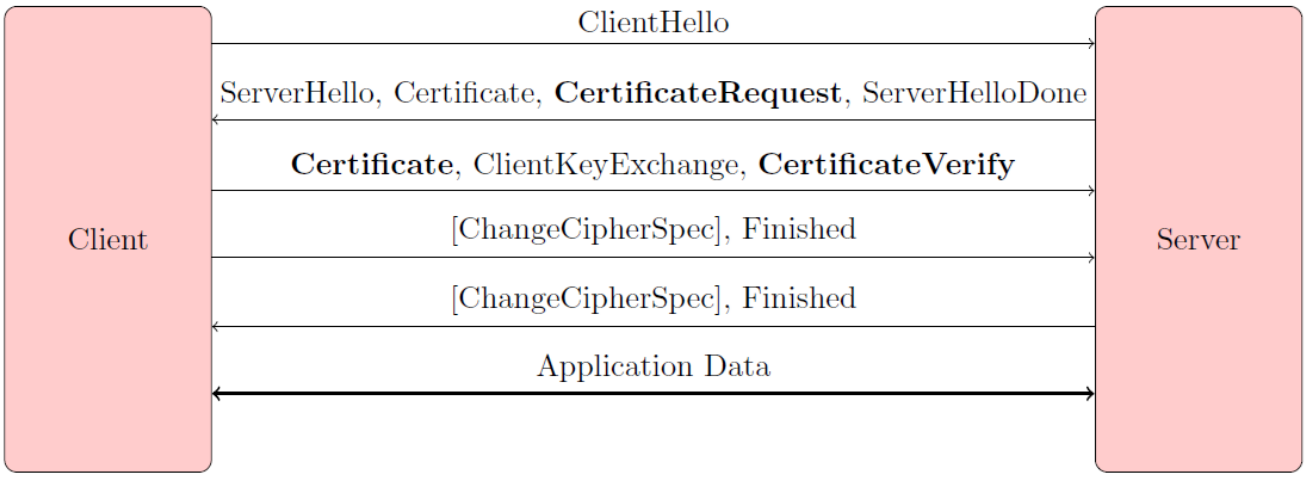
Administration of Clients' Certificates

Smart Web supports authentication of web clients using client certificates. It is a special mode of authentication of clients known as ‘Mutual authentication’ or ‘HTTPS client authentication’ or TLS Client Certificate Authentication.



Smart Web support two ways of authenticating of client certificates configurable in the smartweb.json file:

1. Local authentication (AUTH_CERTIFICATE_LOCALLY) on the WildFly AS side
2. Remote authentication (AUTH_CERTIFICATE_REMOTELY) in the D2000 application

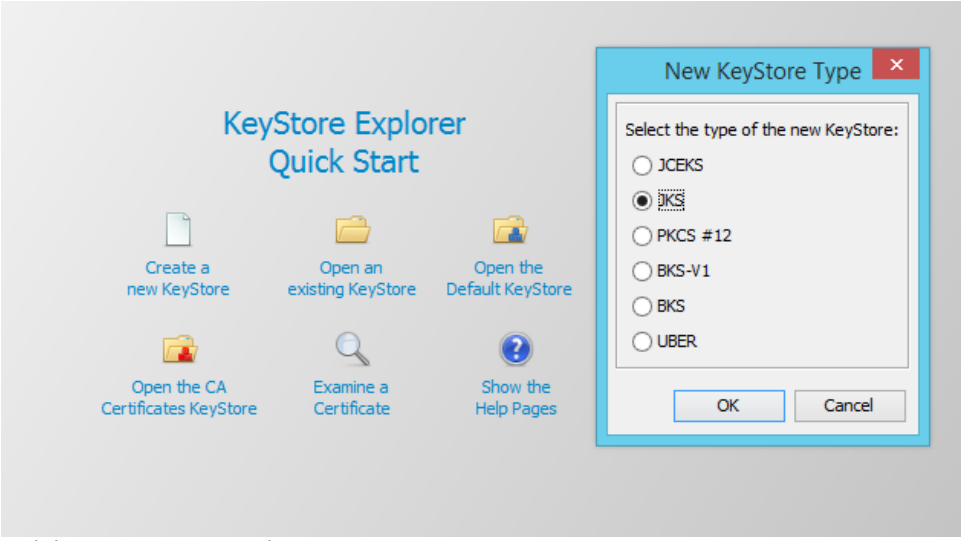
The following chapters contain recommendations for generating and administration of client certificates.

