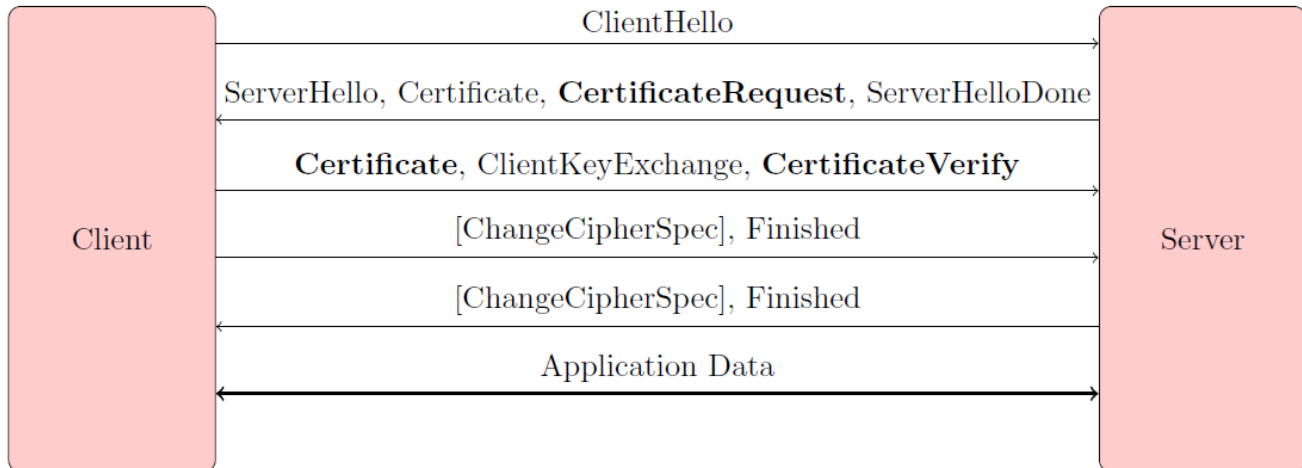


Správa klientských certifikátov

- [Postup generovania klientských certifikátov](#)
- [Správa klientských certifikátov](#)
- [Inštalácia klientskeho certifikátu](#)
 - [Microsoft Windows 7/8/10 – desktop PC](#)
 - [Android](#)
 - [iOS](#)

Smart Web podporuje autentifikácie web klientov pomocou klientských certifikátov. Jedná sa o špeciálny režim autentifikácie klientov známy ako 'Mutual authentication' alebo 'HTTPS client authentication' alebo TLS Client Certificate Authentication.



Smart Web podporuje dva režimy overovania klientských certifikátov konfigurované v súbore `smartweb.json`:

1. Lokálne overovanie (`AUTH_CERTIFICATE_LOCALLY`) na strane WildFly AS
2. Vzdialené overovanie (`AUTH_CERTIFICATE_REMOTELY`) v aplikácii D2000

Nasledujúce kapitoly obsahujú odporúčania pre generovanie a správu klientských certifikátov.

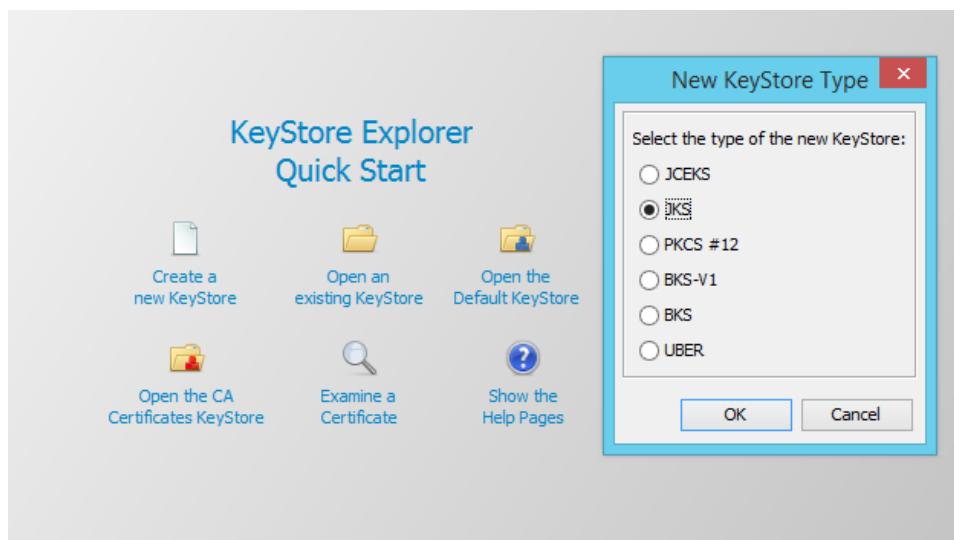
Postup generovania klientských certifikátov

