KEYIDENTITY
WE SECURE IDENTITIES

UNTERSTÜTZTE TOKEN-TYPEN DER KEYIDENTITY MFA-PLATTFORM

KEYIDENTITY MFA-PLATFORM

Token Übersicht

WÄHLEN SIE AUS EINER VIELZAHL UNTERSTÜTZTER TOKEN-TYPEN

Moderne MFA-Lösungen wie LinOTP und die KeyIdentity MFA-Plattform unterstützen eine Vielzahl verschiedener Token-Typen. Insbesondere im Unternehmensumfeld und in B2C-Szenarien besteht die Notwendigkeit eine große Auswahl an Token für verschiedene Anwendungsfälle anzubieten, abhängig von Ihrem Bedarf an Usability, Sicherheit und Kostenersparnis.

HARDWARE-TOKEN

Die klassischen Hardware-Token stellen eine bewährte und sichere Lösung dar, allerdings mit dem Nachteil geringerer Benutzerakzeptanz und eines erhöhten logistischen Aufwands. Hardware-Token finden üblicherweise in Situationen mit hohem Risikoniveau Gebrauch, für die Soft-Token oder Out-of-Band-Token nicht geeignet sind.

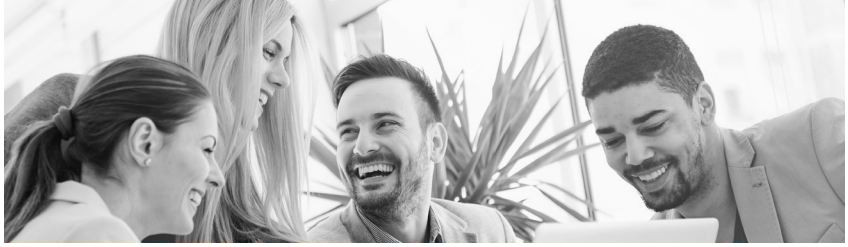
Hardware-Token (mit Display und Batterie) werden von vielen verschiedenen Herstellern zu unterschiedlichen Preisen angeboten. Die meisten folgen dem OATH (HOTP/ TOTP) Industriestandard. Der Benutzer hat somit die Möglichkeit zwischen verschiedenen Formfaktoren und Preisspannen zu wählen, ohne größere Änderungen im Backend vornehmen zu müssen (z. B. unterstützt LinOTP alle Varianten von OATH). Nahezu alle Hersteller unterstützen moderne Hashing-Algorithmen wie SHA-256, die moderne regulatorische Anforderungen mit einem Backend wie LinOTP erfüllen.

Der große Vorteil der klassischen Hardware-Token ist ihre Unabhängigkeit von authentifizierten Geräten. Da Hardware-Token in der Regel über ein eigenes Display und eine eigene Batterie verfügen, können sie unabhängig vom Gerät, auf dem die Anwendung läuft, betrieben werden.

Ein häufiger aufgeführtes Argument gegen den Einsatz von klassischen Hardware-Token betrifft den logistischen Aufwand des Rollouts. Gerade bei internationalen Rollouts kann sich die mit der Post und dem Zoll verbundene Logistik in den Kosten niederschlagen.

Eine besondere Art von Hardware-Token ist das FIDO-U2F-Token (z. B. Yubikey). Diese Token kommen gänzlich ohne Display und Batterie aus, was sich in geringeren Kosten wiederspiegelt. Zudem ist die Anwendung nach dem BYOT-Prinzip möglich (Bring Your Own Token). Der Anstieg von FIDO U2F-basierten Authentifizierungen auf großen Plattformen bringt einen weiteren Vorteil mit sich: die Token können für verschiedene Anwendungsfälle wiederverwendet werden, wodurch der logistische Aufwand (insbesondere bei B2C-Anwendungen) entfällt.

KEYIDENTITY
WE SECURE IDENTITIES



KEYIDENTITY MFA-PLATFORM

Token Übersicht

SOFTWARE TOKEN

Software-Token bieten eine verbesserte Benutzerfreundlichkeit mobiler Plattformen unter Beibehaltung der bewährten Authentifizierungsmechanismen klassischer Token. Sie können unter geringem Kostenaufwand implementiert und gewartet werden und bieten dennoch ein zufriedenstellendes Sicherheitsniveau.

Basierend auf den etablierten OATH (HOTP / TOTP) Standards können die meisten Software-Token mit allen kompatiblen Backends arbeiten. In Abhängigkeit von der verwendeten Token-App und Backend werden moderne Algorithmen unterstützt und gesetzliche Anforderungen erfüllt.

Software-Token können mittels MDM auf einfache Weise sicher implementiert werden. Die meisten Backends ermöglichen die Selbstregistrierung von Soft-Token, sodass sich der logistische Aufwand bei der Implementierung einer MFA-Lösung in Grenzen hält.

Ein Nachteil von Software-Token ist ihre Abhängigkeit von der mobilen Plattform, auf der sie laufen. Sie sind somit abhängig von der Sicherheit, Akkulaufzeit und Hardware der mobilen Plattform. Da das "Secret" von Software-Token auf einer mobilen Plattform gespeichert werden muss, sind sie zudem anfälliger für Angriffe als Hardware-Token.

Für Hochsicherheitsanwendungen kann dieses Risiko durch Verwendung externer Geräte wie einem Yubikey NEO mit NFC verringert werden. NFC ist jedoch nicht für alle Plattformen verfügbar. Bluetooth-basierte externe Geräte sind derzeit nicht weit verbreitet, da der Pairing-Prozess und die Reichweite Probleme darstellen.

