indevis
Sicherheit in einer vernetzten Welt

# CASE STUDY


## INDEVIS AUTHENTICATION SERVICE MIT SOFTWARE-TOKEN

### AUSGANGSLAGE: ERHÖHTE SICHERHEIT DURCH KLASSISCHE STARKE AUTHENTIFIZIERUNGSLÖSUNG

Der simpelste Schutzmechanismus um den Netzwerkzugriff zu beschränken, ist die einfache Authentifizierung mittels Benutzername und eines dazugehörigen statischen Passworts. Allerdings ist dieser Schutz auch leicht zu überwinden. Für eine umfassende Absicherung setzen Unternehmen deshalb traditionell eine starke Authentifizierung über das 2-Faktor-Prinzip ein.

### INDEVIS MULTI-FAKTOR AUTHENTIFIZIERUNGSSERVICE

Beim *indevis Authentication* Service kommt klassischerweise ein Hardware-Token zum Einsatz, der alle 60 Sekunden einen neuen Code (2. Faktor) generiert. Gemeinsam mit einem persönlichen, selbst gewählten Pin (1. Faktor) ist somit eine sichere Anmeldung möglich. Als 2. Faktor können aber auch andere Token zum Einsatz kommen, z.B. Software-Token oder SMS-Token.

indevis übernimmt mit dem Authentication Service den kompletten Token-Lifecycle, versendet beim Einsatz von Hardware-Token diese an die Nutzer, tauscht die Token aus, wenn die Batterie leer ist und ersetzt verloren gegangene Token. Dank dieser Dienstleistung wird die IT-Abteilung entlastet und kann sich wieder auf ihr Kerngeschäft konzentrieren.

Durch den Einsatz von *indevis Authentication* erhalten nicht nur die eigenen Mitarbeiter die Möglichkeit, auf die Server und Daten von überall aus zuzugreifen. Auch externen Dienstleistern können die nötigen Informationen und Dienste auf diese Weise zugänglich gemacht werden, ohne dass in deren Sicherheitsrichtlinie eingegriffen wird oder komplizierte Maßnahmen ergriffen werden müssen, wie die Installation von Smartcard Readern oder Zertifikaten.

### HERAUSFORDERUNG: ERLEICHTERTE AUTHENTISIERUNG MIT SOFTWARE-TOKEN BEI GLEICHEM SCHUTZNIVEAU

Der Einsatz von Authentifizierungs-Token ermöglicht Unternehmen, deren Mitarbeiten und externen Dienstleistern noch mehr Flexibilität und bietet dabei ein deutlich erhöhtes Sicherheitsniveau. Mit allen Token kann sowohl der Zugriff über VPN auf das Unternehmensnetzwerk, als auch Cloud Applikationen geschützt werden. Software-Token erleichtern darüber hinaus den Rollout-Prozess für das Unternehmen und die Handhabung für den Anwender.

Software-Token unterstützen die gängigen Betriebssysteme für Desktop (Microsoft Windows, Mac OS) und Mobilgeräte (iOS, Android, BlackBerry und Windows Phone). Wie Hardware-Token nutzen auch Software-Token einen zeitbasierten Algorythmus, der anhand eines persönlichen Pins und des Token Codes einen Passcode errechnet. Mit diesem ist dann die sichere Authentifizierung möglich, wodurch die Gefahr von unsicheren Passwörtern eliminiert wird. Software-Token erleichtern daher sowohl dem Unternehmen, als auch dem Anwender den Authentifizierungsprozess – bei gleichzeitig unverändert hohem Schutzniveau.

### HERAUSFORDERUNG

- Reduzierung des Aufwands für IT-Abteilungen durch Token-Lifecycle des Hardware-Tokens
- Zugriff auf Server und Daten für eigene Mitarbeiter und externe Dienstleister von überall
- Vereinfachung des Authentifizierungs-Prozesses und Token-Rollouts
- Authentisierung mit Software-Token bei gleichem Schutzniveau
- Schutz von Cloud-Applikationen

