privacyIDEA Authenticator as authenticator app

20.05.2024 13:47:57

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::Zwei-Faktor-Authentifizierung	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	13:38:25 - 15.12.2023

Schlüsselwörter

2FA App Zweifaktor

Lösung (öffentlich)

The authenticator app "privacyIDEA Authenticator" manages one-time passwords for logging in to web applications and other services. This app is recommended and supported for secure digital login at TU Dresden. The app is multilingual, but does NOT offer a data backup option for the managed one-time passwords. If you lose your smartphone or use a new smartphone, you will need to set up a new token.

To set up a one-time password in the Self-Service-Portal as a second factor for login processes, the following steps are necessary in the app, which are shown using iOS as an example; the procedure is identical under Android:

-

Call up the "privacyIDEA Authenticator" app.

Start the "privacyIDEA Authenticator" app
-

Click on the blue symbol for scanning a QR code at the bottom of the screen.

Screenshot app "privacyIDEA": Start capturing the QR code
-

Take a picture of the QR code displayed in the self-service portal with the smartphone camera.

Screenshot app "privacyIDEA": Scanning QR code
- Enter the one-time password for verification in the self-service portal in the "Verification entry" field.

Screenshot app "privacyIDEA": Display of the one-time password
- The one-time password is available for secure digital login. If you have to create a new token in the self service-portal, the old entry will remain in the "FAS-App". To delete the old entry, swipe the entry to the left once and select "Delete".