CATs

[CryptoAuthTokens]

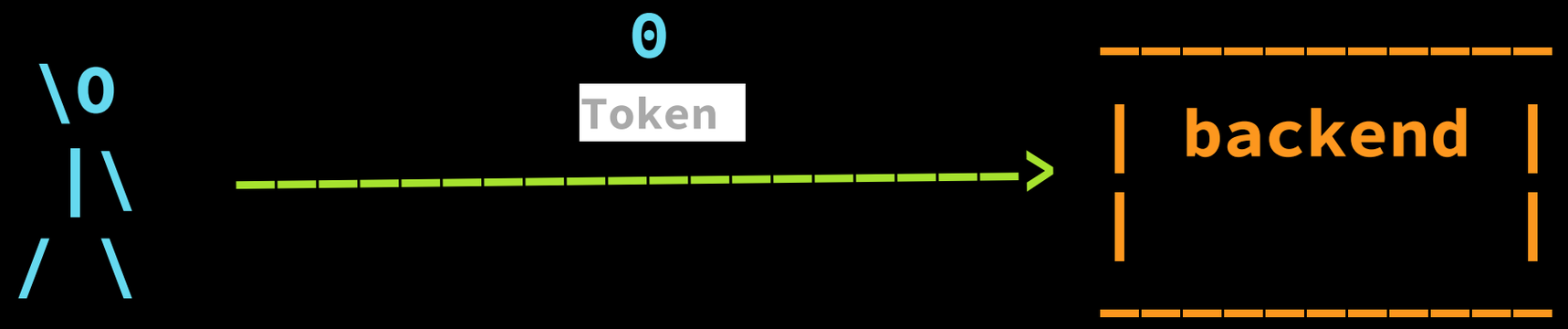
A Tale of Scalable Authentication

Yueting Lee, Kevin Lewi, Haozhi Xiong, Ben Yang

Overview

- Token Authentication
- Authentication models
- Pre-CAT World
- Infrastructure
- Life of a CAT
- Post-CAT World

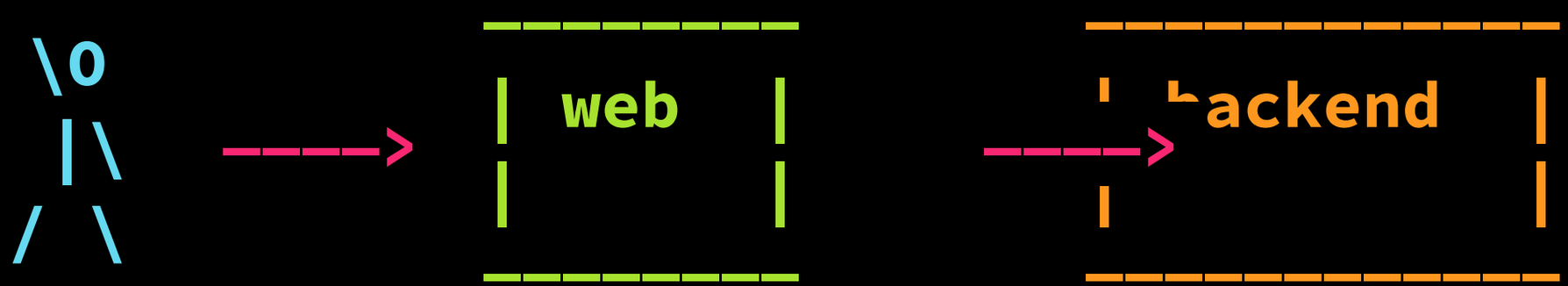
Token Authentication


0
Token
backend
User
credentials
0
Token
Auth
service

Why tokens?

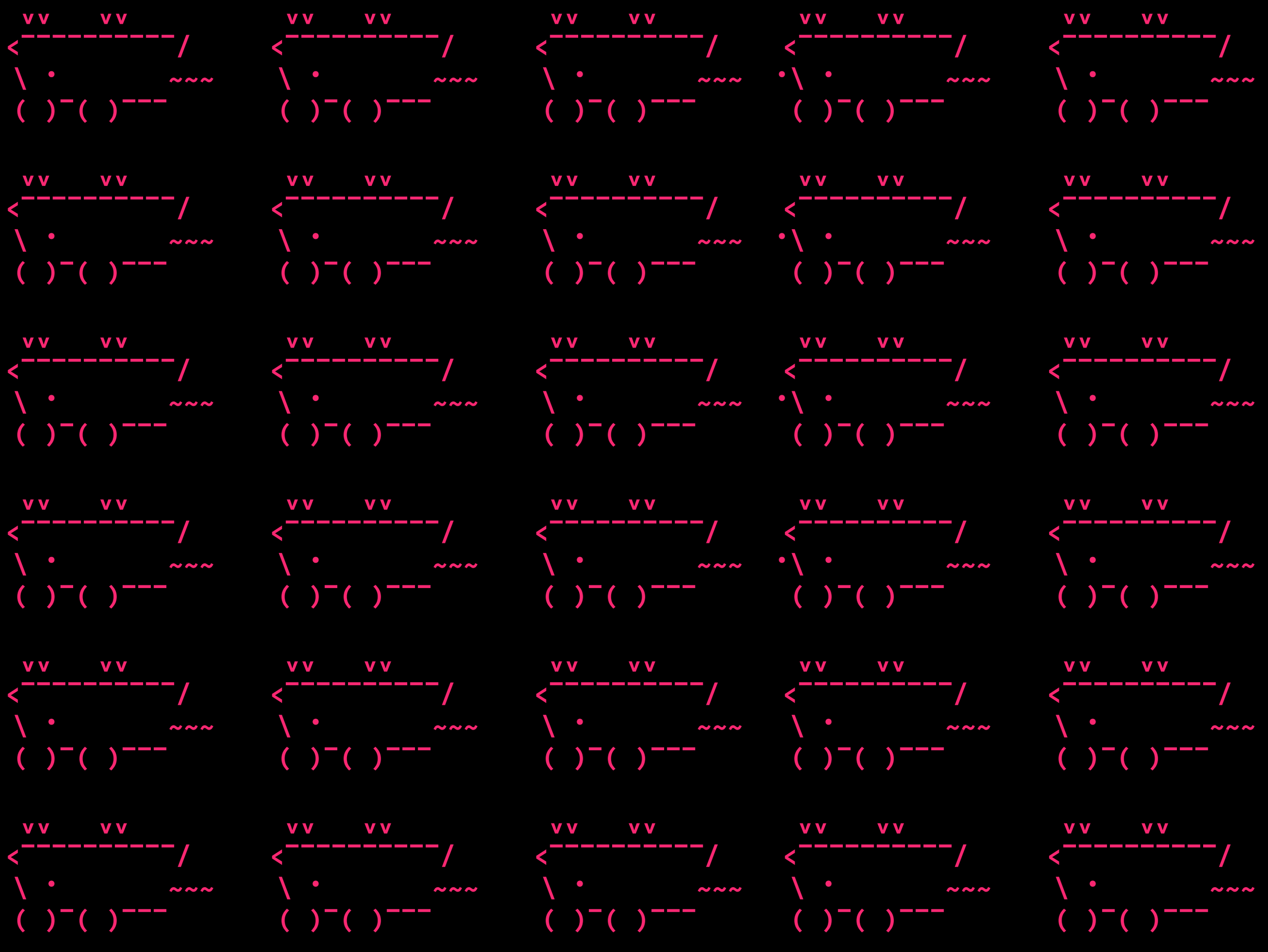
- Trust
- Security?
- Short Living

Authentication Models


web
backend
backend


backend
backend

Pre-CAT World



Pre-CAT World

- Lots of different types of tokens

Pre-CAT World

- Lots of different types of tokens
- Tokens not well-scoped

Pre-CAT World

- Lots of different types of tokens
- Tokens not well-scoped
- Public key cryptography

Pre-CAT World

- Lots of different types of tokens
- Tokens not well-scoped
- Public key cryptography
- Authentication not per request

