PLC for You and Me

Bryan Newbold / Bluesky PBC

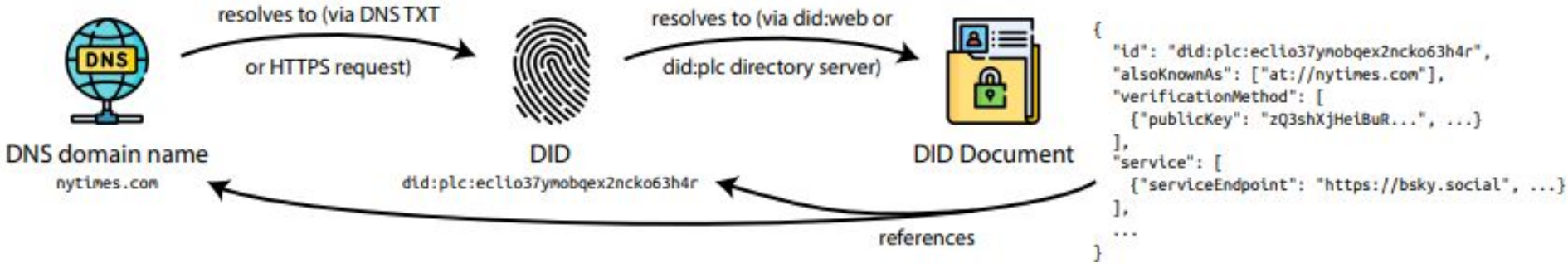
What is this about?

- account identity system Bluesky built for atproto
- where DID PLC fits in to that
- how it is going in production
- ideas for governance and credibility
- other aspects of broader adoption

Backstory: Goals

- open/libre protocol
- credible exit
- own your identity and data
- foundation for new apps

```
{
  "@context": [
    https://www.w3.org/ns/did/v1,
    https://w3id.org/security/multikey/v1,
    https://w3id.org/security/suites/secp256k1-2019/v1
  ],
  id: "did:plc:yk4dd2qkboz2yv6tpubpc6co",
  alsoKnownAs: [
    "at://dholms.xyz"
  ],
  verificationMethod: [
    {
      id: "did:plc:yk4dd2qkboz2yv6tpubpc6co#atproto",
      type: "Multikey",
      controller: "did:plc:yk4dd2qkboz2yv6tpubpc6co",
      publicKeyMultibase: "zQ3shiM8z9mHN3hbkHjM5CSptVKn5xP8u7bZr5esG1xPDbTDC"
    }
  ],
  service: [
    {
      id: "#atproto_pds",
      type: "AtprotoPersonalDataServer",
      serviceEndpoint: https://morel.us-east.host.bsky.network
    }
  ]
}
```


DNS
resolves to (via DNS TXT
or HTTPS request)
resolves to (via did:web or
did:plc directory server)
DNS domain name
nytimes.com
DID
did:plc:eclio37ymobqex2ncko63h4r
DID Document
{
"id": "did:plc:eclio37ymobqex2ncko63h4r",
"alsoKnownAs": ["at://nytimes.com"],
"verificationMethod": [
{"publicKey": "zQ3shXjHeiBuR...", ...}
],
"service": [
{"serviceEndpoint": "https://bsky.social", ...}
],
...
}
references

`did:plc` Method Specification

Version: v0.1 (May 2023)

DID PLC is a self-authenticating DID which is strongly-consistent, recoverable, and allows for key rotation.

An example DID is: `did:plc:ewvi7nxzyoun6zhxrhs64oiz`

Control over a `did:plc` identity rests in a set of reconfigurable rotation keys pairs. These keys can sign update operations to mutate the identity (including key rotations), with each operation referencing a prior version of the identity state by hash. Each identity starts from an initial genesis operation, and the hash of this initial object is what defines the DID itself (that is, the DID URI identifier string). A central directory server collects and validates operations, and maintains a transparent log of operations for each DID.

How it works

The core data fields associated with an active `did:plc` identifier at any point in time are listed below. The

Using the identity system

- DID PLC is general purpose, not atproto-specific
- DID metadata: "also known as", keys, service URLs
- handle system not specific to PLC; or atproto in theory
- all PLC ops permanently public, even after DID tombstone
- handles work with sub-domains, don't require registration
- Bluesky user control of PLC finally enabled this week

How is it working?

January 2024:

3,090,702 total accounts

5 did:web (all others did:plc)

47,588 (1.54%) custom domain handle (not *.bsky.social)

Today: over 5 million / 13 GByte database

database: db.m6i.4xlarge: 16 vCPU / 64 GB RAM, $670/month

VMs: few c6a.large: 2 vCPU / 4 GB RAM, $36/month

130 reads/sec, p95: 2.4ms

12 writes/min, p95: 20ms

The following operations were invalidated and removed from the PLC database. They will not be returned in any audit logs or dataset exports.

