Gruppenzertifikate (Zertifikate für Funktionskennung) beantragen

- Kurzanleitung
- Ausführliche Anleitung
- Gruppenzertifikat verlängern

Postfächer mit mehreren Nutzenden

Es kann für ein Postfach nur ein Zertifikat beantragt werden. D.h. eine Person nutzt den Einladungslink zur Erstellung und bekommt das Zertifikat inkl. privatem Schlüssel. Dieses kann weitergegeben werden, allerdings ist darauf zu achten, dass dies auf sichere Weise geschieht. Dazu bietet es sich an, verschlüsselte E-Mails zu benutzen (nur möglich, wenn man für das verwendete Postfach bereits ein Zertifikat besitzt). USB-Sticks (nachher löschen) etc. können zu dem Zweck ebenfalls verwendet werden.

Verantwortliche mehrerer Postfächer

Wer mehrere Postfächer mit Zertifikaten auszustatten hat, muss sich nicht die Mühe machen, aus jedem heraus eine Anfrage zu stellen. Es kann eine Liste der E-Mailadressen an ca@hhu.de geschickt werden. Wichtig: es müssen exakt dieselben Zeichenketten (insbesondere Groß-/Kleinschreibung) sein.

Kurzanleitung

Zur Beantragung eines Nutzerzertifikats für eine Funktionskennung schicken Sie bitte eine E-Mail **von dem Funktionspostfach aus** mit folgenden Informationen der verantwortlichen Person:

- Vorname
- Nachname
- E-Mailadresse

an **ca@hhu.de**. Sie erhalten spätestens nach wenigen Werktagen einen Einladungslink per E-Mail. Die verantwortliche Person kann dann ein Schlüsselpaar erzeugen und das Zertifikat inkl. des privaten Schlüssels als .p12-Datei herunterladen.

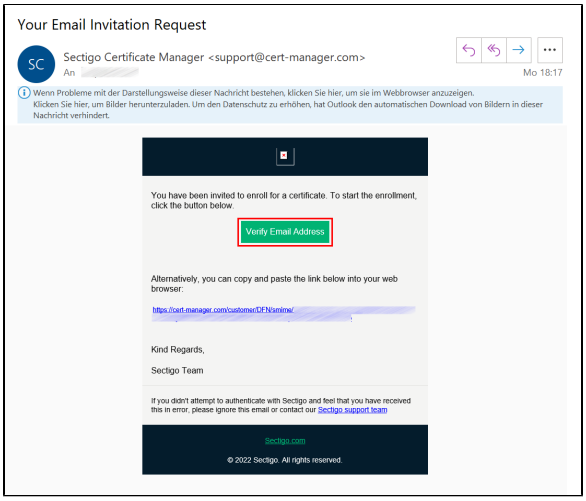
Ausführliche Anleitung

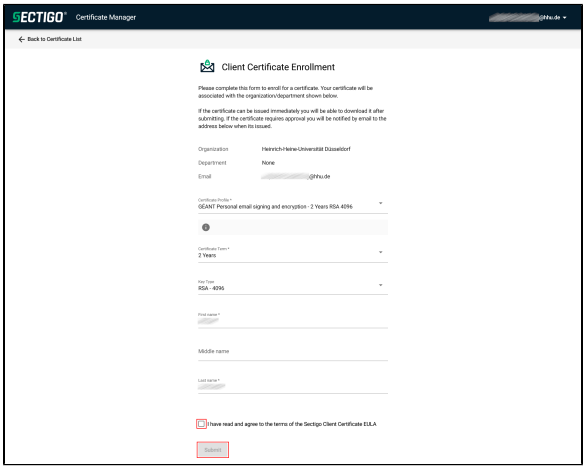
Schritt 1: Sie können den Antrag auf ein Gruppenzertifikat formlos an die Adresse **ca@hhu.de** schicken. Der Antrag sollte folgende Informationen enthalten:

- Name, Vorname des Antragstellers
- persönliche E-Mail-Adresse des Antragstellers.

