

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.

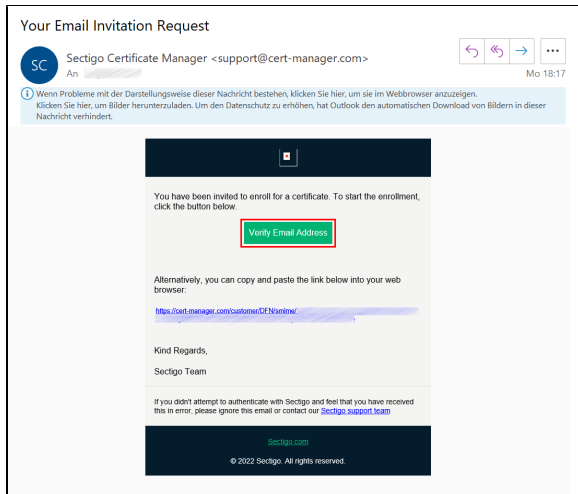
Ausführliche Anleitung

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.



ECTIGO Certificate Manager

← Back to Certificate List

Client Certificate Enrollment

Please complete the form to enroll for a certificate. Your certificate will be associated with the organization/departement shown below.

If the certificate can be issued immediately you will be able to download it after submitting. If the certificate requires approval you will be notified by email to the address below when it is issued.

Organization: H&M-Haus Universal Dienstleistungen
 Department: None
 Email: [redacted]@hmu.de

Certificate Name: SEANT Personal email signing and encryption - 2 Years RSA-4096
 Certificate Validity: 2 Years
 Key Size: RSA - 4096

First Name: [redacted]
 Middle Name: [redacted]
 Last Name: [redacted]

☒ I have read and agree to the terms of the Sectigo Client Certificate EULA

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**".

ECTIGO Certificate Manager

← Back to Certs

IMPORTANT - PLEASE READ THIS SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING OR USING A SECTIGO CERTIFICATE OR BEFORE CLICKING ON "ACCEPT". YOU AGREE THAT BY APPLYING FOR, ACCEPTING OR USING A SECTIGO CERTIFICATE, YOU HAVE READ THIS AGREEMENT, YOU UNDERSTAND IT AND YOU AGREE TO ITS TERMS IF YOU ARE APPLYING FOR, ACCEPTING OR USING A SECTIGO CERTIFICATE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY. YOU REPRESENT THAT YOU ARE AN AUTHORIZED REPRESENTATIVE OF SUCH ENTITY AND HAVE THE AUTHORITY TO ACCEPT THIS AGREEMENT ON SUCH ENTITY'S BEHALF. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT OR USE A SECTIGO CERTIFICATE AND DO NOT CLICK "ACCEPT".

SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT

This Sectigo Certificate Subscriber Agreement (this "Agreement") is between a natural person or the legal entity who applies for and is issued, or identified on, the Certificate(s) resulting from the Agreement ("Subscriber") and Sectigo Limited, a limited company formed under the laws of England and Wales with registered number 04580606 and registered office at 18 Office Village, 3rd Floor, Exchange Quay, Trafford Road, Salford, Manchester M5 3EQ, United Kingdom ("Sectigo"). This Agreement governs Subscriber's application for and use of a Certificate issued from Sectigo. Subscriber and Sectigo agree as follows:

- Definitions.
 - "Application Software Supplier" means a developer of internal business software or other software that develops or uses Sectigo Certificates and distributes Sectigo root Certificates, such as Google Inc., Microsoft Corporation, Mozilla Foundation, etc.
 - "Certificate Portal" means the management of Certificate Issuance and Application Software Suppliers whose website is utilizing only.
 - "CA/B Standards" refers to the set of industry standards published by the CA/Browser Forum relating to the issuance and management of Publicly Trusted Certificates, including (i) the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, or the Guidelines for the Issuance and Management of Extended Validation Certificates; and (ii) the Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates.
 - "Certificate" means a digitally signed document that is a public key Certificate in the version 3 format specified by (i) ITU Recommendation X.509. The Digital Signature on the certificate binds a subject's identity and other data items to a public key value, thus attesting to the ownership of the Public Key by the subject.
 - "Certificate Agreement" means a natural person who is either Subscriber, employee of Subscriber, or an authorized agent who has express authority to represent Subscriber to (i) act as a

Decline:

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

ECTIGO Certificate Manager

← Back to Certificate List

Client Certificate Enrollment

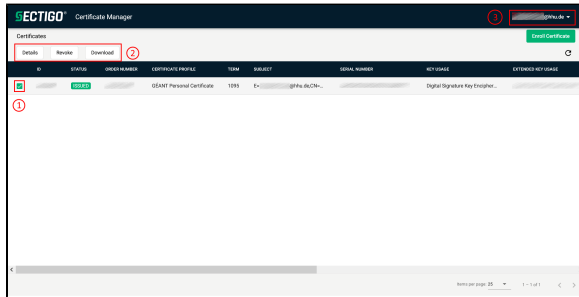
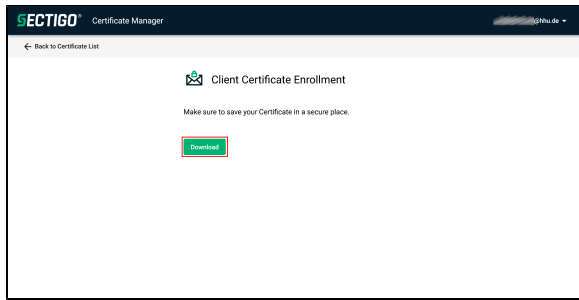
Make sure to save your Certificate in a secure place.

Secure Key/Password: PKCS#12 - SHA256
 This algorithm is more robust and preferred in terms of security. It's faster and has better strength for not all programs support it yet, and there may be problems with installation on iOS or Mac OS. If this algorithm selected, simply password is not allowed.

PKCS#12 Password: [redacted]
 Confirm PKCS#12 Password: [redacted]

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.

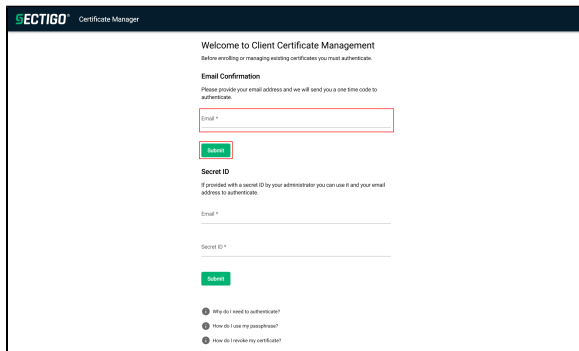


Schritt 7: Sie gelangen nun auf eine Übersichtsseite mit Ihren Zertifikaten. Durch (1) das Setzen eines Häkchens können Sie Ihre Zertifikate (2) verwalten: Sie können sich die Details anschauen, das Zertifikat für ungültig erklären ("Revoke") oder downloaden.

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

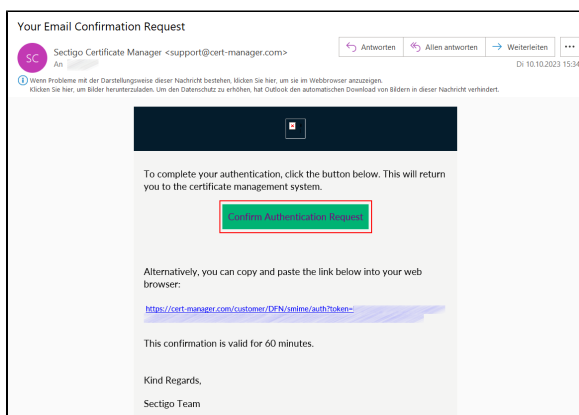


Schritt 1: Gehen auf die Seite <https://cert-manager.com/customer/DFN/smime/login> und melden Sie sich dort unter **"Email Confirmation"** mit der **Funktions-E-Mail-Adresse** an. Klicken Sie dann auf **"Submit"**.



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"**.

ECTIGO® Certificate Manager

Certificates

Export Certificates

ID	STATUS	ORDER NUMBER	CERTIFICATE PROFILE	TERM	SUBJECT	ISSUAL NUMBER	KEY USAGE	CERTIFICATE ENROLLMENT
<input type="checkbox"/>	ENROLLED		GEA001 Personal email signing...	730	CN=...	...	Digital Signature Key Encipher...	1.3.6.1.5.5.7.3.4
<input type="checkbox"/>	ENROLLED		GEA001 Personal email signing...	730	CN=...	...	Digital Signature Key Encipher...	1.3.6.1.5.5.7.3.4

Items per page: 25 1 - 2 of 2

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

ECTIGO® Certificate Manager

Back to Certificate List

Client Certificate Enrollment

Enroll With Access Code
An access code will grant you access to a protected enrollment account.

Access code

Select Enrollment Account
Select from the following enrollment accounts to continue.

Account

Select an account or provide access code.

Next

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

ECTIGO® Certificate Manager

Back to Certificate List

Client Certificate Enrollment

Enroll With Access Code
An access code will grant you access to a protected enrollment account.

Access code

Select Enrollment Account
Select from the following enrollment accounts to continue.

Select...

HHU - Client Certificate Web Form Account

Next

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