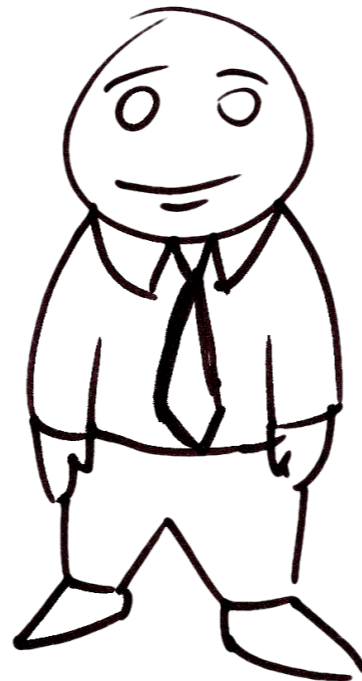
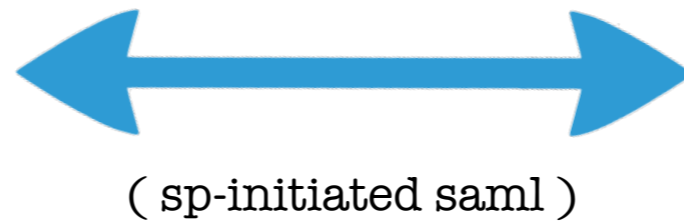


open, mobile, social

these forces are fundamentally changing IT

so what are we doing?

