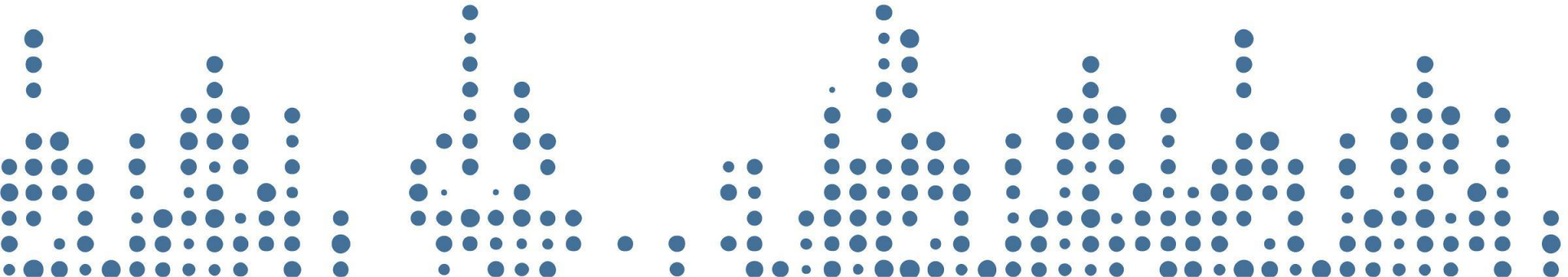
Everything you never wanted to learn about auth

October 29, 2024



Alex K Gold

Solutions Engineering + Support @PositPBC

Former data scientist + Segway tour guide

Econ PhD Dropout



Author: DevOps for Data Science
Blog: alexkgold.space

posit™

Belief:

But that's not **my** problem



posit™

Auth comes for us all.



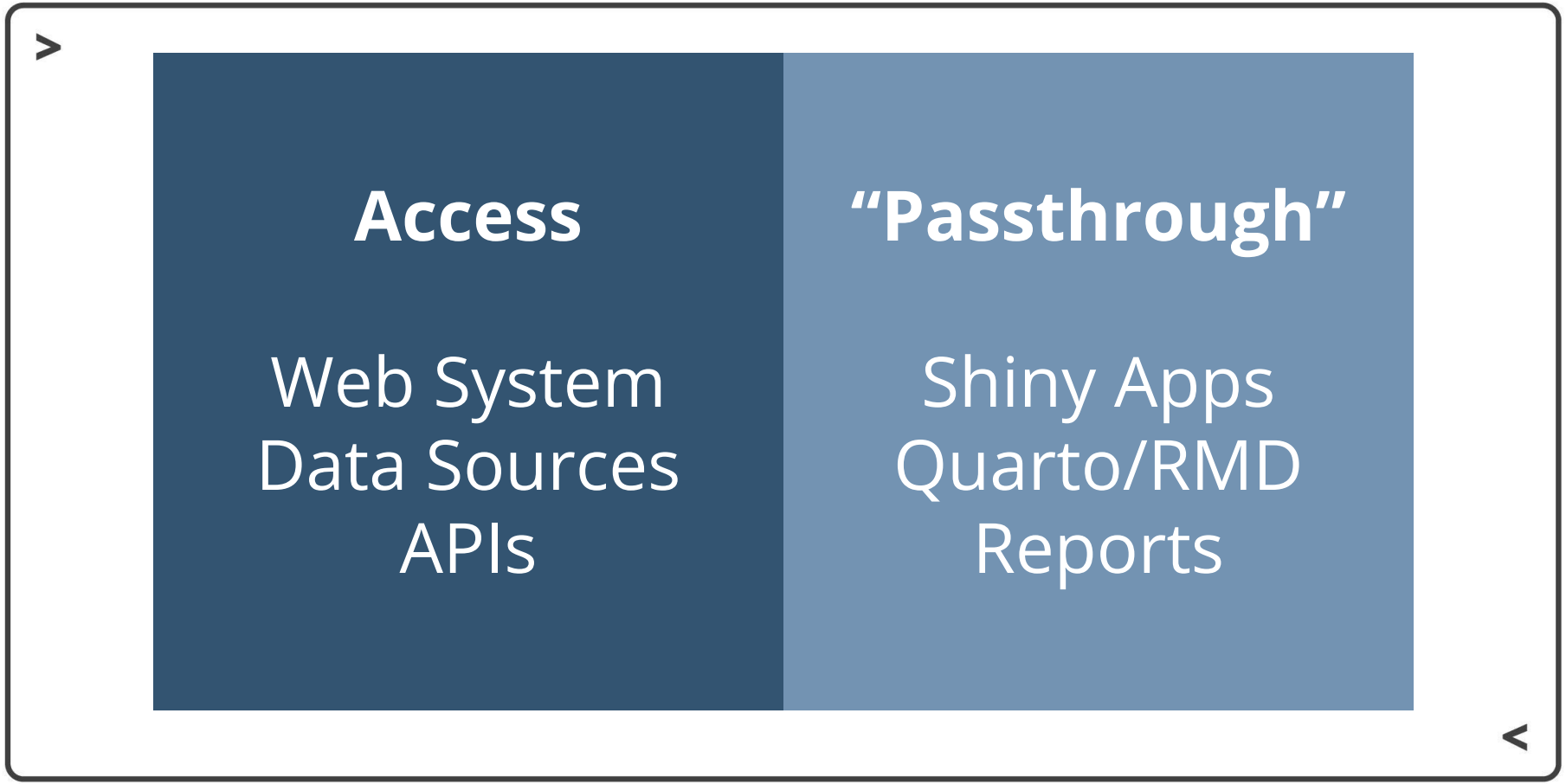

posit™
A long, long time ago...

posit TestDrive!

