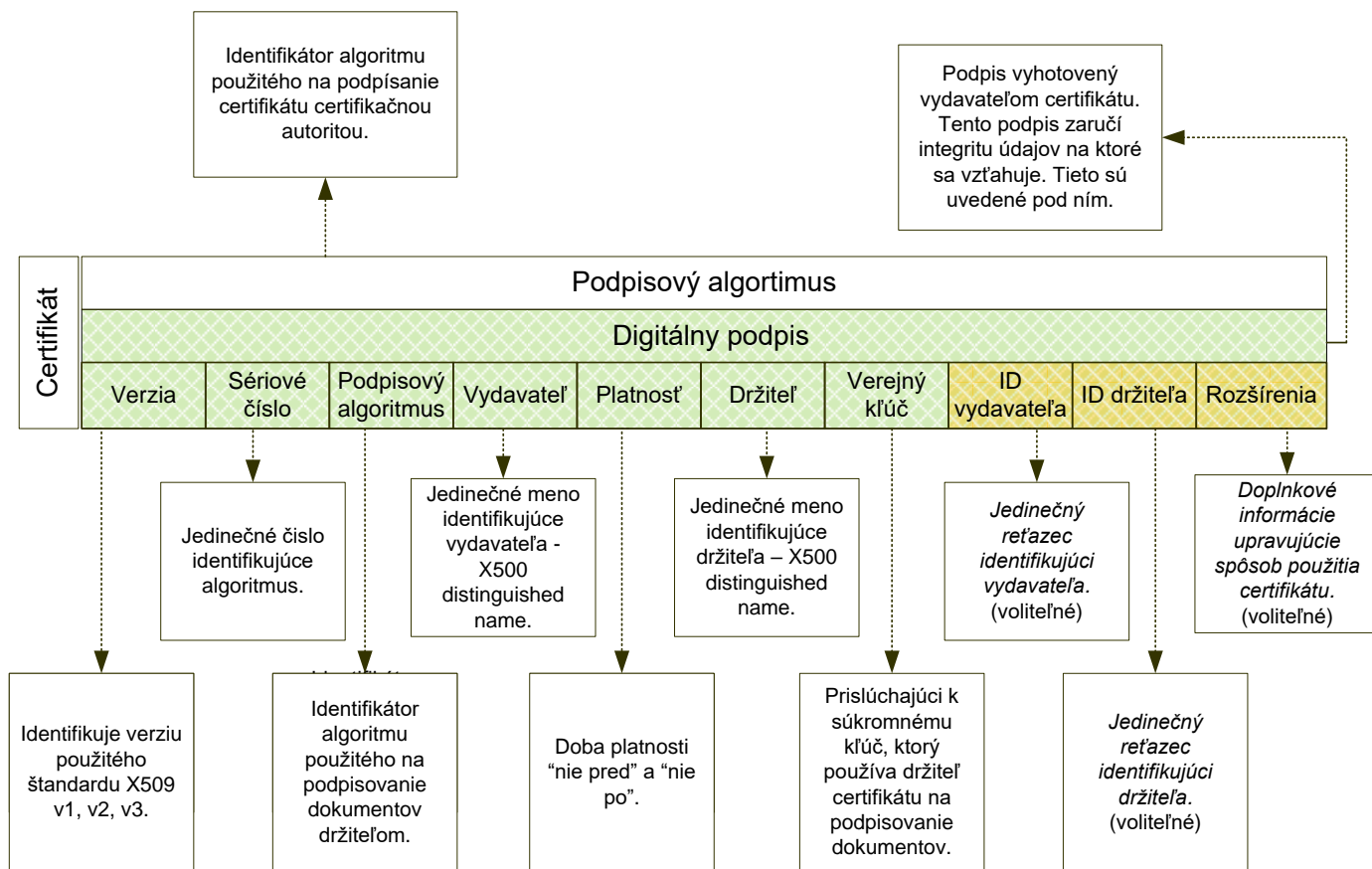
# X509 Certifikát

## Obsahuje najmä informácie o:

- vlastníkovi certifikátu
- **verejnóm kľúči vlastníka certifikátu**
- vydavateľovi certifikátu (certifikačnej autorite)
- dobe platnosti certifikátu
- povolenom spôsobe využitia kryptografických kľúčov

# NEOBSAHUJE

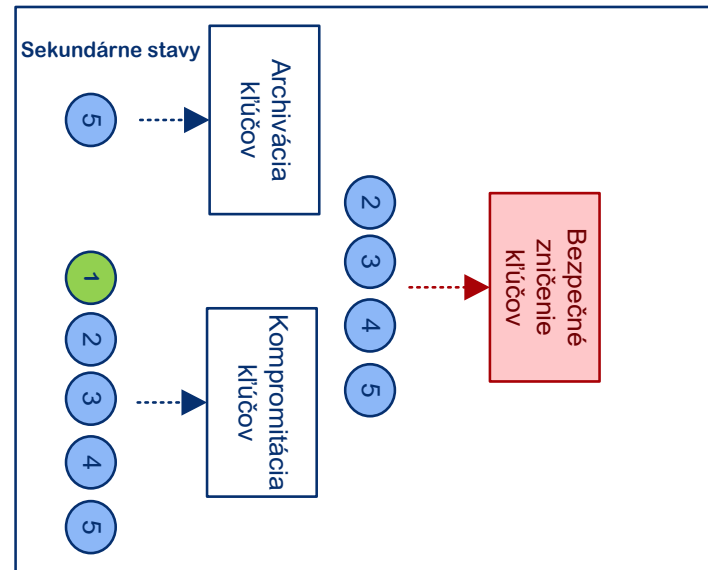
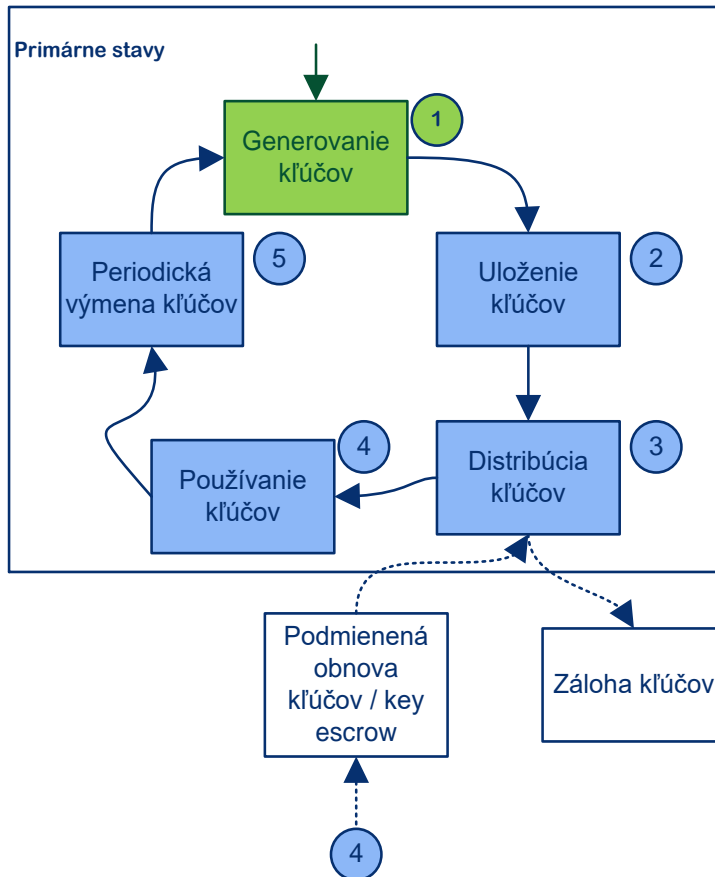
- Informácie o privátnom kľúči



