

Identification, Authentication, Authorization — and the Accounting Nobody Talks About

Mon, Aug 3, 9:00 AM EDT · <https://scottslab.io/posts/identification-authentication-authorization-accounting>



TL;DR

Identification is the claim, authentication is the proof, and authorization is the yes/no on what you're allowed to do. Mix them up and you'll debug the wrong system. The AAA framework adds accounting, the logging that lets you reconstruct who did what after the fact, and it's the piece that quietly matters most once something goes wrong.

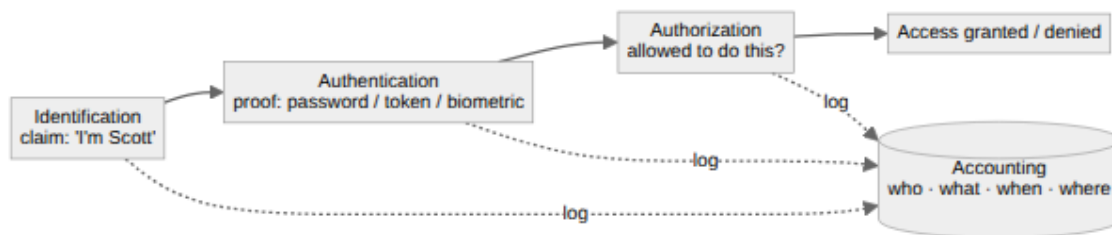
Every access problem I've ever debugged comes down to the same three questions asked in order, and most of the confusion I see comes from smearing them together: it shows up in tickets, in postmortems, in people cramming for the exam. Someone reports "authentication is broken" when the account simply wasn't authorized. That's not pedantry: the fix lives in a completely different system depending on which step actually failed.

Identification is just the claim. I type a username, tap a badge, say "I'm Scott." No proof yet. A username was never meant to be secret, which is exactly why it's usually something as guessable as first-initial-last-name. It's the label everything else hangs on, nothing more.

Authentication is the proof behind the claim. This is where the password, the token, the fingerprint shows up. That's the evidence that I actually am the identity I claimed. The clean way to keep the

first two straight is to look at the mechanism: a username identifies, a password authenticates. One names you, the other proves it.

Authorization is the separate question of whether that proven identity is allowed to do the thing. You can authenticate perfectly and still be told no. A valid login to a system you have no permissions on is authentication succeeding and authorization denying. Conflate the two and you'll spend an hour "fixing" the wrong one.



The framework people quote is AAA (authentication, authorization, accounting), and it's the word that gets dropped that matters most after an incident. Accounting is the logging: who did what, when, from where. The first three happen in the moment; accounting is what lets you reconstruct the moment later. Every detection rule I've written and every investigation I've run leans on that trail existing. The first three decide access. The fourth is how you answer "what happened" when access gets abused. If it isn't being recorded, the honest answer is that you don't know.