

Erstellung eines Benutzer-Zertifikats

Das IT.Service Center der DHBW Mannheim bietet allen Mitgliedern der Hochschule kostenlose Zertifikate für sicheren Datenverkehr an. Digitale Zertifikate sind eine Art digitaler Ausweis mit denen sich Personen, Organisationen und Maschinen im Internet ausweisen können. Damit ist es z. B. möglich, E-Mails rechtsverbindlich zu unterschreiben oder sich für Webseiten zu authentifizieren, sofern dies vom Web-Server unterstützt wird.

- Starten Sie über folgenden Link: [Benutzer-Zertifikat](#)
- Wählen Sie die DHBW Mannheim aus

Find Your Institution

Your university, organization or company

 

Examples: Science Institute, Lee@uni.edu, UCLA

Remember this choice [Learn More](#)

University of Mannheim
uni-mannheim.de

DHBW Mannheim
dhw-mannheim.de

University of Applied Sciences Mannheim

University of Music and Performing Arts Mannh...
muho-mannheim.de

Erstellung eines Benutzer-Zertifikats

➤ Geben Sie Ihren Benutzernamen und das zugehörige Passwort ein



MANNHEIM

Anmelden bei Sectigo Certificate
Manager

Benutzername

 1

Passwort

 2

Anmeldung nicht speichern

**Die zu übermittelnden
Informationen anzeigen, so dass ich
die Weitergabe noch ablehnen kann.**

 3

SECTIGO
Certificate Manager

Erstellung eines Benutzer-Zertifikats

➤ Nehmen Sie folgende Einstellungen vor, wobei Sie bei Punkt 2 zwischen 365,730 und 1095 Tagen auswählen können:

Digital Certificate Enrollment

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

Name **Hans Mustermann**
Organization **DHBW-Mannheim**
Email **hans.mustermann@dhw-mannheim.de**

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*
GÉANT Personal Certificate **1**

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*
365 days **2**

Enrollment Method
 Key Generation **3**
 CSR

Key Type*
RSA - 2048 **4**

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

Password*
..... **5**

Password Confirmati
..... **6**

[I have read and agree to the terms of the EULA](#) **7**

Submit **8**

➤ Nach dem Klicken auf Submit, Zertifikat im p12 Format speichern.