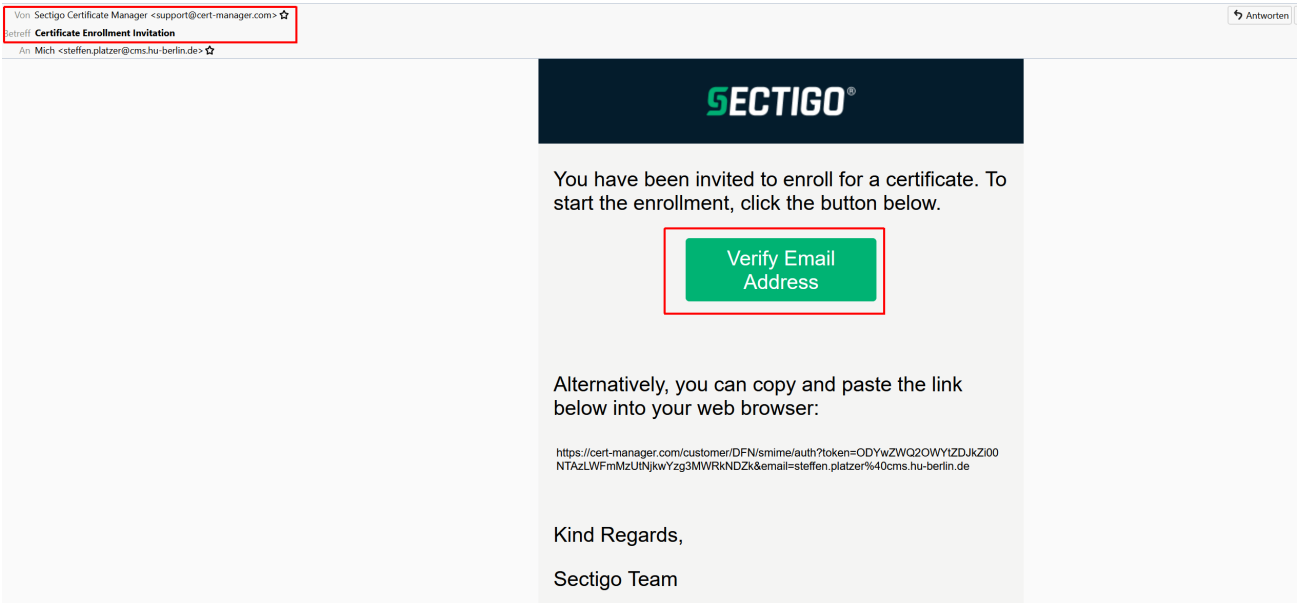
HUMBOLDT-UNIVERSITÄT ZU BERLIN

Nutzerzertifikat downloaden

Sie bekommen eine E-Mail mit dem Betreff: **Certificate Enrollment Invitation**.
Absender dieser E-Mail ist **Sectigo Certificate Manager support@cert-manager.com**
Diese E-Mail enthält einen Link mit dem Sie Ihre E-Mailadresse validieren.



Klicken Sie auf diesen Link, **grüner Button Verify Email Adress**, es öffnet sich ein Formular.
Alternativ können Sie auch den Link in die Adresszeile Ihres Browsers kopieren.
Da die Formularseite in englischer Sprache angezeigt wird, können Sie bei Bedarf in Ihrem Browser eine Übersetzung einzuschalten.

Client Certificate Enrollment

Please complete this form to enroll for a certificate. Your certificate will be associated with the organization/department 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 its issued.