(6/1/23)
Correcting an exploit & recovery due to flexible DID length:

- {"sig":"hedSBC2Sp-lj6da5sJ1Bbp9zdYxiuH0s-VbIFI90eLEnOKVYuCpNg23-4kzfLfxoP2iGMbgp5kesOMZl0UU5zA","prev":"bafyreihmuvr3frdvd6vmdhucih277prdcfcezf67lasg5oekxoimnunjoq","type":"plc_operation","services":{"atproto_pds":{"type":"AtprotoPersonalDataServer","endpoint":"https://bsky.social"}},"alsoKnownAs":["at://retr0id-was-here.bsky.social"],"rotationKeys":["did:key:zQ3shhCGUqDKjStzuDxPkTxN6ujddP4RkEKJJouJGRRkaLGbg","did:key:zQ3shpKnbdPx3g3CmPf5cRVTPe1HtSwVn5ish3wSnDPQCbLJK"],"verificationMethods":{"atproto":"did:key:zQ3shXjHeiBuRCKmM36cuYnm7YEMzhGnCmCyW92sRJ9pribSF"}}
- {"sig":"qU8Yy7Szhjk2GzF2coWHYmO8VewoPNkRg-2bEHm_Y7Fn0snJnF3YEwyN98gAOLxNKNNv4RnkbCiZMCVjpkJOrw","prev":"bafyreidaxmtdx6pb3up6tznwdbdse53uytfl7laql4cdlig22zhktkhfjy","type":"plc_operation","services":{"atproto_pds":{"type":"AtprotoPersonalDataServer","endpoint":"https://bsky.social"}},"alsoKnownAs":["at://bluesky-app.bsky.social"],"rotationKeys":["did:key:zQ3shhCGUqDKjStzuDxPkTxN6ujddP4RkEKJJouJGRRkaLGbg","did:key:zQ3shpKnbdPx3g3CmPf5cRVTPe1HtSwVn5ish3wSnDPQCbLJK"],"verificationMethods":{"atproto":"did:key:zQ3shXjHeiBuRCKmM36cuYnm7YEMzhGnCmCyW92sRJ9pribSF"}}
- {"sig":"Rh799SDONBpbiUuH1-w7SipE0Ny7ilRS3tq47I9HwU0bgvbIX0lsmGgCfba8rxlkBCMrvFw_iFEK_tiXNMOAgQ","prev":"bafyreidgciciiy7gc44mzzvhisqycd3qyhsh2yhpf4vbvwxmk4ru4ijvaa","type":"plc_operation","services":{"atproto_pds":{"type":"AtprotoPersonalDataServer","endpoint":"https://bsky.social"}},"alsoKnownAs":["at://bsky.app"],"rotationKeys":["did:key:zQ3shhCGUqDKjStzuDxPkTxN6ujddP4RkEKJJouJGRRkaLGbg","did:key:zQ3shpKnbdPx3g3CmPf5cRVTPe1HtSwVn5ish3wSnDPQCbLJK"],"verificationMethods":{"atproto":"did:key:zQ3shXjHeiBuRCKmM36cuYnm7YEMzhGnCmCyW92sRJ9pribSF"}

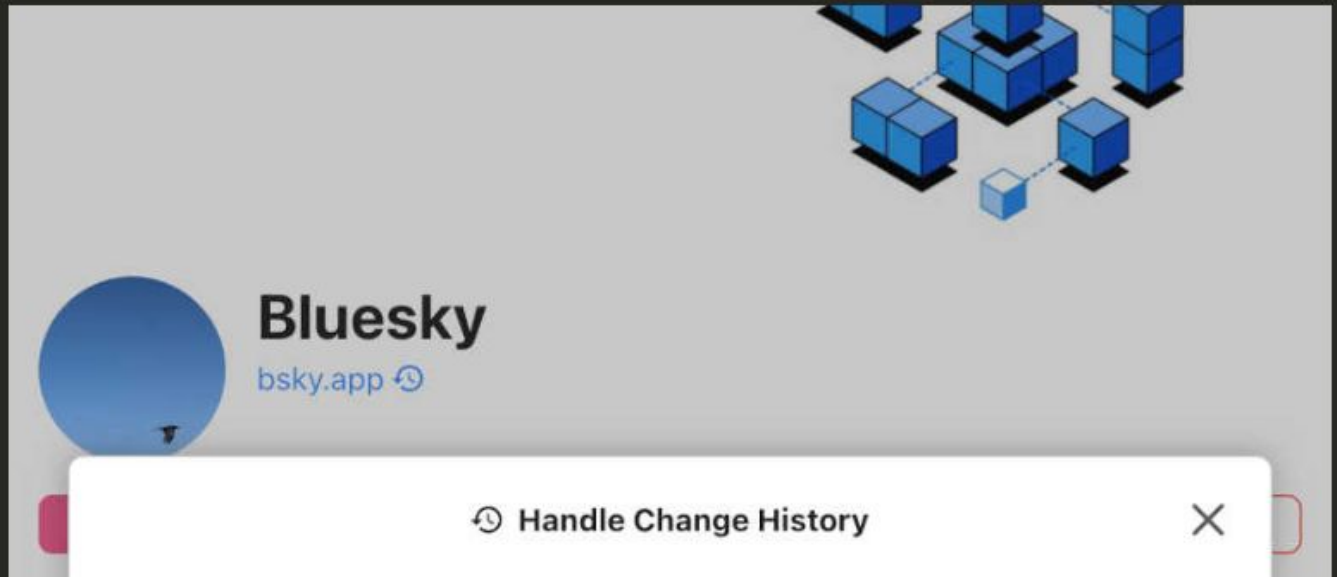
(6/8/23)
Removing operations for dids with identifier length > 24
Note: this action was verified ahead of time with affect accounts