Klientske certifikáty sa generujú pomocou nástroja [KeyStore Explorer](#). Postup je nasledovný:

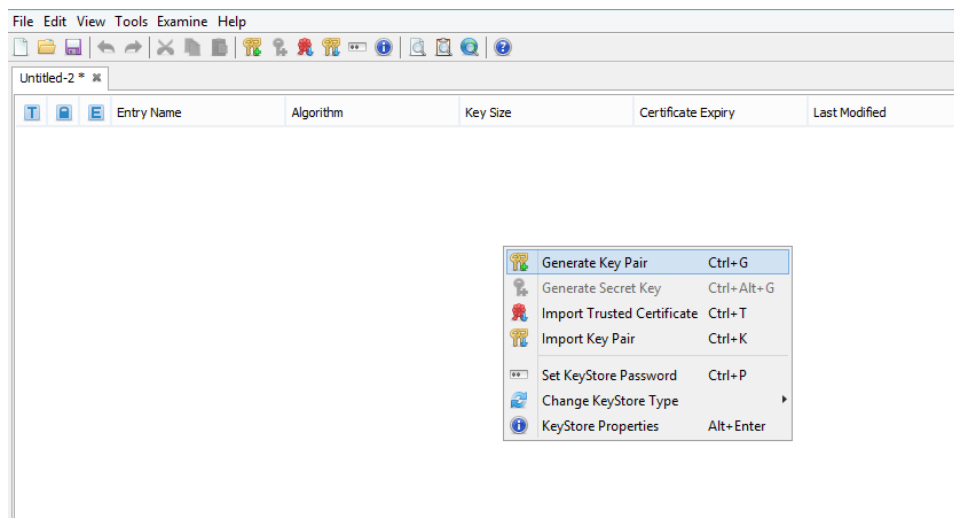
1. Je potrebné vytvoriť keystore, v ktorom bude uložený self-signed *companyca* keypair. Názov tohto súboru je `master-client-credentials.jks`. Vytvorí sa nasledovne, po štarte programu vybrať **Create a new KeyStore**, kde definujeme typ KeyStoru v našom prípade JKS.



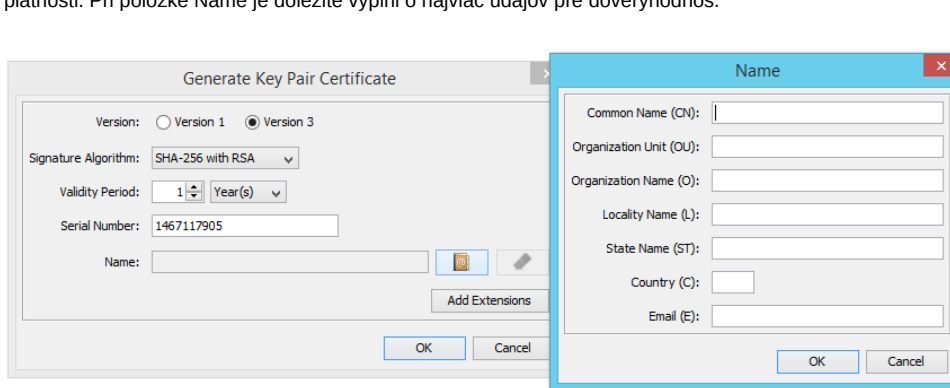
Súbor `master-client-credentials.jks` sa nepoužíva priamo na serveroch, ale slúži len ako repository certifikátov. Zo súboru `master-client-credentials.jks` sa nikdy neexportuje privátny kľúč *companyca* !!!



