S/MIME Zertifikate (Nutzerzertifikate)

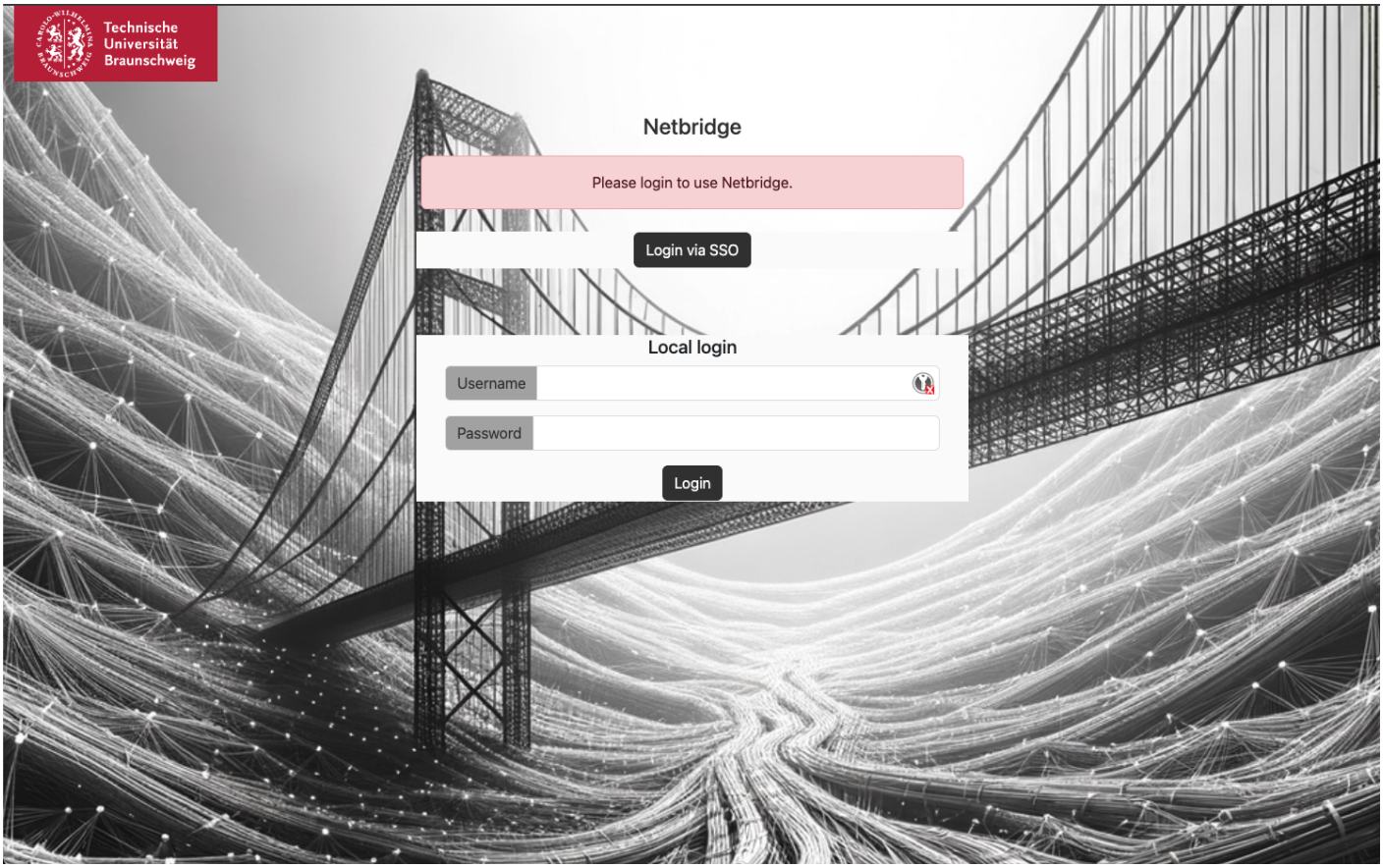
- Allgemeines zu S/MIME Zertifikaten
- Beantragung eines S/MIME Zertifikates durch Passworteingabe
- Beantragung mit einem Zertifikatsantrag (CSR)
- Mit Adobe Acrobat ein PDF signieren

