HUMBOLDT-UNIVERSITÄT ZU BERLIN

Funktionszertifikat beantragen

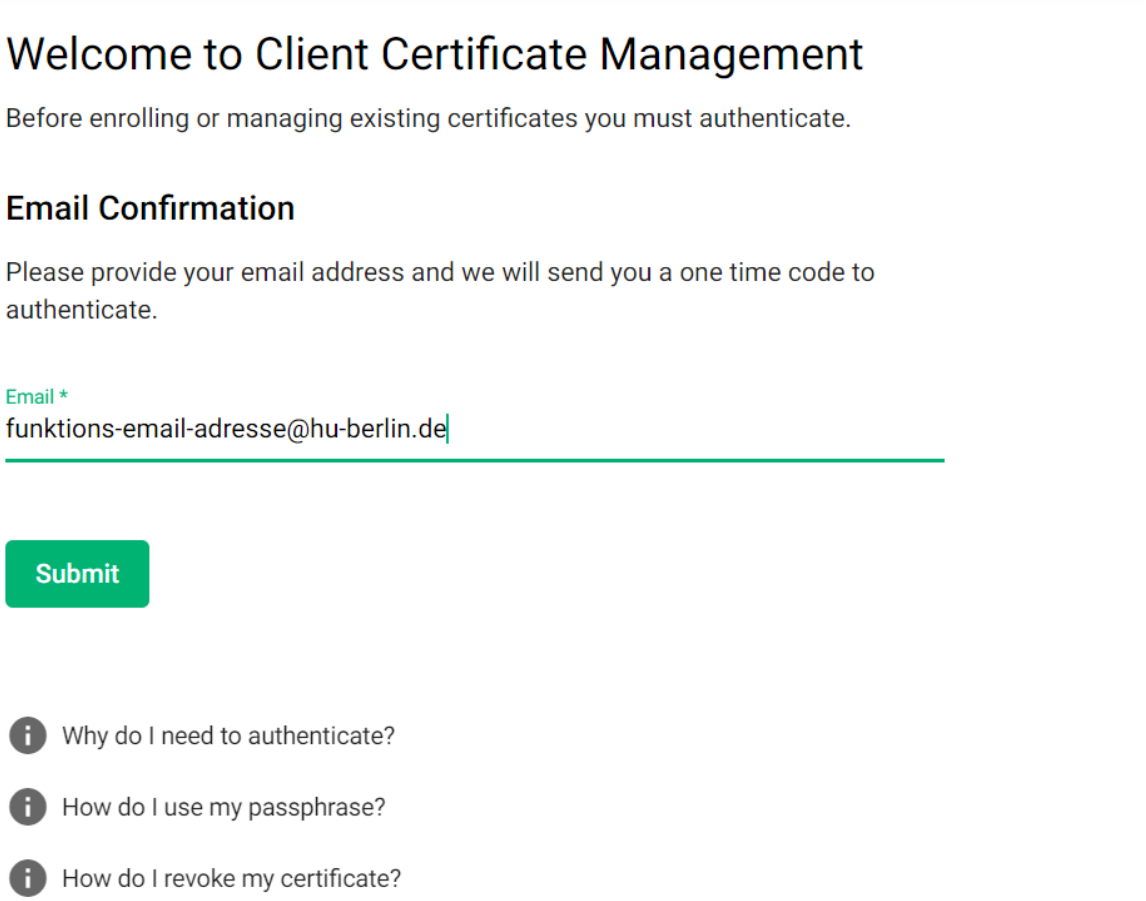
Vorbemerkungen
Nachdem Ihr Funktionsaccount als berechtigt im System eingetragen ist, können sie ein Funktionszertifikat beantragen. Dieses Funktionszertifikat beinhaltet die zugehörige E-Mailadresse und die Organisation „Humboldt-Universität zu Berlin, aber keine Namen oder Pseudonyme.
Sie können damit E-Mail Signieren und/oder Verschlüsseln.

