CACAO

Chain Agnostic CApability Object

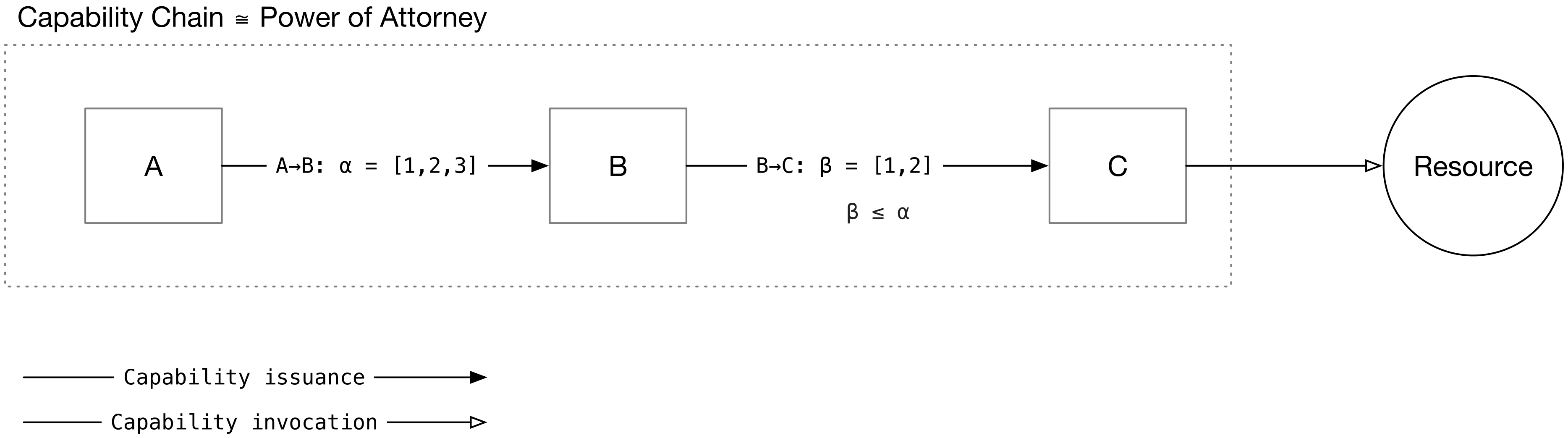
Sergey Ukustov @ Ceramic Network
CASA Gathering, 2022-04-25

ceramic

Basics

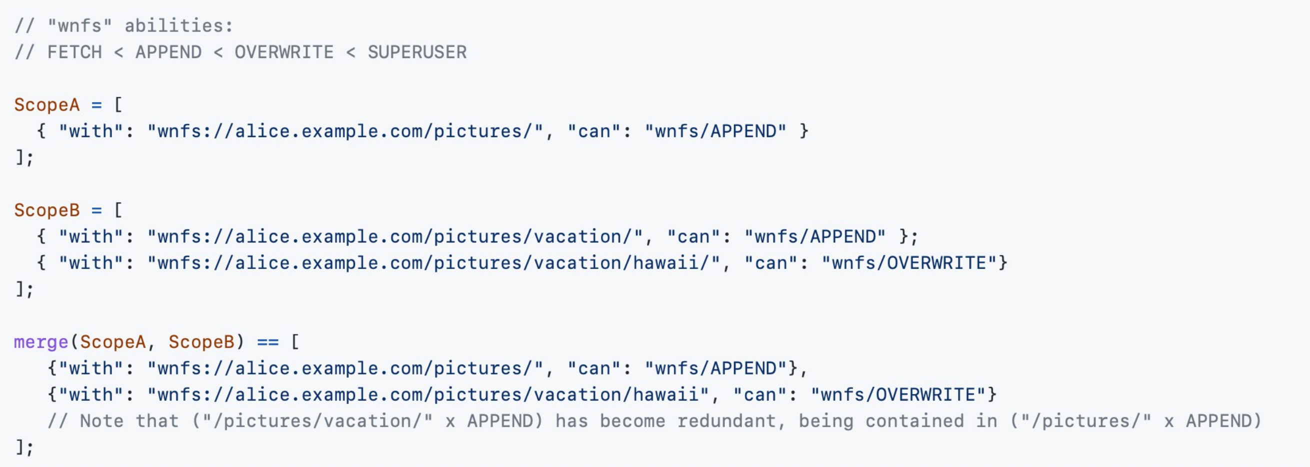
Authorization for Web3

`capability = who + what + proof`



General concerns

- Caveat semantics – application specific
    - caveat = resource + action + conditions
    - merge(A, B): A U B = B U A
    - isPermitted?

