okta

Factor Types & Assurance Levels

Understand the ability of each factor or authenticator to withstand identity attacks

Multi-factor authentication (MFA) refers to a secure access method in which a user is required to use two or more authentication factors or authenticators before being granted access to the requested resource. A factor is a mechanism used to perform authentication, such as a username and password, a one-time passcode (OTP), a smart card, etc. These factors help systems have higher confidence in the identity of a user and help to diminish the likelihood of impersonation attacks and credential theft.

There are many different examples of factors a system secured with MFA can use to increase its confidence in the identity of users. However, not all provide a similar level of security assurance. Factor types can be organized into three main categories:

Knowledge: Users prove they know something (like a password or the answer to a security question)

Possession: Users prove they own something (like a mobile device where they can receive an SMS code)

Inherence: Users verify their identity through something they inherently have (like facial recognition or fingerprint scan)

In general, knowledge-based factors are considered weaker than possession or inherence-based factors.

Here's an overview of commonly available factors and their relative security assurance levels.

Assurance Level	Factor or Authenticator	Advantages	Disadvantages
Low	Password	• Low cost • Easy to use and deploy • Familiar to users	• Easy to hack due to users' poor password management habits (e.g., use of common passwords, writing passwords down, reusing passwords) • At major risk of social engineering and phishing • Users tend to forget passwords
Low	Security Question	• Low cost • Easy to use and deploy • Familiar to users	• At major risk of social engineering and phishing • Answers may be easy to guess or discover • Users often forget the answers

Assurance Level	Factor or Authenticator	Advantages	Disadvantages
Low	SMS, Voice, Email	• Low cost • Easy to use and deploy • Familiar to users	• At major risk of social engineering and phishing • Only as secure as the device • May require using a personal device for work purposes • Limited DMARC standard implementation means detecting email-based spoofing is difficult
Low	Soft Token Examples: Okta Verify OTP, Google Authenticator	• Low cost • Easy to use and deploy • Familiar to users	• At major risk of social engineering and phishing • Answers may be easy to guess or discover • Users often forget the answers
Medium	Push Notification Example: Okta Verify Push	• Low cost • Easy to use and deploy • Algorithmically-generated • Cryptographic signature verification • Some apps support biometric authentication for 2FA	• At risk of real-time adversary-in-the-middle phishing attacks • Only as secure as the device • May require using a personal device for work purposes
Medium	Hardware Token Example: YubiKey OTP	• Easy to use • Algorithmically-generated • Does not require internet/data service to use • Does not require a personal device to use	• At risk of real-time adversary-in-the-middle phishing attacks • Easy for users to lose, and recovery may be high-effort • Higher deployment and provisioning costs • Many OTP tokens do not support biometrics
High	Personal Identity Verification (PIV)/ Common Access Card (CAC)/ Smart Card	• Mature technology • Extremely secure authentication often preferred in highly regulated industries • Phishing-resistant authentication (requires PIN to access)	• Physical smart cards require an insert-based/ contact-based reader • Easy for users to lose, and recovery may be high-effort • Not widely supported on mobile platforms • PIN resets can be painful

Assurance Level	Factor or Authenticator	Advantages	Disadvantages
High	FIDO2 (WebAuthn) Platform Authenticator Examples: Touch ID, Face ID, Windows Hello	• Phishing-resistant authentication • Follows industry authentication standards (FIDO Alliance) • Often available native to the machine • Seamless end-user experience • Puts organizations on a path to passwordless	• Cross-platform support is poor or emerging • User data privacy concerns
High	FIDO2 (WebAuthn) Roaming Authenticator Example: FIDO2 YubiKey	• Phishing-resistant authentication • Follows industry authentication standards (FIDO Alliance) • Cross-platform coverage • Seamless end user experience • Puts organizations on a path to passwordless	• Easy for users to lose, and recovery may be high-effort • Higher deployment and provisioning costs
High	Okta FastPass	• Phishing-resistant for managed and unmanaged iOS, macOS, Windows, and Android devices • Passwordless inline authentication experience that is consistent across platforms • Zero Trust authentication that leverages 1st party and 3rd party device context signals to ensure the security of the device before access is granted • Defense-in-depth with device context re-evaluation before access is allowed to downstream resources • Strong binding between the authenticator, device, and user • Support for biometric authentication or device-bound passcode for 2FA • Support for automated actions that kickoff security remedial workflows and end user alerts	• Okta Verify (an MFA thin client) needs to be installed on devices

Factor or Authenticator	Examples Supported by Okta	Factor Type	Disadvantages
Password, Security Question	Password, Security Question	• Knowledge	• User verification
SMS, Voice	SMS, Voice	• Possession	• User presence
Email	Email, Magic Link	• Possession	• User verification
Soft Token	Okta Verify OTP, Google Authenticator	• Possession	• User presence
Push Notification	Okta Verify Push, Duo	• Possession • Possession + Inherence	• Hardware-protected (authenticator dependent) • User presence • User verification
Hardware Token	YubiKey OTP, RSA SecurID	• Possession	• Hardware-protected • User presence
PIV/CAC/Smart Card	PIV/CAC/Smart Card	• Possession • Possession + Inherence	• Phishing-resistant • Hardware-protected (authenticator dependent) • User presence • User verification
FIDO2 (WebAuthn) Platform Authenticator	Touch ID, Face ID, Android Fingerprint, Windows Hello	• Possession • Possession + Inherence	• Phishing-resistant • Hardware-protected (authenticator dependent) • User presence • User verification
FIDO2 (WebAuthn) Roaming Authenticator	YubiKey, Google Titan	• Possession • Possession + Inherence	• Phishing-resistant • Hardware-protected (authenticator dependent) • User presence • User verification
Okta FastPass	Okta FastPass	• Possession • Possession + Inherence	• Phishing-resistant • Hardware-protected (hardware dependent) • User presence • User verification

Learn more about Adaptive MFA at okta.com/products/adaptive-multi-factor-authentication

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.