Advanced Guides The AT Protocol

The AT Protocol

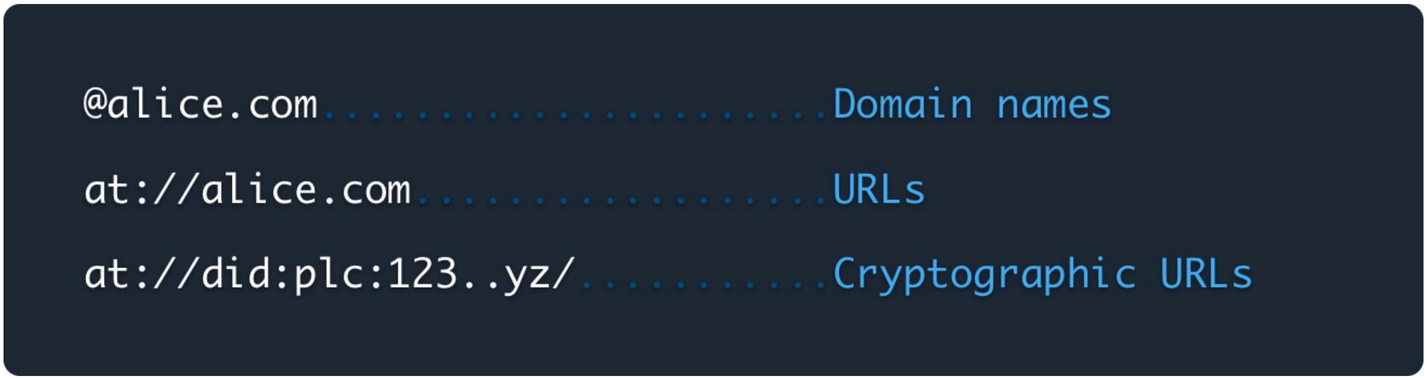
The AT Protocol (Authenticated Transfer Protocol, or atproto) is a standard for public conversation and an open-source framework for building social apps.

It creates a standard format for user identity, follows, and data on social apps, allowing apps to interoperate and users to move across them freely. It is a federated network with account portability.

Basic Concepts

Identity

Users are identified by domain names on the AT Protocol. These domains map to cryptographic URLs which secure the user's account and its data.



```
@alice.com......................Domain names
at://alice.com..................URLs
at://did:plc:123..yz/...........Cryptographic URLs
```

Data repositories

User data is exchanged in signed data repositories. These repositories are collections of records which include posts, comments, likes, follows, media blobs, etc.

@alice.com
signs
repo records

Federation

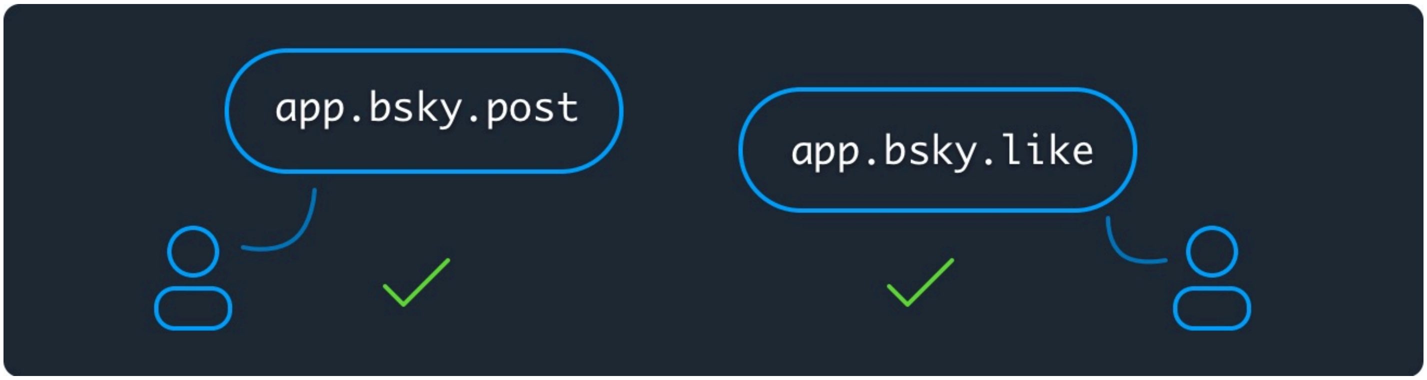
The AT Protocol syncs the repositories in a federated networking model. Federation was chosen to ensure the network is convenient to use and reliably available. Repository data is synchronized between servers over standard web technologies (HTTP and WebSockets).

The three core services in our network are Personal Data Servers (PDS), Big Graph Services (BGS), and App Views. We're also working on feed generators and labelers.

Read more about the federation architecture here.

