

{tip4u://171}

Version 1

Zentraleinrichtung für Datenverarbeitung (ZEDAT)

www.zedat.fu-berlin.de

Server-Zertifikate erstellen

Digitale Server-Zertifikate werden verwendet, um die Identität von Diensteanbietern zu belegen und die Verbindung mittels Verschlüsselung gegenüber Dritten zu sichern. Auf diese Weise wird sichergestellt, dass die Kommunikation mit der richtigen Gegenstelle erfolgt und auf dem Transportweg kein Klartext abgehört werden kann. Dieses Merkblatt beschreibt, wie berechtigte Personen an der Freien Universität Berlin Server-Zertifikate beantragen können.

Server-Zertifikate

Zur Nutzung von gesicherten Verbindungen benötigt das anbietende System ein Zertifikat, mit dem die Identität des Servers verifiziert werden kann. Bei Web-basierten Diensten (https) prüft der Web-Browser, ob das Zertifikat von einem bekannten Stammzertifikat abstammt, welches meist im Browser oder im Betriebssystem enthalten ist.

Systembetreibende an der Freien Universität Berlin können über das Zertifikatsportal der ZEDAT die Berechtigung einholen, automatisiert Server-Zertifikate für ihr System zu erstellen und regelmäßig zu erneuern. Die dafür notwendigen Schritte sind:

1. Mit dem eigenen FU-Account auf dem Zertifikatsportal der ZEDAT über den URL <https://certificate.zedat.fu-berlin.de/> einloggen.
2. Die Berechtigung zur Ausstellung von Server-Zertifikaten für die verwendeten Domainnamen beantragen.
3. Ggf. die Genehmigung einer für die Domains zuständigen, bereichsverantwortlichen Person abwarten, die damit bestätigt, dass der antragstellende FU-Account für die angefragten Domainnamen zuständig ist und zur Zertifikatsausstellung berechtigt werden soll.
4. Neuen ACME-Account für den gewünschten Server im Zertifikatsportal erzeugen und diesem die benötigten Domainnamen zuweisen.
5. Auf dem Server mit einem ACME-Client und den passenden ACME-Accountdaten aus dem Zertifikatsportal ein Zertifikat erzeugen und für den Dienst hinterlegen.
6. Empfehlenswert ist es, auf dem Server einen Automatismus zum regelmäßigen Aufruf des ACME-Clients einzurichten, damit rechtzeitig vor dem Ablaufdatum des Zertifikates automatisch ein neues erstellt, installiert und aktiviert wird.

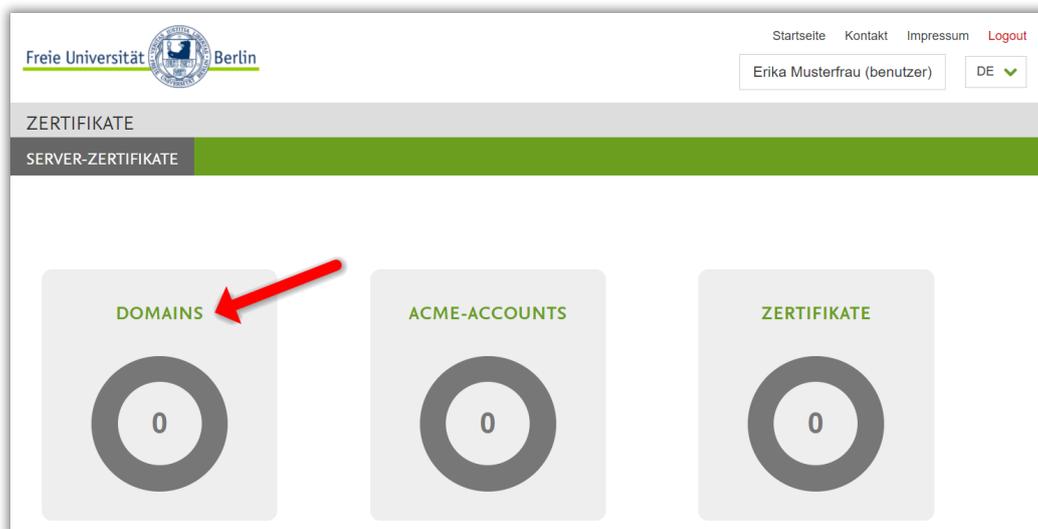
Mit einem ACME-Account können Serverbetreibende Zertifikate automatisch erstellen und erneuern. Wir empfehlen, je Dienst und Server einen eigenen ACME-Account zu erzeugen und diesem nur die jeweils nötigen Domainnamen zuzuweisen.

