Introduction to UCAN

User Controlled Authorization Networks

Brooklyn Zelenka

@expede

Brooklyn Zelenka

@expede

- CTO at Fission
  - https://fission.codes / @FISSIONCodes
  - SDK: local-first, E2EE/EAR, distributed, passwordless

Brooklyn Zelenka

@expede

- CTO at Fission
  - https://fission.codes / @FISSIONCodes
  - SDK: local-first, E2EE/EAR, distributed, passwordless
- Background: PLT, VMs, Formal Methods

Brooklyn Zelenka

@expede

- CTO at Fission
  - https://fission.codes / @FISSIONCodes
  - SDK: local-first, E2EE/EAR, distributed, passwordless
- Background: PLT, VMs, Formal Methods
- Meetups: VanFP, Code & Coffee, Distributed Systems Reading Group

Brooklyn Zelenka

@expede

- CTO at Fission
  - https://fission.codes / @FISSIONCodes
  - SDK: local-first, E2EE/EAR, distributed, passwordless
- Background: PLT, VMs, Formal Methods
- Meetups: VanFP, Code & Coffee, Distributed Systems Reading Group

https://lu.ma/distributed-systems

Cryptography is a tool for turning lots of different problems into key management problems

Dr. Lea Kissner, Google's Global Lead of Privacy Technologies

Intro

What We're Going to Cover

Intro

What We're Going to Cover

- Dependencies
- Intuition for ACL vs Cap
- UCAN Anatomy
- Delegation
- Nontrivial Example

Intro

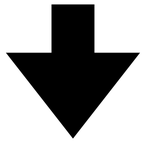
What We're Going to Cover

- Dependencies
- Intuition for ACL vs Cap
- UCAN Anatomy
- Delegation
- Nontrivial Example

- Not going to cover
  - Deep theory
  - Design considerations
  - Full-Blown Object Capabilities
  - UCAN-Based Auth Recovery
  - WebCrypto API Subtleties

UCAN Teaser Token


```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRt
N2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90
ZXMvIiwiY2FwIjoiT1ZFUldSSVRFIn1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN6OXMyTUhzcVl2TG9j
Y3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5W
IAU--TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg
```


```
{
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "exp": 9256939505,
  "nbf": 1639608293,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "OVERWRITE"
    }
  ]
}
```

Preamble

DIDs

Decentralized Digital Identity

DIDs

EXAMPLE 2: Minimal self-managed DID Document

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    // this key can be used to authenticate as DID ...9938
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

Decentralized Digital Identity

DIDs

- Interoperable format
- One or more public keys
- Agnostic about backing
  - Self-attesting
  - Trad. Database
  - Blockchain
- For users, devices, and more
- Relates to verifiable credentials

EXAMPLE 2: Minimal self-managed DID Document

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    // this key can be used to authenticate as DID ...9938
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

Decentralized Digital Identity

Variety

Decentralized Digital Identity

Variety

- Raw Public Keys, Microsoft ION, Ceramic, Sovrin, did:key, >500 others

Decentralized Digital Identity

Variety

- Raw Public Keys, Microsoft ION, Ceramic, Sovrin, did:key, >500 others
- Can federate, but early so rarely done in the wild
  - DIF has a JVM-based "Universal Resolver"
  - Custom e.g. did:key + ION

Decentralized Digital Identity

did:key & UCAN

Decentralized Digital Identity

did:key & UCAN

- “Just” a public key (e.g. RSA, EdDSA)

Decentralized Digital Identity

did:key & UCAN

- “Just” a public key (e.g. RSA, EdDSA)
- Self-certifying, extremely flexible

Decentralized Digital Identity

did:key & UCAN

- “Just” a public key (e.g. RSA, EdDSA)
- Self-certifying, extremely flexible
- Well suited to capabilities/authZ (vs identity/authN)

Decentralized Digital Identity

did:key & UCAN

- “Just” a public key (e.g. RSA, EdDSA)
- Self-certifying, extremely flexible
- Well suited to capabilities/authZ (vs identity/authN)
- UCANs — "transfer authority without transferring keys"
  - did:key → authN
  - UCAN → authZ

DIDs say who you are

DIDs say who you are
UCANs show what you can do

User Controlled, Local-First, Universal Auth & ID

UCAN

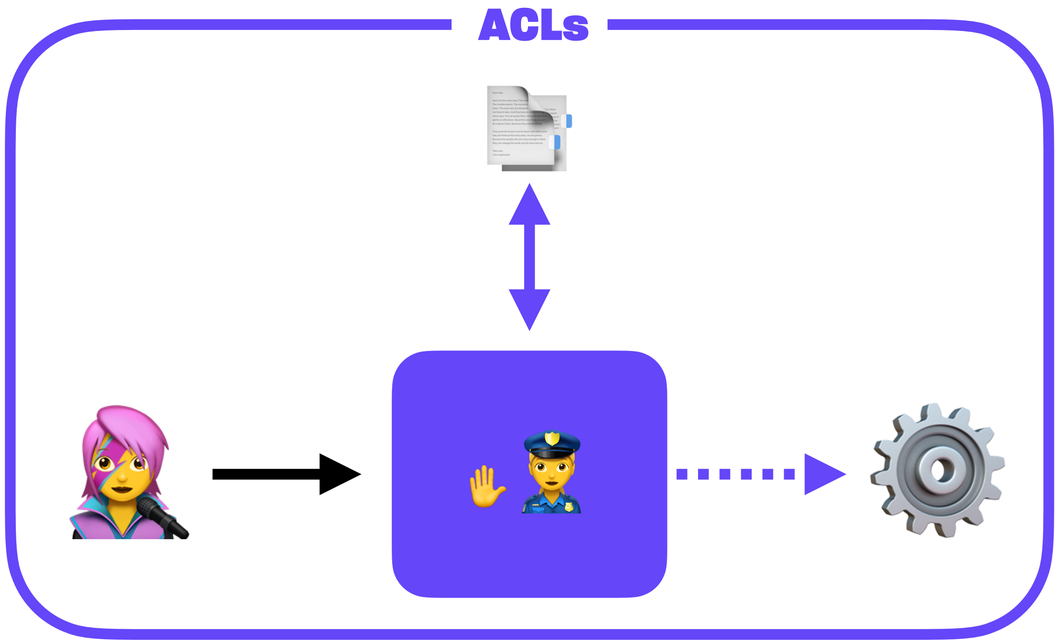
UCAN

Capability Model

UCAN

Capability Model

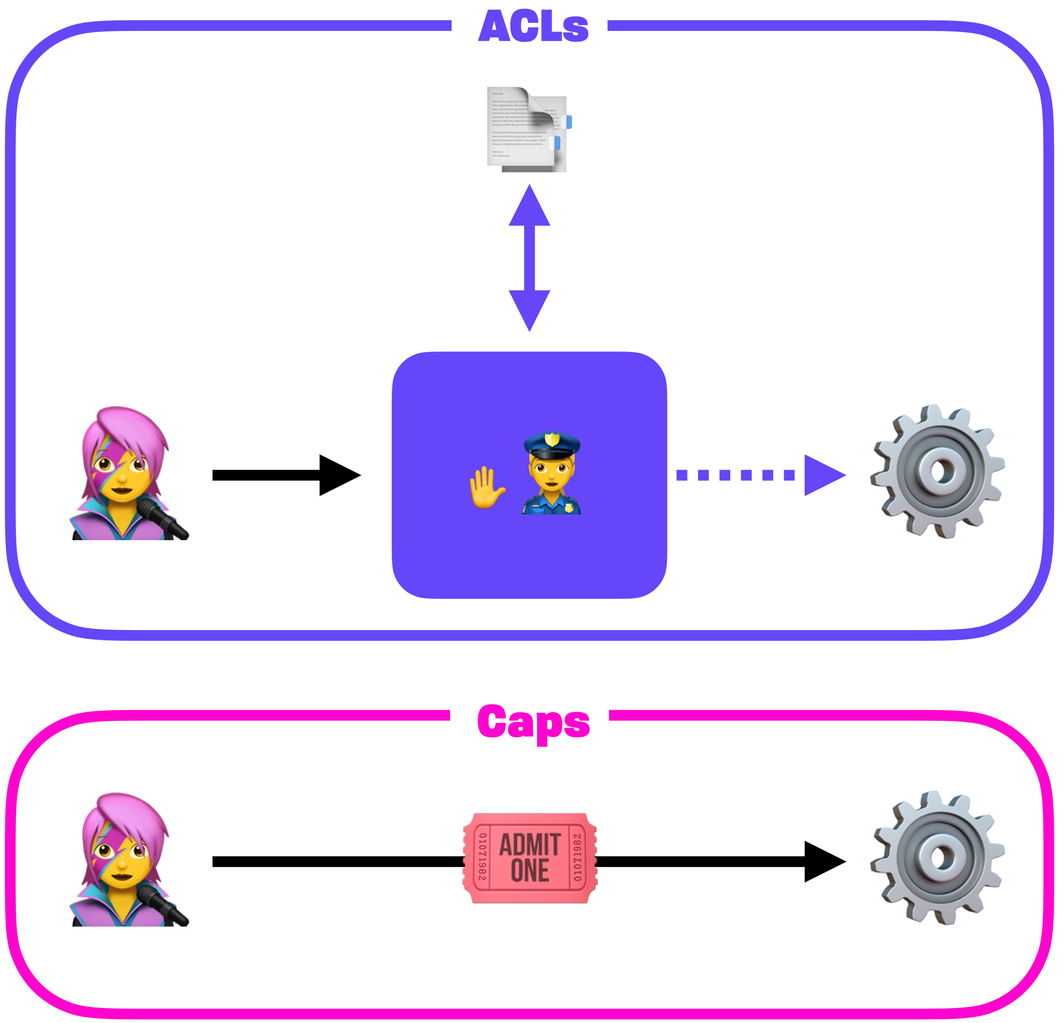
- ACLs are “reactive auth”



UCAN

Capability Model

- ACLs are “reactive auth”
- Capabilities are “proactive auth”
  - Contains all the info about access
  - Any guarding done up front (e.g. time limiting)
  - Generally some reference, proof, or key
    - Anything directly created (parenthood 🐣)
    - Delegate subset to another (introduction 🤝)
  - Long history (e.g. X.509, SPKI/SDSI, Macaroons)



