KeyIdentity veröffentlicht neue Version seiner Multi-Faktor-Authentifizierungslösung

Datum: 31.01.2018 09:11
Kategorie: IT, New Media & Software
Pressemitteilung von: KeyIdentity GmbH

KeyIdentity GmbH

Zukunftsweisende Voice-Token-Technologie ermöglicht Account-Verifizierung mittels Telefonnummer-Überprüfung / Erweiterung von Token-Management, Push-Token-Funktionalität und Self-Service-Portal

Weiterstadt, 30. Januar 2018 – KeyIdentity, ein globaler Anbieter von hoch skalierbaren, einfach einsetzbaren Identity- und Access-Management-Lösungen (IAM) auf Open-Source-Basis, präsentiert die neueste Version seiner Multi-Faktor-Authentifizierungslösung (MFA) LinOTP. Das aktuellste Release der KeyIdentity MFA-Plattform unterstützt ab sofort Voice-Token, mit denen sich Nutzer schnell und einfach über ihre Telefonnummer authentifizieren lassen können. Ebenso hat KeyIdentity sein Token-Management sowie die Funktionalität seiner Push-Token optimiert und sein Self-Service-Portal um eine MFA-Absicherung erweitert.

"Wir arbeiten kontinuierlich daran, unsere Identity- und Access-Management-Lösungen weiter zu verbessern und um neue Features zu ergänzen. Damit wollen wir die digitalen Identitäten von Nutzern noch umfassender absichern und gleichzeitig den Einsatz unserer Open-Source-Technologie so einfach und effizient wie möglich machen", erklärt Dr. Amir Alsbih, CEO von KeyIdentity. "Mit dem neuesten Release unserer MFA-Plattform bieten wir viele zukunftsweisende Funktionen, von denen Unternehmen aller Größen und Branchen profitieren."

Voice-Token für Verifizierung von Telefonnummern

KeyIdentity erweitert sein Token-Angebot um eine innovative Voice-Authentifizierung von Twilio. Nutzer erhalten ihren Authentifizierungs-Code über einen Anruf an ihre hinterlegte Telefonnummer und müssen diesen dann eingeben. Durch dieses Prinzip lassen sich User über ihre Telefonnummer verifizieren. Damit kann unter anderem eine barrierefreie Authentifizierung für blinde User gewährleistet werden, die oftmals großen Schwierigkeiten beim Umgang mit Software-Token gegenüberstehen. Viele Soft-Token können aufgrund der Sicherheitsfeatures nicht durch Hilfs-Tools wie Screenreader wiedergegeben werden. Voice-Token schaffen hier Abhilfe. Dazu kommt, dass kein Smartphone für eine Multi-Faktor-Authentifizierung erforderlich ist und der Voice-Token eine sicherere Alternative zur SMS bietet, die zudem schnell ausgerollt ist. Mit der Einführung der Voice-Authentifizierung bietet KeyIdentity seinen Kunden eine erweiterte Bandbreite an unterschiedlichen Token-Typen – zusätzlich zu den bereits verfügbaren Software-Token wie Push-, QR- und SMS-Token sowie Hardware- und Biometrie-Token.

Optimiertes Token-Management

Mit dem neuen Release seiner MFA-Plattform hat KeyIdentity auch die Verwaltung seiner Token für IT-Administration und Helpdesk vereinfacht. So lassen sich ab sofort der Gültigkeitszeitraum, die Verwendungshäufigkeit oder die Anzahl der Authentifizierungsversuche definieren. Dies dient beispielsweise dazu, Token für Besucher, zeitlich befristete Mitarbeiter oder externe Dienstleister eines Unternehmens auszurollen. Die Token-Gültigkeit lässt sich dafür schnell und einfach über eine webbasierte Benutzeroberfläche einstellen.

Neue Funktionalität für KeyIdentity Push-Token

Push-Token zeichnen sich naturgemäß durch ihre hohe Sicherheit und Usability aus. Denn Nutzer erhalten nach dem Login automatisch eine Push-Nachricht auf ihr Smartphone, die sie nur noch per Klick bestätigen oder ablehnen müssen. KeyIdentity hat die Funktionalität seiner Push-Token mit dem neuen Release noch einmal weiter verbessert und sicherer gemacht: Durch den dezidierten Challenge-Service wird die Push-Funktionalität in einen eigenen Dienst ausgelagert, der eine Verbindung in das Internet benötigt. Auf diese Weise, kann der MFA-Kern mit den sensiblen Daten weiterhin in einem abgesicherten Netzwerk ohne Verbindung in das Internet betrieben werden.

MFA-Absicherung des Self-Service-Portals

Mit der neuen MFA-Version von KeyIdentity lässt sich auch das Self-Service-Portal für die Plattform über die Multi-Faktor-Authentifizierung absichern. Dies ist insbesondere in Umgebungen von Vorteil, in denen das Self-Service-Portal frei im Internet zugänglich ist. Das Login ist konfigurierbar. Nutzer können dadurch ihren Online-Zugriff zusätzlich absichern, ohne ihre gewohnten, bisherigen Workflows umzustellen.

Diese Pressemitteilung wurde auf openPR veröffentlicht.

Pressekontakt:
PSM&W Kommunikation GmbH
Beatrice Gaczensky & Jens Eßer
Clemensstr. 10
60487 Frankfurt am Main
Tel.: +49 69 970705-42 / -32
E-Mail: keyidentity@psmw.de
www.psmw.de

Über KeyIdentity

KeyIdentity ist ein globaler Anbieter von hoch skalierbaren, einfach einsetzbaren Identity-und Access-Management-Lösungen (IAM) auf Open-Source-Basis für die Absicherung und Verwaltung digitaler Identitäten über Netzwerk- und Cloud-Umgebungen. Der Fokus von KeyIdentity liegt auf den Bereichen Transaktionssicherheit, Identitätsmanagement und der starken Authentifizierung mittels Multi-Faktor-Authentifizierung (MFA). Die Lösungen von KeyIdentity zeichnen sich durch ihre hohe Usability und Skalierbarkeit aus und lassen sich mit jedem am Markt verfügbaren Authentifizierungstoken (OTP-Token) nutzen – von Software-Token wie Push-, QR- und SMS-Token über Hardware-Token bis hin zu Biometrie-Token. Darüber hinaus können die Lösungen der KeyIdentity IAM-Plattform durch den API-First-Ansatz in kürzester Zeit in jede verfügbare IT-Infrastruktur integriert werden. Die IAM-Lösungen werden von Anfang bis Ende in Deutschland entwickelt und bereitgestellt und erfüllen höchste Sicherheitsstandards nach deutschem Recht. Durch den Open-Source-Ansatz lassen sich zudem kryptografische Backdoors ausschließen. KeyIdentity bietet seit 2002 "Security made in Germany" und hat seinen Sitz in Weiterstadt bei Darmstadt. Weitere Informationen stehen auf der KeyIdentity Website, im Blog sowie über LinkedIn, Twitter und Facebook zur Verfügung.

Link zur PM:
https://www.openpr.de/news/990833/KeyIdentity-veroeffentlicht-neue-Version-seiner-Multi-Faktor-Authentifizierungsloesung.html