Das Genehmigungsverfahren über die Bereichsverantwortlichen ist nur dann erforderlich, wenn zusätzliche Domainnamen berechtigt werden sollen.

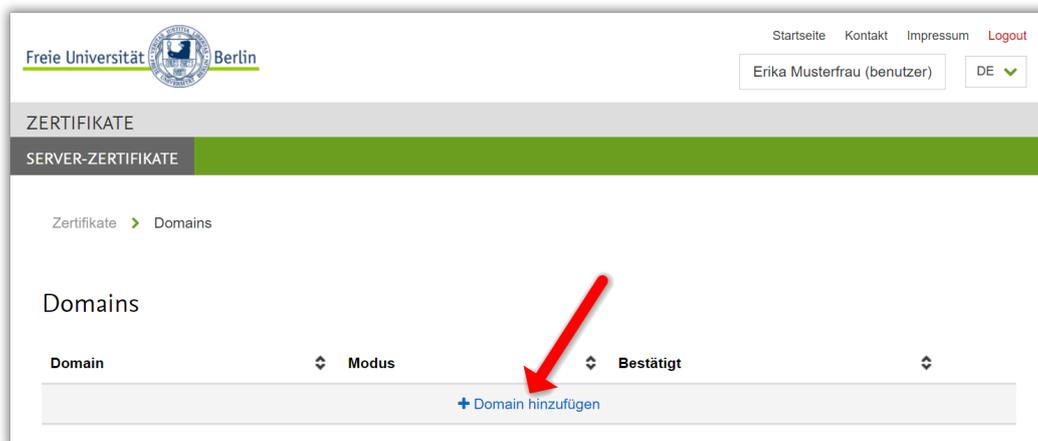
Die Ausstellung von Server-Zertifikaten erfolgt an der Freien Universität Berlin immer mittels des ACME-Protokolls (ACME = Automatic Certificate Management Environment, beschrieben im Internet-Standard RFC 8555). Falls die Ausstellung des Zertifikates nicht direkt auf dem System möglich ist, wo dieses eingesetzt werden soll, kann die Erzeugung auch auf einem anderen Gerät erfolgen; in diesem Fall muss das neue Zertifikat noch auf das Zielsystem übertragen und dort eingespielt werden. Aufgrund der kurzen Laufzeit von Zertifikaten und des erhöhten Aufwandes von Zertifikatswechseln empfehlen wir, die automatische Ausstellung immer auf dem dienstbringenden Server durchzuführen, sofern das technisch möglich ist.

Berechtigung für Domainnamen beantragen

Wählen Sie das Feld *DOMAINS* auf der Übersichtsseite des Zertifikatsportals der ZEDAT (<https://certificate.zedat.fu-berlin.de/>) aus:



Es wird eine Liste der bereits beantragten und genehmigten Domains angezeigt. Am Ende der Liste kann mit *Domain hinzufügen* die Berechtigung zur Ausstellung von Server-Zertifikaten für weitere Domainnamen beantragt werden.



Tragen Sie den gewünschten Domainnamen in das entsprechende Feld ein. Bei *Modus* können Sie auswählen, ob die Berechtigung auch für weitere Namen gelten soll. Die Angaben bedeuten im Einzelnen: Die Berechtigung gilt ...

Exakt	... nur für genau diesen Domainnamen
WWW	... für den Domainnamen mit und ohne vorangestelltem „www.“
Sub	... für den Domainnamen und alle Subdomains

Freie Universität Berlin

Startseite Kontakt Impressum Logout

Erika Musterfrau (benutzer) DE

ZERTIFIKATE

SERVER-ZERTIFIKATE

Zertifikate > Domains > Domain hinzufügen

Domain hinzufügen

Domain: einrichtung.fu-berlin.de

Modus: Exakt WWW Sub

Hinzufügen

Nach dem *Hinzufügen* erhalten Sie eine Liste der Domainnamen. Unbestätigte Domainnamen werden mit einem roten Kreuz gekennzeichnet. Kontaktieren Sie in dem Fall eine bereichsverantwortliche Person und bitten um die Erlaubnis, für den beantragten Domainnamen Server-Zertifikate ausstellen zu dürfen. (Wie der Antrag durch Bereichsverantwortliche bearbeitet werden kann, ist im [Tip4U #174](https://zedat.fu-berlin.de/tip4u_174)¹ beschrieben.)

