Hessische Hochschule für
öffentliches Management
und Sicherheit

HöMS
HESSISCHE HOCHSCHULE
FÜR ÖFFENTLICHES MANAGEMENT
UND SICHERHEIT
University of Applied Sciences

Anleitung

Einrichtung Outlook Web App für

Lehrbeauftragte und Studierende der Hessischen Hochschule für öffentliches Management und Sicherheit (HöMS)

Version 1.0

Herausgeber:
Hessische Hochschule für öffentliches Management und Sicherheit

Schönbergstraße 100
65199 Wiesbaden

Redaktion: WebMail-Team
Für Verbesserungsvorschläge wenden Sie sich bitte an webmail@hoems.hessen.de

Version: 1.0
Erscheinungsdatum: Dez. 2023

Inhaltsverzeichnis

1 Einleitung

1.1 Kontext

Hauptanliegen der Bereitstellung einer dienstlichen E-Mail-Adresse über ein OWA Konto für jeden Lehrbeauftragten und Studierenden ist die Sicherstellung einer schnellen, verbindlichen, einheitlichen und datenschutzkonformen Kommunikation. Darüber hinaus ist die Adresse als eine der ersten, grundlegenden Maßnahmen im Kontext der allgemeinen Digitalisierungsstrategie zu verorten und soll beispielsweise schon in Kürze einem vereinfachten Zugang zu aktuellen und zukünftigen Verwaltungsverfahren dienen.

1.2 Über dieses Handbuch

1.2.1 Allgemeiner Hinweis

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung mehrerer geschlechtsbezogener Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

1.2.2 Zweck

Diese Anleitung beschreibt die notwendigen Schritte, um als Lehrbeauftragter oder Student die Ihnen zur Verfügung gestellte dienstliche E-Mail-Adresse einrichten zu können. Eine Beschreibung des Vorgehens wurde Ihnen in Form einer Kurzanleitung (Anlage 1) bereits mit dem persönlichen Anschreiben zur Verfügung gestellt und wird hier lediglich noch einmal detaillierter beschrieben.

1.2.3 Zielgruppe

Unterstützen möchte dieses Dokument insbesondere Anwender, die Microsoft Outlook und seine Funktionalitäten noch nicht kennen und über wenig Grundwissen verfügen. Dieses Dokument hat keinen Anspruch auf Vollständigkeit und kann auch nicht die ausführlichen, originalen Herstellerbeschreibungen ersetzen.

2 Bevor es losgeht

…haben Sie Ihre **Zugangsdaten über einen persönlichen Brief erhalten**, der an Ihren Campus gesendet wurde. Ihr Benutzername behält ebenso wie Ihre Registrierungs-PIN die Gültigkeit, bis Sie ein neues Schreiben erhalten.

Bitte heben Sie Ihr persönliches Anschreiben unbedingt auf.

2.1 Ihr Benutzername

Ihr Benutzername entspricht Ihrer E-Mail-Adresse und setzt sich in der Regel folgendermaßen zusammen: Vorname.Nachname@owahoems.hessen.de

Wenn Sie einen Namen haben, den es doppelt oder mehrfach gibt, wurde Ihre E-Mail-Adresse mit einer fortlaufenden Nummer zur eindeutigen Identifikation versehen und würde dann z. B. wie folgt lauten: Vorname.Nachname2@owahoems.hessen.de

2.2 Ihr Initialpasswort

Ihr Initialpasswort wurde Ihnen ebenfalls über das persönliche Anschreiben mitgeteilt. Es ist einmalig gültig und notwendig für die Erstregistrierung, muss aber danach sofort von Ihnen geändert werden. Das entsprechende Vorgehen wird Ihnen im nächsten Kapitel ausführlich erläutert.

Sollte das Anschreiben mit dem Initialpasswort verloren gehen, so müssen Sie über das Kontaktformular eine E-Mail an die HZD schreiben und ein neues Initialpasswort beantragen.

2.3 Ihre Registrierungs-PIN

Auch die Registrierungs-PIN wurde Ihnen zusammen mit Ihrem Benutzernamen und dem Initialpasswort **über das persönliche Anschreiben zugestellt.** Sie dient dazu, Ihr Konto einzurichten und Ihr Gerät (Smartphone oder Tablet) für die Zwei-Faktor-Authentifizierung (2FA) zu registrieren. Aus Sicherheitsgründen enthält der Registrierungs-PIN Sonderzeichen, die im Alltag selten benutzt werden.

2.4 Sicherheitsfrage (KBA-Registrierung)[1]

Im Laufe des Registrierungs- und Anmeldeprozesses werden Sie aufgefordert, die Antwort auf eine persönliche Frage zu hinterlegen, wie zum Beispiel den Namen Ihres ersten Haustieres oder den Geburtsnamen Ihrer Mutter. Diese sogenannte Sicherheitsfrage dient als weiterer Authentifizierungsfaktor, der genutzt wird, wenn Sie z. B. Ihr Passwort vergessen haben und ein Neues erstellen müssen [siehe 4.7: Änderung Ihres Passwortes].

