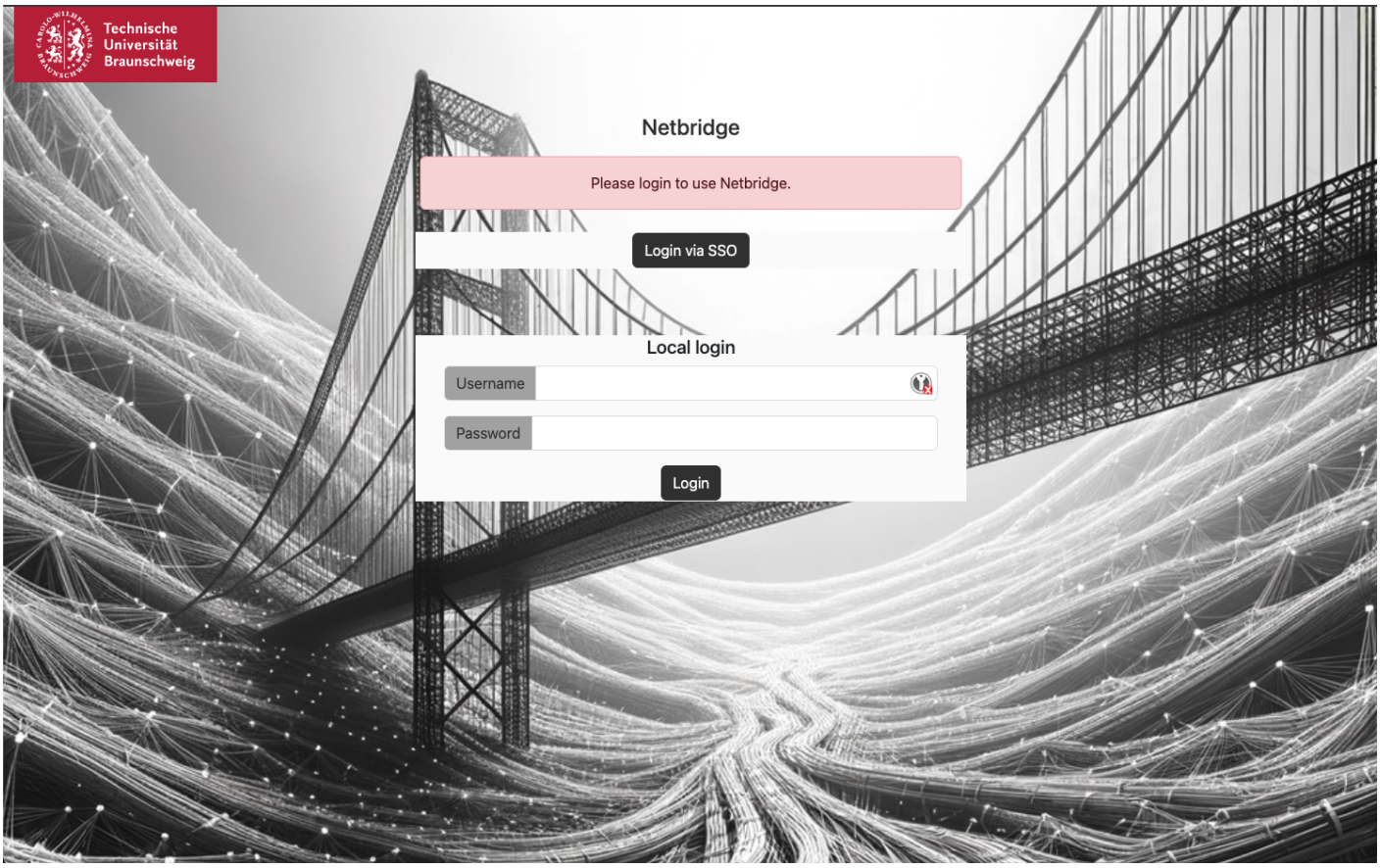
# Allgemeines zu S/MIME Zertifikaten

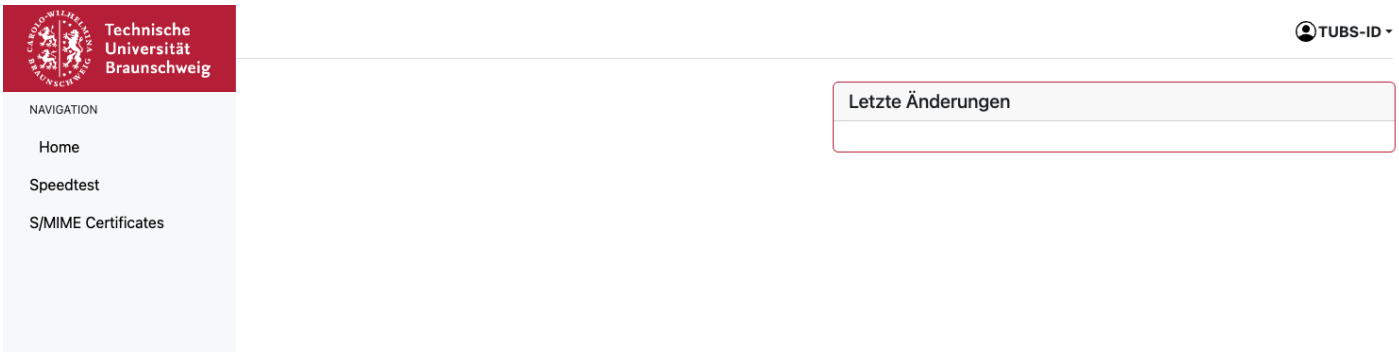
Mit einem S/MIME lässt sich nachweisen, wer der Absender einer E-Mail ist oder von welchem Autor eine Textdatei stammt. Diese sogenannten Nutzerzertifikate können weiterhin eingesetzt werden, um E-Mails zu verschlüsseln, eine