What is Authentication?

Authentication is the process of verifying a user or device before allowing access to a system or resources.

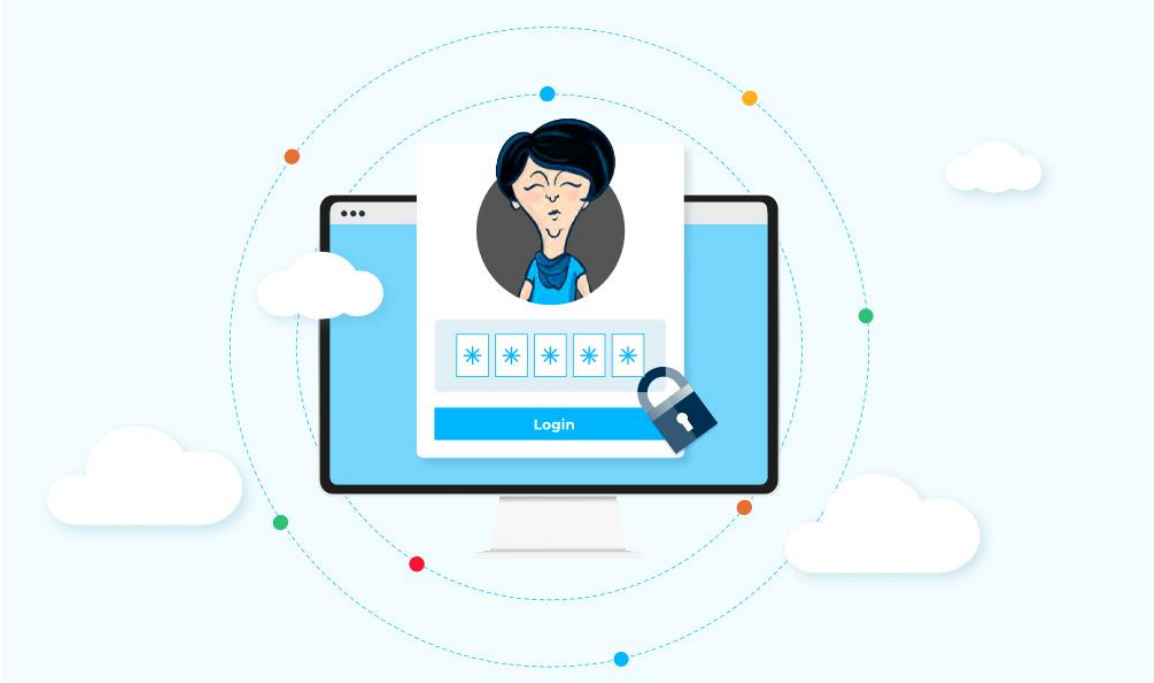
In other words, authentication means confirming that a user is who they say they are. This ensures only those with authorized credentials gain access to secure systems. When a user attempts to access information on a network, they must provide secret credentials to prove their identity. Authentication allows you to grant access to the right user at the right time with confidence. But this doesn't occur in isolation.

Authentication is part of a three-step process for gaining access to digital resources:

- ✓ **identification**—Who are you?
- ✓ **Authentication**—Prove it.
- ✓ **Authorization**—Do you have permission?

Identification requires a user ID like a username. But without identity authentication, there's no way to know if that username actually belongs to them. That's where authentication comes in—pairing the username with a password or other verifying credentials.

The most common method of authentication is a unique login and password, but as cybersecurity threats have increased in recent years, most organizations use and recommend additional authentication factors for layered security.



History of Authentication

Digital authentication goes back to the 1960s when modern computers became available at large research institutes and universities. Back then, computers were massive—often taking up entire rooms—and a scarce resource. Most universities that had a computer only had one. That meant students and researchers had to share it. But this also meant that users could access other users' files without limitation.