2.5 Der Browserzugang

2.5.1 Browserempfehlung

Die meisten der Standardbrowser eignen sich gut für den Zugriff und können entsprechend verwendet werden. Zu nennen wären hier vor **allem Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Microsoft Edge** sowie der **Apple Browser Safari.** Von dem Einsatz anderer Browser bitten wir abzusehen, da die Anwendung hier weder getestet noch unterstützt werden kann.

2.5.2 Browsereinstellungen

Je nachdem für welchen Browser Sie sich entscheiden, können Unterschiede in der Anwendung auftreten. Beispielsweise können Sie die Richtigkeit Ihrer Passwort Eingabe nicht bei jedem Browser automatisch überprüfen, aber auch die Datenschutzeinstellungen unterscheiden sich.

 Sie können die Drittanbieter Cookies deaktivieren, leider nicht alle.

2.6 Die Zwei-Faktor-Authentifizierung (2FA)

Die Anwendung wurde sicherheits- und datenschutzkonform entwickelt und erfordert aus diesem Grund die Eingabe zweier voneinander unabhängiger Sicherheitsfaktoren, im Unterschied zu der Anmeldung nur mit einem Passwort. Über die 2FA wird die Echtheit der Identität sichergestellt und die Zugriffssicherheit auf besonders schützenswerte Daten erhöht.

[1] Knowledge-Based Authentication

Entscheidend für die Wirksamkeit der 2FA ist, dass der zweite Faktor auf einem anderen Gerät für jede Anmeldung neu, einmalig und nicht nachvollziehbar generiert wird.

2.6.1 Die Authenticator App

Es gibt verschiedene Möglichkeiten, den zweiten Faktor zu generieren, viele Unternehmen, wie zum Beispiel Onlineshops, nutzen Kurznachrichten (SMS), über die dann die Transaktionsnummern als zweiter Faktor verschickt werden. **Im Unterschied dazu bieten Authenticator Apps die Möglichkeit, ohne die Angabe der eigenen Telefonnummer einen zweiten Faktor zur Verfügung zu stellen.** Authenticator Apps können von verschiedenen Anbietern aus dem Internet heruntergeladen werden und auf nahezu jedem mobilen Endgerät einfach und unkompliziert installiert werden.

2.6.1.1 Google Authenticator App

Theoretisch sind fast alle auf dem Markt angebotenen Apps einsetzbar, funktionieren aber alle ein bisschen unterschiedlich. Für die Beschreibungen wurde sich für den Einsatz der Google Authenticator App entschieden, die sowohl in dem Google Play Store als auch im Apple Store kostenfrei verfügbar ist.

Für die Benutzung der Google Authenticator App wird kein Google Konto benötigt.

Wir bitten um Verständnis dafür, dass unser Support Sie lediglich bei der Anwendung dieser App unterstützen kann.

Dieses Handbuch beschreibt die Einrichtung und Verwendung der Google Authenticator App am Beispiel eines Android Smartphones, in dem Erklär-Video für die erste Anmeldung wird jedoch ein iPhone verwendet.

2.6.2 Authenticator für den Desktop des Arbeitsplatzes

Bitte benutzen Sie für die Generierung Ihres Einmalpasswortes ein anderes Gerät als das, mit dem Sie Ihre E-Mails bearbeiten.

Theoretisch ist es zwar möglich, auch auf dem Desktop eine Authenticator App zu installieren, aus Sicherheitsgründen raten wir jedoch davon ab bzw. verweisen auf die Notwendigkeit der Verwendung von zwei verschiedenen Geräten für die Verwendung der E-Mail-Adresse auf der einen und der Generierung des zweiten Faktors auf der anderen Seite.

3 Inbetriebnahme Ihres OWA (Outlook Web Apps) Kontos

Die Inbetriebnahme Ihrer dienstlichen E-Mail-Adresse über Ihr OWA Konto erfolgt in fünf Schritten, die Sie zusammengefasst auf der Rückseite Ihres persönlichen Anschreibens beschrieben finden. Wenn Sie Ihr OWA Konto also bereits in Betrieb genommen und Ihr Smartphone erfolgreich registriert haben, ist dieses Kapitel für Sie nicht interessant, da es die entsprechenden Schritte lediglich ausführlicher beschreibt.

1. Voraussetzungen und Vorbereitungen

2. Authenticator App herunterladen

3. Initialpasswort ändern / eigenes Passwort erstellen

4. Smartphone für die Zwei-Faktor-Authentifizierung registrieren

5. Sicherheitsfrage vergeben

3.1 Voraussetzungen und Vorbereitungen

Nehmen Sie die Anmeldung am besten an Ihrem häuslichen Arbeitsplatz vor bzw. auf Ihrem üblichen Arbeitsgerät. Stellen Sie dann sicher, dass Sie Ihr persönliches Anschreiben mit den Zugangsdaten bereithalten

- Ihren **Benutzernamen** (= Ihre E-Mail-Adresse)
- Ihr **Initialpasswort**
- Ihre **Registrierungs-PIN (**eventuell haben Sie Ihre Registrierungs-PIN bereits digitalisiert und kopierbereit [siehe 3.3: Ihre Registrierungs-PIN].