Process of Generating Client Certificates

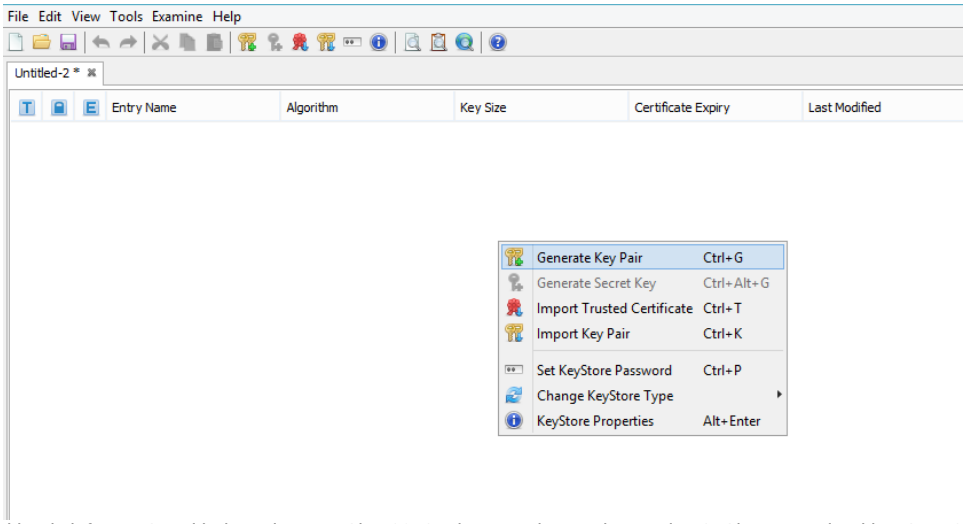
Client certificates are generated using the KeyStore Explorer tool. Steps of the process are as follows:

1. It is necessary to create a keystore in which a self-signed *companyca* keypair will be stored. A name of this file is master-client-credentials.jks. It is created by choosing Create and new KeyStore after the program start where we define the type of KeyStore, in our case JKS.

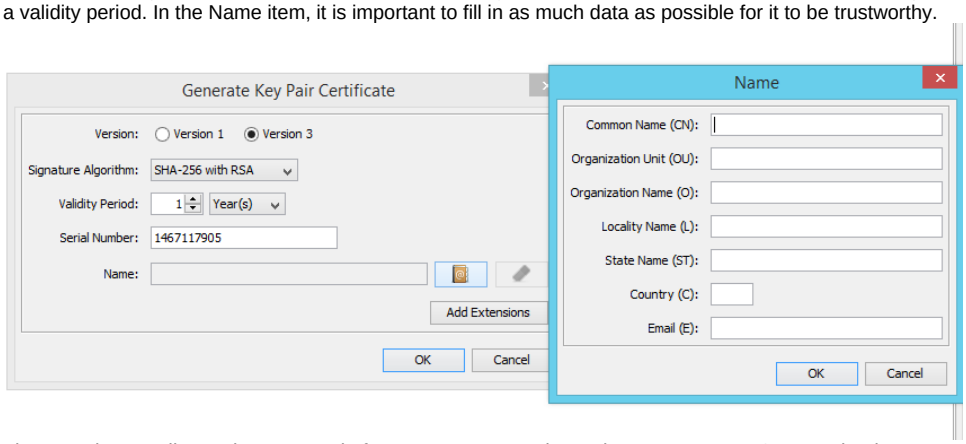
   > The master-client-credentials.jks file is not used directly on servers but serves only as a repository certificate. From the master-client-credentials.jks file, the private key *companyca* is never exported!