UCAN

ACL Read & Write

UCAN

ACL Read & Write

UCAN

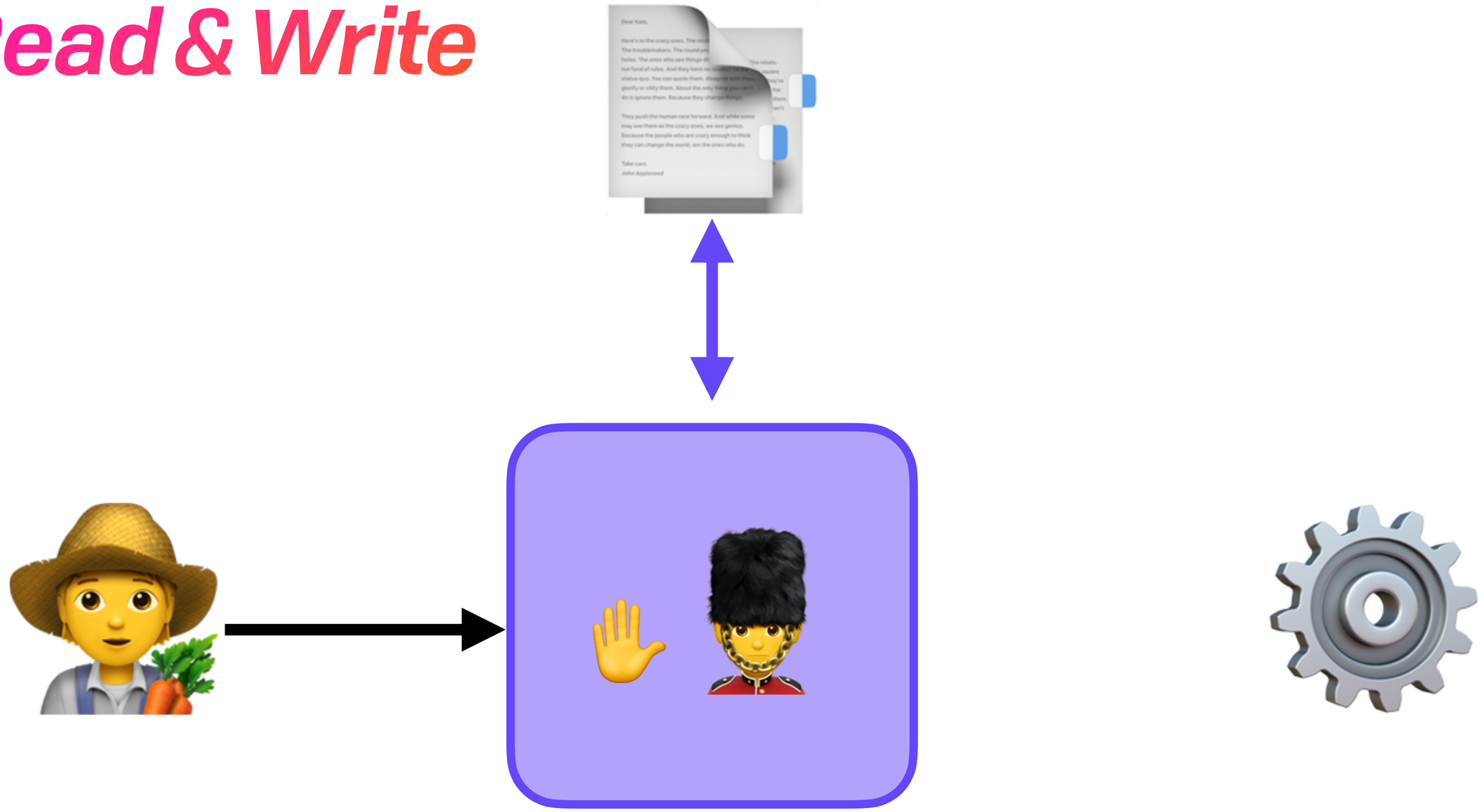
ACL Read & Write

UCAN

ACL Read & Write

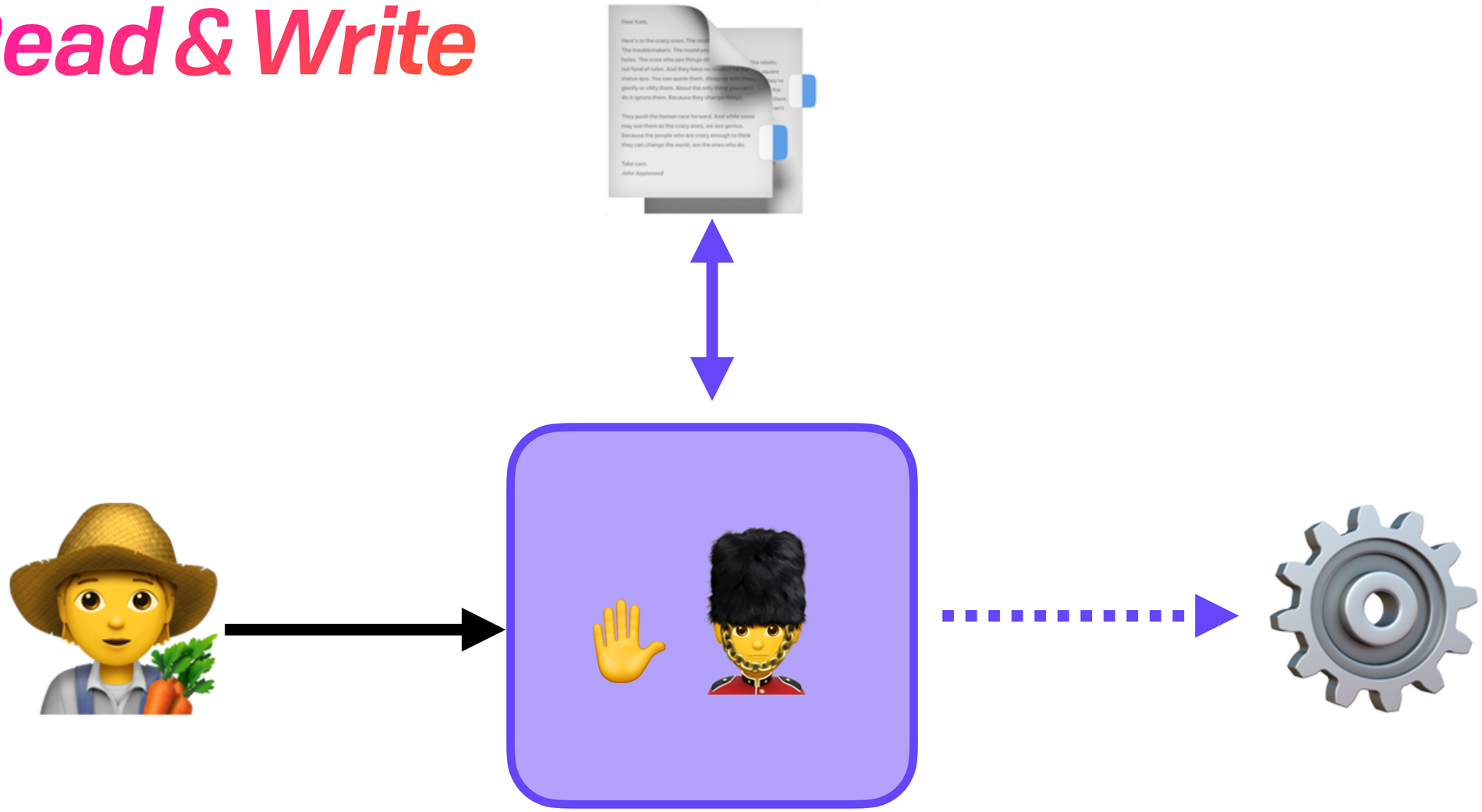
UCAN

ACL Read & Write



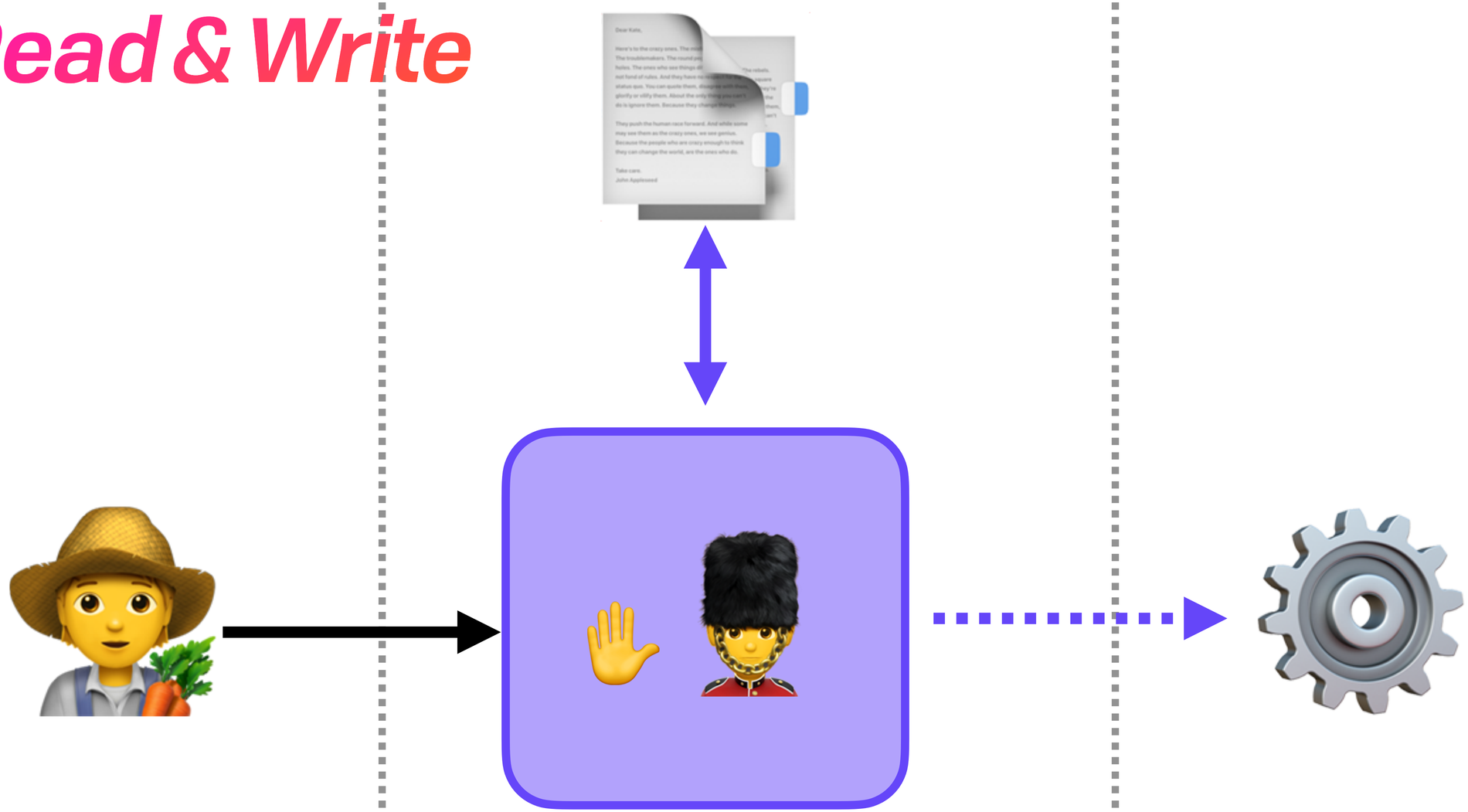
UCAN

ACL Read & Write



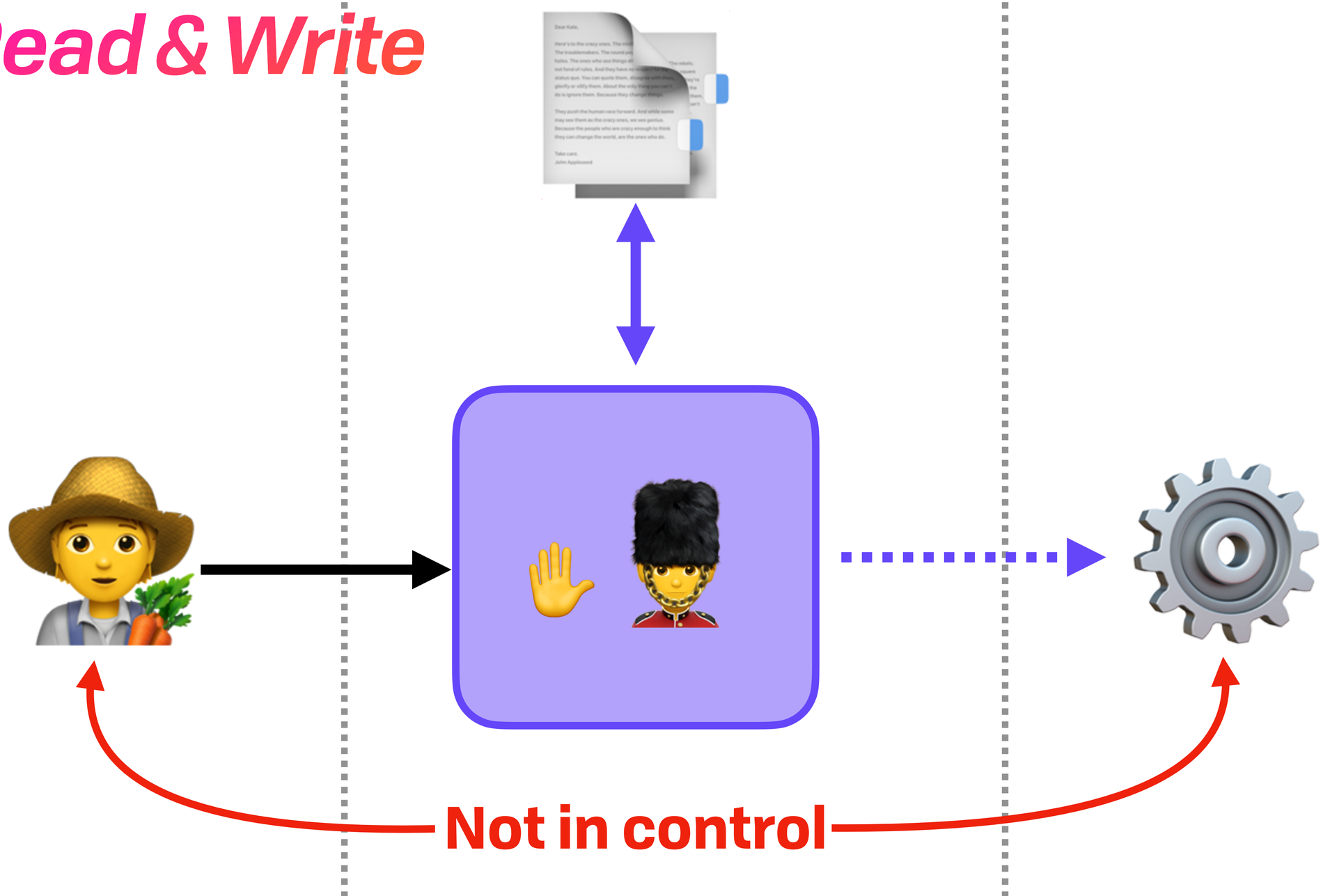
UCAN

ACL Read & Write



UCAN

ACL Read & Write



UCAN

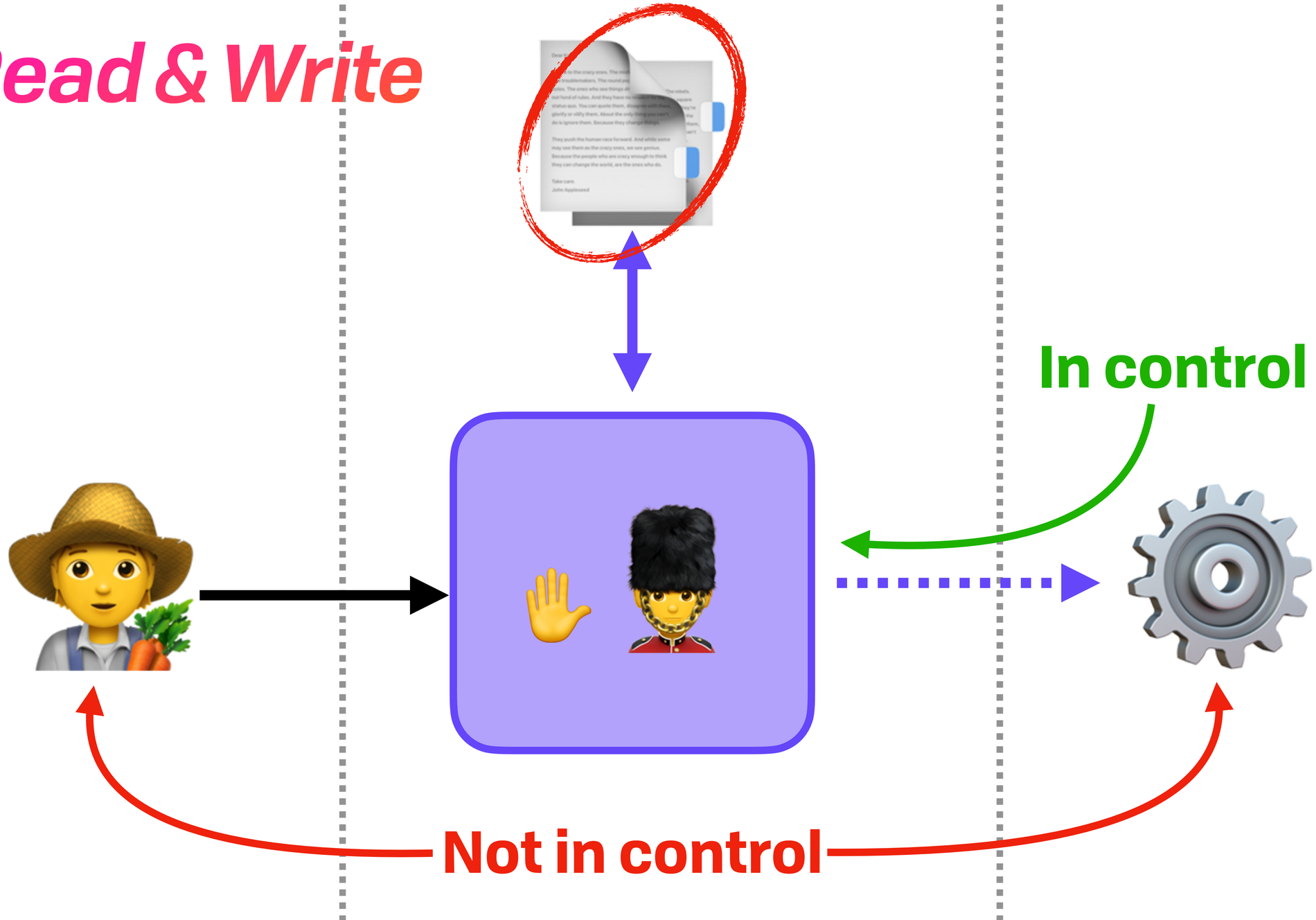
ACL Read & Write

In control

Not in control

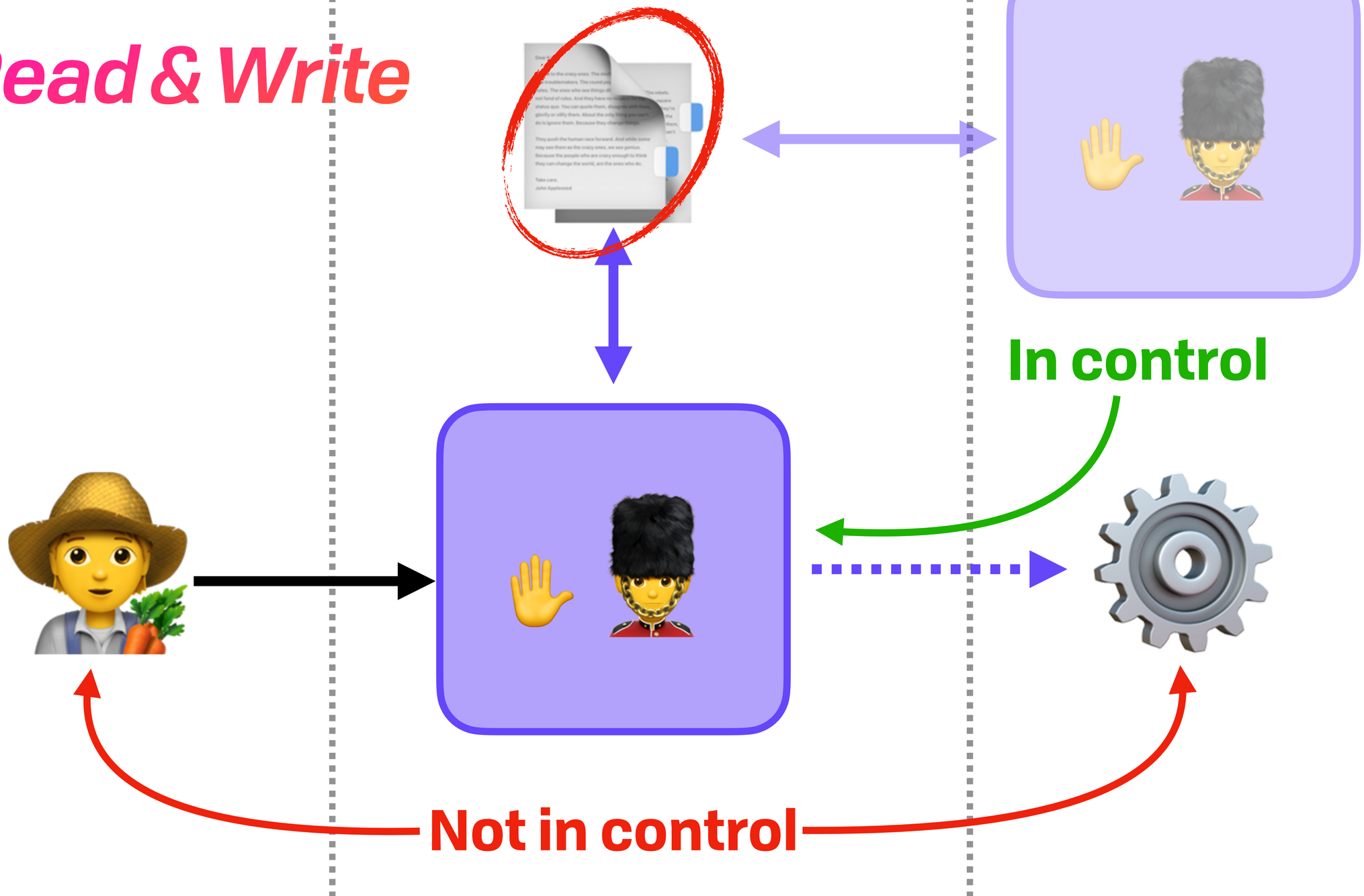
UCAN

ACL Read & Write



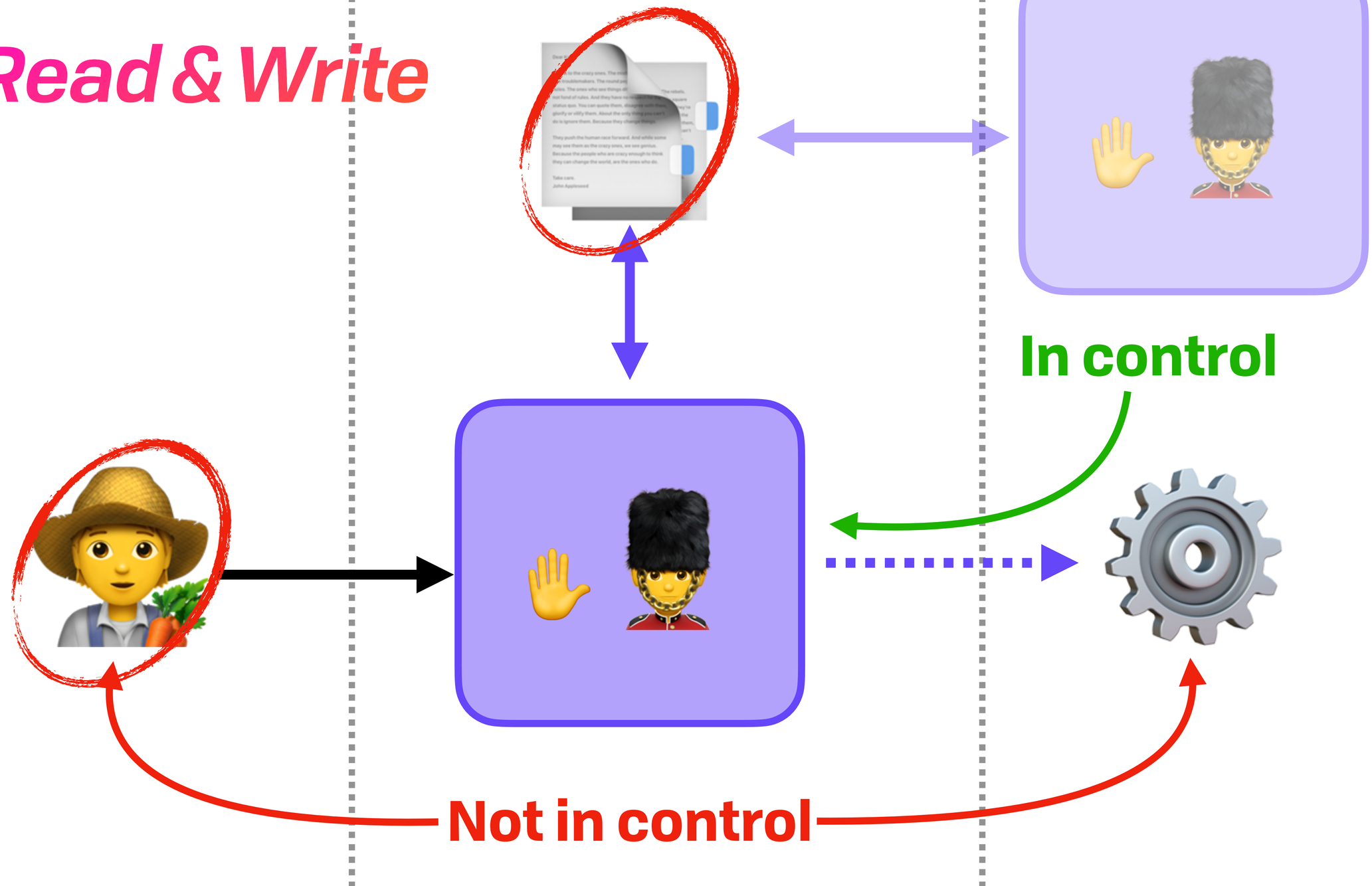
UCAN

ACL Read & Write



UCAN

ACL Read & Write



UCAN

From Actors to Capabilities

UCAN

From Actors to Capabilities

UCAN

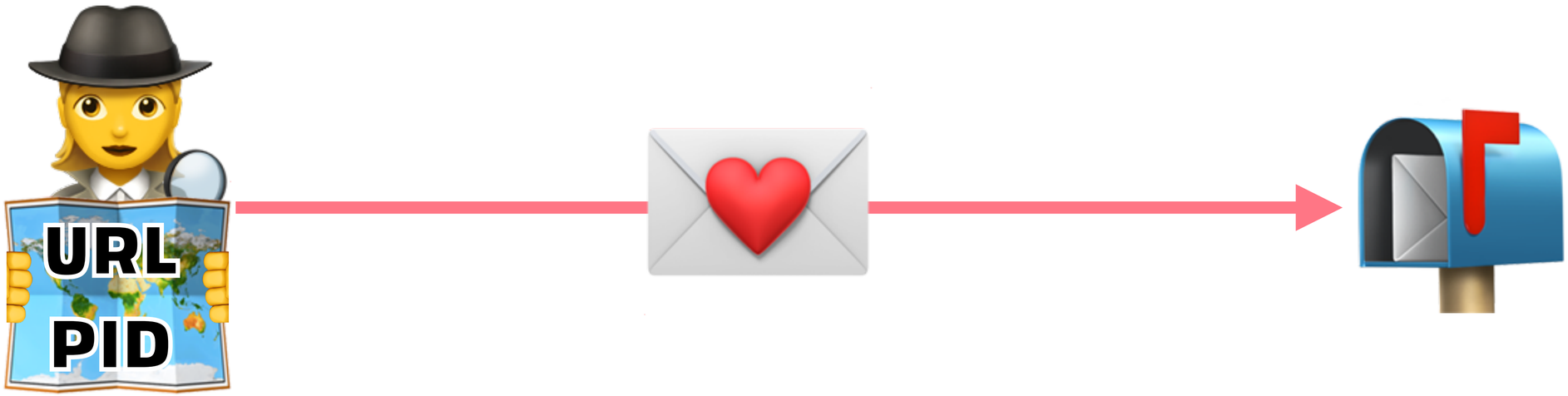
From Actors to Capabilities

UCAN

From Actors to Capabilities

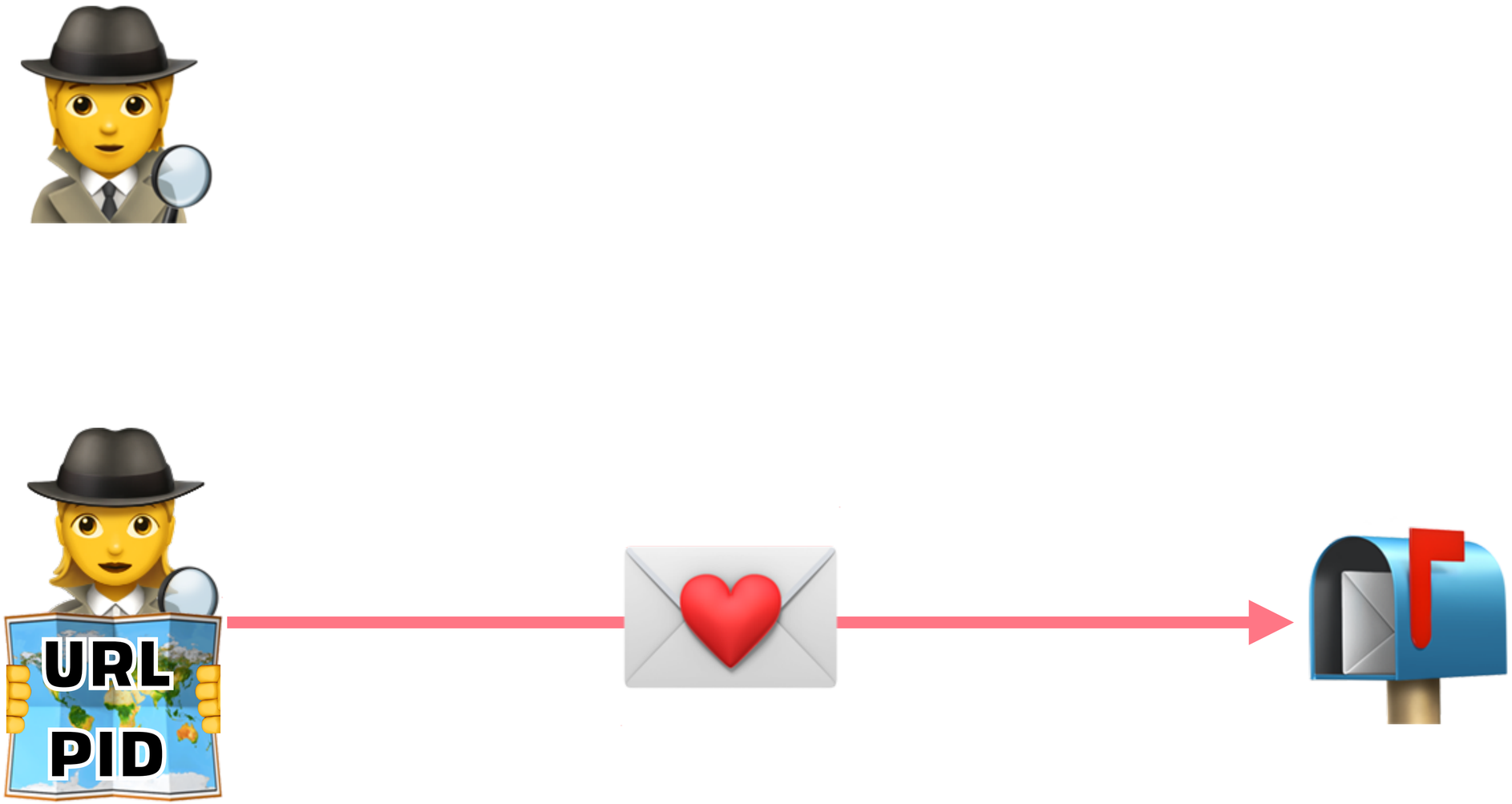
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

