APIIDA

MOBILE AUTHENTICATION

BEYOND PASSWORDS

Willkommen am Arbeitsplatz der Zukunft!

Wir bei APIIDA sind davon überzeugt, dass sich die Vorteile eines modernen Arbeitsplatzes und eine hohe Sicherheit kombinieren lassen. Digitalisierung nicht zum Selbstzweck, sondern als Grundlage einer verbesserten und einfacheren Art zu arbeiten.

Geh mit uns den Weg in eine digitale Zukunft, in der Du im Mittelpunkt stehst!

Anmeldung kann so einfach sein!

… verabschiede Dich von komplexen Passwörtern

… verzichte auf zusätzliche Hardware wie Smartcards und Smartcardlesegeräte

… mach Dein Smartphone zum sicheren Schlüssel

… nutze ein einheitliches anwendungsübergreifendes Anmeldeerlebnis

… sperre Deinen Arbeitsplatz automatisch

Beschütze Dein Unternehmen

Brute Force

10 Sekunden benötigt ein Hacker für das Knacken eines typischen Passworts. Das sichere Passwort von heute ist morgen bereits eine Schwachstelle. Mit der Einführung einer 2 Faktor Authentifzierungslösung verhinderst Du jetzt und in Zukunft Brute Force Angriffe auf die Systeme und Netzwerke Deines Unternehmens.

Social Hacking

Hacker verschaffen sich von Benutzern wertvolle Informationen für einen Systemzugriff durch Phishing Mails etc. Durch die Ergänzung des Anmeldeverfahrens um das Smartphone verhinderst Du die ungewollte Weitergabe von Systemzugriffen.

Haftnotizen

Der Ausweg für viele Benutzer, komplexe Passwortrichtlinien zu erfüllen, sind viel zu oft Haftnotizen an Monitoren. Mit der Vereinfachung des Anmeldeverfahrens werden Sicherheitsvorschriften in den Arbeitsalltag integriert und implizit eingehalten.

Zusätzliche Hardware

Smartcards und Smartcardlesegeräte machen das Verwalten, Mitführen und die Verwendung zusätzlicher Hardware notwendig. Ersetze die Smartcard durch Dein Smartphone, ohne Deine hohen Sicherheitsanforderungen einzuschränken.

„Passwörter bieten nicht den notwendigen Schutz für Deine Daten!“

APIIDA

MOBILE AUTHENTICATION

BEYOND PASSWORDS

USE CASES

1. Primäre Authentifizierung

Melde Dich mit APIIDA Mobile Authentication und Deinem Smartphone an Deinem Windows System an - ganz ohne Passwort.

2. Sekundäre Authentifizierung

Nutze APIIDA Mobile Authentication und Dein Smartphone für die Anmeldung an einer Citrix Umgebung. Mit unserer Lösung ist auch eine sichere Anmeldung an VPN, SSH & RDP Verbindungen möglich.

3. Browserbasierte Authentifizierung

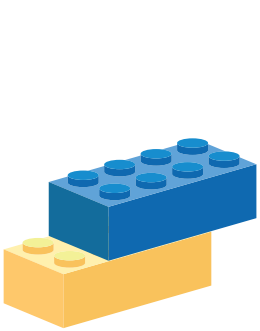
Nutze Dein Smartphone, um Dich direkt oder via Single Sign-On (SSO) sicher an Webanwendungen anzumelden.*

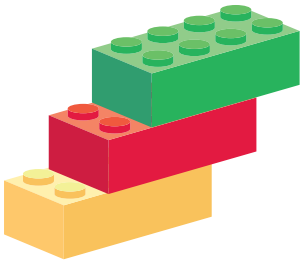
4. Digitale Unterschrift

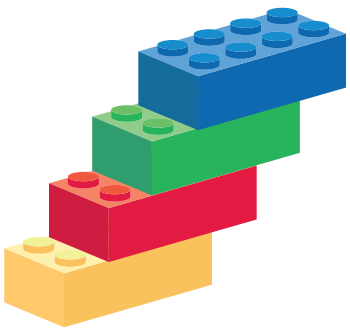
Mit APIIDA Mobile Authentication kannst Du Deine E-Mails signieren und in Zukunft verschlüsseln. Nutze auch hierfür einfach Dein Smartphone im Zusammenspiel mit unserer App.*

Auf Deine Bedürfnisse zugeschnitten:

Wir können unsere Lösung APIIDA Mobile Authentication ganz individuell auf Deine Bedürfnisse zuschneiden. Ob einfache Primär-Authentifizierung oder die Transformation Deiner Anwendungslandschaft, Du entscheidest!







*Beta Feature

Sicherheit bis ins Detail

2 FA + Lokal + Zertifikatsbasiert = sichere Authentifizierung

Smartphone

APIIDA Mobile Authentication unterstützt sowohl iOS sowie Android. Auf dem Smartphone ist die App „APIIDA Mobile Authentication“ via AppStore oder PlayStore zu installieren. Beim Anmeldeprozess kann je nach Gerätetyp die TouchID, FaceID oder eine PIN verwendet werden. Die Identität des Benutzers ist sicher auf dem Trusted Execution Environment des Smartphones hinterlegt.

Windows

Bei der Einrichtung der APIIDA Mobile Authentication Clientkomponente wird der Credential Provider und der APIIDA BLE Service lokal auf dem Windows System installiert. Meldet sich ein Benutzer an, kommuniziert das Smartphone über den BLE-Service verschlüsselt mit dem Credential Provider.

Active Directory

Bei einem Active Directory handelt es sich um einen Verzeichnisdienst. Für die Funktionsfähigkeit der Lösung muss auf Kundenseite ein integrationsfähiges lokales AD oder Azure AD zur Verfügung stehen. Um zu bestimmen, wer ein Zertifikat beantragen darf, benötigt das Backend lesenden Zugriff auf das Kunden-AD.

Backend

Das APIIDA Mobile Authentication Backend wird durch die APIIDA AG verwaltet und benötigt eine lesende Integration zum lokalen AD oder Azure AD des Kunden. Das Backend umfasst das Selfservice Portal, die Benutzerverwaltungskomponente und eine Certificate Authority (CA). Die Benutzer und Zertifikate können über das Backend administrativ verwaltet werden.

APIIDA
MOBILE AUTHENTICATION
BEYOND PASSWORDS

Made in Germany

Wähle aus zwei Optionen

APIIDA Mobile Authentication Server

APIIDA Mobile Authentication kann in eine bestehende lokale oder eine Cloud-Umgebung installiert werden. Dabei ist die Integration an ein bestehendes Active Director (AD) und eine bereits vorhandene PKI notwendig.

APIIDA Mobile Authentication SaaS

Bei der Serviceoption werden die APIIDA Mobile Authentication Komponenten und eine Certificate Authority von APIIDA selbst verwaltet. Dabei wird ein lokales Active Directory (AD) oder ein Microsoft Azure AD via LDAPS an APIIDA Mobile Authentication angebunden.

Beide Optionen skalieren stufenlos mit der Benutzeranzahl!

6 € Benutzer / Monat
Erster Monat kostenlos

JETZT LOSLEGEN...

Schreib uns an:
support@apiida.com

Oder nutze unser Onlineformular auf:
www.apiida.com/apiida-mobile-authentication

10/19

APIIDA
secure connect

APIIDA AG
Marktstrasse 47-49
64401 Gross-Bieberau
Germany

Telefon: +49 6162 800 450
Telefax: +49 6162 800 444
E-Mail: info@apiida.com

apiida.com