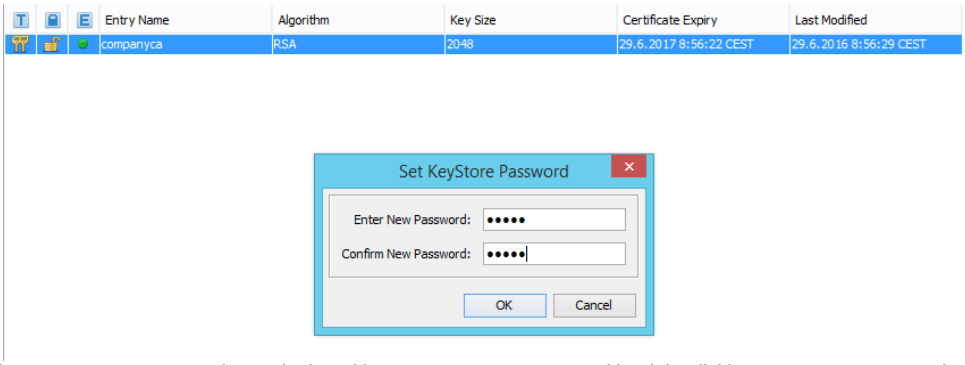
2. Then we right-click and choose Generate Key Pair.



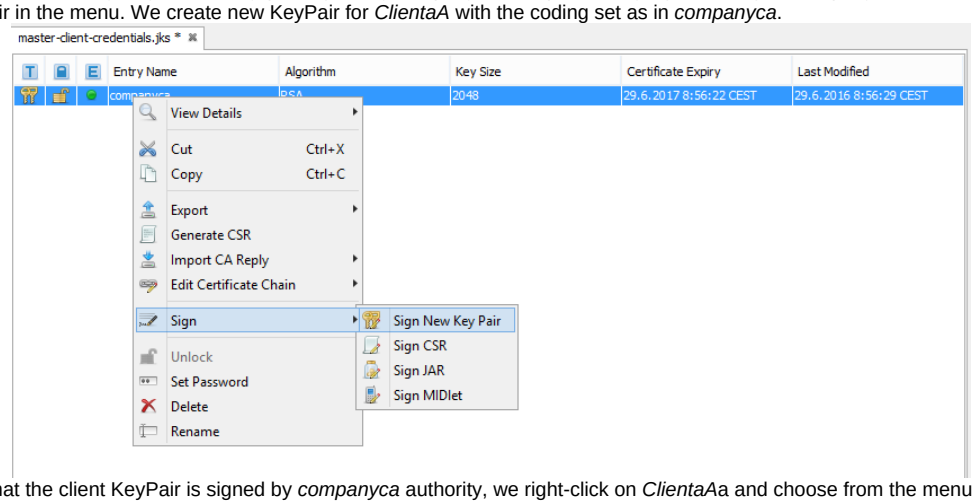
3. The Selection algorithm is left on RSA with the value Key Size 2048. Then we choose the version 3, Signature Algorithm SHA-256 with RSA and a validity period. In the Name item, it is important to fill in as much data as possible for it to be trustworthy.



