

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

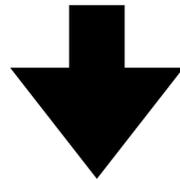
Intro

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.eyJhdWQiOiJkaWQ6a2V50no2TWtzWFFCZkw4b3d6dFRDSlRtN2h0UmY2YjE4WXhYUHAzaTY2b0pIbThMM1lHSiIsImF0dCI6W3sid25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwiaWF0IjoiT1ZFUlSSVRFIn1dLCJleHAiOi0jkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3A1RXN60XMyTUhzcVl2TG9jY3lId1g1U2V5WktwcTc5R3Q0NWZGR0VaUjk5IiwibmJmIjoxNjM5NjA4MjkzLCJwcmYiOi0ldfQ.MgYarLqy7RmQ1AIrqYL6cFy9z7a5WIAU--TYARPSgir0Sszvar3_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



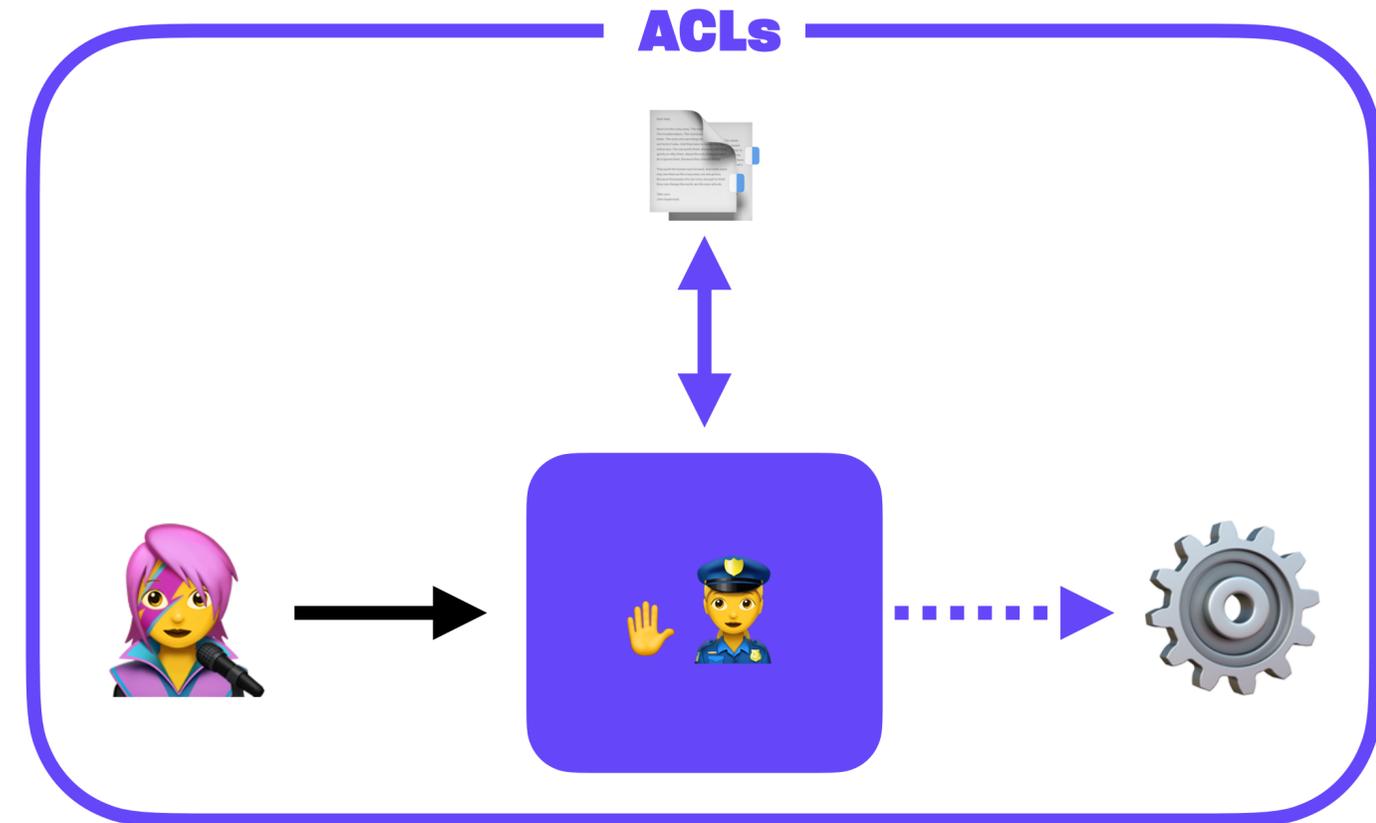
UCAN

Capability Model

UCAN

Capability Model

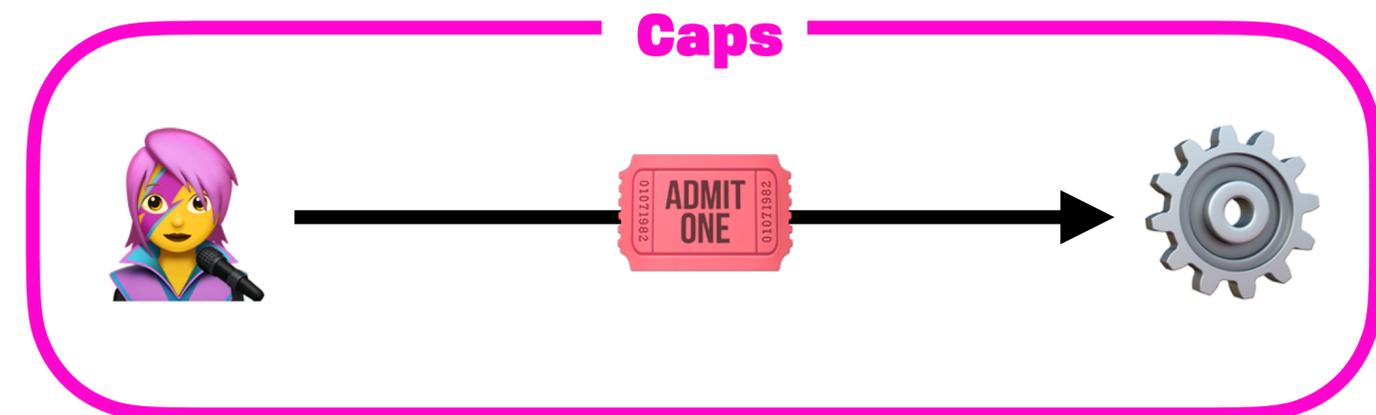
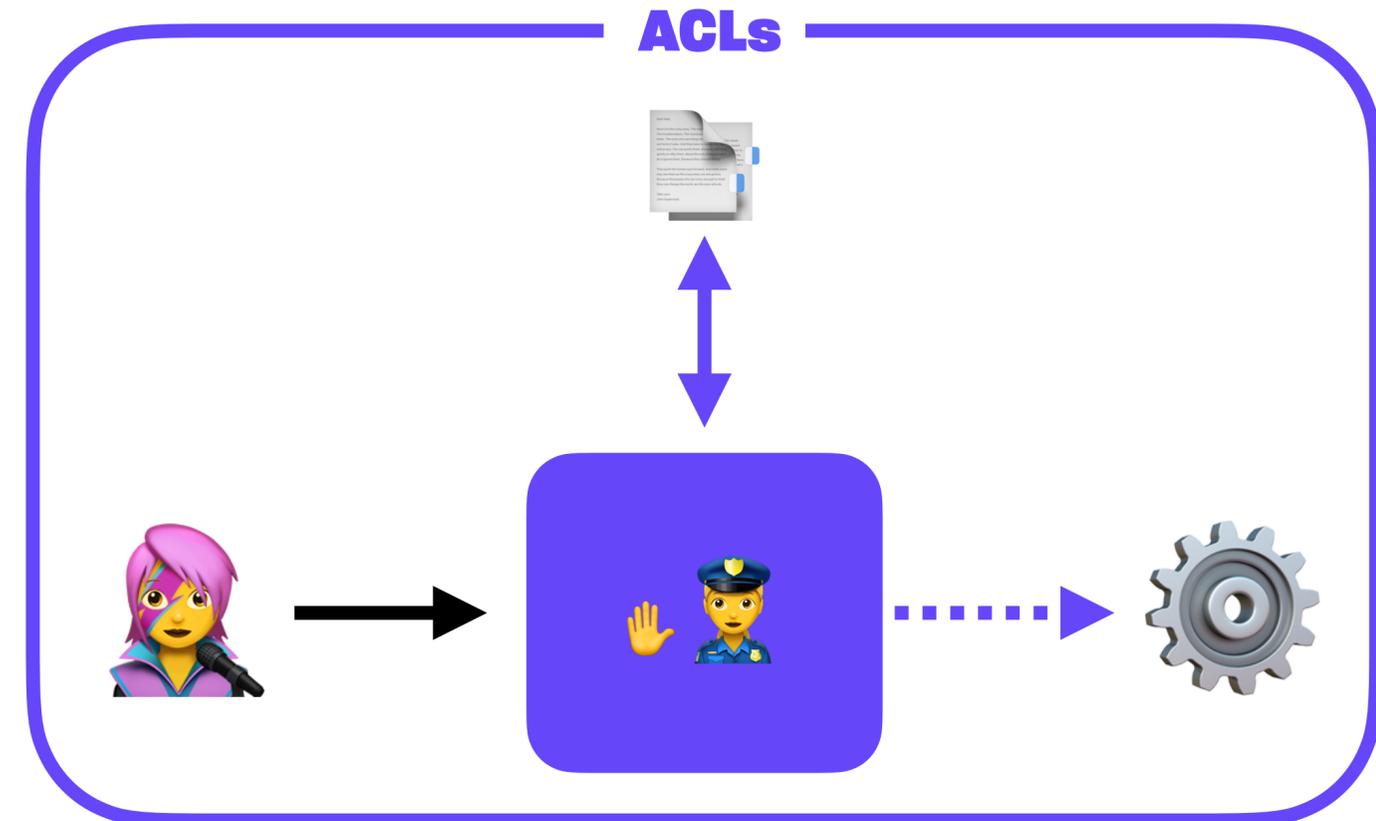
- ACLs are “reactive auth”



