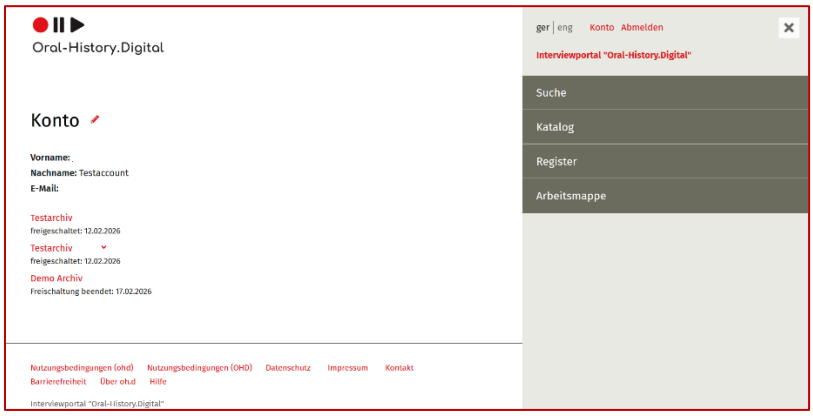
Multi-Faktor-Authentifizierung

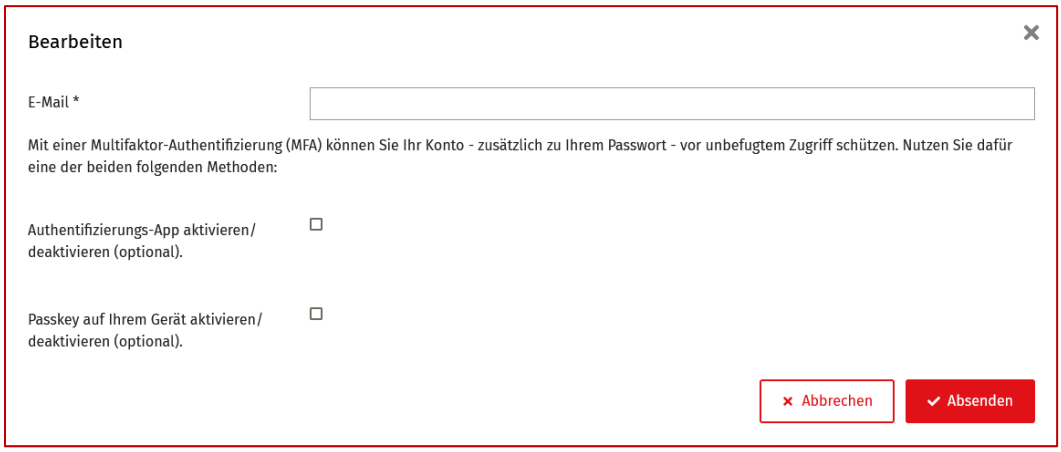
Zur weiteren Stärkung der **IT-Sicherheit** auf der Plattform wird für den Zugang zu *Oral-History.Digital* künftig eine **Multi-Faktor-Authentifizierung** (MFA) eingeführt. Dieses Verfahren erhöht den Schutz vor unbefugtem Zugriff und möglichem Datenmissbrauch, da neben dem Passwort mindestens ein zusätzlicher Authentifizierungsfaktor erforderlich ist.

Das oh.d-Team empfiehlt aus Gründen der Datensicherheit dringend eine Multi-Faktor-Authentifizierung einzurichten.

Nach der Registrierung haben Sie die Möglichkeit in Ihrem **Konto** eine **Multifaktor-Authentifizierung** entweder über eine **Authentifizierungs-App** oder über die Einrichtung eines **Passkeys** einzurichten.



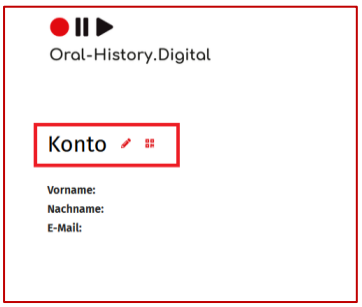
Klicken Sie dafür auf das Stift-Symbol neben dem Konto und wählen Sie die für Sie am besten geeignete Multifaktor-Authentifizierung aus.



