# Skapa certifikat till ARX

Instruktion för att skapa och signera certifikat för säker webbanslutning till ARX

ASSA ABLOY Opening Solutions

The global leader in door opening solutions

UG905342A

and b

#### Teknisk dokumentation och support

Vi förbehåller oss rätten att korrigera eventuella tryckfel och uppdatera informationen efter utskrift. På hemsidan finns utförliga manualer tillgängliga för ARX passersystem.

Om du inte hittar svar på dina frågor i manualen hänvisar vi till ASSAs tekniska support, de nås på +46 (0)8 775 16 60 alternativt: technical.arx@assaabloy.com

ASSA ABLOY Opening Solutions Sweden AB Förmansvägen 11 SE-117 43 Stockholm Sweden

Phone: +46 (0)8-775 16 00 Fax: +46 (0)8-775 16 20

# Innehållsförteckning

Generera och signera ett certifikat för ARX	4
Generering av Java Keystore och ett självsignerat certifikat	5
Generera en CSR (certifikat-signeringsförfrågan från certifikat)	10
Importera det signerade SSL-certifikatet	12
A. Importera SSL-certifikat (.p7b-fil)	13
B. Importera SSL Certitfikat (.crt-filer)	16
Konfigurera ARX för att använda din nya JavaKeystore	25
Generera manuellt via Keytool-kommandon	
Generera en Javakeystore-fil	
Generera en "Certificate Signing Request"	
Importera CSR Response-filerna	

# Generera och signera ett certifikat för ARX

I det här kapitlet förklarar vi hur man skapar, signerar och lägger in ett betrott certifikat i ARX som gör att man kan komma åt olika funktioner i ARX via en webbläsare eller en integration på ett säkert sätt, utan att få certifikatvarningar (SSL / https).



#### VIKTIGT

Den här guiden kommer att innehålla grafiska stegvisa instruktioner om hur du kommer igång, men du som användare förväntas använda programmet KeyStoreExplorer.

Du kan också använda keytoolen som ingår i Java JDK, men vi rekommenderar endast mycket avancerade användare att göra det manuellt. Vi kan inte garantera att du bara kan följa denna guide blint när du skriver kommandon i din terminal.

För att ladda ner programmet, gå till: https://keystore-explorer.org/downloads.html och installera den rätta releasen för din OS-distribution

KeyStore Explorer News Features Specifications Screenshots Release Notes Downloads Contribute License

# Downloads

Getting up and running with KeyStore Explorer is quick and easy. There are packages for all common operating systems.

#### Latest Release

Platform	File	Details
Windows	kse-541-setup.exe	The Windows installer requires Administrator privileges. Parameters: /S for silent install, /D= to specify the installation directory and /AllUsers to install for all users instead of only for the current user
Mac	kse-541.dmg	Double-click the disk image to mount it, then drag KeyStore Explorer to your Applications folder.
Linux	kse_5.4.1_all.deb	DEB for Ubuntu/Debian/Mint etc.
Linux	kse-5.4.1.noarch.rpm	RPM for CentOS/RHEL/Fedora etc.
All	kse-541.zip	ZIP with kse.exe for Windows and kse.sh for Linux/macOS, see included readme.txt for more infos.

#### Older Releases and Source Code

The source code of KeyStore Explorer and older releases since v5.0 are available here: KSE Releases on GitHub

#### Download Java Runtime Environment

Oracle Java Runtime Environment (JRE) Version 8 or above is required to run KSE. The latest JRE can be downloaded for free via the button below:



Copyright 2004 - 2013 Wayne Grant, 2013 - 2018 Kai Kramer

# Generering av Java Keystore och ett självsignerat certifikat

När Keystore Explorer installeras och startas behöver du skapa en keystore.