Requirements

- Narrow down the amount of token libraries

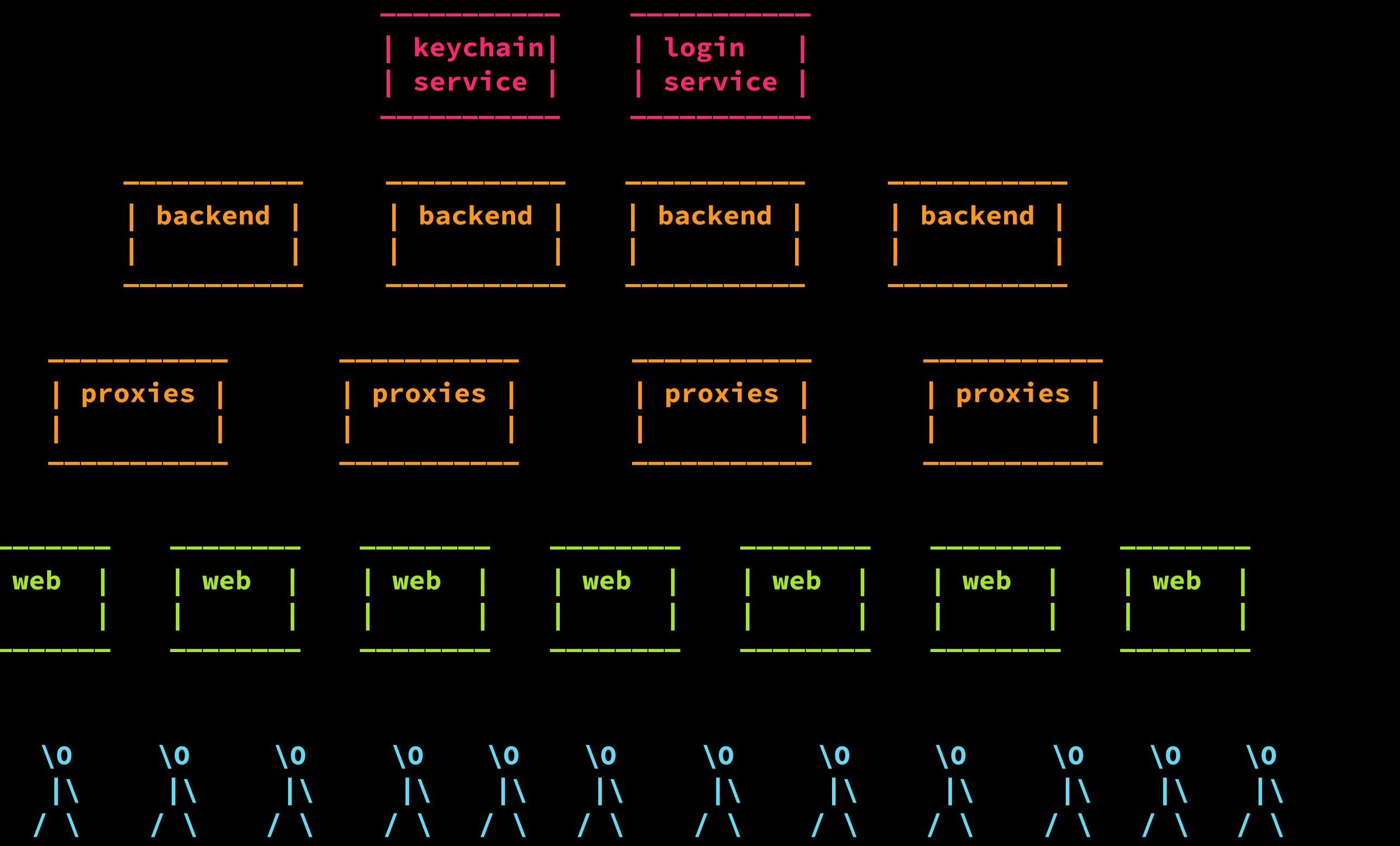
Requirements

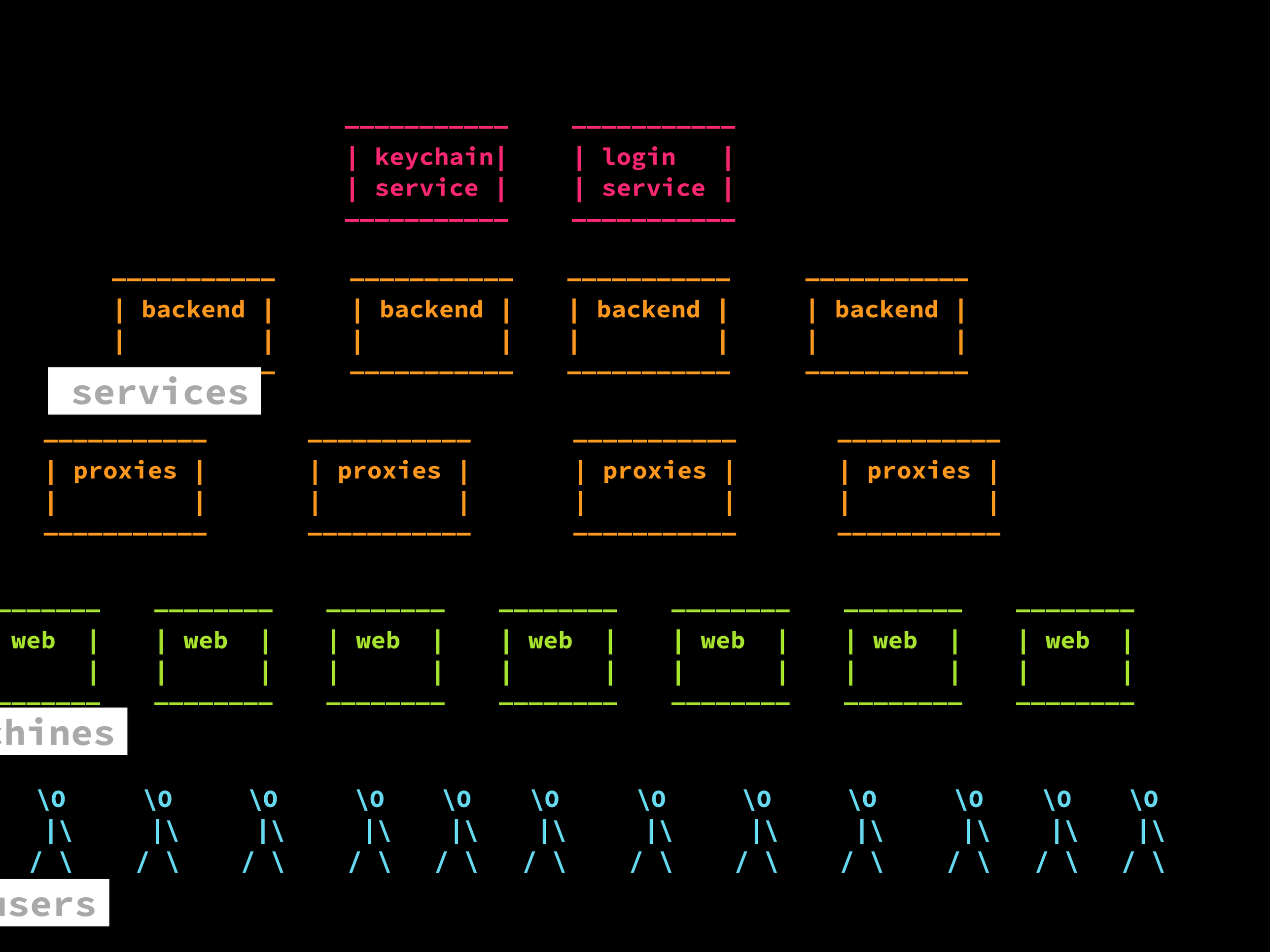
- Narrow down the amount of tokens
- Scoped down and flexible

Requirements

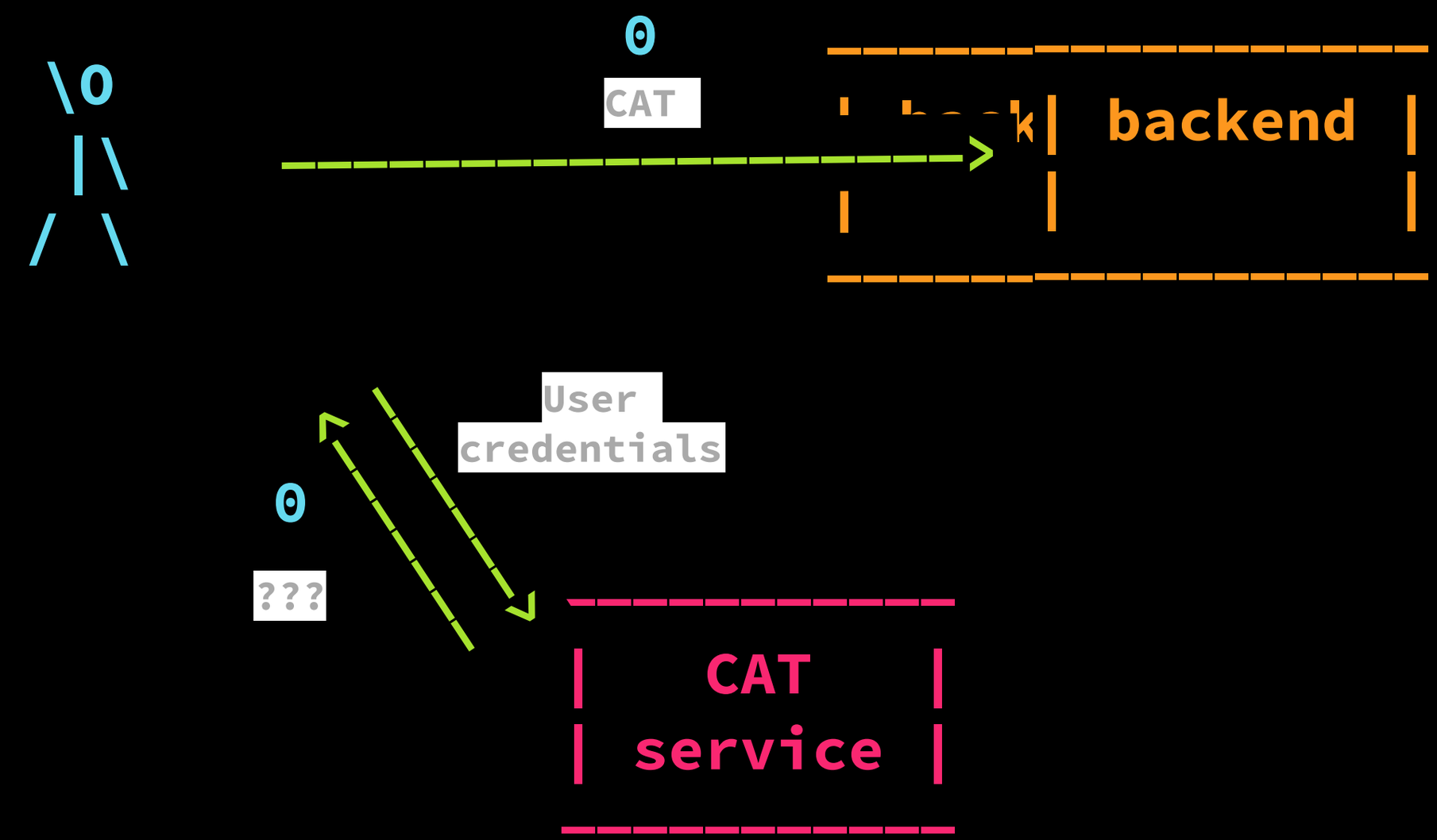
- Narrow down the amount of tokens
- Scoped down and flexible
- **Scalable**

