
DDD & ReBAC:
Revolutionizing Access Management with a Business-Centric Approach

Is access management a bounded context?

AGICAP

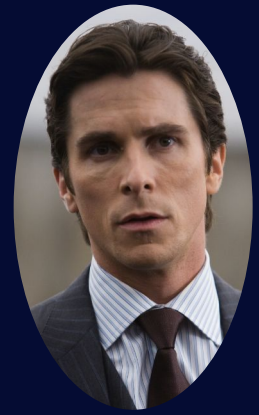
Pauline Jamin
Staff engineer @Agicap
Grenoble 🏔️
Sweet tooth

AGICAP

The members

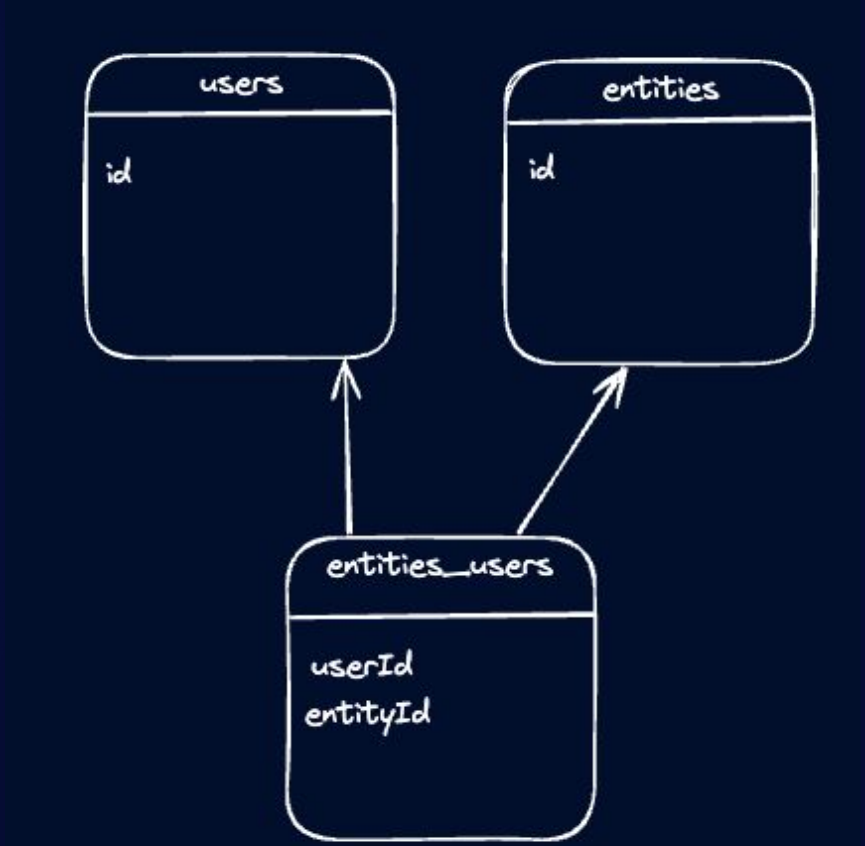
A user has **access** to an **entity** if he/she/they is/are a **member** of the entity

