Hochschule Karlsruhe
University of
Applied Sciences

Rechenzentrum

Anleitungen zu ausgewählten

RZ-Diensten

Version:	2.14
Veröffentlichung:	21.01.2026
Status:	Final
Autor:	X. Balodis, S. Roth, Dr. I. Schwab

https://rz.h-ka.de/intro

INHALTSVERZEICHNIS

1 RZ-Zugangsdaten

Wichtig: Das Initialpasswort muss zwingend im Hochschulnetz geändert werden, bevor Sie die RZ-Dienste nutzen können.

1.1 Studierende: Wo sind die RZ-Zugangsdaten zu finden?

a. Melden Sie sich bitte mit Ihren Bewerbungszugangsdaten beim Campus-Management-System "HISinOne"

https://rz.h-ka.de/campusmgmt

an. Das Campus-Management-System kennen Sie bereits aus dem Bewerbungsprozess.

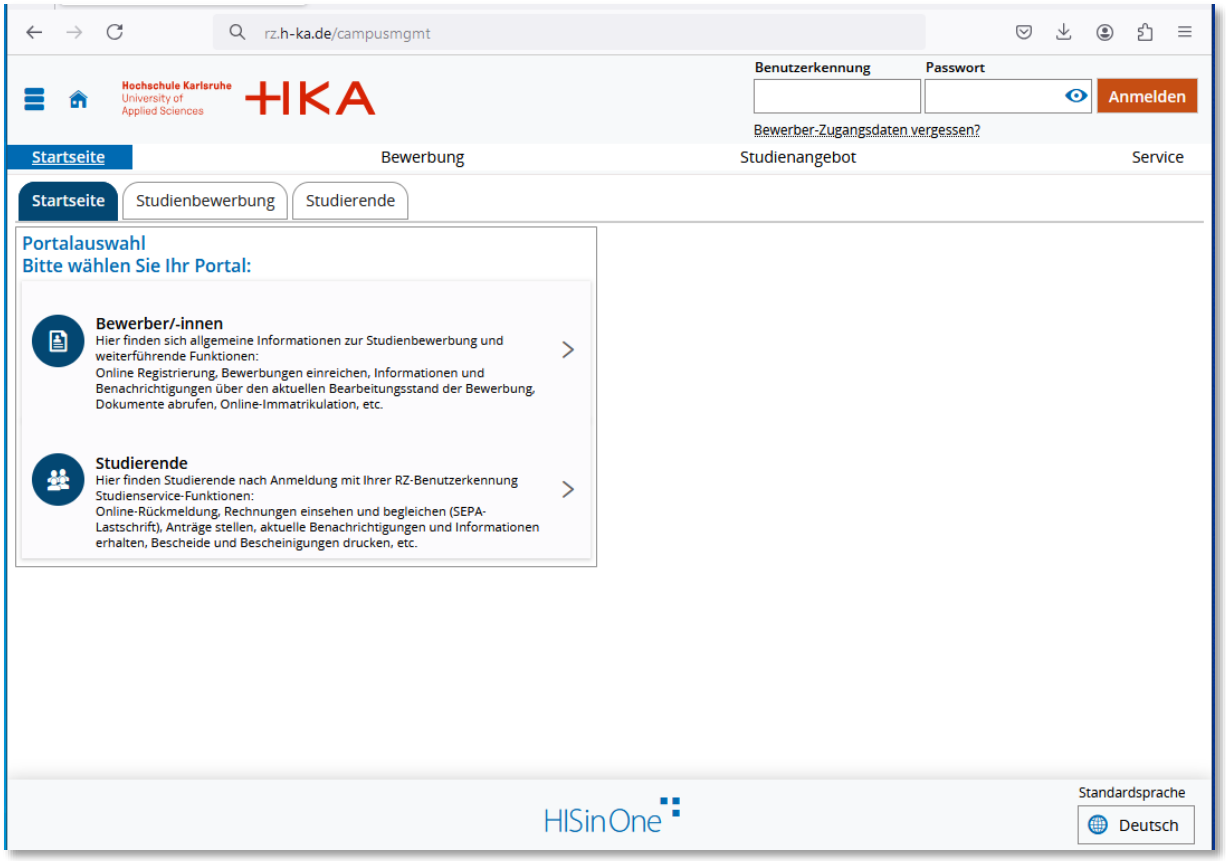

Abbildung 1 - HISinOne

b. Sollten Sie Probleme mit Ihren Bewerbungszugangsdaten oder allgemein mit dem Prozess haben, wenden Sie sich bitte an das Studierendenbüro. (Falls Sie bereits früher an der HKA immatrikuliert waren und mehr als vier Wochen zwischen Exmatrikulation und erneuter Immatrikulation liegen, besuchen Sie bitte die RZ-Benutzerberatung persönlich und bringen Sie Ihre Campuskarte mit).

Falls Sie Ihr **Bewerberpasswort** vergessen haben, wenden Sie sich bitte an das **Studierendenbüro**. Alternativ können Sie auf der HISinOne-Startseite (https://rz.h-ka.de/campusmgmt) den Link **„Bewerber-Zugangsdaten vergessen?“** auswählen. Geben Sie dort Ihre Bewerberkennung oder die private E-Mail-Adresse ein, die Sie bei der Bewerbung hinterlegt haben. Ergänzen Sie anschließend Ihr Geburtsdatum und beantworten Sie die Sicherheitsfrage. Nach einem Klick auf **„Zugangsdaten anfordern“** wird Ihnen ein neues Passwort an Ihre private E-Mail-Adresse gesendet.

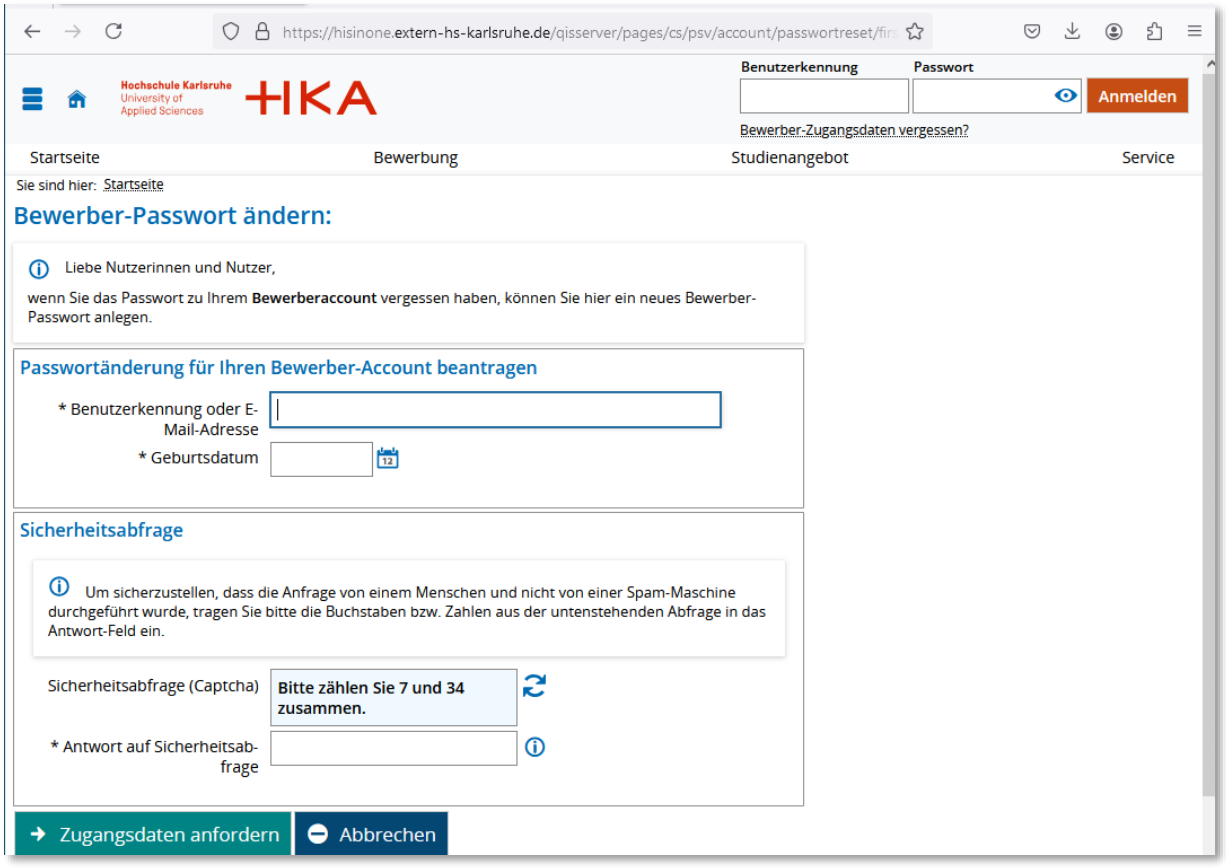

Abbildung 2 - HISinOne Bewerber-Passwort vergessen

c. Sobald Sie mindestens einen Tag vollständig im Studierendenbüro immatrikuliert sind, können Sie Ihre RZ-Zugangsdaten (RZ-Benutzername und zugehöriges RZ-Passwort) im Dokument "RZ-Zugangsdaten" einsehen. Das Schreiben finden Sie nach dem Einloggen bei HISinOne (https://rz.h-ka.de/campusmgmt) im Register "Studienservice" > "Bescheide" unter „Bescheinigungen“.
Beachten Sie, dass das Passwort nur beim **ersten** Aufruf des Dokuments angezeigt wird. Überprüfen Sie daher gegebenenfalls den Download-Ordner Ihres Rechners.
Speichern Sie dieses **Dokument** unbedingt an einem sicheren Ort.

Abbildung 3 - Dokument RZ-Zugangsdaten

d. Wichtig: Ändern Sie Ihr initiales RZ-Passwort unbedingt vor oder während der ersten Vorlesungswochen. Andernfalls kann das Campus-Management-System künftig nicht mehr genutzt werden und Sie können nicht auf die weiteren RZ-Dienste zugreifen. Zur Passwort-Änderung empfehlen wir einen PC auf dem Campus zu verwenden.

1.2 Studierende: Wo ändere ich das Initialpasswort (RZ-Passwort)?

Das **Passwort** kann ausschließlich **innerhalb des Hochschulnetzes** an der Hochschule geändert werden. Melden Sie sich hierzu an einem PC vor Ort (z. B. in Raum LI136 oder LI142) mit Ihren RZ-Zugangsdaten an und öffnen Sie anschließend das **User-Lifecycle-Management-System (ULM)** unter den Link

https://rz.h-ka.de/ulm

Rufen Sie unter „Change Password“ die Passwort-Änderungsseite auf.

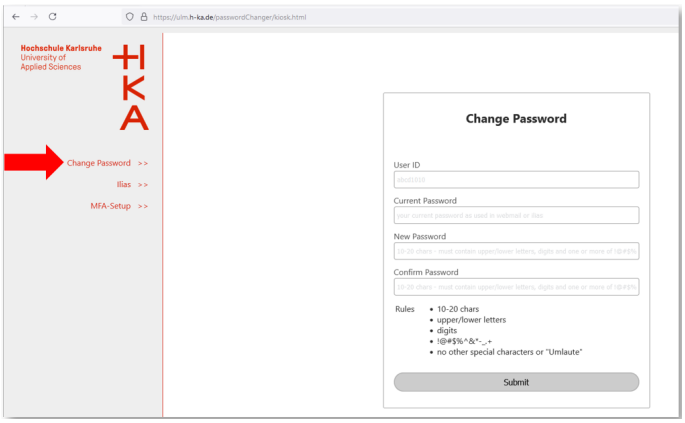

Abbildung 4 – User-Lifecycle-Management (ULM)

Geben Sie anschließend Ihr RZ-Benutzerkürzel unter „**User ID**“ sowie Ihr aktuelles Passwort unter „**Current Password**“ ein. Tragen Sie Ihr gewünschtes Passwort zweimal ein; bei „**New Password**“ und „**Confirm Password**“.
Unter **Rules** finden Sie die Anforderungen an ein neues Passwort, bspw. ist das Fragezeichen als Sonderzeichen nicht zulässig. Klicken Sie anschließend auf „**Submit**“.

Bei erfolgreicher Änderung erscheint die Meldung **password changed.**

1.3 Beschäftigte: Wie erhalte Sie Ihre RZ-Zugangsdaten?

Beschäftigte erhalten ihre **RZ-Zugangsdaten** gegen Vorlage eines amtlichen Lichtbildausweises zu den Öffnungszeiten der **RZ-Benutzerberatung** (Raum LI135). Diese ist **montags** bis **freitags** von **10:00 Uhr** bis **13:00 Uhr** geöffnet.

1.4 Beschäftigte: Wo ändern Sie Ihr Passwort?

Das **Initialpasswort** lässt sich direkt in der **Benutzerberatung** ändern.

Hinweis:
- Bitte bringen Sie auch Ihr Smartphone zur Benutzerberatung mit, damit bei Bedarf die Mehrfaktorauthentifizierung (MFA) eingerichtet werden kann.

- Sobald das Initialpasswort geändert können sich Beschäftigte in Raum LI111 einen ILIAS-Account erstellen lassen (falls benötigt).

Alternativ können Sie Ihr Initial- oder RZ-Passwort jederzeit im Hochschulnetz über

https://rz.h-ka.de/ulm

ändern, beispielsweise am Arbeitsplatzrechner oder in den PC-Pools.
Eine **Passwortänderung** ist außerdem im **eduroam-Netz** möglich, sofern Sie sich am Campus der Hochschule Karlsruhe befinden. Melden Sie sich dazu im eduroam-Netz an und öffnen Sie die Seite

https://rz.h-ka.de/ulm

Klicken Sie anschließend im ULM-System auf **„Change Password“**, um die Seite zur Passwortänderung aufzurufen.

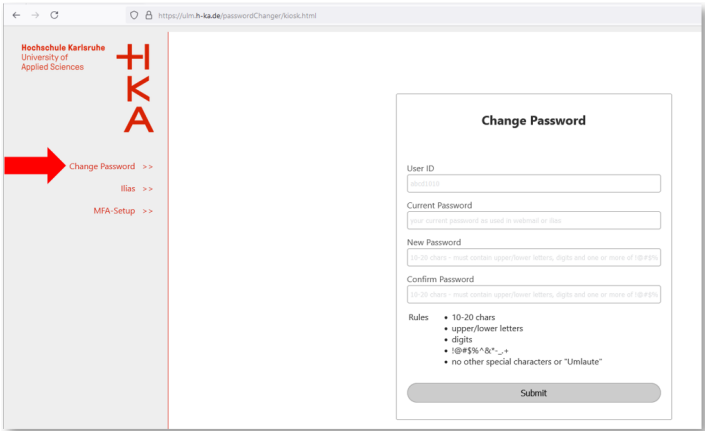

Abbildung 5 - User-Lifecycle-Management (ULM)

Geben Sie Ihr RZ-Benutzerkürzel unter „**User ID**“ ein und Ihr aktuelles Passwort unter „**Current Password**“. Tragen Sie Ihr neues, gewünschtes Passwort zweimal ein (in „**New Password**“ und „**Confirm Password**“). Unter „**Rules**“ werden die Passwortbedingungen angezeigt (z. B. ist das Fragezeichen nicht zulässig). Klicken Sie schließlich auf „**Submit**“. Bei erfolgreicher Änderung erscheint die Meldung „**password changed**“.

1.5 Passwort zurücksetzen

Falls Sie Ihr RZ-Passwort vergessen haben, können Sie es während den Öffnungszeiten in der Benutzerberatung (unter Vorlage eines amtlichen Lichtbildausweises) zurücksetzen lassen.
Aus Sicherheitsgründen ist der Versand von Passwörtern per E-Mail sowie eine telefonische Übermittlung **nicht** gestattet.

2 Mit neuen Zugangsdaten in das Hochschul-WLAN eduroam

Bitte verwenden Sie eduroam und keine anderen WLAN-Netze!

2.1 Was ist eduroam?

eduroam® ist ein globaler Dienst, welcher Studierenden, Forschenden und Lehrenden ermöglicht, eine Internetverbindung über ein Wireless-LAN herzustellen. Egal, ob Sie sich auf dem Campus bewegen oder Zeit damit verbringen, an einer anderen Forschungs- und Bildungseinrichtung zu studieren oder zu arbeiten, eduroam bietet Ihnen eine nahtlose Internetverbindung.

2.1.1 Wie funktioniert eduroam?

Mit eduroam auf Ihrem Laptop, Handy oder anderem Gerät müssen Sie keine speziellen Accounts beantragen oder Ausweise ausleihen – aktvieren Sie einfach Ihr Gerät und Sie sollten online sein. Die sichere und datenschutzfreundliche Technologie von eduroam macht die Eingabe von Benutzernamen und Passwörtern über unsichere Webbrowser-Formulare überflüssig. Ihr Gerät erkennt einen gültigen eduroam-Zugangspunkt und meldet sich automatisch an. Ihr Passwort wird niemals mit einem der Zugangspunkte geteilt. Ihr Passwort für Ihre Online-Identität erhalten Sie von Ihrer „Heimat"-Institution – an der Sie im Studium eingeschrieben oder beschäftigt sind.

2.1.2 Identifizierung gegenüber eduroam

Ihr Benutzername und Ihr Passwort, die Sie von Ihrer Heimatinstitution erhalten, bilden die Grundlage für die Anmeldedaten. Damit eine Zuordnung zur jeweiligen Einrichtung erfolgen kann, muss der Benutzername mit dem sogenannten Realm ergänzt werden. Der Realm der Hochschule Karlsruhe lautet **h-ka.de**.
Studierende und Beschäftigte der Hochschule Karlsruhe melden sich daher mit RZ-Kürzel@h-ka.de und dem zugehörigen RZ-Passwort an.
Gäste anderer Hochschulen, die an eduroam teilnehmen, nutzen hingegen den Benutzernamen ihrer Heimatinstitution ergänzt um den entsprechenden Realm und das zugehörige Passwort. Informationen zum Realm Ihrer eigenen Einrichtung erhalten Sie bei Ihrem zuständigen IT-Team.

2.1.3 Welche Technik nutzt eduroam?

In eduroam basiert die Kommunikation zwischen dem Access Point und der Heimatstation des Nutzers auf dem IEEE 802.1X-Standard; 802.1X umfasst die Verwendung von EAP, dem Extensible Authentication Protocol, das verschiedene Authentifizierungsmethoden zulässt. Abhängig von der Art des verwendeten EAP-Verfahrens wird entweder ein sicherer Tunnel vom Computer des Benutzers zu seiner Heimatstation aufgebaut, durch den die eigentlichen Authentifizierungsinformationen (Benutzername/Passwort usw.) übertragen werden (EAP-TTLS oder PEAP), oder gegenseitig Authentifizierung durch öffentliche X.509-Zertifikate, die nicht abhörbar sind, verwendet (EAP-TLS).

2.1.4 Ist die Nutzung von eduroam sicher?

eduroam basiert auf den sichersten heute existierenden Verschlüsselungs- und Authentifizierungsstandards. Seine Sicherheit geht weit über typische kommerzielle Hotspots hinaus. Beachten Sie jedoch, dass bei Nutzung des allgemeinen Internets an einem eduroam-Hotspot auch für Sie die lokalen Standortsicherheitsmaßnahmen an diesem Hotspot gelten. Beispielsweise können die Firewall-Einstellungen am besuchten Ort anders sein, als Sie es von zu Hause gewohnt sind, und als Gast haben Sie möglicherweise Zugriff auf weniger Dienste im Internet als zu Hause.

2.1.5 Verwendet eduroam ein Captive Portal zur Authentifizierung?

Nein. Webportal-, Captive-Portal- oder Splash-Screen-basierte Authentifizierungsmechanismen sind keine sichere Möglichkeit, eduroam-Anmeldeinformationen zu akzeptieren, selbst wenn die Website durch eine sichere HTTPS-Verbindung geschützt ist. Die verteilte Natur von eduroam würde bedeuten, dass den eduroam-Benutzern viele verschiedene Seiten, Sprachen und Layouts präsentiert würden, wodurch es unmöglich wäre, zwischen legitimen und gefälschten Seiten zu unterscheiden (selbst ein konsistentes Layout kann von einem Angreifer nachgeahmt werden). Eduroam erfordert die Verwendung von 802.1x, dass eine Ende-zu-Ende-Verschlüsselung bietet, um sicherzustellen, dass Ihre privaten Benutzerdaten nur Ihrer Heimatinstitution zur Verfügung stehen. Das Zertifikat Ihrer Heimatinstitution ist der einzige Punkt, dem Sie vertrauen müssen, unabhängig davon, wer eine zwischengeschaltete Infrastruktur betreibt. Webportale verlangen, dass Sie Ihrer Infrastruktur vertrauen, da Sie Ihr Passwort im Klartext erhalten, dies bricht die Ende-zu-Ende-Verschlüsselungsprinzipien von eduroam.

2.1.6 Funktioniert eduroam auf verschiedenen Plattformen

eduroam nutzt offene Standards, um plattformübergreifend einen einheitlichen Zugriff zu ermöglichen. Das heißt, eduroam funktioniert insbesondere auf Microsoft Windows, diversen Unix- und Linux-Varianten, Apple MacOS, Apple iOS und Google Android.

2.2 Wie richte ich eduroam ein?

Besuchen Sie das eduroam Configuration Assistant Tool (CAT), für die Hochschule Karlsruhe unter

https://rz.h-ka.de/eduroam

zu finden und klicken Sie auf den großen blauen Button „eduroam® Installationsprogramm herunterladen“. Folgen Sie den Anweisungen des gerätespezifischen Installationsprogramms. Im Laufe der Installation werden Sie nach den folgenden Parametern gefragt:

Benutzername:	RZ-Kürzel**@h-ka.de**
Password:	RZ-Passwort

Danach können Sie sich jederzeit an jedem Ort in das eduroam-Netzwerk einloggen.
Hinweis: Für Android-Smartphones empfiehlt es sich, vorab die kostenlose App **geteduroam** zu installieren.
Bei IPhone-Smartphones ist auszuwählen, dass Sie der **radius1**-Meldung vertrauen.

2.3 Ausstrahlung von eigenen WLAN-Netzen

Bitte beachten Sie, dass die Ausstrahlung von zusätzlichen WLAN-Netzen, insbesondere auch persönlichen Hotspots, die Bandbreite aller Nutzer massiv beeinträchtigt. Stellen Sie bitte sicher, dass der persönliche Hotspot Ihres Mobiltelefons in den Campusbereichen deaktiviert ist.

3 E-Mail-Kommunikation

3.1 Einführung

Dieses Kapitel erläutert die Verwendung von E-Mail, der Outlook Web App (OWA) und Webmail an der Hochschule Karlsruhe (HKA). Dabei werden die Unterschiede zwischen der browserbasierten OWA und der lokal installierten Outlook-Anwendung beschrieben. Zudem wird die Rolle der Mehrfaktorauthentifizierung (MFA) für den externen Zugriff erklärt und der Zugriff auf Gruppenpostfächer in OWA näher erläutert.

Es gibt mehrere Möglichkeiten die Mails abzurufen:

- **Lokal installierte Outlook-Anwendung**: Mit der lokal installierten Outlook-Anwendung können Sie Ihre Mails bspw. in den PC-Pools oder am Arbeitsplatz-Rechner an der Hochschule abrufen, indem Sie in die Windows-Suchleiste den Suchbegriff **Outlook** eingeben und die Enter-Taste drücken. Eine Mehrfaktorauthentifizierung ist nicht erforderlich.

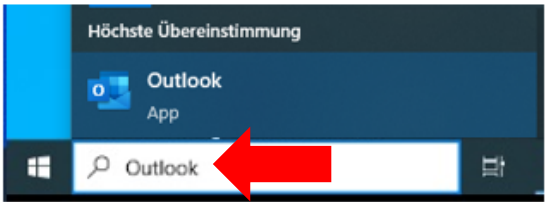

Abbildung 6 - Windows-Suche nach Outlook

- **Webmail an der Hochschule**: Ihre Mails können Sie hochschulintern bspw. in den PC-Pools, an Ihrem Arbeitsplatz-Rechner oder per eduroam (an der Hochschule) mittels Browser-Zugriff über die Seite https://webmail.h-ka.de abrufen. Hierbei benötigen Sie keine Mehrfaktorauthentifizierung.
  Öffnen Sie einen beliebigen Browser, geben Sie in den Browserleiste **https://webmail.h-ka.de** ein und klicken Sie auf die Enter-Taste.
  Bei **Benutzername** geben Sie Ihr RZ-Benutzerkürzel ein (ohne @h-ka.de) und bei **Passwort** geben Sie Ihr RZ-Passwort ein.

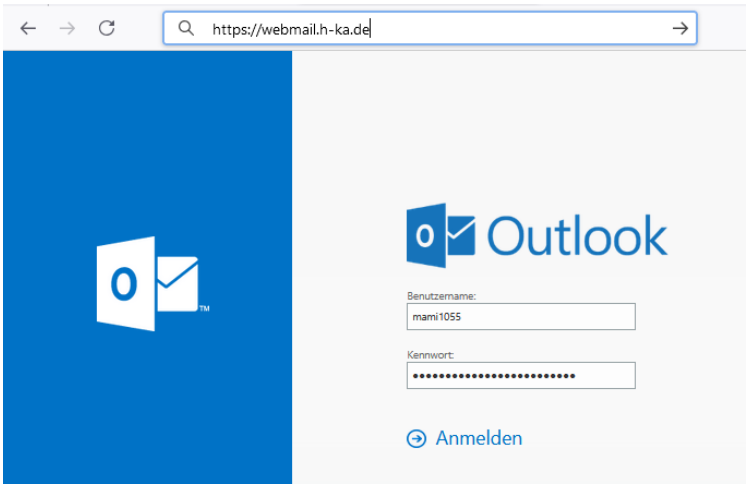

Abbildung 7 - Anmeldung bei Outlook

- **Outlook Web App (OWA)**: Des Weiteren haben Sie die Möglichkeit, Ihre Mails per Mehrfaktorauthentifizierung von außerhalb des Hochschulnetzes mittels Browser-Zugriff über die Seite https://owa.h-ka.de abzurufen. Eine Anleitung für den Abruf der Emails mittels Mehrfaktorauthentifizierung finden Sie im weiteren Verlauf.

3.2 Unterschied zwischen den Zugriffsvarianten

Studierende und Mitarbeitende nutzen ihre HKA-E-Mailkonten täglich. Dabei stellt sich oft die Frage, ob sie E-Mails über einen Webbrowser (OWA) oder mithilfe der lokal installierten Outlook-Anwendung verwalten sollten. Nachfolgend sind die wichtigsten Unterschiede zusammengefasst:

3.2.1 Grundprinzip OWA (Outlook Web App)

Browserbasierter Zugriff:
OWA läuft in gängigen Browsern wie Chrome, Firefox oder Edge, ohne dass eine separate Installation benötigt wird.

Online-Nutzung:
Für den Zugriff ist eine stabile Internetverbindung erforderlich.

Funktionsumfang:
Die wichtigsten E-Mail-Funktionen (Senden/Empfangen, Kalender, Terminverwaltung, Kontaktmanagement, Aufgaben) sind verfügbar. Bestimmte Add-Ins oder Offlinefunktionen stehen jedoch nicht zur Verfügung.

Einfache Erreichbarkeit:
Besonders geeignet, wenn Sie von einem fremden Rechner aus arbeiten oder schnell ortsunabhängig auf Ihr HKA-Konto zugreifen müssen.

3.2.2 Grundprinzip Outlook (lokal installiert)

Installation auf dem Endgerät:
Outlook wird als Teil von Microsoft Office auf den Arbeitsplatzrechnern für Mitarbeitende sowie auf den PC-Pool-Rechnern für Studierende bereitgestellt.

Erweiterte Funktionen:
Die lokale Version unterstützt Offline-Zugriff, komplexe E-Mail-Regeln und die Integration mit anderen Office-Anwendungen.

Performance und Personalisierung:
Outlook ermöglicht umfangreiche Anpassungen, etwa durch eigene Ordnerstrukturen, Farbschemata oder benutzerdefinierte Menüs.

Offline-Nutzung:
E-Mails können auch ohne Internetverbindung gelesen und vorbereitet werden. Eine Synchronisation erfolgt automatisch beim nächsten Online-Zugriff.

Zertifikate:
Zertifizierte Emails können nur über die lokal installierte Outlook Version verschickt werden.

3.2.3 Wann ist welche Zugangsvariante sinnvoll?

OWA:
Geeignet für Gelegenheitsnutzer, für den kurzfristigen oder mobilen Zugriff sowie in Situationen, in denen keine Outlook-Installation zur Verfügung steht.

Outlook (lokal):
Empfehlenswert bei regelmäßiger und intensiver E-Mail-Nutzung, insbesondere wenn fortgeschrittene Funktionen, zertifizierte Emails und häufige Offlinenutzung benötigt werden.

3.2.4 Liste der globalen Emailverteiler

Die Berechtigung zum Hochschulweiten Mailversand über die globalen Verteiler unterliegen einem Moderationsteam, welche die Mails begutachten und entweder freigeben oder ablehnen. Sollte das Moderationsteam innerhalb von 48 Stunden keine Entscheidung treffen, erfolgt eine systemseitige Ablehnung.
Folgende globale Verteilergruppen existieren:

- akadMitarbeitende
- Lehrbeauftragte
- NichtstudentischeMitglieder
- Professorenschaft
- Studenten
- Studentinnen
- Studierende
- VTMitarbeitende

Spezielle Verteiler für die Kommunikation mit Erstsemester-Studierende:

- erstsemester@h-ka.de

- erstsemester.ab@h-ka.de
- erstsemester.eit@h-ka.de
- erstsemester.imm@h-ka.de
- erstsemester.iwi@h-ka.de
- erstsemester.mmt@h-ka.de
- erstsemester.w@h-ka.de

4 Mehrfaktorauthentifizierung (MFA)

4.1 Einführung

Zum Schutz der Sicherheit wird der externe Zugriff auf die Dienste der Hochschule Karlsruhe durch die Mehrfaktorauthentifizierung (MFA) abgesichert. Neben dem Benutzernamen und Passwort (dem ersten Faktor) wird ein zusätzlicher, zweiter Faktor verlangt. Der zweite Faktor kann aus sehr unterschiedlichen Informationen bestehen, beispielsweise aus

- einem TOTP-Code („time-based one-time password“), der sich regelmäßig ändert,
- einer One-Time-Transaktionsnummer (aus einer vordefinierten Liste),
- einem persönlichen Zertifikat,
- einem YubiKey (AES-Schlüssel in einem Hardware-Token), oder
- einem Passkey[1] (kryptografischer Schlüssel).

Für alle externen Zugriffe auf interne Hochschule-Dienste (z. B. OWA und Outlook, Zeiterfassung, Wahlsysteme), VPN-Verbindungen und den QIS-Servern (Online-Service für die Prüfungsanmeldung und Prüfungsabmeldung und zur Noteneinsicht) werden Mehrfaktorauthentifizierung (MFA) vorausgesetzt. Dabei erhöht ein zusätzlicher Code neben Benutzername und Passwort das Sicherheitsniveau deutlich.

4.1.1 Zweck der MFA

Erhöhte Sicherheit:
Selbst wenn Ihr RZ-Passwort kompromittiert wird, verhindert der fehlende zweite Faktor den unberechtigten Zugriff.

Schutz sensibler Daten:
Die MFA bietet einen hohen Schutzlevel für vertrauliche Dokumente, Forschungsdaten und andere kritische Informationen.

4.2 Einrichtung der TOTP-Mehrfaktorauthentifizierung (MFA)

4.2.1 Installation der Authenticator-App

Laden Sie eine passende Authenticator-App auf Ihr Smartphone, beispielsweise privacyIDEA, Microsoft Authenticator oder Google Authenticator.

4.2.2 Abruf der Sicherheitsinformation („Token“)

- Rufen Sie über das Hochschulnetz (etwa eduroam auf dem Campus, PC-Pool-Rechner oder Arbeitsplatzrechner im LAN) die Webseite https://mfa.h-ka.de auf.
  ***Wichtig**:* Diese Seite ist nur innerhalb des Hochschulnetzes zugänglich.

- Melden Sie sich an und wählen Sie **„Token ausrollen“**, um ein neues Token anzulegen.
  ***Hinweis**:* Im Feld **„PIN/Passwort“** ist keine Eingabe erforderlich.

[1] Erst ab Wintersemester 2026/27.

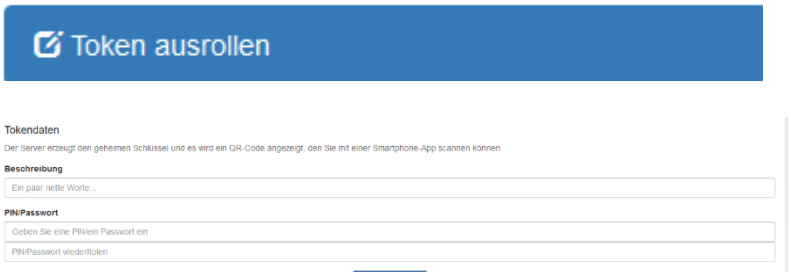

Abbildung 8 - Token ausrollen

4.2.3 Registrierung des Tokens

Scannen Sie den angezeigten QR-Code mit Ihrer Authenticator-App, um das Token in der App anzulegen.

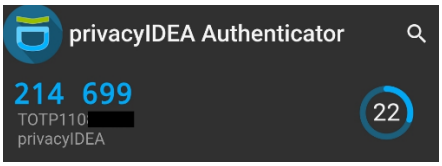

Abbildung 9 – Beispiel einer TOTP-Nummer bei der Authenticator App PrivacyIDEA

Beschreibung: Diese Abbildung 8 zeigt den sechsstelligen TOTP-Code (z. B. 214699) sowie einen Countdown (22 Sekunden), bis der nächste Code generiert wird.

4.2.4 Zurücksetzen des Fehlerzählers

Zur Abwehr von Brute-Force-Angriffen protokolliert das System fehlerhafte Anmeldeversuche. Ab dem zehnten Fehlversuch wird der MFA-Zugang automatisch gesperrt.

Vorgehensweise

Öffnen Sie bei einer Sperrung erneut die MFA-Konfigurationsseite (z. B. https://mfa.h-ka.de) **aus dem Hochschulnetz**.

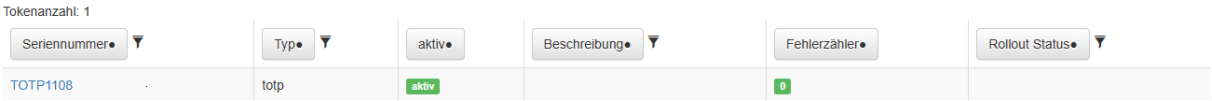

Abbildung 10 - Fehlerzähler prüfen

Abbildung 10: Im Reiter „Fehlerzähler“ können Sie die Anzahl der Fehlversuche einsehen. Sobald dieser Zähler den Wert 10 erreicht, ist das zugehörige Token gesperrt.

Durch Klicken auf die angezeigte Zahl können Sie den Fehlerzähler zurücksetzen. In der Beispieldarstellung (Abbildung 10) wurde der Zähler bereits auf 0 gesetzt.

Abschluss und Hinweise:

- Nach dem erfolgreichen Zurücksetzen des Fehlerzählers können Sie sich mit Ihren korrekten Zugangsdaten und einem gültigen MFA-Code erneut anmelden.
- Sollten dabei Probleme auftreten, wenden Sie sich bitte an die RZ-Benutzerberatung oder Ihre IT-Administratoren.

4.3 TAN-Liste für die Mehrfaktorauthentifizierung

Anstelle eines zeitbasierten Tokens, den Sie mit dem Smartphone scannen, können Sie auch eine **TAN-Liste** auf Papier erstellen.

- Melden Sie sich zunächst auf der MFA-Seite https://mfa.h-ka.de an.
  a. Wählen Sie „**Token ausrollen**“.
  b. Entscheiden Sie sich im Dropdown-Menü für „**TAN: TANs printed on a sheet of paper**“.
  c. Das Feld **„PIN/Passwort“** können/sollten Sie frei lassen – damit würden Sie zusätzlich die Einmalpasswörter absichern.
  d. Klicken Sie anschließend auf „**Token ausrollen**“.

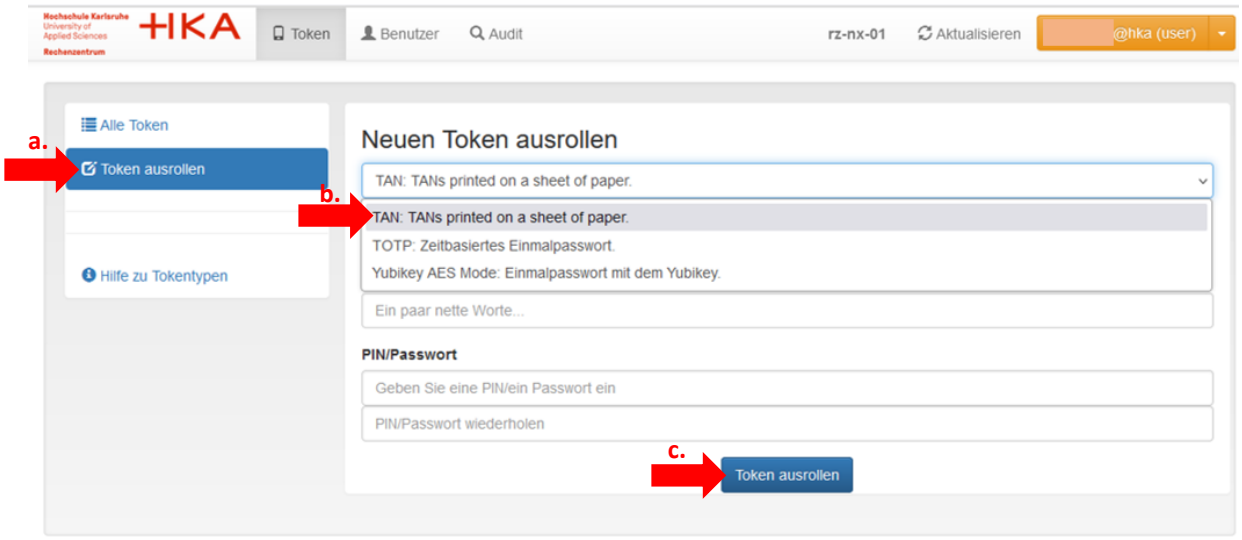

Abbildung 11 - MFA TAN-Liste erstellen

- Es erscheint eine Meldung, dass das **Token mit der Seriennummer … erfolgreich ausgerollt wurde**. Klicken Sie nun auf „**OTP-Liste drucken**“.

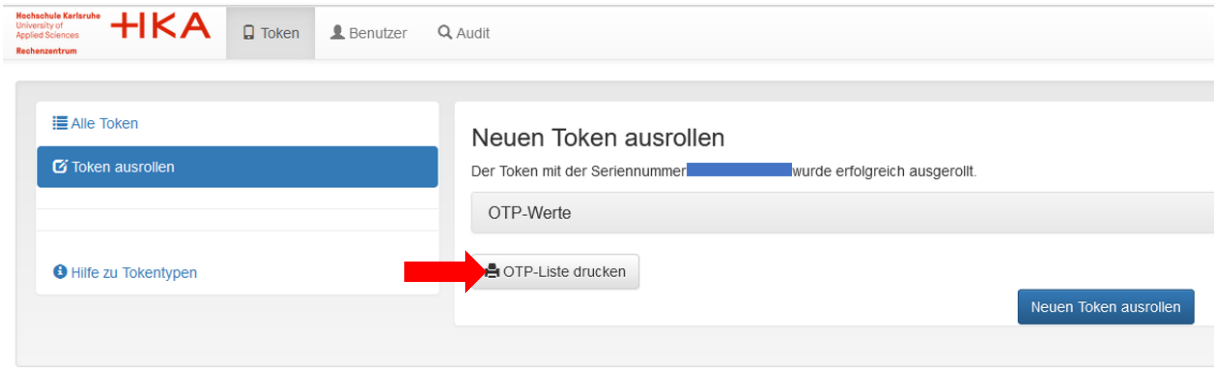

Abbildung 12 – MFA TAN-Liste drucken

- Im nächsten Schritt öffnet sich das **Drucken-Fenster**. Wählen Sie dort unter „Ziel“ die Option „**Als PDF speichern**“ und klicken Sie anschließend auf „**Speichern**“.

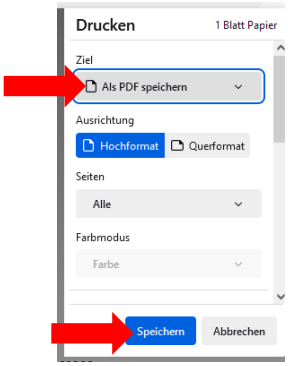

Abbildung 13 - MFA TAN-Liste speichern

- Legen Sie die PDF-Liste der TAN-Nummern beispielsweise auf Ihrem Desktop ab und klicken Sie erneut auf „**Speichern“**.

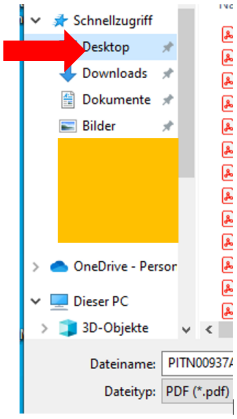

Abbildung 14 - Speicherort wählen

Einsatz der TAN-Liste (beispielsweise zum Abrufen von Emails).

1. Öffnen Sie die Seite https://owa.h-ka.de.
2. Geben Sie bei **„Username“** Ihr **RZ-Benutzerkürzel** ein.
3. Tragen Sie unter **„PIN+TOTP“** die **erste TAN** Ihrer Liste ein (beginnend bei Nummer „0“) und gehen Sie anschließend in aufsteigender Reihenfolge vor.

   ***Hinweis**:* Jede TAN-Nummer kann nur **einmal** verwendet werden und ist nach Gebrauch ungültig.

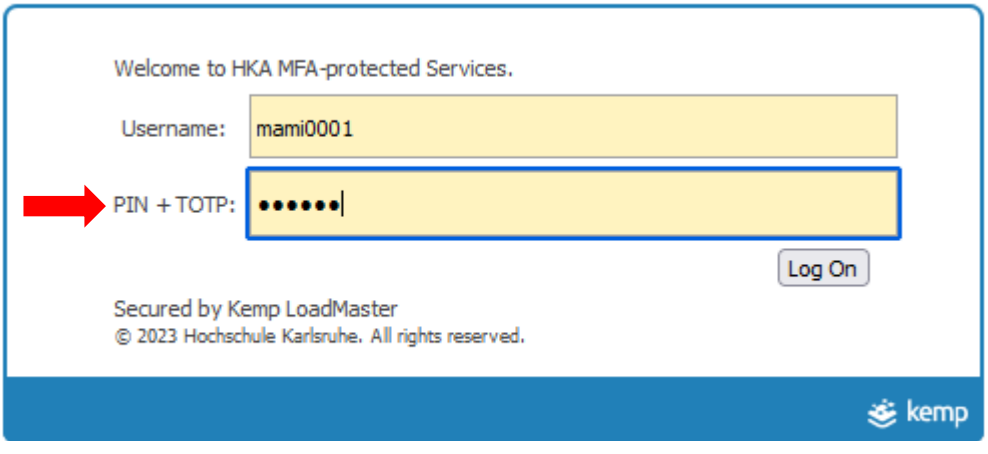

Abbildung 15 – Eingabe der MFA TAN- Zugangsdaten

4.4 Schritt-für-Schritt-Anleitung (Beispiel OWA)

Im Folgenden wird exemplarisch erläutert, wie Sie extern auf Ihr HKA-E-Mail-Postfach zugreifen.

1. **Browser öffnen und OWA aufrufen**
   - Öffnen Sie einen Webbrowser (Chrome, Firefox, Edge etc.) und navigieren Sie zur URL der Outlook Web App (z. B. https://owa.h-ka.de).

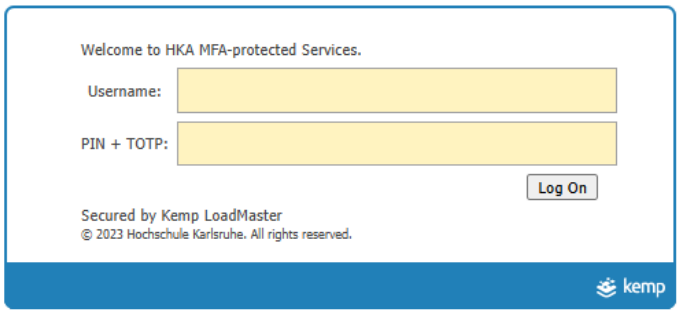

Abbildung 16 - MFA Authentifizierung

2. **Erste Eingabe: RZ-Kürzel & TOTP**
   - Tragen Sie im Feld „Username“ Ihr RZ-Kürzel ein (z. B. abcd0001).
   - Geben Sie im Feld „PIN + TOTP“ **ausschließlich** den sechsstelligen Code Ihrer Authenticator-App ein.
   - ***Hinweis**:* Jeder TOTP-Code ist nur 30 Sekunden gültig. Ein abgelaufener Code führt zu einem Fehlversuch und erhöht den Fehlerzähler der MFA. Erreichen Sie zehn Fehlversuche, wird Ihr Account temporär für MFA-Versuche gesperrt.

Abbildung 17 - Outlook Anmeldemaske

3. **Zweite Eingabe: RZ-Kürzel & Passwort**

   Nach erfolgreicher TOTP-Prüfung erscheint ein zweites Eingabefeld (s. Abbildung 17), in dem Sie Ihr RZ-Kürzel sowie das zugehörige RZ-Passwort eingeben müssen.

   Wichtig: Für die Anmeldung muss Ihr Initialpasswort bereits geändert sein.

4. **Anmeldung abschließen**
   - Klicken Sie auf **Anmelden**. Bei erfolgreicher Verifizierung erhalten Sie Zugriff auf Ihr Exchange-Postfach.
   - Sie können nun E-Mails lesen, verfassen, beantworten und weitere Exchange-Funktionen wie Kalender oder Kontakte nutzen.

4.5 Wichtige Hinweise für die Mehrfaktorauthentifizierung (MFA)

- **Code-Gültigkeit:** Jeder TOTP-Code verfällt nach 30 Sekunden.

- **Fehlversuche:** Nach zehn Fehlversuchen sperrt das System Ihren MFA-Zugang. Der Fehlerzähler zählt sich bei Fehlversuchen immer nur nach oben. Auch bei einer richtigen Eingabe bleiben die bereits vorhandenen Fehlversuche bestehen.

- **Fehlerzähler prüfen:** Bitte prüfen Sie regelmäßig hochschulintern auf der Seite https://mfa.h-ka.de , ob Ihr Fehlerzähler sich hochgezählt hat. Löschen Sie ggf. den Fehlerzähler, indem Sie bspw. auf die rot-hinterlegte Zahl „10“ klicken.

Abbildung 18 - MFA Fehlerzähler

- **Screenshot-Referenz:** In Abbildung 8 sehen Sie den aktuell gültigen Code (**214699**) sowie die noch verfügbaren Sekunden bis zur Neugenerierung. Warten Sie bis sich der Code erneuert hat und geben Sie dann erst den neuen Code ein.

- **Eingabe beachten**: Bei **Username** geben Sie nur Ihr RZ-Benutzerkürzel in Kleinbuchstaben ein und ohne @h-ka.de. Bei **PIN+TOTP** geben Sie **nur** die 6-stellige Nummer der Authenticator-App ein, welche sich nach 30 Sekunden ändern und nicht Ihr RZ-Passwort. Bitte warten Sie mit der Eingabe der 6-Ziffern bis sich die 6-Ziffern nach 30 Sekunden erneut haben.

- **Uhrzeit prüfen**: Falls Sie nach mehreren Versuchen merken, dass die **PIN+TOTP –** Eingabe fehlschlägt, prüfen Sie die Uhrzeit (und die Zeitzone) an Ihren für die MFA eingesetzten Endgeräten und stellen Sie ggf. die Uhrzeit auf automatisch aktualisieren ein.

- **Funktionsfähigkeit des TOTPs prüfen**: Auf der Portalseite haben Sie zwei Möglichkeiten, den Zugang zu prüfen: Mittels „OTP-Wert prüfen“ testen Sie die Funktionsfähigkeit des One-Time-Tokens, mit „Token prüfen“ verifizieren Sie die Gesamtzeichenkette inklusive Ihrer vergebener PIN.

- **Token neu ausrollen**: Falls weiterhin kein Zugriff möglich ist, dann loggen Sie sich hochschulintern unter https://mfa.h-ka.de ein. Klicken Sie anschließend auf die TOTP-Nummer in der Spalte **Seriennummer**.