Freie Universität Berlin

Startseite Kontakt Impressum Logout

Erika Musterfrau (benutzer) DE

ZERTIFIKATE

SERVER-ZERTIFIKATE

Zertifikate > Domains

Domain hinzugefügt!

Domains

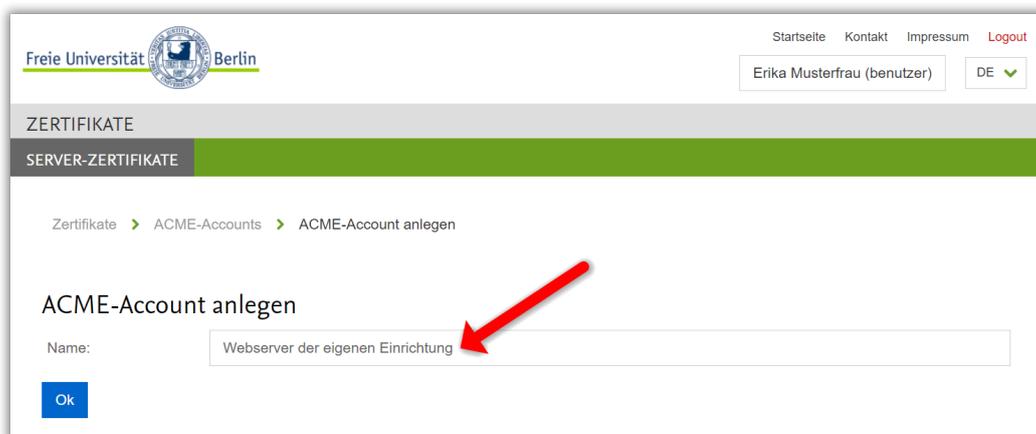
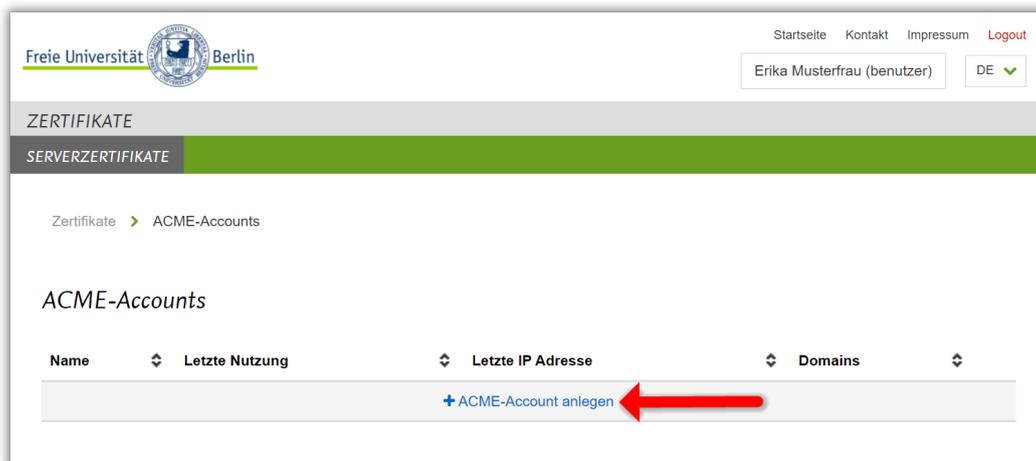
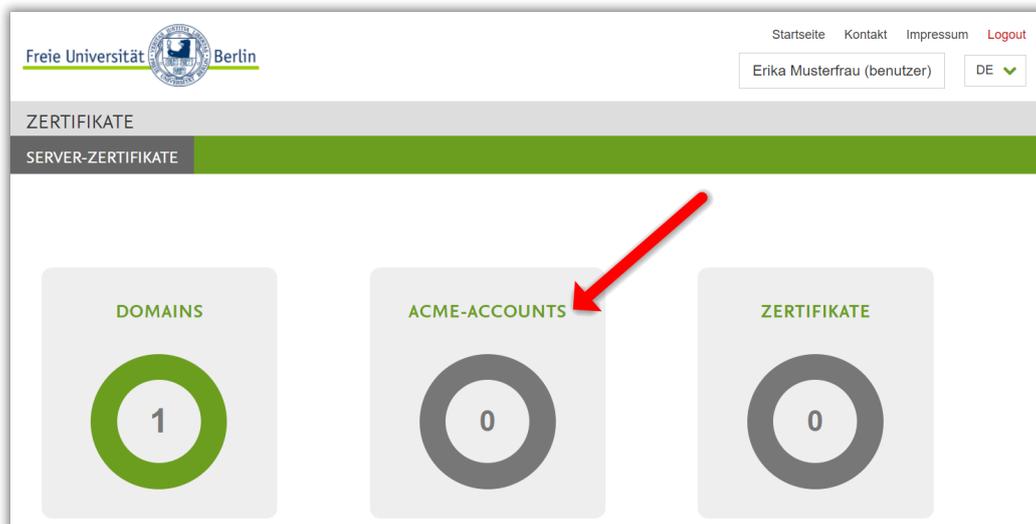
Domain	Modus	Bestätigt	
einrichtung.fu-berlin.de	www	X	Bearbeiten Löschen