User *Bruce has access to* ***entity*** *WayneCorp because he is a* ***member***



AGICAP

The members



AGICAP

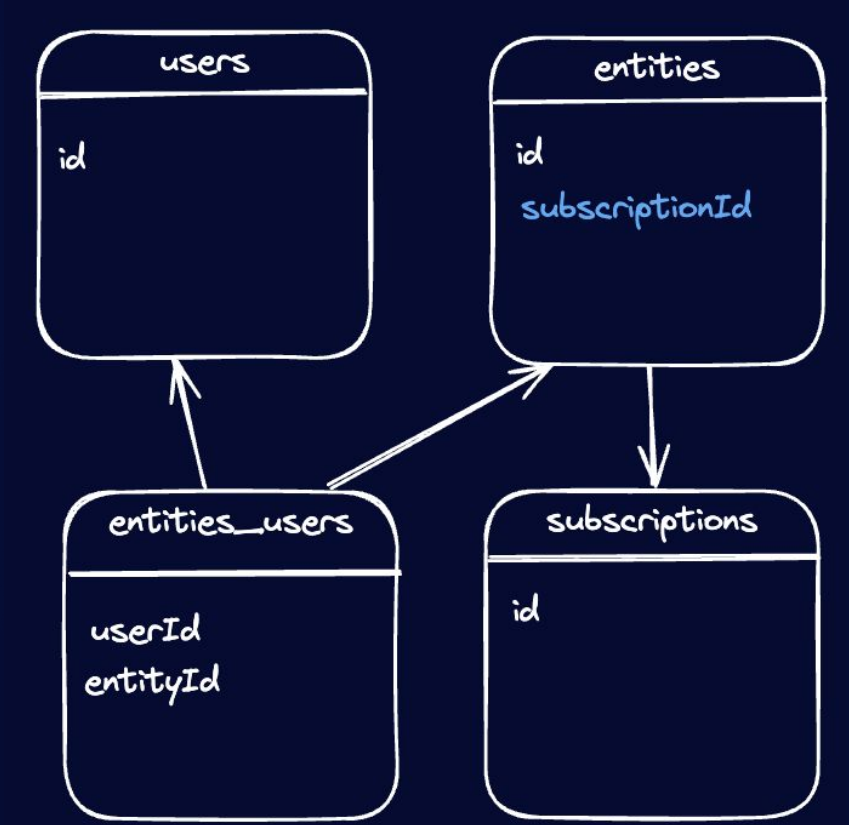
The Agicap's staff

A **staff** can access users' entities if there is no **subscription**

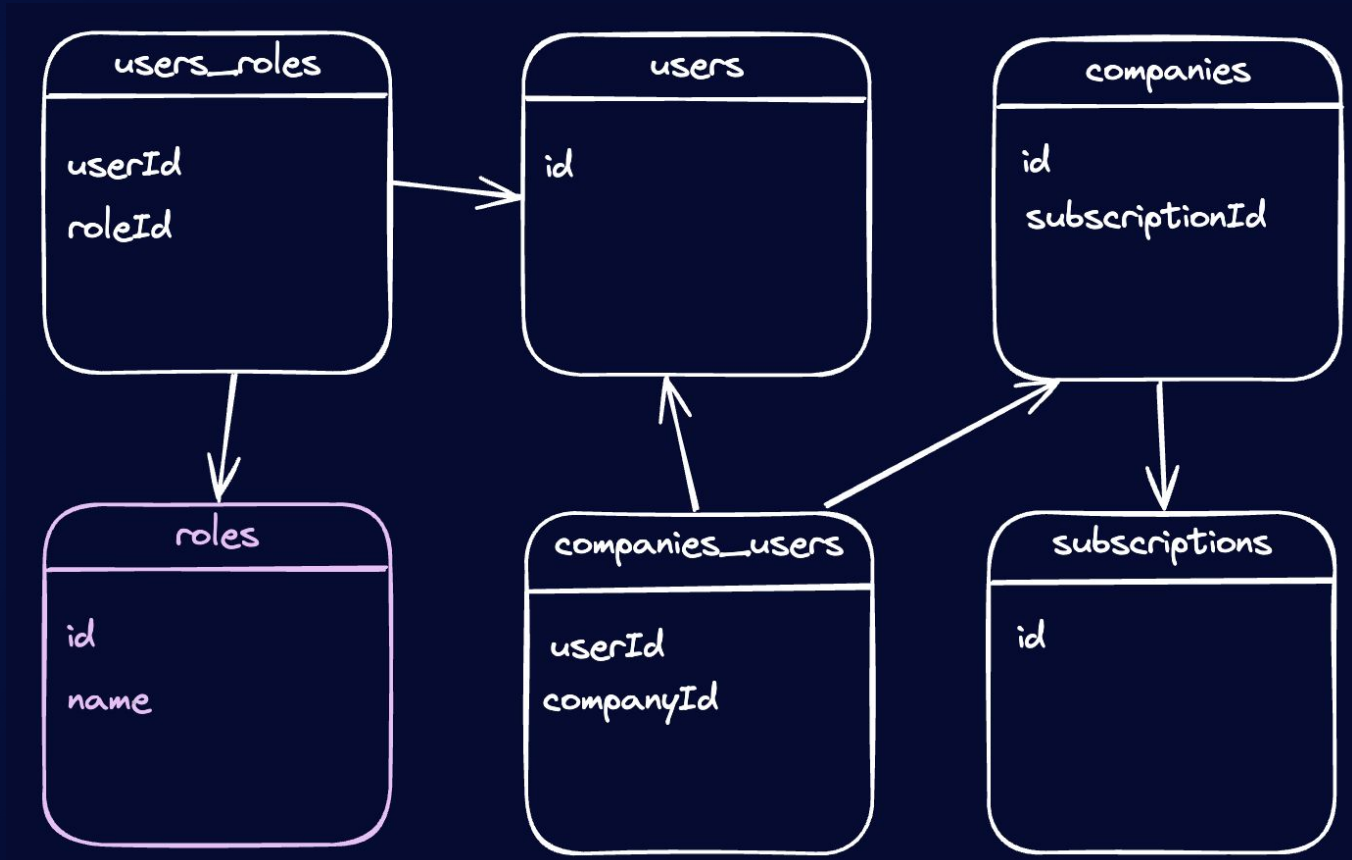
Staff *Gordon has access to* ***entity*** *WayneCorp because it has* ***no subscription***

