Einführung der Multi-Faktor-Authentifizierung

Anleitung

labors.at

Dem Menschen den richtigen Wert geben.

labors.at
Dem Menschen den richtigen Wert geben.

Inhaltsverzeichnis

labors.at
Dem Menschen den richtigen Wert geben.

Darum führt labors.at die Multi-Faktor-Authentifizierung ein

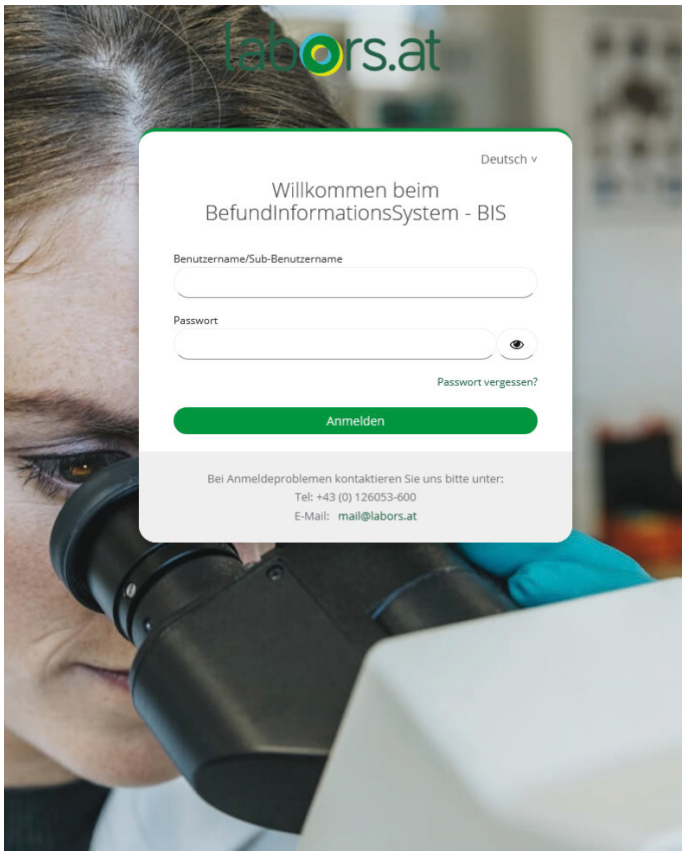
Durch die Nutzung mehrerer Sicherheitsfaktoren – wie z. B. einem Passwort in Kombination mit einem Bestätigungscode auf dem Smartphone – wird das Risiko von Datenlecks und unbefugtem Zugriff deutlich reduziert. Dies ist entscheidend in einer Zeit, in der cyberkriminelle Angriffe auf medizinische Einrichtungen zunehmen. Mit dieser zusätzlichen Sicherheitsstufe gewährleisten wir einen noch besseren Schutz Ihrer Patient:innendaten. Dank neuer technischer Möglichkeiten ist die Einführung der Multifaktor-Authentifizierung jetzt nicht nur einfacher, sondern auch nutzerfreundlicher geworden. Gleichzeitig schaffen wir damit die Grundlage für ein zukünftiges Portal, das Ihnen den Zugang zu einer Vielzahl weiterer Funktionalitäten ermöglichen wird.
Die Multi-Faktor-Authentifizierung wird ab 13.01.2025 anwendbar sein und wir freuen uns, diesen innovativen Schritt mit Ihnen gemeinsam sukzessive umzusetzen.