- {"sig": "uwYlCtorebyjnDM1_AV-MbtlqEvSi4hM2e-tM92_xVtCxhq-hUQypvM_P55j6JM6URHb8K4xDrATor4HUORUcA", "prev": null, "type": "create", "handle": "syui.syui.ai", "service": "https://bsky.syui.ai", "signingKey": "did:key:zDnaeyvyunvK2SqYgq3yWdXHcVuGsKRZRiLR4TSre5hNr6dzo", "recoveryKey": "did:key:zDnaeyvyunvK2SqYgq3yWdXHcVuGsKRZRiLR4TSre5hNr6dzo"}
- {"sig": "txcvJ9Wj2-YAoUVzAIacGAerHqsmSu6aMQnaBF3L49mQs_ZyE5zPRJxkKJKJ5CmjTJodY5erzrHdUSZXorB_KA", "prev": null, "type": "create", "handle": "atproto.forza7.org", "service": "https://atproto.forza7.org", "signingKey": "did:key:zDnaev1CWcwE82K2poDk5Q6vN259e6FQs5cpbDxCLL9LXyp1s", "recoveryKey": "did:key:zDnaev1CWcwE82K2poDk5Q6vN259e6FQs5cpbDxCLL9LXyp1s"}
- {"sig": "AtgsodOZO65kJ1ewh_T7D7MKzMRvmmQVhCEi-XK0GnePseMXE27ZWCrkBq7t14kNWMiLcpo_8EWqEdTi7caMPw", "prev": null, "type": "create", "handle": "forza7.localhost", "service": "http://localhost:2583", "signingKey": "did:key:zDnaesXsY65c58WZmhs3R1s4dHH3euWmtjcrrWmRADywTjtUg", "recoveryKey": "did:key:zDnaesXsY65c58WZmhs3R1s4dHH3euWmtjcrrWmRADywTjtUg"}

Hijacking Bluesky Identities with a Malleable Deputy

By David Buchanan, 28th September 2023

If you don't live under a rock, you might've heard of Bluesky, a decentralised social microblogging app built on top of the AT Protocol. In early June 2023, I identified a vulnerability in Bluesky's core user identity mechanism, `did:plc`, which allowed me to modify the identity information associated with any* account. I tested my hypothesis by changing the handle of the official `@bsky.app` account.



Governance and Trust

Directory Trust / Threat Model

1. entirely remove DID
2. selectively redact existing ops
3. selectively reject or delay new ops
4. manipulate timestamps

Existing Mitigations

- audit log API endpoint
- snapshots to archive.org

Idea: Dedicated Org / Consortium

- social solution to social concern
- existence proof: Let's Encrypt (EFF/ISRG)
- likely!

Idea: Transparency Log

- Certificate Transparency
- WebSocket
- observer consortium?
- likely!

Idea: Closed Blockchain

- less likely

Idea: Read Replicas

- builds on log
- performance, scale, reliability
- client choice
- public "pool" consortium
- likely!

Idea: Write Proxies

- proxy witnesses submission of ops
- client choice
- combines with log and read-replicas
- maybe

Idea: Multi-Writer Consortium

- builds on logs, replicas
- sharded, like a DHT
- clients: stateful or naive
- maybe

Other Adoption Pieces

- demos and example projects
- client libraries
- rotation key management
- formal standardization (IETF / W3C)

authn / authz

- service auth: JWTs, UCANs
- OAuth, IndieAuth, OIDC
- "Login with Handle"

Go Experiment!

@bnewbold.net / @bnewbold@social.coop

https://web.plc.directory/

https://github.com/bluesky-social/proposals/tree/main/0004-oauth

https://atproto.com/specs/did