AGICAP

The Agicap's staff



The Agicap's staff



AGICAP

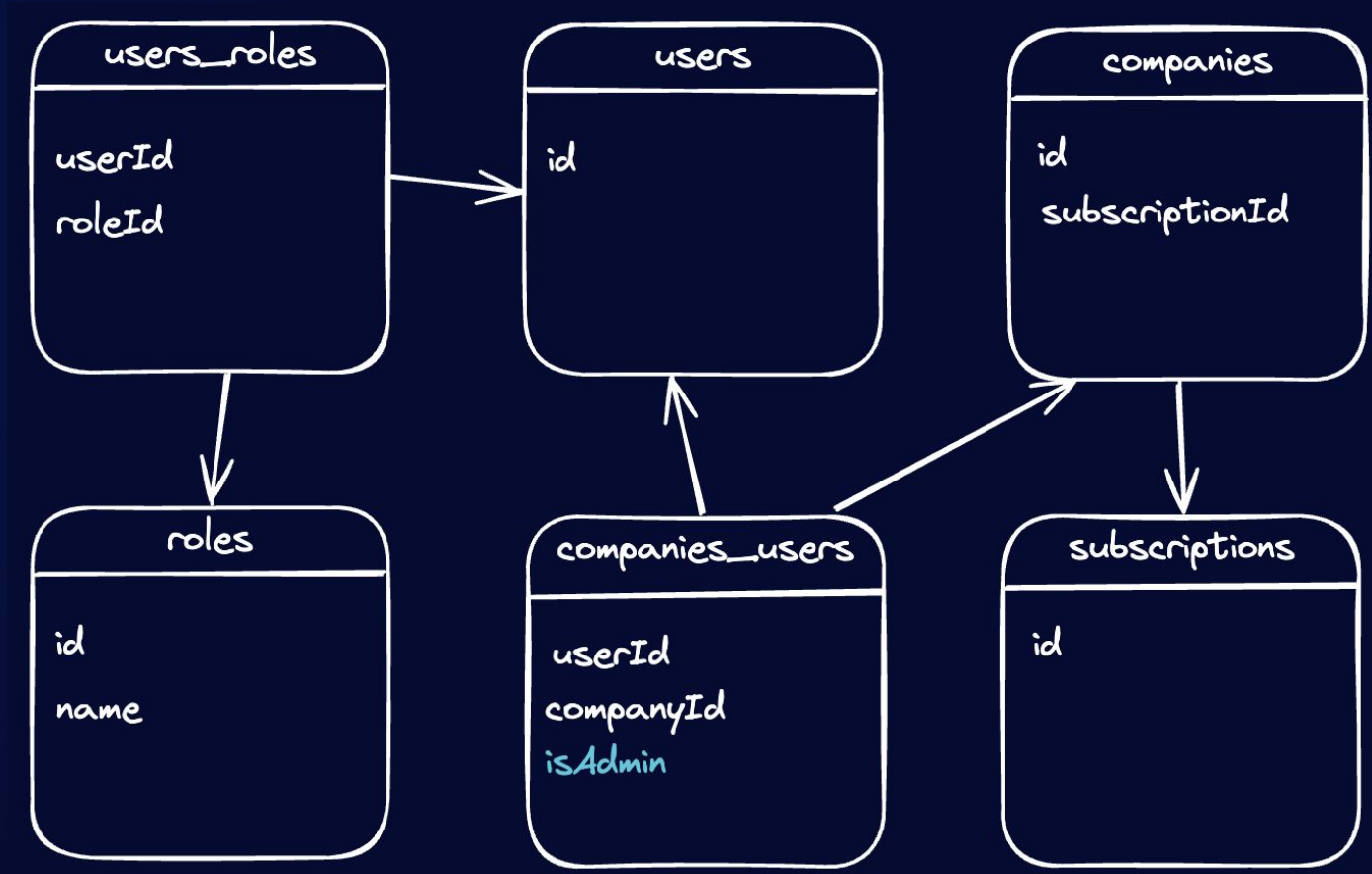
By the way

A staff can access users' entities if there is a subscription but was given access by the **administrator** of the entity

Staff *Gordon has access to* ***entity*** *WayneCorp because he was given* ***an access*** *by WayneCorp* ***administrator****: Lucius*

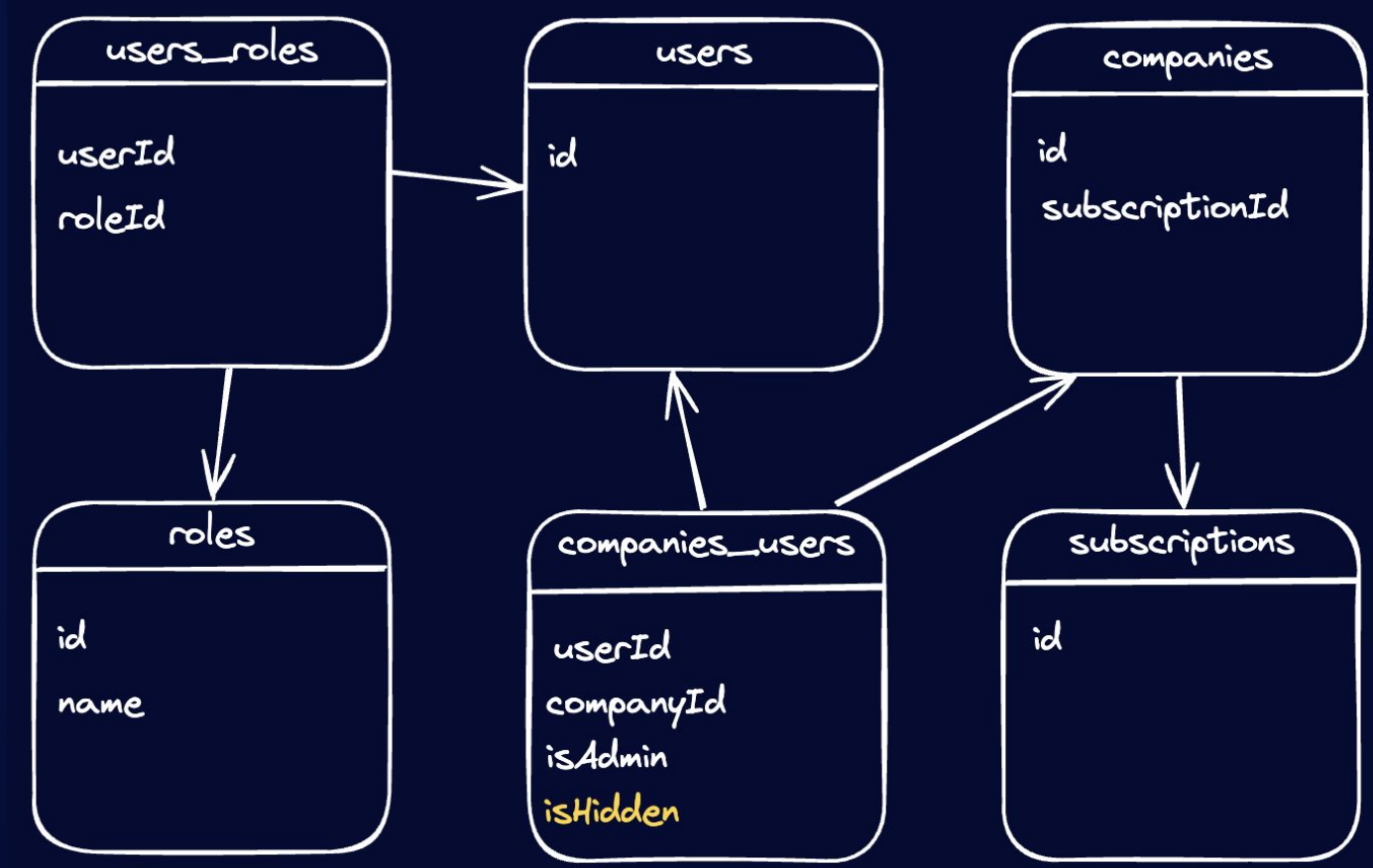
AGICAP

The administrator



AGICAP

IsHidden



AGICAP

Entity access

Can user Batman access entity WayneCorp?

- Is user Batman a member not **hidden** of the entity WayneCorp?
- Does user Batman have **role** staff and the entity has no subscription (i.e in demo mode)?
- Does user Batma have **role** staff and is an **hidden** member of WayneCorp entity?