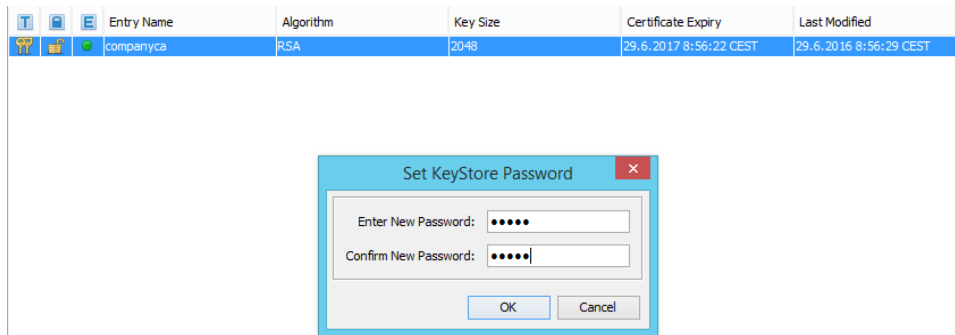
2. alej klikneme pravým tlačidlom a vyberieme Generate Key Pair.



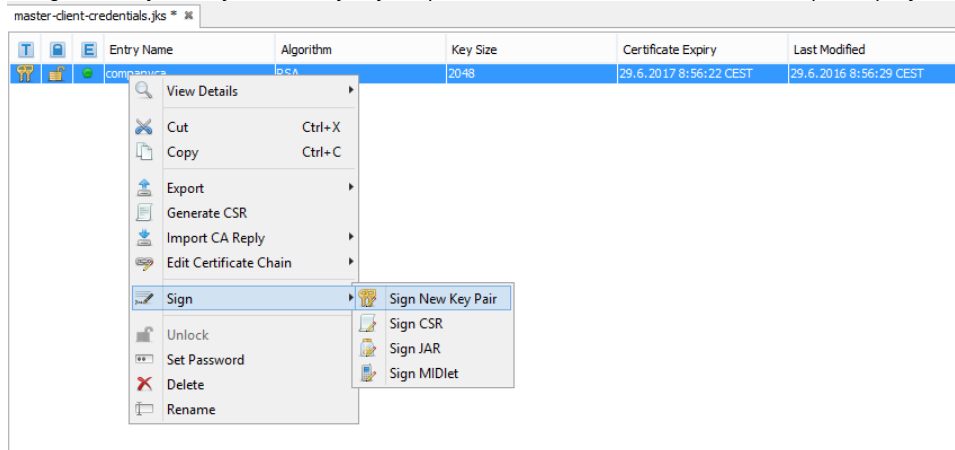
3. Algorithm Selection necháme na RSA s hodnotou Key Size 2048. alej vyberieme verziu 3, Signature Algorithm SHA-256 with RSA a dobu platnosti. Pri položke Name je dôležité vyplni o najviac údajov pre dôveryhodnosť.