SMS-TOKEN

SMS-Token sind weit verbreitet, da keine Software auf dem Mobiltelefon des Benutzers installiert werden muss. Sie können leicht implementiert werden und das Empfangsgerät kann ohne Probleme ausgetauscht werden. Zwar bieten SMS-Token eine viel höhere Sicherheit als ein Passwort allein, jedoch schneiden sie im Vergleich mit anderen Token-Typen eher schlecht ab.

Die Sicherheit von SMS-Token ist aufgrund mehrerer Angriffsvektoren, die von Angreifern aktiv genutzt werden, umstritten. Dennoch können sie eine praktikable Option in risikoarmen Umgebungen sein, in denen die Kosten gering gehalten werden sollen.

KEYIDENTITY
WE SECURE IDENTITIES

KEYIDENTITY MFA-PLATFORM

Token Übersicht

Die Flexibilität der SMS-Token ist gleichzeitig eine große Schwäche. Die Sicherheit der SMS-Token ist abhängig vom Mobilfunknetz, dem Mobiltelefon des Benutzers und der Endpoint Data im Backend. Alle dieser Komponenten geraten regelmäßig unter Beschuss (ZEUS). In letzter Zeit fanden vermehrt Angriffe auf den SMS-Transfer statt (Angriff auf das SS7-Protokoll im Mai 2017), wobei der Schwerpunkt auf Manipulation und Replay von mTAN-Transaktionen liegt. Da zwischen dem gesendeten OTP und der gesicherten Transaktion keine Verbindung besteht, ist die Manipulation der auf dem Mobiltelefon angezeigte SMS einfach. SMS sind auf keiner mobilen Plattform sehr gut geschützt. NIST löschte aus diesem Grund SMS-Token von der Liste ihrer empfohlenen Lösungen.

Insgesamt bieten SMS-Token einen einfach zu implementierenden und zu wartenden OTP-Mechanismus, aber ihre Sicherheit bleibt im Vergleich zu Push-Token und QR-Token fraglich.

PUSH TOKEN

Push-Token nutzen die Möglichkeiten moderner Mobilfunknetze und Plattformen voll aus. Sie bieten Transaktions- und Anmeldesicherheit mit Transaktionsprüfung in einem benutzerfreundlichen Format. Der Endbenutzer kann somit eine Transaktionsprüfung ohne zusätzliche Eingaben vornehmen, die über eine einfache Bestätigung hinausgehen.

Der Reiz von Push-Token liegt in ihrer hohen Benutzerfreundlichkeit. Die One-Touch-Authentifizierung wird unter Beibehaltung der erweiterten Sicherheitsfunktionen moderner Transaktionssicherheitsprozeduren verwendet. Die Sicherheit der Transaktionsgenehmigung oder der Anmeldung werden dabei durch Verschlüsselung und moderne Signaturalgorithmen gewährleistet.

Eine Push-Benachrichtigung über die Transaktion oder das Login wird an das registrierte mobile Gerät des Endbenutzers gesendet. Daraufhin überprüft und akzeptiert der Benutzer die Transaktion oder die Anmeldung basierend auf den gesendeten Daten. Eine zusätzliche Eingabe ist nicht erforderlich. Insbesondere in Bezug auf die Transaktionssicherheit sind Push-Token eine weit überlegene Alternative zu SMS-Token, da Mängel bei der Transaktionssignatur und -verschlüsselung verringert und zudem die Benutzerfreundlichkeit verbessert werden.

KEYIDENTITY
WE SECURE IDENTITIES

QR-TOKEN

QR-Token zeichnen sich durch Transaktions- und Anmeldesicherheit sowie Gerätetrennung und Validierung von Transaktionsdaten aus. Indem sie die Möglichkeiten mobiler Plattformen nutzen, stellen sie eine sichere Lösung für alle Authentifizierungsanforderungen, Logins oder Transaktionen dar. QR-Token basieren auf modernen Signaturalgorithmen und ermöglichen die sichere Authentifizierung von Transaktionen und Logins. Der Benutzer steuert die Transaktion mit Daten, die während der Übertragung validiert werden. Die Transaktion kann nicht validiert werden, wenn diese Daten manipuliert wurden.

Außerdem ermöglichen QR-Token eine sichere Offline-Authentifizierung für Laptops und mobile Geräte, da auf dem authentifizierten Gerät keine geheimen Daten gespeichert werden. Auch wenn keine Verbindung zum Backend besteht, lassen sich der Code und der Login leicht mit dem Mobiltelefon des Benutzers scannen. Auf die Sicherheit hat dies keinen Einfluss.

HARDWARE-TOKEN
- ✓ hohe Sicherheit
- ✓ viele Formfaktoren
- ✓ Zuverlässigkeit

SOFTWARE-TOKEN
- ✓ geringe Kosten
- ✓ einfache Implementierung

PUSH-TOKEN
- ✓ Transaktionssicherheit
- ✓ hohe Benutzerfreundlichkeit
- ✓ fortgeschrittene Authorisierung

QR-TOKEN
- ✓ Gerätetrennung
- ✓ hohe Sicherheit
- ✓ Transaktionssicherheit

OOB/SMS-TOKEN
- ✓ einfache Implementierung
- ✓ keine Installation

TOKEN	SECURITY	USABILITY	MAINTENANCE	COSTS
Classic Hardware-Token	+++	+	++	+
FIDO U2F	+++	+	++	++
Software-Token	++	++	++	+++
SMS-Token	+	++	+++	+++
QR-Token	+++	++	++	+++
Push-Token	++	+++	+++	+++

KeyIdentity GmbH
Robert-Koch-Straße 9
64331 Weiterstadt

Tel +49 6151 86086-277
Fax +49 6151 86086-299

www.keyidentity.com
info@keyidentity.com

Ein Unternehmen der MAX 21-Gruppe