Anmeldung mit MFA an Microsoft - M365-Diensten

Zur Erhöhung der Sicherheit bei der Anmeldung an M365-Diensten für: Lehrende und Mitarbeiter führt die Evangelische Hochschule Darmstadt zum Start des Sommersemesters die Multi-Faktor-Authentifizierung (MFA) ein.

Hinweis:

Die MFA ist **nur** für die Anmeldung an M365-Diensten und Programme die auf diese angewiesen sind notwendig, Moodle, CAS, das WLAN, die Technikausleihe, … usw. funktionieren weiterhin mit den gewohnten Zugangsdaten **ohne MFA.**

M365-Dienste:

MS Teams:	https://teams.microsoft.com/
Exchange Online (E-Mail):	https://outlook.office.com/mail/
Intranet:	https://ehdarmstadtde.sharepoint.com/sites/IntranetderEHD
Office 365:	https://office.com

Lokal Installierte Programme
Outlook
MS Office 365

Zugangsdaten eingeben:

E-Mail-Adresse: [Benutzername + @ maildomain] rainer.tester@eh-darmstadt.de

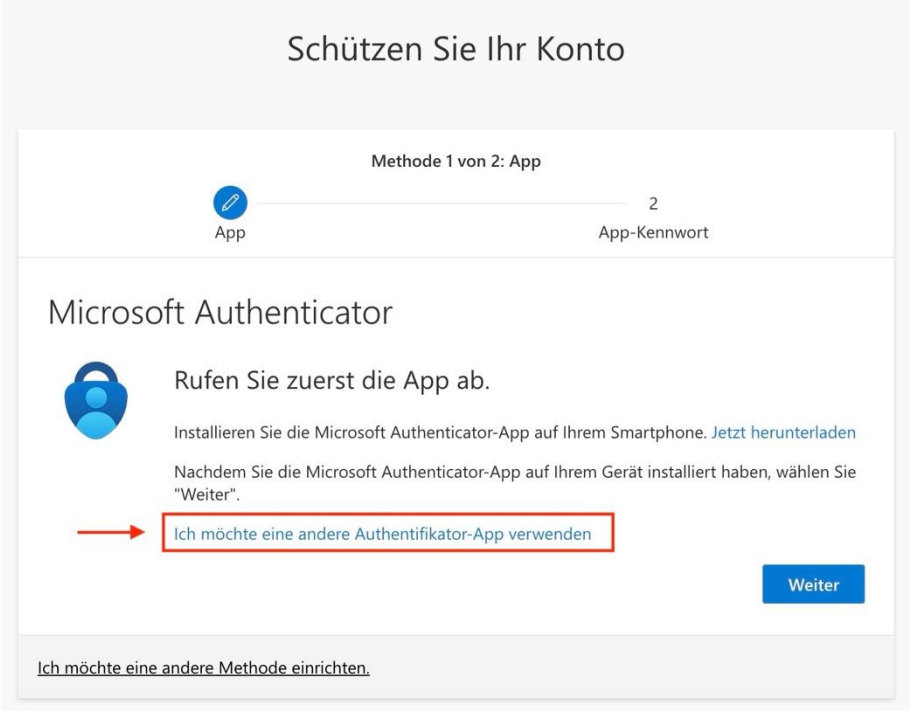
Ihr EHD-Passwort eingeben:

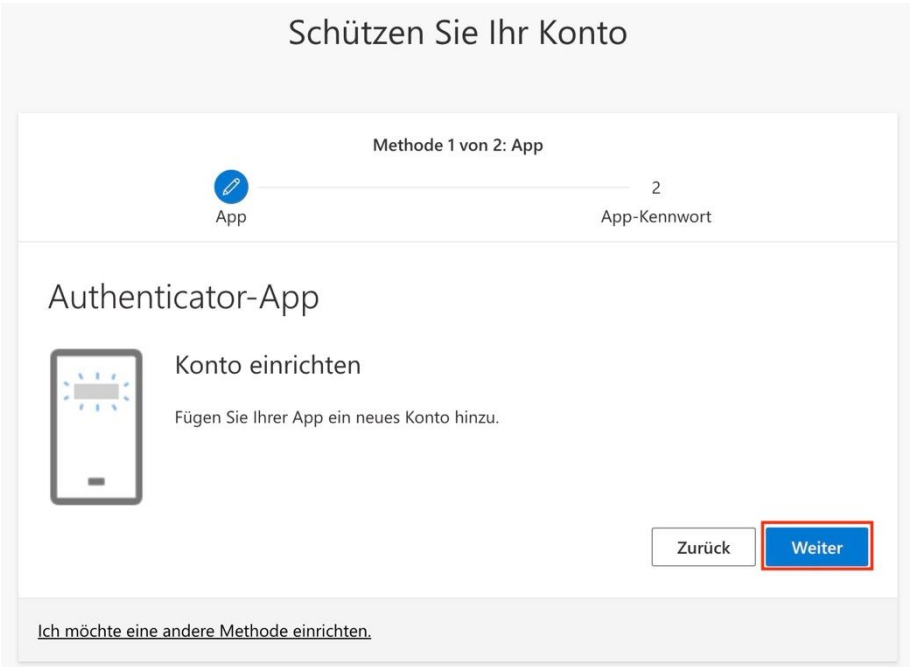
Hinweis zur MFA-Authentifizierung, auf „Weiter“ klicken

