PKI a CA

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Téma 4

PKI/CA

Špecializované IKT systémy Windows

Úvod do problematiky

- PKI
- Autentifikácia
- Autorizácia
- Šifrovanie
- Certifikát
- Kľúč

PKI
Úvod do problematiky

Public Key Infrastructure

Poskytuje „digital trust hierchy" v ktorej autorita (CA) overuje identitu objektov

Primárne sa PKI používa pre užívateľov a zariadenia

- Vydávania CERT
- Udržiavanie CERT (list vydaných certifikátov)
- Revoking CERT
- Bezpečné uloženie kľúčov

Autentifikácia
Úvod do problematiky

Je proces overovania užívateľa alebo zariadenia voči autentifikačnej autorite s cieľom uistiť sa, že sa jedná o oprávnenú osobu alebo zariadenie

Overenie identity

https://www.entersekt.com/solutions/strong-authentication

Autorizácia

Úvod do problematiky

Je proces overovania užívateľa alebo zariadenia voči autentifikačnej autorite so zameraním sa na jeho oprávnenia pre prístup ku zdrojom

https://www.changehealthcare.com/solutions/clearance-authorization

Šifrovanie

Úvod do problematiky

Je proces zabezpečenia senzitívnych dát voči neautorizovanému prístupu tretích strán pomocou matematických operácií a algoritmov

Šifrovaním sa zabezpečuje:

a) Utajenie
b) Autentifikáciu
c) Integritu dát

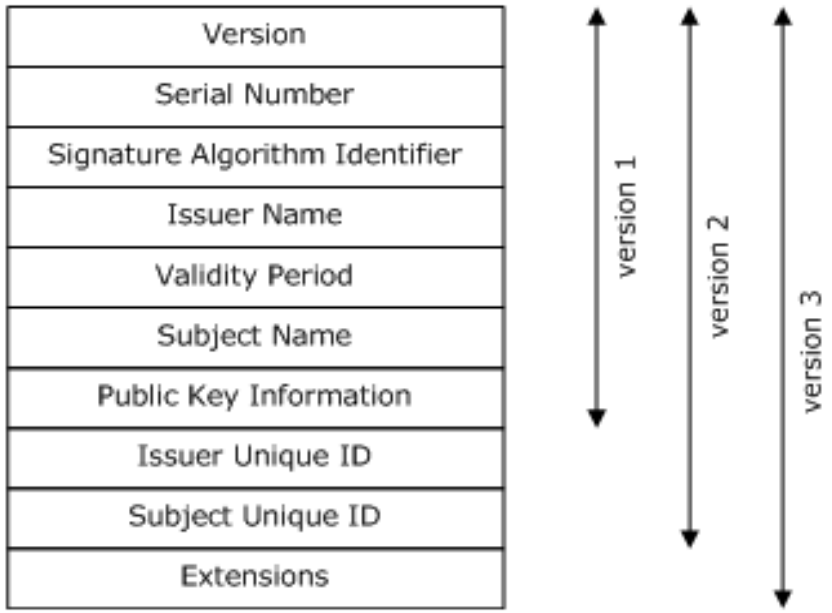
Cieľom je ochrana dát počas ich platnosti pred neoprávnenou entitou

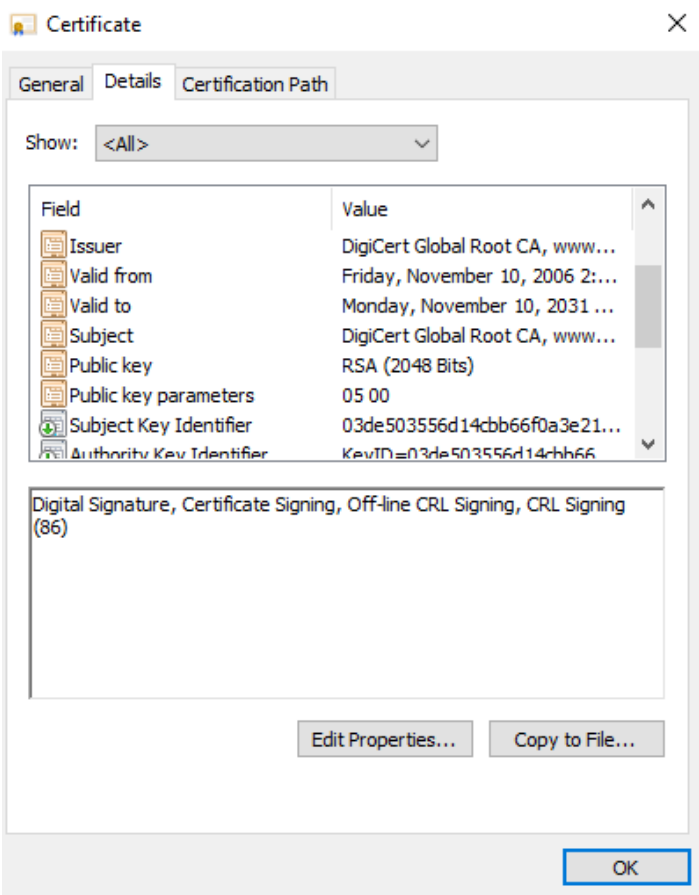
Šifry poznáme symetrické a asymetrické

Blokové šifry 3DES, AES, ...

Certifikát
Úvod do problematiky

- Je špeciálny digitálne podpísaný súbor pre autorizáciu a identifikáciu
- Má definovanú štruktúru (X.509) a obsahuje public key
- Môže byť verzie 1,2,3,4 (classes)
- Obsahuje:





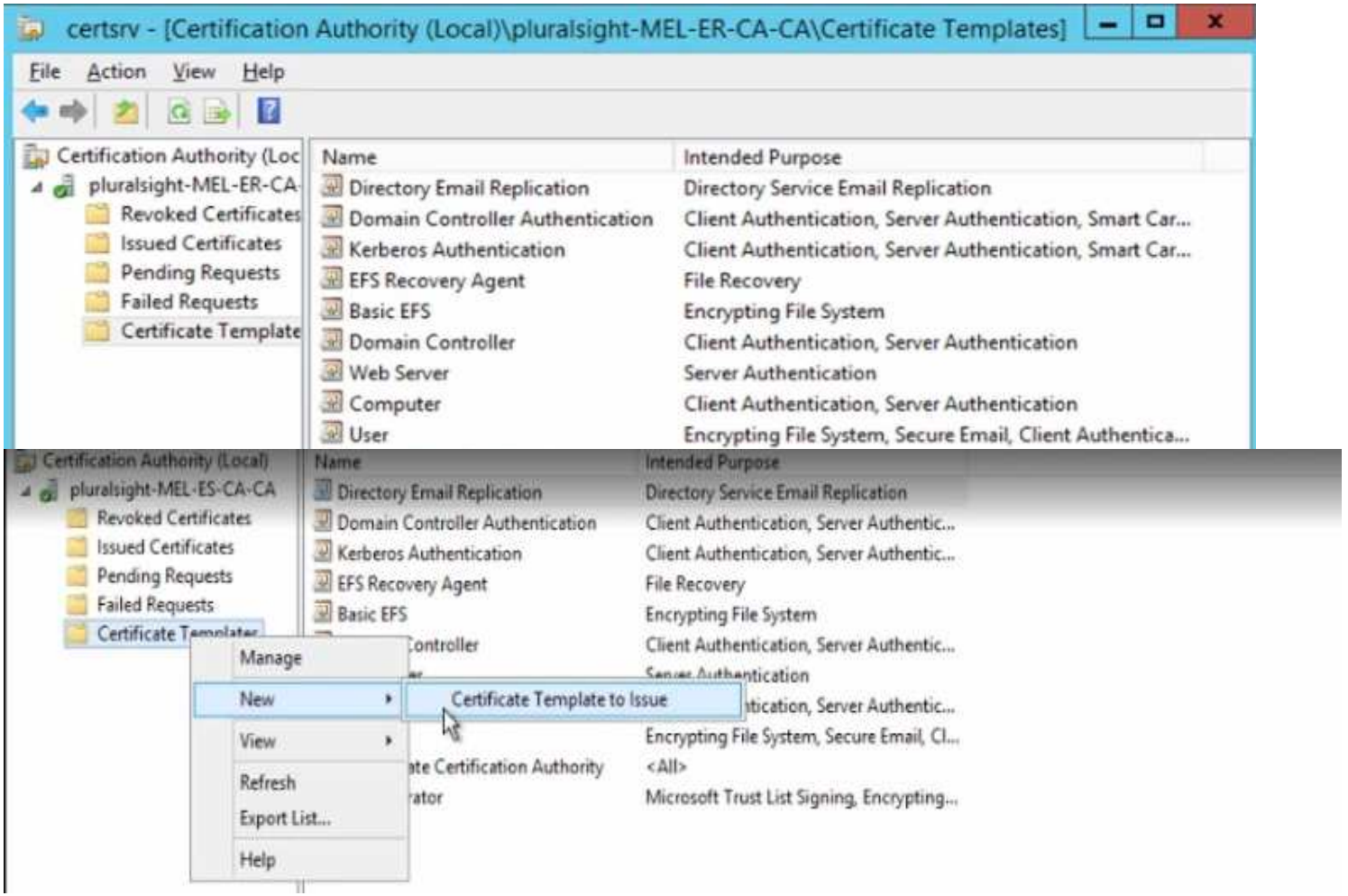
Šablóna certifikátu

Úvod do problematiky

- Definuje účel certifikátu (kryptovanie emailov, kryptovanie pre web sluzbu HTTPS, ...)
- Uložené sú v AD
- Dostupné v rámci celého forest
- Obsahuje niekoľko parametrov
  - Účel
  - Min Key length
  - Algoritmus šifrovania
  - Private key reštrikcie
- Tml je vlasne súhrn parametrov, z ktorých môžu byť vytvorené certifikáty

Šablóna certifikátu

Úvod do problematiky



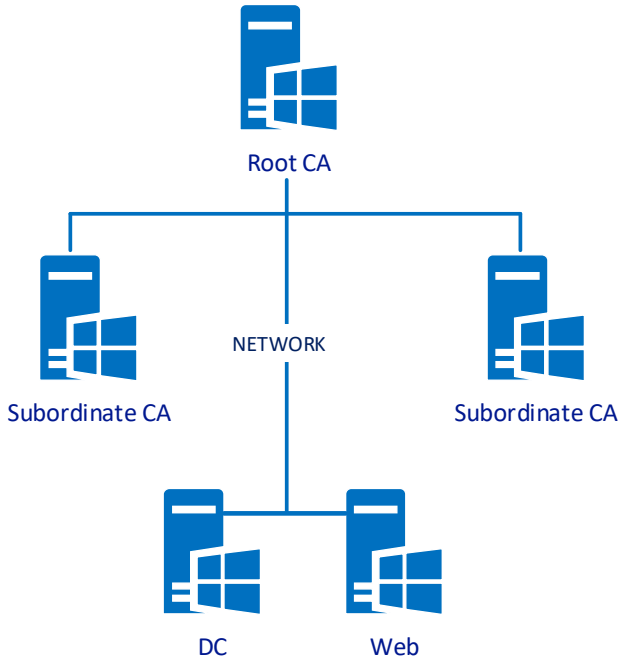
kľúč
Úvod do problematiky

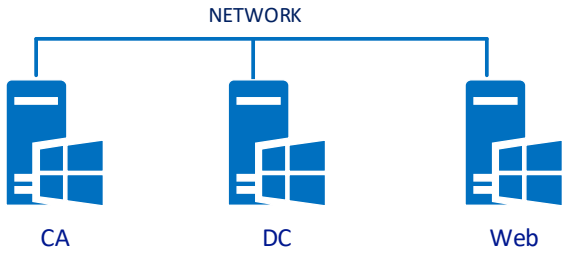
- Kľúč je postupnosť znakov (často krát hexadecimal sústave)
- Slúži na šifrovanie a dešifrovanie
- Jeho dĺžka začína okolo 512 bitov, 1024, 2048, 4096,....bitov
- Dĺžka kľúča je priamo úmerná odolnosti voči brute-force útoku
- V PKI sa používajú privátne a verejné kľúče (tvoriace pár)
  - Data šifrované verejným kľúčom je možné dišifrovať iba príšlušným privatným kľúčom

PKI

Public Key Infrastructure

PKI predstavuje súbor rolí, politík a postupov pre vytváranie, správu a distribúciu digitálnych certifikátov.





Prínos PKI

Public Key Infrastructure

Internetová bezpečnosť je kľúčová služba

Mnohé protokoly umožňujú autentifikáciu a autorizáciu osôb alebo zariadení (overenie a autorizácia je cez dôveryhodný certifikát podpísaný CA)

Použitie certifikátov pri autorizácií alebo autentifikácií je považované za veľmi bezpečné

Certifikáty je možné vydávať pre:

- Užívateľský účet
- Servisný účet
- Počítačový účet

Praktické aplikovanie CERT:

- Web server (https); PowerShell; NAP; Direct Access;

CA

Certification Authority

- Certifikačná autorita pre pre vytvaranie, manazment a distribuciu certifikátov
- Môže byť STANDALONE alebo ENTERPRISE
- Cert enrollment je proces žiadania certifikátu

STANDALONE

- Môže existovať OFFLINE
- Nezávisí od AD DS
- Získať certifikát je možné manuálne alebo cez web
- Schvaľovanie certifikátov je tiež manuálne

ENTERPRISE

- Nemôže existovať OFFLINE
- Závisí a je integrovaná do AD DS
- Môže byť použitý autoenrollment, enrolment on belhalf, web alebo manuálny
- Schvaľovanie certifikátov môže byť automatizované na základe politík

Šifrovanie

Je process ochrany dát pred neoprávneným alebo neautorizovaným použitím

Úlohou šifrovania dát je zabezpečiť integritu a ochranu dát po celú dobu ich platnosti

Moderné šifrovacie algoritmy využívajú tzv šifrovacie kľúče

Kľúč je dlhý náhodne vygenerovaný sled znakov a poznáme:

- Privátny kľúč
- Verejný kľúč

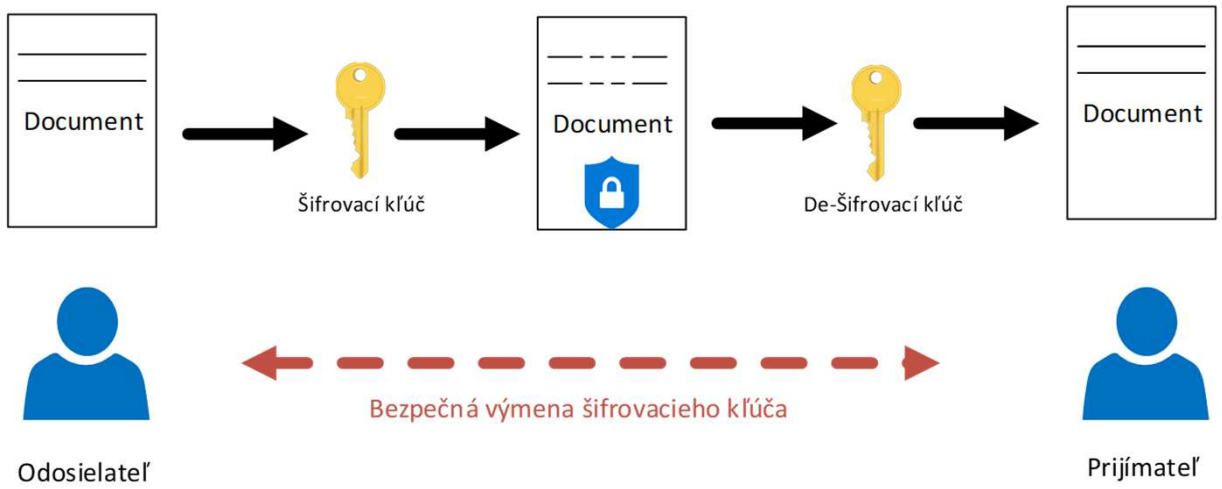
Spôsoby šifrovania

Typy šifier:

A. Symetrické šifrovanie
B. Asymetrické šifrovanie

Symetrické šifrovanie

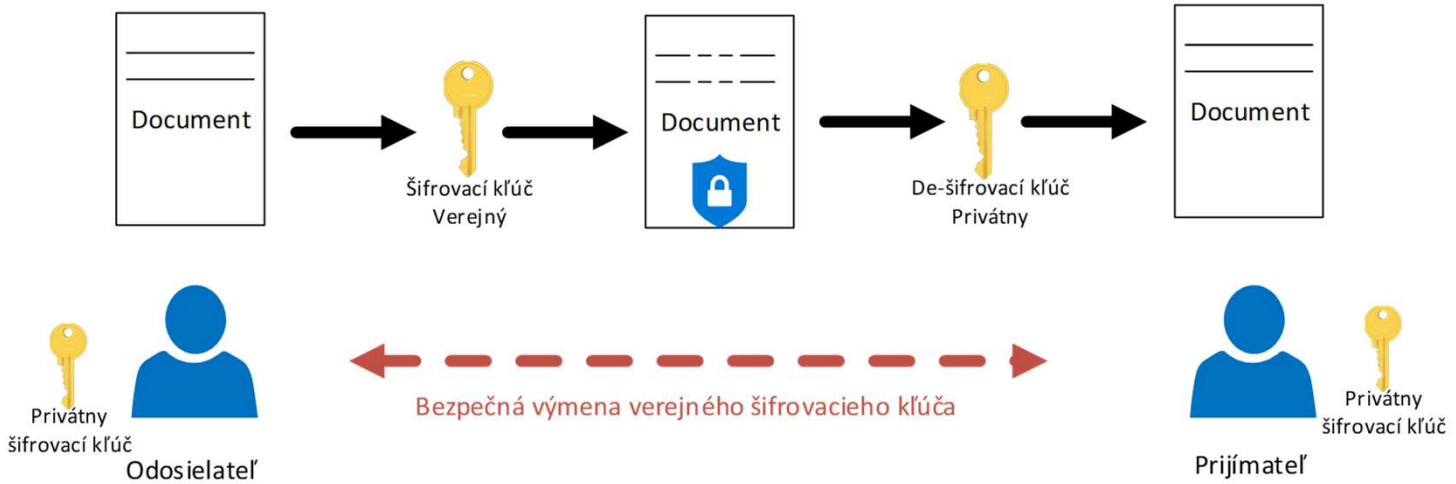
- Rýchle s malý zaťažením zariadení
- Problematická výmena šifrovacích kľúčov
- Kľúče sú 256 bitové
- AES, 3DES, Blowfish, RC4



Spôsoby šifrovania

Asymetrické šifrovanie

- Pomalšie s väčším zaťažením zariadení
- Použité sú verejný a privátny kľúč
- Oba kľúče matematicky súvisia
- Privátny kľúč sa nevymieňa a nie je známi pre tretiu stranu
- Diffie-Hellman, RSA, DSA algorytmus



Overenie integrity dát

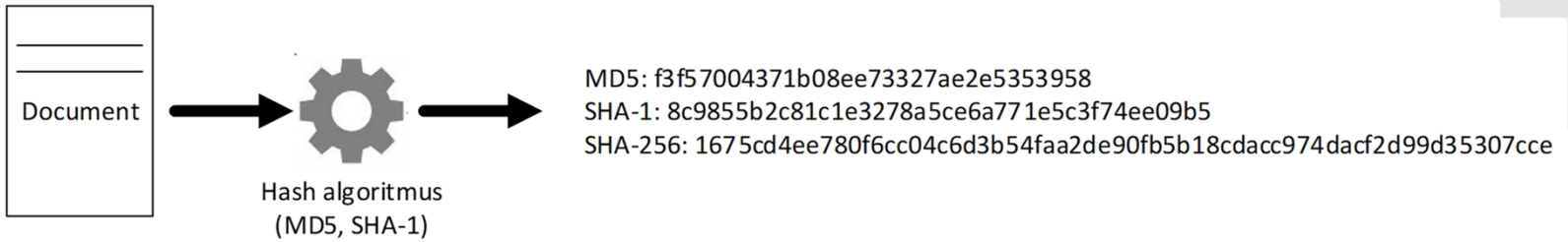
Overenie integrity dát slúži na zabezpečenia, že počas prenosu neboli dáta nijak pozmenené (počas šifrovania, chybou prenosu, treťou stranou a podobne)

Proces spočíva:

1. Pred prenosou je vytvorený otlačok (thumbprint, hash)
2. Po prenose je vytvorený rovnakou metódou nový otlačok
3. Porovnanie oboch

Používanými metódami sú:

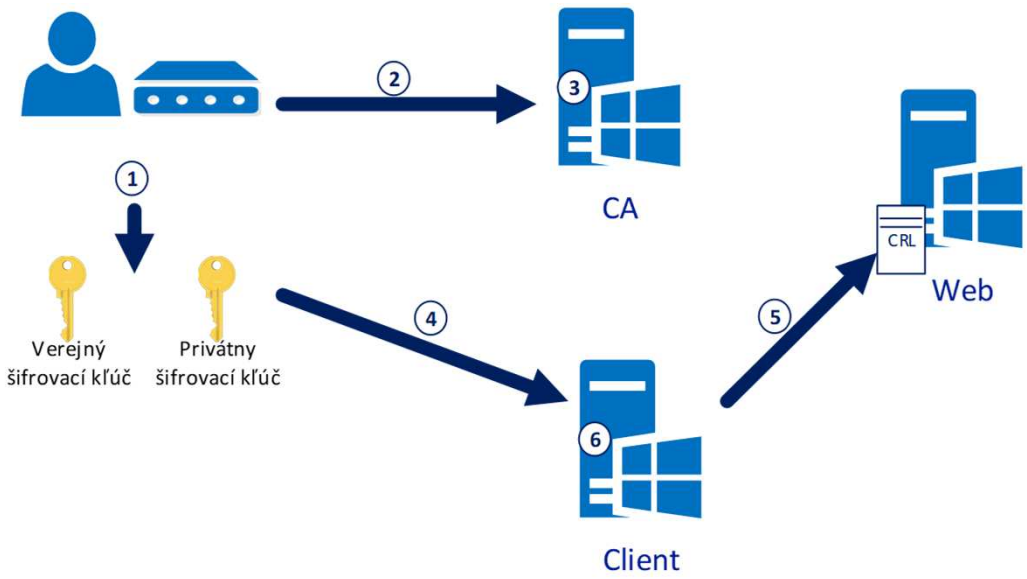
- SHA-256
- SHA-1
- MD5



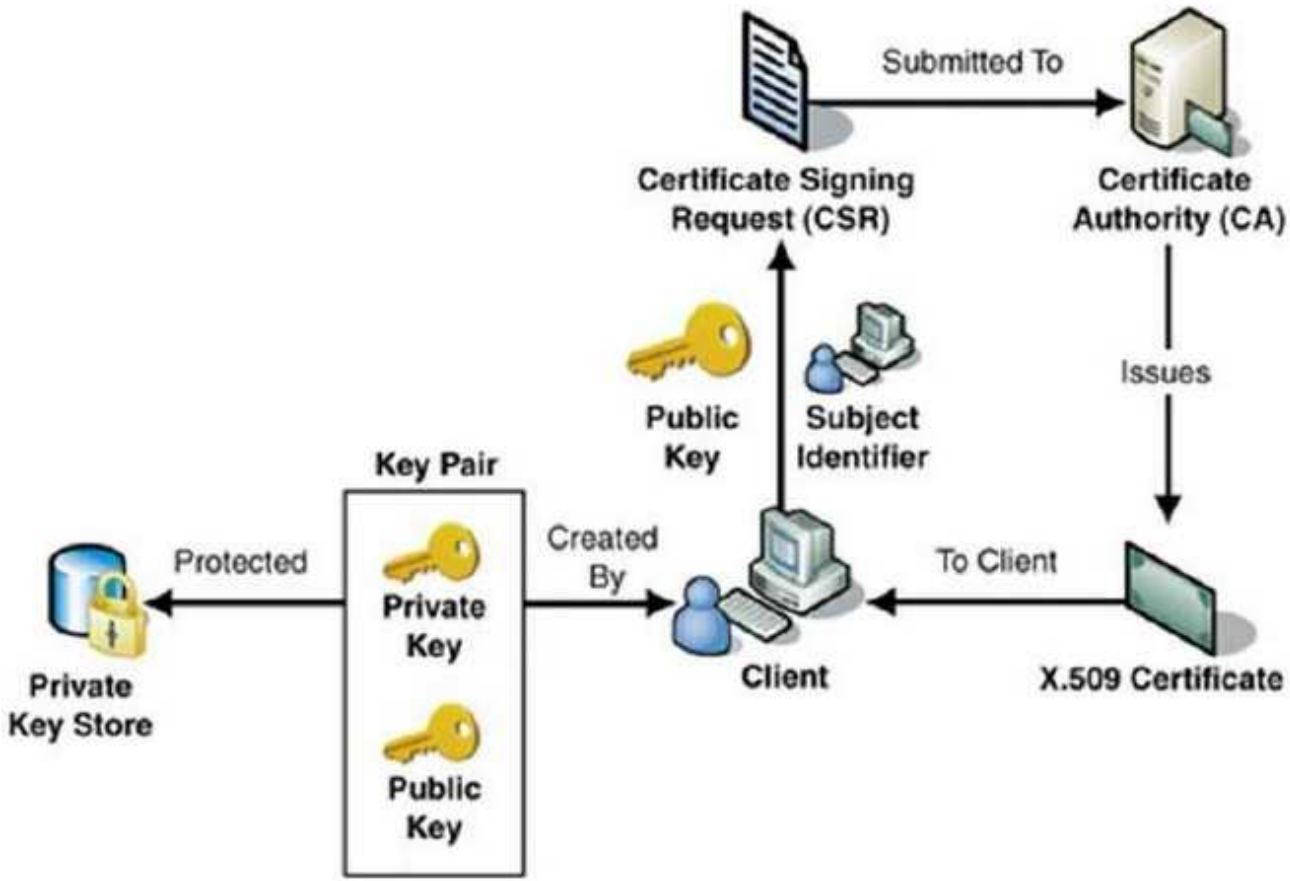
Komponenty

- **CA**
- **CA Web enrollment**
- **Online responder** moze pozriet do CRL, aby overil status certifikatu (platnost, expiraciu) cez http
- **Network device enrollment service** enrollment certifikaty pre router, swtich, ...etc
- **Certificate enrollment service** enrolment certifikatov pre zariadenie pripojene v INTRANET sieti
- **Certificate enrollment policy web service**

Ako to funguje ?



1. Užívateľ alebo zariadenie vygeneruje o vydanie private/public kľúča
2. Užívateľ alebo zariadenie požiada CA o vydanie certifikátu
3. CA vydá certifikát a uloží si ho do svojej databázy (issuing cert process)
4. Užívateľ alebo zariadenie poskytne kľúč na klienta (import cert process)
5. Klient pravidelne overí, čí certifikát sa nenáchadza na CRL
6. Ak sa certifikát nenáchádza na CRL, tak ho akceptuje


Submitted To
Certificate Signing Request (CSR)
Certificate Authority (CA)
Public Key
Subject Identifier
Issues
Key Pair
Protected
Private Key
Created By
To Client
Private Key Store
Private Key
Public Key
Client
X.509 Certificate

OCSP

Online Certificate Status Protocol

- CRL obsahuje SN cert ktoré boli revocate a delta CRL zasa len rozdielove SN cert od posledného publikovania CRL
- Publikovanie CRL robí CA
- Defaultne je publikácia vykonávaná 1 za týždeň a delta CRL 1 za deň
- Pre zistenie satusu musí client stiahnut CRL I delta CRL
- Toto stahovanie generuje nie malý traffic

Výhody

OCSP je check certifikát statusu cez HTTP na OCSP responder a klient tak nemusí sťahovať CRL ale dostane odpoved čí je alebo nie je cert platný (OCSP responder porovnáva CRL listy s daným certifikátom)

OCSP Inštalácia

- ✓Server, ktorý bude hosťovať OCSP nemusí byť členom domény
- ✓idálne je aby nebol na tom istom systéme ako CA)
- ✓ AD DS nainštalovaná v prostredí
- ✓Konfigurácia podporujúca OCSP response