Des Weiteren benötigen Sie ihre Matrikelnummer bzw. Id. sowie ein zweites Gerät, um die **Authenticator-App** darauf zu installieren und zukünftig darüber den zweiten Sicherheitsfaktor zu generieren, in diesem Handbuch **Einmalpasswort** genannt.

Ihre E-Mail-Adresse benutzen Sie optimaler Weise auf Ihrem Arbeitscomputer, das zweite Gerät ist in der Regel Ihr Smartphone oder Tablet.

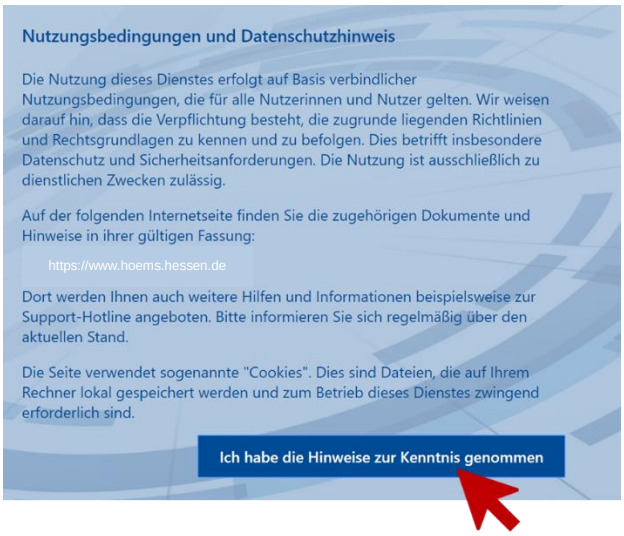
3.2 App herunterladen

Wie angekündigt wird der Prozess der Zwei-Faktor-Authentifizierung in diesem Handbuch mit einem Android Gerät und dem Google Authenticator beschrieben. Weiterhin wird an dieser Stelle das Wissen vorausgesetzt, wie man eine App in den entsprechenden Stores findet und auf dem eigenen Smartphone installiert. Sollte hier dennoch Bedarf bestehen, finden Sie auf den Hilfeseiten der HöMS ein **detailliertes Tutorial.**

Laden Sie die Authenticator App herunter, bevor Sie mit dem nächsten Schritt fortfahren, öffnen Sie diese aber noch nicht, sondern halten Sie nur Ihr Smartphone griffbereit.

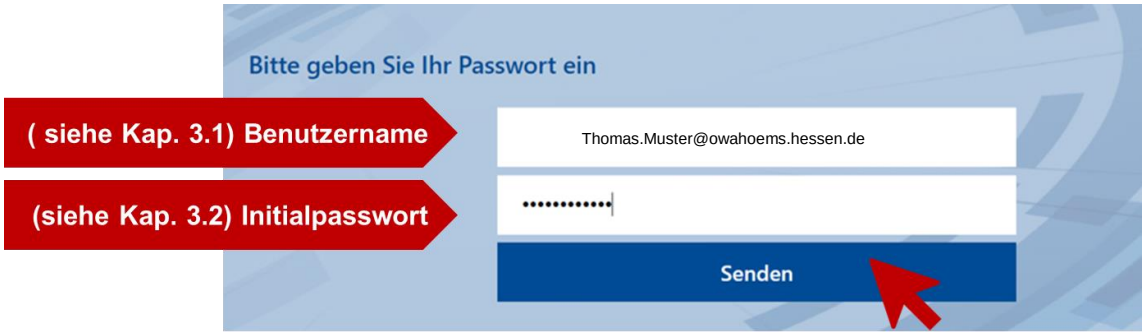
3.3 Initialpasswort ändern / eigenes Passwort erstellen

Vor der Registrierung Ihres Smartphones für die 2FA muss das Ihnen mit dem Anschreiben übersandte Initialpasswort durch ein von Ihnen gewähltes Passwort ersetzt werden. Rufen Sie hierfür bitte über den Browser die folgende Webseite auf: https://selfowa.hessen.de und bestätigen Sie zunächst die Nutzungsbedingungen und den Datenschutzhinweis:

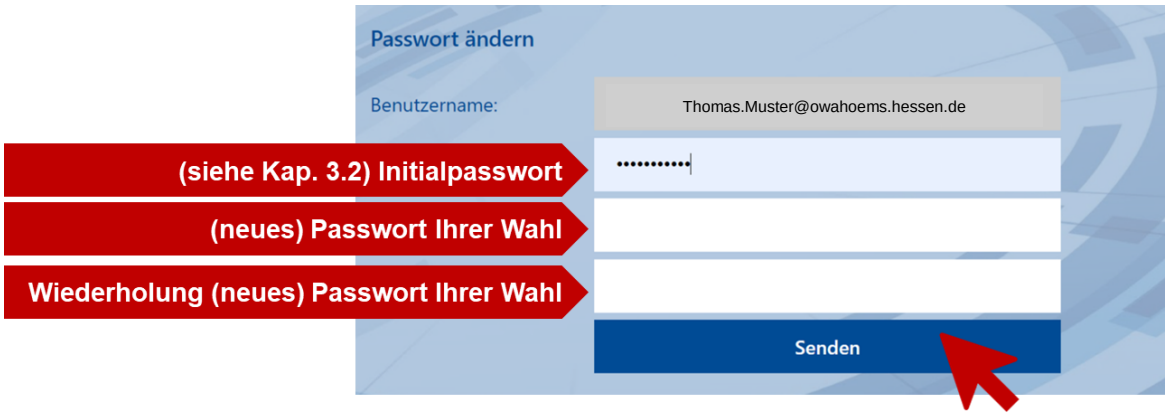


Überprüfen Sie ggf., ob Sie auch das **S** bei https nicht vergessen haben.

Im nächsten Schritt geben Sie Ihren *Benutzernamen* (=Ihre E-Mail-Adresse) und das *Initialpasswort* aus dem Anschreiben ein:



Nach der Bestätigung über *Senden* erscheinen nun zwei weitere Eingabefelder, in die Sie nun jeweils das (neu erstellte) Passwort Ihrer Wahl eintragen. Schließen Sie den Vorgang im Anschluss über *Senden* ab.

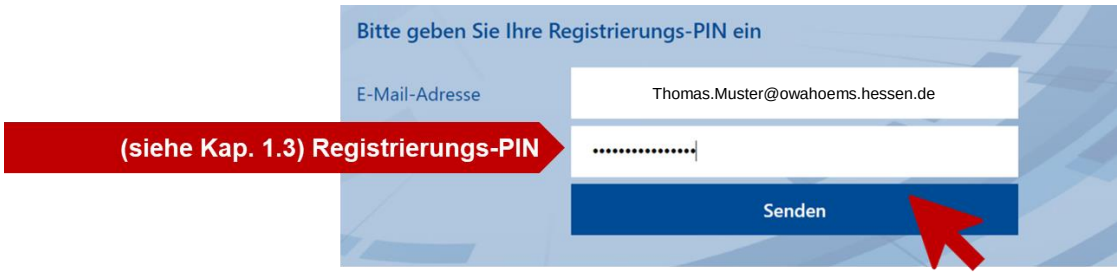


Bitte beachten Sie die Vorgaben für die Erstellung eines sicheren Passwortes.
Sie sind diesem Dokument im Anhang beigefügt:
[siehe 11.2: Anlage 2 - Vorgaben für die Erstellung eines sicheren Passwortes].

3.4 Registrierung Ihres Smartphones

Nachdem Sie Ihr Initialpasswort jetzt durch ein neues und sicheres Passwort ersetzt und bestätigt haben, werden Sie aufgefordert, die *Registrierungs-PIN* aus Ihrem Anschreiben einzutragen.

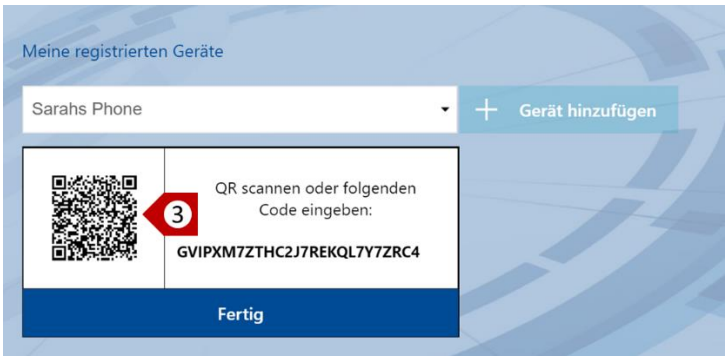
Sie können sich die Eingabe des Registrierungs-Pins zusätzlich erleichtern, **indem Sie die Zeichenfolge zunächst abtippen, auf seine Richtigkeit hin überprüfen und dann in das Eingabefeld kopieren.** Sie verhindern auf diese Weise auch eine mehrmalige Falscheingabe, die zu einer temporären Sperrung führen kann.