### LÖSUNG

- Bequeme Software-Token Verteilung mittels QR-Code
- Einfaches Lizenz-Handling ohne Token-Austausch
- Schutz von Cloud-Applikationen mit indevis Authentication
- Software-Token: leichte Inbetriebnahme, nutzerfreundlich und immer griffbereit auf dem Smartphone

indevis
Sicherheit in einer vernetzten Welt


## LÖSUNG: INDEVIS AUTHENTICATION MIT SOFTWARE-TOKEN

**Bequeme Software-Token Verteilung mit QR-Code**

Durch den Einsatz von Software-Token kann der Workflow für die Verteilung und das Management der Zwei-Faktor-Authentifizierung für weltweite mobile Mitarbeiter optimiert werden. Der Token Seed – der geheime Schlüssel, der das Passwort erzeugt – kann dem Nutzer als QR Code postalisch übersendet werden. Dies erleichtert die Verteilung der Token besonders für Firmen, die global agieren. Beim Versand des QR Codes als Brief müssen keine Import- oder Zollbestimmungen beachtet werden, sodass der Token schnell ankommt. Der Verteilwegselbst ist außerdem sicherer als der Versand über unverschlüsselte E-Mails, da er Hackerangriffe unmöglich macht.

Für Nutzer bietet der Software-Token die Vorteile, dass er leicht in Betrieb zu nehmen, nutzerfreundlich und auf dem Smartphone immer griffbereit ist. Denn der QR Code führt automatisch zur RSA-App, sobald der Nutzer ihn mit seinem Smartphone abfotografiert. Zum Aktivieren des Tokens erhalten die Mitarbeiter separat ein Passwort mit einem zweiten Brief per Post. Die Bedienung über die App ist einfach, da lediglich der persönliche Pin eingegeben werden muss und sich der Passcode aus diesem und dem Token Code automatisch errechnet. Da sich der dynamische Token Code ständig erneuert und die Eingabe der Pin nicht auf dem PC erfolgt, kann das Passwort durch Angreifer nicht ausgelesen werden.

## EINFACHES LIZENZ-HANDLING OHNE TOKEN-AUSTAUSCH

Ein Austausch des Software-Token ist nicht erforderlich. Während Hardware-Token alle drei Jahre aufgrund ihrer Batterieleistung ersetzt werden müssen, ist bei Software-Token lediglich eine Lizenzverlängerung nötig, was den Aufwand für Unternehmen und Mitarbeiter minimal hält. Die Administration und der Token-Rollout können komplett an indevis ausgelagert werden. Auf Wunsch haben Unternehmen dennoch die Möglichkeit, mittels eines Administratorzugangs Nutzer zu entsperren sowie Token auszurollen und zu verwalten.

## SCHUTZ VON CLOUD-APPLIKATIONEN

Während früher wichtige und sensible Unternehmensdaten auf den Servern im Unternehmen selbst abgelegt wurden, wandern heute Exchange und die File Server Infrastruktur immer häufiger in die Cloud ab. Kalkulierbare Kosten, Skalierbarkeit, geringerer administrativer Aufwand und die Möglichkeit, sowohl verschiedene Firmenstandorte anzuschließen als auch externen Mitarbeitern den Zugriff zu ermöglichen, machen diese Technologie zunehmend attraktiv.

Bei allen Vorteilen sehen sich Unternehmen allerdings dem Risiko von Hacker-angriffen ausgesetzt. Eine ungesicherte Cloud gleicht einer offenen Bürotür. Hackern ist es damit ein Leichtes, Passwörter über Brute-Force-Angriffe herauszufinden und Accounts zu kompromittieren, um an sensible Unternehmensdaten zu gelangen. Um sich vor solchen Attacken zu schützen, muss der Zugriff kontrolliert und einge-schränkt werden.

## CLOUD-SCHUTZ MIT INDEVIS AUTHENTICATION

Um unberechtigten Zugriff auf sensible Daten und Applikationen, die sich in der Cloud befinden, zu verhindern, reicht ein klassischer Passwortschutz nicht aus.

Der bequem nutzbare *indevis Authentication* Service ermöglicht den Zugriff auf die Cloud über ein Remote Access Portal, über das sich alle berechtigten Nutzer anmelden können. Hierzu können alle Token-Varianten zum Einsatz kommen: Hardware-, Software- oder SMS-Token.

SIE WOLLEN
MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

**indevis GmbH**

Irschenhauser Straße 10
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de