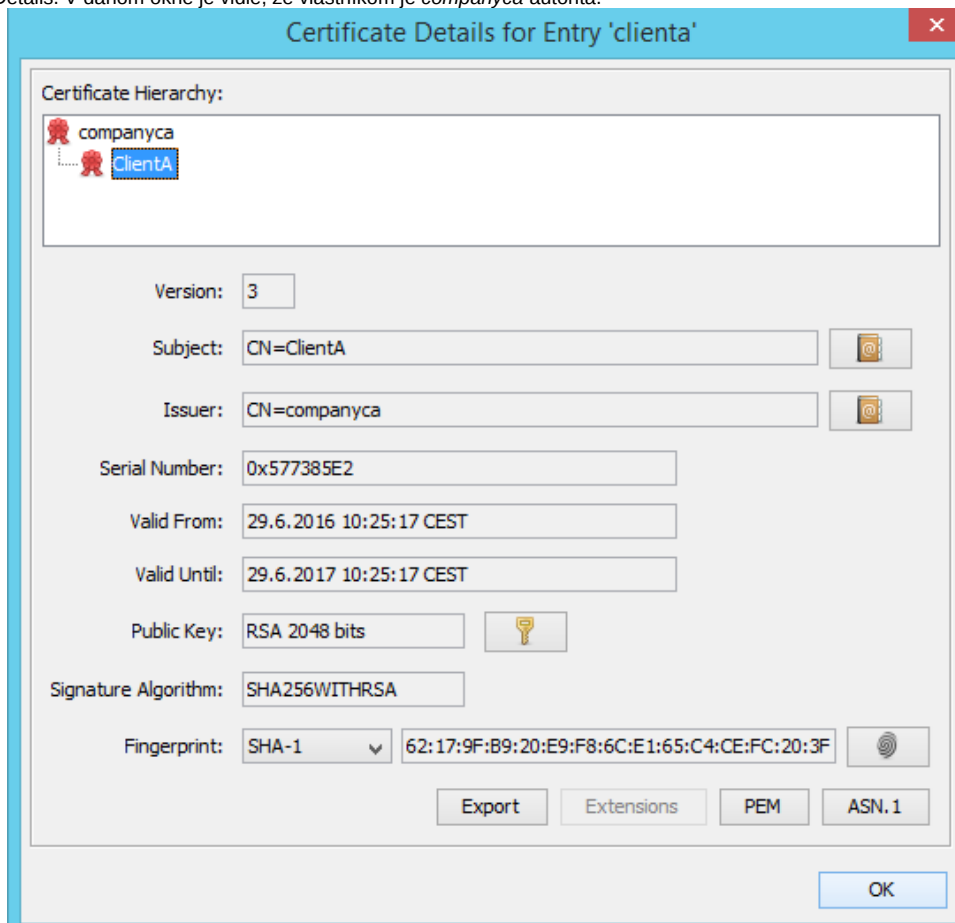
4. Následne zvolíme Alias a heslo *companyca* Key Pair-u. alej uložíme KeyStore pod menom *master-client-credentials.jks*. Pri ukladaní sa opäť vyžaduje nastavenie hesla, tentokrát však na KeyStore.



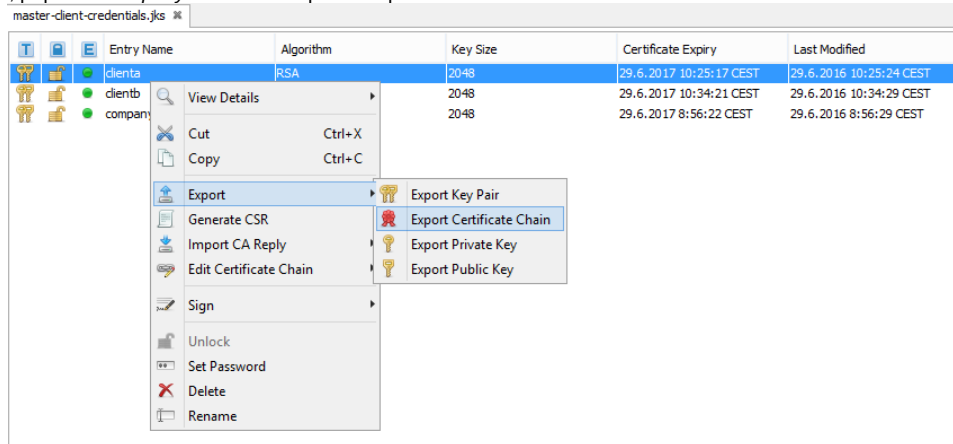
5. Pre každého klienta je potrebné vygenerovať key-pair podpísaný pomocou *companyca*. Postupujeme tak, že klikneme pravým na *companyca* v menu zvolíme Sign a Sign New Key Pair. Vytvoríme nový KeyPair pre *ClientA* s nastaveniami šifrovania ako pri *companyca*.