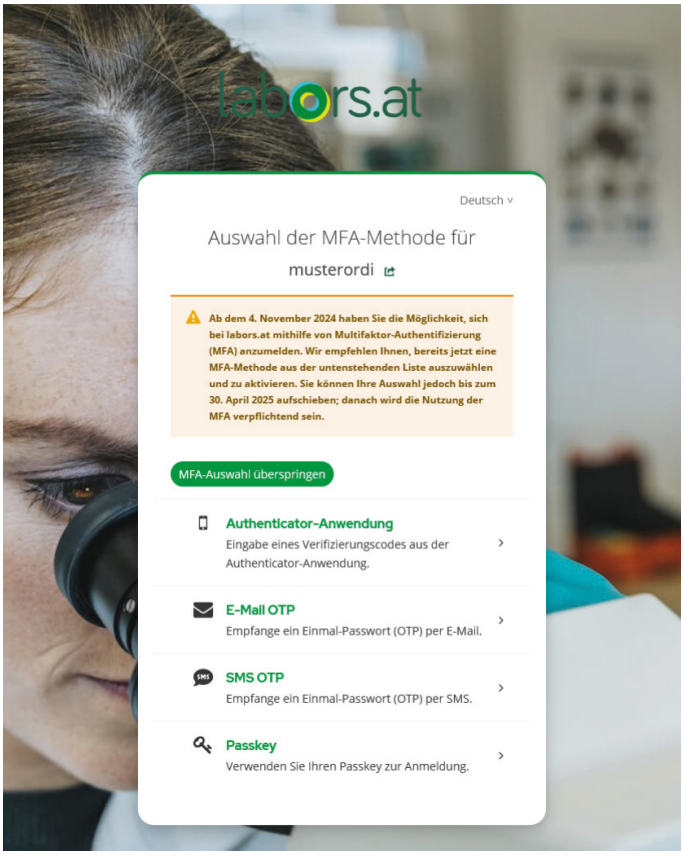
Sie können über den Link:
http://www.labors.at/befundabfrage/?user_type=referrerSubuser
oder über den QR-Code in die Benutzeroberfläche einsteigen

labors.at
Dem Menschen den richtigen Wert geben.

Start und Auswahl MFA-Methode

Sofern Sie dem Link oder QR-Code gefolgt sind, landen Sie auf der Log-In-Seite des Befundinformationssystems,
Hier geben Sie wie gewohnt Benutzernamen und Passwort ein und klicken auf „Anmelden“.