Identität im Internet nachzuweisen oder aber sich an Webseiten oder Diensten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

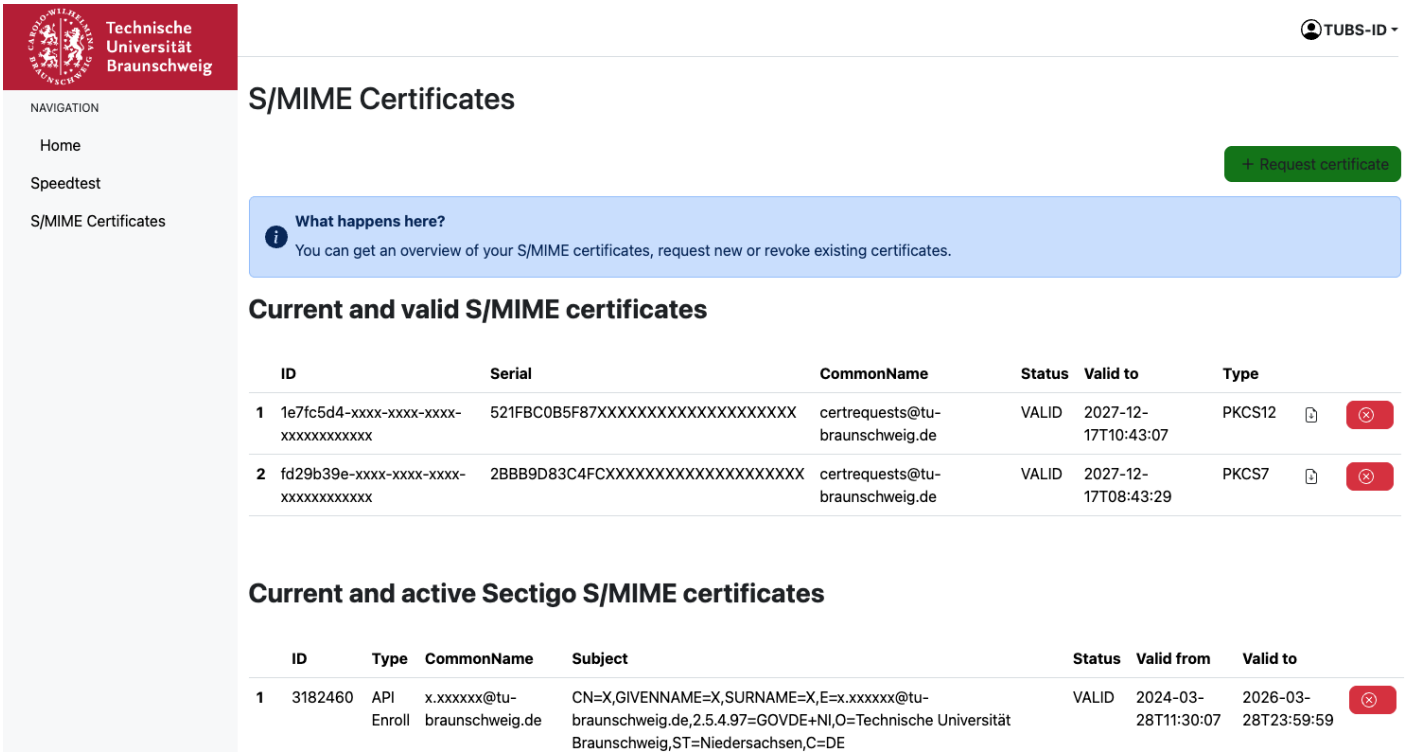
Um in die Zertifikatsverwaltung für S/MIME Zertifikate zu gelangen, navigieren Sie bitte zu folgender URL: https://netbridge.rz.tu-bs.de/ und loggen sich per SSO ein.




