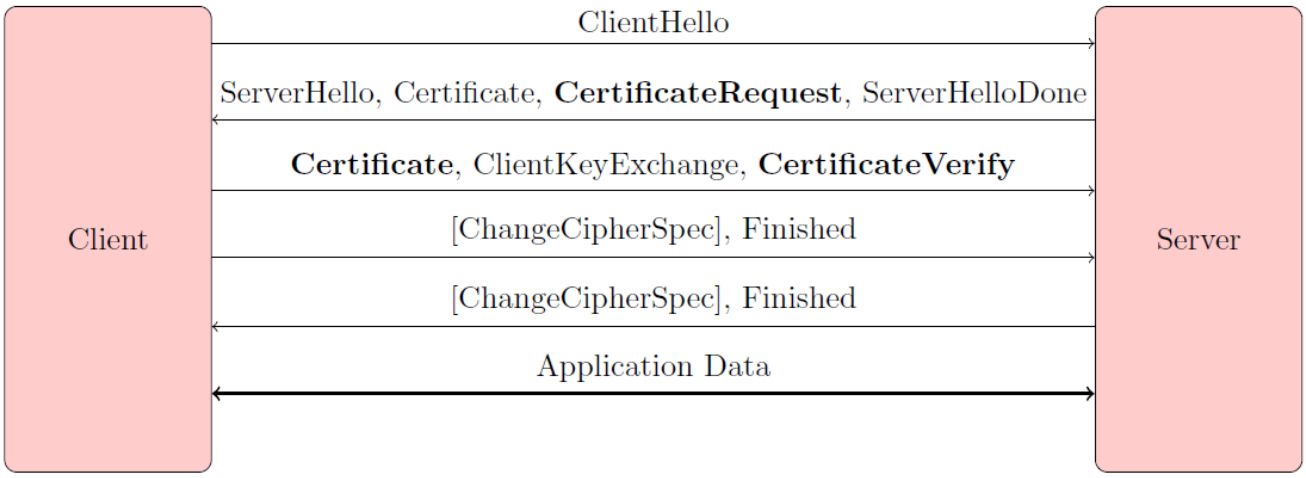
Správa klientských certifikátov

Smart Web podporuje autentifikácie web klientov pomocou klientskych 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 klientskych certifikátov konfigurovatené v súbore smartweb.json:

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

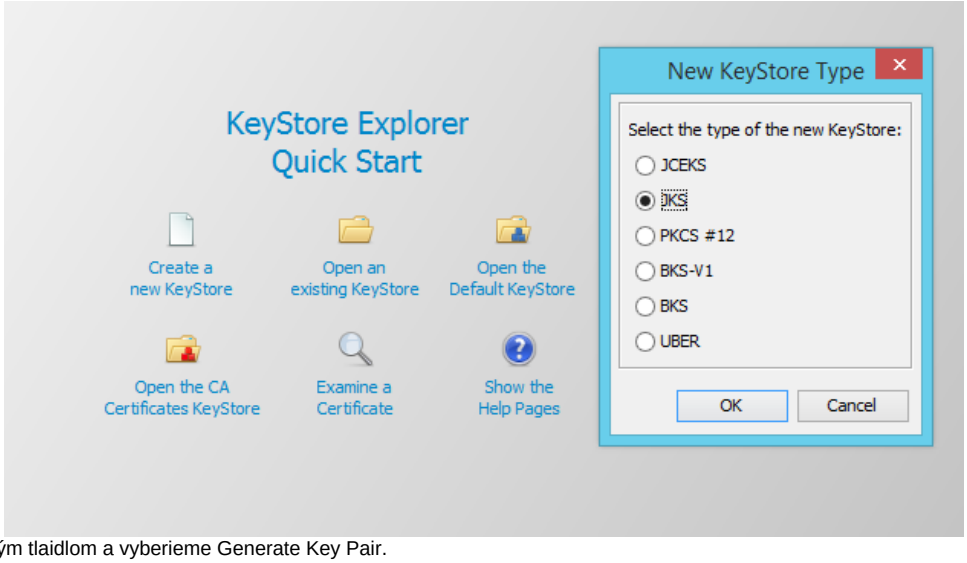
Nasledujúce kapitoly obsahujú odporúania pre generovanie a správu klientskych certifikátov.