Organization	Humboldt-Universität zu Berlin
Department	None
Email	grid-pki@cms.hu-berlin.de

Certificate Profile *
GÉANT Personal email signing and encryption - 2 Years RSA 4096

Certificate Term *
2 Years

Key Type
RSA - 4096

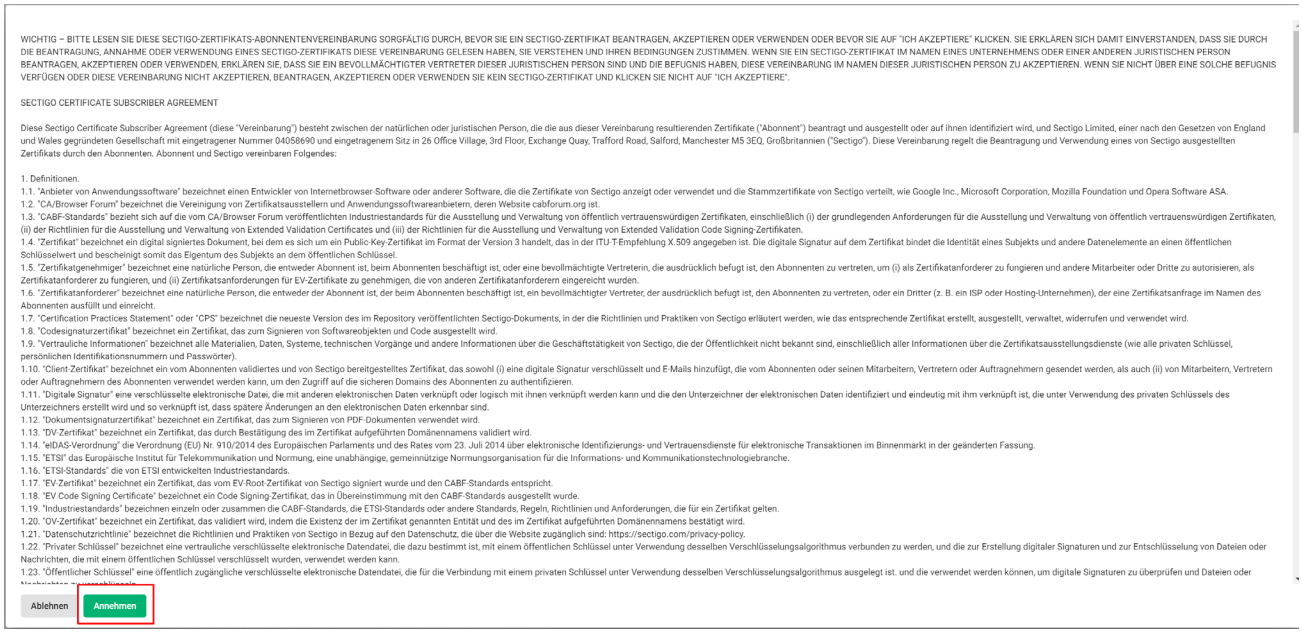
First name *
Steffen

Middle name

Last name *
Platzer

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

Submit



WICHTIG – BITTE LESEN SIE DIESE SECTIGO-ZERTIFIKATS-ABONNENTENVEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE EIN SECTIGO-ZERTIFIKAT BEANTRAGEN, AKZEPTIEREN ODER VERWENDEN ODER BEVOR SIE AUF "ICH AKZEPTIERE" KLICKEN. SIE ERKLÄREN SICH DAMIT EINVERSTANDEN, DASS SIE DURCH DIE BEANTRAGUNG, ANNAHME ODER VERWENDUNG EINES SECTIGO-ZERTIFIKATS DIESE VEREINBARUNG GELESEN HABEN, SIE VERSTEHEN UND IHREN BEDINGUNGEN ZUSTIMMEN. WENN SIE EIN SECTIGO-ZERTIFIKAT IM NAMEN EINES UNTERNEHMENS ODER EINER ANDEREN JURISTISCHEN PERSON BEANTRAGEN, AKZEPTIEREN ODER VERWENDEN, ERKLÄREN SIE, DASS SIE EIN BEVOLLMÄCHTIGTER VERTRETER DIESER JURISTISCHEN PERSON SIND UND DIE BEFUGNIS HABEN, DIESE VEREINBARUNG IM NAMEN DIESER JURISTISCHEN PERSON ZU AKZEPTIEREN. WENN SIE NICHT ÜBER EINE SOLCHE BEFUGNIS VERFÜGEN ODER DIESE VEREINBARUNG NICHT AKZEPTIEREN, BEANTRAGEN, AKZEPTIEREN ODER VERWENDEN SIE KEIN SECTIGO-ZERTIFIKAT UND KLICKEN SIE NICHT AUF "ICH AKZEPTIERE".