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



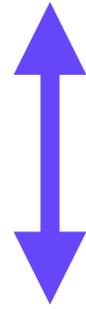
UCAN

ACL Read & Write



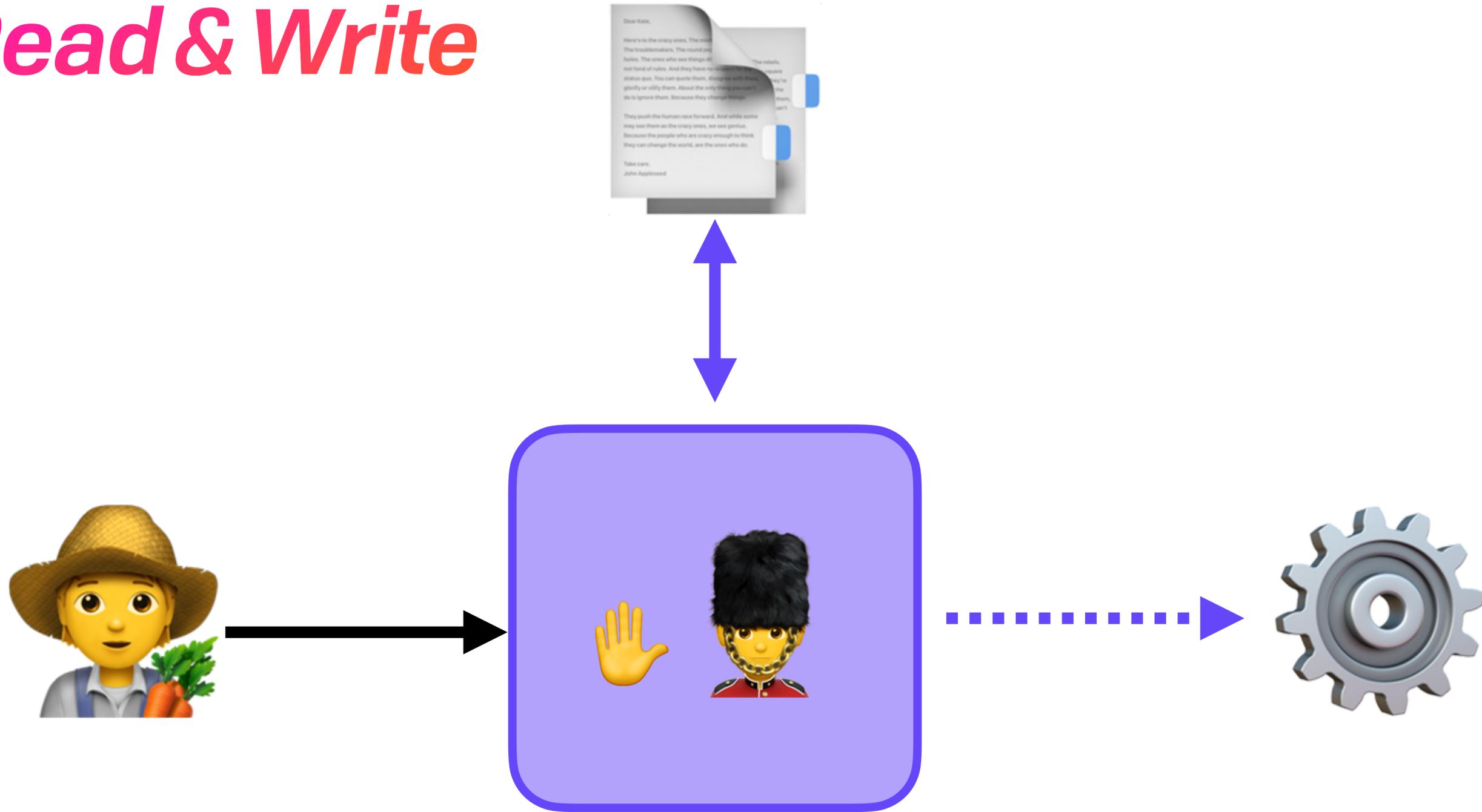
UCAN

ACL Read & Write



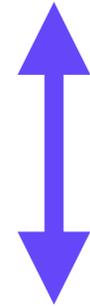
UCAN

ACL Read & Write



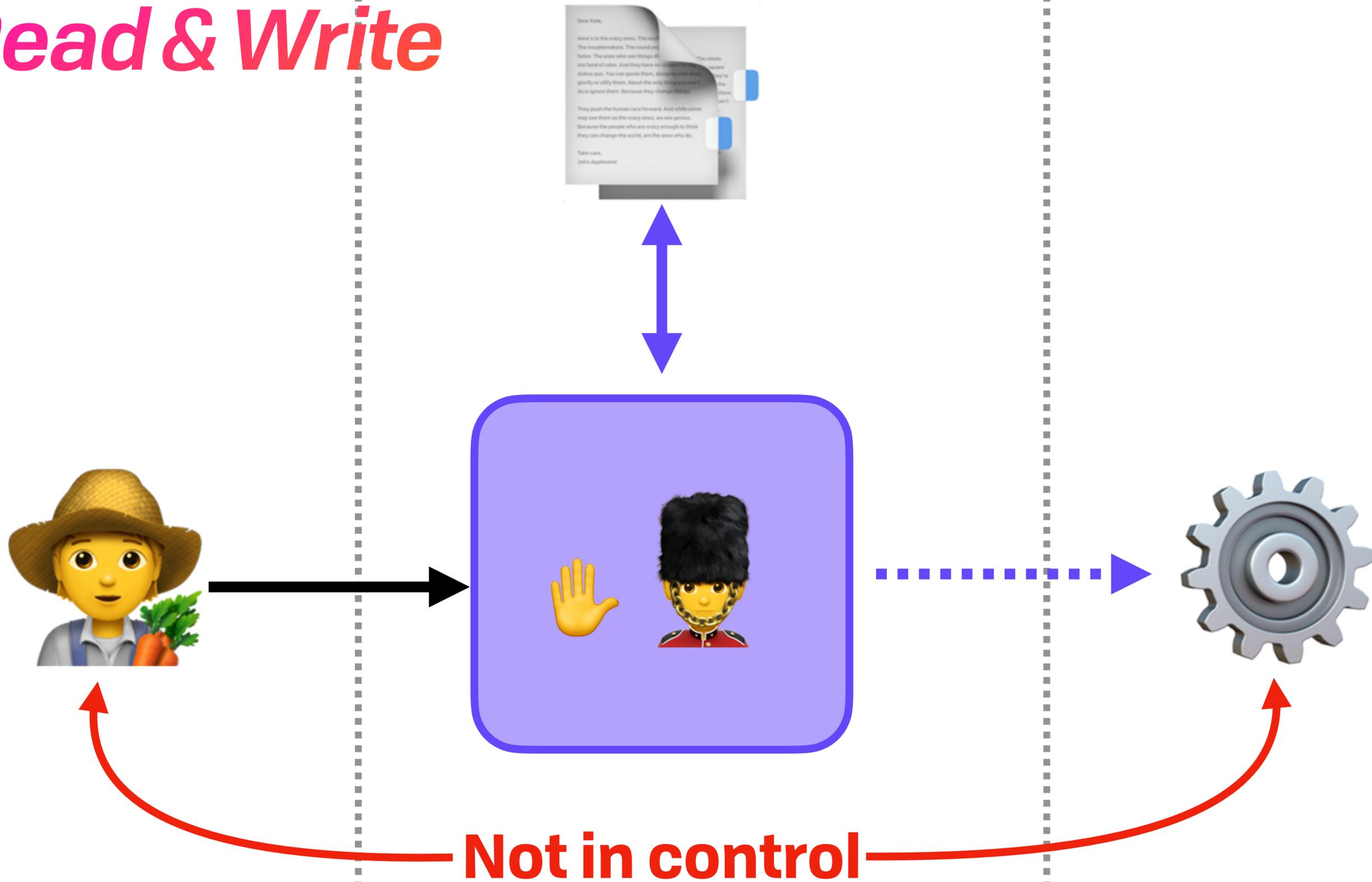
UCAN

ACL Read & Write



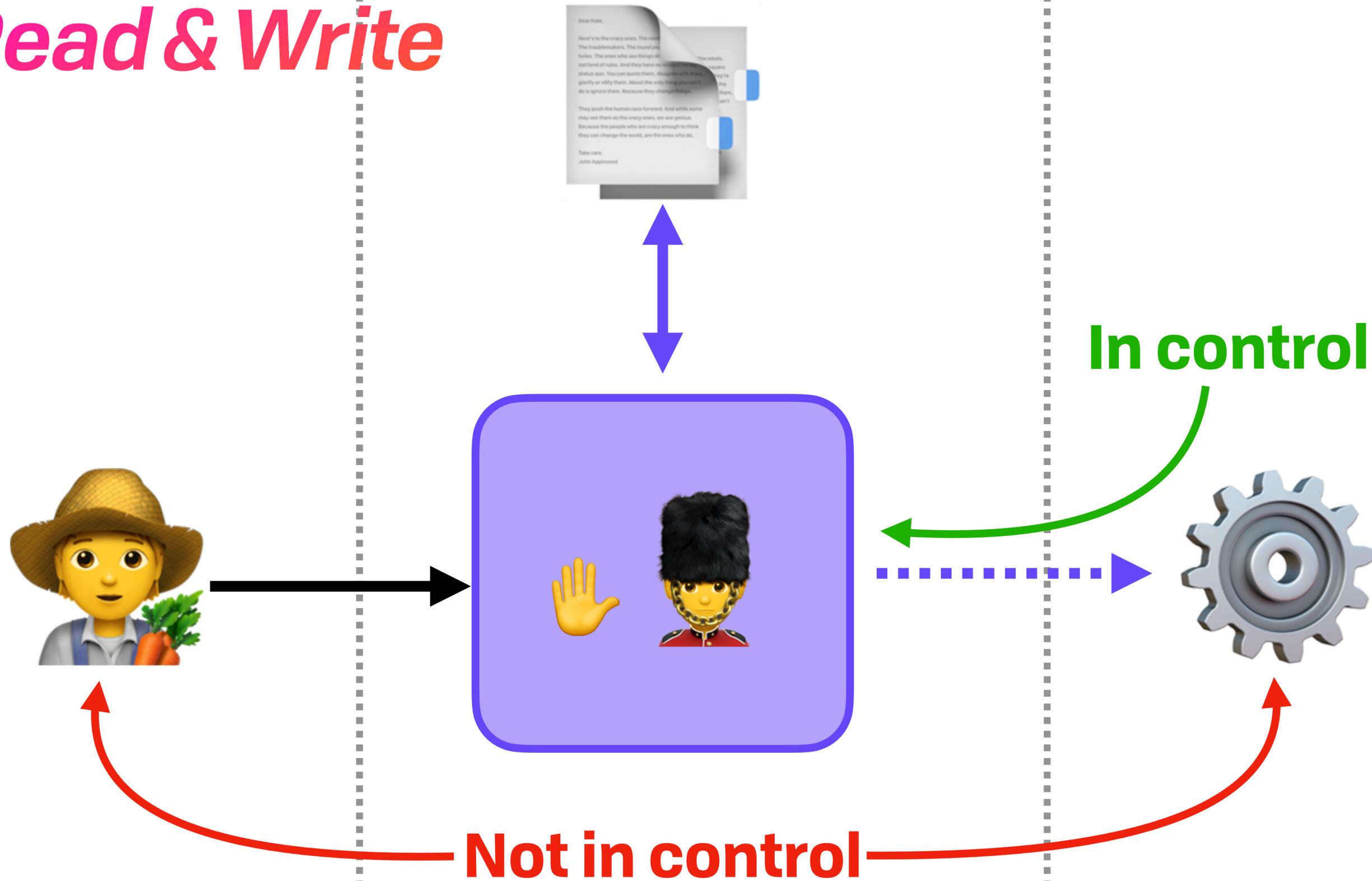
UCAN

ACL Read & Write



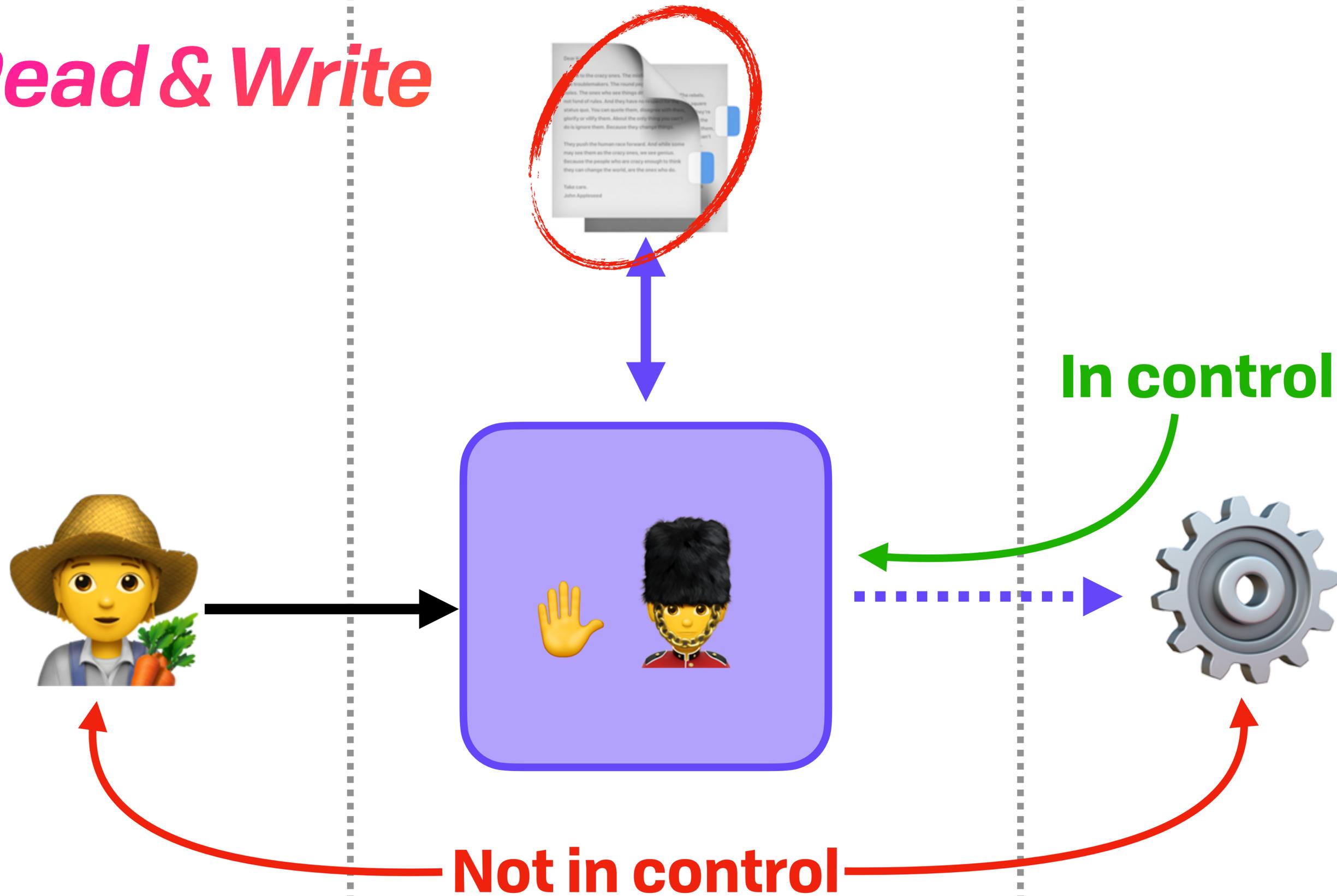
UCAN

ACL Read & Write



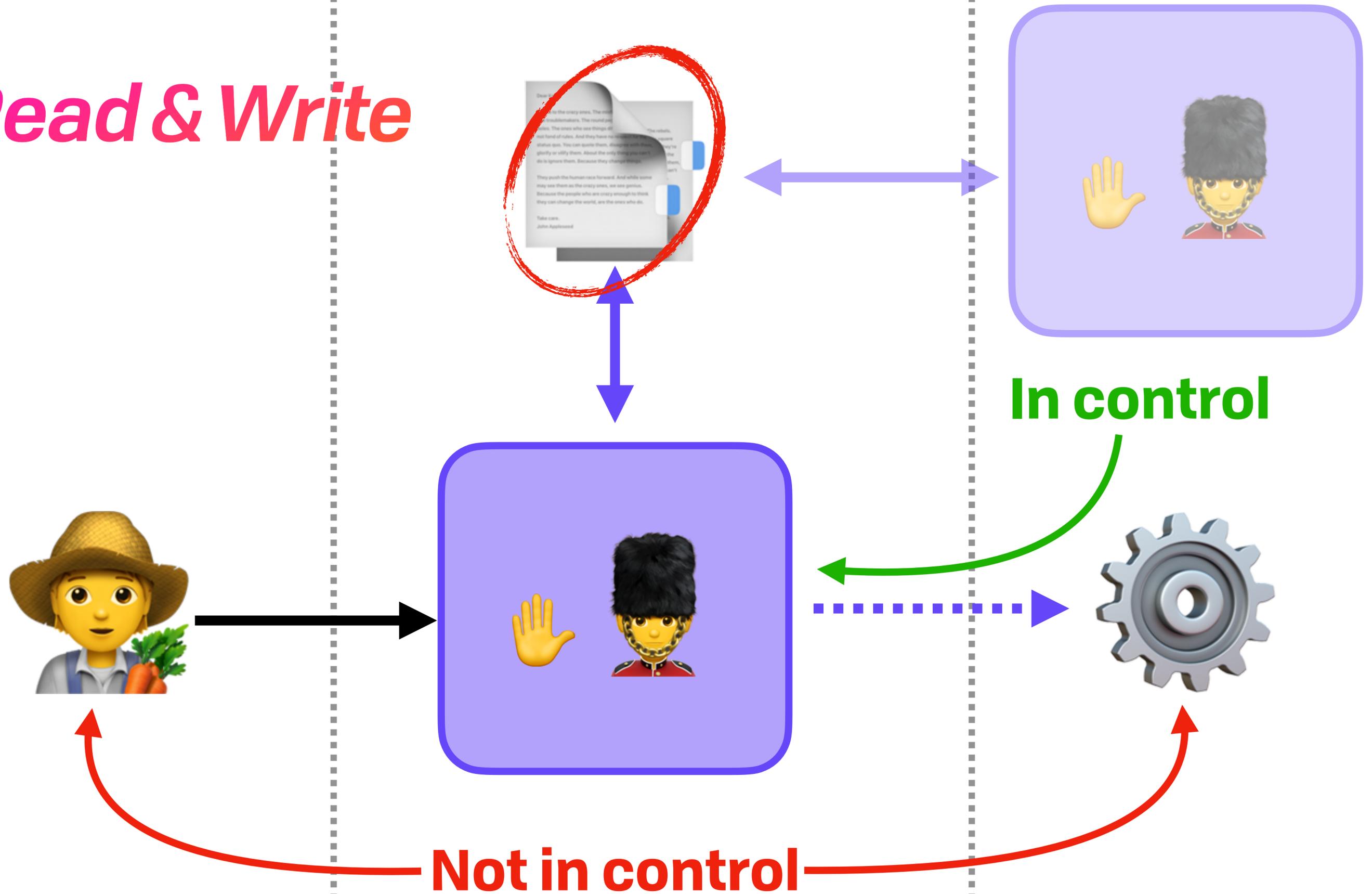
UCAN

ACL Read & Write



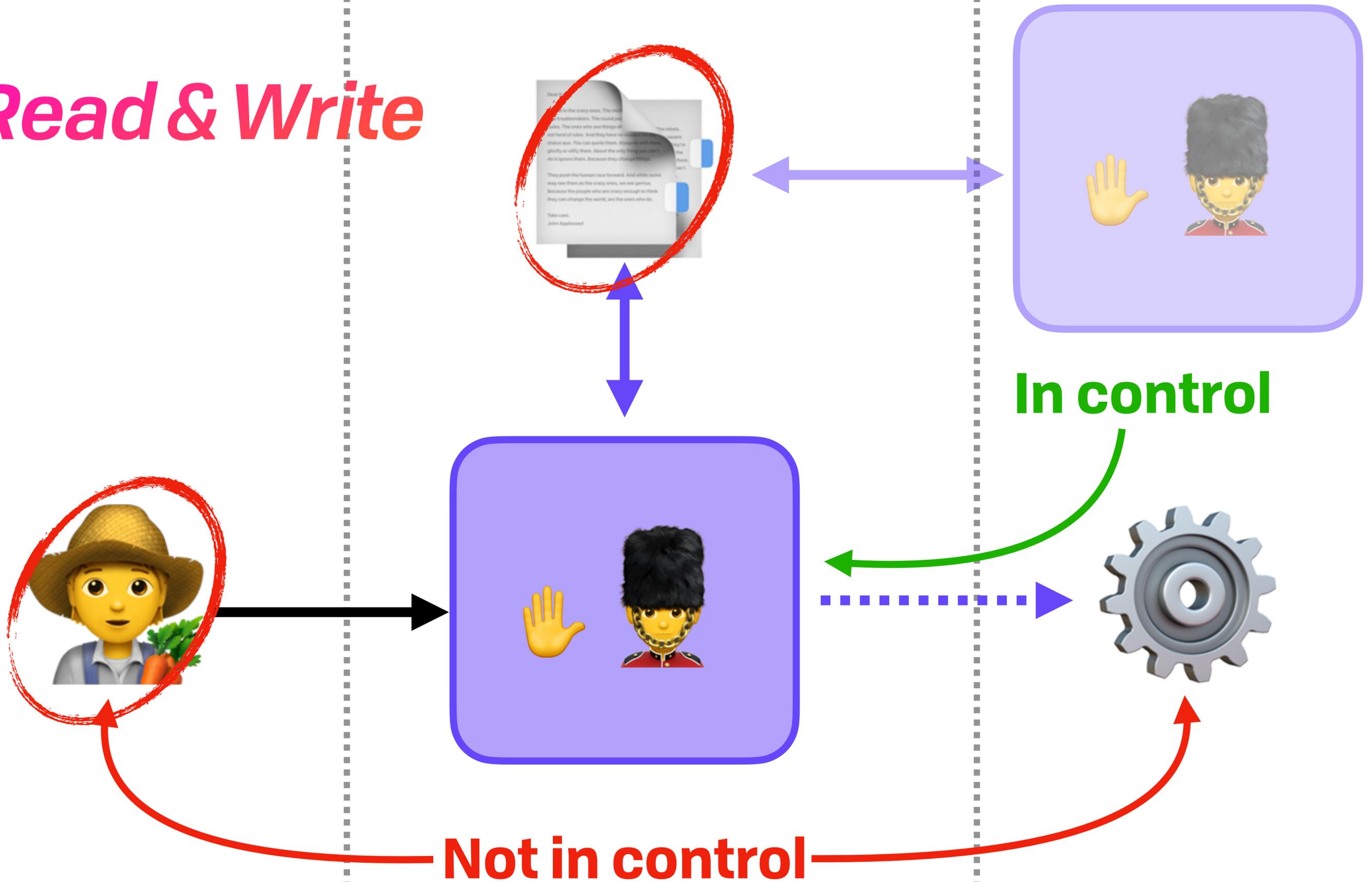
UCAN

ACL Read & Write



UCAN

ACL Read & Write



UCAN

From Actors to Capabilities

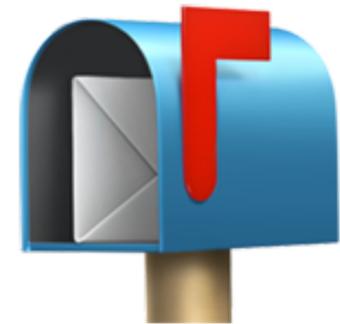
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



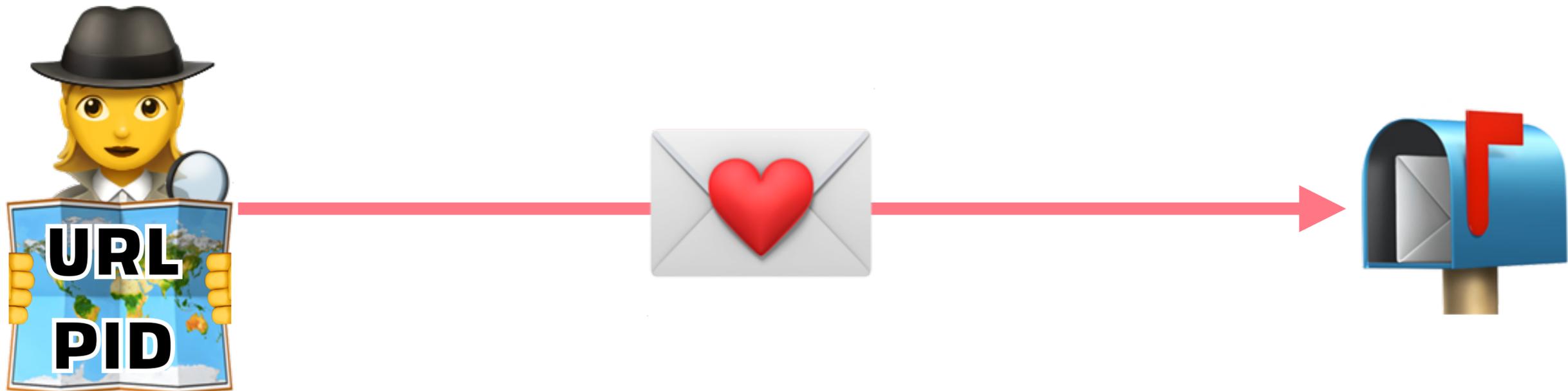
UCAN

From Actors to Capabilities



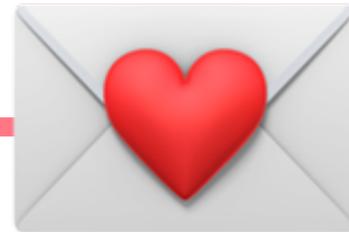
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