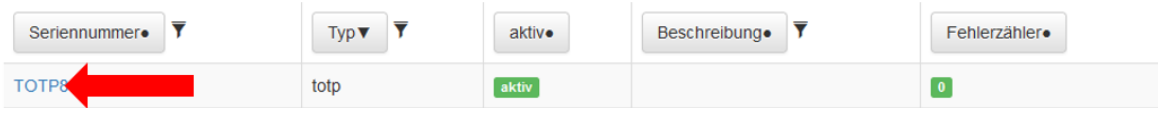

Abbildung 19 - MFA TOTP-Nummer

Es erscheint eine Detail-Ansicht. Klicken Sie nun auf **Löschen**.

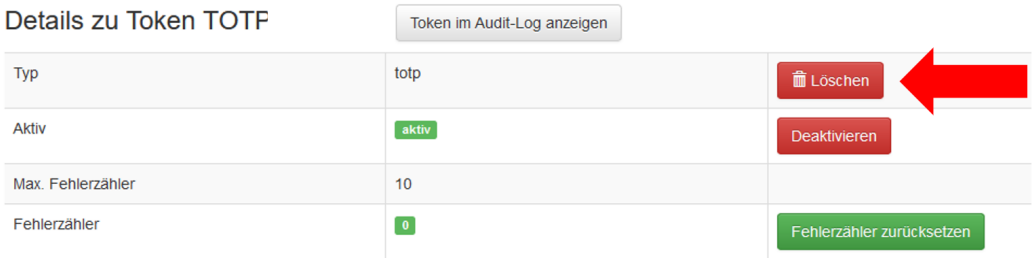

Abbildung 20 - Löschen des Tokens

Löschen Sie den Token auch auf Ihrem Endgerät und legen Sie sich nach den Schritten in Kapitel 4 einen neuen Token an.

- **Authenticator-App des Herstellers PrivacyIDEA**: Des Weiteren kann es hilfreich sein, die Authenticator-App des Herstellers zu verwenden. Hierzu öffnen Sie bspw. bei Ihrem Smartphone den Play-Store, laden sich die privacyIDEA Authenticator-App der Firma NetKnights GmbH herunter und installieren Sie sich diese Authenticator-App. Zum Einrichten der Authentifizierung folgen Sie den Schritten in Kapitel 4.

4.6 Anleitung zur Einrichtung einer Mehrfaktorauthentifizierung ohne Smartphone

Es handelt sich um eine Variante der Mehrfaktorauthentifizierung mittels des Clients **Authenticator Extension**. Der Authenticator Extension generiert Authentifizierungscodes im Browser und es ist kein weiteres Endgerät (wie bspw. ein Smartphone) erforderlich. Der **Authenticator Extension** kann mit folgenden Browsern verwendet werden: Mozilla Firefox, Microsoft Edge und Google Chrome.

Im Folgenden wird die Authentifizierung anhand des Browsers **Mozilla Firefox** gezeigt.

1.) Um den Client **Authenticator Extension** aufzurufen, öffnen Sie den folgenden Link:

https://authenticator.cc

Anschließend wählen Sie einen von Ihnen verwendeten Browser auf, indem man bspw. auf „**Add to Firefox**“ klickt.

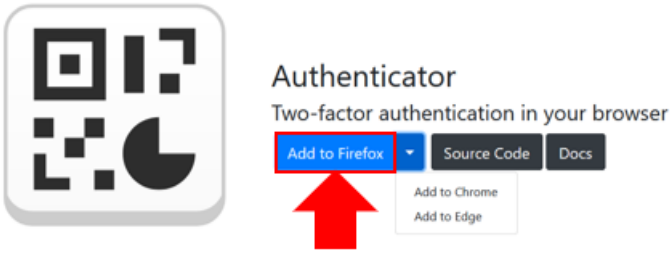

*Abbildung 21 - **Authenticator Extension** in Firefox hinzufügen*

2.) Es öffnet sich die Seite **Firefox Browser ADD-ONS** (https://addons.mozilla.org/en-US/firefox/addon/auth-helper/?src=external-website).
Wählen Sie erneut den Button „**Add to Firefox**“.

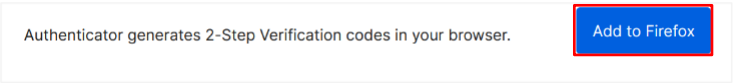

Abbildung 22 – Add to Firefox

3.) Klicken Sie auf das Puzzle-Symbol in Ihrem Browser. Setzen Sie einen Haken bei „**Ausführen der Erweiterung in privaten Fenstern erlauben**“ und bestätigen Sie die Auswahl mit dem Button „**Hinzufügen**“.

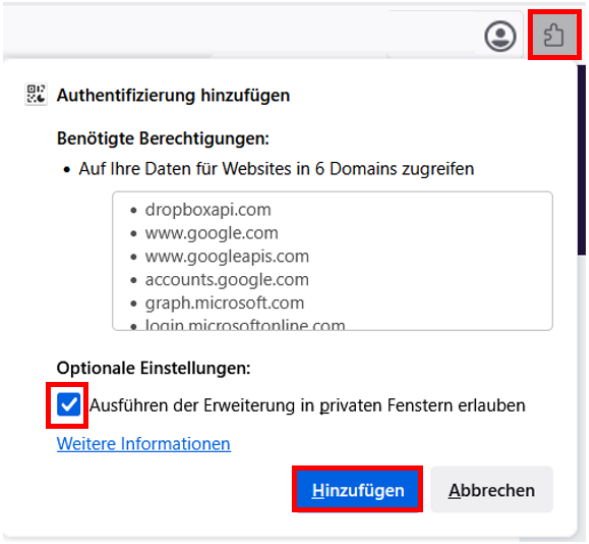

Abbildung 23 - Authentifizierung hinzufügen

4.) Danach öffnet sich das Popup-Fenster **Authentifizierung wurde hinzugefügt**.
Setzen Sie einen Haken bei „**Erweiterung an Symbolleiste anheften**“ und bestätigen Sie die Auswahl mit dem Button „**OK**“.

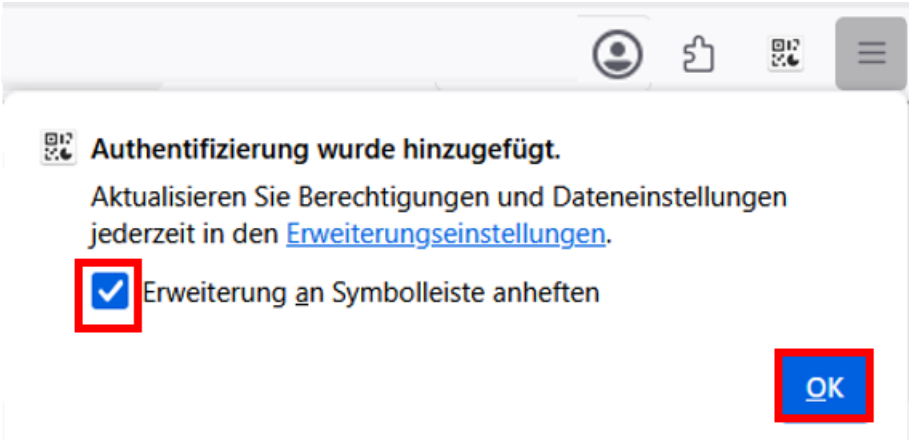

Abbildung 24 – Erweiterung an Symbolleiste anheften

5.) In der Browser-Leiste erscheint nun ein QR-Code-Symbol.

Abbildung 25 – QR-Code-Symbol wählen

6.) Öffnen Sie die Webseite https://mfa.h-ka.de über das Hochschulnetz (bspw. Eduroam auf dem Campus, an einem PC-Pool-Rechner oder am Arbeitsplatzrechner im LAN).
Wichtig: Diese Seite ist nur innerhalb des Hochschulnetzes zugänglich.

7.) Melden Sie sich mit Ihren RZ-Zugangsdaten an und wählen Sie „**Token ausrollen**“, um ein neues Token anzulegen.
Hinweis: Im Feld **„PIN/Passwort“** ist keine Eingabe erforderlich.

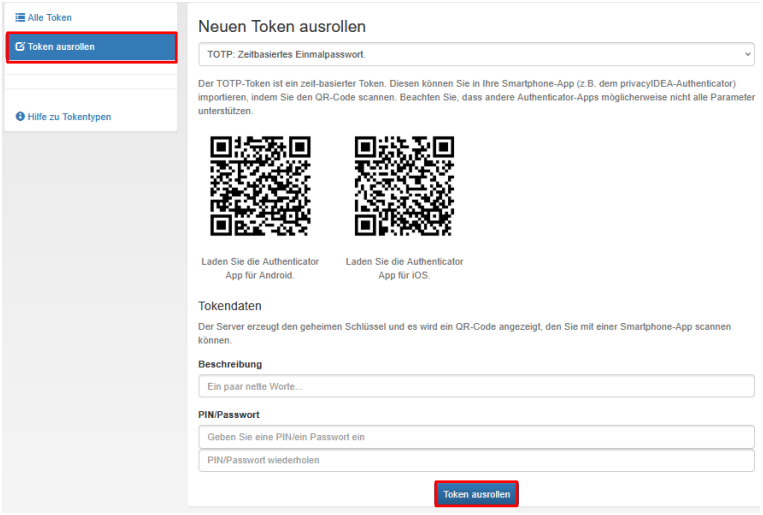

Abbildung 26 - Token ausrollen

8.) Es öffnet sich ein Popup-Fenster, welches mit dem Button „**OK**“ zu bestätigen ist.

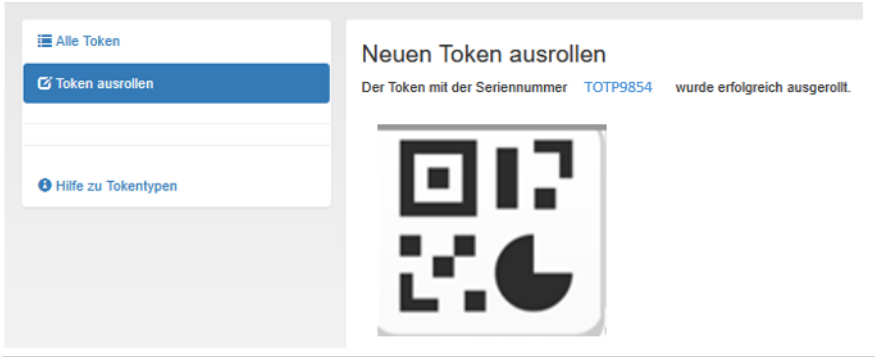

Abbildung 27 – Neuer Token

9.) Klicken Sie nun auf das QR-Code-Symbol . Es öffnet sich das Fenster **Authentifizierung**. Wählen Sie nun auf das Stift-Symbol .

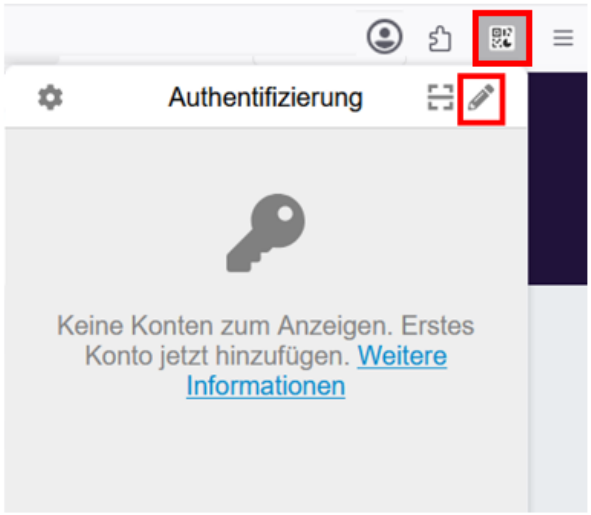

Abbildung 28 – Stift-Symbol

10.) Im nächsten Schritt klicken Sie auf das „**+**“-Zeichen.

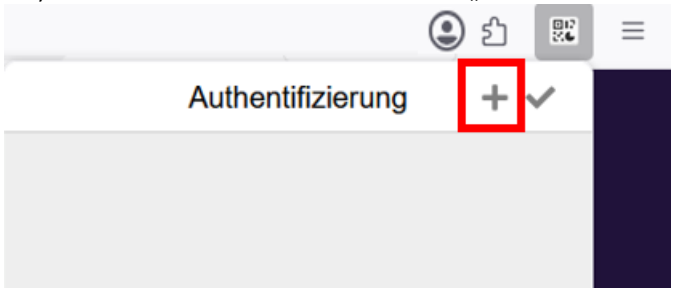

Abbildung 29 – „+“-Zeichen auswählen

11.) Wählen Sie den Button „**QR Code scannen**“ und scannen Sie den QR-Code. Mit gedrückter, linker Maustaste können Sie mit dem Scannen des QR-Codes beginnen.

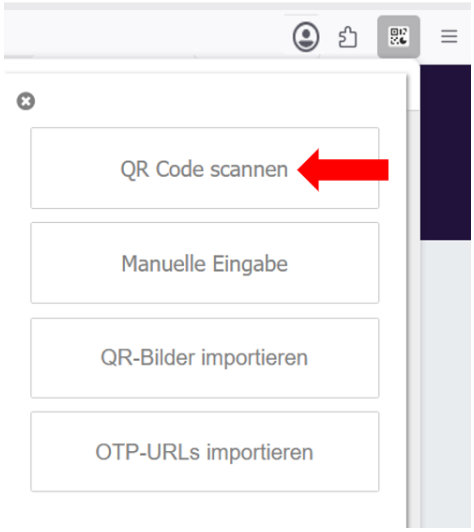

Abbildung 30 - QR Code scannen

12.) Zum Aufrufen Ihres Einmalpasswortes klicken Sie im Browser auf das QR-Code-Symbol. Es erscheint eine sechsstellige Zahl, welche sich nach 30 Sekunden ändert.

Abbildung 31 - Einmalpasswort

5 VPN-Einrichtung

5.1 Was ist ein VPN?

Die Abkürzung "VPN" steht für "Virtual Private Network", übersetzt "virtuelles privates Netzwerk". Die Hochschule sichert nomadische Zugriffe auf Hochschulnetze mittels dem offenen Standard „IPSec“ ab. Ein IPSec-VPN ist eine verschlüsselte, sichere Verbindung zwischen zwei Netzwerken oder zwischen einem Gerät und einem Netzwerk, die direkt auf der IP-Ebene arbeitet. Dabei sorgt IPSec („IP Security“) für zwei Dinge:

- Verschlüsselung – Datenpakete werden so geschützt, dass niemand sie unterwegs mitlesen kann.
- Authentifizierung & Integrität – beide Seiten prüfen einander und stellen sicher, dass die übertragenen Daten unverändert angekommen sind.

5.2 Windows Software für Studierende

Laden Sie sich den FortiClient VPN auf der Seite https://rz.h-ka.de/vpn entsprechend Ihrem Betriebssystem herunter:

forticlient_vpn_*_amd64.deb	*nix auf AMD-Prozessoren,
forticlient_vpn_*_x86_64.rpm	*nix auf Intel-Prozessoren,
FortiClientVPNSetup_*_macosx.dmg	Apple MacOS,
FortiClientVPNSetup_*_ARM64.exe	Windows auf AMD-Prozessoren,
FortiClientVPNSetup_*_x64.exe	Windows auf Intel-Prozessoren

5.3 Windows Software für Beschäftigte

Falls an Ihrem Rechner noch kein VPN-FortiClient installiert ist, dann gehen Sie wie folgt vor:

1.) Öffnen Sie auf Ihrem Arbeitsplatz-Rechner das Software-Center.

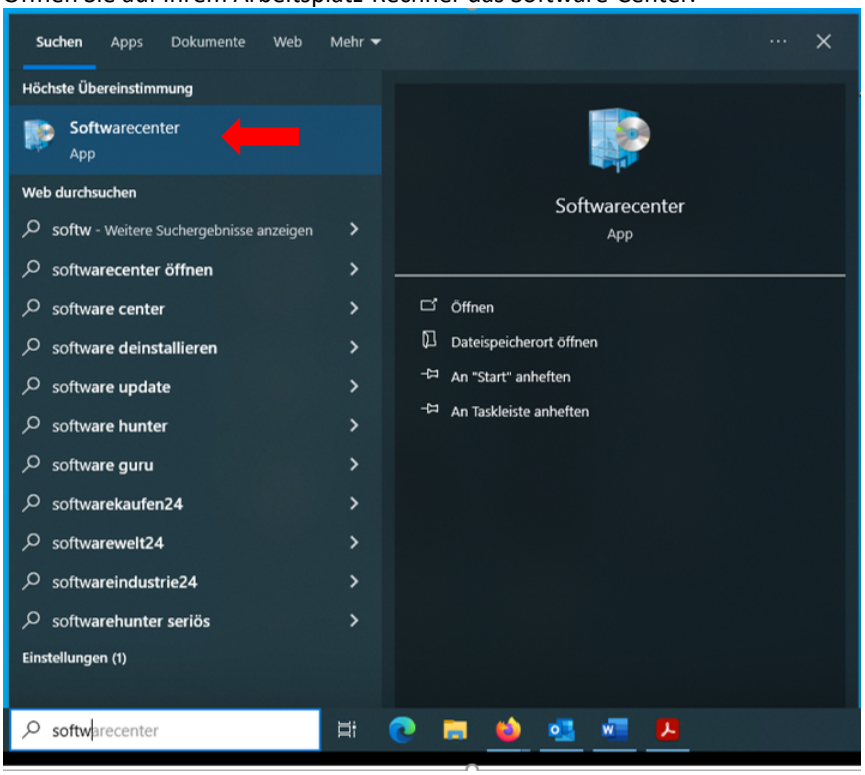

Abbildung 32 - Softwarecenter öffnen

2.) Wählen Sie im Software-Center den VPN-FortiClient aus und klicken Sie zum Installieren die Anwendung **VPN-FortiClient** doppelt an. (Sie müssen im HKA-Netz sein, damit die Anwendung angezeigt wird).

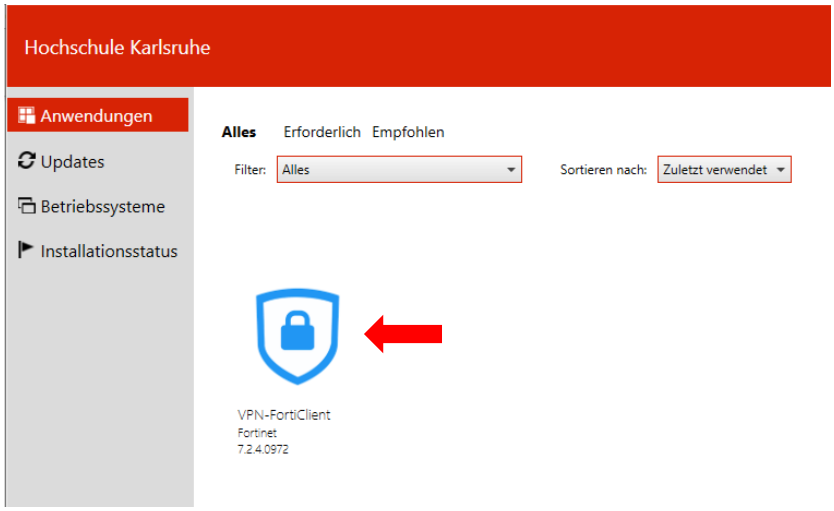

Abbildung 33 - VPN-FortiClient im Softwarecenter auswählen

3.) Der VPN-FortiClient ist installiert, sobald „Deinstallieren“ angezeigt wird.

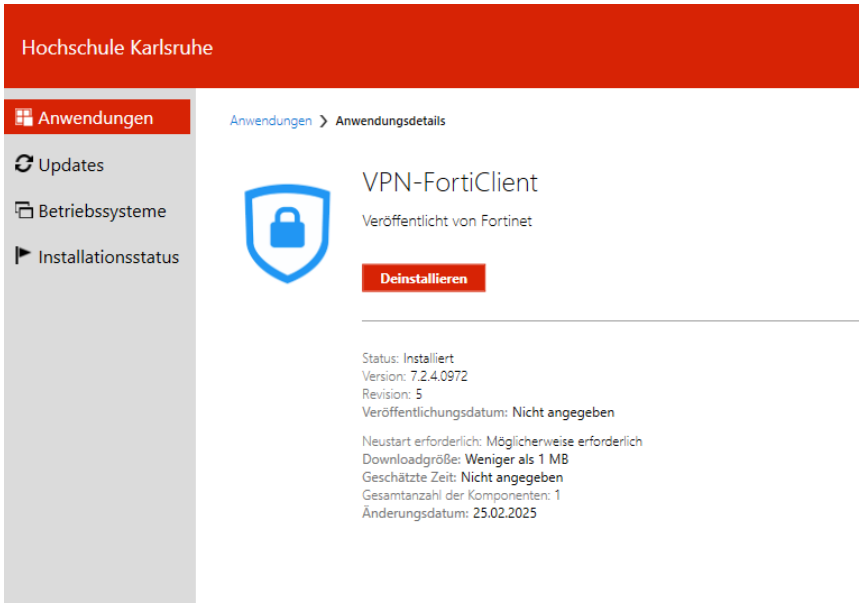

Abbildung 34- VPN-FortiClient im Softwarecenter nach der Installation

5.4 Starten und Einrichten des FortiClient VPN

1.) Zum Starten können Sie bei der Windows-Suchleiste **FortiClient VPN** eingeben.

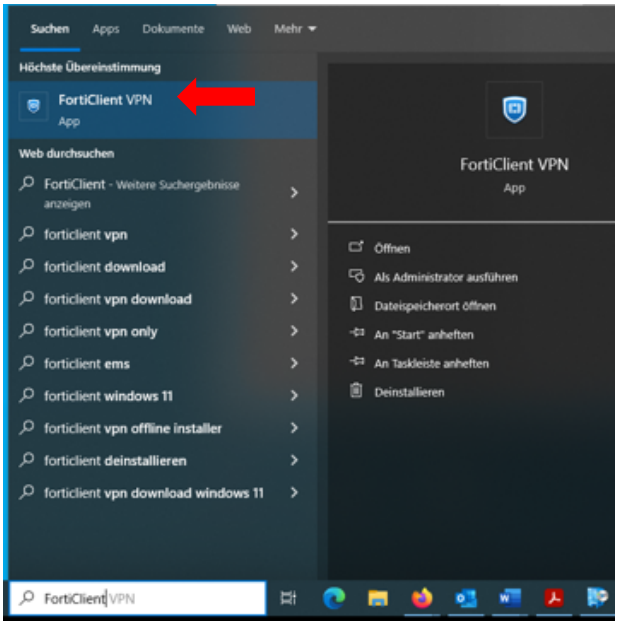

Abbildung 35 - FortiClient VPN über die Windows-Suche öffnen

Auch können Sie zum Starten des FortiClient VPN über die Startleiste aufrufen. Mit einem Rechtsklick auf das FortiClient-Symbol klicken und mit einem Klick auf „Öffne FortiClient Konsole“ öffnen.

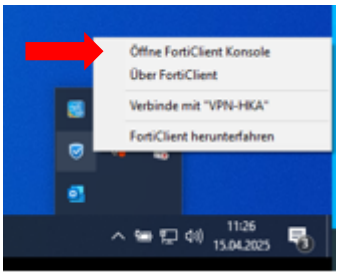

Abbildung 36 - FortiClient VPN über die Taskleiste suchen

2.) Einstellungen für die erste Verbindung:
Klicken Sie auf den Text „VPN konfigurieren“, um die Verbindung einzurichten.

3.) Öffnen Sie mit Klick auf das Plus (+) die Experteneinstellungen und die Einstellungen für Phase 1.
Geben Sie die folgenden Einstellungen ein:

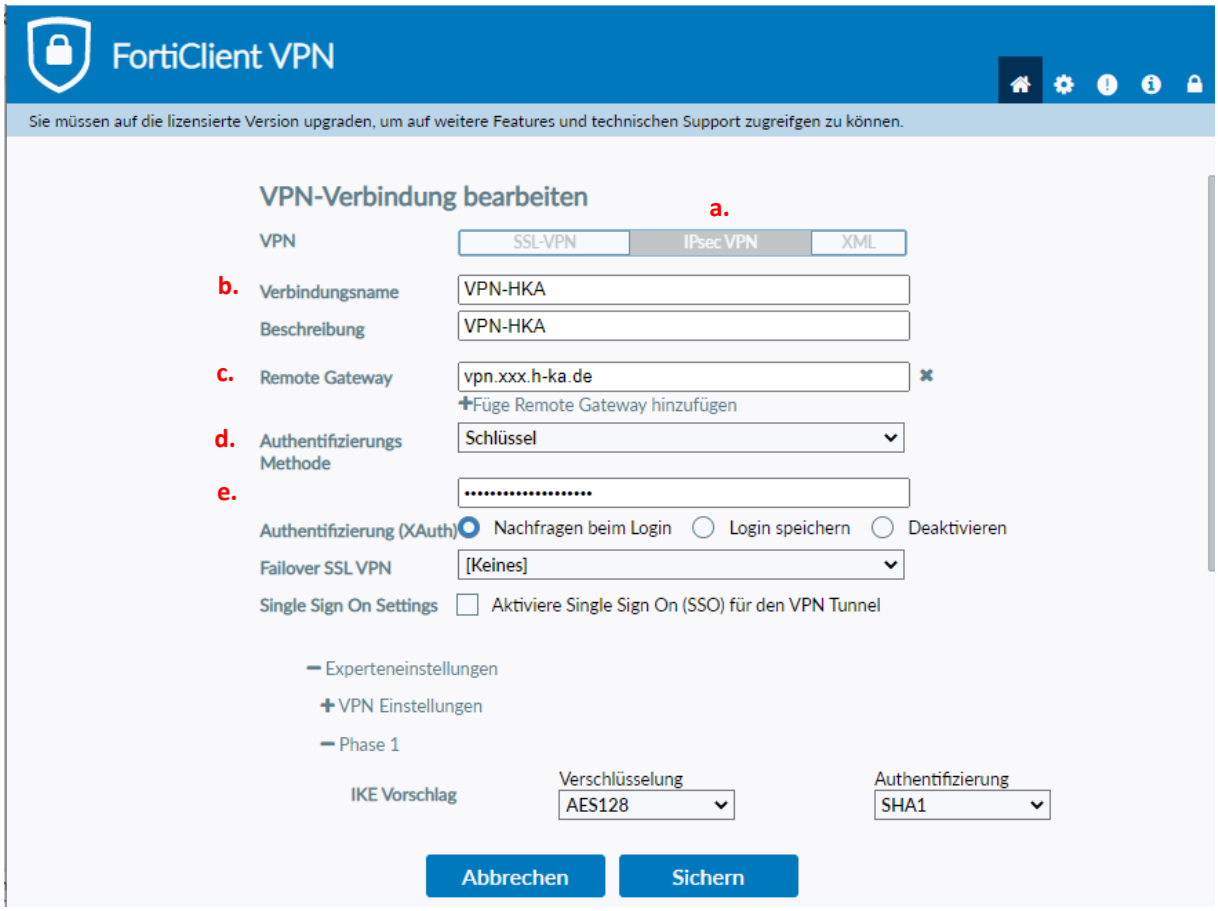

Abbildung 37 - Einstellungen der VPN-Verbindung bearbeiten

a. Stellen Sie bei VPN auf **IPsec VPN**
b. Geben Sie bei **Verbindungsname** einen beliebigen Namen für die Verbindung ein und optional auch bei **Beschreibung** eine Bezeichnung für die Verbindung ein.
c. Tragen Sie bei Remote Gateway je nach Abteilungszugehörigkeit die passende URL ein:
   - Fakultät AB: vpn.ab.h-ka.de
   - Fakultät EIT: vpn.eit.h-ka.de
   - Fakultät IMM: vpn.imm.h-ka.de
   - Fakultät IWI: vpn.iwi.h-ka.de
   - Fakultät MMT: vpn.mmt.h-ka.de
   - Fakultät W: vpn.w.h-ka.de
   - CAR: vpn.car.h-ka.de
   - Verwaltung: vpn.vw.h-ka.de
   - Rechenzentrum: vpn.rz.h-ka.de

d. Stellen Sie die **Authentifizierungsmethode** auf **Schlüssel.**
e. Tragen Sie im Feld darunter das „Shared Secret“ Ihrer Einrichtung ein:
   - Fakultät AB: IPsecFC_FakAB
   - Fakultät EIT: IPsecFC_FakEIT
   - Fakultät IMM: IPsecFC_FakIMM
   - Fakultät IWI: IPsecFC_FakIWI
   - Fakultät MMT: IPsecFC_FakMMT
   - Fakultät W: IPsecFC_FakW
   - CAR: IPsecFC_OUCAR
   - Verwaltung: IPsecFC_OUVW
   - Rechenzentrum: IPsecFC_OURZ

4.) Unter **Experteneinstellungen** in den Einstellungen für **Phase 1**:

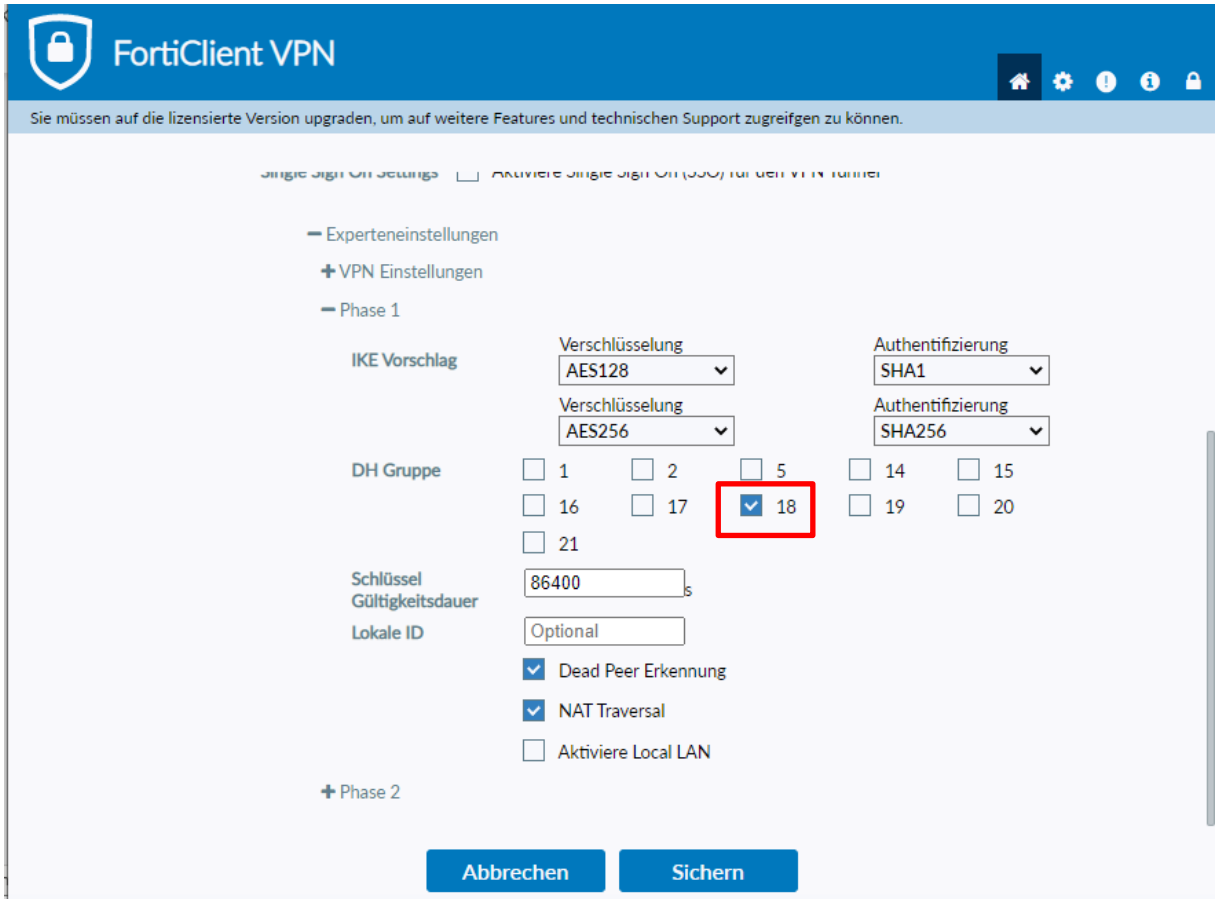

Abbildung 38 - Einstellungen der VPN-Verbindung in Phase 1 bearbeiten

a. Stellen Sie die **DH Gruppe** auf **18** (deaktivieren Sie ggf. andere Gruppen).
b. Die restlichen Einstellungen bleiben wir voreingestellt.
c. Beenden Sie die Einstellungen mit dem Klick auf „**Sichern**“.

5.) Unter **Experteneinstellungen** in den Einstellungen für **Phase 2**:

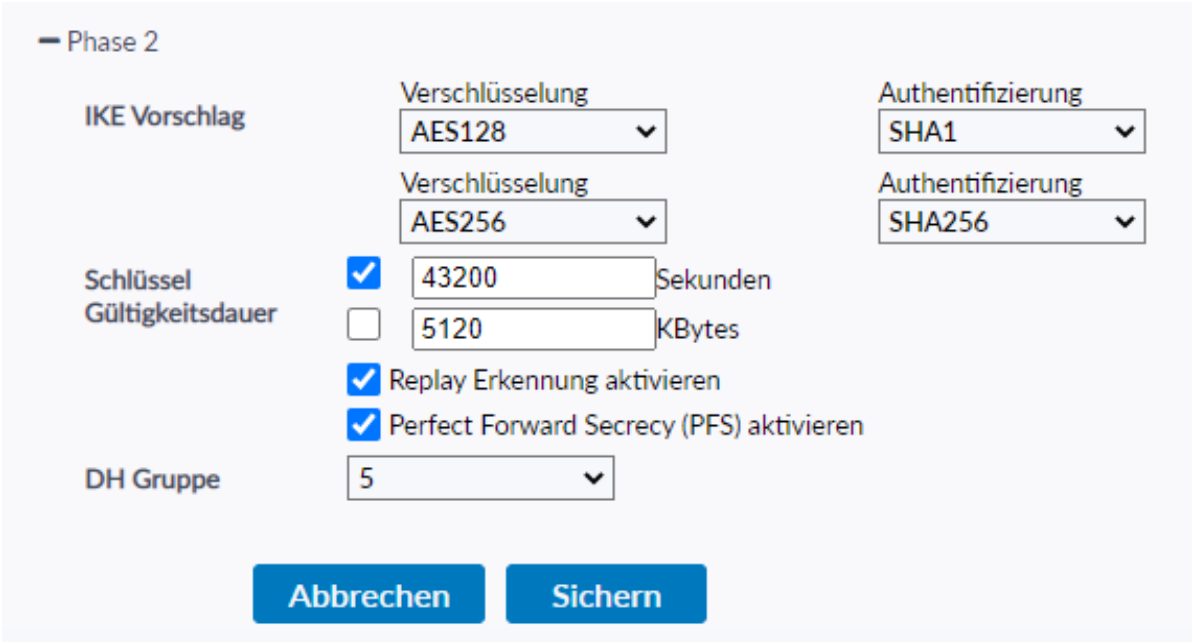

Abbildung 39 - Einstellungen der VPN-Verbindung in Phase 2 bearbeiten

Übernehmen Sie die in der Abbildung dargestellten Einstellungen.

6.) Wählen Sie auf der nun erscheinenden Anmeldemaske, die soeben eingerichtete VPN-Verbindung aus, indem man bei VPN-Name VPN-HKA auswählt.

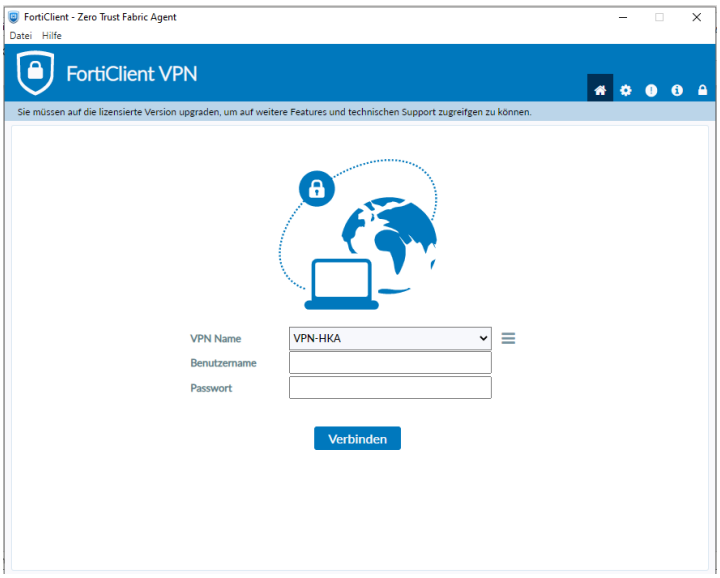

Abbildung 40 - VPN-Name VPN-HKA auswählen

a. Vor der Aktivierung der Verbindung ist der Proxy der HKA zu deaktivieren (siehe Punkt6).
b. Geben Sie bei **Benutzername** Ihr **RZ-Benutzerkürzel** ein.
c. Geben Sie bei **Passwort** das **Einmalpasswort** der Zwei-Faktor-Authentifizierung (z.B. über den Microsoft Authenticator unter Android) ein.

Nach dem „Verbinden“ dauert es einige Sekunden, bis der Verbindungsaufbau durchgeführt wurde.

7.) Prüfen der Proxyeinstellungen:

Öffnen Sie die Proxyeinstellungen, indem Sie in die Windows-Suche **Proxyeinstellungen** eingeben.

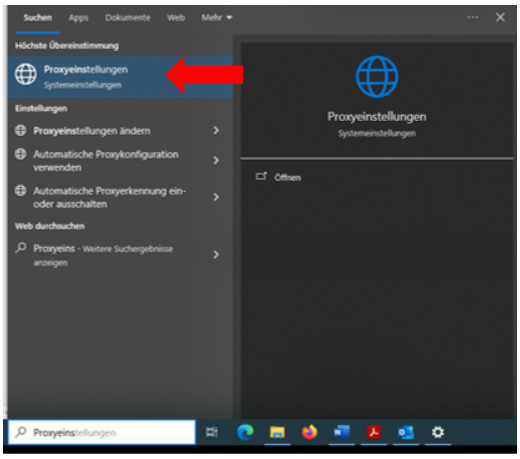

Abbildung 41 - Proxyeinstellungen über die Windows-Suche öffnen

Deaktivieren Sie ggf. die automatische Proxyeinstellung und die **manuelle Einrichtung** des Proxys und klicken Sie anschließend auf **Speichern**.

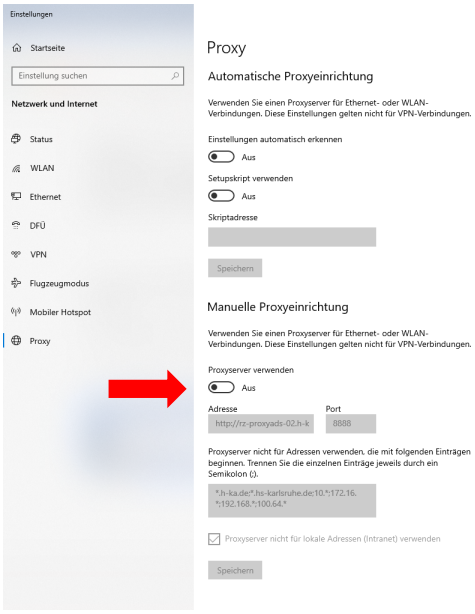

Abbildung 42 - Deaktivieren der Proxyeinstellung

5.5 Einwählen über FortiClient VPN

1.) Per Rechtsklick auf das Symbol FortiClient VPN in der Statusleiste, öffnet sich das Auswahlfenster. Wählen Sie **Verbinde mit „VPN-HKA“.**

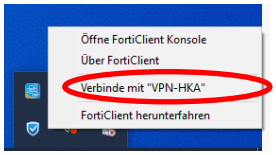

Abbildung 43 - Verbinden mit dem FortClient VPN über die Taskleiste

2.) FortiClient VPN Anmeldemaske:
   a. Wählen Sie den **VPN Name** VPN-HKA aus.
   b. Geben Sie bei **Benutzername** nur Ihr RZ-Benutzerkürzel (ohne@h-ka.de) ein.
   c. Bei **Passwort** geben Sie die 6-Ziffern aus der Authenticator-App ein, welche sich innerhalb von 30 Sekunden ändern. Warten Sie bis sich die Ziffern geändert haben und geben Sie dann die neugenerierten Ziffern ein.
   d. Klicken Sie anschließend auf **Verbinden**.

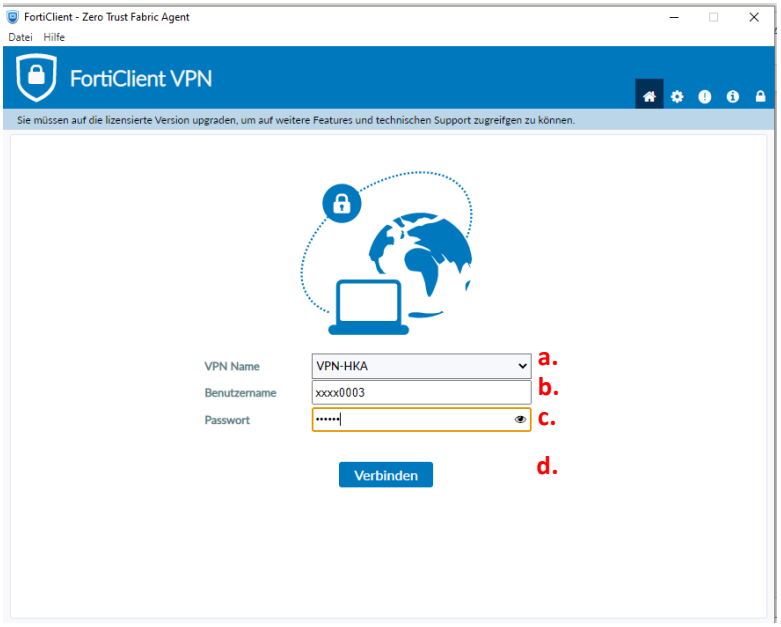

Abbildung 44 - Anmeldemaske des FortClient VPN

5.6 VPN-Verbindung trennen

1.) Zum Trennen der VPN-Verbindung rufen Sie bitte den aktiven VPN-Client mit einem Rechtsklick auf das Symbol FortiClient VPN in der Statusleiste auf.

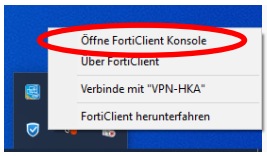

Abbildung 45 - Trennen der FortiClient VPN - Verbindung

2.) Klicken Sie auf den Button **Trennen.**

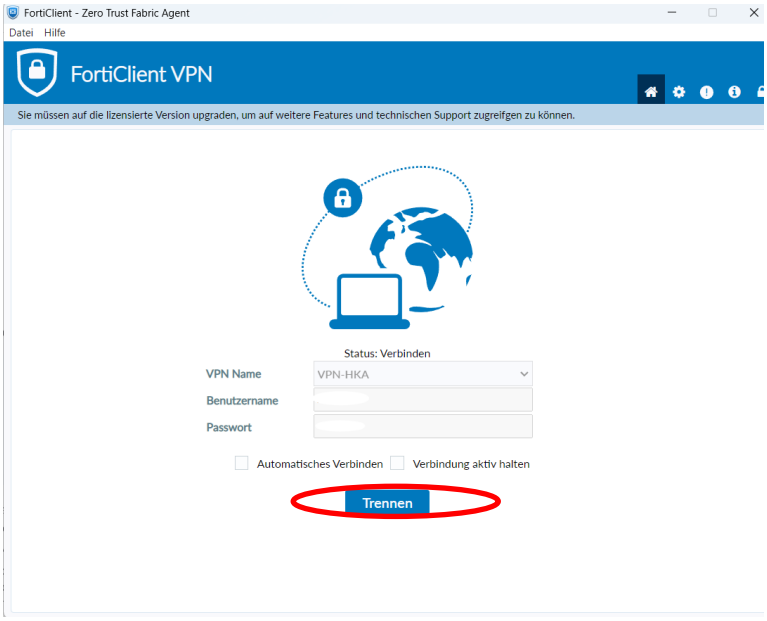

Abbildung 46 - Trennen der FortiClient VPN - Verbindung

6 Nutzerzertifikate erstellen

6.1 Hinweis zur Zertifikatsnutzung

Ein Zertifikat von GÉANT kann für eine fortgeschrittene elektronische Signatur verwendet werden, aber nicht für eine qualifizierte elektronische Signatur (QES). Die QES, die der handschriftlichen Unterschrift gleichgestellt ist, erfordert ein Zertifikat von einem qualifizierten Vertrauensdienste-Anbieter und eine spezielle Hardware wie eine Signaturkarte.

6.2 Einloggen bei GEANT/HARICA

- Öffnen Sie die Seite (https://cm.harica.gr/Login) in Ihrem Browser und wählen Sie **Academic Login** aus.

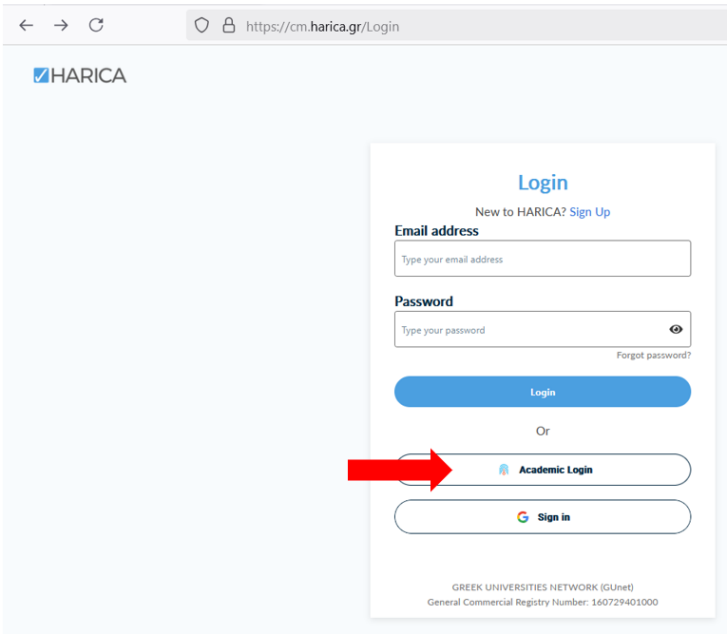

Abbildung 47 - Einloggen bei HARICA

- Wählen Sie die Institution aus und klicken Sie auf den Namen **Hochschule Karlsruhe.**

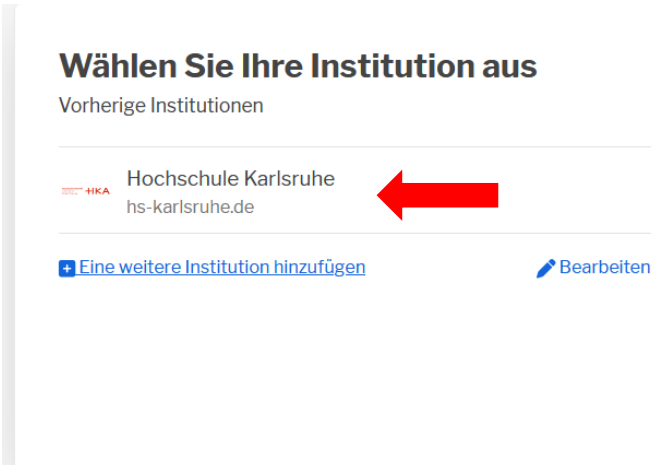

Abbildung 48 - Institution auswählen

- Geben Sie bei Benutzername nur Ihr RZ-Benutzerkürzel (ohne @h-ka.de) ein und bei Passwort Ihr RZ-Passwort und klicken Sie anschließend auf den Button **Anmelden**.