1. consumerization



no passwords, but focused on the web

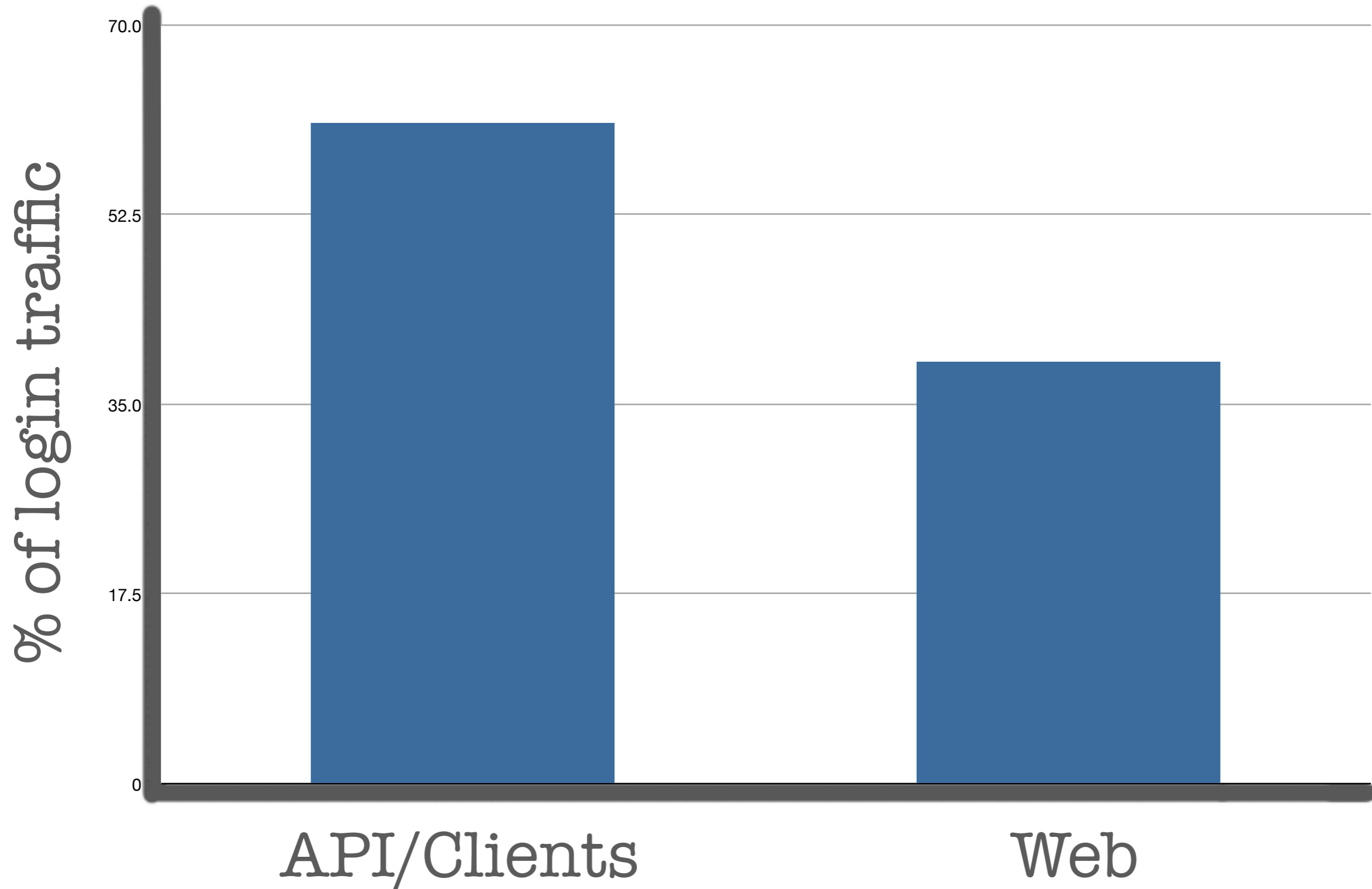
# reality

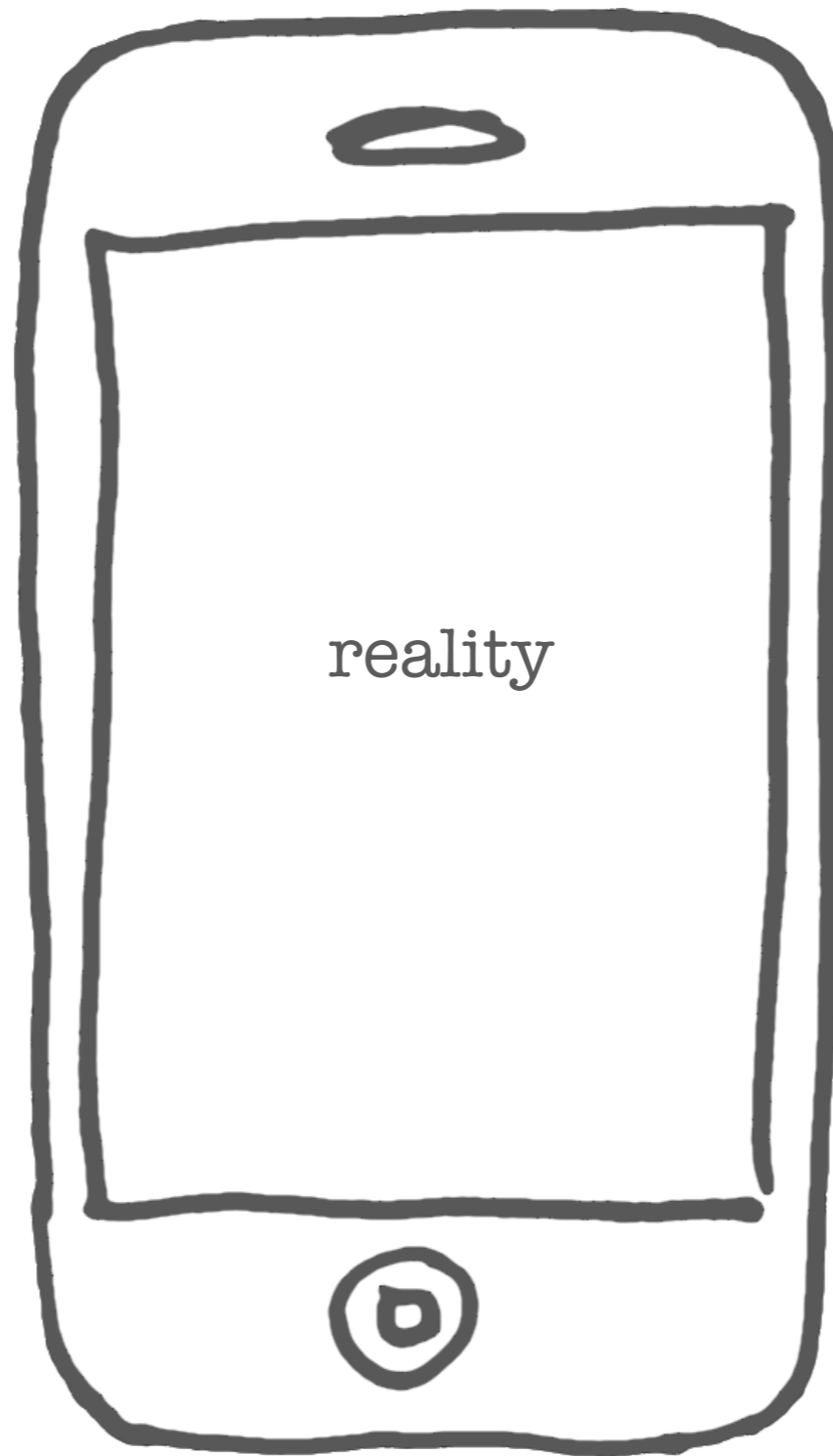
% of login traffic

70.0  
52.5  
35.0  
17.5  
0

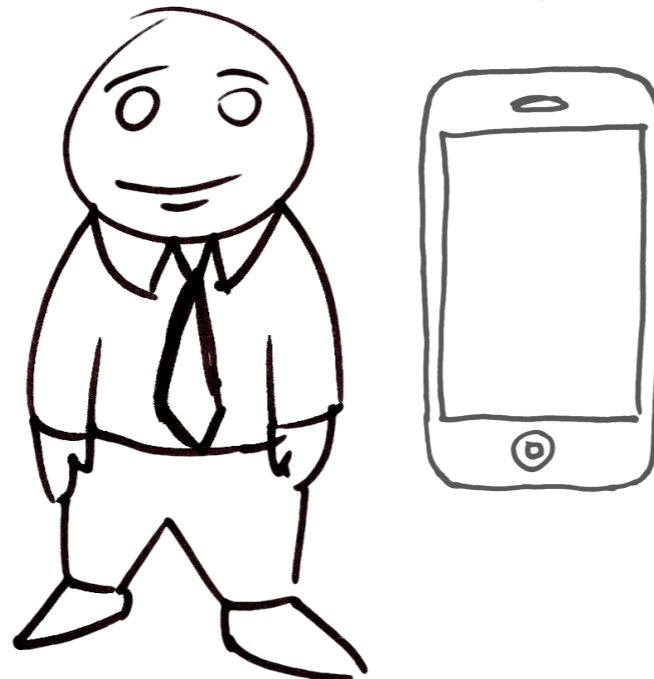


# reality





so what are we doing?

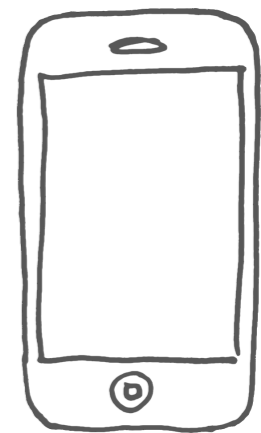
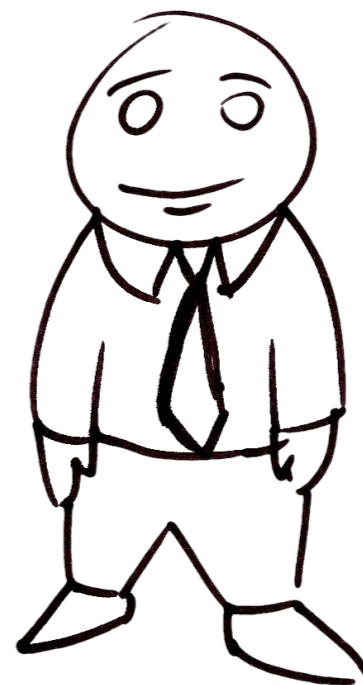


didn't we just get rid of passwords?

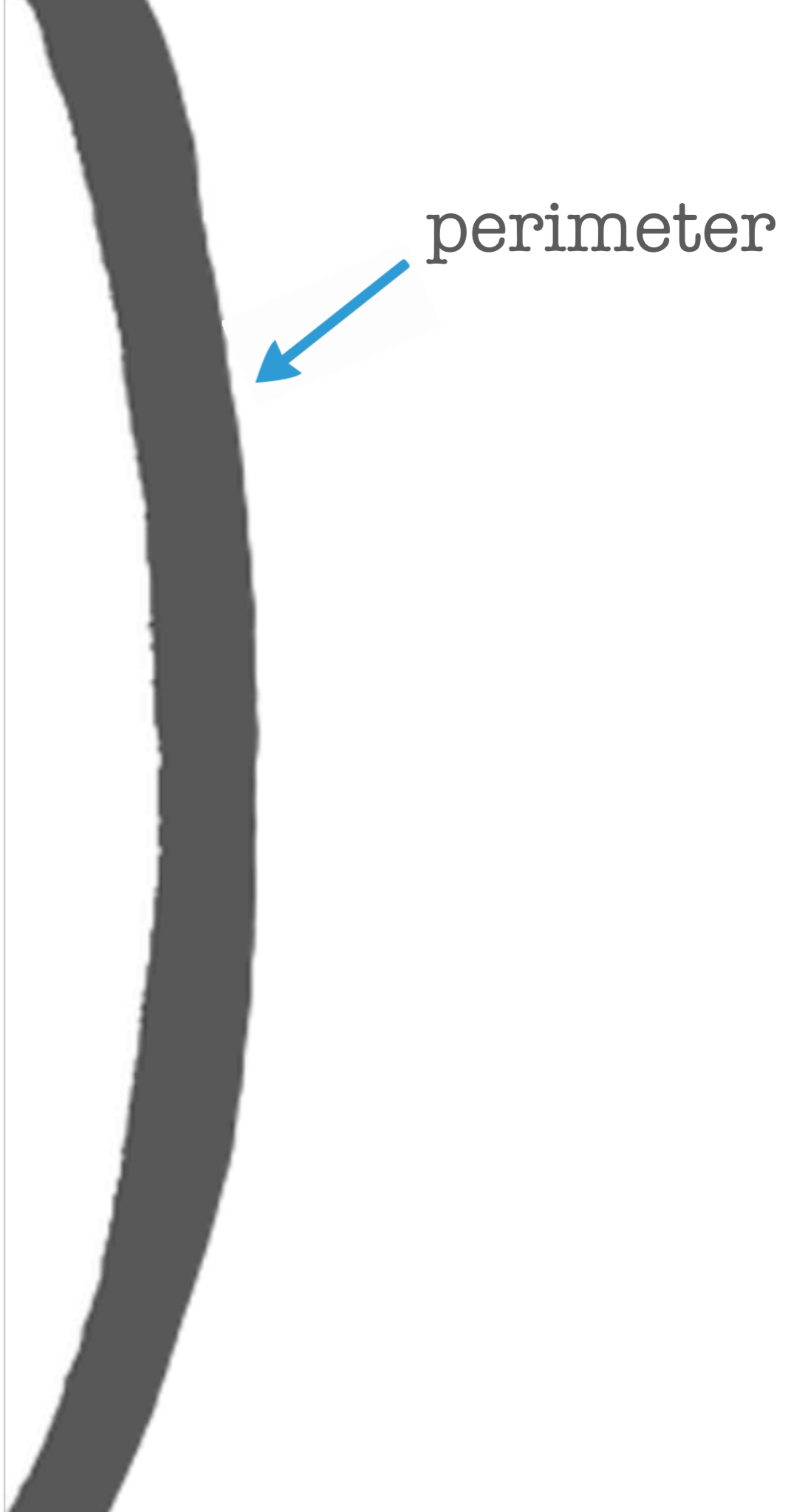
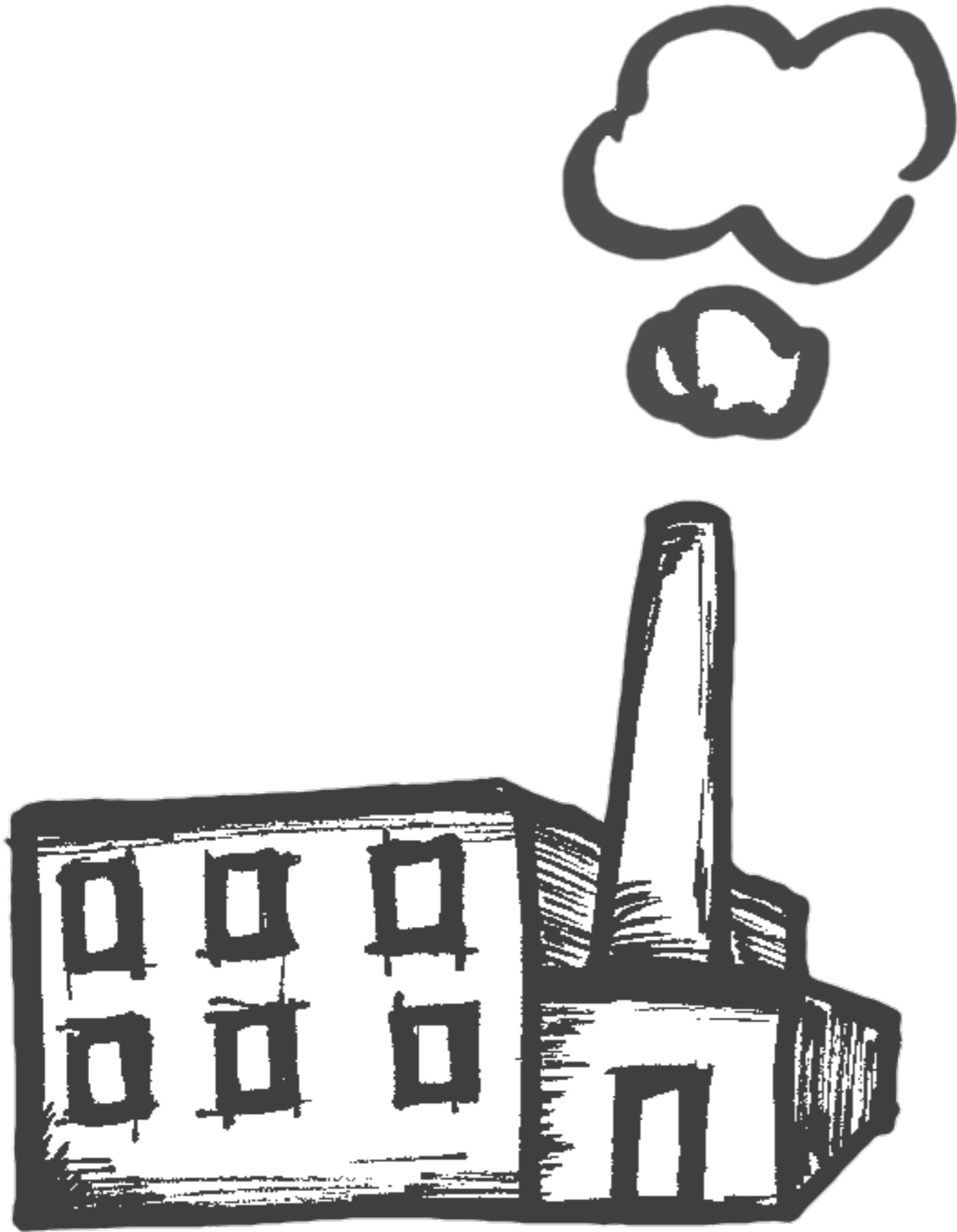
SAML  
IDP