#### Steg 1

A KeyStore Explorer 5.4.1									
File Edit View Tools Examine Help									
□ 🚔 🖩 ち ♂ 🗡 聖 慶 宿 なえ行	? 0 🖻 🛍 🧕	0							
	Ke	yStore Explore Quick Start	er						
	Create a new KeyStore	Open an existing KeyStore	Open the Default KeyStore						
	È	Q	()						
	Open the CA Certificates KeyStore	Examine a Certificate	Show the Help Pages						
No KeyStore Loaded									

Klicka på den markerade knappen för att börja skapa en ny Keystore



Välj JKS Keystore-typen och tryck på OK

🎊 Untitled-1 * - KeyStore Explorer 5.4.1				
File Edit View Tools Examine Help				
🗋 🖴 🗀 🗶 🐚 📓 🎇 🐕 🏶 🔟 🙆 🧕	0			
Untitled-1 * ×				
1 🔳 🔳 Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
Set KeyStore Pass Enter New Pass Confirm New Pass	sword sword: secr	et	Cancel	

Spara JKS-filen du just skapat, lösenordet måste sättas till secret



ARX.YOURDOMAIN.COM - KeyStore Explorer 5.4.1								
File Edit View Tools Examine Help								
🗋 🗁 🔳 (👟 /	R	Generate Key Pair	Ctrl+G					
ARX.YOURDOMA	9. 9. 91	Generate Secret Key Import Trusted Certificate Import Key Pair	Ctrl+Alt+G Ctrl+T Ctrl+K	n	Key Size	Certificate Expiry	Last Modified	
	••	Set KeyStore Password Change KeyStore Type KeyStore Properties	Ctrl+P Alt+Enter	Þ				
		Preferences	Ctrl+Kommatecken					
Generate a Key Pa	ir wi	th a self-signed certificate in the	active KeyStore					

Nu när du har sparat JKS-filen, gå till Tools -> Generate Key Pair

ARX.YOURDOMAIN.COM - KeyStore Explo	rer 5.4.1		
File Edit View Tools Examine Help			
🗋 🚔 🖩 i 🗢 🏕 i 🛪 🐚 💼 i 🏗 🐕 📆 🖷	• 0   0 🗓 0   0		
ARX.YOURDOMAIN.COM *	Generate Key Pair	<b>]</b>	
T E Entry Name		e Expiry	Last Modified
	Algorithm Selection		
	RSA Key Size: 2 048      ✓		
	◯ DSA Key Size: 2 048 🛓		
	◯ EC Set: ANSI X9.62 ▼		
	Named Curve: c2tnb191v1 💌		
	ОК Сапсе		
KeyStore Type: JKS, Size: no entries , Path: 'C:\jobt	\temp_dec\cert_Manual\ARX.YOURDOMAIN.COM'		

Alrogitmen måste vara **RSA** och nyckelstorlek ska vara **2048**, när detta är inställt trycker du på **OK** 

#### Steg 6

ARX.YOURDOMAIN.C	OM - KeyStore Explor	er 5.4.1	
File Edit View Tools E	Generate Key Pair Ce	rtificate 🔀	
ARX.YOURDOMAIN.COM *	Version	Version 3	
T 🖻 E Entry Name	Signature Algorithm:	SHA-256 with RSA 🔹	ast Modified
	Validity Start:	2018-12-19 08:09:33 CET	
	Validity Period:	2 → Year(s) ▼ Apply	
	Validity End:	2020-12-19 08:09:33 CET	
	Serial Number:	1545203373	
	Name:		
		Add Extensions	
		OK Cancel	
KeyStore Type: JKS, Size: no	o entries , Path: 'C:\jobb\	temp_dec\cert_Manual\ARX.YOURDOMAIN.COM'	

Se till att du använder **Version 3** och ange giltighetsperioden för certifikatet till minst **ett år**. Kom ihåg att trycka på **Apply** för att spara din valideringsperiod

När instruktionerna ovan är gjorda trycker du på den markerade knappen (ovanför knappen "Add extensions").

ARX.YOURDOMAIN.COM - KevStore Explorer 5.4.1
File Edit View T Name
ARX.YOURDOMAIN Common Name (CN):  ARX.YOURDOMAIN.COM +
Image: Companization Unit (OU):     Image: Height of the second sec
Organization Name (O): VOUR COMPANY NAME +
Locality Name (L):  + -
State Name (ST): + -
Country (C):
Reset

KeyStore Type: JKS, Size: no entries , Path: 'C:\jobb\temp\_dec\cert\_Manual\ARX.YOURDOMAIN.COM'



#### VIKTIGT

Om du ska använda ett wildcard-SSL-certifikat måste du använda wildcardreferensen i din URL.

