nk

- Installing nk
- Generating NKeys and Configuring the Server

`nk` is a command line tool that generates `nkeys`. NKeys are a highly secure public-key signature system based on Ed25519.

With NKeys the server can verify identity without ever storing secrets on the server. The authentication system works by requiring a connecting client to provide its public key and digitally sign a challenge with its private key. The server generates a random challenge with every connection request, making it immune to playback attacks. The generated signature is validated a public key, thus proving the identity of the client. If the public key validation succeeds, authentication succeeds.

> NKey is an awesome replacement for token authentication, because a connecting client will have to prove it controls the private key for the authorized public key.

Installing nk

To get started with NKeys, you'll need the `nk` tool from https://github.com/nats-io/nkeys/tree/master/nk repository. If you have *go* installed, enter the following at a command prompt:

```
go install github.com/nats-io/nkeys/nk@latest
```

Generating NKeys and Configuring the Server

To generate a *User* NKEY:

```
nk -gen user -pubout
```

```
SUACSSL3UAHUDXKFSNVUZRF5UHPMWZ6BFDTJ7M6USDXIEDNPPQYYYCU3VY
UDXU4RCSJNZOIQHZNWXHXORDPRTGNJAHAHFRGZNEEJCPQTT2M7NLCNF4
```

The first output line starts with the letter `S` for *Seed*. The second letter `U` stands for *User*. Seeds are private keys; you should treat them as secrets and guard them with care.

The second line starts with the letter `U` for *User*, and is a public key which can be safely shared.

To use `nkey` authentication, add a user, and set the `nkey` property to the public key of the user you want to authenticate. You are only required to use the public key and no other properties are required. Here is a snippet of configuration for the `nats-server`:

```
authorization: {
  users: [
    { nkey: UDXU4RCSJNZOIQHZNWXHXORDPRTGNJAHAHFRGZNEEJCPQTT2M7NLCNF4 }
  ]
}
```

To complete the end-to-end configuration and use an `nkey`, the client is configured to use the seed, which is the private key.

□□□ #1
□ cocobook-sync □□□ 2026-10-28 11:10:46 UTC
□ cocobook-sync □□□ 2026-10-28 11:10:46 UTC