Zertifikat beantragen
Aufruf der Start-URL

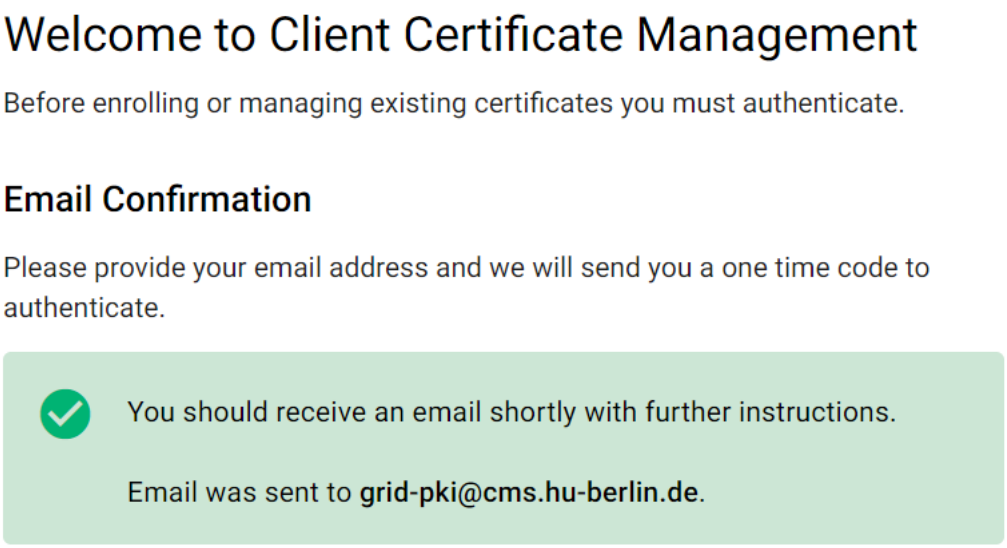
https://cert-manager.com/customer/DFN/smime/3KuOtzM2JNdG9bxADwRI

Da die Antragsseiten mit einer englischsprachigen Oberfläche kommen, können Sie auch eine automatische Übersetzung des Browsers aktivieren.

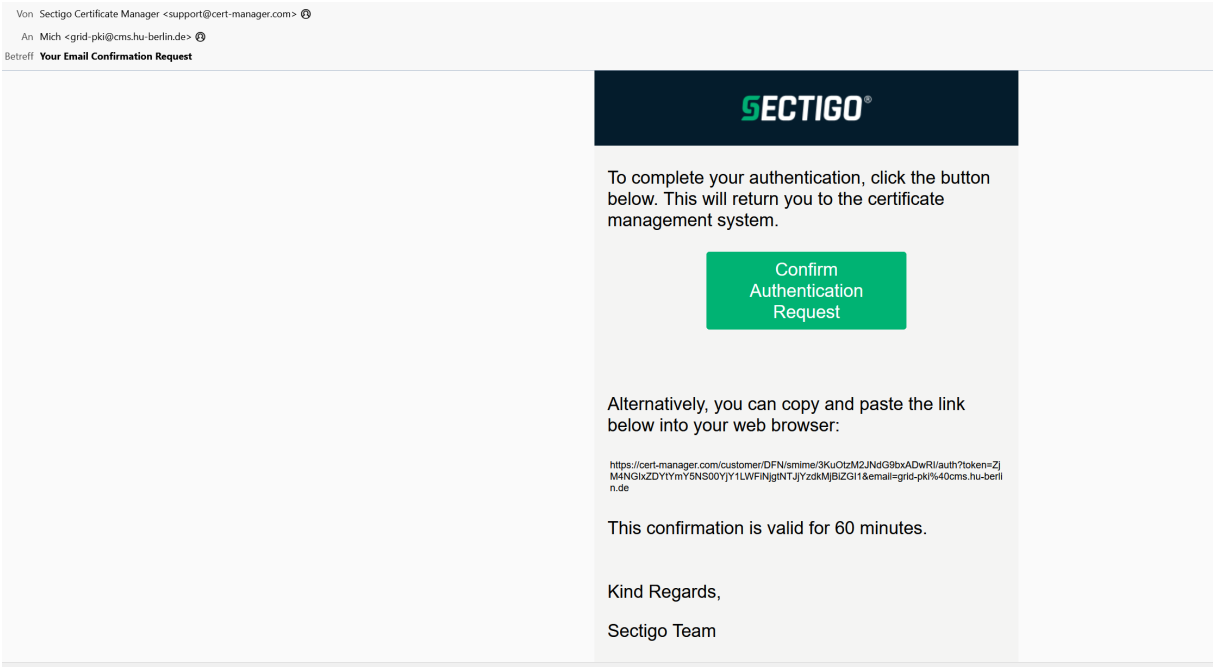
Tragen Sie in das Feld „Email" die betreffende Funktions-E-Mailadresse ein und klicken auf „Submit"



Sie erhalten eine Bestätigung das eine E-Mail mit dem Betreff „Your Email Confirmation Request" und dem Absender „Sectigo Certificate Manager <support@cert-manager.com>" an die Funktions-E-Mailadresse verschickt wurde.