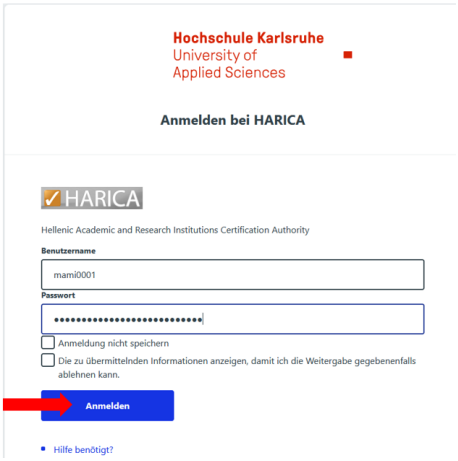

Abbildung 49 - RZ-Benutzerdaten eingeben

- Es folgt eine Übersichtliste, welche Daten an diesen Dienst übermittelt werden. Scollen Sie nach unten und klicken Sie auf den Button **Akzeptieren.**

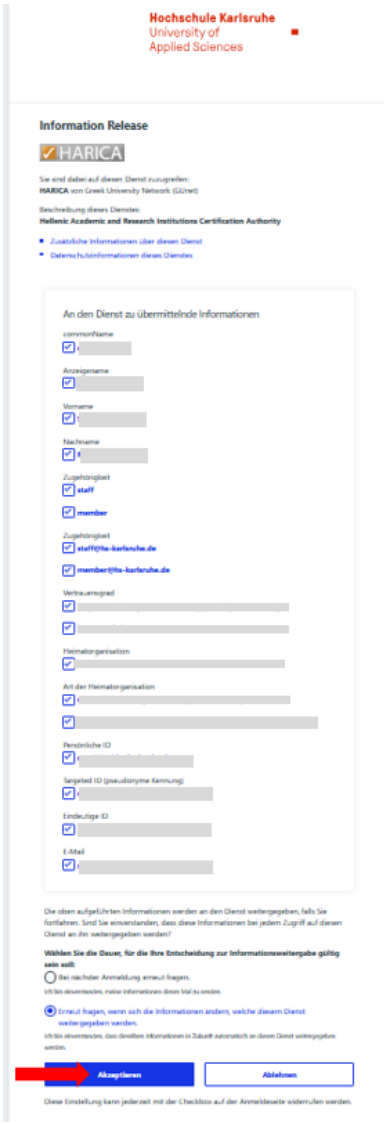

Abbildung 50 - Auswahl akzeptieren

Danach öffnet sich die Seite HARICA. Hier wählen Sie **Email** aus.

6.3 Nutzerzertifikat (Email-only) beantragen

Bitte beachten Sie, dass die nachfolgend beschriebene Vorgehensweise ist NICHT zum Unterschreiben von Dokumenten geeignet, da in den Zertifikaten keine Personenidentitäten hinterlegt sind!

Navigieren Sie zur Ansicht **Select the type of your certificate.**
Hier wählen Sie **Email-only** und klicken auf den Button **Select.**

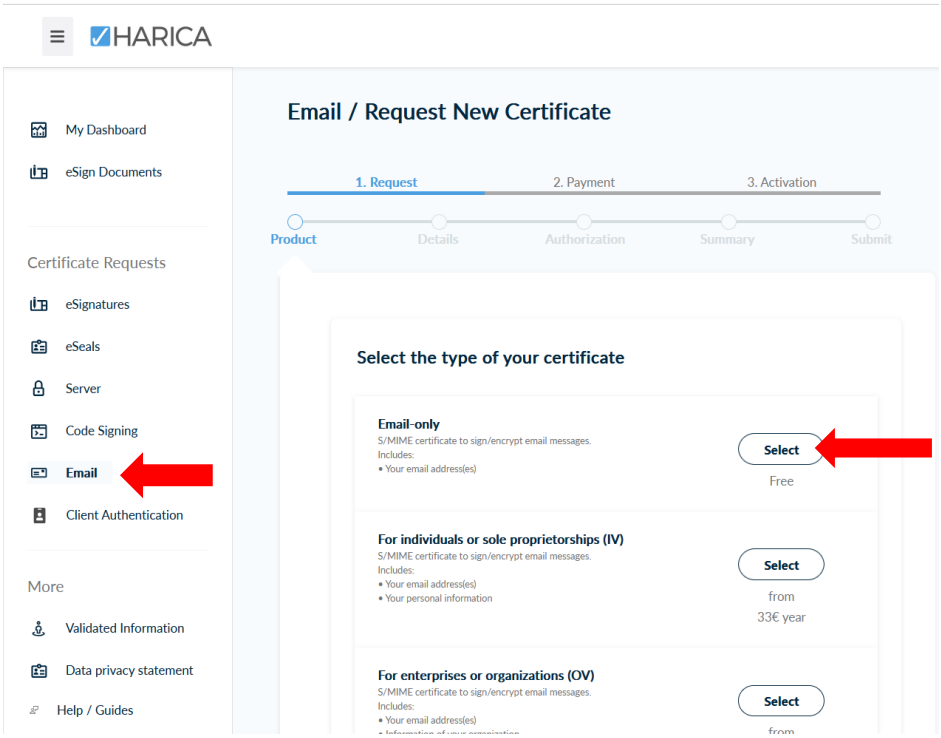

Abbildung 51 - Email-only auswählen

- Es ändert sich die Ansicht und Sie bekommen Ihre Mailadresse angezeigt. Klicken Sie nun auf den Button **Next**.

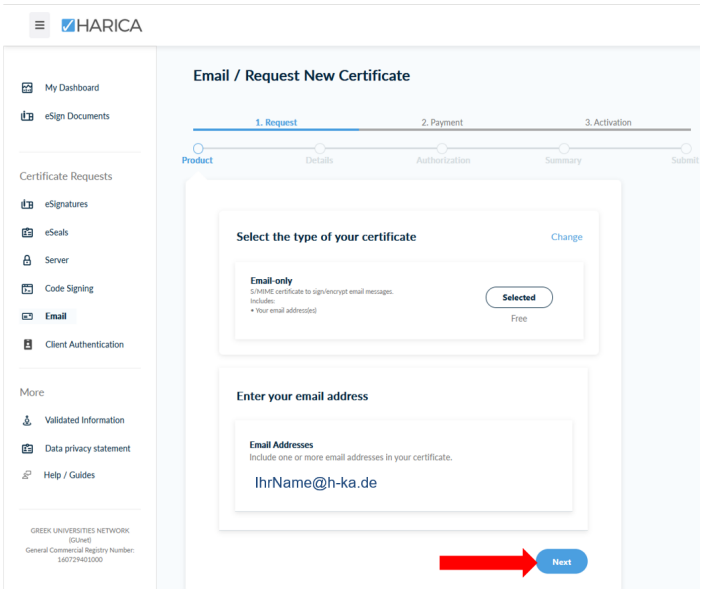

*Abbildung 52 - Button **Next** wählen*

Zu Überprüfung der Gültigkeit wird die Mailadresse verwendet.

- Klicken Sie auf den Button **Next**.

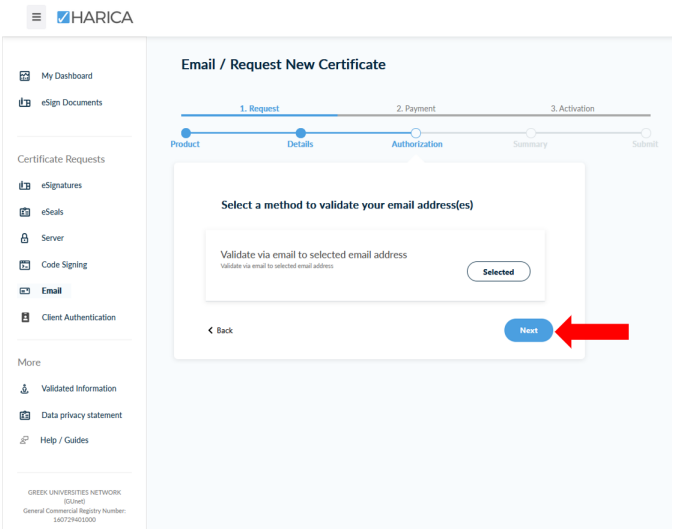

*Abbildung 53 - Erneut den Button **Next** wählen*

- Prüfen Sie nochmals in der Zusammenfassung Ihre Hinterlegungen. Klicken Sie in das Kontrollkästchen und anschließend wählen Sie den Button **Submit**.

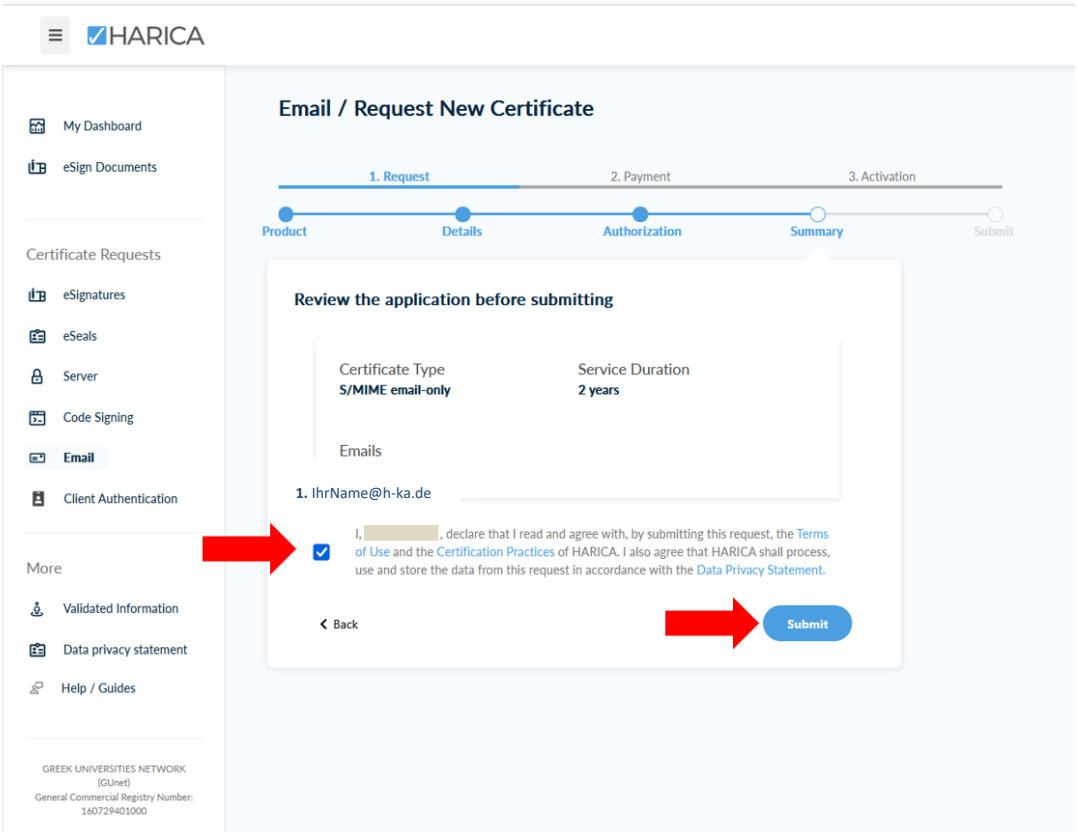

Abbildung 54 - Die Erstellung bestätigen

Weiter geht es in Abschnitt 6.5.

6.4 Nutzerzertifikat mit Identitäts- und Org.-verifikation beantragen

Die nachfolgend beschriebene Vorgehensweise ist zum Unterschreiben von Dokumenten geeignet, da in den Zertifikaten sowohl die Hochschulidentität als auch die von der Hochschule verifizierte Personenidentität hinterlegt sind.

Navigieren Sie zur Ansicht **Select the type of your certificate.**
Hier wählen Sie **For Enterprises or Organisations (IV+OV)** und klicken auf den Button **Select.**

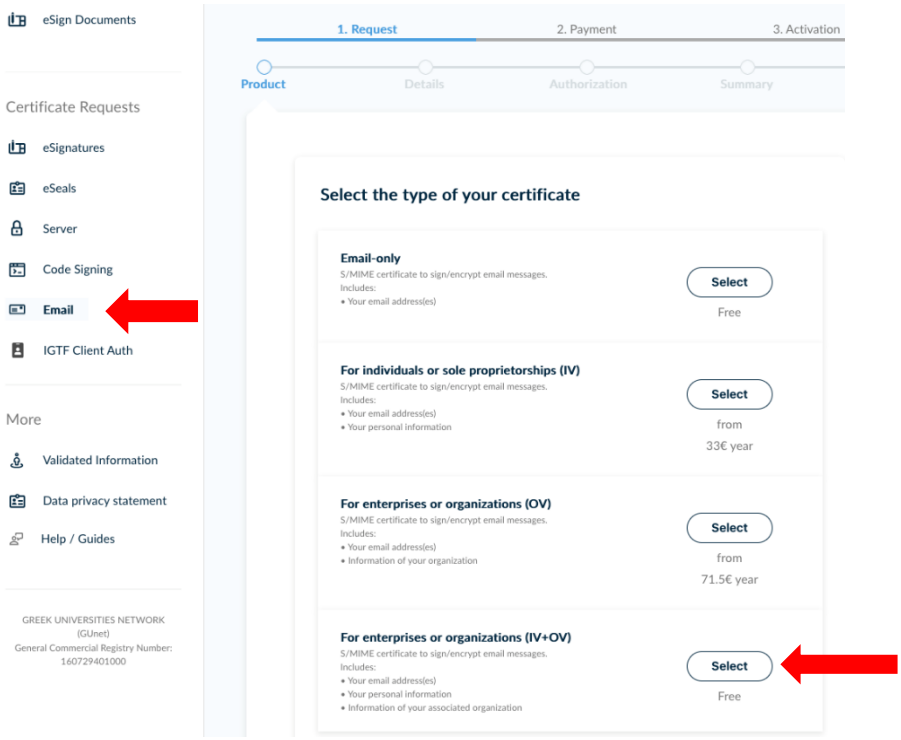

Abbildung 55 – IV+OV auswählen

- Es ändert sich die Ansicht und Sie bekommen Ihre Mailadresse angezeigt. Klicken Sie nun auf den Button **Next**.

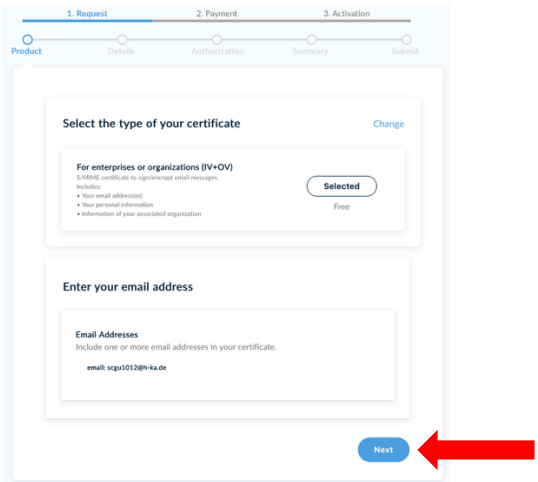

*Abbildung 56 – E-Mail bestätigen, Button **Next** wählen*

- Es ändert sich die Ansicht und Sie bekommen Ihre Identitätsinformationen angezeigt. Klicken Sie nun auf den Button **Next**.

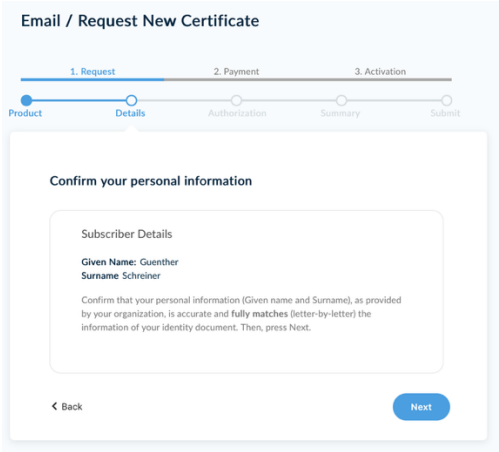

*Abbildung 57 – Identität bestätigen, Button **Next** wählen*

- Es ändert sich die Ansicht und Sie bekommen Ihre Organisationsinformationen angezeigt. Klicken Sie nun auf den Button **Next**.

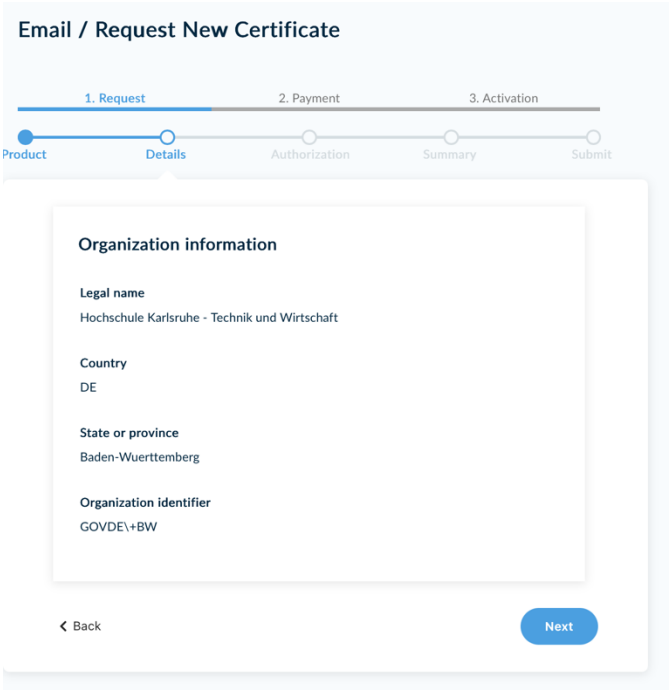

*Abbildung 58 – Organisation bestätigen, Button **Next** wählen*

- Nach zwei weiteren Bestätigungen erhalten Sie eine Nachricht in das Hochschul-Mail-Postfach.

6.5 Nutzerverifikation und Abschluss der Zertifikatsausstellung

Eine Mail von HARICA mit dem Betreff: **HARICA Certificate Manager (CM)** wird an Ihr Hochschul-Mail-Postfach gesandt.

- Bitte öffnen Sie die Mail und bestätigen Sie Ihre Email-Adresse, indem Sie auf den Button **Confirm** klicken.

Abbildung 59 - Die Erstellung bestätigen

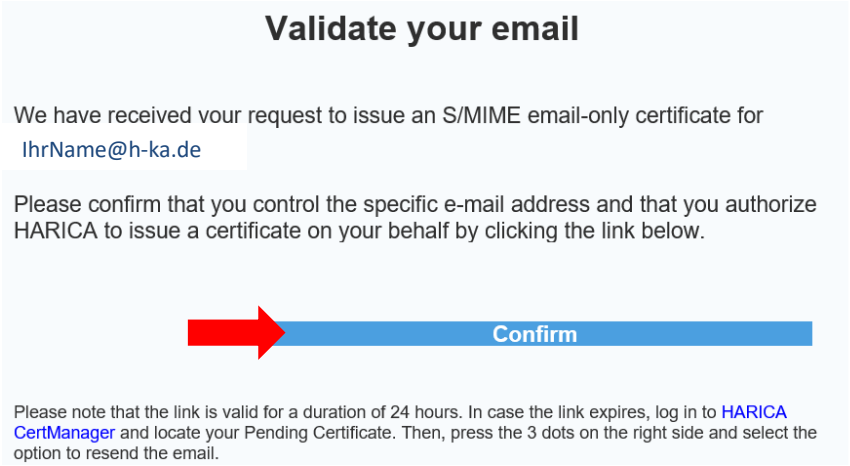

Abbildung 60 - Mail-Autorisierung bestätigen

Wechsel Sie wieder in Ihren Browser auf die Seite von **HARICA** und Sie haben nun eine Bestätigung erhalten und können mit den weiteren Einstellungen fortfahren.

- Klicken Sie auf **Confirm**.

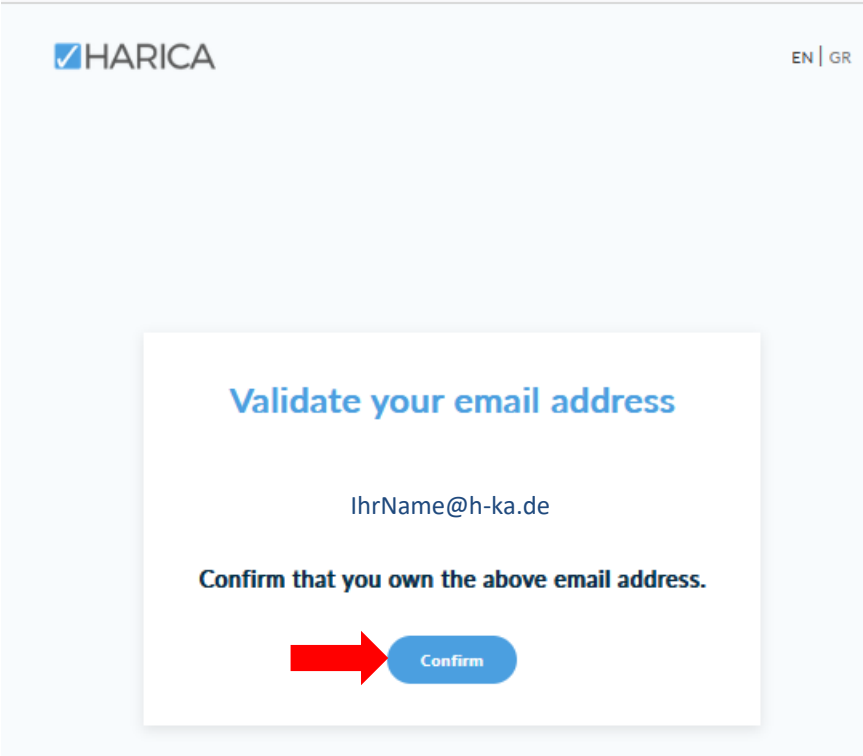

Abbildung 61 - Mail-Adresse bestätigen

- Wechseln Sie auf der Seite von **HARICA** in Seiten-Navigation auf **My Dashboards** und klicken Sie auf **Enroll your Certificate.**

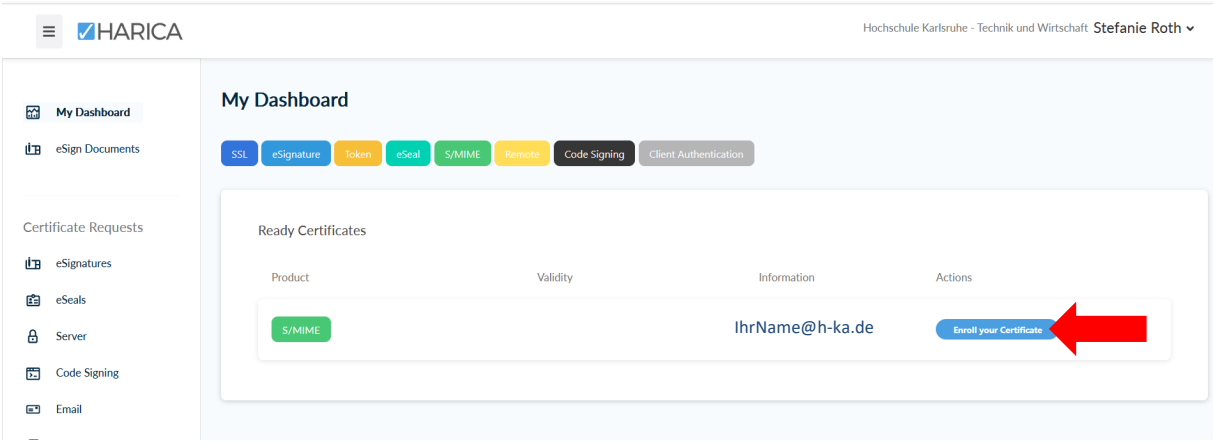

Abbildung 62 - Bestätigen der Mailadresse

Bitte wählen Sie die Auswahlmöglichkeiten wie folgt:

a. Klicken Sie auf **Generate Certificate**.
b. Wählen Sie bei **Algorithm RSA (default)** und als **Key size 4096**.
c. Setzen Sie sich ein Passwort und notieren Sie sich das Passwort. (Bitte nicht Ihr RZ-Passwort verwenden).
d. Wiederholen Sie das Passwort.
e. Klicken Sie zum Bestätigen in das Kontrollkästen.
f. Drücken Sie auf den Button **Enroll Certificate**.

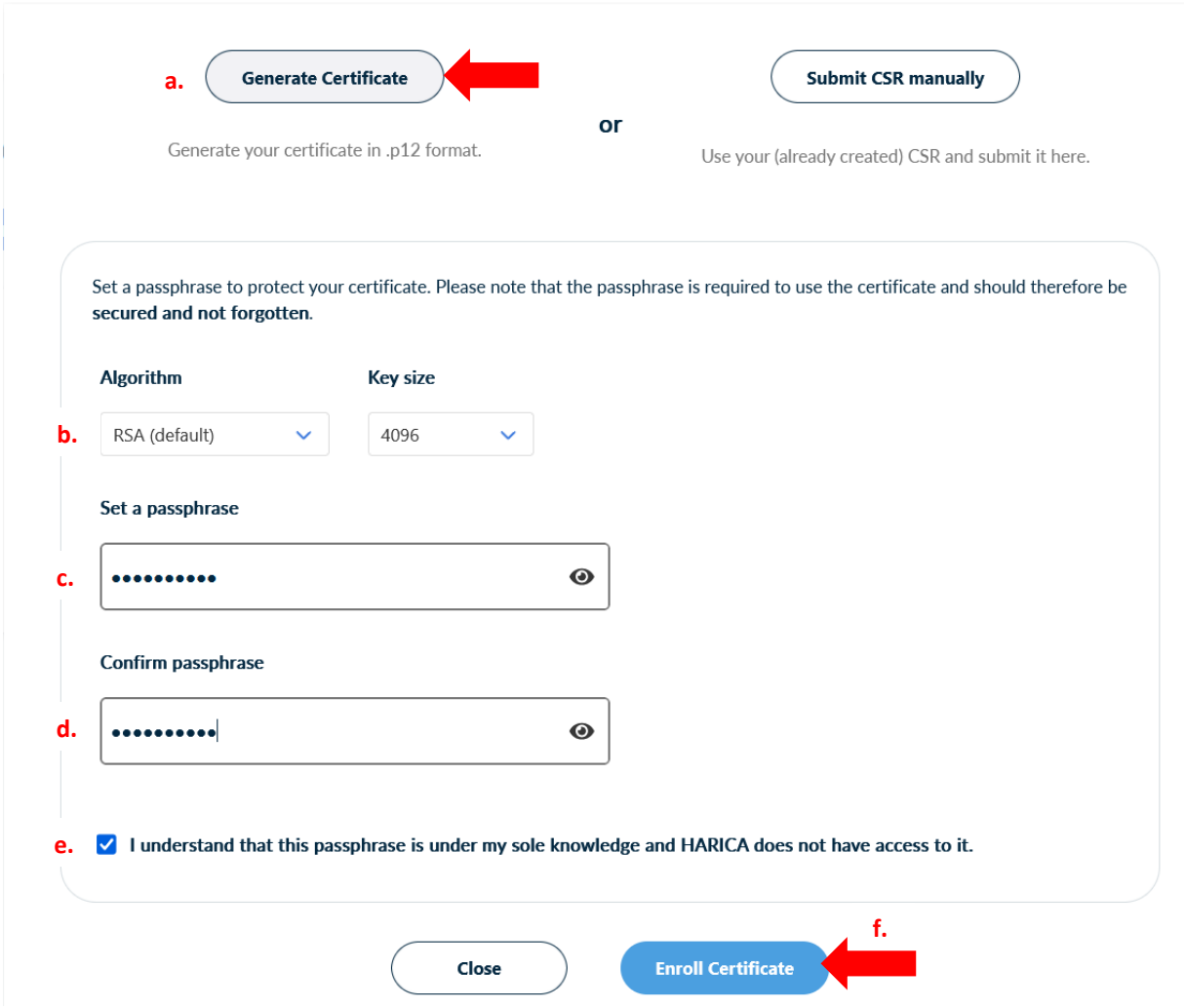

Abbildung 63 - Einstellungen und Passwort setzen

- Als Nächstes erhalten Sie eine Mitteilung, dass Ihr Zertifikat einsatzbereit ist und zum Download bereitsteht.
- Klicken Sie auf den Button **Download**.

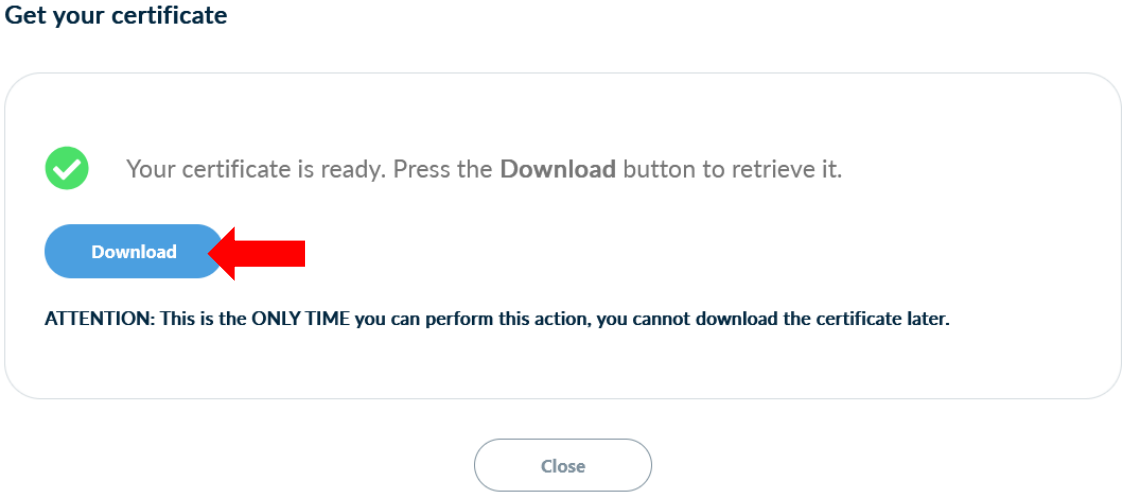

Abbildung 64 - Herunterladen des Zertifikats starten

- Es starten der Download und auf Ihrem Rechner finden Sie in Ihrem Download-Ordner die Datei **Certificate.p12**.

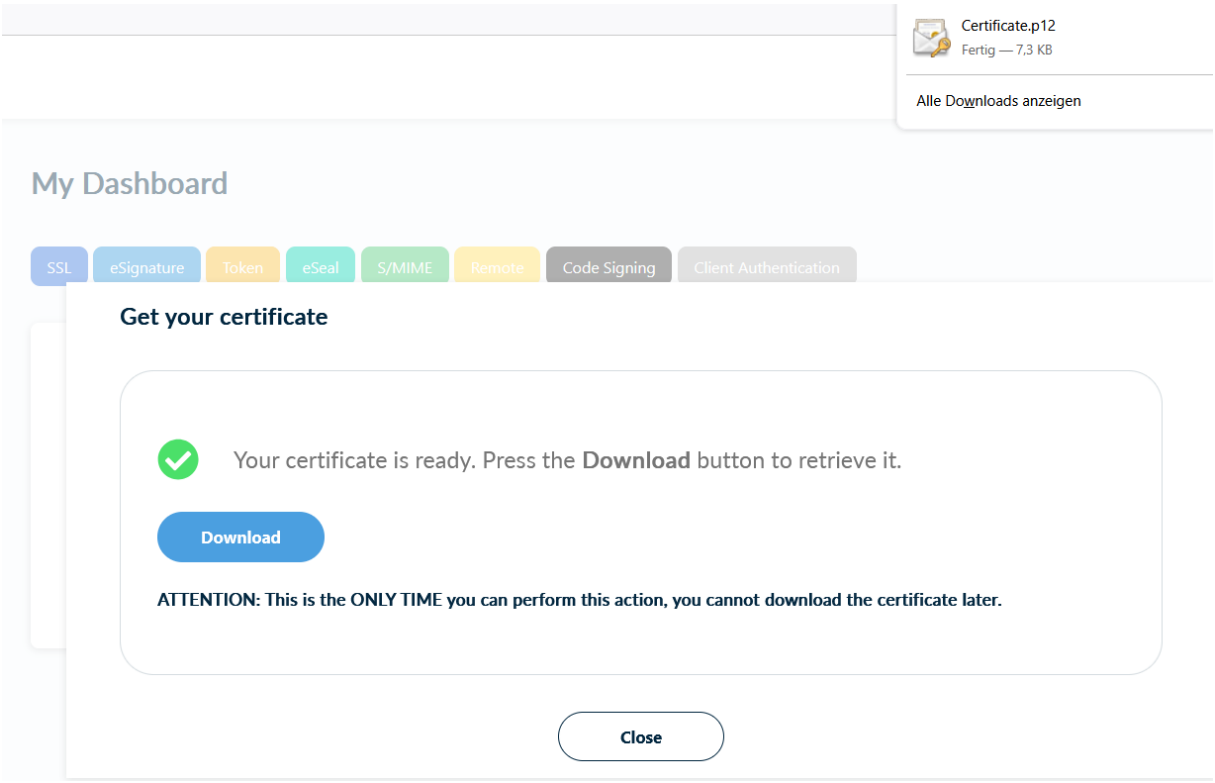

Abbildung 65 - Zertifikat herunterladen

- Wechseln Sie in Ihren **Downloads**-Ordner, indem Sie in die Windows-Suche **Downloads** eingeben.

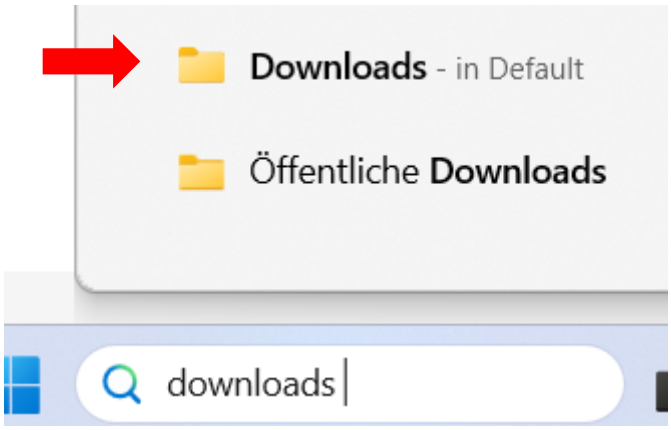

Abbildung 66 - Download-Ordner öffnen

- Legen Sie die Datei Certificate.p12 auf Ihrem Rechner bspw. im Ordner **Dokumente** ab.

6.6 Einbinden des Zertifikats auf Ihrem Rechner und bei Ihrem Emailpostfach

Um das Zertifikat auf Ihrem Rechner einzubinden, klicken Sie die Datei Certificate.p12 doppelt an, welche Sie sich bspw. im Ordner **Dokumente** abgelegt haben. Es öffnet der Zertifikatimport-Assistent.

- Wählen Sie **Aktuelle Benutzer** aus und gehen Sie auf **Weiter.**

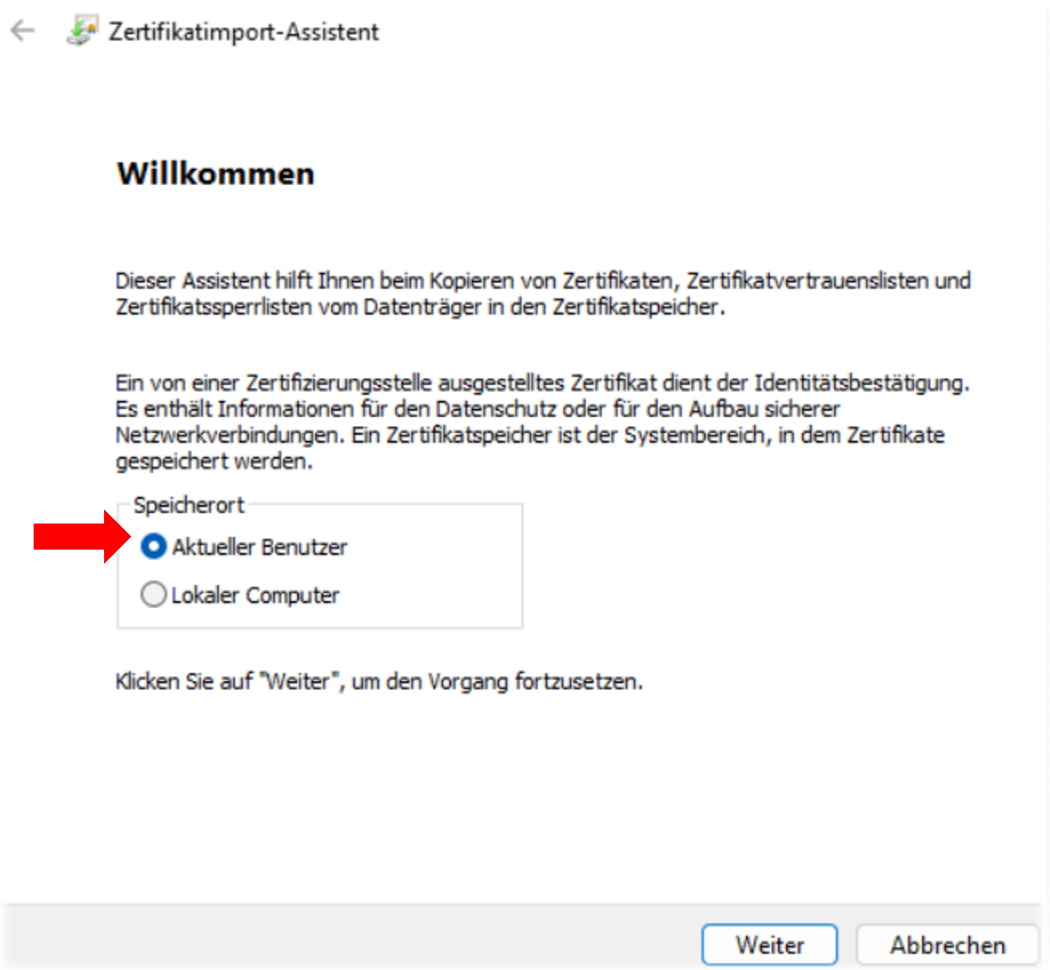

Abbildung 67 - Zertifikat auf den Rechner importieren

- Geben Sie Ihr Zertifikat-Passwort ein, dass Sie sich zuvor notiert haben und setzen Sie einen Haken bei **Alle erweiterten Eigenschaften miteinbeziehen**.
  Klicken Sie auf **Weiter**.

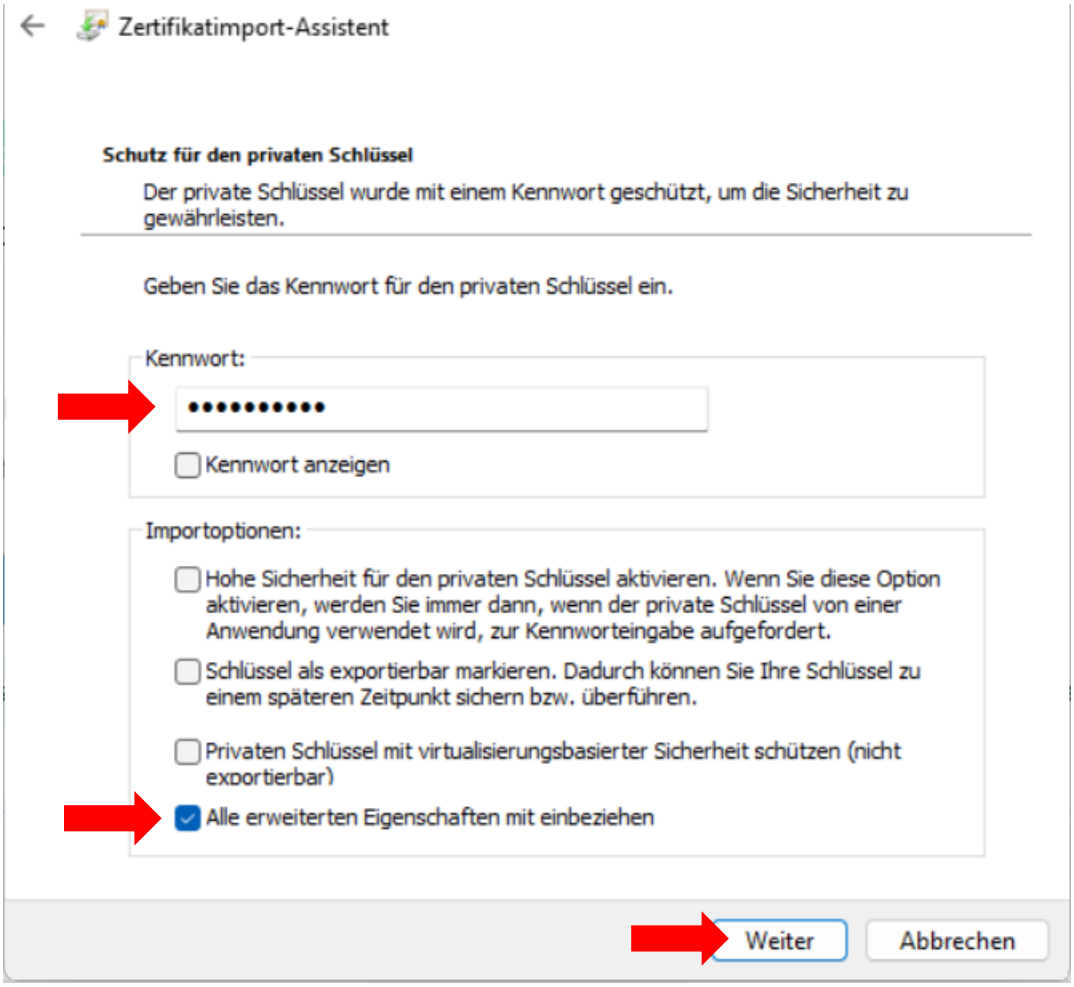

Abbildung 68 - Kennwort bei Zertifikatsimport eingeben

- Suchen Sie die Datei **Certificate.p12** auf Ihrem Rechner, indem Sie auf **Durchsuchen**… gehen und bspw. in den Dokumenten-Ordner (**Documents**) wechseln.

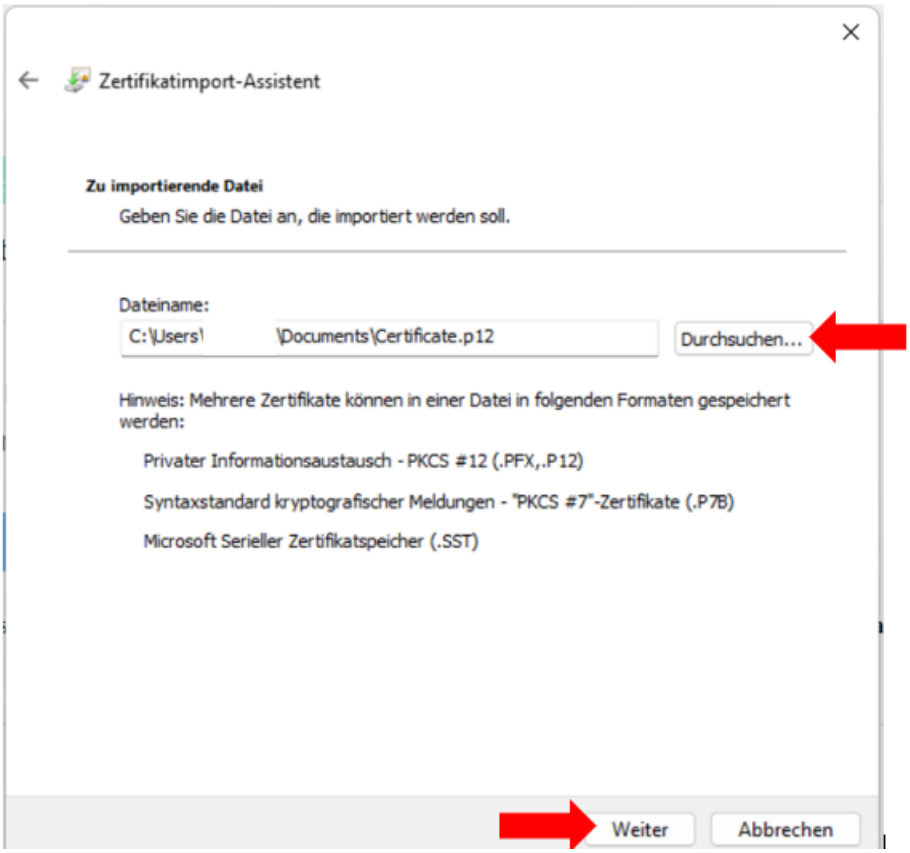

Abbildung 69 - Zertifikatsimport

- Im nächsten Schritt wählen Sie **Zertifikatsspeicher automatisch auswählen (auf dem Zertifikattyp basierend)** und klicken Sie auf den Button **Weiter.**

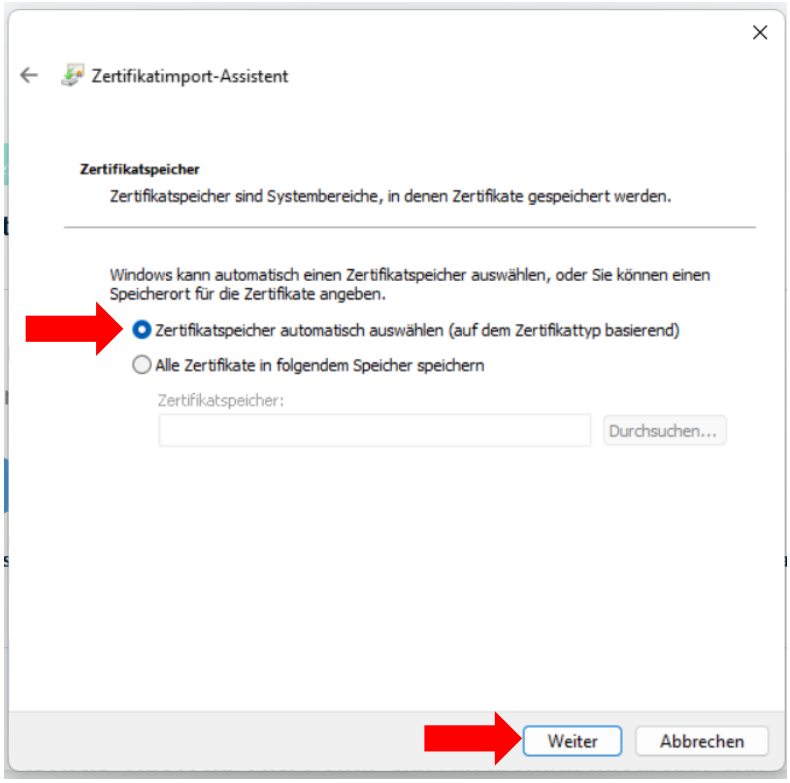

Abbildung 70 - Einstellung für den Zertifikatsimport

- Zum Fertigstellen des Assistenten klicken Sie nun auf den Button **Fertig stellen**.

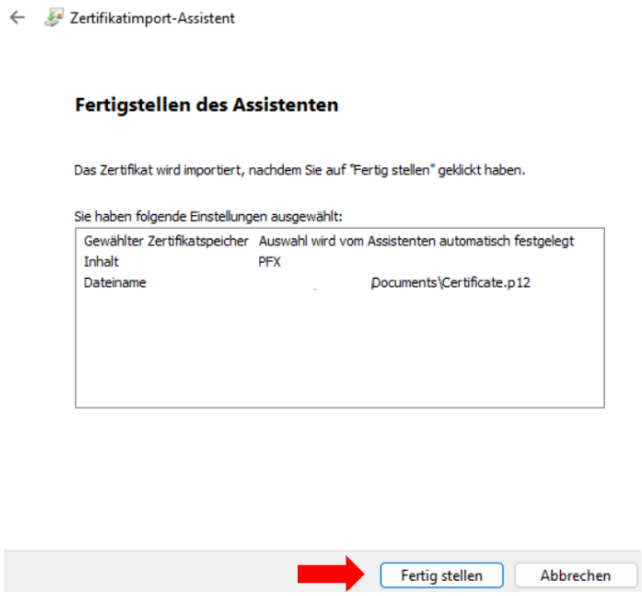

*Abbildung 71 - Button **Fertig stellen** wählen*

- Es kommt nun eine Sicherheitswahrung: Hier klicken Sie zum Bestätigen auf **Ja**, um zu bestätigen, dass Sie das Zertifikat installieren möchten.