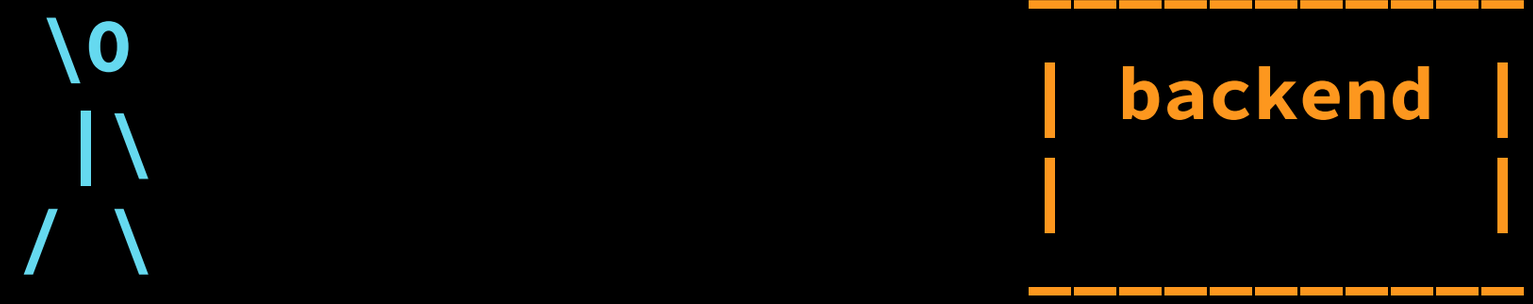
Infrastructure

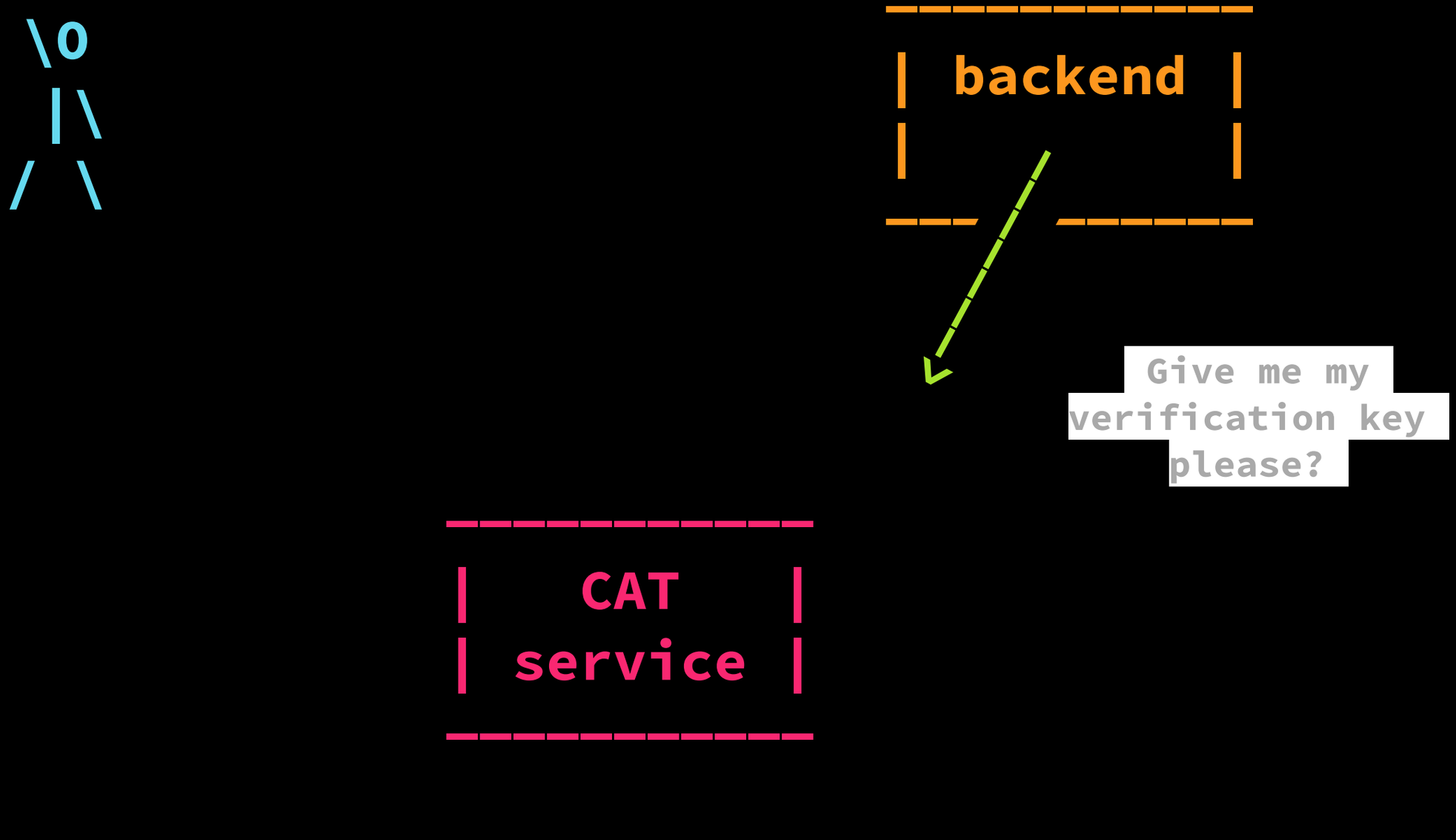

keychain service
login service
backend
backend
backend
backend
proxies
proxies
proxies
proxies
web
web
web
web
web
web
web
web

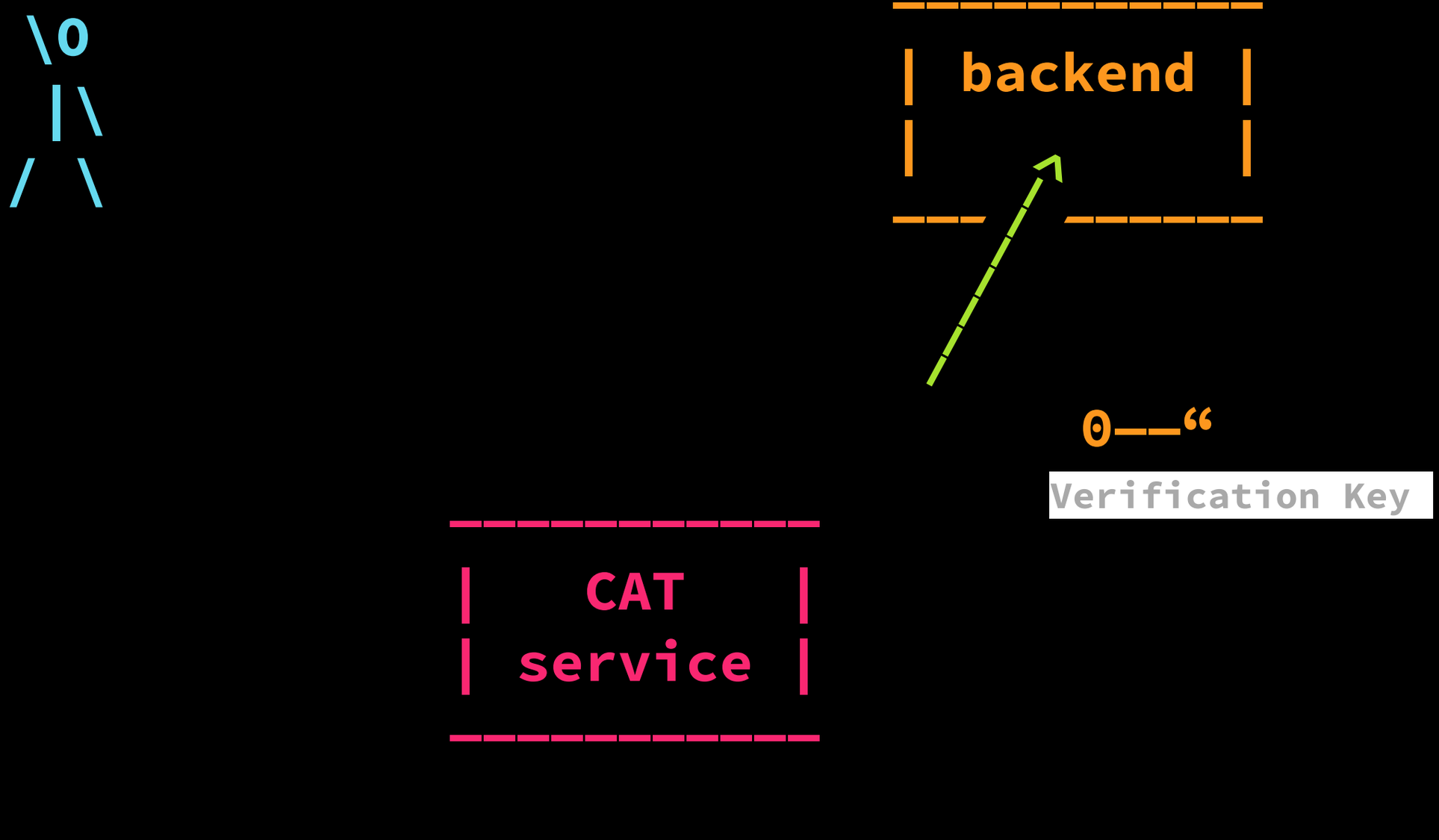

keychain service
login service
backend
backend
backend
backend
services
proxies
proxies
proxies
proxies
web
web
web
web
web
web
web
web
chines
users