⚠️ Bitte beachten Sie, dass der Antrag **aus dem Funktionspostfach heraus** verschickt werden muss, für welches das Gruppenzertifikat beantragt wird! ⚠️

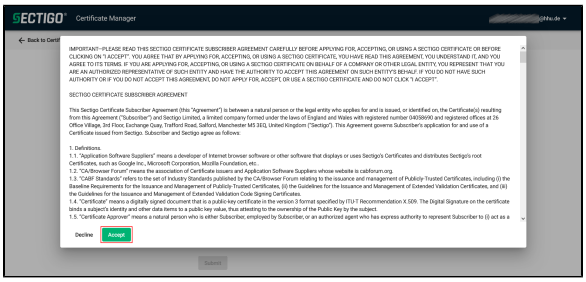
Schritt 2: Sobald der Antrag bearbeitet wurde, erhalten Sie vom Dienstleister Sectigo eine **Einladungsmail** mit einem Link. Um das Zertifikat zu aktivieren, klicken Sie den Link/Button **"Verify Email Adress"** an.



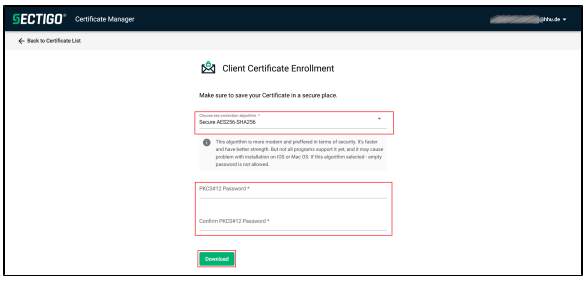


Schritt 3: Im Browser öffnet sich nun eine Homepage von Sectigo. Anders als früher ist die Gültigkeitsdauer des Gruppenzertifikats jetzt nicht mehr variabel festlegbar, sondern automatisch auf zwei Jahre befristet. Auch der "Key Type" lässt sich nicht mehr verändern, sondern ist auf "RSA-4096" voreingestellt.

Um fortzufahren, setzen Sie bitte unten auf der Seite ein **Häkchen** bei **"I have read and agree to the terms of the Sectigo Client Certificate EULA"** (Zustimmung zu den Nutzungsbedingungen). Klicken Sie anschließend auf **"Submit"**.

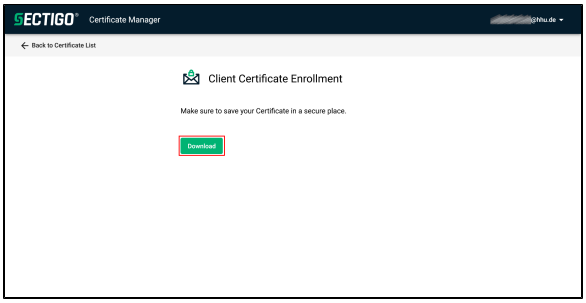


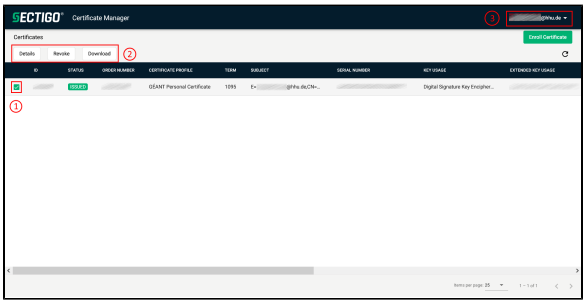
Schritt 4: Sie bekommen nun die Nutzungsbedingungen angezeigt. Stimmen Sie diesen mit einem Klick auf **"Accept"** zu.



Schritt 5: Achten Sie darauf, dass als Verschlüsselungsalgorithmus **"Secure AES256-SHA256"** ausgewählt ist. Legen Sie bei **"PKCS#12 Password"** ein Passwort für Ihr Zertifikat fest, und wiederholen ("Confirm") Sie dieses in der nächsten Zeile. Klicken Sie anschließend auf **"Download"**, um das Zertifikat herunterzuladen.

Schritt 6: Sie haben nun die Möglichkeit, über **"Download"** die Zertifikatsdatei im .p12-Format herunterzuladen.



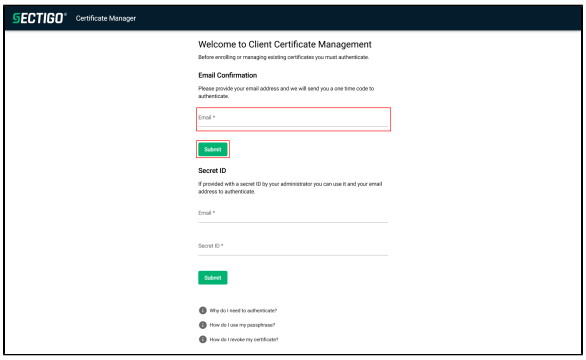


Schritt 7: Sie gelangen nun auf eine Übersichtsseite mit Ihren Zertifikaten. Durch (1) das Setzen eines Häkchens können Sie Ihre Zertifikate (2) verwalten: Sie können sich die Details anschauen, das Zertifikat für ungültig erklären ("Revoke") oder downloaden.