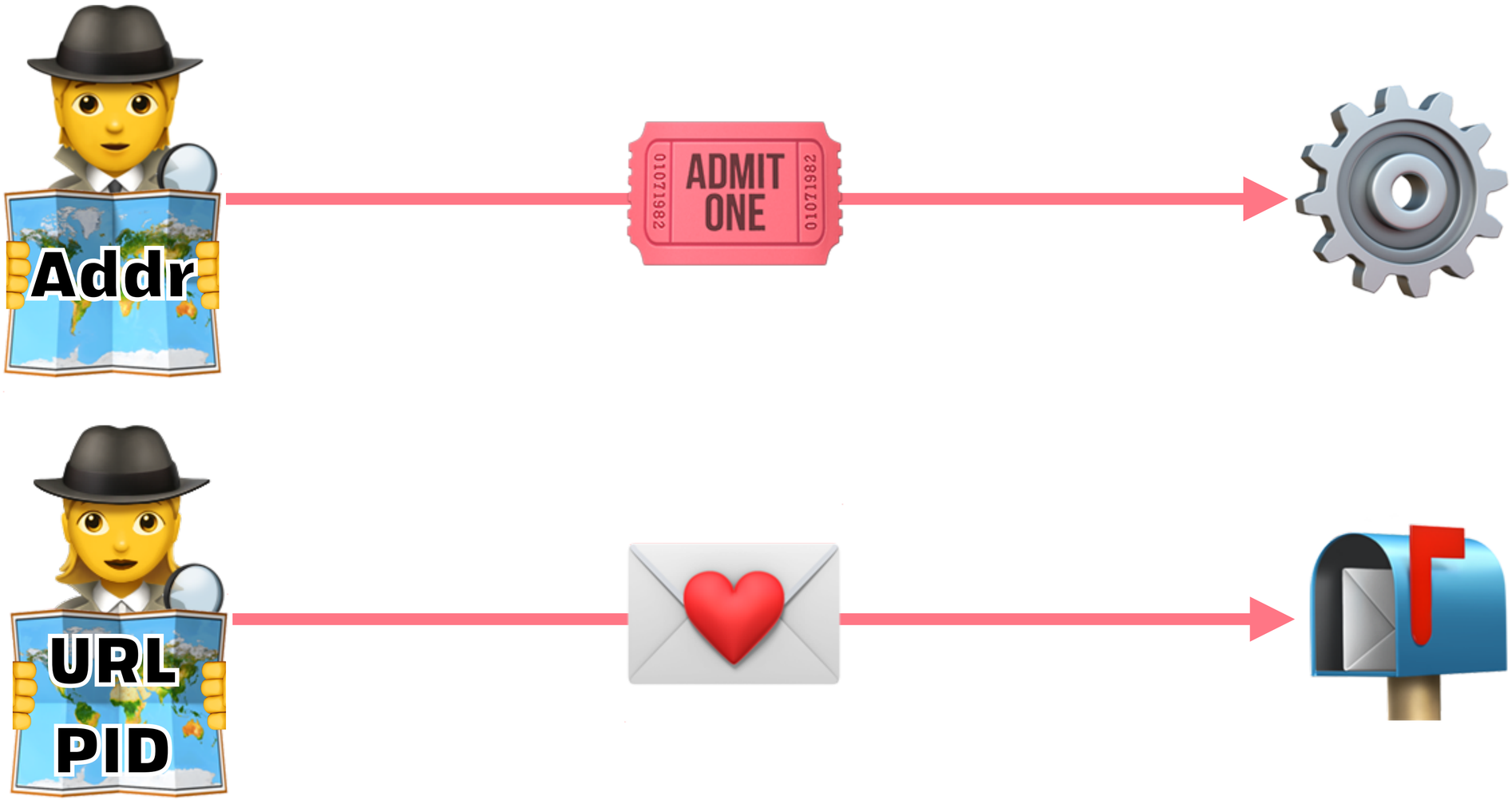
From Actors to Capabilities

UCAN

From Actors to Capabilities

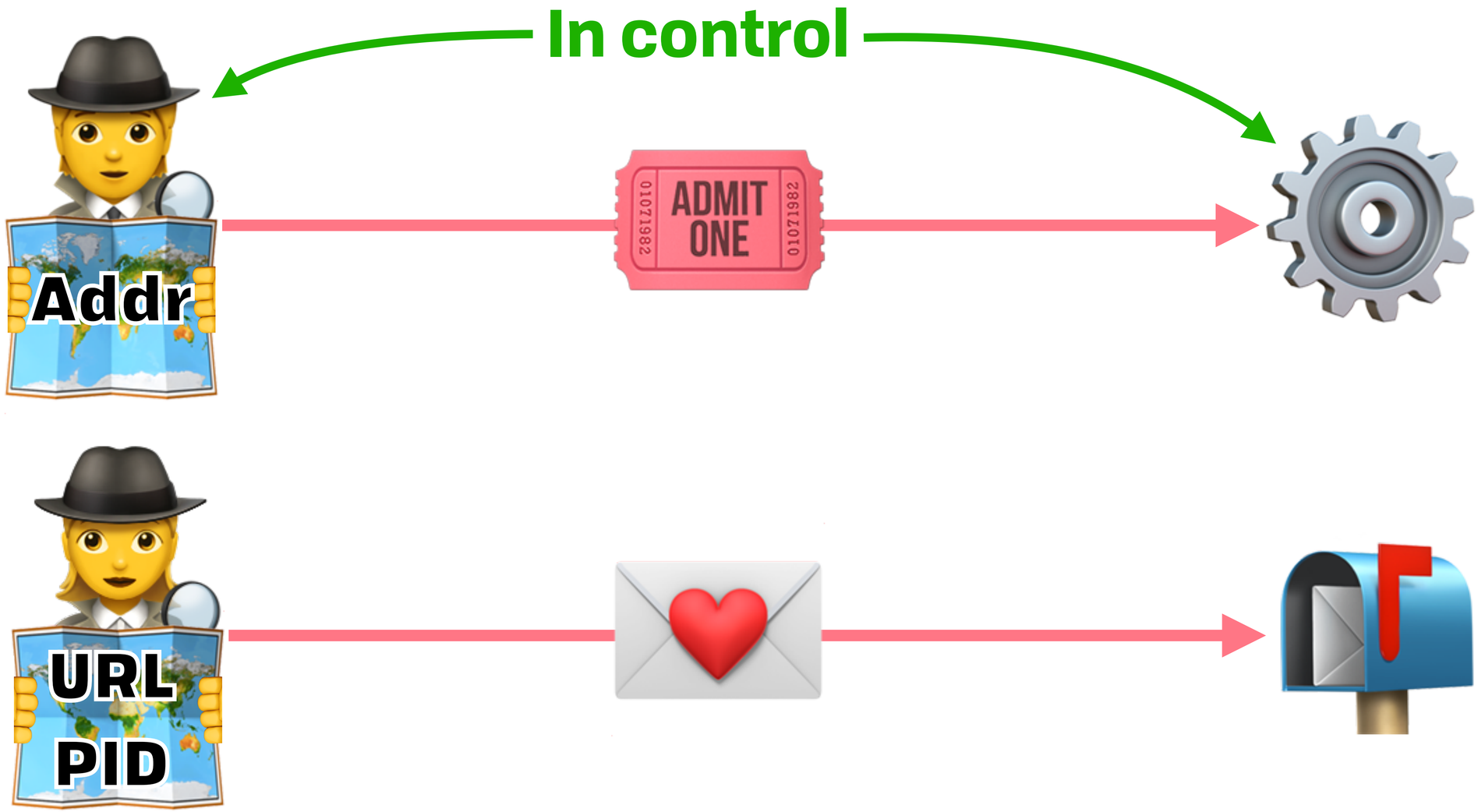
UCAN

From Actors to Capabilities



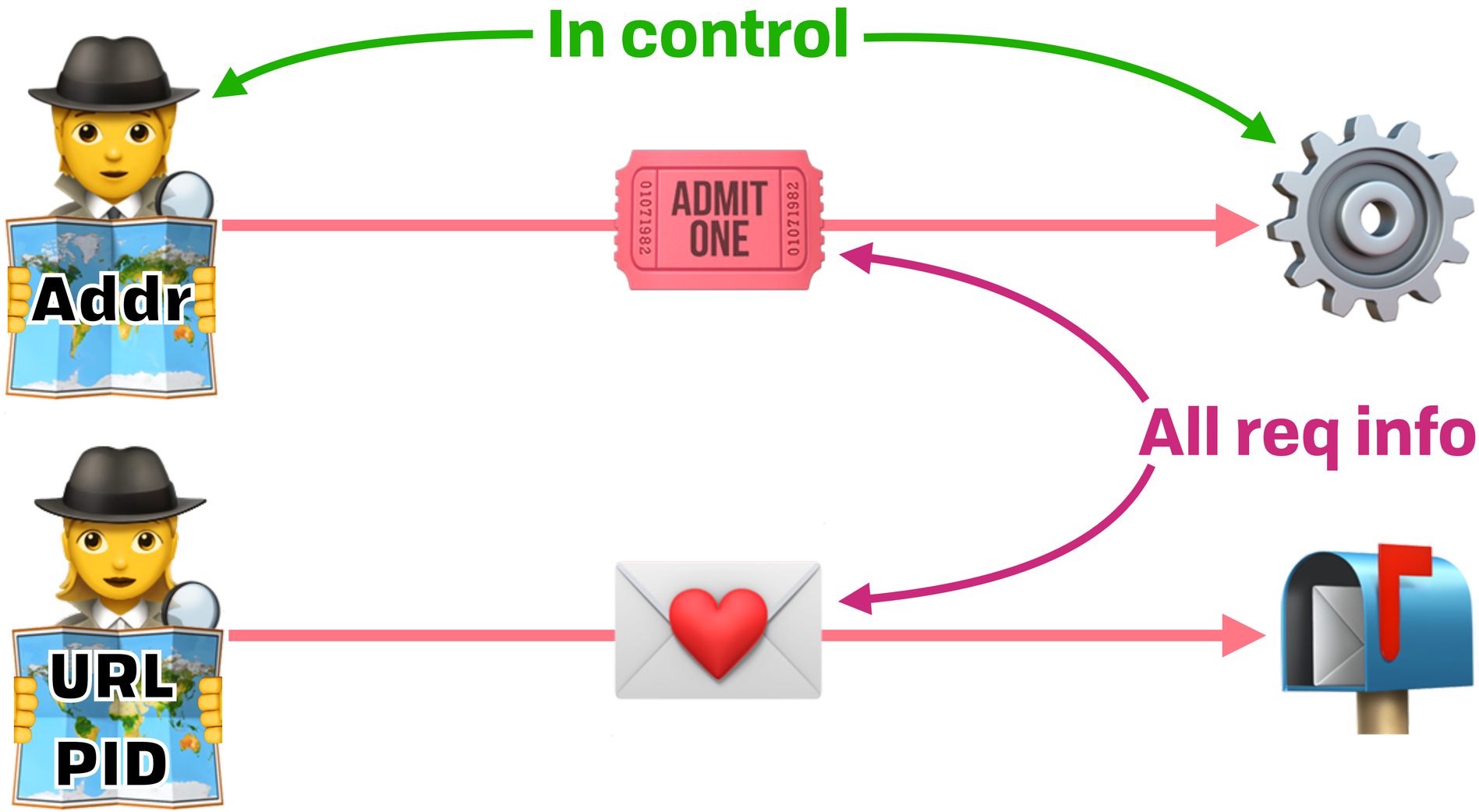
UCAN

From Actors to Capabilities



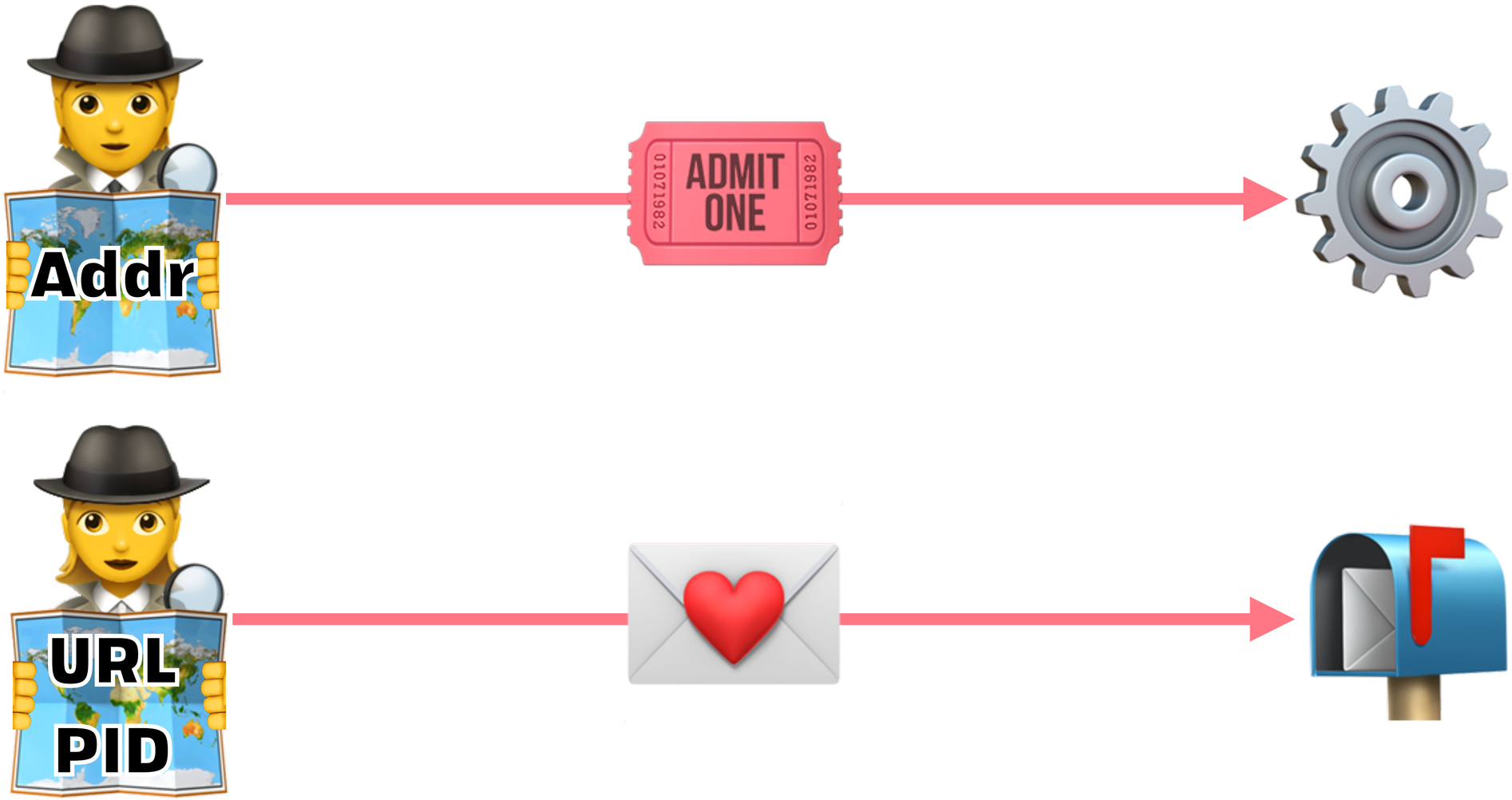
UCAN

From Actors to Capabilities



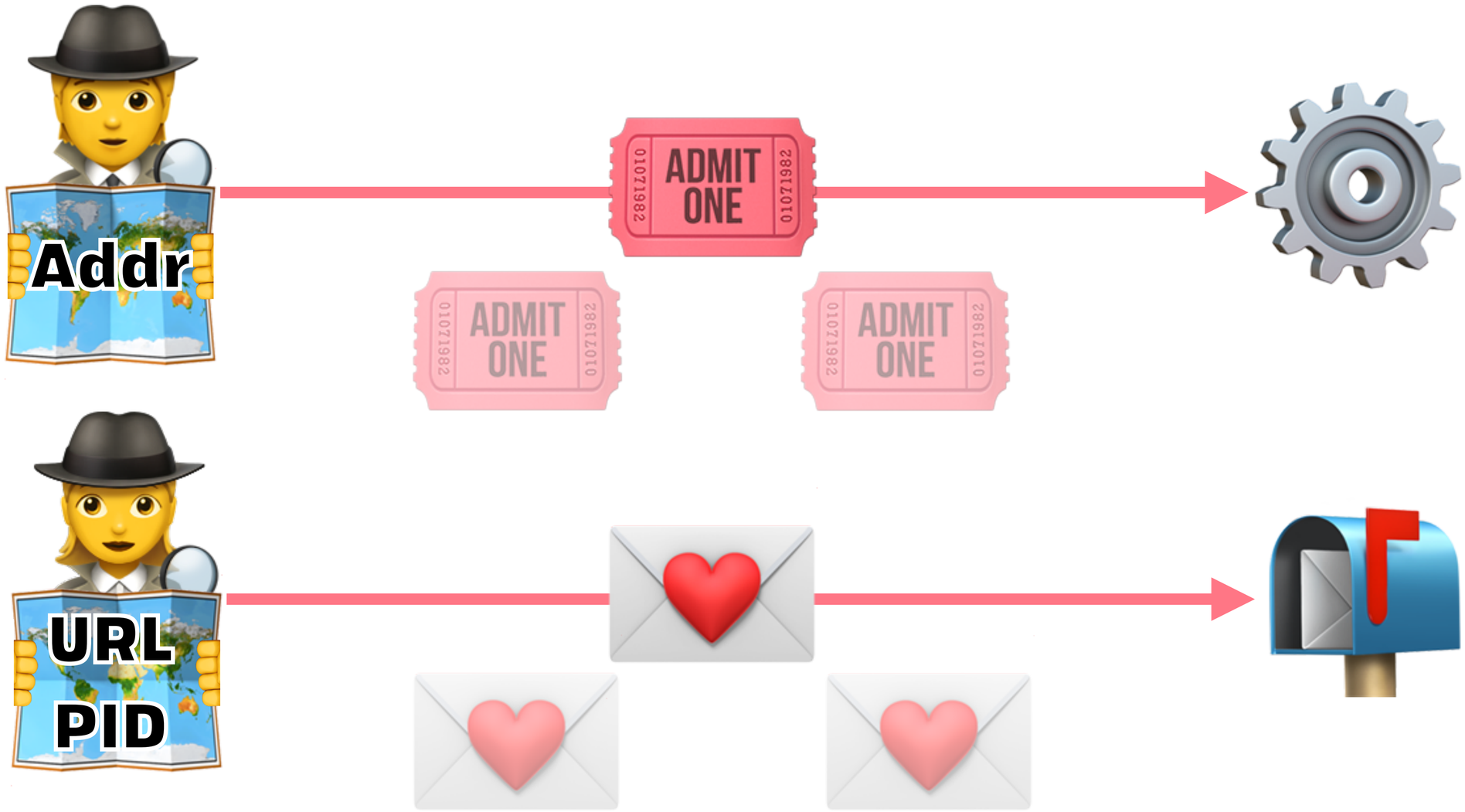
UCAN

From Actors to Capabilities



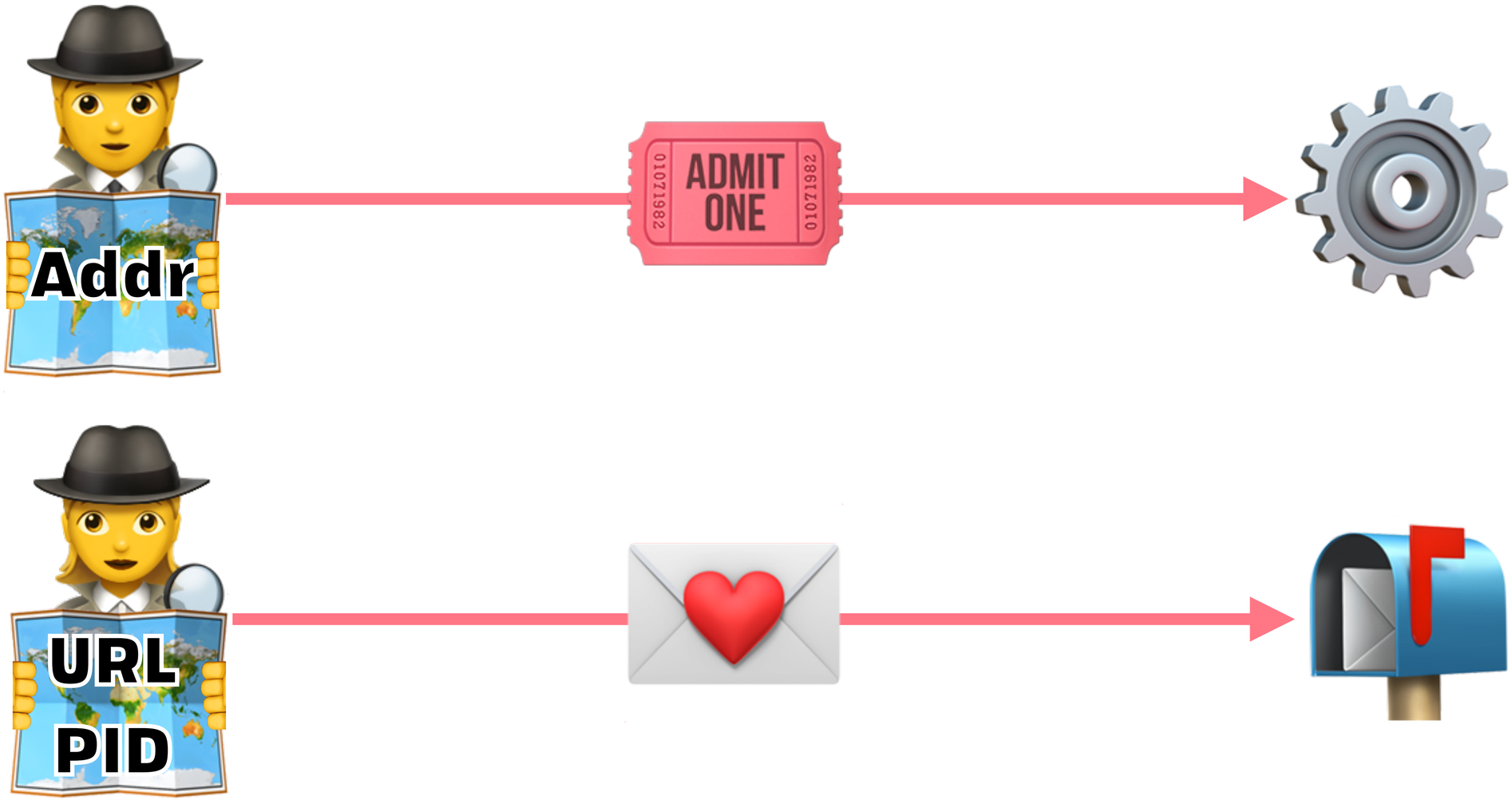
UCAN

From Actors to Capabilities



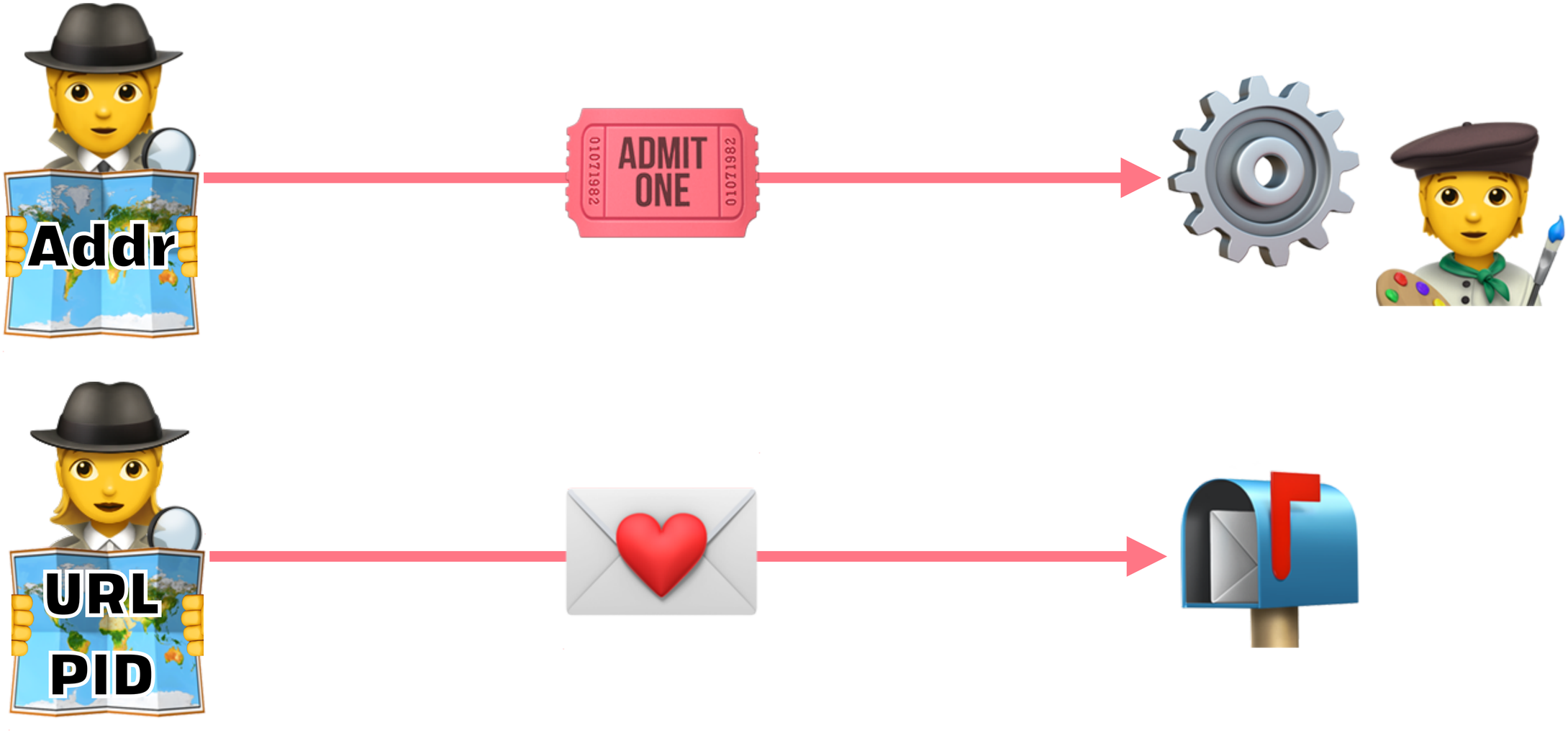
UCAN

From Actors to Capabilities



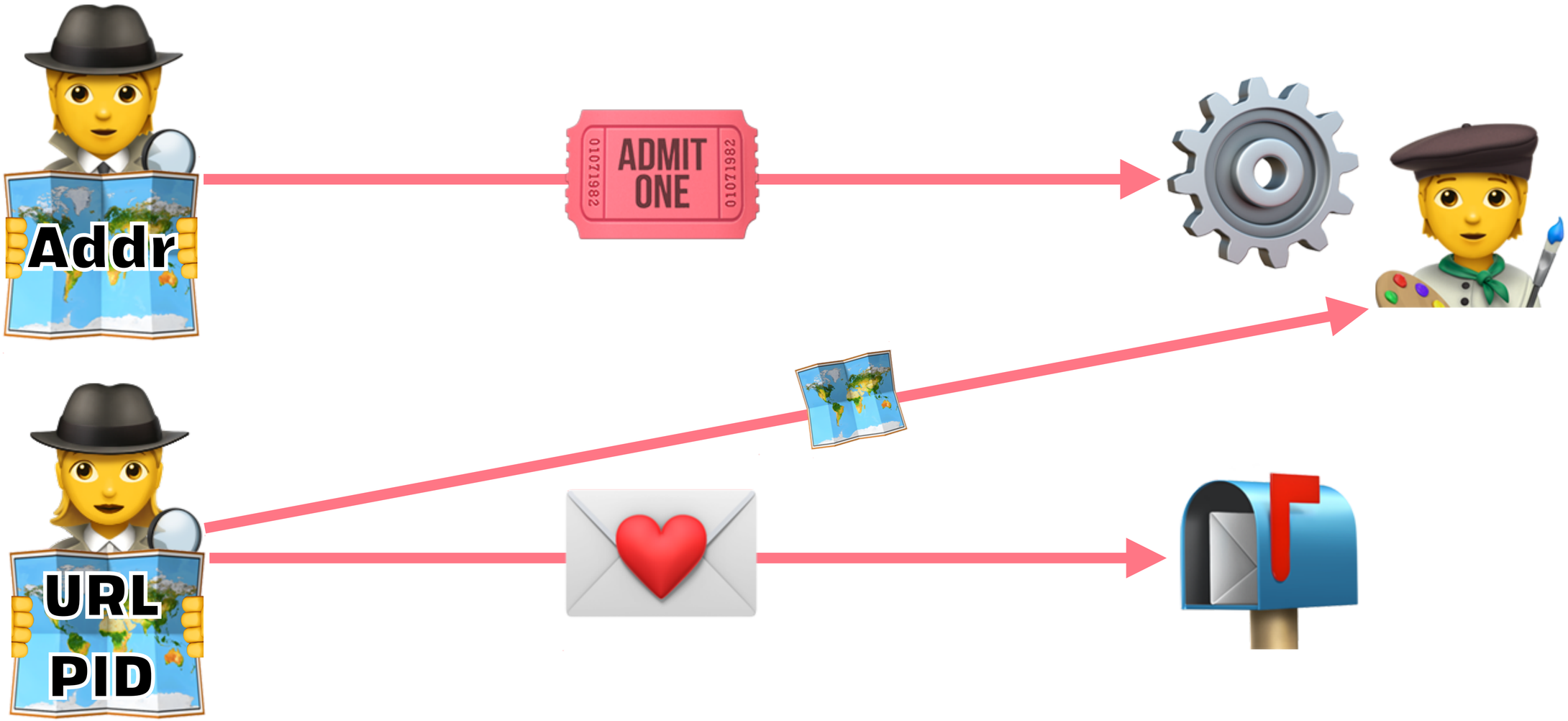
UCAN

From Actors to Capabilities



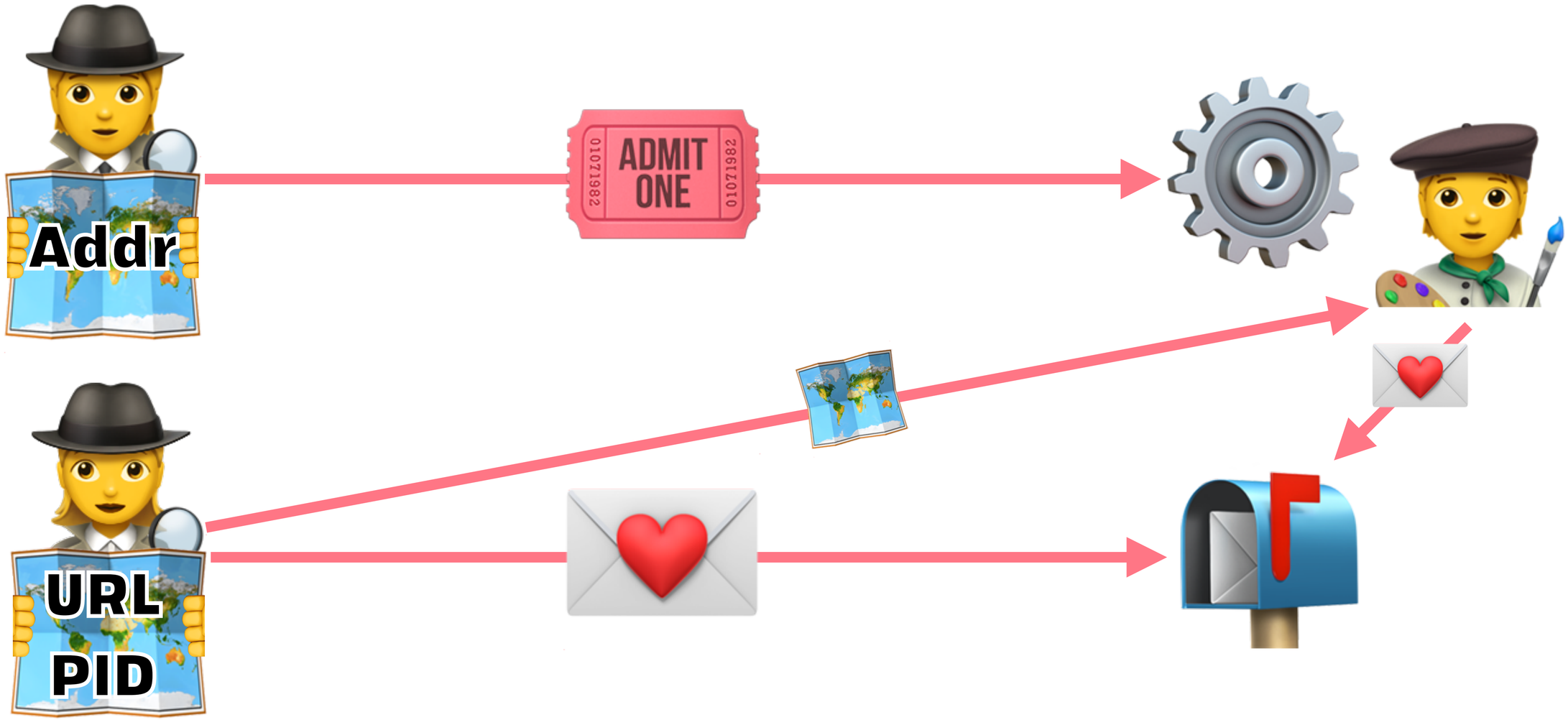
UCAN

From Actors to Capabilities



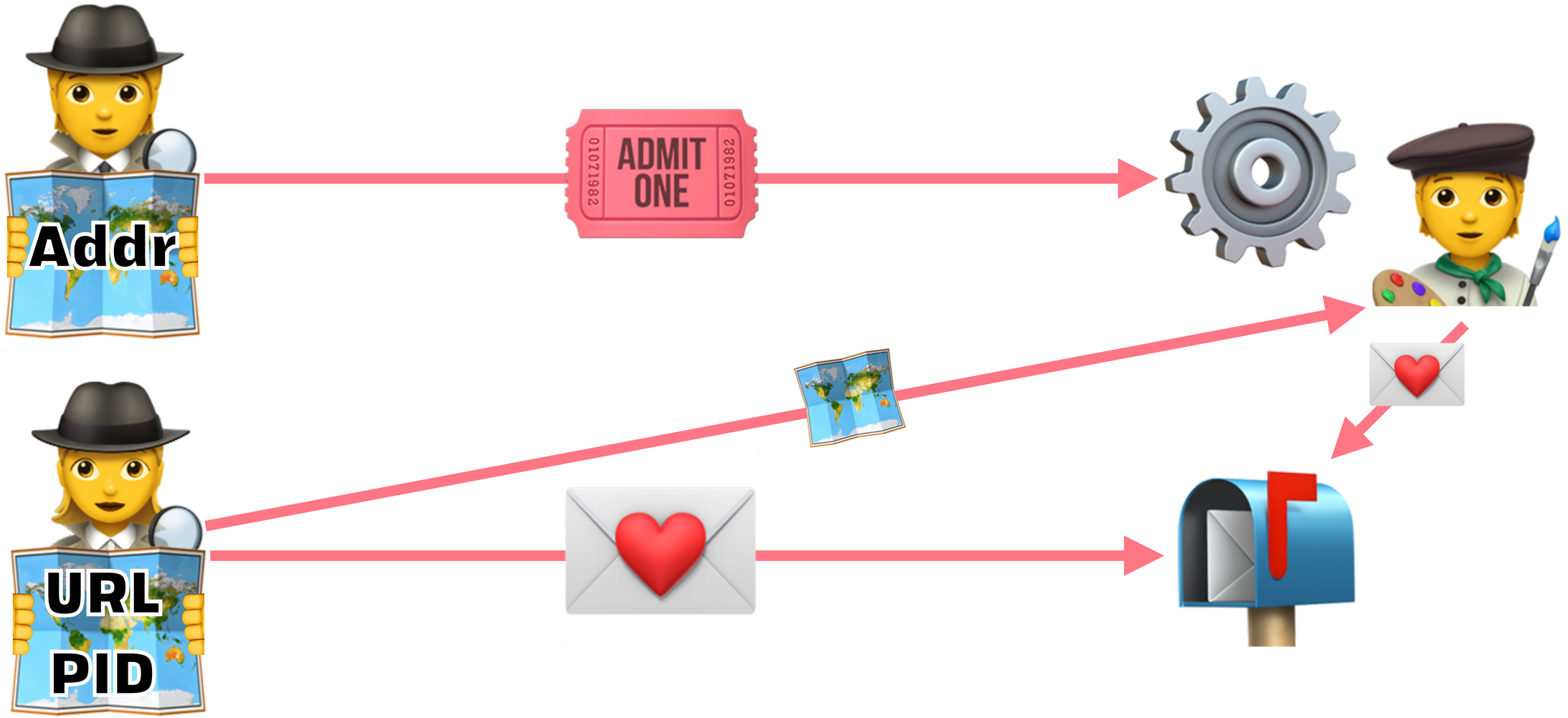
UCAN

From Actors to Capabilities



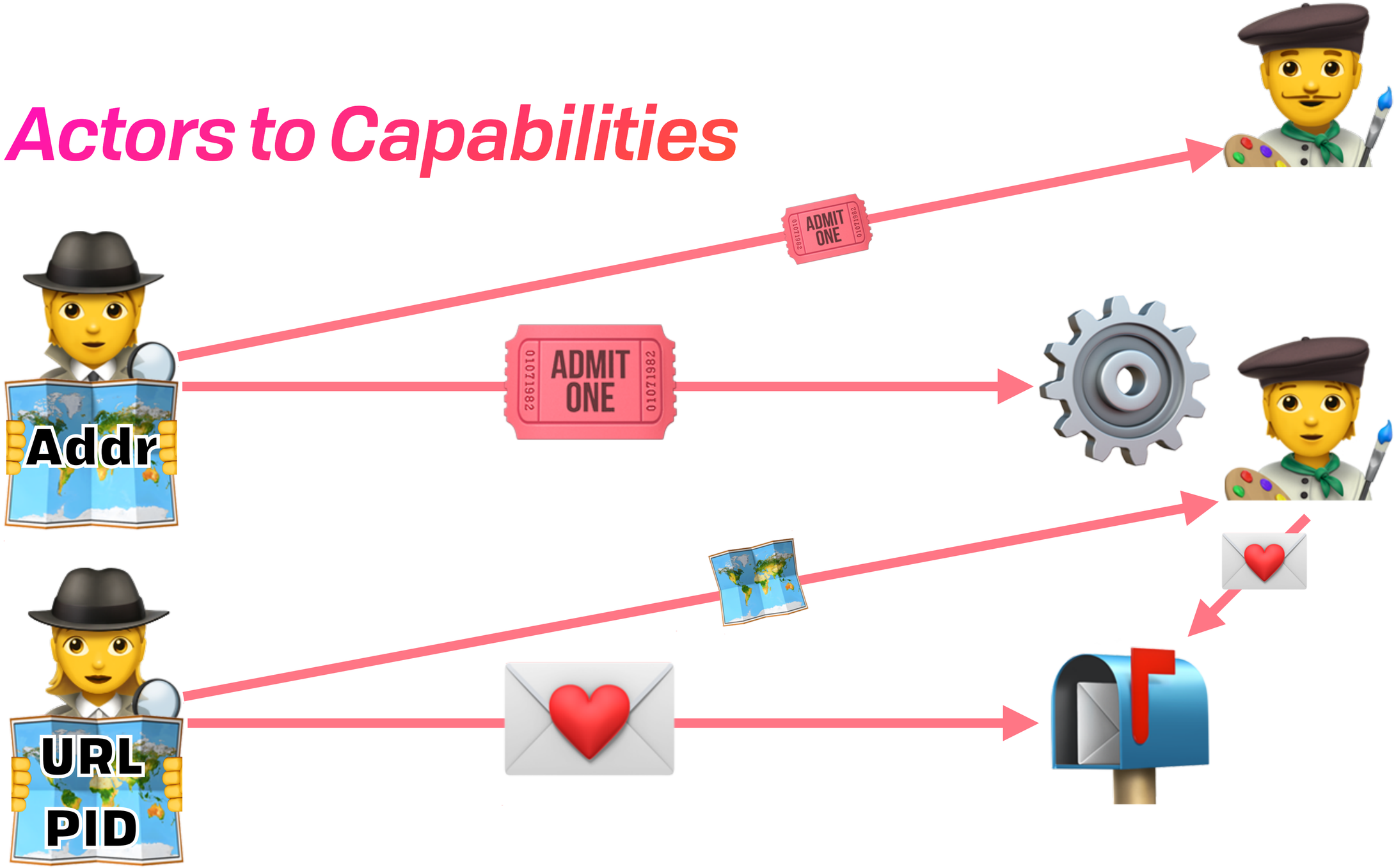
UCAN

From Actors to Capabilities



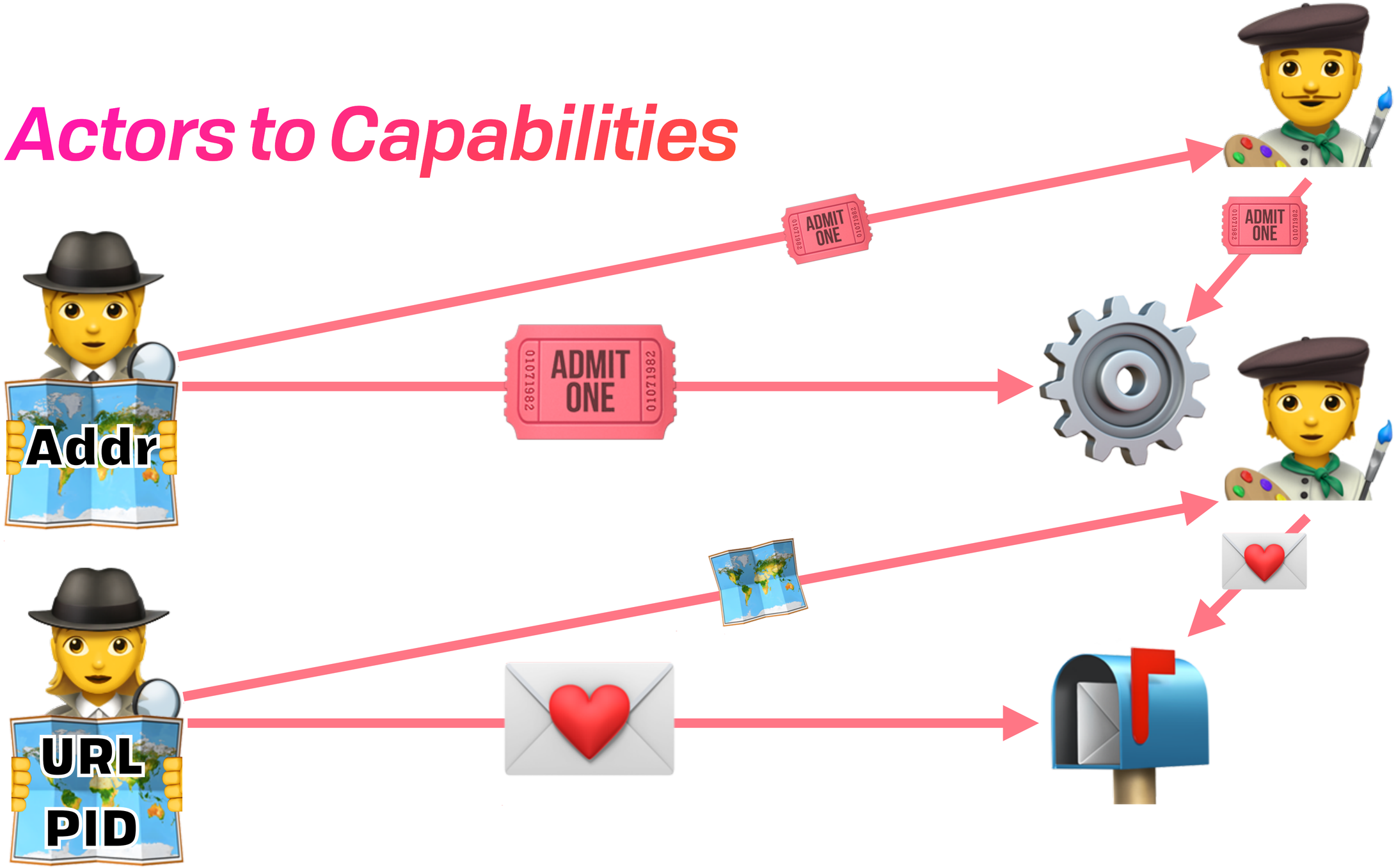
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