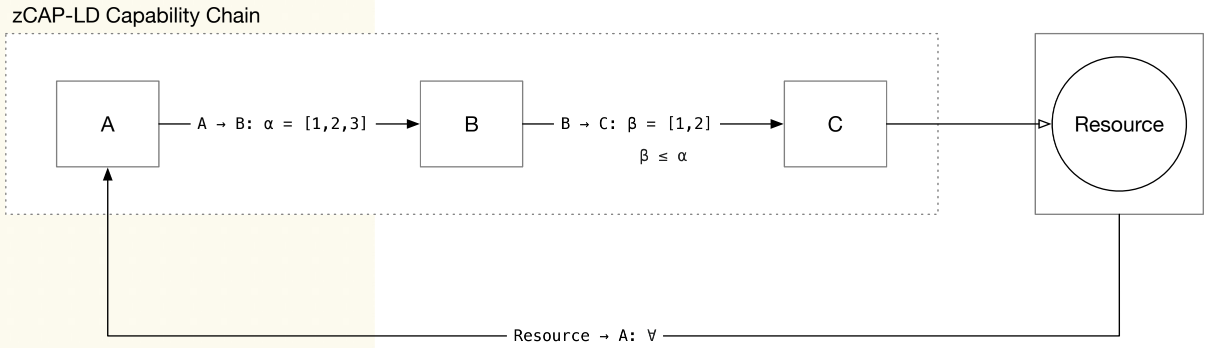


```
// "wnfs" abilities:
// FETCH < APPEND < OVERWRITE < SUPERUSER

ScopeA = [
  { "with": "wnfs://alice.example.com/pictures/", "can": "wnfs/APPEND" }
];

ScopeB = [
  { "with": "wnfs://alice.example.com/pictures/vacation/", "can": "wnfs/APPEND" };
  { "with": "wnfs://alice.example.com/pictures/vacation/hawaii/", "can": "wnfs/OVERWRITE"}
];

merge(ScopeA, ScopeB) == [
   {"with": "wnfs://alice.example.com/pictures/", "can": "wnfs/APPEND"},
   {"with": "wnfs://alice.example.com/pictures/vacation/hawaii", "can": "wnfs/OVERWRITE"}
   // Note that ("/pictures/vacation/" x APPEND) has become redundant, being contained in ("/pictures/" x APPEND)
];
```

- Format
    - store, retrieve, transfer, verify – interoperability
    - compatibility with transport – IPLD, HTTP (including chains)

