Serverzertifikat beantragen

Diese Seite befindet sich aktuell noch im Aufbau ⚠️

Hinweis

Das Serverzertifikat OV Multi-Domain aus TCS enthält sowohl den Zertifikatzweck *serverAuth* als auch *clientAuth*. Es können also prinzipiell alle Zwecke mit dem Standard-Zertifikatprofil abgedeckt werden.

IP-Adressen können nicht in Serverzertifikate aus TCS aufgenommen werden. Die Antragswege über Webformulare ergeben Fehlermeldungen. Beim Einreichen eines Requests mit einer IP-Adresse im *SubjectAlternativeName* wird diese stillschweigend herausgefiltert.

Mit OV Multi Domain können Wildcard-Zertifikate erstellt werden, wobei die Wildcard-Namen sowohl im *SubjectAltName* als auch im *CN* verwendet werden können.

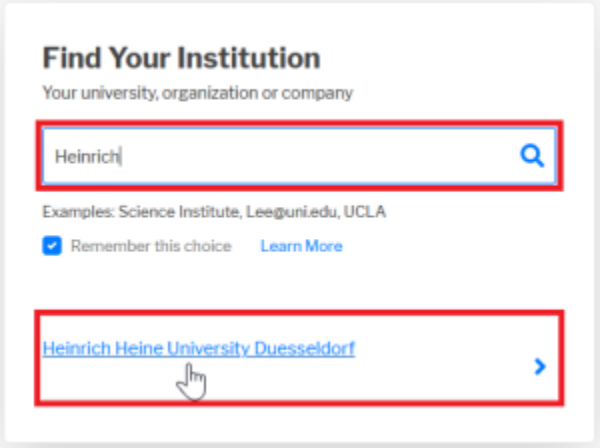
Es können nur Serverzertifikate für *.hhu.de und *.uni-duesseldorf.de-Domains erstellt werden.

Schritt-für-Schritt-Anleitung

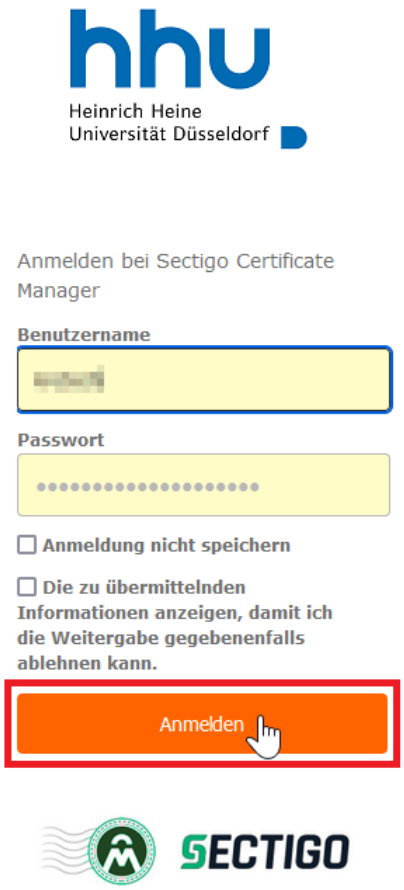
Serverzertifikat beantragen

1. Klicken Sie auf folgenden **Link**: **Serverzertifikat beantragen**

2. Wählen Sie die HHU aus, indem Sie im Suchfeld "HHU", "Heinrich" o.ä. eingeben. Im unteren Teil wird Ihnen unsere Einrichtung angeboten. Mit Klick auf das Feld **„Heinrich Heine University Duesseldorf“** werden Sie zur Anmeldung weitergeleitet.



3. Im Anmeldefenster tragen Sie unter Benutzername Ihre **Uni-Kennung** und das dazugehörige **Passwort** ein und klicken anschließend auf **„Anmelden“**.