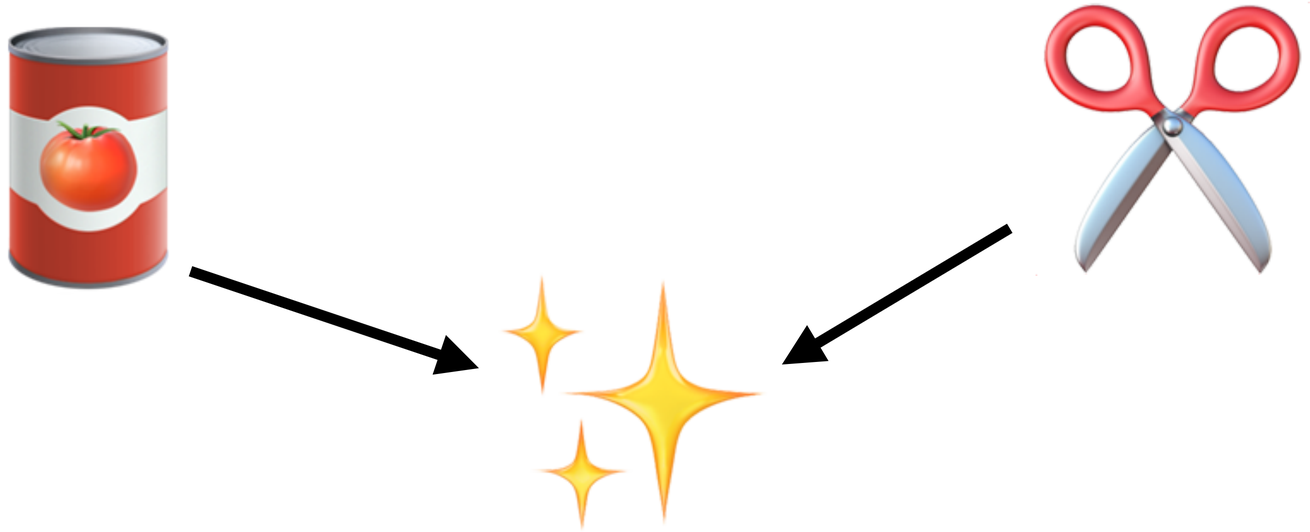
Rights Amplification

UCAN

Rights Amplification

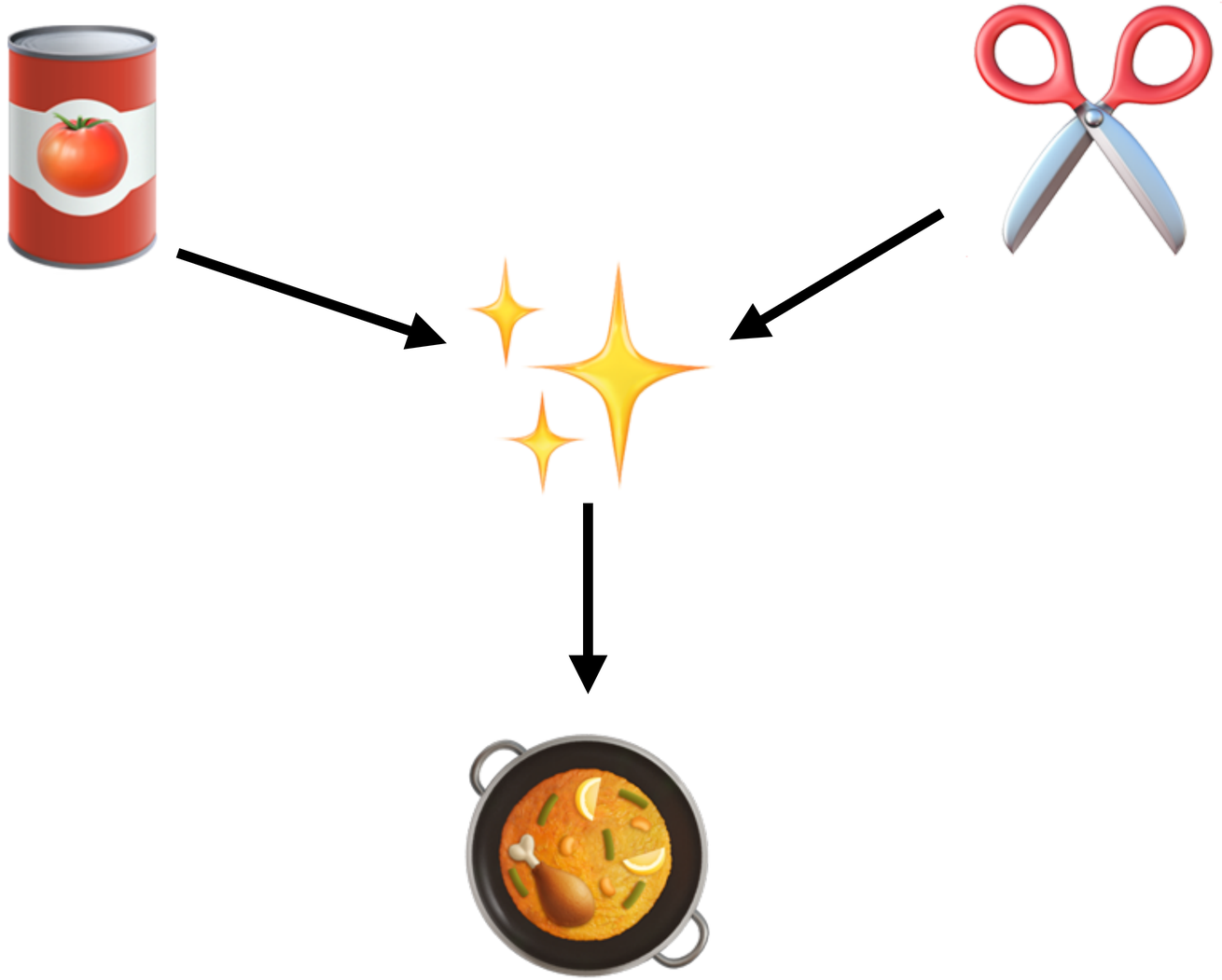
UCAN

Rights Amplification



UCAN

Rights Amplification



UCAN

JWT → UCAN

UCAN

JWT → UCAN

Header

```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```

UCAN

JWT → UCAN

Header

```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```

Payload

```
{
  "iss":
"did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "aud":
"did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
  "nbf": 1639608293,
  "exp": 9256939505,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/photos/",
      "can": "OVERWRITE"
    },
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "APPEND"
    }
  ]
}
```

UCAN

JWT → UCAN

Header

```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```

Payload

```
{
  "iss":
"did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "aud":
"did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
  "nbf": 1639608293,
  "exp": 9256939505,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/photos/",
      "can": "OVERWRITE"
    },
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "APPEND"
    }
  ]
}
```

Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

UCAN

JWT → UCAN

Header

```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```

Payload

```
{
  "iss":
"did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "aud":
"did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
  "nbf": 1639608293,
  "exp": 9256939505,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/photos/",
      "can": "OVERWRITE"
    },
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "APPEND"
    }
  ]
}
```

✅

Signature

```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

UCAN

Anatomy of a Capability

UCAN

Anatomy of a Capability

```
[
  {
     "with": "http://example.com/alice/photos/",
     "can": "GET"
  },
  {
    "with": "mailto:boris@fission.codes",
    "can": "SEND",
    "to": "/.*@fission.codes/"
  }
]
```

UCAN

Anatomy of a Capability

Resource / "noun"

