

Nutzerzertifikat beantragen

Diese Anleitung beschreibt, wie Sie ein Nutzerzertifikat (S/MIME-Zertifikat) beantragen können.

DAS ZERTIFIKAT KANN NICHT ZUM SIGNIEREN VON DOKUMENTEN VERWENDET WERDEN! Bitte sehen Sie von einer Beantragung eines Nutzerzertifikats für diesen Anwendungszweck ab!

Hintergrund

Digitale Nutzerzertifikate (S/MIME-Zertifikate) bestehen aus einem Schlüsselpaar (privater und öffentlicher kryptographischen Schlüssel) sowie der Bestätigung ihrer Identität durch eine Zertifikat-Authorität. Sie erlauben Ihnen das verschlüsselte Senden von E-Mails (unter Verwendung des öffentlichen Schlüssels Ihres Kommunikationspartners), sowie die digitale und fälschungssichere Unterschrift von E-Mails unter Verwendung Ihres privaten Schlüssels. Damit die Sicherheit gewährleistet und möglicher Missbrauch ihrer digitalen Unterschrift vermieden werden, ist es essentiell, dass Sie ihren privaten Schlüssel geheim halten und mit einem guten Passwort schützen.

Das Nutzerzertifikat kann zum digitalen Signieren und Verschlüsseln von E-Mails, oder auch zur Authentifizierung (zertifikatbasierter Login) verwendet werden.

Da in unserem E-Mail-System die E-Mail-Adressen zur Zeit nicht grundsätzlich in der Form Vorname.Nachname@FB.hs-fulda.de vorliegen, kann das Zertifikat für diese Zwecke ggf. nicht mit dem GroupWise-Client genutzt werden, möglich ist die Nutzung jedoch mit anderen E-Mail-Clients, wie Thunderbird oder Outlook.

Die **digitale Signierung von Dokumenten** - als Alternative zur handschriftlichen Unterschrift - unterliegt hohen Auflagen und **kann mit den derzeit zur Verfügung stehenden Mitteln nicht angeboten werden**. Juristisch wird zwischen *einfachen, fortgeschrittenen und qualifizierten elektronischen Signaturen* unterschieden, wobei diese sich in der *Art der Identitätsprüfung* und der *Art der Erzeugung* unterscheiden. Nutzerzertifikate die aus der Sectigo PKI bezogen werden genügen (auf Grund der organisatorischen Gestaltung des Prozesses an der Hochschule Fulda) derzeit ausschliesslich den Anforderungen an eine einfache elektronische Signatur, nicht aber an eine fortgeschrittene oder qualifizierte elektronische Signaturen nach eIDAS. Rechtlich ist das Resultat daher gleichzusetzen mit dem Einfügen des eigenen Namens in Druckbuchstaben oder als Bild in ein Dokument. Die Beweiskraft ist juristisch kaum gegeben. **Für Dokumente, die nur Hausintern verwendet werden, ist die Nutzung einer elektronischen Signatur nicht nötig bzw. vorgesehen. Für Dokumente, die im Rahmen externer Kommunikation verwendet werden, ist die Beweiskraft juristisch nicht gegeben und die Nutzung elektronischer Signaturen daher derzeit nicht möglich.**

Zertifikat beantragen

Die Beantragung des Zertifikats erfolgt über das Webportal der Zertifizierungsstelle HARICA:
<https://cm.harica.gr>.

Klicken Sie auf der Anmeldeseite zunächst die Schaltfläche **Academic Login**. Tippen Sie „Fulda“ in das Suchfeld und wählen Sie anschließend die Organisation **Hochschule Fulda** aus. Anschließend können Sie sich über den gewohnten **AAI-Login** mit Ihrer fd-Nummer und dem dazugehörigen Passwort anmelden.

Nach erfolgreicher Anmeldung wird Ihnen das HARICA-Dashboard angezeigt. Klicken Sie im linksseitigen Menü auf **Email** und wählen Sie anschließend das Produkt **Email-only**.

Die folgenden drei Ansichten können Sie jeweils mit einem Klick auf **Next** bzw. **Submit** bestätigen.

The first screenshot shows the 'Email / Request New Certificate' step, where a user selects 'Email-only' as the certificate type and enters their email address. The second screenshot shows the 'Validation' step, where the user is prompted to validate their email via a link sent to the specified address. The third screenshot shows the final 'Summary' step before submission, displaying the certificate type (S/MIME email-only), service duration (2 years), and the email address used (stefan.friedmann@rz.hs-fulda.de). A checkbox for accepting terms and conditions is checked.

