RSA Checkliste

SSL-Zerfikate erstellen mit XCA für Portainer

Portainer kann leider noch keine ECC (**secp256k1**), deshalb mit RSA Key.

☐ 1. XCA installieren (https://hohnstaedt.de/xca/index.php)

☐ 2. XCA starten (XCA-Menü: Zubehör-XCA,http://blog.wenzlaff.de/?p=20761)

☐ 3. Erstellen Sie eine neue PKI-Datenbank, falls noch nicht geschehen (XCA-Menü: Datei > Neue Datenbank), geben Sie den Namen der Datenbank: **rsa.xdb** und **Speichern** und ein selbst ausgedachtes Passwort zweimal ein

☐ 4. Erstellen Sie einen neuen Privaten Key. Klicken Sie auf den Tab **Private Schlüssel** dann **Neue Schlüssel.** Dort eingeben:
Name: **rsa-priv-key**
Schlüsseltyp: **RSA**
Schlüssellänge: **2048 bi**
und auf **Erstellen** klicken.

☐ 5. Erstellen Sie ein neues selbstsigniertes Zertifikat. Klicken Sie auf **Zertifikate** und auf **Neues Zertifikat**.

Auf dem 1. Tab **Herkunft** muss bei Unterschreiben: **Selbstsigniertes Zertifikat erstellen** ausgewählt sein und als Signatur algorithmus: **SHA256**. Dann auf Vorlage für das neue Zertifikat: **default CA** auswählen und auf **Alles übernehmen** klicken.

Auf den 2. Tab, als Inhaber folgende Eingaben (Beispiel anpassen)
Interner Name: **rsa-zertifikat** und unter Distinguished name:
countryName: **DE**
stateOrProvinceName: **Germany**
localityName: **Niedersachsen**
organizationName: **TWSoft**
organizationalUnitName: **TWSoft**
commonName: **pi-vier** (dieser Name (CN) ist Wichtig, und muss genau dem Rechnername entsprechen!)
emailAddress:**info-anfrage@wenzlaff.de**

nun unten im Feld: Privater Schlüssel den oben erstellten **rsa-priv-key (RSA:2048 bit)** auswählen.

Auf dem 3. Tab Erweiterungen auch noch den Key identifier: **X509v3 Authority Key Identifier** und X509v3Subject Key Identifier auswählen. Die X509v3 Basis Constraints bleiben auf Typ: **Zertifikats Authorität** und auf **Critical**. Evl. Noch die Gültigkeit anpassen oder auf 10 Jahre lassen. Evl. Noch X509v3 Subject Alternative Namen um alle Namen bzw. IP-Adressen ergänzen unter der das Zertifikat gültig sein soll.

Auf dem 4. Tab. Schlüsselverwendung X509v3 Key Usage **Digital Signature** und **Key Encipherment** wählen und unter X509v3 Extended Key Usage den **TLS Web Server Authentication** und **TLS Web Client Authentication** auswählen.