# Správa a ochrana kryptografických klíčů



# Životný cyklus kryptografických kľúčov



- Počty kľúčov, ich typy/použitie a ich citlivosť
- Spôsob distribúcie kľúčov
- Dôležité otázky pre každú fázu/stav životného cyklu :
  - Identifikácia, autentifikácia a autorizácia
  - Spôsob ochrany kľúčov

# Najčastejšie hrozby

- Krádež kľúča
  - Kľúče sú dlhodobo dostupné útočníkovi
  - Útočník môže dešifrovať údaje
  - Útočník môže falšovať údaje
- Strata kľúča
  - Šifrované údaje nie je možné dešifrovať
- Kompromitácia servera / aplikácie ktoré kľúče využíva
  - (Dočasný) prístup k údajom / dešifrovanie
  - (Dočasná) možnosť falšovať údaje



# Možnosti ochrany pred krádežou kryptografických kľúčov I. (súbory)

- Kľúče sú uložené v súboroch a chránené pomocou práv na súborovom systéme
  - Príklad: OpenSSL bez passphrase (PKCS1)
  - Výhody: ľahká dostupnosť kľúčov
  - Nevýhody: Ktokoľvek dokáže čítať key file má prístup ku kľúčom, Nie je možná distribúcia nezabezpečeným kanálom
- Kľúče sú uložené v súboroch chránené pomocou práv na súborovom systéme a hesla
  - Príklad:
    - OpenSSL s passphrase (PKCS8),
    - PFX/PKCS12
    - Java Key Store / JCE Key Store
  - Výhody: ľahká dostupnosť kľúčov
  - Nevýhody: Heslo je ťažké zmeniť/prístup revokovať, ak už raz niekto heslo má

# Možnosti ochrany pred krádežou kryptografických kľúčov II. (Windows Specific Keystores)

- Windows DPAPI/Cryptography stores
  - Ochrana na základe prostriedkov / API operačného systému
  - Operačný systém riadi prístup k ku kľúčov
  - Teoretická možnosť pred exportom kľúčov (non exportable private key), poskytuje však ochranu iba na predošlej úrovni (chráni pred bežnými používateľmi nie pred administrátorom)
  - Administrátor dokáže exportovať napr. pomocou (**NEPODPOROVANÝCH NÁSTROJOV**):
    - mimikatz
    - iSEC Partners Jailbreak

# Možnosti ochrany pred krádežou kryptografických kľúčov III. (špecializovaný hardvér)

- Na kryptografické operácie sa využíva dedikovaný systém (hardvér/softvér/API):
  - čipové karty / smart-cards
  - hardvérové šifrovacie moduly / hardware security modules (HSM)
- Kryptografické kľúče nikdy neopúšťajú tento hardvér v nešifrovanom stave (nie je tým pádom možná ich krádež, bez krádeže hardvéru)
- Dedikovaný hardvér má obmedzený/znížený attack surface

# Rozdiely medzi čipovými kartami a HSM

- Čipové karty
  - Primárny účel: ochrana kľúčov pre používateľov
  - Nízky výkon
  - Portabilita (používateľ môže využiť čipovú kartu pri viacerých zariadeniach/počítačoch)
- HSM
  - Primárny účel: ochrana kľúčov pre servery / služby
  - Vysoký výkon (teoreticky), POZOR: do vysokej miery závisí od implementácie aplikácie a celého stacku (HSM/OS/Middleware/Aplikácia)

# Možnosti ochrany pred stratou kľúčov

- Zálohovanie kľúčov
  - Obyčajne šifrovanie kľúčov, ktoré sa bežne používajú pomocou kľúčov, ktoré sa používajú výnimočne (len pri obnove)
  - Key Recovery Agent
  - Administrátorské karty HSM
- Obnova kľúčov
  - Obyčajne procesne náročnejšia
  - Mala by byť pravidelne testovaná (najmä pre HSM)

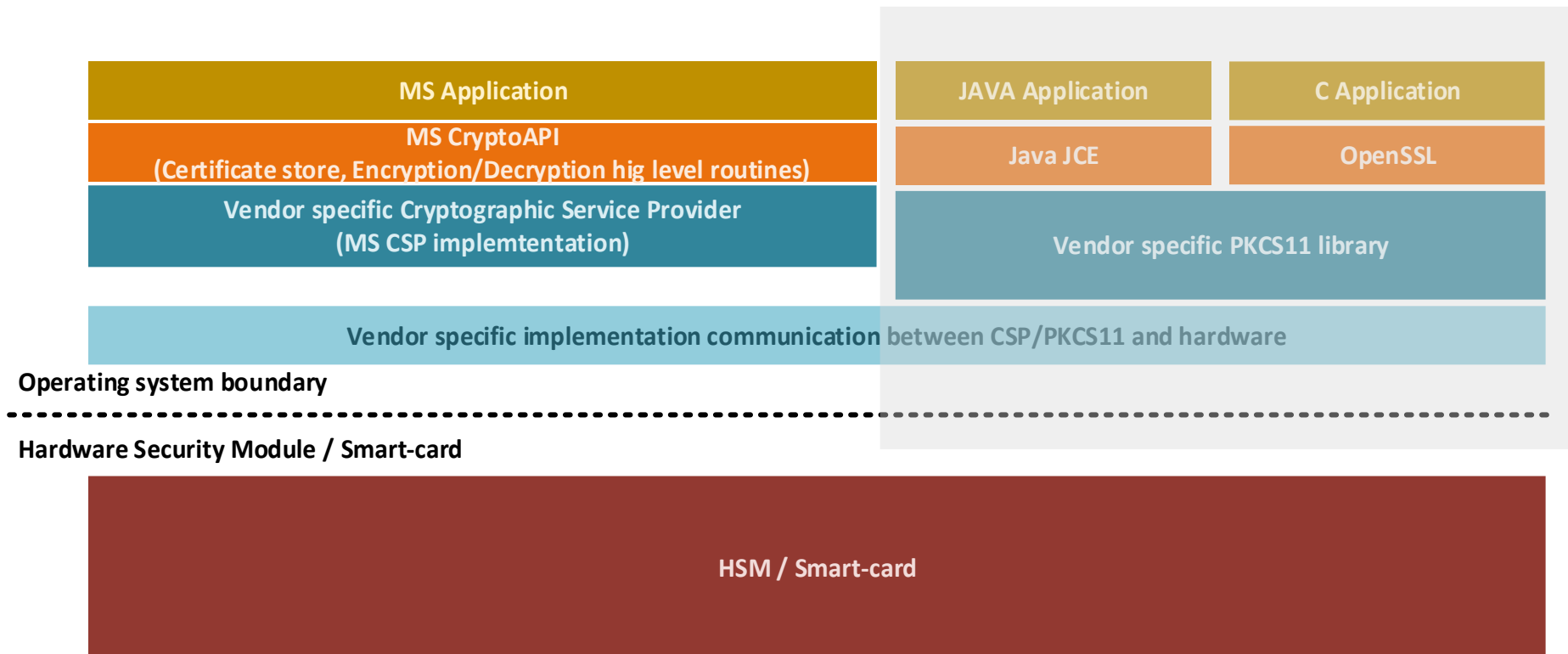
# API a frameworky pre kryptografickú ochranu údajov