The use case

Admins or staff can see payments

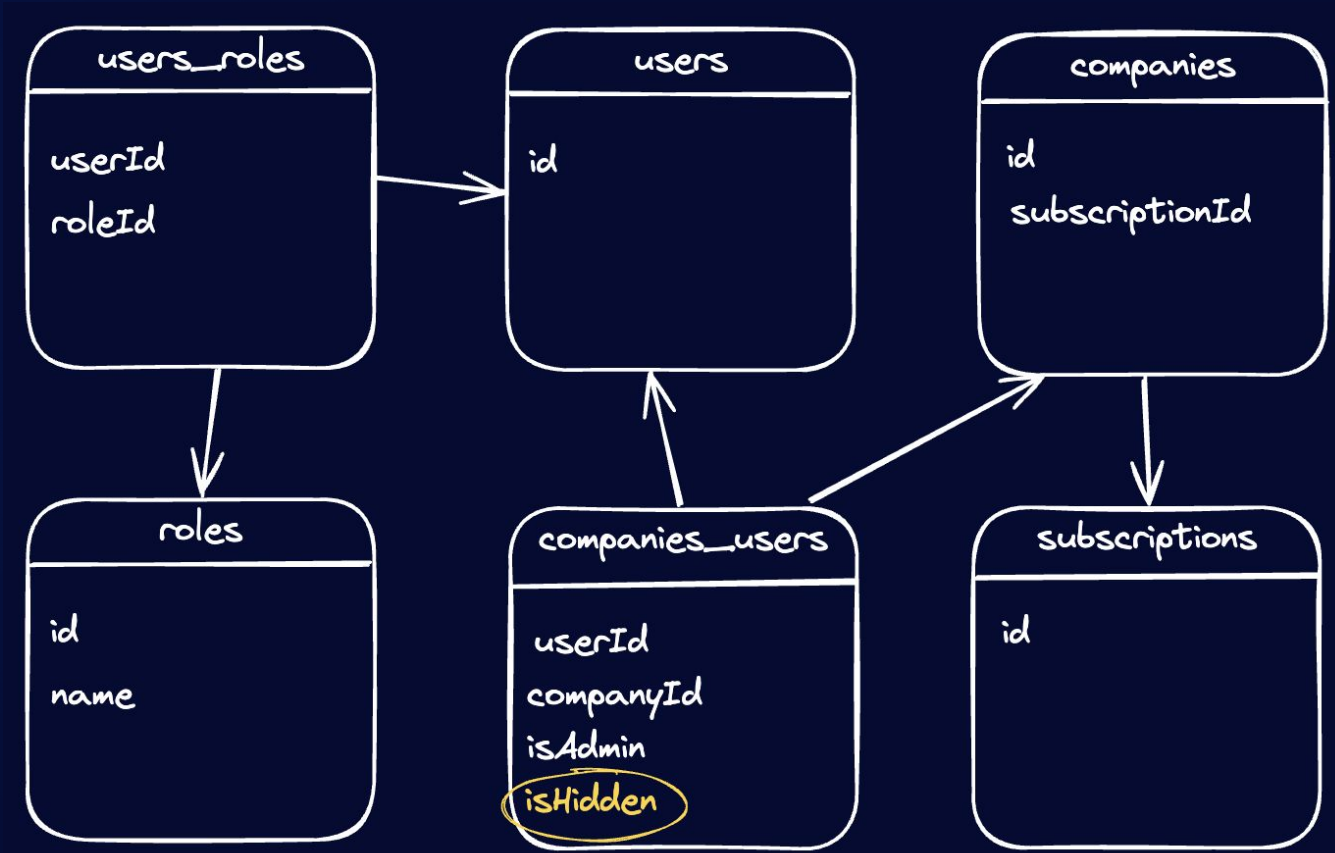
BUT

Only admins can approve payments

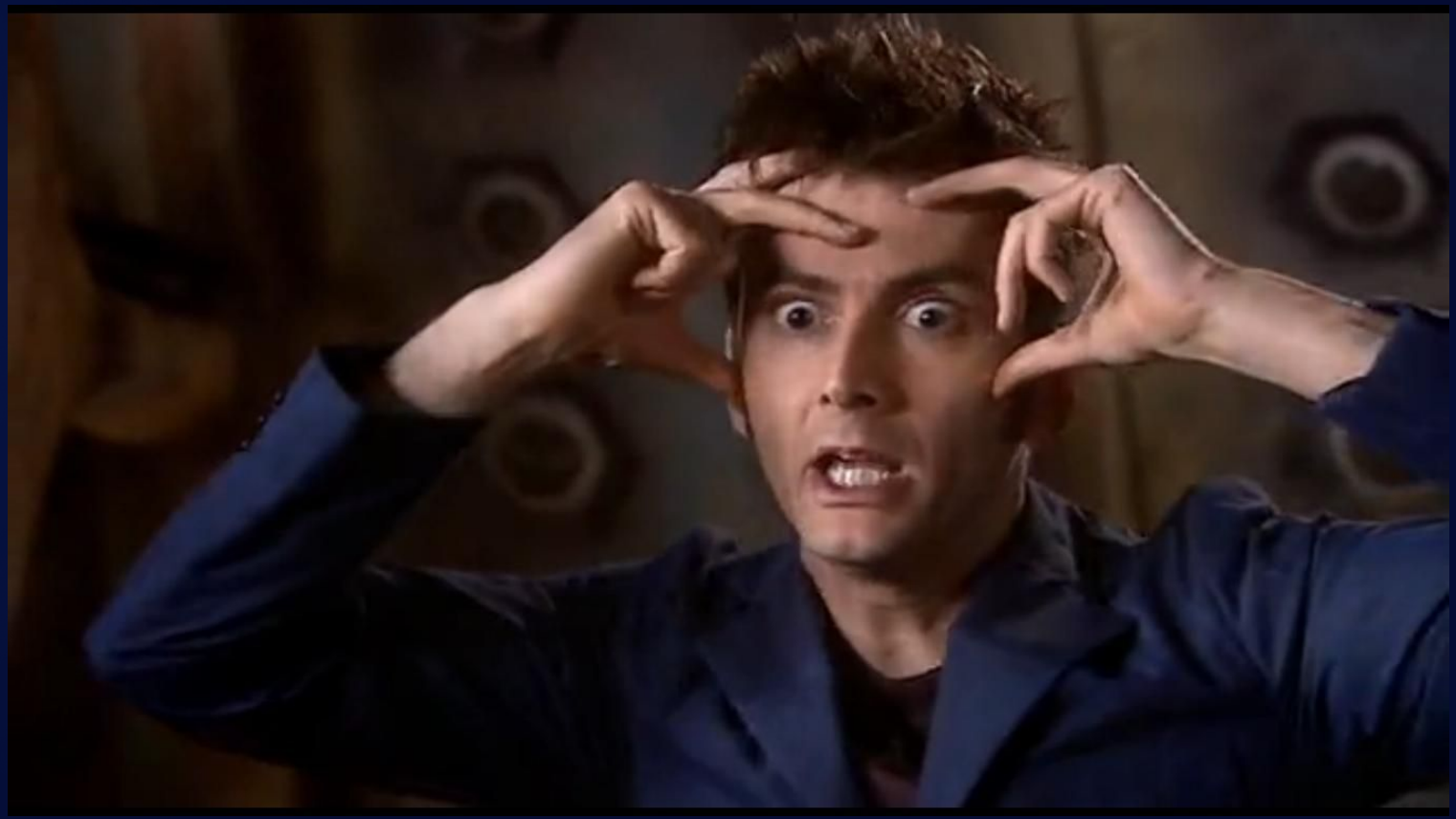
Only Lucius can approve payments

