

KEYIDENTITY AUTHENTICATOR - PUSH-TOKEN

KOMFORTABLE MFA AUTHENTIFIZIERUNG FÜR LOGINS UND TRANSAKTIONEN MIT EINEM SCHRITT.

Die Herausforderung, vollkommen neue Anwendungsfälle mit Multi-Faktor-Authentifizierung (MFA) abzusichern, erfordert einen hohen Level an Verwendbarkeit ohne Vernachlässigung der Sicherheit.

Die Authentifizierung von Logins und Transaktionen kann mit Hilfe des KeyIdentity Push-Tokens schnell und einfach durch den Benutzer bestätigt werden. Basierend auf der bewährten Sicherheit von LinOTP und den Möglichkeiten moderner, mobiler Plattformen, wird die Nutzbarkeit und die Sicherheit gegenüber klassischen Software-Token erheblich erhöht.

Die starke Integration in die bewährte KeyIdentity MFA Plattform ermöglicht die Nutzung des KeyIdentity Push-Token in

bestehenden, klassischen MFA Szenarien. Der „API first“ Ansatz vereinfacht die Integration in bestehende Anwendungen und bringt einen hohen ROI bei einer einfachen, zentralen Administration.

Die hohe Nutzbarkeit, gepaart mit dem Transaktions-basierten Verfahren des KeyIdentity Push-Token, erlaubt eine einfache Implementierung von Transaktionsabsicherungen. „4 Augen Prinzip“ und „N von M“ Szenarien können schnell und einfach in bestehende Umgebungen eingebunden werden. Basierend auf der Möglichkeit zur Ablehnung von Transaktionen durch den Benutzer, können Betrugsversuche schnell erkannt, verhindert und Reaktionen eingeleitet werden.

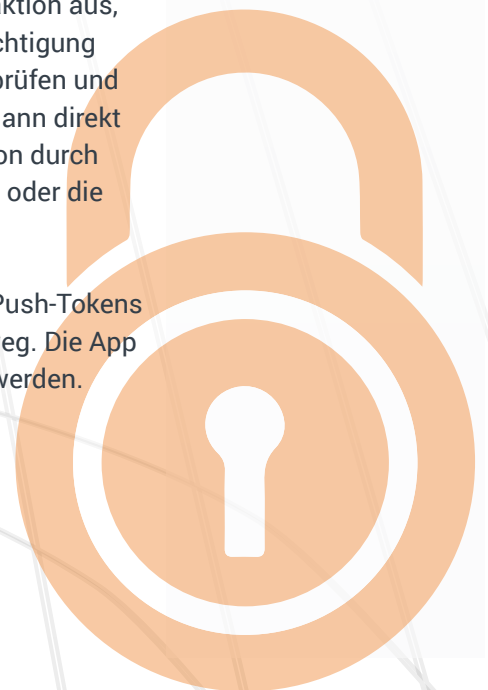
Push-Token

- Einfacher Rollout durch QR-Code basiertes Verfahren. Im Self Service oder Out-of-Band.
- Hohe Nutzerakzeptanz durch einfache Nutzung.
- Idealer Ausgangspunkt für „4 Augen“ und „N von M“ Szenarien.
- Optional mit der Offline-Fähigkeit des KeyIdentity QR-Token kombinierbar.

Funktionsweise des KeyIdentity-PushToken

Greift der Benutzer auf einen geschützten Inhalt zu oder führt eine Transaktion aus, wird eine Push-Bestätigung ausgelöst. Der Benutzer erhält eine Benachrichtigung auf dem eingerichteten mobilen Endgerät und kann die Transaktion dort prüfen und direkt bestätigen oder ablehnen. Die kryptographische Bestätigung wird dann direkt an den definierten Endpunkt gesendet. Es ist keine Eingabe zur Transaktion durch den Benutzer notwendig. Der Zugriff auf den Inhalt wird dann freigegeben oder die Transaktion durchgeführt.

Im Hintergrund sorgen die kryptographischen Verfahren des KeyIdentity Push-Tokens für eine Absicherung der Transaktion gegen Eingriffe auf dem Transportweg. Die App kann optional mit einem Passwort zusätzlich kryptographisch gesichert werden.



Mehr Sicherheit durch Token plus KeyIdentity Authenticator

Der KeyIdentity Push-Token ist voll in die KeyIdentity MFA Plattform integriert. Im Zusammenspiel mit den KeyIdentity Authentication Providern für Windows und macOS wird der Desktop-Login um eine einfache MFA Authentifizierung erweitert. Der Benutzer kann den Login mit einfach nachzuvollbaren Daten auf dem mobilen Endgerät abgleichen und bestätigen. Es ist keine weitere Eingabe durch den Benutzer notwendig.

Im Zusammenspiel mit dem KeyIdentity QR-Token sind hier auch Offline Szenarien einfach umsetzbar.

Technische Daten

Plattformen: Der KeyIdentity Push-Token und QR-Token werden durch den KeyIdentity Authenticator für iOS 9.0 (und größer) und Android 5.0 (und höher) bereitgestellt.	Backend: Der KeyIdentity Push-Token basiert auf der bewährten KeyIdentity MFA Plattform, verfügbar on-premise und als Cloud, mit dem Open Source Kern LinOTP von KeyIdentity.
Integrationen: • Native Integration mit offener API • KeyIdentity Authentication Provider for operating system Microsoft Windows/macOS • SAML	Rollout-Möglichkeiten: • Out-of-Band (z.B. Brief) • Self Service durch den Benutzer • Repairing (optional) • Gerätewechsel (optional)
Branding KeyIdentity bietet optional die Möglichkeit, den KeyIdentity Authenticator in Branding und CI des Kunden zur Verfügung zu stellen. Hier ist neben der Möglichkeit der optischen Anpassung auch eine Anpassung der Funktionalität an die Anforderungen umsetzbar. So kann die Passwortvergabe erzwungen werden oder ein Gerätewechsel optional erlaubt werden.	

Über KeyIdentity

KeyIdentity ist ein globaler Anbieter von skalierbaren, einfach einzusetzenden Multi-Faktor-Authentifizierungslösungen (MFA), welche die Absicherung von Authentifizierung und Transaktionen auf Open Source-Basis ermöglicht. Die LinOTP Suite bietet durch SVA, LAP und weitere Produkte unternehmensrelevante Funktionen und ist durch einen API First-Ansatz einfach zu integrieren. Zusätzlich werden Kunden von KeyIdentity durch die Sicherheitsberatung Foxmole mit tiefem Fachwissen unterstützt. Fox-

mole bietet eine Reihe von strategischen und diagnostischen Dienstleistungen wie Security-Assessments, Penetrationstests und Source Code Audits, sowie Managed Security Services, um die Auswirkungen von Datenschutzverletzungen zu reduzieren und Best Practices zu schaffen. Die durch die Beratertätigkeit gewonnenen Erkenntnisse helfen KeyIdentity außerdem, neue innovative Produkte zu entwickeln.

KeyIdentity GmbH

Robert-Koch-Strasse 9 |
64331 Weiterstadt |
Germany

+49 6151 860 86-0 |
info@keyidentity.com

www.keyidentity.com