okta

# Factor Types and Authenticator Assurance Levels: An Overview

## Understanding the security of each authenticator type

Your users are your most important asset — that's why it's critical to provide secure access to apps for both your workforce and customers. Smart organizations have already implemented multi-factor authentication to prevent account takeover. However, not all factors and authenticators provide the same level of security assurance. The classic paradigm for authentication systems identifies three **factors** as the cornerstones of authentication:

- ***Knowledge***: Something you know (e.g., a password)
- ***Possession***: Something you have (e.g., an ID badge or a cryptographic key)
- ***Inherence***: Something you inherently are (e.g., a fingerprint or other biometric data)

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

An **authenticator** is something an end user possesses and has control over (e.g., PIV Card , security question, password) that is used to authenticate to the user's account.

Here's a brief overview of the common authenticators organizations use, and the relative assurance levels of those authenticators. For more details on combinations of factors that can be used to establish and increase confidence in validating a user's identity, see the official Authenticator Assurance Levels topic.

The table below provides an overview of the pros and cons of various authenticators with their assurance levels.

| Assurance level | Authenticator | Pros | Cons |
|---|---|---|---|
| Low | **Password** | – Provides baseline security at a low cost<br>– Easy to use and deploy<br>– Users are familiar with the process of logging in with a password | – Vulnerable to data breaches due to users' poor password management habits (use of common passwords, writing passwords down, reusing passwords, etc.)<br>– Major risks from social engineering and phishing<br>– Users tend to forget passwords when password requirements are too complex<br>– Difficult to type on mobile devices |
| Low | **Security Question** | – Provides baseline security at a low cost<br>– Users are familiar with process of answering a security question during login | – Users often forget their answers<br>– Many questions are weak, making answers easy to guess or discovery<br>– Subject to social engineering and phishing |

| Assurance level | Authenticator | Pros | Cons |
|---|---|---|---|
| Low | **SMS, Voice, Email One-time Password (OTP)** | – Familiar experience for users as many consumer apps already use OTP as a form of account/identity verification<br>– Easy to deploy as most individuals have a phone | – Relies on phone/internet service provider for security; subject to social engineering (e.g. SIM swapping)<br>– May require using a personal device, which cannot be enforced in some regions<br>– Limited DMARC standard implementation means detecting email-based spoofing is difficult |
| Low | **Mobile/Desktop One-time Password (OTP) apps**<br><br>**Examples: Okta Verify OTP, Google Authenticator, Authy** | – Low cost, many users able to install an app on laptop or phone<br>– Algorithmically generated<br>– Crypto-based security<br>– Does not require internet/data service to use (i.e. airplanes, international travel) | – Biometric verification can be set intrinsic to authentication<br>– Limited protection against a stolen device<br>– May require using a personal device, which cannot be enforced in some regions<br>– Subject to real-time adversary-in-the-middle attacks |
| Medium | **Mobile app push notifications**<br><br>**Examples: Okta Verify with Push** | – Low cost, many users able to install an app on laptop or phone<br>– Algorithmically generated, not delivered over insecure channels<br>– Some apps support biometrics<br>– User-friendly | – May require using a personal mobile device. Users may have privacy concerns & cannot be enforced in some regions<br>– Subject to man-in-the-middle and phishing attacks |
| Medium | **Physical token One-time Password (OTP)**<br><br>**Examples: YubiKey, Symantec VIP** | – Algorithmically generated<br>– Does not require internet/data service to use<br>– Does not require a personal phone/device | – Subject to loss and may require a separate recovery option<br>– Higher deployment and provisioning costs, orgs may not deploy to all users<br>– Many OTP tokens do not support biometrics |

| Assurance level | Authenticator | Pros | Cons |
|---|---|---|---|
| High | **Personal Identity Verification (PIV)/ Common Access Card (CAC) smart cards** | – Mature technology<br>– Extremely strong authentication level<br>– Phishing resistant inbuilt MFA (required PIN to access) | – Needs an insert-based, contact-based reader, not contactless<br>– Can be easily lost or stolen<br>– Not widely supported on mobile platforms<br>– PIN resets can be painful |
| High | **FIDO2.0 / WebAuthn and CTAP2 Examples: Mac Touch ID, Android fingerprint, Windows Hello, YubiKey** | – Phishing resistant<br>– Support for both on-device biometrics and security keys<br>– Seamless end-user experience<br>– Puts organizations on a path to passwordless<br>– Can reduce IT and support costs for factor enrollment and reset | – Not yet widely adopted<br>– May require purchasing new hardware<br>– Only applies to web-based authentication |
| High | **Okta FastPass** | – Phishing-resistant for all managed devices and for MacOS, Windows, and Android on unmanaged devices<br>– Seamless end-user experience<br>– Leverages the device context signals (some collected by Okta Verify itself and others through integration partners such as CrowdStrike and Tanium) to help administrators make policy decisions based on the device posture<br>– Can reduce IT and support costs for factor enrollment and reset | – Not yet widely adopted<br>– Only applies to web-based authentication<br>– Not FIDO2.0 certified as of today |

okta

# Authenticator type comparison

| Authenticator Type | Deployability | Usability | Phishing Resistance | Real-Time AiTM Resistance |
|---|---|---|---|---|
| **Password** | Good | Moderate | No | Very weak |
| **Security Question** | Good | Moderate | No | Very weak |
| **SMS, Voice, Email OTP** | Good | Strong | No | Weak |
| **Mobile/Desktop OTP apps** | Moderate | Moderate | No | Weak |
| **Physical token OTP** | Weak | Moderate | No | Weak |
| **PIV smart card** | Weak | Moderate | Yes | Strong |
| **Mobile app push notifications** | Good | Strong | No | Moderate |
| **FIDO2.0 / WebAuthn + CTAP2** | Moderate | Strong | Yes | Strong |
| **Okta FastPass** | Good | Strong | Yes | Moderate |

Interested in learning more about multi-factor authentication?

Visit our website https://www.okta.com/products/adaptive-multi-factor-authentication