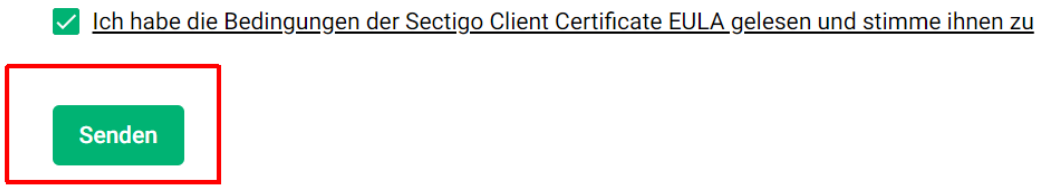
SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT

Diese Sectigo Certificate Subscriber Agreement (diese "Vereinbarung") besteht zwischen der natürlichen oder juristischen Person, die die aus dieser Vereinbarung resultierenden Zertifikate ("Abonnent") beantragt und ausgestellt oder auf ihnen identifiziert wird, und Sectigo Limited, einer nach den Gesetzen von England und Wales gegründeten Gesellschaft mit eingetragener Nummer 04058690 und eingetragenem Sitz in 26 Office Village, 3rd Floor, Exchange Quay, Trafford Road, Salford, Manchester M5 3EQ, Großbritannien ("Sectigo"). Diese Vereinbarung regelt die Beantragung und Verwendung eines von Sectigo ausgestellten Zertifikats durch den Abonnenten. Abonnent und Sectigo vereinbaren Folgendes:

1. Definitionen.
1.1. "Anbieter von Anwendungssoftware" bezeichnet einen Entwickler von Internetbrowser-Software oder anderer Software, die die Zertifikate von Sectigo anzeigt oder verwendet und die Stammzertifikate von Sectigo verteilt, wie Google Inc., Microsoft Corporation, Mozilla Foundation und Opera Software ASA.
1.2. "CA/Browser Forum" bezeichnet die Vereinigung von Zertifikatsausstellern und Anwendungssoftwareanbietern, deren Website cabforum.org ist.
1.3. "CABF-Standards" bezieht sich auf die vom CA/Browser Forum veröffentlichten Industriestandards für die Ausstellung und Verwaltung von öffentlich vertrauenswürdigen Zertifikaten, einschließlich (i) der grundlegenden Anforderungen für die Ausstellung und Verwaltung von öffentlich vertrauenswürdigen Zertifikaten, (ii) der Richtlinien für die Ausstellung und Verwaltung von Extended Validation Certificates und (iii) der Richtlinien für die Ausstellung und Verwaltung von Extended Validation Code Signing-Zertifikaten.
1.4. "Zertifikat" bezeichnet ein digital signiertes Dokument, bei dem es sich um ein Public-Key-Zertifikat im Format der Version 3 handelt, das in der ITU-T-Empfehlung X.509 angegeben ist. Die digitale Signatur auf dem Zertifikat bindet die Identität eines Subjekts und andere Datenelemente an einen öffentlichen Schlüsselwert und bescheinigt somit das Eigentum des Subjekts an dem öffentlichen Schlüssel.
1.5. "Zertifikatgenehmiger" bezeichnet eine natürliche Person, die entweder Abonnent ist, beim Abonnenten beschäftigt ist, oder eine bevollmächtigte Vertreterin, die ausdrücklich befugt ist, den Abonnenten zu vertreten, um (i) als Zertifikatanforderer zu fungieren und andere Mitarbeiter oder Dritte zu autorisieren, als Zertifikatanforderer zu fungieren, und (ii) Zertifikatsanforderungen für EV-Zertifikate zu genehmigen, die von anderen Zertifikatanforderern eingereicht wurden.
1.6. "Zertifikatanforderer" bezeichnet eine natürliche Person, die entweder der Abonnent ist, der beim Abonnenten beschäftigt ist, ein bevollmächtigter Vertreter, der ausdrücklich befugt ist, den Abonnenten zu vertreten, oder ein Dritter (z. B. ein ISP oder Hosting-Unternehmen), der eine Zertifikatsanfrage im Namen des Abonnenten ausfüllt und einreicht.
1.7. "Certification Practices Statement" oder "CPS" bezeichnet die neueste Version des im Repository veröffentlichten Sectigo-Dokuments, in der die Richtlinien und Praktiken von Sectigo erläutert werden, wie das entsprechende Zertifikat erstellt, ausgestellt, verwaltet, widerrufen und verwendet wird.
1.8. "Codesignaturzertifikat" bezeichnet ein Zertifikat, das zum Signieren von Softwareobjekten und Code ausgestellt wird.
1.9. "Vertrauliche Informationen" bezeichnet alle Materialien, Daten, Systeme, technischen Vorgänge und andere Informationen über die Geschäftstätigkeit von Sectigo, die der Öffentlichkeit nicht bekannt sind, einschließlich aller Informationen über die Zertifikatsausstellungsdienste (wie alle privaten Schlüssel, persönlichen Identifikationsnummern und Passwörter).
1.10. "Client-Zertifikat" bezeichnet ein vom Abonnenten validiertes und von Sectigo bereitgestelltes Zertifikat, das sowohl (i) eine digitale Signatur verschlüsselt und E-Mails hinzufügt, die vom Abonnenten oder seinen Mitarbeitern, Vertretern oder Auftragnehmern gesendet werden, als auch (ii) von Mitarbeitern, Vertretern oder Auftragnehmern des Abonnenten verwendet werden kann, um den Zugriff auf die sicheren Domains des Abonnenten zu authentifizieren.
1.11. "Digitale Signatur" eine verschlüsselte elektronische Datei, die mit anderen elektronischen Daten verknüpft oder logisch mit ihnen verknüpft werden kann und die den Unterzeichner der elektronischen Daten identifiziert und eindeutig mit ihm verknüpft ist, die unter Verwendung des privaten Schlüssels des Unterzeichners erstellt wird und so verknüpft ist, dass spätere Änderungen an den elektronischen Daten erkennbar sind.
1.12. "Dokumentsignaturzertifikat" bezeichnet ein Zertifikat, das zum Signieren von PDF-Dokumenten verwendet wird.
1.13. "DV-Zertifikat" bezeichnet ein Zertifikat, das durch Bestätigung des im Zertifikat aufgeführten Domänennamens validiert wird.
1.14. "eIDAS-Verordnung" die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierungs- und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt in der geänderten Fassung.
1.15. "ETSI" das Europäische Institut für Telekommunikation und Normung, eine unabhängige, gemeinnützige Normungsorganisation für die Informations- und Kommunikationstechnologiebranche.
1.16. "ETSI-Standards" die von ETSI entwickelten Industriestandards.
1.17. "EV-Zertifikat" bezeichnet ein Zertifikat, das vom EV-Root-Zertifikat von Sectigo signiert wurde und den CABF-Standards entspricht.
1.18. "EV Code Signing Certificate" bezeichnet ein Code Signing-Zertifikat, das in Übereinstimmung mit den CABF-Standards ausgestellt wurde.
1.19. "Industriestandards" bezeichnen einzeln oder zusammen die CABF-Standards, die ETSI-Standards oder andere Standards, Regeln, Richtlinien und Anforderungen, die für ein Zertifikat gelten.
1.20. "OV-Zertifikat" bezeichnet ein Zertifikat, das validiert wird, indem die Existenz der im Zertifikat genannten Entität und des im Zertifikat aufgeführten Domänennamens bestätigt wird.
1.21. "Datenschutzrichtlinie" bezeichnet die Richtlinien und Praktiken von Sectigo in Bezug auf den Datenschutz, die über die Website zugänglich sind: https://sectigo.com/privacy-policy.
1.22. "Privater Schlüssel" bezeichnet eine vertrauliche verschlüsselte elektronische Datendatei, die dazu bestimmt ist, mit einem öffentlichen Schlüssel unter Verwendung desselben Verschlüsselungsalgorithmus verbunden zu werden, und die zur Erstellung digitaler Signaturen und zur Entschlüsselung von Dateien oder Nachrichten, die mit einem öffentlichen Schlüssel verschlüsselt wurden, verwendet werden kann.
1.23. "Öffentlicher Schlüssel" eine öffentlich zugängliche verschlüsselte elektronische Datendatei, die für die Verbindung mit einem privaten Schlüssel unter Verwendung desselben Verschlüsselungsalgorithmus ausgelegt ist. und die verwendet werden können, um digitale Signaturen zu überprüfen und Dateien oder