Postup generovania klientských certifikátov

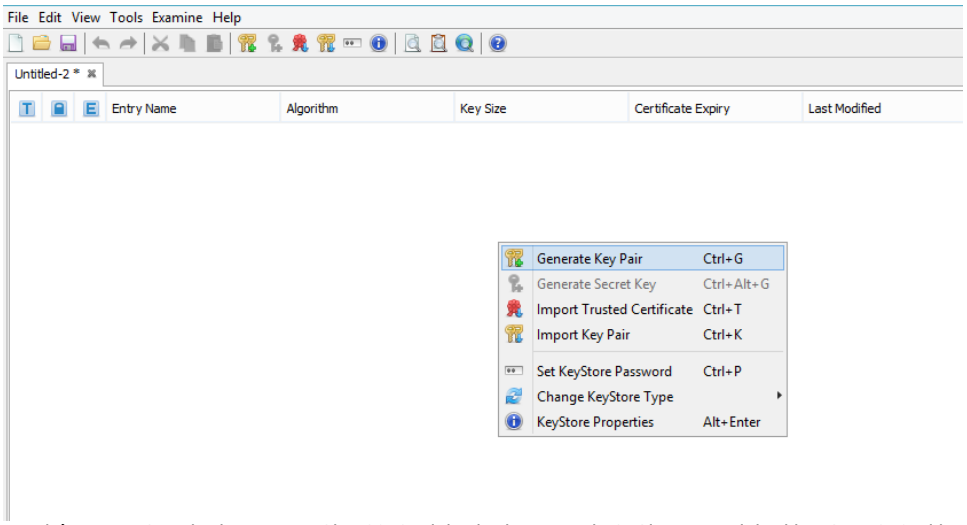
Klientske certifikáty sa generujú pomocou nástroja KeyStore Explorer. Postup je nasledovný:

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

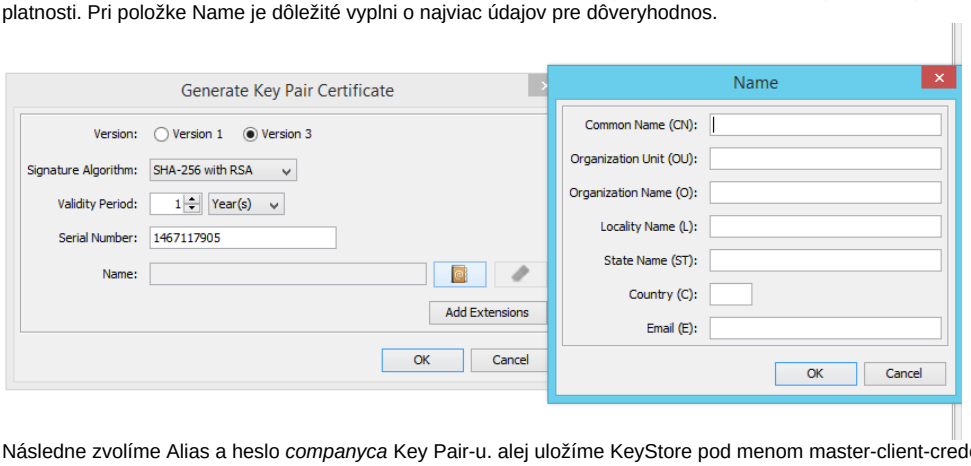
   > Súbor master-client-credentials.jks sa nepoužíva priamo na serveroch, ale slúži len ako repository certifikátov. Zo súboru master-client-credentials.jks sa nikdy neexportuje privátny kú *companyca* !!!