SAML  
Service & OAuth  
Provider AuthZ  
Server



## 2. de-perimeterization



perimeter

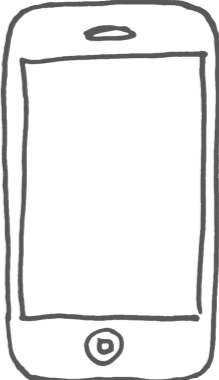
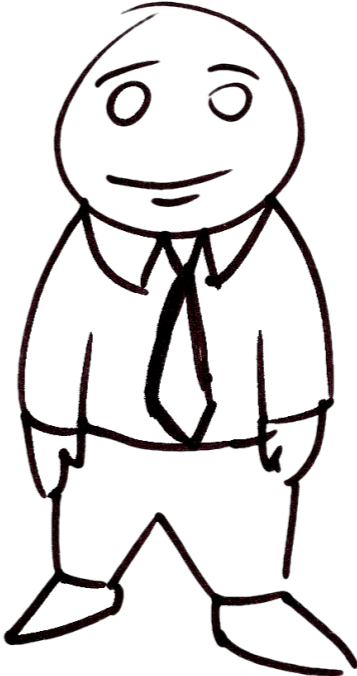


still here?

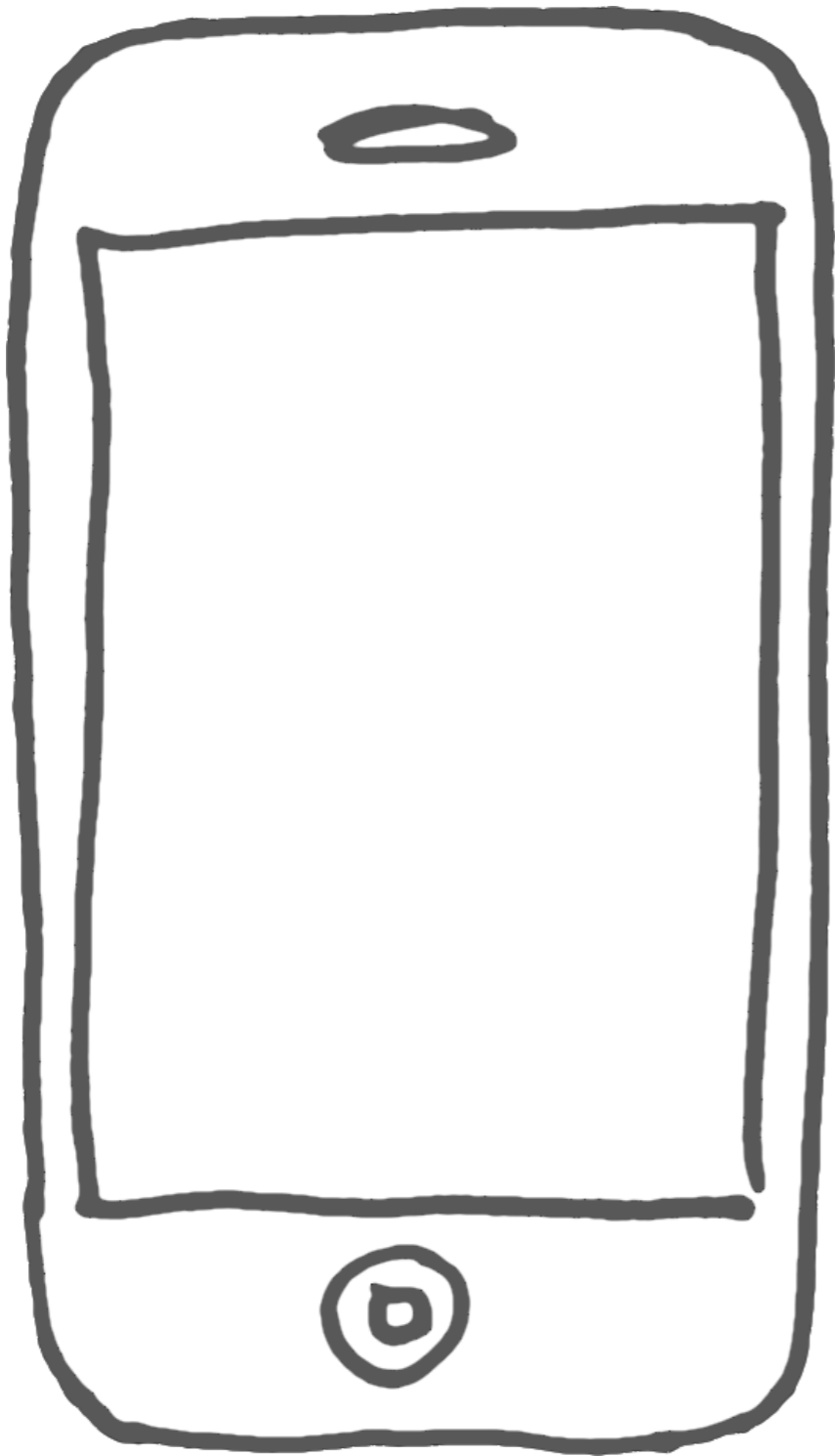




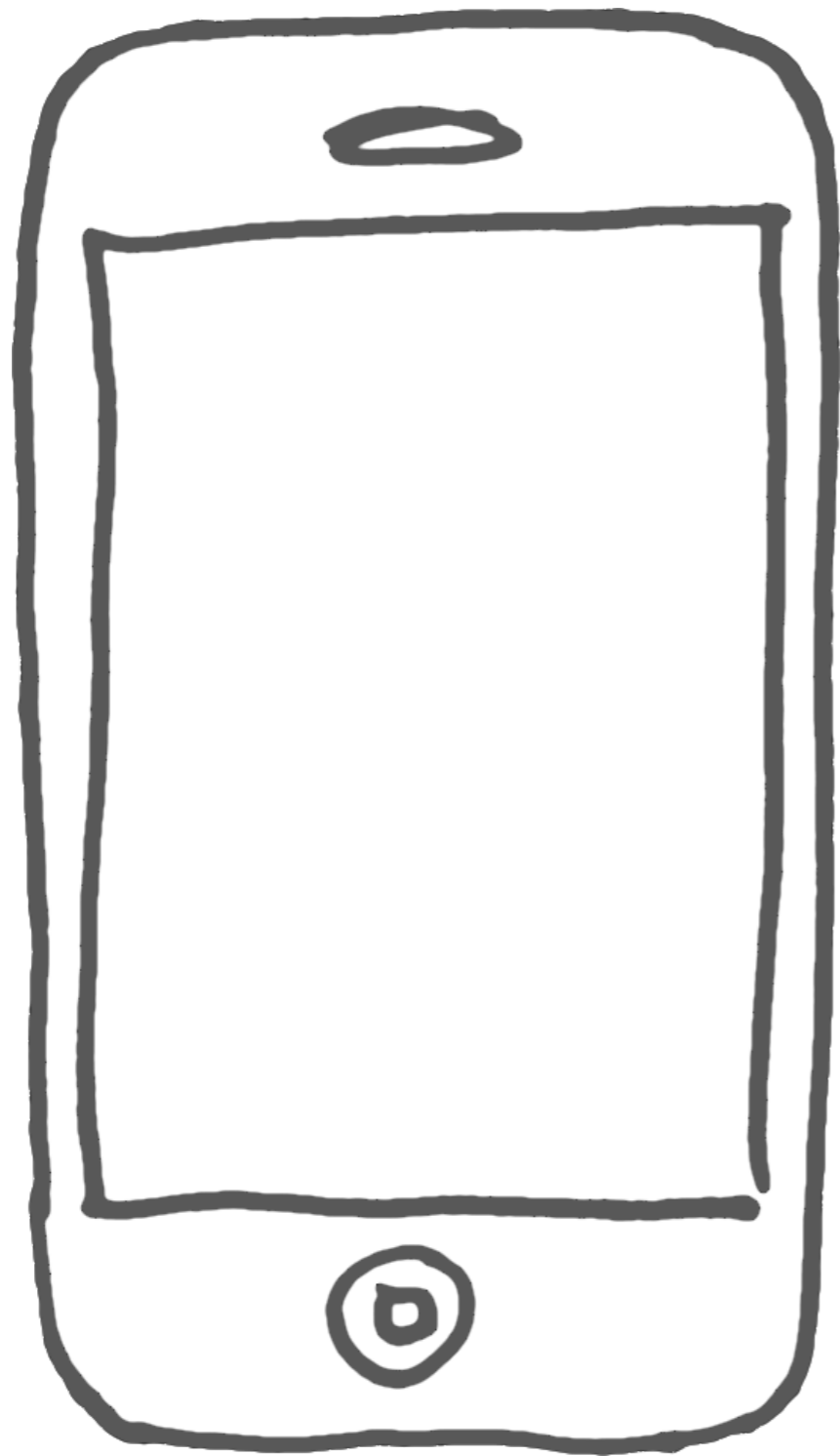
now what?



