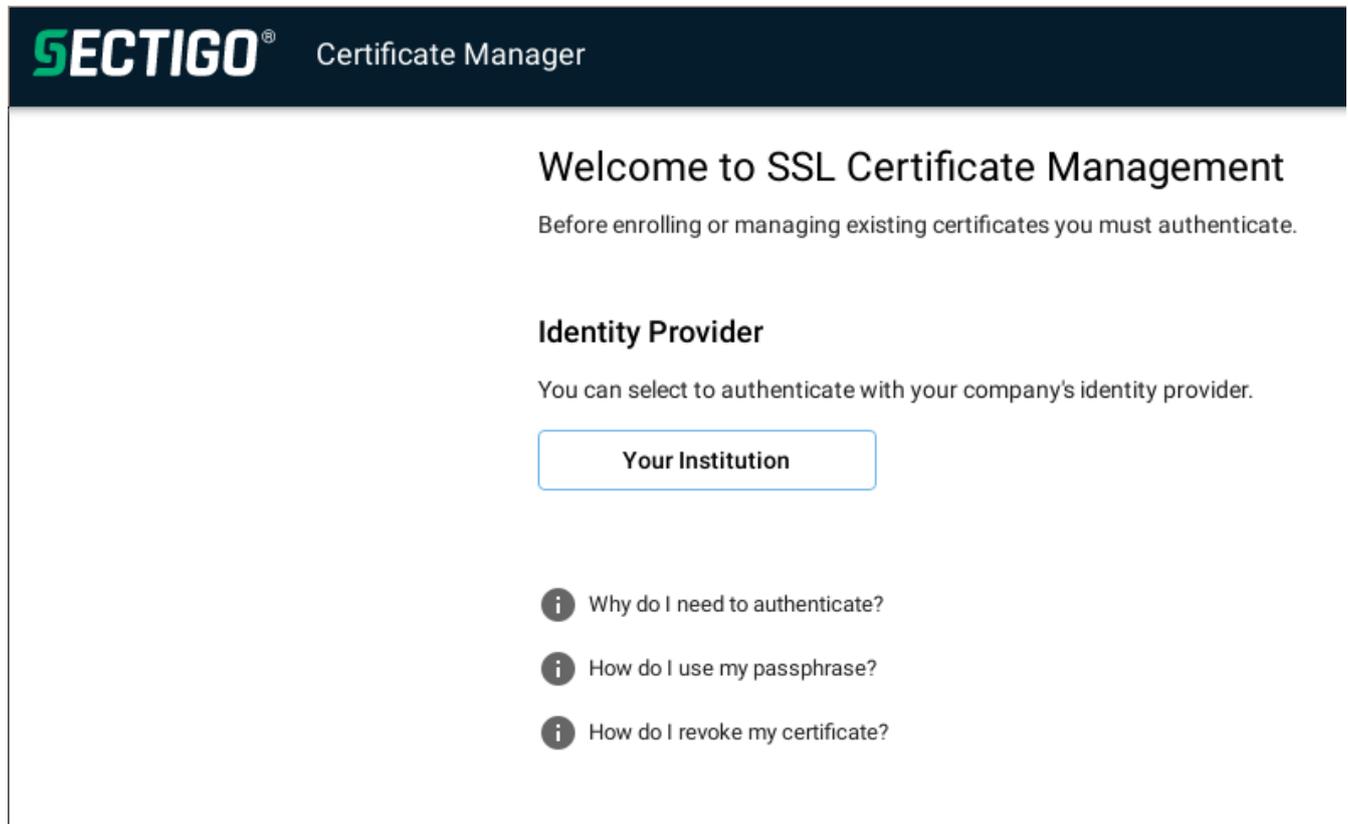


Nutzerzertifikat beantragen

Achtung: Der DFN-Verein, der bisher unsere Zertifikate ausgestellt hat, hat die Zertifikatserzeugung und -verwaltung an einen externen Anbieter (Sectigo) ausgelagert. Dadurch ändert sich der Prozess des Zertifikatantrages grundlegend. Die Beantragung erfolgt ab sofort papierlos und eine Identitätsprüfung alle 39 Monate ist nicht mehr notwendig. Die Identitätsprüfung erfolgt in Zukunft dadurch, dass der jeweilige Nutzer sich über eine Shibboleth- Anmeldung als der Hochschule angehörig ausweisen kann.