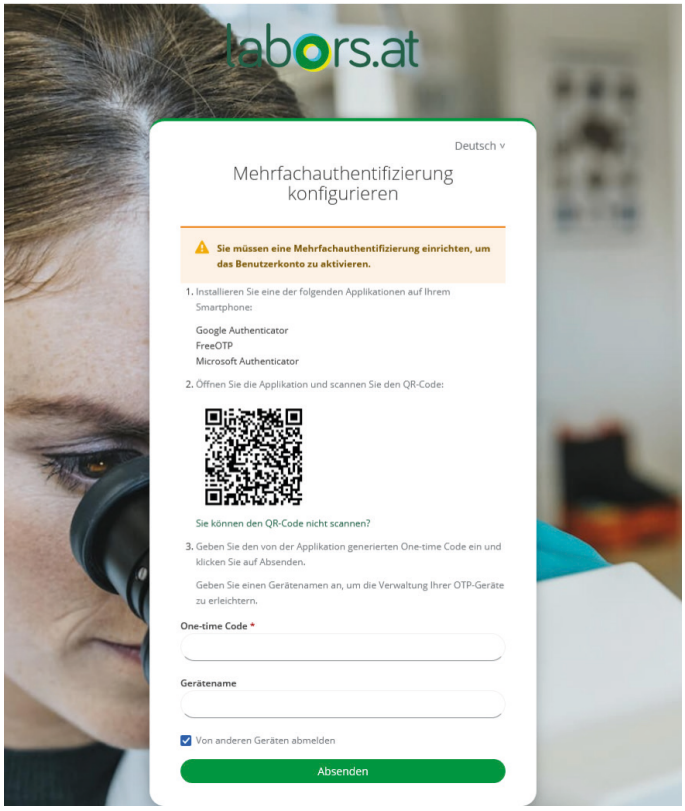


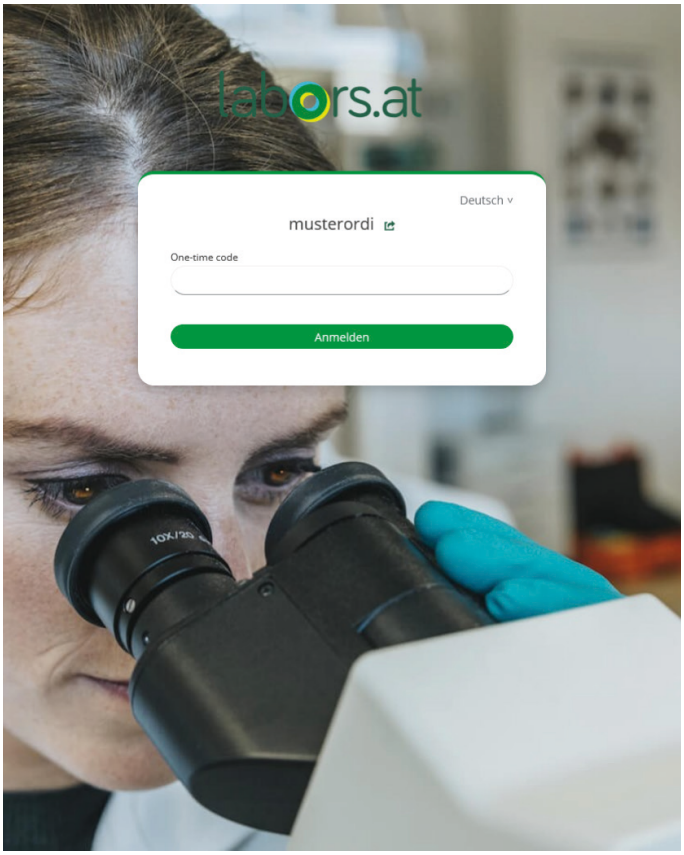
Bitte wählen Sie die MFA-Methode, mit der Sie die Authentifizierung durchführen möchten.
Es stehen die folgenden Methoden zur Auswahl:

- Authenticator-Anwendung S.6
- E-Mail Einmalpasswort (OTP) S.7
- SMS Einmalpasswort (OTP) S.8
- Passkey S.9-10

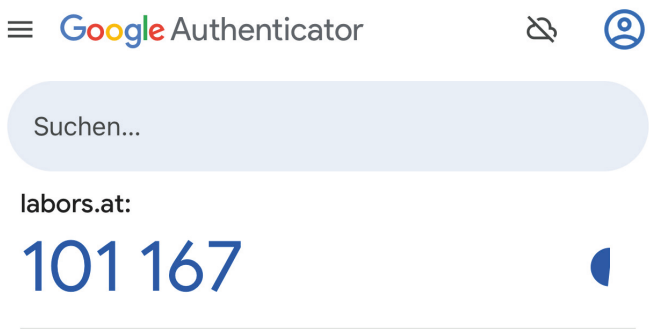
Authenticator-Anwendung

Wenn Sie die Authenticator-Anwendung wählen, kommen Sie zu diesem Bildschirm.
Authenticator-Anwendungen gibt es für Mobiltelefone und PC/Mac.





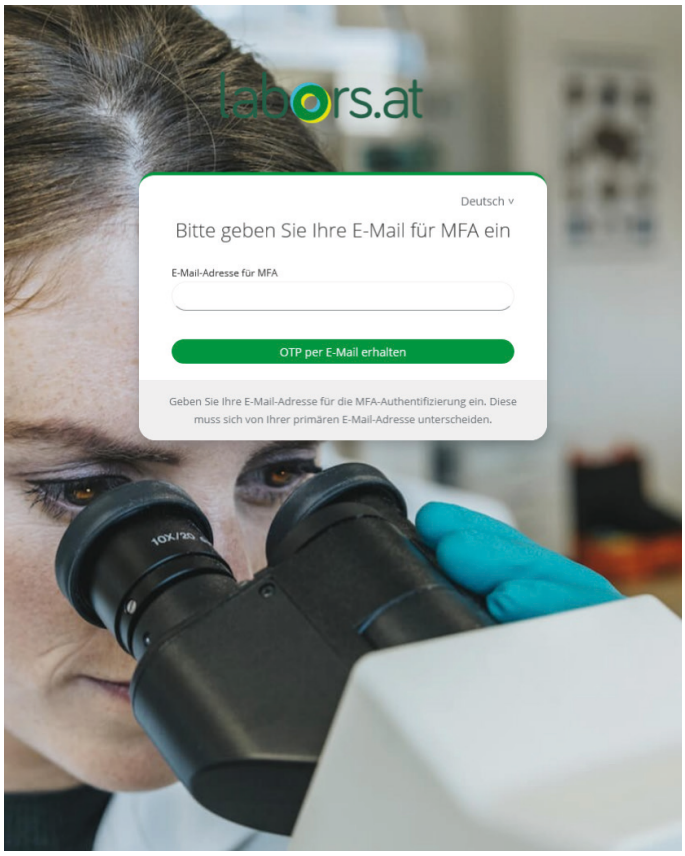
Sie haben die Auswahl zwischen verschiedenen Anbietern.
In der Authenticator-Anwendung wird ein temporär gültiger Code erzeugt, den Sie als zweiten Faktor bei der Anmeldung bei labors.at eingeben können.