Ablehnen | Annehmen

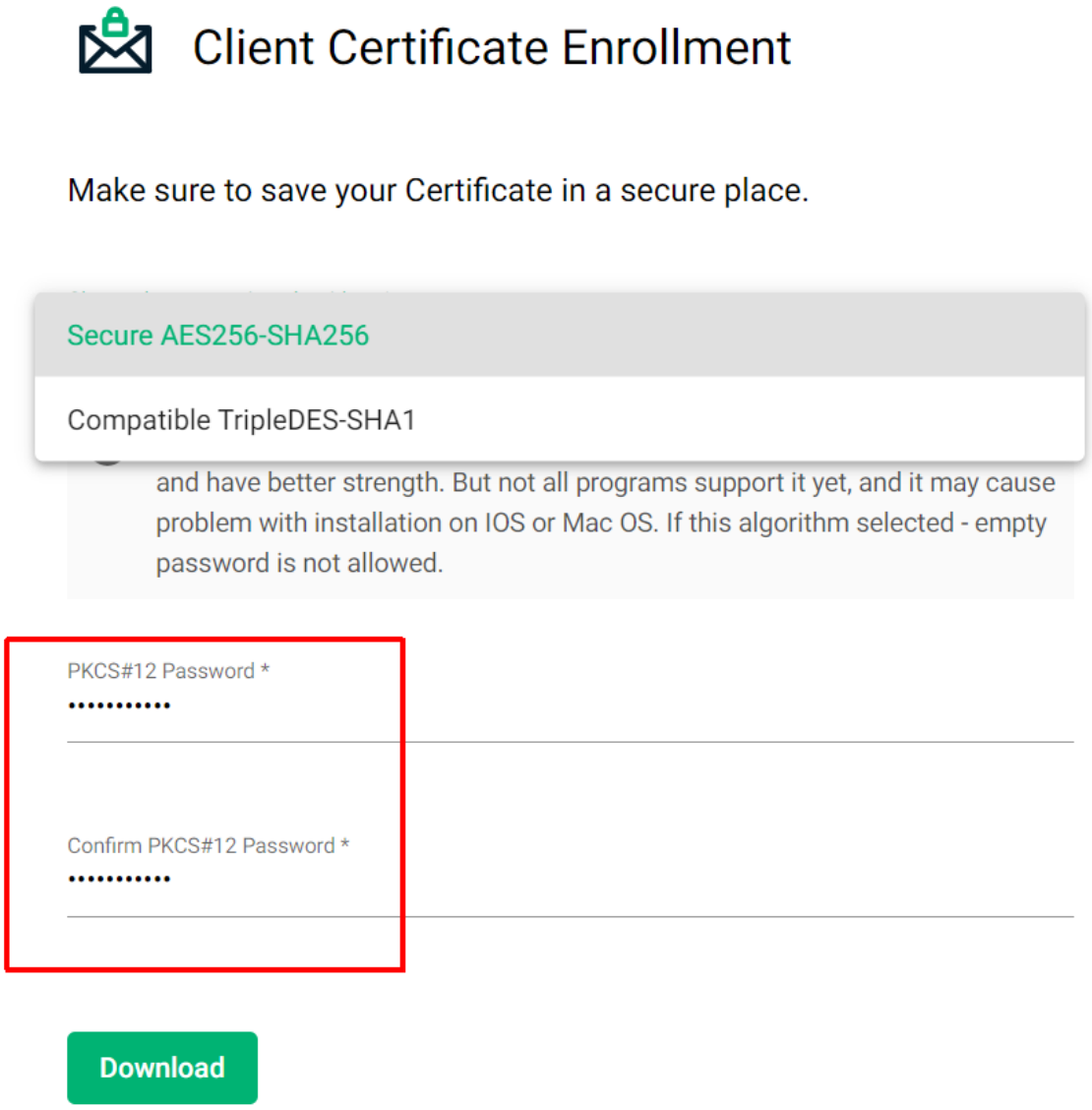
Bestätigen Sie die angezeigte EULA durch klicken auf den grünen Button **Annehmen** und dann auf **Senden**.