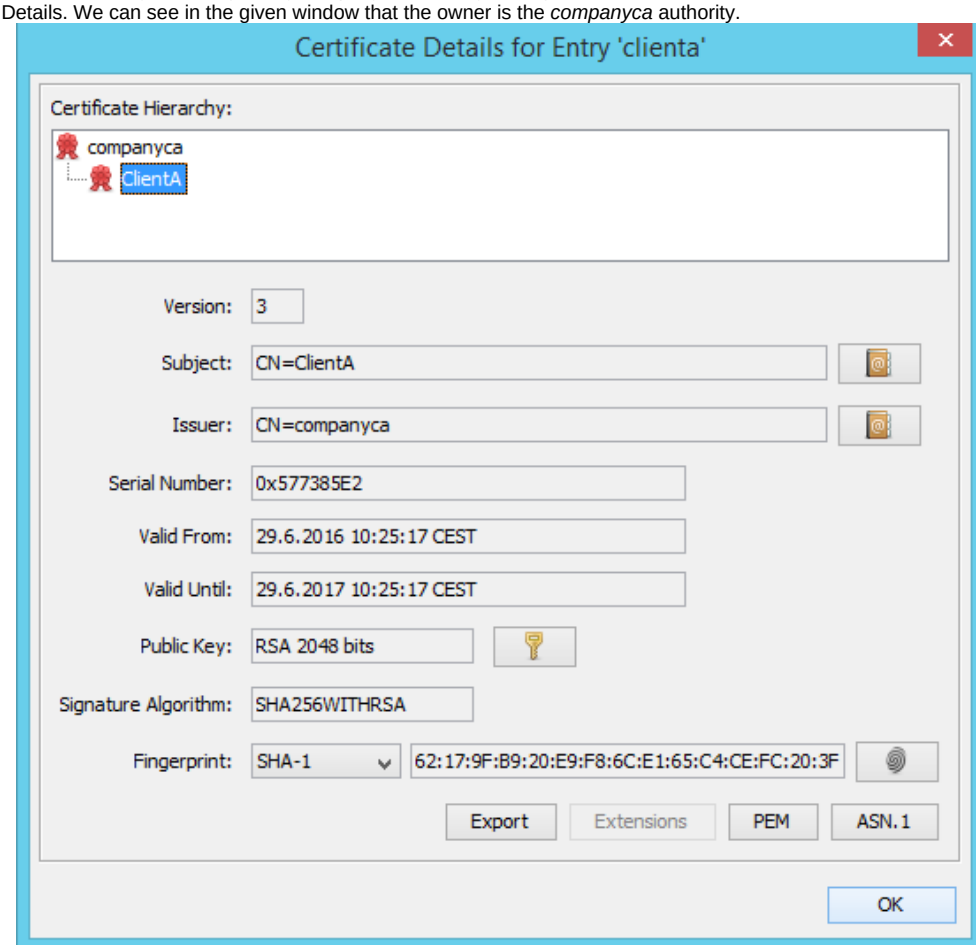
4. Then we choose Alias and a password of *companyca* Key Pair. Further, we store KeyStore under the master-client-credentials.jks name. When storing, setting password is again required but this time on KeyStore.



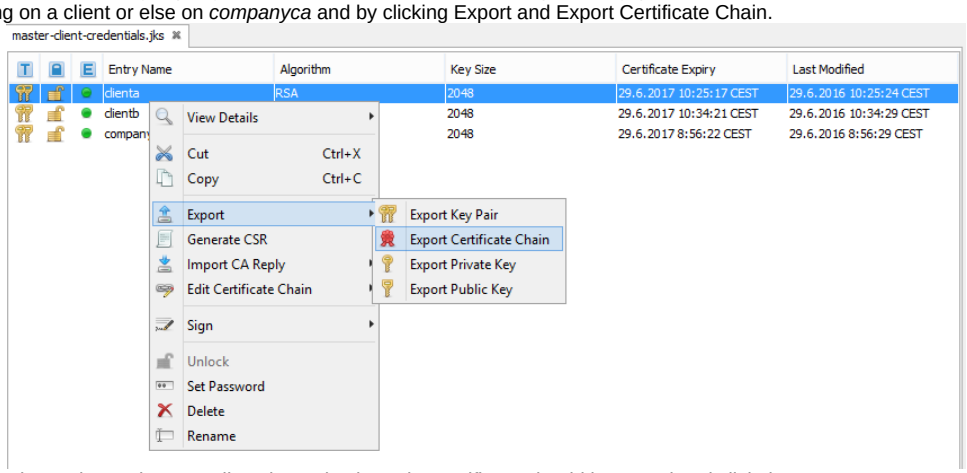
5. For every client, it is necessary to generate key-pair signed by *companyca*. We proceed by right-clicking on *companyca,* we choose Sign and Sign New Key Pair in the menu. We create new KeyPair for *ClientaA* with the coding set as in *companyca*.