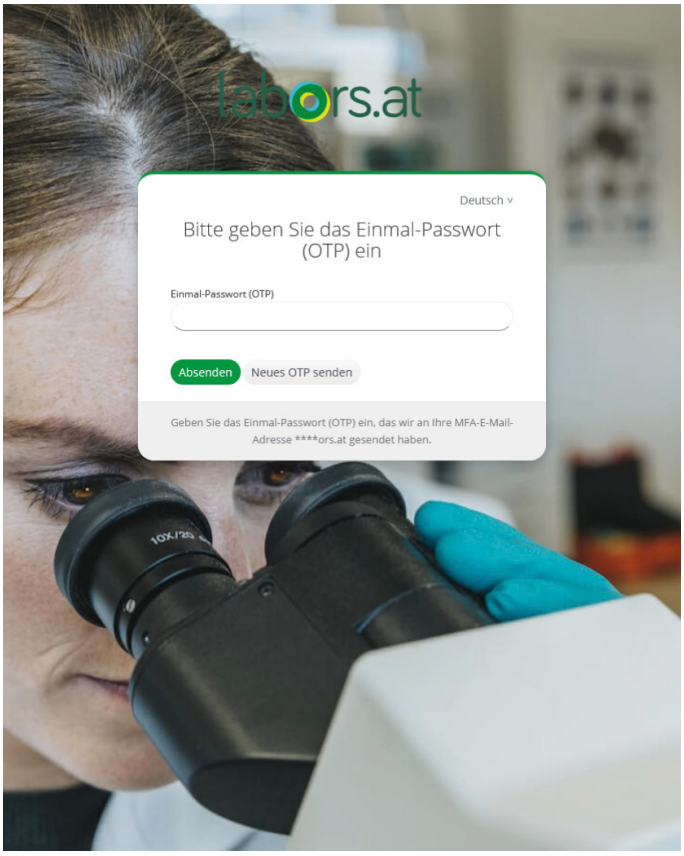


Hier sehen Sie den Google Authentificator als Beispiel

E-Mail OTP

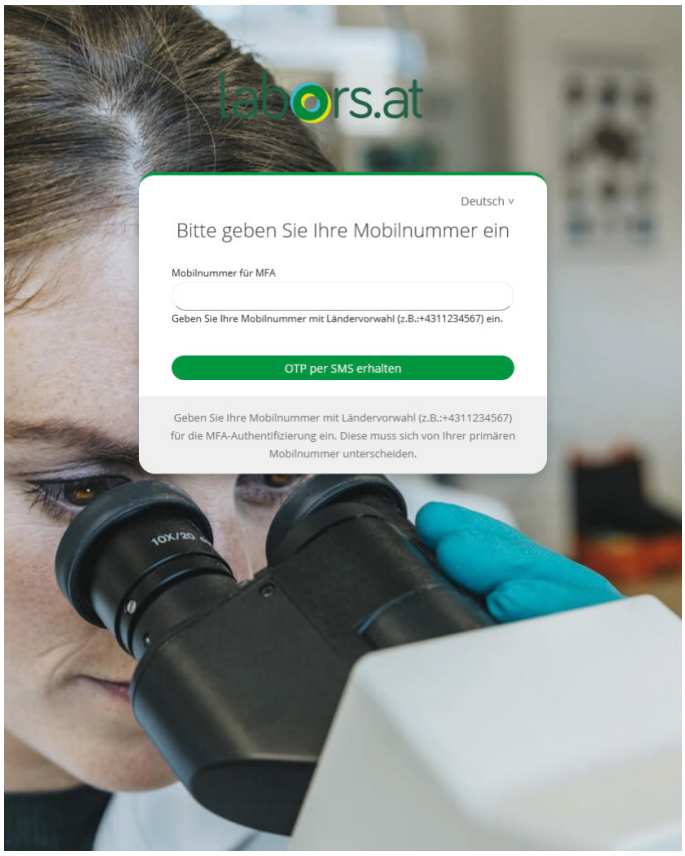
Bei der Nutzung von E-Mail OTP wird ein Einmal-Passwort generiert, welches per E-Mail zugestellt wird. Diese Passwort wird als zweiter Faktor bei der Anmeldung bei labors.at verwendet. Nach der Anmeldung verliert das Passwort seine Gültigkeit und kann für den nächsten Anmeldevorgang nicht mehr verwendet werden. Fordern Sie im Bedarfsfall ganz einfach ein weiteres Einmal-Passwort (OTP) an.
Die E-Mail-Adresse die Sie angeben, darf nicht dieselbe E-Mail-Adresse sein, mit der Sie Ihr Passwort zurücksetzen können.