```
[
  {
    "with": "http://example.com/alice/photos/",
    "can": "GET"
  },
  {
    "with": "mailto:boris@fission.codes",
    "can": "SEND",
    "to": "/.*@fission.codes/"
  }
]
```

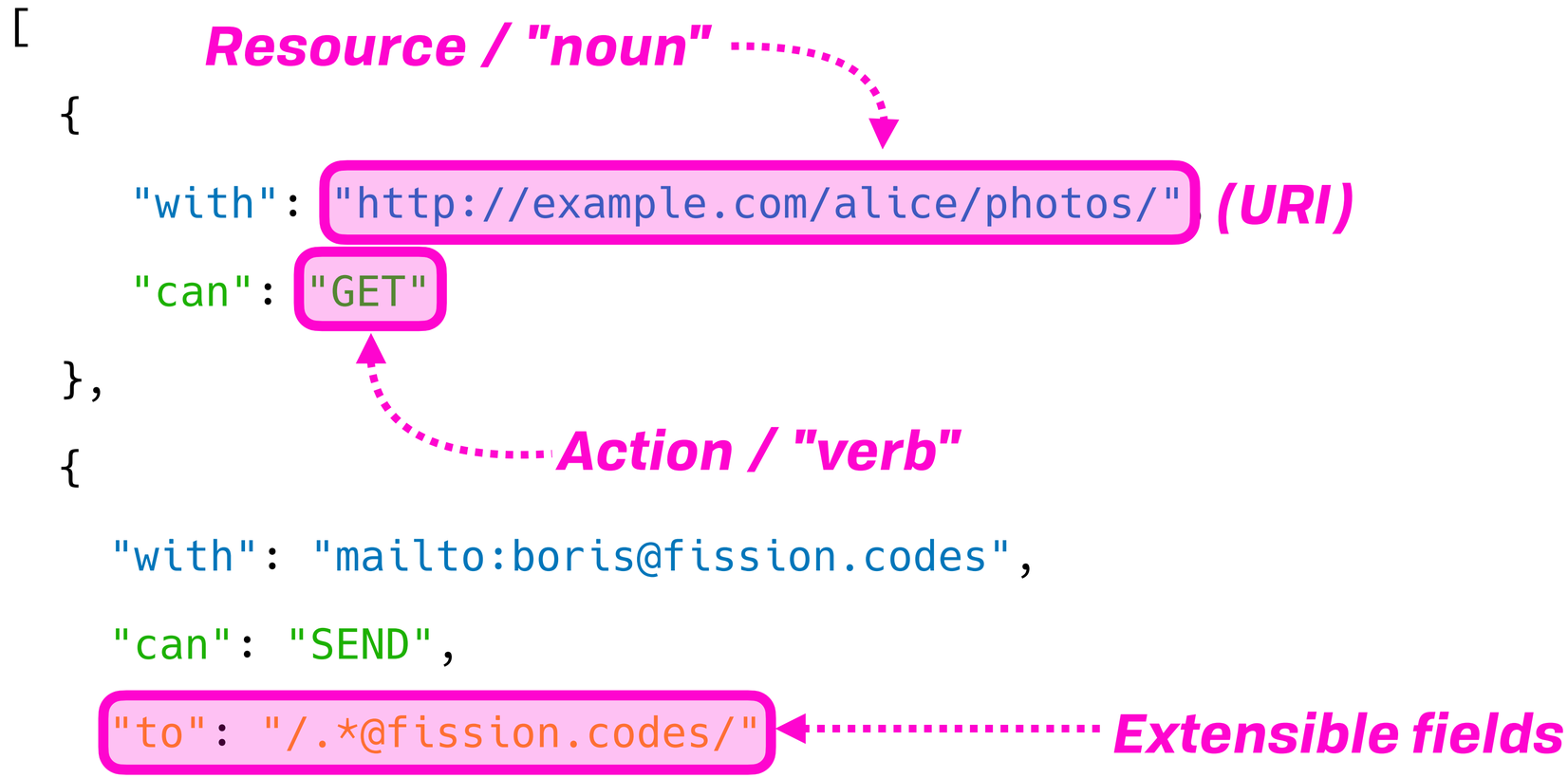
(URI)

UCAN

Anatomy of a Capability

UCAN

Anatomy of a Capability



UCAN

Chain Witnesses

UCAN

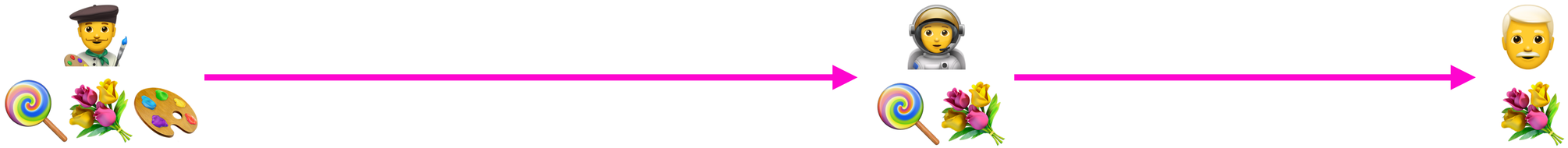
Chain Witnesses

UCAN

Chain Witnesses

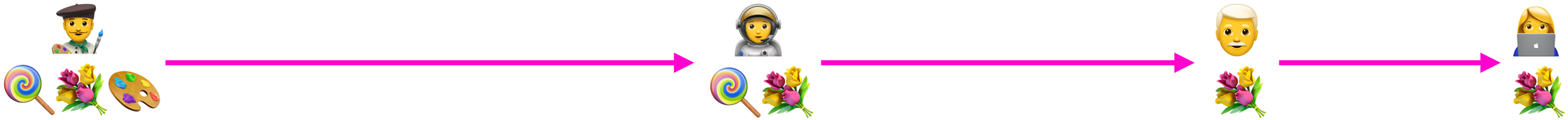
UCAN

Chain Witnesses



UCAN

Chain Witnesses

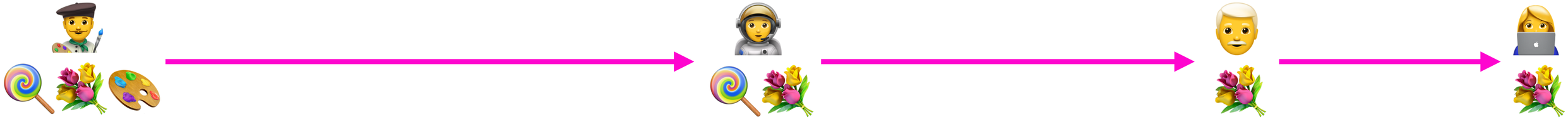


UCAN

Chain Witnesses

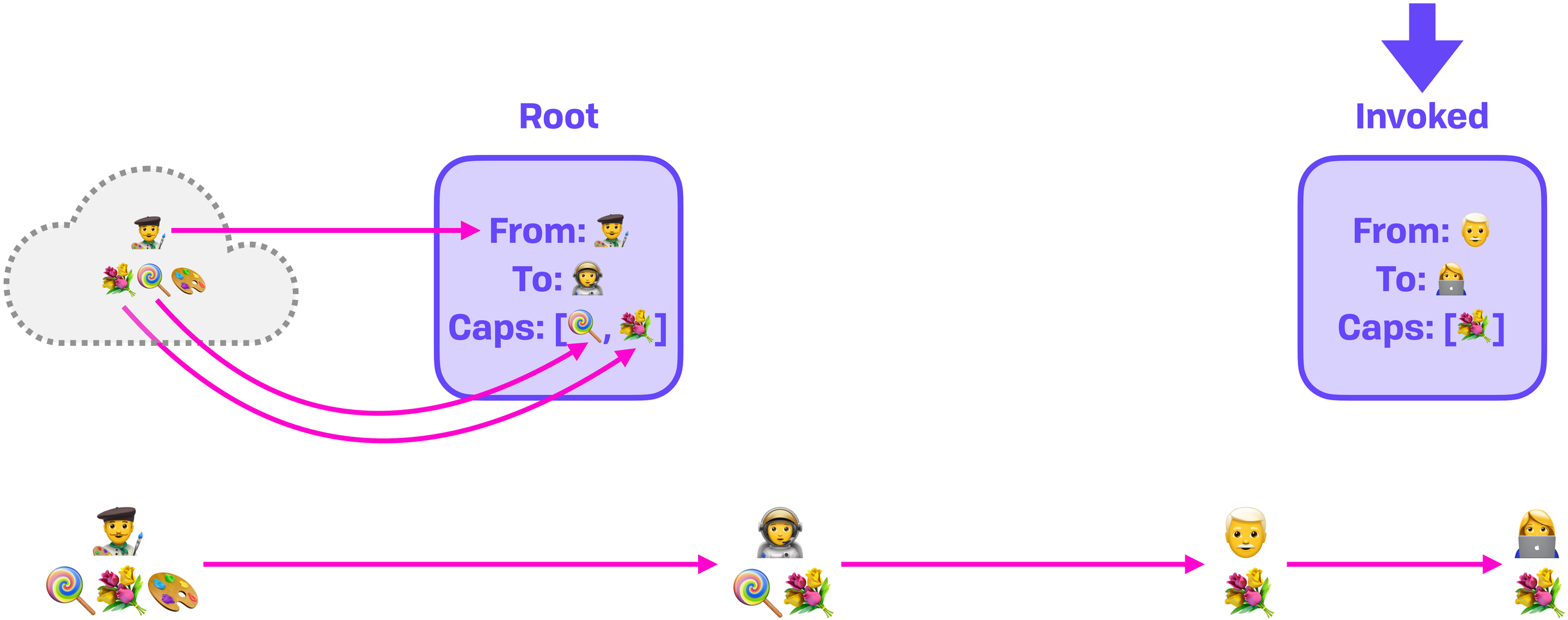
Invoked

From: 👴
To: 👩‍💻
Caps: [💐]



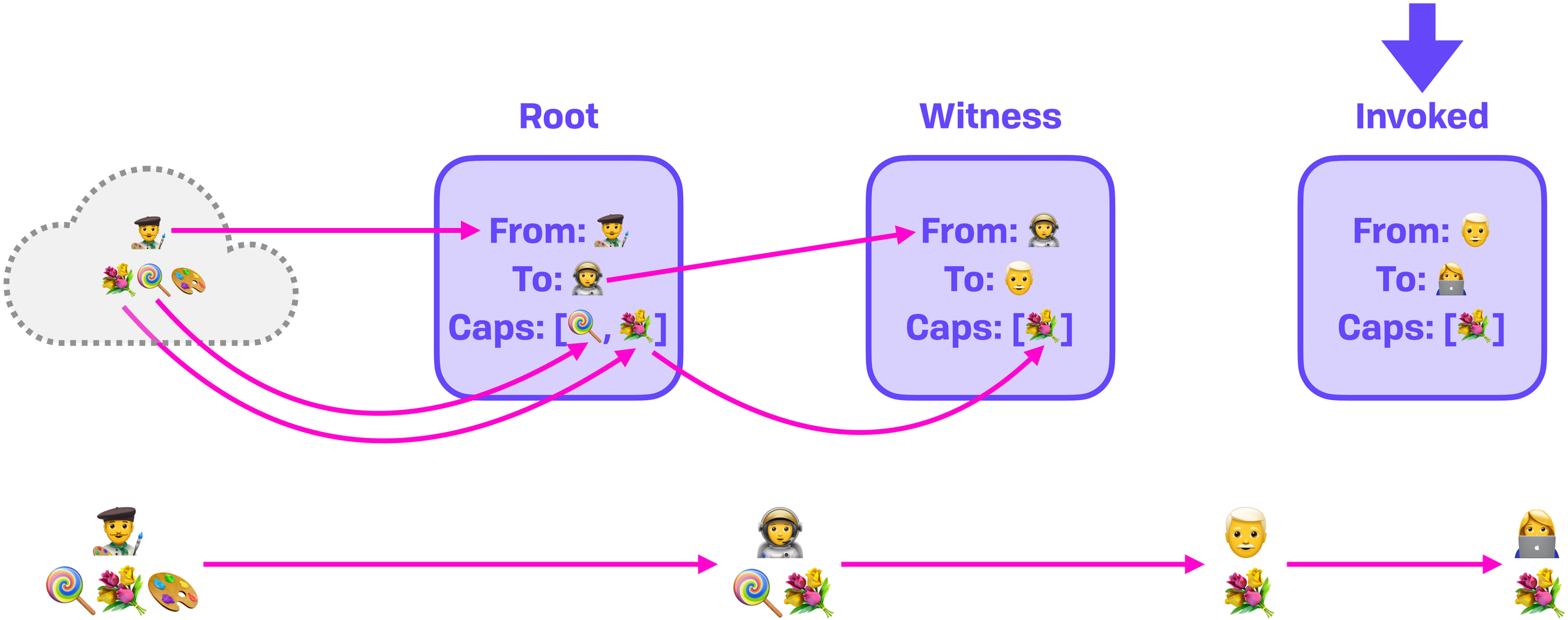
UCAN

Chain Witnesses



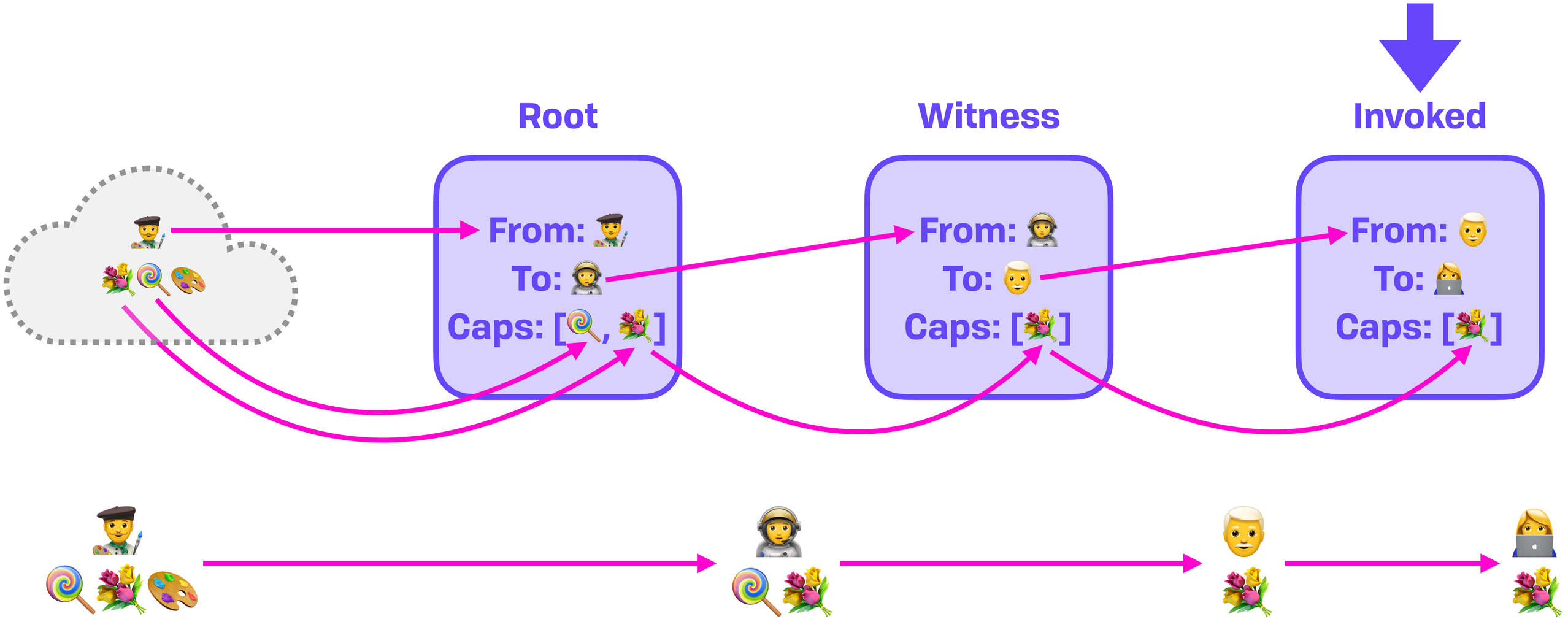
UCAN

Chain Witnesses



UCAN

Chain Witnesses



UCAN

Zoomed Out

UCAN

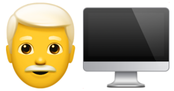