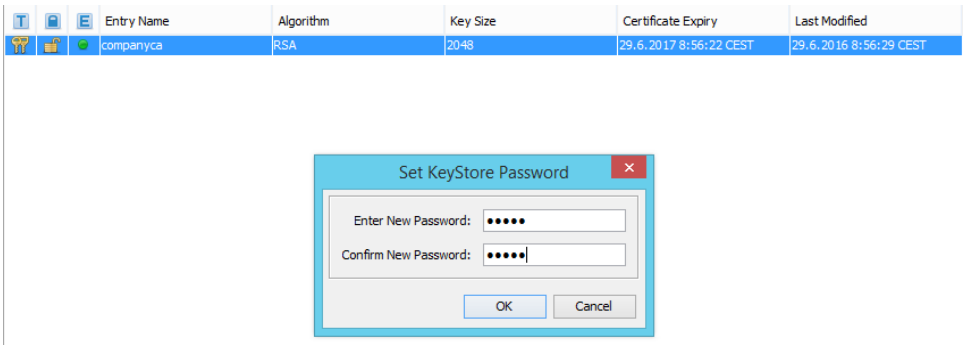
2. alej klikneme pravým tlaidlom a vyberieme Generate Key Pair.



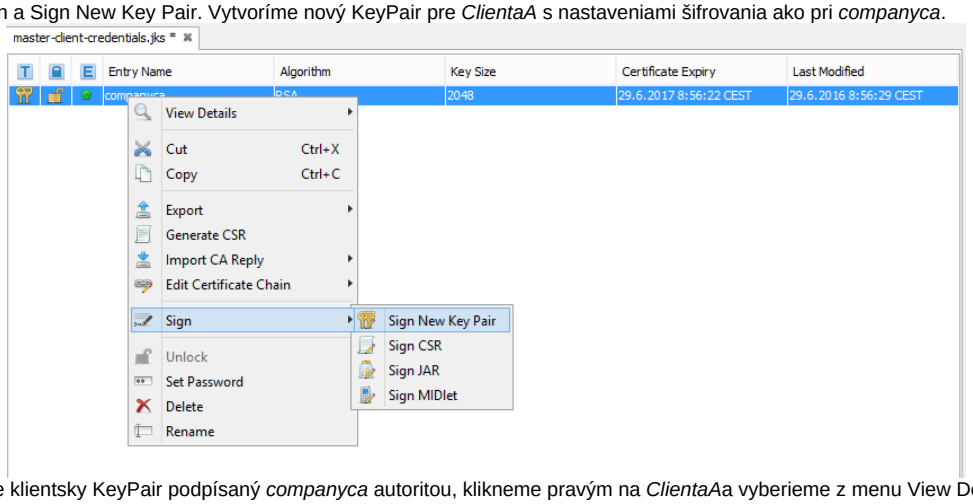
3. Algorithm Selection necháme na RSA s hodnotou Key Size 2048. alej vyberieme verziu 3, Signature Alghorithm SHA-256 with RSA a dobu platnosti. Pri položke Name je dôležité vyplni o najviac údajov pre dôveryhodnos.