the perimeter has dissolved



this looks like risk



you can't be sure  
it's your app

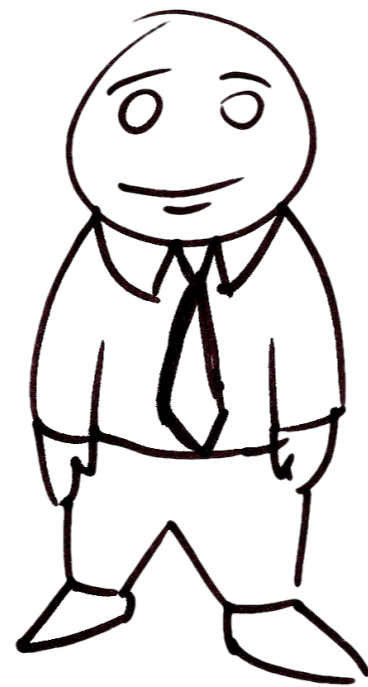
so what are we doing?

identity + context becomes your perimeter

oauth makes the application an actor

## 3. composition

the promise of user-centric



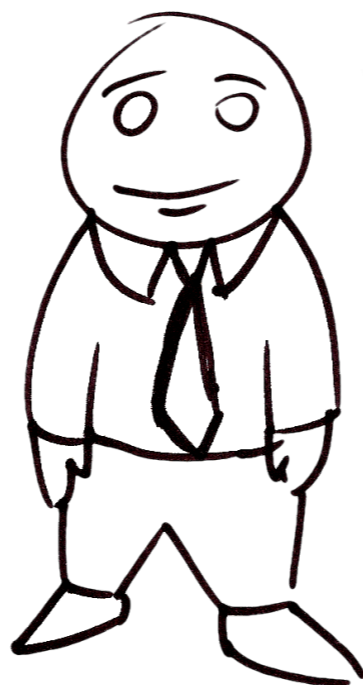
openid  
providers

( claims issuers )



openid  
providers  
( claims issuers )

relying  
parties



what's the reality

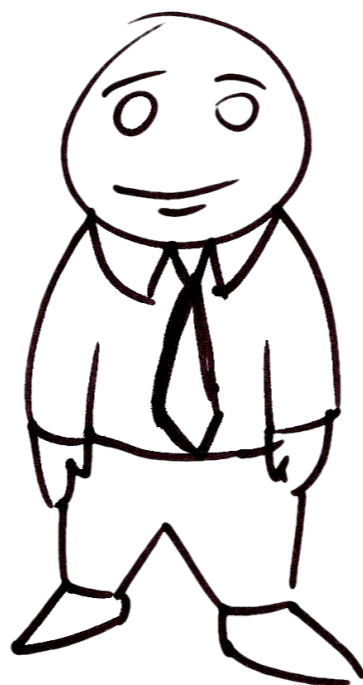
user's don't identify with URLs

consumer trust  $\approx$  brand

rp's economics favor op's of scale

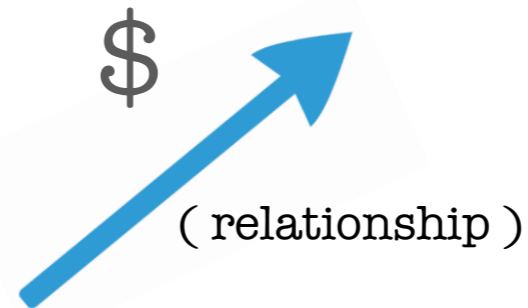
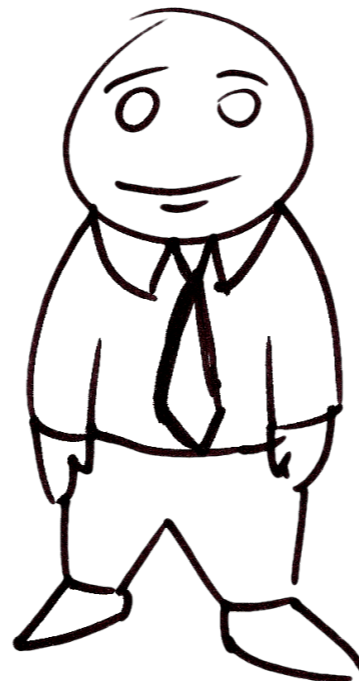
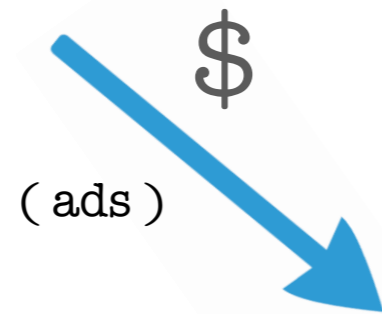
openid  
providers  
( claims issuers )

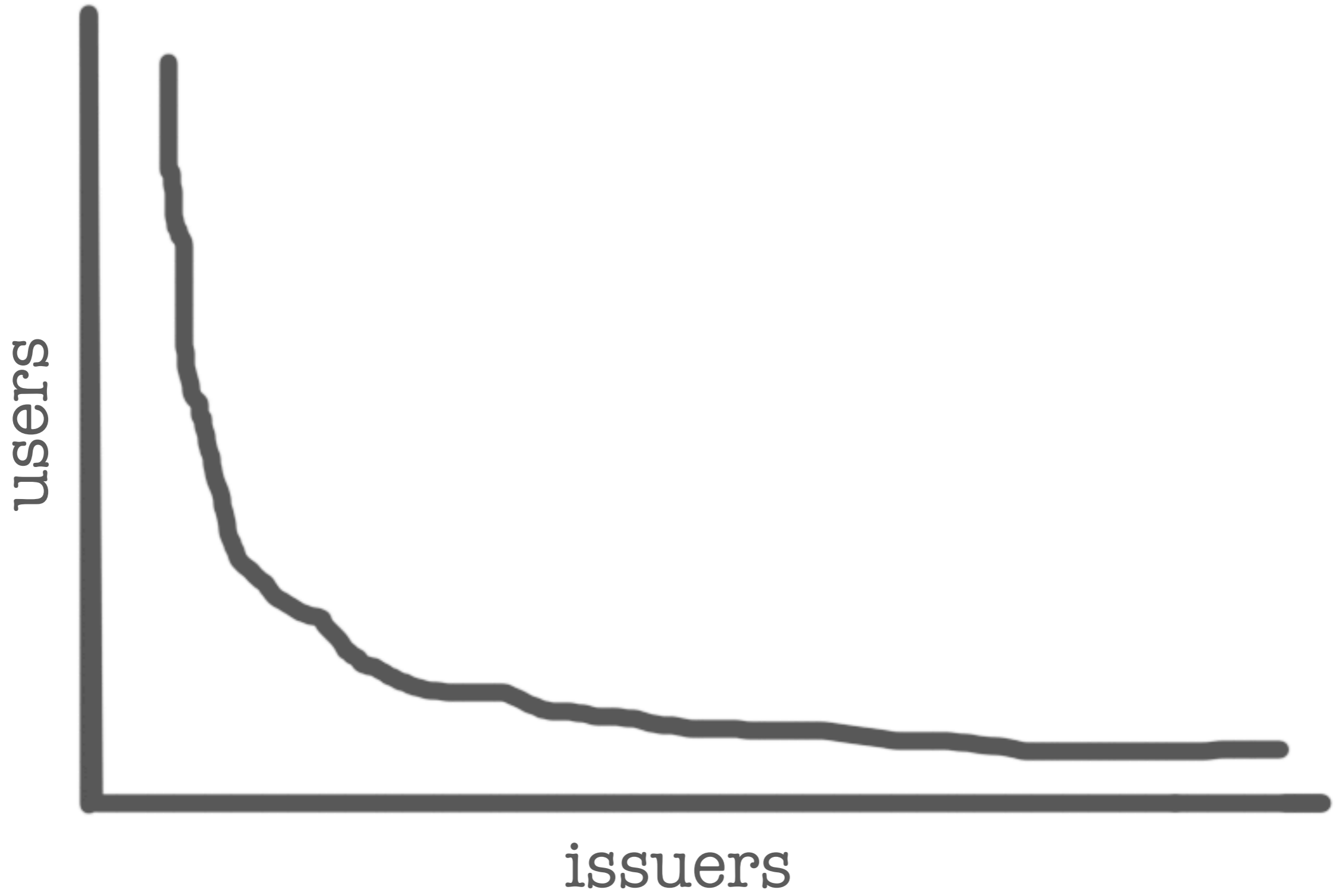
relying  
parties



openid  
providers  
( claims issuers )