I denna bild hänvisar vi till adressen **ARX.YOURDOMAIN.COM**, men om du använder wildcard SSL skulle du behöva skriva \* **.YOURDOMAIN.COM** 

**CN**: krävs. Här anger du din adress (om ARX kommer att vara värd på din adress **arx.yourdomain.com** då är det detta du skriver).

Alla andra fält är valfria, men vi rekommenderar att du anger ett organisationsnamn (**Organization Name**).

ARX.YOURDOMAIN.C	OM - KeyStore Explo	rer 5.4.1	
File Edit View Tools E	Generate Key Pair Ce		
	Senerate Rey Full Co		
ARX.YOURDOMAIN.COM ×	Version:	Version 1 OVersion 3	
🔳 📄 🔳 Entry Name	Signature Algorithm:	SHA-256 with RSA 🔻	st Modified
	Validity Start:	2018-12-19 08:09:33 CET	
	Validity Period:	2 💭 Year(s) ▼ Apply	
	Validity End:	2020-12-19 08:09:33 CET	
	Serial Number:	1545203373	
	Name:	CN=ARX.YOURDOMAIN.COM,O=YOUR COMPANY NAME	
		Add Extensions	
		OK Cancel	
KeyStore Type: JKS, Size: no	o entries , Path: 'C:\jobb'	temp_dec\cert_Manual\ARX.YOURDOMAIN.COM'	

Se till att du kan se CN= innan du trycker på OK

#### Steg 9

ARX.YOURDOMAIN.COM - KeyStore Explorer 5.4.1							
File Edit View Tools Examine Help							
🗋 🖴 🖩   👟 🏕   🗶 🐘 🏙   🎇 🐕 🌻 🐨 📵   🗟 🔯 🤕	0						
ARX.YOURDOMAIN.COM *							
T E Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified			
New Key Pair Entry Alias Enter Alias: ARX.YOURDOMAIN.COM OK Cancel							

Du kan spara ditt certifikat som vad som helst, men för att göra det enklare att navigera i rätt certifikat rekommenderar vi att du namnger det som den webbadress du angav tidigare och tryck **OK**.

ARX.YOURDOMAIN.COM - KeyStore Explorer 5.4.1							
File Edit View Tools Examine Help							
🗋 🚔 🗮 📥 🖈 😹 腌 🏙 🎇 🕺 🎗 🏗 🚥	0 0 0						
ARX.YOURDOMAIN.COM *							
T E Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified			
Image: Text of the second s							
KeyStore Type: JKS, Size: no entries , Path: 'C:\jobb\te	emp_dec\cert_Manual\ARX.YO	URDOMAIN.CO	DM'				

I detta steg krävs det att du anger lösenordet: secret. Avsluta med OK.

ARX.YOURDOMAIN.COM * - KeyStore Explorer 5.4.1							
File Edit View Tools Examine Help							
🗋 🖴 📥 😹 🗅 💼 📅 % 免 📆 📼 📵 🖄 🛍	2 0						
ARX.YOURDOMAIN.COM * *							
I LE Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified			
📅 📑 🔍 arx.yourdomain.com	RSA	2048	2020-12-19 08:09:33 CET	2018-12-19 08:19:11 CET			
KeyStore Type: JKS, Size: 1 entry , Path: 'C:\jobb\temp_dec\cert_Manual\ARX.YOURDOMAIN.COM'							

Spara dina ändringar och nu är ditt självsignerade certifikat skapat!

Du kan enkelt dubbelklicka på certifikatet för att få mer information om det. Nästa steg innan du kan använda certifikatet är att skapa en CSR (Certificate Signing Request)

# Generera en CSR (certifikat-signeringsförfrågan från certifikat)

ARX.YOURDOMAIN.COM - KeyStore	Explorer 5.4.1				- • ×
File Edit View Tools Examine Help					
🗋 🖴 🔳 (🗢 🏕 ) 🔉 🗈 📓 🎇 🐕 🕱	, 🏗 📼 🕕 🚊 🚺	2 0			
ARX.YOURDOMAIN.COM *					
🔳 🔳 🔳 Entry Name		Algorithm	Key Size	Certificate Expiry	Last Modified
₩ e arx.yourdomain.com	<ul> <li>View Details</li> <li>Cut</li> <li>Copy</li> <li>Export</li> <li>Generate CSR</li> <li>Import CA Rei</li> </ul>	Ctrl+ Ctrl+	→ <sup>48</sup> X C →	2020-12-19 08:09:33 CET	2018-12-19 08:19:11 CET
	<ul> <li>Edit Certificat</li> <li>Sign</li> <li>Unlock</li> <li>Set Password</li> <li>Delete</li> <li>Rename</li> </ul>	e Chain	•		