Username	

Password	

Username: Admin
Password: Admin

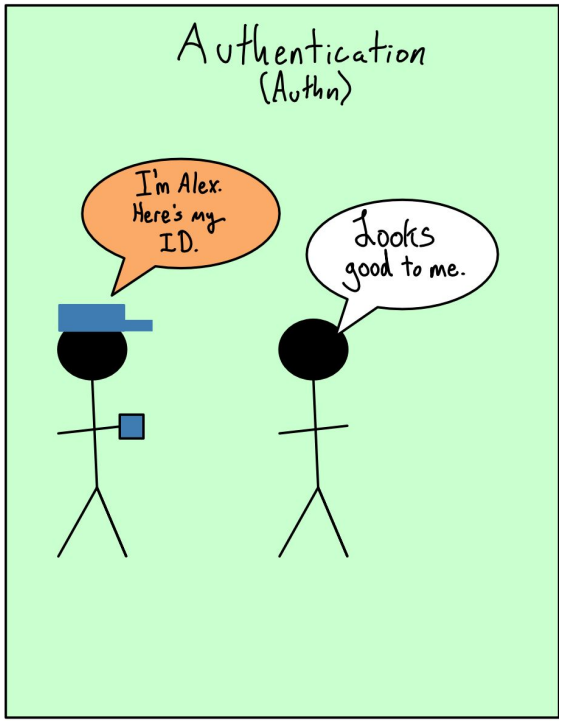

Access
Web System
Data Sources
APIs
“Passthrough”
Shiny Apps
Quarto/RMD
Reports

posit™

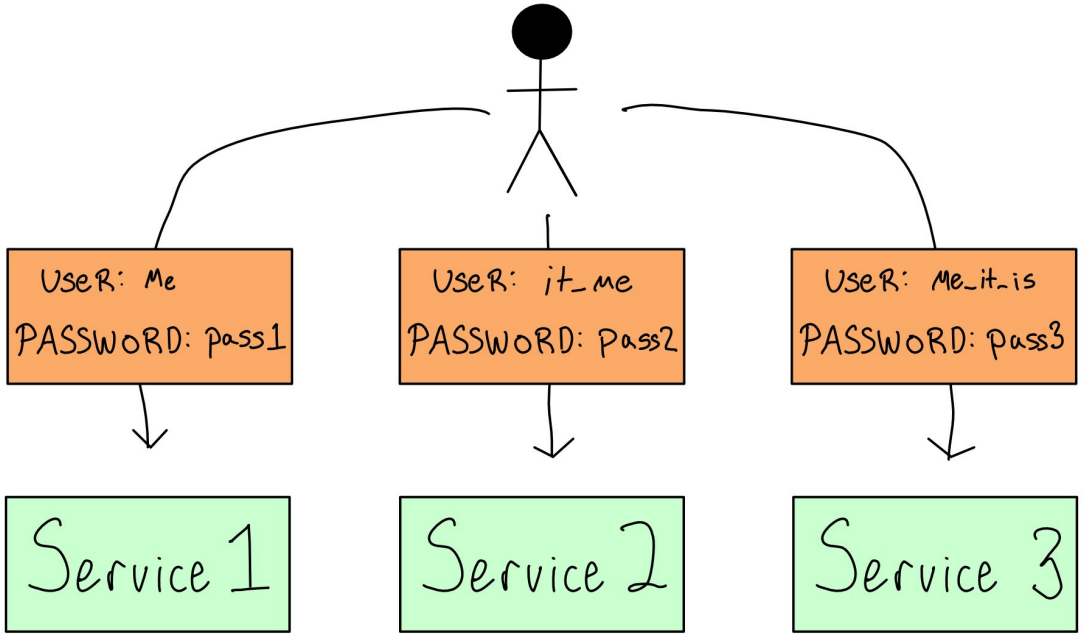
Imagine a building...