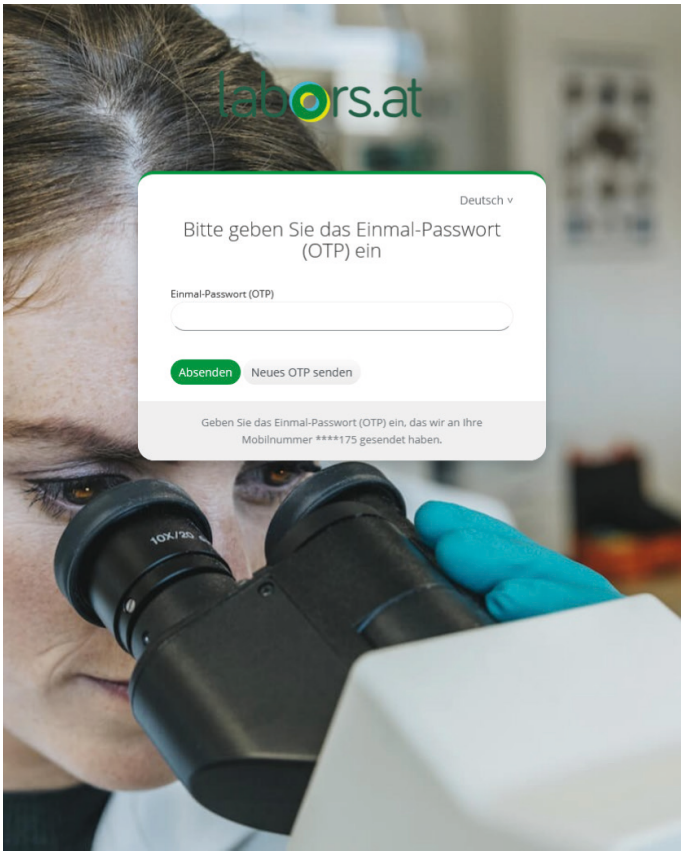




SMS OTP

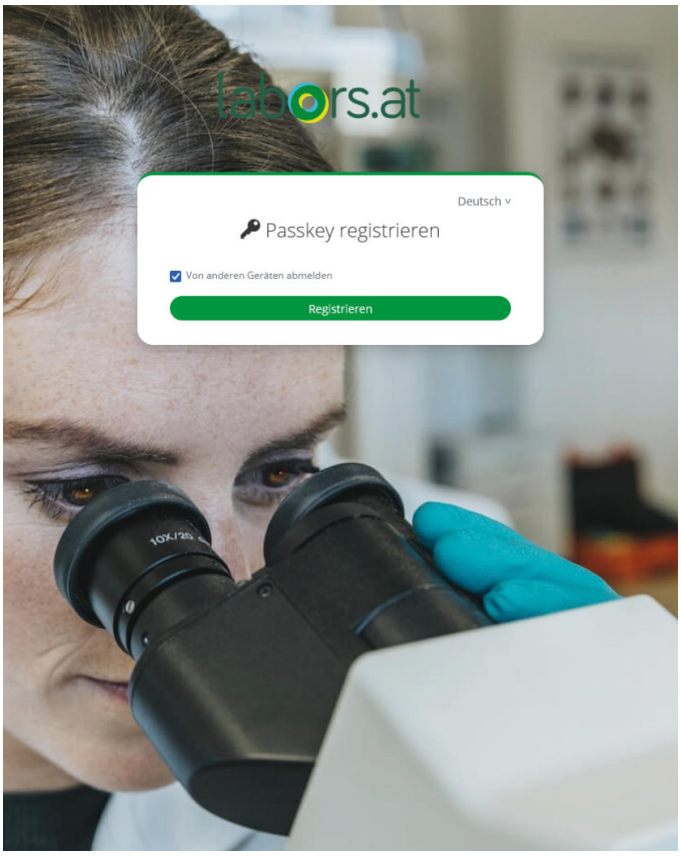
Bei der Nutzung von SMS OTP wird ein Einmal-Passwort generiert, welches per SMS auf Ihr Mobiltelefon zugestellt wird. Dieses Passwort wird als zweiter Faktor bei der Anmeldung verwendet. Nach der Anmeldung verliert das Passwort seine Gültigkeit und kann für den nächsten Anmeldevorgang nicht mehr verwendet werden. Fordern Sie im Bedarfsfall ganz einfach ein weiteres Einmal-Passwort an.