Hinweis: Es wird bei der Anmeldung immer die Möglichkeit geben, sich einen Einmal-Code an die hinterlegte E-Mail-Adresse senden zu lassen, für den Fall, dass eine MFA über die App oder per Passkey nicht möglich ist.

Authentifizierungs-App

- Nach der Aktivierung der **MFA** erscheint in Ihrem **Konto** ein Icon für einen QR-Code. Sie haben nun die Möglichkeit, mit einer **Authentifizierungs-App** (2FAS, Authy, Google Authenticator, ...) den QR-Code zu scannen.

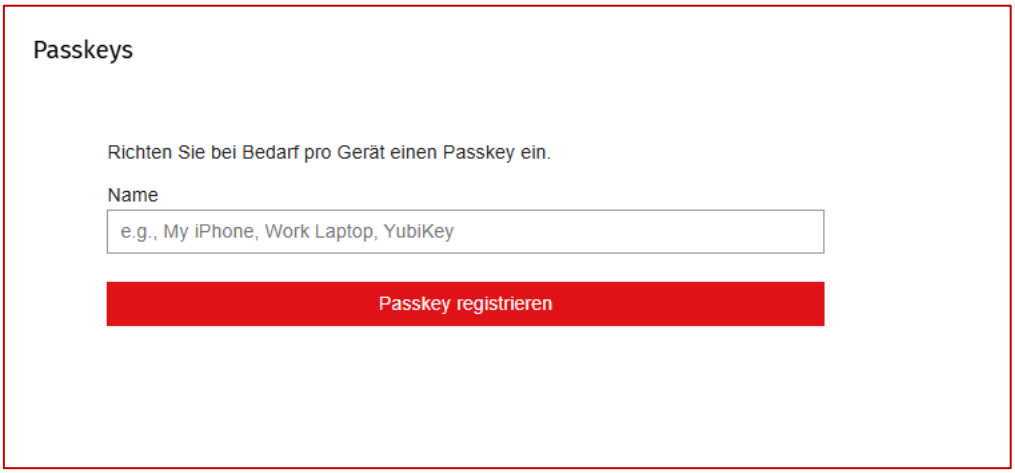


- Nach dem Scannen des **QR-Codes** sollte eine Verknüpfung mit ihrer Authentifizierungs-App hergestellt sein. Sie können nun über die von Ihnen gewählte App Codes für die Authentifizierung beim Anmelden generieren.
- Sollten Sie keine Authentifizierungs-App mit Ihrem Account verknüpft haben oder wenn Sie nicht auf Ihre App zugreifen können, haben Sie zusätzlich die Möglichkeit, sich einen Einmal-Code an die E-Mail-Adresse Ihres Accounts schicken zu lassen.

Passkey

- Anstelle der Authentifizierungs-App können Sie auch ihren **Passkey** mit der oh.d-Anmeldung verknüpfen. Hierfür benötigen Sie zunächst einen Passkey ihrer Wahl (Apple iCLoud Keychain, Microsoft Windows Hello, bitwarden, etc.). Passkeys bieten im Vergleich zu herkömmlichen Passwörtern ein **höheres Sicherheitsniveau**, da sie auf deinem Gerät individuell für jeden Account erzeugt werden und dadurch deutlich besser gegen Phishing-Angriffe geschützt sind.
- Nachdem Sie Passkey aktiviert haben, klicken Sie auf das **Schlüssel-Symbol** neben dem Konto.

- Hier haben Sie nun die Möglichkeit den Passkey Ihres Gerätes hinzuzufügen. Klicken Sie auf Passkey registrieren. Wenn Sie erfolgreich Ihren Passkey verknüpft haben, sollte Ihr Passkey im Pop-Up-Fenster angezeigt werden. Hier haben Sie auch die Gelegenheit, Ihren Passkey zu löschen oder einen anderen Passkey einzurichten.



- Sollte es doch mal Probleme mit ihrem Passkey geben, haben Sie immer die Möglichkeit, sich einen **Einmal-Code** an die E-Mail-Adresse Ihres Accounts schicken zu lassen, um sich dann mit ihrem Passwort anzumelden. Bitte beachten Sie, dass Sie dann auf "Anmelden" und nicht auf "mit Passkey anmelden" klicken.