Databáza certifikátov

Po nainštalovaní role CA bude vytvorená databáza

Defaultná cesta je System32\Certlog

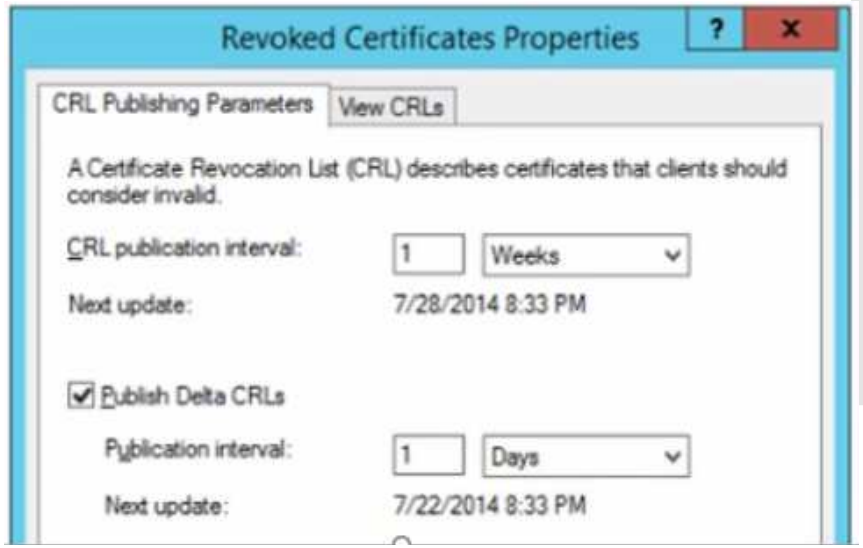
Meno databázy je <CAMeno>.edb

Databáza obsahuje:

- Zoznam vydaných certifikátov
- Archivované privátne kľúče
- Požiadavky o vydanie certifikátov
- Neplatné certifikáty

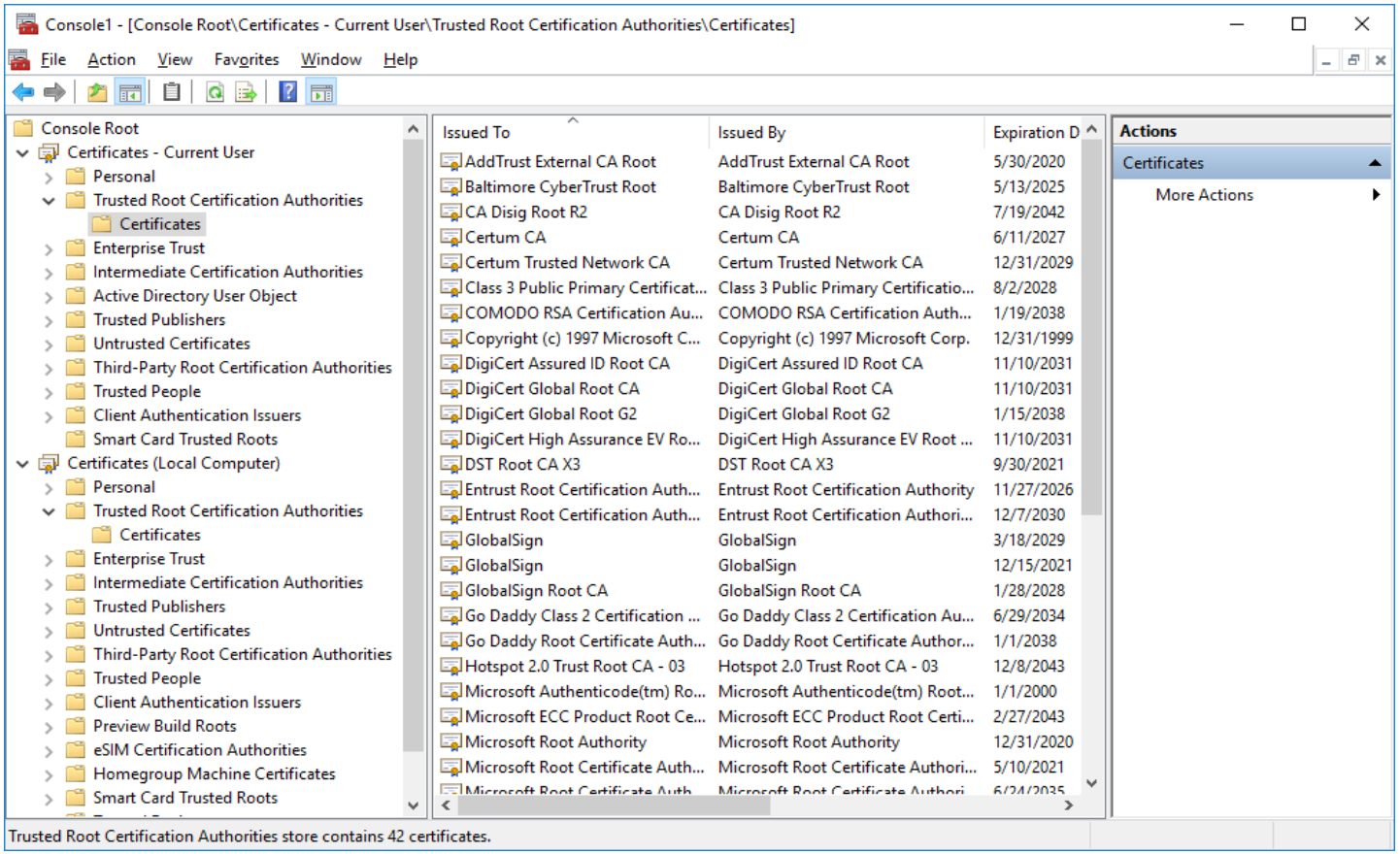
Certificate revocation

- certifikát sa stane neplatným, takéto certifikátu sú uložené v certification server revocation list (CRL),
- ak napríklad dôjde k odcudzeniu privátneho kľúča, je treba použiť revocation
- CRL je regulárne publikovaný by CA
- Klienty skontrolujú CRL, ked je pridelený nový certifikát
- Defaultne je publikovanie nastavene na 1 x za týždeň pre CRL a 1x za deň pre deltaCRL
- CRL môžu byť uložené v AD DS, file share, web site, local storage ale tak, aby boli prístupné pre klientov