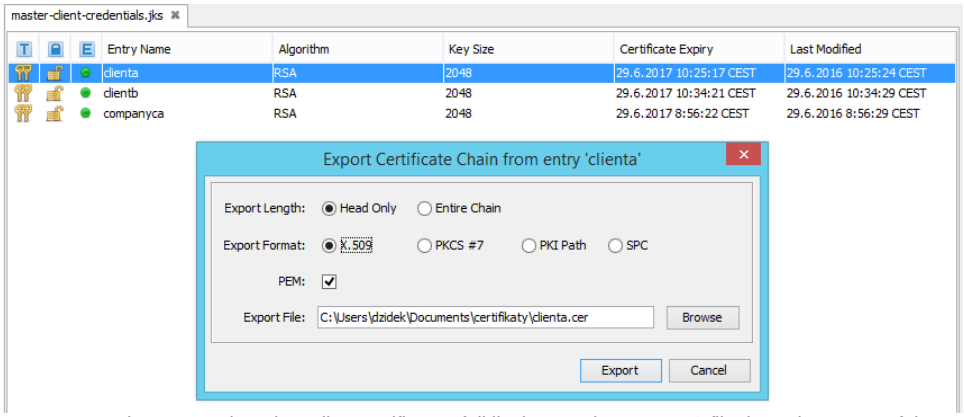
6. To authenticate that the client KeyPair is signed by *companyca* authority, we right-click on *ClientaA*a and choose from the menu View Details and Certificate Chain Details. We can see in the given window that the owner is the *companyca* authority.



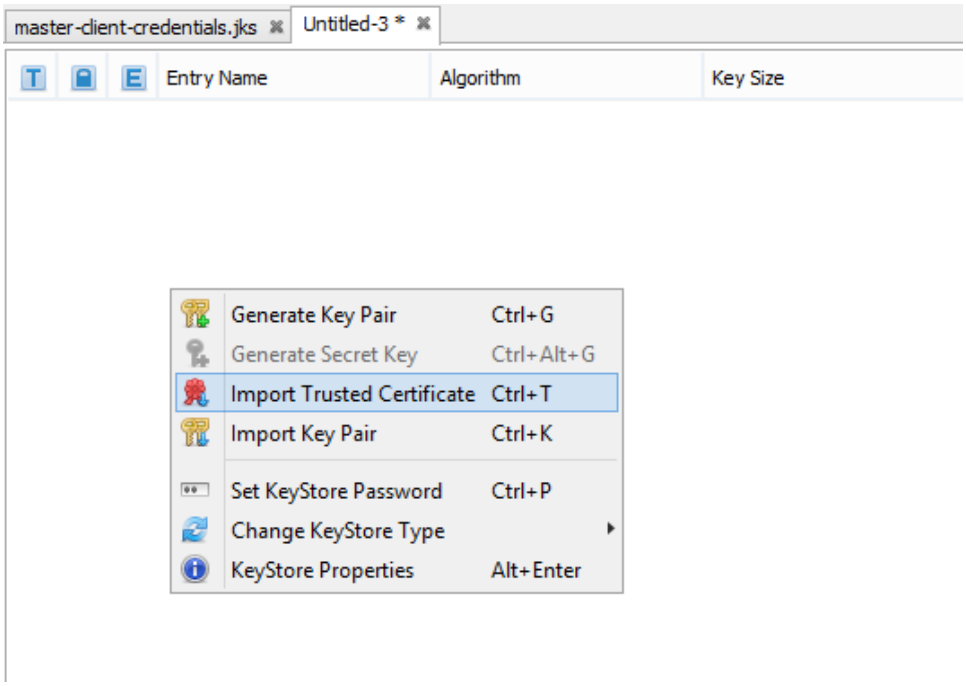
7. From the master-client-credentials.jks file, client certificates are exported and *companyca* into files clientcertificates-full.jks, client-certificates-d2ws.jks, client-certificates-d2000.jks (They are located on servers and contain public keys). Certificates od individual clients and *companyca* are exported by clicking on a client or else on *companyca* and by clicking Export and Export Certificate Chain.

