

S/MIME Zertifikate (Nutzerzertifikate)

- [Allgemeines zu S/MIME Zertifikaten](#)
- [Beantragung eines S/MIME Zertifikates durch Passworteingabe](#)
- [Beantragung mit einem Zertifikatsantrag \(CSR\)](#)

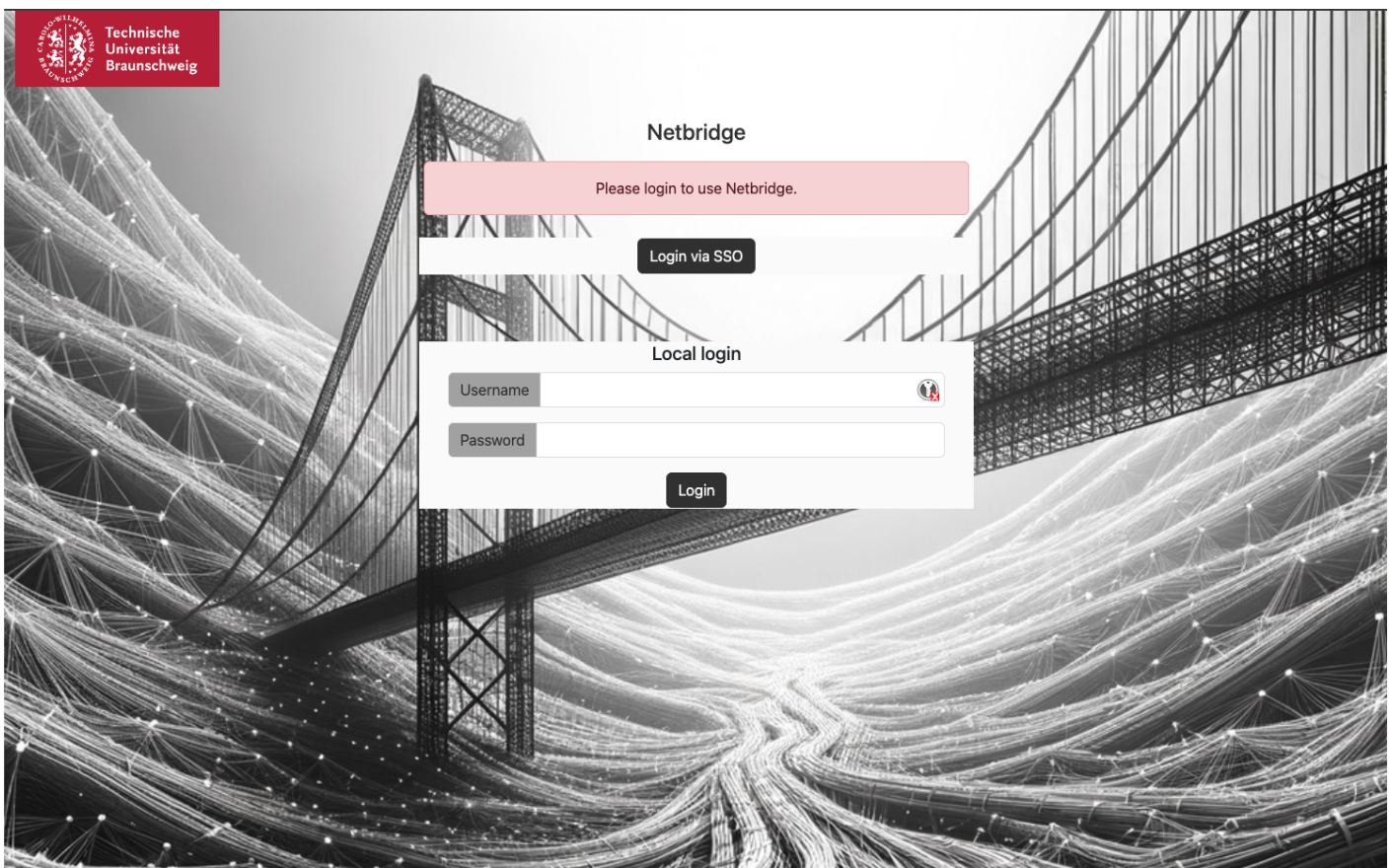
Allgemeines zu S/MIME Zertifikaten

Mit einem S/MIME lässt sich nachweisen, wer der Absender einer E-Mail ist oder von welchem Autor eine Textdatei stammt. Diese sogenannten Nutzerzertifikate können weiterhin eingesetzt werden, um E-Mails zu verschlüsseln, eine Identität im Internet nachzuweisen oder aber sich an Webseiten oder Diensten anzumelden.

