KEYIDENTITY

KI-AUTHENTICATION PROVIDER FÜR DAS BETRIEBSSYSTEM MICROSOFT WINDOWS

MFA AUTHENTIFIZIERUNG FÜR DESKTOP, SERVER UND TERMINALSERVER

Die alleinige Authentifizierung mit Passwörtern ist immer stärker automatisierten und großflächigen Angriffen ausgesetzt. Speziell die Verwendung von Rechnern in mobilen Szenarien beim Kunden, auf Konferenzen oder auf Reisen stellt extreme Anforderungen an die Passwortsicherheit.

Das Etablieren immer komplexerer Passwortrichtlinien erreicht die Grenzen der Nutzerakzeptanz und bringt nur einen geringen Sicherheitsgewinn gegen computergestützte Angriffe.

Die starke Authentifizierung mit der KeyIdentity MFA Plattform bringt eine signifikante Steigerung der Sicherheit und erlaubt gleichzeitig eine hohe Nutzerakzeptanz durch moderne Authentifizierungsverfahren.

Die KeyIdentity Authentication Provider (KAP) für die Betriebssysteme Microsoft Windows und macOS erlauben eine einfache und sichere Authentifizierung, nativ integriert in die Authentifizierungsframeworks der Hersteller.

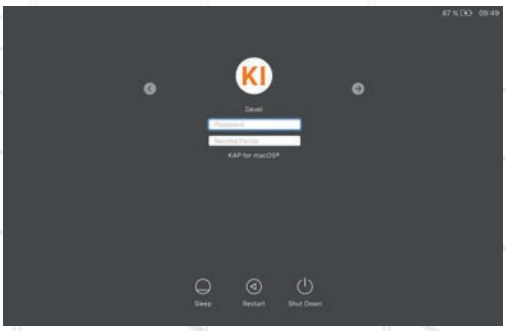
Durch die Möglichkeit der Offline-Authentifizierung kann die einfach auszurollende und managebare MFA Authentifizierung auch in mobilen Szenarien glänzen. Es werden keine zusätzlichen Lesegeräte oder CA-Setup benötigt. Laptop und Smart-Phone des Mitarbeiters reichen aus, um eine sichere Authentifizierung auch in kritischen Umgebungen zu gewährleisten.

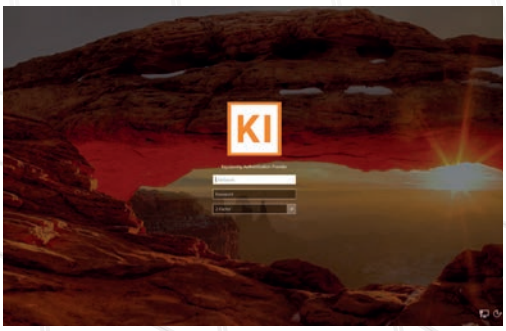
Der KAP bringt die volle Funktionalität der KeyIdentity MFA Plattform direkt zum Benutzer. Neben der fortgeschrittenen Möglichkeit der Offline-Authentifizierung durch den KeyIdentity QR-Token, werden alle durch LinOTP unterstützte Hardware- und Software-Token, inklusive des Push-Token, abgebildet.

Dabei werden die Möglichkeiten der Microsoft Windows und macOS Umgebungen durch die Unterstützung von nativen Methoden der Administration (z.B. Gruppenrichtlinien) ausgenutzt.

Authentication Provider

- Unterstützung der KeyIdentity Push-Token und QR-Token
- Offline Authentifizierung
- Einfacher Rollout durch betriebssystemeigene Mechanismen
- Einfache Verwaltung
- LinOTP API oder RADIUS als Backend
- Unterstützung von Hochverfügbarkeits- und Fail-Over-Szenarien
- breite Unterstützung von Hardware-Token (z.B. Feitian, Yubikey, Gemalto SafeNet, usw.)
- breite Unterstützung von Software-Token (z.B. KeyIdentity Authenticator, FreeOTP, Google Authenticator, Authomator (Blackberry), Microsoft Authenticator, SMS/ mTAN, E-Mail)





mit KeyIdentity KAP für Windows -> OTP-Abfrage für den 2. Faktor

Datenblatt Authentication Provider

KEYIDENTITY

Anpassung an Ihre Bedürfnisse

Basierend auf dem Credential Provider Framework von Micrsoft Windows und den Authentication Plugins von macOS erlaubt der KAP eine große Bandbreite von Authentifizierungsmöglichkeiten. Dabei wird individuell auf den Risikolevel und die Bedürfnisse eines Benutzers eingegangen. Die KeyIdentity MFA Plattform mit LinOTP als Open Source Kern erlaubt eine individuelle Zuordnung von Tokentypen und Tokeneigenschaften.

Der KAP unterstützt standardmäßig eine direkte Verbindung an die mächtige und offene API von LinOTP, um fortgeschrittene Authentifizierungen wie den KeyIdentity Push-Token und QR-Token und die damit möglichen Szenarien wie die Offline-Authentifizierung zu ermöglichen. Zusätzlich wird das RADIUS Protokoll zur Anbindung klassischer Umgebungen unterstützt.

Anwendung in Ihrem Netzwerk

Der KAP kann individuell und koordiniert per Softwareverteilung verteilt und konfiguriert werden. Alle Einstellungen werden in nativen Bereichen abgelegt und können zentral verwaltet werden.

Die Integration in die Authentifizierung von Microsoft und macOS erlaubt eine einfache Verwaltung der Authentifizierung durch ein natives grafisches Frontend.

Der Benutzer erhält, je nach eingesetzten Tokentypen konfigurierbar, einen bekannten, nativen, erweiterten Login-Dialog. Hier werden alle von LinOTP unterstützten Tokentypen zur Authentifizierung abgebildet.

Offline Authentifizierung

In der Verbindung mit KeyIdentity LinOTP und dem KAP QR-Token können auch mobile Zugriffsszenarien umgesetzt werden. Dabei ermöglicht die Verwendung des Smartphones als Token eine hohe Nutzerfreundlichkeit und Flexibilität.

Der Benutzer authentifiziert sich regulär mit Benutzername und Passwort und bekommt einen QR-Code angezeigt. Dieser wird mit dem KeyIdentity Authenticator gescannt und die resultierenden Verifizierungsdaten an den LinOTP Server übertragen und verarbeitet. Der Benutzer wird ohne weitere Eingaben eingeloggt.

Im Offlinefall wird im KeyIdentity Authenticator eine TAN erzeugt, die im KAP eingegeben und verifiziert wird.

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 an und ist durch einen API First-Ansatz einfach zu integrieren.

Technische Daten

Unterstützte Plattformen:

- **Microsoft Windows 10, Microsoft Windows 8.1**
- **Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2008 R2**
- **macOS 10.11 und 10.12**

Backend:

- **KeyIdentity LinOTP**
- **KeyIdentity SVA**
- **KeyIdentity Cloud**
- **RADIUS basierte Backends**

KeyIdentity GmbH

Robert-Koch-Strasse 9 |
64331 Weiterstadt |
Germany

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

www.keyidentity.com

2017/04/DB_KAP/V1