Högerklicka på ditt certifikat och väl Generate CSR

Generate CSR	
Format:	PKCS #10      SPKAC
Signature Algorithm:	SHA-256 with RSA
Distinguished Name (DN)	CN=arx.powerlvl.se,O=Powerlevel,L=Luleå,ST=,C=SE
Challenge:	
Optional Company Name:	
Extensions:	Add certificate extensions to request
CSR File:	C:\certs\server.csr Browse
	OK Cancel

Välj lämplig plats för att spara filen och tryck **OK** 



#### VIKTIGT

Nu när du har skapat din CSR måste du ladda upp den till en SSL-återförsäljare för att göra den signerad och betrodd.

l denna guide har vi två olika exempel A och B. **A** är import från p7b-fil och **B** där du själv skapar kedjan.

Dessa exempel använder filerna som kommer ifrån **Digicert** eller **Comodo** respektive

# Importera det signerade SSL-certifikatet

Vi kommer att förklara två olika sätt att importera SSL-certifikatet till din skapade Java Keystore (som genereras ovan)



#### VARNING

Kom ihåg att innan du kan fortsätta härifrån måste du ha köpt ett SSL-certifikat från en återförsäljare och fått det signerade certifikatet.

# A. Importera SSL-certifikat (.p7b-fil)

.p7b-filer innehåller både certifikat och certifikatkedja, vilket gör att de importeras till Keystore mycket lättare än en .crt-fil

#### Steg 1

<u>}</u> •	KeyStore Explo	rer 5.4.1				
File	Edit View To	ols Examine H	Help			
	New	Ctrl+N	i. s. fi == 0 🖻 🖉 Q	•		
	Open	Ctrl+O				
	Open Special	,				
	Close	Ctrl+W	-			
	Close All	Ctrl+Skift+W				
	Couro	Ctol + C	Ke	eyStore Explore	er	
1	Save As			Quick Start		
a.	Save All	Ctrl+Skift+S		<u>e</u>	<b>—</b>	
0	Recent Files	,	new KeyStore	open an existing KeyStore	Open the Default KeyStore	
	Exit	Alt+F4			ć	
				Q	2	
			Open the CA	Examine a	Show the	
			Certificates ReyStore	Certificate	Help Pages	
No K	eyStore Loaded					

Starta programmet KeyStore Explorer och öppna din tidigare självsignerade certifikatfil (du skickade till SSL-återförsäljaren).

#### Steg 2

ARX.YOURDOMAIN.COM - KeyStore Explorer 5.4	4.1				
File Edit View Tools Examine Help					
🗋 🚔 🖬   🖘 🥕 🖍 🛅 📲 🚏 🕏 🕅 🚥 🕕	🖻 🗖 🧕	0			
ARX.YOURDOMAIN.COM *					
I 🔳 🔳 Entry Name		Algorithm	Key Size	Certificate Expiry	Last Modified
📅 🔒 😐 arx.yourdomain.com 🔍	View Det	tails	•	2020-12-19 08:09:33 CET	2018-12-19 08:19:11 CET
*	Cut		Ctrl+X		
	Сору		Ctrl+C		
<u></u>	Export		•		
[10]	Generate	CSR			
*	Import C	A Reply	•	From File	
	Edit Cert	ificate Chain		From Clipboard	
, all	Sign		+		
	Unlock				
	Set Passv	vord			
×	Delete				
Ĩ.	Rename				
Import a Certificate Authority (CA) Reply into the Key Pair e	entry				

Högerklicka på certifikatet och välj Import CA Reply och välj From file



Välj **p7b-filen** du fick i retur från SSL-återförsäljaren.