An der TU-Braunschweig bieten wir über die Public Key Infrastructure (PKI) des Deutschen Forschungsnetzes (DFN) und den Zertifikatsaussteller HARICA S/MIME Zertifikate an. Diese Zertifikate decken die meisten der oben genannten Anwendungsgebiete ab, eignen sich aber nicht zum Signieren von Dokumenten.

Übersicht der vorhandenen S/MIME Zertifikate

Um in die Zertifikatsverwaltung für S/MIME Zertifikate zu gelangen, navigieren Sie bitte zu folgender URL: <https://netbridge.rz.tu-bs.de/> und loggen sich per SSO ein.



Sie gelangen auf eine Startseite, auf der Sie im linken Menü den Unterpunkt "S/MIME Certificates" auswählen.

Letzte Änderungen

Je nach Anzahl der vorhandenen Zertifikate kann es einige Zeit dauern, bis die Übersichtsseite geladen ist. Hier sehen Sie eine Auflistung der aktuellen und gültigen Zertifikate des aktuellen (HARICA) und des vorherigen Zertifikatsanbieters (Sectigo). Zurückgerufene oder abgelaufene Zertifikate werden nicht aufgelistet. Beide Listen sind unterschiedlich aufgebaut und an die jeweiligen Informationen angepasst. Ein Zertifikat von HARICA wird mit einer ID, der Seriennummer, dem sogenannten Common Name, dem Status, dem Ablaufdatum und dem Typ angegeben. Der Typ unterscheidet sich, je nachdem, ob Sie das Zertifikat mit Passwort (PKCS12) oder mit CSR (PKSC7) beantragt haben. Weiterhin können Sie HARICA Zertifikate herunterladen oder zurückrufen.

S/MIME Certificates


+ Request certificate

What happens here?
 You can get an overview of your S/MIME certificates, request new or revoke existing certificates.

Current and valid S/MIME certificates

ID	Serial	CommonName	Status	Valid to	Type
1	1e7fc5d4-xxxx-xxxx-xxxx-xxxxxxxxxxxx	521FBC0B5F87XXXXXXXXXXXXXXXXXXXXX certrequests@tu-braunschweig.de	VALID	2027-12-17T10:43:07	PKCS12  
2	fd29b39e-xxxx-xxxx-xxxx-xxxxxxxxxxxx	2BBB9D83C4FCXXXXXXXXXXXXXXXXXXXXX certrequests@tu-braunschweig.de	VALID	2027-12-17T08:43:29	PKCS7  

Current and active Sectigo S/MIME certificates

ID	Type	CommonName	Subject	Status	Valid from	Valid to
1	3182460 API	x.xxxxx@tu-braunschweig.de	Enroll CN=X,GIVENNAME=X,SURNAME=X,E=x.xxxxx@tu-braunschweig.de,2.5.4.97=GOVDE+NI,O=Technische Universität Braunschweig,ST=Niedersachsen,C=DE	VALID	2024-03-28T11:30:07	2026-03-28T23:59:59 

(Das rote "Entfernen-Symbol" bei den Sectigo-Zertifikaten wurde in der Zwischenzeit entfernt.)

Mit einem Klick auf "+ Request certificate" gelangen Sie auf die Beantragungseite, wo sie zwischen Beantragung per Passwort und per CSR wählen können.