relying  
parties



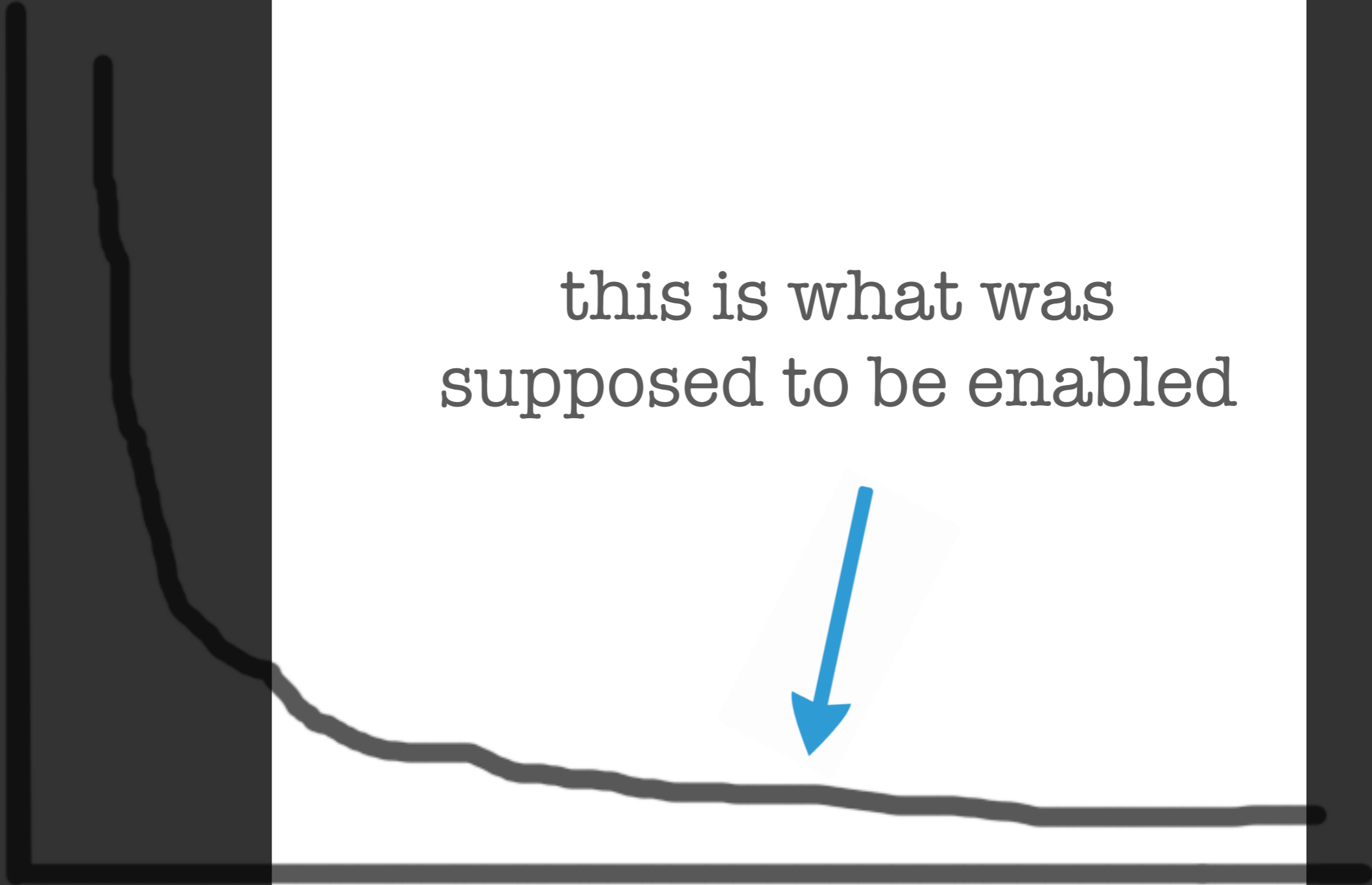


users

this is what was  
supposed to be enabled



issuers



users

..but this is what we got

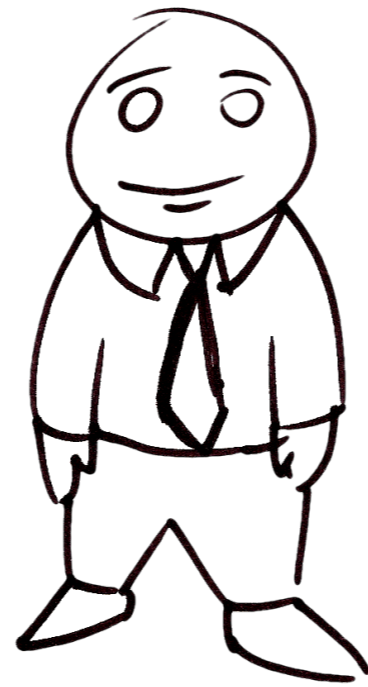
issuers



power is consolidated in a few brands

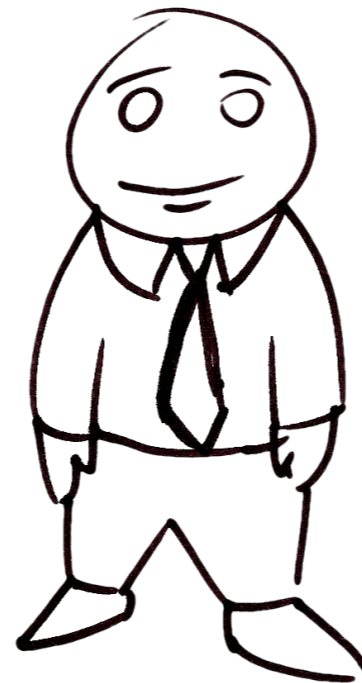
provider-centric

let's look at the enterprise



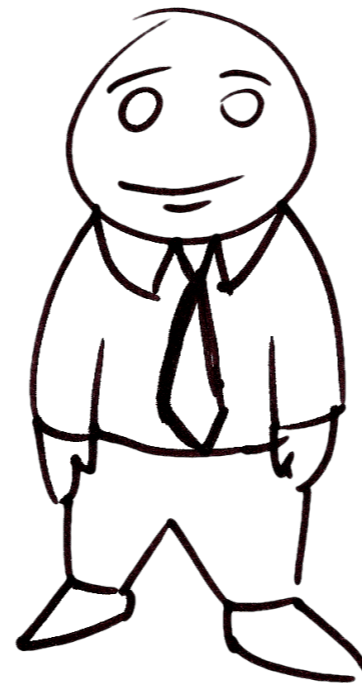
marketing

( few powerful issuers )



marketing

( few powerful issuers )



internal

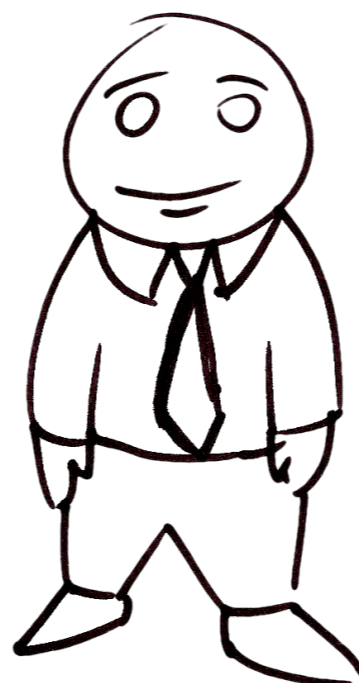
( 1 all powerful issuer )