Sie erhalten nun eine Bestätigungs-E-Mail von HARICA, mit der Sie die Kontrolle über die angegebene E-Mail Adresse nachweisen. Öffnen Sie die E-Mail und klicken Sie auf den Text **Confirm**. Sie werden dadurch wieder auf die HARICA-Webseite geleitet und müssen hier nochmals auf **Confirm** klicken.

The left screenshot shows an email from 'HARICA Certificate Manager (CM) <noreply@harica.gr>' to the user. It contains instructions to validate the email and a 'Confirm' link. An arrow points to the 'Confirm' link. The right screenshot shows a 'Validate your email address' page with the email address 'stefan.friedmann@rz.hs-fulda.de' and a 'Confirm' button.

Nun wird der zuvor gestartete Vorgang angezeigt und können hier auf **Enroll your certificate** klicken, um das eigentliche Zertifikat zu erstellen.

The dashboard shows a table of 'Ready Certificates'. One row is highlighted for an S/MIME certificate, which has a red arrow pointing to the 'Enroll your Certificate' button in the 'Actions' column.

Das Formular erlaubt Ihnen die Festlegung der Zertifikat-Parameter. Wir empfehlen hier lediglich die Schlüssellänge auf 4096 Bit zu erhöhen und keine sonstigen Änderungen vorzunehmen.

Certificate Enrollment

[Generate Certificate](#)

[Submit CSR manually](#)

or

Generate your certificate in .p12 format.

Use your (already created) CSR and submit it here.

Set a passphrase to protect your certificate. Please note that the passphrase is required to use the certificate and should therefore be **secured and not forgotten**.

Algorithm

Key size

RSA (default)

4096

Set a passphrase

.....



Confirm passphrase

.....



I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.

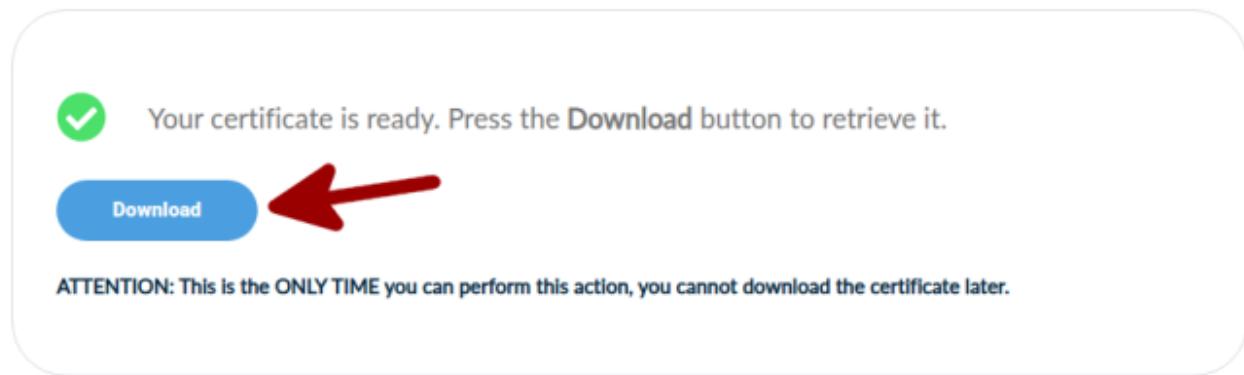
[Close](#)

[Enroll Certificate](#)

Abschließend wird Ihnen das Zertifikat zum Download angeboten.

Speichern Sie das Zertifikat in diesem Schritt unbedingt ab, da dies später nicht mehr möglich ist.

Get your certificate



Die Datei enthält Ihr vollständiges S/MIME Zertifikat (privaten und öffentlichen Schlüssel) und ist mit dem zuvor festgelegten Passwort geschützt. Heben Sie diese Datei gut auf, da sie quasi ein Backup Ihres gesamten S/MIME-Schlüsselpaares enthält und Ihnen erlaubt, das Nutzerzertifikat in weitere Programme (E-Mail, Webbrower) oder auf anderen PCs zu importieren.

Informationen zur Nutzung des Zertifikats finden Sie [hier](#).

From:
<https://doku.rz.hs-fulda.de/> - **Rechenzentrum**



Permanent link:
<https://doku.rz.hs-fulda.de/doku.php/docs:dfnpki:client>

Last update: **20.10.2025 12:00**