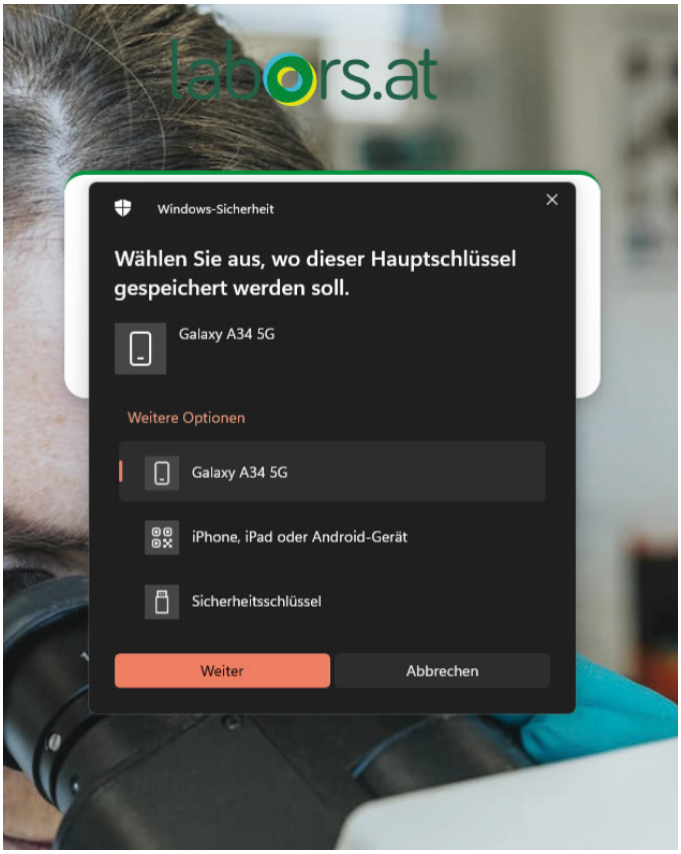


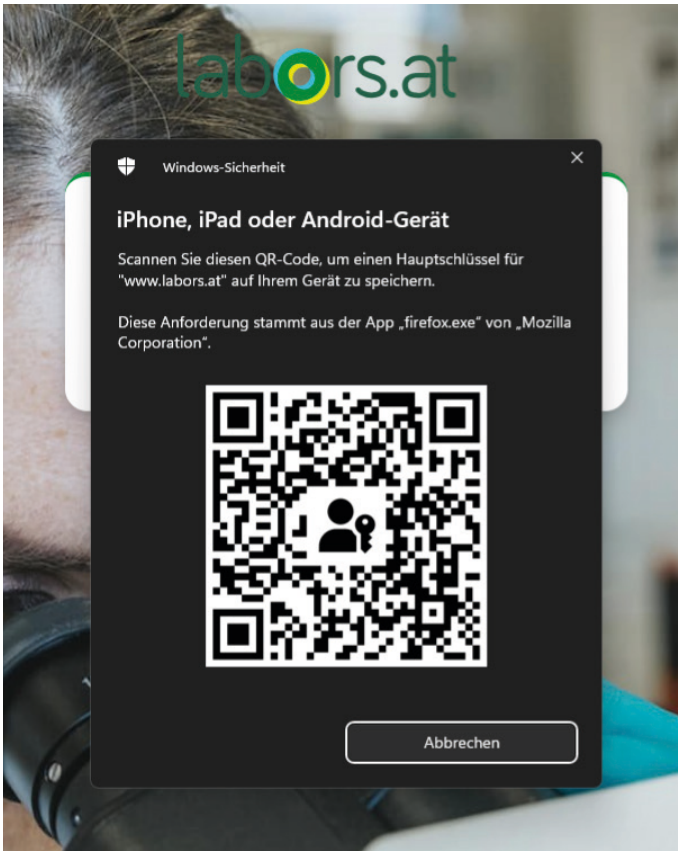


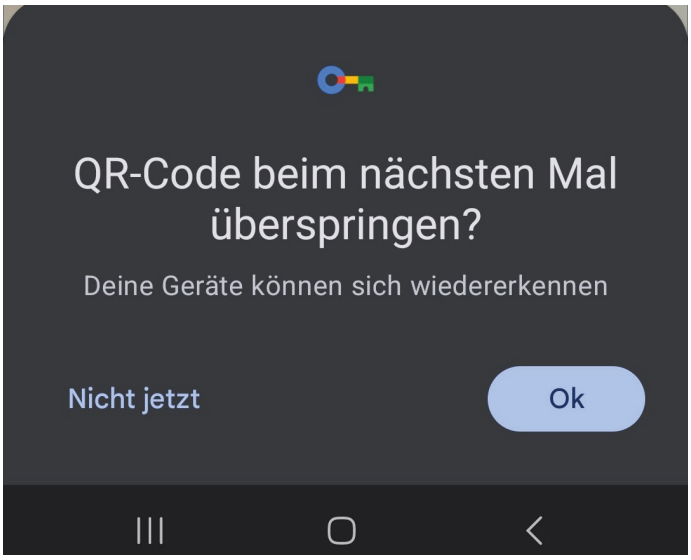
Passkey

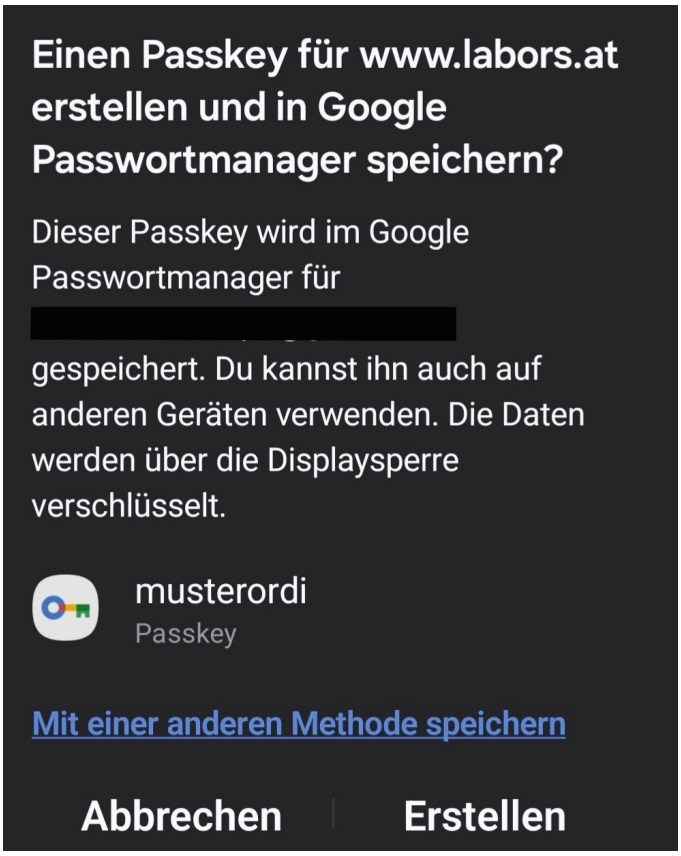
Wenn Sie sich bei labors.at über die MFA-Methode Passkey anmelden, kommuniziert die Website mit dem Passkey auf Ihrem lokalen Gerät (z.B. Mobiltelefon oder PC/Mac). Die Website sendet dazu eine Anfrage. Danach sendet Ihr Gerät eine digitale Signatur an die Website zurück. Sind alle Prüfungen erfolgreich abgeschlossen, sind Sie bei labors.at authentifiziert.
Folgen Sie dazu den Schritten der Screenshots. Je nach Gerät, kann es zu Abweichungen kommen.