Allgemeines zu S/MIME Zertifikaten

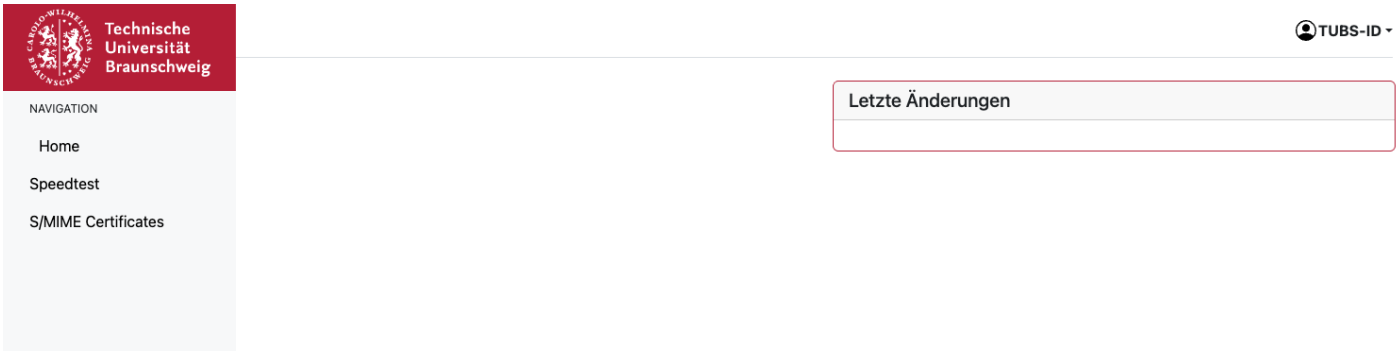
Mit einem S/MIME lässt sich nachweisen, wer der Absender einer E-Mail ist oder von welchem Autor eine Textdatei stammt. Diese sogenannten Nutzerzertifikate können weiterhin eingesetzt werden, um E-Mails zu verschlüsseln, eine Identität im Internet nachzuweisen oder aber sich an Webseiten oder Diensten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

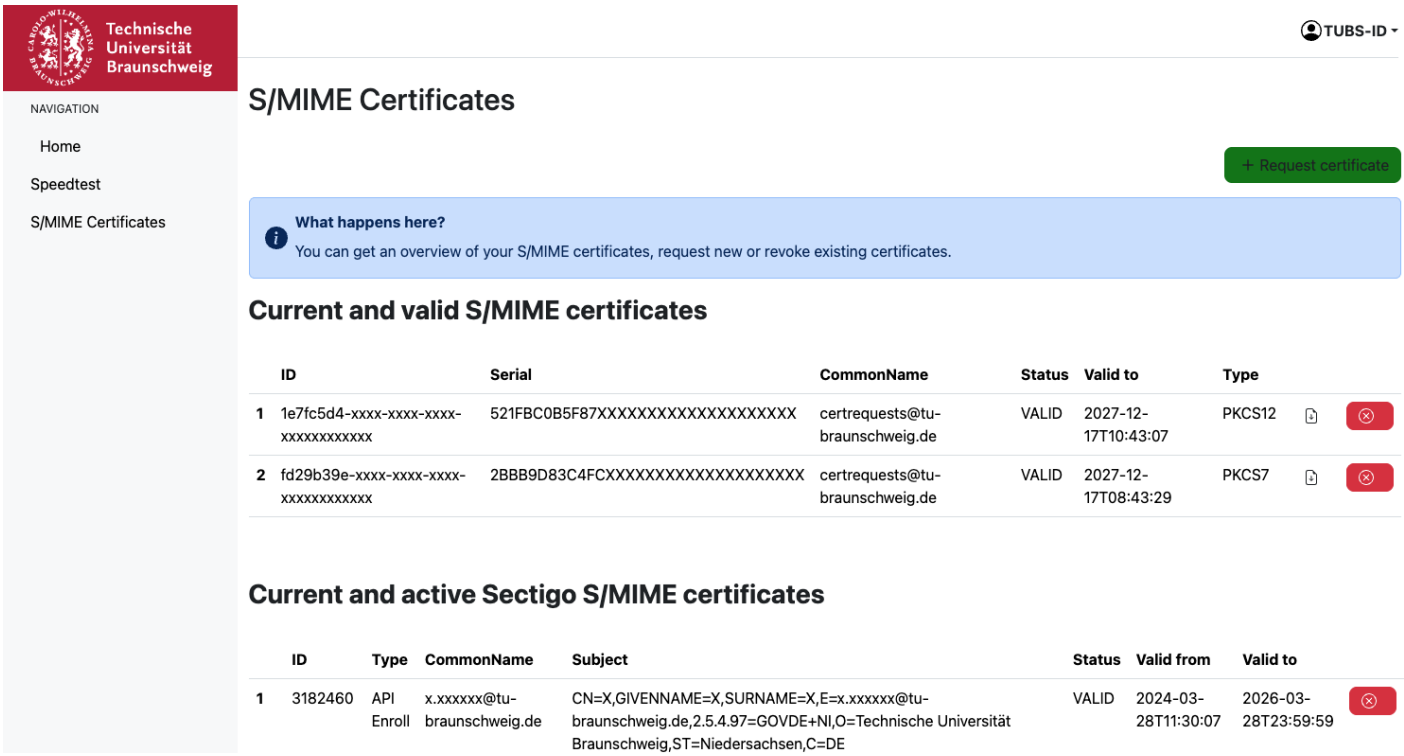
Um in die Zertifikatsverwaltung für S/MIME Zertifikate zu gelangen, navigieren Sie bitte zu folgender URL: https://netbridge.rz.tu-bs.de/ und loggen sich per SSO ein.