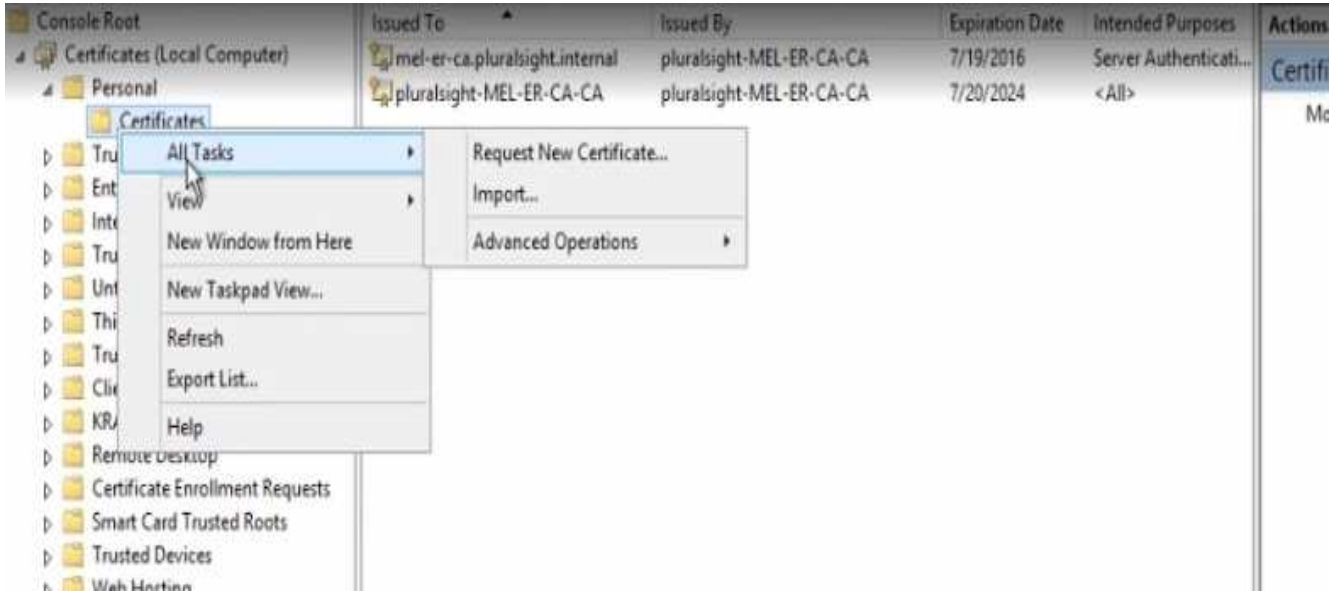
Manažment certifikátov

Cez konzolu mmc Certificates



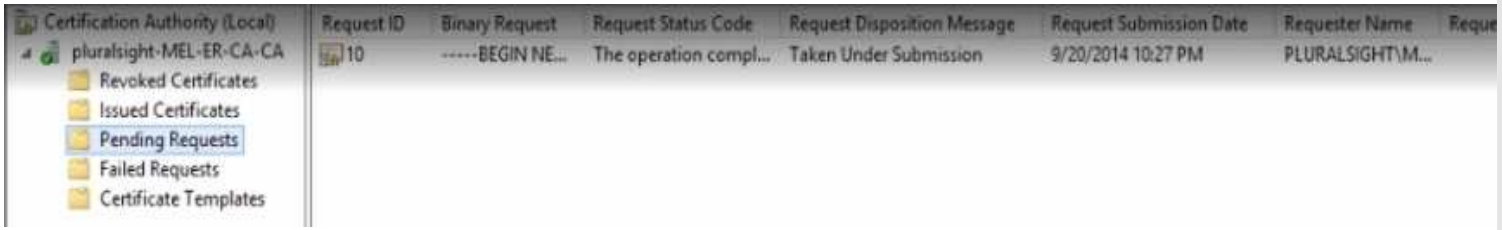
Vyžiadanie certifikátu

Cez konzolu mmc Certificates



Schvaľovanie certifikátu

Cez konzolu mmc Certificates



Je možné nastaviť auto schvaľovanie

- **Configure certificate approval on the template**

Self-signed cert

Takýto certifikát je tzv self identity cert

Certifikát je podpísaný vlastným privátnym kľúčom

Nepotrebuje CA pre jeho vytvorenie

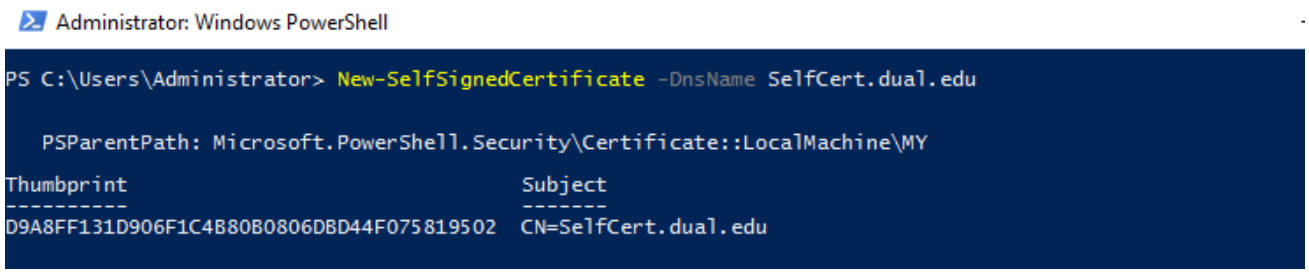
Takýto cert nemôže byť na žiadnom revoke liste

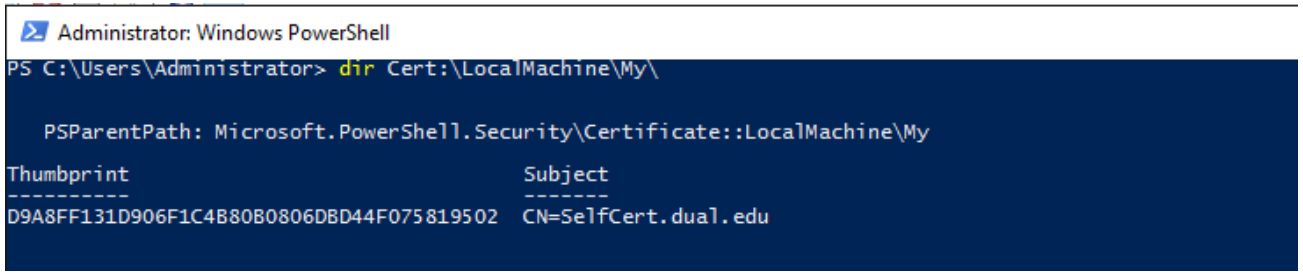
Revocation sa urobí odstránením z trusted certifikát úložiska