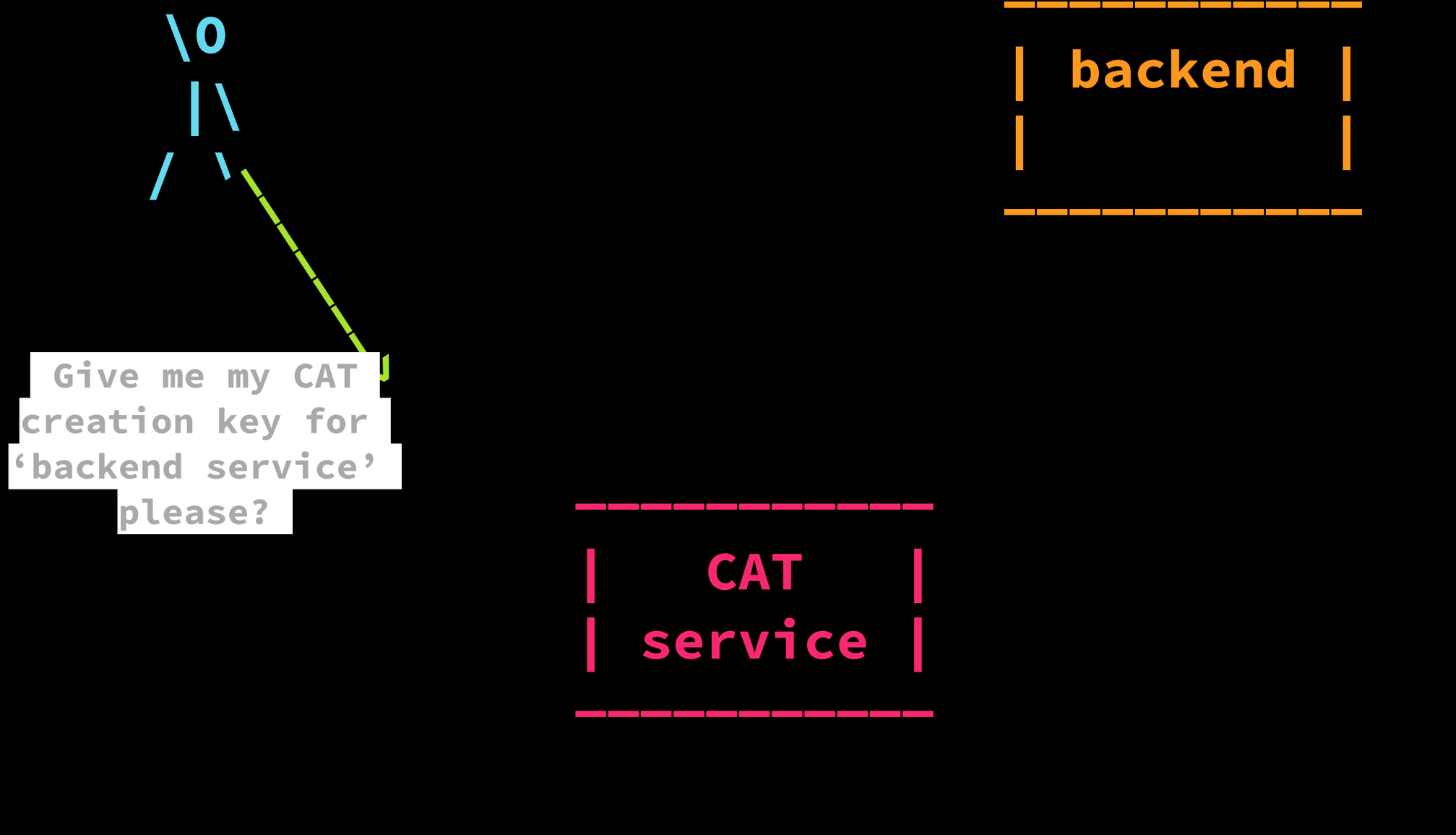
Life of a CAT


0
CAT
backend
\0
User
credentials
0
???
CAT
service


\o
backend


backend
Give me my verification key please?
CAT service


backend
0—“
Verification Key
CAT
service


\o
|\
/ \
Give me my CAT creation key for ‘backend service’ please?
o—-“
Verification Key
backend
CAT service


\o
|\
/ \
o——“
Creation Key
o——“
Verification Key
| backend |
| |
| CAT |
| service |

CAT Keys

0——“

Verification Key -->

ONCE DERIVED KEY

Backend Service Gets

CAT Keys

0——“

CAT Root Key

↓

Derivation

PRF(CAT Root Key, Backend Service Identity)