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

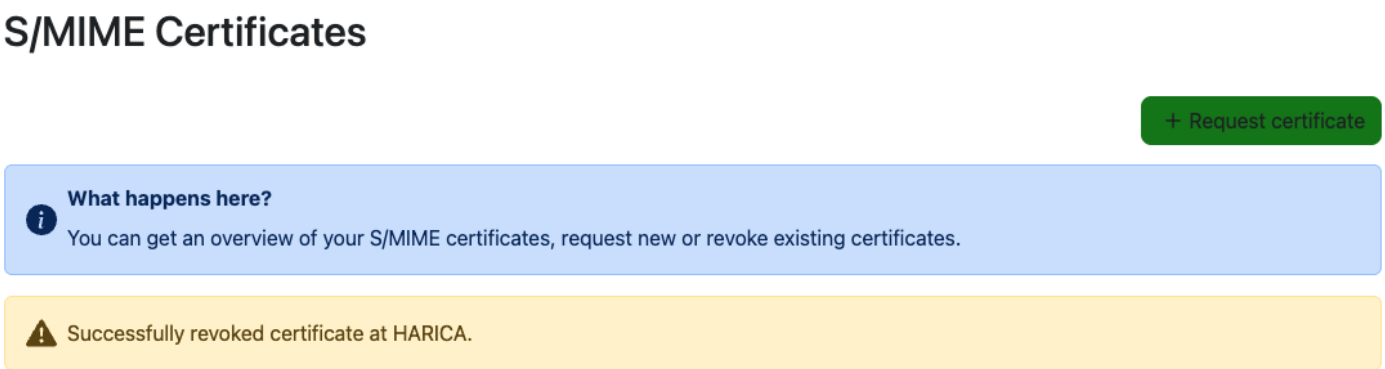
HARICA bietet zwei Arten von Zertifikaten an, sogenannte "email_only" und "IV+OV" Zertifikate.

"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.

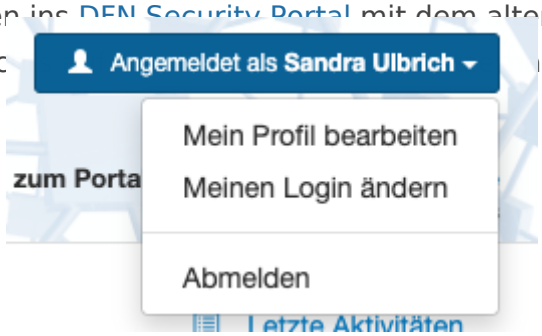
Zurückziehen eines Zertifikates

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.