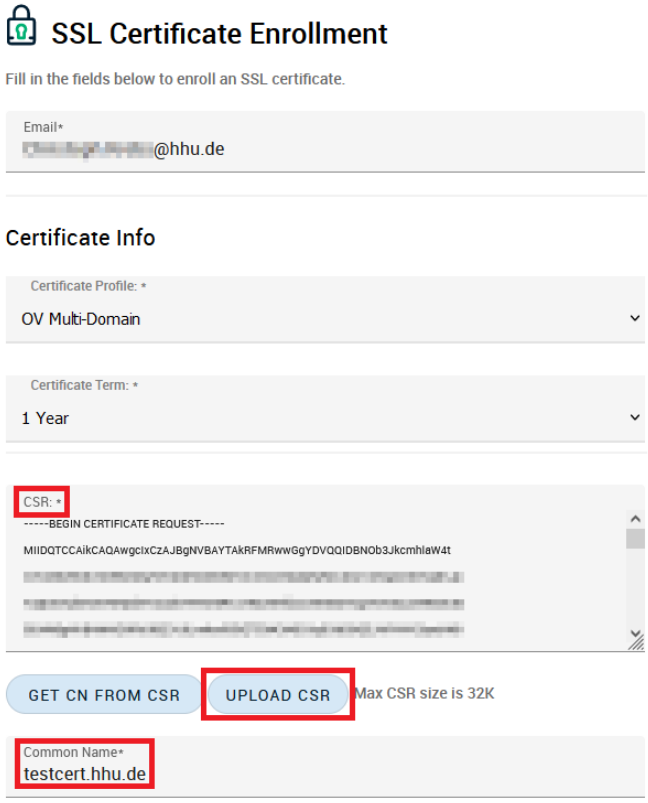
> Es werden Ihnen nun die an Sectigo übermittelten Attribute angezeigt. Das sind im Wesentlichen Ihr Name und die Mailadresse sowie die Einrichtung von der aus Sie sich anmelden (in Ihrem Fall: HHU Düsseldorf). Diese Informationen werden benötigt, um das Zertifikat Ihrer Person zuordnen zu können. Mit Klick auf **„Akzeptieren“** werden Sie weitergeleitet.

4. Ihnen wird nun die Mailadresse des Zertifikatsinhabers angezeigt. Das **Zertifikatsprofil** (OV Multi-Domain) und die **Gültigkeitsdauer** (1 Jahr) sind **festg elegt**.

Bei der Methode können Sie entscheiden, ob Sie Ihre .csr-Datei **hochladen** („UPLOAD CSR“) **oder** Ihren CSR mittels Copy & Paste in das Eingabefeld („CSR: *“) **kopieren**.

> **Hinweis**
>
> Sie haben noch keinen CSR? Wie Sie einen CSR erstellen, erfahren Sie hier: **CSR erstellen**
>
> Es gibt eine Größenbeschränkung des CSR auf 32k. Laut Sectigo liegt das Limit der Anzahl alternativer Namen bei 250. In der Praxis konnten jedoch auch schon 400 alternative Namen aufgenommen werden. Die Größe für akzeptierte CSR liegt irgendwo zwischen 15000 und 19000 Byte.
>
> Nicht verfügbar sind die Funktionalitäten: *Webserver mustStaple, DomainController*

Anschließend sollte der Name Ihrer Domain (**CN**/Common Name) **automatisch** vom CSR **übernommen** werden. Wenn nicht, geben den Domainnamen (z.B. dienst.hhu.de) händisch ein.

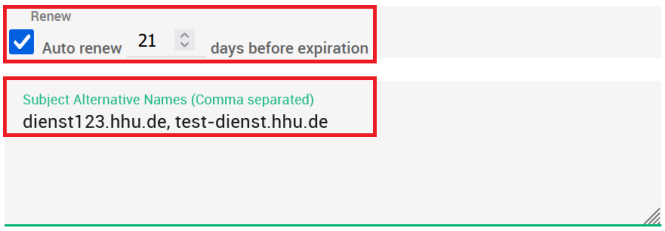


Fehlerbehebung

Es kann zu Problemen kommen, wenn Ihre Haupt-Mail-Adresse mit "@uni-duesseldorf.de" (anstatt "@hhu.de") endet. In diesem Fall kann die Fehlermeldung "Access code or email is invalid" unter dem Feld Ihrer Email-Adresse erscheinen.