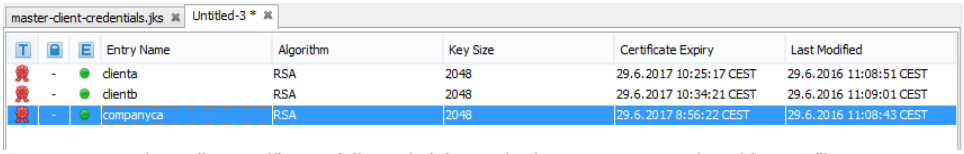


8. When exporting, we leave the settings or adjust the path where the certificate should be stored and click the export.

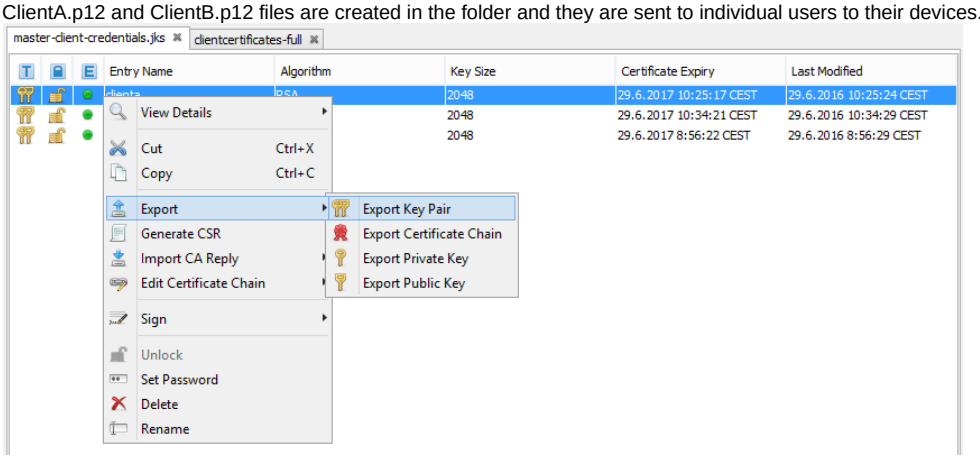


9. When all certificates are exported, we store them into clientcertificates-full.jks by creating new JKS file through a menu of the program KeyStore File > New and choose the JKS type. Here we import certificates by right-clicking and choose Import Trusted Certificate and the certificate which we want to import.