Zertifikatsbeantragung unter folgenden Link:

<https://cert-manager.com/customer/DFN/idp/clientgeant>



SECTIGO® Certificate Manager

Welcome to SSL Certificate Management

Before enrolling or managing existing certificates you must authenticate.

Identity Provider

You can select to authenticate with your company's identity provider.

Your Institution

- i** Why do I need to authenticate?
- i** How do I use my passphrase?
- i** How do I revoke my certificate?

- Wählen Sie über die Schaltfläche "Your Institution " die "Magdeburg-Stendal University of Applied Sciences" aus. Wird diese nicht angeboten, können Sie sie durch Suche nach "Magdeburg-Stendal" auswählen.



Access to **Sectigo Certificate Manager**

Choose Your Institution

Recent institutions



Magdeburg-Stendal University of Applied Sciences

hs-magdeburg.de



[+ Add another institution](#)

[Edit](#)

Es erscheint die Shibboleth-Anmeldemaske der Hochschule mit einem Sectigo-Logo im unteren Teil. Dort können Sie sich mit Ihrem zentralen Hochschul-Account anmelden. Nach erfolgreicher Anmeldung gelangen Sie zum Zertifikaterstellungsformular von Sectigo:



Digital Certificate Enrollment

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name

Organization **Hochschule Magdeburg-Stendal**

Email @h2.de

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*
GÉANT Personal email signing and encryption

i Personal Certificate - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents).

Term*

Hier sind bereits einige Datenfelder aus den von der Hochschule übergebenen Daten ausgefüllt. Andere Felder (diese werden erst nacheinander sichtbar) müssen Sie noch ausfüllen:

- Im Feld Term wählen Sie eine Gültigkeitsdauer aus
- Im Feld Enrollment Method wählen Sie "Key Generation"
- Im Feld KeyType wählen Sie "RSA - 4096"

- Wählen Sie ein Passwort, um die Zertifikatsdatei, die Sie im Anschluss erhalten zu schützen (2 mal eingeben)
- **Wichtig:** Ändern Sie im Feld "Choose key protection algorithm" den Algorithmus auf "Compatible TripleDES-SHA1" wenn Sie Ihr Zertifikat mit einem Mac oder iPhone/iPad nutzen wollen. Auch einige Windows-Systeme sind mit dem neueren Verfahren ("Secure AES256-SHA256") nicht voll kompatibel.
- Bestätigen Sie im Feld "I have read and agree to the terms of the Sectigo Client Certificate EULA", dass Sie die Zertifikatsbedingungen gelesen haben und anerkennen.



Select your Certificate Profile to enable your enrollment options.

Certificate Profile*

GÉANT Personal email signing and encryption

i Personal Certificate - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents).

Term*

730 days

Enrollment Method

Key Generation

CSR

Key Type*

RSA - 4096

Password is required to unlock the certificate file download to protect private key.

Password*

.....



Password Confirmation*

.....



Choose key protection algorithm.

Algorithm

Compatible TripleDES-SHA1

[I have read and agree to the terms of the EULA](#)

Submit

- Wählen Sie die Schaltfläche "Submit".
- Warten Sie, bis die Erzeugung des Zertifikates und dessen Download abgeschlossen ist. **Schließen Sie solange nicht Ihren Browser oder den Browsertab.**

Im Downloadordner Ihres Browsers finden Sie danach eine Datei "certs.p12."

Kopieren Sie diese Datei mit einem sprechenden Namen an einen sicheren Ort.

Diese Datei können Sie jetzt wieder wie gewohnt in die Anwendungsprogramme auf den Endgeräten integrieren, in denen Sie es benötigen (E-Mail-Programm, Adobe-Reader siehe [Nutzer-Zertifikate](#)).