# Prehľad

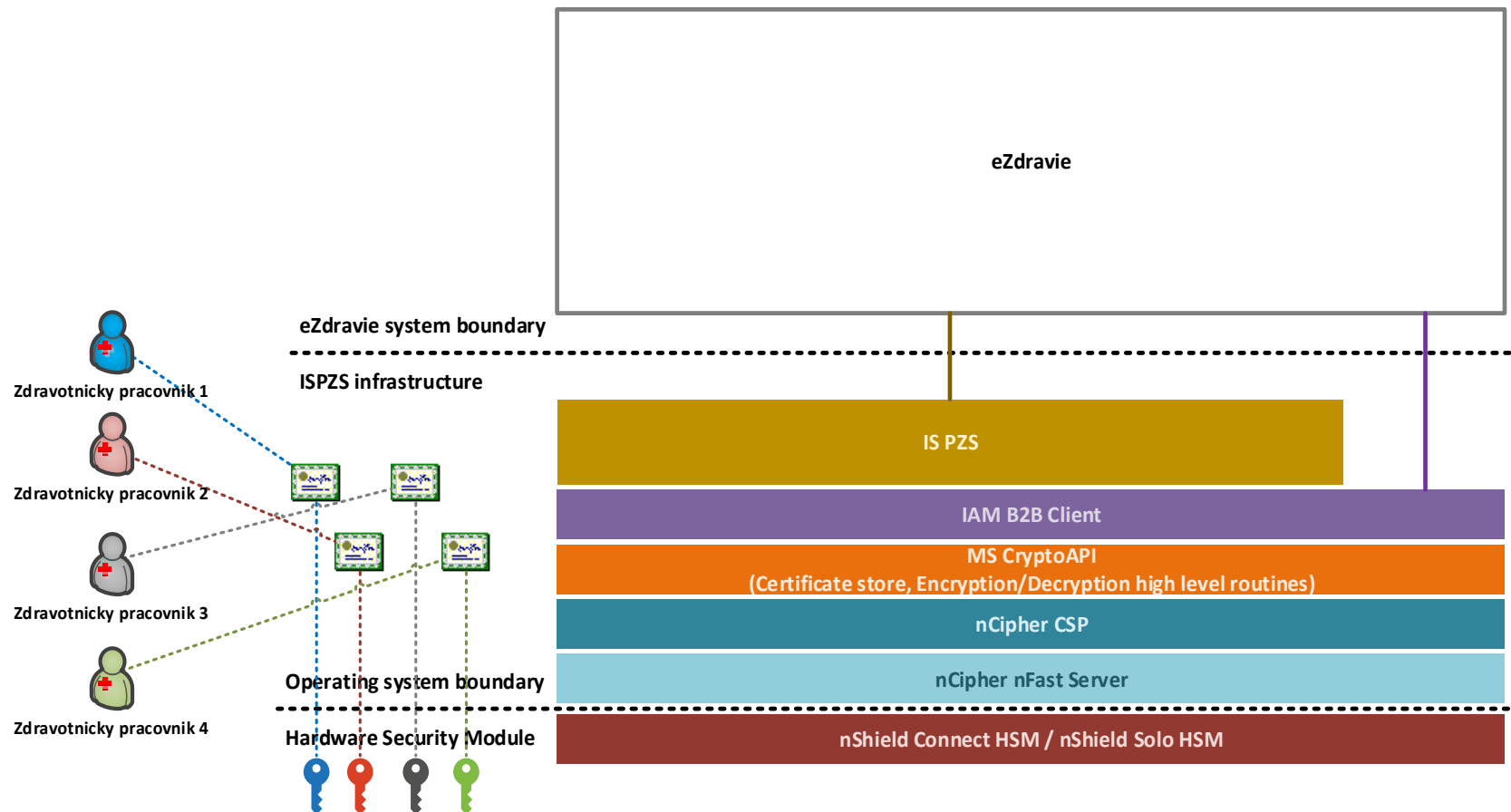
- Aplikračné frameworky a knižnice
  - .NET Cryptography / Windows CryptoAPI
  - .NET Cryptography / CryptoAPI Next Generation (NG)
  - Java Cryptography Extensions (JCE)
  - OpenSSL
- API pre integráciu čipových kariet a HSM
  - CryptoAPI Cryptographic Service Provider (CSP)
  - CryptoAPI NG Key Service Provider (KSP)
  - PKCS11

# Framework stack illustrated





# Logická architektúra v kontexte eZdravia a IAM B2B Client



# Architektonický přehľad nCipher HSM



# Fyzická architektúra (realizácia)

## nShield Solo

- PCIe karta / interný modul
- Prístupný len z jedného servera
- Nie je možné používať vo virtuálnych serveroch



## nShield Connect

- Sieťové appliance / server
- Prístupný z viacerých serverov, je nevyhnutné spárovať klienta a HSM
- Možno využívať služby HSM aj z virtuálnych serverov



# Logická architektúra

## (základný zjednodušený koncept)

- Kryptografické kľúče sú uložené v súboroch na **jednotlivých aplikačných serveroch**, ktoré ich využívajú v **šifrovanom stave** (šifrovaný pomocou kľúča ktorý pozná HSM)
- Ak aplikačný server chce využiť kľúč po prvý raz (za nejakú dobu) “nahrá” kľúč na HSM. HSM kľúč dešifruje (interne) a následne umožní pomocou neho vykonávať operácie dešifrovania / podpisovania
- Koncept takejto ochrany nazýva Thales/nCipher „**Security World**“

# Logická architektúra (Security World)

- Security World predstavuje de-facto bezpečnostnú hranicu
  - Security World vymedzuje kľúč, ktorý využíva HSM na dešifrovanie kľúčov od klientov
- Security World môže byť zdieľaný viacerými HSM
  - v rámci jedného Security World môže byť pripojených viacero HSM
  - Vhodné napr. pri potrebe zdieľať jeden kľúč medzi viacerými servermi (typický príklad pre vysoko-dostupné servery)
- Jedno HSM nemôže byť pripojené do viacerých Security World
- Jeden klient nemôže byť pripojený do viacerých Security World

# Logická architektúra (Admin cardset)

- Security World kľúč možno
  - Vygenerovať pri inicializácii HSM
  - Nahrať na HSM
- Inicializácia HSM / Generovanie Security World
  - Pri úvodnej konfigurácii HSM sa vygeneruje kľúč
  - Tento kľúč sa uloží do HSM a ako záloha sa rozdelí na niekoľko administrátorských kariet (Admin cardset) k/n schéma
  - Karty v rámci Admin cardset možno chrániť pomocou PINu
- Nahratie Security World na HSM
  - Potrebné vtedy ak sa HSM pripája do Security World (napr. kvôli vysokej dostupnosti alebo pri obnove HSM v prípade zlyhania)
  - Pri nahrávaní je nevyhnutné prezentovať **k z n administrátorských kariet** pre daný Security World

