```
token.redeem_shield(to, amount, secret)
```

requires user to know the secret to redeem shielded tokens. If secrets are generated randomly, there should be a database (local on user machine or global on Aztec servers) to store user secrets. I can clearly see the cons of this approach:

1. In case of a local DB, secrets can be lost if user loses/changes their phone

2. In case of a global DB, user puts trust in Aztec (or other 3rd party) servers and if those go offline for any reason, user secrets are lost.

I am thinking about deterministically deriving secrets from user's private key. An example formula:

```
secret = hash(private_key, domain_separator, secret_index)
```

With this approach a user can derive their secrets with a simple for loop on any device without relying on any third parties.

Questions:

1. Is this secure and privacy preserving?

2. Any other methods of managing user secrets?