Authentication Methods

To comment on this article, please visit our [GitHub repository]() and [submit an issue]().

Table of Contents

Abstract

This introductory article describes the basics of different types of authentication methods and their security implications. The descriptions are scoped to workforce authentication, not customer (CIAM) authentication, though there is certainly overlap between the two areas.

Introduction

Authentication (AuthN) is the process of ensuring ownership of an identity at the time the identity is used to access a resource or establish a session. There are several different methods of authentication, and organizations can blend combinations of these methods for different business scenarios and user populations. Each method has it's own security implications and user experience that are worth considering.

Terminology

Many of these terms have been sourced from the "Terminology in the IDPro Body of Knowledge".

Flanagan (Editor) | Terminology in the IDPro Body of Knowledge | IDPro Body of Knowledge

Term	Source	Definition
Authentication	Epping | Authentication and Authorization (v2) | IDPro Body of Knowledge	Authentication is the process of proving a digital identity to a user and verifying that the requestor is the owner of that identity. An identity can be requested for a device or a service by an individual or an organization. Some identities may not need any verification, but others may require a high level of assurance.
Multi-Factor Authentication (MFA)	Saxe | Account Recovery (v3) | IDPro Body of Knowledge	Multi-Factor Authentication (MFA) is a security feature that requires combining more than one method to prove the identity of a user. An example would be combining something that a user knows such as a password with something that a user has such as a device or a security token. There is an option to use biometric verification such as a fingerprint for authentication.
Passwordless	Glazer | Introduction to Customer Identity and Access Management | IDPro Body of Knowledge	Passwordless authentication does not require a human remembered shared secret and instead relies on credentials such as one-time passcodes (OTPs), authenticatior apps, and passkeys.
Certificate-based Authentication	What is Certificate-Based Authentication | Yubico	Certificate-based authentication leverages digital certificates to identify users, devices, and machines before granting access across all endpoints. The use of cloud-based management platforms simplifies the administrative burden and allows for efficient management, monitoring, and issuance of new certificates, which is particularly

		beneficial for large organizations with many employees.
One Time Passcode (OTP): software or hardware keys	Cybersecurity Glossary | Yubico	A code sent to a user to prove “something they have”. OTP codes are valid only one time for a login session or transaction. A common implementation is an OTP SMS sent to a mobile phone. Stronger forms of OTPs are sent to the user through an Authenticator Apps (defined next).
Authenticator Apps	Epping | Authentication and Authorization (v2) | IDPro Body of Knowledge	Apps which prompt an end user upon sign in with a push notification
Biometric	biometric - Glossary | CSRC (nist.gov)	Biometrics are used for proving “something you are” by leveraging physical characteristics or behavioral traits that can be used to verify a user’s identity. Examples include facial recognition, fingerprints, keyboard biometrics, and more.
FIDO2 Security Keys	FIDO2 - FIDO Alliance User Authentication Specifications Overview - FIDO Alliance	FIDO2 Security Keys are hardware devices used for passwordless authentication

Passkeys	Passkeys - FIDO Alliance	Passkeys are a passwordless authentication method that leverage cryptographic key pairs. Passkeys can be synced between devices or device-bound.

Single Factor Authentication

There are several factors that a user can leverage to authenticate. Factors are often thought of as:

- “something you know” such as a password,
- “something you have” such as a physical device, or
- “something that you are” like a biometric such as fingerprint, facial recognition, or even behavior.

Leveraging one of these factors is referred to as single-factor authentication.

Why Passwords are Weak

The most common form of single-factor authentication is a password.

Passwords are the weakest authentication method because they are often chosen by humans and contain patterns. Humans also frequently reuse passwords across multiple sites, so if a password is breached, a bad actor can replay the same username and password combination against the user’s identity on another website. Passwords can easily be shared and reshared outside scope of the original identity

Multi-Factor Authentication

The combination of multiple factors is referred to as multi-factor authentication (MFA) which is stronger than single-factor authentication due to the pairing of a password with another factor to prove the user is who they say they are.

The phrase two-factor authentication (2FA) can also be used to describe a combination of two factors; however, the term MFA is more frequently used. MFA methods range in terms of strength due to how easy it would be for a bad actor to pretend to be a user or trick them into accepting an MFA prompt that would compromise the identity.

Common MFA Methods and Their Risks

For example, SMS text messages or phone calls are popular MFA methods because they leverage a phone and a code passed along to the user via this medium proving it is “something you have”. Because there is potential for a bad actor to intercept this code or trick the user into giving their code with phishing attacks or social engineering, it is less secure than other MFA methods.

Stronger MFA Options

MFA methods such as One Time Passcode (OTP) security keys, authenticator apps, and PINS are tied to devices, so they reduce risk of identity compromise in comparison to a text message or phone call. In most cases, the bad actor would have to mislead the user into accepting an MFA prompt for their sign in or entering their OTP code into a bad actor-run website order to compromise the identity.

Passwordless Authentication

Passwordless authentication methods remove the weakest link – passwords – from the user’s authentication flow, making it phishing-resistant and stronger than traditional MFA methods. Passwordless methods typically consist of authenticator apps or FIDO2 security keys which leverage both “something you have” and “something you are”. Passwordless authentication methods reduce helpdesk calls within organizations because users don’t need to go through password reset processes, and they provide an easier user experience during login.

Passkeys

Passkeys are a form of passwordless authentication that use public key cryptography. They leverage cryptographic key pairs with the website the user is signing into and the user’s device. Similar to other passwordless methods, it is a better user experience than traditional single factor logins, and they are more secure than other MFA methods like text message or phone call.

Federation and SSO as Authentication Strategies

Authentication can also be delegated to a third-party using federation protocols. This approach is commonly known as Single Sign-On (SSO), where users authenticate once with a central identity provider (IdP) and are then able to access multiple systems or services without re-authenticating. This not only improves the user experience but also centralizes authentication controls, making it easier to enforce consistent security policies.

Protocols such as SAML (Security Assertion Markup Language), Kerberos, and LDAP (Lightweight Directory Access Protocol) have long been used to implement SSO in enterprise environments. While each protocol functions differently, the shared benefit is that authentication is handled externally and trust is established between the identity provider and the relying party (the system the user is trying to access). These technologies are still widely used, particularly in environments with legacy systems or existing Active Directory infrastructure.

SSO does not eliminate the need for strong authentication. It simply moves that responsibility upstream. For example, an identity provider in an SSO environment may still require MFA or passwordless authentication. Organizations should ensure that the initial authentication to the identity provider is appropriately secured, as it becomes the gateway to multiple downstream services.

Conclusion

This document covers the concept of authentication methods, bringing together information found across several IDPro Body of Knowledge articles. Various forms of authentication methods are discussed ranging from traditional single factor methods to more modern passwordless methods. The best methods to leverage for reducing security risks and optimizing end user experience are passwordless methods such as passkeys, authenticator apps, and FIDO2 security keys.