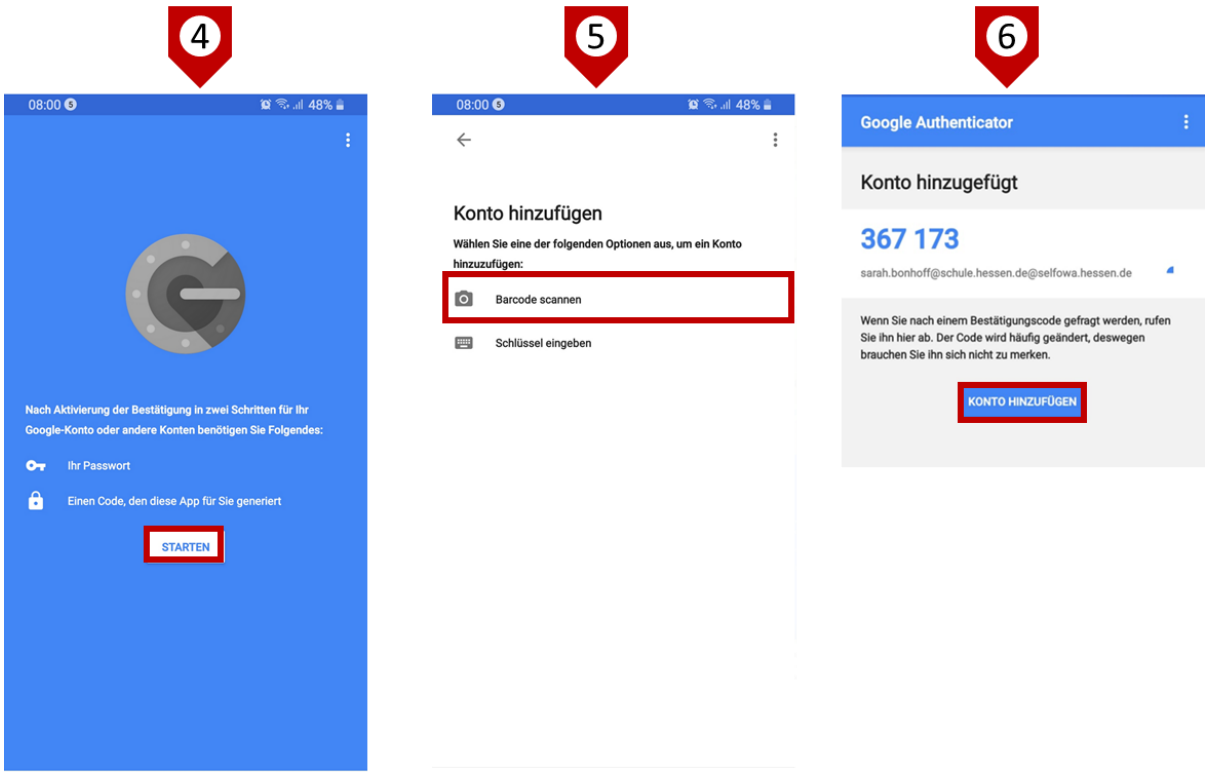
Wenn Sie Ihre Eingabe über *Senden* bestätigt haben, sehen Sie im nächsten Schritt, dass noch kein Gerät registriert ist. Wählen Sie daher nun *+ Gerät hinzufügen* (1) und geben danach Ihrem Gerät einen Namen (2), zum Beispiel: *Myphone*.

Verwenden Sie für den Namen nur Buchstaben, keine Zahl am Anfang und keine Sonderzeichen.

Nach der Bestätigung über *OK* ist Ihr Gerät benannt und es erscheint ein QR-Code (3), über den Sie Ihre bereits heruntergeladene Authenticator App aktivieren können.

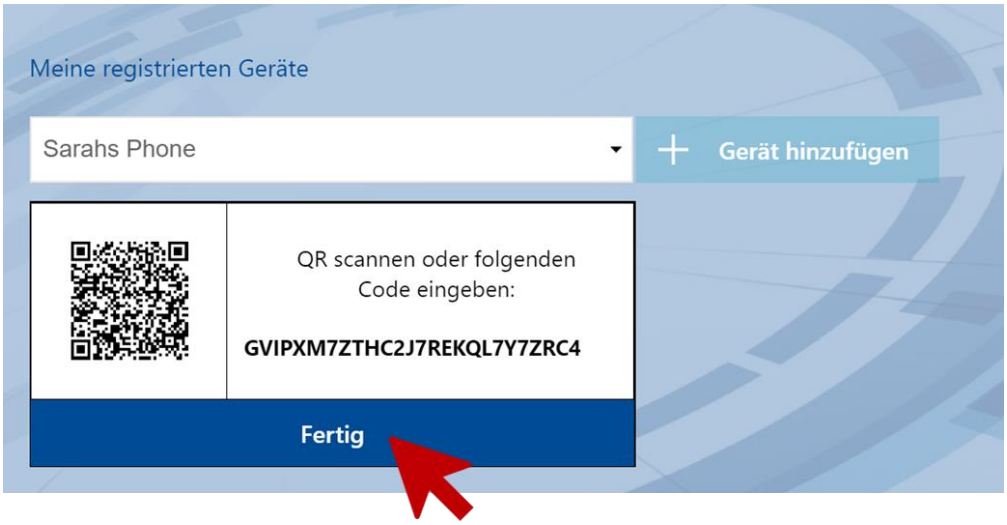


Öffnen Sie hierfür nun die Authenticator App auf Ihrem Smartphone, bestätigen Sie über *Starten* (4) und wählen Sie dann *Barcode scannen* aus (5). Daraufhin öffnet sich automatisch die Kamera Ihres Gerätes, über die Sie nun den QR-Code (= Barcode) einscannen können.