Využíva sa pre testovanie, vytváranie konceptu

Self-signed cert

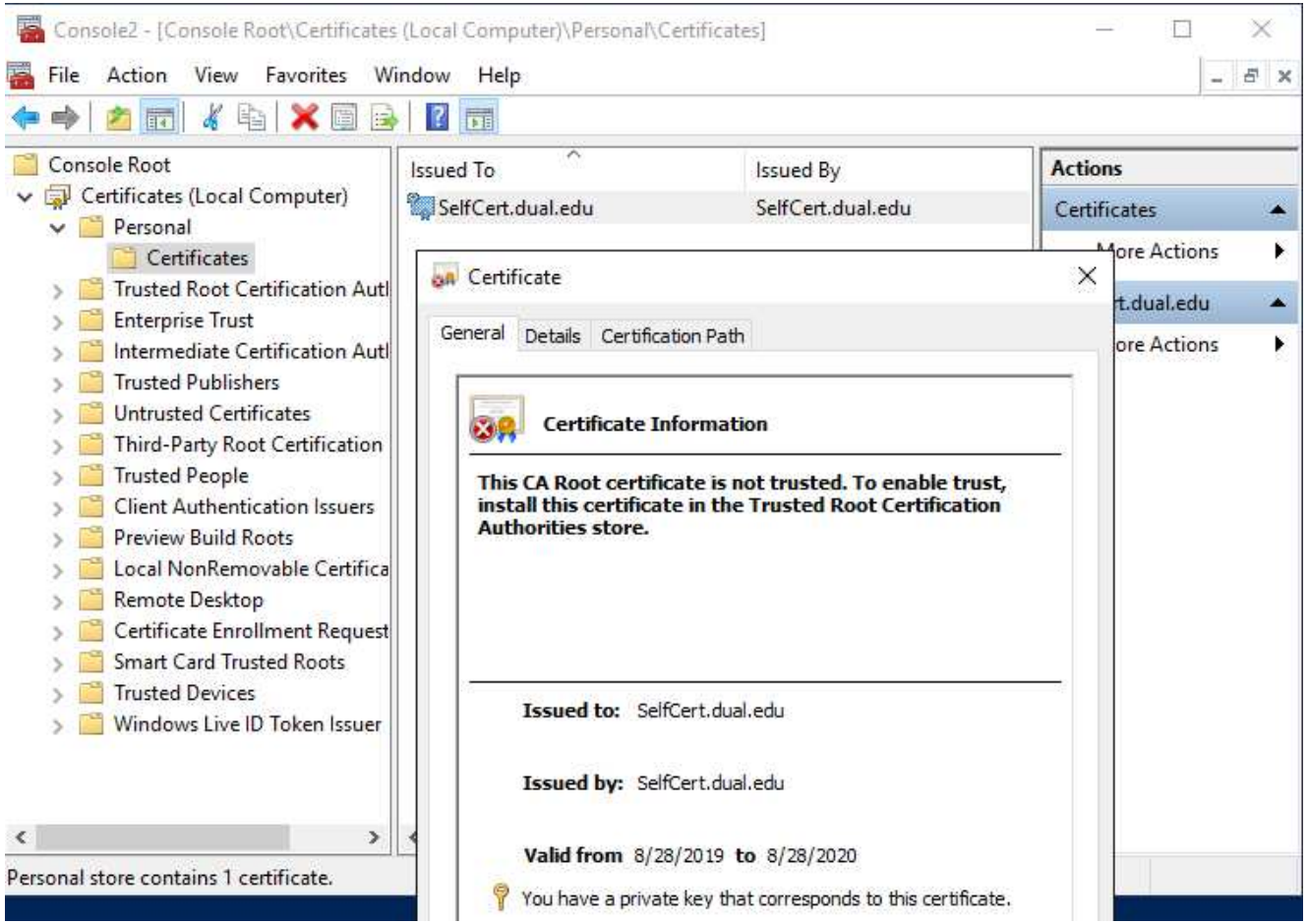
Vytvorenie self-signed cert cez PS





Self-signed cert

Vytvorenie self-signed cert cez PS

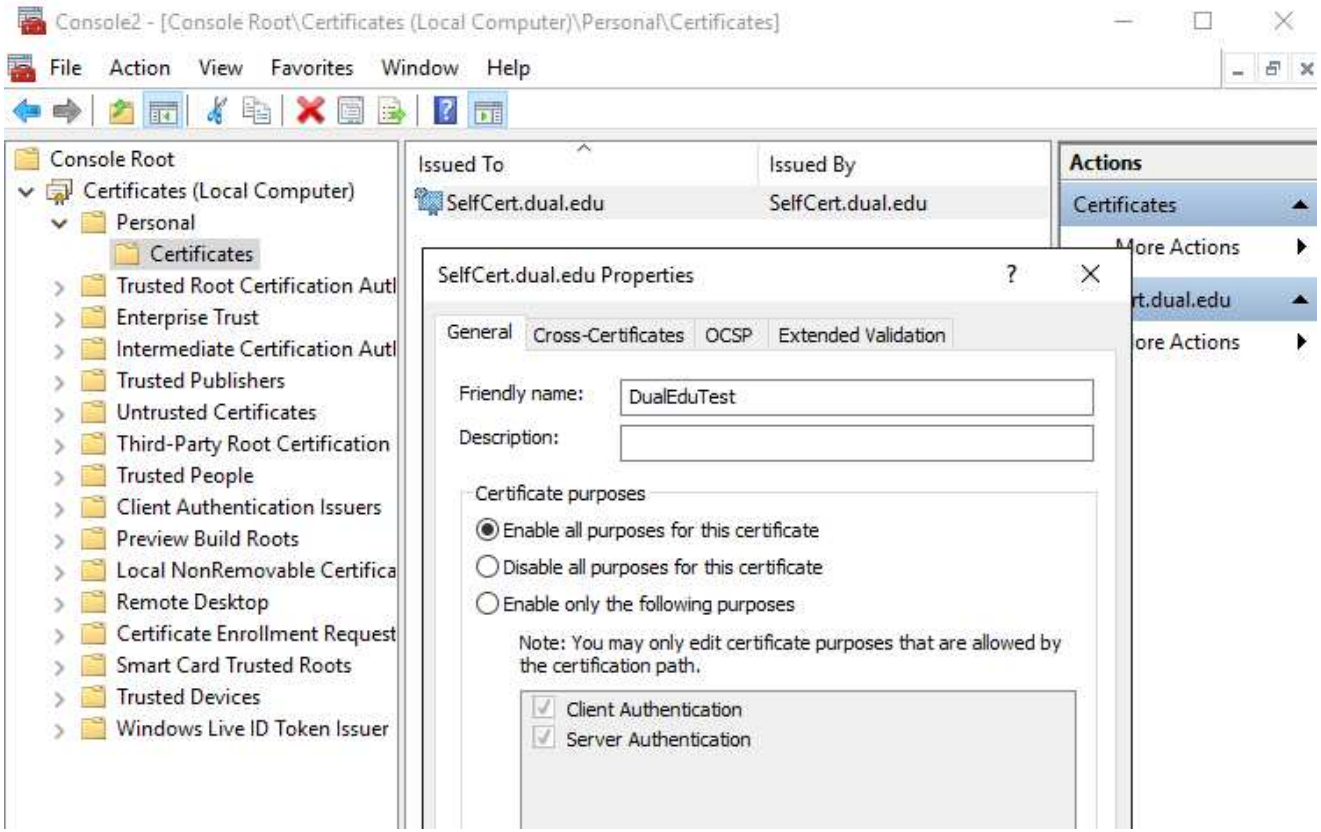


Self-signed cert

Vytvorenie self-signed cert cez PS

Self-signed cert

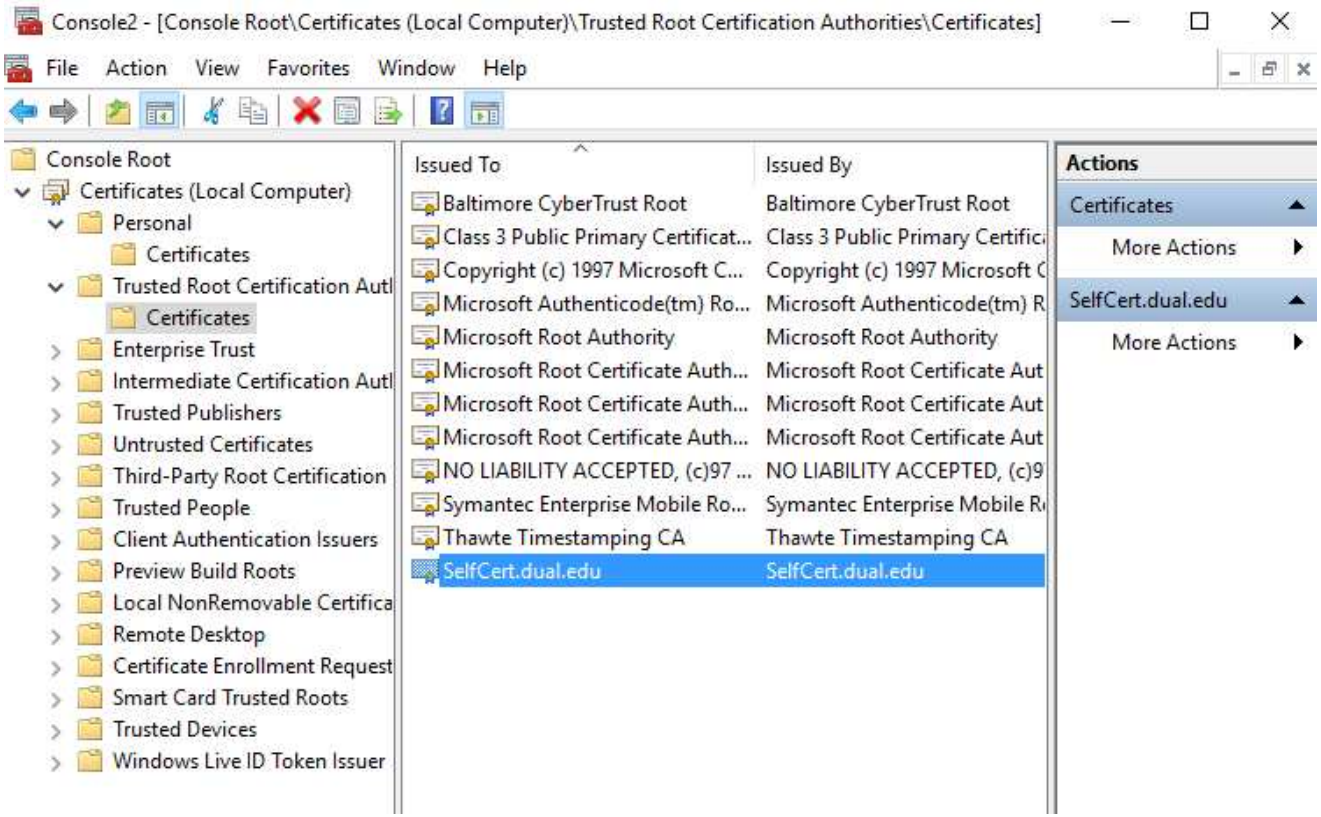
Vytvorenie self-signed cert cez PS



Self-signed cert