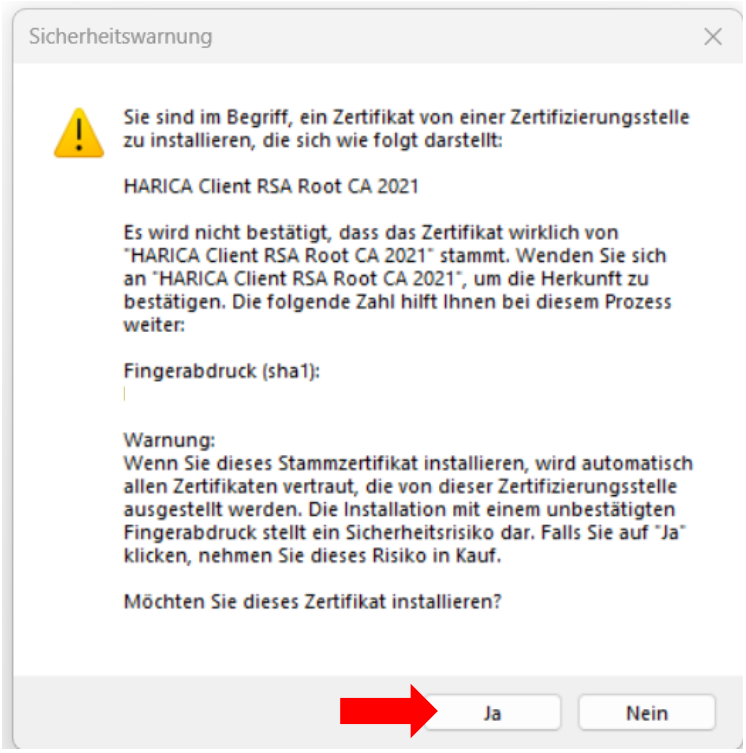

Abbildung 72 - Installation des Zertifikats bestätigen

- Anschließend erhalten Sie die Meldung **Der Importvorgang war erfolgreich** und Sie klicken auf **OK**.

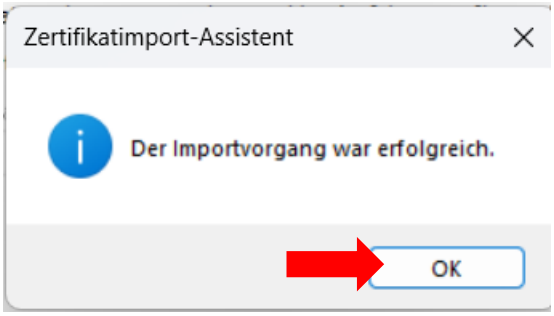

Abbildung 73 - Bestätigen des Imports

- Auf der Seite von HARICA erscheint ein Validiy-Datum.

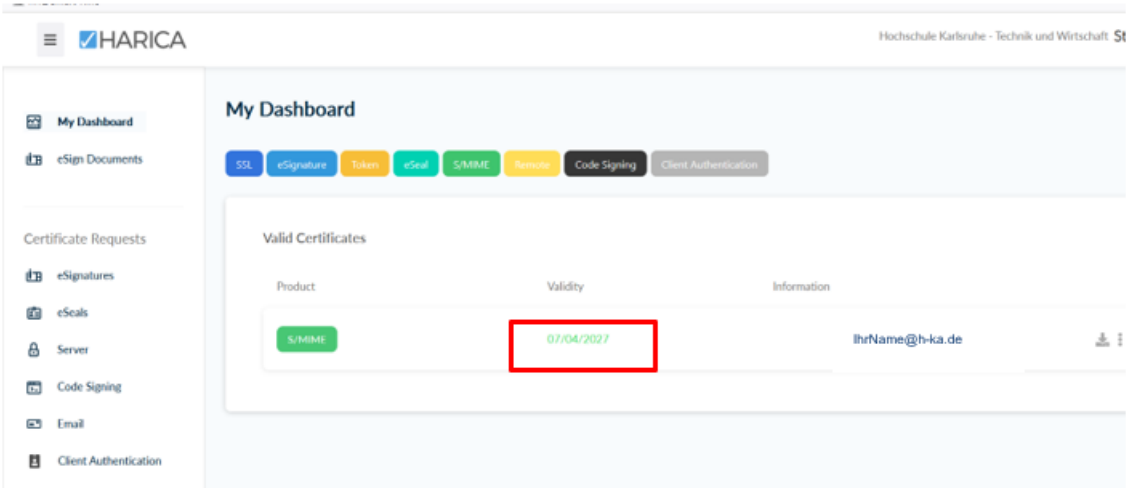

Abbildung 74 - Gültigkeitsdatum des Zertifikats

Zum Einbinden des Zertifikats bei MS-Outlook einzubinden, öffnen Sie zunächst Outlook.

- Klicken auf das Register **Datei**.

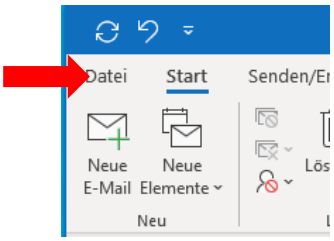

Abbildung 75 - Register Datei bei MS-Outlook

- Wählen Sie **Optionen** aus.

*Abbildung 76 - **Optionen** in Outlook wählen*

- Wählen Sie den Punkt **Trust Center** und dann den Button **Einstellungen für das Trust Center…**

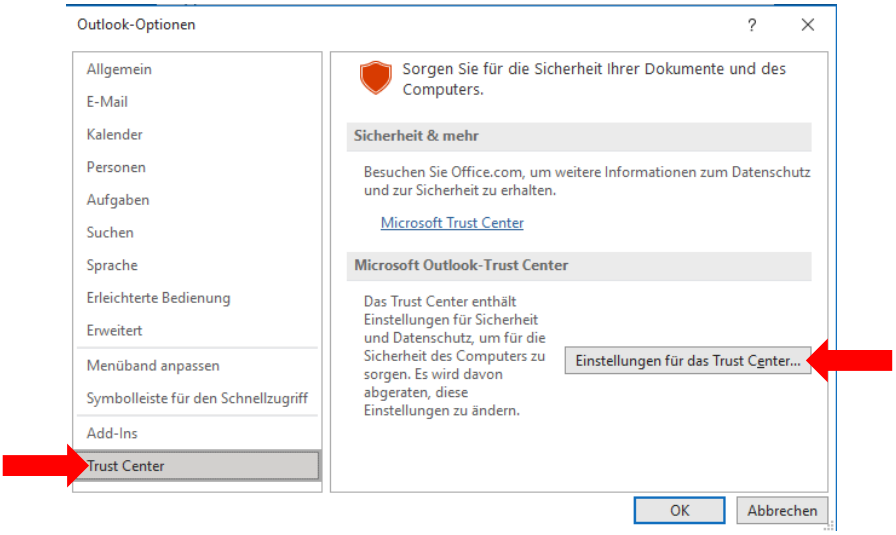

Abbildung 77 - Zertifikat in Outlook Trust Center hinterlegen

- Wählen Sie **E-Mail-Sicherheit** aus, setzen einen Haken bei **Ausgehenden Nachrichten digitale Signatur hinzufügen** und klicken Sie auf den Button **Importieren/Exportieren…**

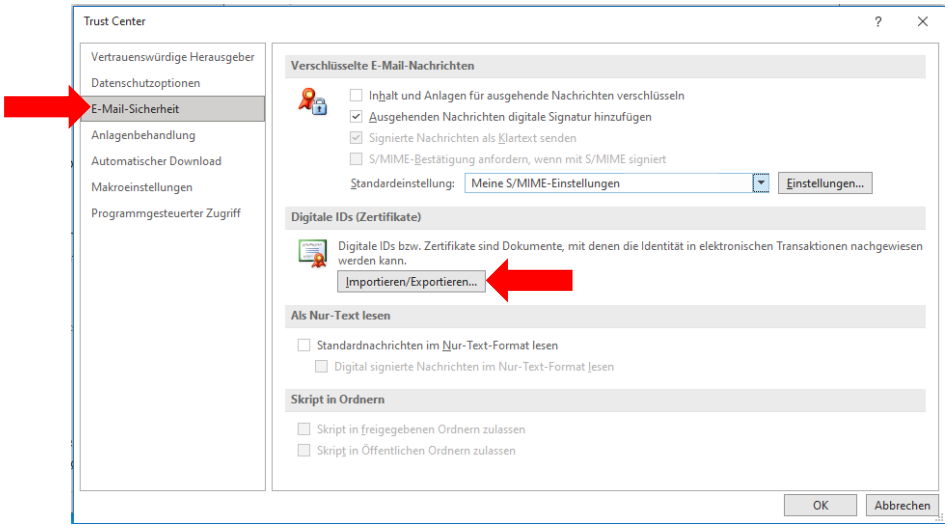

Abbildung 78 - Importieren des Zertifikats

- Es öffnet sich das Fenster **Digitale ID importieren/exportieren.**
  Klicken Sie auf **Durchsuchen…**

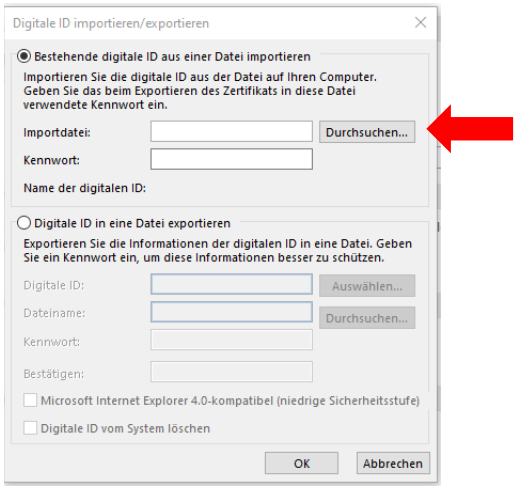

Abbildung 79 - p12-Datei importieren

- Wählen Sie die Zertifikatsdatei **Certificate.p12** aus, bspw. unter **Dokumente**, falls Sie dort die Datei **Certificate.p12** abgelegt haben**.**
  Klicken Sie die Datei **Certificate.p12** doppelt an und gehen Sie auf **Öffnen.**
  Nun ist das Zertifikat bei Ihrem Email-Konto eingebunden.
  Führen Sie einen Neustart Ihres Rechners durch.
  Anmerkung: Bei nicht Windows-Betriebssystemen ist das Zertifikat im Browser zu hinterlegen.

- Weiteres Vorgehen bei einem Gruppenpostfach-Zertifikat

  1. Überprüfen Sie in den **Outlook-Optionen** unter den Menu-Punkt **Trust-Center** die Einstellungen, indem Sie den Button **Einstellungen für das Trust Center..** anklicken.

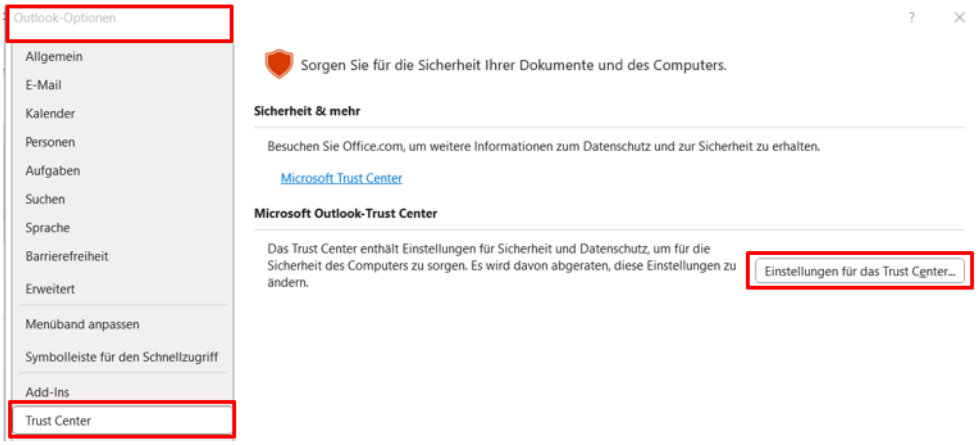

Abbildung 80 - Weitere Einstellungen bei Gruppenpostfach-Zertifikat

2. Im Trust Center wählen Sie den Menu-Punkt **E-Mail-Sicherheit** und klicken auf den Button **Einstellungen..**

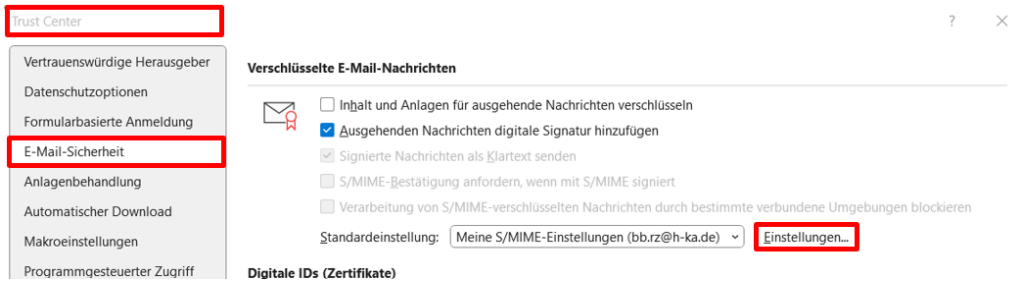

Abbildung 81 - Einstellungen bei Gruppenpostfach-Zertifikat prüfen

3. Falls Ihr Gruppenpostfachzertifikat nicht angezeigt wird, wählen Sie den Button **Neu**.

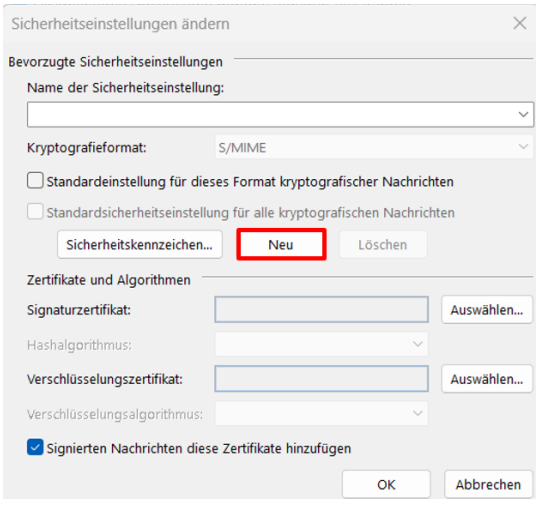

Abbildung 82 - Einstellungen beim Gruppenpostfach-Zertifikat vornehmen

4. Anschließend wählen Sie im Drop-Down-Menu unter **Name der Sicherheitseinstellung** das Gruppenpostfach aus.

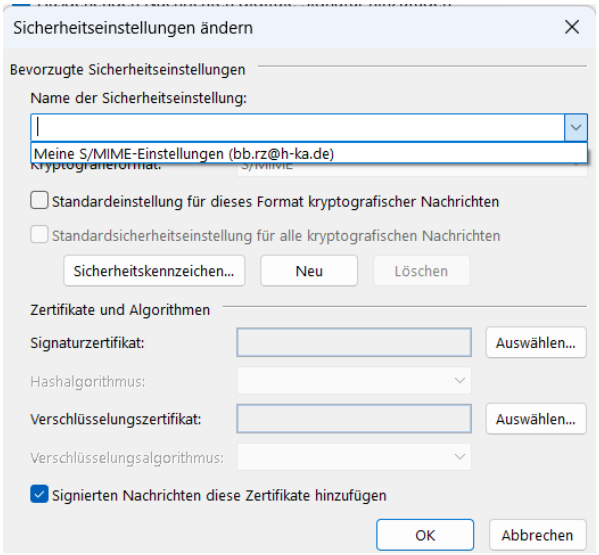

Abbildung 83 - Gruppenpostfach auswählen

5. Prüfen Sie die Einstellungen und klicken Sie anschließend auf **OK**.
Danach führen Sie einen Neustart Ihres Rechners durch.

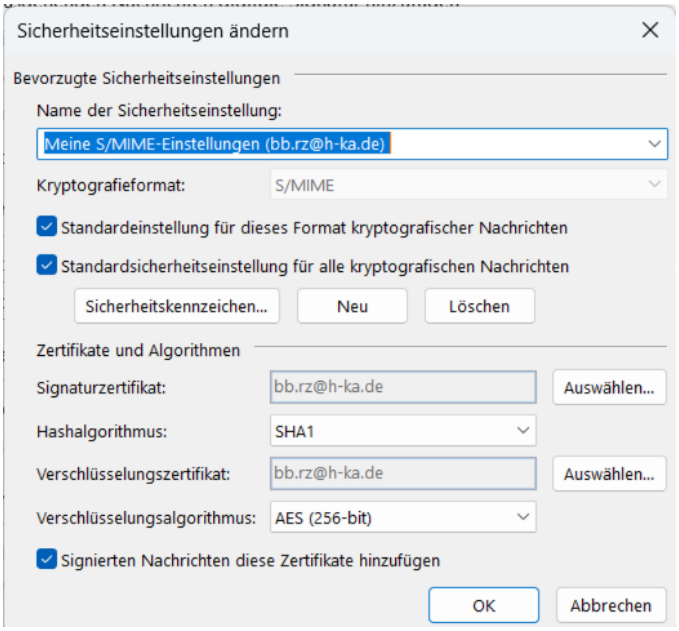

Abbildung 84 - Sicherheitseinstellungen überprüfen

6.7 Gruppenpostfach-Zertifikat erstellen

Falls Sie ein Gruppenpostfach verwenden, legen Sie sich bitte ein Gruppenpostfach-Zertifikat an.

1.) Zum Erstellen eines Gruppenpostfach-Zertifikats öffnen Sie die Seite von HARICA **https://cm.harica.gr** und wählen Sie **Sign Up**.

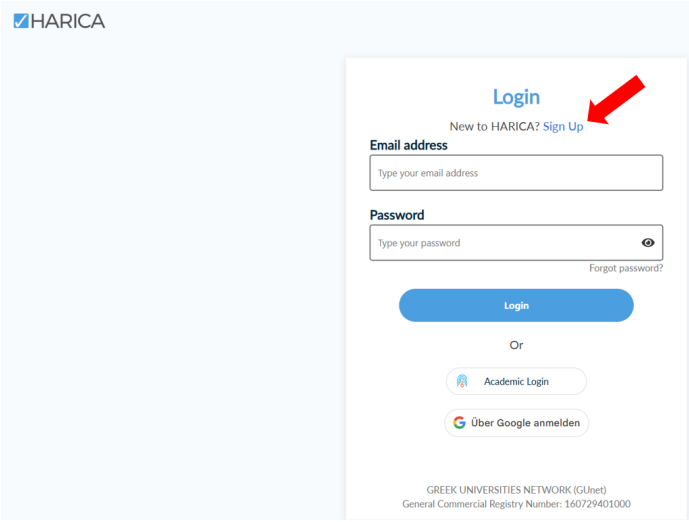

Abbildung 85 - HARICA Login

2.) Es öffnet sich die Seite **Sign Up** (s. Abbildung 70 – HARICA Sign Up).
   a.) Geben Sie bei **Email address** die Emailadresse Ihres Gruppenpostfaches mit @h-ka.de ein.
   b.) Bei **Given name** geben Sie den Namen Ihres Gruppenpostfachs ohne Punkt ein.
   c.) Dann geben Sie bei **Surname *Gruppenpostfach*** ein.
   d.) Anschließend geben Sie unter **Password** und **Confirm password** ein Passwort ein und notieren Sie sich bitte das Passwort.
   e.) Zum Bestätigen der eigegebenen Daten klicken Sie auf den blauen Button **Sign Up**.

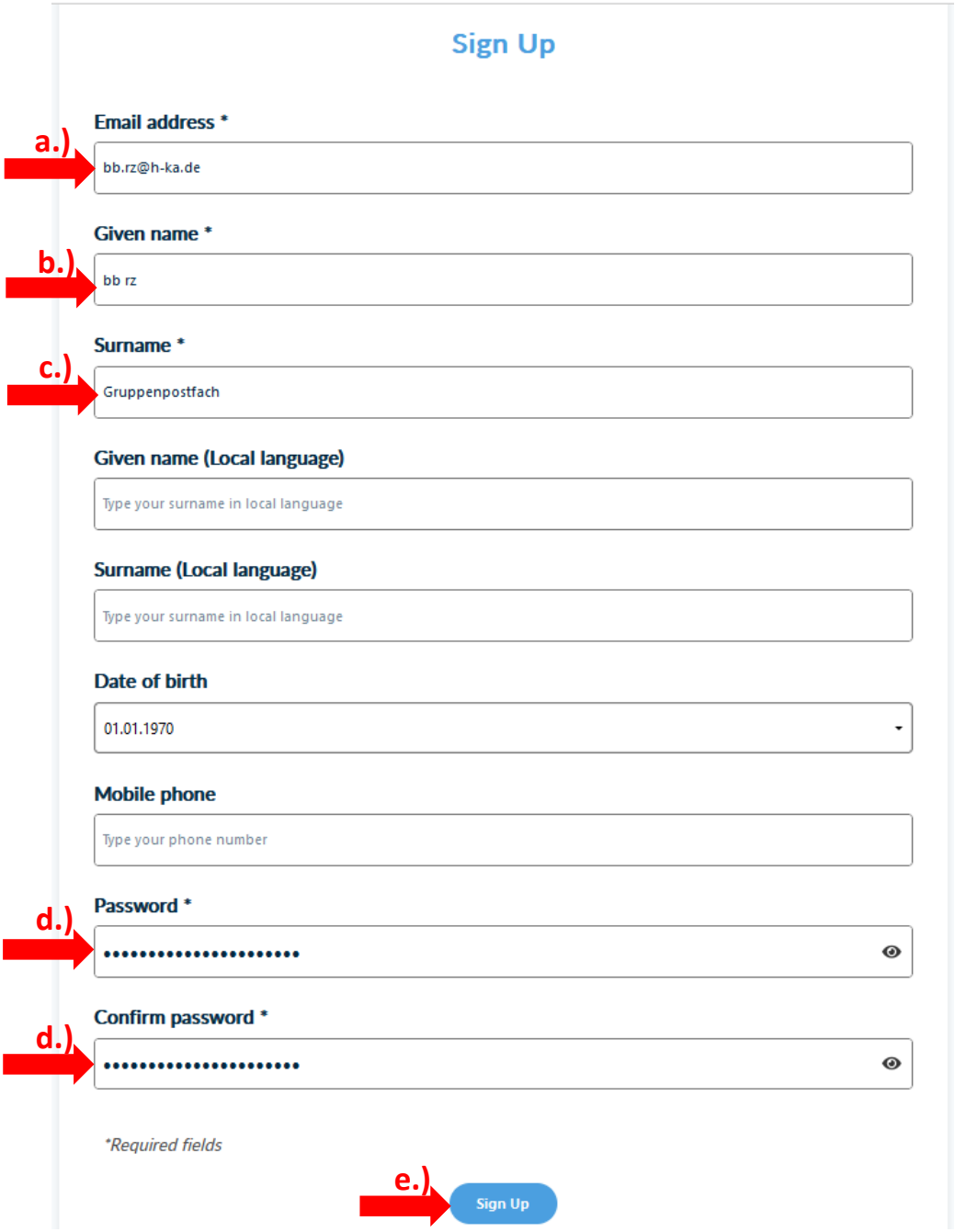

Abbildung 86 - HARICA Sign Up

3.) Sie erhalten folgende Mitteilung: **Activate your account - Your account has been created.**

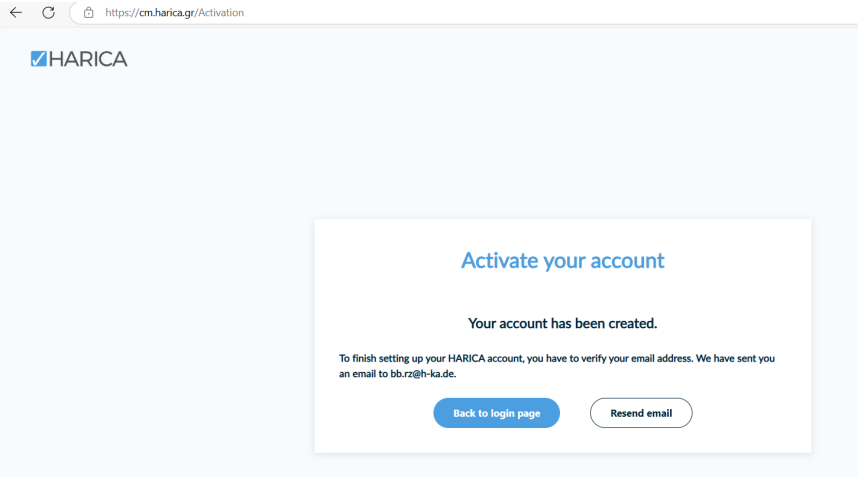

Abbildung 87 - Benachrichtigung über die Mailzustellung

4.) Wechseln Sie nun in Ihr Email-Gruppenpostfach und Sie haben eine Mail von HARICA erhalten.

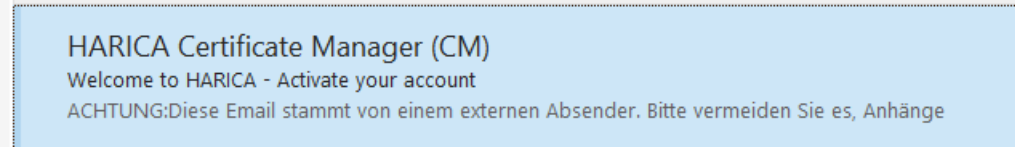

Abbildung 88 - Email von HARICA

Bitte klicken Sie in der Mail auf **Confirm email.**

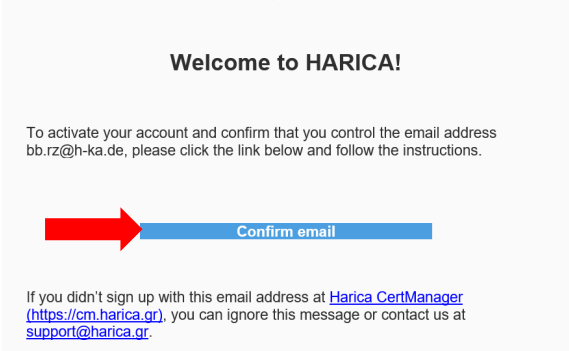

Abbildung 89 - Bestätigen der Gruppenpostfach-Mailadresse

5.) Wechseln Sie wieder in den Browser und klicken Sie auf den Button **Activate.**

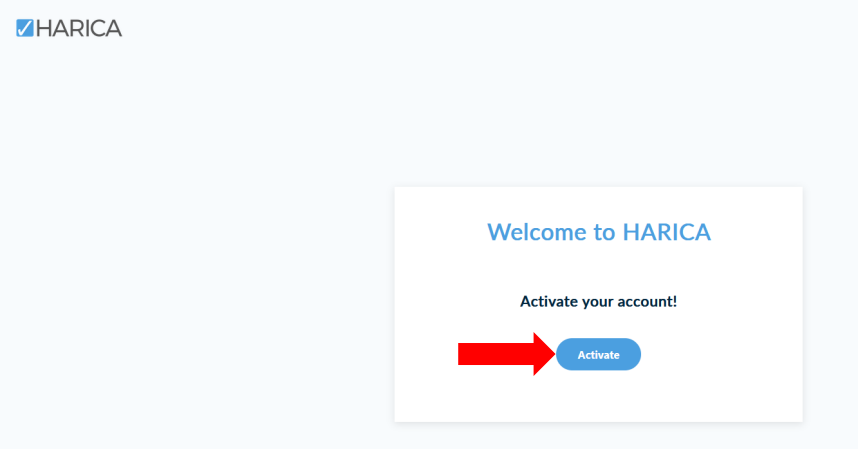

Abbildung 90 - Bestätigung bei HARICA

6.) Anschließend erhalten Sie auf der Seite von HARICA eine Meldung **Your account has been activated**. Klicken Sie nun auf den Button **Go to login page**.

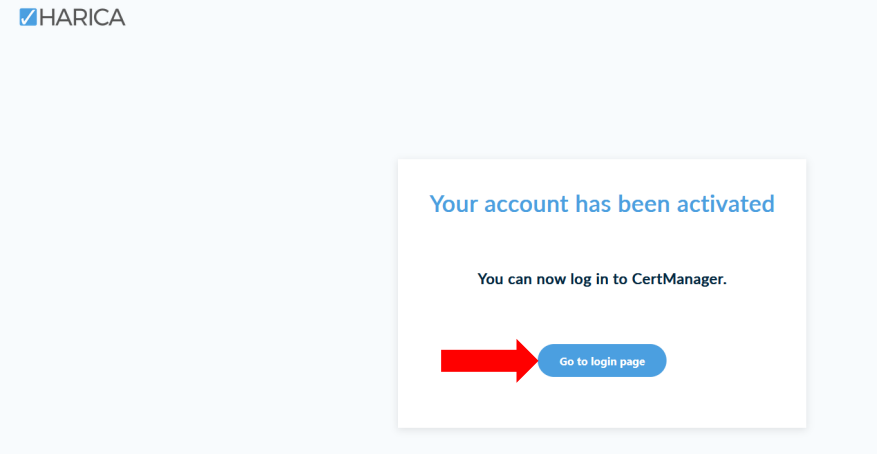

Abbildung 91 - Zur Login-Seite wechseln

7.) Es öffnet sich ein **Login**-Maske. Geben Sie bei **Email address** Ihr Gruppenpostfach mit @h-ka.de und das Passwort, welches Sie sich unter Punkt 2d.) gesetzt haben ein und klicken Sie auf den Button **Login**.

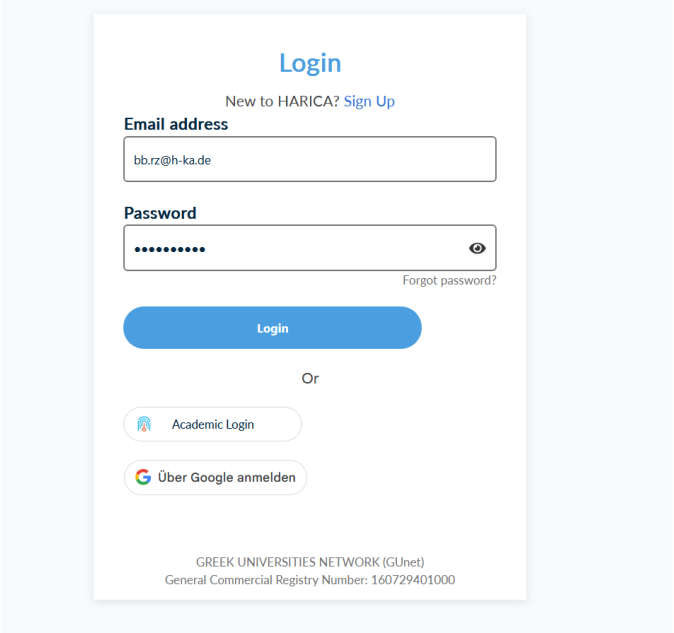

Abbildung 92 - Einloggen bei HARICA

8.) In der rechten oberen Leiste können Sie erkennen, ob Sie mit dem Namen des Gruppenpostfachs eingeloggt sind.

Wählen Sie nun in der Seitenleiste **Email** aus.

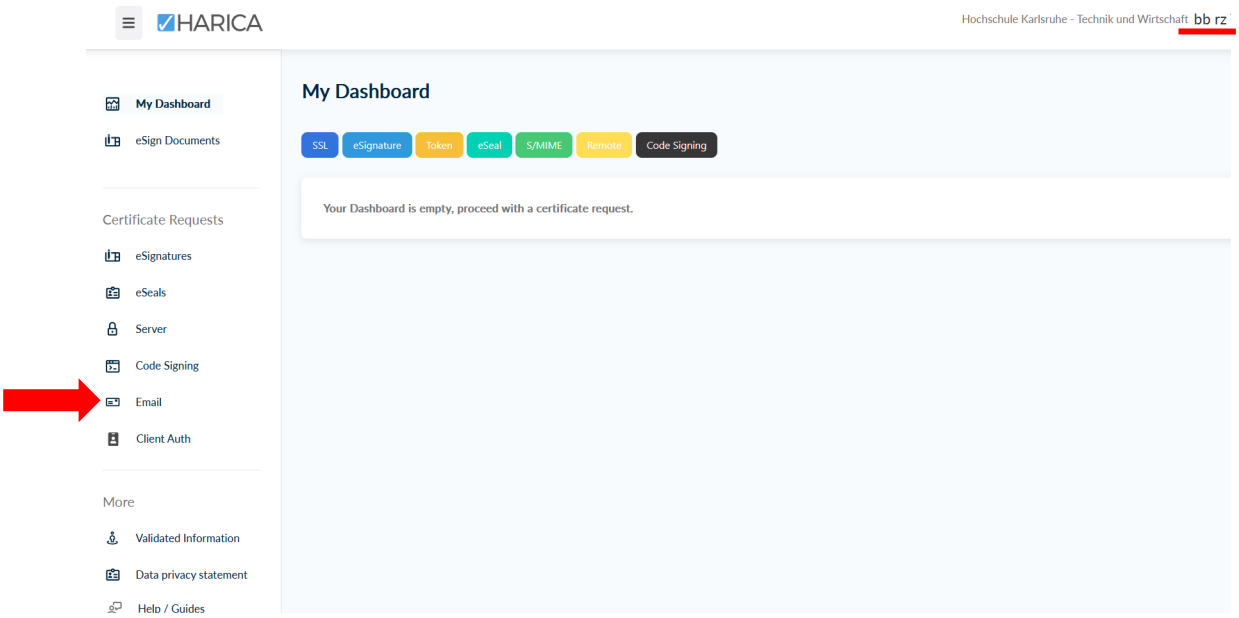

Abbildung 93 - My Dashboard bei HARICA

9.) Klicken Sie nun bei **Email-only** auf den Button **Select**.

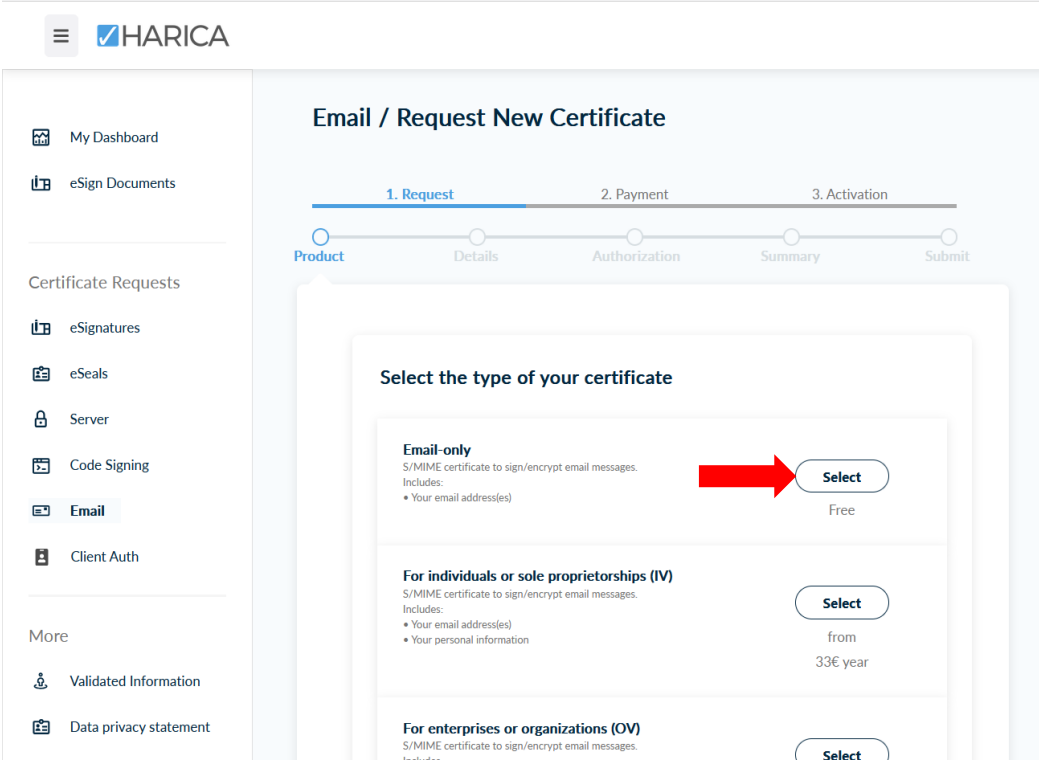

Abbildung 94 - Email-only wählen

10.) Scollen Sie nach unten und drücken Sie auf den blauen Button **Next**.

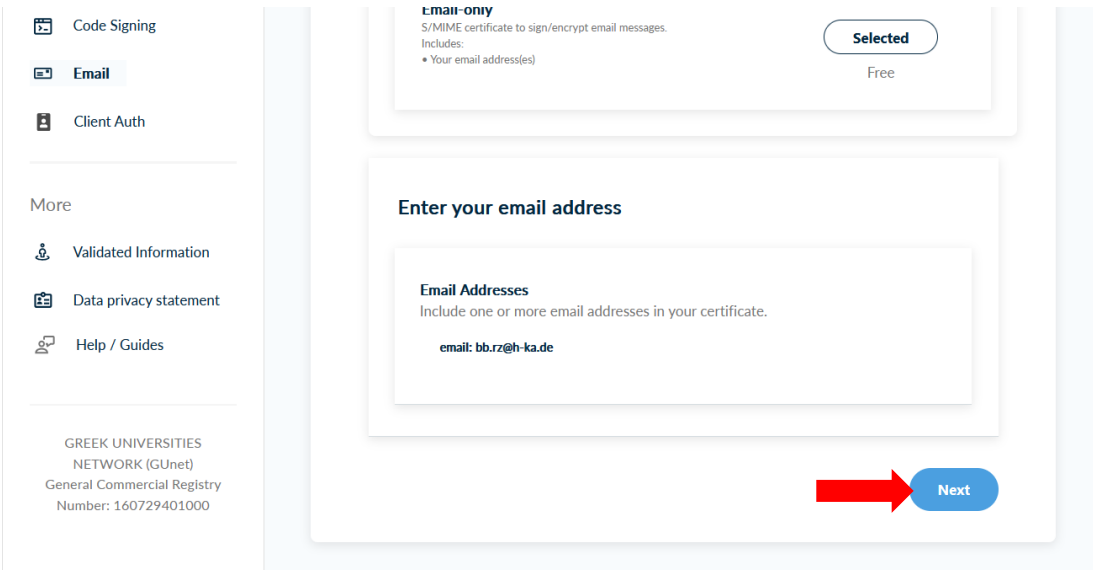

Abbildung 95 - Bestätigung der GP-Mailadresse

11.) Zum Validieren Ihre Gruppenpostfach-Zertifikats per Emailadresse klicken Sie auf **Selected** und anschließend auf **Next**.

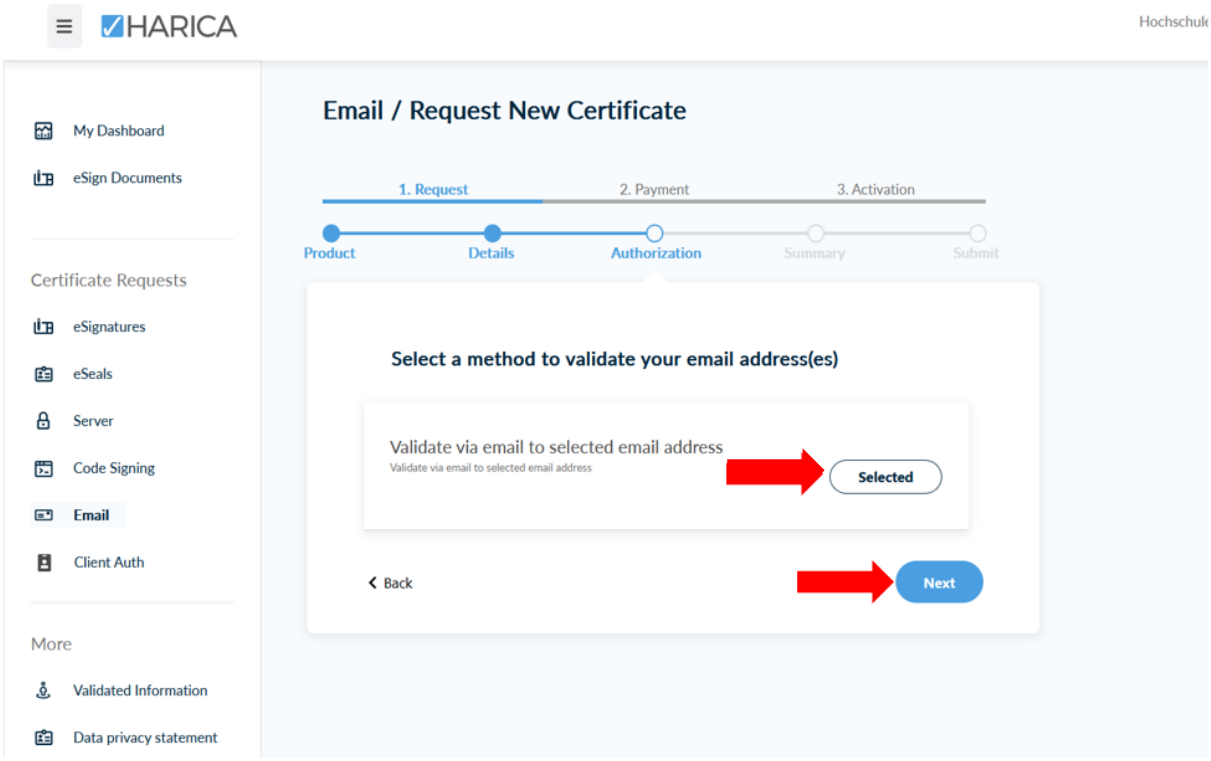

Abbildung 96 - Validierungsmethode bestätigen

12.) Bestätigen Sie die Bedingungen und klicken Sie auf **Submit**.

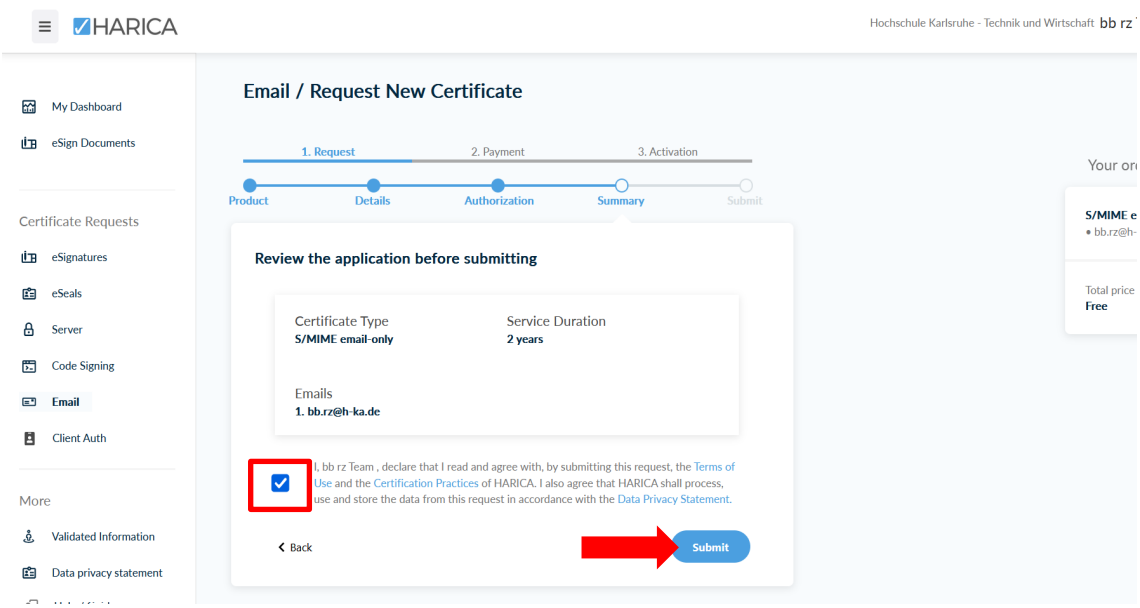

Abbildung 97 - Den Bedingungen von HARICA zustimmen

13.) Das Gruppenpostfach-Zertifikat finden Sie nun in **My Dashboard**.

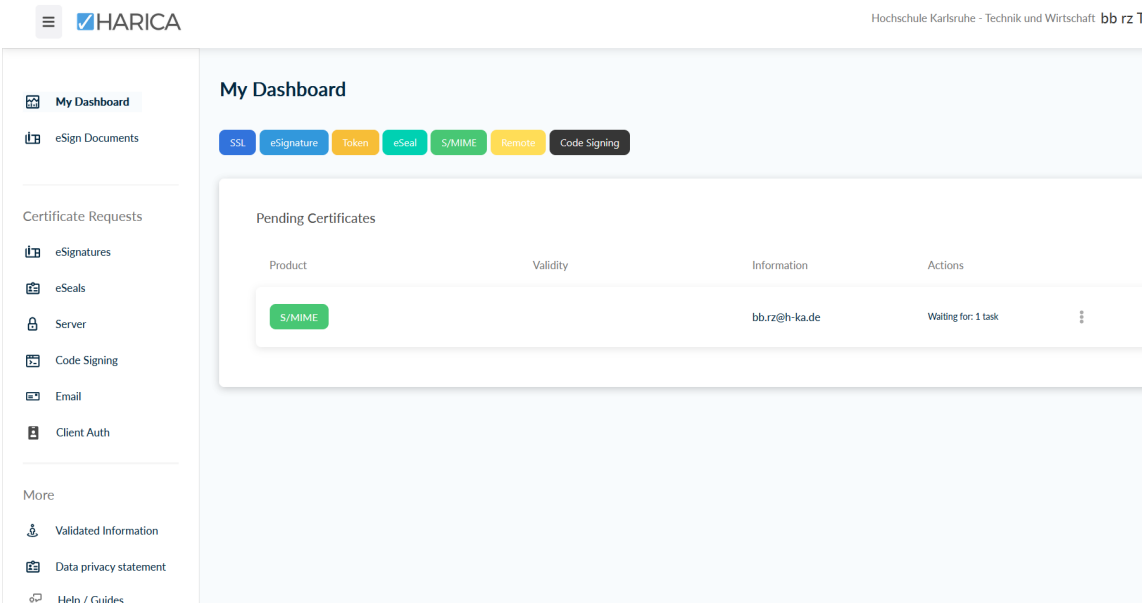

Abbildung 98 - Offene Aktion

14.) Wechseln Sie erneut in Ihr Gruppenpostfach und öffnen Sie die Mail von **HARICA – Email confirmation for certificate issuance**.

Abbildung 99 – Email wurde zugestellt

15.) Klicken Sie nun auf **Confirm**.

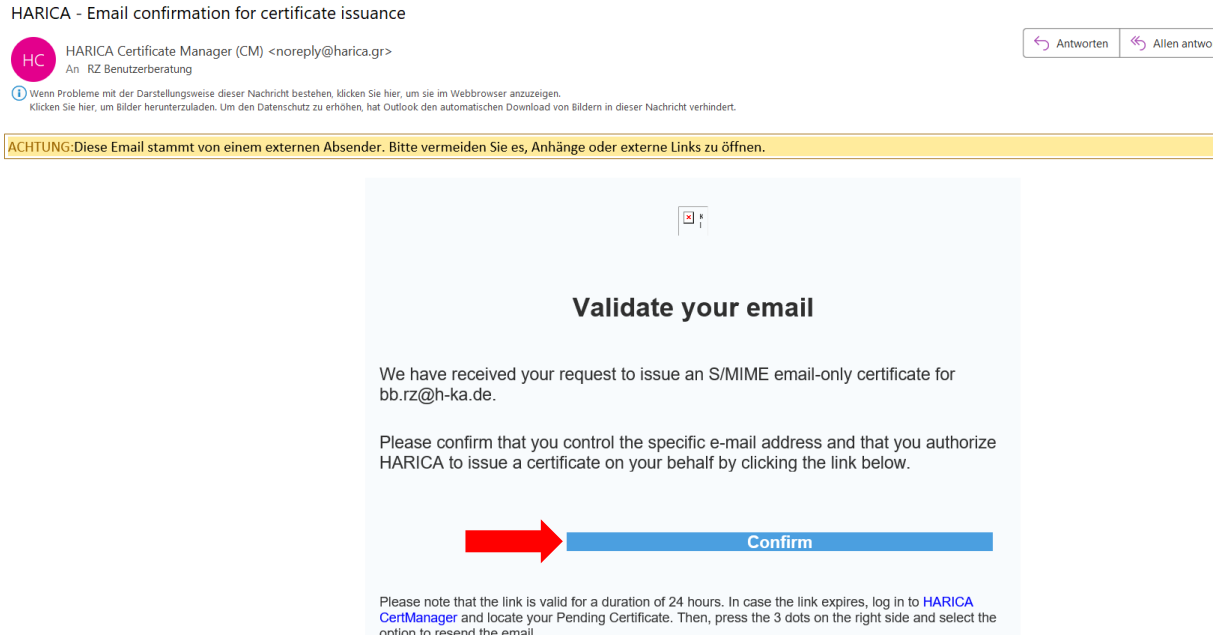

Abbildung 100 - Email bestätigen

16.) Wechseln Sie wieder in den Browser und klicken Sie auf **Confirm**.