Sie können sich oben rechts von der Sectigo-Seite abmelden. Die Aktivierung des Gruppenzertifikats ist abgeschlossen.

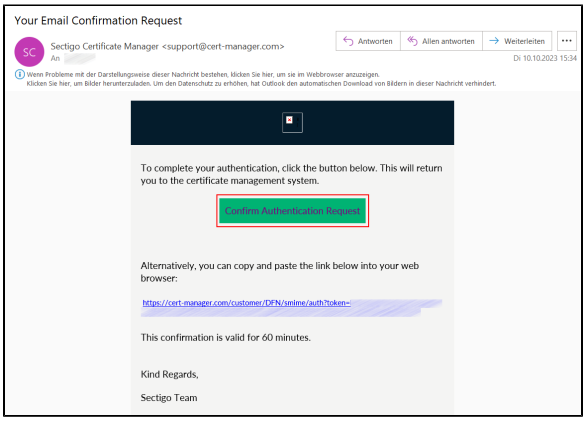
Wie Sie das Zertifikat in ein **E-Mail-Programm einbinden** können, sehen Sie hier.

Gruppenzertifikat verlängern



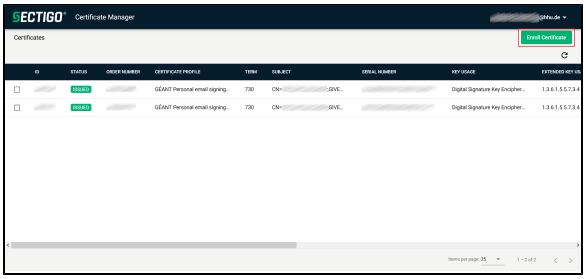
Schritt 1: Gehen auf die Seite **https://cert-manager.com/customer/DFN/smime/login** und melden Sie sich dort unter **"Email Confirmation"** mit der **Funktions-E-Mail-Adresse** an. Klicken Sie dann auf **"Submit"**.

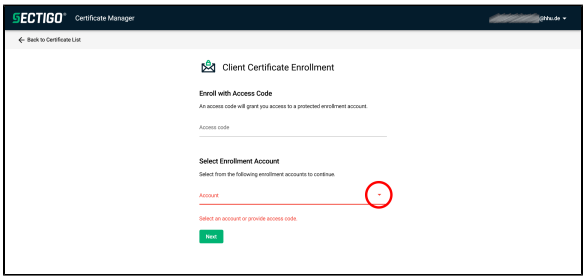
> **WICHTIG**
>
> Es ist wichtig darauf zu achten, sich exakt mit der Funktions-E-Mail-Adresse anzumelden, mit der das Zertifikat beantragt wurde!



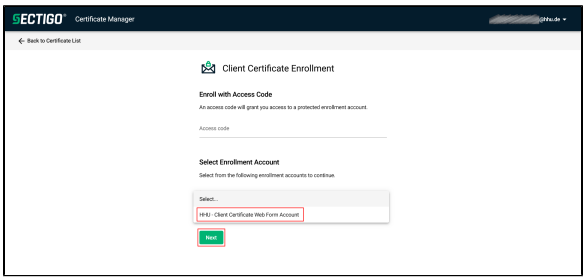
Schritt 2: Sie erhalten nun eine E-Mail mit einem Bestätigungslink. Klicken Sie in der E-Mail entweder das grüne Feld **"Confirm Authentication Request"** an oder den darunter stehenden, mit "https://cert-manager.com" beginnenden Link.

Schritt 3: Sie gelangen nun auf die Übersichtsseite mit den aktuell existierenden Zertifikaten für Ihre Funktionskennung. Um ein neues Zertifikat zu erstellen, klicken Sie oben rechts auf das grüne Feld **"Enroll Certificate"**.





Schritt 4: Klicken Sie nun bei "Select Enrollment Account" auf den **Drop down-Pfeil** neben "Account".



Wählen Sie dann **"HHU - Client Certificate Web Form Account"** und klicken Sie anschließend auf **"Next"**.

Führen Sie nun die Schritte zum Erstellen eines Zertifikats wie in der Anleitung oben beschrieben durch.