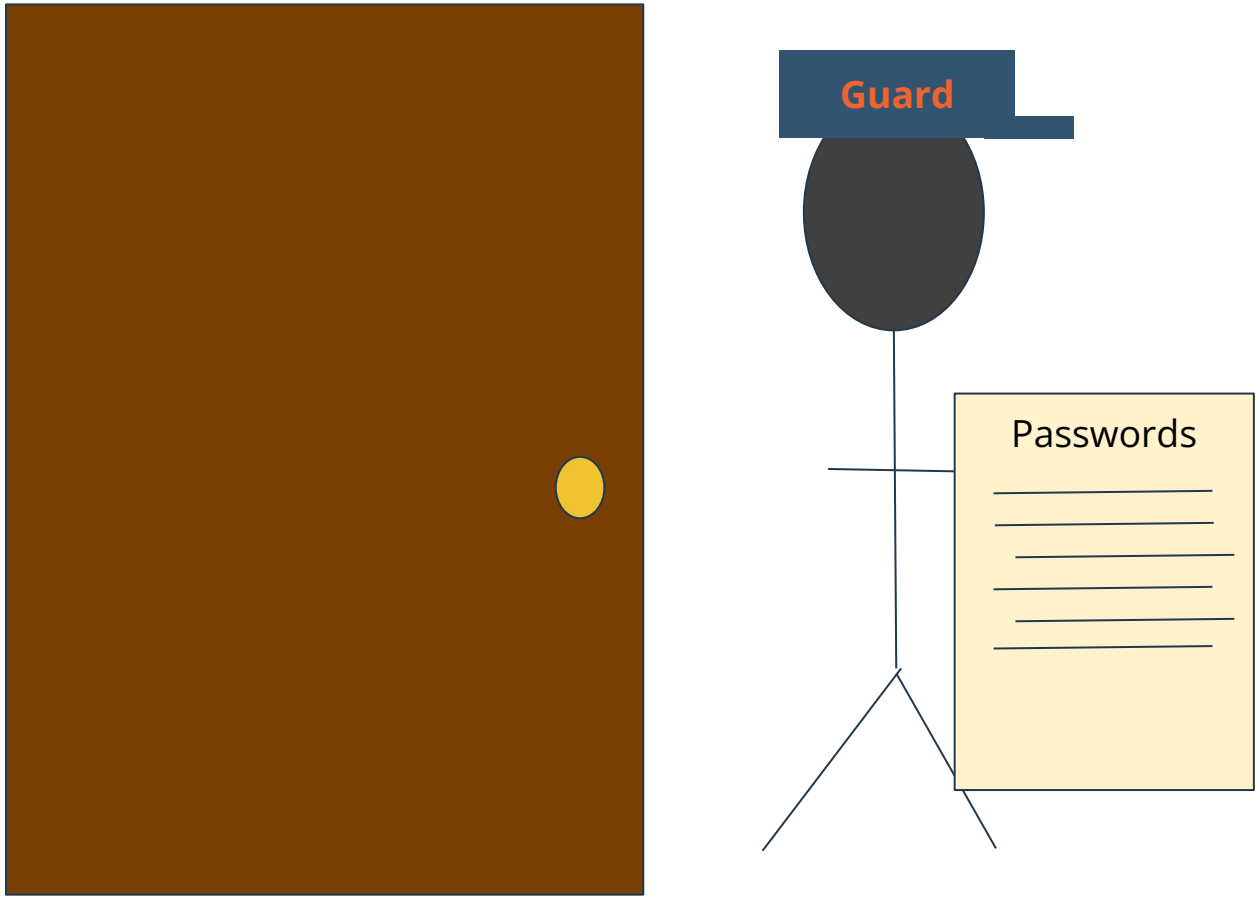


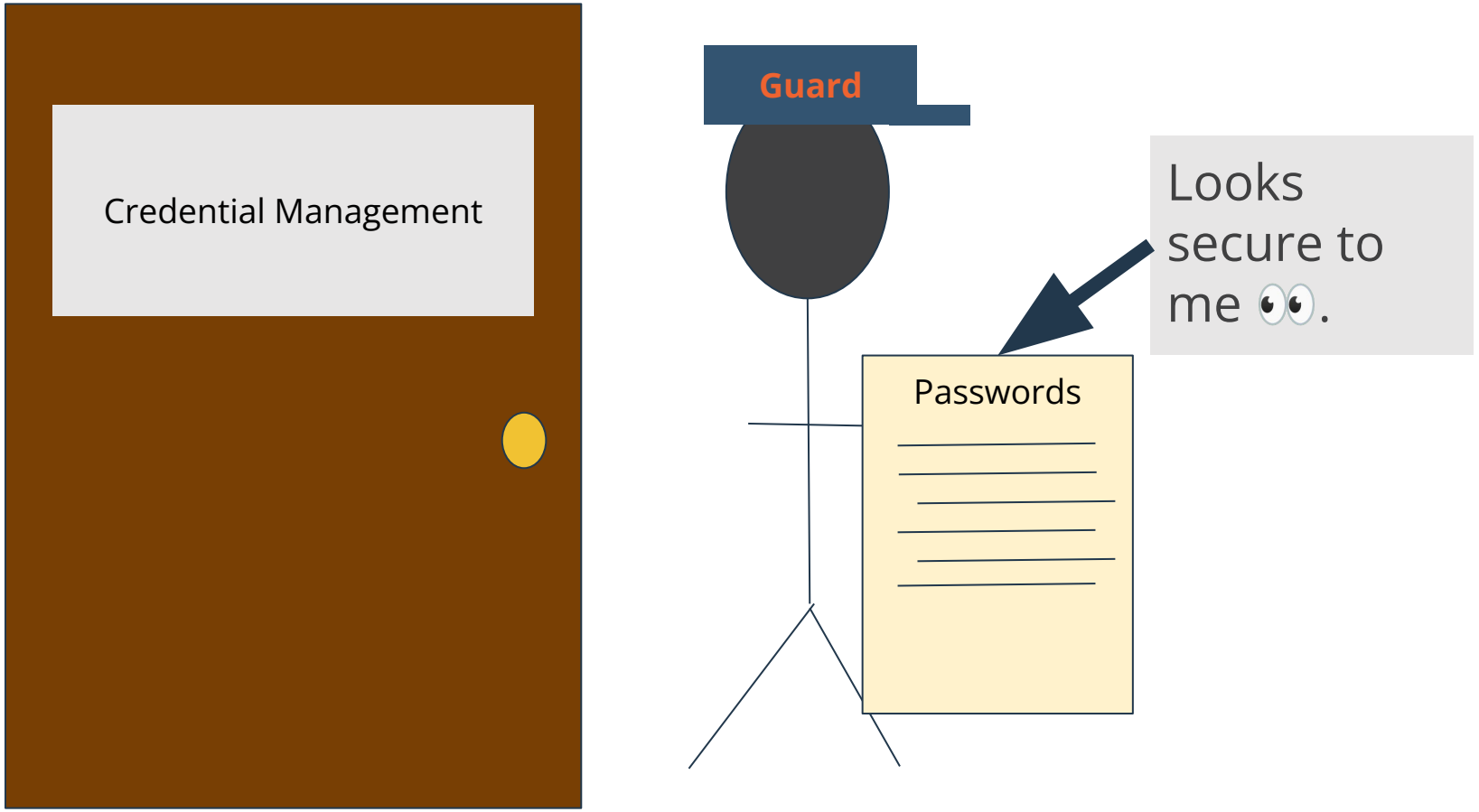
Auth

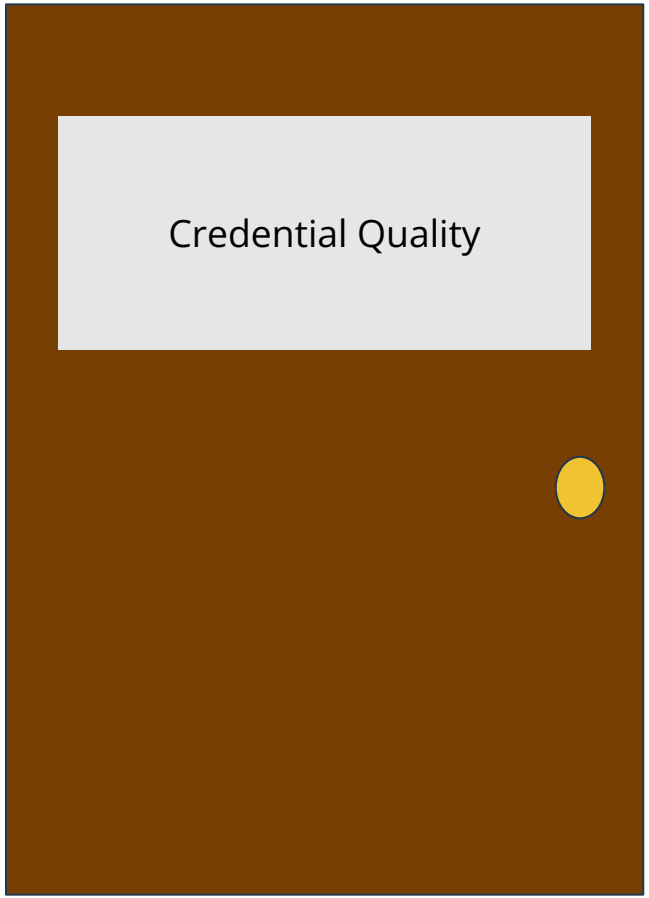


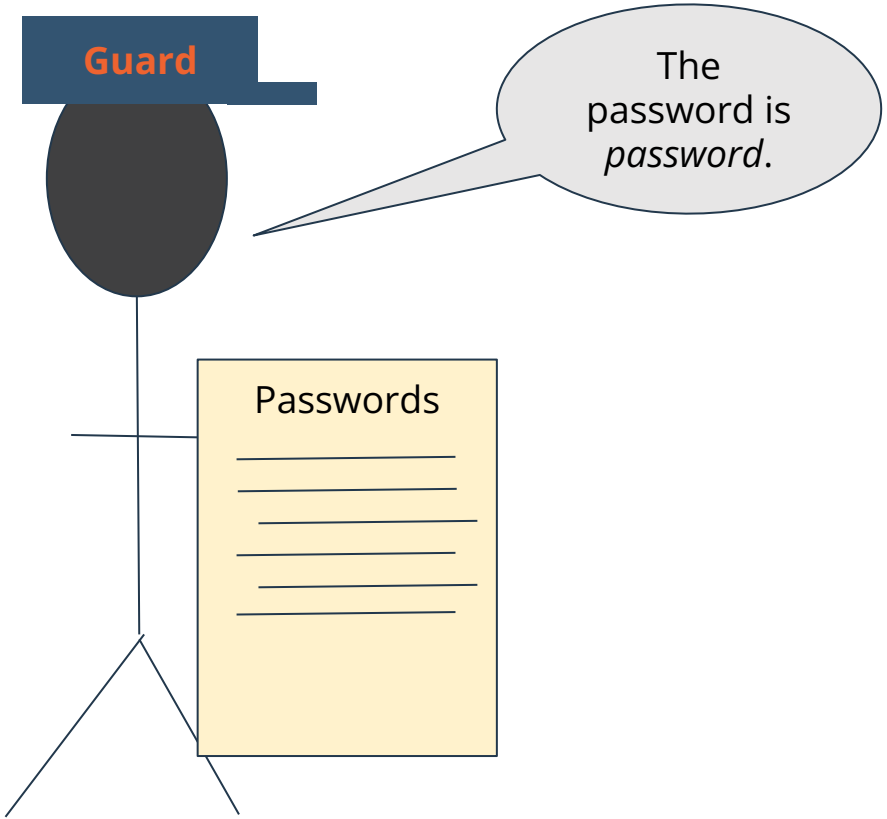