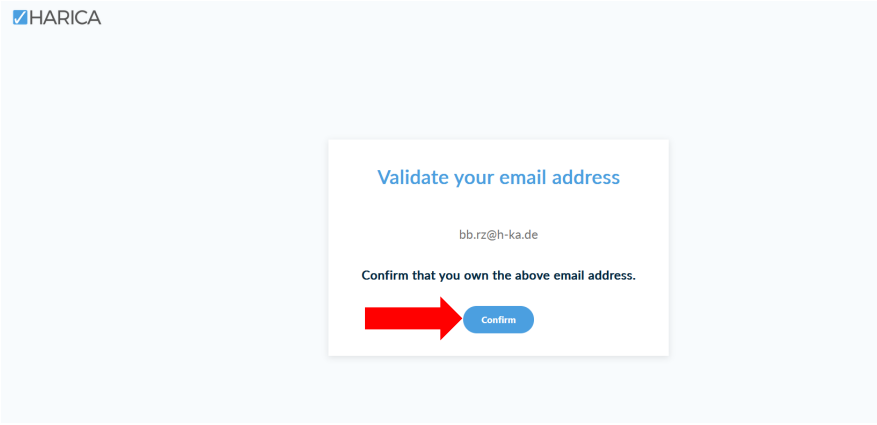

Abbildung 101 - Bei HARICA bestätigen

17.) Nun wählen Sie den Button **Enroll your Certificate.**

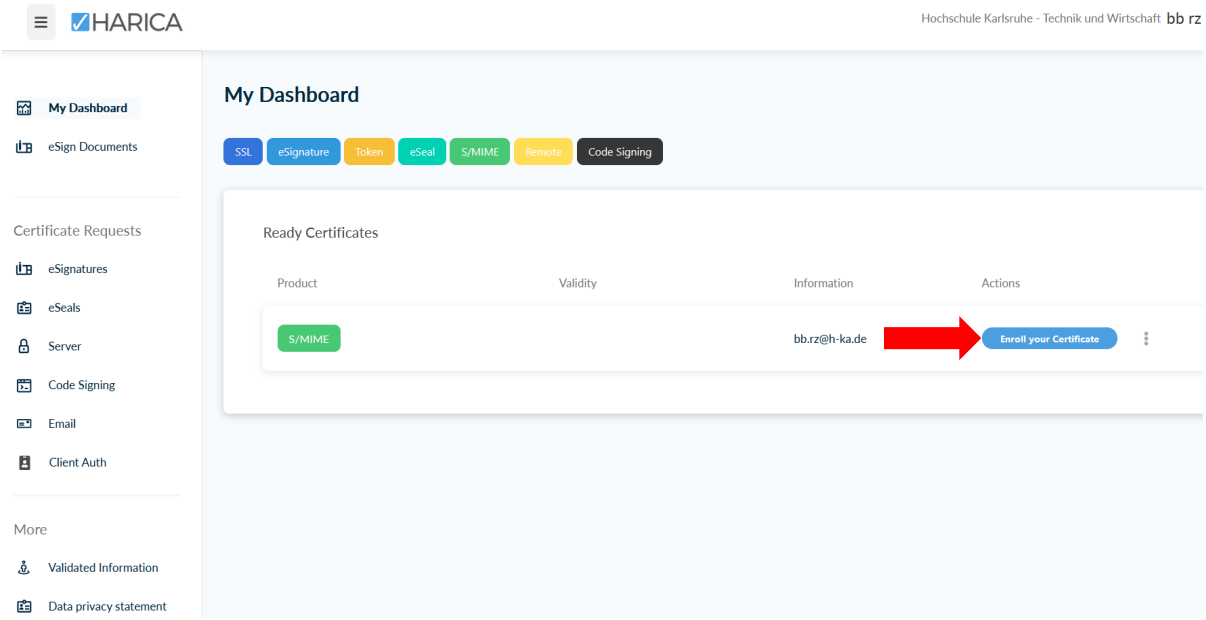

Abbildung 102 - Zertifikat ausrollen

18.) Setzen Sie folgende Einstellungen:

a.) **Algorithm**: RSA (default)
b.) **Key size**: 4096
c.) Setzen Sie ein Passwort unter **Type your passphrase** und wiederholen Sie das Passwort unter **Retype your passphrase**. Notieren Sie sich dieses Passwort.
d.) Setzen Sie ein Haken zum Bestätigen der HARICA-Bedingungen.
e.) Klicken Sie auf **Enroll Certificate**.

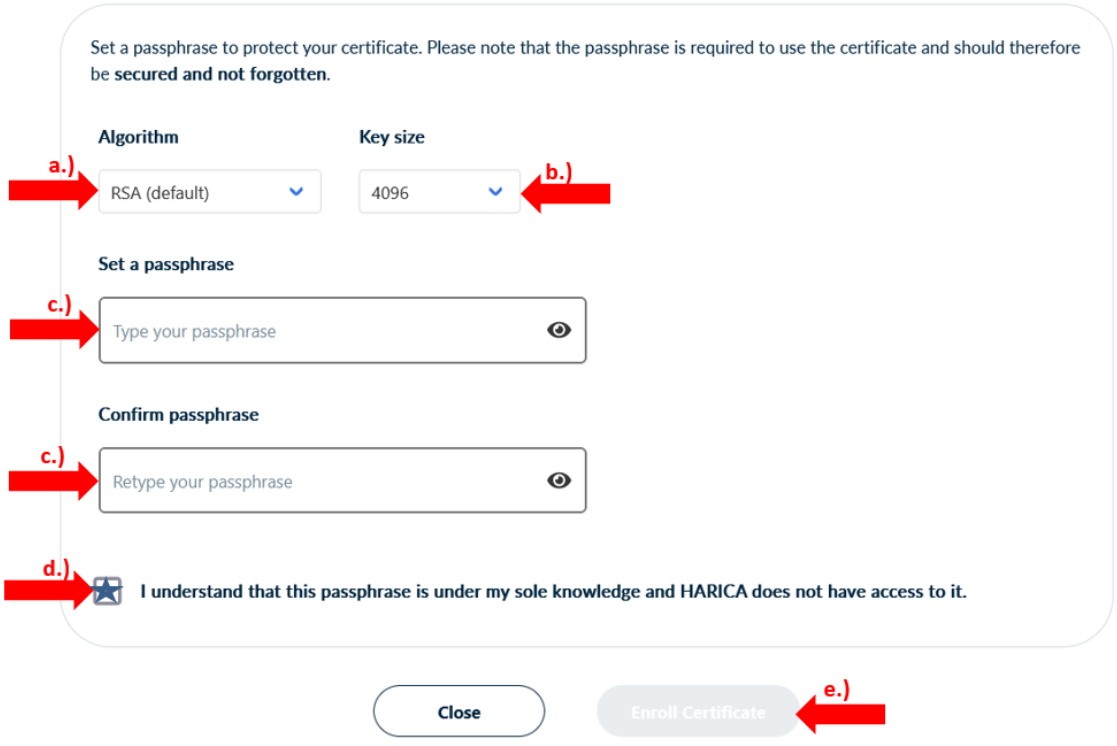

Abbildung 103 - Zertifikat erstellen

19.) Das Zertifikat steht zum Download bereit und kann über den **Download**-Button heruntergeladen werden.

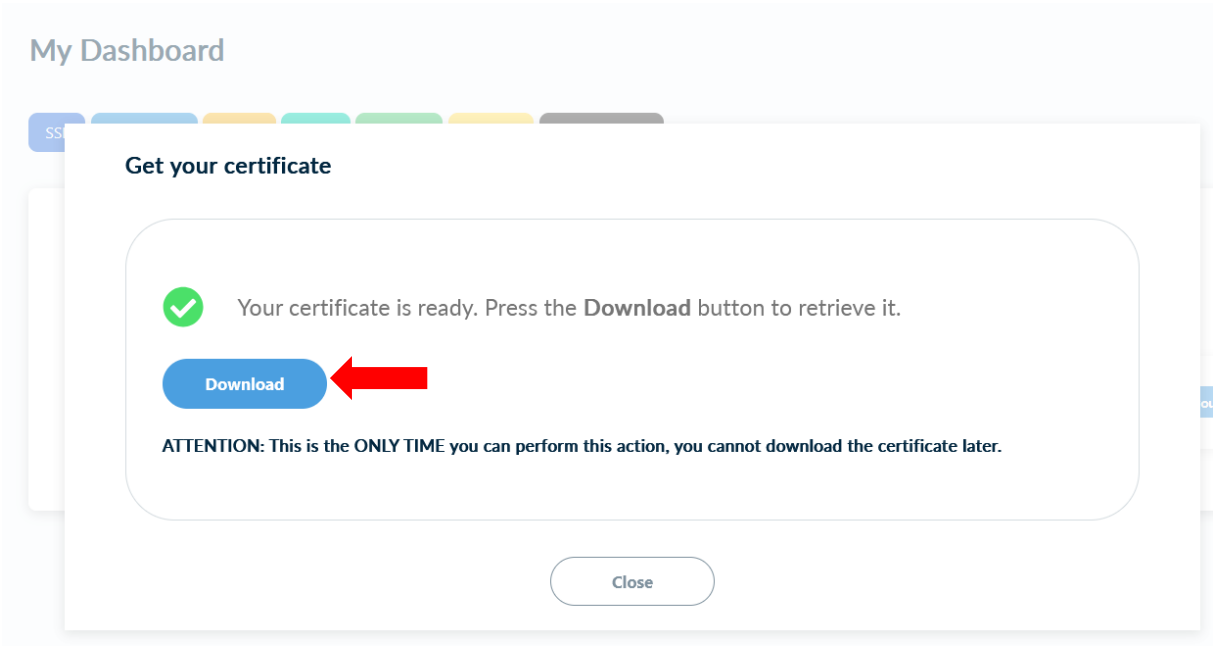

Abbildung 104 - Zertifikat herunterladen

20.) Sie finden die p12-Datei in Ihrem Download-Ordner.

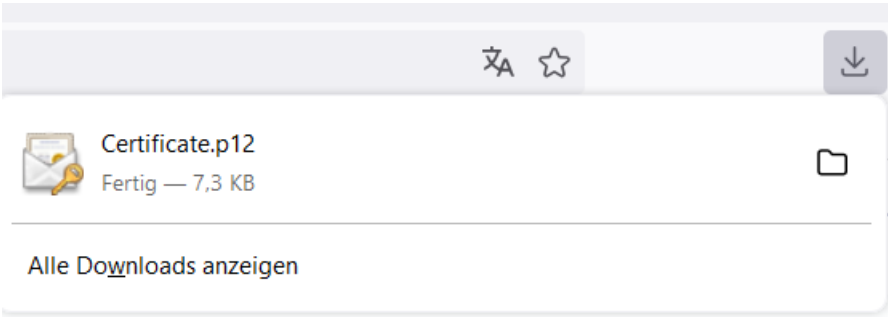

Abbildung 105 - Zertifikat in Download-Ordner

21.) Nach dem erfolgreichen Herunterladen können Sie auf den Button **Close** drücken.

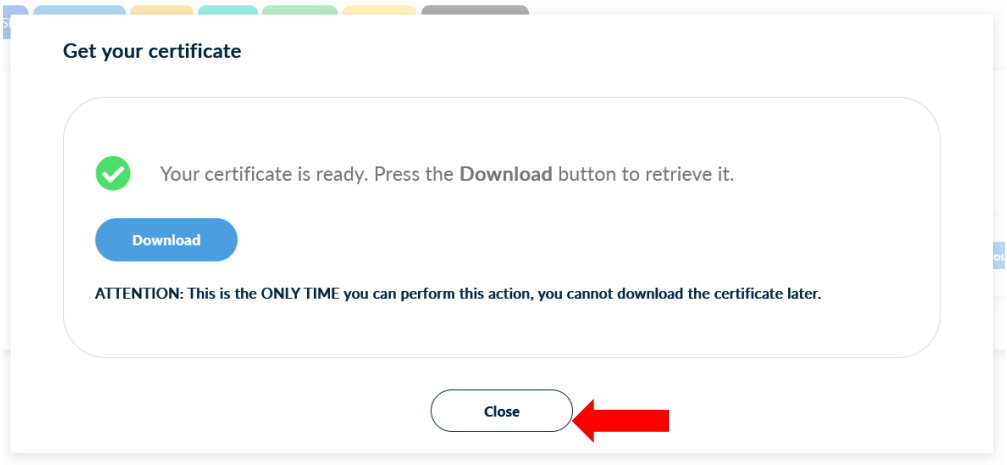

Abbildung 106 – Zertifikaterstellung bei HARICA beenden

22.) In **My Dashboard** bei HARICA sehen Sie, wie lange Ihr Gruppenpostfachzertifikat gültig ist.

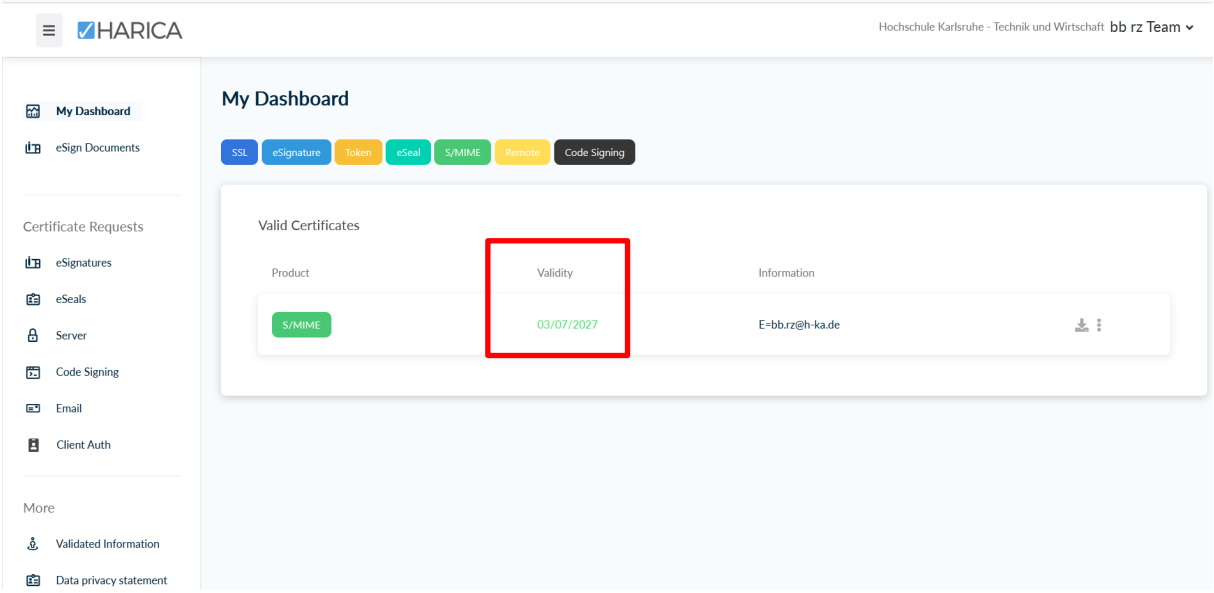

Abbildung 107 - Gültigkeit des GP-Zertifikats

6.8 Einbinden des Gruppenpostfach-Zertifikats

Zum Einbinden Ihres Gruppenpostfach-Zertifikats folgen Sie den Schritten in der Intro-Anleitung unter dem Punkt 6.6 (Einbinden des Zertifikats bei Ihr Emailpostfach).

6.9 Arbeiten mit Gruppenpostfächer und Verteiler

Um ein Gruppenpostfach oder einen Verteiler einrichten zu lassen, müssen Sie zunächst einen Antrag ausfüllen. Den Antrag finden Sie im internen Bereich des Rechenzentrums auf den Hochschulseiten unter **RZ-Formular: „Antrag auf Einrichtung/Änderung eines Emailverteilers / Exchangepostfachs**“.

1.) **Gruppenpostfach-Mitglieder hinzufügen und entfernen**
Nur der Gruppenpostfach-Administrator kann sich im Hochschulnetz unter der Seite

https://portal.adb.h-ka.de

einloggen und weitere Mitglieder des Gruppenpostfachs hinzufügen.
Hierzu wählen Sie unter dem Seitenregister „**Gruppenpostfächer“** und klicken im Dropdown-Menu unter „**Gruppenpostfach auswählen**“ Ihr Gruppenpostfach an.

Abbildung 108 - Gruppenpostfach auswählen

Anschließend geben Sie das RZ-Benutzerkürzel der hinzuzufügenden Person ein und klicken auf „**Hinzufügen**“.

Abbildung 109 - Neues Gruppenpostfach-Mitglied anhand des RZ-Benutzerkürzels hinzufügen

Falls der Gruppenpostfach-Administrator auch Mitglied des Gruppenpostfach ist, muss sich der Gruppenpostfach-Administrator anhand des RZ-Benutzerkürzels als Mitglied hinzufügen.
Zum Entfernen eines Mitglieds aus dem Gruppenpostfach ist unter der Spalte **Value** „**Entfernen**“ auszuwählen.

Abbildung 110 - Gruppenpostfach-Mitglied entfernen

2.) **Gruppenpostfach in Outlook**
Falls das neue Gruppenpostfach nicht direkt erscheint, dann führen Sie bitte einen Neustart Ihres Rechners durch.

3.) **Gruppenpostfach im Outlook-Browser öffnen**
Varinate1:
Im Hochschulnetz können Sie entweder über einen direkten Link auf das Gruppenpostfach zugreifen:
https://webmail.h-ka.de/owa/**Name des Gruppenpostfachs**@h-ka.de/?offline=disabled#path=/mail
In der Anmeldemaske geben Sie Ihre RZ-Zugangsdaten ein.

Varinate2:
a.) Rufen Sie zunächst im Browser Ihr persönliches Postfach auf:

https://webmail.h-ka.de (im Hochschulnetz) oder https://owa.h-ka.de

b.) Klicken Sie auf das Profil-Symbol und wählen Sie „**Weiteres Postfach öffnen…**“.

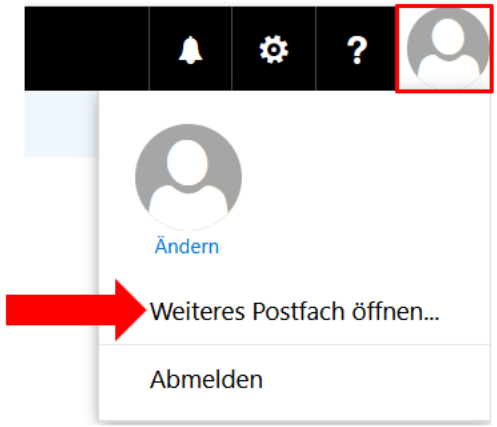

Abbildung 111 - Weiteres Postfach öffnen

c.) Es öffnet sich das Popup-Fenster „**Weiteres Postfach öffnen**“. Geben Sie den Namen Ihres Gruppenpostfach ein und klicken Sie auf „**Verzeichnis durchsuchen**“.

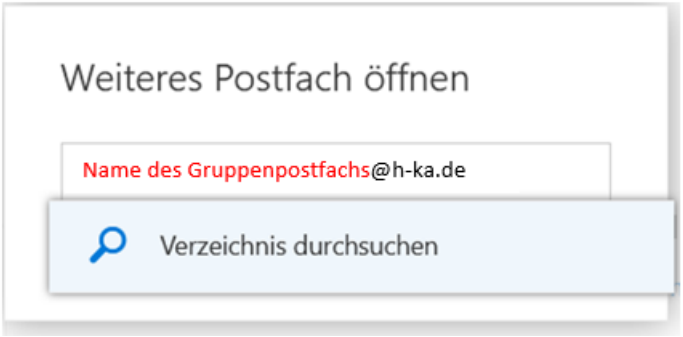

Abbildung 112 - Name des Gruppenpostfach eingeben

d.) Zum Öffnen des Gruppenpostfachs klicken Sie auf „**Öffnen**“.

Abbildung 113 - Gruppenpostfach öffnen

e.) Danach öffnet sich das Gruppenpostfach in einem weiteren Browser-Fenster.

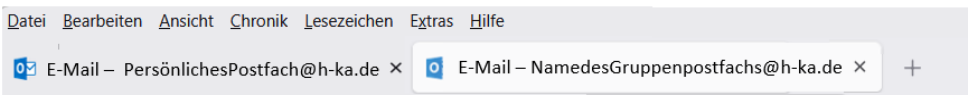

Abbildung 114 - Weiteres Browser-Fenster öffnet sich

4.) Verteiler-Mitglieder hinzufügen und entfernen
Allgemein leitet ein Verteiler eingehende Mails direkt an Ihr persönliches Postfach weiter.

Der Administrator des Verteilers fügt neue Verteiler-Mitglieder wie folgt hinzu:
1.) Öffnen Sie das Outlook-Adressbuch.
2.) Beim Dropdown-Menu „**Adressbuch**“ wählen Sie den Punkt „**Alle Verteilerlisten**“.
Wichtig: Outlook wird in den meisten Fällen kurz nicht reagieren und die Warnmeldung anzeigen, dass versucht wird, die Daten vom Exchange zu laden. Es kann auch eine zusätzliche Warnmeldung kommen, dass etwas falsch gelaufen ist. Sollte diese Warnmeldung kommen, dann rufen Sie nochmals im Dropdown bei „**Adressbuch**“ zum Beispiel „**Alle Kontakte**“ auf und wechseln Sie zurück auf „**Alle Verteilerlisten**“. Nun sollten alle Verteilerlisten angezeigt werden.
3.) Suchen Sie den Verteiler im Adressbuch.
4.) Wählen Sie mit einem Rechtsklick den Verteiler aus und klicken Sie auf „**Eigenschaften**“.
5.) Klicken Sie auf den Punkt „**Mitglieder ändern…**“ und fügen Sie entweder ein neues Mitglied hinzu oder entfernen Sie ggf. ein Mitglied.

7 Zertifikatsgesicherte Hochschuldienste

Zur leichtgängigen Nutzung von Hochschuldiensten befinden sich erste webbasierte Dienstangebote in einem zertifikatsgesicherten Bereich.

Mit dem Import eines Nutzerzertifikats (vgl. Kapitel 6) sind Sie in der Lage, solche Dienste per Webbrowser ohne Angabe eines TOTP-Tokens zu verwenden.

7.1 Zertifikatsgesicherter Webmail-Zugang

Der Pilotbetrieb umfasst insbesondere den Webmail-Zugang unter

- https://owa-cert.h-ka.de

Wenn Sie noch kein Zertifikat in Ihrem Account importiert haben, wird der Zugang zu diesem Dienst abgelehnt:

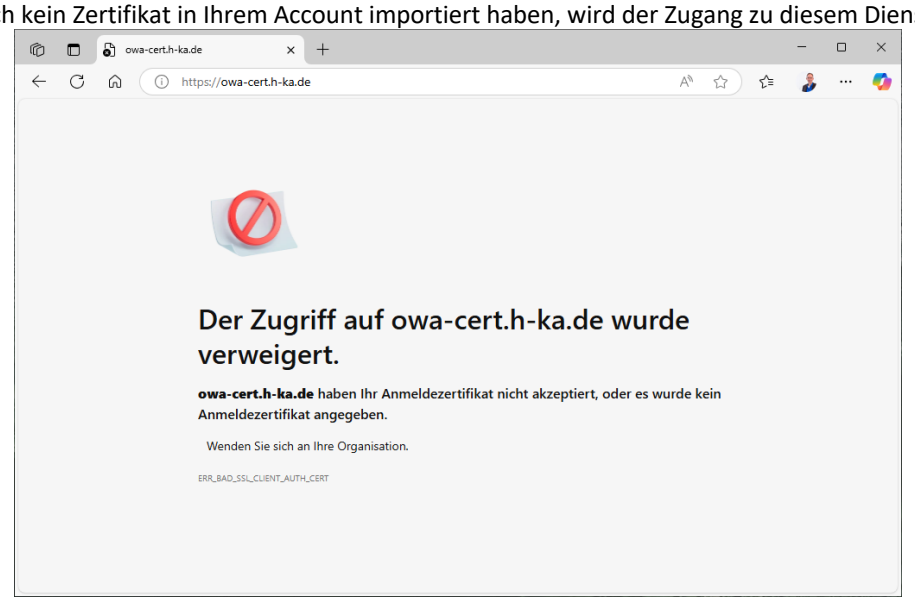

Abbildung 115 - Meldung bei fehlendem Zertifikatsimport

Sobald ein Zertifikat bereitsteht, können Sie es beim Aufruf der Webseite auswählen.

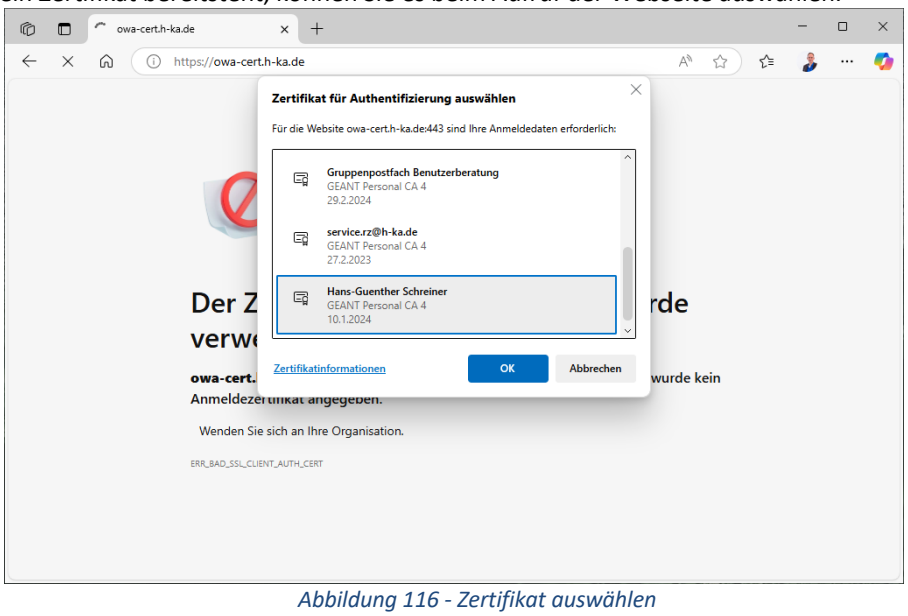

Abbildung 116 - Zertifikat auswählen

7.2 Zertifikatsgesicherter Zugang zu der Zeiterfassung

Der Pilotbetrieb umfasst ebenso den Zugang zur Zeiterfassung unter

- https://ze-cert.h-ka.de

Wenn Sie noch kein Zertifikat in Ihrem Account importiert haben (vgl. Kapitel 6), wird der Zugang zu diesem Dienst abgelehnt. Sobald ein Zertifikat bereitsteht, können Sie es beim Aufruf der Webseite auswählen.

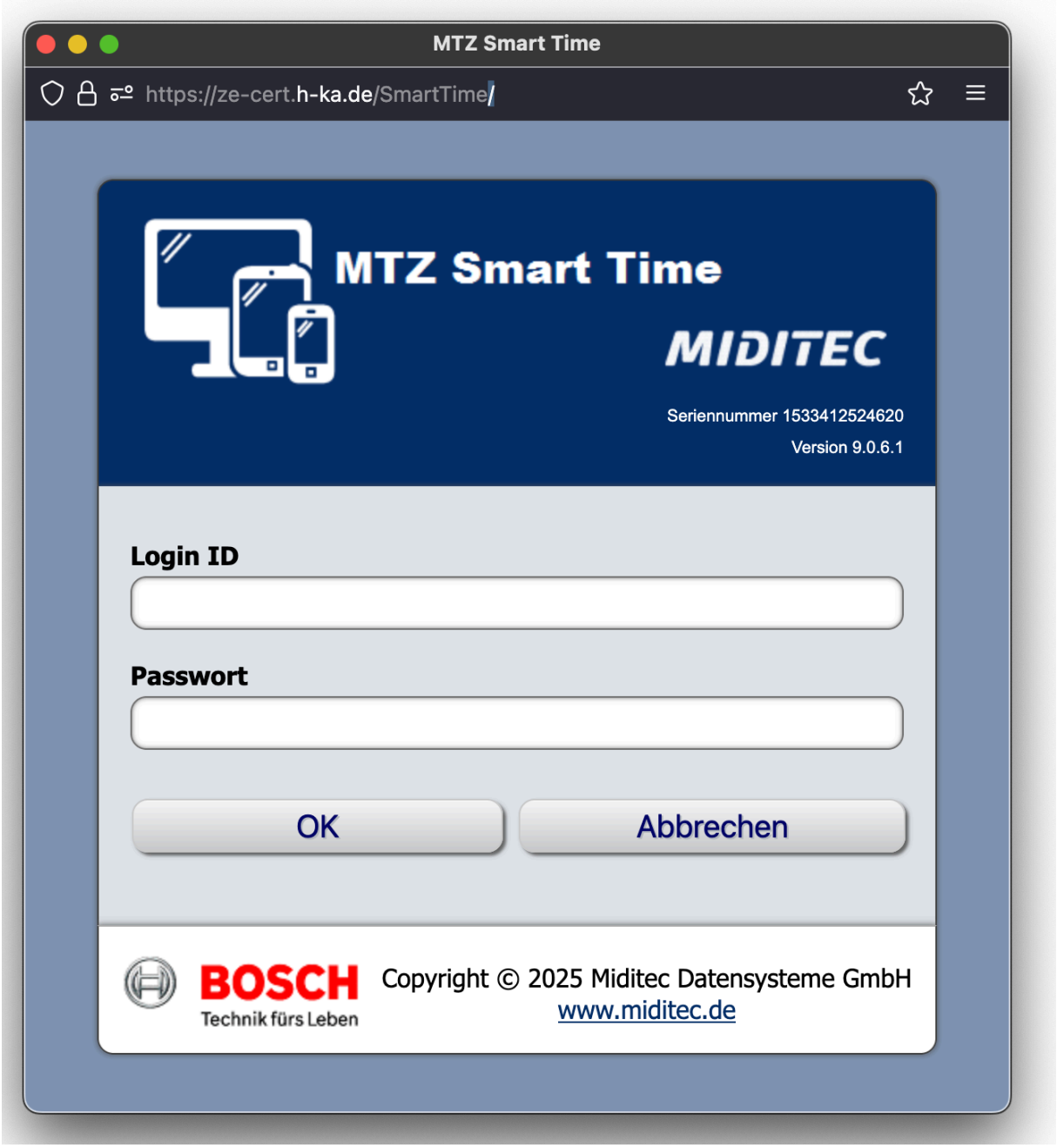

Abbildung 117 - MRZ-Smart-Time

8 ISEC7 Mail App für Apple iOS und Android

8.1 Was ist ISEC7 Mail?

Mit ISEC7 Mail greifen Sie sicher von Ihrem Smartphone oder Tablet auf Ihr Microsoft Exchange-Konto zu – inklusive E-Mails, Kalender und öffentlichen Ordnern. Diese Anleitung beschreibt die Einrichtung der ISEC7 Mail App für iPhones und Android-Smartphones.

Abbildung 118 - Die App "ISEC7 Mail".

8.2 Voraussetzung für ISEC7 Mail:

- Ein iPhone mit iOS-Betriebssystem 10.0 oder höher
  oder
  Ein Smartphone mit Android-Betriebssystem
- Ihr HARICA-Nutzerzertifikat und das Passwort
- Internetzugang z.B. über WLAN „eduroam“
- Laptop/PC
- Zugriff auf Outlook und OWA

Hinweis: Die von der Hochschule verwalteten iPhones/iPads und Android-Smartphones erhalten die **ISEC7 Mail** kostenlos. Für private iPhones/iPads Android-Smartphones kostet die Nutzung der Premiumversion etwa 37 Euro/Jahr.

8.3 Zielgruppe dieser Anleitung

Diese Anleitung richtet sich an Beschäftigte der Hochschule Karlsruhe, denen ein iPhone/iPad oder ein Android-Smartphone über die Hochschule zur Verfügung gestellt wurde

8.4 Vorgehen

Wenn die App „ISEC7 Mail“ auf einem hochschulverwalteten Gerät installiert werden soll, ist ein vollständig ausgefülltes MDM-Formular an die Benutzerberatung zu senden. Die Benutzerberatung leitet das Formular zur weiteren Bearbeitung an die zuständige Stelle weiter.

8.5 Installation der App „ISEC7 Mail“ (für Studierende)

Dieser Abschnitt richtet sich an Studierende. Die App „ISEC7 Mail“ kann im Apple App Store (iPhone) oder im Google Play Store (Android) gesucht, heruntergeladen und installiert werden.

1. Öffnen Sie den App Store bzw. Google PlayStore und suchen Sie nach der App „**ISEC7 Mail**“.
2. Klicken Sie auf „**Installieren**“, um die App auf Ihr iPhone/Ihr Android-Smartphone herunterzuladen und zu installieren.
3. Folgen Sie nach der Installation der Einrichtung ab Kapitel 8.6 (für iPhone/iPad) und Kapitel 8.7 (für Android-Smartphones).

8.6 „ISEC7 Mail für Apple iOS

8.6.1 Einrichten des Hauptkontos

1. Sobald die App auf Ihrem iPhone installiert ist, können Sie auf „Öffnen“ neben der App klicken, um diese zu starten.
2. Klicken Sie oben rechts auf den Kreis mit den drei Punkten, um die Einstellungen zu öffnen.

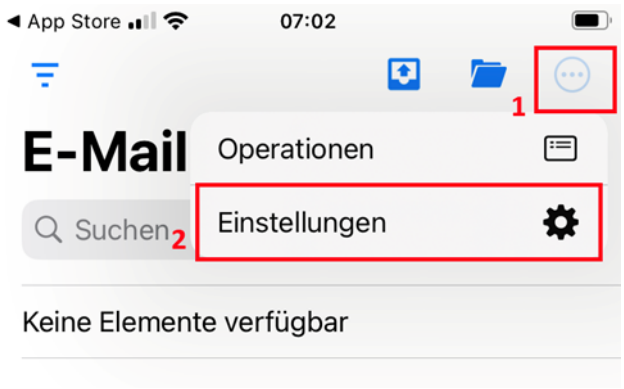

Abbildung 119 - Der Kreis mit den drei Punkten zum Öffnen der Einstellungen in "ISEC7 Mail".

3. Wählen Sie in den Einstellungen „Hauptkonto hinzufügen“.
4. Achten Sie darauf, dass unter „Typ“ die Option „Standard“ ausgewählt ist.
5. Füllen Sie die Maske wie folgt aus:
   - **E-Mail**: Geben Sie Ihre H-KA-E-Mailadresse ein (vorname.nachname@h-ka.de)
   - **Benutzername**: Tragen Sie Ihr RZ-Kürzel ein
   - **Passwort**: Geben Sie das Passwort zu Ihrem RZ-Kürzel ein.
6. **Alle Ordner hinzufügen**: Regler nach rechts verschieben. Klicken Sie auf „**Automatische Konfiguration**“ und anschließend auf „**Weiter**“.
7. Unten sollte nun erneut „**Weiter**“ angezeigt werden.
8. Klicken Sie auf „**Speichern**“. Danach erscheint der nächste Bildschirm.
9. Zum Abschluss klicken Sie oben links auf „**Fertig**“.

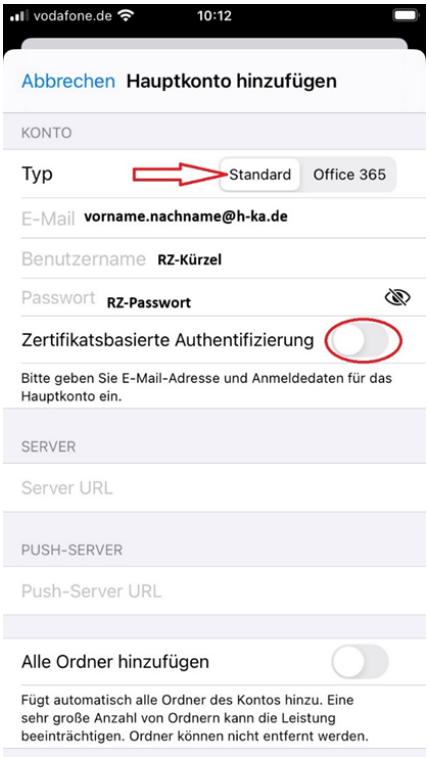

Abbildung 120 - Einrichten des Hauptkontos in ‚ISEC7 Mail' über die Eingabemaske.

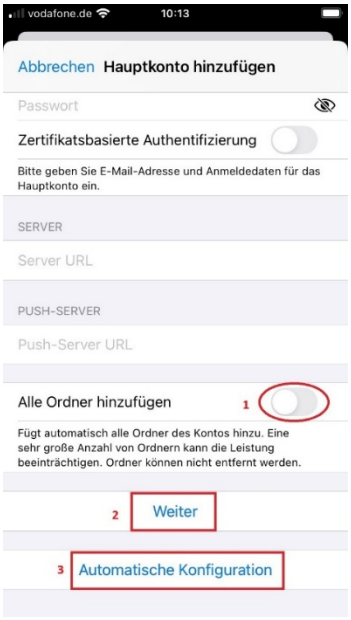

Abbildung 121 - Einrichten des Hauptkontos in ‚ISEC7 Mail': Fokus auf die automatische Konfiguration.

Abbildung 122 - Das fertig eingerichtete Hauptkonto in ‚ISEC7 Mail'.

8.6.2 Kopieren des HARICA-Nutzerzertifikats

Bitte führen Sie diese Schritte an Ihrem Laptop/PC durch:

1. Suchen Sie Ihr HARICA-Zertifikat „**Certificate.p12**".
2. Kopieren Sie die Datei und ändern Sie die Dateiendung der Kopie in **.medpfx** um.
3. Senden Sie sich das neu benannte Zertifikat und das HARCIA-Nutzerzertifikat per E-Mail zu.

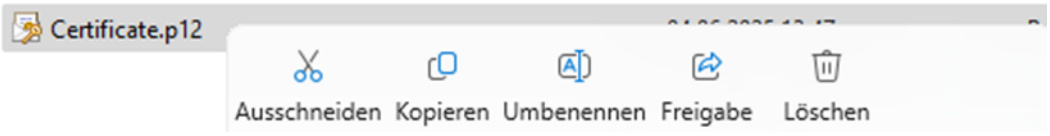

Abbildung 123 - Das Kopieren des HARICA-Nutzerzertifikats.

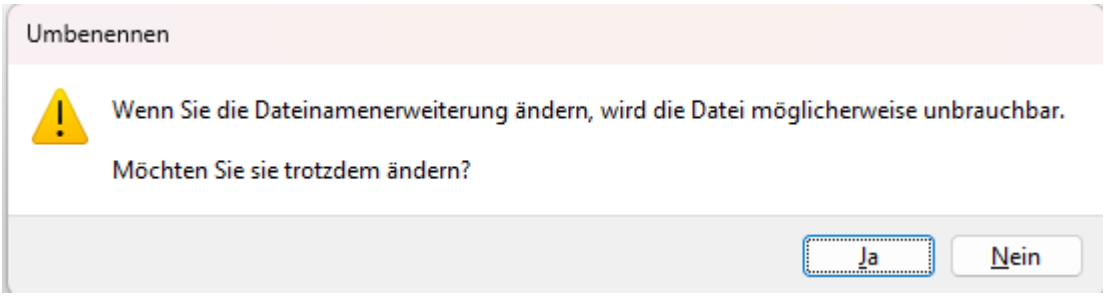

Abbildung 124 - Die Meldung, die bei der Neubenennung der Kopie des HARICA-Nutzerzertifikats erscheint.

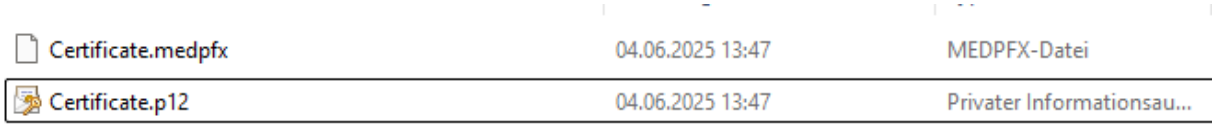

Abbildung 125 - Zwei Zertifikate: Das Original-Zertifikat von HARICA und das neu benannte Zertifikat.

Abbildung 126 - Eine E-Mail an sich selbst mit dem umbenannten Zertifikat.

8.6.3 Importieren des HARICA-Nutzerzertifikats in ISEC7 Mail

Sobald Sie sich das Zertifikat per E-Mail zugeschickt haben, öffnen Sie diese. In der ISEC7 Mail App sieht es wie folgt aus:

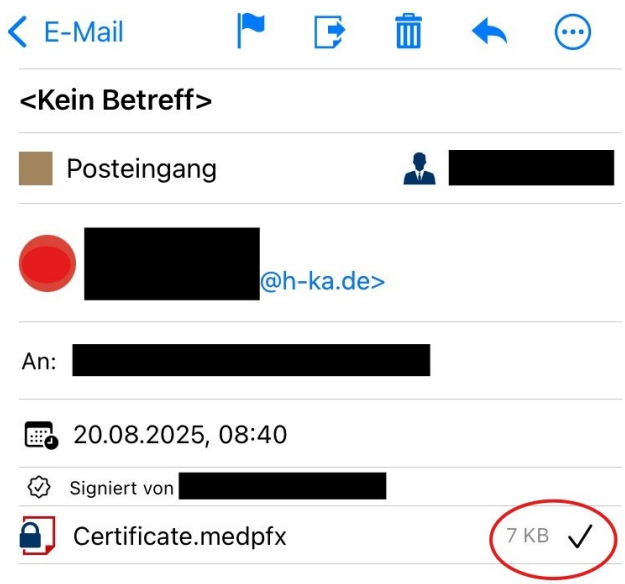

Abbildung 127 - Die E-Mail mit dem neu benannten Zertifikat.

1. Öffnen Sie die E-Mail und klicken Sie auf das angehängte Zertifikat.
2. Ein neues Fenster öffnet sich. Geben Sie dort das **Passwort** ein, das Sie bei der Erstellung des **HARICA Nutzerzertifikats** vergeben haben.

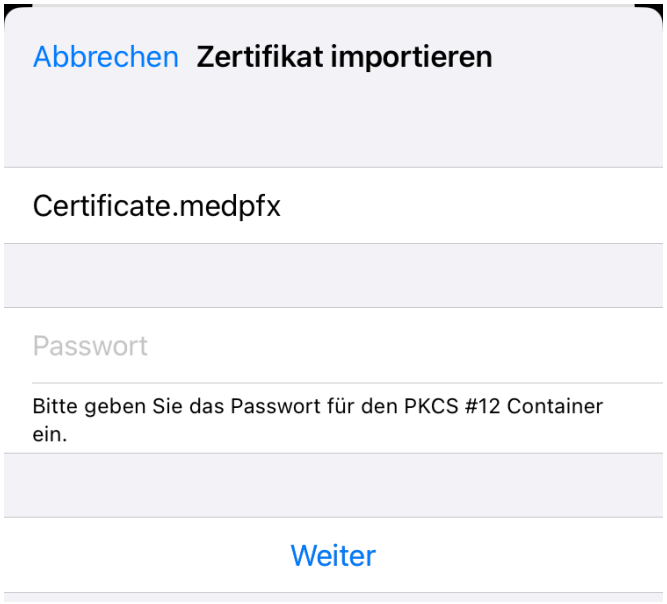

Abbildung 128 - Die Passworteingabe des Zertifikats, um es importieren zu können.

3. Klicken Sie anschließend auf „**Weiter**“.
4. Sie erhalten die Meldung, dass das Zertifikat erfolgreich eingebunden wurde und können die relevanten Daten einsehen.

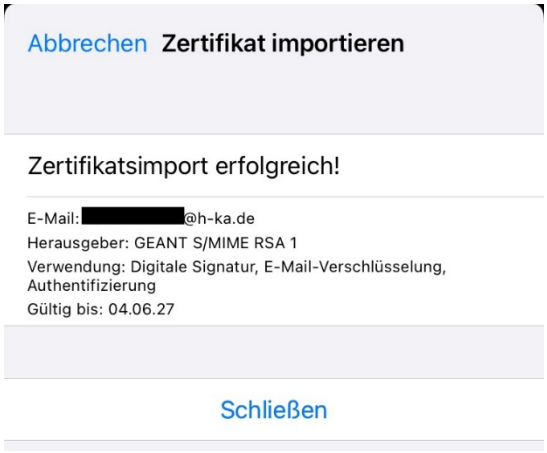

Abbildung 129 - Die Meldung, dass das Zertifikat erfolgreich importiert wurde.

5. Zum Abschluss klicken Sie auf „**Schließen**“.

Ab sofort können Sie über „ISEC7 Mail“ E-Mails schreiben senden und empfangen.
Hinweis: Zurzeit funktioniert die Verschlüsselung noch nicht.

8.6.4 Manuelle Konfiguration von ISEC7 Mail mit dem Hochschulserver

1. Öffnen Sie die Einstellungen und klicken Sie auf das Hauptkonto. Scrollen Sie in den Einstellungen des Hauptkontos nach unten bis zum Punkt „**Konto löschen**“.
2. Klicken Sie auf „**Konto löschen**“. Ein neues Fenster öffnet sich. Bestätigen Sie die Löschung mit einem Klick auf „**Löschen**“. Anschließend gelangen Sie automatisch zurück in die Einstellungen.
3. Wählen Sie erneut „**Hauptkonto hinzufügen**“.

4. Geben Sie die Daten, wie im Schritt 5 der Anleitung „**Einrichtung des Hauptkontos**“ ein.
   - **Server: owa-isec7.h-ka.de**
   - „**Alle Ordner hinzufügen**”: Regler aktivieren.
5. Klicken Sie auf „**Weiter**“, die Mailbox wird nun geladen. Danach klicken Sie auf „**Speichern**“ und anschließend auf „**Fertig**“

Ihr Hauptkonto mit dem Server owa-cert.h-ka.de wurde erfolgreich eingerichtet. Ab sofort können Sie außerhalb des Hochschulnetzes E-Mails senden und empfangen.

8.6.5 Signatur in ISEC7 Mail hinzufügen

Wie bei Outlook können Sie auch in ISEC7 Mail eine Signatur einrichten, die automatisch beim Verfassen von E-Mails eingefügt wird.

1. Öffnen Sie die Einstellungen und wählen Sie Ihr Hauptkonto aus.
2. Scrollen Sie zum Bereich Signatur und tippen Sie auf Signaturen.
3. Klicken Sie auf das „+“-Symbol und geben Sie einen Namen sowie den Text der Signatur ein.

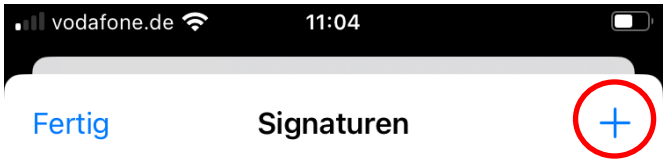

Abbildung 130 - Um eine Signatur zu erstellen, klicken Sie auf das „+“-Symbol.

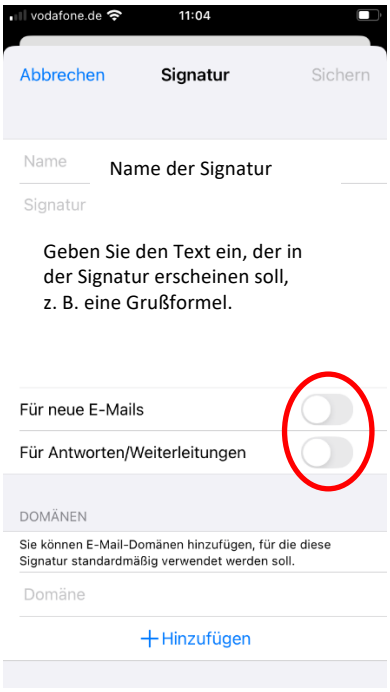

Abbildung 131 - Hier können Sie eine E-Mail-Signatur erstellen, die bei neuen Nachrichten und Antworten/Weiterleitungen automatisch eingefügt wird.

4. Aktivieren Sie die Schalter für „Für neue E-Mails“ und „Für Antworten/Weiterleitungen“.
5. Speichern Sie die Eingaben mit „Sichern“ und bestätigen Sie anschließend mit „Fertig“.
6. Aktualisieren Sie die Einstellungen über „Aktualisieren“ und wählen Sie danach „Speichern“.
7. Kehren Sie zurück zu den Einstellungen und schließen Sie mit „Fertig“ ab.

Die eingerichtete Signatur wird nun automatisch bei neuen E-Mails sowie bei Antworten und Weiterleitungen eingefügt.

8.6.6 Automatische Antworten in ISEC7 Mail einrichten

Wenn Sie beispielsweise im Urlaub oder anderweitig abwesend sind, können Sie in ISEC7 Mail eine automatische Antwort aktivieren. Diese wird anschließend auch in Outlook angezeigt.