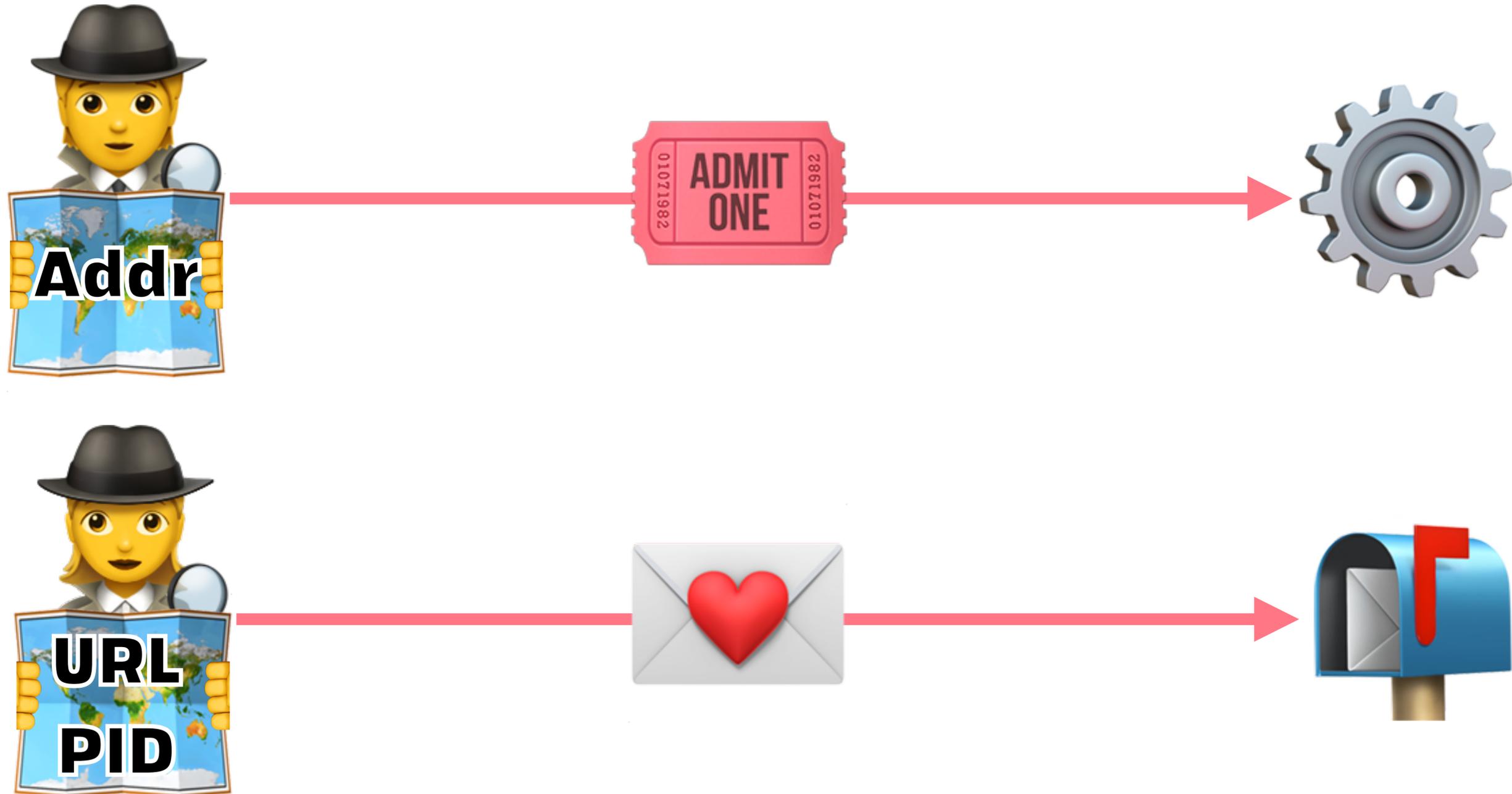
UCAN

From Actors to Capabilities



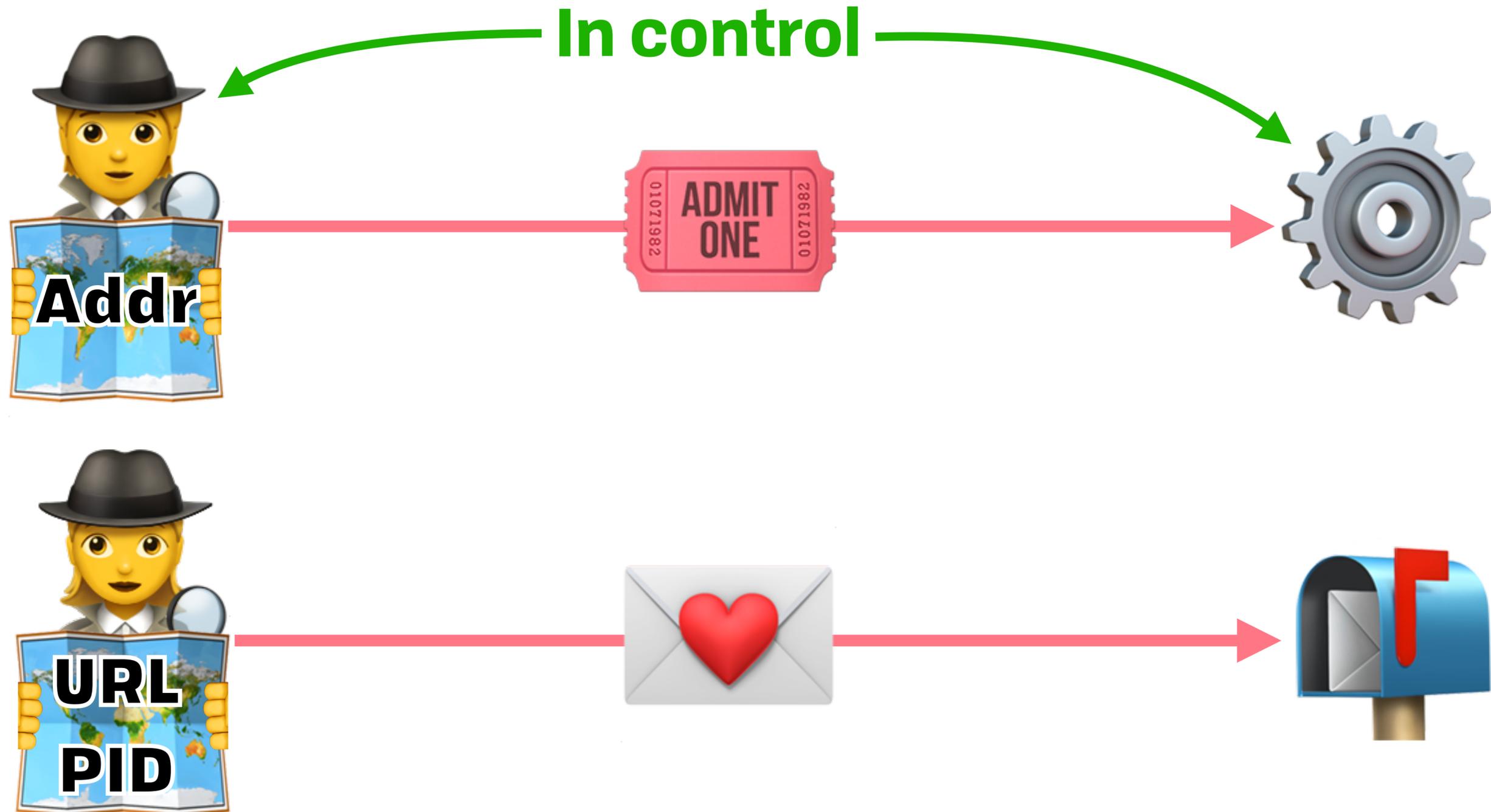
UCAN

From Actors to Capabilities



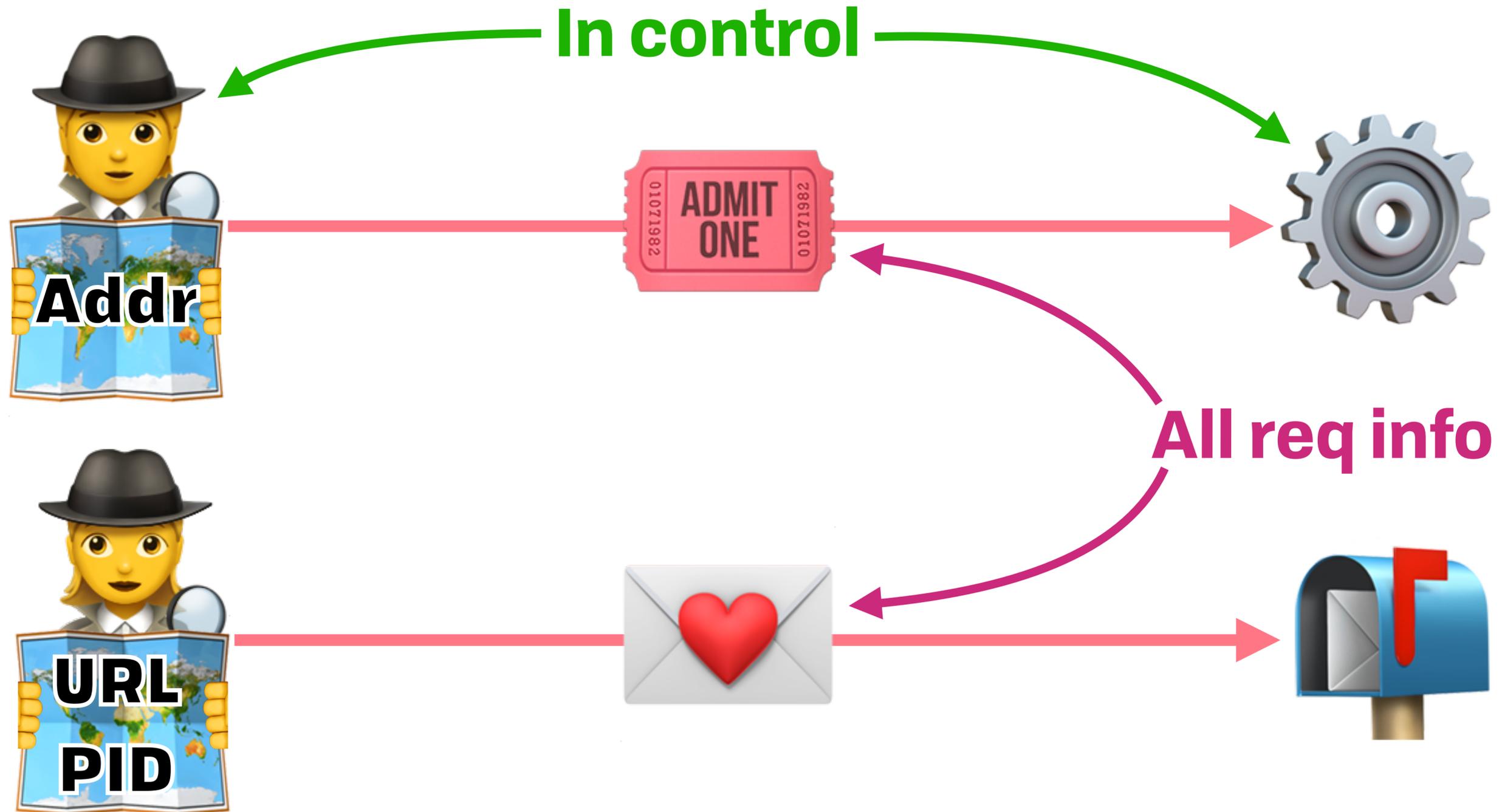
UCAN

From Actors to Capabilities



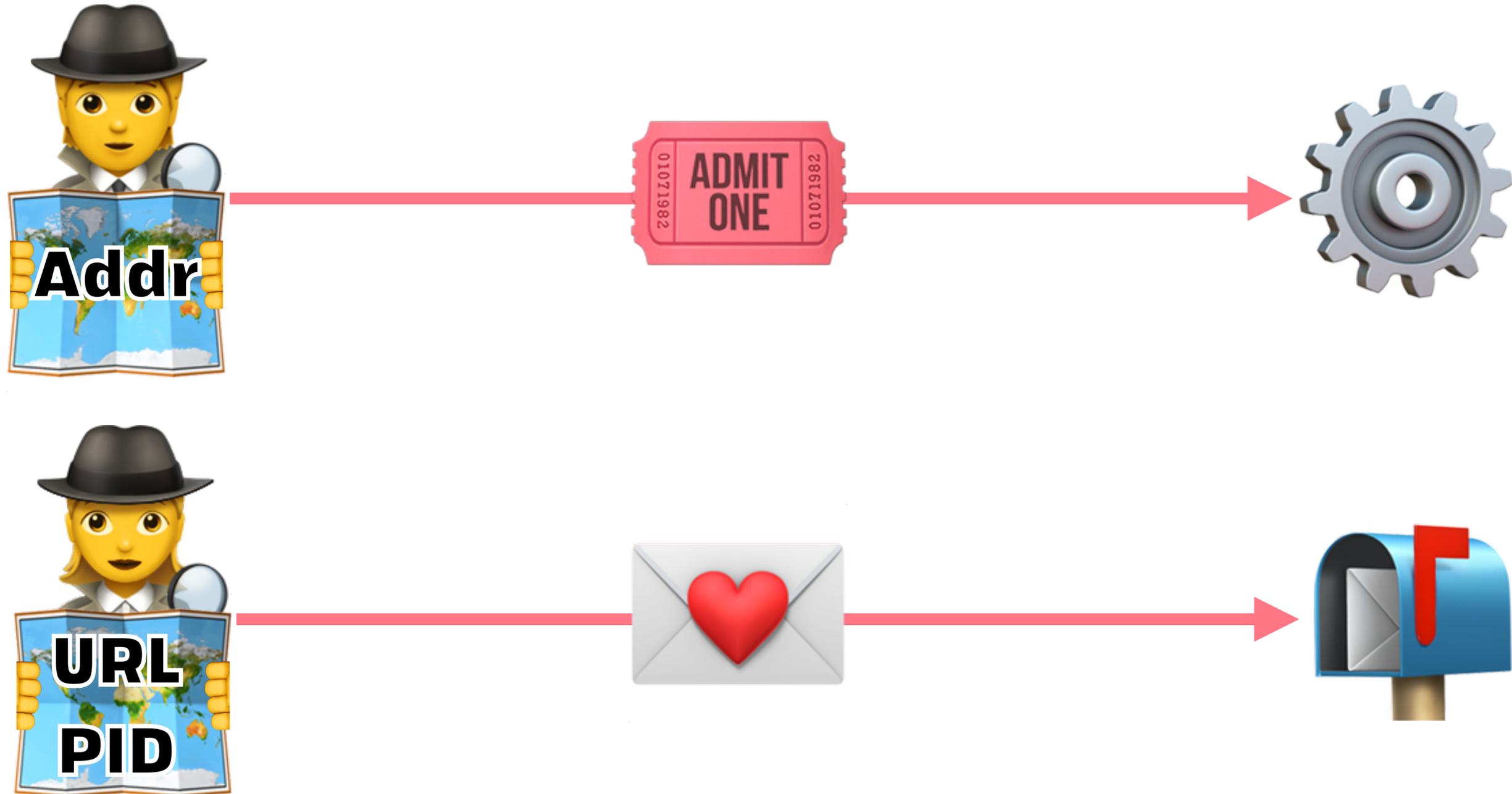
UCAN

From Actors to Capabilities



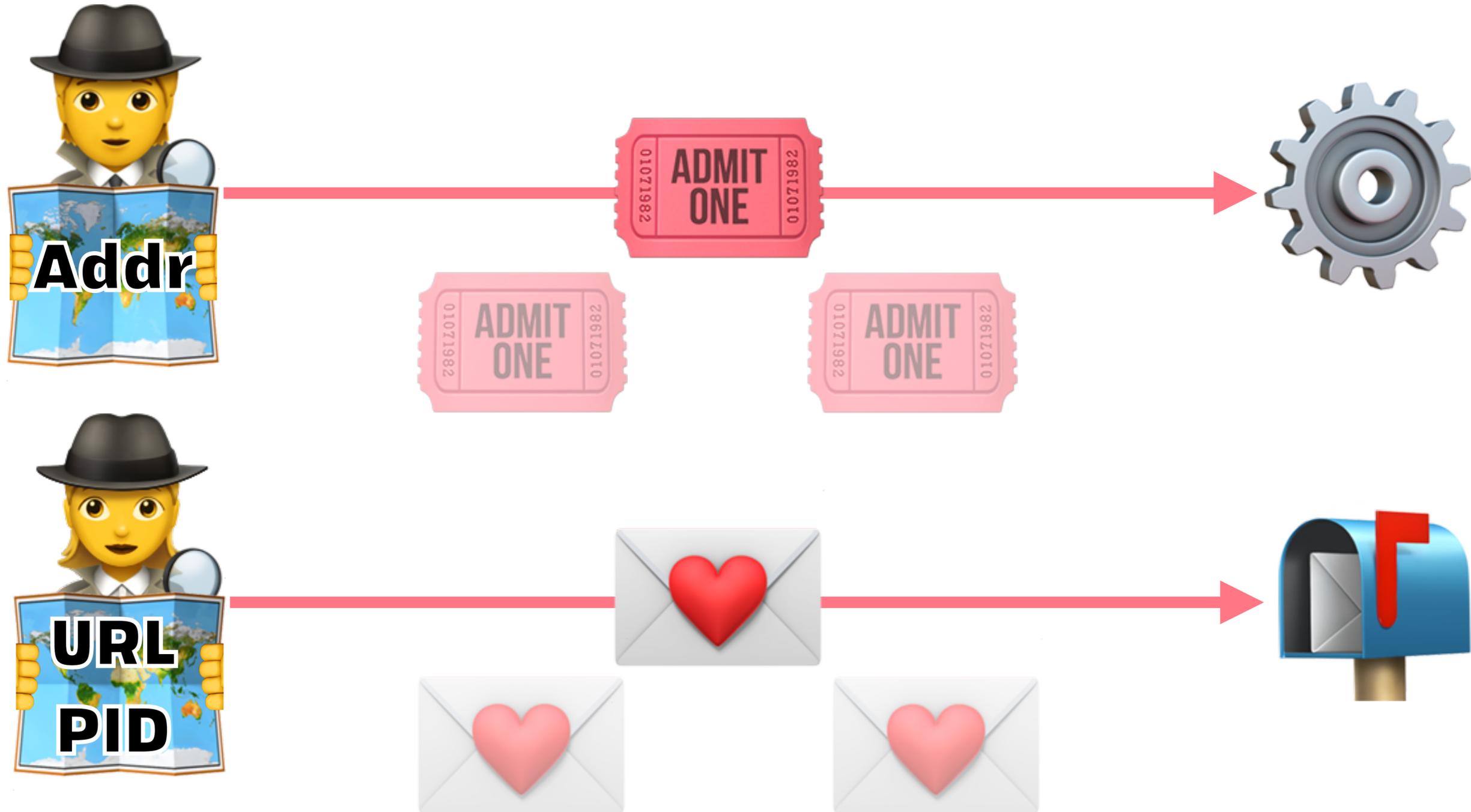
UCAN

From Actors to Capabilities