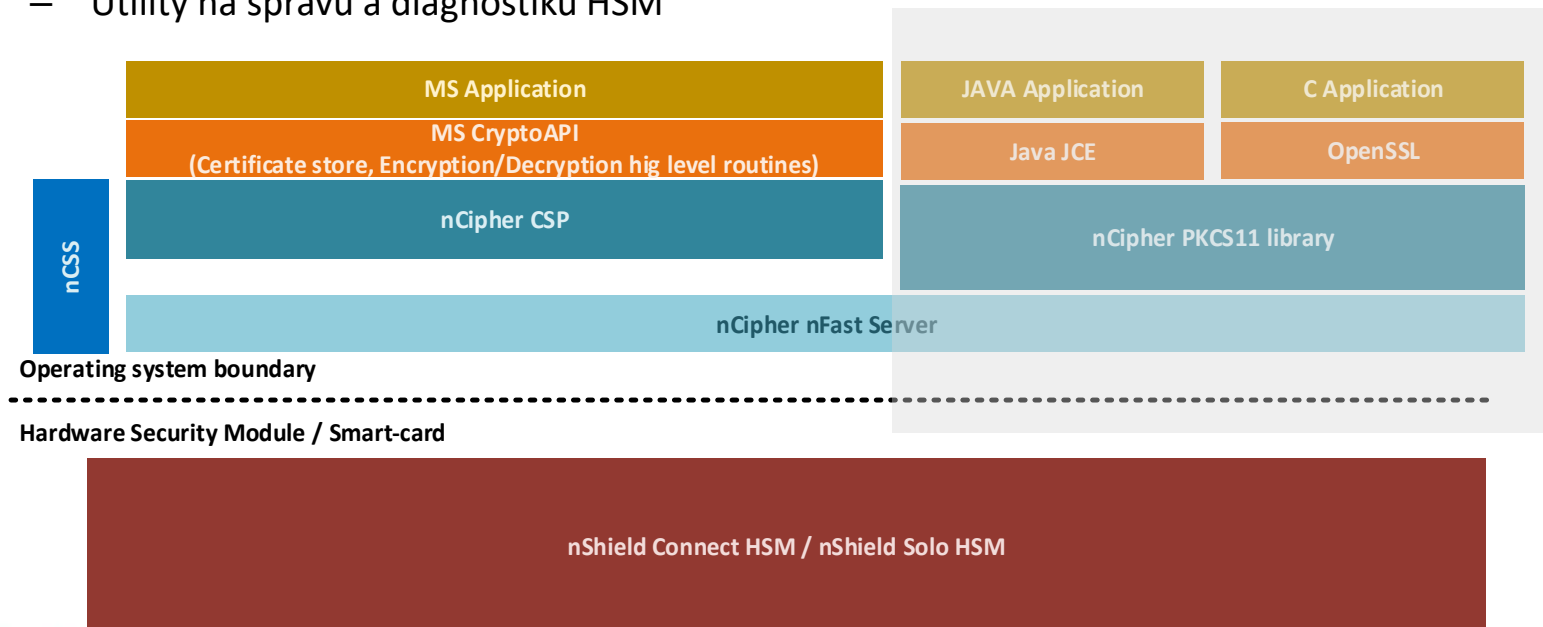
# Admin cardset

## (príklad a odporúčania)

- Príklad admin cardset 3/6
  - Pri inicializácii Security World sa vytvorí 6 administrátorských kariet
  - Pri obnove / nahraní Security World sú potrebné 3 karty
- Odporúčania
  - Admin cardset predstavuje dôležité aktívum
  - Odporúča sa tieto karty uchovať na bezpečné miesto / zdokumentovať kde sa karty nachádzajú
  - Zvážiť použitie PINu (ak sa PIN zabudne nie je možné kartu použiť)
  - Pravidelne testovať obnovu HSM

# Logická architektúra (software stack)

- Middleware nCipher Support Software (nCSS)
  - Knižnice
    - nCipher CSP
    - nCipher KSP
    - PKCS11
  - Monitoring cez SNMP
  - Služba na komunikáciu s HSM (Windows Service / linux daemon)
  - Utility na správu a diagnostiku HSM





# Logická architektúra (Remote File System)

- Súborový systém ktoré využívajú (sieťové) HSM na
  - Uloženie konfigurácie HSM (napr. informácie o klientoch)
  - Uloženie logov HSM
  - Na uloženie zašifrovaného kľúča Security World (možno použiť pri nahrávaní spolu s admin cardset)
  - Uloženie kľúčov v prípade, že sa používa RFS ako prostriedok pre ich zdieľanie medzi jednotlivými aplikačnými servermi
- Jeden HSM môže mať len jeden RFS server
- Jeden RFS server môže slúžiť pre viacero HSM

# Logická architektúra (komunikačné toky)

- V prípade PCIe / nShield Solo nie je nevyhnutné otvárať komunikačné toky (ak sa nepoužíva RFS na synchronizáciu kľúčov)
- V prípade nShield Connect (sieťové HSM) musí viesť:
  - aplikačný server komunikovať s ==> HSM (TCP:9004)
  - HSM komunikovať s RFS serverom (TCP:9004)
  - Každý klient je identifikovaný pomocou IP adresy a KNETI hash (niečo ako autentifikačný pre-shared secret), nie je možné/prinajmenšom sa neodporúča mať medzi klientom a HSM NAT