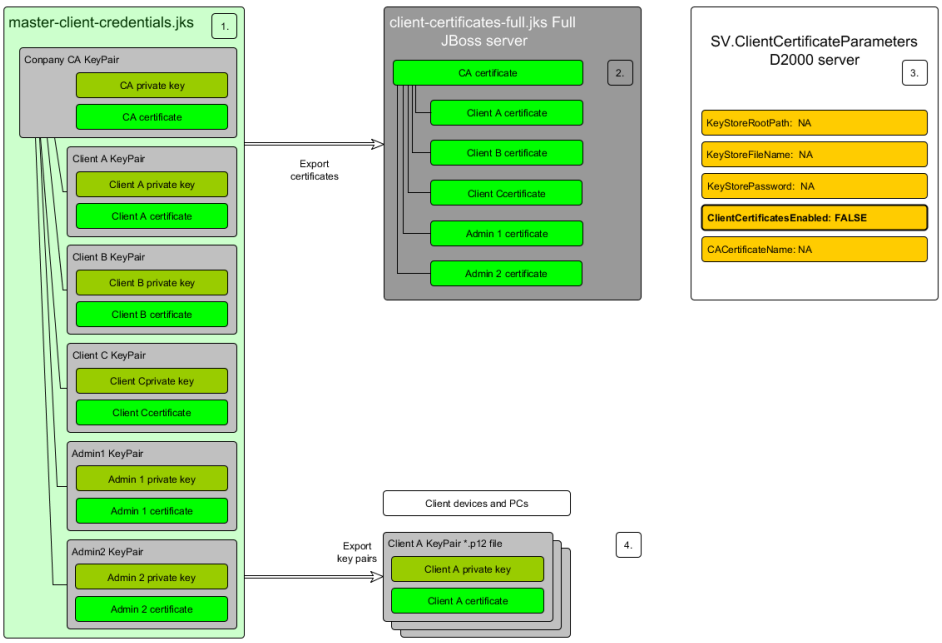


10. After importing KeyStore, we store it as clientcertificates-full. Again it is required to set a password on this JKS file.
    We store the clientcertificates-full.jks file on a particular server where it is required.
11. From the master-client-credentials.jks file, key-pairs of clients are exported in the *.p12 format (they contain public and private keysit is given to customers on devices - PC, Tablet ...). We export in the master-client-credentials.jks file where we right-click on individual clients and click Export > Export Key Pair. ClientA.p12 and ClientB.p12 files are created in the folder and they are sent to individual users to their devices.



Administration of Client Certificates

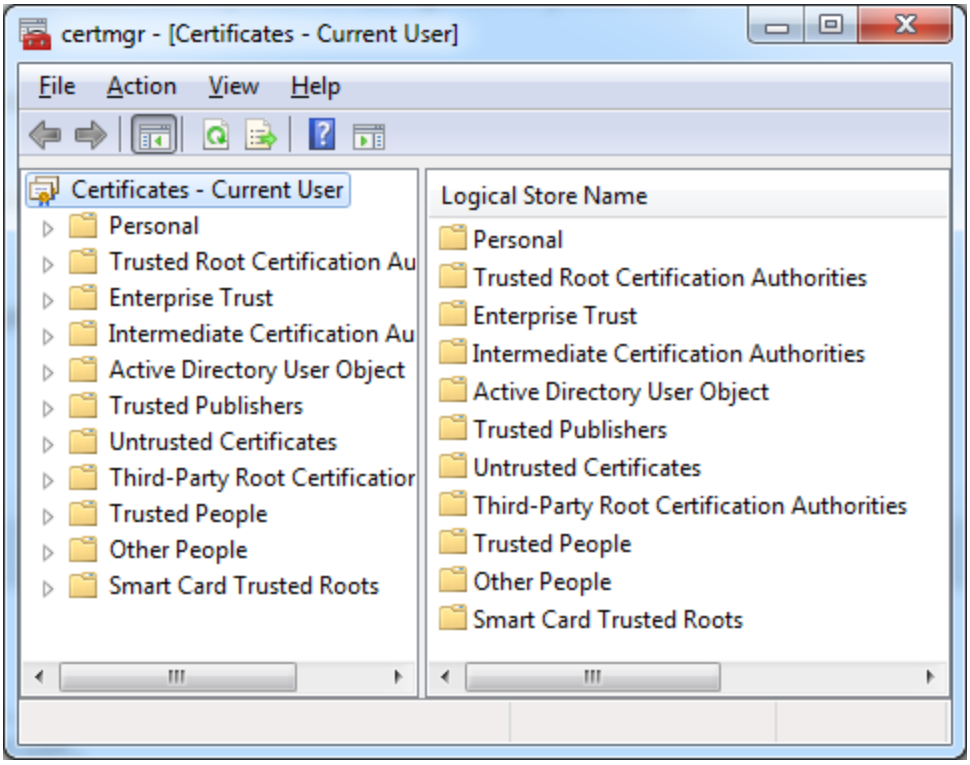
1. The master-client-credentials.jks keystore contains master companyca key-pair and by them signed client key-pairs.
2. Client certificates for clients of the Smart Web application and *companyca* certificate must be exported to the client-certificates-full.jks file that must be accessible for reading for jvm process in which the WildFly AS runs.
3. Client certificates and private keys must be exported from the master-client-credentials.jks file in the *.p12 file.



Installation of Client Certificate

Microsoft Windows 7/8/10 – desktop PC

To import client certificates, it is suitable to use the certmgr.msc application that is standardly a part of OS Windows. It is necessary to choose the folder “Personal” and select action import for the relevant *.p12 key-pair.



Android

The client *.p12 key-pair must be stored in the directory “Downloads” and imported through system settings.

iOS

The client *.p12 key-pair must be sent in an attachment of a mail to the client device and imported through system settings.