Im Folgenden schließen Sie innerhalb der App die Registrierung Ihres Handys ab, indem Sie *Konto Hinzufügen* aktivieren (6).

In Ihrer OWA Anwendung schließen Sie die Registrierung über *Fertig* ab.



Der Registrierungsprozess bietet Ihnen nun an, über die Eingabe eines Einmalpasswortes den Vorgang zu testen. Da diese aber eher als Übung für den Anwender gedacht ist und nichts als Prüfung für die erfolgreiche Registrierung, wird auf eine Beschreibung an dieser Stelle

verzichtet. Sollte hier dennoch Bedarf bestehen, finden Sie auf den Hilfeseiten der HöMS ein **detailliertes Tutorial.**

Sie haben nun Ihr Smartphone erfolgreich registriert *(MyPhone wurde hinzugefügt*) und die Authenticator App eingerichtet. In Zukunft wird Ihnen jedes Mal, wenn Sie die App öffnen, für 30 Sekunden eine **einmalige, sechsstellige Nummer** angezeigt, die Ihnen für diese Anmeldung als **Einmalpasswort** dient.

Eine andere Bezeichnung für das Einmalpasswort ist OTP (One True Pairing).

3.4.1 Registrierung weiterer Smartphones

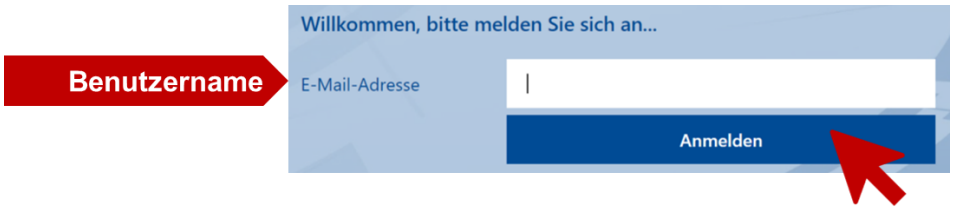
Wenn Sie ein anderes Smartphone oder weitere für die Zwei-Faktor-Authentifizierung registrieren möchten, ist dies jederzeit möglich. Halten Sie hierfür Ihre Registrierungs-PIN bereit und rufen Sie über den Browser die Registrierungsseite https://selfowahoems.hessen.de auf. Hier können Sie das aktuelle Smartphone löschen und gemäß des vorab beschriebenen Vorgehens ein neues Gerät registrieren.

Sie können bis zu vier Smartphones insgesamt registrieren.

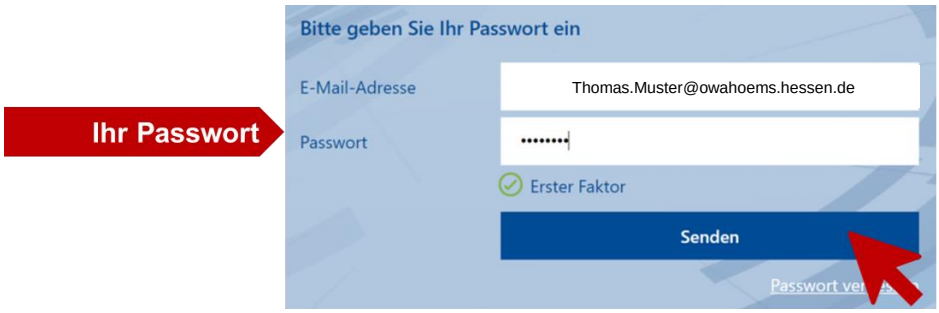
3.5 Sicherheitsfrage vergeben

Nachdem Sie Ihr Smartphone registriert haben, rufen Sie bitte im nächsten Schritt in Ihrem Browser die folgende Adresse auf: https://owahoems.hessen.de und bestätigen zunächst wieder Ihre Kenntnisnahme der Nutzungsbedingungen und des Datenschutzhinweises.

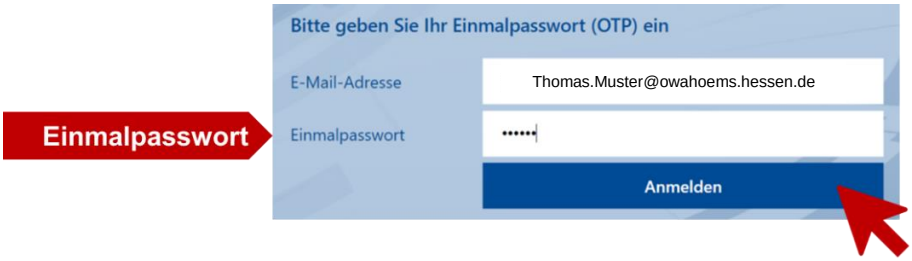
Danach geben Sie wie immer als erstes Ihren **Benutzernamen** *(E-Mail-Adresse)* ein**:**