Steg 4 (klart)

Certificate Details for Entry 'server'	×
Certificate Hierarchy: DigiCert Global Root CA DigiCert SHA2 Secure Server CA R DigiCert SHA2 Secure Server CA	
Version: 3	
Subject: CN=DigiCert Global Root CA,OU=w	ww.digicert.com,O=DigiCert Inc,C=US
Issuer: CN=DigiCert Global Root CA,OU=w	ww.digicert.com,O=DigiCert Inc,C=US
Serial Number: 0x83BE056904246B1A1756AC95991	LC74A
Valid From: 2006-11-10 01:00:00 CET	
Valid Until: 2031-11-10 01:00:00 CET	
Public Key: RSA 2048 bits	
Signature Algorithm: SHA1WITHRSA	
Fingerprint: SHA-1   A8:98:5D:3A:65:	E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1
	Export Extensions PEM ASN.1
	ОК

Dubbelklicka på ditt certifikat och verifiera att certifikatkedjan ser ut som något liknande det här.

Klicka på certifikatet som ligger längst upp i trädet (vilket har namnet **Root CA** eller liknande) och verifiera att den har samma **Subject** och **Issuer**, Det betyder att det inte finns några fler certifikat att lägga till i kedjan. (Detta är ett certifikat från en betrodd certifikatmyndighet CA).



#### OBSERVERA

Kom ihåg att spara innan du fortsätter



#### VIKTIGT

Nu när du har gjort dessa steg kan du gå till det sista steget: Konfigurera ARX för att använda din nya JavaKeystore [25]

### B. Importera SSL Certitfikat (.crt-filer)

.crt-filer innehåller certifikatet från vilket du kan skapa certifikatkedjan

#### Steg 1



Starta programmet KeyStore Explorer och öppna din tidigare självsignerade certifikatfil (du skickade till SSL-återförsäljaren).

ARX.YOURDOMAIN.COM - KeyStore Explorer 5.4	4.1					
File Edit View Tools Examine Help						
🗋 🚔 🖩 ( 🖘 🏕 ) 🔉 🗈 🛯 🎇 🐕 🕱 📼 🕕	🖻 🗖 🧕	0				
ARX.YOURDOMAIN.COM *						
I 🖻 🗉 Entry Name		Algorithm	Key Size	Certificate Expiry		Last Modified
📅 🔒 😐 arx.yourdomain.com 🔍	View De	tails	•	2020-12-19 08:09:	33 CET	2018-12-19 08:19:11 CET
*	Cut		Ctrl+X			
	Сору		Ctrl+C			
<b>≜</b>	Export		۱.			
	Generate	e CSR			_	
ž	Import C	A Reply	•	From File		
	Edit Cert	ificate Chain	1	From Clipboard		
	Sign		+			
	Unlock					
	Set Pass	vord				
X	Delete					
Ť	Rename					
Import a Certificate Authority (CA) Reply into the Key Pair e	entry					

Högerklicka på certifikatet och välj Import CA Reply och välj From File



Välj crt filen du fick i retur från SSL-återförsäljaren

I det här exemplet har vår fil namnet arx\_powerlvl\_se.crt

Certificate Details for Entry 'server'
Certificate Hierarchy:
R arx.powerW.se
Version: 3
Subject: CN=arx.powerlvl.se,OU=PositiveSSL,OU=Domain Control Validated
Issuer: CN=COMODO RSA Domain Validation Secure Server CA,0=COMODO CA Limi
Serial Number: 0x87CC2850E0B5D05EAEDDDB36D56B9AD4
Valid From: 2018-12-18 01:00:00 CET
Valid Until: 2019-12-19 00:59:59 CET
Public Key: RSA 2048 bits
Signature Algorithm: SHA256WITHRSA
Fingerprint: SHA-1 F2:EA:D0:88:93:38:1F:19:2F:38:51:04:EE:ED:AF:43:83:
Export     Extensions     PEM     ASN.1
ОК

Dubbelklicka på ditt certifikat och kontrollera att utgivaren har uppdaterats.



#### VIKTIGT

Observera att utgivaren i detta fall är **COMODO RSA Domain Validation Secure Server.** Det här är relevant för oss när du väljer nästa certifikat (i nästa steg)

#### Steg 5



Högerklicka på ditt certifikat igen, men välj i det här fallet **Edit Certificate Chain** och välj **Append Certificate** 

Här kommer vi att börja bygga förtroendekedjan, du kommer att se vad det betyder i de senare stegen.



