

Proving Identity, Part 1: Usernames and Access Cards

Mon, Aug 3, 4:00 PM EDT · <https://scottslab.io/posts/usernames-and-access-cards>



TL;DR

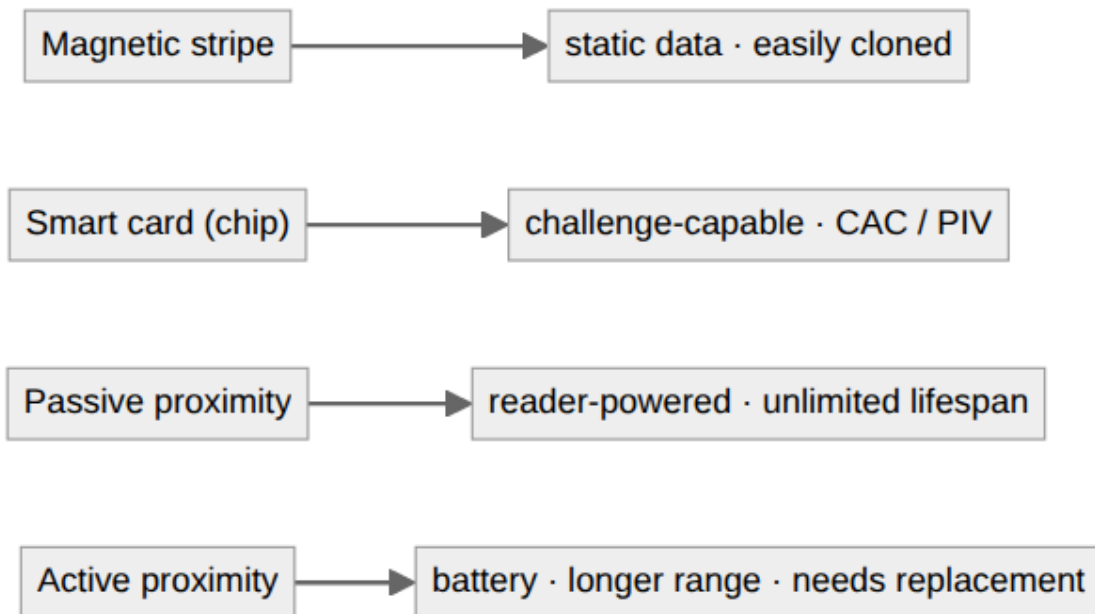
A username is a label, not a secret, so stop hardening it. The secret belongs in the authentication step. Access cards run from trivially cloneable magnetic stripes to challenge-capable smart cards, with passive and active proximity cards trading read range against a battery you'll eventually have to replace. Pick the mechanism whose failure mode you can actually live with.

Identification is the cheap step, but the mechanisms people use for it have wildly different threat models, and it's worth knowing which is which before you trust any of them. Start with the two most common: the username you type and the card you carry.

The username is the baseline, and the thing to internalize is that it was never meant to be a secret. First-initial-last-name is fine. The username is a label, not a control. Hiding it or rotating it is effort spent on the wrong layer. The secret belongs in the authentication step. If your security depends on nobody guessing the username, you don't have a security control, you have a naming convention.

Access cards are where physical and logical security meet, and the technology matters more than the plastic suggests. A magnetic stripe is trivial to clone with gear off the internet. It's static data on

a strip, so anything that can read it can copy it. I wouldn't trust one to guard anything that matters. A smart card is a real step up: an embedded chip that participates in a challenge instead of just handing over static data, which is why the DoD's Common Access Card is a chip, not a stripe. You can't clone what won't reveal its secret.



Proximity cards split one more level down, and it's a convenience-versus-maintenance trade. A passive prox card draws its power from the reader, so it has no battery and effectively lasts forever, at the cost of short range. An active prox card carries its own battery for a longer read range, which helps with gates and vehicles. But that battery eventually dies, so now you've signed up for a replacement cycle across every badge you issued.

None of these are interchangeable. A username you can shout across the room, a magstripe you can clone in a parking lot, a smart card you can't easily forge. Pick the mechanism whose failure mode you can actually live with, and don't let the fact that a badge "feels" secure stand in for knowing how it works.