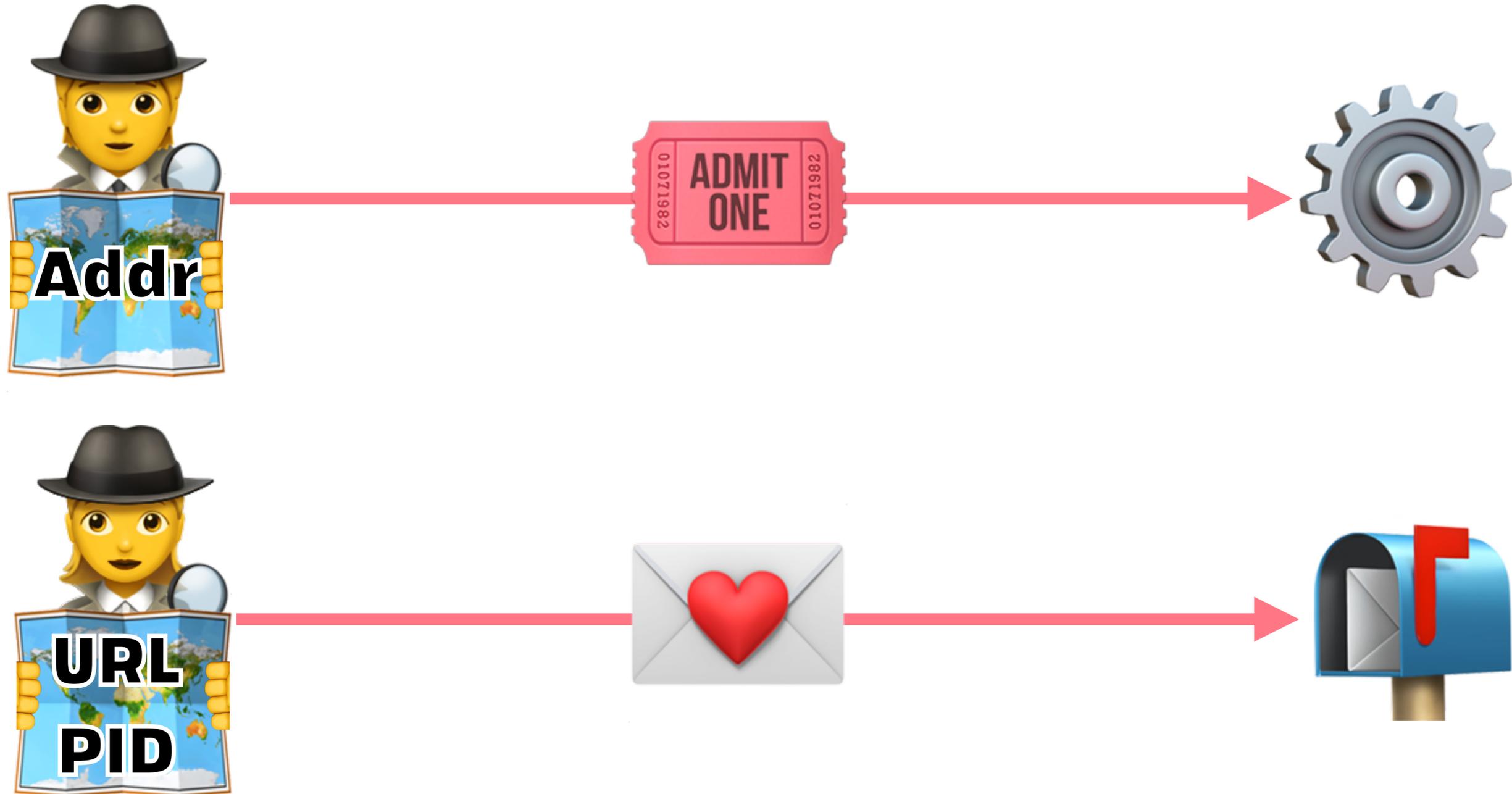
UCAN

From Actors to Capabilities



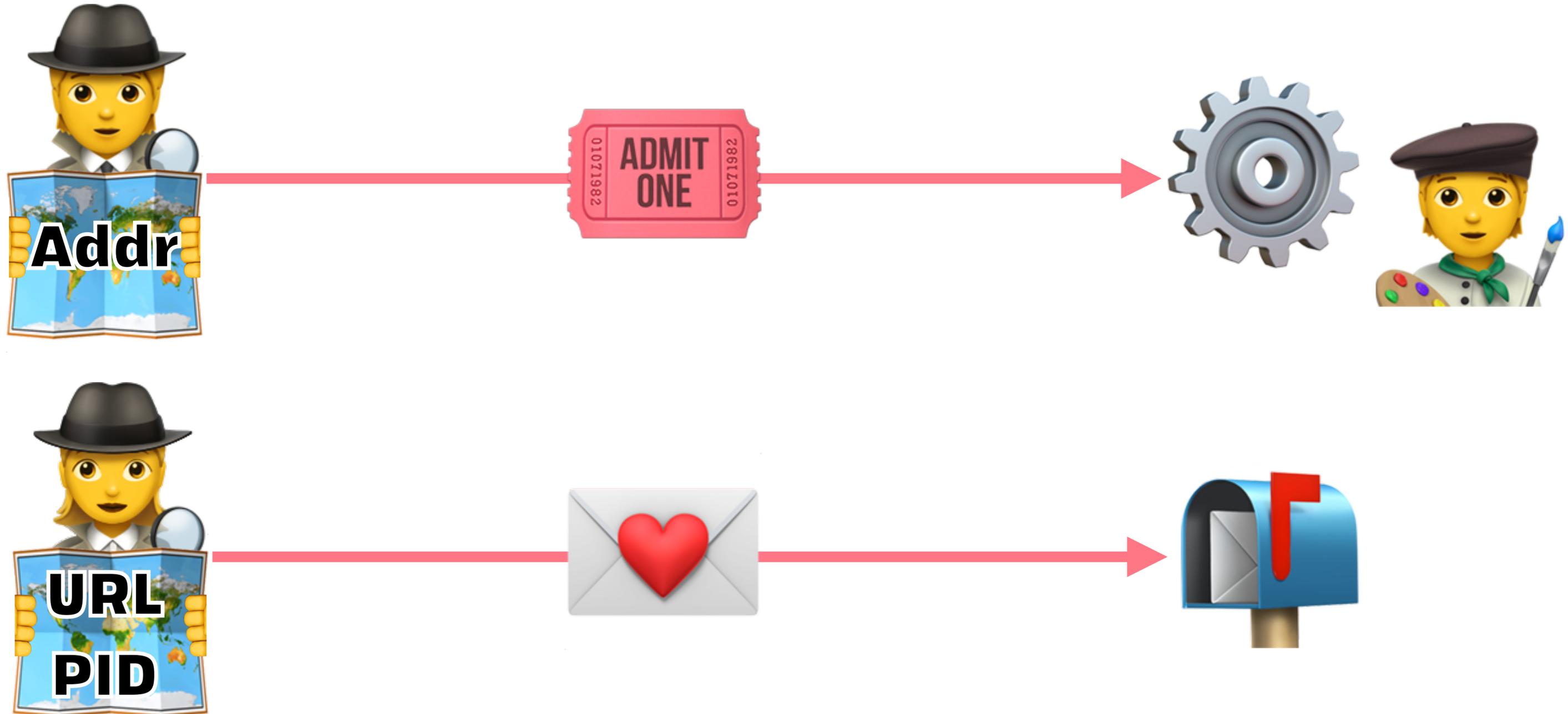
UCAN

From Actors to Capabilities



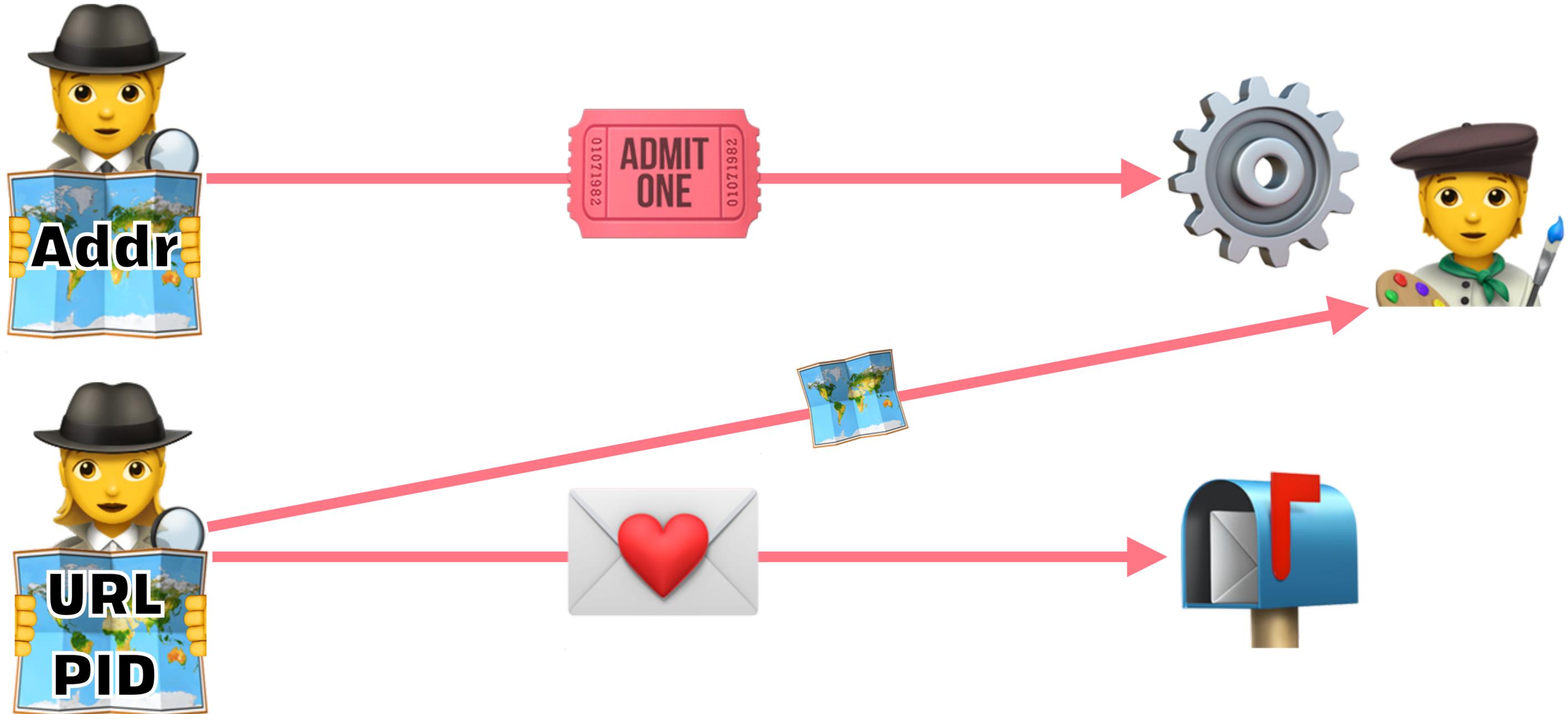
UCAN

From Actors to Capabilities



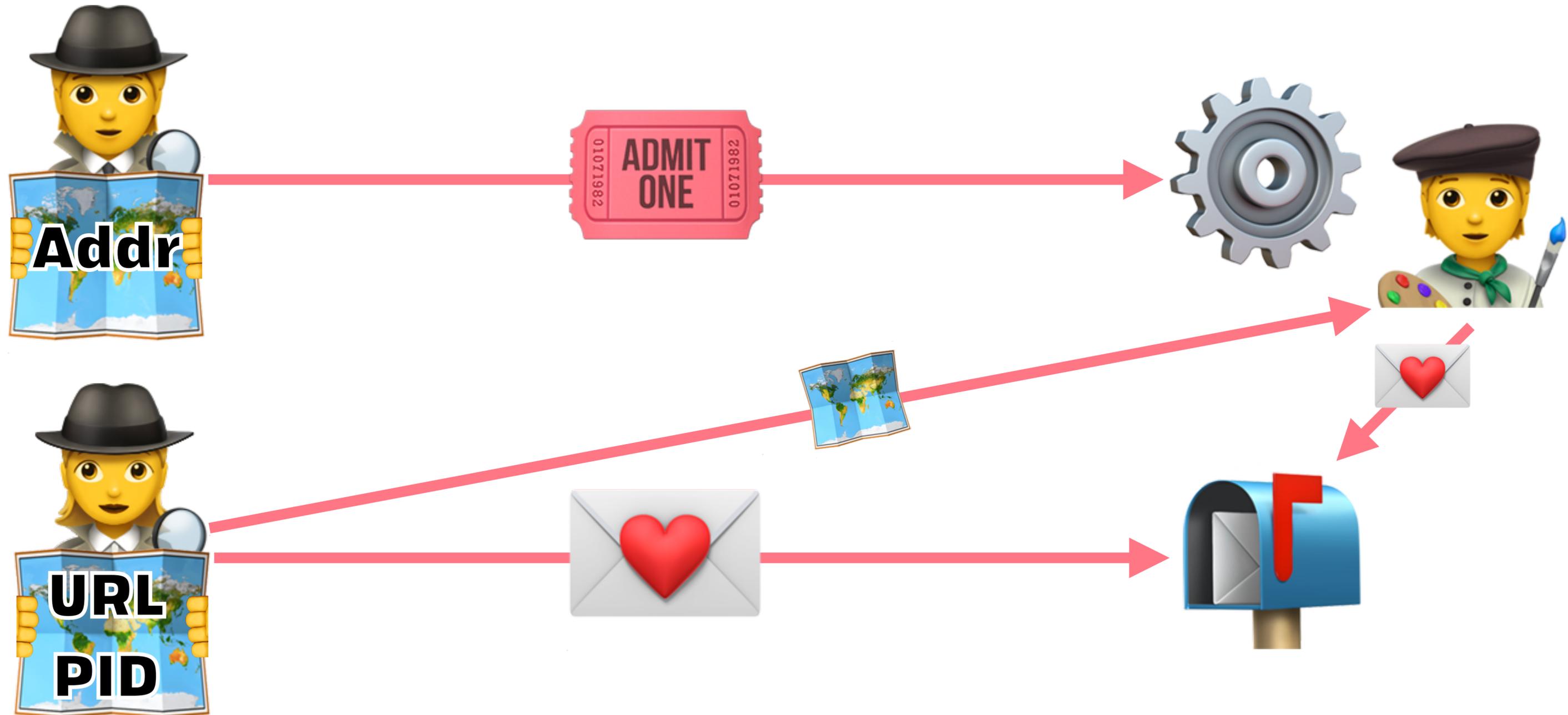
UCAN

From Actors to Capabilities



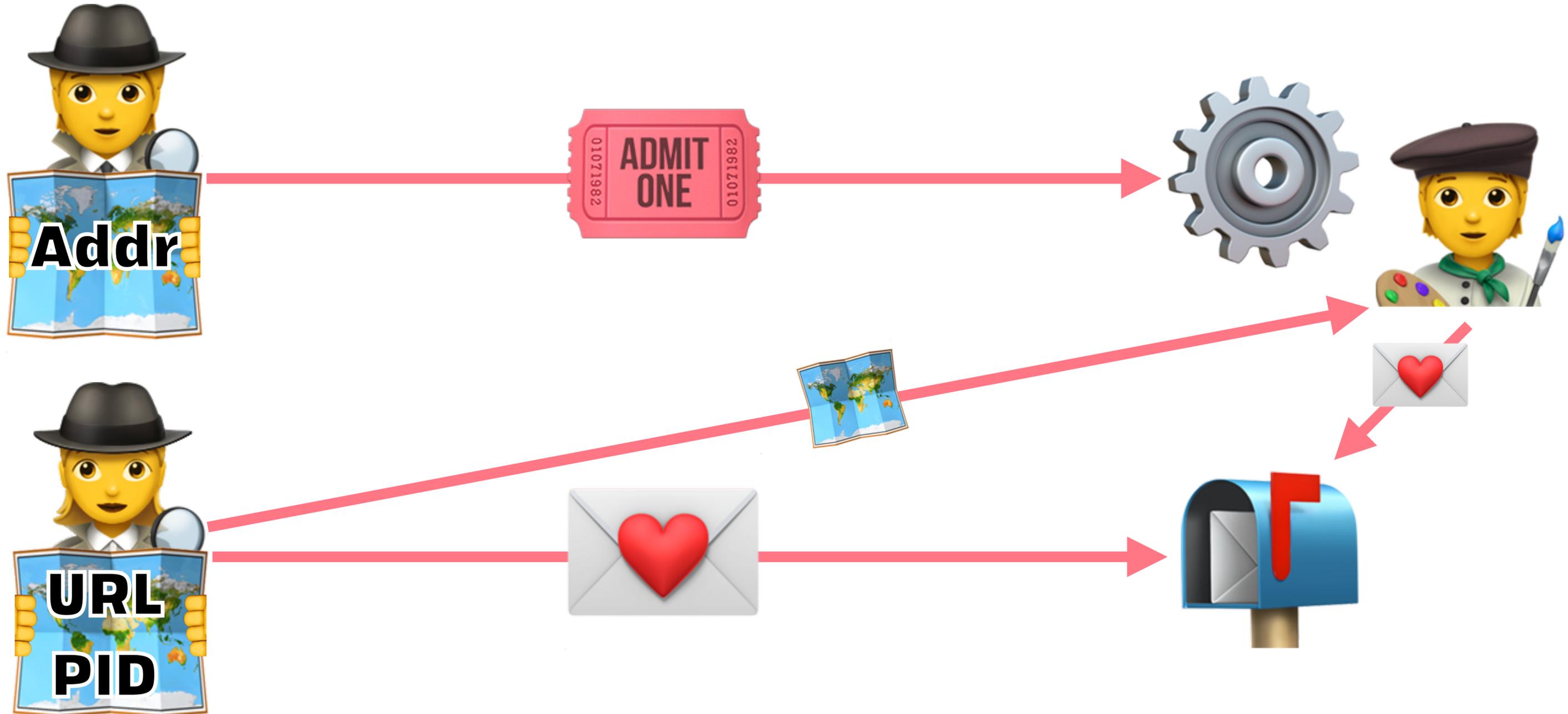
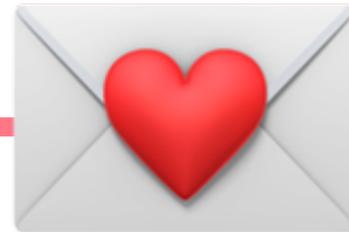
UCAN