Nu väljer vi certifikatet som har ett liknande namn som den som utfärdade vårt certifikat (se steg 4)



#### VIKTIGT

*Till exempel: Vår utgivare som vi hittat i steg 4 har namnet COMODO RSA Domain Validation Secure Server* 

Så filen vi måste välja i detta fall är COMODORSADomainValidationSecureServerCA.crt

Steg 7

Certificate Details for Entry 'server'
Certificate Hierarchy:
Recomodo RSA Domain Validation Secure Server CA
Version: 3
Subject: CN=COMODO RSA Domain Validation Secure Server CA,O=COMODO CA Limi
Issuer: CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,
Serial Number: CA262EC EAD975366C148A6EDBA37C8C07
Valid From: 2014-02-12 01:00:00 CET
Valid Until: 2029-02-12 00:59:59 CET
Public Key: RSA 2048 bits
Signature Algorithm: SHA384WITHRSA
Fingerprint: SHA-1    33:9C:DD:57:CF:D5:B1:41:16:9B:61:5F:F3:14:28:78:2D:
Export Extensions PEM ASN.1
ОК

Dubbelklicka på ditt certifikat igen, nu ser du att det har fått en trädstruktur (i toppen). Klicka på det nya certifikatet och notera namnet på **utfärdaren (Issuer)** eftersom detta är relevant i nästa steg



Nu väljer vi certifikatet som har ett liknande namn som utfärdaren vi hittade i Steg 7

*i det här fallet var utfärdarens namn* **COMODO RSA Certificate Authority** och vi väljer filen **COMODORSAAddTrustCA.crt** 

Certificate Details for Entry 'server'
Certificate Hierarchy: COMODO RSA Certification Authority COMODO RSA Domain Validation Secure Server CA Composed arx.powerlvl.se
Version: 3
Subject: CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,
Issuer: CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddT
Serial Number: 0x2766EE56EB40 dEABD770A2FC84DE22
Valid From: 2000 05-30 12:48:38 CEST
Valid ontil: 2020-05-30 12:48:38 CEST
Public Key: RSA 4096 bits
Signature Algorithm: SHA384WITHRSA
Fingerprint: SHA-1 <b>•</b> F5:AD:0B:CC:1A:D5:6C:D1:50:72:5B:1C:86:6C:30:AD:92
Export Extensions PEM ASN.1
ОК

Som i Steg 7 dubbelklicka på ditt certifikat och nu har vi ännu ett certifikat i vår förtroendekedja.

Igen notera namnet på utfärdaren, i detta fall AddTrust External CA Root



Först upprepa **Steg 5** att lägga till ett nytt certifikat.

Nu väljer vi certifikatet som har ett liknande namn som utfärdaren vi hittade iSteg 9

I det här fallet var utfärdarens namn AddTrust External CA Root och vi väljer filen AddTrustExternalCARoot.crt

#### Steg 11 (klart)

Certificate Details for Entry 'server'
Certificate Hierarchy:
AddTrust External CA Root
Version: 3
Subject: CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddT
Issuer: CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddT
Serial Number: 0x1
Valid From: 2000-05-30 12:48:38 CEST
Valid Until: 2020-05-30 12:48:38 CEST
Public Key: RSA 2048 bits
Signature Algorithm: SHA1WITHRSA
Fingerprint: SHA-1 • 02:FA:F3:E2:91:43:54:68:60:78:57:69:4D:F5:E4:5B:68:8
Export Extensions PEM ASN.1
ОК

Dubbelklicka på ditt certifikat och verifiera att certifikatkedjan ser ut som något liknande det här.

Klicka på certifikatet som ligger längst upp i trädet (vilket har namnet **Root CA** eller liknande)

Verifiera att den har samma Subject och Issuer

 $\triangle$ 

**OBSERVERA** Kom ihåg att spara innan du fortsätter

#### Konfigurera ARX för att använda din nya JavaKeystore

Om du har lyckats skapa ditt certifikat och din JavaKeystore enligt ovan.