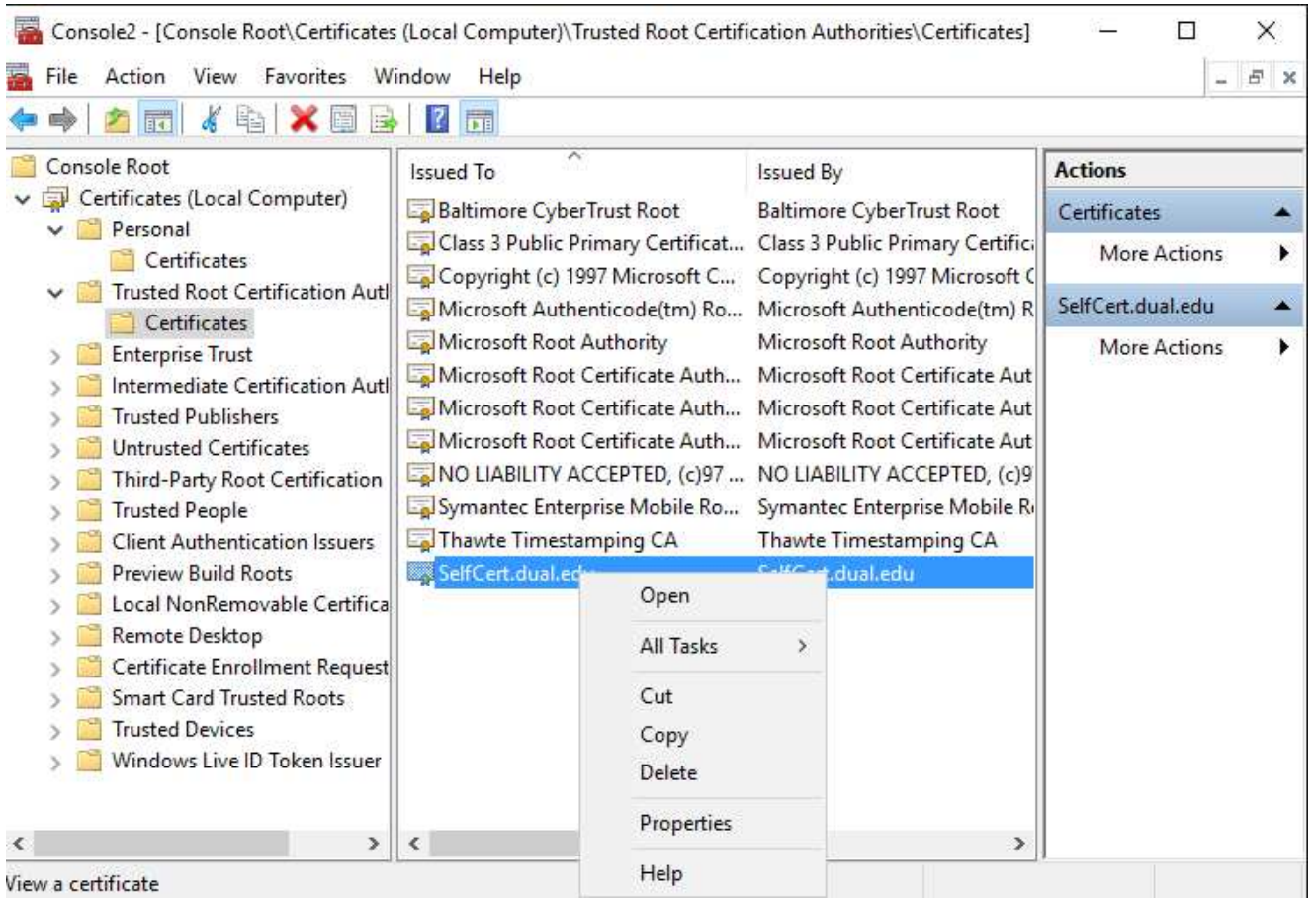
Vytvorenie self-signed cert cez PS

Copy/paste cert do trusted



Self-signed cert

„Revocation“ self-signed cert



Next

https://blogs.technet.microsoft.com/yungchou/2013/10/21/enterprise-pki-with-windows-server-2012-r2-active-directory-certificate-services-part-1-of-2/

https://www.tech-coffee.net/public-key-infrastructure-part-3-implement-pki-active-directory-certificate-services/