Zoomed Out

UCAN

Zoomed Out

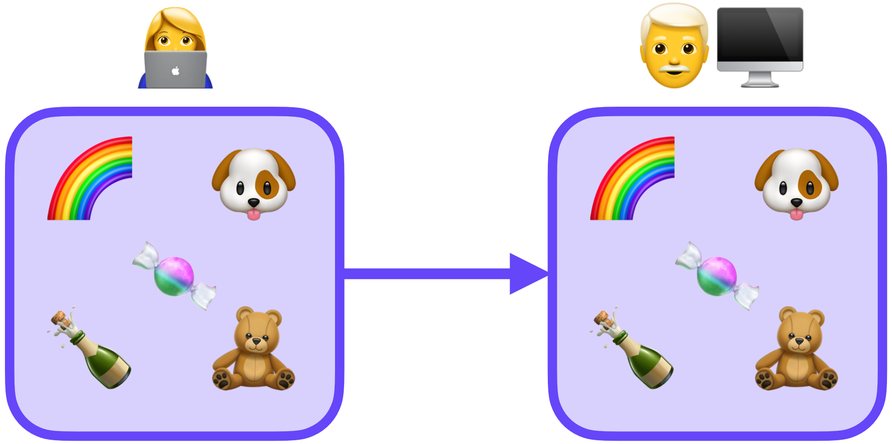
UCAN

Zoomed Out



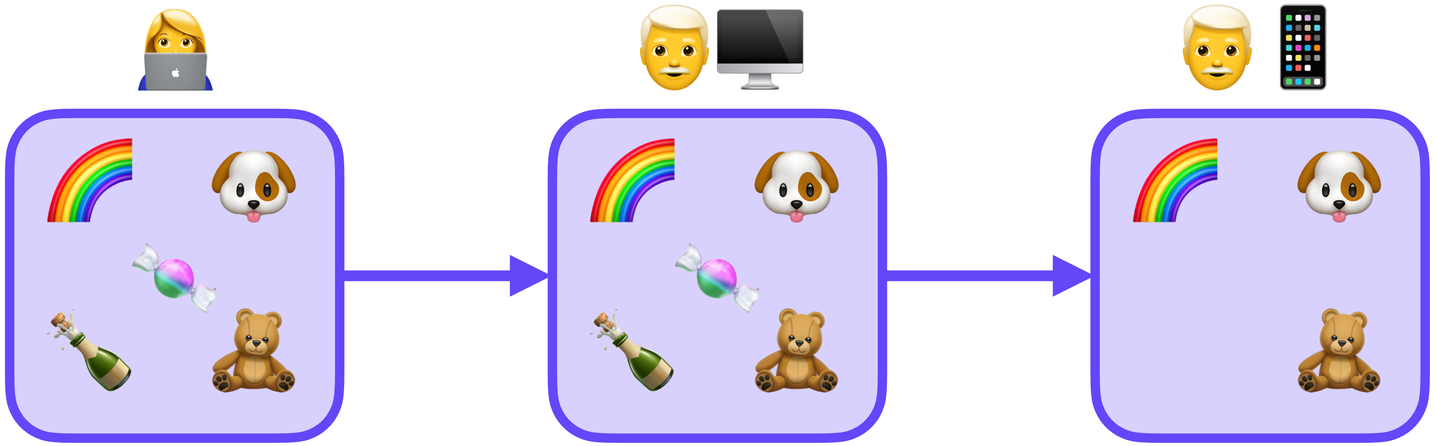
UCAN

Zoomed Out



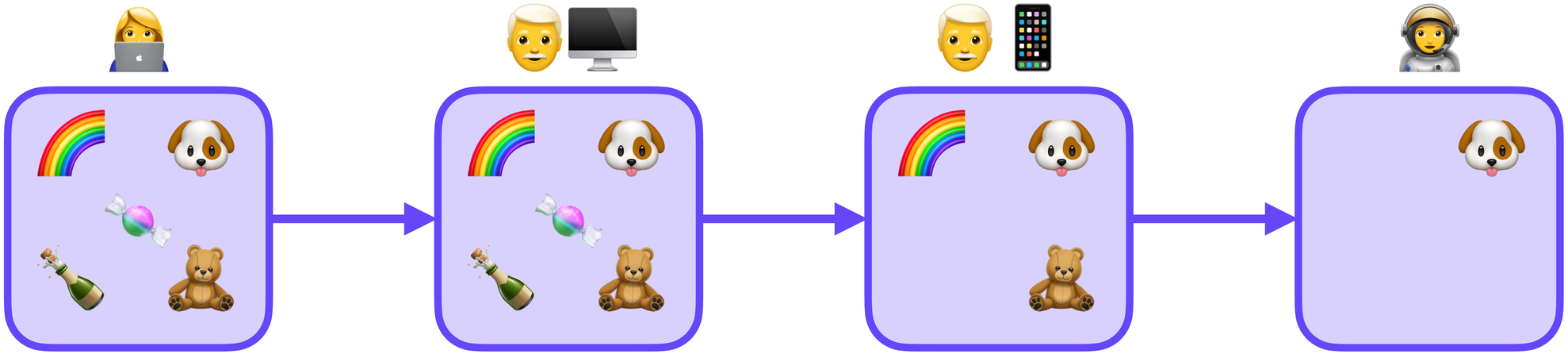
UCAN

Zoomed Out



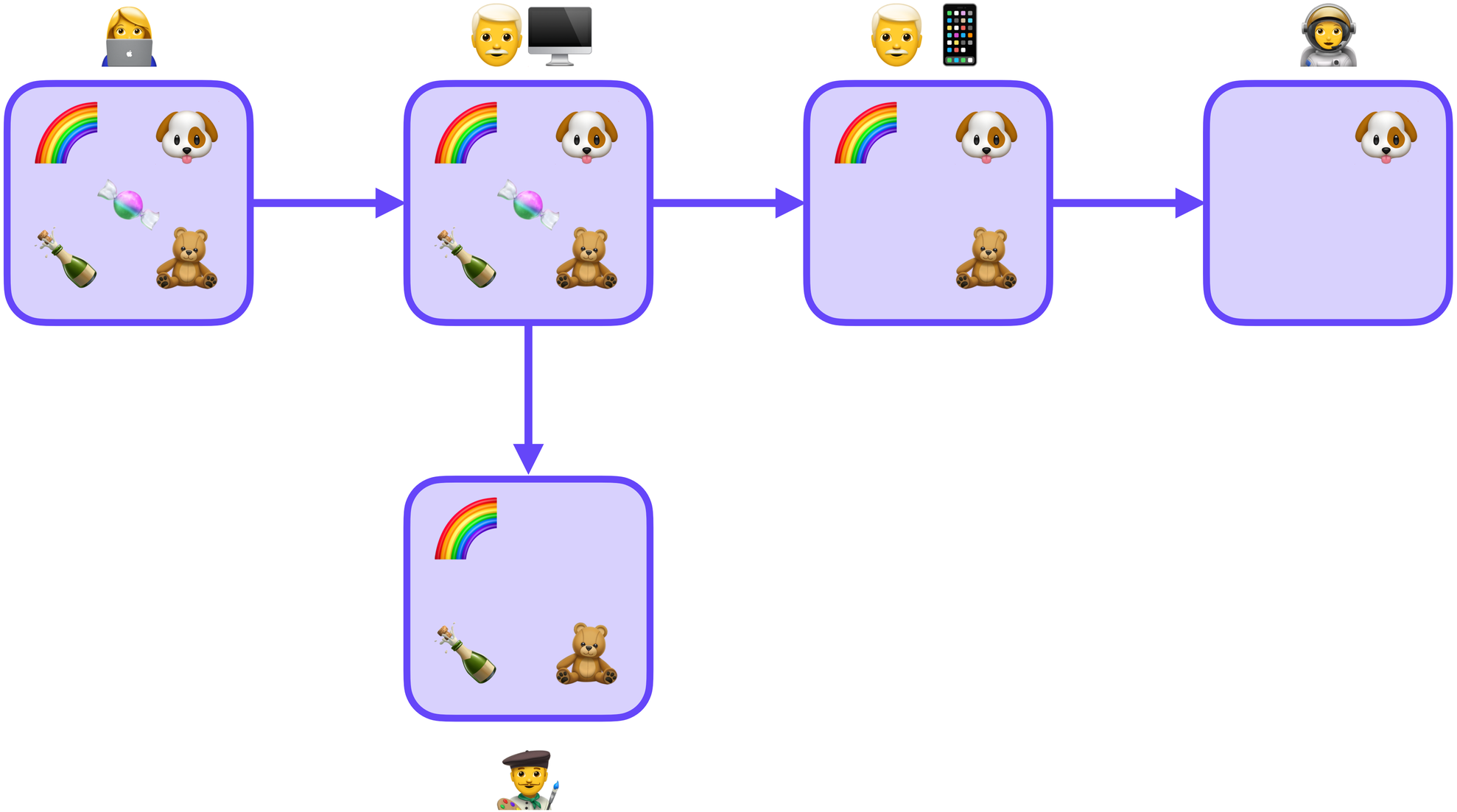
UCAN

Zoomed Out



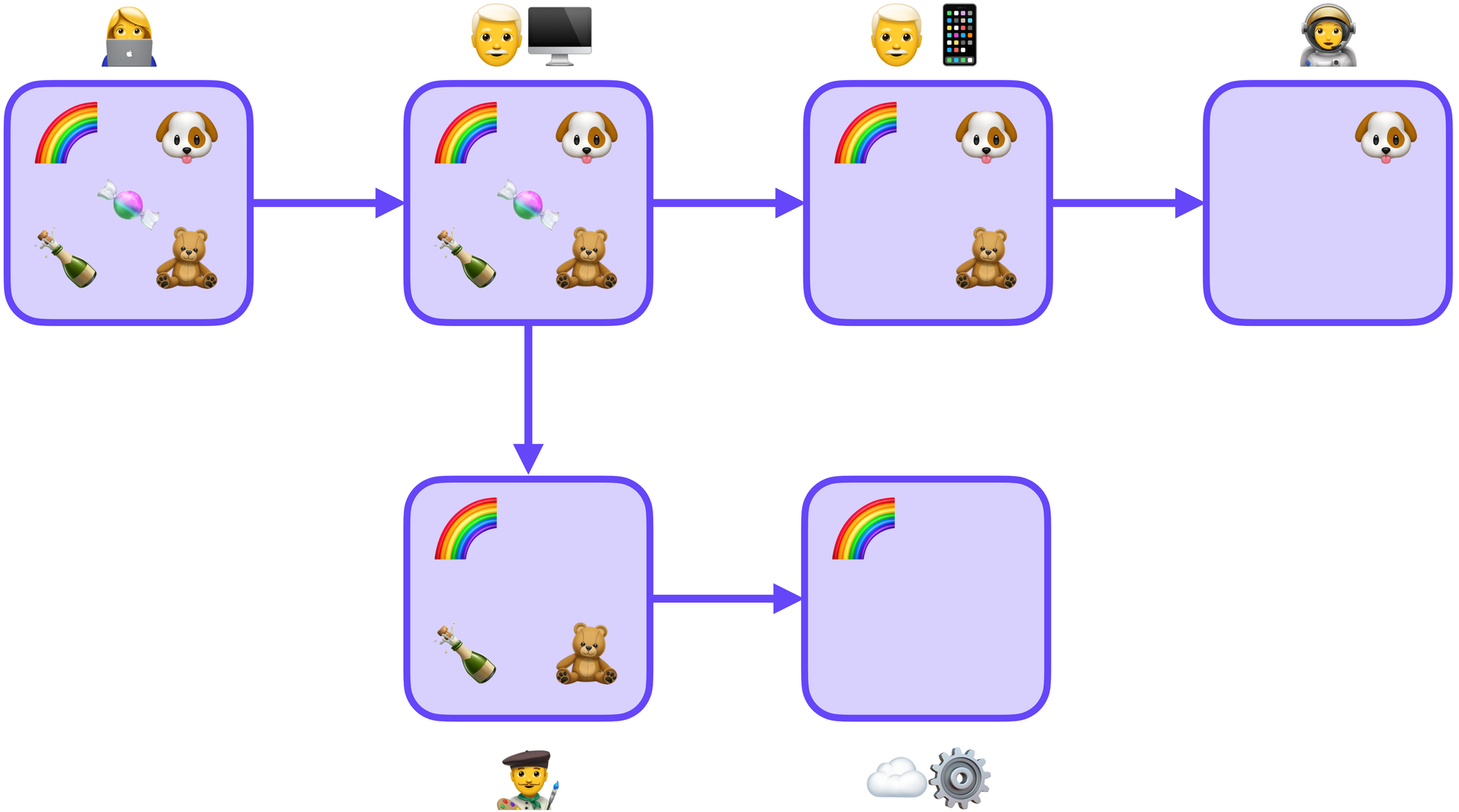
UCAN

Zoomed Out



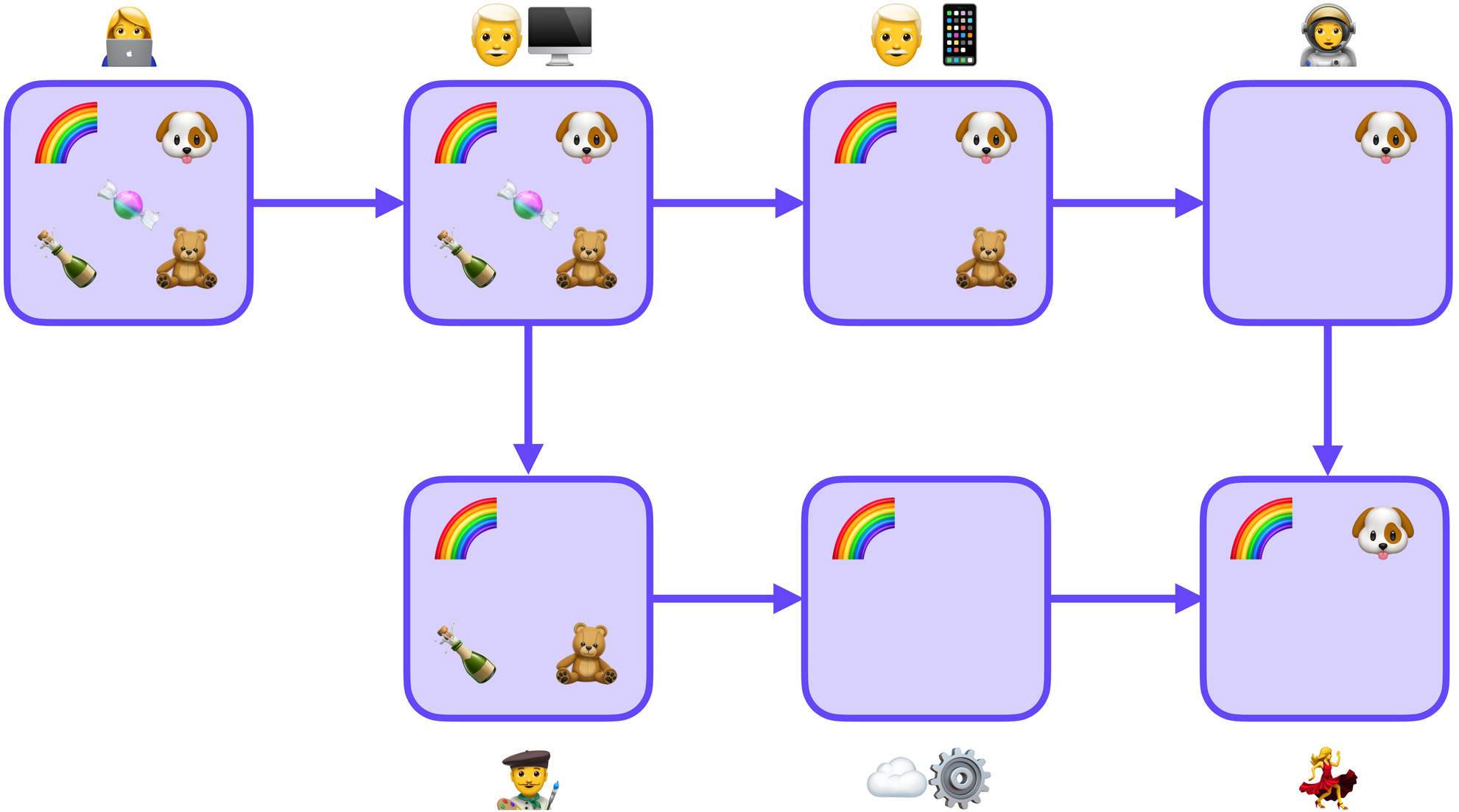
UCAN

Zoomed Out



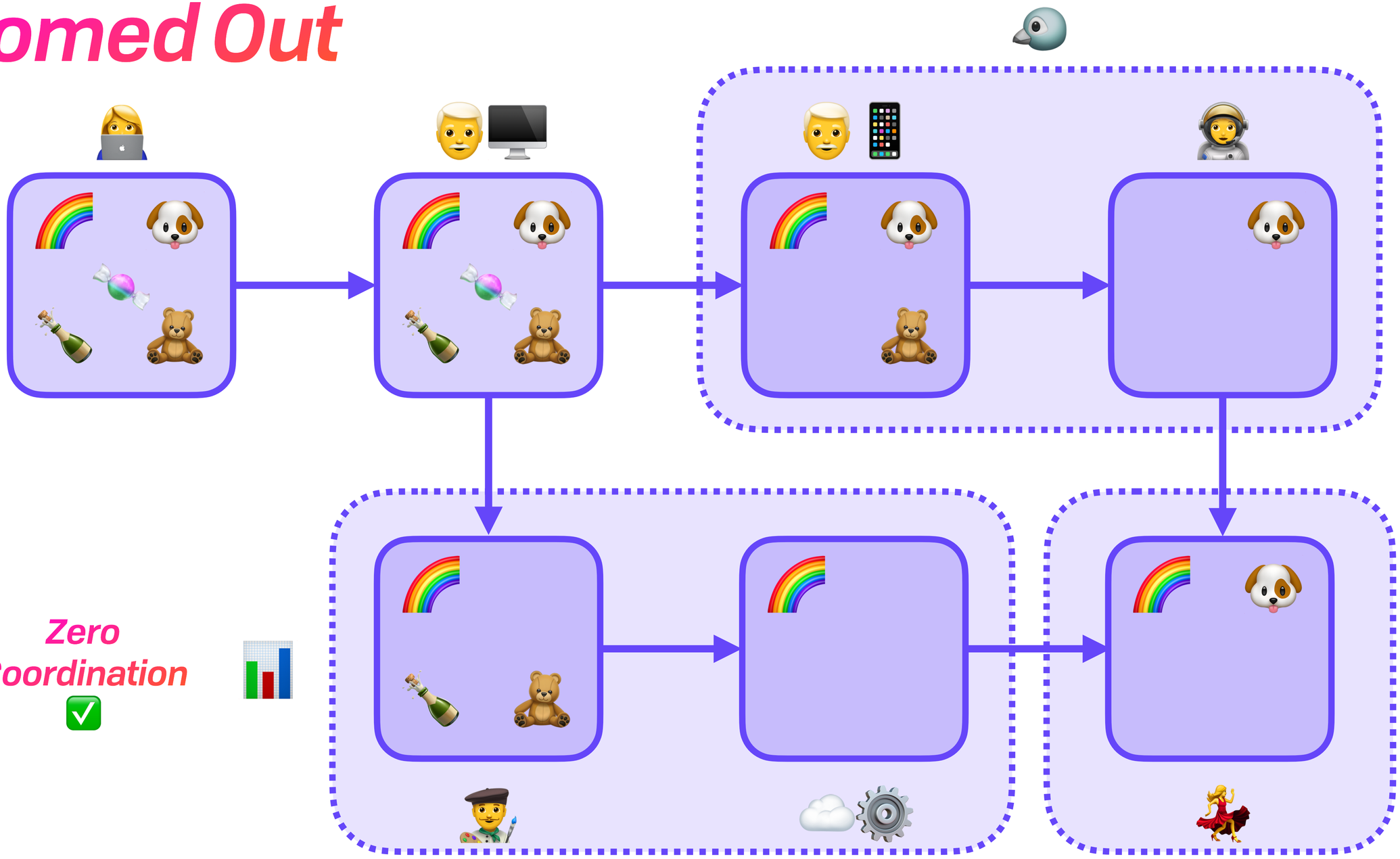
UCAN

Zoomed Out



UCAN

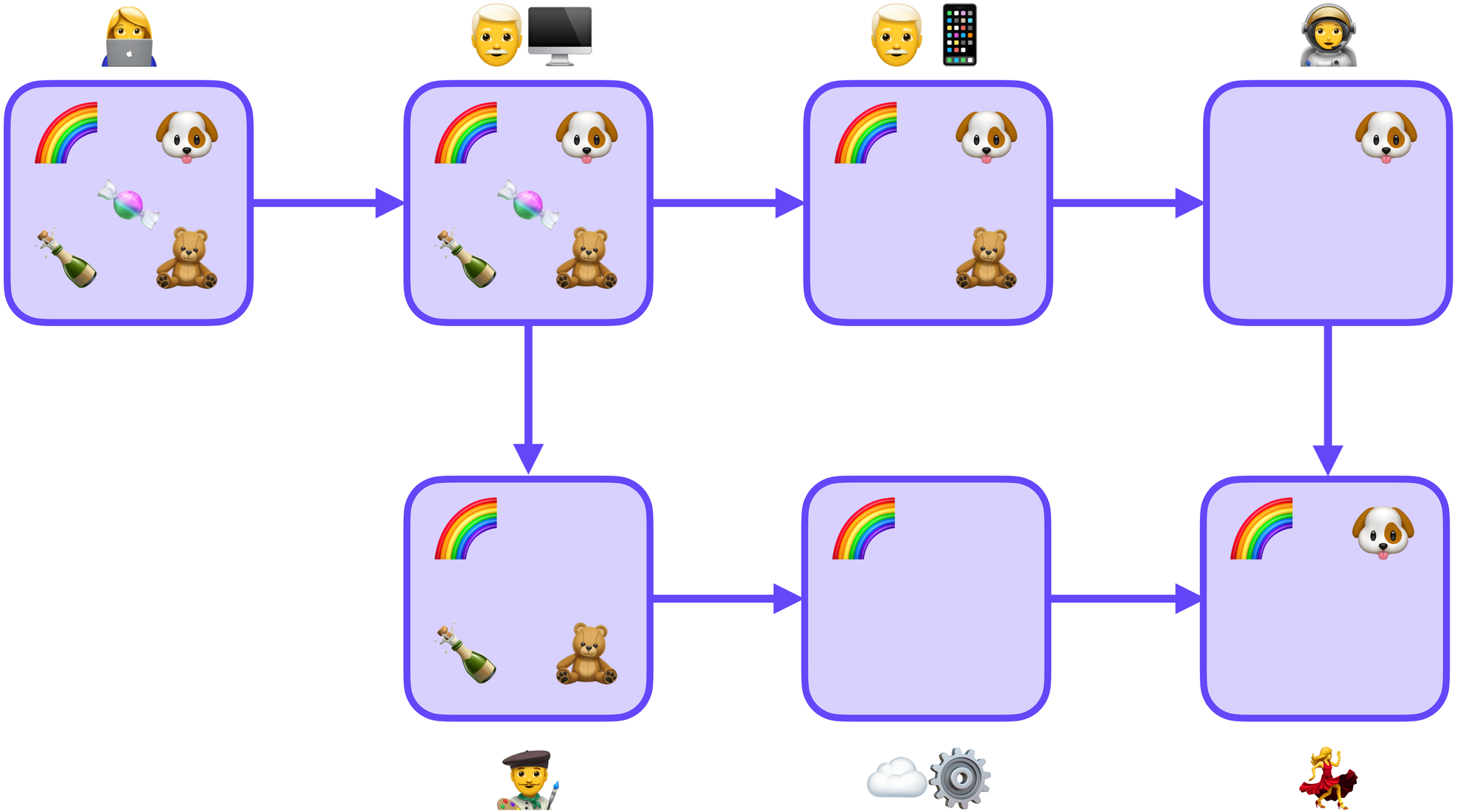
Zoomed Out



Zero Coordination ✅

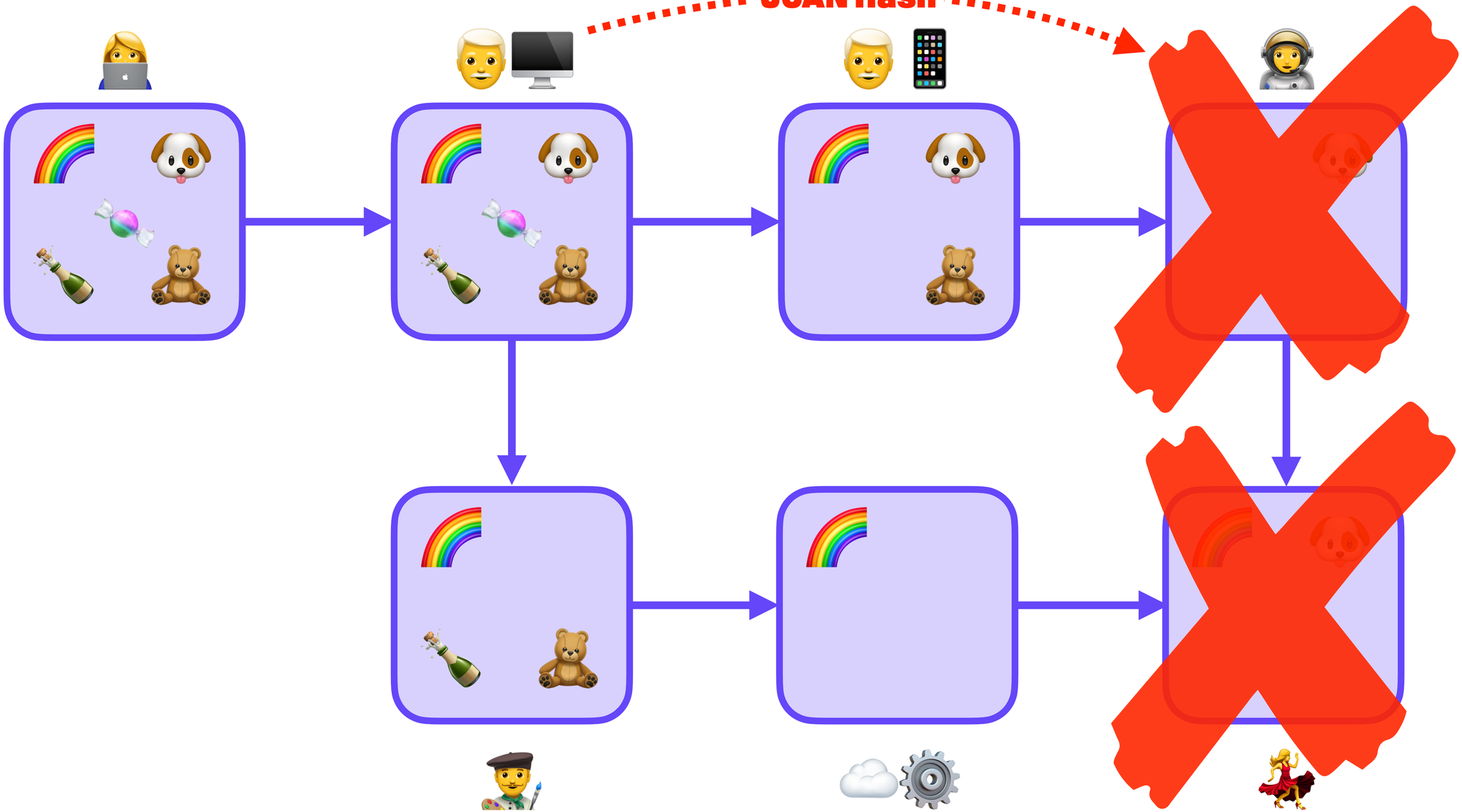
UCAN

Revocation Cascade



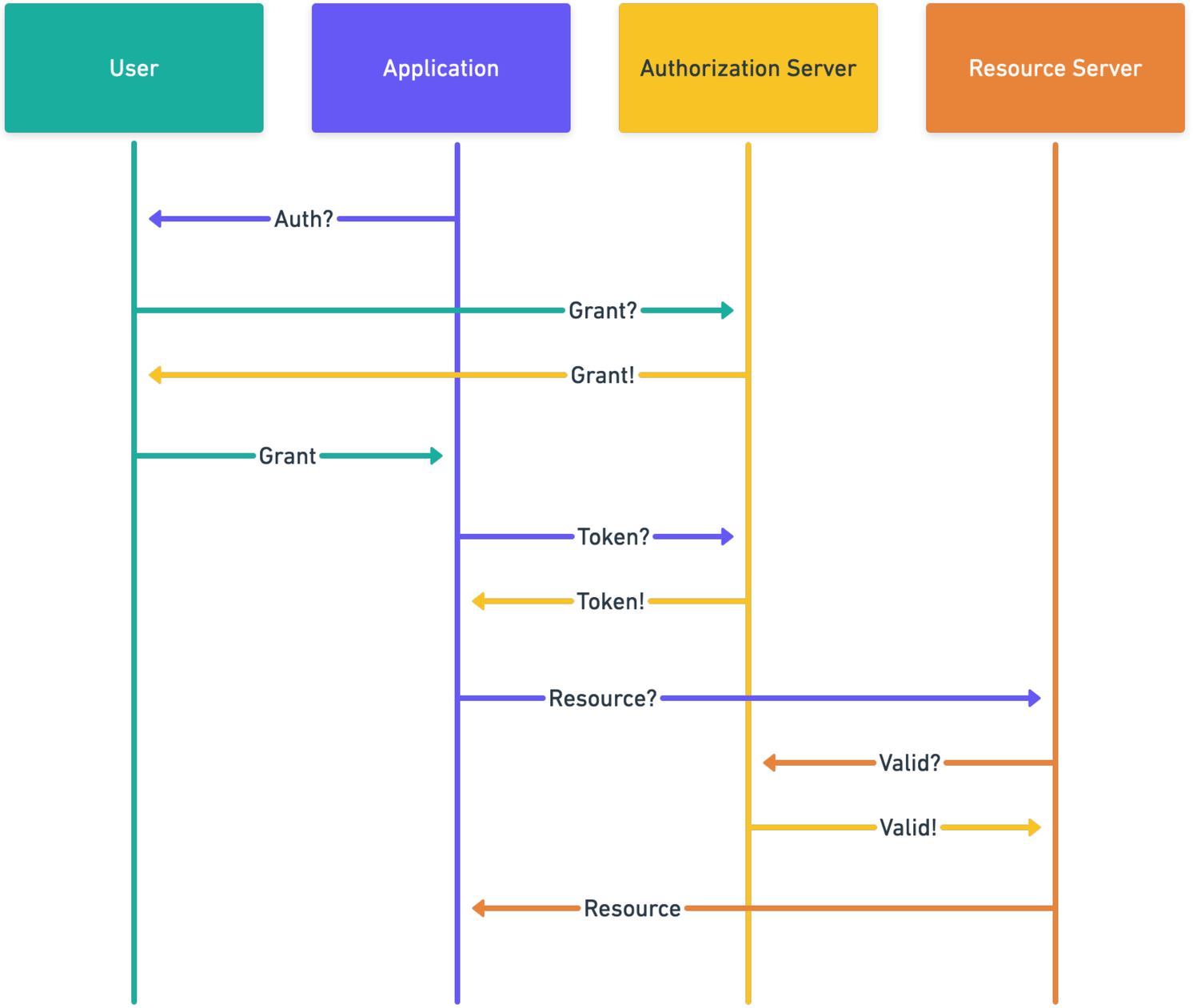
UCAN

Revocation Cascade



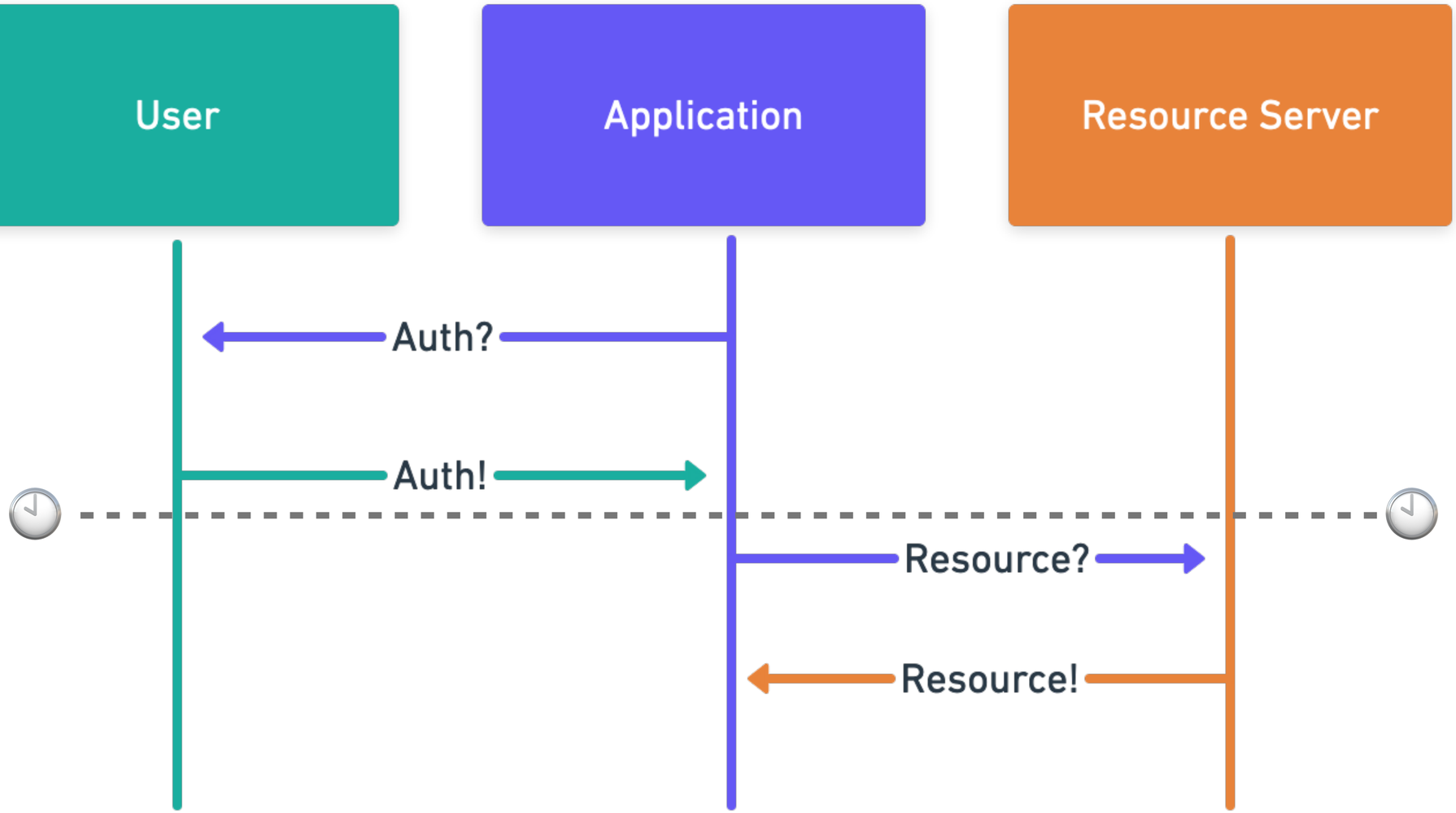
UCAN

OAuth Sequence



UCAN

UCAN Sequence



Nontrivial Example

Nontrivial Example

Encoded

Nontrivial Example

Encoded