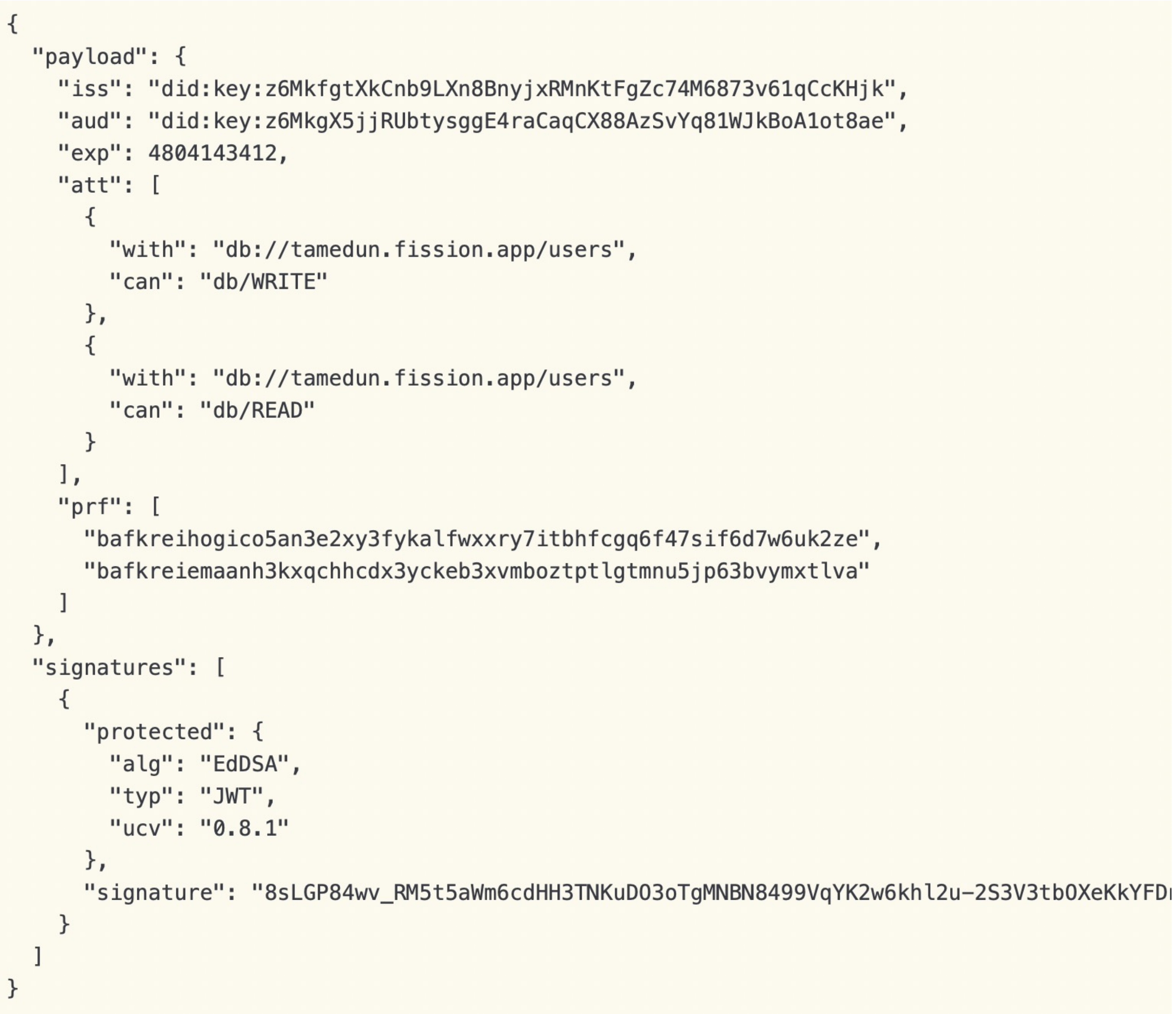
Landscape: zCAP-LD

```
{"@context": ["https://example.org/zcap/v1",
              "https://autopower.example/"],
 "id": "https://social.example/alyssa/caps#79795d78",

 // Pointing up the chain at the capability from which Alyssa was
 // initially gained authority
 "parentCapability": "https://whatacar.example/a-fancy-car/proc/7a397d7b",

 // Alyssa grants authority specifically to one of Ben's
 // cryptographic keys
 "invoker": "https://chatty.example/ben/#key-33",

 // Alyssa adds a caveat: Ben can drive her car, unless she flips
 // the bit at this url
 "caveat": [
   {"type": "ValidWhileTrue",
    "uri": "https://social.example/alyssa/ben-can-still-drive"}],

 // Finally Alyssa signs this object with the key she was granted
 // authority with
 "proof": {
    "type": "RsaSignature2016",
    "proofPurpose": "capabilityDelegation",
    "created": "2017-03-28T06:01:25Z",
    "creator": "https://social.example/alyssa/#key-for-car",
    "signatureValue": "..."}}
```



- ❌ Serialization
- ❌ Caveats semantics
- 🟡 Chain semantics
- ✅ Existing tooling available