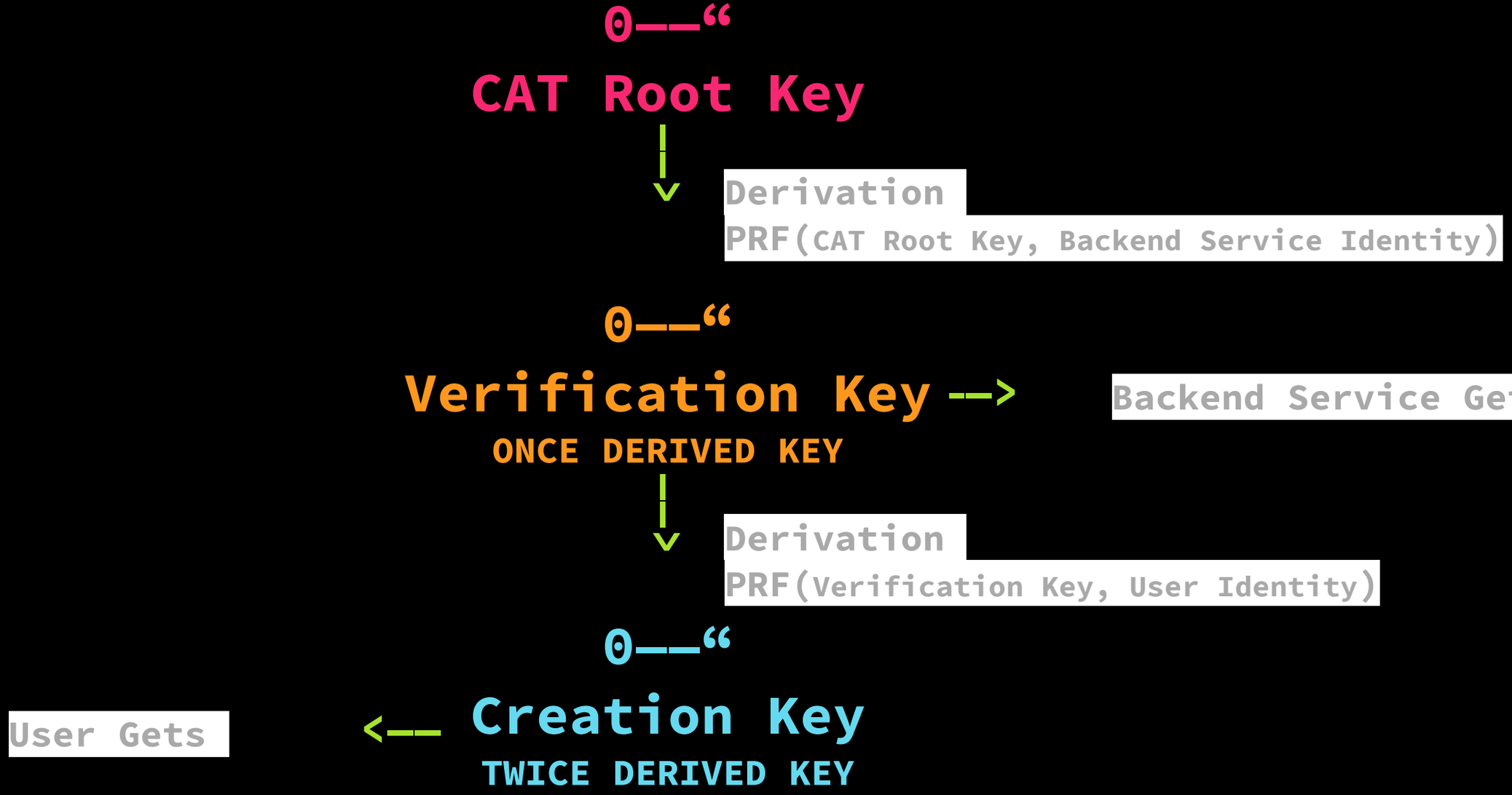
0——“

Verification Key——>

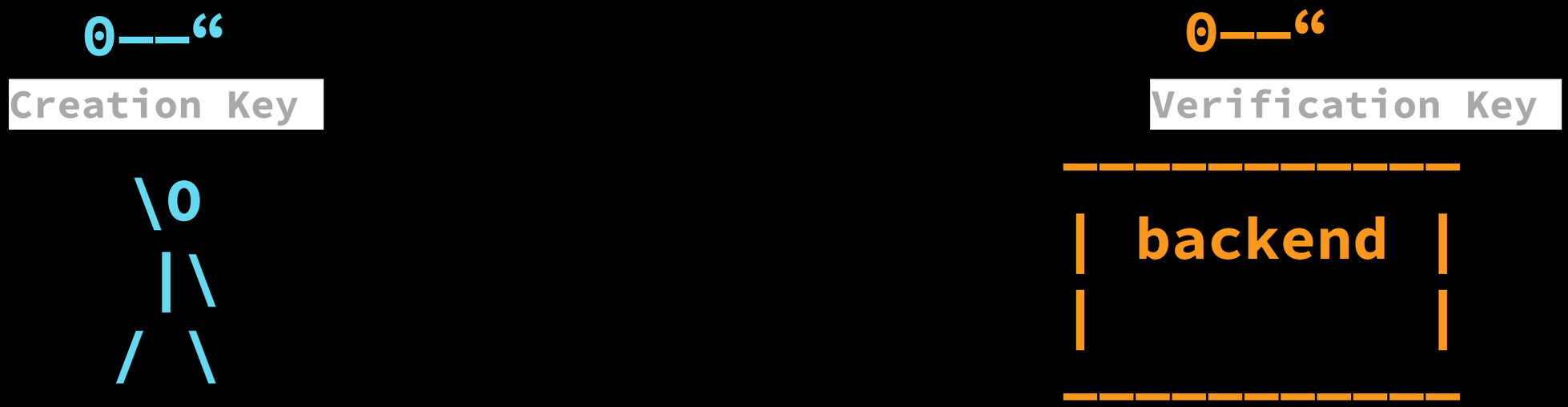
ONCE DERIVED KEY

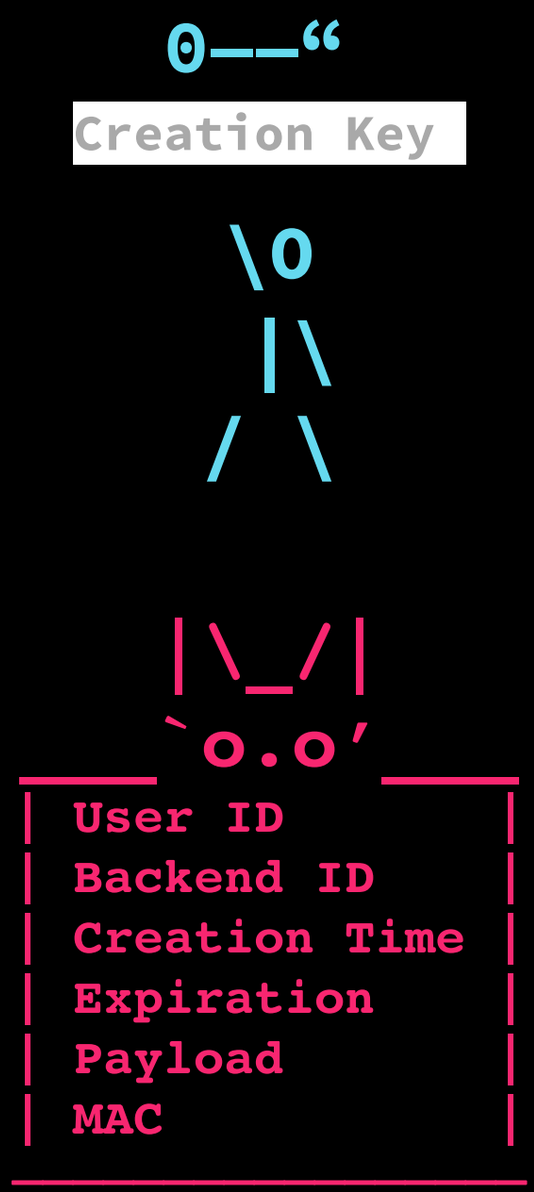
Backend Service Gets

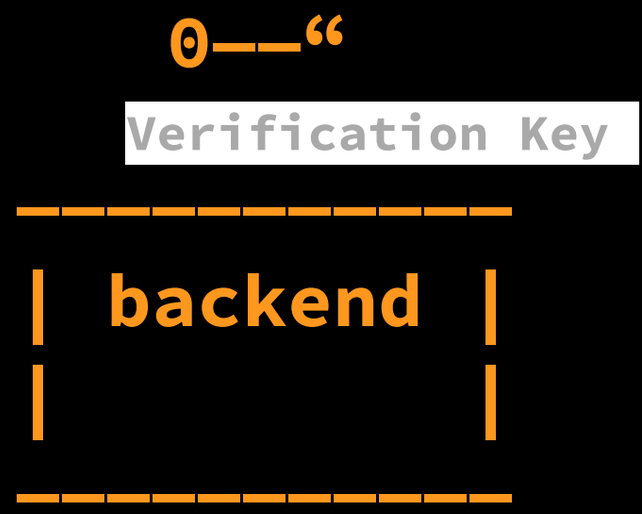
CAT Keys

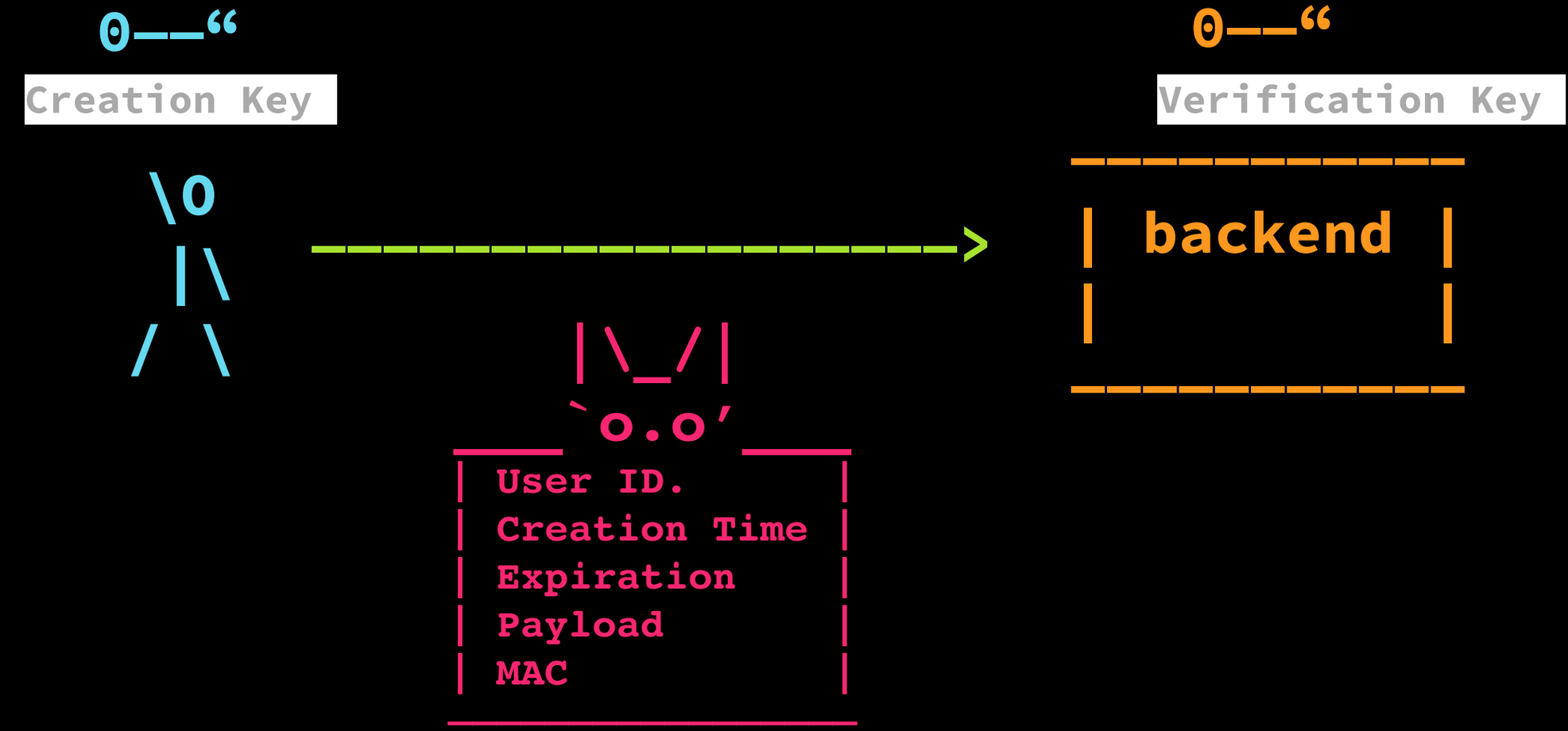

0——“
CAT Root Key
Derivation
PRF(CAT Root Key, Backend Service Identity)
0——“
Verification Key —>
Backend Service Gets
ONCE DERIVED KEY
Derivation
PRF(Verification Key, User Identity)
0——“
<— Creation Key
User Gets
TWICE DERIVED KEY