+ Domain hinzufügen

¹https://zedat.fu-berlin.de/tip4u_174.pdf

ACME-Account erzeugen

Wählen Sie auf der Übersichtsseite das Feld **ACME-ACCOUNTS** und anschließend unterhalb der angezeigten Liste **ACME-Account anlegen** aus. Vergeben Sie eine Bezeichnung, um diesen ACME-Account gemäß seiner Verwendung zu kennzeichnen, und bestätigen Sie dies mit einem Klick auf **OK**.



Der ACME-Account wurde angelegt und Ihnen werden die Zugangsdaten angezeigt, die Sie für Ihren ACME-Client benötigen. Fügen Sie jetzt die Domainnamen hinzu, die diesem ACME-Account zugeordnet sein sollen. Sofern noch keine Berechtigung für den Domainnamen existiert, wird intern automatisch ein entsprechender Antrag gestellt. Die Angabe *Modus* entspricht der obenstehenden Erläuterung.

Freie Universität Berlin

Startseite Kontakt Impressum Logout

Erika Musterfrau (benutzer) DE

ZERTIFIKATE

SERVER-ZERTIFIKATE

Zertifikate > ACME-Accounts > Webserver der eigenen Einrichtung

ACME-Account angelegt!

ACME-Account: Webserver der eigenen Einrichtung

ACME-Server	https://certificate.zedat.fu-berlin.de/acme/	
EAB-KID	c926d567-dca9-48dd-	
EAB-HMAC		

Name bearbeiten ACME-Account löschen

Domains 0 Zertifikate 0 ACME-Clients 0

Domain	Modus	Bestätigt
+ Domain hinzufügen		

Freie Universität Berlin

Startseite Kontakt Impressum Logout

Erika Musterfrau (benutzer) DE

ZERTIFIKATE

SERVER-ZERTIFIKATE

Zertifikate > ACME-Accounts > Webserver der eigenen Einrichtung > Domain hinzufügen

Domain hinzufügen

Domain: einrichtung.fu-berlin.de

Modus:

- Exakt
- WWW
- Sub

Hinzufügen

Sobald alle benötigten Domainnamen dem ACME-Account hinzugefügt wurden und für diese eine Bestätigung vorliegt, übernehmen Sie die ACME-Zugangsdaten und den URL des ACME-Servers, um damit Ihren ACME-Client einzurichten. Die Übernahme der Daten erfolgt am einfachsten über das Kopiersymbol. Falls nötig, können Sie das Passwort (EAB-HMAC) mit dem Auge-Symbol auch in Klarschrift anzeigen lassen. Beachten Sie bitte, dass die Zugangsdaten sicher gespeichert und gegenüber dem Zugriff Dritter geschützt werden müssen.

Freie Universität Berlin

Startseite Kontakt Impressum Logout

Erika Musterfrau (benutzer) DE

ZERTIFIKATE

SERVER-ZERTIFIKATE

Zertifikate > ACME-Accounts > Webserver der eigenen Einrichtung

Domain hinzugefügt!

ACME-Account: Webserver der eigenen Einrichtung

ACME-Server <https://certificate.zedat.fu-berlin.de/acme/>

EAB-KID c926d567-dca9-48dd-...