SAML  
IDP

enterprise



service  
provider

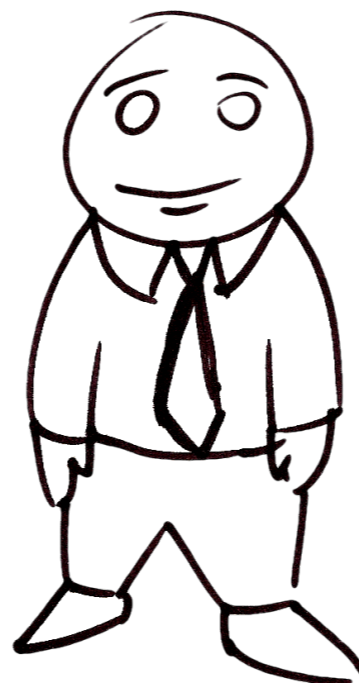


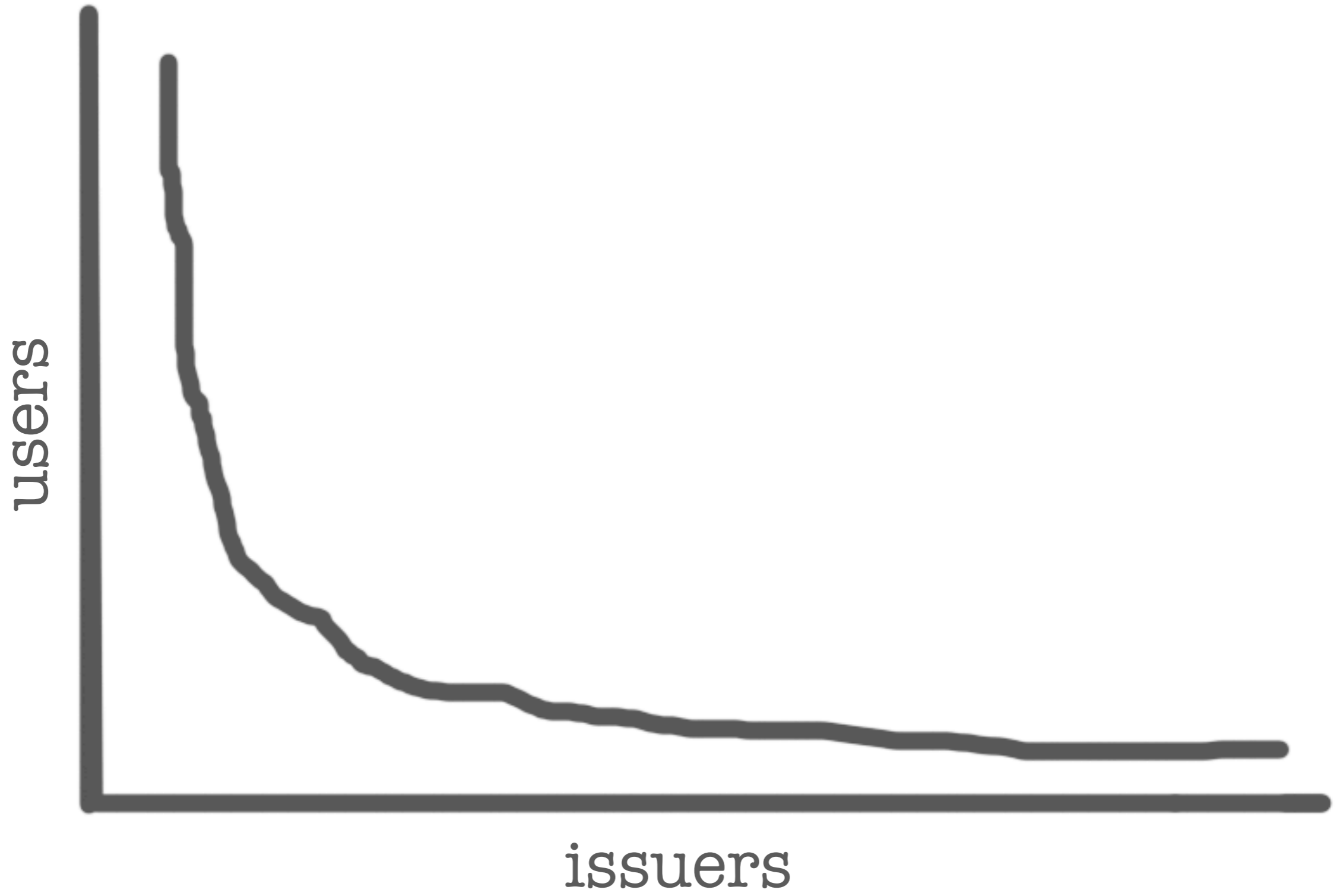
SAML  
IDP

enterprise



service  
provider





users

so while this is what was  
supposed to be enabled



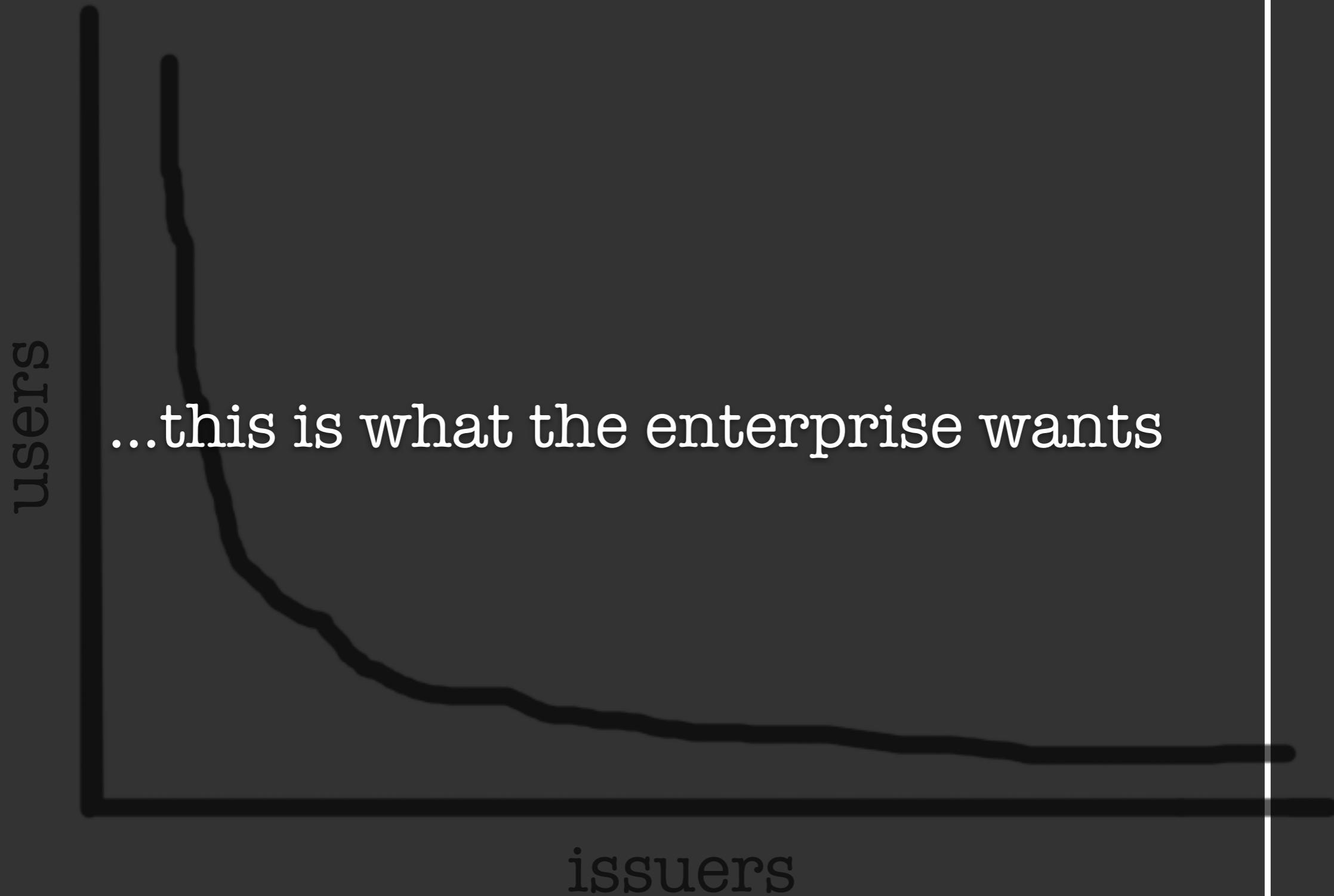
issuers

users



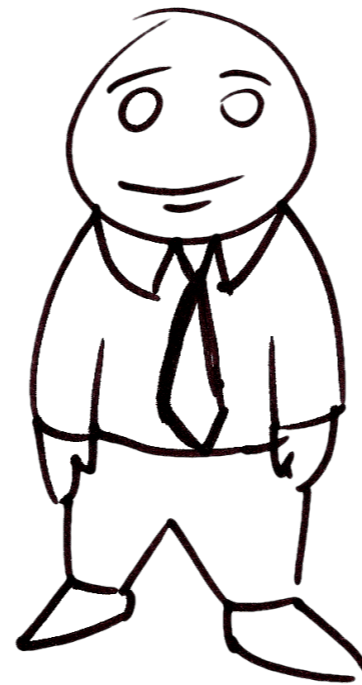
...and this is what we got

issuers



marketing

( few powerful issuers )



internal

( 1 all powerful issuer )

marketing

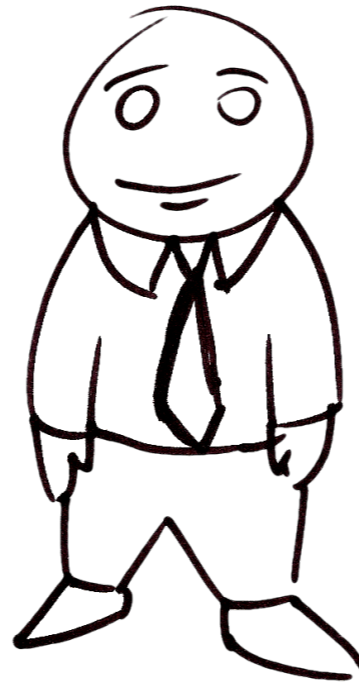
( few powerful issuers )

internal

( 1 all powerful issuer )

partner

( long tail of issuers )