```
eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V5Ono2T
Wt2WGZQVXY4Ynh0c1ZRaUdvN050azRxS0pOY2dLMml0NTJwYzczdGVVcFJMVCIsImF0dCI6W3sid25mcy
I6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhcCI6Ik9WRVJXUklURSJ9LHs
id25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiY2FwIjoiT1ZFUldSSVRF
In1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKVG03aE5SZ
jZiMThZeFhQcDNpNjZvSkhtOEwzWUdKIiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOlsiZXlKaGJHY2lPaU
pGWkVSVFFTSXNJblI1Y0NJNklrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E
2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnROMmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBJ
YlRoTU0xbEhTaUlzSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMyVnlMbVpwYzNOcGIyNHVibUZ0W
lM5d2RXSnNhV012Y0dodmRHOXpMeUlzSW1OaGNDSTZJazlXUlZKWFVrbFVSU0o5WFN3aVpYaHdJam81TW
pVMk9UTTVOVEExTENKcGMzTWlPaUprYVdRNmEyVjVPbm8yVFd0d05VVnplamx6TWsxSWMzRlpka3h2WTJ
ONVNIZFlOVk5sZVZwTGNIRTNPVWQwTkRWbVJrZEZXbEk1T1NJc0ltNWlaaUk2TVRZek9UWXdPREk1TXl3
aWNISm1JanBiWFgwLjRUTmh1SFJyUEc5YUhvODY5SFhsc05LOF9GbWxTaFE1R3pHNGl0TjJOS2steUtUY
kFNb0Z3VHVwdEcwWEZnTkl2SHVsUHBsVnpaWURWRGV4bzc2a0F3IiwiZXlKaGJHY2lPaUpGWkVSVFFTSX
NJblI1Y0NJNklrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E2YTJWNU9ubzJ
UV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnROMmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBJYlRoTU0xbEhT
aUlzSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMyVnlMbVpwYzNOcGIyNHVibUZ0WlM5d2RXSnNhV
012Ym05MFpYTXZJaXdpWTJGd0lqb2lUMVpGVWxkU1NWUkZJbjFkTENKbGVIQWlPamt5TlRZNU16azFNRF
VzSW1semN5STZJbVJwWkRwclpYazZlalpOYTNBMVJYTjZPWE15VFVoemNWbDJURzlqWTNsSWQxZzFVMlY
1V2t0d2NUYzVSM1EwTldaR1IwVmFVams1SWl3aWJtSm1Jam94TmpNNU5qQTRNamt6TENKd2NtWWlPbHRk
ZlEuTWdZYXJMcXk3Um1RMUFJcnFZTDZjRnk5ejdhNVdJQVUtLVRZQVJQU2dpck9Tc3p2YXIzX0ROcjI1c
mJQcmV0SGJuVDBtTVZLeW9hUVhydVI3S2JyQmciXX0.kwRdqPN74pkcpXGgdk7Z7FW3M1mRRYaDE5ZgkG
6srAuu6V6mvMVRdBLnD5CWid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded

Header


```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```


Payload


```
{
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
  "nbf": 1639608293,
  "exp": 9256939505,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/photos/",
      "can": "OVERWRITE"
    },
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "APPEND"
    }
  ],
  "prf": [
"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhc
CI6Ik9WRVJXUklURSJ9XSwiZXhwIjo5MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWtwNUV
zejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE3OUd0NDVmRkdFWlI5OSIsIm5iZiI6MTYzOTYwO
DI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG4itN2NKk-
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw",

"eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiY2FwI
joiT1ZFUldSSVRFIn1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN
6OXMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4M
jkzLCJwcmYiOltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--
TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg"
  ]
}
```


Signature


```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded

Header


```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```


Payload


```
{
  "iss": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "aud": "did:key:z6MkvXfPUv8bxtsVQiGo7Ntk4qKJNcgK2it52pc73teUpRLT",
  "nbf": 1639608293,
  "exp": 9256939505,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/photos/",
      "can": "OVERWRITE"
    },
    {
      "with": "wnfs://demouser.fission.name/public/notes/",
      "can": "APPEND"
    }
  ],
  "prf": [
    "eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
    2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
    0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhc
    CI6Ik9WRVJXUklURSJ9XSwiZXhwIjo5MjU2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWtwNUV
    zejlzMk1Ic3FZdkxvY2N5SHdYNVNleVpLcHE3OUd0NDVmRkdFWlI5OSIsIm5iZiI6MTYzOTYwO
    DI5MywicHJmIjpbXX0.4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG4itN2NKk-
    yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDexo76kAw",
    "eyJhbGciOiJFZERTQSIsInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a
    2V5Ono2TWtzWFFCZkw4b3d6dFRDSlRtN2hOUmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF
    0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiY2FwI
    joiT1ZFUldSSVRFIn1dLCJleHAiOjkyNTY5Mzk1MDUsImlzcyI6ImRpZDprZXk6ejZNa3A1RXN
    6OXMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4M
    jkzLCJwcmYiOltdfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--
    TYARPSgirOSszvar3_DNr25rbPretHbnT0mMVKyoaQXruR7KbrBg"
  ]
}
```


Signature


```
kwRdqPN74pkcpXGgdk7Z7FW3M1mRR
YaDE5ZgkG6srAuu6V6mvMVRdBLnD5
CWid-X4tDIKpliVjlCSLTntB4pCw
```

Nontrivial Example

Decoded Witness #1

Header

