Key management

Christian Grothoff

Using GNU Anastasis

1. Installing anastasis-gtk

To install binaries on Debian or Ubuntu, follow the first steps in section 3.3.1 or 3.3.3 of `https://docs.taler.net/taler-merchant-manual.html` to add the `deb.taler.net` repository to your system. Then, you can just:

```
# apt install anastasis-gtk
```

You could of course also try to build the system from source, starting with its dependencies.

Alternatively, but **not** as securely, you can use `https://webui.anastasis.lu/` in your browser.

2. Backup and recovery

Use GNU Anastasis to back up a secret (does not have to be a real one) and to recover it. The GUI will check some of your identity data client-side for validity.

3. What is the adversary model of GNU Anastasis?

Specifically, what does an adversary need to gain access to a user's secret? What information does give an adversary at least some partial knowledge about a user, but not access to the user's secret?