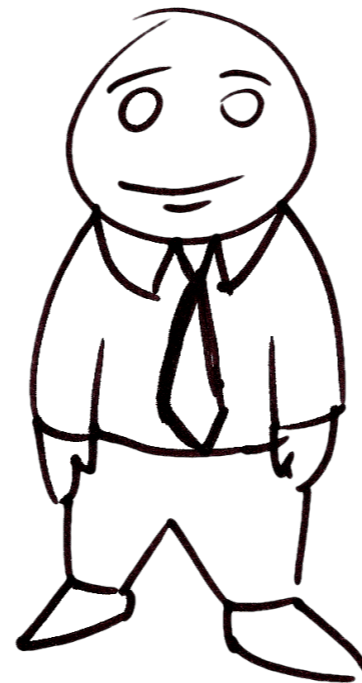


marketing

( few powerful issuers )

internal

( 1 all powerful issuer )



partner

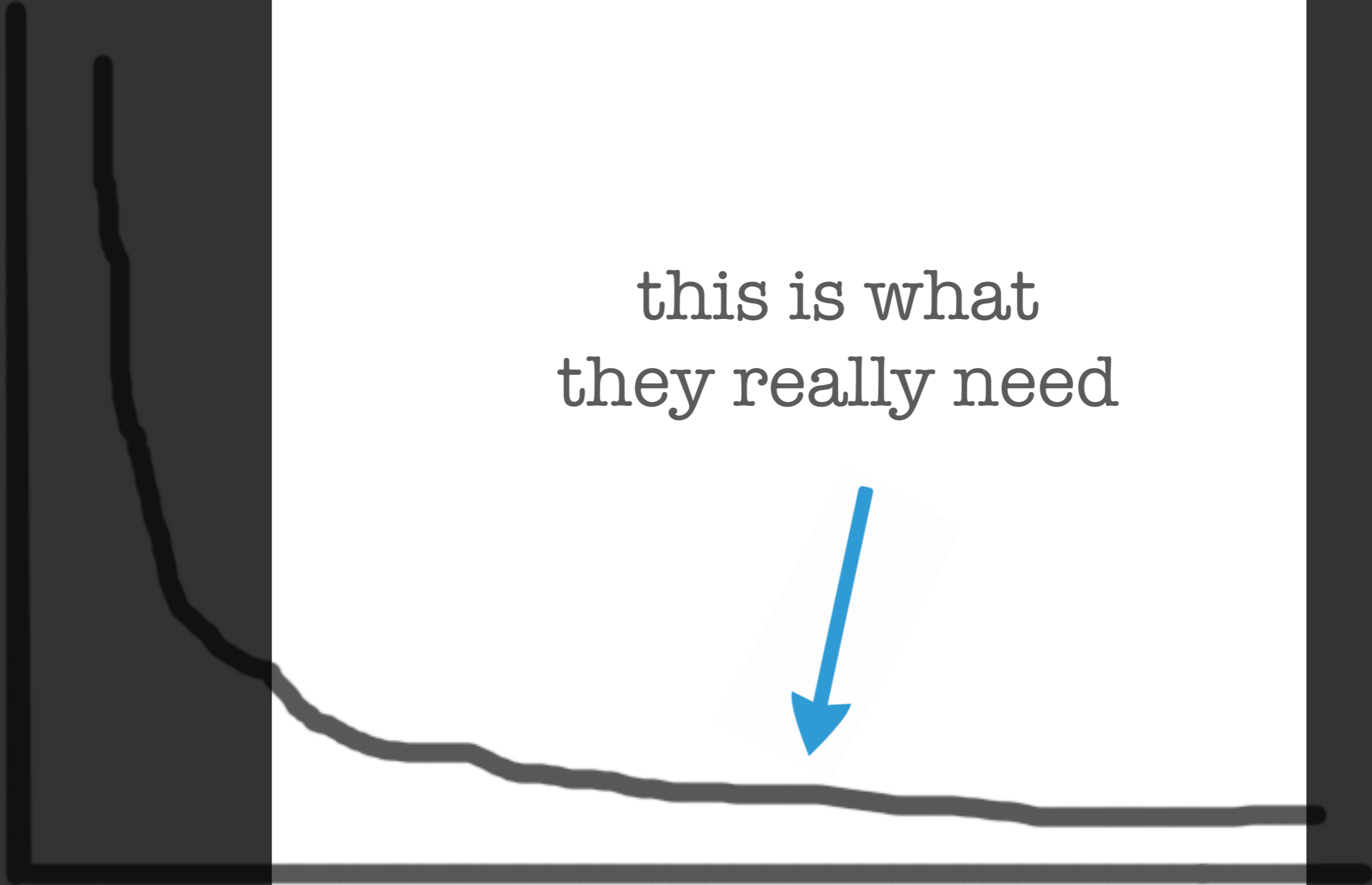
( long tail of issuers )

customer

( long tail of issuers )