Börja med att hitta din JavaKeystore-fil, i den här guiden har vi kallat filen **ARX.YOURDOMAIN.COM.jks** 

Nu måste vi kopiera den här filen till mappen secrets där ARX är installerad



VIKTIGT

Som standard är ARX installerad i katalogen:

#### C:\Program Files\ASSA\ARX

Nästa steg är nu att redigera filen **system.properties** filen finns i ARX installationskatalog. Leta upp följande textrader och se till att det står "true" på två av raderna och att rätt certifikatfil-namn hamnar på dom andra två raderna. Om någon av textraderna saknas i filen så lägg till dom i slutet av filen.

system.httpsIntegrationServerEnabled=true

system.httpsIntegrationServerJks=ARX.YOURDOMAIN.COM.jks

system.httpsWebServerEnabled=true

system.httpsWebServerJks=ARX.YOURDOMAIN.COM.jks



#### VIKTIGT

Du kan bara använda samma JavaKeystore-fil för integrationsservern och webbservern om de använder samma adress.

# Generera manuellt via Keytool-kommandon

Det här är de kommandon som behövs om du inte vill installera Keystore Explorer-programmet. (Rekommenderas bara för avancerade användare.)



#### VIKTIGT

Se till att du kan använda kommandot keytool i din terminal.

Enklast att verifiera detta är att öppna konsolen och skriva keytool

#### Generera en Javakeystore-fil

Här skapar vi en JavaKeystore-fil liknande den som skapades ovan med programmet KeyStore Explorer

keytool -genkeypair -alias server -keyalg RSA -keysize 2048 -storepass secret keypass secret -keystore **ARX.YOURDOMAIN.COM.jks** -dname "CN=**ARX.YOURDOMAIN.COM**, O=**YOUR COMPANY NAME**, ST=, C=**SE**"

Följande värden måste ändras:

Detta kommando kommer att generera en nyckelkatalogfil som heter ARX.YOURDOMAIN.COM.jks

Certifikatet kommer att ha det gemensamma namnet ARX.YOURDOMAIN.COM

Organisationen i certifikatet skall vara DITT FÖRETAGS NAMN

Det land som certifikatet kommer att innehålla kommer att vara SE vilket är sverige

#### Generera en "Certificate Signing Request"

När du har ditt självsignerade certifikat, då kan du skapa en CSR.

keytool -certreq -alias server -file **ARX.YOURDOMAIN.COM.csr** -storepass secret - keypass secret -keystore **ARX.YOURDOMAIN.COM.jks** 

Filnamnet kan vara vad som helst, i det här fallet var det ARX.YOURDOMAIN.COM.csr

#### Importera CSR Response-filerna

I den här guiden hanterar vi bara två exempel, en är där du har fått en **.p7b** fil och en annan där du fått en **.crt** fil.

#### .p7b fil import

För att lägga till det signerade certifikatet i din keystore:

keytool -import -alias server -file **ARX.YOURDOMAIN.COM.crt** - keystore **ARX.YOURDOMAIN.COM.jks** -storepass secret

#### .crt fil import

Det här kan vara lite knepigt. Först måste du lägga till det signerade certifikatet i din keystore, sen måste du importera rätt filer i rätt ordning.

Vi måste nu först lägga till Root CA-certifikatet och sen ta det en efter en, här är dom kommandon som vi behöver gå igenom för att få vår SSL från återförsäljaren **Comodo** att fungera.

keytool -import -alias RootCert -file **fromComodo\AddTrustExternalCARoot.crt** - keystore ARX.YOURDOMAIN.COM.jks -storepass secret

keytool -import -alias Middle1 -file **fromComodo\COMODORSAAddTrustCA.crt** - keystore ARX.YOURDOMAIN.COM.jks -storepass secret

keytool -import -alias Middle2 -file fromComodo \COMODORSADomainValidationSecureServerCA.crt -keystore ARX.YOURDOMAIN.COM.jks -storepass secret keytool -import -alias **server** -file **fromComodo\ARX.YOURDOMAIN.COM.crt** - keystore ARX.YOURDOMAIN.COM.jks -storepass secret



#### OBSERVERA

Kom ihåg att de olika aliaserna ska vara unika utom i det sista steget där du lägger till ditt signerade SSL-certifikat i din Keystore, det är därför du måste använda **server** alias i sista steget.