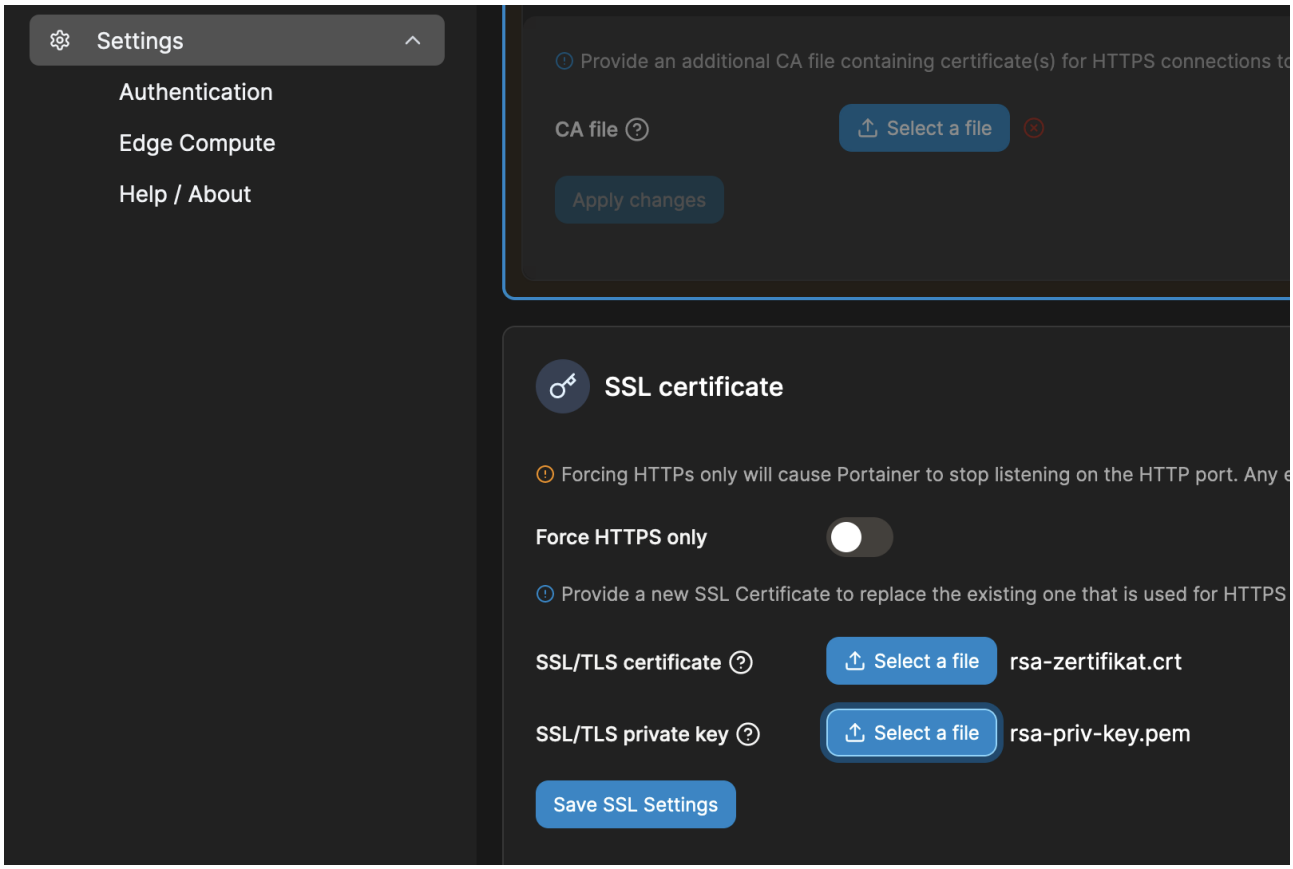
Auf den 5. Tab. Netscape unter Netscape Cert Typ den **SSL Server** auswählen. Dann auf OK klicken und das Zertifikat wurde erstellt.

☐ 6. Nun das Zertifikat als Datei exportieren. Im 3. Tab Zertifikate das erstellte **rsa-zertifikat** selektieren und auf Export klicken und das Exportformat: **PEM (*.crt)** auswählen und als **rsa-zertifikat.crt** speichern.

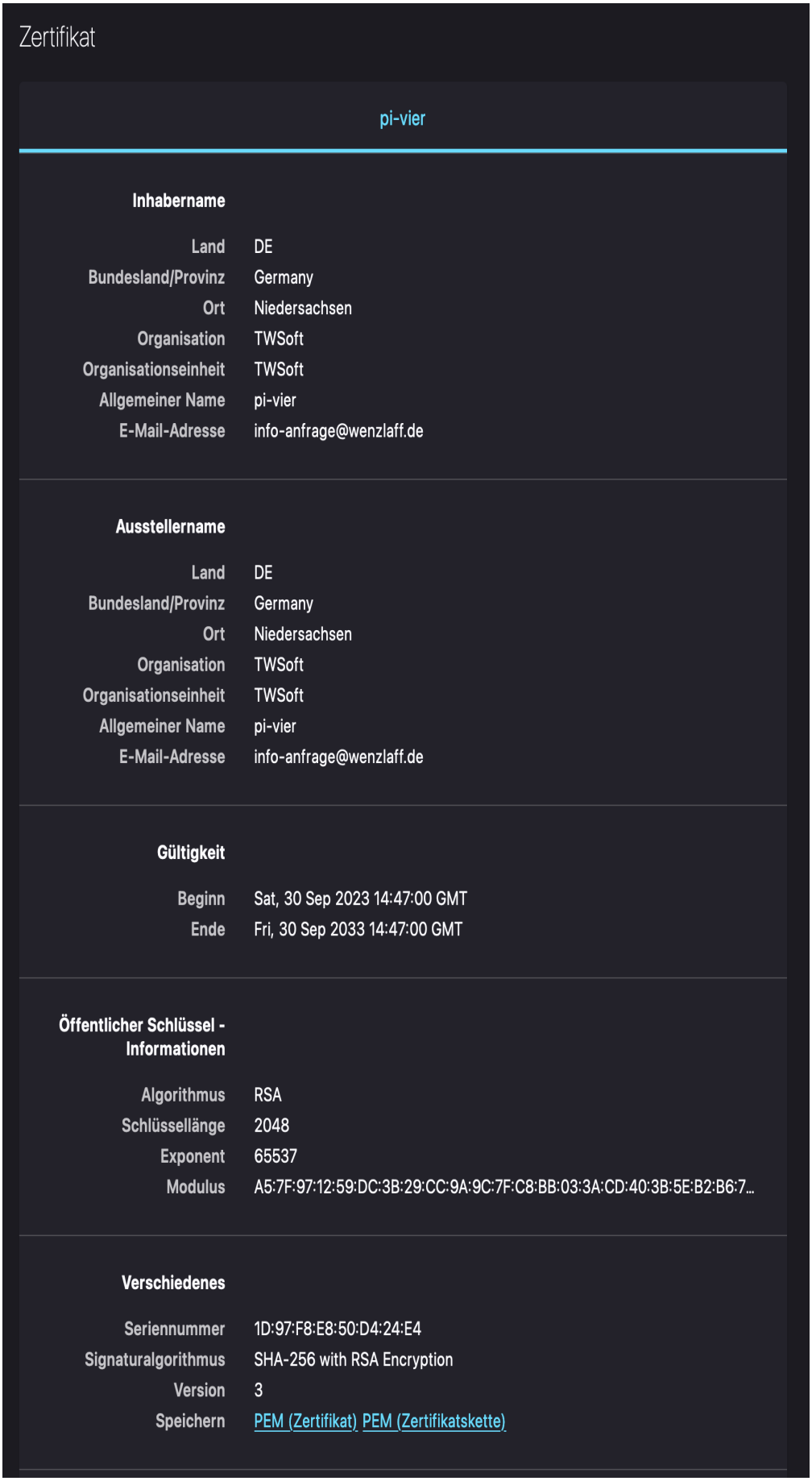
☐ 7. Nun noch den privaten Schlüssel als Datei exportieren. Im 1. Tab Private Schlüssel den rsa-priv-key selektieren und auf Export klicken. Dann das Exportformat: **PEM private (*.pem)** auswählen und als **rsa-priv-key.pem** speichern

