

# {tip4u://172}

Version 1

Zentraleinrichtung für Datenverarbeitung (ZEDAT)  
[www.zedat.fu-berlin.de](http://www.zedat.fu-berlin.de)

## ACME-Client unter Windows

Dieses Merkblatt richtet sich an Personen, die Windows Server an der Freien Universität Berlin betreiben. Es beschreibt die Verwendung einer Software zur initialen Beantragung und Erneuerung von Server-Zertifikaten.

## Server-Zertifikate: ACME-Client unter Windows

Voraussetzung für das Erzeugen von Zertifikaten auf einem Server der Freien Universität Berlin ist die Freischaltung der gewünschten Domains sowie das Erstellen eines so genannten ACME-Accounts im Zertifikatsportal der ZEDAT. Beides wird im Merkblatt [Tip4U #171](#)<sup>1</sup> beschrieben.

Es ist empfehlenswert, einen dezidierten ACME-Account für jeden Server bzw. Dienst anzulegen, für den ein Zertifikat genutzt werden soll. Die Daten dieses ACME-Accounts werden dann auf dem jeweiligen Server hinterlegt und können dort auch zur automatischen Verlängerung der Zertifikate verwendet werden. Im Folgenden wird beschrieben, wie ein Zertifikat einerseits initial und andererseits im Verlängerungsfall auf einem Windows-Server eingespielt wird.

Für Windows gibt es verschiedene ACME-Clients. Wir stellen hier die Verwendung von win-acme vor, aber andere Programme wie certbot (siehe [Tip4U #173](#)<sup>2</sup>) sollten ebenfalls funktionieren.

win-acme kann von der offiziellen Webseite unter <https://www.win-acme.com/> heruntergeladen werden. Nach dem Download muss die ZIP-Datei in einen geeigneten Ordner (z.B. C:\Program Files\win-acme\) entpackt werden.

Danach wird eine Kommandozeile mit Administrator-Rechten benötigt. Dazu muss im Startmenü **cmd** eingegeben und mit *Als Administrator ausführen* in der rechten Spalte gestartet werden.

In der Eingabeaufforderung kann win-acme folgendermaßen ausgeführt werden:

```
"\Program Files\win-acme\wacs.exe" ^
  --baseuri https://certificate.zedat.fu-berlin.de/acme/ ^
  --eab-key-identifizier <EAB-KID> --eab-key <EAB-HMAC>
```

Dabei müssen <EAB-KID> und <EAB-HMAC> durch die entsprechenden Werte des ACME-Accounts aus dem Zertifikatsportal ersetzt werden.

Es startet ein interaktives Menü, mit dem das Zertifikat erstellt werden kann:

```
Administrator: Eingabeaufforderung - "\Program Files\win-acme\wacs.exe" --baseuri https://certificate.zedat.fu-berlin.de/acme/ --eab-key-identifizier a...
Microsoft Windows [Version 10.0.19045.2364]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>"\Program Files\win-acme\wacs.exe" --baseuri https://certificate.zedat.fu-berlin.de/acme/ --eab-key-identifizier <EAB-KID> --eab-key <EAB-HMAC>

A simple Windows ACMEv2 client (WACS)
Software version 2.1.23.1315 (release, trimmed, standalone, 64-bit)
Connecting to https://certificate.zedat.fu-berlin.de/acme/...
Connection OK!
Scheduled task looks healthy
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (1 total)
O: More options...
Q: Quit

Please choose from the menu:
```

<sup>1</sup>[https://zedat.fu-berlin.de/tip4u\\_171.pdf](https://zedat.fu-berlin.de/tip4u_171.pdf)

<sup>2</sup>[https://zedat.fu-berlin.de/tip4u\\_173.pdf](https://zedat.fu-berlin.de/tip4u_173.pdf)

Mit **N** kann ein neues Zertifikat beantragt werden. Wird ein Microsoft IIS-Webserver benutzt, so werden die verwendeten Hostnamen automatisch ausgelesen – anderenfalls müssen die Domainnamen manuell angegeben werden.

Im Anschluss muss festgelegt werden, wie das Zertifikat installiert werden soll. Es wird standardmäßig im Windows-Zertifikatspeicher hinterlegt, optional auch automatisch im IIS. Als Alternative kann ein Script oder Programm aufgerufen werden, um die Konfiguration einer anderen Server-Software zu aktualisieren. win-acme bringt einige Beispiel-Scripts im Verzeichnis Scripts mit.

Durch win-acme wird danach sofort das Zertifikat beantragt und eine Aufgabe in der Aufgabenplanung von Windows angelegt, mit der das Zertifikat später automatisch erneuert wird.

Mit der Option **M** in win-acme können weitere Details des Zertifikats festgelegt werden, wie zum Beispiel der verwendete Algorithmus oder die Länge des privaten Schlüssels.

Weitere Optionen und die Verwendung der mitgelieferten Scripts können in der offiziellen Dokumentation unter <https://www.win-acme.com/reference/cli> nachgelesen werden.