Simple Auth

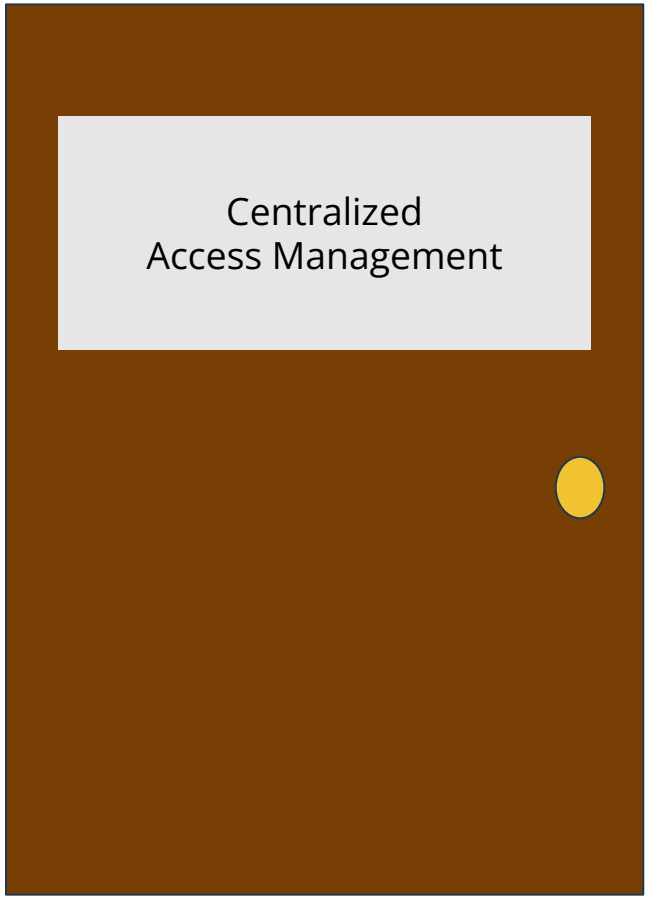

USER: Me
PASSWORD: pass1
USER: it_me
PASSWORD: pass2
USER: me_it_is
PASSWORD: pass3
Service 1
Service 2
Service 3