1. Öffnen Sie die **Einstellungen** über den Kreis mit den drei Punkten.
2. Wählen Sie Ihr **Hauptpostfach** aus und scrollen Sie zum Bereich „**Automatische Antworten“**.

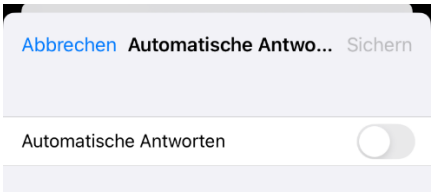

Abbildung 132 - Klicken Sie auf den Regler, um eine automatische Antwort einzurichten.

3. Tippen Sie darauf und aktivieren Sie den **Regler**. Nun erscheinen weitere Optionen:

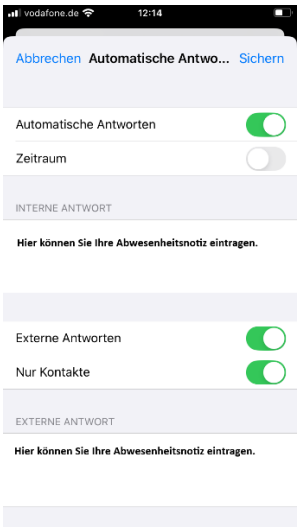

Abbildung 133 - Das Eingabefenster zur Erstellung einer Abwesenheitsnotiz

- Optional können Sie einen **Zeitraum** festlegen.
- Bearbeiten Sie die Texte für **interne** und **externe Antworten**.
- Aktivieren Sie den Regler für **externe Antworten** sowie bei Bedarf für **„Nur Kontakte“**.

4. Speichern Sie Ihre Eingaben mit **„Sichern“**.

5. Kehren Sie zu den Kontoeinstellungen zurück, klicken Sie auf **„Aktualisieren“**, anschließend auf **„Speichern“** und zum Schluss auf **„Fertig“**.

Nach der Aktualisierung ist die automatische Antwort aktiv. In Outlook erkennen Sie dies am gelben Hinweisbalken.

8.7 „*ISEC7 Mail*“-App für Android-Smartphones

In diesem Kapitel wird auf die Einrichtung der App „**ISEC7-Mail**“ auf einem Android-Smartphone beschrieben. Im Vergleich zu einem iPhone erfolgt die Konfiguration auf Android-Geräten in einer abweichenden Reihenfolge.

8.7.1 Einbinden des HARCIA-Zertifikat zur Identitäts- und Organisationsverifikation

In diesem Kapitel wird die Einbindung des HARCIA-Nutzerzertifikats in die ISEC7 Mail-App erläutert, sodass nach der Einrichtung des Hauptkontos der Empfang und Versand signierter sowie verschlüsselter E-Mails möglich ist.

8.7.2 Voraussetzung*:*

- Das persönliche HARICA-Nutzerzertifikat inklusive Passwort
- Die zugewiesene „ISEC7 Mail“-App über MDM auf Ihrem hochschulverwalteten Smartphone
- Laptop/PC und Zugriff auf Outlook und OWA

8.7.3 Import des HARCIA-Zertifikats in die „*ISEC7 Mail*“-App

1. Suchen Sie auf Ihrem Laptop bzw. Arbeitsgerät Ihr HARCIA-Nutzerzertifikat und senden Sie dieses per E-Mail an Ihre eigene E-Mail-Adresse.
2. Öffnen Sie die E-Mails in OWA und tippen Sie auf das angehängte Zertifikat und laden Sie dieses herunter.
3. Öffnen Sie die Einstellungen in der „ISEC7 Mail“-App, indem Sie auf die drei waagrechten Strichte (siehe Abbildung 134) und anschließend auf das Zahnrad-Symbol (siehe Abbildung 135) tippen.

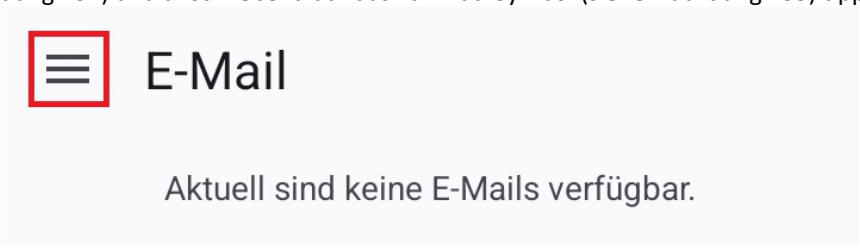

Abbildung 134 Ausschnitt aus der "ISEC7 Mail"-App ohne ein eingerichtetes E-Mail-Konto.

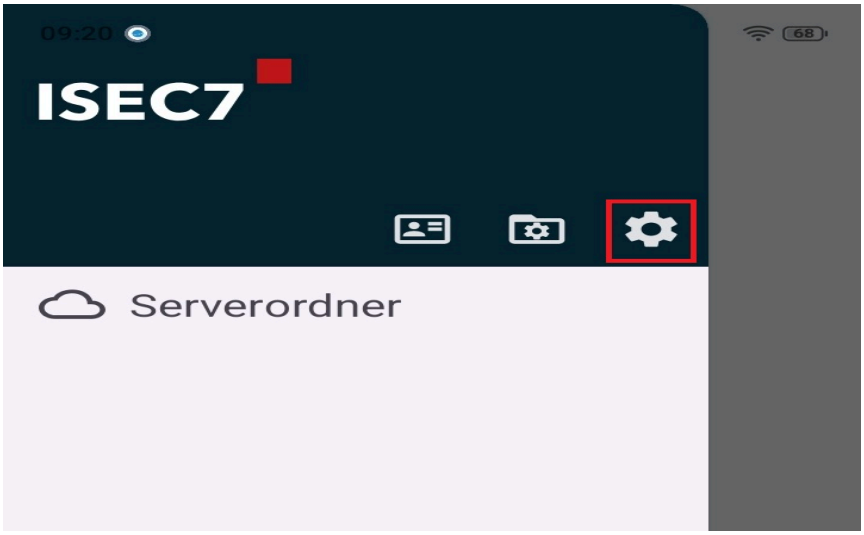

Abbildung 135 Ein weiterer Ausschnitt aus der Anwendung "ISEC7 Mail", der das Zahnrad zum Aufrufen der Einstellungen zeigt.

4. Wählen Sie im Menü „**Konfiguration**“ den Punkt „**Zertifikat**“ aus (siehe Abbildung)

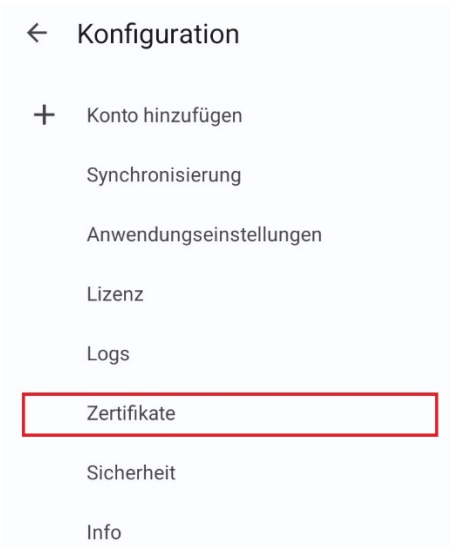

Abbildung 136 In den Einstellungen klicken Sie auf "Zertifikat".

5. Tippen Sie im Reiter „**Zertifikat**“ auf „**Zertifikatsbasierte Authentifizierung**“. Es öffnet sich die Ansicht „**Privater Schlüssel**“ (siehe Abbildung 137 und Abbildung 138).

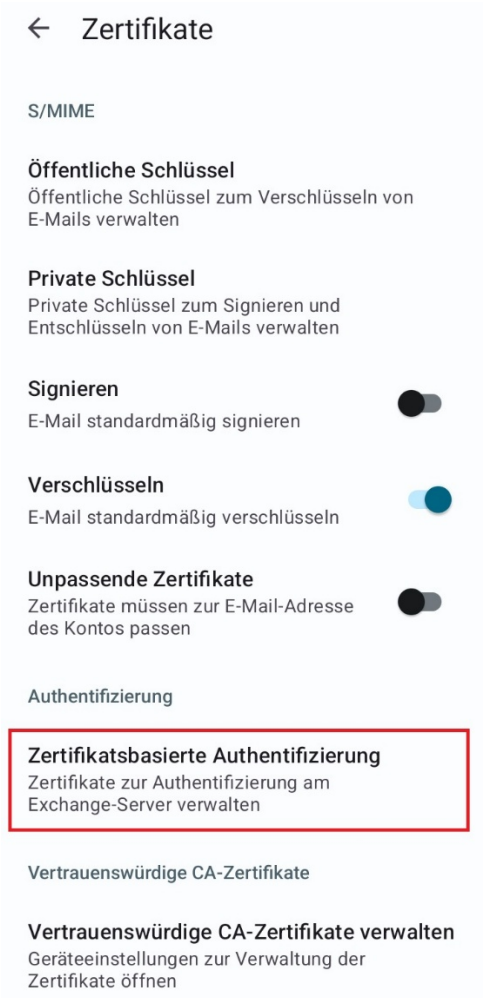

*Abbildung 137 Klicken Sie in den Einstellungen unter "**Zertifikat**" auf "**Zertifikatsbasierte Authentifizierung**", um dort das HARCIA-Identitätszertifikats hochzuladen.*

*Abbildung 138 Im Bereich „**Private Schlüssel**“ ist ersichtlich, dass bislang kein Zertifikat hinzugefügt wurde. Über das „+“-Symbol kann ein Zertifikat hinzugefügt werden.*

6. Tippen Sie auf das “**+**”-**Symbol**, um ein neues Zertifikat hinzuzufügen (siehe Abbildung 139).

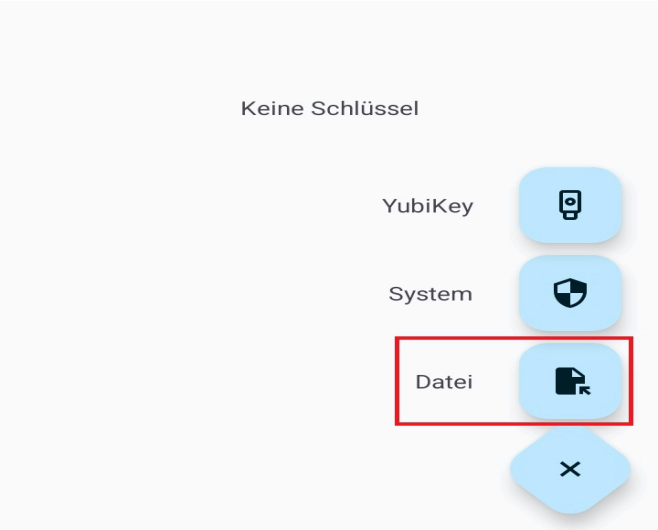

Abbildung 139 Im Bereich "Private Schlüssel" zeigt das "+"-Symbol drei Optionen zum hinzufügen des Identitätszertifikats. In dieser Anleitung wird die Option "Datei" beschrieben.

7. Wählen Sie die Option „**Datei**“ aus und navigieren Sie in den **Download-Ordner** (siehe Abbildungen 139 und 140).

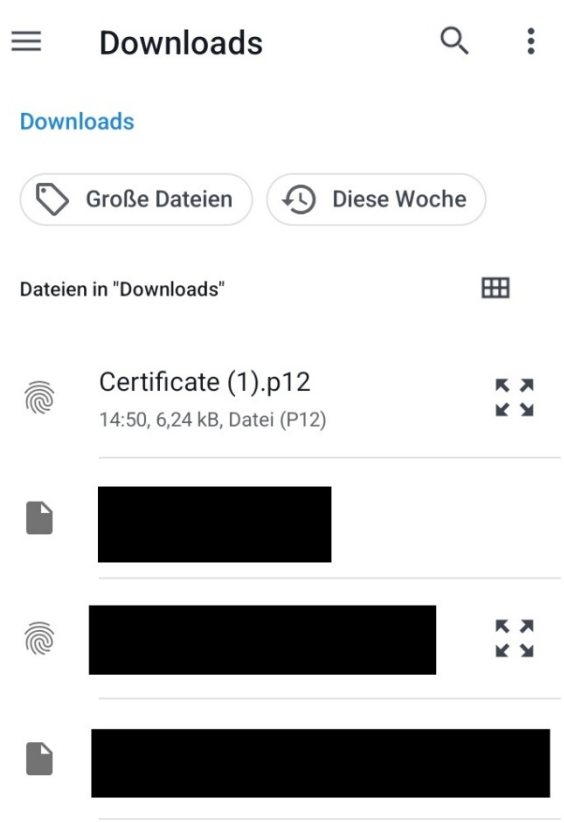

*Abbildung 140 Klicken Sie im „**Download**“-Ordner auf Ihr Identitätszertifikat, das in der Abbildung durch das Fingerabdruck-Symbol gekennzeichnet ist.*

8. Tippen sie auf Ihr **HARICA-Identitätszertifikat**. Geben Sie im erscheinenden Dialog des Zertifikat-Passwort ein und bestätigte Sie mit „**OK**“ (siehe Abbildung 141).

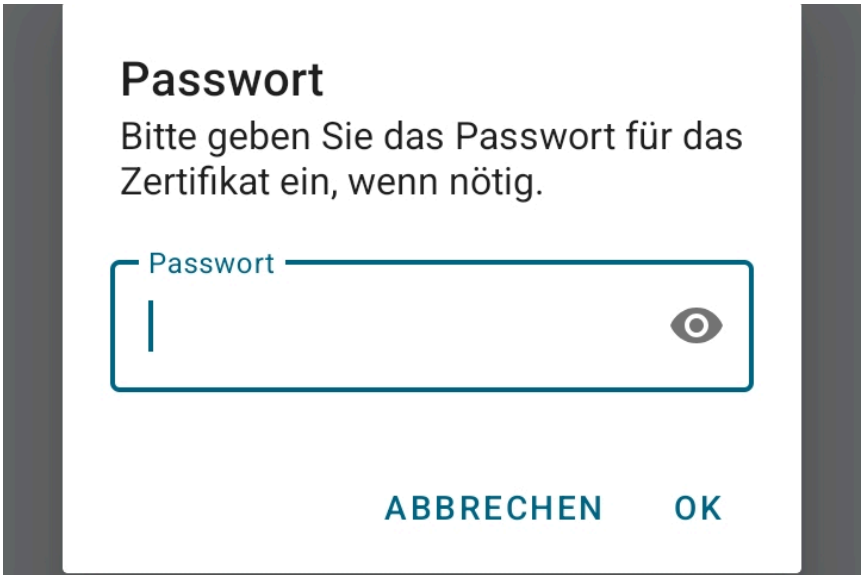

Abbildung 141 Geben sie hier das Passwort Ihres Identitätszertifikats ein und klicken Sie anschließend auf "OK", um das Zertifikat in die ISEC7 Mail-App einzubinden.

9. In der folgenden Ansicht werden die Zertifikatsdaten angezeigt. Tragen Sie im Feld „**Namen angeben**“ einen eindeutigen Namen (z.B. Vor- & Nachnamen) ein und tippen Sie auf „**Fortfahren**“ (siehe Abbildung 142).

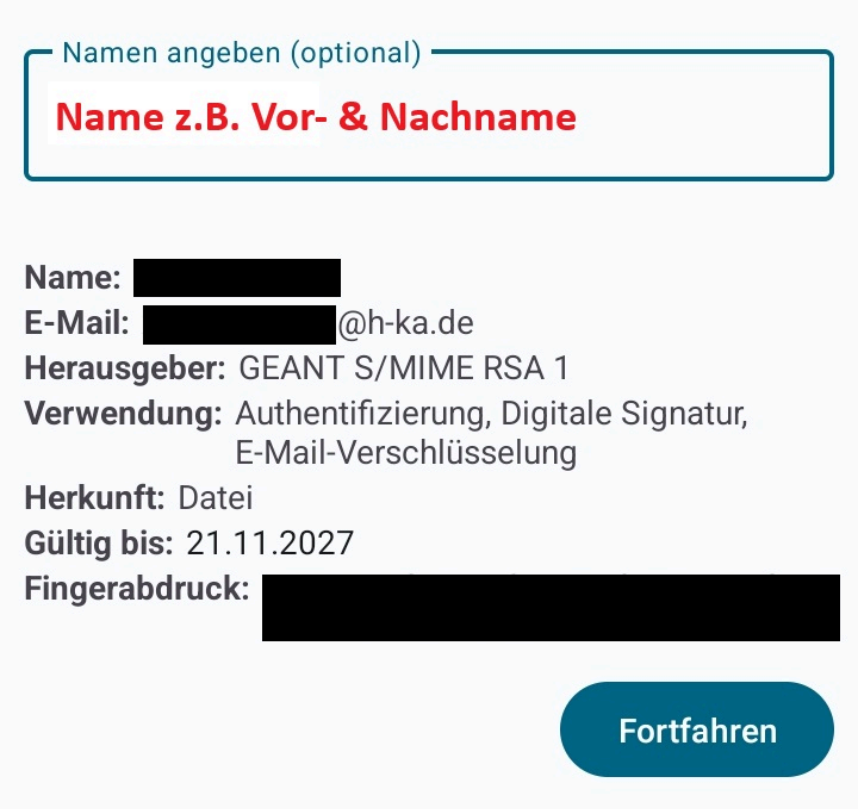

Abbildung 142 Hier weisen Sie dem hinzugefügten Zertifikat einen Namen zu, in diesem Beispiel den Vor- und Nachnamen.

10. Das Zertifikat wird nun im Fenster „**Privater Schlüssel**“ angezeigt (siehe Abbildung 143).

Abbildung 143 Das in der „ISEC7 Mail“-App eingebundene Zertifikat.

11. Navigieren Sie über den Pfeil oben links zurück zum Menü „**Zertifikate**“ und aktivieren Sie die Optionen „**Signieren**“ und „**Verschlüsseln**“ (siehe Abbildung 144).

Abbildung 144 Aktivieren Sie im Bereich "Zertifikat" auf die Punkte "Signieren" und "Verschlüsseln" über die beiden Regler.

12. Kehren Sie anschließend über den Pfeil oben links in die Einstellungen zurück.

8.7.4 Einrichten des Hauptkontos

In diesem Kapitel wird erläutert, wie das Hauptkonto in der ISEC7 Mail-App auf einem Android-Gerät Schritt für Schritt eingerichtet wird.

1. Öffnen Sie die Einstellungen der App, indem Sie auf die drei waagrechten Striche (siehe Abbildungen 134) und anschließend auf das Zahnrad-Symbol (siehe Abbildung 135) tippen.
2. Tippen Sie in den Einstellungen auf „**Konto hinzufügen**“ (siehe Abbildung 145).

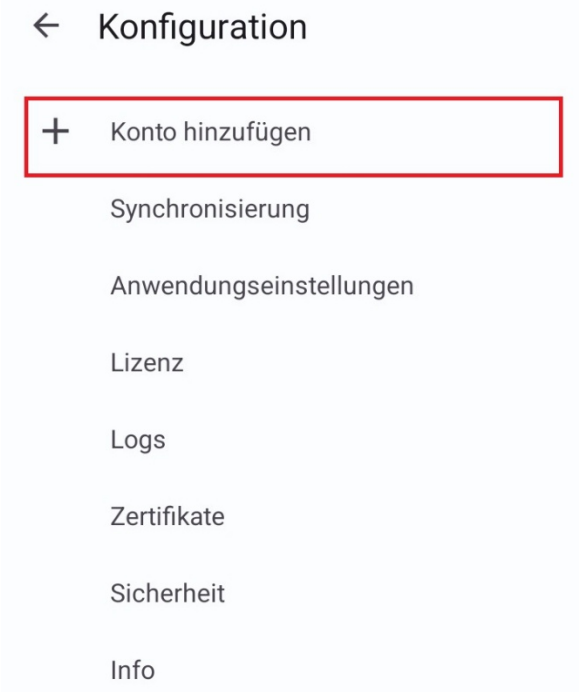

Abbildung 145 Darstellung der Einstellungen der „ISEC7 Mail“-App mit der markierten Funktion „Konto hinzufügen“ zum Einrichten eines E-Mail-Kontos.

3. Geben Sie die folgenden Daten ein (siehe Abbildung 146):

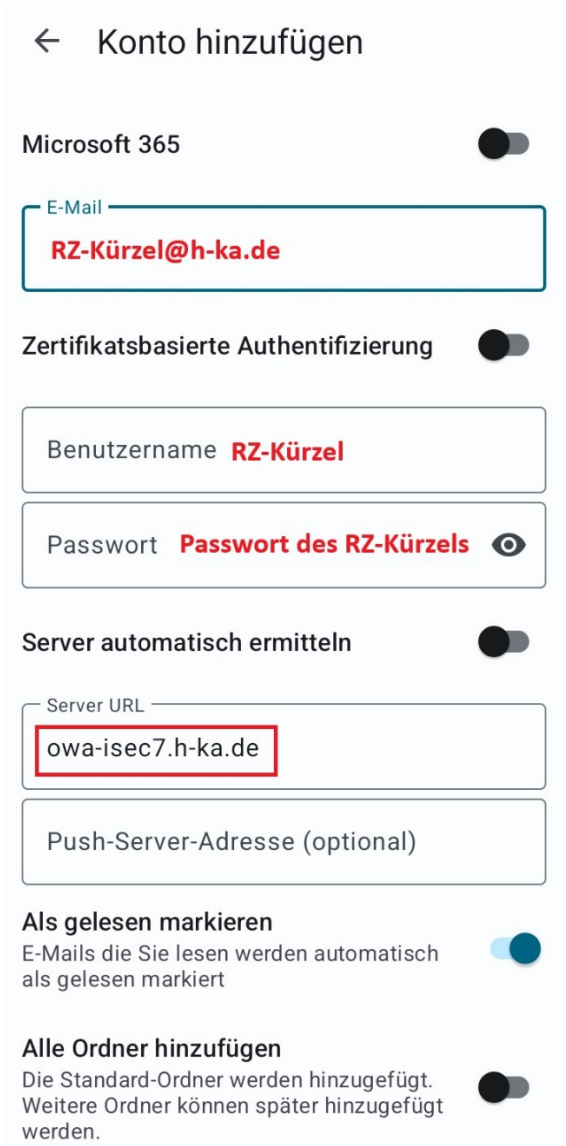

Abbildung 146 Eingabefenster der App ‚ISEC7 Mail' zum Hinzufügen eines Kontos.

- **E-Mail:** Ihre Hochschul-E-Mail-Adresse
- **Benutzername:** Ihr RZ-Kürzel
- **Passwort:** Das Passwort Ihres RZ-Kürzels
- **Server URL:** owa-isec7.h-ka.de (muss eingetragen sein)

4. Scrollen Sie nach dem Ausfüllen aller Felder nach unten und tippen Sie auf „Weiter".

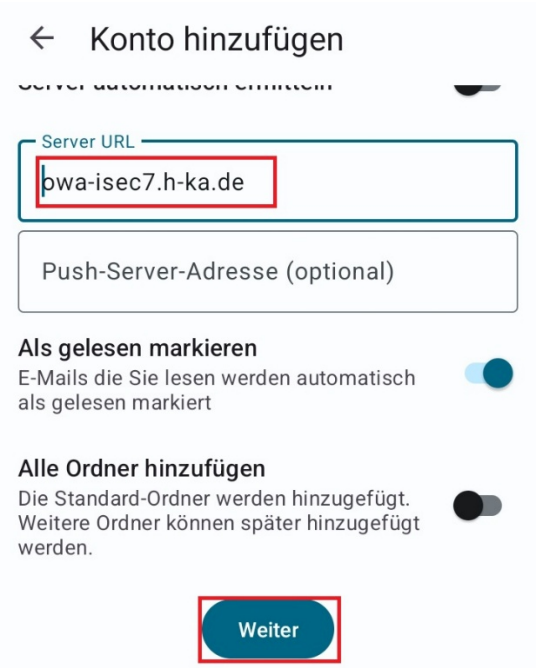

Abbildung 147 Als Server-URL ist owa-isec7.h-ka.de einzutragen. Über die Schaltfläche ‚Weiter' werden die Eingaben bestätigt und gespeichert.

5. Es erscheint ein kleiner Ladekreis, und nach einem kurzen Moment wird Ihnen die Schaltfläche „**Speichern**" (**rote 2**) angezeigt. Darunter sehen Sie fünf Menüpunkte (**roter Kasten mit roten 1**) mit Häkchen und Reglern, die Sie aktivieren können. Es ist wichtig, dass der Menüpunkt-„E-Mail" aktiviert wird, damit Ihre E-Mails geladen werden. Die restlichen Punkte können Sie selbst entscheiden oder zu einem späteren Zeitpunkt aktivieren (siehe Abbildung 147).

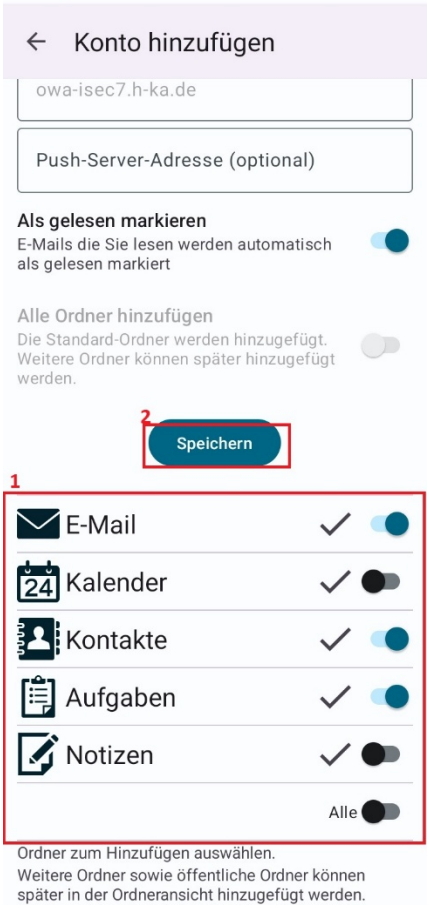

*Abbildung 148 Um das E-Mail-Konto einzurichten, muss der Regler für E-Mails aktiviert werden. Empfehlung: Aktivieren Sie die Regler für E-Mails, Kalender und Kontakte. Vergessen Sie nicht, auf „**Speichern**" zu klicken, um die Einrichtung des E-Mail-Kontos abzuschließen*

6. Anschließend werden Sie zu den Einstellungen zurückgeleitet. Es erscheint eine kurze Pop-up-Meldung „**Konto wurde hinzugefügt**". In den Einstellungen wird das neu hinzugefügte E-Mail-Konto oben angezeigt (siehe Abbildung 149).

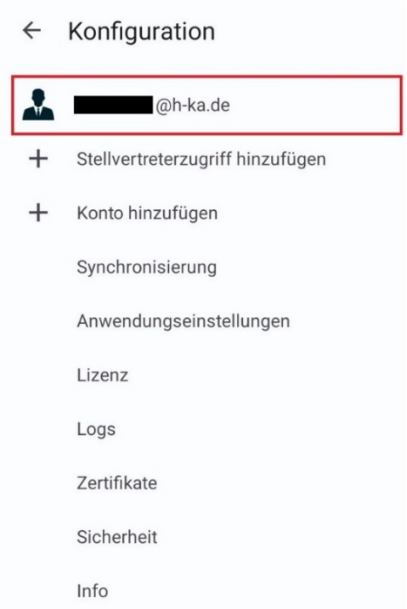

Abbildung 149 Die Einstellungen und das hinzugefügte Konto (rot markiert).

7. Nun können Sie mit ISEC7-Mail-App Ihre E-Mails lesen, senden und empfangen.

8.7.5 Erstellen einer E-Mail-Signatur „*ISEC7 Mail*“-App

In diesem Abschnitt wird beschrieben, wie eine E-Mail-Signatur erstellt wird.

1. Öffnen sie die Einstellungen in der App.
2. Wählen Sie Ihr E-Mail-Konto (**RZ-Kürzel@h-ka.de**) aus (siehe Abbildung 150).

Abbildung 150 Fokus auf das eingefügte Hauptkonto in den ISEC7-Mail-Einstellungen. Klicken Sie auf das Konto, um die zugehörigen Einstellungen zu bearbeiten.

3. Scrollen Sie zum Abschnitt „**Konto**“ und tippen Sie auf „**Signaturen**“.

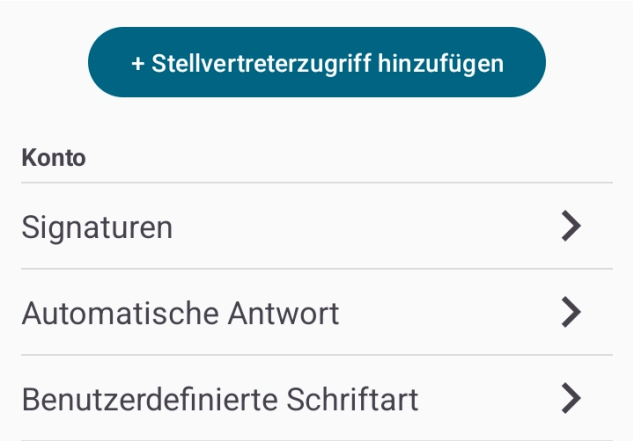

Abbildung 151 In den Einstellungen unter „Konto editieren“ finden Sie unten den Punkt „Signaturen“. Hier können Sie Ihre E-Mail-Signaturen erstellen, die automatisch bei jeder neuen E-Mail oder Antwort verwendet werden.

4. Tippen sie auf das **„+“-Symbol**, um eine neue Signatur zu erstellen.
5. Erfassen Sie die Signaturdaten gemäß folgender Struktur:

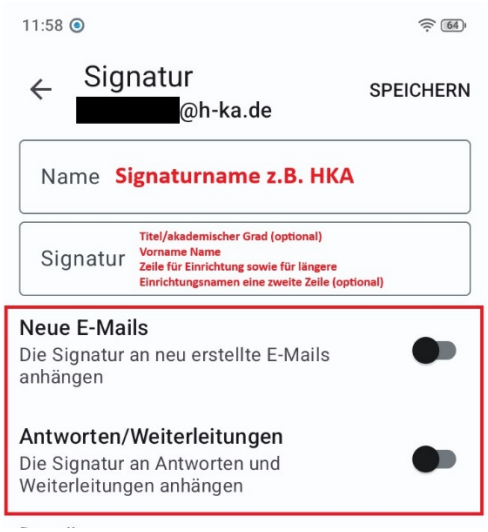

Abbildung 152 Unter „Signatur“ lässt sich eine E-Mail-Signatur gemäß dem Corporate Design der Hochschule erstellen. Zudem können Sie die Regler für „Neue E-Mails“ und „Antworten/Weiterleitungen“ aktivieren, damit die erstellten Signaturen automatisch verwendet werden.

- **Name:** Bezeichnung der Signatur
- **Signatur(-inhalt)** (Beispiel Hochschule Karlsruhe)
  - Titel/akademischer Grad (optional)
  - Vorname Nachname
  - Organisationseinheit
    (bei längeren Bezeichnungen optional zweite Zeile)

6. Aktivieren Sie die Optionen „**Neue E-Mails**“ sowie „**Antworten/Weiterleitungen**“, um die Signatur standardmäßig zu verwenden (siehe Abbildung 152)
7. Speichern Sie die Signatur über „**Speichern**“ (oben rechts).
8. Navigieren Sie über den Pfeil oben links zurück in die **Einstellungen**.

8.7.6 Verwenden der E-Mail-Signatur „*ISEC7 Mail*“-App

In diesem Abschnitt wird beschrieben, wie Sie die Signatur in der Android-Version von ISEC7 Mail verwenden können.

1. Tippen Sie in der **ISEC7 Mail-App** auf das **Stift-Symbol** (unten rechts), um eine neue E-Mail zu verfassen (siehe Abbildung 153).

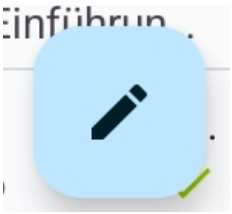

Abbildung 153 Tippen Sie auf das Stift-Symbol, um in der „ISEC7 Mail“-App eine neue E-Mail zu verfassen.

2. Die ausgewählte Signatur wird automatisch in die E-Mail eingefügt.

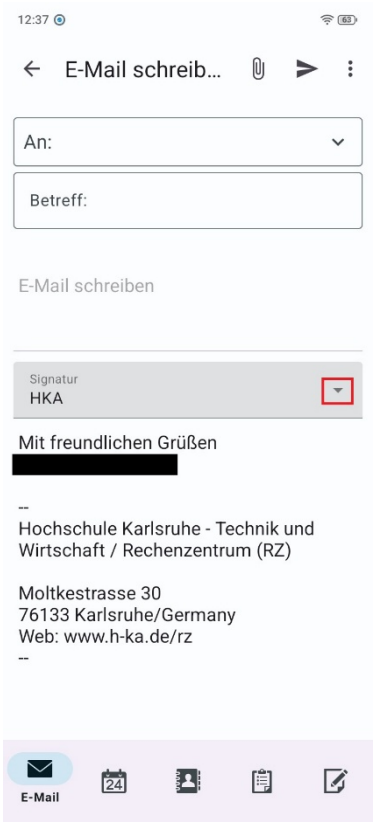

Abbildung 154 Das Layout einer neuen E-Mail mit der Signatur „HKA“. Über die nach unten zeigendem Pfeil können Sie zwischen den verfügbaren Signaturen auswählen. Ein Klick auf die gewünschte Signatur zeigt diese in der E-Mail an.

3. Über das Dropdown-Menü (Pfeilsymbol) können bei Bedarf alternative Signaturen ausgewählt werden (siehe Abbildung 20).
4. Verfassen und versenden Sie die E-Mail wie gewohnt.

9 Adobe Creative Cloud

Für Beschäftigte: Im Software-Center Ihres Arbeitsplatz-Rechners liegt die Anwendung **Adobe Creative Cloud Desktop Applikation** ab.

9.1 Zum Öffnen der Applikation klicken Sie **Adobe Creative Cloud Desktop App** an und wählen den Button **Installieren**.

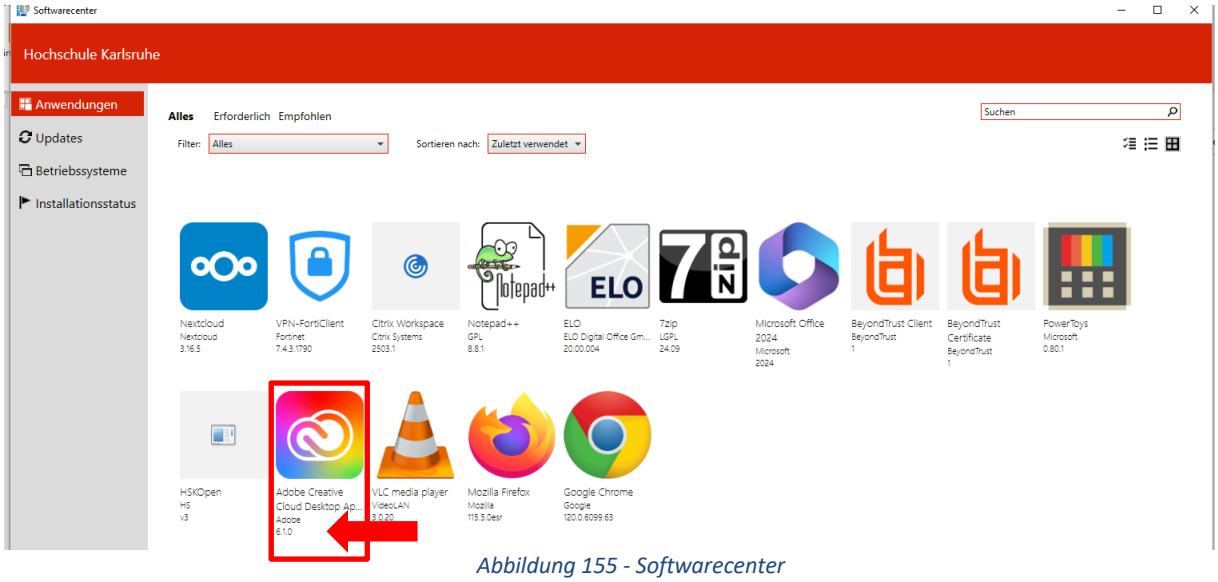

Abbildung 155 - Softwarecenter

Abbildung 156 - Button zum Installieren

9.2 Sobald **Adobe Creative Cloud** installiert ist, finden Sie **Adobe Creative Cloud** über die Windows-Suchfunktion.

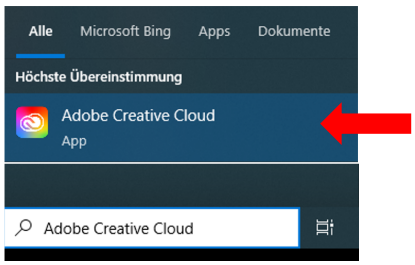

Abbildung 157 - Windows-Suchfunktion

9.3 Zum Anmelden bei **Adobe Creative Cloud** geben Sie bei E-Mail-Adresse **RZ-Benutzerkürzel@hs-karlsruhe.de** ein und wählen Sie den Button **Weiter**.
WICHTIG: Der Mail-Domain-Name muss **@hs-karlsruhe.de** lauten.

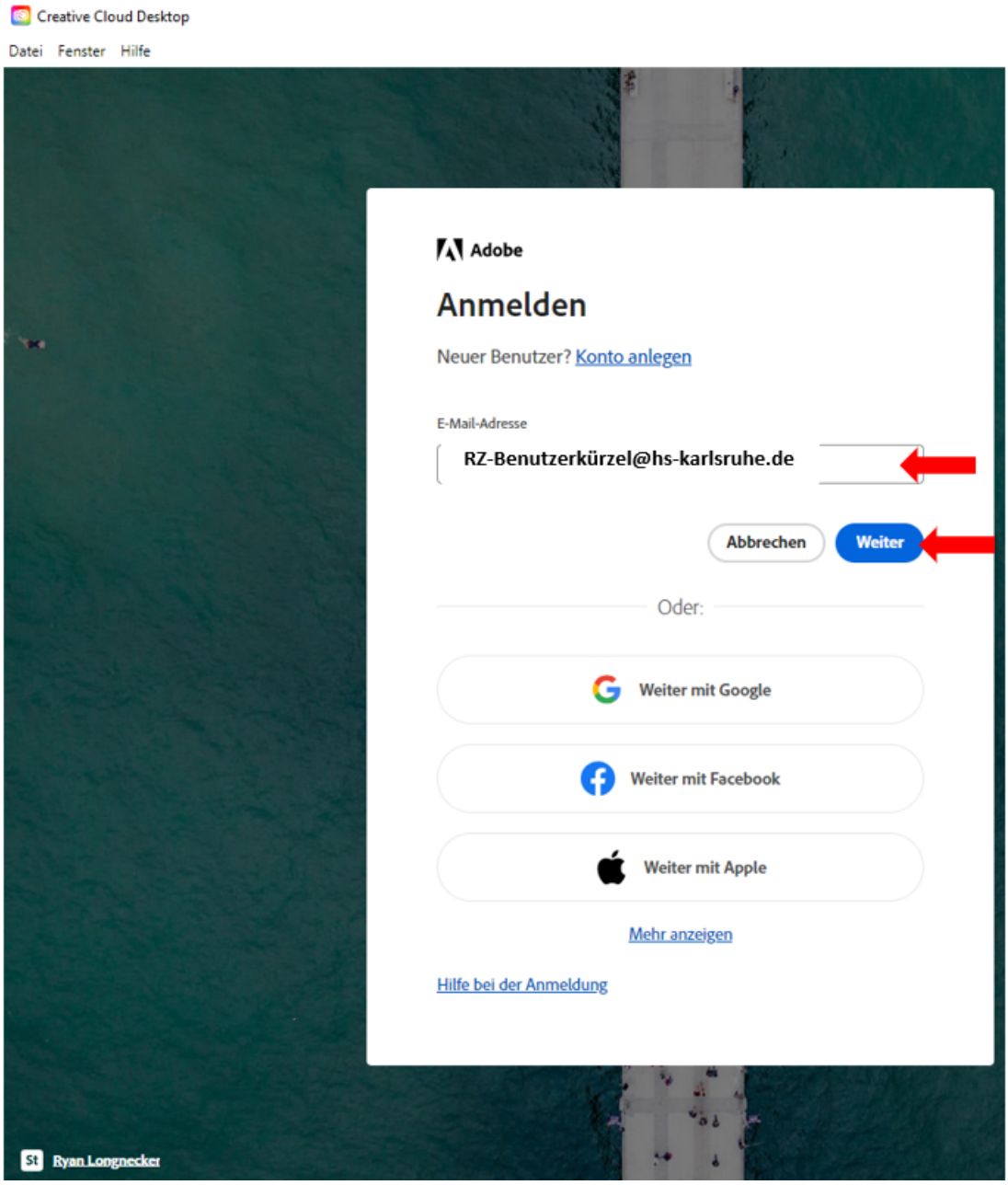

*Abbildung 158 - Anmeldung bei Adobe mit dem Domain-Name **hs-karlsruhe.de***

9.4 Es öffnet sich die Shibboleth-Anmeldung und Sie geben bei **Benutzername** Ihr RZ-Benutzerkürzel ein und bei **Passwort** Ihr RZ-Passwort und wählen den Button **Anmelden**.

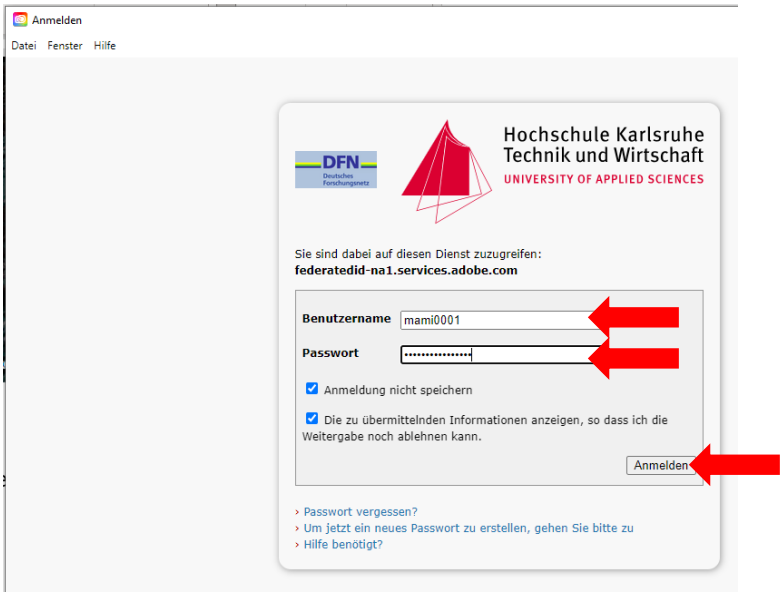

Abbildung 159 - Anmeldung bei Adobe über Shibboleth

9.5 Bestätigen Sie die Nutzungsbedingungen, indem Sie auf den Button **Akzeptieren** klicken.

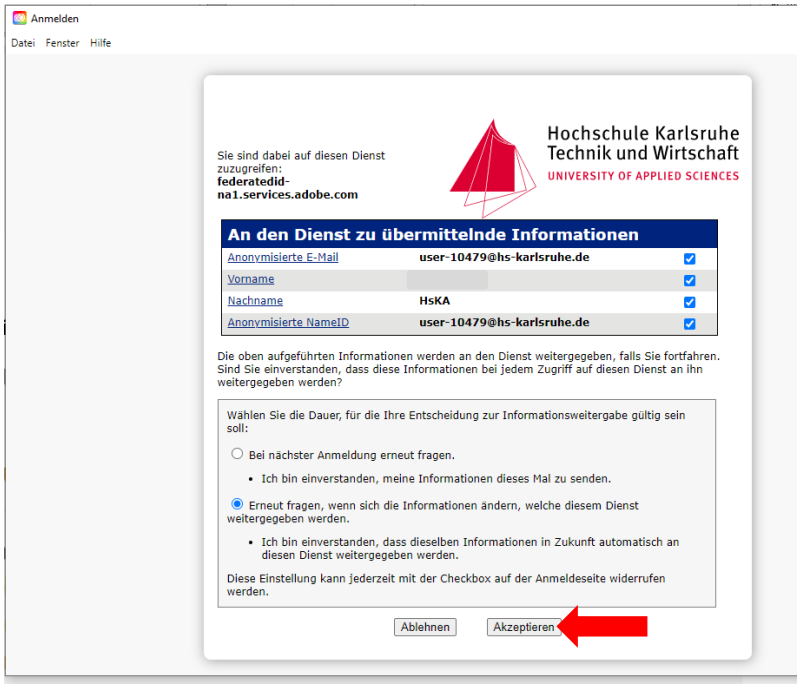

Abbildung 160 - Nutzungsbedingungen

9.6 Bei einer erfolgreichen, anonymisierten Anmeldung ist nicht Ihre Hochschulmail-Adresse enthalten.

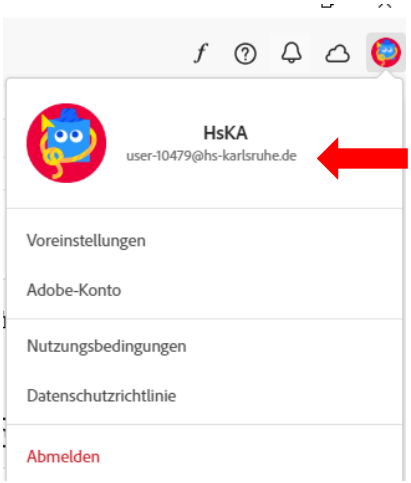

Abbildung 161 - Anonyme Adresse

9.7 Wählen Sie im Seitenregister **Applikationen** aus und es stehen Ihnen die Adobe Produkte zum Installieren bereit, bspw. Adobe Acrobat. Klicken Sie bei den gewünschten Adobe Produkten auf **Installieren**.