we've been conflating issuers with idps

users



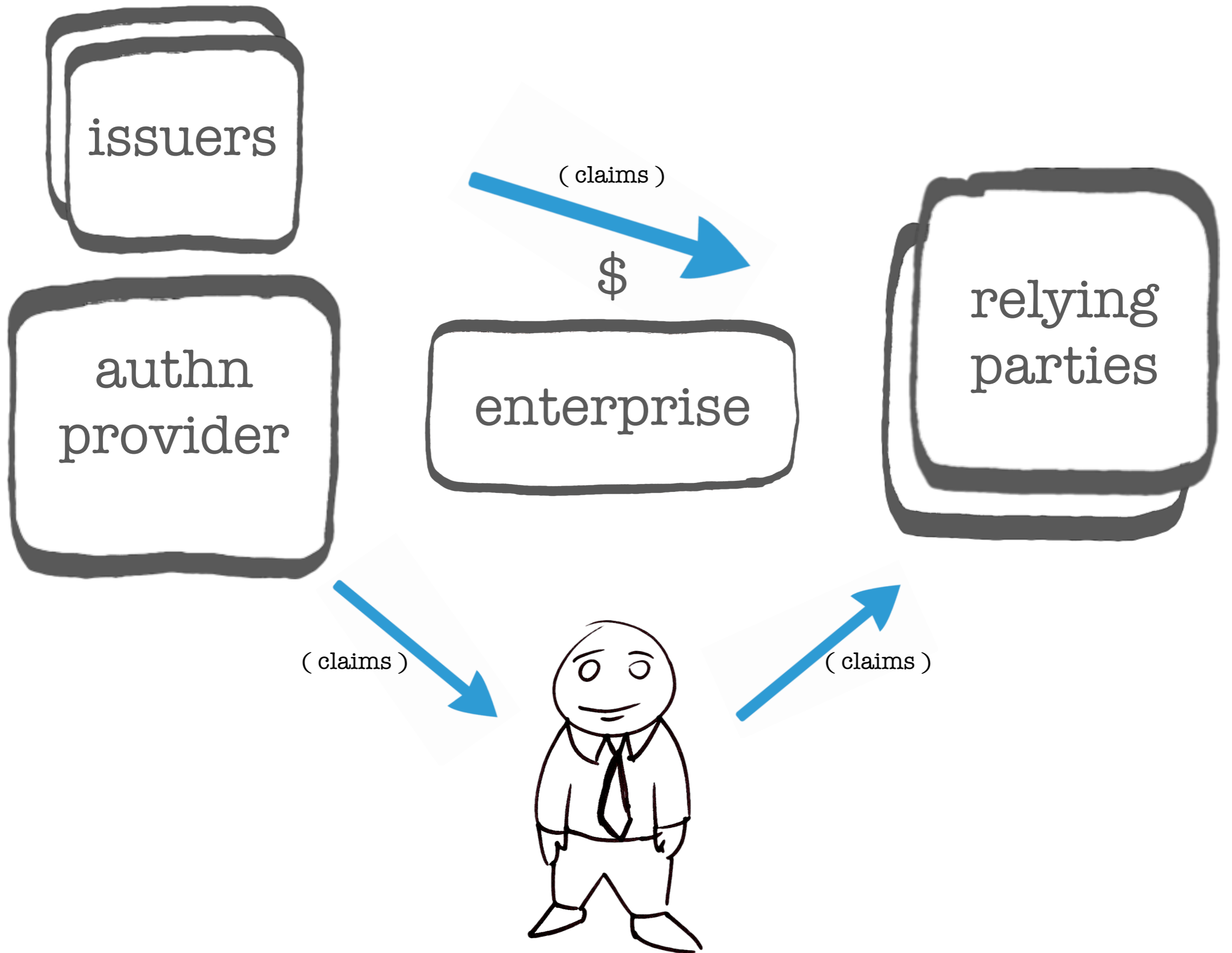
this is what  
they really need

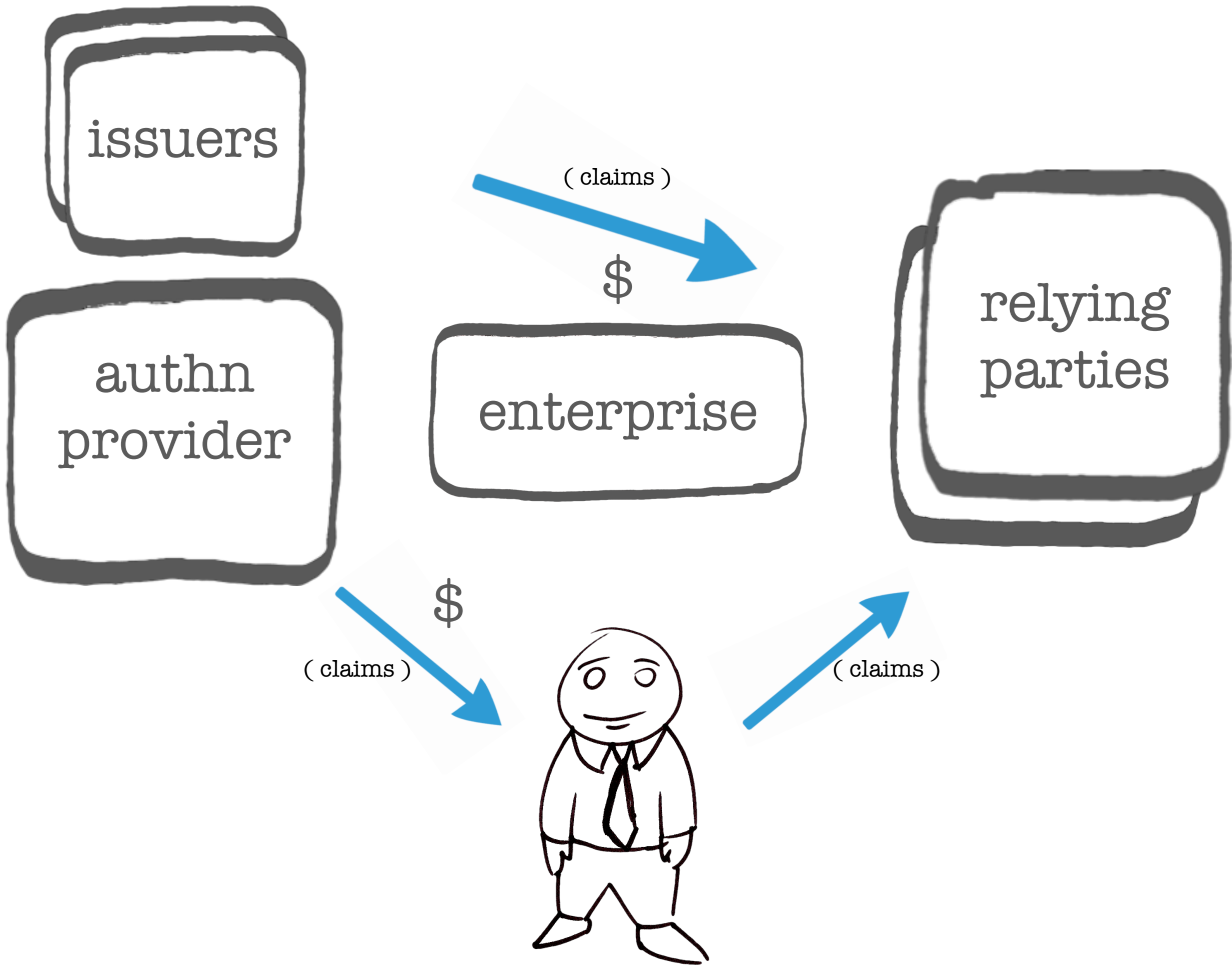
issuers

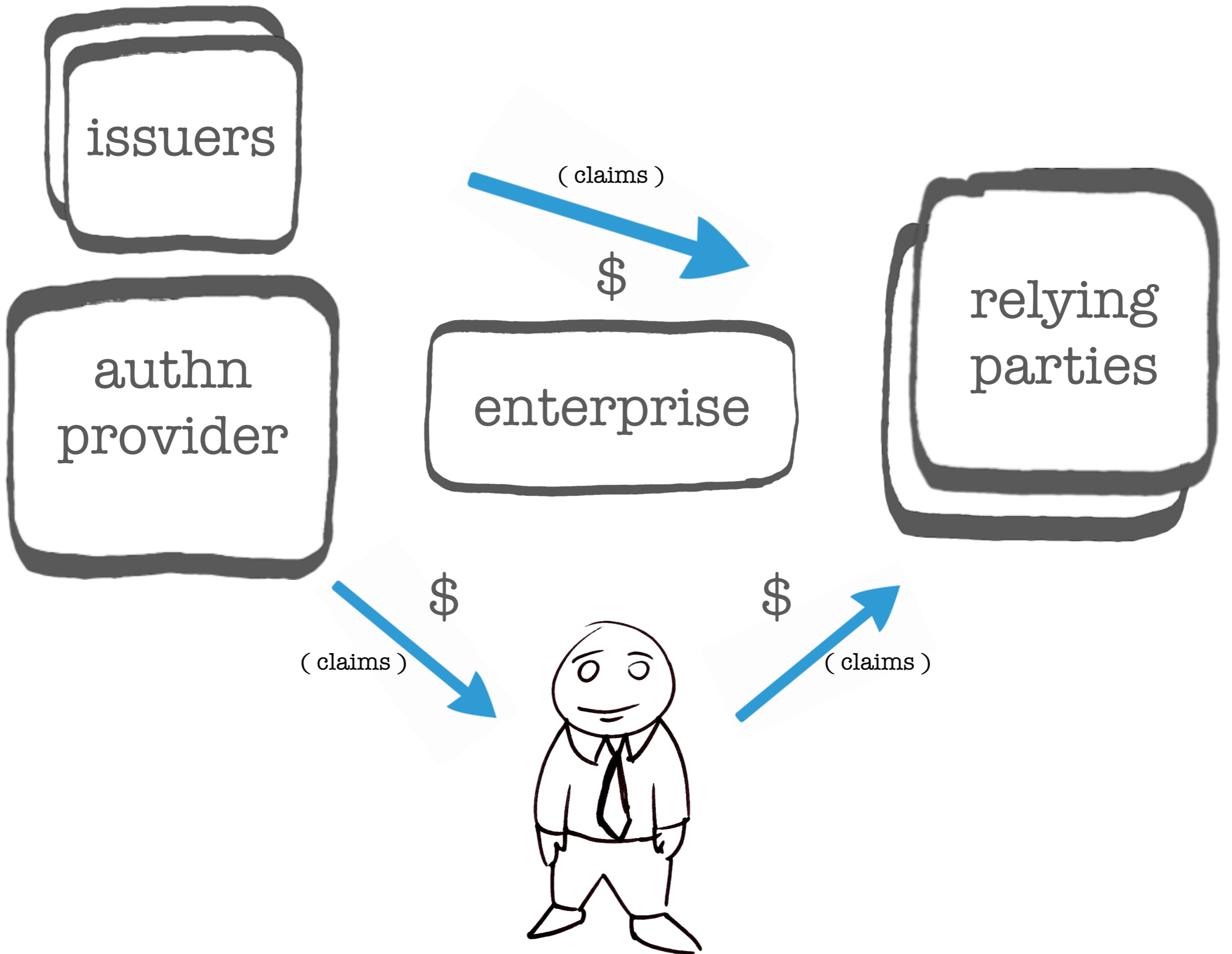
claims-centric

so what are we doing?

openid connect







multi-cloud



so what are we doing?

SCIM: Simple Cloud Identity Management

simple, extensible schema

# RESTful API

so why might this work?

paving cow paths

architecturally aligned with providers

the economics are different

the politics are different

[www.simplecloud.info](http://www.simplecloud.info)

@cmort