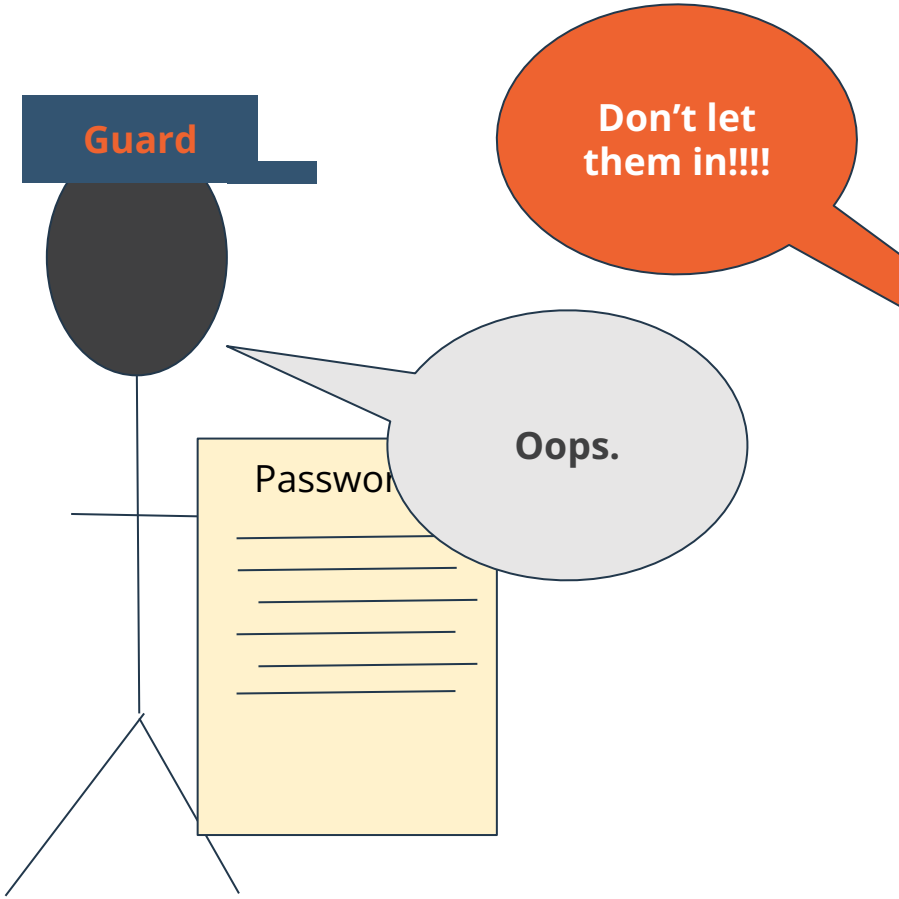

Guard
Passwords


Credential Management
Guard
Looks secure to me 👀.
Passwords

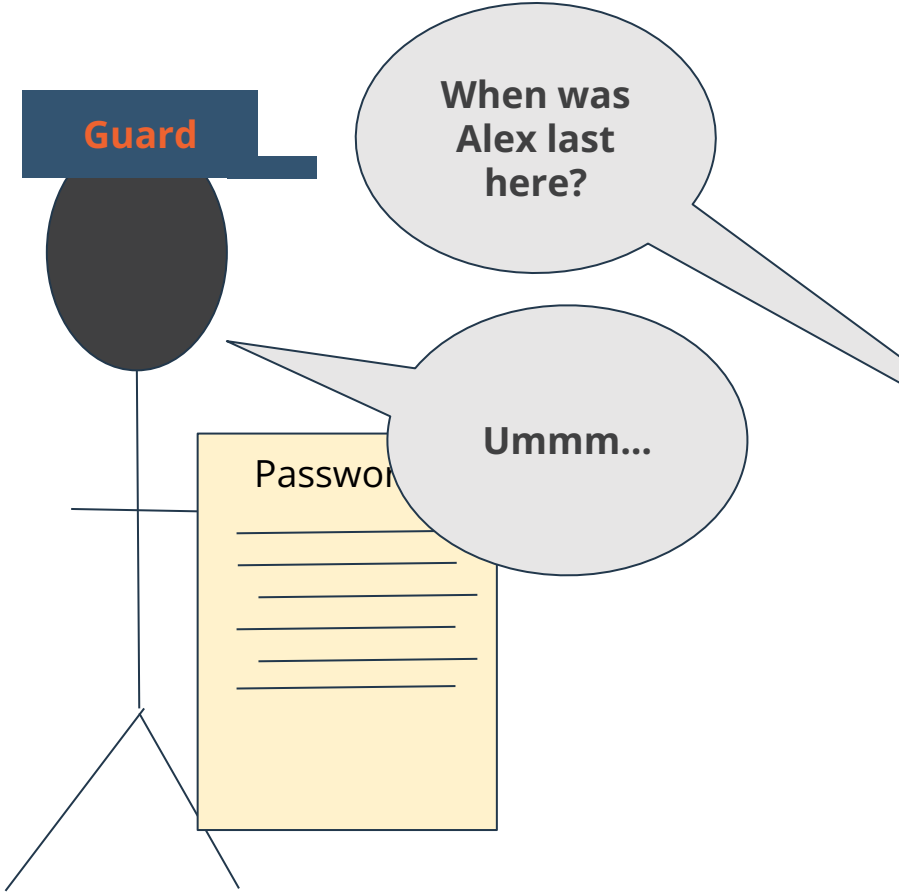

Credential Quality


Guard
The password is *password*.
Passwords


Centralized
Access Management


Guard
Don’t let them in!!!!
Oops.
Passwor

Auditing and Monitoring



An IT/Admin's auth concerns

1. Credential Handling
2. Credential Type
    a. Multi-Factor (MFA), Biometrics, CAC, Passkeys
3. Centralized Management
4. Compliance and Auditability
5. Cloud/SaaS

6. (System compatibility)

posit™

What does *really* SSO mean?



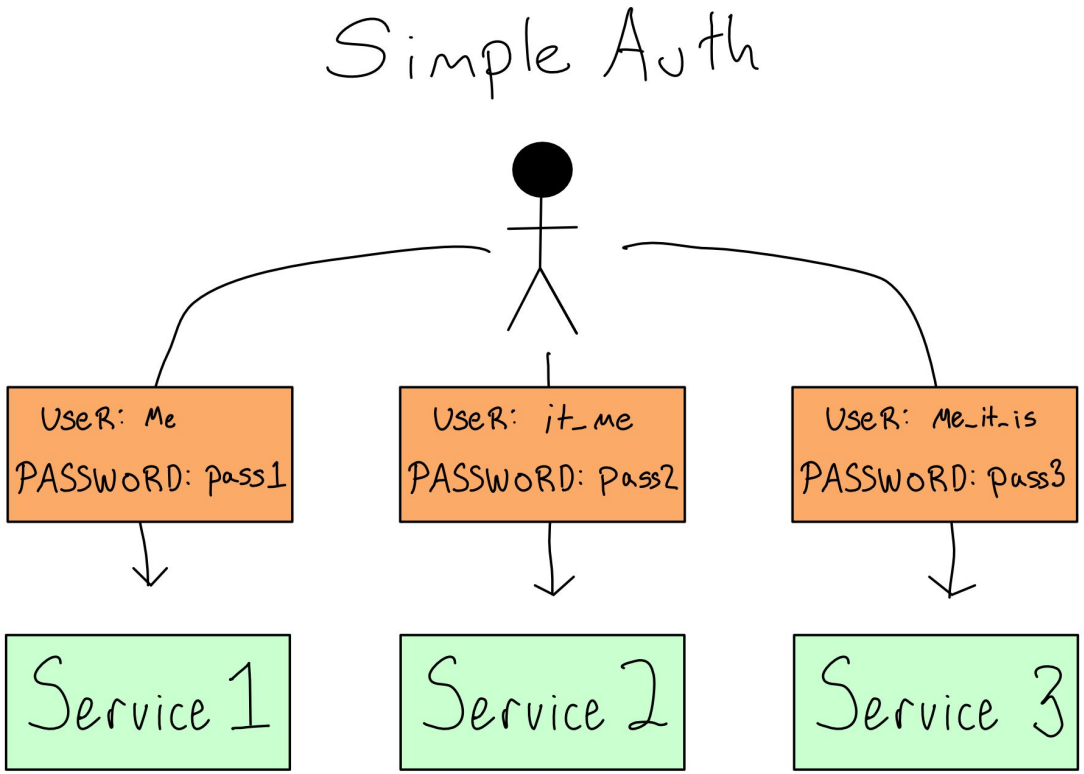
What SSO *should* mean

Credential Handling	
Credential Type	
Centralized Management	
Compliance and Auditability	
Cloud	

