1 Privacy Policy: SecuIAM Mobile Token (english)

This privacy policy sets out how the app provider will treat users' personal data. If you do not agree to the terms of this policy, please do not install or use the app.

1.1 THE APP PROVIDER

OEDIV SecuSys GmbH
Brückenweg 5
18146 Rostock

Further details about the app provider can be found in the Legal Notice on our website:
http://www.secusys.de/impressum

1.2 PERSONAL DATA

This app has been designed to collect as little personal data as possible. It collects only the data required for the app to function correctly.

1.2.1 DATA COLLECTION AND STORAGE

The app needs to collect the following data in order to function properly:

- The **device ID** is collected and temporarily stored each time the app is launched. When you register the device, the device ID is passed to the specified server. Device registration is required for the proper functioning of the app.
- The **device name** is collected by the device management system and transmitted to the specified server.
- In order to ensure the correct language is used, the **user language setting** is checked each time the app is launched.
- The **username** and **server address** required for logging on to the SecuIAM Web Portal are stored locally, if entered.

No log data is written to the mobile device. Data on the mobile device is stored permanently until the app is uninstalled.

Please note:
App store operators may collect data in the course of app installation; this is something over which OEDIV SecuSys GmbH has no control. We therefore recommend that you read your app store's Privacy Policy carefully. OEDIV SecuSys GmbH does not collect any data during the installation process.

1.2.2 DATA TRANSFERS TO THIRD PARTIES

We will **never** pass your data to third parties for any purpose whatsoever. In accordance with the purpose of the software, data will be transferred to the specified SecuIAM database.

1.3 SECURITY

If a registered device is lost, the SecuIAM administrator can block it for server-side use. This also disables the dual authentication function.
The app does not call any websites. No password is required.

1.4 PERMISSIONS ENABLED

In order to function properly the app requires the following permissions on the user's mobile device:

- Device identification: access required for dual authentication.
- Internet: access required for the registration process.
- Memory: local memory access required for the storage of username and server address.

The user's rights to delete and correct data:
The user has the right to delete the app at any time, together with all associated data on the device.
It is not possible to delete or correct data in the associated database, as this would defeat the purpose of the app.
A different approach is used for data deletion in the associated database, in line with legal and/or corporate requirements.

1.5 CONTACT

For more information about this app, please contact OEDIV SecuSys GmbH. Contact details can be found in our Legal Notice. Please send any data protection queries to privacy@secusys.de.

Privacy policy version: 27.05.2020

2 Datenschutzerklärung: SecuIAM Mobile Token (deutsch)

Diese Datenschutzerklärung erläutert, wie der Anbieter der App mit personenbezogenen Daten der Nutzer umgeht. Wenn Sie mit dieser Datenschutzerklärung nicht einverstanden sind, sollten Sie die App nicht installieren und nicht nutzen.

2.1 ANBIETER DER APP

OEDIV SecuSys GmbH
Brückenweg 5
18146 Rostock

Nähere Angaben zum Anbieter finden Sie im Impressum der Webseite:
http://www.secusys.de/impressum

2.2 PERSONENBEZOGENE DATEN

Diese App ist so konzipiert, dass so wenig personenbezogene Daten wie möglich erhoben werden. Grundsätzlich werden nur Daten erhoben, die für die technische Funktionsfähigkeit der App erforderlich sind.

2.2.1 DATENERHEBUNG UND -SPEICHERUNG

Für die Nutzung der App-Funktionen ist die Erhebung folgender Daten erforderlich:

- Die **Geräte-ID** wird bei jedem App-Start ermittelt und zwischengespeichert. Bei der Registrierung des Gerätes wird die Geräte-ID an den angegebenen Server übermittelt. Die Registrierung des Gerätes ist Voraussetzung zur sachgemäßen Nutzung.
- Der **Gerätename** wird zur Geräteverwaltung ausgelesen und an den angegebenen Server übermittelt.
- Zur korrekten Sprachausgabe wird bei jedem Starten der App die **Benutzersprache** abgeprüft.
- Der **Username** und die **Serveradresse** für die Anmeldung am SecuIAM Web Portal wird bei Angabe lokal gespeichert.

Auf dem mobilen Gerät erfolgt keine Logschreibung. Die Daten auf dem mobilen Gerät werden bis zur Deinstallation der App **dauerhaft** gespeichert.

Hinweis:
Möglicherweise erheben die App-Store-Betreiber bei der Installation Daten; hierauf hat die OEDIV SecuSys GmbH keinen Einfluss. Wir bitten deshalb um Beachtung der Datenschutz-Hinweise des genutzten App Store. Die OEDIV SecuSys GmbH selbst erhebt bei der Installation der App keine Daten.

2.2.2 DATENÜBERMITTLUNG AN DRITTE

Es erfolgt **keine** Datenübertragung an Dritte, z. B. zur Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung von Telemedien unter Pseudonym.

Als Softwarefunktionalität werden Daten an die entsprechende bi Cube Datenbank übertragen.

2.3 SICHERHEIT

Bei Verlust des Gerätes kann der jeweilige SecuIAM Administrator das registrierte Gerät für den serverseitigen Gebrauch sperren. Damit wird die duale Authentifizierung als Softwarefunktionalität blockiert. In die App ist kein Webseitenaufruf eingebunden. Ein Passwort wird nicht benötigt.

2.4 FÜR DIE APP FREIGESCHALTETE BERECHTIGUNGEN

Für den ordnungsgemäßen Betrieb der App werden folgende Berechtigungen auf dem mobilen Gerät des Nutzers benötigt:

- Gerätekennung: Für die duale Authentifizierung benötigt die App Zugriff auf die Gerätekennung.
- Internetzugriff: Für die Registrierung benötigt die App Zugriff auf das Internet.
- Speicherzugriff: Für das Speichern von Username und Serveradresse benötigt die App Zugriff auf den lokalen Speicher.

Rechte des Nutzers bezüglich Löschung, Berichtigung der Daten:
Der Nutzer hat jederzeit das Recht, die App und damit alle Daten auf dem Gerät zu löschen.
Eine Löschung und Berichtigung von Daten in der angeschlossenen Datenbank ist nicht möglich und unzulässig, da es der inhaltlichen Funktionalität der App widerspricht.
Die Datenlöschung in der angeschlossenen Datenbank erfolgt nach einem separaten Löschkonzept gemäß gesetzlichen oder unternehmerischen Vorgaben.

2.5 KONTAKT

Für Auskünfte zu dieser App können Sie sich stets an die OEDIV SecuSys GmbH wenden. Die Kontaktdaten finden Sie im Impressum.
Datenschutzfragen senden Sie bitte an datenschutz@secusys.de.

Stand der Datenschutzerklärung: 27.05.2020