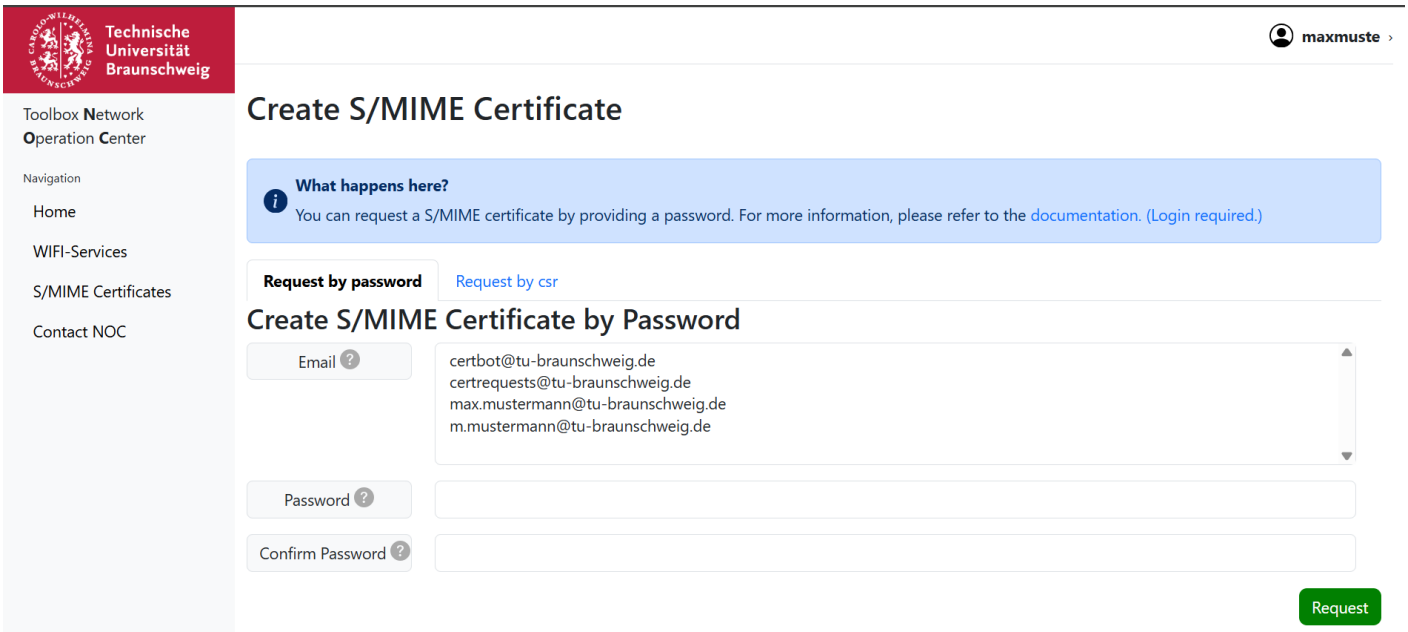
Verwenden Nutzerzertifikates

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

Zertifikatsimport S/MIME Outlook

Beantragung eines S/MIME Zertifikates durch Passworteingabe

Beantragung per Passwort



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.

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-xxxxxxxxxxxx	60xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	max.mustermann@tu-braunschweig.de	VALID	2028-06-10T12:33:58	PKCS12		
2	5df95200-xxxx-xxxx-xxxx-xxxxxxxxxxxx	52xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	m.mustermann@tu-braunschweig.de	VALID	2028-06-10T12:33:37	PKCS12		

Nach erfolgreicher Beantragung, welche einen Moment dauern kann, gelangen Sie wieder auf die Übersichtsseite. Dort können Sie ihr P12-Zertifikat herunterladen und sofort nutzen.