Ich habe die Bedingungen der Sectigo Client Certificate EULA gelesen und stimme ihnen zu

Senden

Es öffnet sich eine neue Formularseite auf der Sie eine PIN (*PKCS#12 Passwort*) zum Schutz Ihrer Zertifikatsdatei vergeben müssen. Sie haben die Möglichkeit unterschiedliche Algorithmen zum Schutz Ihres privaten Schlüssels auszuwählen.
Secure AES256-SHA256 ist das modernste und sicherste Verfahren, kann aber bei einigen Anwendungen wie MacOSX, Adobe Acrobat, MS Outlook zu Problem führen. Verwenden Sie dann lieber das Verfahren *Compatible TripleDES-SHA1*.



Diese PIN (PKCS#12 Passwort) benötigen Sie um Ihre Zertifikatsdatei zu installieren, diese müssen Sie unbedingt sorgfältig aufbewahren, es gibt keine Wiederherstellungsmöglichkeit durch die HU-PKI.

Klicken Sie auf Download, kurze Zeit später wird der Download Ihrer Zertifikatsdatei angeboten, oder erfolgt automatisch in Ihren Downloadordner

Schließen Sie ihren Browser nicht vor Ende des Downloads und speichern Ihrer Zertifikatsdatei. Der Prozess kann nicht noch einmal gestartet werden!
Sie müssten dann über das Formular neu beantragen.

Sie können sich jederzeit eine neue Zertifikatsdatei erstellen, es gibt aber immer nur 2 gültige Zertifikate. Wird ein drittes Zertifikat erstellt wird das älteste automatisch gesperrt, sie erhalten dazu aber keinen expliziten Hinweis.
Beachten Sie aber das neu ausgestellte Zertifikatsdateien auch einen neuen privaten Schlüssel beinhalten. Bereits verschlüsselte E-Mails, die mit einem früher ausgestellten Zertifikat verschlüsselt wurden, lassen sich damit nicht lesen.

Wichtige Hinweise zur Zertifikatsdatei und zum Kennwort

Sie sind für die sichere Aufbewahrung Ihrer Zertifikatsdatei und Ihres vergebenen Kennwortes selbst verantwortlich. Es gibt keine Möglichkeit der Wiederherstellung bei Verlust.
Verwenden Sie einen sicheren Speicherort z.B. einen Kennwort geschützten Ordner in der HU-Box, oder einen anderen sicheren Datenspeicher.

Anleitungen zur Installation Ihrer Zertifikatsdatei

E-Mailprogramm zum Signieren/Verschlüsseln

Thunderbird

Outlook

AppleMail

Signieren in Dokumenten (diese Funktion ist eingeschränkt für interne Prozesse nutzbar)

Adobe Acrobat

Anleitung Nutzerzertifikat sperren

Nutzerzertifikat sperren