Správa klientských certifikátov

- Postup generovania klientských certifikátov
- Správa klientskych certifikátov
 Ipštalácia klientskeho certifikát
 - Inštalácia klientskeho certifikátu
 - Microsoft Windows 7/8/10 desktop PC
 - Android
 - ° iOS

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-clientcredentials.jks sa nikdy neexportuje privátny kú companyca !!!

			New KeyStore Type
Key	Store Exploi	rer	Select the type of the new KeyStore:
	Quick Start	⊖ JCEKS	
			() KS
			O PKCS #12
Create a	Open an	Open the	O BKS-V1
new Reystore	existing Reystore	Default ReyStore	⊖ BKS
	Q	2	
Open the CA	Examine a	Show the Help Pages	OK Cancel

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

Fil	File Edit View Tools Examine Help										
	〕 🖴 🖬 🖴 オ 米 腌 🎆 🐕 🎗 🌹 🚥 📵 🔄 🔟 😡										
U	ntitle	ed-2 *	×								
	T		E	Entry Name	Algorithm	Key Size		Certificate	Expiry	Last Mod	lified
						-				-	
						1	2	Generate Key Pair	Ctrl+G		
						9	2	Generate Secret Key	Ctrl+Alt+G		
						9		Import Trusted Certificate	Ctrl+T		
						1	2	Import Key Pair	Ctrl+K		
							•	Set KeyStore Password	Ctrl+P		
							2	Change KeyStore Type	,		
								KeyStore Properties	Alt+Enter		

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.

Version: Version 1 Version 3 Signature Algorithm: SHA-256 with RSA Organization Unit (OU): Validity Period: 1 Year(s) Organization Name (O): Serial Number: 1467117905 Locality Name (J): Item of the series of t	Generate Key Pair Certificate	Name
	Version : Version 1 Version 3 Signature Algorithm: SHA-256 with RSA v Validity Period: 1 Version 3 Serial Number: 1467117905 Name: Add Extensions OK Cancel	Common Name (CN):

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.

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
8	f	0	companyca	RSA	2048	29.6.2017 8:56:22 CEST	29.6.2016 8:56:29 CEST
				Set Ke	eyStore Password	×	
				Enter New Pass	word:		
				Confirm New Pass	word: •••••		
					OK Cancel		
					OK Cancel		

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*.

	E	Entry Nar	ne	Algorithm	Key	ize	Certificate Expiry
7 🖆	۲	company/c	a	DCV	2048		29.6.2017 8:56:22 CEST
		9	View Details	•			
		\approx	Cut	Ctrl+X			
			Copy Ctrl+				
		1	Export	+			
			Generate CSR				
		*	Import CA Reply	•			
		~	Edit Certificate Ch	ain 🕨			
		-	Sign	•	📅 Sign New Key I	air	
		-6			🧾 Sign CSR		
			Set Password		👰 Sign JAR		
		×	Delete		🦻 Sign MIDlet		
		Ť	Rename				

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.

	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. 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.

		E	Entry N	Entry Name		Algorithm		Key Size	Key Size		Last Modified
8	f	0	dienta		RSA	RSA		2048	2048		29.6.2016 10:25:24 CEST
17	ı fi	۲	dientb	Q	View Details	+		2048		29.6.2017 10:34:21 CEST	29.6.2016 10:34:29 CEST
17	ı 🗈	۲	company	6.4	-			2048		29.6.2017 8:56:22 CEST	29.6.2016 8:56:29 CEST
				X	Cut	Ctrl+X					
				0	Сору	Ctrl+C					
				1	Export	•	77 E	Export Key Pair			
				F	Generate CSR		👷 E	Export Certificate Chain			
				*	Import CA Reply	1	📍 E	Export Private Key			
				9	Edit Certificate Chair	n 1	7 E	Export Public Key			
				7	Sign	+					
				лÊ.	Unlock						
					Set Password						
				X	Delete						
				Ť	Rename						

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

mast	er-clie	nt-cre	edentials.jks 🕷								
Ι		E	Entry Name	Algor	ithm	hm Key Size		Certificate	Expiry	Last Modified	
17	f	۲	dienta	RSA		2048		29.6.2017	10:25:17 CEST	29.6.2016 10:25:24 CEST	
1	n f	۲	dientb	RSA		2048		29.6.2017	10:34:21 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 Certi Head Only K.509 C: \Users\dzidek	ificate Chain f O Entire Chain O PKCS #7 Pocuments \certifik	rom entry 'cl O PKI Path (aty\dienta.cer	ienta'	Browse		
								Export	Cancel		

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.



master-client-credentials.jks 🕱 Untitled-3 * 🕷									
Τ		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		
2	-		companyca	RSA	2048	29.6.2017 8:56:22 CEST	29.6.2016 11:08:43 CEST		

- 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.
- 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.