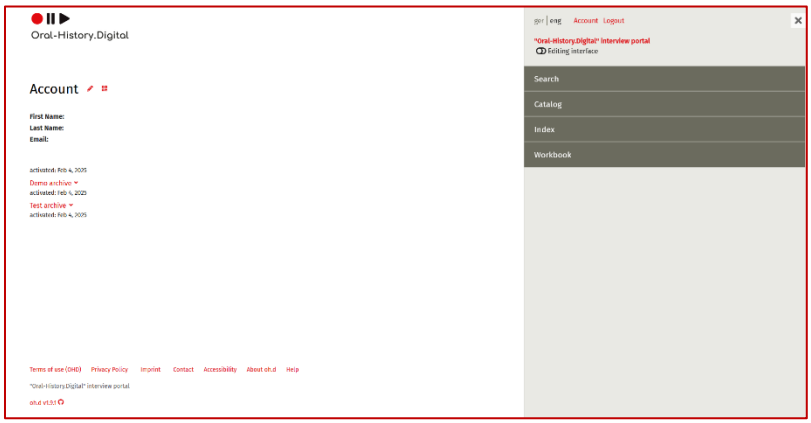
Multi-Factor-Authentification

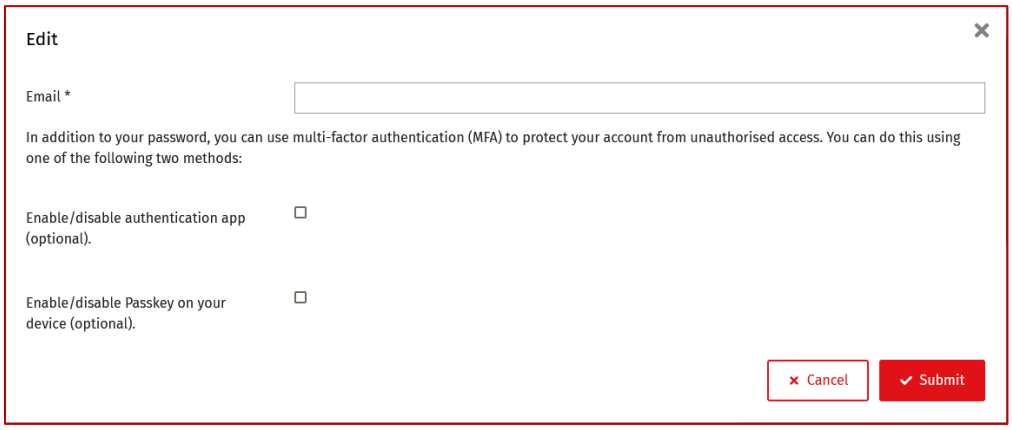
In order to further strengthen **IT security** on the platform, **multi-factor authentication (MFA)** will be introduced to access *Oral-History.Digital*. This procedure will increase protection against unauthorised access and possible misuse of data, as it will require at least one additional authentication factor in addition to the password.

For data security reasons, the oh.d team strongly recommends setting up multi-factor authentication.

Once you have registered, you can set up **multi-factor authentication** in your **account** either via an **authentication app** or by creating a **passkey**.



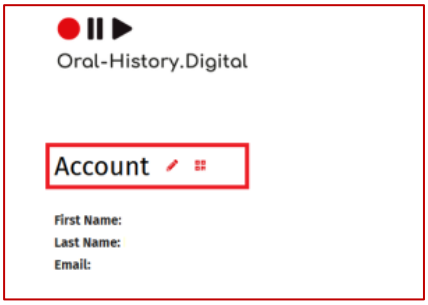
To do this, click on the pencil icon next to your account and select the method that suits you best.



Please note that when logging in, you will always have the option of having a one-time code sent to your registered email address if MFA via the app or passkey is not possible.

Authentication app

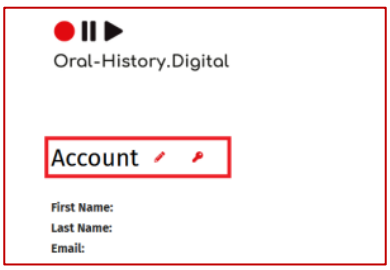
- Once you have activated **MFA**, a QR code icon will appear in your **account**. You can then scan this code using a suitable **authentication app** (such as 2FAS, Authy or Google Authenticator).



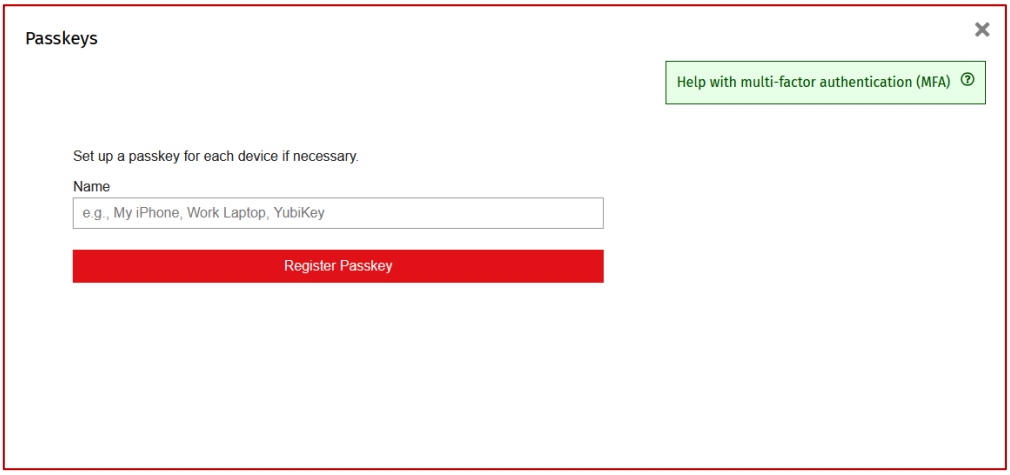
- After scanning the **QR code**, a link to your chosen app should be established. You can then use this app to generate authentication codes when logging in.
- If you do not have an authentication app linked to your account, or if you cannot access it, you can request a one-time code to be sent to the email address associated with your account.

Passkey

- As an alternative to using the authentication app, you can link your **passkey** to your oh.d login. To do this, you will first need to set up a passkey (Apple iCloud Keychain, Microsoft Windows Hello, Bitwarden, etc.). Passkeys offer a **higher level of security** than traditional passwords because they are generated individually for each account on your device, making them much more secure against phishing attacks.
- Once you have activated Passkey, click on the **key icon** next to your account.



- You will now have the option to add your device's passkey. Click Register Passkey. Once your passkey has been successfully linked, it should be displayed in the pop-up window. You can also delete your passkey here or set up a different one.



- If you encounter any problems, you can have a **one-time code** sent to the email address associated with your account, which you can use to log in with your password. Please note that you should click on 'Login' rather than 'Login with passkey'.