DEFINITION

key fob

By **Rahul Awati** | **Diana Hwang**

What is a key fob?

A key fob is a small, programmable device that provides access to a physical object. Also known as a *hardware token*, a key fob provides on-device, one-factor authentication to facilitate access to a system or device, such as a car, computer system, restricted area or room, mobile device, network service or other kind of keyless entry system.

With a key fob, the user does not have to unlock the device with a real key as with manual locks. In addition to providing remote-enabled access, the key fob is more convenient and more secure.

Key fobs are among a class of physical security tokens that includes smart cards, proximity cards and biometric keyless entry fobs.

Key fobs, along with smart cards, proximity cards and biometric keyless entry fobs, are a type of physical security token.

How a key fob works

A key fob contains a short-range radio transmitter/radio frequency identification (RFID) chip and antenna. It uses radio frequencies to send a distinct coded signal to a receiver unit in the device.

This receiver also contains an RFID tag, which is some form of stored information. The reader's transmitter sends a signal to the fob, which then adjusts to the transmitter's frequency. The communication between the fob and the receiver device happens instantaneously when the user presses a button on the fob.

The RFID chip on the key fob is designed to transmit specific RFID tag information. This information always matches what the receiver device has been programmed to accept.

For example, a key fob programmed to work with a car will only lock or unlock that car, and no other key fob will work with that car. So, if the information from the receiver tag matches the information that the fob is requesting, the locking or unlocking function will be

completed. If there is a mismatch, the function will not be performed.

RFID key fobs often can be programmed to transmit various commands. For example, automotive key fobs often have different functions assigned to different buttons; in addition to remote vehicle lock and unlock, these functions include the following:

- starting the ignition
- arming or disarming the security system
- popping the latch on the trunk
- controlling automatic windows

Key fobs and multifactor authentication

Key fobs are also used as one of the authentication factors for devices that require two-factor (2FA) or multifactor authentication (MFA). These authentication methods help safeguard a company's network, devices, applications and data.

Unlike traditional password-only systems, MFA requires more than one method of authentication to verify a user's identity before they can access any of these assets. These factors are as follows:

- **possession:** something you have
- **inherence:** something you are
- **knowledge:** something you know

The use of such multiple factors makes it difficult for bad actors to steal or compromise credentials and harm the company in other ways. It thus provides more reliable and stronger security than passwords.

In typical key fob deployment in a 2FA/MFA system, the user first enters a personal identification code to log in to the network or device. The fob generates a pseudo-random token code, also known as a *passcode*, that validates the user to confirm they are legitimate and authorized to access the system or network. Once the validation is complete, the user is given access.

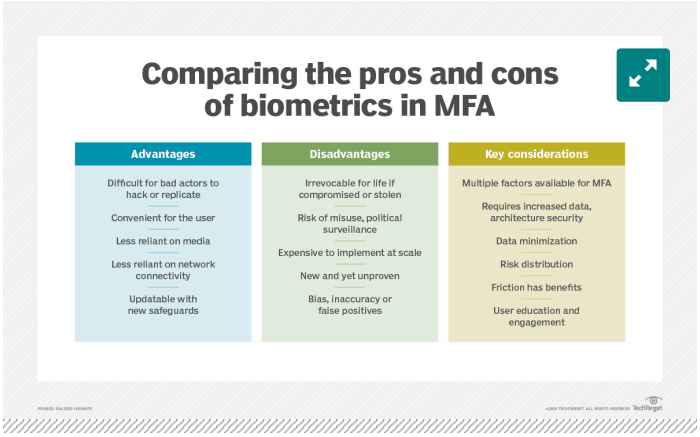
The passcode only works for a certain amount of time -- 30 to 60 seconds. If the user fails to input this passcode into the system within this period, it automatically times out, and they won't be able to use it again. To access the system or service, they need to regenerate the passcode on the fob.

How multifactor authentication works

Key fobs and biometric authentication

Biometric authentication is authentication based on a user's unique biological qualities, such as fingerprints, iris scans and voice prints. Used increasingly as the inherence factor in MFA, biometric authentication may be incorporated into key fobs to provide additional security protection.

Some devices use the traditional fingerprint method, while others require users to swipe the fob. This action reads the fingerprint ridges and the finger pad's seven layers of skin to authenticate the user.



The pluses and minuses of biometrics in multifactor authentication

What are the benefits of key fobs?

One of the biggest benefits of a hardware key fob is that it provides an additional layer of security in enterprise settings. Passwords are easy to intercept and steal, and attackers often do so by means of brute-force attacks, phishing campaigns or social engineering.

This enables malicious actors to access a network or system in order to install malware, lock the system and demand a ransom to unlock it, steal data, commit identity fraud, and engage in espionage and other cybercrimes.

A key fob prevents such issues. If a bad actor does try to hack into a system, they need more than a set of compromised credentials. They also need access to the fob. Although it is possible to copy and hack key fobs, if users are careful about storing the devices, the chances of their being stolen and then used for a cyber attack are low.

Moreover, since passcodes are randomly generated, transmit a unique access/unlock sequence every time and time out after a fixed period, the fob prevents attackers from reusing them, even if they do manage to intercept them. Fobs also offer a simple interface to minimize friction for users.

Key fobs increase security by randomly generating passcodes that are used only one time for multifactor authentication purposes.

With the help of back-end software that controls all connected RFID readers from a common server, administrators can program multiple key fobs remotely. The server communicates with multiple fobs and readers to grant or prevent user access.

Moreover, admins can create multiple levels of access to better control who can access their network, facility or devices. This kind of multilevel remote entry access is suitable for facilities that require extensive security and access control but don't want to keep changing locks and keys.

The versatility and security of hardware key fobs make them applicable for many kinds of commercial facilities, including the following:

- factories
- offices
- restricted areas, such as server rooms
- laboratories
- hospitals

This was last updated in September 2021

Continue Reading About key fob

- Exploring multifactor authentication benefits and technology
- Belgian security researcher hacks Tesla with Raspberry Pi
- Strong authentication methods: Are you behind the curve?
- Security Think Tank: Zero trust – just another name for the basics?
- Top 10 cyber security stories of 2020

Related Terms

digital signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or... See complete definition

OpenID (OpenID Connect)

OpenID Connect is an open specification for authentication and single sign-on (SSO). See complete definition

out-of-band authentication

Out-of-band authentication is a type of two-factor authentication (2FA) that requires a secondary verification method through a ... See complete definition

Dig Deeper on Identity and access management

one-time password
By: Kathleen Richards

Secure printing: The foundation of multi-layered security
By: Louella Fernandes

soft token
By: Paul Kirvan

Google Authenticator
By: Robert Sheldon

Latest TechTarget **resources**

- NETWORKING
- CIO
- ENTERPRISE DESKTOP
- CLOUD COMPUTING

Networking

Cloud networking sustainability strategies yield benefits

As enterprises seek ways to reduce their environmental footprints, one popular way is to migrate on-premises networking ...

The complete secure access service edge (SASE) guide

SASE helps organizations manage and secure traffic across locations. But is it the best choice for your environment? Use this ...

COMPUTER WEEKLY