

This is a step-by-step introduction in how to create a client-certificate keystore in Java environment. In this document we use KeyStore explorer software that is free and available for download for several operating systems.

# 1 Basic Setup

Download and install free KeyStore Explorer software from <a href="https://keystore-explorer.org/">https://keystore-explorer.org/</a>

KeyStore Explorer is far more user-friendly that Java's command line Keytool.

# 2 Generating Private Key and Keystore

Open KeyStore Explorer and select "Create a new KeyStore" (or File->New). New KeyStore Type should be **JKS**.

۸	KeyStore Explo	rer 5.4.1														-	×
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>T</u> o	ols E <u>x</u> amine <u>H</u> e	elp														
	New	Ctrl+N	17	<u>ß</u> 1	l 11	1.000	0	d I	<u>i</u> (	Q	2						
	<u>O</u> pen	Ctrl+O															
<b>1</b>	Ogen Special	>															
	<u>C</u> lose	Ctrl+W															
	Close All	Ctrl+Shift+W															
	Save	Ctrl+S															
14	Save <u>A</u> s	Ctrl+Alt+S										Chave F					
10	Sav <u>e</u> All	Ctrl+Shift+S								P	ley		xpio	rer			
0	<u>R</u> ecent Files	>									(	QUICK S	tart				
	E <u>x</u> it	Alt+F4															
								Cr new l	eate KeyS	a itore		Open a existing Ke	n /Store	Open the Default KeySto	pre		
												Q		?			
							Ce	Ope ertifica	n the tes K	e CA CeySt	ore	Examine Certifica	e a ite	Show the Help Pages	5		
Creek	ta a naw KauCta																
Grea	te a new Keysto	e															

Generate a new key pair. This selection is available if you right-click the window or from the Tools menu (in version 5.4). Use the default values (Algorithm: RSA, Key Size: 2048).



Generate Key	/ Pair	×
Algorithm S	election	
● RSA	Key Size:	2 048 ≑
<u>D</u> SA	Key Size;	2 048 🜲
OEC	Set:	ANSI X9.62 🗸 🗸
	Named Curve:	c2tnb191v1 $\sim$
	Oł	Cancel

Version:	O Version 1 Nersion 3	
Signature Algorithmu		
Signature Algorithm.		
Validity Start:	18.11.2019 12:26:44 EET	
Validity Period:	2 🜩 Year(s) 🗸 Apply	
Validity End:	17.11.2020 12:26:44 EET	
Serial Number:	1574072804	
Name:		
		Add Extensions

Select the following values from the next dialog:

- Version: Version 3
- Signature Algorithm: SHA-256 with RSA
- Validity Period: 2
- Click the button next to Name to open another dialog.

lame					×
Common Name (CN):	~	MyOrg_name_1	+	-	^
Organization Unit (OU):	$\sim$	MyOrg unit name	+	-	
Organization Name (O):	$\sim$	MyOrganization	+	-	
Locality Name (L):	~	Helsinki	+	-	
State Name (ST):	~	Uusimaa	+	-	
Country (C):	$\sim$	FI	+	-	~
				Re	set
			OK	Cance	I

Fill in the details. Common Name (CN) should be distinguishable among all other certificates (in Finland). Use only ASCII characters in all fields.

Click OK, then OK again.

KeyStore Explorer suggests an alias for the key pair, leave it unmodified.



	New Key Pair Entry Password X
New Key Pair Entry Alias X Enter Alias: MyOrg_name_1	Enter New Password: ••••••• Confirm New Password: ••••••
OK Cancel	OK Cancel

Enter password for private key and <u>store it in a safe place!</u> You will need this password later and if you lose it, your private key is unusable. This password protects your private key and you must not give it or send it to any outside partner in any case.

Save your Keystore using File->Save. You'll be asked for password for keystore file itself. This password should be the same as your key pair's password from last step. It can also be different, but to make sure that your Java implementation is able to use keystore file and key pair properly, use same password. <u>Store password in safe place!</u>

Save KeyStore As × > Työkansiot > projektit > Testi م 1 Uusi kansio **I**EE 👻 Järjestä 🔻 ? Muokkauspäivä 📮 Tämä tietokone \land Nimi Tila Туур 🧊 3D-objektit Hakuehtoja täyttäviä kohteita ei löytynyt. Kuvat 👆 Ladatut tiedost 💧 Musiikki 🔮 Tiedostot 🔜 Työpöytä 🚦 Videot × < MyOrg.jks Tiedostonimi: Muoto: All Files (\*.\*) T<u>a</u>llenna Peruuta Piilota kansiot

Enter a name for your keystore and use file extension .jks

Now you have a Java Keystore containing a private key. Next we need to acquire a signed certificate.