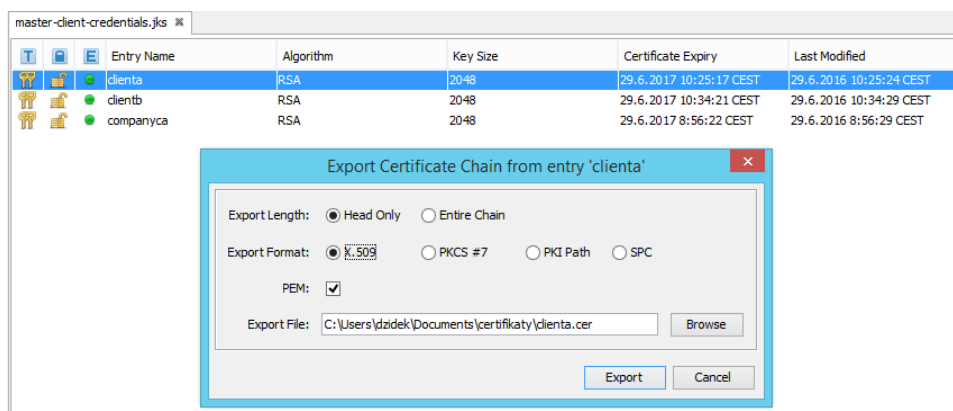
6. Pre overenie, že je klientsky KeyPair podpísaný *companyca* autoritou, klikneme pravým na *ClientA* a vyberieme z menu View Details a Certificate Chain Details. V danom okne je vidieť, že vlastníkom je *companyca* autorita.



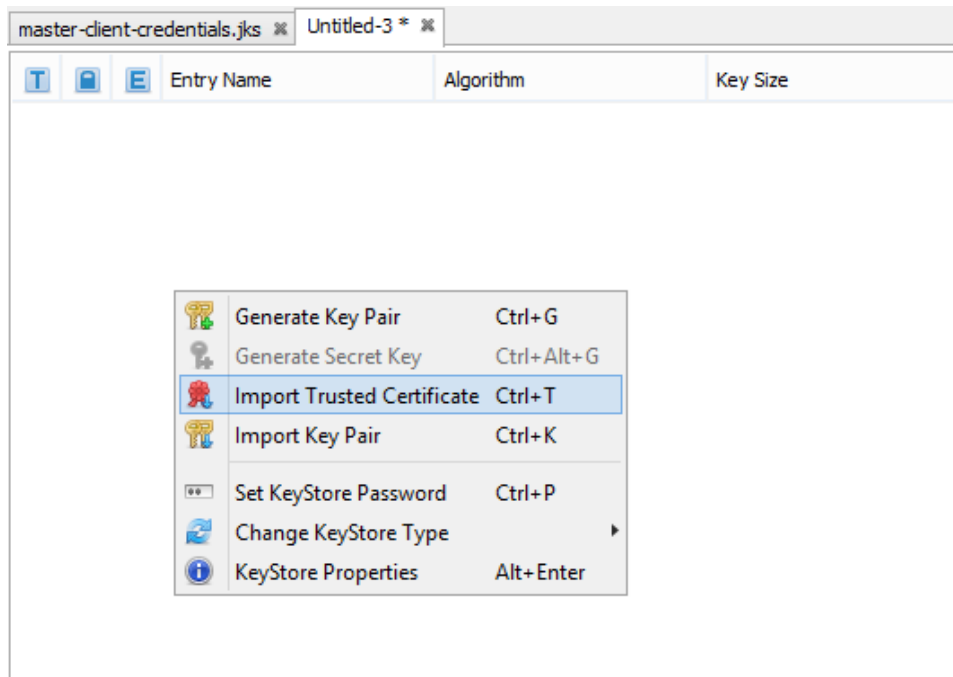
7. Zo súboru master-client-credentials.jks sa exportujú certifikáty klientov a *companyca* do súborov clientcertificates-full.jks, client-certificates-d2ws.jks, client-certificates-d2000.jks (Dávajú sa na servery, obsahujú verejné kúe). Certifikáty jednotlivých klientov a *companyca* vyexportujeme kliknutím na klienta, prípadne *companyca* a dáme Export a Export Certificate Chain.