When Fernando Corbato, a student at MIT, noticed this weakness, he created a basic password program that prompted the user to enter their password and saved it within a plaintext file in the file system. From there, digital authentication was born.

Importance of Authentication

- Cyberattacks are a critical threat to organizations today. As more people work remotely and cloud computing becomes the norm across industries, the threat landscape has expanded exponentially in recent years.
- As a result, authentication has become an increasingly important mitigation strategy to reduce risk and protect sensitive data. Authentication helps organizations and users protect their data and systems from bad actors seeking to gain access and steal (or exploit) private information
- Organizations that invest in authentication as part of an identity and access management (IAM) infrastructure strategy
- enjoy multiple ***benefits***, including:

✓ Limiting data breaches

✓ Reducing and managing organizational costs

✓ Achieving regulatory compliance

Authentication Use Cases

Today, authentication is common practice not only among IT professionals and scientists, but for non-technical users as well. Whether that's logging in to Facebook with a username and password or opening a phone with Touch ID or a unique PIN, most people have used authentication to access their private information and devices at home and at work.

Of course, as technology has advanced and hackers have become more adept and widespread, new methods of authentication are gaining traction to better

secure personal, business, and government resources from unauthorized access.

Types of Authentication

Cybercriminals always improve their attacks. As a result, security teams are facing plenty of authentication-related challenges. This is why companies are starting to implement more sophisticated incident response strategies, including authentication as part of the process. The list below reviews some common authentication methods used to secure modern systems.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code. These additional forms of authentication can be based of the following types:

1. What you know. Example: An email and password combination
2. What you possess: A credit / debit card, a hardware key (Yubikey)
3. What you are: Biometrics such as fingerprints or retinal scans

- adding a recovery phone number to your Google Account can block up to 100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks that occurred during our investigation.

- Microsoft found that enabling MFA blocks 99.9% of unauthorized login attempts—even if hackers have a copy of a user's current password. This is especially important as passwords alone are no longer enough to

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or a passport.

The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

Users provide their digital certificates when they sign in to a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.