AGICAP

Model the world with booleans?



Sweet madness



AGICAP

Sweet madness

AGICAP

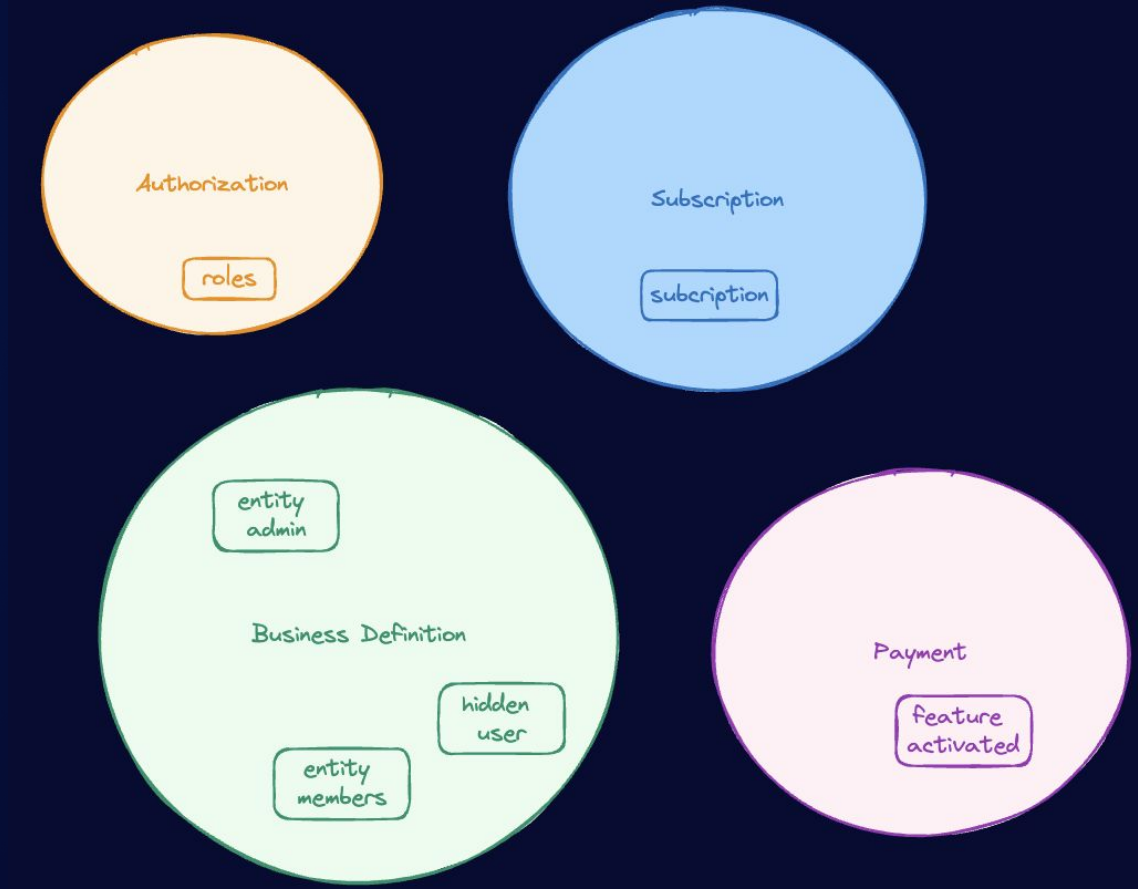
The ACL administrator trap

AGICAP

Is access management a bounded context?