Fahren fort mit **Ihrem selbst erstellten, aktuellen *Passwort*:**

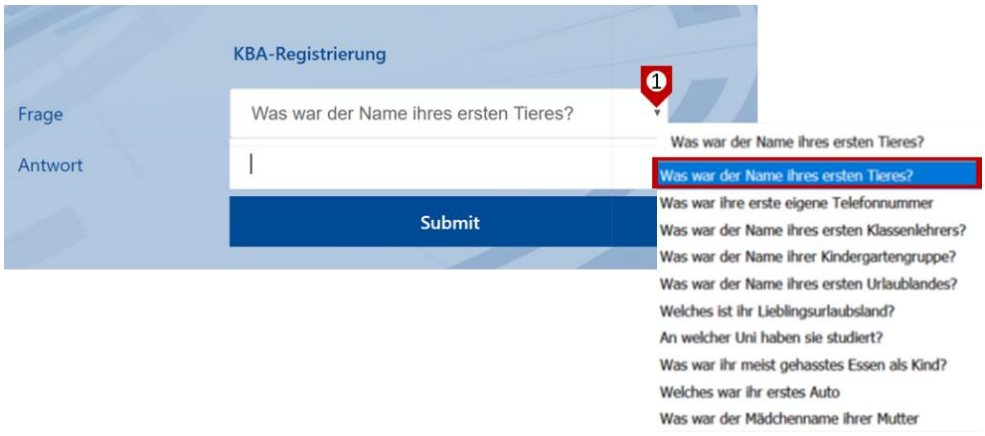


Und fügen als letztes das *Einmalpasswort* aus Ihrer Authenticator App ein:



Da sich das Einmalpasswort (sechsstelliger Zahlencode) alle 30 Sekunden ändert, müssen Sie ziemlich schnell sein. Es kann sonst passieren, dass die angezeigte Ziffernfolge nicht mehr gültig ist. Nach dreimaliger falscher Codeeingabe wird Ihr Konto für 6 Stunden gesperrt, **lassen Sie daher zwischen der Eingabe Ihres Passwortes und der Generierung und Eingabe des zweiten Faktors so wenig Zeit wie möglich vergehen.**

Als nächstes können Sie sich nun über die Direktschaltfläche (1) aus einer Reihe von Möglichkeiten die für Sie passende Frage auswählen und geben Sie die Antwort auf diese Frage in dem Eingabefeld ein. Bestätigen Sie danach über *Submit.*



Seien Sie sicher, dass Sie eine Frage wählen, auf die Sie auch künftig dieselbe Antwort geben würden und/oder notieren Sie die Antwort auf Ihre Sicherheitsfrage am besten getrennt von den anderen Zugangsdaten.

3.6 Anmeldungen nach erfolgter Registrierung

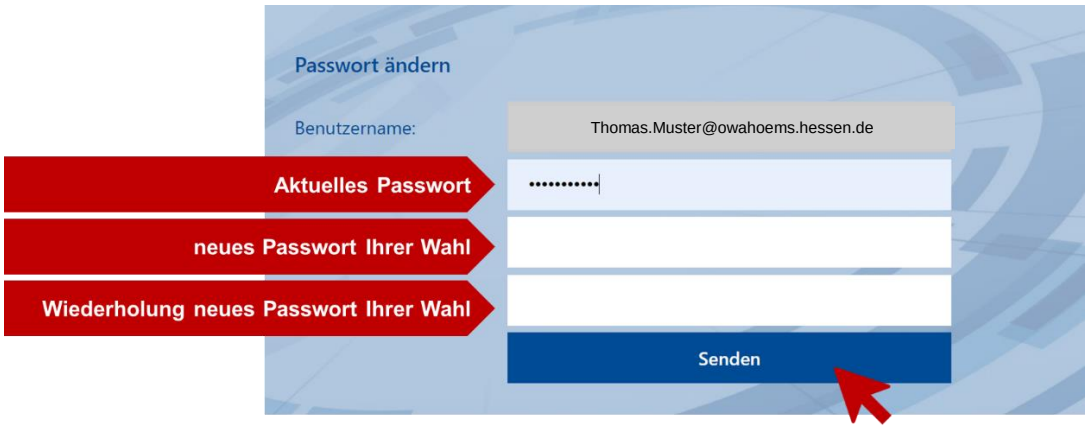
Im Anschluss an die Vergabe der Sicherheitsfrage haben Sie sich das das erste Mal erfolgreich bei Ihrem OWA Konto angemeldet.

Für jede weitere Neuanmeldung navigieren Sie zukünftig ebenfalls über https://owahoems.hessen.de, geben Ihren Benutzernamen, Ihr Passwort sowie das Einmalpasswort aus Ihrer Authenticator App ein.