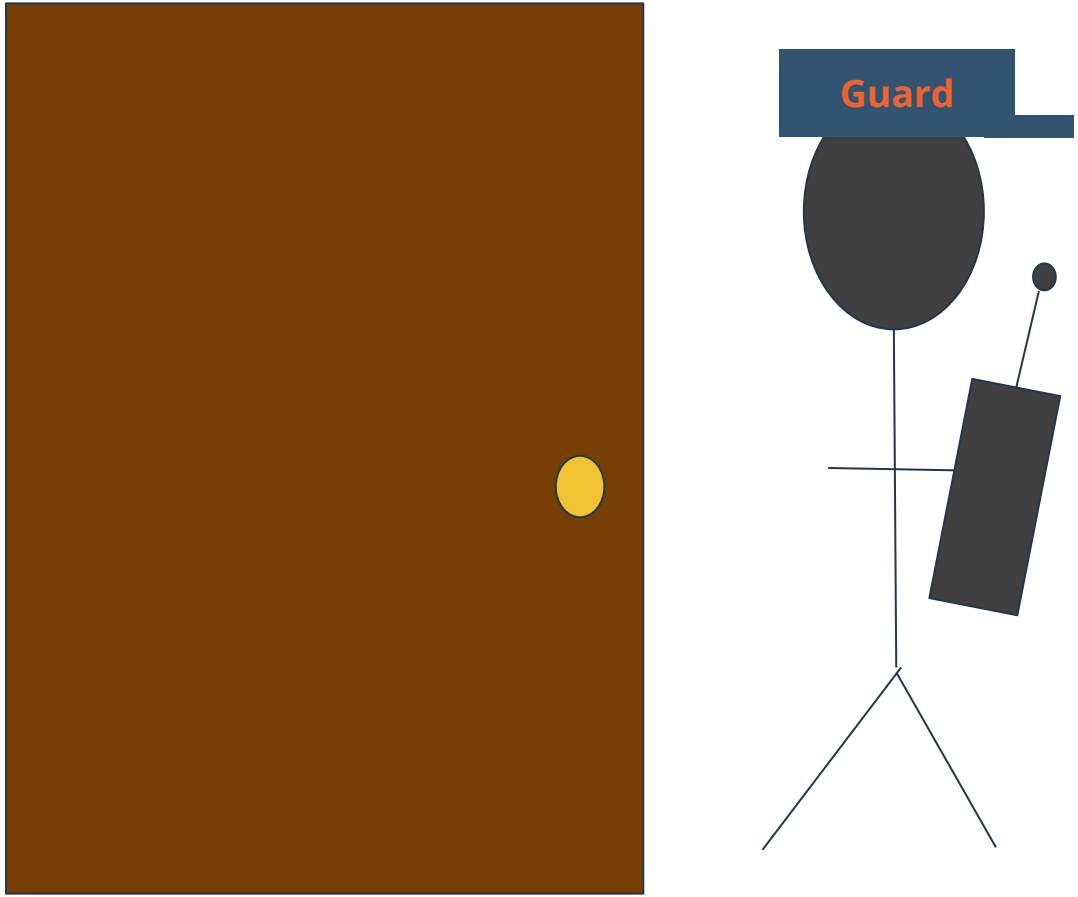
posit™

Evaluating Auth

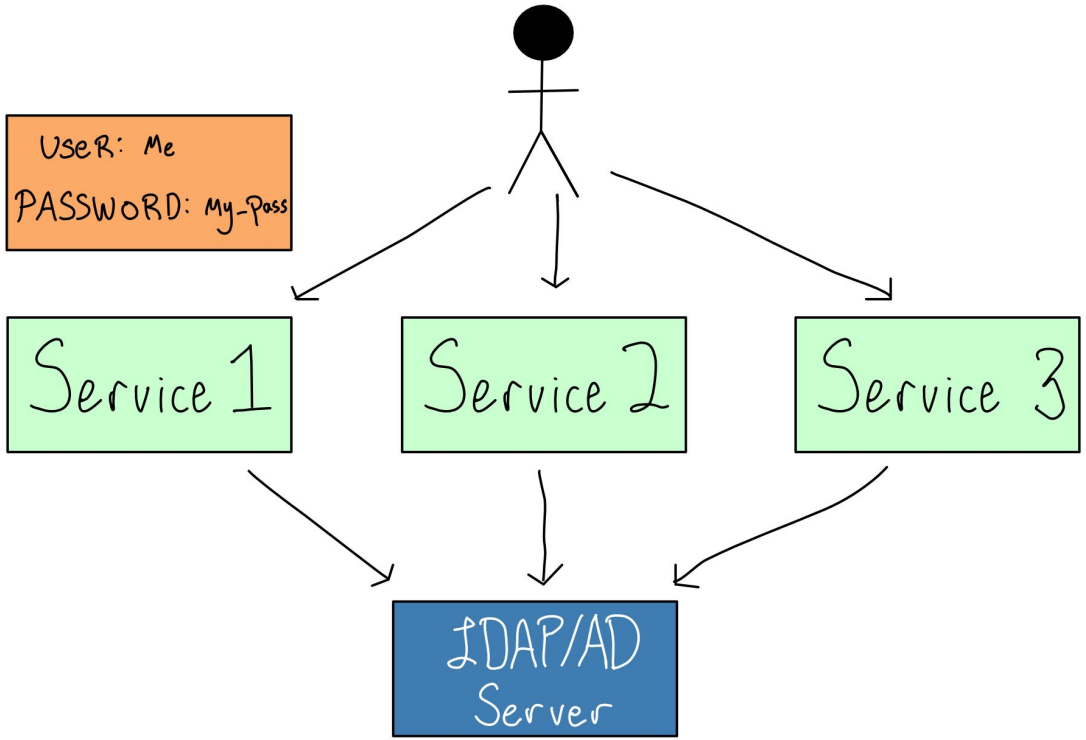




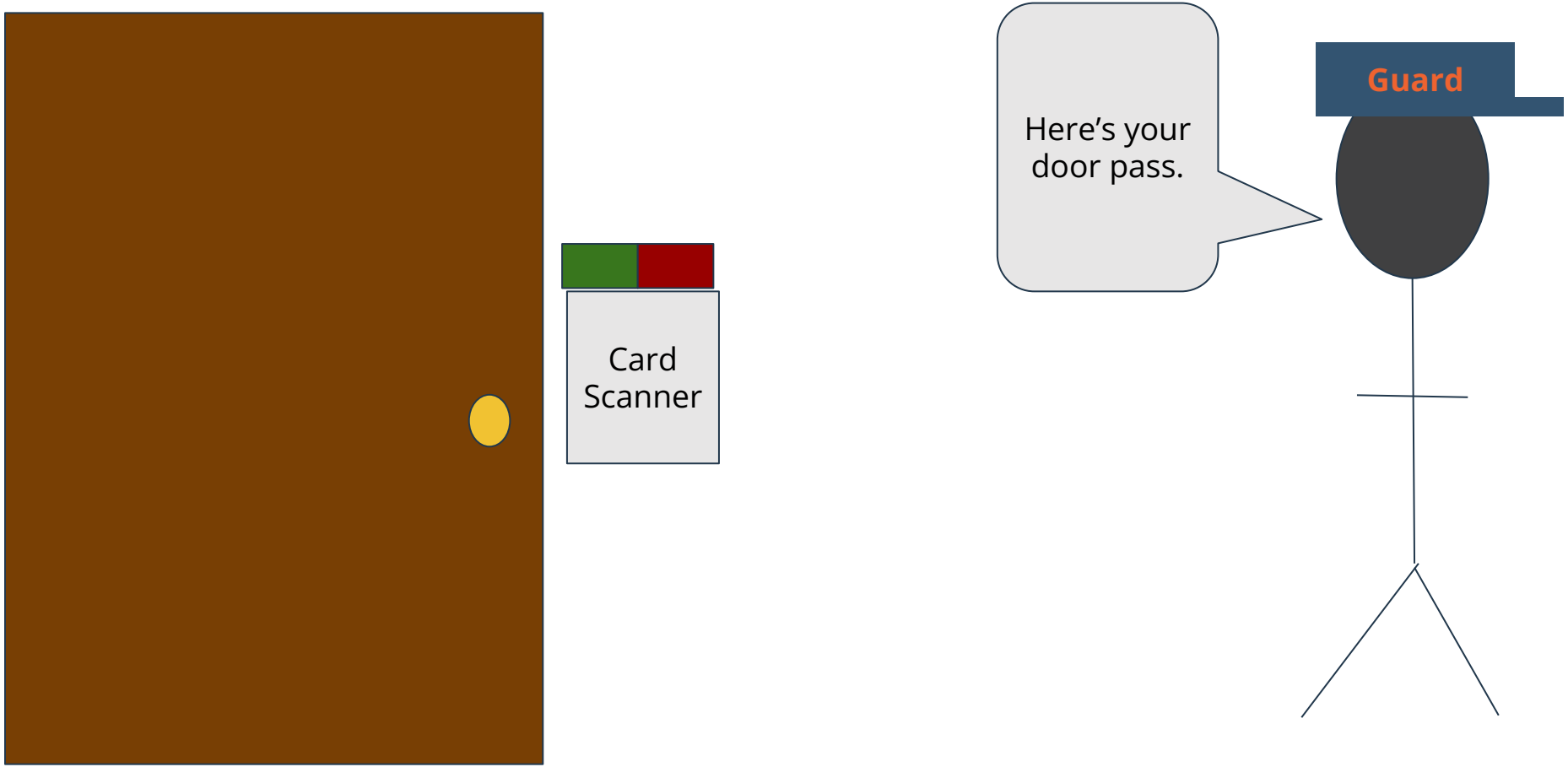
Rubric	
Credential Handling	😱
Credential Type	😱
Centralized Management	😱
Compliance and Auditability	🤷‍♂️
Cloud	❌


Guard

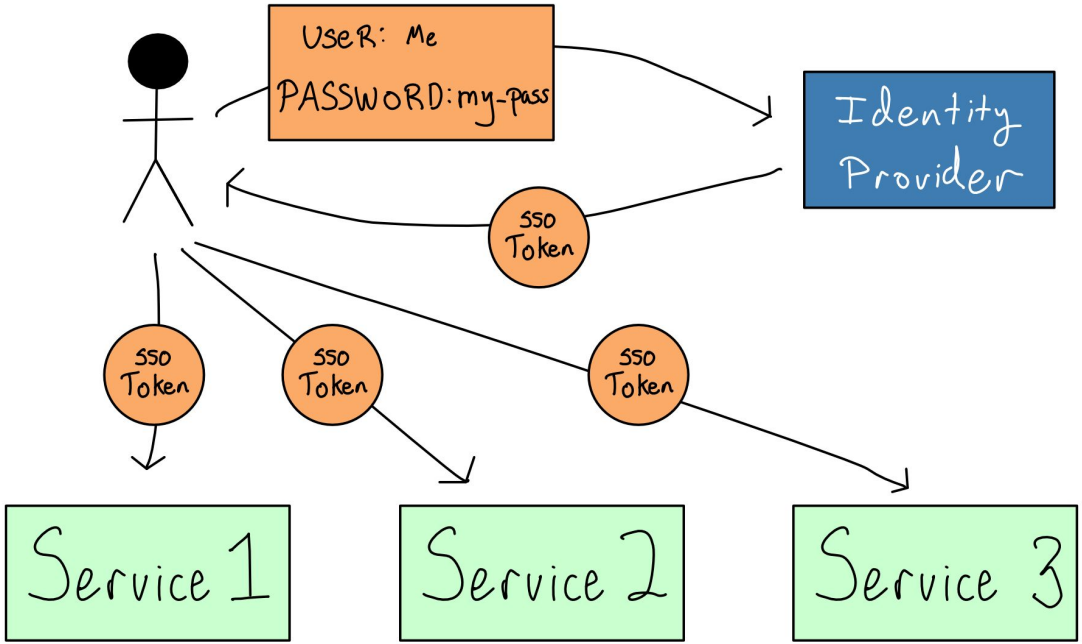
LDAP/AD Auth



Rubric	
Credential Handling	😱
Credential Type	😱
Centralized Management	👍
Compliance and Auditability	🟡
Cloud?	❌


Here’s your door pass.
Guard
Card Scanner

SSO



Rubric	
Credential Handling	👍
Credential Type	👍
Centralized Management	👍
Compliance and Auditability	👍
Cloud	👌

posit™

Now, let's get to some R code!