Beantragen eines S/MIME Zertifikates

Für die Beantragung von Nutzerzertifikaten stehen zwei Arten zur Verfügung, die Beantragung per Passwort und die Beantragung per CSR. Entscheidet man sich für die Beantragung mit Passworteingabe, so werden serverseitig ein CSR (Zertifikatsantrag) und ein privater Schlüssel erstellt. Der erstellte CSR wird dann bei dem Zertifikatsaussteller (HARICA) eingereicht. Der Zertifikatsaussteller erzeugt eine Datei, in der das digitale Zertifikat und die Zwischenzertifikate enthalten sind (P7B-Format). Mit dieser Datei, dem zuvor erzeugten privaten Schlüssel und dem eingegebenen Passwort wird dann ein P12-Zertifikat erstellt. Der private Key und alle Zwischendateien werden serverseitig nicht gespeichert. Lediglich das P12-Zertifikat wird gespeichert, um es dem Antragsteller jederzeit zum Download anzubieten. Der Antragsteller ist für die sichere Verwahrung des Passworts zuständig. Bei Passwortverlust kann das Zertifikat nicht neu eingebunden werden und verschlüsselte Daten gehen verloren. Eine detaillierte Anleitung zur Beantragung durch Passworteingabe erhalten Sie [hier](#).

Wird die Beantragung per CSR gewählt, so werden der private Schlüssel und der Zertifikatsantrag auf dem Nutzersystem erstellt. Auch das Zusammenfügen des privaten Schlüssels und des P7B-Zertifikates erfolgt auf dem Nutzersystem. Lediglich das P7B-Zertifikat wird serverseitig gespeichert. Der Antragsteller ist für eine sichere Verwahrung des privaten Schlüssels verantwortlich. Bei Verlust des privaten Schlüssels kann das P12-Zertifikat nicht neu erstellt werden. Eventuell verschlüsselte Daten gehen verloren. Eine detaillierte Anleitung zur Beantragung nach Erzeugen eines CSRs erhalten Sie [hier](#)

Verschieden Zertifikatstypen und Nutzerkonten

HARICA bietet zwei Arten von Zertifikaten an, sogenannte "email_only" und "IV+OV" Zertifikate.

"Email_only" Zertifikate enthalten nur die validierte Email-Adresse. Solche Zertifikate werden für Studenten und Funktionsaccounts (Gruppenemailadressen) ausgestellt. "IV+OV" Zertifikate enthalten darüber hinaus den validiertem Vor- und Nachnamen sowie Organisationsinformationen. Diese Art von Zertifikaten können aus rechtlichen Gründen nur Angestellte erhalten, diese Zertifikate können weder für Studenten noch für Funktionsaccounts ausgestellt werden.

Es können, limitiert durch den Zertifikatsanbieter, Zertifikate für bis zu drei Emailadressen beantragt werden. Ist mindestens eine persönliche Emailadresse einer angestellten Person enthalten, wird der Typ "IV+OV" beantragt. Wird ein Zertifikat durch die Eingabe eines Passwortes beantragt, so wird eine persönliche Emailadresse immer bevorzugt als "Common Name" im Zertifikat verwendet. Weitere Emailadressen tauchen als "alternative" Emailadressen im Zertifikat auf. Die Reihenfolge der Emailadressen im Zertifikat lässt sich nur bei Beantragung mittels eines CSRs durch den Nutzer beeinflussen.

Zurückziehen eines Zertifikates

Durch Klicken auf das rote Kreuz am Ende einer Zeile, können Sie ein Zertifikat zurückrufen. Nach erfolgreichem Rückruf gelangen Sie wieder auf die Übersichtsseite. Das Zertifikat ist aus der Auflistung verschwunden.

Sectigo Zertifikate lassen sich nicht mehr automatisiert zurückziehen. Dazu wenden Sie sich bitte per Email an noc@tu-braunschweig.de.

S/MIME Certificates

+ Request certificate



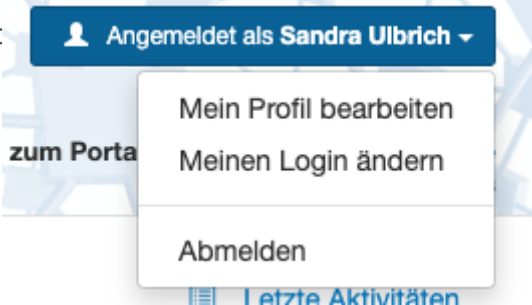
What happens here?