Es gibt zwei verschiedene Arten von S/MIME-Zertifikaten. Studenten und Funktionsaccounts erhalten sogenannte "**email_only**" Zertifikate. "email_only" Zertifikate enthalten nur die ausgewählten Email-Adressen und bezeugen somit, dass diese Email-Adressen an der TU Braunschweig existieren. An der TU Braunschweig angestellte Personen erhalten ein sogenanntes "**IV+OV**" Zertifikat. Diese Zertifikate enthalten zusätzlich den validiertem Vor- und Nachnamen sowie Organisationsinformationen.

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`

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

     - 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
   ```

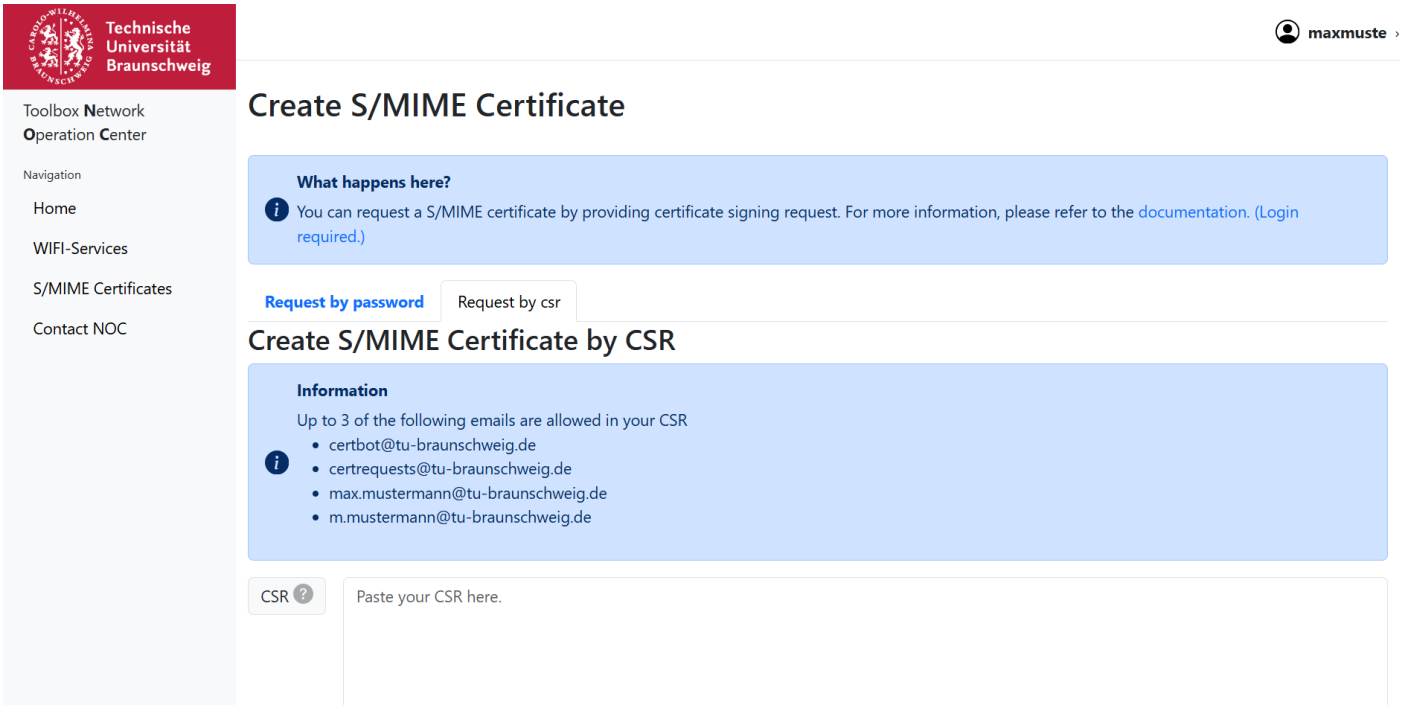
6. Die beiden Dateien <certificate_key>.key und <certificate_request>.csr finden Sie nun in dem Verzeichnis, aus dem Sie den Befehl ausgeführt haben.

> Mit dem Befehl unter Punkt 5 wird ein Zertifikatsantrag mit privatem Schlüssel ohne Passwort erstellt. Für den Fall, dass ein privater Schlüssel mit Passwort gewünscht ist, nutzen Sie bitte folgenden Befehl:

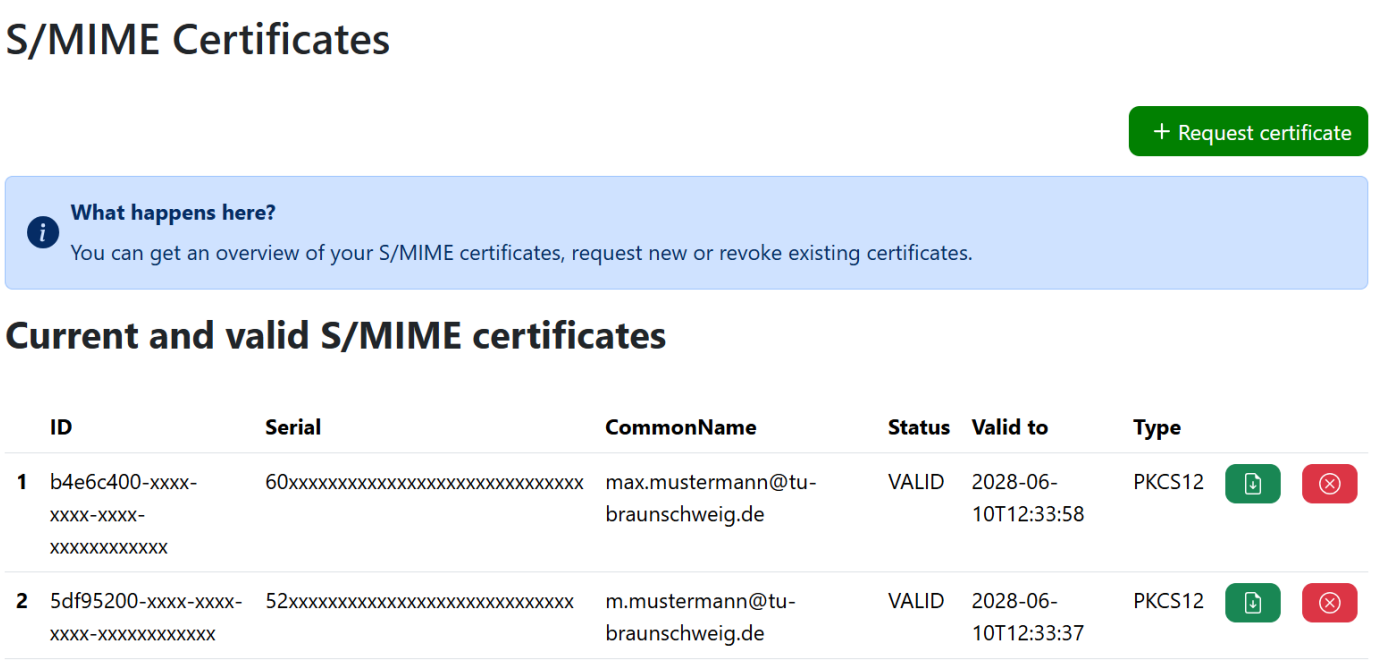
```
openssl req -new -newkey rsa:4096 -keyout <certificate_key>.key -out <certificate_request>.csr
-config <smime_config>.cnf
```

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.



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.



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 Datein in das P12 Format:

   ```
   openssl pkcs12 -export -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -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.

Mit Adobe Acrobat ein PDF signieren

In dem Dokument taucht nun die Signatur auf, diese kann (r

Mit einem S/MIME-Zertifikat lassen sich PDF-Dokumente digital signieren. Der Empfänger kann dadurch eindeutig nachvollziehen, dass das Dokument wirklich von Ihnen unterschrieben wurde. Das gleiche Zertifikat kann in verschiedenen Programmen verwendet werden, die das Signieren von PDFs unterstützen. In dieser Anleitung zeigen wir, wie Sie die Signaturfunktion in **Adobe Acrobat** nutzen.