8. Pri exporte ponecháme nastavenia prípadne upravíme cestu, kde sa ma certifikát uloží a klikneme na export.



9. Ke sú všetky certifikáty vyexportované, uložíme ich do clientcertificates-full.jks a to tak, že vytvoríme nový JKS súbor cez menu programu KeyStore File > New a vyberieme typ JKS. Tu naimportujeme certifikáty kliknutím pravým tlačidlom myši a vyberieme Import Trusted Certificate a certifikát, ktorý chceme importovať.



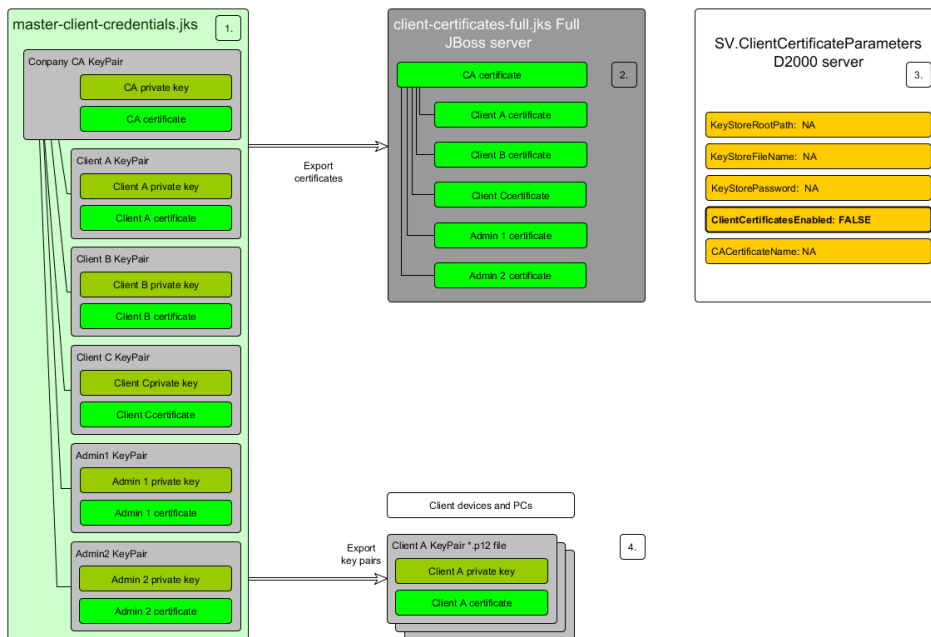
master-client-credentials.jks		Untitled-3 *			
	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	clienta	RSA	2048	29.6.2017 10:25:17 CEST	29.6.2016 11:08:51 CEST
	clientb	RSA	2048	29.6.2017 10:34:21 CEST	29.6.2016 11:09:01 CEST
	companyca	RSA	2048	29.6.2017 8:56:22 CEST	29.6.2016 11:08:43 CEST

- Po naimportovaní KeyStore uložíme ako clientcertificates-full. Opä je vyžadované nastavenie hesla na tento JKS súbor. Tento súbor clientcertificates-full.jks uložíme na konkrétny server, kde to je vyžadované.
- Zo súboru master-client-credentials.jks sa exportujú key-pairs klientov vo formáte *.p12 (obsahujú verejné aj súkromné kúe, dáva sa zákazníkovi na zariadenie (PC, Tablet ...)). Export vykonáme v súbore master-client-credentials.jks, kde klikneme pravým tlačidlom na jednotlivých klientov a dáme Export > Export Key Pair. V zložke sa nám vytvoria súbory ClientA.p12 a ClientB.p12, ktoré sa pošlú jednotlivým užívateľom na zariadenia.

