KEYIDENTITY
WE SECURE IDENTITIES

SUPPORTED TOKEN-TYPES
IN THE KEYIDENTITY
MFA-PLATTFORM

KEYIDENTITY MFA PLATFORM

Token Overview

PROS AND CONS OF AVAILABLE TOKEN-TYPES

Modern MFA solutions like LinOTP and the KeyIdentity MFA platform support a wide range of token. Particularly in enterprise environments and B2C scenarios, there is a need to offer a variety of token in an implementation to accommodate all the different use-cases, risk-levels and cost considerations. *Below you will find an overview of typical token-types.*

HARDWARE-TOKEN

The classic hardware-token provide an proven and secure solution while coming up a bit short on user acceptance and logistics. Hardware-token are popular for higher risk levels and situations where soft-token or out-of-band-token cannot be used.

Hardware-token (with a display and a battery) are available from many different vendors at a variety of price points. Most follow the OATH (HOTP/TOTP) industry standard. The user can choose between different form factors and price ranges without any major changes in the backends (for example, LinOTP supports all varieties of OATH). Almost all vendors support modern hashing algorithms like SHA-256 which fulfill modern regulatory requirements with a backend like LinOTP.

A strong point of classic hardware-token is their independence from the authenticated device. Since hardware-token generally come with their own display and battery, they can operate independently of the device running the application.

A common argument against the use of classic hardware-token relates to the logistics of the enrolment process. Particularly in the case of international enrolment, the logistics associated with postal and customs can be expensive.

A special type of hardware-token is the FIDO-U2F-token (such as Yubikey). It has no need for a display or battery, bringing costs down. It permits BYOT (bring your own token) scenarios. With the rise of FIDO U2F based authentications on large platforms, providing a FIDO U2F based authentication permits the reuse of token provisioning by the customer, thereby eliminating the cost of logistics, especially in B2C use cases.

KEYIDENTITY
WE SECURE IDENTITIES

KEYIDENTITY MFA PLATFORM

Token Overview

SOFTWARE TOKEN

Software-token allow one to leverage the usability of mobile platforms while retaining the proven authentication mechanisms of classical token. They can be rolled out and maintained with little cost and still provide a satisfactory level of security. Based on the established OATH (HOTP/TOTP) standards, most software-token can work with all compatible backends. Depending on the token-app and backend, modern algorithms are supported and regulations are met. When integrated with a MDM, software-token can be easily rolled out in a secure manner. Most backends provide for self-enrolment of soft-token, so the normal logistical challenges in enroling an MFA solution do not apply. A common complaint about software-token is their dependence on the mobile platform upon which they run. They depend on the security, battery life and hardware of the mobile platform. With frequent attacks on mobile platforms, software-token are more vulnerable than hardware-token, since the secret has to be saved on a mobile platform. For high security applications, this risk can be mitigated using external devices such as a Yubikey NEO with NFC; however, NFC is not available to all platforms. Bluetoothbased external devices are not currently widely available and the pairing process and extensive range pose problems.

SMS-TOKEN

SMS-token are in widespread use as they do not need any software installed on the user's phone. They can be easily enrolled and the receiving device can be easily changed. They provide much better security than a password alone, but security has to be considered when compared to other token-types. The security of SMS-token has come into question, however, with several attack vectors actively used by attackers. They can still be a viable option in low-risk environments where costs have to be at a minimum. The flexibility of the SMS-token is also its biggest weakness. The security of SMS-token depends on the carrier network, the mobile phone of the user and the end point data in the backend. All of these are constantly under attack (ZEUS). Lately, several attacks on carriers' transport of SMS were described and carried out (attack on SS7 protocol in May 2017), with the specific point being the manipulation and replay of mTAN transactions. Since there is no association between the OTP sent and the transaction secured, it is easy to manipulate the SMS shown on the phone. SMS are not very well protected on any mobile platform. NIST just dropped SMS-token from their recommended solutions. Overall, SMS-token provide an easy to enroll and maintain OTP mechanism, but their security is questionable compared to push-token and QR-token.

KEYIDENTITY
WE SECURE IDENTITIES

HARDWARE-TOKEN

- ✓ high security
- ✓ many form factors
- ✓ reliable

SOFTWARE-TOKEN

- ✓ low costs
- ✓ easy deployment

PUSH-TOKEN

- ✓ transaction security
- ✓ high usability
- ✓ advanced authorization

QR-TOKEN

- ✓ device separation
- ✓ high security
- ✓ transaction security

OOB/SMS-TOKEN

- ✓ easy deployment
- ✓ no installation

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

KEYIDENTITY

WE SECURE IDENTITIES

PUSH-TOKEN

Push-token fully leverage the possibilities of modern mobile networks and platforms. They offer transaction and login security with transaction validation in a highly usable format. The end user can check the transaction without any additional input beyond the confirmation. Push-token provide a high level of user acceptance while retaining a high level of security.

The charm of push-token is their high usability, using one touch authentication, while retaining the advanced security features of modern transaction security procedures. Encryption and modern signing algorithms ensure the security of the transaction approval or login.

For the end user, a push notification about the transaction or login is sent to the user's registered mobile device. The user reviews and accepts the transaction or login, based on the data sent to the device. No additional input is needed.

Particularly in respect to transaction security, push-token are a far superior alternative to SMS-token, mitigating their shortcomings in transaction signing and encryption while even improving usability.

QR-TOKEN

QR-token provide transaction and login security along with device separation and transaction data validation. Leveraging the possibilities of mobile platforms, they provide a secure solution to all authentication needs, logins or transactions alike. QR-token are based on modern signing algorithms and facilitate the secure authentication of transactions and logins. The user is able to control the transaction with data validated during the transport. If the data is manipulated, the transaction cannot be validated.

Finally, the nature of QR-token enables secure offline authentication for laptops and mobile devices. No secret data is saved on the authenticated device. With the user's phone it is easy to scan the code and login, even when there is no connection to the backend possible at the time, without compromising on security.

KeyIdentity GmbH
Robert-Koch-Straße 9
64331 Weiterstadt

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

www.keyidentity.com
info@keyidentity.com

Member of the MAX 21 AG Group