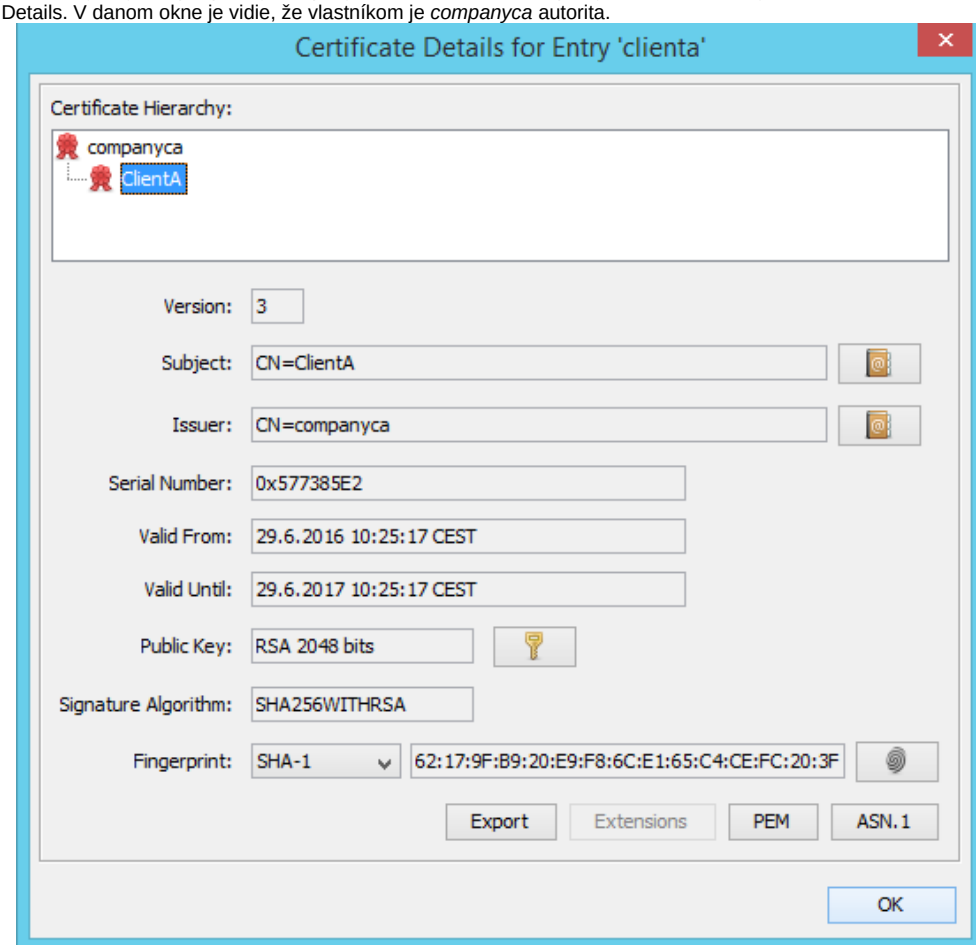
4. Následne zvolíme Alias a heslo *companyca* Key Pair-u. alej uložíme KeyStore pod menom master-client-credentials.jks. Pri ukladaní sa opä vyžaduje nastavenie hesla, tentokrát však na KeyStore.



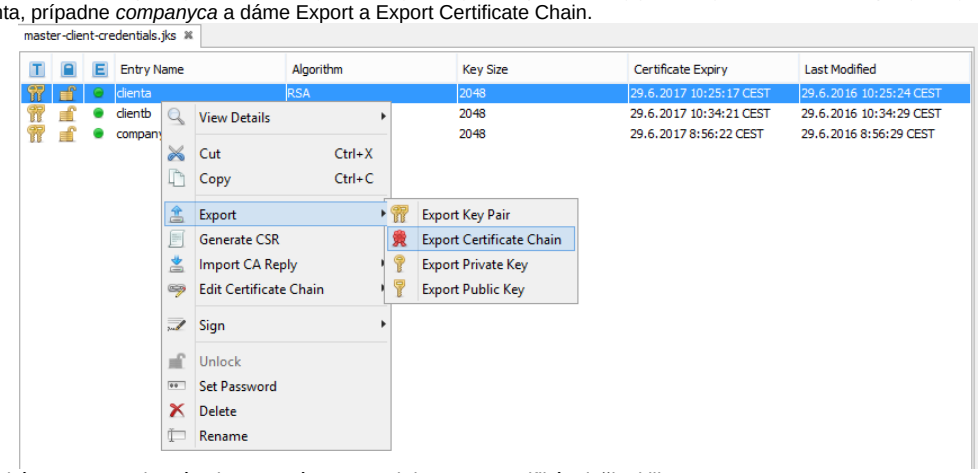
5. Pre každého klienta je potrebné vygenerova key-pair podpísaný pomocou *companyca*. Postupujeme tak, že klikneme pravým na *companyca* v menu zvolíme Sign a Sign New Key Pair. Vytvoríme nový KeyPair pre *ClientaA* s nastaveniami šifrovania ako pri *companyca*.