From Actors to Capabilities



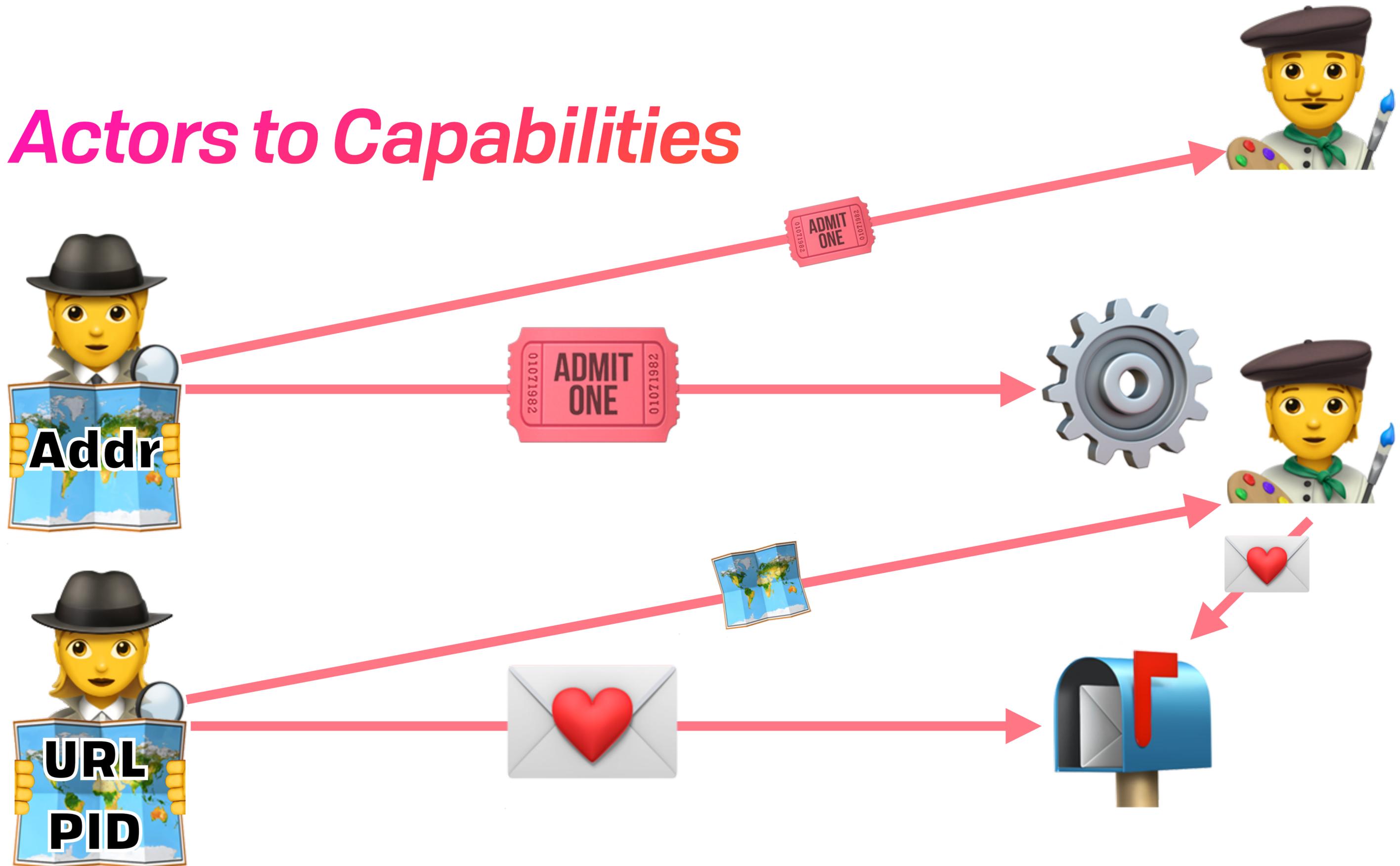
UCAN

From Actors to Capabilities



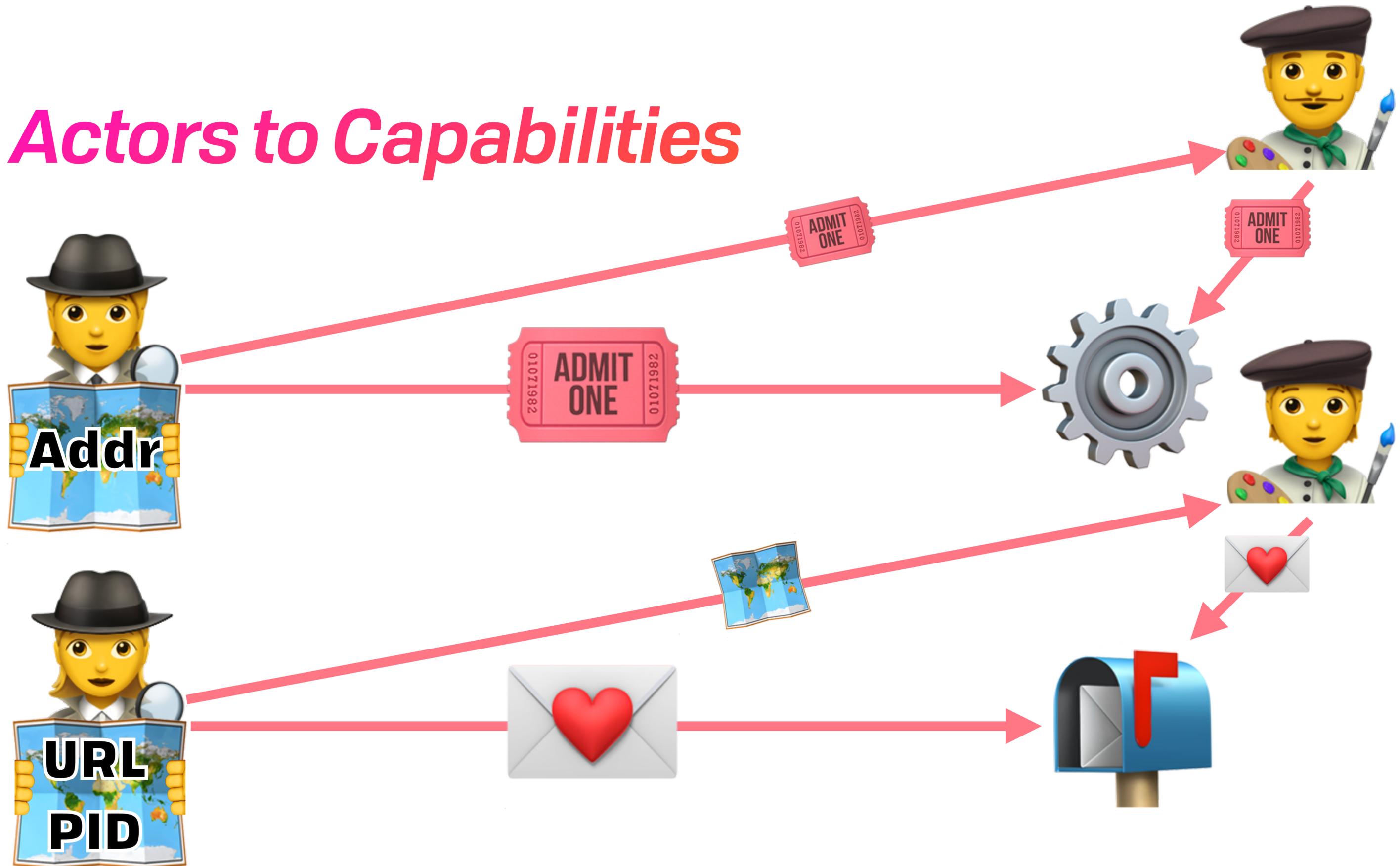
UCAN

From Actors to Capabilities



UCAN

From Actors to Capabilities



UCAN

Rights Amplification

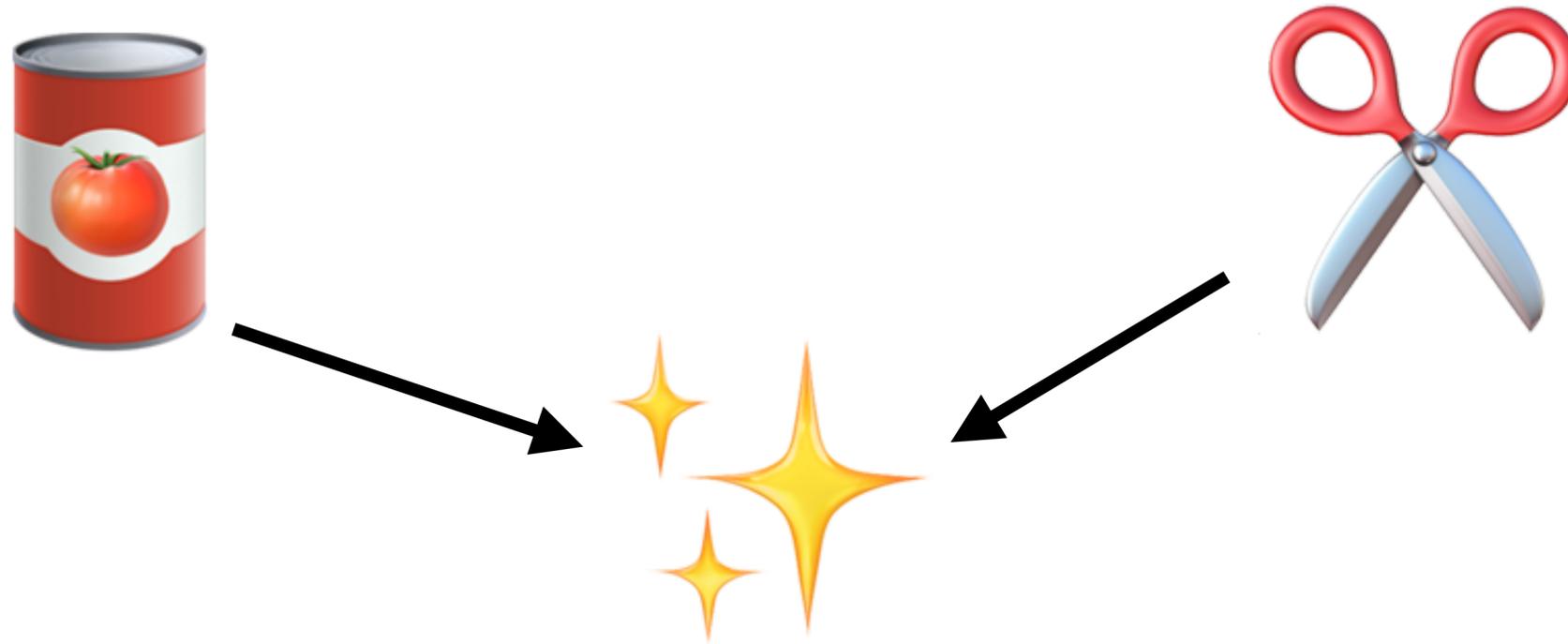
UCAN

Rights Amplification



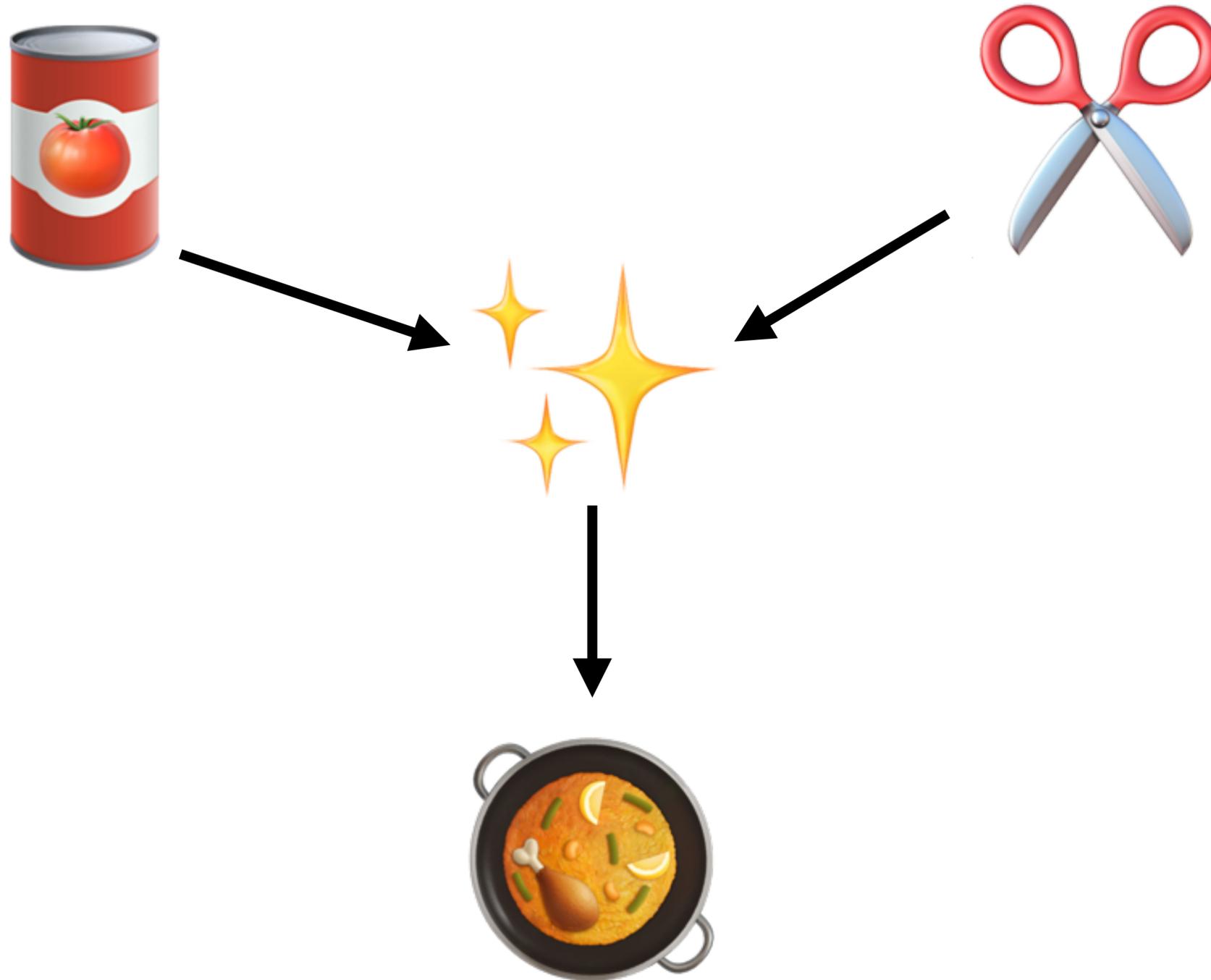
UCAN

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

Payload

Header

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

```
{  
  "iss":  
  "did:key:z6MksXQBfL8owztTCJm7hNRf6b18YxXPp3i66oJHm8L3YGJ"  
  "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

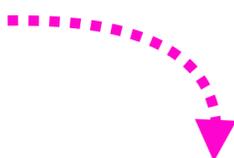
UCAN

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/" (URI)  
    "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/" (URI)  
    "can": "GET"  
  },  
  {  
    Action / "verb"  
    "with": "mailto:boris@fission.codes",  
    "can": "SEND",  
    "to": "/*@fission.codes/"  
  }  
]
```

The diagram illustrates the structure of a UCAN capability. It shows a JSON array containing two objects. The first object represents a resource, with a pink dashed arrow pointing from the label "Resource / 'noun'" to the "with" field value "http://example.com/alice/photos/". The "can" field value "GET" is also highlighted with a pink rounded rectangle, and a pink dashed arrow points from the label "Action / 'verb'" to it. The second object represents an action, with fields "with", "can", and "to".

UCAN

Anatomy of a Capability

```
[  
  {  
    Resource / "noun"  
    "with": "http://example.com/alice/photos/" (URI)  
    "can": "GET"  
  },  
  {  
    Action / "verb"  
    "with": "mailto:boris@fission.codes",  
    "can": "SEND",  
    "to": "/*@fission.codes/" Extensible fields  
  }  
]
```