2. Methode der Multi-Faktor-Authentifizierung

Sie haben nun verschiedene Auswahlmöglichkeiten für die zusätzliche Authentifizierungsmethode zur Verfügung:

a. Microsoft Authenticator (bevorzugte Variante)
b. Weitere Authenticator Apps (z. B. Google Authenticator)
c. Hardware Token (z. B. ReinerSCT Authenticator)
d. andere Methode z. B. über SMS





3. Reiner SCT Authenticator

1. „OK“ drücken zum Einschalten.

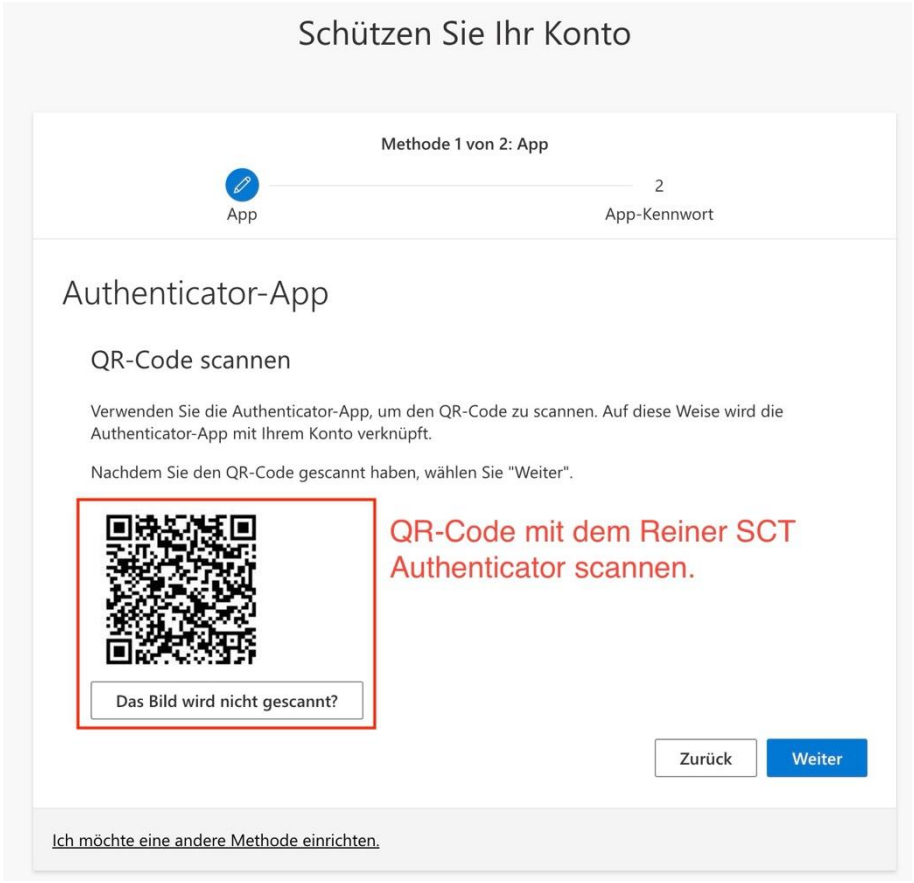
2. Das „Zahnrad“ drücken um in die Einstellungen zu gelangen.

