Biometric Authentication

Return to Glossary

Biometric Authentication is a security process that relies on the unique biological characteristics of individuals to verify they are who they say they are. Biometric authentication systems compare physical or behavioral traits to stored, confirmed, authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Typically, biometric authentication is used to manage access to physical and digital resources, such as buildings, rooms, and computing devices.

Biometric identification uses biometrics, such as fingerprints or retina scans, to identify a person, whereas biometric authentication is the use of biometrics to verify people are who they claim to be.

Biometric authentication methods

The following technologies can be used to digitally identify people or grant them permission to access a system:

Chemical biometric devices

- **DNA (deoxyribonucleic acid) matching** uses genetic material to identify a person.

Visual biometric devices

- **Retina scans** identify subjects by analyzing the pattern of blood vessels at the back of their eyes.
- **Iris recognition** uses a picture of the iris to identify people.
- **Fingerprint scanning** identifies people based on their fingerprints.
- **Hand geometry recognition** verifies identity or authorizes transactions using a mathematical representation of the unique characteristics of people's hands. This is done by measuring the distances between various parts of the hand, including finger length, finger breadth and the shape of the valleys between the knuckles.
- **Facial recognition** relies on the unique characteristics and patterns of people's faces to confirm their identity. The system identifies 80 nodal points on a human face, which make up numeric codes called faceprints.
- **Ear authentication** verifies identity-based on users' unique ear shape.
- **Signature recognition** uses pattern recognition to identify individuals based on their handwritten signature.

Vein or vascular scanners

- **Finger vein ID** identifies individuals based on the vein patterns in their fingers.

Behavioral identifiers

- **Gait analyzes** the way people walk.
- **Typing recognition** establishes people's identity based on their unique typing characteristics, including how fast they type.

Auditory biometric devices

- **Voice ID** identifies individuals by their voice and relies on characteristics created by the shape of the mouth and throat.

Source: https://searchsecurity.techtarget.com/definition/biometric-authentication