UCAN

Chain Witnesses

UCAN

Chain Witnesses



UCAN

Chain Witnesses



UCAN

Chain Witnesses



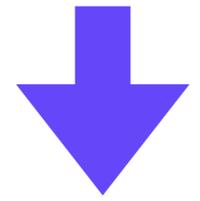
UCAN

Chain Witnesses



UCAN

Chain Witnesses

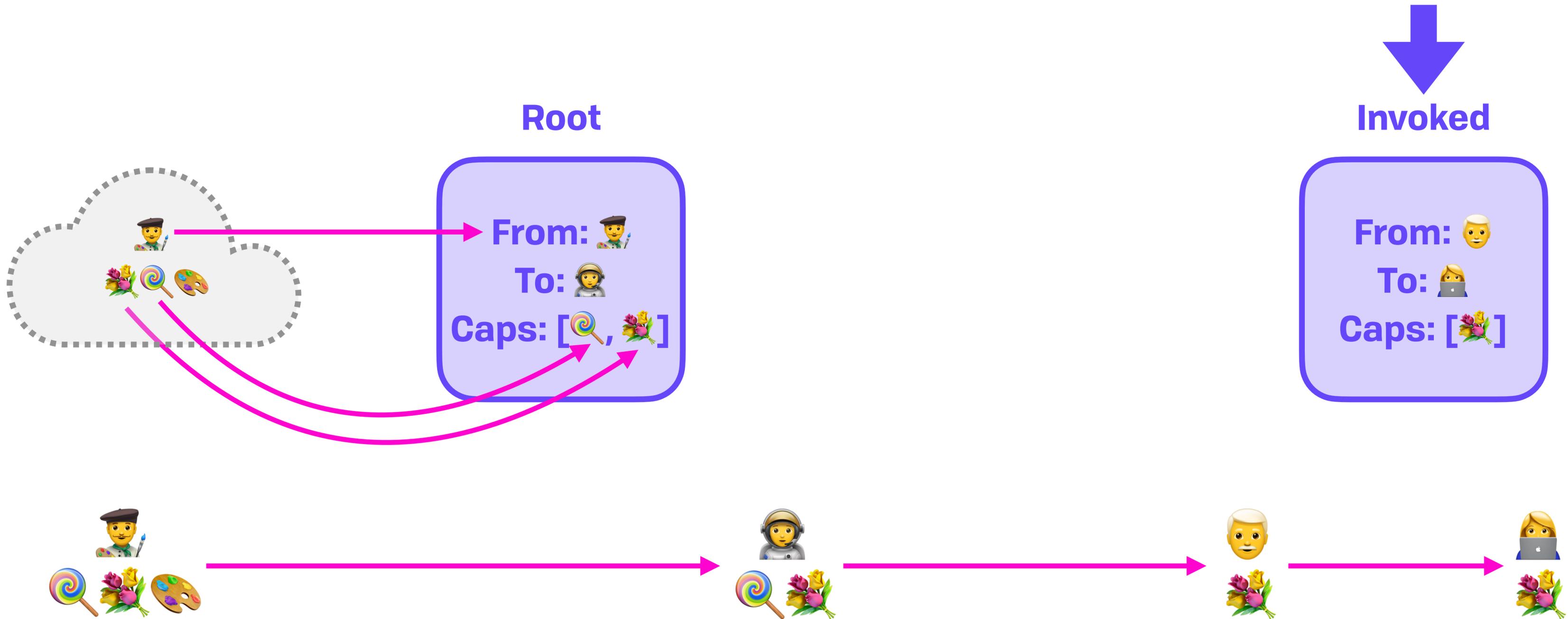


Invoked



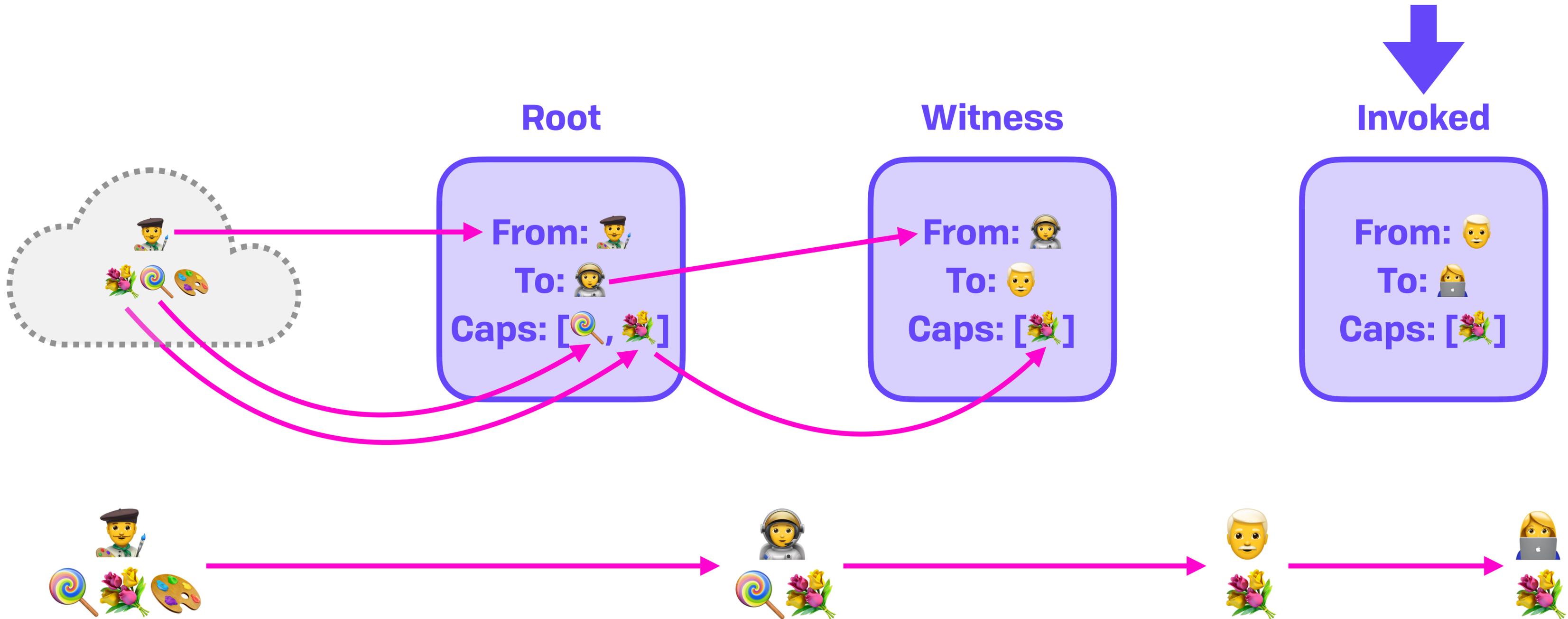
UCAN

Chain Witnesses



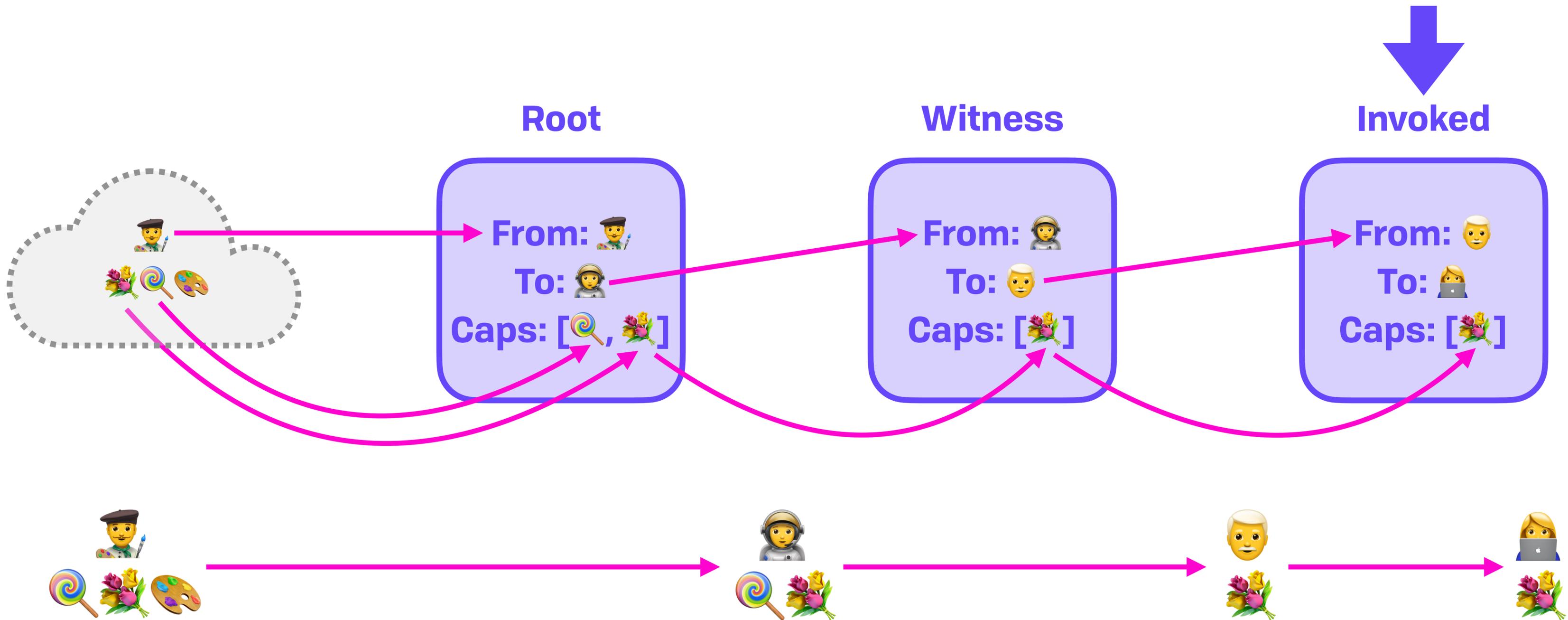
UCAN

Chain Witnesses



UCAN

Chain Witnesses



UCAN

Zoomed Out

UCAN

Zoomed Out



UCAN

Zoomed Out



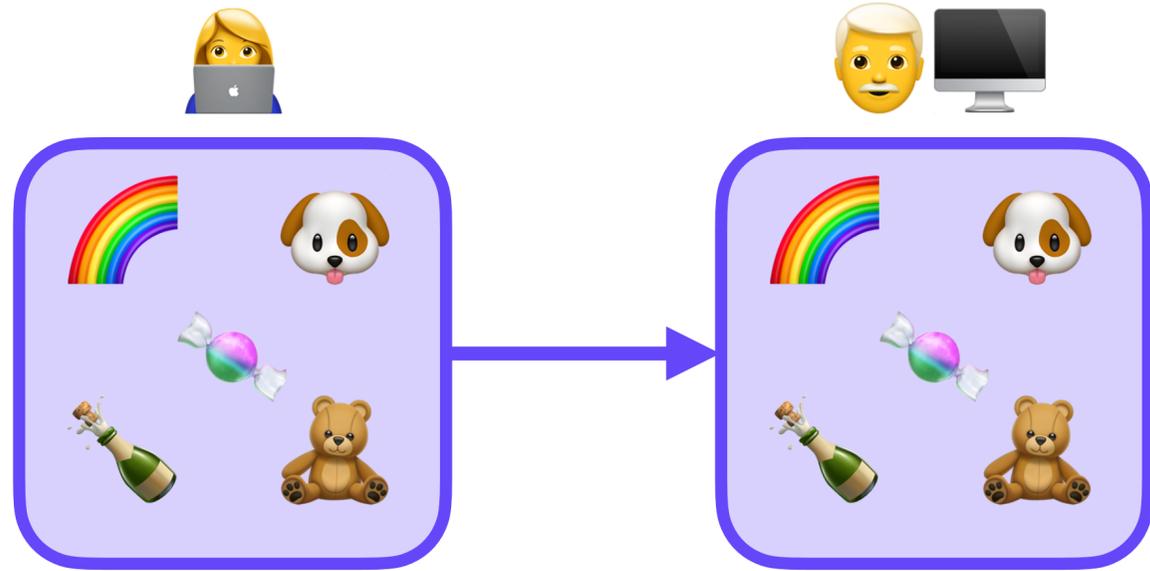
UCAN

Zoomed Out



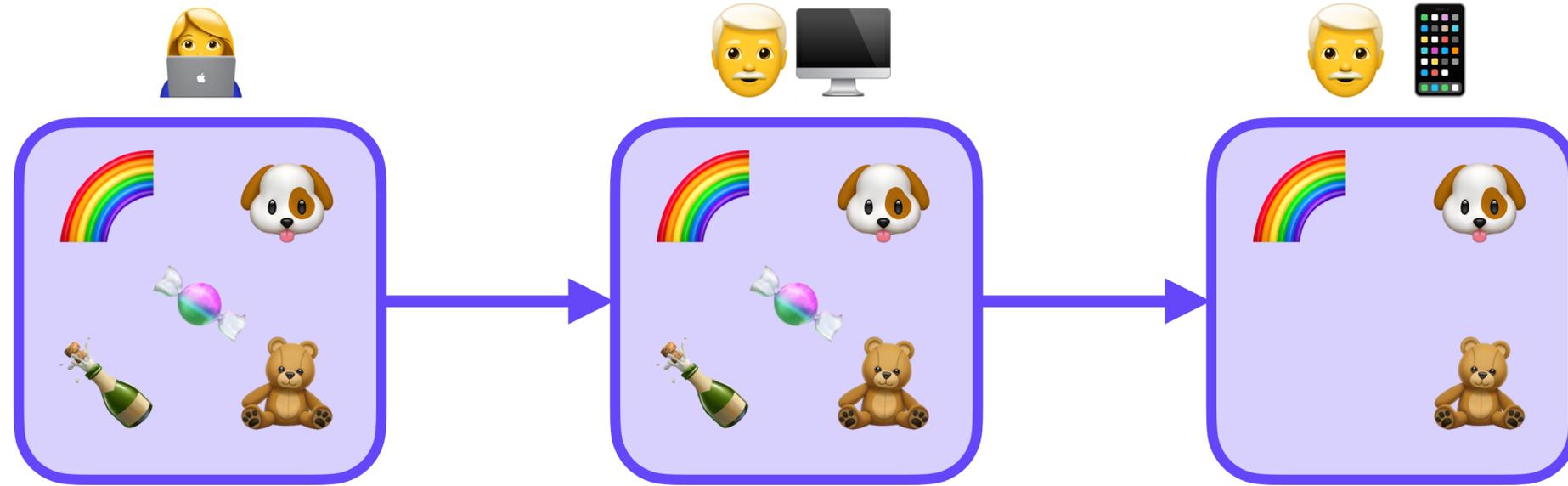
UCAN

Zoomed Out



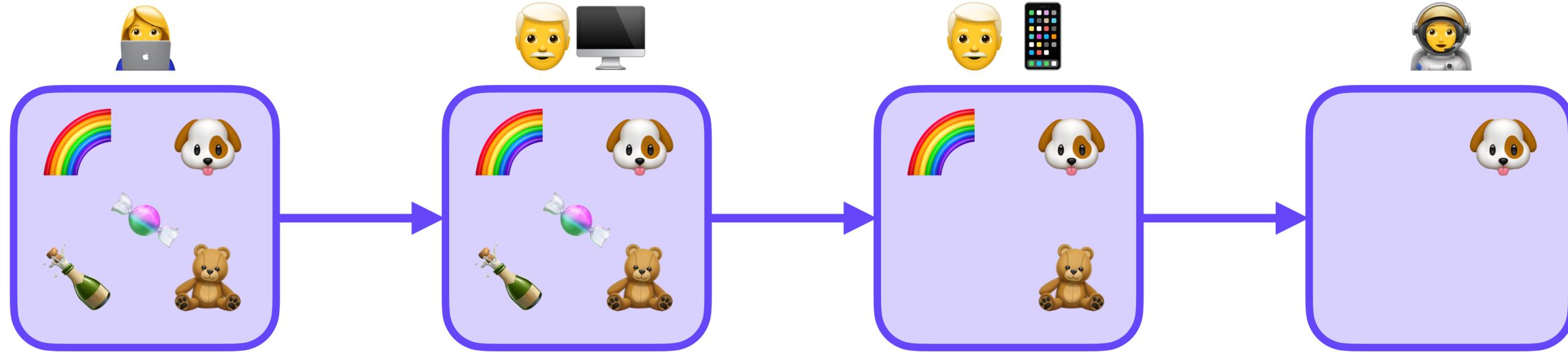
UCAN

Zoomed Out



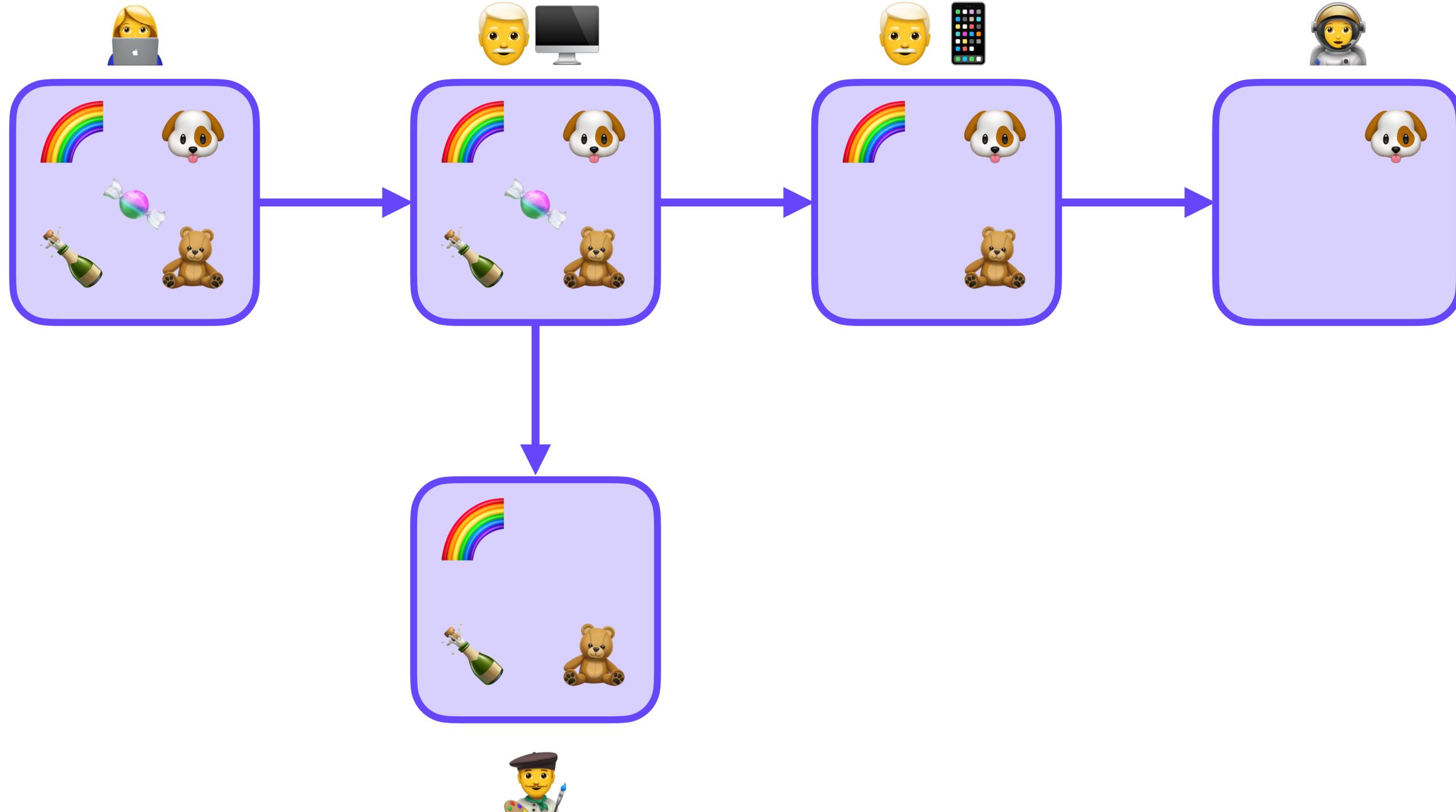
UCAN

Zoomed Out



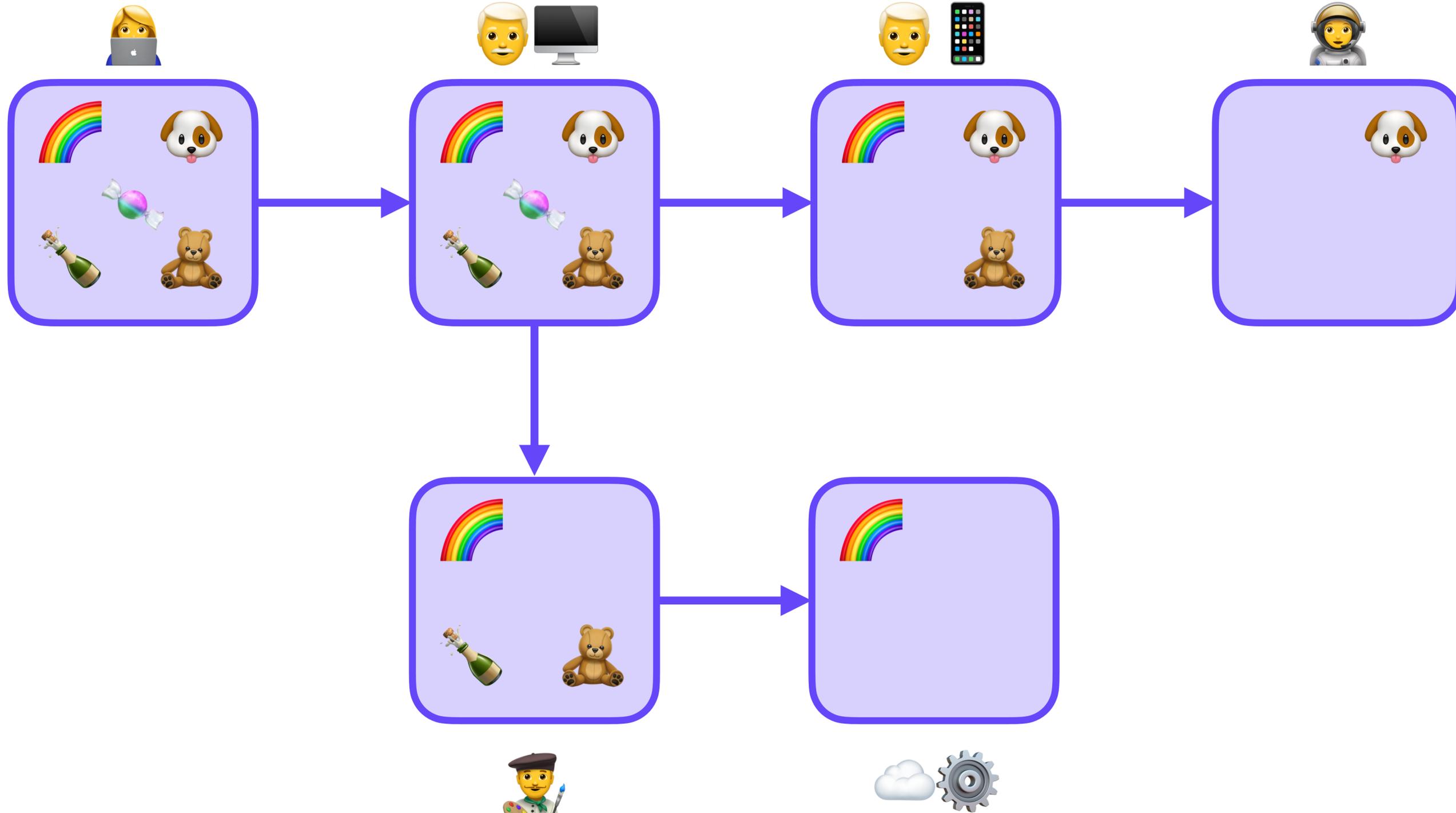
UCAN

Zoomed Out



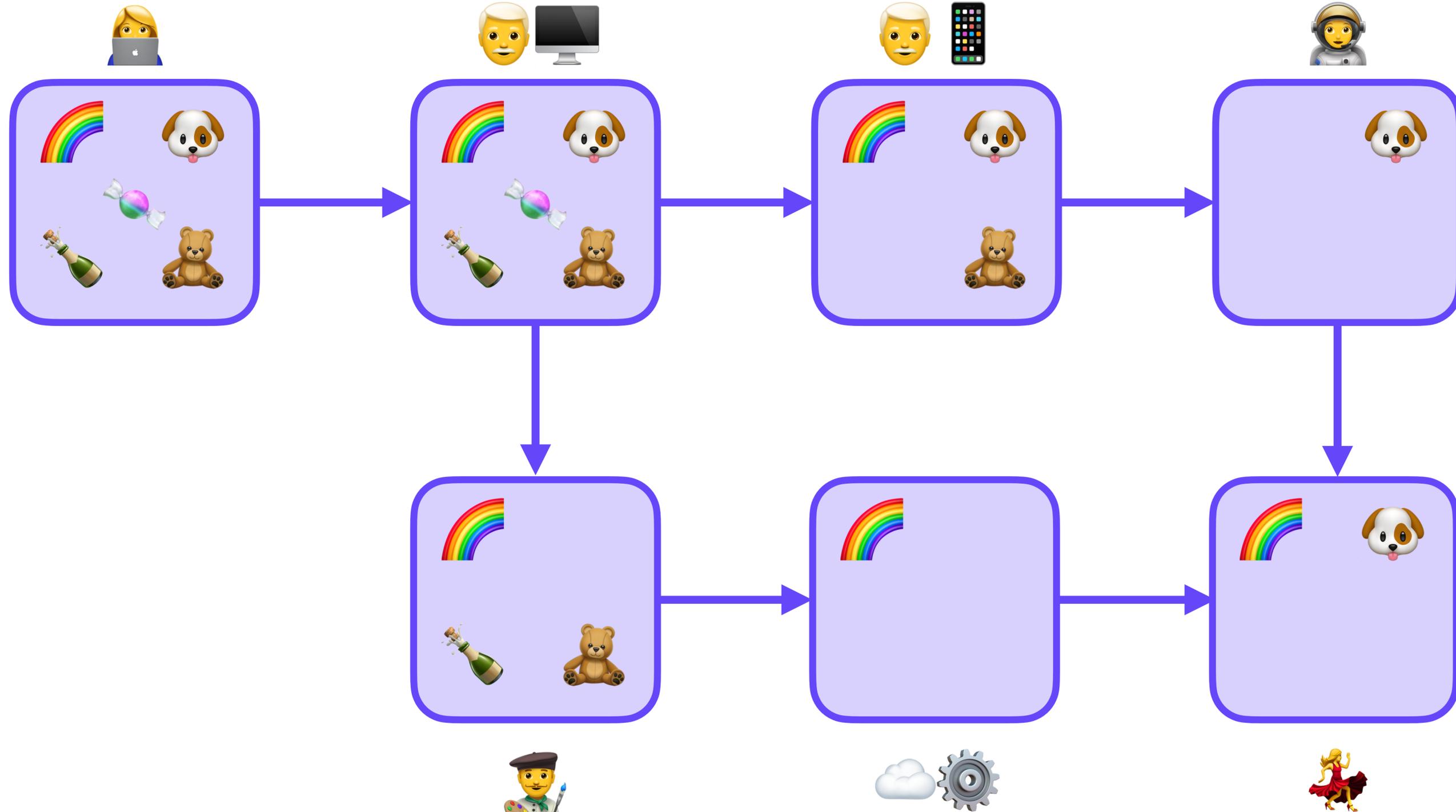
UCAN

Zoomed Out



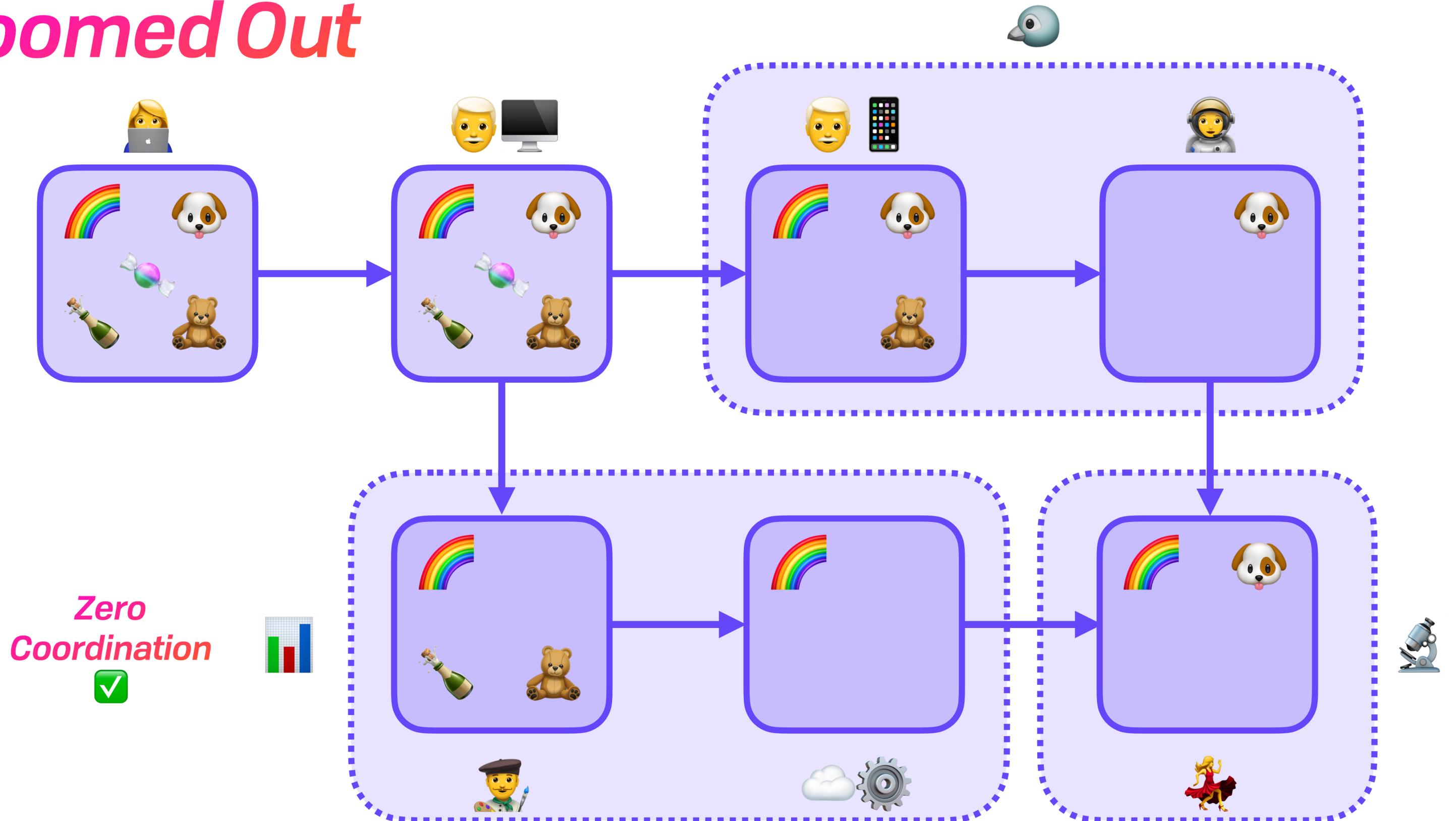
UCAN

Zoomed Out



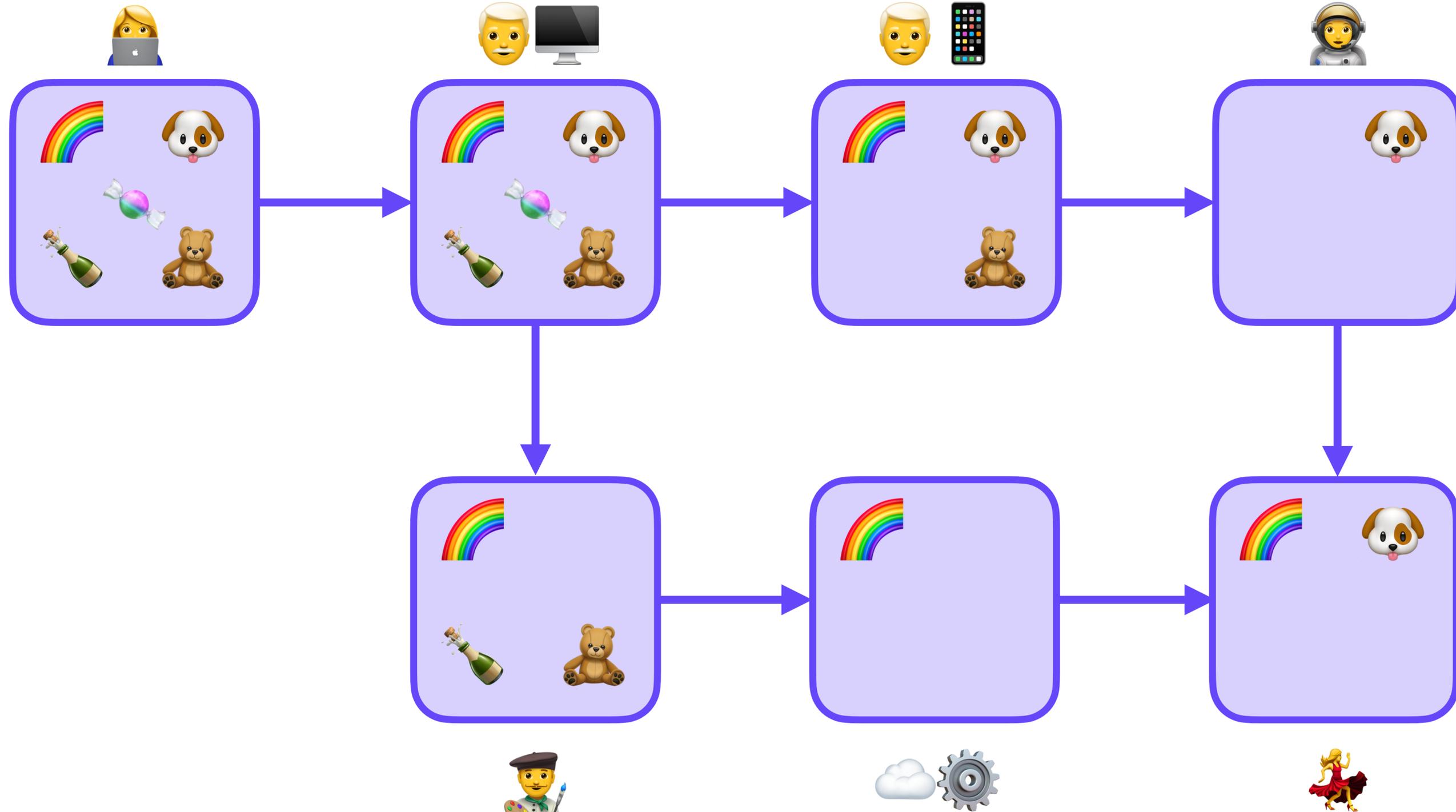
UCAN

Zoomed Out



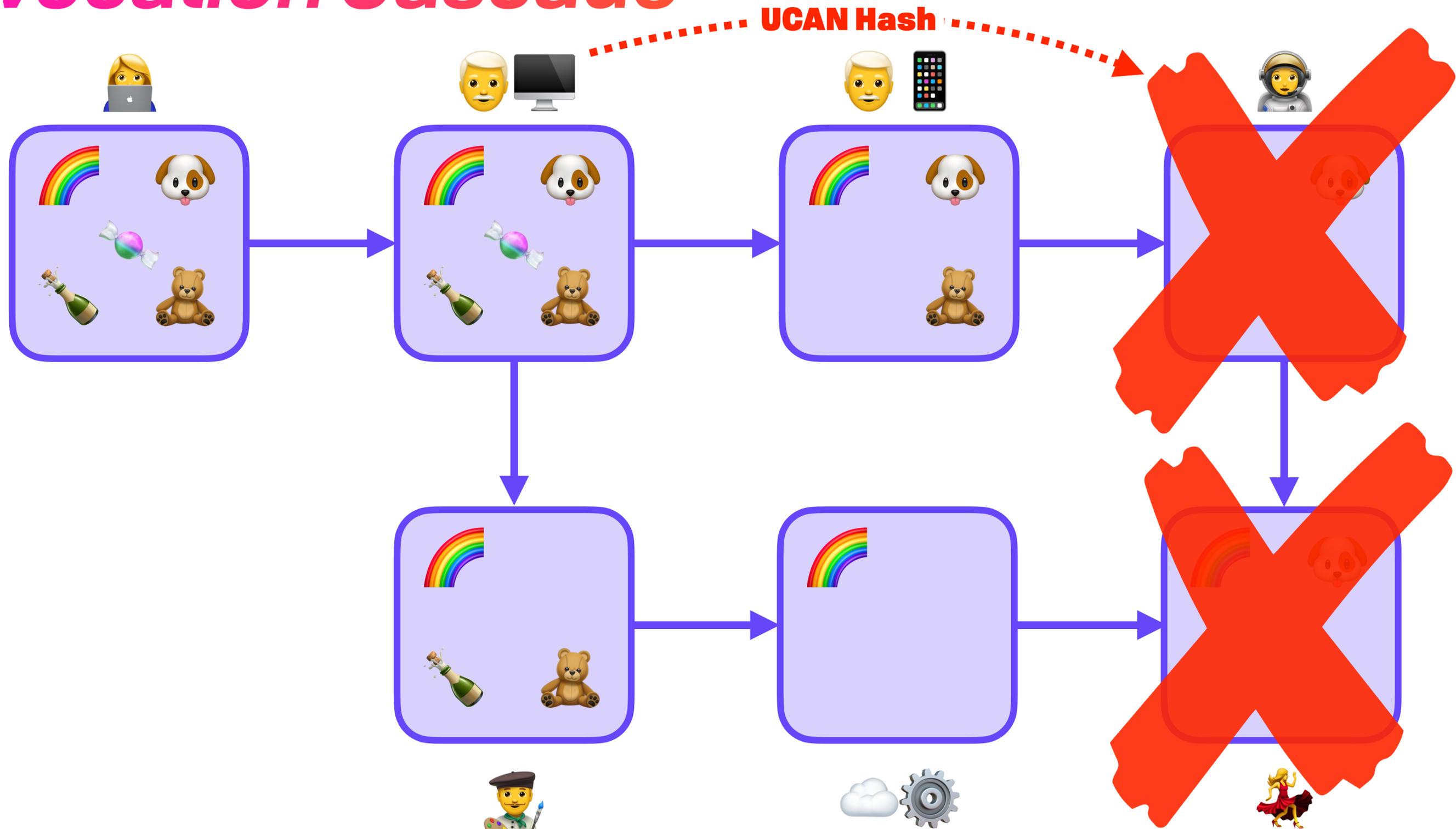
UCAN

Revocation Cascade



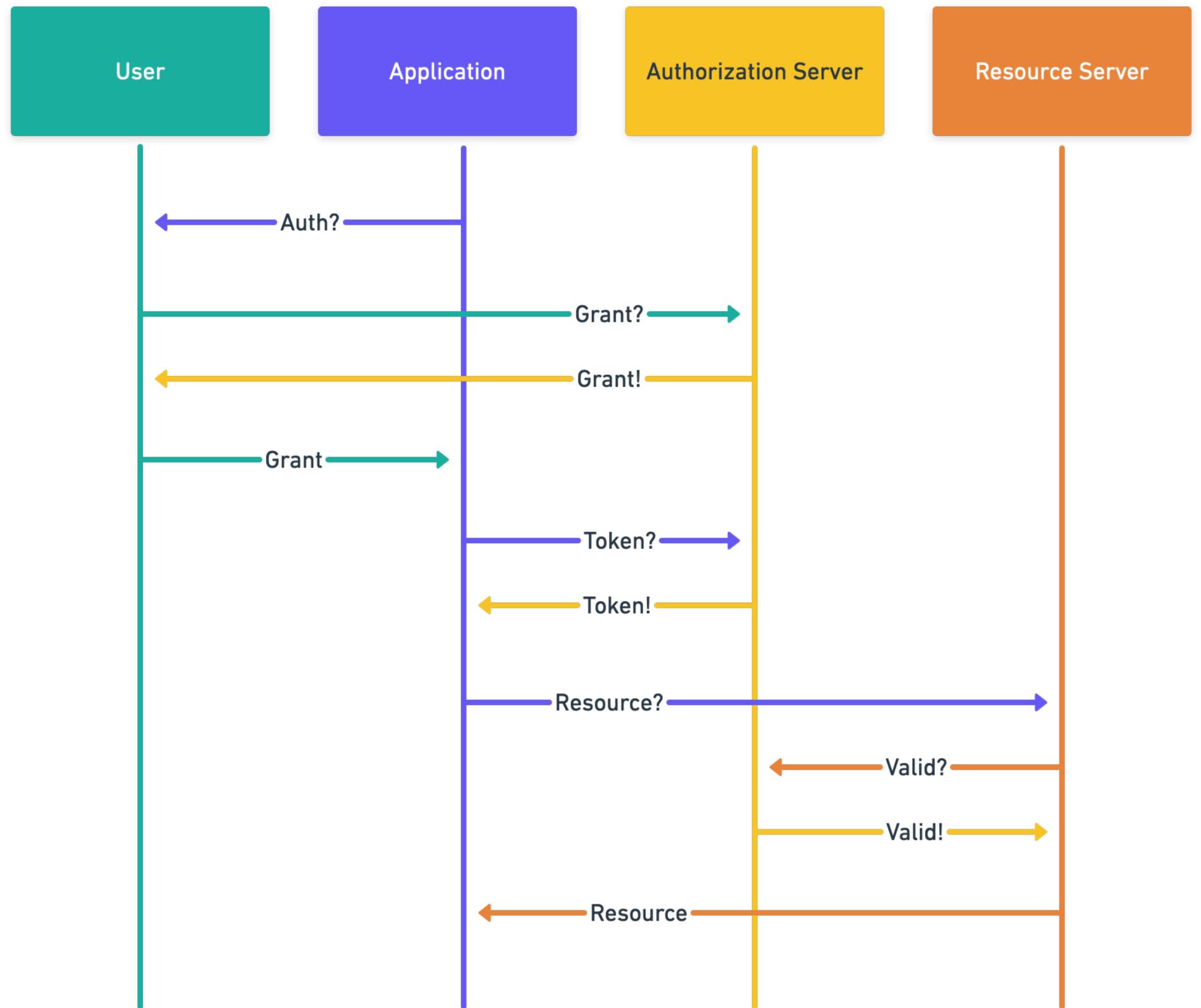
UCAN

Revocation Cascade



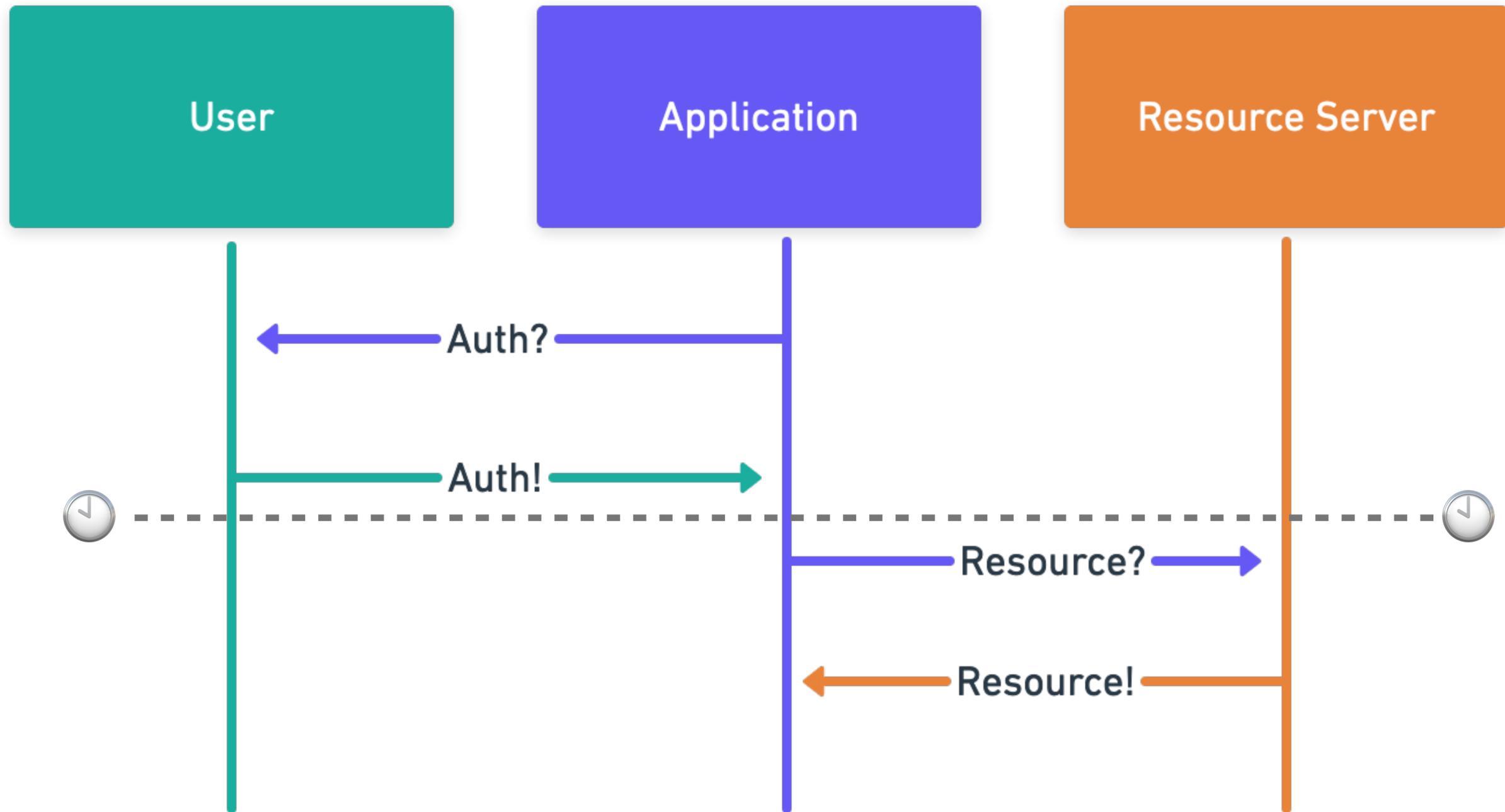
UCAN

OAuth Sequence



UCAN

UCAN Sequence



Nontrivial Example



Nontrivial Example

Encoded

Nontrivial Example

Encoded

eyJhbGciOiJFZERTQSIiInR5cCI6IkpXVCIsInVjdiI6IjAuNy4wIn0.eyJhdWQiOiJkaWQ6a2V50no2T
Wt2WGZQVXY4Ynh0c1ZRaUdvN050azRxS0p0Y2dLMml0NTJwYzcdGVVcFJMVCIiImF0dCI6W3sid25mcy
I6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvcGhvdG9zLyIsImNhci6I6Ik9WRVJXUklURSJ9LHs
id25mcyI6ImRlbW91c2VyLmZpc3Npb24ubmFtZS9wdWJsaWMvbm90ZXMvIiwia2FwIjoiaT1ZFUldSSVRF
In1dLCJleHAiOiJkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKVG03aE5SZ
jZiMThZeFhQcDNpNjZvSkht0EwzWUdKIiwibmJmIjojoxNjM5NjA4MjkzLCJwcmYiOiIsiZlKaGJHY2lPaU
pGwkVSVFFTSXNjbI1Y0NjNkIrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E
2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnR0MmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBj
YlRoTU0xbEhTaUlsSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMvVnI6ImVpYzN0cGIyNHVibUZ0W