master-client-credentials.jks		clientcertificates-full			
	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	clienta	RSA	2048	29.6.2017 10:25:17 CEST	29.6.2016 10:25:24 CEST
	clientb	RSA	2048	29.6.2017 10:34:21 CEST	29.6.2016 10:34:29 CEST
	companyca	RSA	2048	29.6.2017 8:56:22 CEST	29.6.2016 8:56:29 CEST

Správa klientských certifikátov

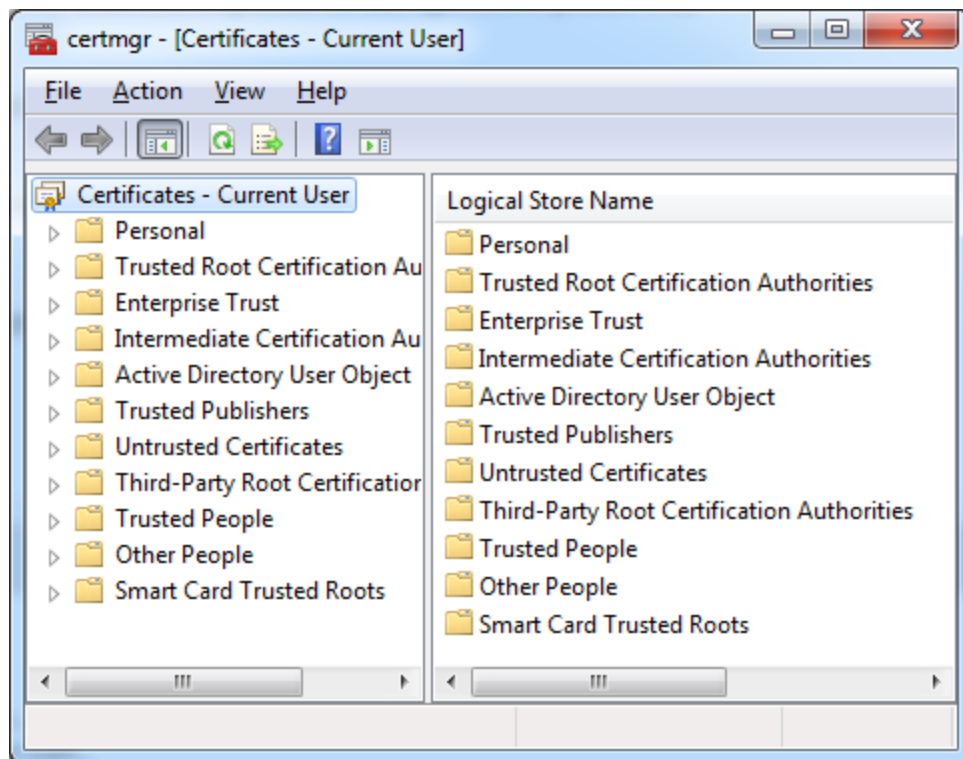
- master-client-credentials.jks keystore obsahuje master companyca key-pair a ním podpísané klientske key-pairs.
- Klientske certifikáty pre klientov Smart Web aplikácie a companyca certifikát je potrebné vyexportovať do súboru client-certificates-full.jks, ktorý musí byť prístupný na čítanie pre JVM proces, v ktorom beží WildFly AS.
- Klientske certifikáty a súkromné kúe je potrebné exportovať zo súboru master-client-credentials.jks vo formáte *.p12.



Inštalácia klientskeho certifikátu

Microsoft Windows 7/8/10 – desktop PC

Na import klientských certifikátov je vhodné použiť aplikáciu certmgr.msc, ktorá je štandardnou súčasťou OS Windows. Je potrebné vybrať priečinok "Personal" a zvoliť akciu import pre príslušný *.p12 key-pair.



Android

Klientsky *.p12 key-pair je potrebné uložiť do adresára "Downloads" a importovať cez nastavenia systému.

iOS

Klientsky *.p12 key-pair je potrebné poslať v prílohe mailom na klientske zariadenia a importovať cez nastavenia systému.