Umwandlung einer p12-Datei in PEM-Format

Grundsätzlich empfehlen wir bei einer zertifikatsbasierten Authentifizierung eine P12-Datei zu verwenden!

Wird in den Einstellungen des Authenticators die TLS-Authentisierung Zertifikat PEM-Format gewählt, muss der Private-Key sowie der Client-Key im PEM-Format vorliegen, da es ansonsten zu einer Fehlermeldung führt:

🧯 gematik Authenticator		– – ×
Anmeldung <u>Einstellungen</u>		🛲 gematik
Konnektor-Einstellungen		
Host	IP des Ko	nnektors
Port		
Mandant-ID	\mathbf{X}	
Client-ID		
Arbeitsplatz-ID	Ausgewählte Zertifikatsdatei ist falso	ch
TLS Authentisierung	formatiert.	~
Privater Schlüssel im PEM-Fe	o	AP_CI5_088.pem X
Client-Zertifikat im PEM-Form	at	1
Automatische Updates		
1 Impressum		Version 3.0.1 (release-6)

- Step-by-Step: Umwandlung der p12-Datei
 - 1 Öffnen der p12-Datei im KeyStore Explorer
 - 2 Exportieren des Private Keys
 - 3 Exportieren des Client Zertifikats
 - 4 Überprüfung der exportierten Zertifikate im PEM-Format

Step-by-Step: Umwandlung der p12-Datei

Die p12-Datei ist durch ein Passwort geschützt und enthält zwei Schlüsselpaare (Private-Key und Client-Key). Die p12-Datei kann mit dem Programm Key Store Explorer geöffnet werden, sodass der Private-Key und der Client-Key im PEM-Format aus dem RSA-Schlüsselpaar exportiert werden können. Sollten Sie beispielsweise auch ein EC-Schlüsselpaar erhalten haben, wird dieses hierfür nicht benötigt.

1 Öffnen der p12-Datei im KeyStore Explorer

- Öffnen Sie den KeyStore Explorer (dieser kann hier heruntergeladen werden: KeyStore Explorer)
- Die p12-Datei kann nun einfach per Drag and Drop in den KeyStore Explorer hineingezogen werden, sodass Sie nach einem Passwort gefragt werden
- Geben Sie das benötigte Passwort ein
- Es sollte nun ungefähr so bei Ihnen aussehen:

1	Datei	Bearbeiten Anzeigen Wer	kzeuge Unter	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
		S # X h B 🕯	i i 🕺 📆	••• 📵 📃	<u>i</u>	
rise	.p12 🛎					
Ι		Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
T	<u>_</u>	client-system-x	RSA	2048	22.07.2027, 15:21:12 MESZ	-

2 Exportieren des Private Keys

• Wählen Sie das RSA-Schlüsselpaar:

🍌 Datei Bearbe	eiten Anzeigen Werk:	zeuge Unter	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
🗋 🖴 📾 🖘 🥔 🔉 💼 🏗 🐍 🏚 🏗 🚥 📵 🗟 🔯 🥥 🐵					
rise.p12 🗯					
T E Nam	ne des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
📅 🔒 😐 clien	t-system-x	RSA	2048	22.07.2027, 15:21:12 MESZ	-
		R	SA		

- Nutzen Sie den Rechtsklick, um das Menü aufzurufen
- Klicken Sie auf den Menüpunkt Exportieren und anschließend auf Privaten Schlüssel exportieren:

🍌 Datei Bearbeiten Anzeigen Werkz	zeuge Unters	uchen Hilfe ri	rise.p12 - KeyStore Explore 🗕 🛛 🗙
	1. 🕺 🏗	••• 📵 📃	
rise.p12 🕷			
T E Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats Zuletzt geändert
📅 🔒 😑 client-system-x	RSA	2048	22.07.2007.15:01:10 MES7 Q Details anzeigen →
			Ausschneiden Strg-X
			 Exportieren CSR erstellen Zertifikat verifizieren Zertifikatskette bearbeiten Zertifikatskette bearbeiten Zertifikatskette bearbeiten Signieren Finsperren Passwort festlegen Löschen Umbenennen

- Hinweis: Es kann sein, dass eine erneute Passwort-Abfrage erscheint Geben Sie das gleiche Passwort, wie zuvor ein
 Es öffnet sich ein Dialogfenster, klicken Sie auf OpenSSL und anschließend auf OK

, Datei Bearbeiten Anzeigen W	'erkzeuge Untei	rsuchen Hilfe ri	se.p12 - KeyStore Explore	$ \Box$ \times
🗋 😂 😸 (🖘 🖂 🛍 🗎	17. 1. f. 17	. 🗉 📵 💆	<u>ì</u>	
rise.p12 🕱				
🔳 🔳 🔳 Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
📅 💼 client-system-x	RSA	2048	22.07.2027, 15:21:12 MESZ	-
 Typ zum Ex Für den private PKCS #8 PVK OpenSSL 	port des private Si	chlüssels der Typ des Expo Of	<pre>x rts angegeben werden: Abbrechen</pre>	

- Ein neues Dialogfenster öffnet sich, übernehmen Sie die Einstellungen wie nachfolgend dargestellt
 Klicken Sie anschließend auf Export

*	Datei Bearbeiten Anzeigen	Werkzeuge Unter	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
	🗎 🔚 (🖘 🏓 👗 🛅)	E 77 % A 77	••• 📵 📃	<u>ì</u>	
rise	.p12 🕷				
Ι	E Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
W	🏃 Export des privaten Schlüss	els als OpenSSL aus de	m Schlüsselspeicł	ner »client-system-x«	×
	Verschlüsseln:				
	Verschlüsslungsalgorithmus:	Passwort-basierende	Verschlüsselung ı	mit DES CBC 🗸 🗸	
	Verschlüsselungspasswort:				
	Passwortbestätigung:				
	PEM:				
	Export-Datei:	C:\Users	client_system	ı_x.key	Navigieren
	L			Export	Abbrechen

