BM Tech Convertir PFX o P12 a CER y KEY

Requisito: Tener java instalado

Si no cuenta con java lo puede descargar mediante este enlace: https://www.java.com/es/download/

1. Ingresar al siguiente link y descargar el Keystore Explorer: https://www.bmtech.pe/certs/kse-532-setup.exe



BMTech

👸 KeyStore Explorer 5.3.2	Setup: File Associations	—		×
<u>A</u>	File Associations Select the file types to associate	with KeyStore Ex	oplorer.	
Associated file types:				
🗹 Java KeyStores (*	.ks, *.jks, *.jceks, *.keystore)			
PKCS #12 KeyStor	es (*.pfx, *.p12)			
Bouncy Castle Key	Stores (*.bks, *.uber)			
Copyright 2004 - 2013 Way	ne Grant, 2013 - 2017 Kai Kramer — < Back	Next >	Can	cel

🐞 KeyStore Explorer 5.3.2 S	etup	_		Х
	Choose Install Location Choose the folder in which to install KeySto	ore Expl	orer 5.3.2.	
Choose a directory to insta	ll to:			
Destination Folder C:\Program Files (x86)	(KeyStore Explorer 5.3.2)	Brov	vse	
Space required: 10.6MB Space available: 379.6GB	Curch 2012 2017 Kei Kunnen			
Copyright 2004 - 2013 Wayne	Grant, 2013 - 2017 Kai Kramer	all	Cance	1



2. Abrir el Keystore Explorer 5.3.2



3. Elegimos "Open an existing KeyStore" y seleccionamos el archivo pfx o p12, solicitará ingresar la contraseña

Unlock KeyStore 'cert.pfx'	×
Enter Password:	
OK	Cancel



4. Una vez ingresada, veremos el certificado incluido.

ile]	ert.pf	fx * - ⊻iew	KeyStore Explorer 5.: <u>T</u> ools E <u>x</u> amine <u>H</u>	3.2 elp			- 🗆 X
] [6	4	* × • •	1 🐮 % 死 📆 📼 🕖	0 0		
cert.	pfx *	×					
T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
Ŧ	đ	•	test	RSA	2048	01/02/2019 07:00:00 AM COT	ι.

5. Le damos doble clic, y podemos apreciar la cadena completa de certificados.

ertificate Hierarchy:		
DigiCert Global Roo	bt CA	
RapidSSL RSA	CA 2018	
20		
Margian		
version:		
Subject:	CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert In	e
Issuer:	CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert In	<u>ē</u>
Serial Number:	0x83BE056904246B1A1756AC95991C74A	
Valid From:	09/11/2006 07:00:00 PM COT	
Valid Until:	09/11/2031 07:00:00 PM COT	
Public Key:	RSA 2048 bits	
ignature Algorithm:	SHA1WITHRSA	
Fingerprint:	SHA-256 v 43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44	9
	Export Extensions PEM A	SN.1



Para extraer la llave privada:

Clic derecho > Export > Export Private Key

A cert.pfx * - KeyStore Explorer	5.3.2	
File Edit View Tools Examine	Help 🚯 📆 % 免 🃆 📼 📵 🔯 [ũ Q 0
cert.pfx * #		
T E Entry Name	Algorithm	Key Size Certifi
₩ 🖬 º test	View Details Cut Ctr Copy Ctr	11+X rl+C
	 Export Generate CSR Import CA Reply Edit Certificate Chain 	Y Export Key Pair R Export Certificate Chain Y Export Private Key Y Export Private Key Y Export Public Key
	 ✓ Sign ✓ Unlock ✓ Set Password ✓ Delete ✓ Rename 	>

Export the Kev Pair entry's private kev as PKCS #8. PVK or OpenSSL

Elegir tipo OpenSSL

Select t	he type of private k	ey export required:
OPK	CS #8	
OPU	<	
	enSSL	

En el siguiente panel, se debe elegir la ruta donde se guardará, así como también se elige si la llave privada tendrá una contraseña o no.

Encrypt:		
Encryption Algorithm:	PBE with DES CBC $\qquad \checkmark$	
Encryption Password:		
Confirm Password:		
PEM:		
Export File:	D:\Escritorio\test.key	Browse



Al hacer clic en Export, se mostrará la confirmación.

Export P	rivate Key as OpenSSL	×
i	Export Private Key as OpenSS	L Successful.
	Aceptar	

Para extraer la cadena de certificados:

Clic derecho > Export > Export Certificate Chain



En la siguiente opción elegimos Entire Chain, formato X.509, y seleccionamos la ruta.

Export Length:	◯ <u>H</u> ead Only	• Entire <u>C</u> hain		
Export Format:	<u>۵ ٪.</u> 509	○ PKCS #7	○ P <u>K</u> I Path	
PEM:				
	Dul Facilitaria \ Ch	sin Rundlo 2 set		 Browse



Recibiremos el mensaje de confirmación al presionar Export



Para exportar el certificado del servidor:

Clic derecho > Export > Export Certificate Chain



En la siguiente opción elegimos Head Only, formato X.509, y seleccionamos la ruta.

Export Length:	● <u>H</u> ead Only	O Entire Chain		
Export Format:	<u>۵ ٪.</u> 509	O <u>P</u> KCS #7	○ P <u>K</u> I Path	
PEM:				
Export File:	D:\Escritorio\Se	rverCertificate.crt		Browse



Recibiremos el mensaje de confirmación al presionar Export

Export C	ertificate Chain	×
0	Export Certificate Chain Su	iccessful.
	Aceptar	