3.7 Änderung Ihres Passwortes

3.7.1 Regelmäßige Änderung des Passwortes

Sie werden systemseitig alle **42 Tage aufgefordert, Ihr Passwort zu ändern.** In diesem Fall folgen Sie den vorgegebenen Schritten, die im Wesentlichen denen unter 4.3 entsprechen, nur, dass Sie dieses Mal nicht das Initialpasswort ersetzen, sondern Ihr aktuelles Passwort, also immer das letzte, was Sie selbst erstellt haben:



Danach werden Sie wie immer nach dem Einmalpasswort gefragt und können dann ganz normal mit Ihrer Anmeldung fortfahren.

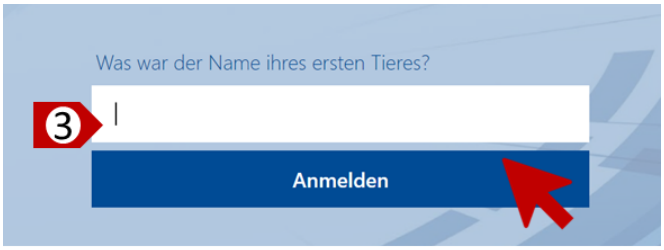
3.7.2 Passwort zurücksetzen

Sollten Sie einmal Ihr Passwort vergessen haben oder es aus anderen Gründen zurücksetzen wollen oder müssen, haben Sie immer bei dem ersten Schritt Ihrer Anmeldung die Möglichkeit, ein neues zu erstellen.

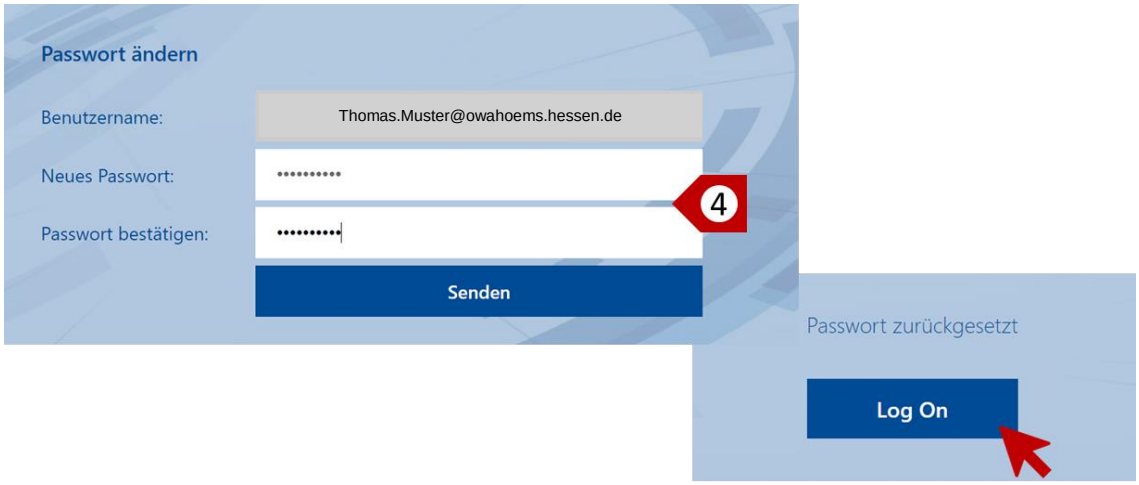
Nach dem Aufruf der Anmeldeseite und der Kenntnisnahme der Nutzungsbedingungen sowie der Datenschutzhinweise geben Sie kein Passwort ein, sondern wählen stattdessen *Passwort vergessen* (1) aus, geben im nächsten Feld Ihre E-Mail-Adresse ein und bestätigen über *Senden.*

Als nächstes generieren Sie über Ihre Authenticator-App das Einmalpasswort, tragen es ein (2) und bestätigen über *Anmelden*.

Als letztes tragen Sie die Antwort auf Ihre gewählte Sicherheitsfrage ein (3).



Danach erstellen Sie unter Berücksichtigung der entsprechenden Vorgaben [siehe Anlage 3 - 11.3: Vorgaben für die Erstellung eines sicheren Passwortes] Ihr neues Passwort, geben es zweimal ein (4) und bestätigen abschießend über *Log On*, ehe Sie sodann mit dem regulären Standardprozess Ihre Anmeldung abschließen.



4 Support und Onlinehilfen

4.1 Hotline:

Der ServiceDesk der HZD ist unter der Telefonnummer: **0611 - 340 8125** zu erreichen.

Montag bis Donnerstag von 08:00 - 16:00 Uhr und

Freitags von 8:00 - 14:30 Uhr

4.2 E-Mail

Per Email ist der IT Service Desk rund um die Uhr zu erreichen, Reaktionen erfolgen allerdings nur innerhalb der Geschäftszeiten.

Hier finden Sie das Kontaktformular der HZD.

4.3 Weitere Dokumente und Links

Weitere Hilfen können Sie der Webseite https://hoems.hessen.de/ entnehmen.