- Es erscheint ein neues Dialogfenster, welches den erfolgreichen Export bestätigt
 Klicken Sie auf **OK**

🏃 Datei Bearbeiten Anzeigen V	Verkzeuge Unters	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
🗋 🖨 🔚 (🖘 🏕 👗 🖺	17 1. 1. 17	••• 🕕 📃	<u>i</u> Q	
rise.p12 🕷				
🔳 🔳 🔳 Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
📅 💼 client-system-x	RSA	2048	22.07.2027, 15:21:12 MESZ	-
>> Den pri	vaten Schlüssel im G port des privaten So	OpenSSL Format chlüssel als Open	exportieren × SSL war erfolgreich.	

3 Exportieren des Client Zertifikats

• Wählen Sie das RSA-Schlüsselpaar:

\nearrow	Date	ei	Bearbeiten Anzeigen Werk	zeuge Unter	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
			S 🖉 👗 🗈 🖹 🎢	12 f 17	•• 🕦 📃	<u>i</u> Q	
rise	e.p12	×					
Π		E	Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
17	Ĥ	۲	client-system-x	RSA	2048	22.07.2027, 15:21:12 MESZ	-
				R	SA		

- Nutzen Sie den Rechtsklick, um das Menü aufzurufen
- Klicken Sie auf den Menüpunkt Exportieren und anschließend auf Zertifikatskette exportieren:



• Es erscheint ein Dialogfenster, übernehmen Sie die Eingaben wie folgt und klicken Sie anschließend auf Export

*	Datei	Bearbeiten A	Anzeigen Werk	zeuge Unter	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
		628	(là là 📅	16 👧 17	••• 🕕 🚊	<u>í</u>	
rise	e.p12 🕱						
Ι		Name des Eir	ntrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
8	<u> </u>	client-system	1-X	RSA	2048	22.07.2027, 15:21:12 MESZ	-
) Exp	oort der Zertifika	atskette »client-sy s: Nur Haup 	rstem-x«	Komplette Kette		×
	Forma	at für den Expor	t: 💿 X.509	\bigcirc	PKCS #7	O PKI Path O SPC	
		PEN	1: 🗹				
		Export-Date	i: C:\Users\	,cl	ient_system_x.cer	1	Navigieren
						Export	Abbrechen

- Es erscheint ein neues Dialogfenster, welches den erfolgreichen Export bestätigt
- Klicken Sie auf OK

	Date	ei	Bearbeiten Anzeigen	Werkzeuge Unter	suchen Hilfe ri	se.p12 - KeyStore Explore	- 🗆 X
			5 a 🗙 🗅 🖻	17. 1. f. 17	••• 📵 📃	<u>i</u> Q	
rise	.p12	×					
Т		Ε	Name des Eintrags	Algorithmus	Schlüsselgröße	Ablaufdatum des Zertifikats	Zuletzt geändert
T	f	۲	client-system-x	RSA	2048	22.07.2027, 15:21:12 MESZ	-
			E				
			· · ·	A Zertifikatskette	exportieren	X	
				Zertifikats	kette erfolgreich e	xportiert.	
						ОК	

4 Überprüfung der exportierten Zertifikate im PEM-Format

- Die exportierten Dateien finden Sie in dem im vorherigen Dialogfenster unter Export-Datei von Ihnen hinterlegtem Ablagepfad
 Navigieren Sie dorthin und öffnen Sie die beiden PEM-Dateien jeweils in einem Texteditor
 Die Datei sollte für das Client-Zertifikat folgendes Format aufweisen:

1	BEGIN CERTIFICATE
2	MIIDHjCCAgagAwIBAgIGAYImEboAMA0GCSqGSIb3DQEBCwUAMCIxIDAeBgNVBAM
3	F2tvbm5la3Rvci1jbGllbnQua29ubGFuMB4XDTIyMDcyMjEzMjExMloXDTI3MDc
4	MjEzMjExMlowIjEgMB4GA1UEAwwXa29ubmVrdG9yLWNsaWVudC5rb25sYW4wggE:
5	MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdV8uhGNE/5ATzmwH8Fsb/M9Cl
6	a2ZLXB47Rs+TBjF3kuG4Pvt/W/ILyA4io0rLUua6mW27X6xFxTkcx7EwDQazj0h

• Für den **Private Key** sollte die Datei folgendes Format haben:

- ----BEGIN RSA PRIVATE KEY-----
- MIIEpAIBAAKCAQEAnVfLoRjRP+QE85sB/BbG/zPQm2tmS1we00bPkwYxd5LhuD77
- 3 flvyC8gOIqNKy1Lmupltu1+sRcU5HMexMA0Gs49IdF2HN219mYF6bEiCyyfFQuLH
- 4 zBiidqkmTC7ngC/mB8RRyYJWcnwipkxfooiDbyPqC0JbAjWB6hoJSTt8/h1m5p9t
- vnwT6hmntyYm5AId36N3FzDgePwqHipESs6L3a91wFRoVgWrDiOW6Y+KQRZJCAYj PEb0p5wUgpKgpwWo0+34gM5g(C2WEBbC(20TWB00CB544bau+4g3Co0V2SB70B+

Der Private-Key und das Client-Zertifikat sind nun im PEM-Format und können unter Einstellungen im Authenticator geladen werden.