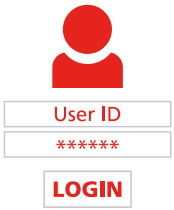
Multi-Faktor-Authentifizierung.

Etwas, das Sie wissen.



Etwas, das Sie haben.

Etwas, das Sie sind.

KEYIDENTITY

Leicht gemacht!

Rufen Sie uns doch einfach mal an

+41 44 552 44 88

KeyIdentity´s LinOTP

KeyIdentity´s LinOTP ist die höchst skalierbare, am einfachsten zu integrierende und am schnellsten betriebsbereite Multi-Faktor-Authentifizierungslösung (MFA). Durch den modularen Aufbau und den API-First Gedanken ist LinOTP zukunftssicher. Das sowohl im Hinblick auf zukünftige Authentifizierungsmöglichkeiten, als auch auf später benötigte Use-Cases. Dank dem Open-Source-Kern ist die Lösung auditierbar, transparent und garantiert ohne Hintertüren. Die LinOTP-Suite kann für das Zusammenspiel existierender Tokens konfiguriert werden. Damit werden bestehende Investitionen geschützt und Vendor-Lock-Ins vermieden. Mit der Transaktionssicherheit schützt KeyIdentity kritische Unternehmensprozesse auf einfachem Weg und unterstützt Sie bei der Digitalisierung. Easy-to-use ist der Schlachtruf und das Produkt ist genau das: Es ist einfach zu bedienen, erfüllt die höchsten Sicherheitsansprüche, wird komplett in Deutschland entwickelt und betrieben und schützt die größten Kunden-Umgebungen und Clouds.

Warum Multi-Faktor-Authentifizierung?

- **Schwache Passwörter**
  LinOTPs MFA Lösung reduziert die Risiken von Datenschutzverletzungen selbst dann, wenn ein Hacker ein schwaches Passwort knacken kann, denn der zweite Faktor bleibt ihm unbekannt.
- **Betrug**
  KeyIdentity ermöglicht die Implementierung zusätzlicher Authentifizierungsanforderungen für Transaktionen mit hohem Wert. So werden Betrüger der Möglichkeit beraubt, Geldmittel vom dem Konto eines potentiellen Opfers zu transferieren.
- **Compliance**
  Die Verwendung einer MFA aus LinOTP verringert die Auswirkungen einer Datenschutzverletzung, da sie eine eindeutige Kennung erfordert, bevor der Zugriff auf ein System oder Konto gewährt wird.
- **Phishing**
  Dank der MFA, die im Moment eines Phishing-Versuchs eingefordert wird, kann der Angreifer keinen Schaden anrichten.
- **Anbieterabhängigkeit**
  LinOTP verfügt über eine herstellerneutrale API-first-Architektur, die die Integration beschleunigt, während sie eine Reihe von etablierten Standards unterstützt.
- **Hohe Benutzerakzeptanz**
  LinOTP verfügt über eine Reihe von leichten und einfachen Lösungen, um eine schnelle Akzeptanz bei den Mitarbeitern anzutreiben. Dazu gehören Hardware und digitale Tokens, eine Offline-Authentifizierung und QR-Codes.

Das 1x1 der Passwörter

Ein einzelnes Passwort …

… ist leicht zu hacken.
Die meisten Benutzer verwenden die gleichen Passwörter wieder und wieder und nehmen nur geringfügige Änderungen vor, wenn sie diese aktualisieren müssen oder ein neues Konto eröffnen.

… wird geteilt.
Insbesondere im Fall von unternehmensbezogenen Anwendungen können Anmeldeinformationen unter Umständen von einem Teammitglied an ein anderes in der irrigen Ansicht weitergegeben werden, dass dies weniger Zeitaufwand für die Administration bedeutet und möglicherweise Lizenzgebühren spart.

… ist schwer zu merken.
Das Aufzwingen eines übermäßig komplizierten Passworts birgt bekanntermaßen das Risiko, dass das Passwort nicht angenommen oder vergessen wird. Dazu kommen Sicherheitsrisiken, wenn es irgendwo aufgeschrieben werden muss.

Smart Virtual Applicance

Die KeyIdentity Smart Virtual Appliance (SVA) ist eine Plattform, um LinOTP und andere KeyIdentity Produkte einfach in verschiedensten IT-Umgebung auszurollen. Als komplette Lösung erlaubt Sie Ihnen, alle Aspekte der Konfiguration des Betriebssystems und der betriebssystemnahen Komponenten einer LinOTP Installation zu konfigurieren.

Die KeyIdentity Smart Virtual Appliance ist eine robuste, einfach zu installierende, virtuelle Appliance. Sie ist ausgelegt für den dauerhaften und sicheren Betrieb der KeyIdentity Produkte, insbesondere LinOTP. Die SVA ist eine komplette, integrierte und sofort einsatzfähige Backend-Lösung für die Integration eines herstellerunabhängigen MFA Token Management in Enterprise- und Cloudumgebungen. LinOTP, RADIUS Server, eine graphische Oberfläche und Self Service sind installiert und integriert konfiguriert. Starten Sie die Installation von der erhaltenen ISO, lassen Sie den Wizard laufen und schon ist Ihr System zur MFA-Authentifizierung verfügbar. Die SVA wurde sowohl für kleine als auch große Umgebungen ausgelegt.

Übersicht der KeyIdentity Smart Virtual Applicance

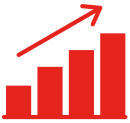
Anzahl Tokens	Preis pro Token in CHF für 1 Jahr	Preis pro Token in CHF für 3 Jahre
10-49		
50-99		
100-249		
250-499		
500-749		
750-999		
1000+		

Preise auf Anfrage

Diese Branchen benötigen Multi-Faktor-Authentifizierung

Telekommunikation

Handel



Finanzwesen

Versicherung

Behördenwesen

Öffentlichen Dienst

Online Shops

ALLNET® SWISS

the network people

ALLNET Schweiz AG
Thurgauerstrasse 117, 8152 Glattpark

Tel.: +41 44 552 44 88
Fax: +41 44 552 44 81

E-Mail: info@allnetch.com
www.allnetch.com