# Praktická část

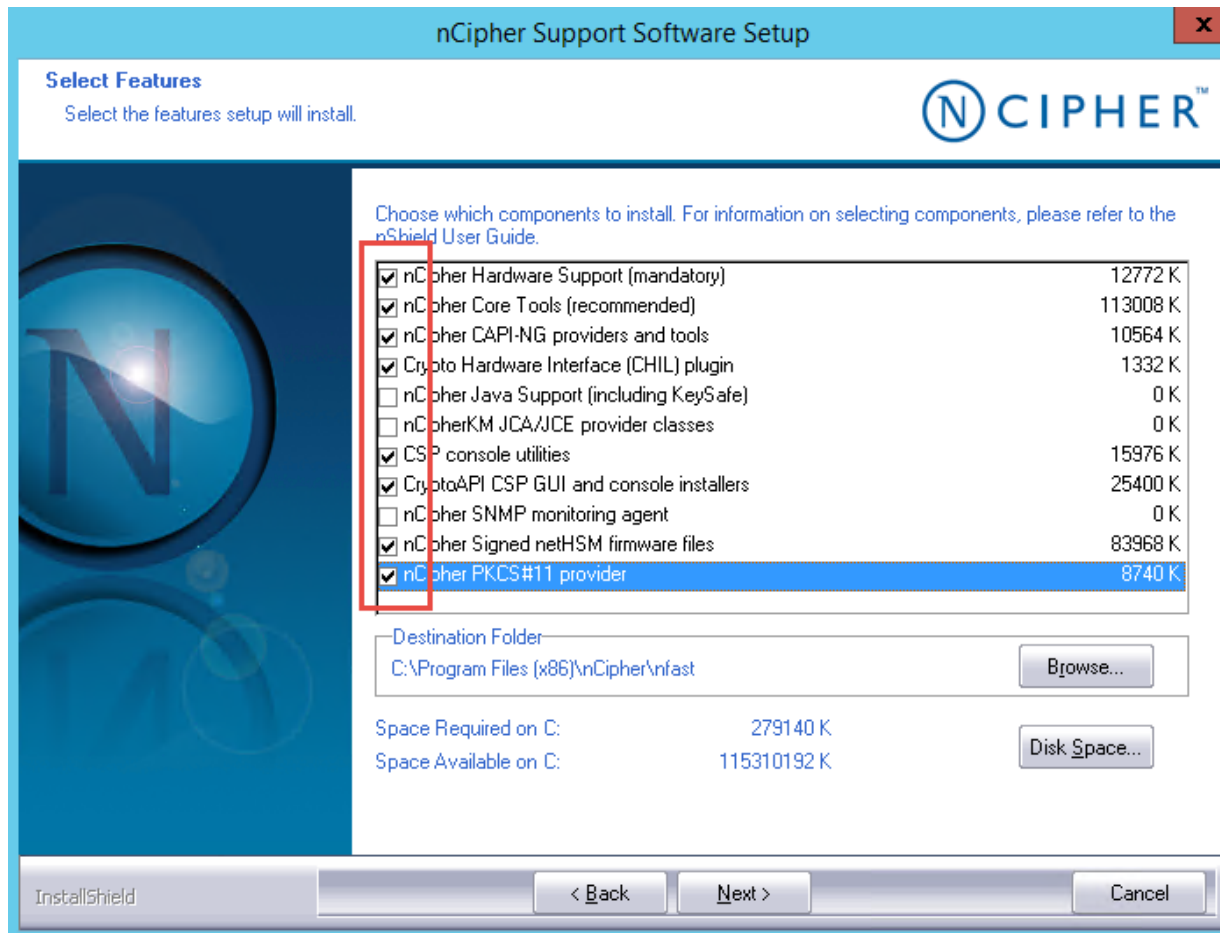


# Prehľad

Inštalácia spočíva z:

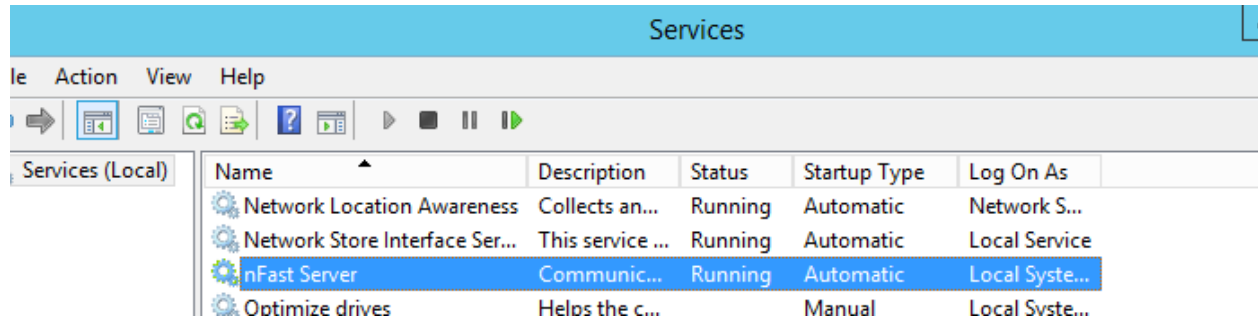
- Úvodnej konfigurácii
  - HSM: Factory reset/Konfigurácia sieťového subsystému/inštalácia licencií
  - SRV: Inštalácia middleware nCSS
  - SRV: Vytvorenie Remote Filesystem (RFS)
  - HSM: Vytvorenie Security World / Inicializácia
- Pripojenia klienta
  - SRV: Inštalácia middleware nCSS
  - HSM: Konfigurácia klienta
  - SRV: Enrollment HSM
  - SRV: Kopírovanie súborov *MODULE\_<ESN> a WORLD* do *C:\ProgramData\nCipher\Key Management Data\local*
  - SRV: Inštalácia / konfigurácia nCipher CSP/KSP

# SRV: Inštalácia middleware nCSS



# nCSS

- C:\Program Files (x86)\nCipher\nfast\bin
  - Programové súbory
- C:\ProgramData\nCipher
  - Šifrované kľúče
  - Prípadne aj RFS
- ENV premenné
  - NFAST\_CERTDIR=C:\ProgramData\nCipher\Feature Certificates
  - NFAST\_HOME=C:\Program Files (x86)\nCipher\nfast
  - NFAST\_KMDATA=C:\ProgramData\nCipher\Key Management Data
  - NFAST\_LOGDIR=C:\ProgramData\nCipher\Log Files
- Service



RFS sa vytvára len jedno pre celú  
infraštruktúru



# SRV: Vytvorenie Remote Filesystem (RFS)

```
cd %NFAST_HOME%\bin  
.\anonkneti.exe HSM-IP  
.\rfs-setup --force HSM-IP HSM_KNETI
```

The screenshot displays the execution of the RFS setup process in an Administrator Windows PowerShell window and the resulting directory structure in File Explorer.

**PowerShell Command Window:**

```
Administrator: Windows PowerShell  
PS C:\Program Files (x86)\nCIPHER\nfast\bin> .\anonkneti.exe 10.201.1.44  
C06F-149B-D545 12c8b409f56ae6095cca13a07c5665f2e3584428  
PS C:\Program Files (x86)\nCIPHER\nfast\bin> .\rfs-setup.exe --force 10.201.1.44 C06F-149B-D545 12c8b409f56ae6095cca13a07c5665f2e3584428  
Removing old remote_file_system entries with remote_esn C06F-149B-D545  
Adding read-only remote_file_system entries  
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\local exists  
Adding new writable remote_file_system entries  
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-C06F-149B-D545 exists  
Ensuring the directory C:\ProgramData\nCipher\Feature Certificates exists  
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-C06F-149B-D545\features exists  
Ensuring the directory C:\ProgramData\nCipher\Key Management Data\hsm-C06F-149B-D545\config exists  
Ensuring the directory C:\ProgramData\nCipher\Log Files\hsm-C06F-149B-D545 exists  
Saving the new config file and configuring the hardserver  
Done  
PS C:\Program Files (x86)\nCIPHER\nfast\bin>
```

**File Explorer:**

The File Explorer window shows the directory structure created by the setup process. The path is: This PC > Local Disk (C:) > ProgramData > nCipher > Key Management Data.

Name	Date modified	Type	Size
config	13.4.2018 16:19	File folder	
features	13.4.2018 16:11	File folder	
hardserver.d	13.4.2018 16:11	File folder	
hsm-C06F-149B-D545	13.4.2018 16:18	File folder	
local	13.4.2018 16:11	File folder	
tmp	13.4.2018 16:11	File folder	



# Povolenie portu 9004 na FW (pre RFS a sieťové HSM)

```
netsh advfirewall firewall add rule  
name="nCipher Impath" dir=in action=allow  
protocol=TCP remoteip="HSM-IP"  
localport=9004
```

