

Software bereitstellen und Installieren

Basierend auf dieser Quelle: <https://certbot.eff.org/instructions?ws=other&os=windows>

Download der Software: https://github.com/certbot/certbot/releases/latest/download/certbot-beta-installer-win_amd64_signed.exe

Also einmal den Certbot installer für Windows herunterladen und installieren. Um ein Zertifikat zu erhalten gibt es 2 Wege. Einmal die DNS Challenge, dabei werden in deiner DNS-Zone bei deinem DNS Provider TXT Records angelegt diese werden dann von R3 abgefragt und Validiert. Danach erhältst das Zertifikat. Das geht auch völlig automatisiert, kann aber nicht jeder DNS-Provider. Deshalb gehe ich hier den 2. Weg per HTTP Challenge. Dabei wird vom Certbot Port 80 geöffnet. R3 fragt den DNS Record zu deinem Hostnamen ab und wenn dann der gestartete certbot von deinem Rechner antwortet ist die Authentifizierung abgeschlossen und du erhältst ein Zertifikat.

Los gehts:

Nach der Installation öffnest du eine CMD mit Administrativen rechten. Danach wechselst du in das Verzeichnis:

```
cd "C:\Program Files\Certbot\bin"
```

Hier sollte sich nun die Certbot.exe befinden:

```
Eingabeaufforderung
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\root>cd "C:\Program Files\Certbot\bin"

C:\Program Files\Certbot\bin>dir
Datenträger in Laufwerk C: ist System
Volumeseriennummer: 6413-60B0

Verzeichnis von C:\Program Files\Certbot\bin

26.02.2024  16:22    <DIR>          .
26.02.2024  16:22    <DIR>          ..
08.02.2024  20:49                109.112 certbot.exe
                1 Datei(en),       109.112 Bytes
                2 Verzeichnis(se), 38.229.487.616 Bytes frei

C:\Program Files\Certbot\bin>
```

Stellt sicher das der Port 80 auf eurem Windows Client oder Server aus dem Internet erreichbar ist. Falls ein IIS oder ähnliches läuft diesen bitte für diesen Zeitraum deaktivieren.

Mit diesem Befehl wird die Challenge gestartet.

```
certbot certonly --email <deine-mailAdresse@example.com> -d <hostname.example.com>
```

Bei einem Erfolg sollte das Ergebnis so aussehen:

```

Saving debug log to C:\Certbot\log\letsencrypt.log

How would you like to authenticate with the ACME CA?
-----
1: Runs an HTTP server locally which serves the necessary validation files under
the /.well-known/acme-challenge/ request path. Suitable if there is no HTTP
server already running. HTTP challenge only (wildcards not supported).
(standalone)
2: Saves the necessary validation files to a .well-known/acme-challenge/
directory within the nominated webroot path. A separate HTTP server must be
running and serving files from the webroot path. HTTP challenge only (wildcards
not supported). (webroot)
-----
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Requesting a certificate for win11b.soika.click

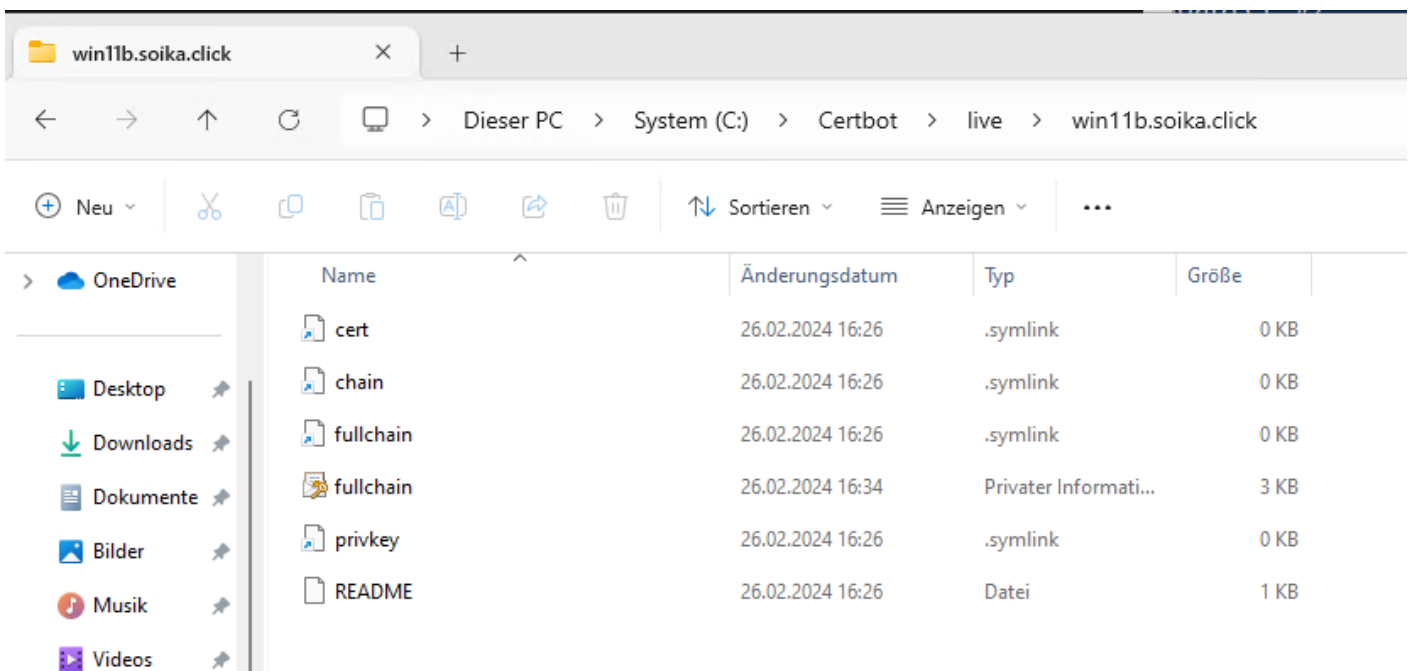
Successfully received certificate.
Certificate is saved at: C:\Certbot\live\win11b.soika.click\fullchain.pem
Key is saved at:      C:\Certbot\live\win11b.soika.click\privkey.pem
This certificate expires on 2024-05-26.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

-----
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
 * Donating to EFF: https://eff.org/donate-le
-----

C:\Program Files\Certbot\bin>

```

Unter C:\Certbot liegt nun das Zertifikat im PEM Format vor.



Soweit so gut, nur kann unser Windows damit nichts anfangen. Microsoft verwendet ein anderes format für seine Zertifikate deshalb müssen wir das noch Konvertieren.

Version #3

Erstellt: 2024-02-27 10:27:20 UTC von Schwanzus Longus

Zuletzt aktualisiert: 2024-02-27 11:04:29 UTC von Schwanzus Longus