Interoperation

A global schemas network called Lexicon is used to unify the names and behaviors of the calls across the servers. Servers implement "lexicons" to support featuresets, including the core atproto Lexicon for syncing user repositories and the Bsky lexicon to provide basic social behaviors.

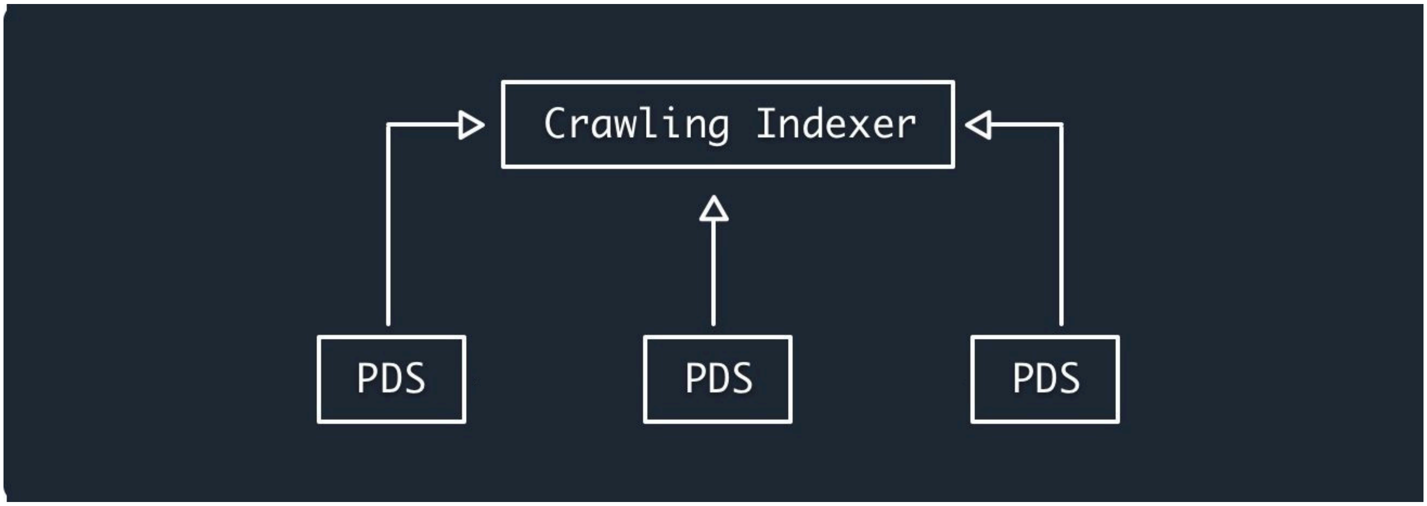


While the Web exchanges documents, the AT Protocol exchanges schematic and semantic information, enabling the software from different orgs to understand each others' data. This gives atproto clients freedom to produce user interfaces independently of the servers, and removes the need to exchange rendering code (HTML/JS/CSS) while browsing content.

Achieving scale

Personal data servers are your home in the cloud. They host your data, distribute it, manage your identity, and orchestrate requests to other services to give you your views.

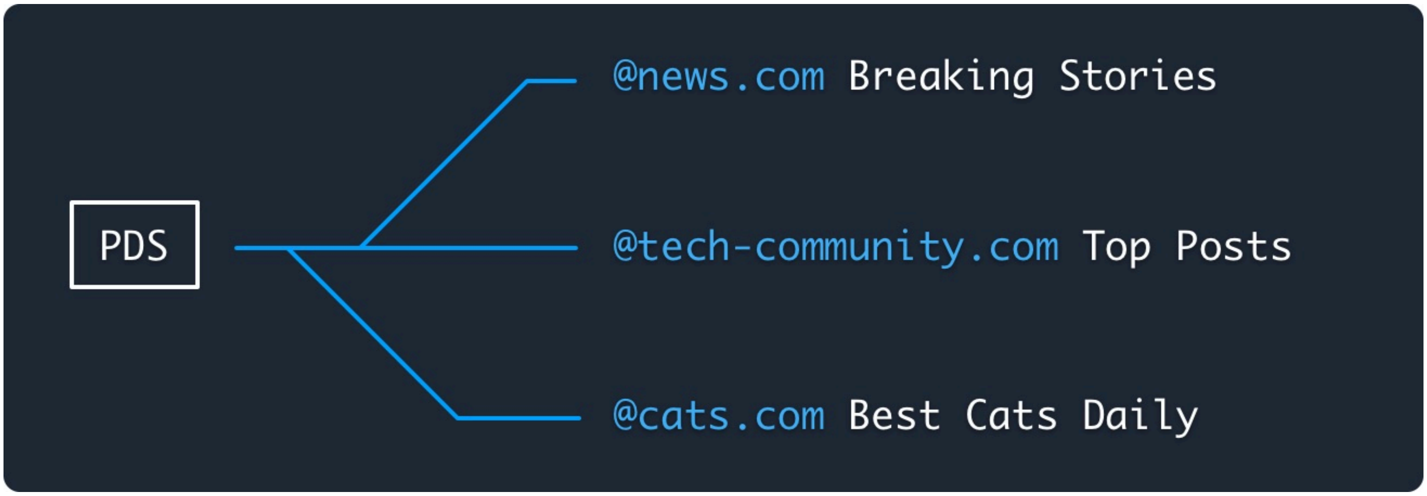
Relays handle all of your events, like retrieving large-scale metrics (likes, reposts, followers), content discovery (algorithms), and user search.