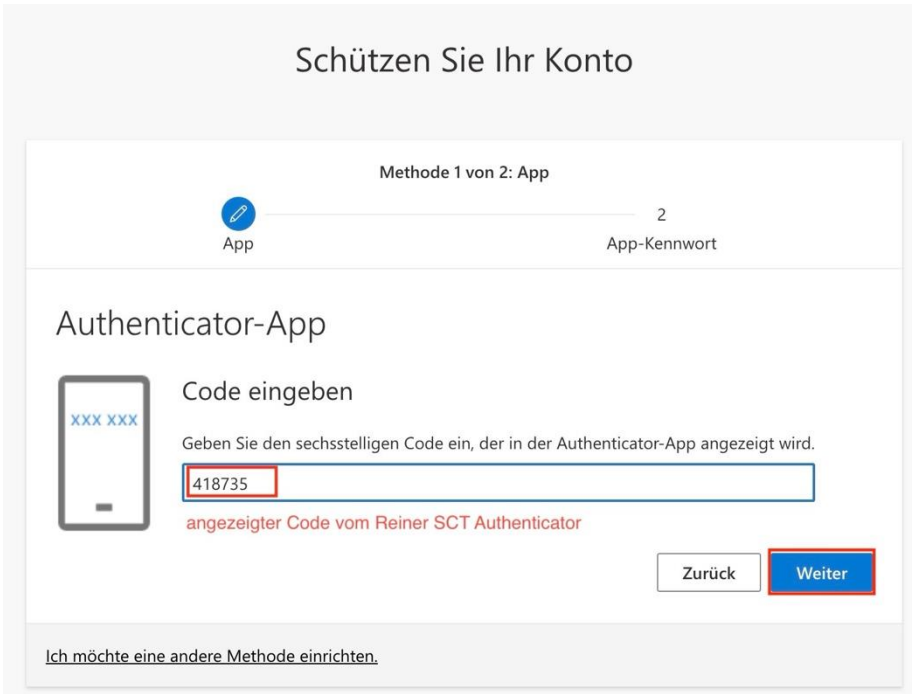
3. Die Taste „3“ drücken, um Konten hinzuzufügen.

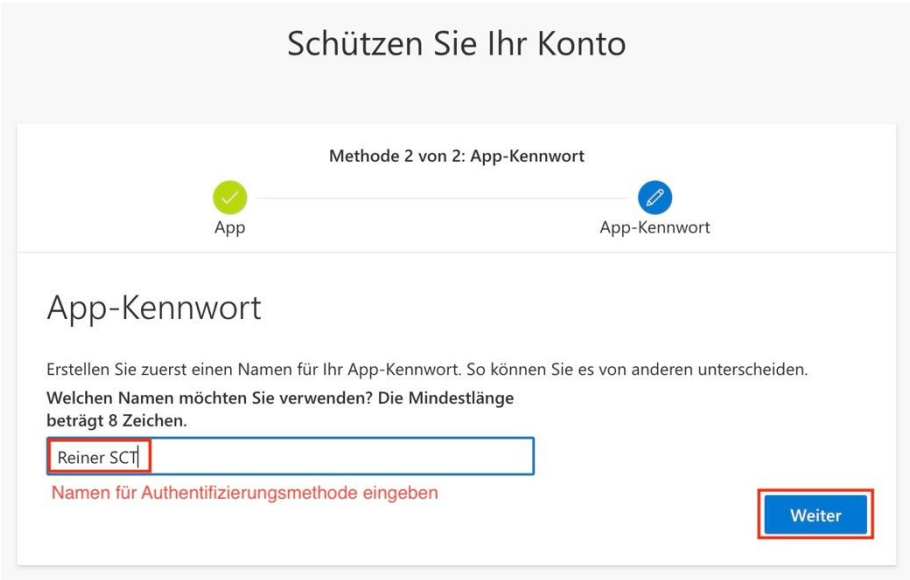
4. Die Taste „1“ drücken, um den QR-Code mit der integrierten. Kamera zu scannen.

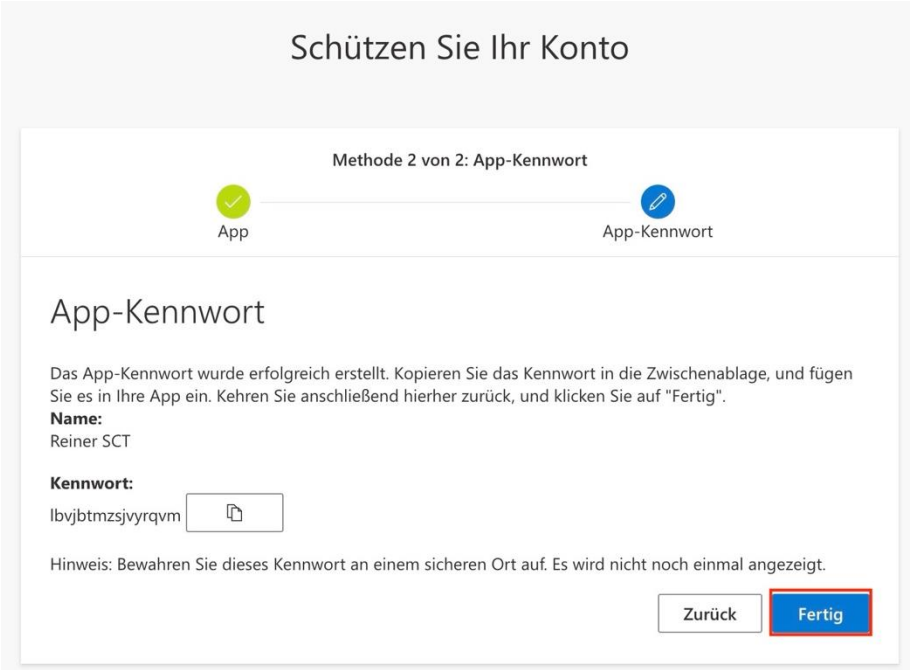
5. Die Einrichtung des Microsoft-Kontos ist abgeschlossen, der angezeigte Code kann jetzt zur Verifizierung des Kontos genutzt werden.