```
{
  "alg": "EdDSA",
  "typ": "JWT",
  "ucv": "0.8.0"
}
```

Payload

```
{
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "nbf": 1639608293,
  "exp": 9256939505,
  "att": [
    {
      "with": "wnfs://demouser.fission.name/public/photos/",
      "can": "OVERWRITE"
    }
  ],
  "prf": []
}
```

Signature

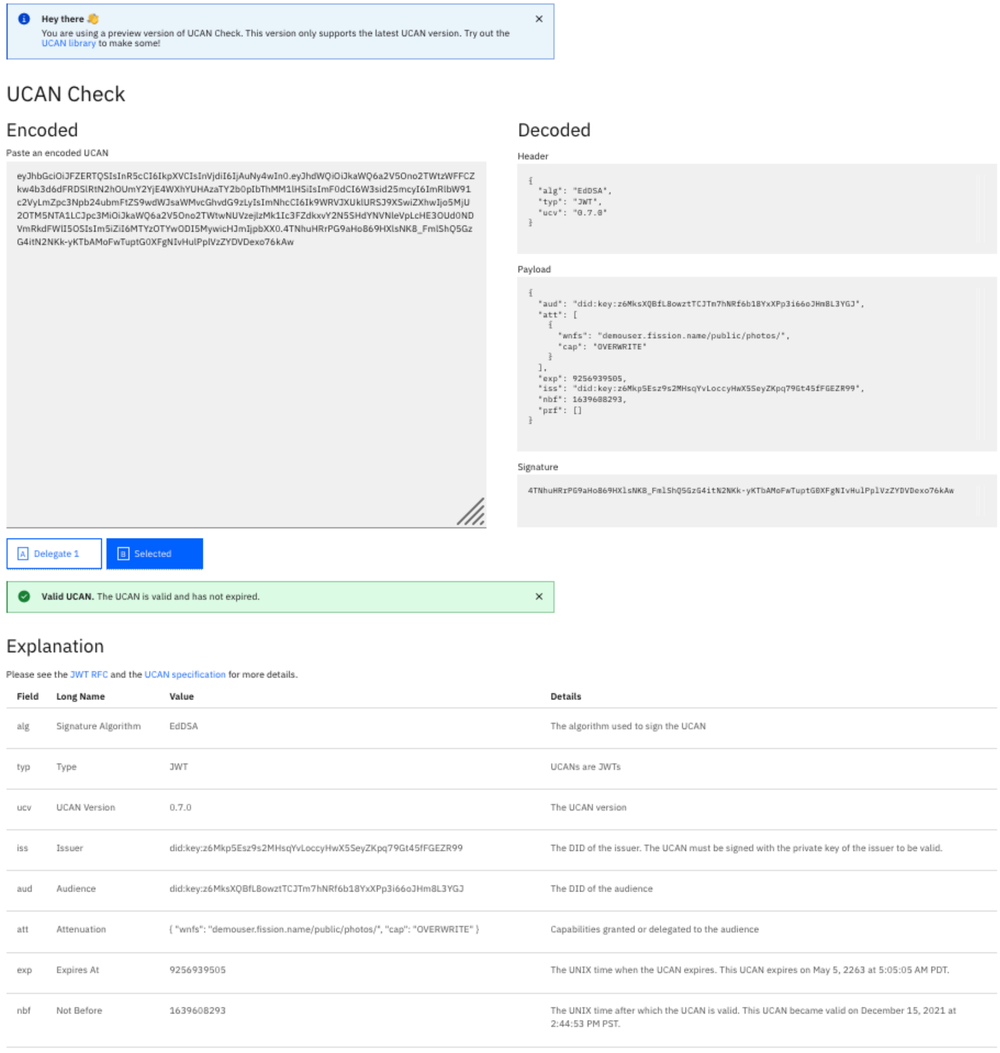
```
4TNhuHRrPG9aHo869HXlsNK8_FmlShQ5GzG
4itN2NKk-
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDe
xo76kAw
```

Nontrivial Example

ucan.xyz — Online Explorer / Validator

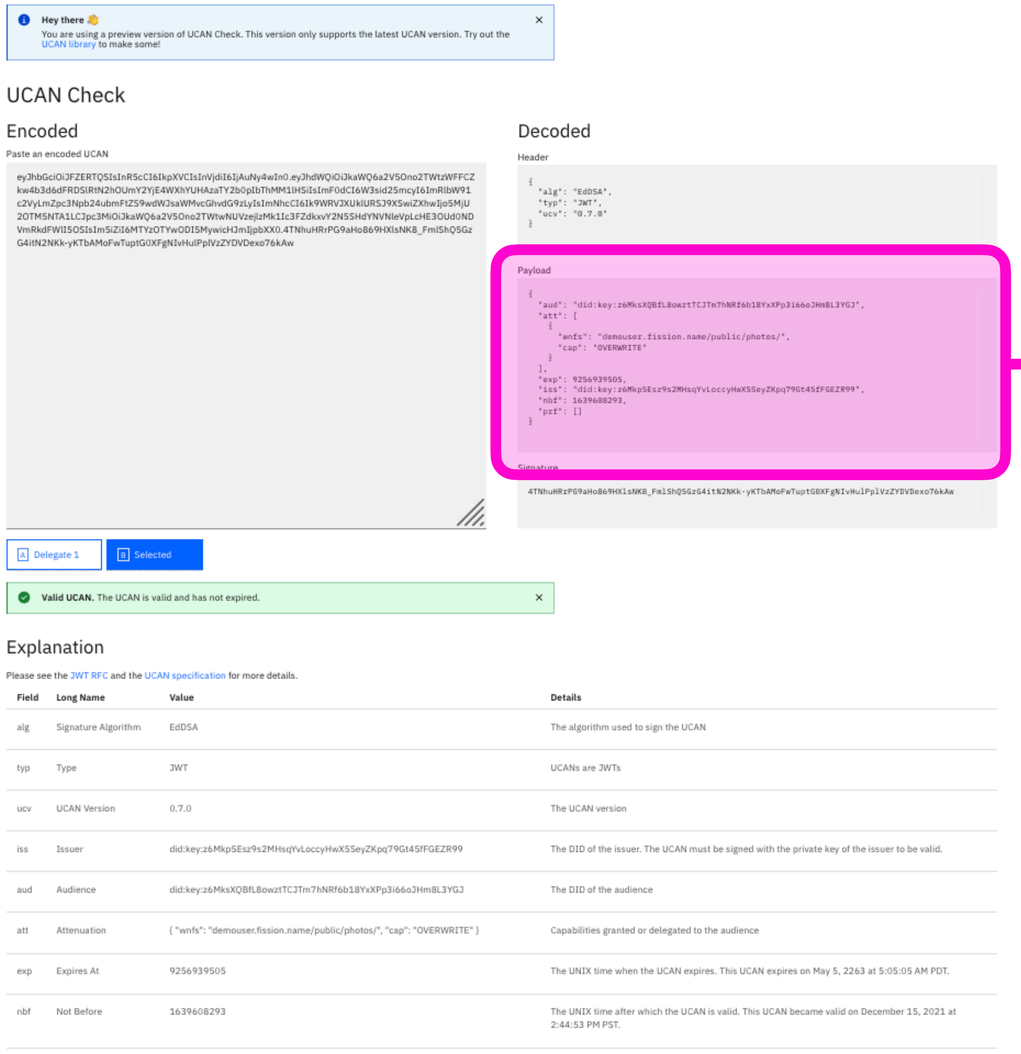
Nontrivial Example

ucan.xyz — Online Explorer / Validator



Nontrivial Example

ucan.xyz — Online Explorer / Validator

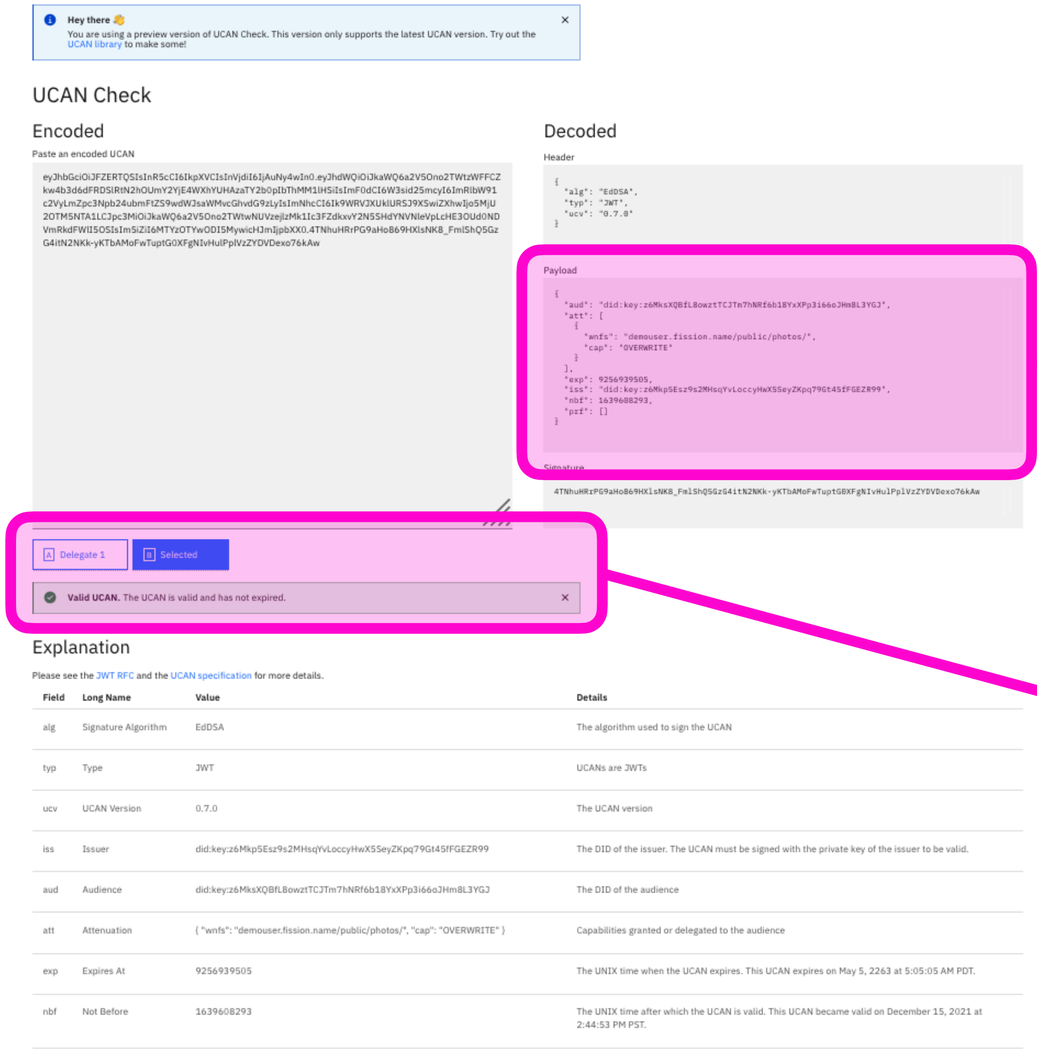


Payload


```
{
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "att": [
    {
      "wnfs": "demouser.fission.name/public/photos/",
      "cap": "OVERWRITE"
    }
  ],
  "exp": 9256939505,
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
  "nbf": 1639608293,
  "prf": []
}
```

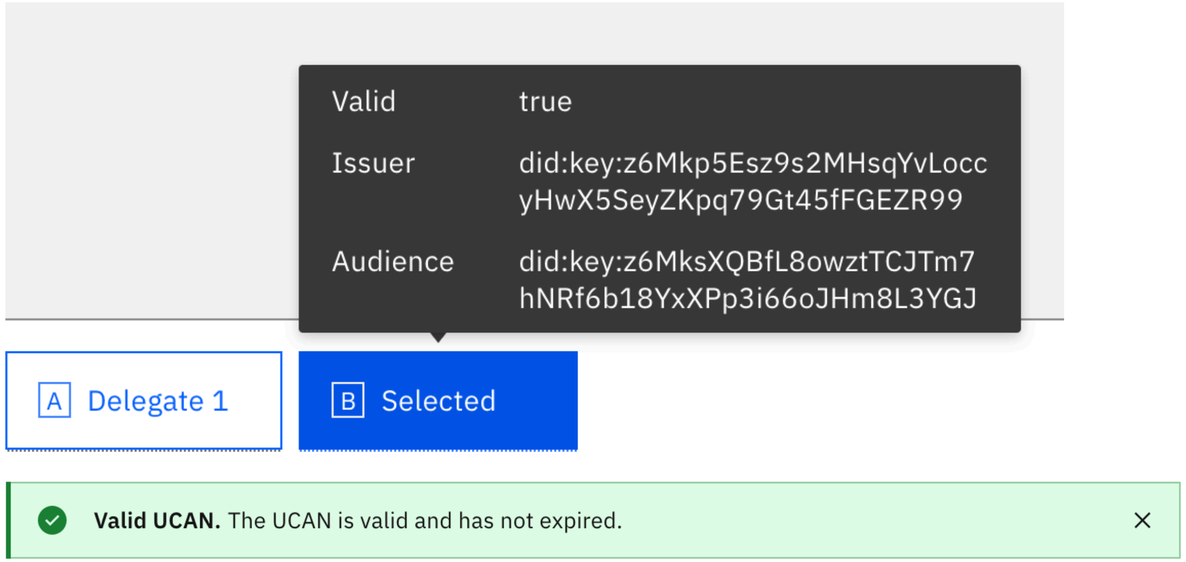
Nontrivial Example

ucan.xyz — Online Explorer / Validator



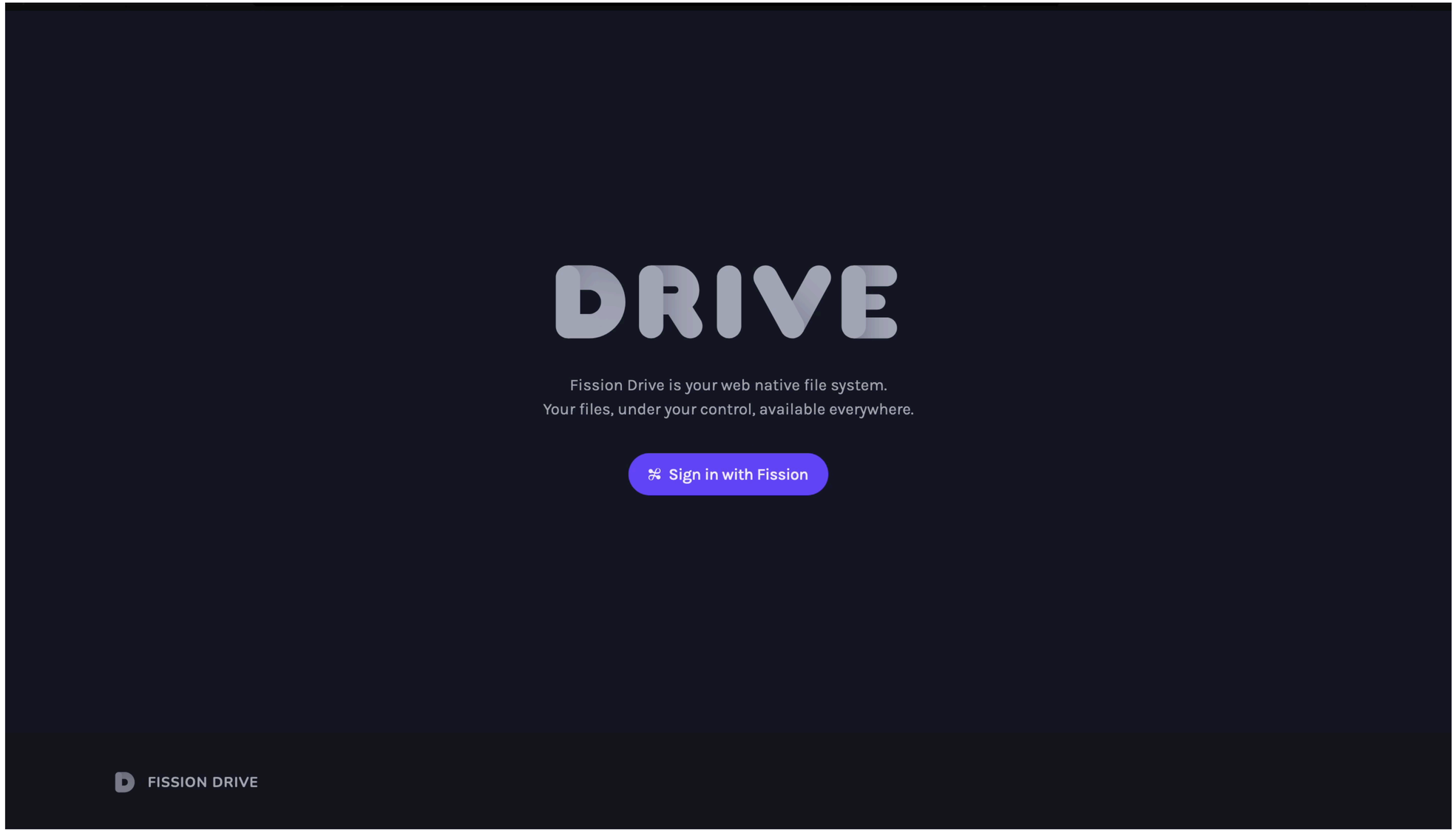
Payload


```
{
  "aud": "did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ",
  "att": [
    {
      "wnfs": "demouser.fission.name/public/photos/",
      "cap": "OVERWRITE"
    }
  ],
  "exp": 9256939505,
  "iss": "did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99",
  "nbf": 1639608293,
  "prf": []
}
```

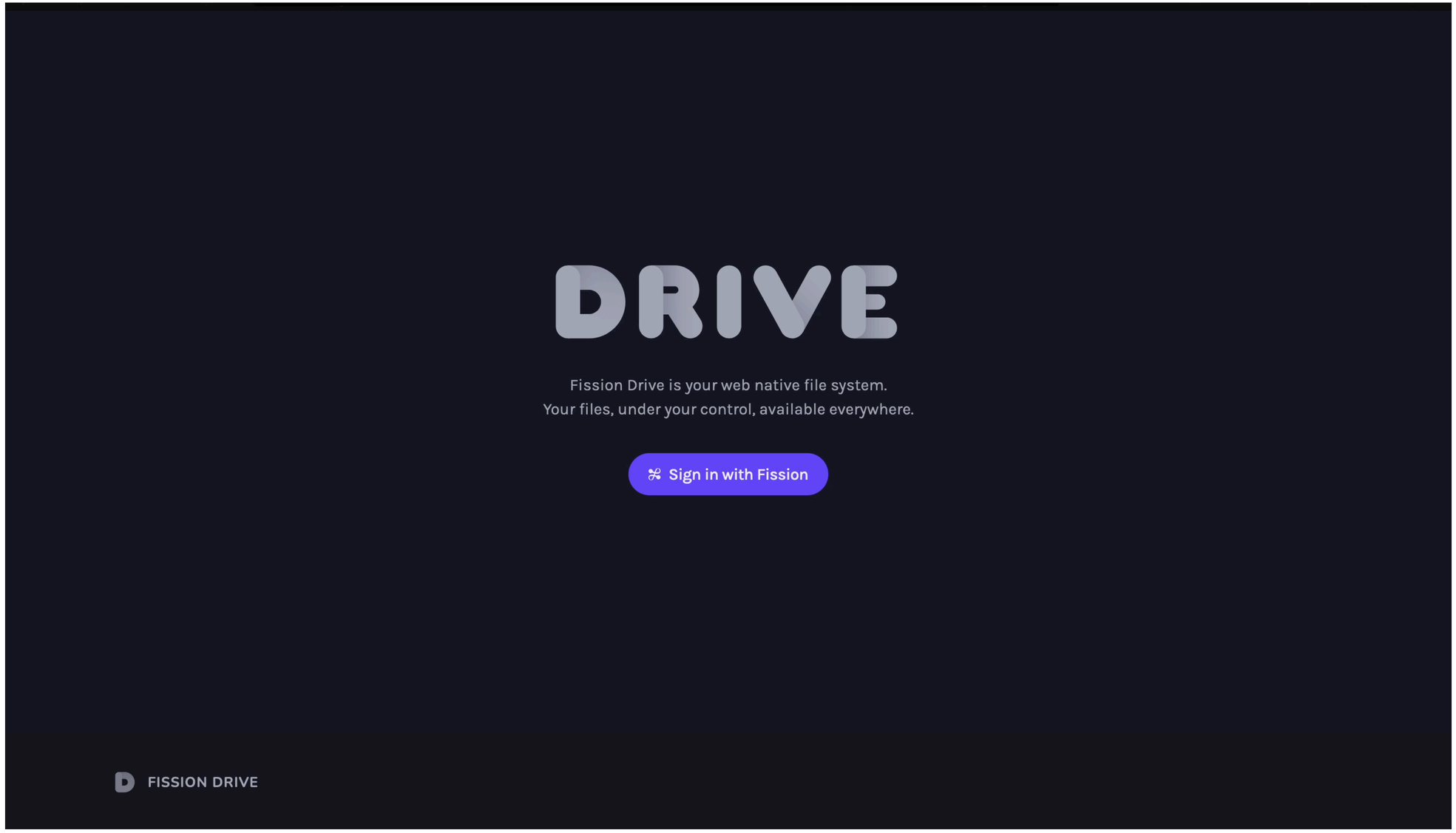
Nontrivial Example

Auth Should be Boring!



Nontrivial Example

Auth Should be Boring!



Resources

Resources

Further Reading

Resources

Further Reading

- https://talk.fission.codes/t/user-controlled-authorization-networks-ucan-resources/1122
- https://github.com/ucan-wg/
  - Spec, Improvement Proposals
  - Libraries: TypeScript, Golang, Haskell, (Rust soon)
- Capability Myths Demolished (https://srl.cs.jhu.edu/pubs/SRL2003-02.pdf)
- ACLs Don't (http://waterken.sourceforge.net/aclsdont/current.pdf)
- https://erights.org
- https://theworld.com/~cme/html/spki.html

https://ucan.xyz

https://github.com/ucan-wg

Thank You, Ink & Switch

brooklyn@fission.codes

https://fission.codes

github.com/expede

@expede