Diese E-Mail enthält einen Verifikationslink hinter dem grünen Button „Confirm Authentication Request". Beachten Sie das dieser Link nur 60 Minuten lang gültig ist.



Klicken Sie auf den Button „Confirm Authentication Request".
Sie werden auf ein „Client Certificate Enrollment"-Formular geleitet.

Die Angaben in First name und Last name erscheinen nicht im Zertifikat, sondern dienen ausschließlich Verwaltungszwecken.

Setzen Sie einen Haken in der rot markierten Checkbox.

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 Organisation email signing - 2 Years RSA 4096

Certificate Term *
2 Years

Key Type
RSA - 4096

First name *
Steffen

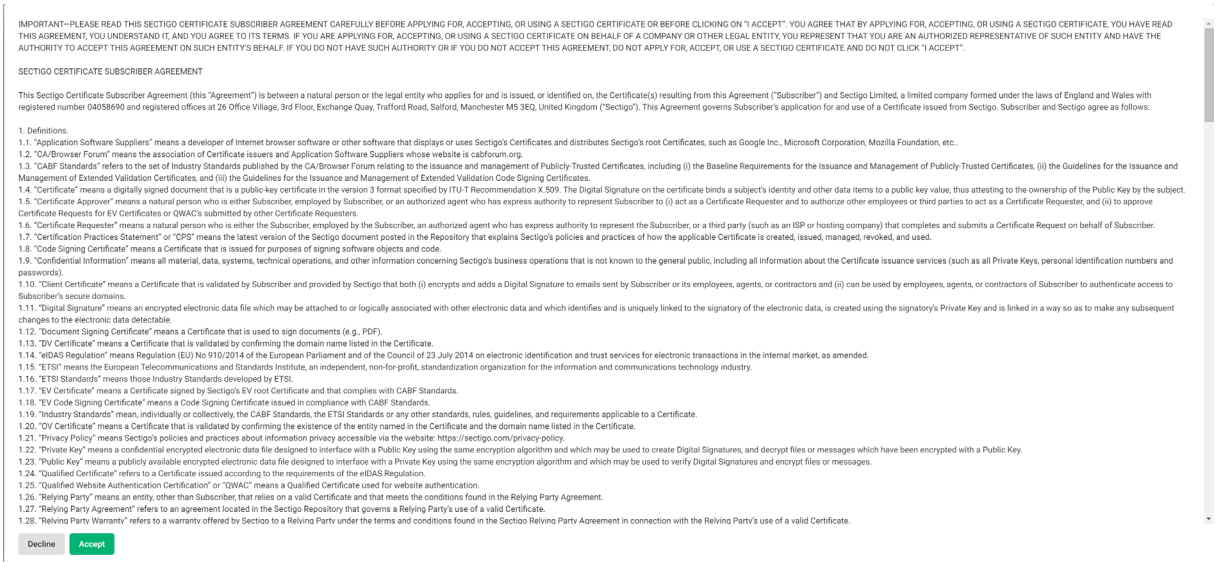
Middle name

Last name *
Platzer

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

Submit

Sie müssen sich mit den Bedingungen des Endbenutzervertrages (Eula) einverstanden erklären und dies durch Haken setzen bestätigen.
Sie bekommen den Text angezeigt und müssen mit den Button „Agree/Zustimmen" bestätigen.



IMPORTANT—PLEASE READ THIS SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE OR BEFORE CLICKING ON "I 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 "I ACCEPT".

SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT

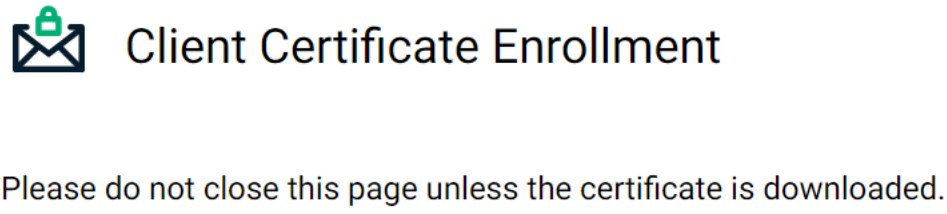
This Sectigo Certificate Subscriber Agreement (this "Agreement") is between a natural person or the legal entity who applies for and is issued, or identified on, the Certificate(s) resulting from this Agreement ("Subscriber") and Sectigo Limited, a limited company formed under the laws of England and Wales with registered number 04058690 and registered offices at 26 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:

1. Definitions.
1.1. "Application Software Suppliers" means a developer of Internet browser software or other software that displays or uses Sectigo's Certificates and distributes Sectigo's root Certificates, such as Google Inc., Microsoft Corporation, Mozilla Foundation, etc..
1.2. "CA/Browser Forum" means the association of Certificate issuers and Application Software Suppliers whose website is cabforum.org.
1.3. "CABF 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, (ii) the Guidelines for the Issuance and Management of Extended Validation Certificates, and (iii) the Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates.
1.4. "Certificate" means a digitally signed document that is a public-key certificate in the version 3 format specified by ITU-T 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.
1.5. "Certificate Approver" means a natural person who is either Subscriber, employed by Subscriber, or an authorized agent who has express authority to represent Subscriber to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve Certificate Requests for EV Certificates or QWAC's submitted by other Certificate Requesters.
1.6. "Certificate Requester" means a natural person who is either the Subscriber, employed by the Subscriber, an authorized agent who has express authority to represent the Subscriber, or a third party (such as an ISP or hosting company) that completes and submits a Certificate Request on behalf of Subscriber.
1.7. "Certification Practices Statement" or "CPS" means the latest version of the Sectigo document posted in the Repository that explains Sectigo's policies and practices of how the applicable Certificate is created, issued, managed, revoked, and used.
1.8. "Code Signing Certificate" means a Certificate that is issued for purposes of signing software objects and code.
1.9. "Confidential Information" means all material, data, systems, technical operations, and other information concerning Sectigo's business operations that is not known to the general public, including all information about the Certificate issuance services (such as all Private Keys, personal identification numbers and passwords).
1.10. "Client Certificate" means a Certificate that is validated by Subscriber and provided by Sectigo that both (i) encrypts and adds a Digital Signature to emails sent by Subscriber or its employees, agents, or contractors and (ii) can be used by employees, agents, or contractors of Subscriber to authenticate access to Subscriber's secure domains.
1.11. "Digital Signature" means an encrypted electronic data file which may be attached to or logically associated with other electronic data and which identifies and is uniquely linked to the signatory of the electronic data, is created using the signatory's Private Key and is linked in a way so as to make any subsequent changes to the electronic data detectable.
1.12. "Document Signing Certificate" means a Certificate that is used to sign documents (e.g., PDF).
1.13. "DV Certificate" means a Certificate that is validated by confirming the domain name listed in the Certificate.
1.14. "eIDAS Regulation" means Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, as amended.
1.15. "ETSI" means the European Telecommunications and Standards Institute, an independent, non-for-profit, standardization organization for the information and communications technology industry.
1.16. "ETSI Standards" means those Industry Standards developed by ETSI.
1.17. "EV Certificate" means a Certificate signed by Sectigo's EV root Certificate and that complies with CABF Standards.
1.18. "EV Code Signing Certificate" means a Code Signing Certificate issued in compliance with CABF Standards.
1.19. "Industry Standards" mean, individually or collectively, the CABF Standards, the ETSI Standards or any other standards, rules, guidelines, and requirements applicable to a Certificate.
1.20. "OV Certificate" means a Certificate that is validated by confirming the existence of the entity named in the Certificate and the domain name listed in the Certificate.
1.21. "Privacy Policy" means Sectigo's policies and practices about information privacy accessible via the website: https://sectigo.com/privacy-policy.
1.22. "Private Key" means a confidential encrypted electronic data file designed to interface with a Public Key using the same encryption algorithm and which may be used to create Digital Signatures, and decrypt files or messages which have been encrypted with a Public Key.
1.23. "Public Key" means a publicly available encrypted electronic data file designed to interface with a Private Key using the same encryption algorithm and which may be used to verify Digital Signatures and encrypt files or messages.
1.24. "Qualified Certificate" refers to a Certificate issued according to the requirements of the eIDAS Regulation.
1.25. "Qualified Website Authentication Certification" or "QWAC" means a Qualified Certificate used for website authentication.
1.26. "Relying Party" means an entity, other than Subscriber, that relies on a valid Certificate and that meets the conditions found in the Relying Party Agreement.
1.27. "Relying Party Agreement" refers to an agreement located in the Sectigo Repository that governs a Relying Party's use of a valid Certificate.
1.28. "Relying Party Warranty" refers to a warranty offered by Sectigo to a Relying Party under the terms and conditions found in the Sectigo Relying Party Agreement in connection with the Relying Party's use of a valid Certificate.