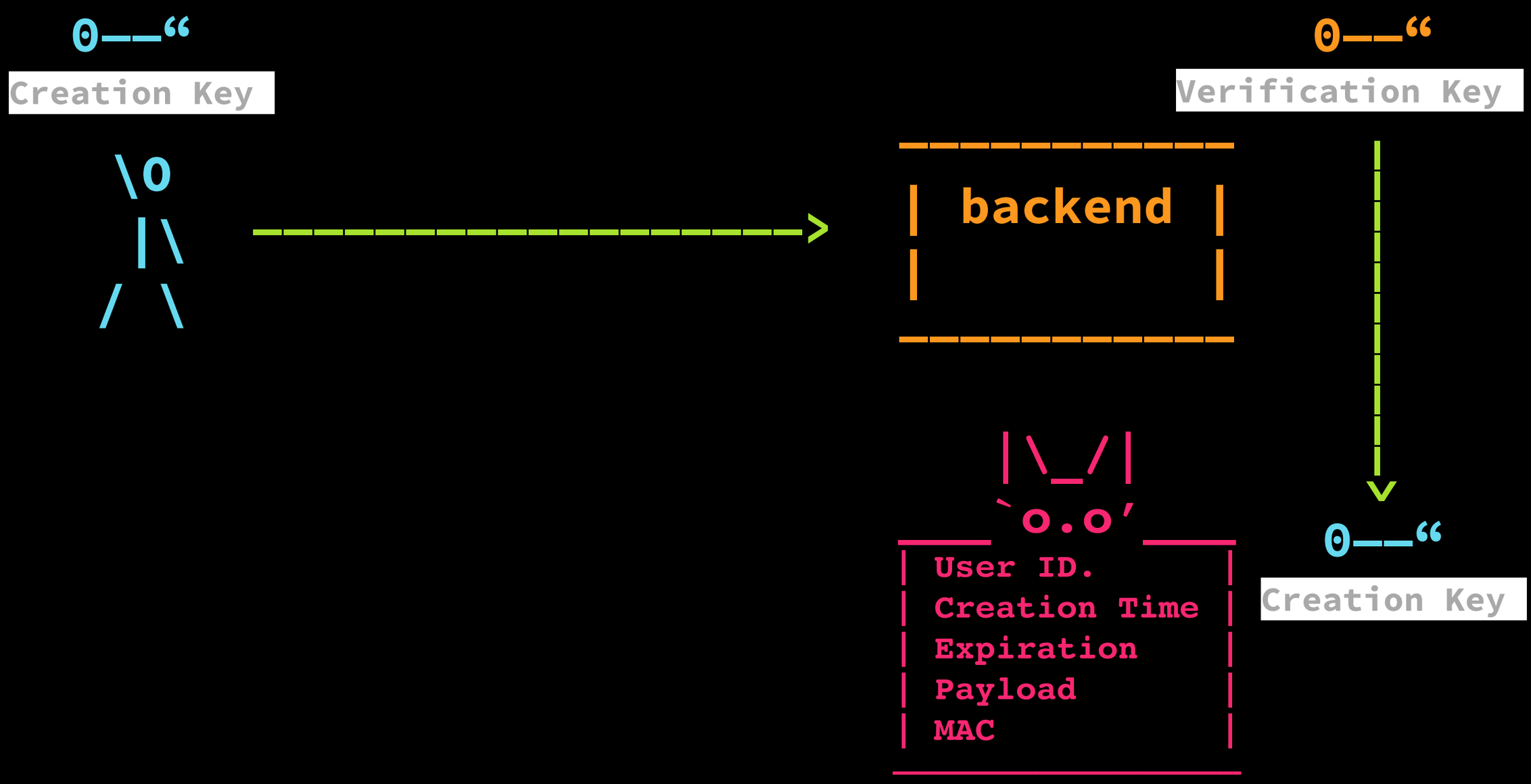

\o
|\
/ \
o——“
Creation Key
o——“
Verification Key
| backend |
| |
| CAT |
| service |