Wir haben nun den Privaten Schlüssel **rsa-priv-key.pem** und das Zertifikat **rsa-zertifikat.crt** in einer Datei.
Die können wir nun in Portainer wie folgt auswählen.

☐ 8. In Portainer unter dem Menü: Settings und SSL certificate wählen wir für SSL/TLS certificat mit klick auf den Select a file den **rsa-zertifikat.crt** und für SSL/TLS den private key **rsa-priv-key.pem** aus und klicken dann auf **Save SSL Settings** Button.



☐ 9. Nun über die https://pi-vier:9443 Seite anmelden und als Ausnahme hinzufügen, da es ein selbstsigniertes Zertifikat ist. So sieht das Zertifikat dann für die nächsten 10 Jahre im Browser aus:


Zertifikat
pi-vier
Inhabername
Land DE
Bundesland/Provinz Germany
Ort Niedersachsen
Organisation TWSoft
Organisationseinheit TWSoft
Allgemeiner Name pi-vier
E-Mail-Adresse info-anfrage@wenzlaff.de
Ausstellername
Land DE
Bundesland/Provinz Germany
Ort Niedersachsen
Organisation TWSoft
Organisationseinheit TWSoft
Allgemeiner Name pi-vier
E-Mail-Adresse info-anfrage@wenzlaff.de
Gültigkeit
Beginn Sat, 30 Sep 2023 14:47:00 GMT
Ende Fri, 30 Sep 2033 14:47:00 GMT
Öffentlicher Schlüssel - Informationen
Algorithmus RSA
Schlüssellänge 2048
Exponent 65537
Modulus A5:7F:97:12:59:DC:3B:29:CC:9A:9C:7F:C8:BB:03:3A:CD:40:3B:5E:B2:B6:7...
Verschiedenes
Seriennummer 1D:97:F8:E8:50:D4:24:E4
Signaturalgorithmus SHA-256 with RSA Encryption
Version 3
Speichern PEM (Zertifikat) PEM (Zertifikatskette)

Fingerabdrücke	
SHA-256	4D:47:0F:A9:C1:20:84:22:BE:F9:5F:5D:E4:91:90:0D:8C:84:51:4F:9E:2F:17:...
SHA-1	BA:64:21:C2:DD:93:6E:5F:10:38:86:AF:72:D5:8F:AB:99:64:93:CA
Basiseinschränkungen	
Zertifizierungsstelle	Ja
Schlüsselverwendung	
Verwendungen	Digital Signature, Key Encipherment
Erweitere Schlüsselverwendung	
Verwendungen	Server Authentication, Client Authentication
ID für verwendeten Schlüssel des Zertifikatinhabers (Subject Key ID)	
Schlüssel-ID	94:5F:57:83:E7:18:F9:24:A7:3C:AD:DB:41:22:4D:12:EF:89:F0:25