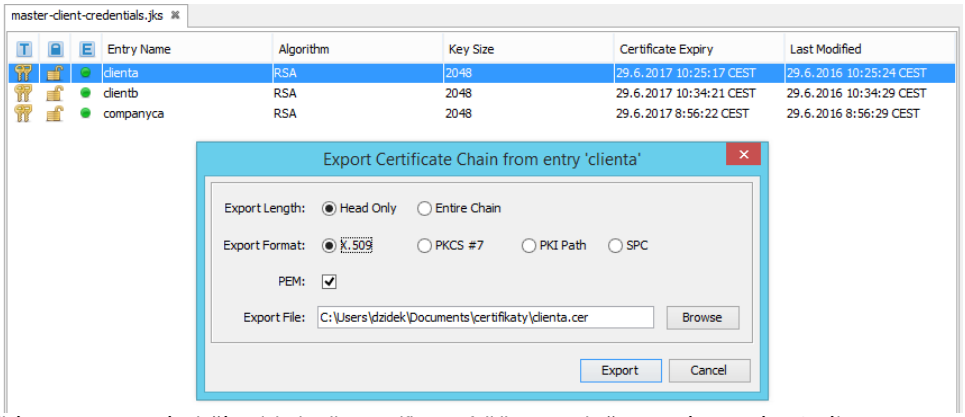
6. Pre overenie, že je klientsky KeyPair podpísaný *companyca* autoritou, klikneme pravým na *ClientaA*a vyberieme z menu View Details a Certificate Chain Details. V danom okne je vidie, že vlastníkom je *companyca* autorita.



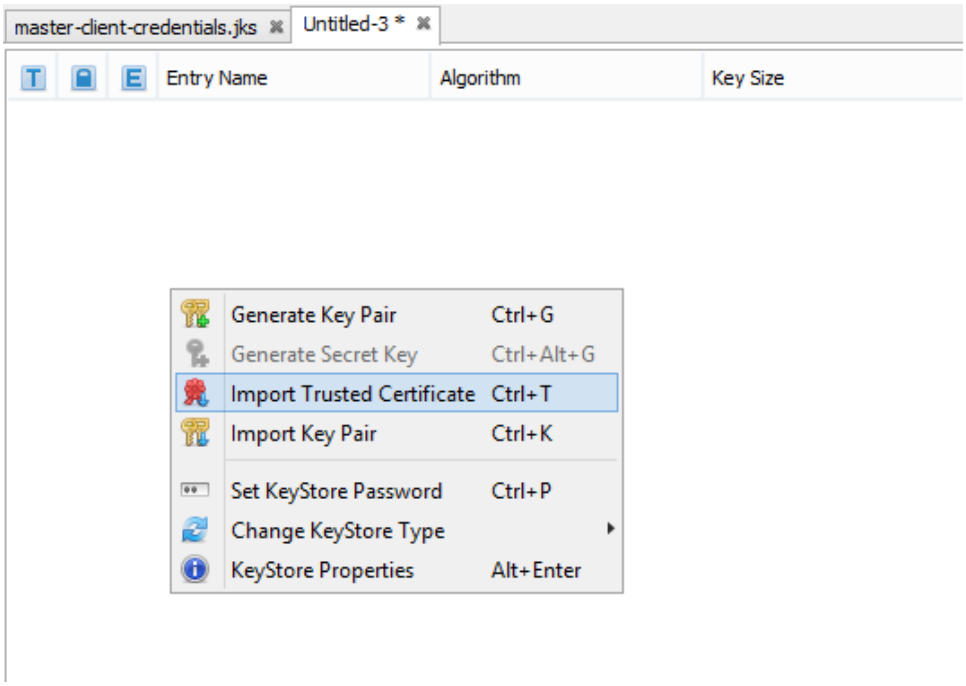
7. Zo súboru master-client-credentials.jks sa exportujú certifikáty klientov a *companyca* do súborov clientcertificates-full.jks, client-certificates-d2ws.jks, client-certificates-d2000.jks (Dávajú sa na servery, obsahujú verejné kúe). Certifikáty jednotlivých klientov a *companyca* vyexportujeme kliknutím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