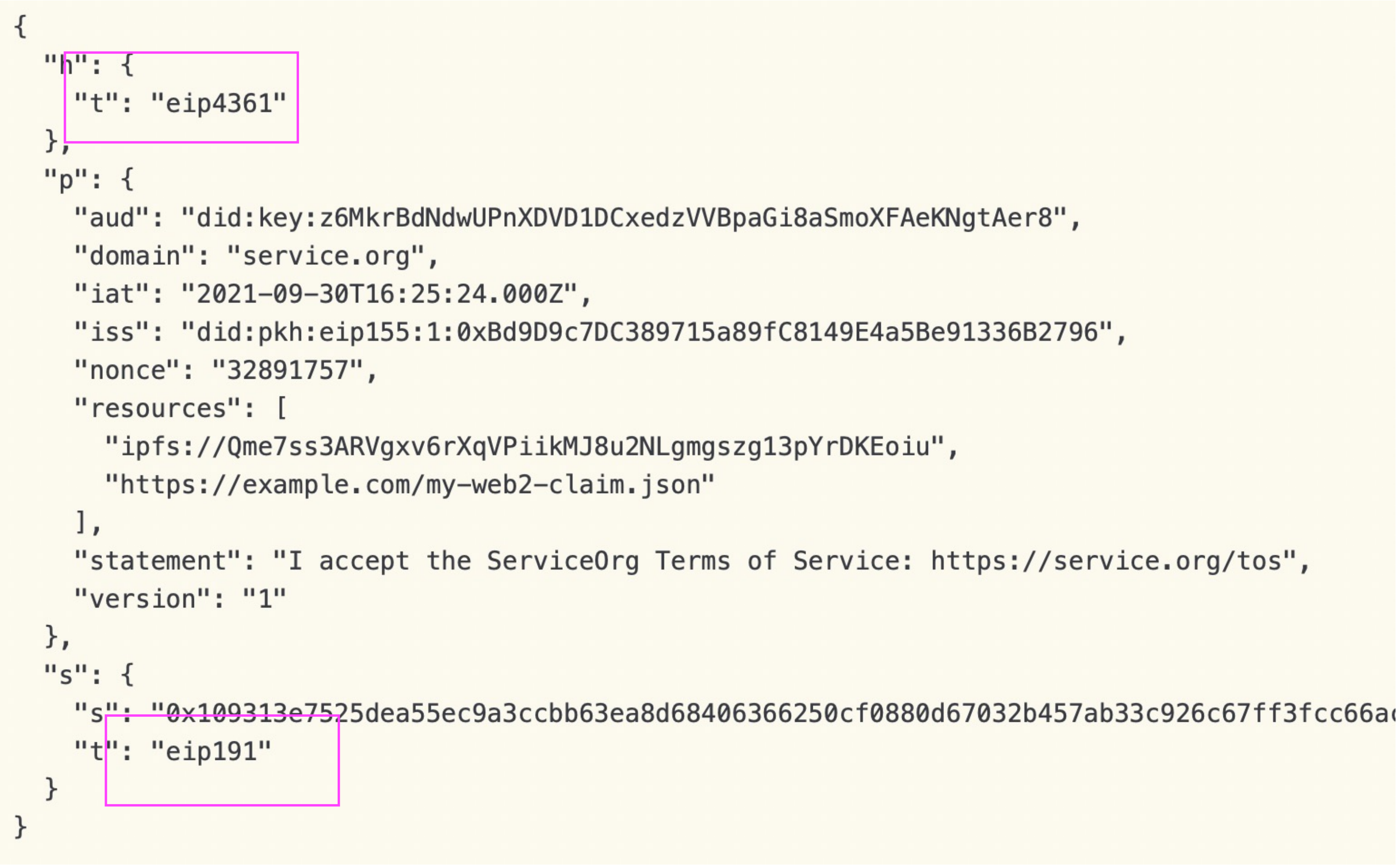
Landscape: UCAN



```
{
  "payload": {
    "iss": "did:key:z6MkfgtXkCnb9LXn8BnyjxRMnKtFgZc74M6873v61qCcKHjk",
    "aud": "did:key:z6MkgX5jjRUbtysggE4raCaqCX88AzSvYq81WJkBoA1ot8ae",
    "exp": 4804143412,
    "att": [
      {
        "with": "db://tamedun.fission.app/users",
        "can": "db/WRITE"
      },
      {
        "with": "db://tamedun.fission.app/users",
        "can": "db/READ"
      }
    ],
    "prf": [
      "bafkreihogico5an3e2xy3fykalfwxxry7itbhfcgq6f47sif6d7w6uk2ze",
      "bafkreiemaanh3kxqchhcdx3yckeb3xvmboztptlgtmnu5jp63bvymxtlva"
    ]
  },
  "signatures": [
    {
      "protected": {
        "alg": "EdDSA",
        "typ": "JWT",
        "ucv": "0.8.1"
      },
      "signature": "8sLGP84wv_RM5t5aWm6cdHH3TNKuDO3oTgMNBN8499VqYK2w6khl2u-2S3V3tbOXeKkYFD
    }
  ]
}
```

- 🟡 IPLD Serialization
- ✅ JWT compatibility
- ✅ Caveats semantics: UCAN
- ✅ Existing tooling available

