Multifactor Authentication

1.1 Definition/Description

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Multifactor authentication combines two or more independent factors:

- Something you know ("knowledge") – for example, passwords, PINS, knowledge-based answers
- Something you have ("possession") – for example, card, bracelet, key fob, mobile phone
- Something you are ("inherence") – for example, fingerprint, voice, facial image

A system that depends on only one factor (e.g., a password) is vulnerable to fraud. MFA reduces that vulnerability by adding one or more unaffiliated factors.

A variation of MFA is "out-of-band" authentication. With out-of-band authentication, each factor is delivered through a separate communication channel. A one-time password delivered through a hard token with a user-provided password is an example of two factors delivered though different communication channels.

Examples of MFA include:

- Swiping or inserting a card and entering a PIN.
- Logging into a website and being requested to enter an additional one-time password
- Swiping/inserting a card, scanning a fingerprint, and answering a security question.
- Using a USB hardware token with a desktop computer to generate a one-time passcode and using the one-time passcode to log into a VPN client.
- Using voice recognition on a phone call.[1]

1.2 Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	Yes	Customer onboarding	Yes	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	Yes	Issuers	Yes: internal
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	Yes	Acquirer processors	Yes: for clients[2]

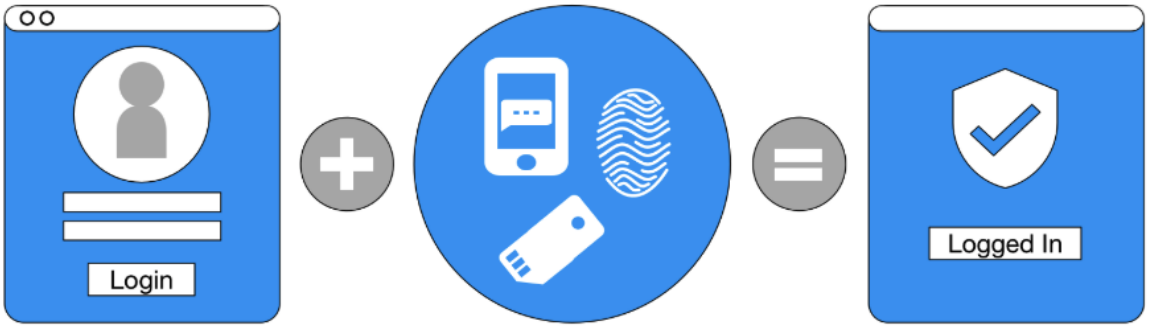
[1] This method is explained in Section 6.

[2] Often done by whoever provides website.

1.3 Technical Features/How the Technique Works

With MFA, the customer is asked for two or more factors—typically a password (“something you know”) and at least one other factor. The additional factor or factors come from different sources, including:

- “Something you have”, such as
  - One-time password delivered through SMS
  - One-time password delivered through a hard token; the hard token can be separate device or embedded in a plastic card.
  - One-time password delivered through an application
- “Something you are” — biometric authentication, such as
  - Fingerprint ID
  - Face ID
  - Iris scan



Source: NIST

Figure 1. Using Multifactor Authentication for Login

Many factors can be used, but all are not equally convenient and safe. A very secure second factor may increase customer friction and decrease completion of a transaction, and so be less beneficial to a business. The disadvantages of some factors can be balanced by the advantages of others.

Despite greater security, adding authentication factors increases the effort and time it takes to authenticate a user and authorize access. Using MFA trades off customer friction for increased security.

MFA techniques typically involve more than one party, such as an issuer and a vendor. It is not common for one stakeholder to offer all factors internally.

1.4 Risks Associated with Technique

Some methods of sending the second factor are more secure than others.

Using SMS to send one-time passwords is vulnerable to hacking. In 2016, the National Institute of Standards and Technology (NIST) withdrew support for SMS-based two-factor authentication, pointing to the risk of interception or spoofing.

App-based second factor generators are more secure. These require customers to have their mobile devices on hand; however, the applications can be hacked.

Hardware tokens can be even more secure. However, they are costly and can be misplaced by customers.

Biometrics are convenient, but, if compromised, can eliminate that factor completely.

Given the potential risks of MFA alone, it is often used as part of a layered approach.

1.5 Customer Impact/Level of Friction

All MFA methods involve some customer friction; the amount depends on the method used. Using a hardware token, for example, causes significant friction. If a time limit is required for use, the friction can be greater. Biometric authentication generally causes much less friction.

1.6 Implementation Considerations

As with customer friction, implementation difficulty depends on the MFA method used. Using a password plus a one-time password delivered via SMS is relatively easy to implement. Offering hard tokens or implementing biometrics generally requires significantly more time and resources.

1.7 Maturity

Patents for multi-factor authentication were issued as early as 1995.[3] Widespread use did not begin until the middle of the following decade.

1.8 Applicable Industry Standards

Industry standards for MFA include:

- NIST SP 800-63 Digital Identity Guidelines
- FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) and the Client to Authenticator Protocols (CTAP)

1.9 Publicly Available Statistics on Implementations and Use

A categorized list of websites that have implemented two-factor authentication can be found at www.twofactorauth.org.

1.10 Further Reading

https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

https://www.onelogin.com/learn/what-is-mfa

https://www.protectimus.com/blog/two-factor-authentication-types-and-methods/

[3] "Kim Dotcom claims he invented two-factor authentication—but he wasn't first," ars Technica, May 23, 2013, https://arstechnica.com/information-technology/2013/05/kim-dotcom-claims-he-invented-two-factor-authentication-but-he-wasnt-first/