EAB-HMAC [redacted]

Name bearbeiten ACME-Account löschen

Domains 1 Zertifikate 0 ACME-Clients 0

Domain	Modus	Bestätigt	
einrichtung.fu-berlin.de	www	✓	Löschen

+ Domain hinzufügen

Sobald der ACME-Account verwendet wurde, wird Ihnen dies in der Liste angezeigt. Über *Bearbeiten* können Sie die Bezeichnung des Accounts bei Bedarf nachträglich anpassen.

Freie Universität Berlin

Startseite Kontakt Impressum Logout

Erika Musterfrau (benutzer) DE

ZERTIFIKATE

SERVER-ZERTIFIKATE

Zertifikate > ACME-Accounts

ACME-Accounts

Name	Letzte Nutzung	Letzte IP Adresse	Domains	
Webserver der eigenen Einrichtung	2022-12-12 23:13:33+01	130.133.9.73	1	Bearbeiten

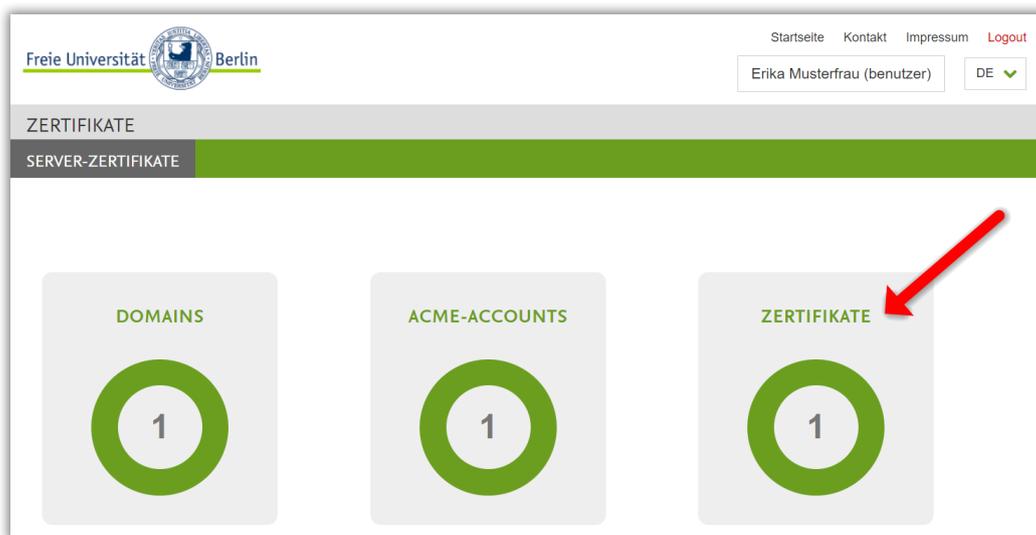
+ ACME-Account anlegen

Die Ausstellung von Zertifikaten mit einem ACME-Client ist in gesonderten Merkblättern beschrieben:

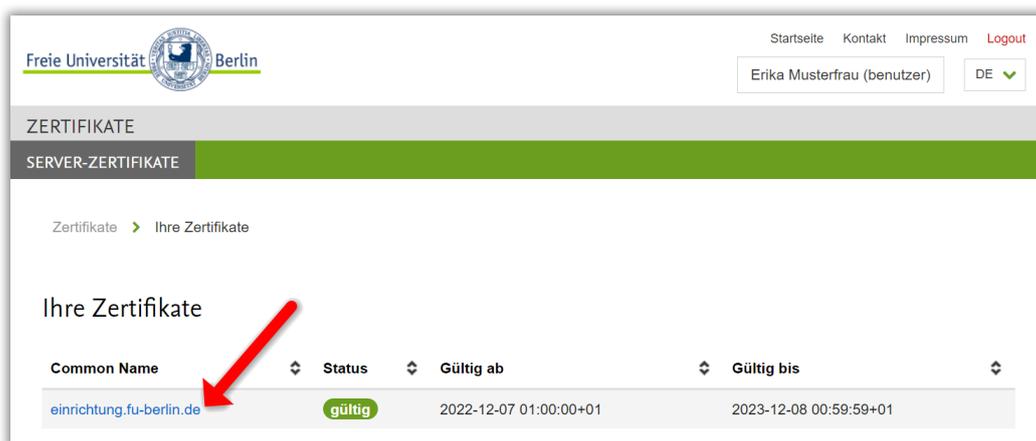
- [Tip4U #172²](#) ACME-Client unter Windows
- [Tip4U #173³](#) ACME-Client unter Linux

Zertifikatsübersicht

Sobald mit einem ACME-Client Zertifikate ausgestellt wurden, wird Ihnen dieses auf der Übersichtsseite angezeigt. Wählen Sie die Schaltfläche *ZERTIFIKATE*, um eine Liste zu erhalten:



Sie können ein Zertifikat auswählen, um sich dessen Details anzuzeigen zu lassen.