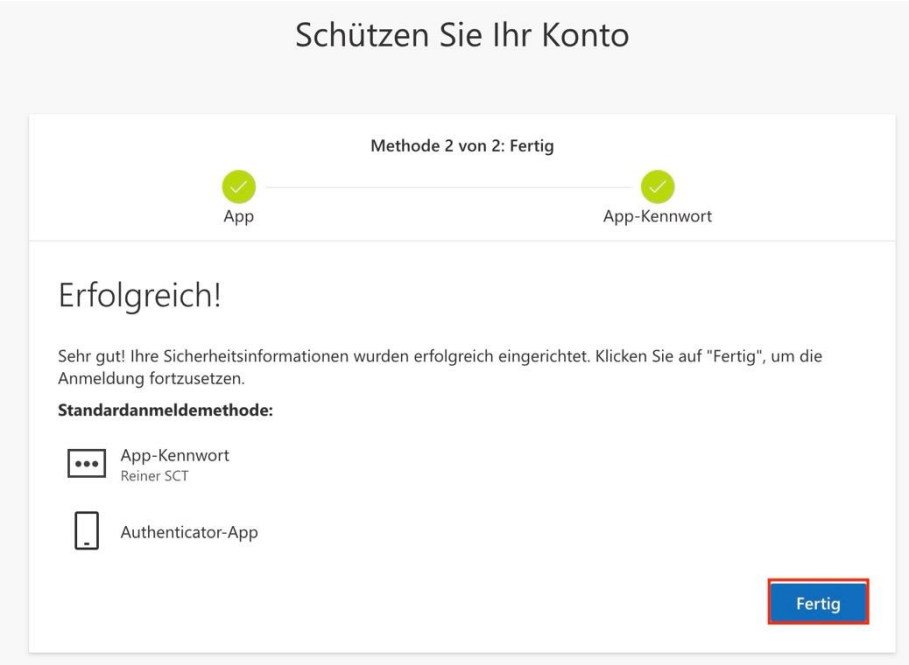
4. QR-Code mit dem Reiner SCT Authenticator scannen.






Schützen Sie Ihr Konto
Methode 2 von 2: App-Kennwort
App
App-Kennwort
App-Kennwort
Erstellen Sie zuerst einen Namen für Ihr App-Kennwort. So können Sie es von anderen unterscheiden.
Welchen Namen möchten Sie verwenden? Die Mindestlänge beträgt 8 Zeichen.
Reiner SCT
Namen für Authentifizierungsmethode eingeben
Weiter


Schützen Sie Ihr Konto
Methode 2 von 2: App-Kennwort
App
App-Kennwort
App-Kennwort
Das App-Kennwort wurde erfolgreich erstellt. Kopieren Sie das Kennwort in die Zwischenablage, und fügen Sie es in Ihre App ein. Kehren Sie anschließend hierher zurück, und klicken Sie auf "Fertig".
Name:
Reiner SCT
Kennwort:
lbvjbtmzsjvyrqvm
Hinweis: Bewahren Sie dieses Kennwort an einem sicheren Ort auf. Es wird nicht noch einmal angezeigt.
Zurück
Fertig



Die Einrichtung ist erfolgreich abgeschlossen.

Der Reiner SCT Authenticator ist erfolgreich eingerichtet und kann ab sofort für die Authentifizierung verwendet werden.

Sobald Sie versuchen, sich an einem Microsoft M365-Dienst anzumelden, und eine zusätzliche Authentifizierung per MFA nötig ist, benötigen Sie den Reiner SCT Authenticator, um sich anzumelden.

Bei Verlust wenden Sie sich umgehend an die IT, damit der verloren gegangene Reiner SCT Authenticator aus Ihrem Account gelöscht wird.

Wichtiger Hinweis:

Ein deaktivieren der MFA bei Verlust ist nicht möglich!
Um bei Verlust weiter Arbeiten zu können, müssen Sie entweder direkt ein Ersatzgerät beschaffen oder abholen oder den MS Authentifikator (App) als zweiten Faktor einrichten.

Schützen Sie den Reiner SCT Authenticator mit einem persönlichen PIN.
Eine Anleitung und weitere Informationen finden Sie unter:

https://www.reiner-sct.com/material/downloads/bedienungsanleitung/REINER-SCT-Bedienungsanleitung-REINER-SCT-Authenticator.pdf