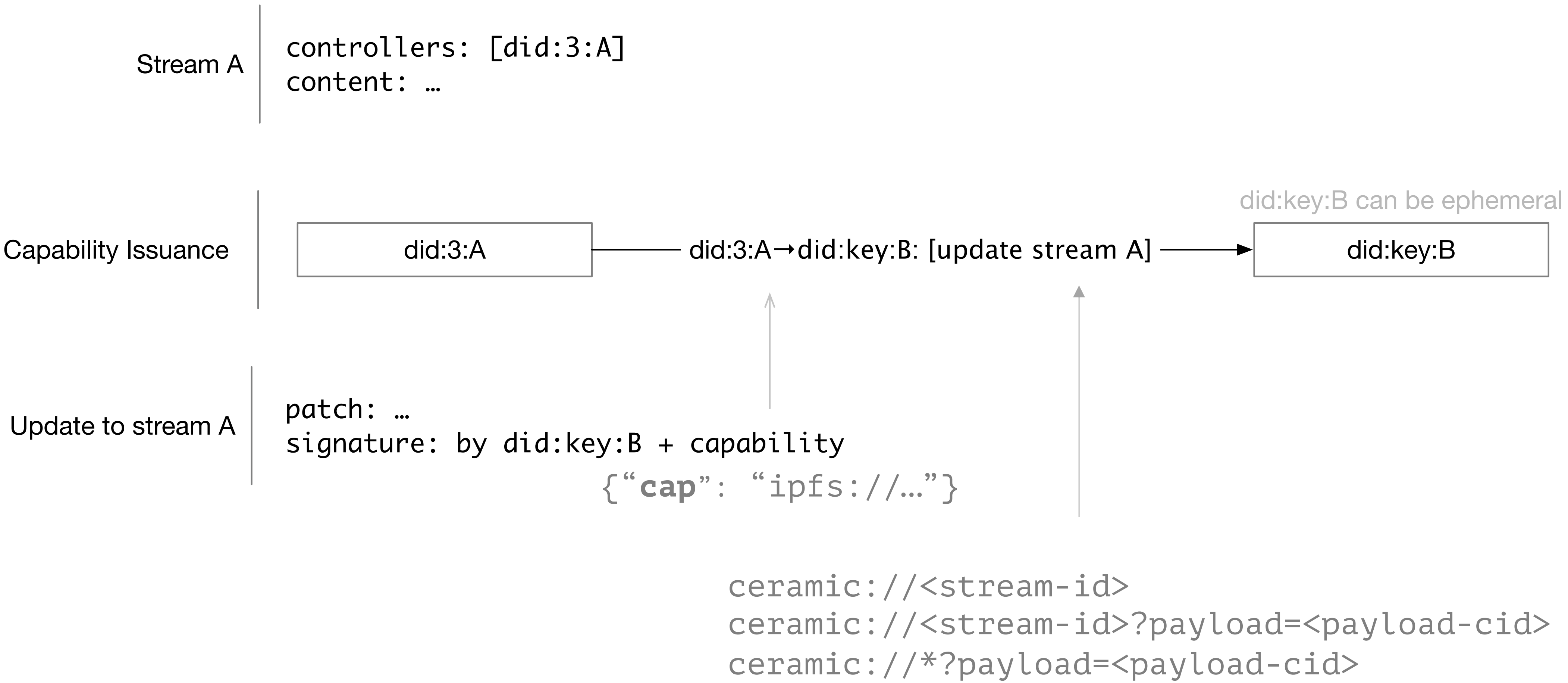
CACAO



```
{
  "h": {
    "t": "eip4361"
  },
  "p": {
    "aud": "did:key:z6MkrBdNdwUPnXDVD1DCxedzVVBpaGi8aSmoXFAeKNgtAer8",
    "domain": "service.org",
    "iat": "2021-09-30T16:25:24.000Z",
    "iss": "did:pkh:eip155:1:0xBd9D9c7DC389715a89fC8149E4a5Be91336B2796",
    "nonce": "32891757",
    "resources": [
      "ipfs://Qme7ss3ARVgxv6rXqVPiikMJ8u2NLgmgszg13pYrDKEoiu",
      "https://example.com/my-web2-claim.json"
    ],
    "statement": "I accept the ServiceOrg Terms of Service: https://service.org/tos",
    "version": "1"
  },
  "s": {
    "s": "0x109313e7525dea55ec9a3ccbb63ea8d68406366250cf0880d67032b457ab33c926c67ff3fcc66a
    "t": "eip191"
  }
}
```