AGICAP

Bounded contexts

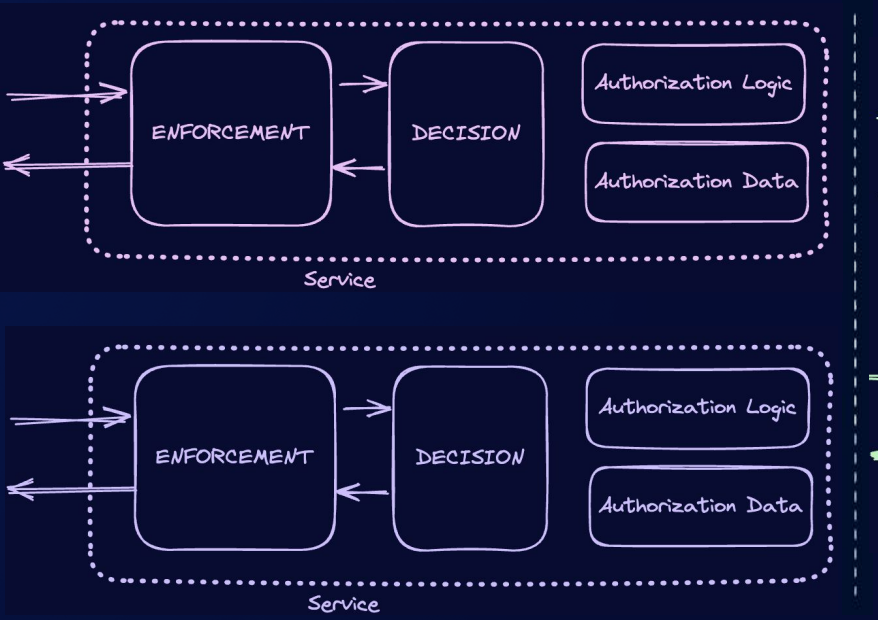


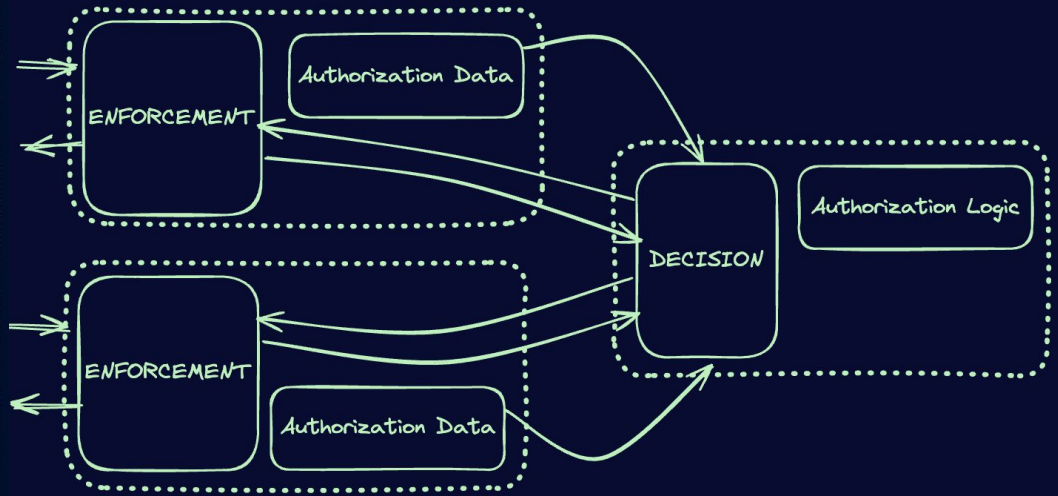
Where the authorization logic should be?

Business data & access management data

AGICAP

Decentralized vs Centralized





AGICAP

Centralized service

AGICAP


GOOGLE ZANZIBAR

Relationship-Based Access Control - ReBAC

AGICAP

Relationship-Based Access Control - ReBAC

Access Control Requirements for Web 2.0 Security and Privacy

Dr. Carrie E. Gates
CA Labs, CA, Islandia, NY 11749
carrie.gates@ca.com

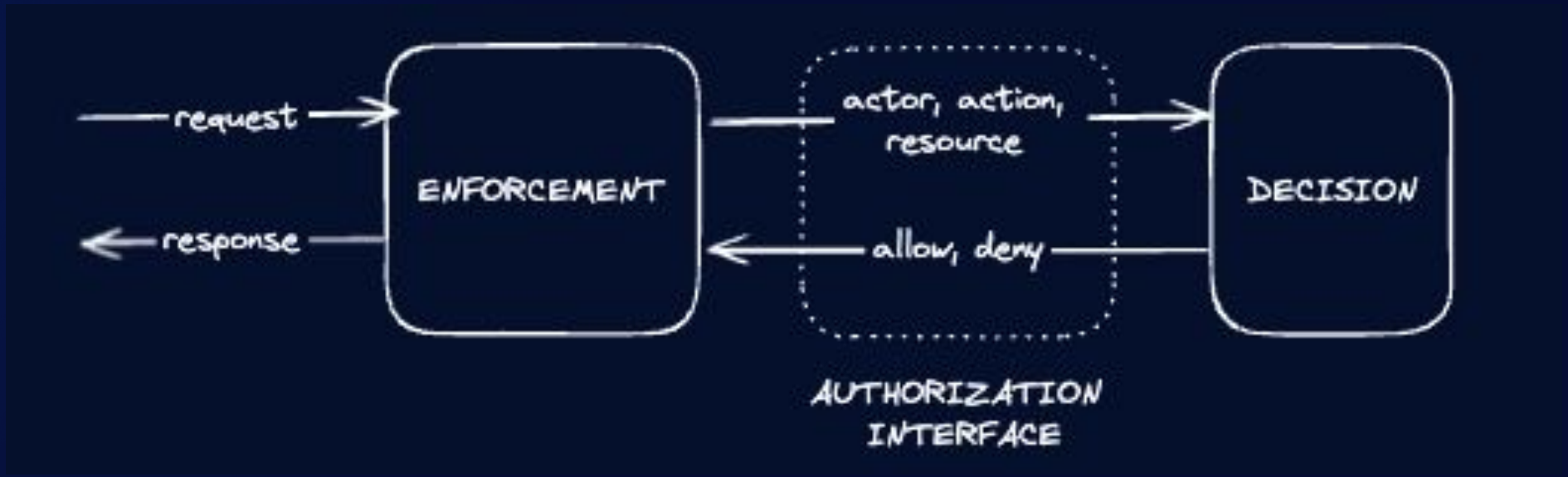
AGICAP

Zanzibar syntax

```
<tuple> ::= <object>'#'<relation>'@'<user>
<object> ::= <namespace>':'<object_id>
<user> ::= <namespace>':'<user_id> | <userset>
<userset> ::= <object>'#'<relation>
```

entity:WayneCorp#member@user:Bruce
team:engineers#member@user:Lucius
entity:WayneCorp#admin@team:engineers#member

Authorization Interface



Is user:x related to object:y with relation z?

Who?

What?

To what?