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




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.




(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

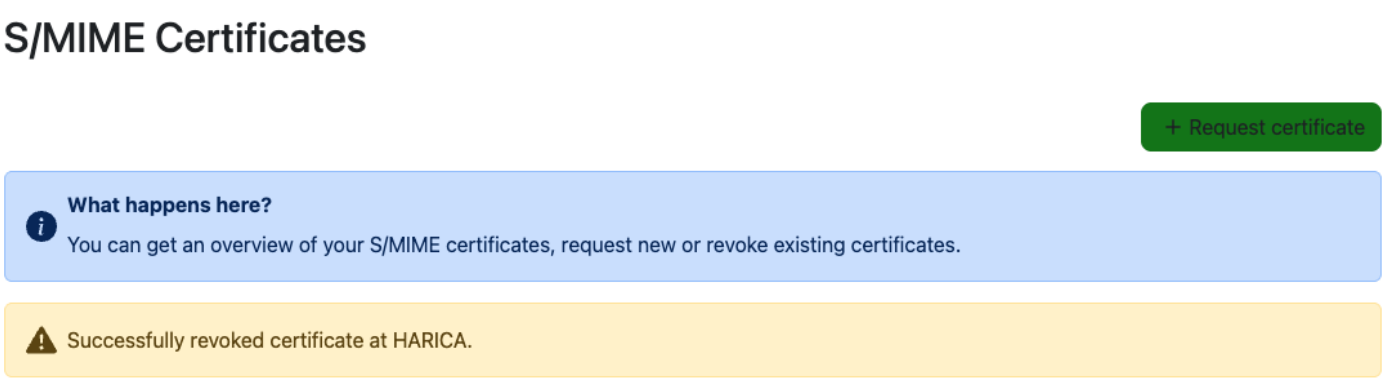
HARICA bietet zwei Arten von Zertifikaten an, sogenannte "email_only" und "IV+OV" Zertifikate.

"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 Srudenten 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 denn Nutzer beeinflussen.

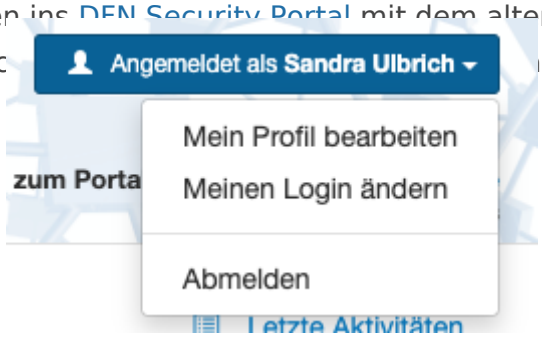
# Zurückziehen eines Zertifikates

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.




# 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 rec men 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.


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

---

Revision #9
Created 2026-01-15 05:20:53 UTC by Sandra Ulbrich
Updated 2026-06-17 11:36:22 UTC by Sandra Ulbrich