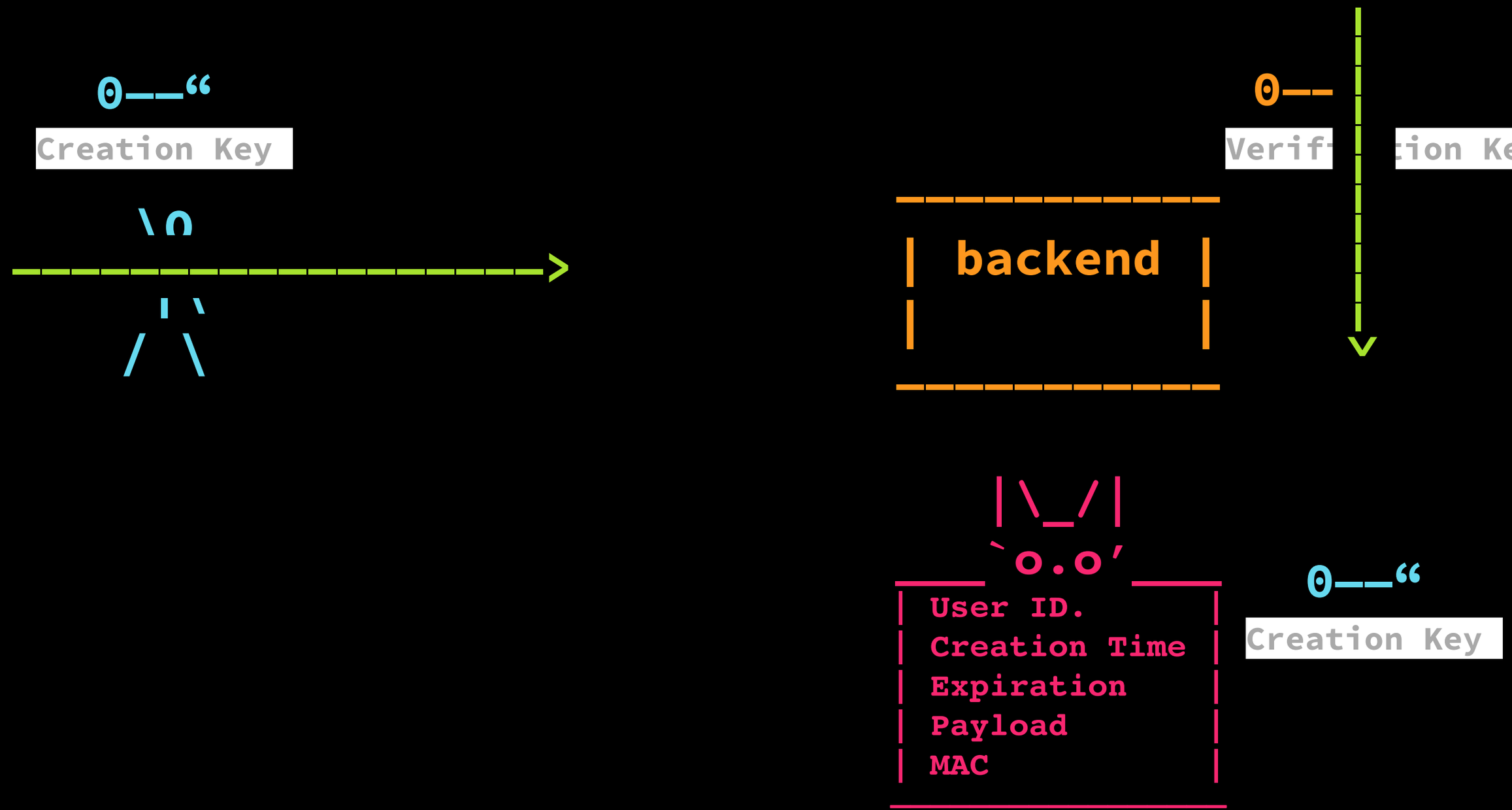

Creation Key
Verification Key
backend

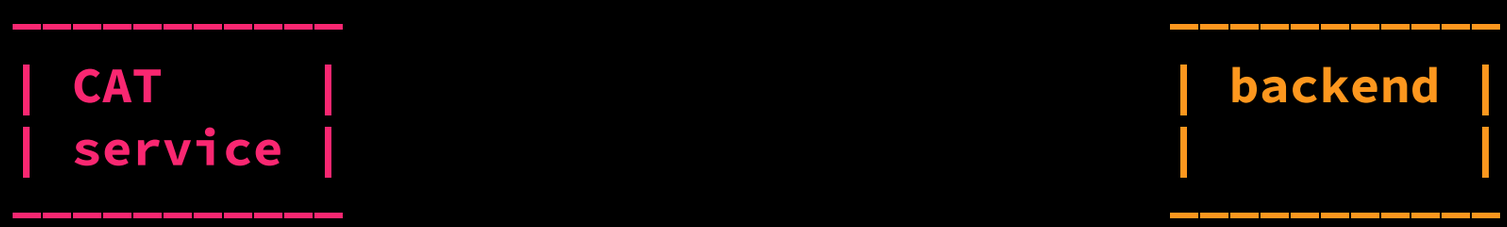

Creation Key
User ID
Backend ID
Creation Time
Expiration
Payload
MAC

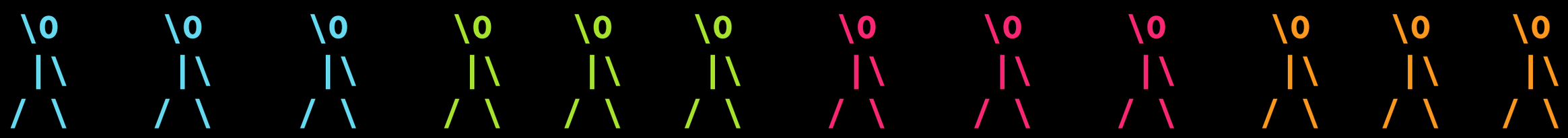

Verification Key
backend

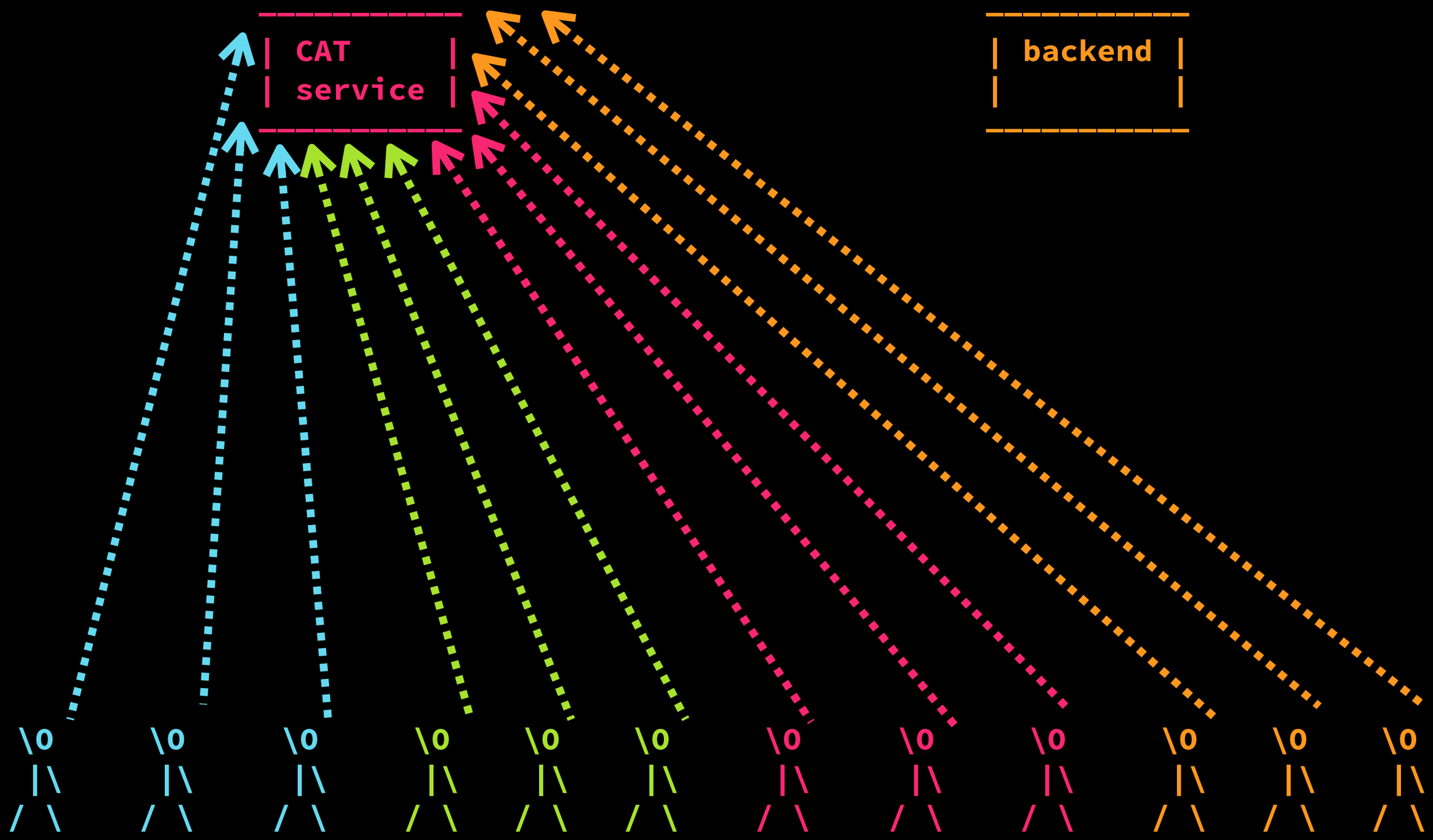

Creation Key
Verification Key
backend
User ID.
Creation Time
Expiration
Payload
MAC

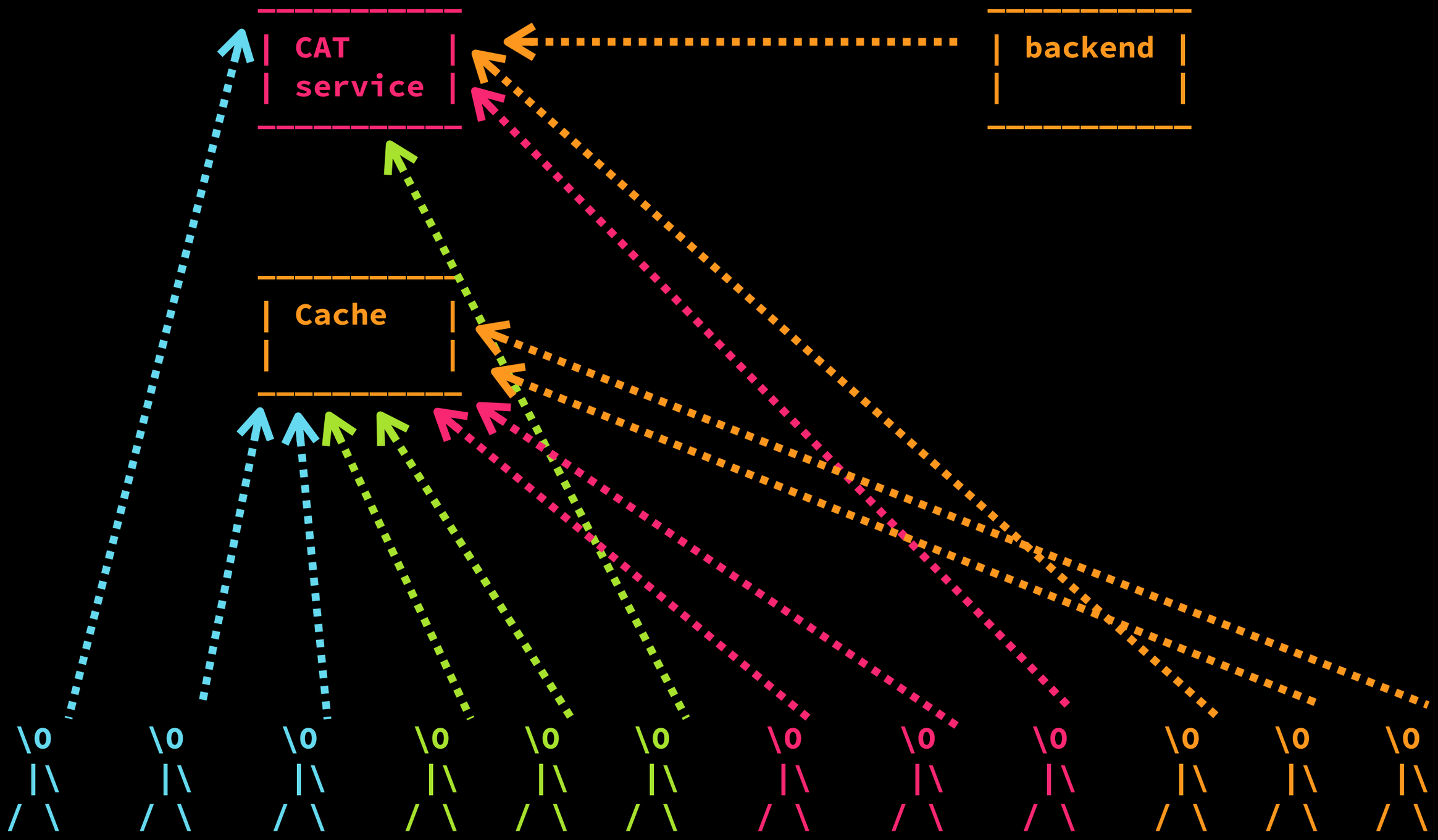

Creation Key
backend
Verification Key
User ID.
Creation Time
Expiration
Payload
MAC
Creation Key