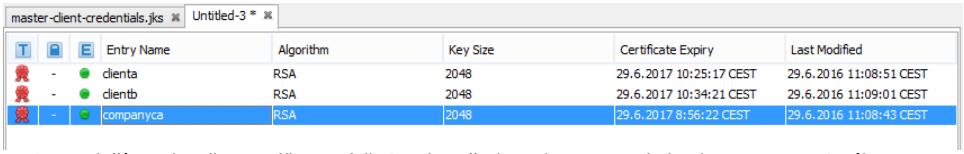


8. Pri exporte ponecháme nastavenia prípadne upravíme cestu, kde sa ma certifikát uloži a klikneme na export.

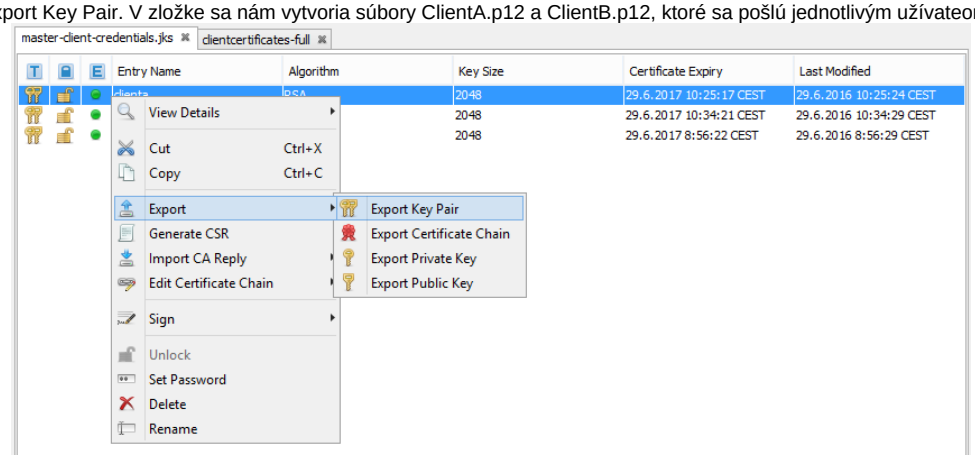


9. Ke sú všetky certifikáty vyexportované, uložíme ich do clientcertificates-full.jks a to tak, že vytvoríme nový JKS súbor cez menu programu KeyStore File > New a vyberieme typ JKS. Tu naimportujeme certifikáty kliknutím pravým tlaidlom myši a vyberieme Import Trusted Certificate a certifikát, ktorý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



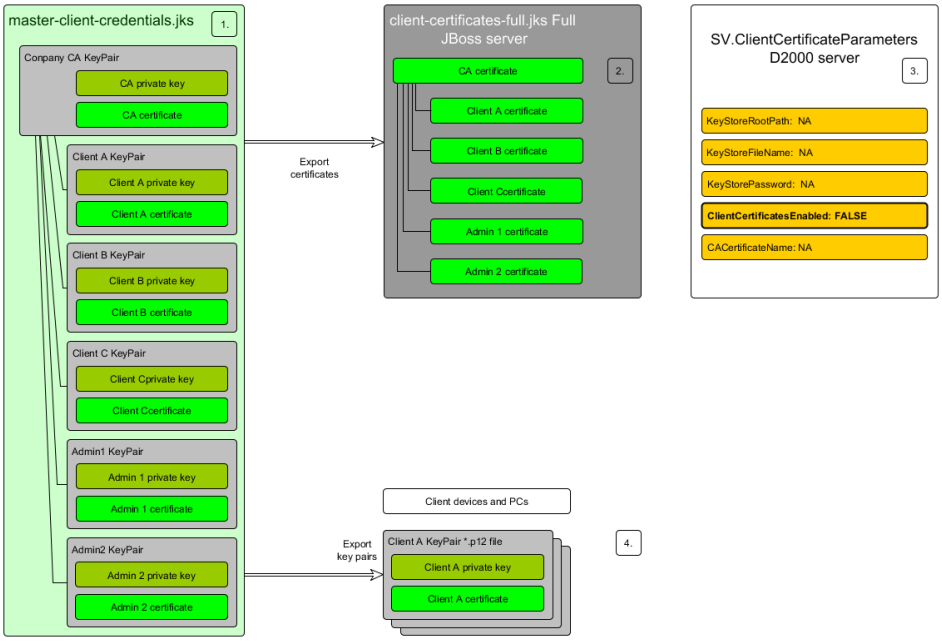


10. Po naimportovaní KeyStore uložíme ako clientcertificates-full. Opä je vyžadovanie nastavenie hesla na tento JKS súbor. Tento súbor clientcertificates-full.jks uložíme na konkrétny server, kde to je vyžadované.
11. Zo súboru master-client-credentials.jks sa exportujú key-pairs klientov vo formáte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