# HSM: Nastavenie RFS

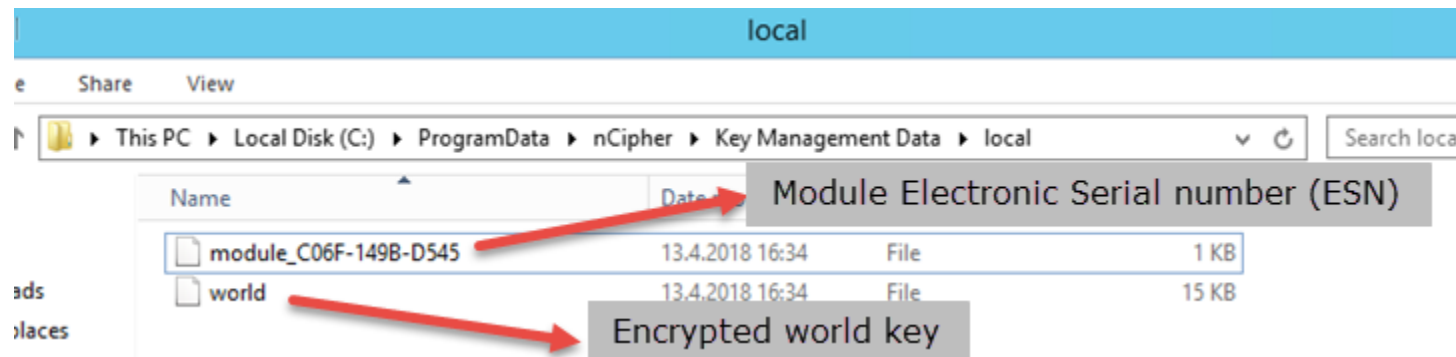
1. Zadať adresu RFS servera do HSM: System | System configuration | Remote file system (1-1-3) [SELECT]
2. Zadať IP adresu RFS servera [TAB], ponechať „default port 9004“ a stlačiť [ENTER]
3. Systém odpovie: „Remote file setup completed OK“ stlačiť [ENTER]
4. System – System configuration | Config file options | Allow auto push (1-1-6-2) [SELECT]
5. Klávesnicovými šípkami vybrať voľbu „Off“ a stlačiť [CONFIRM]

# HSM: Vytvorenie Security World / Inicializácia

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

# Security World

- Po vytvorení / inicializácii pribudnú nové súbory
  - *module\_ESN* (*module\_C06F-149B-D545*)
  - *world*



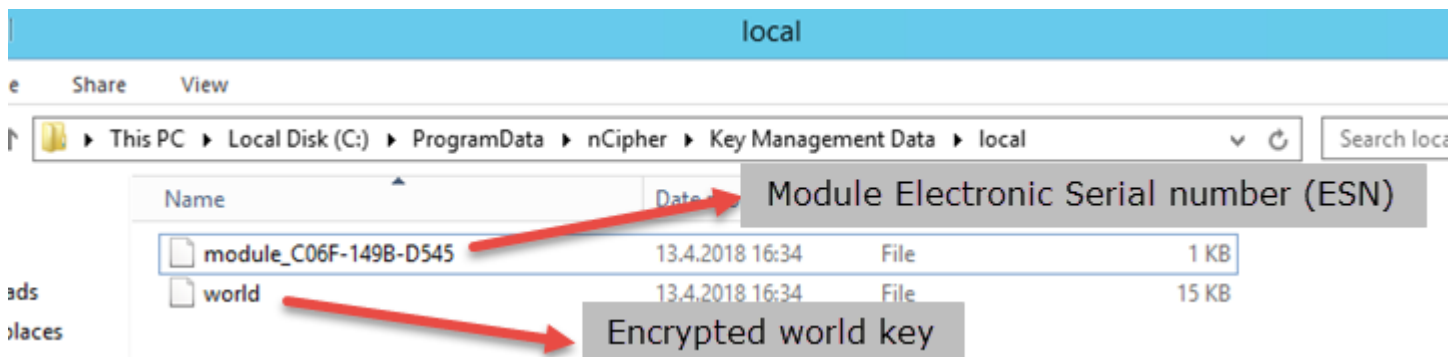
Klientov/aplikačných serverov môže  
byť viacero, nie každý musí (ani  
nemôže) byť RFS server

# HSM: Pridanie konfigurácie pre aplikačný server

1. Zvoliť System | System configuration | Client config | New client (1-1-4-1)
2. Zadať IP adresu servera [NEXT]
3. Šípkami zvoliť „Unprivileged“ [NEXT]
4. Na otázku „Do you wish to enroll with nToken?“ zvoliť šípkami „No“ a potvrdiť [NEXT]
5. Systém odpovie „Client configuration completed OK“ [CONTINUE]

# SRV: Enrollment klienta

- Na serveri sa musia nachádzať súbory z RFS servera (*module\_<ESN>* a *world*)
- Ak je klient zároveň RFS serverom zrejme nie je potrebné nič kopírovať
- **Ak tieto súbory na klientovi nebudú nie je možné vykonať korektne ďalší krok**



```
cd %NFAST_HOME%\bin
```

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

reštartovať službu „nFast Server“

```
C:\Program Files (x86)\nCIPHER\nfast\bin>nethsmenroll.exe --force 10.201.1.44
Remote module returned ESN: C06F-149B-D545
HKNETI: 12c8b409f56ae6095cca13a07c5665f2e3584428
Is the above correct? (yes/no): yes
OK configuring hardserver's nethsm imports

C:\Program Files (x86)\nCIPHER\nfast\bin>exit
PS C:\Program Files (x86)\nCIPHER\nfast\bin> Restart-Service 'nFast Server'
PS C:\Program Files (x86)\nCIPHER\nfast\bin>
```

# SRV: Inštalácia / konfigurácia nCipher CSP/KSP

nCipher



32bit CSP install wizard



64bit



CNG

**nCipher CSP Install Wizard**

**Initial setup**  
Perform initial setup steps required for correct operation of nCipher Windows Support Software.

You already have a security world set up on this server. You can use this security world or create a new security world.

☒ Use the existing security world  
Select this option to keep all your existing security worlds and integrate new nCipher modules into an existing security world.

☐ Create a new security world  
Select this option to create a totally new security world with new private keys, and certificates created with the nCipher software. Any existing security world is backed up. Or you are sure you need a new security world.

☐ Install cryptographic acceleration only  
Select this option if you have an nFast or nFast2 hardware device.

**nCipher CSP Install Wizard**

**Key Protection Setup**  
Set up the private key-protection method and ensure a suitable Operator Card Set exists if necessary.

Select a method to protect private keys generated by the CSPs.

☒ Module protection (requires no extra cards but is less secure)  
☐ Operator Card Set protection  
Always use the wizard when creating or importing keys  
You must create an Operator Card Set before you can continue.

Card set name: mscapi

Number of cards required (K): 2 Total number of cards: 2

☐ Card set has a time-out Card set time-out:

☐ Persistent ☐ Usable remotely

< Back Next >

**nCipher CSP Install Wizard**

**Software Installation**  
Ready to install nCipher support software.

You now have a valid security world. The wizard will now install the CSP.

Select the option below to set the nCipher CSP as the default SChannel CSP, enabling it for the IIS certificate enrollment wizard. Leaving it unselected sets the Microsoft CSP as the default but the nCipher CSP is still available to applications.

☒ Select to set the nCipher CSP as the default SChannel CSP.