No chance

J/K

Nope



Lol



⚠️ Bias ⚠️

But I'm not wrong...

posit™

Don’t DIY auth.

Integrate with auth.



Some words you might use:

- Hash/Salt – DIY auth. It bad.
- LDAP/Active Directory (AD) – Microsoft 1990s central access server
- Kerberos – very secure “passthrough” data access, 1990s Microsoft tech
- SAML – early 2000s SSO tech
- OAuth/OIDC – late 2000s SSO tech (cloud-first)
- JWT (JSON Web Token) – the SSO token for OAuth

>

Some things you might actually do:

- Environment variables
  - Sys.setenv(), Sys.getenv()
- Working with JWTs
  - {googledrive}
- In an app on Connect/ShinyApps
  - session$user

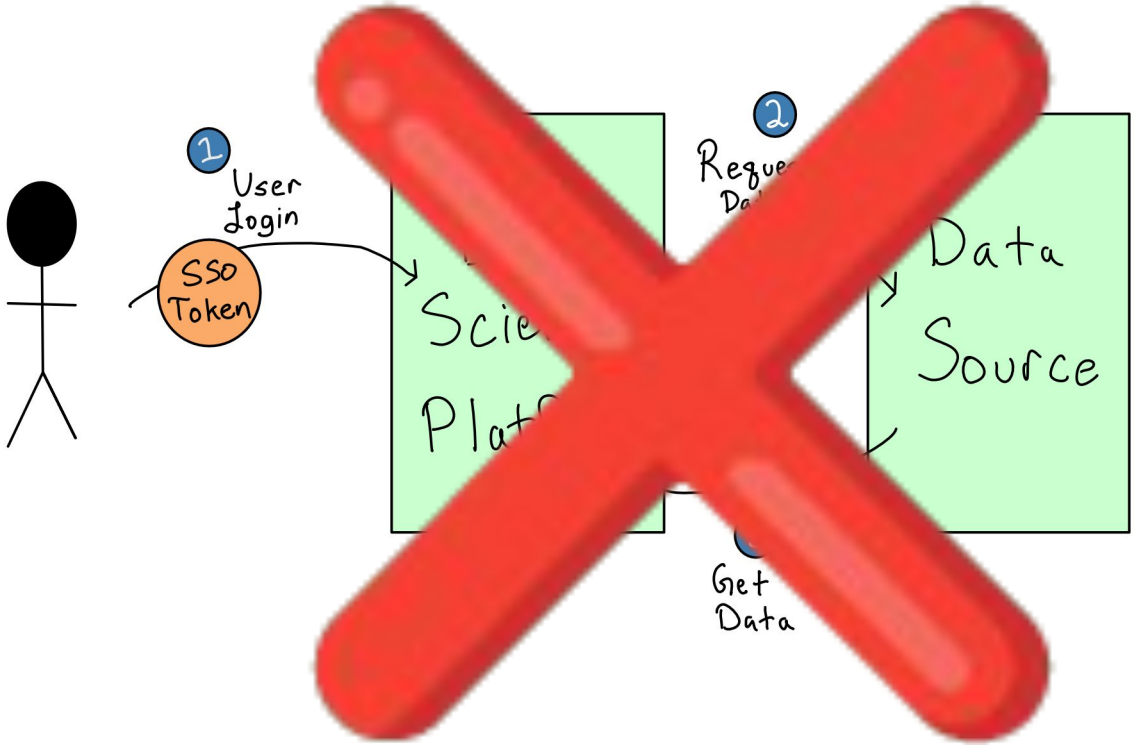
<

posit™

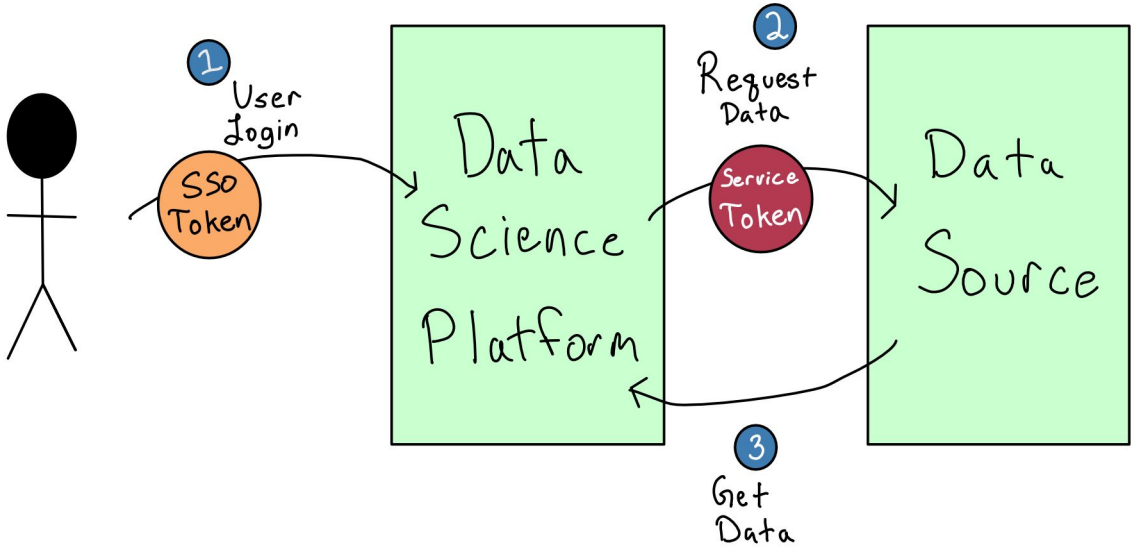
Data “passthrough” is not all it seems.



"Passthrough Auth"



"Passthrough Auth"



You matter for auth and auth matters for you.

 **do4ds.com** 

alexkgold.space