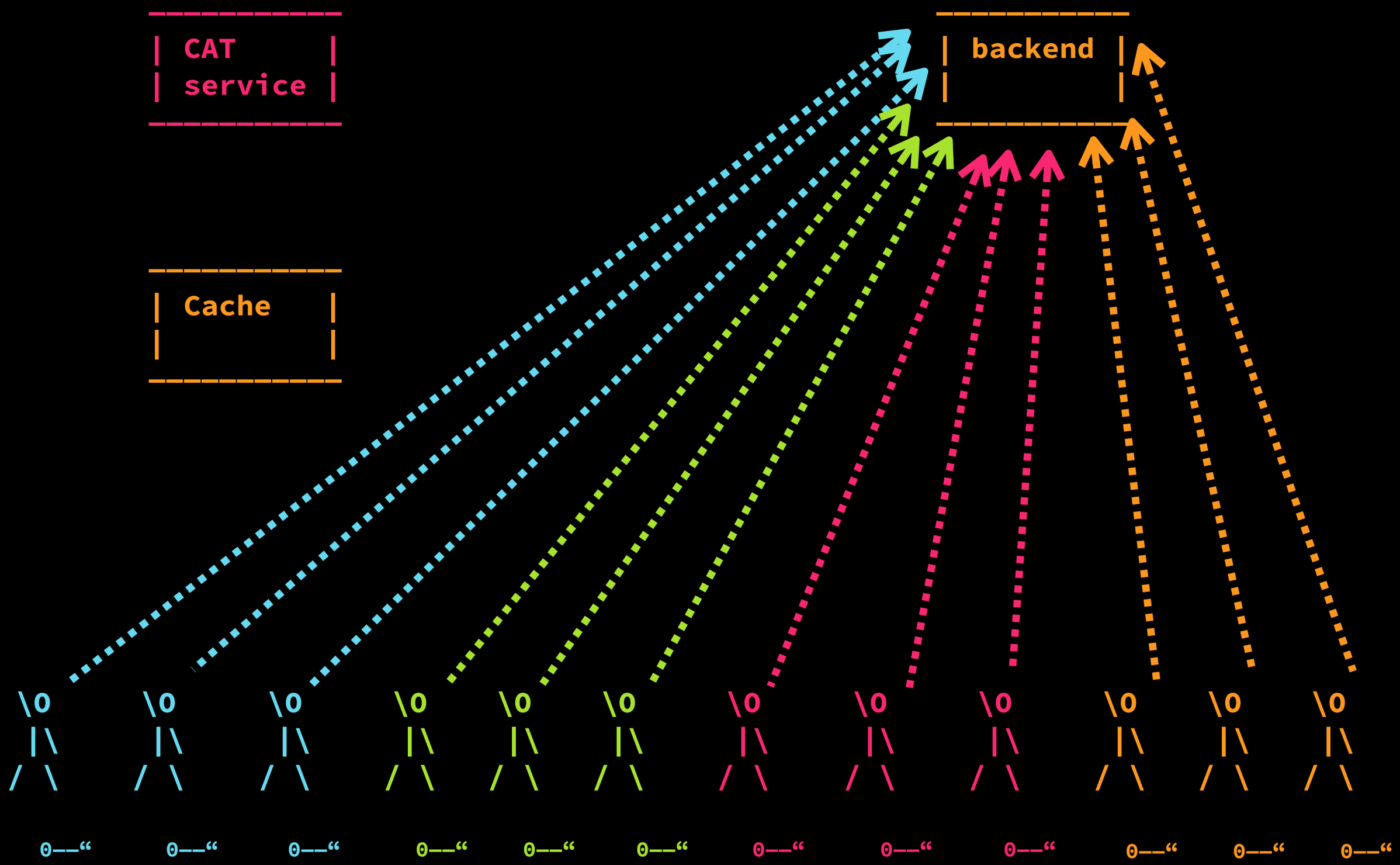

Creation Key
backend
Verif
tion Ke
User ID.
Creation Time
Expiration
Payload
MAC
Creation Key


CAT
service
backend




CAT service
backend


CAT service
backend
Cache

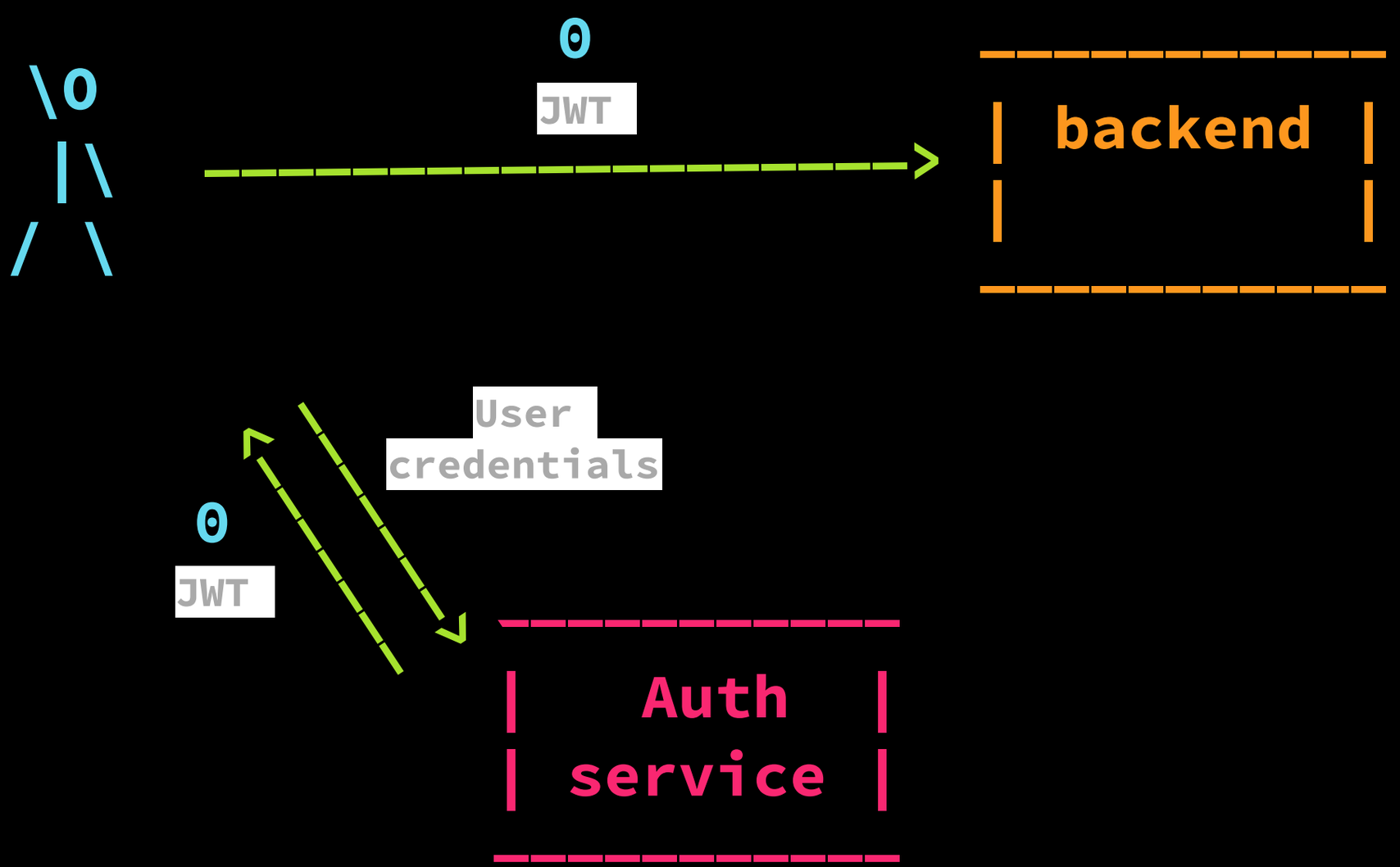

CAT service
Cache
backend

CATs, JWTs, and Macaroons walk into a bar…

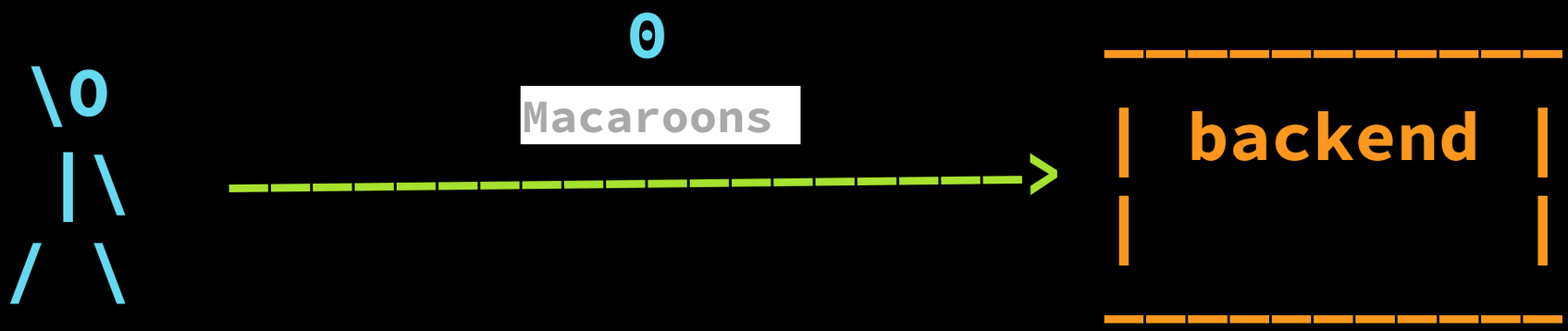
CATs, JWTs, and Macaroons walk into a bar…

#TODO (find punchline)

JWT



Macaroons



Post-CAT World

Post-CAT World

- Flexible token for authentication

Post-CAT World

- Flexible token for authentication
- Well-scoped token

Post-CAT World

- Flexible token for authentication
- Well-scoped token
- Authentication for every request

Post-CAT World

- Flexible token for authentication
- Well-scoped token
- Authentication for every request
- Faster

Questions?

(no mice were harmed in the creation of this protocol)