This distinction is intended to achieve scale as well as a high degree of user-choice.

Algorithmic choice

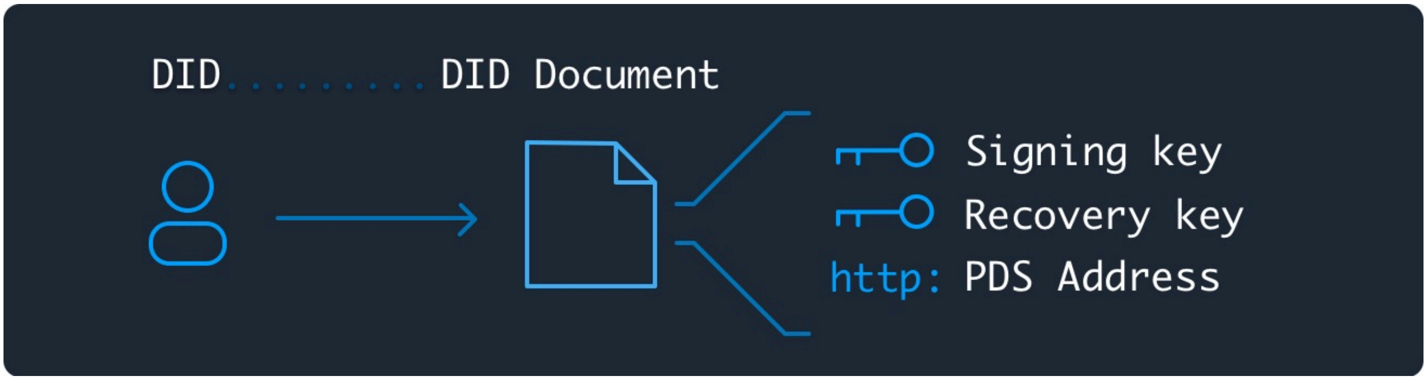
As with Web search engines, users are free to select their aggregators. Feeds, App Views, and search indices can be provided by independent third parties, with requests routed by the PDS based on user configuration.


PDS
@news.com Breaking Stories
@tech-community.com Top Posts
@cats.com Best Cats Daily

Account portability

We assume that a Personal Data Server may fail at any time, either by going offline in its entirety, or by ceasing service for specific users. The goal of the AT Protocol is to ensure that a user can migrate their account to a new PDS without the server's involvement.

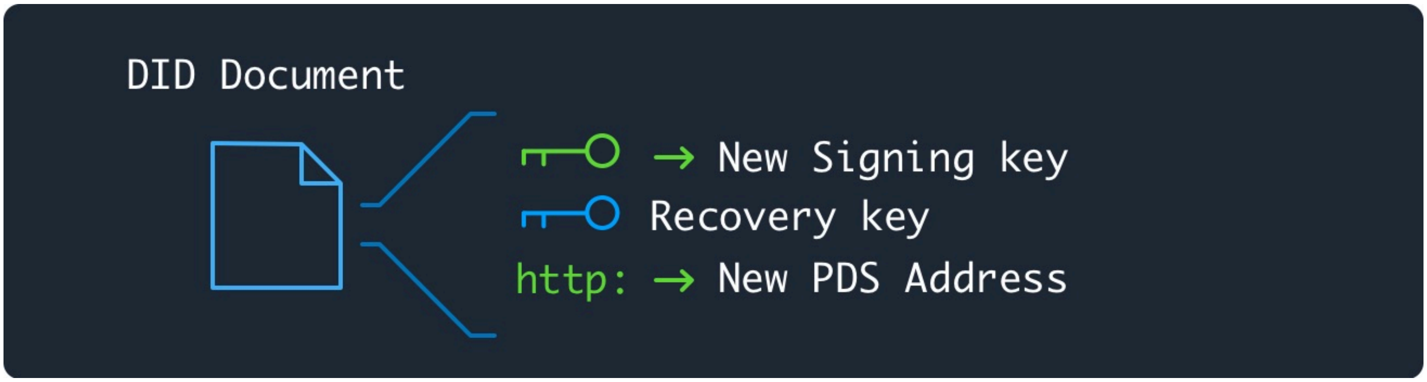
User data is stored in signed data repositories and verified by DIDs. Signed data repositories are like Git repos but for database records, and DIDs are essentially registries of user certificates, similar in some ways to the TLS certificate system. They are expected to be secure, reliable, and independent of the user's PDS.