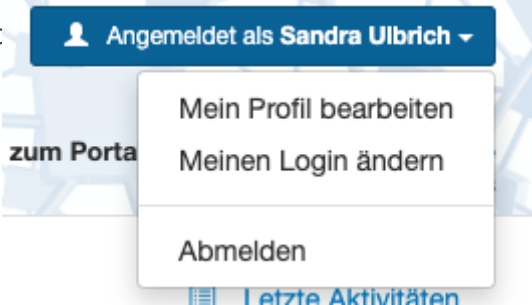
You can get an overview of your S/MIME certificates, request new or revoke existing certificates.



Successfully revoked certificate at HARICA.

Ändern des Zertifikates für das DFN.Security-Portal

1. Bevor das alte Zertifikat ungültig wird, muss ein neues beantragt werden!
2. Einloggen ins [DFN Security Portal](#) mit dem alten Zertifikat!
3. Oben rechts  klicken und auf **Meinen Login ändern**



klicken.

4. Es erscheint ein PopUp-Fenster. Hier bitte auf **Zertifikat ändern** klicken. Man erhält eine Email an die im Portal eingerichtete Email-Adresse mit weiteren Anweisungen.

Aktive Zertifikate

Dieses Benutzerkonto ist aktuell mit den folgenden Zertifikaten verknüpft:

Gültig bis

Subject

Issuer

SHA256 Fingerprint

Serial

Zertifikat ändern

Um das Zertifikat oder die Authentisierungsmethode zu ändern, nutzen Sie bitten den folgenden Link. Wir werden eine E-Mail mit weiteren Instruktionen an die registrierte Adresse **sandra.ulbrich@tu-braunschweig.de** verschicken.

Zertifikat ändern

Die Email-Adresse im Zertifikat muss mit der Email-Adresse übereinstimmen, mit der man im DFN.Security Portal angemeldet ist.

Verwenden Nutzerzertifikates

Eine Anleitung zum Einbinden des erhaltenen Zertifikates in Outlook finden Sie hier:

[Zertifikatsimport S/MIME Outlook](#)

Beantragung eines S/MIME Zertifikates durch Passworteingabe

Beantragung per Passwort

Technische Universität Braunschweig

maxmuste

Create S/MIME Certificate

What happens here?
You can request a S/MIME certificate by providing a password. For more information, please refer to the [documentation](#). (Login required.)

Request by password | [Request by csr](#)

Create S/MIME Certificate by Password

Email ?
certbot@tu-braunschweig.de
certrequests@tu-braunschweig.de
max.mustermann@tu-braunschweig.de
m.mustermann@tu-braunschweig.de

Password ?

Confirm Password ?

Request

Um ein Zertifikat mit Eingabe eines Passwortes zu beantragen, wählen Sie bitte bis zu drei Email-Adressen aus. Mehrere Email-Adressen gleichzeitig können zusammenhängend mit der Shift-Taste oder unabhängig voneinander mit der STRG- (Windows) bzw. Command-Taste (MacOS) in der Liste angeklickt werden. Nur personenbezogene Email-Adressen sind berechtigt und werden hier aufgelistet. Fehlt eine Ihrer Email-Adressen, wenden Sie sich bitte per Email an noc@tu-braunschweig.de. Im Folgenden vergeben Sie bitte ein Passwort und geben es ein zweites Mal ein. Bitte verwahren Sie dieses Passwort sicher. Sie benötigen es, um das Zertifikat später in den Zertifikatsspeicher ihres Betriebssystems zu importieren.

Beantragung mit einem Zertifikatsantrag (CSR)

Erstellen einer CSR-Datei

Haben Sie die Beantragung durch einen Zertifikatsantrag gewählt, müssen Sie zuerst einen solchen erstellen. Dazu gehen Sie bitte wie folgt vor.