- ✅ Serialization
- 🟡 Caveats semantics
- ✅ Payload semantics
- 🟡 New kid on the block

CACAO with Ceramic



Stream A

```
controllers: [did:3:A]
content: …
```

Capability Issuance

did:3:A

did:3:A→did:key:B: [update stream A]

did:key:B

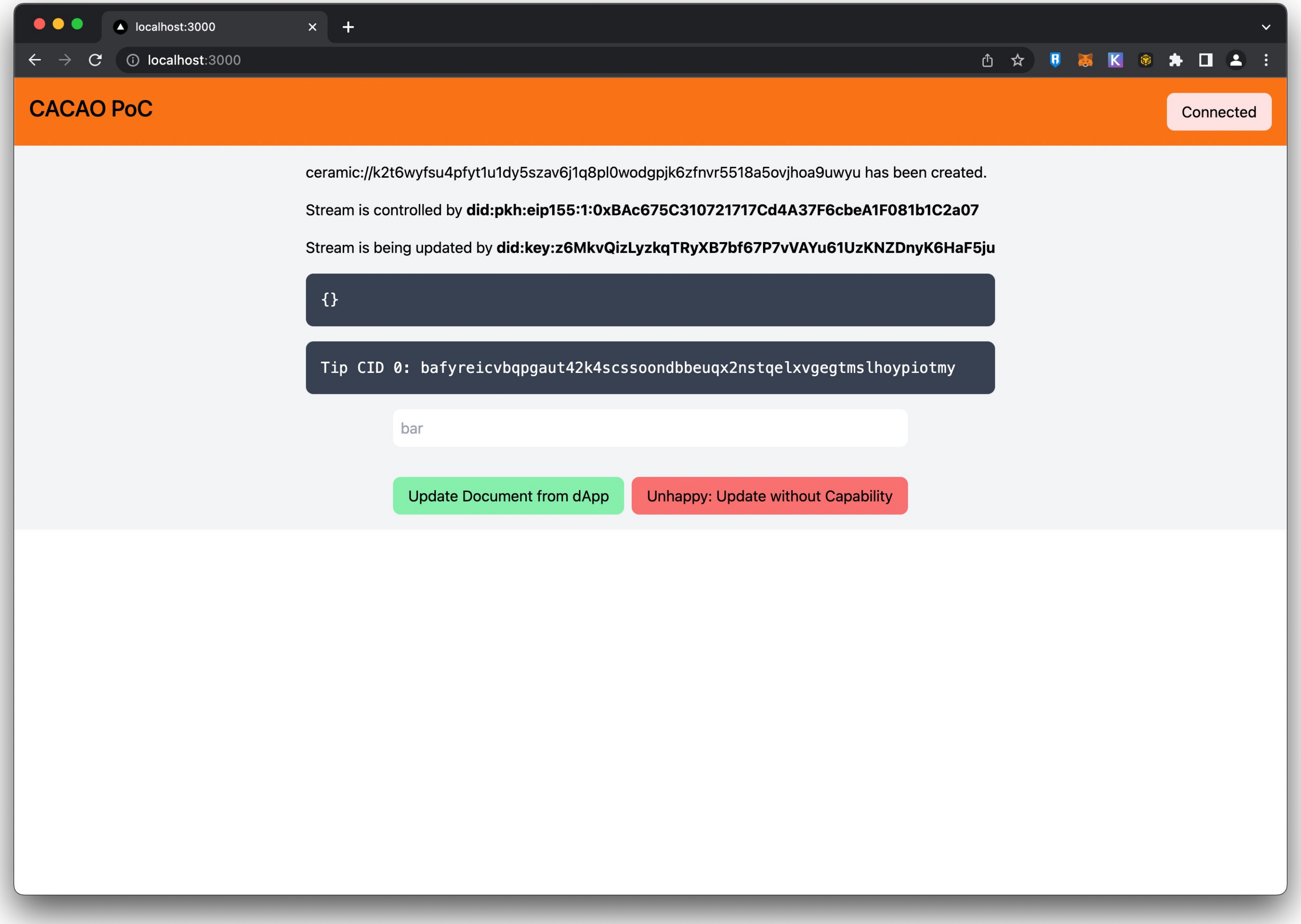
did:key:B can be ephemeral

Update to stream A

```
patch: …
signature: by did:key:B + capability
{“cap”: “ipfs://…”}
```

```
ceramic://<stream-id>
ceramic://<stream-id>?payload=<payload-cid>
ceramic://*?payload=<payload-cid>
```

CACAO with Ceramic



ceramic://k2t6wyfsu4pfyt1u1dy5szav6j1q8pl0wodgpjk6zfnvr5518a5ovjhoa9uwyu has been created.

