

# Biometrics: When You Are the Credential

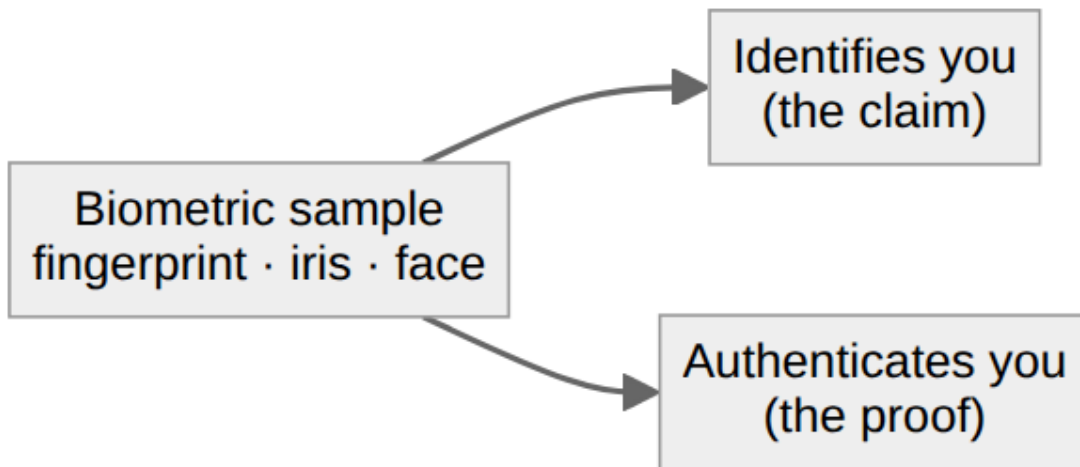
Tue, Aug 4, 9:00 AM EDT · <https://scottslab.io/posts/biometrics-something-you-are>



## TL;DR

A biometric does identification and authentication in a single gesture, which is why it counts as "something you are." Every modality trades security against how much users hate it: fingerprints won on convenience, iris scans on security, voiceprints lose to replay. And unlike a password, a leaked biometric is permanent, so treat it as one strong factor, never the only one.

Biometrics are the odd one out among identification mechanisms, because a single fingerprint does two jobs at once: it identifies you and it authenticates you. That's why they file under "something you are." A username needs a password behind it; a biometric is the claim and the proof in the same gesture.



The engineering reality is that every modality trades security against how much users hate using it, and that trade decides where each one actually gets deployed. Fingerprints won the consumer world because they're accurate enough and nobody minds touching a sensor: low friction, good-enough security, everywhere. Iris and retina scans are far harder to fool and far more intrusive, so they live where the security bar justifies making people lean into a scanner. Voiceprints are easy to accept and easy to defeat with a recording, which is why they rarely stand on their own. Facial recognition keeps getting more accurate and keeps making people uneasy, and that discomfort is its own deployment cost. There's a long tail beyond these (vein patterns, hand geometry, even gait analysis) that mostly shows up in niches where the mainstream options don't fit.



Two failure modes are worth holding onto. The first is that a biometric measurement is fuzzy in a way a password never is. It's a probabilistic match, so the system is always balancing letting the wrong person in against locking the right person out. (That balance has real metrics behind it, which is a topic on its own.) The second is the one people forget in the excitement: you can't change your fingerprint. A leaked password is a reset; a leaked biometric template is permanent. That's the whole reason a biometric is best treated as one strong factor among several, not the single thing standing between an attacker and the account.