lM5d2RXSnNhV012Y0dodmRH0XpMeUlsSW10aGNDSTZJazlXUllZKWFVrbFVSU0o5WFN3aVpYaHdJam81TW
pVMk9UTTVOVEExTENKcGMzTWlPaUprYVdRNmEyVjVPbm8yVFd0d05VVnplamx6TWsxSWMzRlpka3h2WTJ
0NVNIZFl0Vks5sZVZwTGNIrTNPVWQwTkRwbVJrZEZXBek1T1Njc0ltNWlaaUk2TVRZek9UWXDPREk1TXl3
aWNISm1JanBiWFgwLjRUTmh1SFJyUEc5YUhv0DY5SFhsc05L0F9GbWXTaFE1R3pHNGl0TjJ0S2steUtUY
kFNb0Z3VHVwdEcwWEZnTkI2SHVsUHBsVnpaWURWRGV4bzc2a0F3Iiwia2FwIjoiaT1ZFUldSSVRFIn1dLCJleHAiOiJkyNTY5Mzk1MDUsImZcyI6ImRpZDprZXk6ejZNa3NYUUJmTDhvd3p0VENKVG03aE5SZjZiMThZeFhQcDNpNjZvSkht0EwzWUdKIiwibmJmIjojoxNjM5NjA4MjkzLCJwcmYiOiIsiZlKaGJHY2lPaUUpGwkVSVFFTSXNjbI1Y0NjNkIrcFhWQ0lzSW5WamRpSTZJakF1Tnk0d0luMC5leUpoZFdRaU9pSmthV1E2YTJWNU9ubzJUV3R6V0ZGQ1prdzRiM2Q2ZEZSRFNsUnR0MmhPVW1ZMllqRTRXWGhZVUhBemFUWTJiMHBjYlRoTU0xbEhTaUlsSW1GMGRDSTZXM3NpZDI1bWN5STZJbVJsYlc5MWMvVnI6ImVpYzN0cGIyNHVibUZ0WlM5d2RXSnNhV012Ym05MFpYTXZJaXdpWTJGd0lqb2lUMVpGVWxkU1NWUkZJbjFkTENKbGVlQWlPamt5TlRZNU16azFNRFVzSW1semN5STZJbVJwWkRwcLpYazZlaLp0YTNBMVJYTjZPWE15VFVoemNwbDJURzllqWTNsSWQxZzFVmlY1V2t0d2NUYzVSM1EwTldaR1IwVmFVams1SWl3aWJtSm1Jam94TmPNUU5qQTRNamt6TENKd2NtWwlpbHRkZlEuTWdZYXJMcXk3Um1RMUFJcnFZTDZjRnk5ejdhNVdJQVUtLVRZQVJQU2dpck9Tc3p2YXIzX0R0cjI1cmJQcmV0SGJuVDBtTVZLeW9hUVhydVI3S2JyQmciXX0.kwRdqPN74pkcpXGgdk7Z7FW3M1mRRYaDE5ZgkG6srAuu6V6mvMVRdBLnD5Cwid-X4tDIKplivjlCSLTntB4pCw

Nontrivial Example

Decoded Witness #1

Payload

Header

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

```
{  
  "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_Fm1ShQ5GzG  
4itN2NKk-  
yKTbAMoFwTuptG0XFgNIvHulPplVzZYDVDe  
xo76kAw
```

Nontrivial Example

ucan.xyz — Online Explorer / Validator

Nontrivial Example

ucan.xyz — Online Explorer / Validator

Hey there 🤖
You are using a preview version of UCAN Check. This version only supports the latest UCAN version. Try out the [UCAN library](#) to make some!

UCAN Check

Encoded

Paste an encoded UCAN

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTJ0IiwiaWF0IjoiYXN5bWVudC5kaWQ6a2V5Ono2TWtZWFFCZ  
kw4b3d6dFRDSIRIN2hOumY2YjE4WkYyUHAzaTY2b0plbThMM1HSIsImF0dCI6W3sid25mcyI6ImRlbW91  