Stream is controlled by **did:pkh:eip155:1:0xBAc675C310721717Cd4A37F6cbeA1F081b1C2a07**

Stream is being updated by **did:key:z6MkvQizLyzkqTRyXB7bf67P7vVAYu61UzKNZDnyK6HaF5ju**

```
{}
```

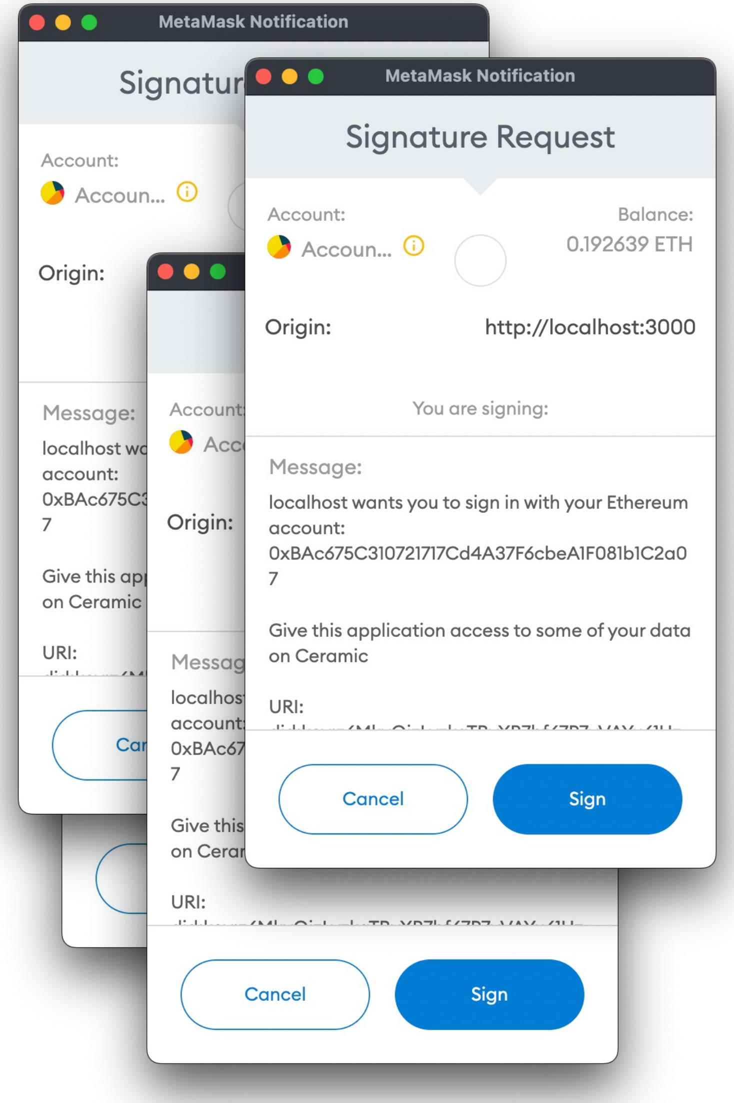
```
Tip CID 0: bafyreicvbqpgaut42k4scssoondbbeuqx2nstqelxvgegtmslhoypiotmy
```

bar

https://github.com/haardikk21/cacao-poc

Benefits

- Privacy as a user-controlled data flow
    - Off-chain
    - Decentralized
    - Narrow permissions
    - Application specific
- Better UX and DX
- Better security



Account: Accoun...

Balance: 0.192639 ETH

Origin: http://localhost:3000

You are signing:

Message:

localhost wants you to sign in with your Ethereum account:
0xBAc675C310721717Cd4A37F6cbeA1F081b1C2a07

Give this application access to some of your data on Ceramic

URI:

Thank you!

@ukstv

@ceramicnetwork