Example: is user:Lucius related to entity:WayneCorp with relation administrator?

AGICAP

Google Zanzibar

Concepts

Centralized authorization system

Highly scalable

Create, save and evaluate permissions

Services

Youtube
Gmail
Google drive
Calendar
Maps
Photos
etc

Data

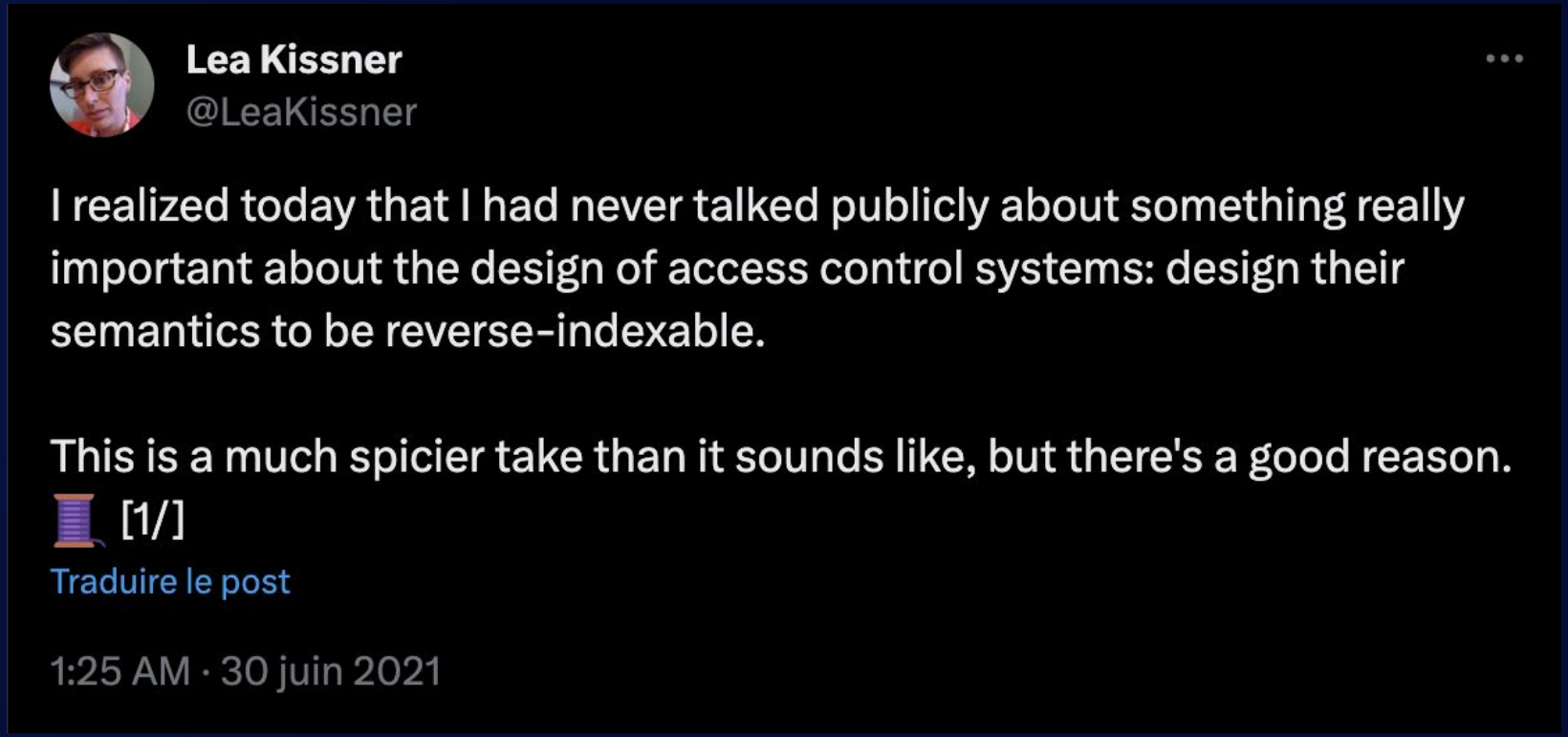
95% <10ms response time

Millions of millions of ACL

+ 99,9999% disponibility

Millions of authorizations evaluated by second

Reverse index



Lea Kissner
@LeaKissner

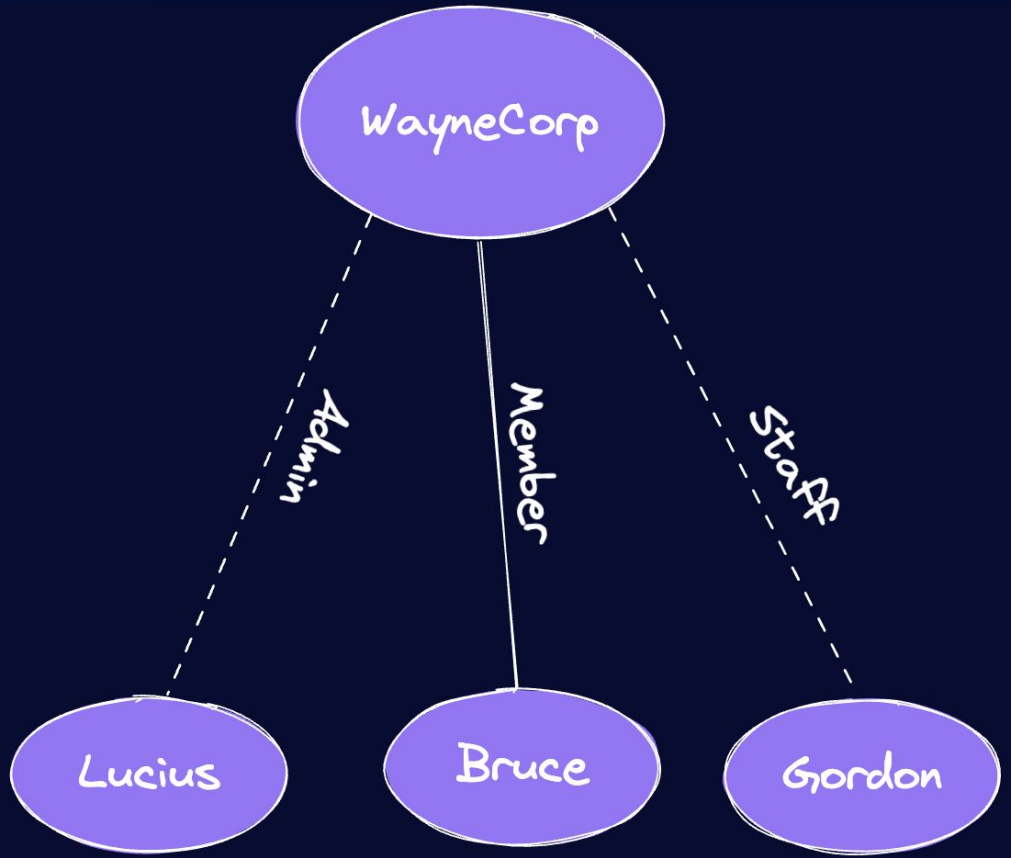
I realized today that I had never talked publicly about something really important about the design of access control systems: design their semantics to be reverse-indexable.