< Back Next > Cancel



# SRV: Generovanie žiadosti o certifikát

```
GenerateCSR -FirstName "Karol" -LastName  
"STVRTY" -OutputFile C:\Temp\csr01.txt -  
Store LocalMachine
```

Console1 - [Console Root\Certificates (Local Computer)\Certificate Enrollment Request]

File Action View Favorites Window Help

Console Root

- Certificates (Local Computer)
  - Personal
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Client Authentication Issuers
  - Remote Desktop
  - Certificate Enrollment Requests
    - Certificates
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purpose
Karol STVRTY	Karol STVRTY	13.4.2019	<All>

local

File Home Share View

This PC > Local Disk (C:) > programdata > nCipher > Key Management Data > local

Name	Date modified	Type
key_mscapi_a9446bcedbc23c788242032d6478624227fe0505	13.4.2018 16:56	File
key_mscapi_container-12a3d93fd27ae968a55155d15699b3810051...	13.4.2018 16:56	File
module_C06F-149B-D545	13.4.2018 16:34	File
world	13.4.2018 16:34	File

# SRV: inštalácia certifikátu

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

```
.\cert.txt  
PS C:\Install> certreq -accept .\cert.txt  
PS C:\Install> certutil -store my  
my "Personal"  
===== Certificate 0 =====  
Serial Number: 4f0ba499e86c55b62dff9959  
Issuer: CN=NCZI B2B CA R1-1, O=NCZI, C=SK  
NotBefore: 13.4.2018 16:54  
NotAfter: 12.4.2023 17:04  
Subject: SERIALNUMBER=00020217832, CN=Karol STURTY, OU=00000346874, OU=Zdravotnický pracovník, O=NCZI, C=SK  
Non-root Certificate  
Cert Hash(sha1): 7d 98 26 d6 92 ce 52 4e a5 51 f4 34 68 9d 94 96 1a 72 e1 37  
Key Container = CertReq-4437bbea-1430-4813-99ae-cebb73b8260b  
Provider = nCipher Enhanced RSA and AES Cryptographic Provider  
Private key is NOT exportable  
Encryption test passed  
CertUtil: -store command completed successfully.  
PS C:\Install>
```

# Troubleshooting / utility na kontrolu funkčnosti



# enquiry

C:\Program Files (x86)\nCipher\nfast\bin\enquiry

- Slúži na základnú diagnostiku overenie dostupnosti komponentov
  - nFast Server (služba na komunikáciu s HSM)
  - HSM

```
PS C:\Program Files (x86)\nCipher\nfast\bin> .\enquiry.exe
Server:
enquiry reply flags  none
enquiry reply level  Six
serial number       C06F-149B-0545
mode                operational
version            2.42.5
speed index         440
rec. queue          422..622
level one flags      Hardware HasTokens
version string       2.42.5cam1, 2.33.60cam1 built on Jul 17 2007 16:17:38, 2.41.2cam2
checked in           00000000487235e7 Mon Jul 07 17:27:35 2008
level two flags      none
max. write size      8192
level three flags    KeyStorage
level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNS0PermsCmd ServerHasPollCmds FastPollSlotList HasSEE HasKLF H
asShareACL HasFeatureEnable HasFileOp HasPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard
module type code     0
product name         nFast server
device name          EnquirySix version 4
impath kx groups     none
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-0545
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 HasNS0PermsCmd ServerHasPollCmds FastPollSlotList HasSEE HasKLF H
asShareACL HasFeatureEnable HasFileOp HasPCIPush HasKernelInterface HasLongJobs ServerHasLongJobs AESModuleKeys NTokenCm
ds JobFragmentation LongJobsPreferred Type2Smartcard
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-0545; addr = INET/10.201.1.44/9004; ku hash = 12c8b409f56ae6095cca13a07c5665f2e358
4428, mech = DSA; time-limit = 24h; data-limit = 8mb
max exported modules  6
rec. longjobs queue   18
```

nFast Server

HSM

# nfkminfo

C:\Program Files (x86)\nCipher\nfast\bin\nfkminfo

- Služi na základnú diagnostiku Security World

## Korektný stav

```

Administrator: Windows PowerShell

PS C:\Program Files (x86)\Nciperh\nfast\bin> .\nfkminfo.exe
world
generation 2
state 0x7370000 Initialised Usable Recovery !IPINRecovery !ExistingClient RTC NVRAM
Debug StrictFIPS140
n_modules 1
hknso aba9b5e2a969404c7d8753efde268fe2e4ad885e
hkm 8efbd1a1397d7572ee9f5fa7aa83f75f14c64abe (type Rijndael)
hkmwk 1d572201be33ebc89f30fdd8f3f6ca3395bf0
hkrea 29859080eb0603a72a5a0c7e66396a18e5ac569b
hkra 4cf62542aa92194659ef6c122e5f89ba5f523293
hkrips 23787ca3b2dd9645cc2f3bceeb960493879f3b68
hkmc add025b38875ed3916b362ec278db6b79d20f6b0
hkrtc 1659ae58c6264ab00e3551616a5ffdd194e6082
hkvn 69008d76b96dc2b611f22a75983f9699df19e13
hkdee afc6a3af78ec888d549939d0e7498bc82c8e538
hknull 0100000000000000000000000000000000000000
ex_client none
k-out-of-n 1/1
other quora m=1 r=1 nv=1 rtc=1 dsee=1
createtime 2014-09-17 17:43:33
nso timeout 10 min
ciphersuite DLF1024s160mRijndael
min pp 0 chars

Module #1
generation 2
state 0x2 Usable
Flags 0x10000 ShareTarget
n_slots 2
esn C06F-1498-D545
hkm1 c423b677f4a008106b0c0fbe151903b22dbdf407

```

## Nekorektný stav

- Stav kedy nesedí *world* súbor a súbor *module-ESN*

```
2018-04-16 16:08:48] [IAM\ADMINISTRATOR@iam-hsm-devel-1]  
S C:\Users\Administrator.IAM> cd "C:\Program Files (x86)\nCipher\nfast\bin\"  
2018-04-16 16:28:00] [IAM\ADMINISTRATOR@iam-hsm-devel-1]  
S C:\Program Files (x86)\nCipher\nfast\bin> .\nfkinfno.exe  
6:28:03 WARNING: Module #1: Module file (ESN C06F-149B-D545) is stale, has wrong KML  
world  
generation 2  
state 0x7350000 Initialised !Usable Recovery !PINRecovery !ExistingClient RTC NVRAM !P  
EDebug StrictFIPS140  
n_modules 1  
hkns0 aba9b5e2a969404c7d8753efde268fe2e4ad885e  
hkml 8efbd1a1397d7572ee9f5fa7aa83f75f14c464be (type Rijndael)  
hkmmwk 1d572201be533ebc89f30fdd8f3fac6ca3395bf0  
hkre 29859080eb0603a72a5a0c7e66396a18e5ac569b  
hkra 4cf62542aa92194659ef6c122e5f89ba5f523293  
hkfpips 23787ca3b2dd9645cc2f3bceeb960493879f3b68  
hkmc add025b388755ed3916b362ec728d6b79d20f6b0  
hkrtc 1659ae58c6a264ab00e3551616a5fffd194e6062  
hknsv 69008d76b96dc2b611f22ea75983f9699df19e13  
hkdssee afc6a3af78ec888d549939de07498c62c82ec538  
hknull 0100000000000000000000000000000000000000  
ex.client none  
k-out-of-n 1/1  
other quora m=1 r=1 nv=1 rtc=1 dsee=1  
createtime 2014-09-17 17:43:33  
nso timeout 10 min  
ciphersuite DLF1024s160mRijndael  
min pp 0 chars
```