c2VyLmZpc3Npb24ubmFIZS9wdWJ3aWVmcGhvdG9zLyIsImNhcCI6Ikh9WRV3XUkiUR539S5wZXBwIjoiMjU  
2OTM5NTA1LCJpc3MiOiJkaWQ6a2V5Ono2TWtWNUVzejlzMK1Ic3FZdkxvY2N5SHdYVnVleVpLcHE3OUd0ND  
VmRkdFwII5O5IsIm5iZiI6MTYzOTYwODI5MywiczHmIjpbXX0.4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5Gz  
G4iN2NKK-yKTbAMoFwTuptG0XFGNivHulPpIvZyYDvDexo76kAw
```

Decoded

Header

```
{  
  "alg": "EdDSA",  
  "typ": "JWT",  
  "ucv": "0.7.0"  
}
```

Payload

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

Signature

```
4TNhuHRrPG9aHo869HXlsNKB_FmIshQ5GzG4iN2NKK-yKTbAMoFwTuptG0XFGNivHulPpIvZyYDvDexo76kAw
```

Payload

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

Delegate 1 Selected

Valid UCAN. The UCAN is valid and has not expired.

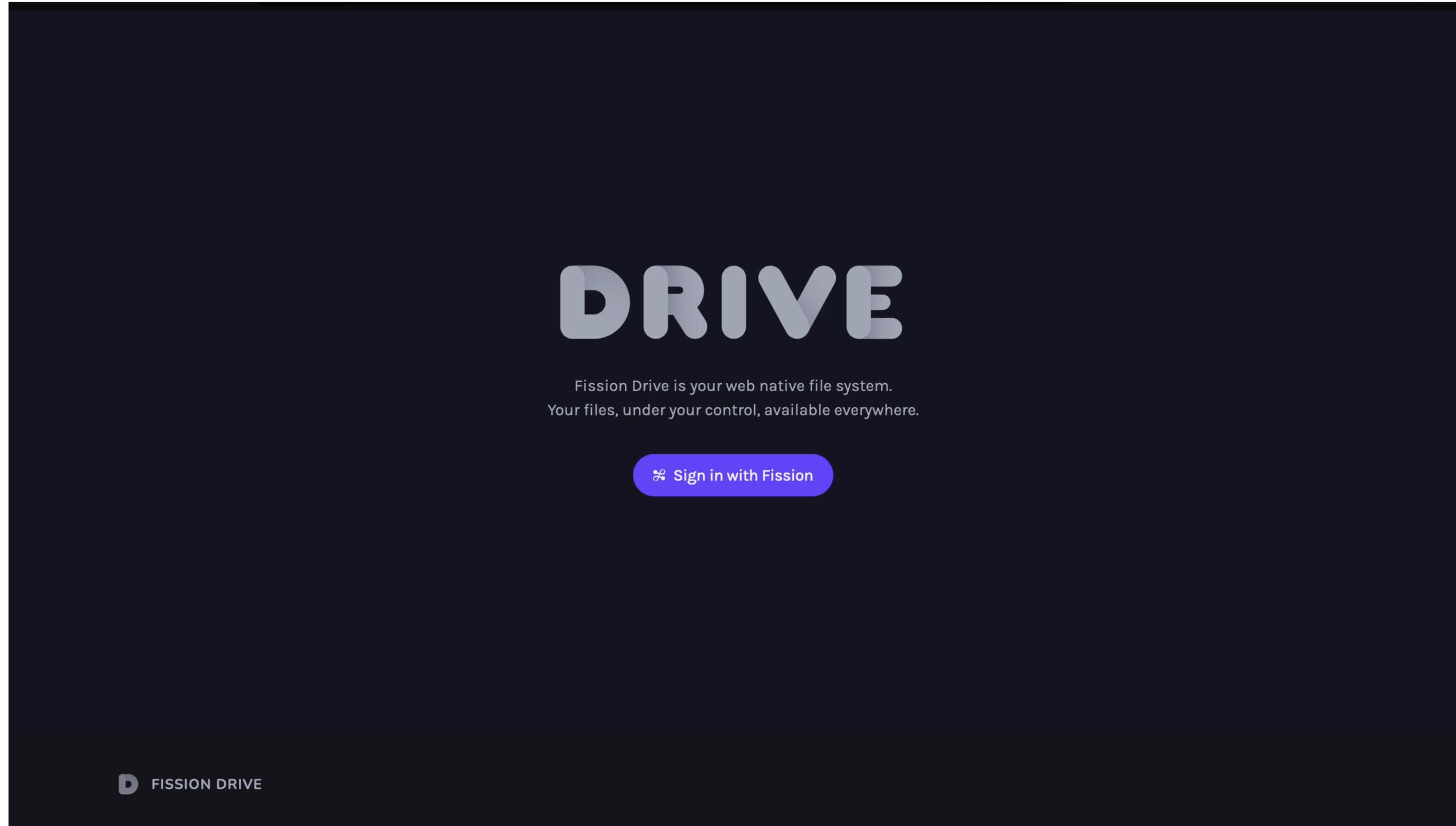
Explanation

Please see the [JWT RFC](#) and the [UCAN specification](#) for more details.

Field	Long Name	Value	Details
alg	Signature Algorithm	EdDSA	The algorithm used to sign the UCAN
typ	Type	JWT	UCANs are JWTs
ucv	UCAN Version	0.7.0	The UCAN version
iss	Issuer	did:key:z6Mkp5Esz9s2MHsqYvLoccyHwX5SeyZKpq79Gt45fFGEZR99	The DID of the issuer. The UCAN must be signed with the private key of the issuer to be valid.
aud	Audience	did:key:z6MksXQBfL8owztTCJTm7hNRf6b18YxXPp3i66oJHm8L3YGJ	The DID of the audience
att	Attenuation	{ "wnfs": "demouser.fission.name/public/photos/", "cap": "OVERWRITE" }	Capabilities granted or delegated to the audience
exp	Expires At	9256939505	The UNIX time when the UCAN expires. This UCAN expires on May 5, 2263 at 5:05:05 AM PDT.
nbf	Not Before	1639608293	The UNIX time after which the UCAN is valid. This UCAN became valid on December 15, 2021 at 2:44:53 PM PST.

Nontrivial Example

Auth Should be Boring!



Nontrivial Example

Auth Should be Boring!

DRIVE

Fission Drive is your web native file system.
Your files, under your control, available everywhere.

 Sign in with Fission

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/acldsont/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