Decline Accept

Accept/Bestätigen klicken und dann auf den Submit-Button klicken.

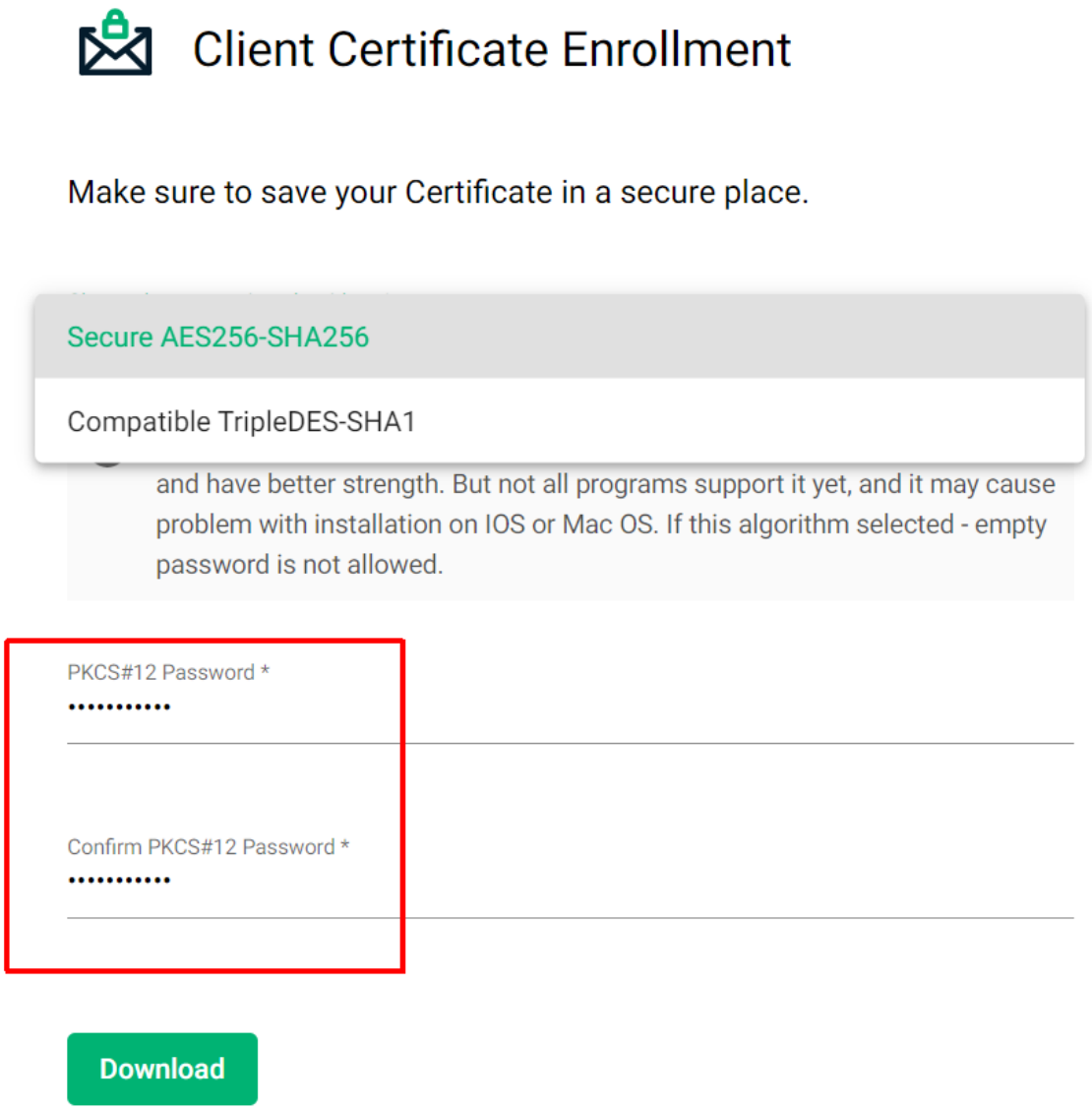
Ihr Browser startet dann einen Prozess der Ihre Zertifikatsdatei erstellt, dies kann bis zu 2 Minuten dauern.