# certutil -store my

- Slúži na zobrazenie certifikátov a ich kontrolu

```
PS C:\Program Files (x86)\nCipher\nfast\bin> certutil -store my
my "Personal"
===== Certificate 0 =====
Serial Number: 4f0ba499e86c55b62dff9959
Issuer: CN=NCZI B2B CA R1-1, O=NCZI, C=SK
NotBefore: 13.4.2018 16:54
NotAfter: 12.4.2023 17:04
Subject: SERIALNUMBER=00020217832, CN=Karol STURTY, OU=00000346874, OU=Zdravotnický pracovník, O=NCZI, C=SK
Non-root Certificate
Cert Hash(sha1): 7d 98 26 d6 92 ce 52 4e a5 51 f4 34 68 9d 94 96 1a 72 e1 37
Key Container = CertReq-4437bhea-1430-4813-99ae-cebb73b8260b
Provider = nCipher Enhanced RSA and AES Cryptographic Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
PS C:\Program Files (x86)\nCipher\nfast\bin>
```

```
Administrator: Windows PowerShell

PS C:\Program Files (x86)\nCipher\nfast\bin> certutil -store my
my "Personal"
===== Certificate 0 =====
Serial Number: 4f0ba499e86c55b62dff9959
Issuer: CN=NCZI B2B CA R1-1, O=NCZI, C=SK
NotBefore: 13.4.2018 16:54
NotAfter: 12.4.2023 17:04
Subject: SERIALNUMBER=00020217832, CN=Karol STURTY, OU=00000346874, OU=Zdravotnický pracovník, O=NCZI, C=SK
Non-root Certificate
Cert Hash(sha1): 7d 98 26 d6 92 ce 52 4e a5 51 f4 34 68 9d 94 96 1a 72 e1 37
Key Container = CertReq-4437bhea-1430-4813-99ae-cebb73b8260b
Provider = nCipher Enhanced RSA and AES Cryptographic Provider
Encryption test FAILED
CertUtil: -store command completed successfully.
PS C:\Program Files (x86)\nCipher\nfast\bin>
```

# certutil -repairstore I.

- Slúži na opätovnú asociáciu kľúča a certifikátu

The image shows two overlapping windows from a Windows operating system. The top window is an Administrator PowerShell terminal showing the execution of the command `certutil -store my`. The output displays details for a certificate, including its serial number, issuer, validity dates, and subject. A red box highlights an error message: "ERROR: missing key association property: CERT\_KEY\_IDENTIFIER\_PROP\_ID". The bottom window is the Certificate console, showing the 'Personal' store for the local computer. A table lists the certificates, with the first entry highlighted by a red box, matching the details shown in the PowerShell output.

```
Administrator: Windows PowerShell
PS C:\Program Files (x86)\nCipher\nfast\bin> certutil -store my
my "Personal"
===== Certificate 0 =====
Serial Number: 4f0ba499e86c55b62dff9959
Issuer: CN=NCZI B2B CA R1-1, O=NCZI, C=SK
NotBefore: 13.4.2018 16:54
NotAfter: 12.4.2023 17:04
Subject: SERIALNUMBER=00020217832, CN=Karol STURTY, OU=00000346874, OU=Zdravotnický pracovník, O=NCZI, C=SK
Non-root Certificate
Cert Hash(sha1): 7d 98 26 d6 92 ce 52 4e a5 51 f4 34 68 9d 94 96 1a 72 e1 37
No key provider information
Provider: nCipher Enhanced Cryptographic Provider
Simple container name: CertReq-4437bbea-1430-4813-99ae-cebb73b8260b
Unique container name: CertReq-4437bbea-1430-4813-99ae-cebb73b8260b
ERROR: missing key association property: CERT_KEY_IDENTIFIER_PROP_ID
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
PS C:\Program Files (x86)\nCipher\nfast\bin>
```

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificate]

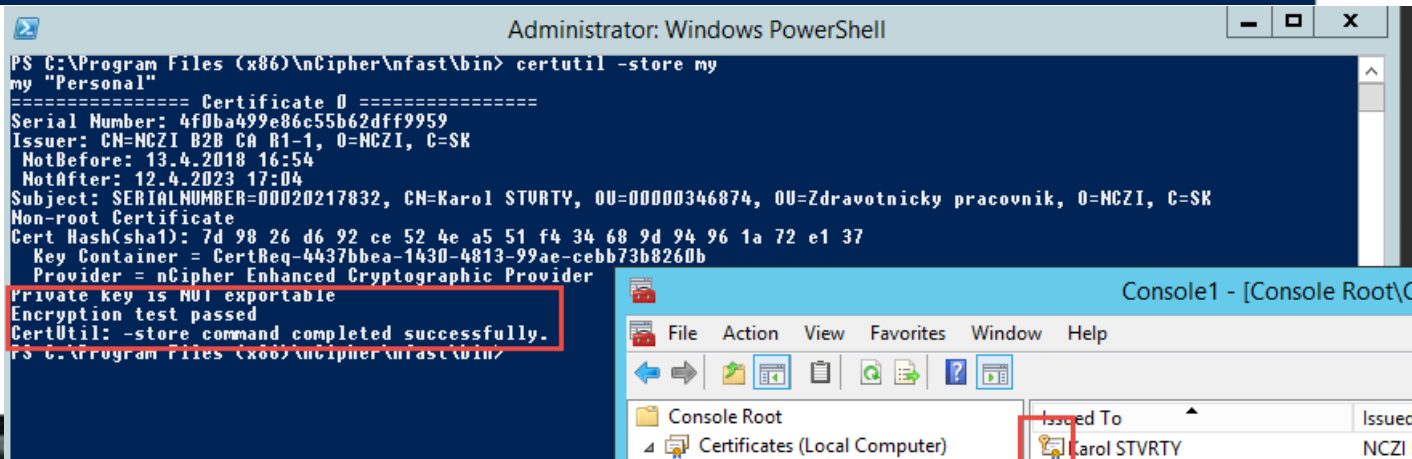
Issued To	Issued By	Expiration Date	Intended Purpose
Karol STURTY	NCZI B2B CA R1-1	12.4.2023	Client Authentication



# certutil -repairstore II.

certutil -f -csp "nCipher Enhanced Cryptographic Provider" -repairstore my 4f0ba499e86c55b62dff9959

```
PS C:\Program Files (x86)\nCipher\nfast\bin> certutil -f -csp "nCipher Enhanced Cryptographic Provider" -repairstore my 4f0ba499e86c55b62dff9959 my "Personal"
===== Certificate 0 =====
Serial Number: 4f0ba499e86c55b62dff9959
Issuer: CN=NCZI B2B CA R1-1, O=NCZI, C=SK
NotBefore: 13.4.2018 16:54
NotAfter: 12.4.2023 17:04
Subject: SERIALNUMBER=00020217832, CN=Karol STVRTY, OU=00000346874, OU=Zdravotnický pracovník, O=NCZI, C=SK
Non-root Certificate
Cert Hash(sha1): 7d 98 26 d6 92 ce 52 4e a5 51 f4 34 68 9d 94 96 1a 72 e1 37
Key Container = CertReq-4437bbea-1430-4813-99ae-cebb73b8260b
Provider = nCipher Enhanced Cryptographic Provider
Private key is NOT exportable
Encryption test passed
Signature test passed
Encryption test FAILED (CMG)
CertUtil: -repairstore command completed successfully.
PS C:\Program Files (x86)\nCipher\nfast\bin>
```



# Záloha / obnova

- Zálohovať na **VŠETKÝCH SERVEROCH**
  - C:\ProgramData\nCipher\Key Management Data\local
- Pre obnovu treba:
  - HSM
  - Súbory z C:\ProgramData\nCipher\Key Management Data\local
  - **Kvórum administrátorských kariet / PIN**