# 3 Certificate Signing Request

Next thing we need is a signed client certificate. We start by creating a certificate request using your private key. This will be then signed by the certificate authority.

Right-click your private key and select -Generate CSR' from the context menu.

A MyOrg.jks - KeyStore Explorer 5.4	1					-	×
<u>File Edit View Tools Examine Help</u>	0						
🗋 🚔 🗮 🐟 🏞 🔉 🛅	🏗 🐍 党 🏗 🚥 🕕	000	3				
MyOrg.jks 🕷							
T E Entry Name			Algorithm	Key Size	Certificate Expiry	Last Modified	
₩ <mark>1 0 myorg_name_1</mark>	View Details	>	RSA	2048	17.11.2020 12:26:44 EET	18.11.2019 12:40:09 EET	
>	Cut	Ctrl+X					
l C	Сору	Ctrl+C					
4	Export	>					
	Generate CSR						
	Import CA Reply	>					
9	Edit Certificate Chain	>					
2005	🖉 Sign	>					
	Unlock						
	Set Password						
2	Delete						
Ĭ	Rename						
Generate a Certificate Signing Request (C	SR) for the Key Pair entry as	PKCS #10 or SPKA	IC.				
senerate a der andate bigning recidest (e	and the network of the cities us	1.100 // 20 01 01 01		@ 1.0			 _

Use the following values:

- PKSC #10
- Signature Algorithm: SHA-256 with RSA
- Challenge: empty
- CSR File: name ending in \_request followed by a number if you're creating multiple requests from multiple private keys. File extension .csr

Generate CSR		$\times$
Format:	● PKCS #10 ○ SPKAC	
Signature Algorithm:	SHA-256 with RSA 🗸 🗸	
Distinguished Name (DN)	CN=MyOrg_name_1,OU=MyOrg unit name,O=MyOrganization,L=I	
Challenge:		
Optional Company Name:		
Extensions:	Add certificate extensions to request	
CSR File:	\Users\03073143\Work Folders\projektit\Testi\myorg_name_1.csr	
	OK Cancel	



Now you have created the certificate signing request using your private key. Send the file (myorg\_name\_1\_request.csr) to the designated contact person along with user rights application. <u>Never</u> <u>send your keystore file or any password to anyone!</u>

# 4 Combining Signed Certificate with Private Key

After receiving the signed certificate from the certificate authority you must combine it with your private key. The certificate may have one of several file extensions, for example: .cer, .p7r, .pem or .der. The Finnish Food Authority supplies a .cer file along with two CA certificates.

Open the Keystore, right-click the private key and select 'Import CA Reply' from the context menu.



Select the signed certificate (myorg\_name\_1\_request.cer) and click ok.

KeyStore Explorer will confirm that the import was successful. This does not indicate that the certificate chain is in order and it should be checked.





Open the context menu once again by right-clicking the key. Select View Details -> Certificate Chain Details.

MyOrg.jks * - KeyStore Exp File Edit View Iools Examin   □ </th <th>lorer : ie <u>H</u>e</th> <th>5.4.1 Ip 🌃 🐍 🎗 🏗 🚥</th> <th>•</th> <th></th> <th>0</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>-</th> <th>×</th>	lorer : ie <u>H</u> e	5.4.1 Ip 🌃 🐍 🎗 🏗 🚥	•		0						-	×
T E Entry Name						Algorithm	Key S	ize	Certificate Expiry	Last Modified		
W myorg_name_1	Q	View Details	:	*	Certifi	cate Chain Det	ails		22.11.2021 10:29:37 EET	20.11.2019 11:44:39	EET	
	*	Cut Copy	Ctrl+X Ctrl+C	7	Private Public	Private Key Details Public Key Details						
	<b>*</b>	Export Generate CSR Import CA Reply	:	>								
	<ul><li>Edit Certificate Chai</li><li>Sign</li></ul>	Edit Certificate Chain Sign	:	> >								
	1111 1111 1111 1111 1111 1111	Unlock Set Password Delete Rename										

If the Certificate Hierarchy tree contains only the newly acquired certificate, you need to construct the certificate chain by hand.

