

privacyIDEA Authenticator als Authenticator-App

03.07.2024 13:29:08

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::Zwei-Faktor-Authentifizierung	Bewertungen:	2
Status:	öffentlich (Alle)	Ergebnis:	50.00 %
Sprache:	de	Letzte Aktualisierung:	13:34:20 - 15.12.2023

Schlüsselwörter

2FA App Zweifaktor

Lösung (öffentlich)

Die Authenticator-App "privacyIDEA Authenticator" verwaltet Einmalpasswörter zur Anmeldung an Webanwendungen und weiteren Diensten. Für die sichere digitale Anmeldung an der TU Dresden wird diese App empfohlen und unterstützt. Die App ist mehrsprachig, bietet jedoch KEINE Möglichkeit einer Datensicherung (Backup) für die verwalteten Einmalpasswörter an. Im Falle des Verlustes des Smartphones oder bei der Verwendung eines neuen Smartphones müssen Sie sich einen neuen Token einrichten.

Um sich im Self-Service-Portal ein Einmalpasswort als zweiten Faktor für Anmeldevorgänge einzurichten, sind folgende Schritte in der App notwendig, die am Beispiel von iOS gezeigt werden, unter Android ist das Vorgehen identisch:

-

Rufen Sie die App "privacyIDEA Authenticator" auf.

Start der App "privacyIDEA Authenticator"

-

Klicken Sie auf das blaue Symbol zum Scannen eines QR-Codes am unteren Bildrand.

Screenshot App "privacyIDEA": Aufnahme QR-Code starten

-

Nehmen Sie den im Self-Service-Portal angezeigten QR-Code mit der Smartphone-Kamera auf.

Screenshot App "privacyIDEA": QR-Code scannen

-

Geben Sie das Einmalpasswort zur Kontrolle im Self-Service-Portal im Feld "Kontrolleingabe" ein.

-

Das Einmalpasswort steht zur sicheren digitalen Anmeldung zur Verfügung. Wenn Sie sich über das Self-Service-Portal einen neuen Token ausrollen, bleibt der alte Eintrag in der privacyIDEA-App bestehen und muss manuell entfernt werden. Wischen Sie dazu auf dem Eintrag einmal nach links und wählen Sie "Löschen".

Screenshot App "privacyIDEA": Anzeige des Einmalpassworts