# **Administration of Clients' Certificates**

- Process of Generating Client Certificates
  - Administration of Client Certificates
  - Installation of Client Certificate
    - Microsoft Windows 7/8/10 desktop PC
    - Android

٠

° iOS

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!

			New KeyStore Type
Key	Store Explo	Select the type of the new KeyStore:	
(	Quick Start	○ JCEKS	
			● JKS
			O PKCS #12
Create a	Open an	Open the	O BKS-V1
new KeyStore	existing ReyStore	Default ReyStore	⊖ BKS
	Q	2	
Open the CA	Examine a	Show the	OK Cancel
Certificates Reystore	Ceruncate	neip Pages	Cancer

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

-												
	File Edit View Tools Examine Help											
	🗋 🚔 🖶 🛧 🔺 🔝 📲 🐕 윢 🥐 🏧 📵 🔯 🔯 🚱											
	Untit	led-2 *	x									
	Τ		E	Entry Name	Algorithm	Key Size		Certificate	Expiry	Last Modified		
						9	Generate Key F	air	Ctrl+G	]		
						6	Generate Secre	t Kev	Ctrl+Alt+G			
						9	Import Trusted	l Certificate	Ctrl+T			
						9	Import Key Pai	r	Ctrl+K			
							Cat Kau Chana D		Chillin D			
							Set KeyStore P	assword	Ctri+P			
							Change KeySto	ore type	All			
						<u>(</u>	Keystore Prop	erties	Ait+Enter			

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.

	Generate Key Pair Certificate	Name ×
Version: Signature Algorithm: Validity Period: Serial Number: Name:	Oversion 1     Oversion 3       SHA-256 with RSA        1     Year(s)       1467117905       Add Extensions       OK	Common Name (CN): Organization Unit (OU): Organization Name (O): Locality Name (L): State Name (ST): Country (C): Email (E):
		UK Calice

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.

Ι		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
8	<b>f</b>	۲	companyca	RSA	2048	29.6.2017 8:56:22 CEST	29.6.2016 8:56:29 CEST
						-	
				Set Ke	eyStore Password	×	
				Enter New Passv	word: ••••		
				Confirm New Passy	word:		
					OK Cancel		
					Curren		

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*.

T		E	Entry Na	ime	Algorithm	Key Size
R	ſ	0	company Q	view Details	Den 🕨	2048
				Cut Copy Export Generate CSR Import CA Reply	Ctrl+X Ctrl+C	
				Sign	•	Sign New Key Pair
				Unlock		Sign CSR
				Set Password		Sign JAR
			X	X Delete		
		💭 Rename				

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.

	Certificate Details for Entry clienta
Certificate Hierarchy:	
n companyca	
Version:	3
Subject:	CN=ClientA
Issuer:	CN=companyca
Serial Number:	0x577385E2
Valid From:	29.6.2016 10:25:17 CEST
Valid Until:	29.6.2017 10:25:17 CEST
Public Key:	RSA 2048 bits
Signature Algorithm:	SHA256WITHRSA
Fingerprint:	SHA-1 V 62:17:9F:B9:20:E9:F8:6C:E1:65:C4:CE:FC:20:3F
	Export Extensions PEM ASN.1
	ОК

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.

Τ		E	Entry N	ame	Algorithm			Key Size	Certificate Expiry	Last Modified
8	ſ	0	dienta		RSA			2048	29.6.2017 10:25:17 CEST	29.6.2016 10:25:24 CEST
ĩ	il i		dientb	Q	View Details	•		2048	29.6.2017 10:34:21 CEST	29.6.2016 10:34:29 CEST
п			company	$\ge$	Cut Ctrl+	·x		2048	29.0.2017 8:56:22 CEST	29.0.2010 0:50:29 CEST
				<u>r</u>	Copy Ctrl+	·C				
				1	Export	•	m Expor	t Key Pair		
				F	Generate CSR		👮 Expor	t Certificate Chain		
				*	Import CA Reply		P Expor	t Private Key		
				9	Edit Certificate Chain		P Expor	t Public Key		
				, <b>/</b>	Sign	•				
				лÊ.	Unlock					
					Set Password					
				X	Delete					
				Ť	Rename					

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

master-client-credentials.jks 🕷										
Ι		E	Entry Name	Algorith	hm Key Size		Certificate Expiry		Last Modified	
1	<b>f</b>	۲	dienta	RSA		2048		29.6.2017 10:25:1	7 CEST	29.6.2016 10:25:24 CEST
8	e f	۲	dientb	RSA		2048		29.6.2017 10:34:2	1 CEST	29.6.2016 10:34:29 CEST
R	n f	۲	companyca	RSA		2048		29.6.2017 8:56:22	CEST	29.6.2016 8:56:29 CEST
				Export Length: Export Format: PEM: Export File:	Export Certif	ficate Chain fi Dentre Chain PKCS #7 Documents\certifik	OPKI Path	o spc Brows	2	
								Export Cano	el	

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.



master-cient-credentials.jks x Untitled-3 * x											
Ι		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified				
费	-	۲	dienta	RSA	2048	29.6.2017 10:25:17 CEST	29.6.2016 11:08:51 CEST				
党	-	۲	dientb	RSA	2048	29.6.2017 10:34:21 CEST	29.6.2016 11:09:01 CEST				
党	-		companyca	RSA	2048	29.6.2017 8:56:22 CEST	29.6.2016 11:08:43 CEST				

- 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.
- 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.