Certificate Details for E	ntry 'myorg_name_1'	Х
Certificate Hierarchy:		
👮 MyOrg_name_1		
Version:	3	
Subject:	O=MyOrganization,OU=MyOrg unit name,C=FI,CN=MyOrg_name.	
Issuer:	E=administrator@mmm.fi,CN=MMM TESTI Intermediate CA 2018,C	
Serial Number:	0x2591F1B7C	
Valid From:	20.11.2019 10:29:37 EET	
Valid Until:	22.11.2021 10:29:37 EET	
Public Key:	RSA 2048 bits	
Signature Algorithm:	SHA256WITHRSA	
Fingerprint:	SHA-1 V 88:1A:12:92:02:02:99:32:26:11:64:E4:94:9A:3E:	
	Export Extensions PEM ASN.1	
	ОК	



From the context menu, select Edit Certificate Chain -> Append Certificate.



Choose the intermediate certificate (mmm\_intermediate\_ca\_2018.cer) first. Confirmation will be displayed. Then repeat the procedure for the root certificate (mmm\_root\_ca\_2018.cer).





Page/pages Guide/version Valid from

Client Certificate Guide

Now the Certificate Hierarchy should display two parent certificates (test certificates shown). This does not guarantee that any software using the keystore trusts the issuer certificates. You may need to add these certificates to a separate trust store. In any case our keystore now contains information about the certificate's issuers.

Certificate Details for I	ntry 'myorg_name_1'	×
Certificate Hierarchy:		
MMM TESTI Root	CA 2018	
MyOrg_na	termédiate CA 2018 ime_1	
Version:	3	
Subject:	E=administrator@mmm.fi,CN=MMM TESTI Root CA 2018,OU=Tietc	
Issuer:	E=administrator@mmm.fi,CN=MMM TESTI Root CA 2018,OU=Tietc	
Serial Number:	0x2EE90041	
Valid From:	11.1.2018 12:24:39 EET	
Valid Until:	11.1.2028 12:24:39 EET	
Public Key:	RSA 4096 bits	
Signature Algorithm:	SHA256WITHRSA	
Fingerprint:	SHA-1 V AF:62:48:72:24:6C:98:26:B5:CA:F7:5A:C0:DE:44	
	Export Extensions PEM ASN.1	
	ОК	

# 5 Exporting key pair to PKCS12 (.p12) format

If you need to have the key pair (private key and signed certificate) as Windows friendly pkcs12-format, it can be done with Keystore Explorer by following steps

Right click key entry in Keystore Explorer. Choose Export -> Export Key pair. Enter password for private key from earlier.

	5.4.1							-	×
<u>File Edit View Tools Examine H</u>	elp								
	🏗 🐕 👧 🏗 📼	0 🛛	0	0					
MyOrg.jks Ж									
🔳 📄 E Entry Name				Algorithm	Key Size	Certificate Expiry	Last Modified		
📅 🖆 🔹 myorg_name_1	🔍 View Details	>		RSA	2048	17.11.2020 12:26:44 EET	18.11.2019 12:40:0	09 EET	
	K Cut	Ctrl+X							
C.	🛅 Сору	Ctrl+C							
2	🟦 Export	>	п Б	oport Key Pair					
1	Generate CSR		<u>я</u> Б	oport Certificate (	Chain				
2	Import CA Reply	2	📍 Б	oport Private Key					
2	P Edit Certificate Cha	in >	Ϋ́́Ð	oport Public Key					
	🖉 Sign	>							
	Unlock								
	Set Password								
	Delete								
đ	Rename								
No. Charle Trans. WC. Cons. 1 andres. Date	h. (C.)(()02072142)(4)		a data tar						
Reystore Type: JKS, Size: 1 entry , Pat	n: c:\users\03073143\W	ork Poiders (pro	ojekůt(l)	esu myorg.jks					



### Enter new passwords for pkcs12 file. Filename extension is p12.

Export Key Pair from Key	Store Entry 'myorg_name_1'	×
Format:	● PKCS#12 ○ PEM	
Password for Output File:	•••••	
Confirm Password:	•••••	
Export File:	Work Folders\projektit\Testi\myorg_name_1.p12	Browse
	Export	Cancel

You'll be notified if exporting was successful.

Export Key Pair		×
i	Export Key Pair Successful.	
	ОК	

Now you have a file named myorg\_name\_1.p12. It contains key pair in pkcs12-format. It can be installed to Windows' certificate management by opening the file and following the instructions.