Správa klientskych certifikátov

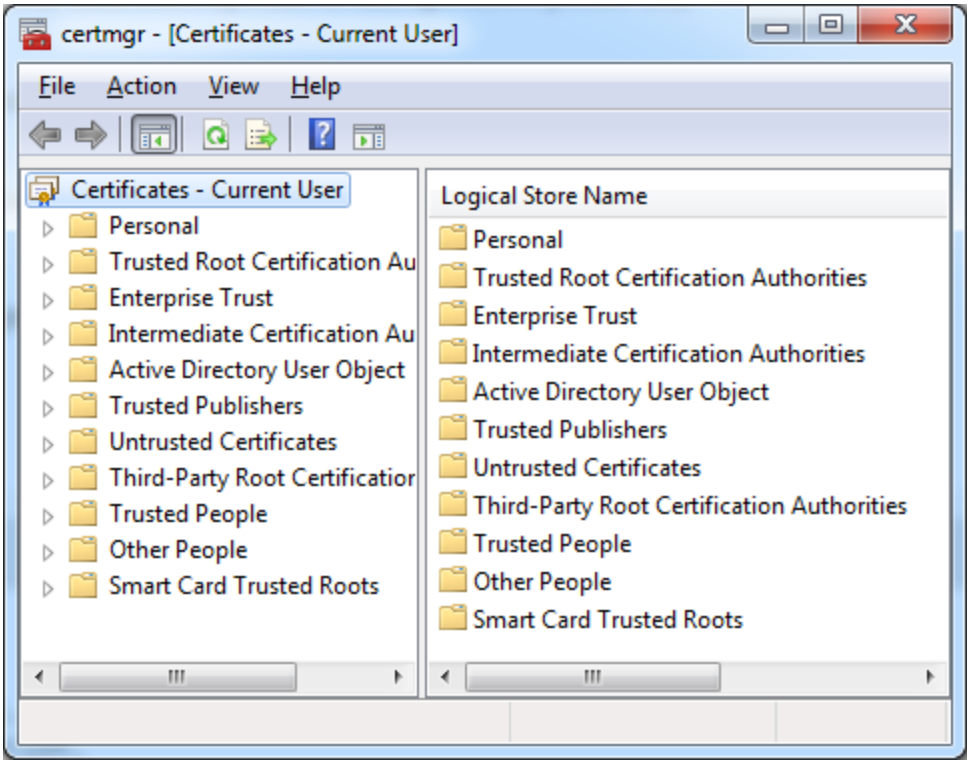
1. master-client-credentials.jks keystore obsahuje master companyca key-pair a ním podpísané klientske key-pairs.
2. Klientske certifikáty pre klientov Smart Web aplikácie a *companyca* certifikát je potrebné vyexportova do súboru client-certificates-full.jks, ktorý musí by prístupný na ítanie pre jvm proces, v ktorom beží WildFly AS.
3. Klientske certifikáty a privátne kúe je potrebné exportova zo súboru master-client-credentials.jks vo formáte *.p12.



Inštalácia klientskeho certifikátu

Microsoft Windows 7/8/10 – desktop PC

Na import klientskych certifikátov je vhodné použi aplikáciu certmgr.msc, ktorá je štandardnou súasou OS Windows. Je potrebné vybra prieinok “Personal” a zvoli akciu import pre príslušný *.p12 key-pair.



Android

Klientsky *.p12 key-pair je potrebné uloži do adresára “Downloads” a importova cez nastavenia systému.

iOS

Klientsky *.p12 key-pair je potrebné posla v prílohe mailom na klientske zariadenia importova cez nastavenia systému.