4. Biometric authentication

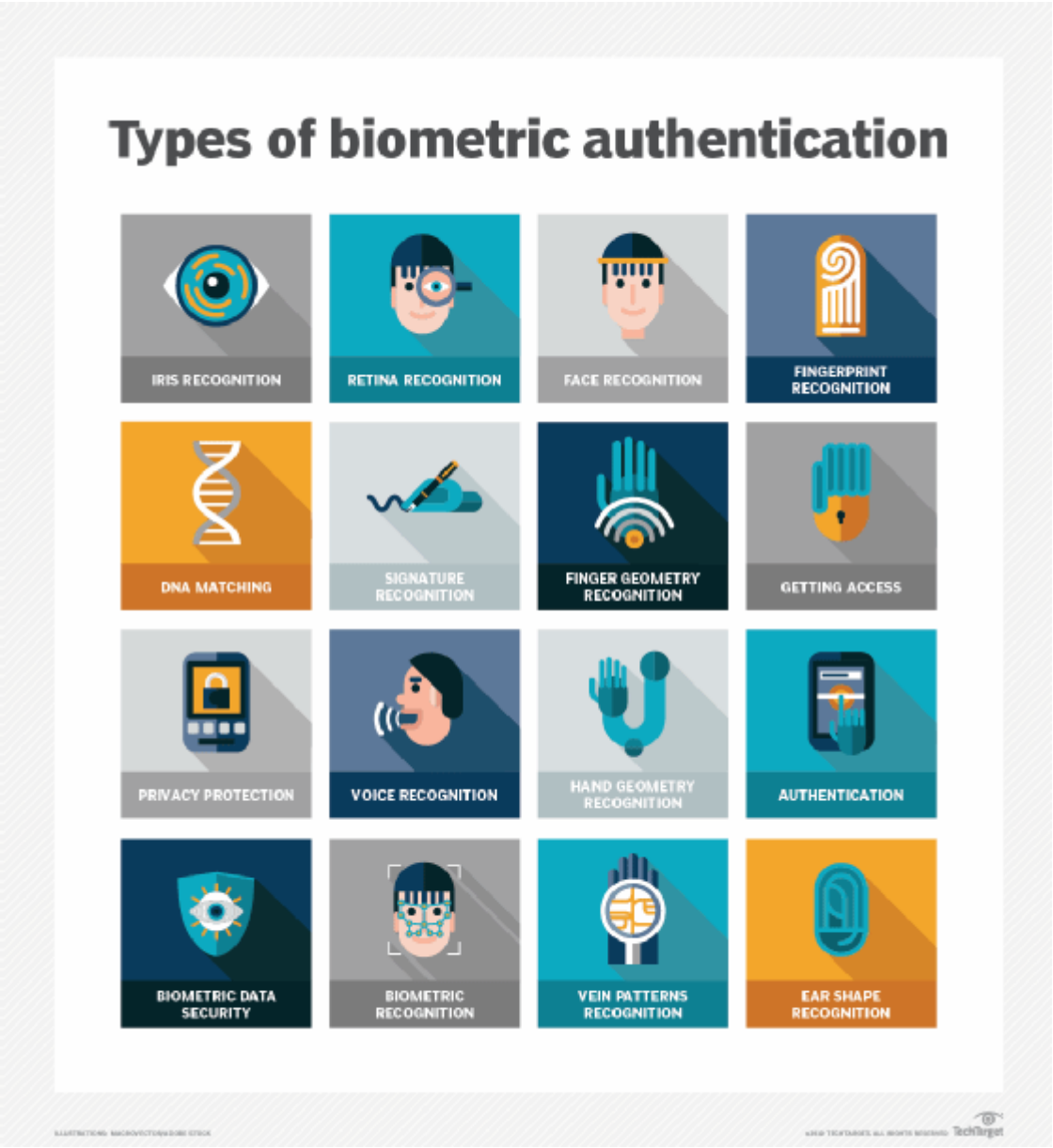
Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Here are key advantages of using biometric authentication *technologies*:

- ***Biological characteristics*** can be easily compared to authorized features saved in a database.
- ***Biometric authentication*** can control physical access when installed on gates and doors.
- ***You can add biometrics*** into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication *methods* include:

- **Facial recognition**—matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar, like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.
- **Fingerprint scanners**—match the unique patterns on an individual's fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people's fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers, despite their frequent inaccuracies. This popularity can be attributed to iPhones.
- **Speaker Recognition** —also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities. A voice-protected device usually relies on standardized words to identify users, just like a password.
- **Eye scanners**—include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the colored ring around the pupil of the eye. The patterns are then compared to approved information stored in a

database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses.



What is a passphrase?

A passphrase is a sentence like string of words used for authentication that is longer than a traditional password, easy to remember and difficult to crack. Typical passwords range, on average, from eight to 16 characters, while passphrases can reach up to 100 characters or more.

What is challenge-response authentication and why is it useful?

Challenge-response authentication refers to a set of protocols that helps validate actions to protect digital assets and services from unauthorized access. This protocol usually has two components – a question and a response – where a verifier presents a challenge to a user, who must provide a correct answer for authentication. Challenge-response protocols can be as simple as a password or a dynamically generated request.

What Is a Security Token?

Security tokens are **physical devices** that people use as hardware authenticators to securely access a system. The token typically contains cryptographic information that is specific for each user and is used for user authentication into that system.

Security tokens come in many form factors such as a USB key or a name badge containing a chip inside. Car remotes are examples of security tokens people use regularly.

Security tokens are used to authenticate users, and they can be used either to substitute passwords or other authentication methods or used as additional authentication in multi-factor authentication (MFA) flow. When used in an MFA flow the security token is considered a “possession” factor ie “something the user has”, which can be combined with an inherence or knowledge factor for MFA.