1. Laden Sie sich folgenden OpenSSL .cnf-Datei runter: [smime_config.cnf](#)
2. Öffnen Sie die Datei mit einem Texteditor und passen Sie folgende Textzeilen an:
 - Erforderlich:
 - OU = Ihr(e) Institut/ Abteilung
 - CN = Ihr Name laut Personalausweis
 - emailAddress = Ihre EMail-Adresse, für die sie das Zertifikat erstellen wollen
 - Optional, falls Sie eine oder zwei alternative Email-Adressen eintragen möchten:
 - Entfernen Sie die Raute (#) aus dem Anfang der letzten Zeile (`#subjectAltName = @alt_names`) sowie die Rauten vor email.1 bzw. email.2, je nachdem, welche Sie benutzen.
 - email.1 = Ihre erste alternative Email-Adresse
 - email.2 = Ihre zweite alternative Email-Adresse
3. Belassen Sie den Rest der Datei mit den bereits eingetragenen Werten und speichern sie diese unter einem beliebigen Namen ab.
4. Öffnen Sie das Terminal auf Ihrem Computer.
5. Mit folgendem Befehl erstellen Sie eine CSR-Datei:

```
openssl req -nodes -newkey rsa:4096 -keyout <certificate_key>.key -out  
<certificate_request>.csr -config <smime_config>.cnf
```


6. Die beiden Dateien `<certificate_key>.key` und `<certificate_request>.csr` finden Sie nun in dem Verzeichnis, aus dem Sie den Befehl ausgeführt haben.

Beantragung des Zertifikates

Kehren Sie nun zur Beantragungsoberfläche zurück und kopieren Sie den CSR in das dafür vorgesehene Feld. Nur personenbezogene Email-Adressen sind berechtigt und werden hier aufgelistet. Fehlt eine Ihrer Email-Adressen, wenden Sie sich bitte per Email an noc@tu-braunschweig.de.

Create S/MIME Certificate

What happens here?

 You can request a S/MIME certificate by providing certificate signing request. For more information, please refer to the [documentation](#). (Login required.)


Request by password

Request by csr

Create S/MIME Certificate by CSR

Information

Up to 3 of the following emails are allowed in your CSR

-  • certbot@tu-braunschweig.de
- certrequests@tu-braunschweig.de
- max.mustermann@tu-braunschweig.de
- m.mustermann@tu-braunschweig.de

CSR 

Paste your CSR here.

Nach erfolgreicher Beantragung gelangen Sie auch hier wieder zurück auf die Übersichtsseite und können dort Ihr P7B-Zertifikat herunterladen. Um dieses Zertifikat nutzen zu können, müssen sie zusammen mit dem privaten Schlüssel zuerst ein P12-Zertifikat erstellen. Die Anleitung dazu finden Sie weiter unten.




S/MIME Certificates

[+ Request certificate](#)

What happens here?

 You can get an overview of your S/MIME certificates, request new or revoke existing certificates.

Current and valid S/MIME certificates

ID	Serial	CommonName	Status	Valid to	Type	
1 b4e6c400-xxxx-xxxx-xxxx-xxxxxxxx	60xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	max.mustermann@tu-braunschweig.de	VALID	2028-06-10T12:33:58	PKCS12	 
2 5df95200-xxxx-xxxx-xxxx-xxxxxxxx	52xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	m.mustermann@tu-braunschweig.de	VALID	2028-06-10T12:33:37	PKCS12	 

Konvertieren der erhaltenen P7B-Datei

Nach erfolgreicher Beantragung eines Zertifikats mit eigenem CSR erhalten sie eine Datei mit der Endung ".p7b". Der Dateiname entspricht der ID des erstellten Zertifikates. Hierbei handelt es sich noch nicht um ein vollständiges Zertifikat. Sie müssen aus dieser Datei und dem bei Erstellung des CSRs erzeugten privaten Schlüssel erst noch eine Datei mit der Endung ".p12" erstellen. Dazu

gehen Sie wie folgt vor:

1. Konvertieren der P7B-Datei in das PEM Format:

```
openssl pkcs7 -print_certs -in <cert_id>.p7b -out <cert_id>.pem -inform der
```

2. Exportieren der PEM Dateien in das P12 Format:

```
openssl pkcs12 -export -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -nomac -inkey  
<certificate_key>.key -in <cert_id>.pem -out <cert_id>.p12
```

Bei diesem Befehl werden Sie aufgefordert, ein Passwort einzugeben. Dieses Passwort schützt Ihr Zertifikat vor Missbrauch. Es wird gebraucht, um es in den Zertifikatsspeicher Ihres Betriebssystems zu importieren.