Client Certificate Enrollment

Please do not close this page unless the certificate is downloaded.

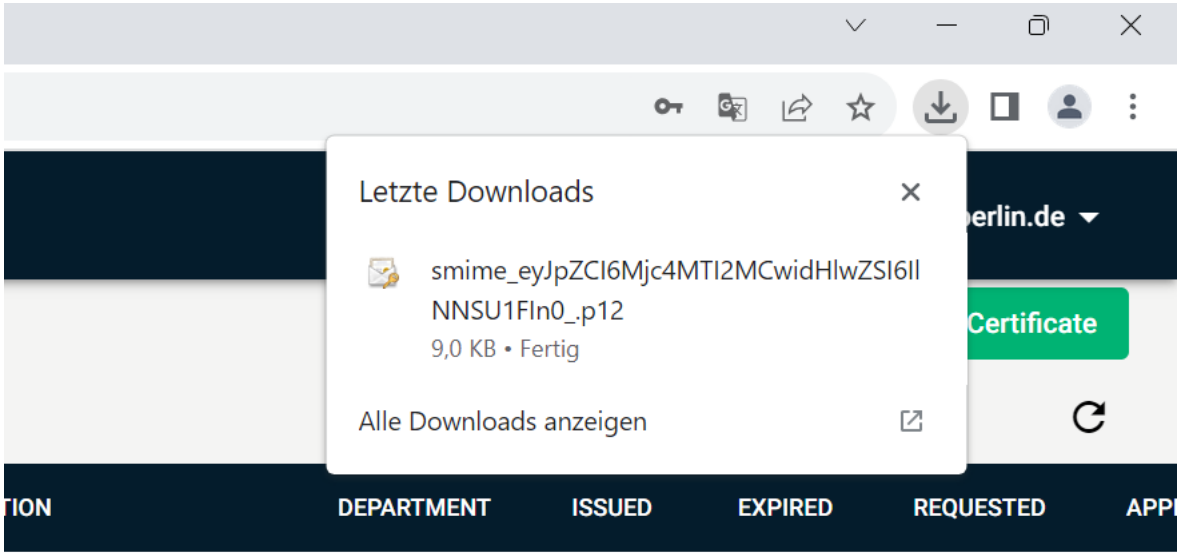
Es öffnet sich eine neue Formularseite auf der Sie eine PIN (*PKCS#12 Passwort*) zum Schutz Ihrer Zertifikatsdatei vergeben müssen. Sie haben die Möglichkeit unterschiedliche Algorithmen zum Schutz Ihres privaten Schlüssels auszuwählen.
Secure AES256-SHA256 ist das modernste und sicherste Verfahren, kann aber bei einigen Anwendungen wie MacOSX, Adobe Acrobat 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, der Download Ihrer Zertifikatsdatei wird gestartet, oder erfolgt automatisch in Ihren Downloadordner. Dies kann einige Zeit dauern.

Schließen sie ihren Browser noch nicht. Sobald Sie die Seite verlassen, besteht keine Möglichkeit mehr, ihre Zertifikatsdatei herunterzuladen!



Wenn sie möchten können sie ihren Browser jetzt schließen.

Sie finden nun in ihrem Downloadordner ihre Zertifikatsdatei und können diese in ihren gewünschten Anwendungen installieren.

Wichtige Hinweise:

Sie sind für die sichere Aufbewahrung der Zertifikatsdatei und des vergebenen Passwortes/PIN selbst verantwortlich. Es gibt keine Möglichkeit der Wiederherstellung bei Verlust. Verwenden sie einen sicheren Speicherort z.B. einen Passwort geschützten Ordner in der HU-Box, oder einen anderen sicheren persönlichen Datenspeicher.

Anleitungen zur Installation der Zertifikatsdatei finden hie hier:

Thunderbird

Outlook

AppleMail