1. S/MIME Zertifikat beantragen

Als erstes müssen Sie das S/MIME Zertifikat selbst beantragen, falls Sie bisher noch keins besitzen.

Folgen Sie dafür der Anleitung "Beantragung eines S/MIME Zertifikates durch Passworteingabe" und kehren hierher zurück, sobald sie das Zertifikat beantragt und gespeichert haben.

2. Zertifikat zu Adobe Acrobat hinzufügen

Als nächstes wird das S/MIME Zertifikat importiert, um damit eigene PDFs zu signieren. Halten Sie dafür ihr S/MIME Zertifikat im .p12-Format bereit und fahren Sie mit der Schritt-Für-Schritt-Anleitung fort.

Anleitung: Zertifikat zu Adobe hinzufügen

1. Adobe Reader öffnen und die Einstellungen über "Menü - Einstellungen" öffnen.

Adobe Reader öffnen und die Einstellungen über "Menü - Einstellungen" öffnen.

2. In der Kategorie "Unterschriften" den Button "Weitere" im Bereich "Identitäten und vertrauenswürdige Zertifikate" auswählen.

In der Kategorie "Unterschriften" den Button "Weitere" im Bereich "Identitäten und vertrauenswür

3. Wählen Sie nun "Digitale IDs" aus und fügen Sie über das "+"-Symbol eine neue eigene ID hinzu.
Wählen Sie nun "Digitale IDs" aus und fügen Sie über das "+"-Symbol eine neue eigene ID hinzu.

4. Die digitale ID soll über eine Datei importiert werden.
Die digitale ID soll über eine Datei importiert werden.

5. Wählen Sie nun Ihr persönliches Nutzerzertifikat im .p12-Format für den Import aus.
Wählen Sie nun Ihr persönliches Nutzerzertifikat im .p12-Format für den Import aus.

6. Geben Sie das Passwort des Nutzerzertifikats ein, um dieses zu entsperren. Dieses Passwort haben Sie beim Beantragen des Zertifikats selbst festgelegt.
Geben Sie das Passwort des Nutzerzertifikats ein um dieses zu entsperren.

7. Nach dem erfolgreichen Entsperren des Nutzerzertifikates werden Informationen zum Zertifikat angezeigt. Klicken Sie auf "Fertigstellen".
Nach dem Erfolgreichen Entsperren des Nutzerzertifikates werden Informationen zum Zertifikat ar

Das Zertifikat wird nun als "Digitale ID" angezeigt und kann im Folgenden für das Signieren von PDFs verwendet werden.
Das Zertifikat wird nun als "Digitale ID" angezeigt und kann im Folgenden für das Signieren von PI

3. PDF signieren

Nachdem diese Vorbereitungen abgeschlossen sind, können Sie nun PDFs signieren.

Anleitung: PDF in Adobe signieren

1. Öffnen Sie eine PDF mit dem Adobe Reader. Gehen Sie dann in das Menü "Werkzeuge" und wählen "Zertifikate" aus.
Öffnen Sie eine PDF mit dem Adobe Reader. Gehen Sie dann in das Menü "Werkzeuge" und wähle

2. Klicken Sie auf "Digital unterschreiben". Sie können mit der Maus nun ein Rechteck in den Teil des PDFs ziehen, in welchem Ihre digitale Unterschrift angezeigt werden soll.

Klicken Sie auf "Digital unterschreiben".

Nun können Sie mit der Maus ein Rechteck an der Stelle ziehen, wo Ihre digitale Signatur in

3. Wählen Sie nun Ihr zuvor importiertes Nutzerzertifikat zum Signieren aus. Eine Vorschau der Signatur wird angezeigt. Sie müssen Ihr Passwort vom Nutzerzertifikat eingeben, um dieses zu entsperren und für die Signatur zu verwenden.

Wählen Sie Ihr zuvor importiertes Nutzerzertifikat zum Signieren aus.