This is a much spicier take than it sounds like, but there's a good reason. 🧵 [1/]

Traduire le post

1:25 AM · 30 juin 2021

Reverse index

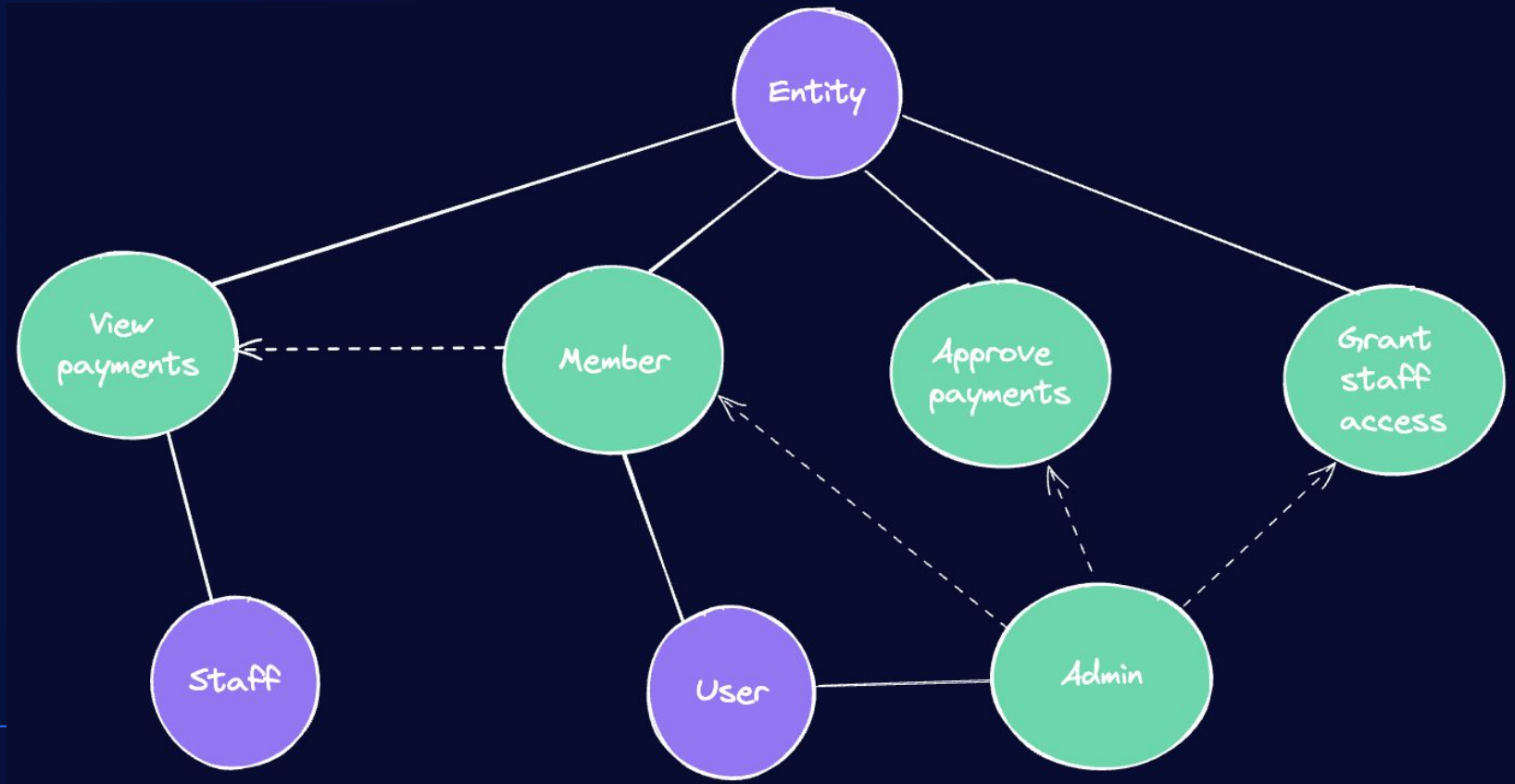


OpenFGA

- Open source
- Fine grained
- User friendly API
- Simple and readable model

AGICAP

Demo time



AGICAP

Key takeaways

- Authorization rules are business rules
- Access management is a bounded context on its own
- ReBAC is cool like Ryan: we can use our ubiquitous language

Why “Zanzibar”?

AGICAP

THANK YOU!

https://github.com/paulinejamin/dddeurope2024

AGICAP

Ressources

https://zanzibar.academy/#!
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/10683a8987dbf0c6d4edcafb9b4f05cc9de5974a.pdf
https://openfga.dev/
https://authorizationinsoftware.auth0.com/public/49/Authorization-in-Software-f9b69587/7889bb9c
https://www.aserto.com/blog/google-zanzibar-drive-rebac-authorization-model
https://www.osohq.com/post/zanzibar

France - Deutschland - España - Italia - UK & Ireland