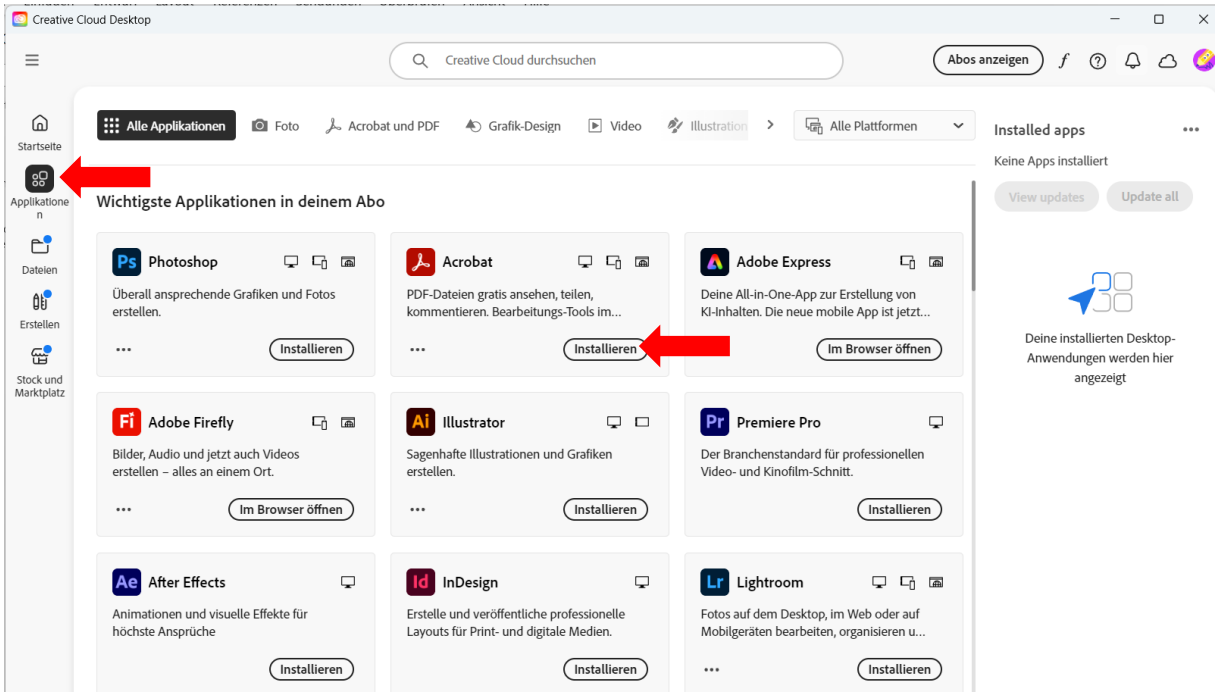

Abbildung 162 - Adobe Produkte

9.8 Nach der Installation sehen Sie im rechten Seitenregister die installierten Adobe Produkte.

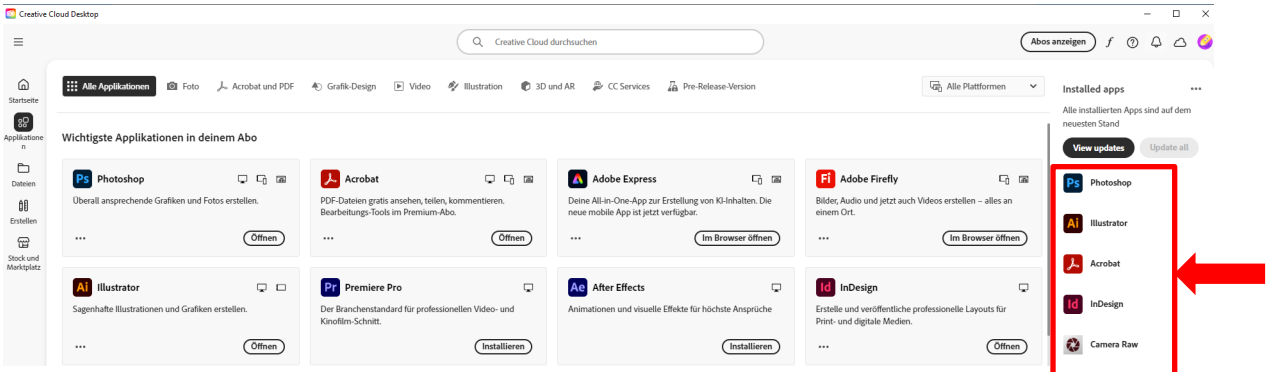

Abbildung 163 - Installierte Adobe Produkte

9.9 Damit ggf. auch ältere Versionen zur Verfügung stehen, klicken Sie auf das Sandwich-Menu, wählen **Datei** aus und dann **Voreinstellungen.**

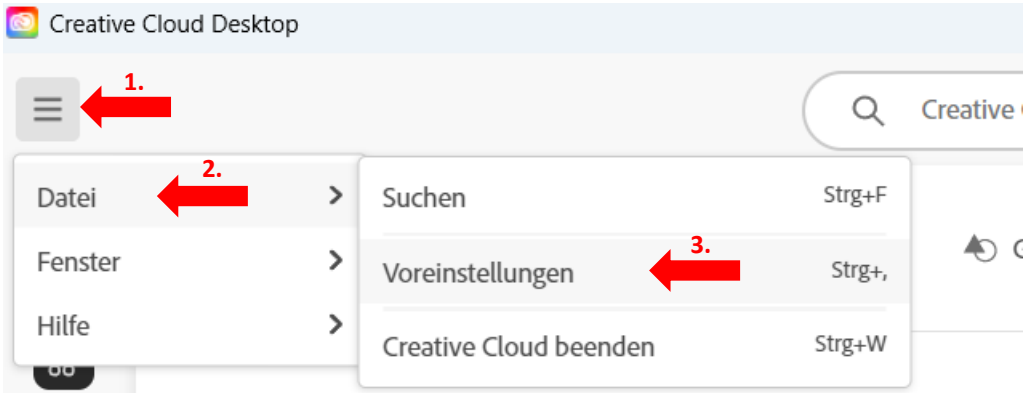

Abbildung 164 - Voreinstellungen für ältere Versionen

9.10 Wählen Sie **Applikationen** aus und gehen Sie auf **Erweiterte Optionen**. Entfernen Sie den Haken bei **Ältere Versionen entfernen** und klicken Sie auf den Button **Fertig**. Somit stehen Ihnen zukünftig auch ältere Versionen zur Auswahl zur Verfügung.

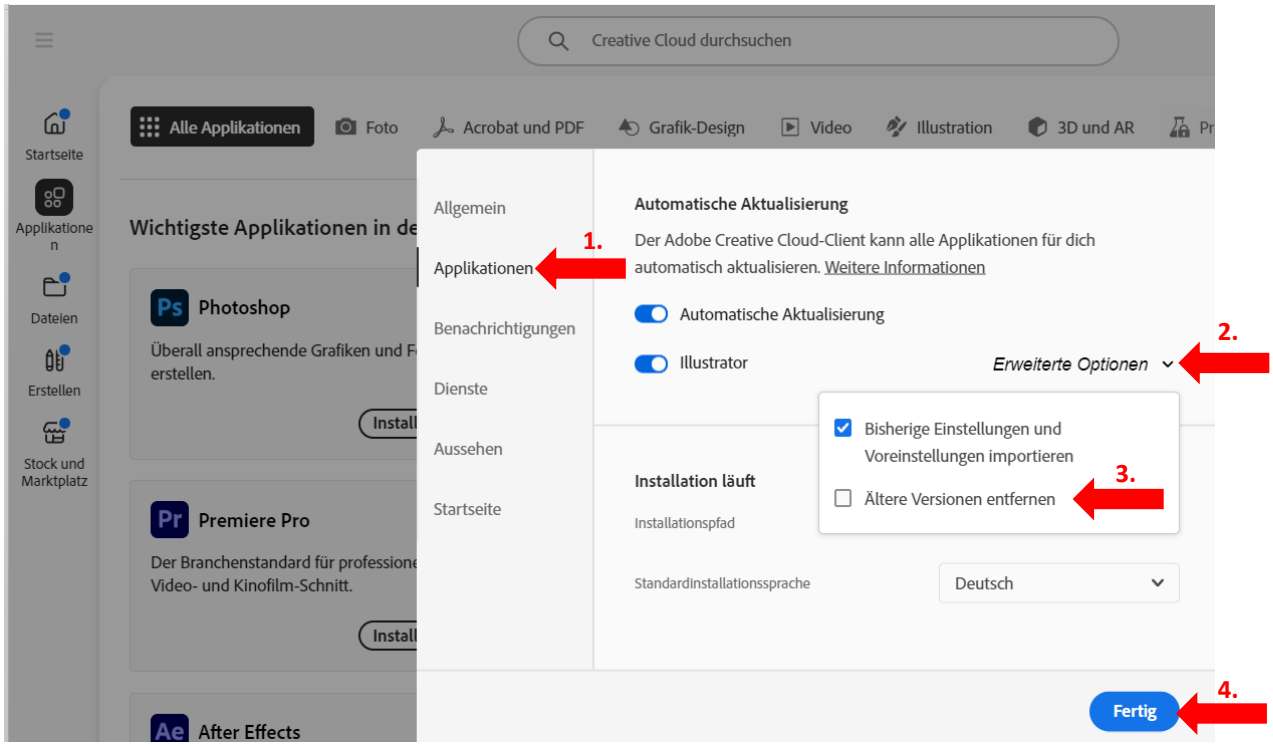

Abbildung 165 - Haken prüfen

10 Collaborationswerkzeuge

10.1 Zoom

Der Dienst Zoom Meeting ist ein virtuelles Videokonferenz und wird an der Hochschule als Ergänzung zu BigBlueButton für die Online-Lehre bereitgestellt. Die Voreinstellungen wurden so gewählt, dass der Datenschutz bei der Nutzung gewährt bleibt. Für das Erstellen von Räumen ist ein Account nötig.

10.1.1 Registrierung?

Folgende Personengruppe wie Professoren/-innen, Lehrbeauftragte erhalten einen Zoom-Account.

Wie kann ich den Account beantragen?
Damit die Lehrenden einen Zoom-Account erhalten, schicken diese eine Mail an die Benutzerberatung.
Mailadresse: bb.rz@h-ka.de

Kann ich als Student*in einen Zoom Account bekommen?
Studierende können Zoom-Lizenzen erhalten, wenn sie für die Hochschule tätig sind, z. B. als Tutor*innen oder in der Fachschaft. Falls dies auf Sie zutrifft, benötigt die Benutzerberatung eine kurze Begründung, in der Sie angeben, für wen Sie an der Hochschule Karlsruhe arbeiten. Bitte setzen Sie die für die Veranstaltung verantwortliche Person in CC dieser E-Mail.

Wie ist ein Zoom-Account aufgebaut?
Der Zoom-Account wird ausschließlich der HKA E-Mailadresse <vorname.nachname@h-ka.de> zugewiesen.

Wie kann ich mein Passwort für Zoom ändern?
Falls Sie Ihr Zoom-Passwort vergessen haben, können Sie die **„Kennwort vergessen“** Funktion nutzen unter https://h-ka-de.zoom.us nutzen.
Das neue Passwort kommt in Ihrem HKA-Posteingang (HKA-Mailadresse = Zoom-Benutzername) an.

10.1.2 Wie erstelle ich ein Meeting in Zoom?

1. Bei Zoom anmelden:

   Melden Sie sich bei Zoom https://h-ka-de.zoom.us an. Klicken Sie anschließend auf das Personensymbol, wodurch Ihr persönliches Profil geöffnet wird. Hier können Sie Ihr Profil um zusätzliche Daten erweitern.

Abbildung 166 - Menüleiste von Zoom. Zeitplan (Rot markiert).

2. Meeting erstellen:

   Auf der linken Seite finden Sie das Menü. Der zweite Menüpunkt ist „Meetings“. Dieser unterteilt sich in folgende Kategorien:
   - Bevorstehende
   - Vorherige
   - Privater Raum
   - Meetingvorlagen
   - Umfragen/Quiz

Bei „Bevorstehend“ können Sie auf die blaue Schaltfläche „+ Ein Meeting planen“ klicken, um ein neues Meeting zu erstellen.

Alternative Möglichkeit:
Eine weitere Möglichkeit, ein Meeting zu planen, ist die Verlinkung „Zeitplan“.

3. Besprechung planen:

   Nach dem Klicken auf „+ Ein Meeting planen“ öffnet sich eine neue Eingabemaske mit dem Titel „Besprechung planen“. In diesem Fenster können Sie folgende Angaben festlegen:

   - Thema: (Name des Meetings)
   - Beschreibung: (optional)
   - Wann: Datumsangabe samt Uhrzeit (unterteilt in AM für Vormittag und PM für Nachmittag/Abend)
   - Dauer (in Stundenangaben)
   - Zeitzone
   - Wiederkehrendes Meeting: Setzen Sie ein Häkchen, wenn das Meeting regelmäßig stattfinden soll.
   - Eingeladene: Geben Sie die Teilnehmer anhand ihrer HKA-Mailadresse ein.
   - Registrierung: Haken setzen, wenn eine Registrierung erforderlich ist.
   - Meeting-ID:
     - Entweder „Automatisch erzeugen“ oder
     - „Personal-Meeting-ID XXX XXX XXXX“ verwenden.
   - Vorlage: Falls Sie bereits Vorlagen erstellt haben.
   - Whiteboard: Klicken Sie auf „Whiteboard hinzufügen“, wenn Sie ein Whiteboard für das Meeting benötigen.

4. Speichern:
   Sobald alle erforderlichen Daten eingetragen sind, klicken Sie auf „Speichern“.

5. Link teilen:

   Nachdem das Meeting erstellt wurde, können Sie den Link zum Zoom-Meeting in ILIAS hinterlegen, entweder als eigenständige Verlinkung (externe Verlinkung) oder innerhalb einer Veranstaltung, die in ILIAS mit allen relevanten Informationen zur Veranstaltung erstellt wird.

10.2 BigBlueButton

BigBlueButton (kurz: BBB) ist eine Open-Source-Web-Konferenzplattform, die an der Hochschule Karlsruhe für die Live-Online-Lehre eingesetzt wird. Diese Plattform ermöglicht es, Audio, Video, Chat und Bildschirm in Echtzeit mit anderen zu teilen. BBB benötigt keine zusätzliche Software und läuft vollständig im Browser.

10.2.1 Registrierung

Die Erstellung von Meetings, im BBB-Jargon „Räumen“, ist nur für registrierte Nutzende möglich. Registrieren Sie sich über den folgenden Link:

https://online-leh.re/

Bitte verwenden Sie bei der Registrierung Ihre Hochschul-E-Mail-Adresse. Die Freischaltung erfolgt durch die Benutzerberatung des Rechenzentrums.

10.2.2 **Nutzung**

Nach der Freischaltung und Anmeldung bei BigBlueButton erscheint die Startseite der Plattform. Dort können Sie sofort einen eigenen Raum, d.h. ein neues Meeting, erstellen.

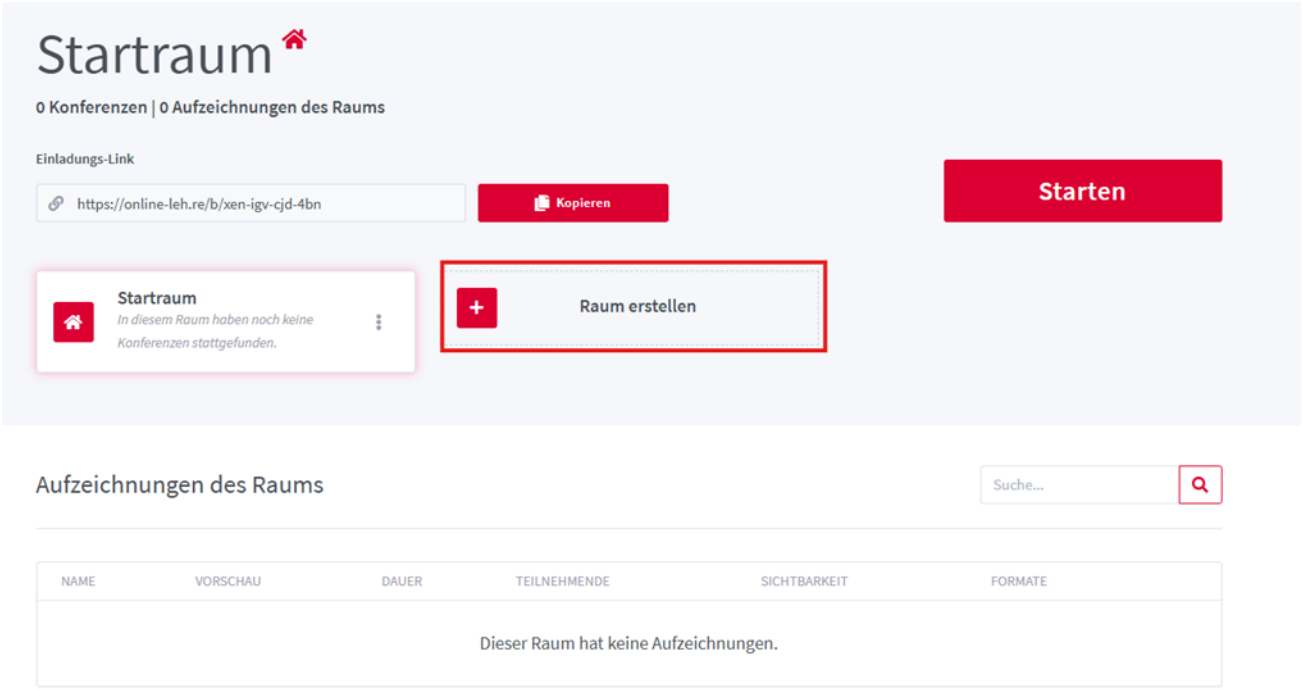

Abbildung 167 - Startseite: Raum erstellen

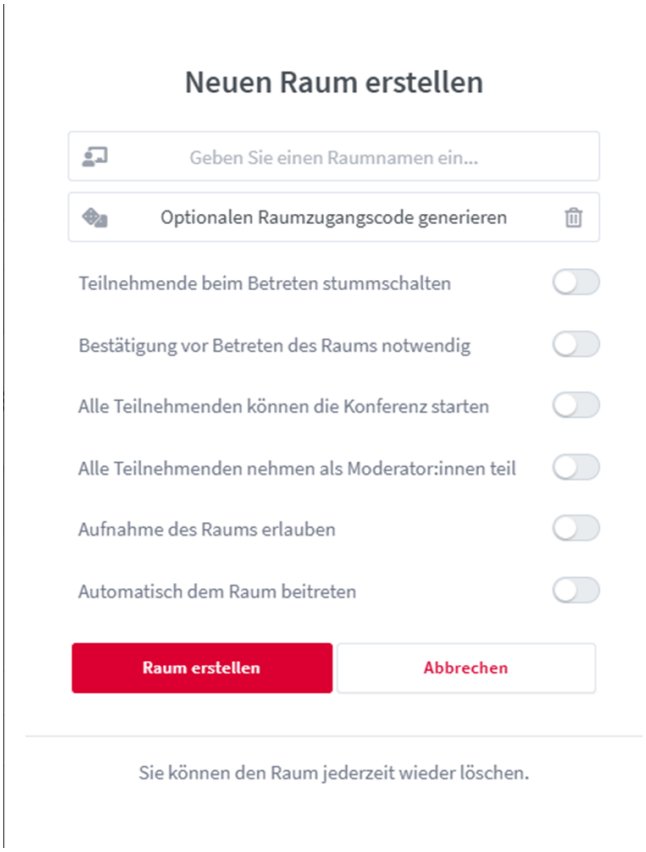

Abbildung 168 - Fenster "Neuen Raum erstellen"

Nachdem Sie einen Raum erstellt haben, können Sie die Raumeinstellungen jederzeit ändern, indem Sie auf die drei Punkte rechts neben dem Raum klicken (siehe Abbildung 169). In den Einstellungen können Sie den Teilnehmenden verschiedene Rechte zuweisen.

Wenn Sie möchten, dass die Teilnehmenden unabhängig vom Initiator im Raum arbeiten können, können Sie hier die entsprechenden Zugangs- und Moderationsrechte aktivieren. Nachdem Sie Ihre Aus-wahl getroffen haben, klicken Sie auf den roten Button „Raum erstellen“, um den Raum zu erstellen. Der Raum bleibt nach Beendigung der Konferenz erhalten und kann für weitere Videochats genutzt werden.

Abbildung 169 - Ändern der Einstellungen des Online-Konferenzraum sind möglich.

Einen Raum starten

Nachdem Sie den Raum erstellt haben, erscheint er neben Ihrem Startraum und kann jederzeit durch Anklicken aktiviert und über den roten Button „Starten“ gestartet werden.

Teilnehmende einladen

Der erzeugte Link zur Konferenz kann an die Teilnehmenden über das „Kopieren“-Feld verschickt werden. Zum Beispiel können Sie den Link zu BBB-Räumen in ILIAS-Veranstaltungen einbinden oder als externen Link in ILIAS bereitstellen.
Die Konferenz startet erst, wenn der Moderator oder die Moderatorin den Raum betritt.

Rollen in BigBlueButton

In BBB gibt es mehrere Rollen:

- Rolle **„Präsentator“**
  Die Präsentationsfläche kann nur von einer Person mit der Rolle des Präsentators/der Präsentatorin (blaues Fenster-Icon) gesteuert werden. Präsentatoren können Präsentationen hochladen und Bildschirme teilen.

- Rolle **„Moderator“** (Kennzeichnung durch ein Quadrat)
  Es können mehrere Personen die Rolle des Moderators oder der Moderatorin zugewiesen bekommen. Z.B. kann beim Anlegen des Online-Raums jeder eingeladene Teilnehmer der Rolle Moderator zugewiesen werden.

- Rolle **„Zuhörer*innen“** (Kennzeichnung durch einen Kreis)
  Weitere Einstellungen zu den Teilnehmenden können über die Einstellungen vorgenommen werden.

Weitere Funktionen gibt es noch in BBB:

- **Erstellung von Breakout-Rooms (Gruppenräumen):**
  In BBB können Breakout-Rooms mit einer festgelegten Teilnehmeranzahl und einer definierten Dauer eingerichtet werden.
- **Audioaufnahme der Konferenz:**
  Während der Konferenz kann eine Audioaufnahme gestartet werden, um die Sitzung für spätere Zwecke zu dokumentieren.
- **Hochladen von Präsentationen:**
  Präsentationen können während der Sitzung hochgeladen werden, um sie mit den Teilnehmenden zu teilen.
- **Verändern des Layouts:**
  Das Layout der Konferenz kann nach Bedarf angepasst werden, um den spezifischen Anforderungen der Sitzung gerecht zu werden.

11 bwSync&Share

11.1 Was ist bwSync&Share

Bei bwSync&Share handelt es sich um einen Online-Speicherdienst für Mitarbeiterinnen und Mitarbeiter sowie Studierende der Universitäten und Hochschulen in Baden-Württemberg. Der Dienst wird seit dem 01. Januar 2014 am Karlsruher Institut für Technologie (KIT) betrieben und im Rahmen der DFN-Cloud aus den Mitgliedern des DFN-Vereins angeboten. Seit 2021 steht bwSync&Share zudem im Rahmen der Helmholtz Cloud auch den Angehörigen der Helmholtz-Zentren zur Verfügung.
Jedem Hochschulmitglied stehen 50 GB Speicherkapazität zur Verfügung, die für das sichere Speichern, Synchronisieren und Teilen von Daten genutzt werden können.

11.2 Anmeldung bei bwSync&Share

Um sich beim Online-Dienst bwSync&Share anzumelden, gehen Sie wie folgt vor:
Link: https://bwsyncandshare.kit.edu/

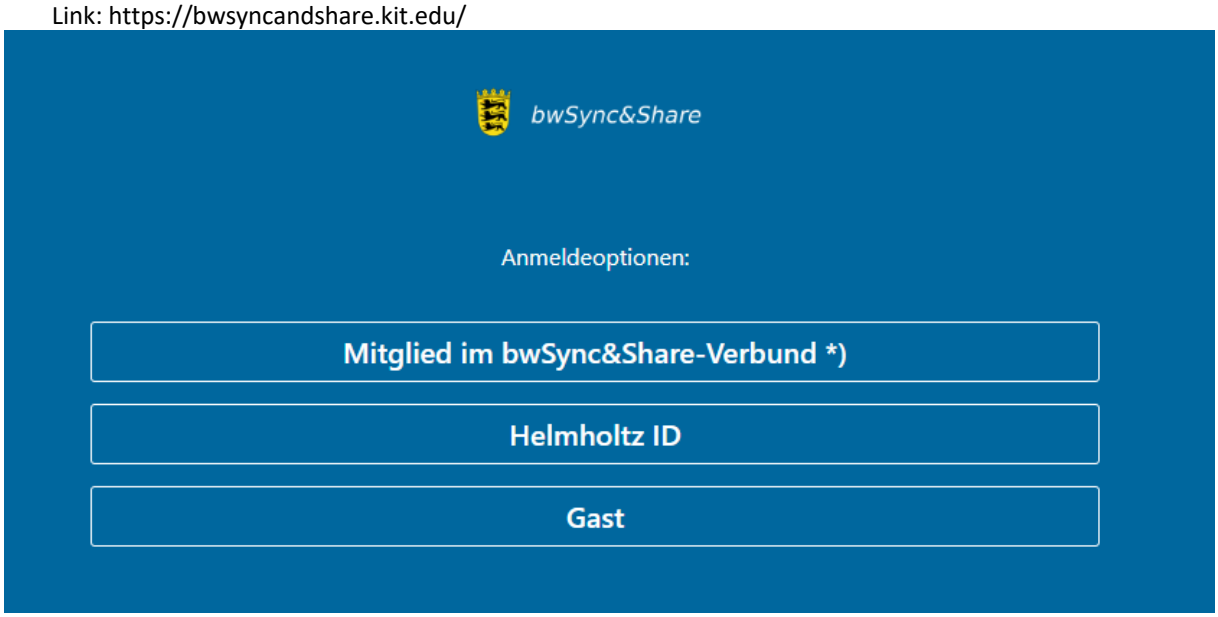

Abbildung 170 - Das Anmeldefenster bei bwSync&Share.

1. Klicken Sie auf „***Mitglied im bwSync&Share-Verbund *)***“

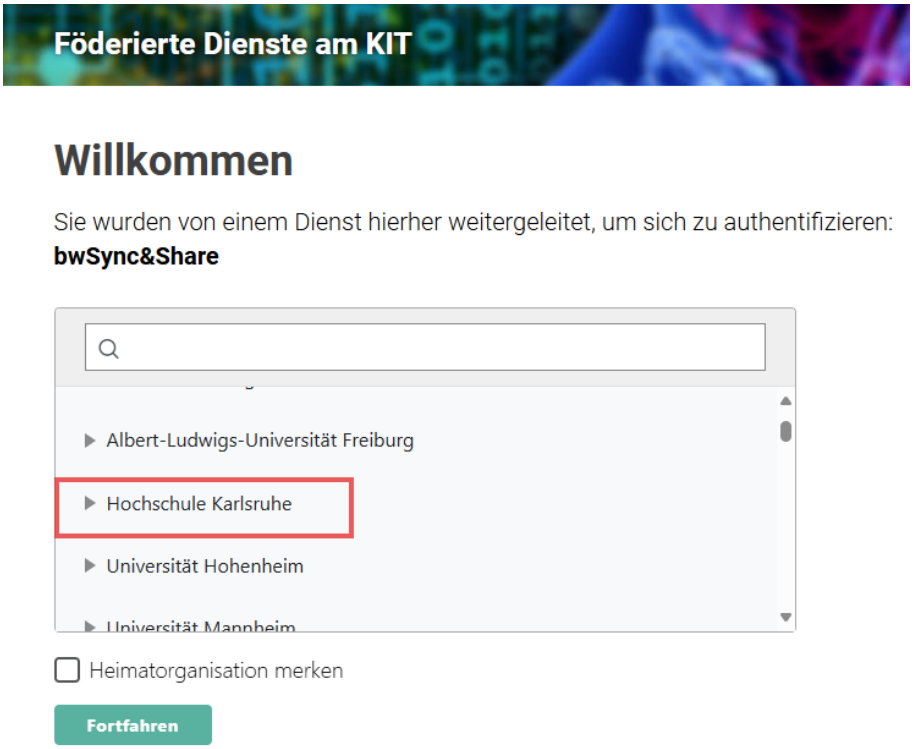

Abbildung 171 - Die Hochschule Karlsruhe als Heimatorganisation raussuchen.

2. Wählen Sie Ihre Heimatorganisation aus:

   - Geben Sie im Suchfeld „**Hochschule Karlsruhe“** ein.
   - Klicken Sie anschließend auf „**Hochschule Karlsruhe“**.
   - Klicken Sie anschließend auf „**Fortfahren“** klicken.

3. Darauf erscheint ein neues Fenster mit dem Logo der Hochschule Karlsruhe.
4. Scrollen Sie nach unten und klicken Sie auf die blaue Schaltfläche „**Akzeptieren“**.
5. Anschließend erscheint das Startfenster von **bwSync&Share** (in zwei unterschiedlichen Blautönen und Weiß mit dem Wappen des Landes Baden-Württemberg).

Abbildung 172 - Das Eingabefenster von bwSync&Share mit dem Logo der Hochschule Karlsruhe.

a. Benutzername: Eintippen vom **RZ-Kürzel**
b. Passwort: Eintippen vom **Passwort des RZ-Kürzels**
c. Anschließend auf „**Anmelden“** klicken

6. Nach der Anmeldung erscheint ein neues Fenster mit den Daten, die Ihrem RZ-Kürzel zugeordnet sind.
7. Scrollen Sie nach unten bis zur blauen Schaltfläche „**Akzeptieren“** und klicken Sie drauf.
8. Danach öffnet sich ein weiteres Fenster in verschiedenen Blautönen und dem Wappen des Land Baden-Württemberg.

3. Verwenden und Verwalten von bwSync&Share

3.1. Ein Dokument/eine Datei hochladen

Bevor Sie eine Datei über **bwSync&Share** mit anderen Personen teilen können, muss diese zunächst hochgeladen werden.

Klicken Sie dazu auf das **Ordner-Symbol** (rotes Rechteck) und anschließend – sobald die Seite geladen ist – auf **„+ Neu“** (roter Kreis).
In der untenstehenden Abbildung sind die entsprechenden Symbole markiert.

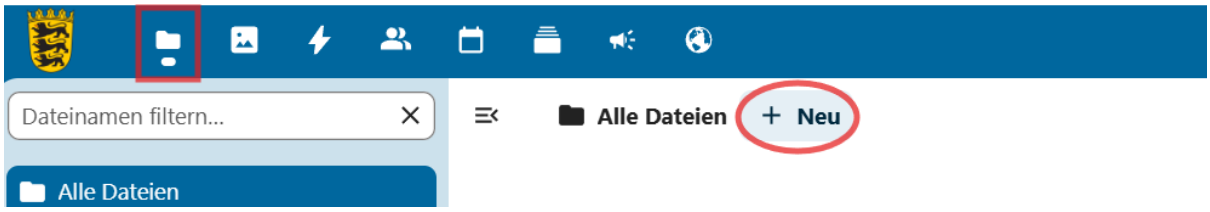

Abbildung 173 - Ein Ausschnitt der oberen Menüleiste in bwSync&Share.

Wenn Sie auf **„+ Neu“** klicken, öffnet sich ein Dropdown-Menü mit allen verfügbaren Funktionen.

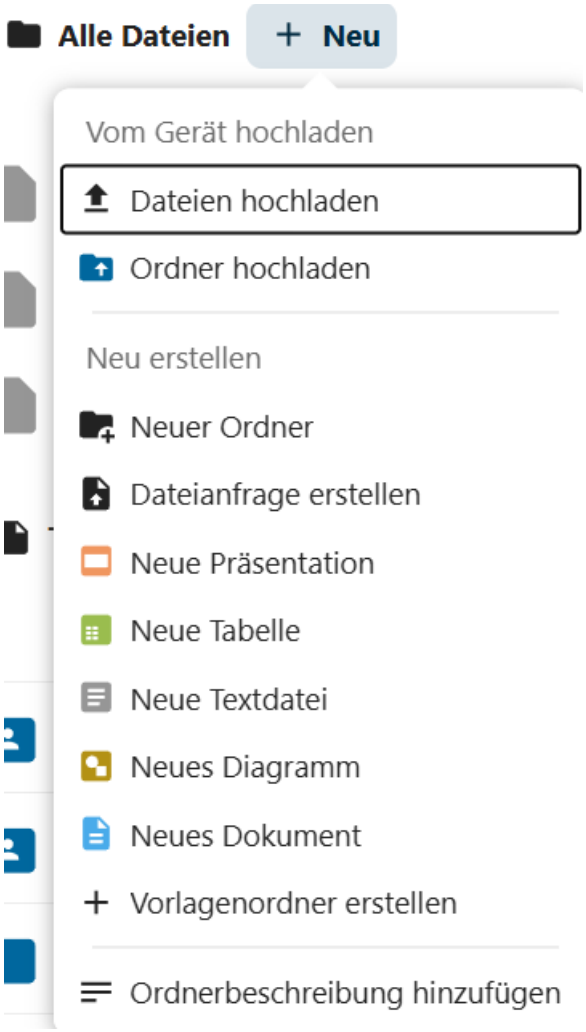

Abbildung 174 - Drop-Down-Menü in bwSync&Share.

In diesem Abschnitt liegt der Fokus auf „**Datei hochladen“**. Klicken Sie mit der linken Maustaste auf „**Datei hochladen“**. Je nach verwendetem Browser öffnet sich nun entweder direkt der **Explorer** oder eine Vorauswahl, aus der Sie über „**Alle anzeigen“** in den Explorer gelangen.

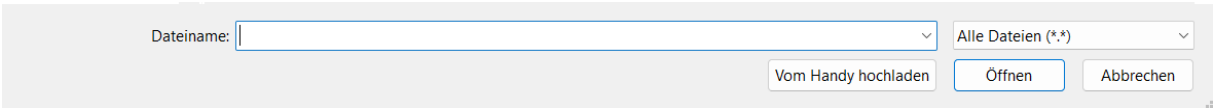

Abbildung 175 - Der untere Teil des Windows-Explorer-Fensters zum Hochladen ausgewählter Dateien in bwSync&Share.

Im Explorer-Fenster wählen Sie die Datei aus, die Sie auf bwSync&Share hochladen möchten, und klicken auf „**Öffnen**“. Nach Abschluss dieser Schritte wird die Datei erfolgreich hochgeladen und erscheint in der Liste „**Alle Dateien**“. Dort sehen Sie zusätzlich die Dateigröße sowie das Datum der letzten Änderung.

11.3 Das Hochladen von Dateien

Auch das Hochladen ganzer Ordner ist möglich. Das Vorgehen unterscheidet sich nur geringfügig vom Hochladen einzelner Dateien. Klicken Sie wieder auf **„+ Neu“** und anschließend auf „**Ordner hochladen“**. Daraufhin öffnet sich erneut das Explorer-Fenster, in dem Sie den gewünschten Ordner auswählen und auf „**Hochladen“** klicken.

Abbildung 176 - Der untere Teil des Windows-Explorer-Fensters zum Hochladen ausgewählter Ordner oder mehrerer Dateien in bwSync&Share.

Alternativ können Sie einen bereits geöffneten Ordner per **Drag & Drop** in das Upload-Feld im oberen Fensterbereich von **bwSync&Share** ziehen.

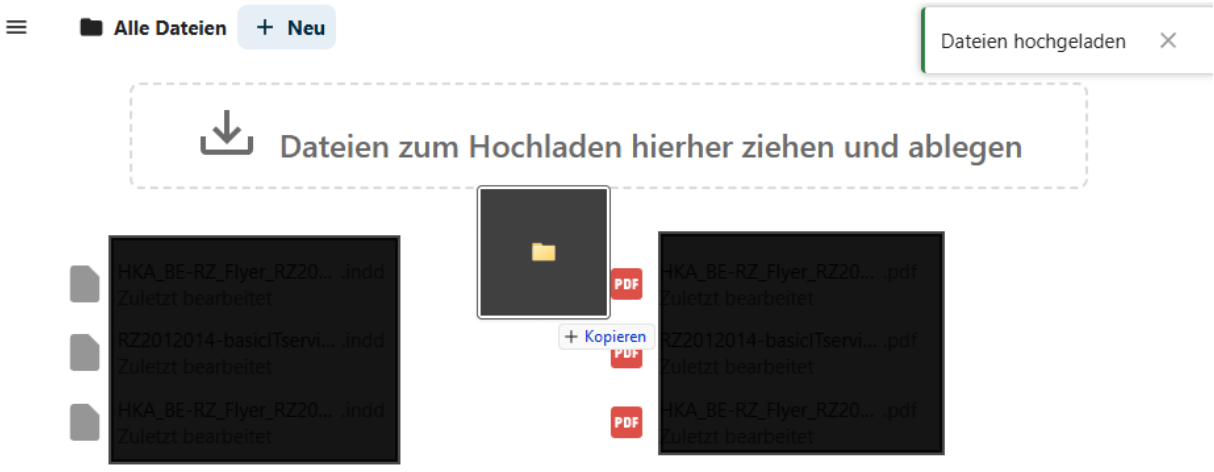

Abbildung 177 - Drag&Drop als alternative Möglichkeit zum Hochladen von einer oder mehreren Dateien.

11.4 Das Erstellen von Inhalten

Um einen neuen Inhalt direkt in **bwSync&Share** zu erstellen, klicken Sie auf **„+ Neu“** und wählen anschließend das gewünschte **Dateiformat** aus. Im folgenden Beispiel wird ein neues Dokument erstellt.

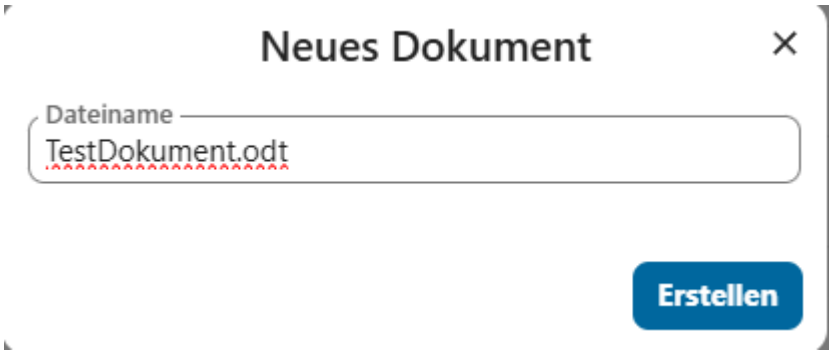

Abbildung 178 - Das Fenster, um ein neues Dokument zu erstellen.

In diesem Fenster können Sie Ihrem Dokument einen **Titel** geben und sehen zugleich, welche **Dateiendung** es erhält. Nachdem Sie den Titel eingegeben haben, klicken Sie auf **„Erstellen“** und das neue Dokument öffnet sich und kann direkt bearbeitet werden. Wie in Microsoft Word können Sie nun den Text formatieren, z. B. **Schriftgröße** oder **Schriftart** anpassen. Sobald Sie mit der Bearbeitung fertig sind, klicken Sie oben rechts auf das **„X“**, um das Dokument zu schließen.

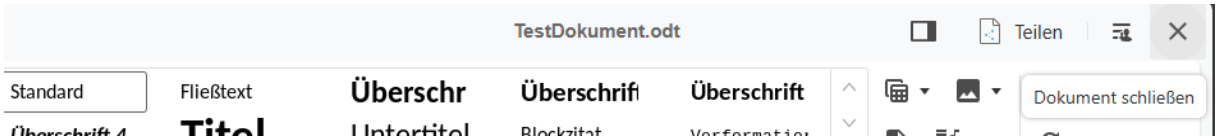

Abbildung 179 - Über das "X" oben rechts kann die Bearbeitung beendet werden. Die Speicherung erfolgt automatisch.

Nach dem Schließen werden Sie zurück auf die **bwSync&Share-Oberfläche** geleitet, wo das neu erstellte Dokument nun angezeigt wird.

11.5 Das Teilen von Inhalten

In bwSync&Share können Sie Ihre erstellten Inhalte bzw. Ihre hochgeladenen Inhalte mit einer oder mehreren Personen. Um z.B. eine PDF-Datei zu teilen, gehen Sie wie folgt vor:

- Suchen Sie die Datei, die Sie teilen möchten.
- Klicken Sie, bei der Datei, auf der Personen-Symbol (rote Markierung), um die Freigabeoptionen in einem Fenster auf der Seite zu öffnen.

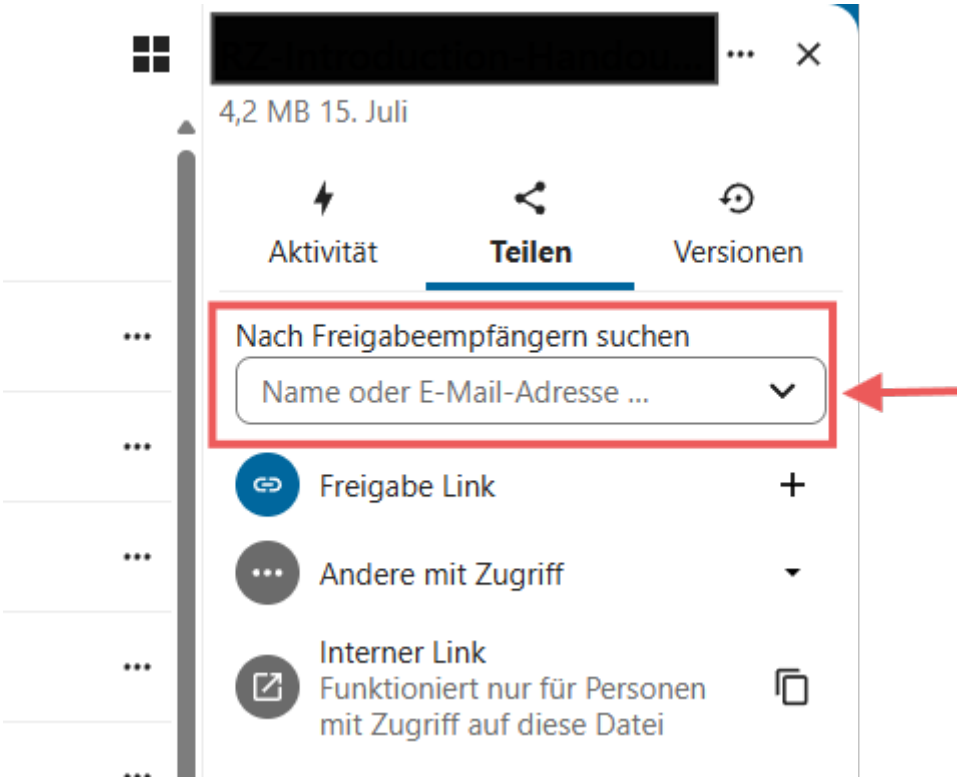

Abbildung 180 - Das Eingabefeld zum Teilen von Medien mit Namen oder E-Mail-Adresse.

- Im Tab „**Teilen“** können Sie im Eingabefeld die **Namen** oder die E-Mail-Adressen der Personen eintragen, mit denen Sie das Dokument teilen möchten.
- Sobald ein Name bzw. eine E-Mailadresse hinzugefügt wurde, erscheinen die Freigabeoptionen z.B. Die Berechtigung für **Lesen, Teilen** und **Bearbeiten** (siehe Abbildung 180).

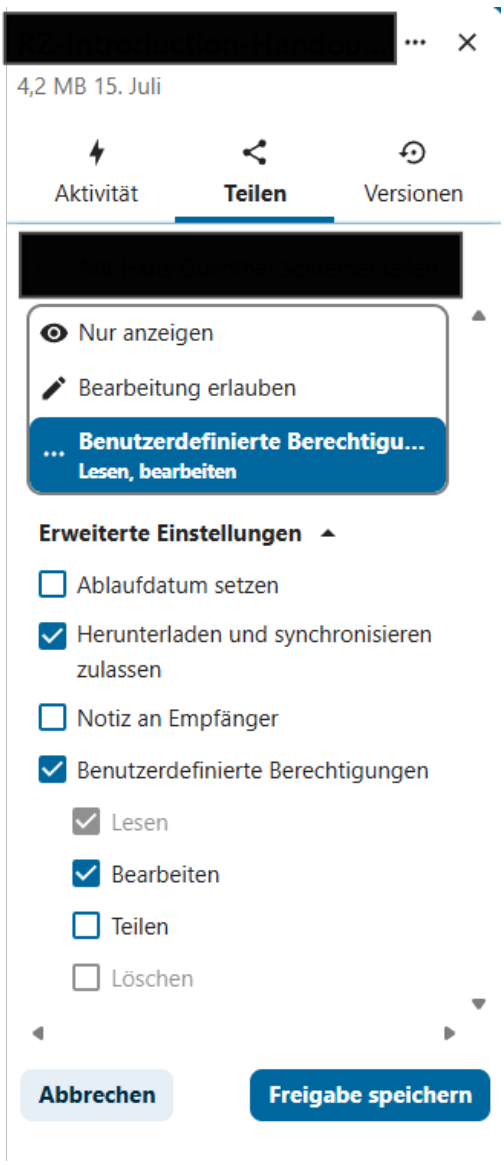

Abbildung 181 - Die Berechtigungsoptionen für die geteilten Dateien.

- Nach Auswahl der gewünschten Berechtigungen klicken Sie auf „**Freischalten**“. Die Datei wird nun geteilt, und die betreffenden Personen erhalten automatisch eine **E-Mail-Benachrichtigung** über den Zugriff.

11.6 Das Herunterladen von Inhalten

In diesem Unterkapitel steht das Herunterladen von Dateien, Dokumente oder Ordnern aus **bwSync&Share** beschrieben. Wenn Sie eine Datei von **bwSync&Share** herunterladen, wird diese auf Ihren Rechner gespeichert.

Einzelne Datei herunterladen:

- Klicken Sie auf die drei Punkte („…“) rechts neben der Datei.
- Wählen Sie im erscheinenden Menü die Option „Herunterladen“ (rot markiert).

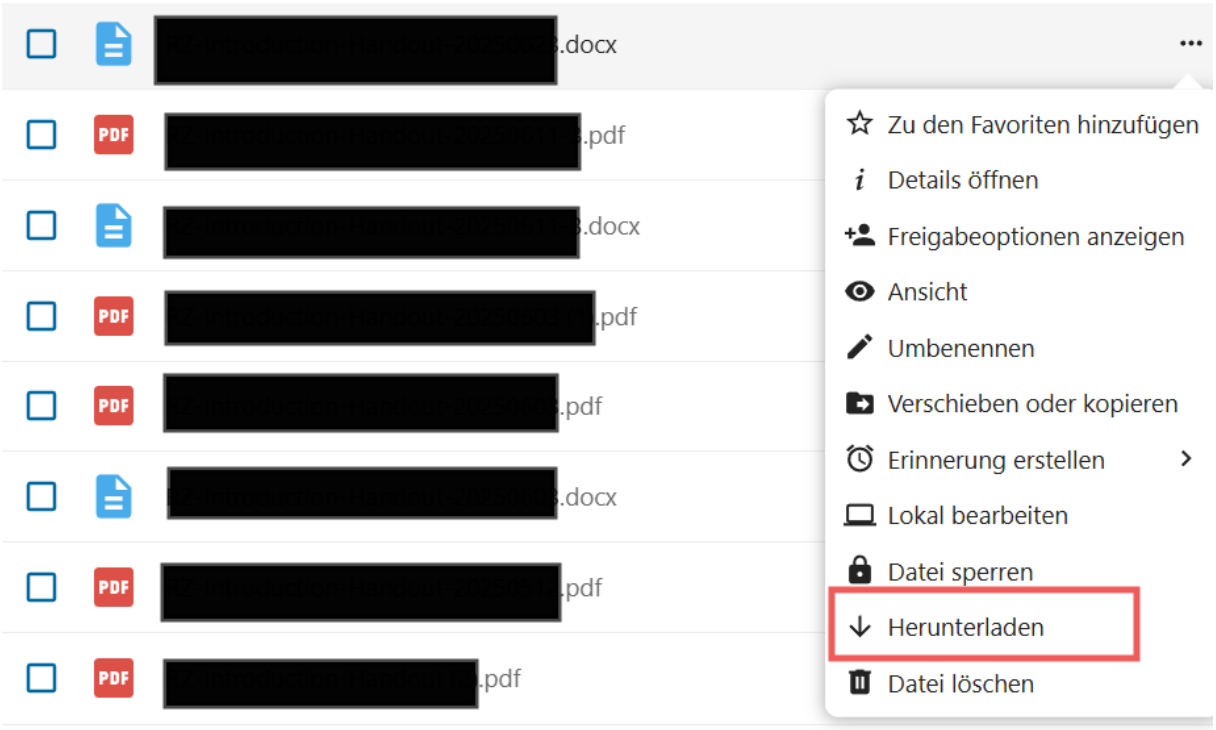

Abbildung 182 - Ein Dokument, das heruntergeladen werden soll.

Die heruntergeladene Datei befindet sich in der Regel in Ihrem **„Downloads“-Ordner**.

Mehrere Dateien oder Ordner herunterladen:

- Setzen Sie links die **Häkchen** bei den gewünschten Dateien oder Ordnern.
- Klicken Sie anschließend auf **„…Aktionen“** und wählen Sie **„Herunterladen“**.
- Die ausgewählten Dateien oder Ordner werden in einer **ZIP-Datei** zusammengefasst und in Ihrem **Download-Ordner** gespeichert.

Heruntergeladene ZIP-Dateien entpacken

- Öffnen Sie Ihren **Download-Ordner** und doppelklicken Sie auf die heruntergeladene ZIP-Datei.
- Klicken Sie im sich öffnenden Ordner auf **„Alle extrahieren“**.
- Es öffnet sich ein Fenster, in dem Sie den **Zielordner** auswählen können, in dem die Dateien abgelegt werden sollen.

1. Setzen Sie unbedingt den Haken bei **„Dateien nach Extrahierung anzeigen“**.

- Klicken Sie auf **„Extrahieren“**.
- Nach kurzer Zeit öffnet sich der Ordner mit den **extrahierten Dateien**, die nun bereit zur Nutzung sind.

11.7 bwSync&Share in Nextcloud einbinden

Als Mitarbeiterin oder Mitarbeiter der **Hochschule Karlsruhe** können Sie die **Nextcloud-Anwendung** direkt aus dem **Softwarecenter** installieren:

- Öffnen Sie das **Softwarecenter**.
- Suchen Sie nach „**Nextcloud“** und klicken Sie auf die Anwendung.
- Klicken Sie auf die rote Schaltfläche **„Installieren“**.

Abbildung 183 - Die Anwendung "Nextcloud". Als Beschäftigte der Hochschule Karlsruhe können Sie diese Anwendung direkt aus dem Softwarecenter beziehen und installieren.

11.8 Einrichten des bwSync&Share-Kontos in der lokalen Nextcloud-Anwendung

1. Nach der Installation suchen Sie in der **Windows-Suche** nach **Nextcloud** und öffnen die Anwendung.
2. Klicken Sie auf **„Anmelden“**.

