



SmartToken

Virtuelle Security Token für Ihr Smartphone

Was ist SmartToken?

SmartToken ist eine App für Ihr Smartphone, die Ihnen virtuelle Security Token zur sicheren Authentifizierung am Betriebssystem zur Verfügung stellt. In Verbindung mit der 2-Faktor-Authentifizierungslösung SmartLogon™ gelingt eine sichere und einfache Authentifizierung ganz ohne zusätzliche Hardware.

Wie funktioniert die Lösung?

Die App wird einfach auf einem Smartphone installiert und dient als erster Faktor bei der Authentifizierung. Als zweiter Faktor muss dann nur noch eine kurze PIN direkt am Mobilgerät eingegeben werden oder der Nutzer authentifiziert sich beispielsweise mit einem biometrischen Merkmal über sein Smartphone.

Was macht die Software besonders?

Ist der Nutzer auf seinem Endgerät angemeldet erkennt die App, wenn er sich von seinem Arbeitsplatz entfernt und führt automatisch die Sperrung bzw. Abmeldung durch – und das ganz ohne die Notwendigkeit von aktiviertem Bluetooth. So ist sichergestellt, dass der Rechner stets vor unbefugten Zugriffen geschützt ist.



SmartToken

- ✓ maximale Sicherheit bei der Anmeldung am Betriebssystem
- ✓ bequeme 2-Faktor-Authentifizierung ohne zusätzliche Hardware
- ✓ Smartphone dient als Class2-Leser
- ✓ Autocoupling-Funktion für schnellen Verbindungsaufbau
- ✓ automatische Sperrung/Abmeldung bei Entfernen vom Computer
- ✓ häufige Arbeitsplatzwechsel werden unterstützt

Unser Versprechen als Hersteller

Alle Lösungen aus unserem Haus sind aufgrund von konkreten Anforderungen und Bedürfnissen aus der Praxis entstanden. Viele individuelle Konfigurationsmöglichkeiten bringen die Lösungen daher schon mit. Als Hersteller entwickeln wir jedoch auch gern gemeinsam mit Ihnen Anpassungen, die Ihre spezifischen Anforderungen bestmöglich erfüllen.

Kontakt

digitronic®
computersysteme gmbh
 Oberfrohaer Str. 62
 09117 Chemnitz

+49 371 81539 0
 vertrieb@digitronic.net
 www.digitronic.net



SmartToken

Virtuelle Security Token für Ihr Smartphone

Funktionsweise & Features

In wenigen Minuten herunterladen, installieren und sofort loslegen

Die SmartToken App ist eine Erweiterung der Token Engine von digitronic® und wird anstelle eines physischen Security Tokens in Verbindung mit der Authentifizierungslösung SmartLogon™ für die sichere und bequeme Anmeldung am Betriebssystem verwendet.

Selbstverständlich können mehrere Security Token in der App verwaltet werden – ideal für Administratoren und Umgebungen mit häufigem Arbeitsplatzwechsel. Um bei mehreren Security Token nicht den Überblick zu verlieren, lässt sich die Autocoupling-Funktion natürlich auch deaktivieren.

In der aktuellsten Version von SmartLogon™ sind bereits alle technischen Anforderungen implementiert, um SmartToken nutzen zu können. Sie müssen die Anwendung nur noch über den App Store bzw. Google Play Store herunterladen und installieren.

Technische Details

Unterstützte Betriebssysteme

Android und iOS

Download

Google Play Store & App Store

Voraussetzungen

SmartLogon™ sowie Token Engine mit der Erweiterung RemoteToken müssen auf dem Endgerät installiert sein.

Download unter:

<https://www.digitronic.net/download-smartlogon/>

Kostenfreier Testzeitraum

Die Authentifizierungssoftware SmartLogon™ kann 30 Tage kostenfrei getestet werden. Die Verwendung der SmartToken App ist kostenfrei.

Sicherheitsinformationen

Das Smartphone baut keine direkte Verbindung zum Rechner oder zu schützendem Endgerät auf. Stattdessen übernimmt ein Relay Service die Kommunikation. Die Verbindung zwischen den einzelnen Komponenten ist durch eine Transportverschlüsselung gesichert. Zusätzlich ist die Beziehung vom Smartphone zum Gerät Ende-zu-Ende-verschlüsselt. Auf dem Smartphone selbst wird zum Schutz der Daten das Trusted Platform Module (TPM) verwendet. Damit ist ein Extrahieren der Schlüssel nicht möglich.

Das Smartphone dient als Class2-Leser, d.h. die PIN-Eingabe bei der Authentifizierung erfolgt direkt über das Smartphone. Es werden keine Passwörter auf dem Endgerät gespeichert.

Die Verwendung der SmartToken App auf gerooteten Smartphones wird aus Sicherheitsgründen nicht empfohlen.

digitronic[®]
net