Eine Vorschau der Signatur wird angezeigt. Sie müssen Ihr Passwort vom Nutzerzertifikat ein

4. Das signierte Dokument wird in einer neuen Datei gespeichert. Wählen Sie einen passenden Dateinamen und speichern Sie die signierte PDF ab. Die originale PDF-Datei wird nicht überschrieben.
Das signierte Dokument wird in einer Extra-Datei gespeichert. Wählen Sie einen passenden

5. In dem neuen Dokument taucht nun die Signatur auf. Diese kann auf Ihre Gültigkeit überprüft werden - Adobe Acrobat tut dies beim Öffnen des Dokuments automatisch und zeigt die Ergebnisse über dem Dokument an.

In dem Dokument taucht nun die Signatur auf, diese ka

Problemlösungen

Die Signatur konnte nicht validiert werden

Adobe benutzt bestimmte Signaturen innerhalb Ihres Zertifikats, um zu bestätigen, das dieses tatsächlich gültig ist. Dafür wird auf einen internen Speicher von bereits bekannten und vertrauten sogenannten Wurzelzertifikaten zurückgegriffen. Es ist möglich, das das Wurzelzertifikat von Harica, welche für die TU Braunschweig die S/MIME Zertifikate ausstellt, nicht auf ihrem Gerät vorinstalliert ist. Um dieses Wurzelzertifikat von Harica dem Speicher hinzuzufügen, gehen Sie daher wie folgt vor:

1. Laden Sie das Wurzelzertifikat über diesen Link auf ihr Gerät: HARICA-Client-Root-2021-RSA.p7b

2. Öffnen Sie die Einstellung von Adobe Reader über Menü > Einstellungen.

Adobe Reader öffnen und die Einstellungen über "Menü - Einstellungen" öffnen.

3. Wählen Sie in der Kategorie "Unterschriften" den Button "Weitere" im Bereich "Identitäten und vertrauenswürdige Zertifikate" aus.

In der Kategorie "Unterschriften" den Button "Weitere" im Bereich "Identitäten und ver

4. Im Bereich "Vertrauenswürdige Zertifikate" kann nun über den "Import"-Button das Wurzelzertifikat importiert werden.

Im Bereich "Vertrauenswürdige Zertifikate" kann nun über den "Import"-Button das Wu

5. Weiter geht es über den Button "Durchsuchen".

Weiter geht es über den Button "Durchsuchen".

6. Wählen Sie nun das zuvor heruntergeladene Wurzelzertifikat aus.

Wählen Sie nun das zuvor heruntergeladene Wurzelzertifikat aus.

7. Nach dem Öffnen wird das Wurzelzertifikat angezeigt. Klicken Sie zuerst auf den Namen des Wurzelzertifikats im Bereich "Kontakte", dann erneut auf den Namen im Bereich "Zertifikate" und anschließend auf den Button "Vertrauenswürdigkeit".

Nach dem Öffnen wird das Wurzelzertifikat angezeigt. Klicken Sie zuerst auf den Name

8. Das Wurzelzertifikat soll als vertrauenswürdiger Stamm verwendet und für zertifizierte Dokumente als vertrauenswürdig gelten. Dies ist notwendig, damit Signaturen von Nutzerzertifikaten von HARICA im PDF-Viewer als gültig angezeigt werden.

Das Wurzelzertifikat soll als vertrauenswürdiger Stamm verwendet und für zertifizierte

9. Nun kann das Wurzelzertifikat mit den richtigen Einstellungen importiert werden.

Nun kann das Wurzelzertifikat mit den richtigen Einstellungen importiert werden.

10. Der Import des Wurzelzertifikats ist erfolgreich. Das Wurzelzertifikat wird nun in der Liste angezeigt und Signaturen, welche mit Zertifikaten von HARICA ausgestellt wurden, sollten nun als valide angezeigt werden. Der Import des Wurzelzertifikats ist erfolgreich.

Das Wurzelzertifikat wird nun in der Liste angezeigt.

Sollte Ihr eigenes Zertifikat weiterhin als ungültig angezeigt werden, bitten wir Sie, ein neues Zertifikat - wie unter Punkt 1 dieser Dokumentation beschrieben - zu beantragen.