Hauptemailadresse ändern.

5. Optional: Wenn Ihr Zertifikat **nach einem Jahr** abläuft, können Sie bereits jetzt unter "Renew" **automatisiert** eine Mail erhalten, die Sie darüber informiert, dass Ihr Zertifikat in x Tagen ausläuft. Setzen Sie dazu den Haken bei „Auto renew". Im Feld "External Requester" können Sie weitere Mail-Adressen angeben, die eine Benachrichtigungs-Mail erhalten sollen. (Stand 2023-07: Es ist scheinbar möglich, dass keine E-Mail zur Erinnerung verschickt wird. Erfahrungen bitte an ca@hhu.de.)



6. Auch die **„Subject Alternative Names"** sollten **automatisch** vom CSR **übernommen** werden. Falls nicht, tragen Sie die entsprechenden *.hhu.de bzw. *.uni-duesseldorf.de-Domains händisch ein und trennen diese mit einem Komma und Leerzeichen.

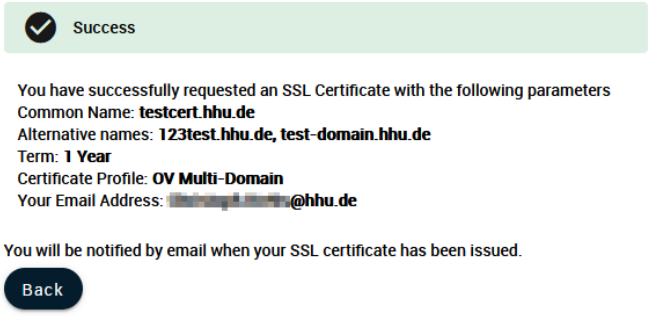
7. Optional: Haben Sie sich für die **jährliche, automatisierte Benachrichtigung** entschieden, müssen Sie nun ein **Passwort** („Annual Renewal Passphrase") festlegen, um Ihr Zertifikat jährlich erneuern - oder widerrufen zu können. Geben Sie das Passwort 2x ein.

8. Um uns zu benachrichtigen, dass ein Zertifikatsantrag gestellt wurde, schreiben Sie bitte in das Feld „External Requester" ca@hhu.de. Hier können Sie außerdem **weitere Mailadressaten** angeben, die Benachrichtigungen zum Zertifikat erhalten. Die Mailadressen müssen auf @hhu.de oder @uni-duesseldorf.de enden. Mehrere Mailadressen trennen Sie mit einem Komma und Leerzeichen.

8. Optional: Unter „Comments“ können Sie der CA (Certificate Authority) noch ergänzende Informationen zukommen lassen.

9. Mit Klick auf **„Enroll“** schicken Sie Ihren Antrag ab. Das Zertifikat wird manuell von der CA bestätigt.

Die Bearbeitungszeit beträgt 2 Arbeitstage . Sie werden per E-Mail benachrichtigt, sobald Ihr Zertifikat ausgestellt wurde.



10. Optional: Nach Erhalt des Zertifikats per Mail können Sie sich erneut bei **Sectigo** anmelden, um eine **Liste aller Ihrer genehmigten Zertifikate** zu sehen. Hinweis: es werden nur Zertifikate angezeigt, bei denen der eingeloggte Nutzer **und** die URL des Antragsformulars übereinstimmen. Falls die URL des Formulars sich geändert hat, werden die Zertifikate in der Darstellung ausgefiltert, aber sind natürlich weiterhin gültig.