Each DID document publishes two public keys: a signing key and a recovery key.

- **Signing key**: Asserts changes to the DID Document *and* to the user's data repository.
- **Recovery key**: Asserts changes to the DID Document; may override the signing key within a 72-hour window.

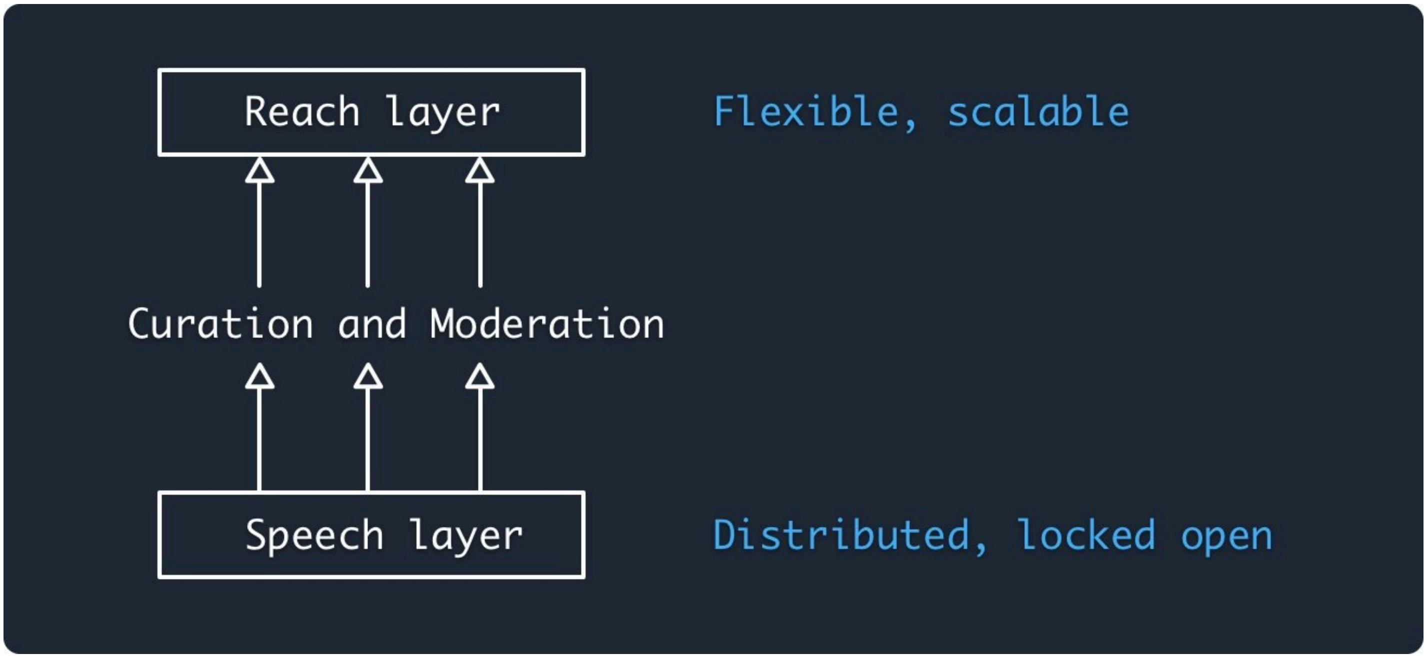
The signing key is entrusted to the PDS so that it can manage the user's data, but the recovery key is saved by the user, e.g. as a paper key. This makes it possible for the user to update their account to a new PDS without the original host's help.



A backup of the user’s data will be persistently synced to their client as a backup (contingent on the disk space available). Should a PDS disappear without notice, the user should be able to migrate to a new provider by updating their DID Document and uploading the backup.

Speech, reach, and moderation

Atproto's model is that *speech* and *reach* should be two separate layers, built to work with each other. The “speech” layer should remain permissive, distributing authority and designed to ensure everyone has a voice. The “reach” layer lives on top, built for flexibility and designed to scale.



The base layer of atproto (personal data repositories and federated networking) creates a common space for speech where everyone is free to participate, analogous to the Web where anyone can put up a website. The indexing services then enable reach by aggregating content from the network, analogous to a search engine.

Read More

You can read the AT Protocol specs here.

✎ Edit this page