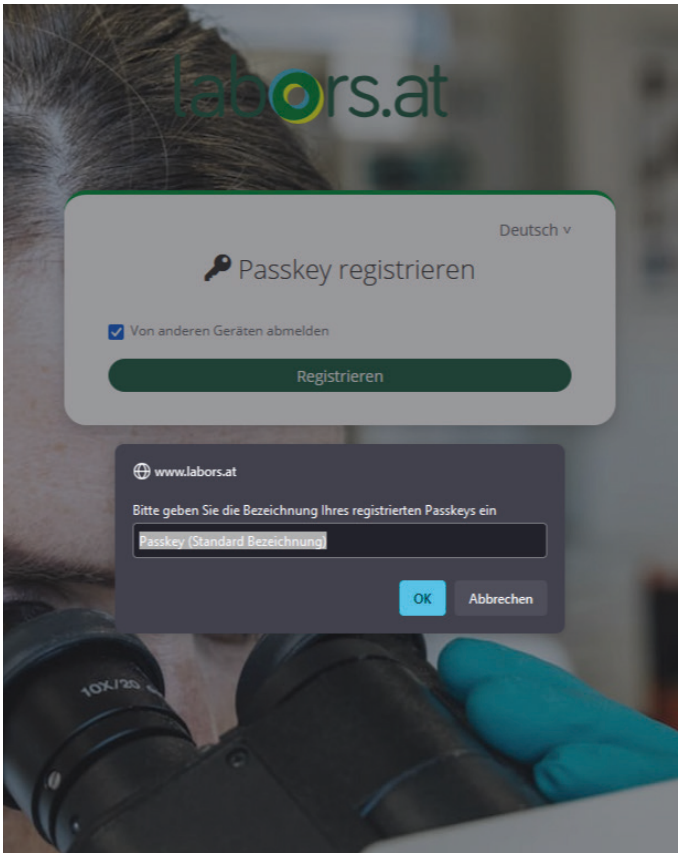





QR-Code beim nächsten Mal überspringen?
Deine Geräte können sich wiedererkennen
Nicht jetzt
Ok


Einen Passkey für www.labors.at erstellen und in Google Passwortmanager speichern?
Dieser Passkey wird im Google Passwortmanager für
[redacted]
gespeichert. Du kannst ihn auch auf anderen Geräten verwenden. Die Daten werden über die Displaysperre verschlüsselt.
musterordi
Passkey
Mit einer anderen Methode speichern
Abbrechen
Erstellen


labors.at
Deutsch
Passkey registrieren
Von anderen Geräten abmelden
Windows-Sicherheit
Hauptschlüssel gespeichert
Sie können sich jetzt mit Ihrem Gerät bei "www.labors.at" anmelden.
OK


labors.at
Deutsch
Passkey registrieren
Von anderen Geräten abmelden
Registrieren
www.labors.at
Bitte geben Sie die Bezeichnung Ihres registrierten Passkeys ein
Passkey (Standard Bezeichnung)
OK
Abbrechen