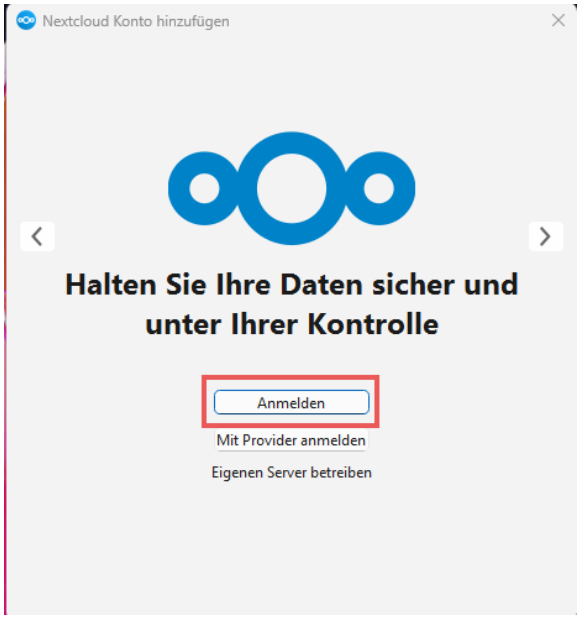

Abbildung 184 - Das Anmeldefenster der lokal installierten Nextcloud-Anwendung.

3. Geben Sie die **Serveradresse** ein: https://bwsyncandshare.kit.edu/ und klicken Sie auf „**Anmelden“** (roter Kreis).

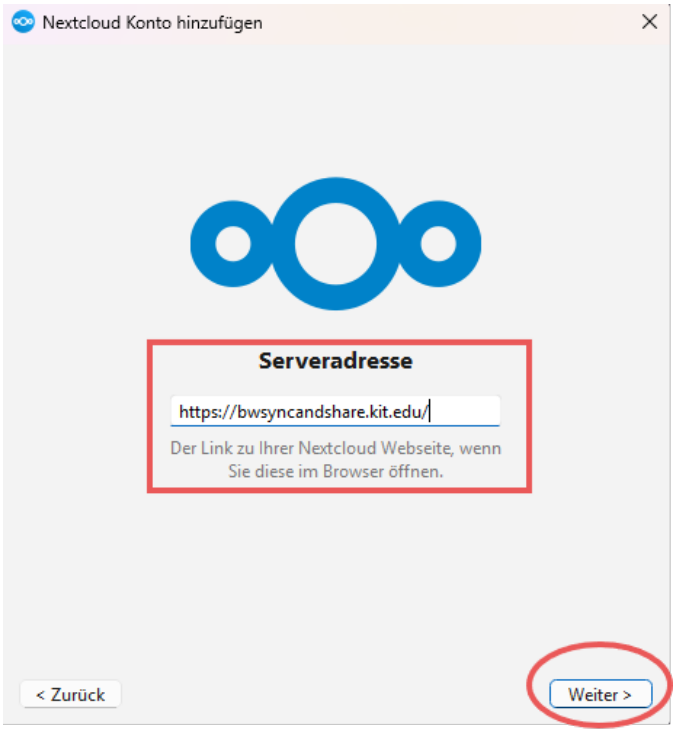

Abbildung 185 - Serveradresse

4. In der Zeile "Serveradresse" wurde der bwSync&Share-Link eingefügt. Klicken Sie anschließend auf "**Weiter**".

5. Überprüfen Sie den Namen des Geräts, das den Kontozugriff anfordert, und klicken Sie auf **Zugriff gewähren**.

6. Ein neues Fenster erscheint mit dem Titel „Wechseln Sie zu Ihrem Browser, um Ihr Konto zu verbinden“. Klicken Sie auf die Schaltfläche **Browser öffnen**.

7. Im Browser wird ein neues Fenster angezeigt, in dem in Blautönen steht: „Verbinden Sie sich mit Ihrem Konto“. Ihr PC-/Laptopnamen wird angezeigt, der Zugriff auf Ihr bwSync&Share-Konto angefordert wird. Klicken Sie auf **Anmelden**.

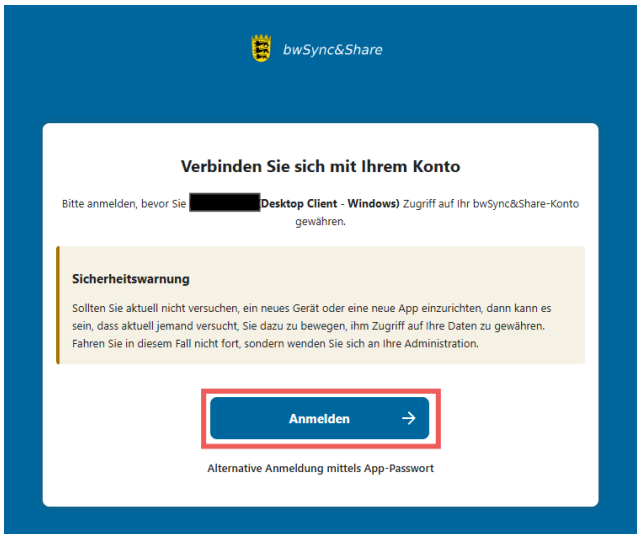

Abbildung 186 - Verwendung des lokalen Nextcloud-Ordners mit dem bwSync&Share-Konto.

8. Ein weiteres Fenster mit dem Titel „Kontozugriff“ erscheint, in dem Sie gefragt werden, ob der lokal PC-/Laptop (namentlich genannt) Zugriff auf Ihr bwSync&Share-Konto erhalten soll. Klicken Sie auf **Zugriff gewähren**.

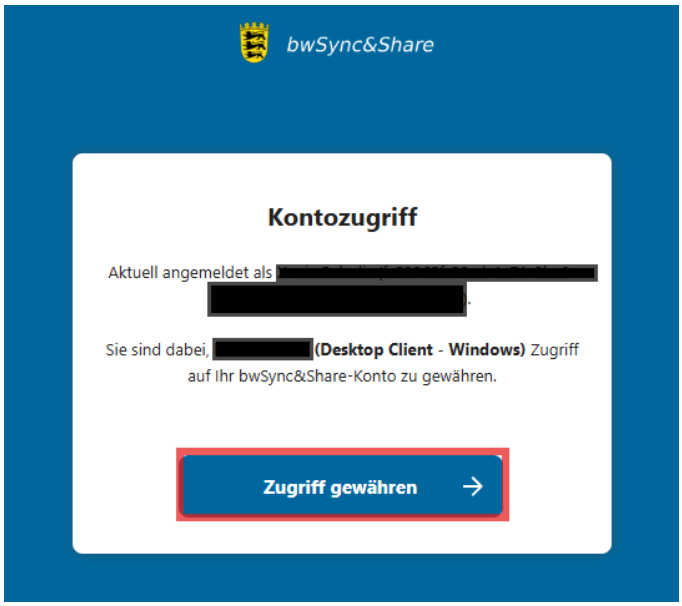

Abbildung 187 - „Zugriff gewähren“, um den Zugriff zwischen Ihrem lokalen Rechner und dem bwSync&Share-Konto zu erlauben.

9. Danach erscheint eine neue Meldung „Konto verbunden“. Sie können nun den lokalen Nextcloud-Ordner nutzen, um Ihre Dateien auf Ihr bwSync&Share-Konto hochzuladen.

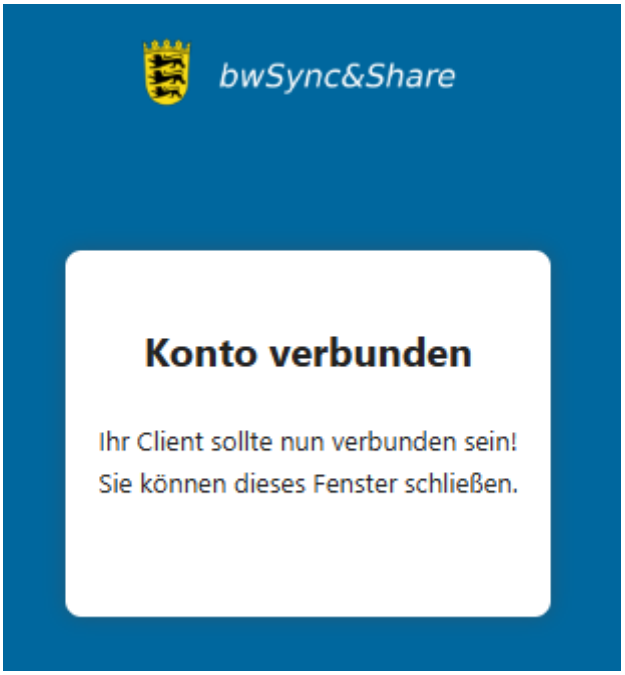

Abbildung 188 - Die Meldung "Konto verbunden" erscheint im Browser.

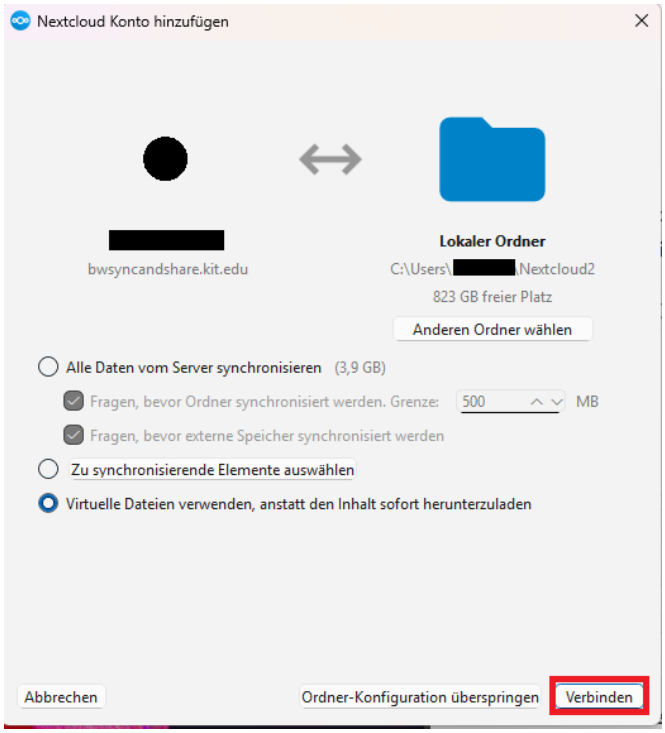

Abbildung 189 - Fenster zur Verbindung des lokalen Nextcloud-Ordners mit dem bwSync&Share-Konto.

12 BeyondTrust – lokaler Admin für meinen Rechner

12.1 Die Zielgruppe von BeyondTrust

Die Zielgruppe von BeyondTrust sind die **Mitarbeitenden** der Hochschule Karlsruhe, die lokale Administrationsrechte auf Ihren Arbeitsgeräten (Stand-PC oder Laptop) benötigten, um unabhängiger von den IT-Administratoren ihrer Organisationseinheit arbeiten zu können.

12.2 Die Voraussetzungen für die Vergabe von lokalen Administrationsrechten

Um die lokalen Administrationsrechte zu erhalten, müssen folgende Bedingungen erfüllt sein:

- Ausgefüllter „**Antrag auf Vergabe von lokalen Administrationsrechten**“
    - Das Word-Dokument bzw. die ausfüllbare PDF-Datei wird Ihnen per E-Mail von Seiten der Benutzerberatung zur Verfügung gestellt.
    - Der Antrag **muss vollständig** ausgefüllt sein und **alle erforderlichen Unterschriften** enthalten.
- Eine erfolgreiche Teilnahme am Awareness-Training vom Team der Informationssicherheit
    - ILIAS-Pfad: Magazin → Zentrale Einrichtungen → Informationssicherheit → Awareness Training

12.3 Die Verfügbarkeit des BeyondTrust-Clients

An der Hochschule Karlsruhe steht der BeyondTrust-Client für das folgende Betriebssystem zur Verfügung:

- Windows 11

12.4 Ablauf zum Erhalt der lokalen Administrationsrechten

12.4.1 Interesse bekunden

Sie äußern Ihren Wunsch nach den lokalen Administrationsrechten für Ihr Arbeitsgerät, indem Sie beispielsweise eine E-Mail an die Benutzerberatung schicken.

12.4.2 Der Erhalt vom Antrag und den Hinweis auf das Awareness Training

Sie erhalten den „**Antrag auf Vergabe von lokalen Administrationsrechten**“ sowie den Hinweis auf das Absolvieren des Awareness Trainings, der in ILIAS vom Informationssicherheitsteam zur Verfügung gestellt wurde.

12.4.3 Das Awareness Training absolvieren und den Antrag ausfüllen

Sie absolvieren das Awareness Training in ILIAS (Pfad oben angegebenen). Nach erfolgreichem Abschluss des Awareness Trainings füllen Sie den Antrag aus, indem Sie Ihre persönlichen Daten eintragen. Anschließend müssen vier weitere Personen den Antrag unterschreiben.
Diese Personen sind:

1. Der Dekan bzw. der Leiter der Organisationseinheit, bei dem der Interessenten angehört.
2. Der zuständige IT-Administrator der Organisation
3. Der Leiter des Rechenzentrums
4. Die Personalabteilung bzw. das Informationssicherheitsteam

12.4.4 Die Abgabe des vollständig ausgefüllten Antrags

Sobald alle erforderlichen Unterschriften vorliegen und das vollständig ausgefüllte Dokument (einschließlich des bestandenen Awareness Training-Zertifikats) im Rechenzentrum eingegangen ist, werden Ihnen die lokalen Administrationsrechte für Ihr Arbeitsgerät zugewiesen.

Der Prozess läuft wie folgt ab:

1. Sie als Antragsteller senden den ausgefüllten und vollständig unterschriebenen Antrag sowie das bestandene Awareness Training-Zertifikat an die Benutzerberatung.
2. Die Mitarbeitenden der Benutzerberatung leiten die beiden Dokumente an die zuständige Person, dem Leiter des Rechenzentrums, weiter.
3. Nach erfolgreicher Prüfung werden Ihre lokalen Adminrechte freigeschaltet. Über die Zuweisung Ihrer lokalen Administrationsrechte werden Sie per E-Mail informiert. Der Antrag wird anschließend an die Personalabteilung bzw. an das Informationssicherheitsteam weitergeleitet und dort abgelegt.

12.4.5 Die Installation der BeyondTrust-Pakete

Im Softwarecenter können Sie die beiden BeyondTrust-Pakete installieren:

- BeyondTrust-Client
- BeyondTrust-Certificate

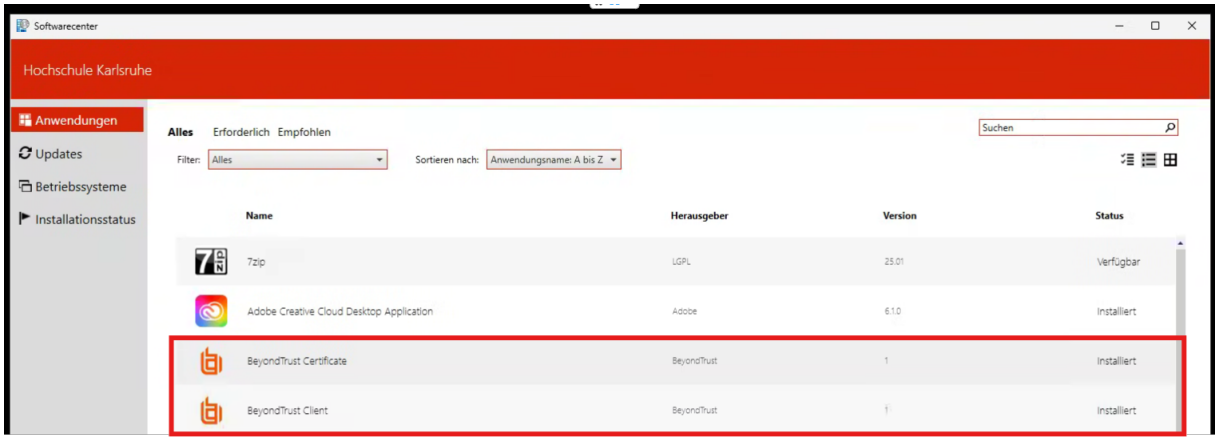

Abbildung 190 Das Softwarecenter, aus dem Sie den BeyondTrust-Client und das BeyondTrust-Certificate beziehen können.

Sie klicken auf „**BeyondTrust-Client**“ und schon können Sie auf die Schaltfläche „**Installieren**“ klicken (siehe Abbildung 191).

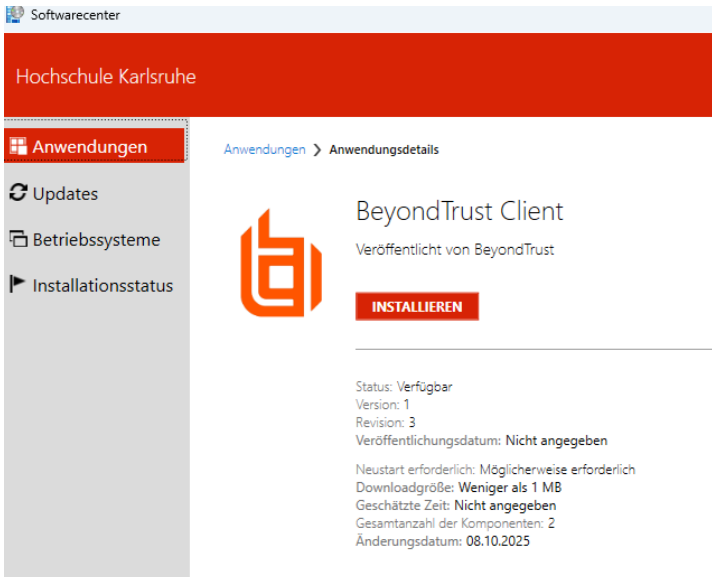

Abbildung 191 Das Softwarecenter: "BeyondTrust-Client" bereit zur Installation.

12.4.6 Installation, Neustart und Öffnen von BeyondTrust

Nach der Installation beider „***BeyondTrust***“-Pakte startet ihr Arbeitsgerät automatisch neu. Das *BeyondTrust-Certificate* wird automatisch im Zertifikatsspeicher des Arbeitsgeräts hinterlegt.
Hinweis!!: Nach der Installation erscheint *BeyondTrust* unter folgenden Namen: „***Privilege Management Console***“

12.4.7 Ausführen des BeyondTrust („*Privilege Management Console*“)

Hierfür haben Sie zwei Wege:
1. Weg: Sie tippen in der Windows Suchleiste den Namen „***Privilege Management Console***“ ein und klicken mit Rechtsklick auf die Anwendung, um es „***Als Administrator auszuführen***“.
Oder
2. Weg: Sie klicken auf die Windows Kachel, ob auf die Schaltfläche „Alle“, um anschließend alle installierten Anwendungen anzeigen zu lassen. Dann scrollen Sie runter bis zum „***Privilege Management Console***“. Sobald Sie die Anwendung gefunden haben, klicken Sie mit Rechtsklick drauf, um es „**Als Administrator auszuführen**“.

Darauf erscheint ein neues Fenster.

12.4.8 Das Fenster „Informationssicherheitsrichtlinie – Berechtigungsprüfung erforderlich“

Im Fenster „**Informationssicherheitsrichtlinie**“ erfolgt die Prüfung ihrer Berechtigung (siehe Abbildung 192):

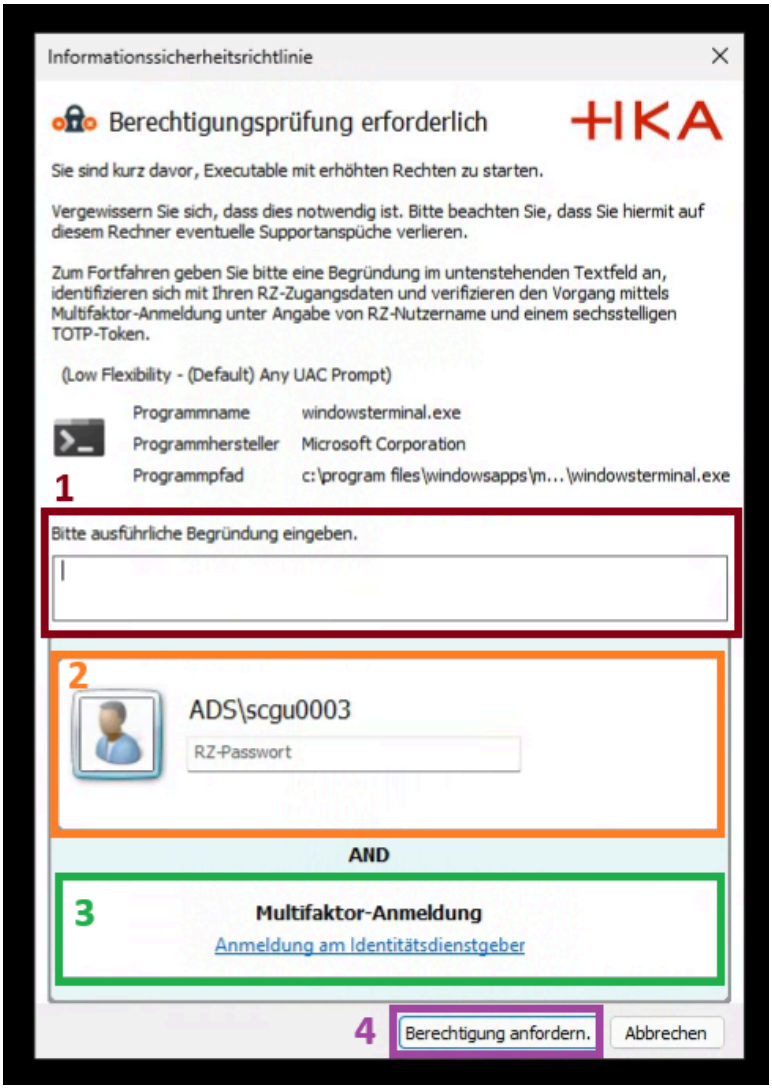

Abbildung 192 Das neue Fenster, das erscheint, wenn die "Privilege Management Console" als Administrator ausgeführt wird.

Bitte geben Sie in den hier farbig markierten Feldern Folgendes ein:

1. Geben Sie den Zweck ein, für den Sie BeyondTrust verwenden möchten (**dunkelrote 1**).
2. Hier tippen Sie das Passwort Ihres RZ-Kürzels ein (**orange 2**).
3. Klicken Sie auf den Link „**Anmeldung am Identitätsdienstgeber**“ (**grüne 3**), um ein neues Fenster zu öffnen.

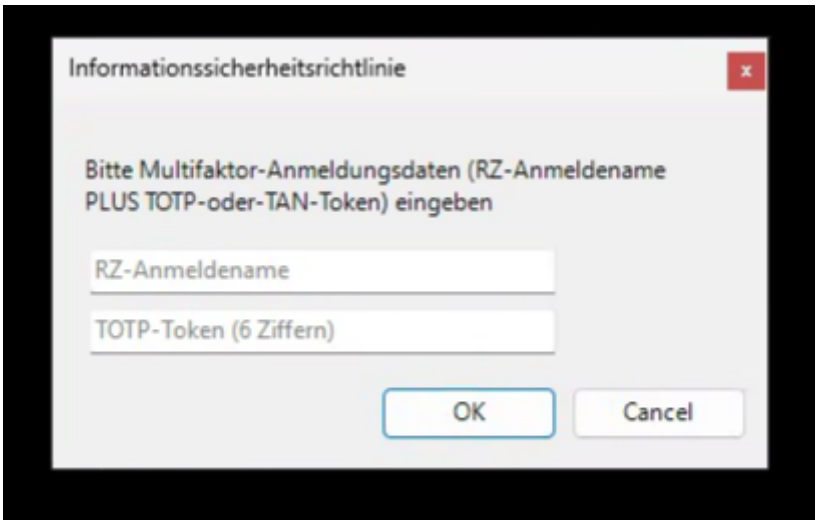

Abbildung 193 Hier geben Sie ihr RZ-Kürzel und den 6-stelligen Token aus der Authenticator-App ein.

Im neuen Fenster führen Sie die Multifaktor-Authentifizierung durch, indem Sie ihr RZ-Kürzel und den 6-stelligen Token aus der Authenticator-App (oder von der TAN-Liste (siehe Kapitel 4.3.)) eingeben. Bestätigen Sie mit „**OK**“ (siehe Abbildung 193).

4. Anschließend kehren Sie zum Fenster „**Berechtigungsprüfung erforderlich**“ zurück und klicken Sie auf „**Berechtigung anfordern**“ (**lilafarbene 4**).

12.4.9 Lokale Administrationsrechte

Nach erfolgreicher Prüfung stehen Ihnen auf ihrem lokalen Arbeitsgerät die Administrationsrechte zur Verfügung.

13 Telefon (Digitalen Endgeräten wie Alcatel 4029/4039/4028)

Ausführliche Anleitungen und Anträge finden Sie auf den Hochschulseiten im internen Bereich des Rechenzentrums (https://www.h-ka.de/rz) unter der Rubrik **RZ-Dokumente.**
Bei Fragen zum Telefon wenden Sie sich bitte an die Emailadresse: tk.rz@h-ka.de.

13.1 Kurzwahlcodes

Im Folgenden finden Sie die Kurzwahlcodes, welche bei uns aktiviert sind, wie CFNA, Gruppenwahl, etc.
Sofern an Ihrem Telefon eine Taste für die gewünschte Funktion vorhanden ist, können Sie diese wie folgt verwenden.

Leistungsmerkmale	Kennziffer	Beachten	Bemerkung
Verbindung mit dem Amt für Dienstgespräche	**0**		
Verbindung mit dem Amt für Privatgespräche	**80**	Pineingabe	mit persönlichem Pin (vierstellig)
Verbindung mit der Vermittlung	**99**		
Rufumleitung allgemein deaktivieren	***10**		
Rufumleitung sofort aktivieren	***11**	plus Zielrufnummer	Externe Umleitung muss v. Administrator eingerichtet werden
Rufumleitung bei Besetzt aktivieren	***12**	plus Zielrufnummer	Externe Umleitung muss v. Administrator eingerichtet werden
Rufumleitung nach Zeit aktivieren (nach viermal Klingeln)	***13**	plus Zielrufnummer	Externe Umleitung muss v. Administrator eingerichtet werden
Passwort festlegen oder ändern	***29**		standart 4 x 0000
Apparat sperren /entsperren	***28**	mit Passwort	Telefonate sind dann nur intern möglich
Anrufschuz aktivieren / deaktivieren	***32**	mit Passwort	der Anrufer wird mit bitte nicht stören informiert
Sprachbedienerführung ein / ausschalten	***44**		es kommt keine Sprachansage mehr
Gespräche in einer Heranholgruppe übernehmen	**##**		wenn Gruppe eingerichtet ist
Gespräche geziehlt holen	**#***	plus Zielrufnummer	unabhängig von einer Gruppe
MFV aktivieren (bei einer bestehenden Verbindung)	****8**	anschließend Ziffereingabe	bei Sprachansagen / Hotlines / Konferenzen
Gespräche weiterverbinden	**Rückfrage**	plus Zielrufnummer	Beim analogen Apparat Taste **"R"** wählen
Rückruf (beim anwählen des Teilnehmers)	**1**	Rückruftaste o. Taste "1"	der Angerufene erhält eine Nachricht im Briefkasten
Rückruf bei besetzt (beim anwählen des Teilnehmers)	**1**	Rückruftaste o. Taste "1"	der Angerufene wird sofort nach Freigabe angewählt
Dreierkonferenz (bei best. Verbindung mit zwei Teilnehmern)	**3**	Konferenztaste o. Taste "3"	mit drei Gesprächspartner eine Verbindung aufbauen

Abbildung 194 - Kurzwahlcodes

Erläuterung:

- Zu Kennziffer *13: Rufumleitung nach Zeit einschalten, nach ca. 5 x klingeln: *13 + Zielrufnummer
- Zu Kennziffer *28: Hier ist es wichtig, dass zuvor mit *29 Passwort eingeben, Standard „0000“ und Passwort ändern. Den Apparat sperren / entsperren mit *28

Erläuterung (bei bestehenden Verbindungen):

- Makeln: Bei einer Verbindung mit zwei Teilnehmer, kann zwischen dem ersten und dem zweiten Teilnehmer mit „Taste2“ gewechselt werden.
- Rückruf: Der Angerufene erhält eine Nachricht im Briefkasten („Taste 1“/ Funktionstaste).
- Rückruf bei besetzt: Der Angerufene wird sofort nach Freigabe angewählt.
- Dreierkonferenz (mit 3 Gesprächspartner eine Verbindung aufbauen):
  1. Teilnehmer anrufen.
  2. Rückfragetaste drücken und zweiten Teilnehmer anrufen.
  3. „Taste 3“ drücken (oder Konferenztaste drücken).

13.2 Phonebox

Vorrausetzung für den Gebrauch der Phonemailbox ist, dass diese für die entsprechende Nebenstelle eingerichtet ist.
Dies kann man selbst prüfen, in dem man die Mailbox „2099“ anruft und die eigene Rufnummer als Mailboxnummer eingibt. Kommt die Ansage „dies ist keine bekannte Mailboxnummer“ ist, dann ist die Mailbox noch nicht eigerichtet. Bitte wenden Sie sich an die E-Mail-Adresse: **tk.rz@h-ka.de** wenden.

Wichtig bei Erstbenutzung:
1. Es muss die eigene Rufnummer als Kennwort eingegeben werden. Anschließend ein neues Kennwort erstellt und gespeichert werden.
2. Name aufsprechen und Standartbegrüßungstext auswählen oder selber besprechen und die Einrichtung abschließen. „Nun ist die Mailbox fertig eingerichtet“.
3. Um nun Anrufe auf der Mailbox zu erhalten, muss eine Rufumleitung eingerichtet werden (siehe auch unter Kennziffern).
4. Rufumleitung (z.B. „*11“) zur Sprachmailbox wird mit „2099“aktiviert.
5. Oder obere rechte Taste drücken, Rufumleitungsart wählen und mit Rufnummer „2099“ abschließen.
6. Die Mailbox wird über die Briefkastenfunktion abgefragt.
7. Die Mailbox kann auch von der eigenen o. anderen Nebenstelle mit „2099“ abgefragt werden (folge Sprachanweisung).
8. Bei Fernabfrage von einem anderen Festnetz o. Handy „0721-925-2099“ und nach Sprachanweisung die vierstellige Telefonnummer eingeben.

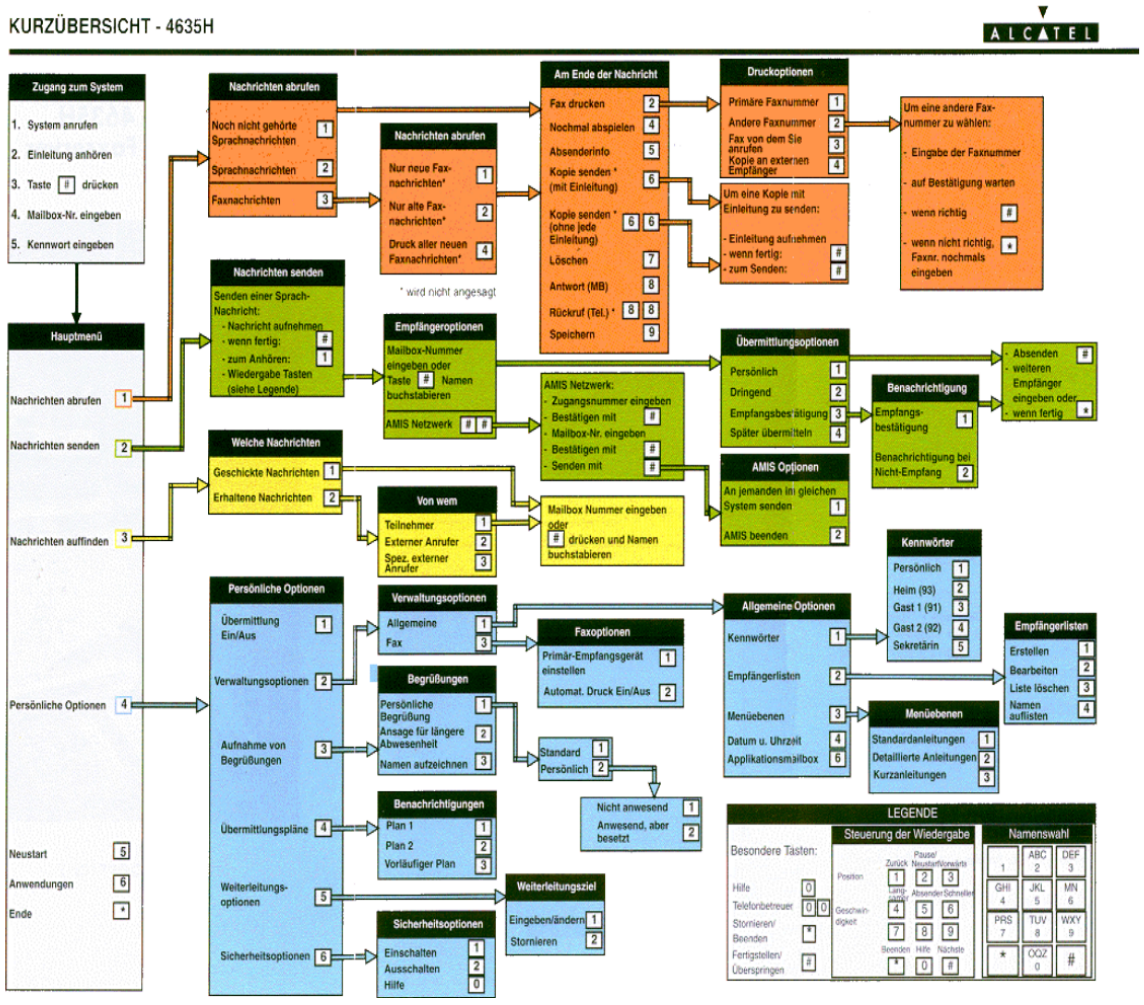

Abbildung 195 - Kurzübersicht

13.3 Kurzanleitung Tastenprogrammierung

1. Im Display linker Reiter "Menü" aufrufen
2. Dann folgende Tasten drücken:
   - Einstellungen
   - Telefon
   - Tasten programmieren
   - Persönliche Seite
   - Taste Auswählen: Merkmale oder Kurzwahl (z.B. bei Kurzwahl)
   - Telefon-Nr. und Namen eingeben
   - anschließend mit Übernehmen abschließen
     Oder direkt unter Reiter **Info** eine freie Taste auswählen und Merkmale oder Kurzwahl einrichten.

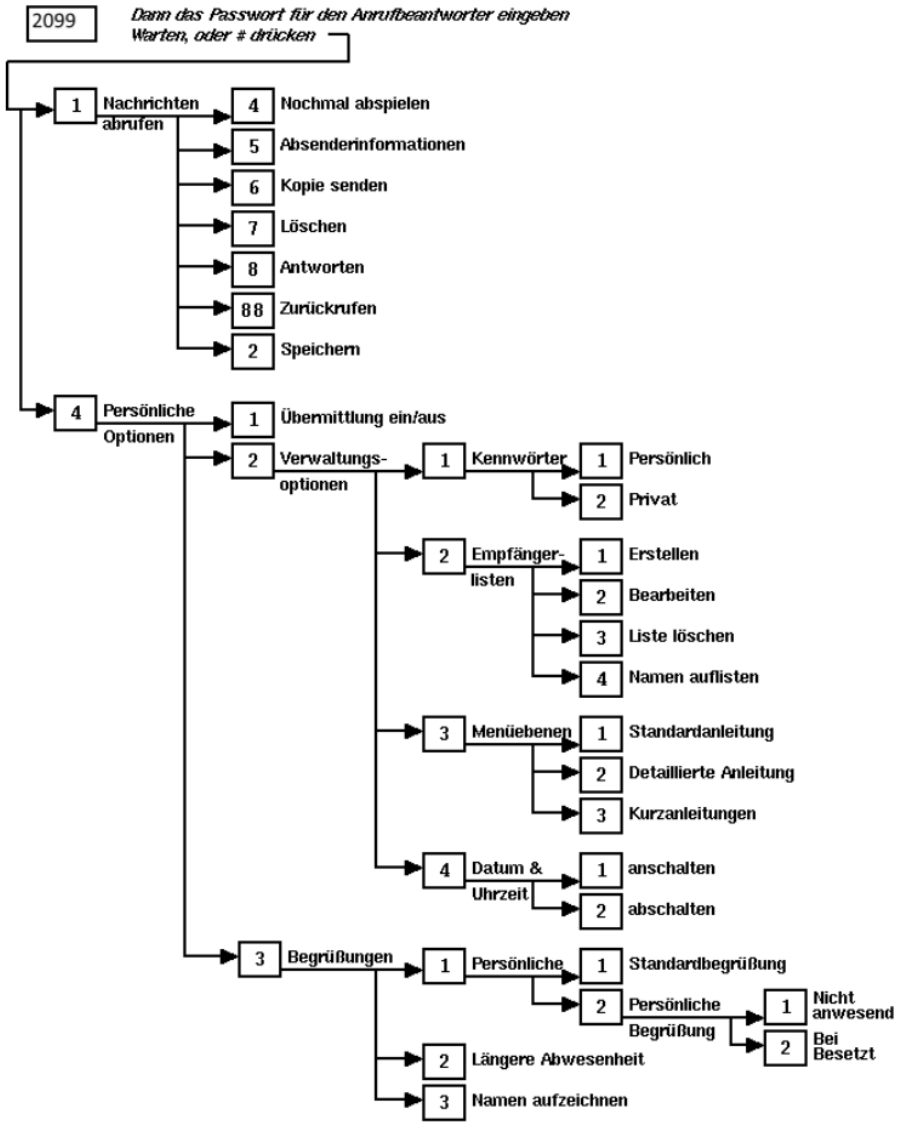

Abbildung 196 - Phonebox

13.4 Anfragen an den Telefon-Support

1. Bitte geben Sie bei jeder Telefon-Support-Anfrage Ihren Namen, Ihre Telefonnummer und Ihre Raumnummer an, wenn möglich auch die Markierung der Telefondose.

2. Jede Handlung an Telefonen, wie das Ein- und das Ausschalten, Stecker aus der Steckdose ziehen, mitnehmen in ein anderes Gebäude usw., ist nur nach Absprache mit der TK möglich.

3. Wenn das DECT-Handteil nicht lädt, versuchen Sie zuerst, den Akku herauszunehmen und wieder einzusetzen und prüfen Sie bitte, ob das Telefon richtig in der Ladeschale positioniert ist. Nach ein paar Minuten sollte die Lampe blinken.

14 LKIT Laborinformation

14.1 Verbindung mit dem Internet herstellen

14.2 Netzlaufwerke im Labor

15 Wo bekomme ich Hilfe?

Studierende erhalten Unterstützung von der **RZ-Benutzerberatung** (Raum LI135). Diese ist **montags** bis **freitags** von **10:00 Uhr** bis **13:00 Uhr** geöffnet.

Bei allen Fragen zur Nutzung der IT-Dienste an der Hochschule Karlsruhe wenden Sie sich bitte als **nichtstudentische Angehörige/r** an das **IT-Administrationsteam** Ihrer Fakultät, Ihrer Einrichtung (OU) oder Ihres Instituts.

Fakultät/ OU/Institut	Mail-Adresse	IT-Administratoren der Fakultät/ OU/ Institut	Raum	Telefon: 0721- 925…
AB		Necmettin Gündüzoglu Julian Reiling Alexander Keller	B 302	2647 2649 2642
BWIM		Viatcheslav Hahne	HO 213	2585
CAR	it-support.car.rz@h-ka.de			
EIT		Tristan Gantner Simone Brandt	M 214 N 306	2242 1258
GHD		Thorsten Gutsche		1764
IAF	it-support.iaf.rz@h-ka.de			
IDEV	it-support.idev.rz@h-ka.de			
IDM	it-support.idm.rz@h-ka.de			
IDSS	it-support.idss.rz@h-ka.de			
IEEM	it-support.ieem.rz@h-ka.de			
IFS	it-support.ifs.rz@h-ka.de	Jan Kupper Uwe Fidelak	LI 105 LI 106	2385 2390
IIIX	it-support.iiix.rz@h-ka.de			
IISRG	it-support.iisrg.rz@h-ka.de			
IKKU	it-support.ikku.rz@h-ka.de			
ILIN	it-support.ilin.rz@h-ka.de			
IMM		Günther Baumgärtner	AM 103	2989

Fakultät/ OU/Institut	Mail-Adresse	IT-Administratoren der Fakultät/ OU/ Institut	Raum	Telefon: 0721- 925…
		Viatcheslav Hahne	HO 213	2585
IMP	it-support.imp.rz@h-ka.de			
IRAS	it-support.iras.rz@h-ka.de			
ITA	it-support.ita.rz@h-ka.de	Jan Kupper Uwe Fidelak	LI 105 LI 106	2385 2390
ITF	it-support.itf.rz@h-ka.de			
ITS	it-support.its.rz@h-ka.de	Gülhan Akar	LI 134	2343
IVI	it-support.ivi.rz@h-ka.de			
IWI		Steffen Teichmann Holger Bechtold Oskar Kovac	LI 140 E 005A E 005	2334 2958 2937 2917 2950
IWW	it-support.iww.rz@h-ka.de			
MMT		Dimitrij Gordienko Bernd Hölzer Nils Werling Matthias Bürkle Jonas Hansert	LI 037 LI 037 LI 037 F 105 LI 037	1840 1840 1840 1692 1805
RTWE		Thorsten Gutsche		1764
VW	it-support.vw.rz@h-ka.de	Jan Kupper Uwe Fidelak	LI 105 LI 106	2385 2390
W		Dieter Durigon Corinna Kraft	K 004a SH 108	1939 1929

16 Meine ersten Tage als nichtstudentische(r) Hochschulangehörige(r)

Die ersten Schritte in der Hochschule bringen eine Menge an Informationen mit sich. Mit dieser kurzen Aktionsliste möchten wir von der Seite des Rechenzentrums dazu beitragen, dass Sie sich schnell in die IT-Arbeitsumgebungen der Hochschule zurechtfinden.

☑	RZ-Zugangsdaten im Sicherheitsumschlag	(von RZ via Fakultätssekretariat/Vorgesetzten)
☐	Gebäude/Raum-Zugangstransponder	(von BI via Fakultätssekretariat/Vorgesetzten)
☐	Einrichtung RZ-Multifaktor-Zugangsdaten	(vgl. Kapitel 4)
☐	Web-Visitenkarte ausfüllen	(vgl. Einführungsfolien)
☐	Eintragung in eMail-Verteilerlisten	(via Fakultäts-/OU-IT-Administrationsteam)
☐	(optional) Telefon	(von RZ via Fakultätssekretariat/Vorgesetzten)
☐	(optional) CampusCard	(via Personalabteilung)
☐	(optional) Persönliches Zertifikat einrichten	(vgl. Kapitel 6)
☐	(optional) BBB-Registrierung durchführen	(vgl. Kapitel 10.2)
☐	(optional) Zoom-Registrierung abschließen	(vgl. Kapitel 10.1)
☐	(optional) Arbeitsplatz / PC / Laptop	(von Fakultäts-/OU-IT-Administrationsteam)
☐	(optional) Webcam/Headset	(von Fakultäts-/OU-IT- Administrationsteam)
☐	(optional) Mobilfunk(rahmen)vertrag	(von RZ via Fakultätssekretariat/Vorgesetzten)
☐	(optional) Einrichtung WLAN (BYOD)	(vgl. Kapitel 2)
☐	(optional) eLearning-Umgebung testen	(vgl. Einführungsfolien: ILIAS)
☐	(optional) CampusMgmt-Umgebung testen	(vgl. Einführungsfolien: HIS-Dienste)
☐	(optional) Visitenkarten bestellen	(von PK; vgl. Hochschulwebseite)

17 Abbildungsverzeichnis

(A) Zielsetzung

Das Ziel dieses Dokuments ist die Beschreibung der grundlegenden Rechenzentrumsdienste der Hochschule Karlsruhe.

(B) Kontrolle

X. Balodis, S. Roth, Dr. I. Schwab kontrolliert dieses Dokument.

(C) Freigaben

Dieses Dokument erfordert die nachfolgenden Freigaben:

Name	Titel	Datum	Unterschrift
N.N.	Abteilungsleiter ITS		
Günther Schreiner	Leiter Rechenzentrum	21.01.2026	(GS)

(D) Versionshistorie

Dieses Dokument unterlag folgenden Änderungen:

Version	Datum	Autor	Status	Kurzbeschreibung
1.0	05/05/25	Stefanie Roth, Ingo Schwab	Final	Initiale Beschreibung
1.2	07/05/25	Stefanie Roth, Ingo Schwab	Final	Verfeinerung der SW-Bereitstellung, TOTP-Ergänzungen, weitere URLs
1.3	12/05/25	Stefanie Roth, Ingo Schwab	Final	Hinweis bei SW-Bereitstellung
1.4	03/06/25	Stefanie Roth, Ingo Schwab	Final	Nutzerzertifikate erstellen
1.5	11/06/25	Stefanie Roth, Ingo Schwab	Final	Abbildung FortiClient VPN
1.6	14/06/25	G. Schreiner	Final	Rechtliche Hinweise zum HARICA IV+OV ergänzt, Varianten des FortiClients erläutert
1.7	16/06/25	Stefanie Roth	Final	Korrekturen
1.8	24/06/25	G. Schreiner	Final	Weiterer zertifikatsgesicherter Dienst ze-cert
1.9	02/07/25	Stefanie Roth	Final	Ergänzung der Telefonanlagenbeschreibung
2.0	04/07/25	Stefanie Roth	Final	Erstellung eines Gruppenpostfach-Zertifikat, Anfragen an den Telefon-Support
2.1	10/07/25	Stefanie Roth	Final	Globale Postfächer, Liste des IT-Administrationteams
2.2	13/08/25	Stefanie Roth	Final	Adobe Creative Cloud, Liste des IT-Administrationteams ergänzt, Globale Postfächer ergänzt
2.3	20/08/25	Xenia Balodis	Final	Collaborationswerkzeuge ergänzt
2.4	21/08/25	G. Schreiner	Final	OV+IV Zertifikate ergänzt
2.5	02/09/25	Xenia Balodis	Final	ISEC7 Mail Anleitung ergänzt
2.6	03/09/25	G. Schreiner	Final	OV vs. OV+IV Zertifikate angepasst
2.7	04/11/25	Stefanie Roth	Final	Korrekturen, MFA ohne Smartphone, Arbeiten mit Gruppenpostfächer und Verteiler
2.8	26/11/25	Xenia Balodis	Final	Kleine Verbesserung bei ISEC 7 Mail.
2.9	26/11/25	Xenia Balodis	Final	Kleine Verbesserung bei ISEC 7 Mail.
2.10	02/12/25	G. Schreiner	Final	Restrukturierung plus „Erste Tage“
2.11	05/12/25	Stefanie Roth	Final	Korrekturen
2.12	08/01/26	Xenia Balodis	Final	BeyondTrust-lokale Administrationsrechte
2.13	19/01/26	Xenia Balodis	Final	ISEC 7 Mail-App für Android-Smartphones (Veränderung & Erweiterung Kapitel 8)
2.14	21/01/26	G. Schreiner	Final	MFA Erläuterungen und Perspektive

(E) Veröffentlichung

Dieses Dokument wurde verteilt an:

Name / Team / Intranet URL	**Datum**
Leiter ITS	21.01.2026
Leiter ITA	21.01.2026
Gruppe RZ	21.01.2026

(F) Referenzierte Dokumente / URLs

- https://rz.h-ka.de/campusmgmt Campus Management Portal
- https://rz.h-ka.de/ulm User-Lifecycle-Management-Portal
- https://rz.h-ka.de/eduroam eduroam Konfigurationsportal
- https://webmail.h-ka.de Web-basierter Mailzugang
- https://owa.h-ka.de MFA-gesicherter Web-basierter Mailzugang
- https://mfa.h-ka.de MFA Konfigurationsportal
- https://authenticator.cc MFA Authenticator Extension
- https://portal.adb.h-ka.de Gruppenpostfach-Mitglieder hinzufügen
- https://rz.h-ka.de/vpn VPN Software-Portal
- https://owa-cert.h-ka.de Zertifikatsgesicherter Web-basierter Mailzugang
- https://ze-cert.h-ka.de Zertifikatsgesicherter Zugang zur Zeiterfassung
- https://h-ka-de.zoom.us ZOOM
- https://online-leh.re/ BigBlueButton
- https://cm.harica.gr/MyDashboard HARICA Registrar
- https://apps.apple.com/us/app/isec7-mail/id1045017598 App Store