²https://zedat.fu-berlin.de/tip4u_172.pdf

³https://zedat.fu-berlin.de/tip4u_173.pdf

Zertifikats-Detailanzeige

Zertifikate > Ihre Zertifikate > einrichtung.fu-berlin.de

einrichtung.fu-berlin.de

Zertifikatdetails

Subject	C=DE, ST=Berlin, O=Freie Universität Berlin, CN=einrichtung.fu-berlin.de
Issuer	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
Serial	04:5B:A7:4A:BF:C3:3A:B6:22:77:16:8D:30:C9:6D:7E
notBefore	Dec 7 00:00:00 2022 GMT
notAfter	Dec 7 23:59:59 2023 GMT
Fingerprint (SHA1)	12:52:96:F9:BC:4F:8A:B0:80:97:E2:8E:92:39:E2:4D:41:4C:F4:E5
Fingerprint (SHA512)	C6:18:67:DD:91:6B:12:F8:95:91:26:C8:01:B2:25:4F:1B:71:A0:BB:5D:69:43:29:17:56:E5:D4:24:B9:61:D9:CB:B4:6C:1F:F2:2B:15:A5:11:CD:17:06:C6:FD:58:2D:70:78:1B:69:1C:8B:03:04:87:C9:2E:38:44:FF:1F:A9
Signature Algorithm	sha256WithRSAEncryption
Signature	18:05:1D:EE:D2:88:2B:2A:D0:B3:A9:C2:B4:B1:ED:5F:21:7D:79:B4:49:51:09:06:F4:AE:65:C6:9F:AD:C6:CF:6D:F8:DC:24:0A:BF:3B:75:47:BA:73:4C:B0:3F:44:A5:4E:85:FE:29:FB:4F:38:66:4E:BE:D6:57:49:F9:76:0D:1B:9D:E0:AD:C5:BE:AF:D2:EE:67:CB:62:76:22:84:A7:1E:6D:50:B9:24:57:E8:FB:4A:B3:28:25:E8:97:AA:E0:2E:0B:DB:30:6E:E5:53:17:EC:9A:61:E9:4F:D0:10:32:90:D7:F2:B3:10:71:DD:1A:BD:E4:A6:14:22:9A:FA:8F:EA:BD:7A:80:D7:12:2D:9A:42:57:1A:0A:D0:77:E5:14:16:DC:28:25:18:02:A8:BD:A0:80:BE:BF:77:EC:34:48:81:6B:50:11:8A:47:C0:D6:F6:2D:ED:F5:86:A1:04:ED:E7:1B:A1:8A:EC:8C:D7:17:00:7E:DF:3B:E3:31:4C:F3:99:58:DA:F4:C1:5A:41:9F:48:FA:87:74:6C:B7:46:02:8C:DA:8D:E8:1F:4B:B7:C0:01:06:BA:BA:E9:76:62:40:8C:DA:0B:9E:AF:23:8C:9D:EA:F9:2F:0B:FF:B4:7F:68:9F:54:55:92:36:AF:23:C8:6E:72:92:00:7F:D9:B7:C6
Subject Alternative Names	dNSName=einrichtung.fu-berlin.de dNSName=www.einrichtung.fu-berlin.de
Subject Key Identifier	E3:94:31:1D:3B:AE:65:22:2F:1B:A8:D7:10:C4:62:8E:CE:9C:63:8A
Public Key Size	2048
Public Key Algorithm	rsaEncryption
Status	gültig
Heruntergeladen	Heruntergeladen am 2022-12-07 12:47:15+01 von 91.66.98.163

📄 Zertifikat herunterladen
🗑️ Zertifikat sperren

Mittels *Zertifikat sperren* können Sie ein ausgestelltes Zertifikat zurückziehen und damit ungültig machen.

Außerdem besteht hier auch die Möglichkeit, das Zertifikat herunterzuladen. Dies ist aber normalerweise nicht erforderlich, weil das bereits durch den ACME-Client erfolgt.