

Hei!

- Om oss
- Tekniske forklaringer
- Oversikt over løsningen
- Demo!

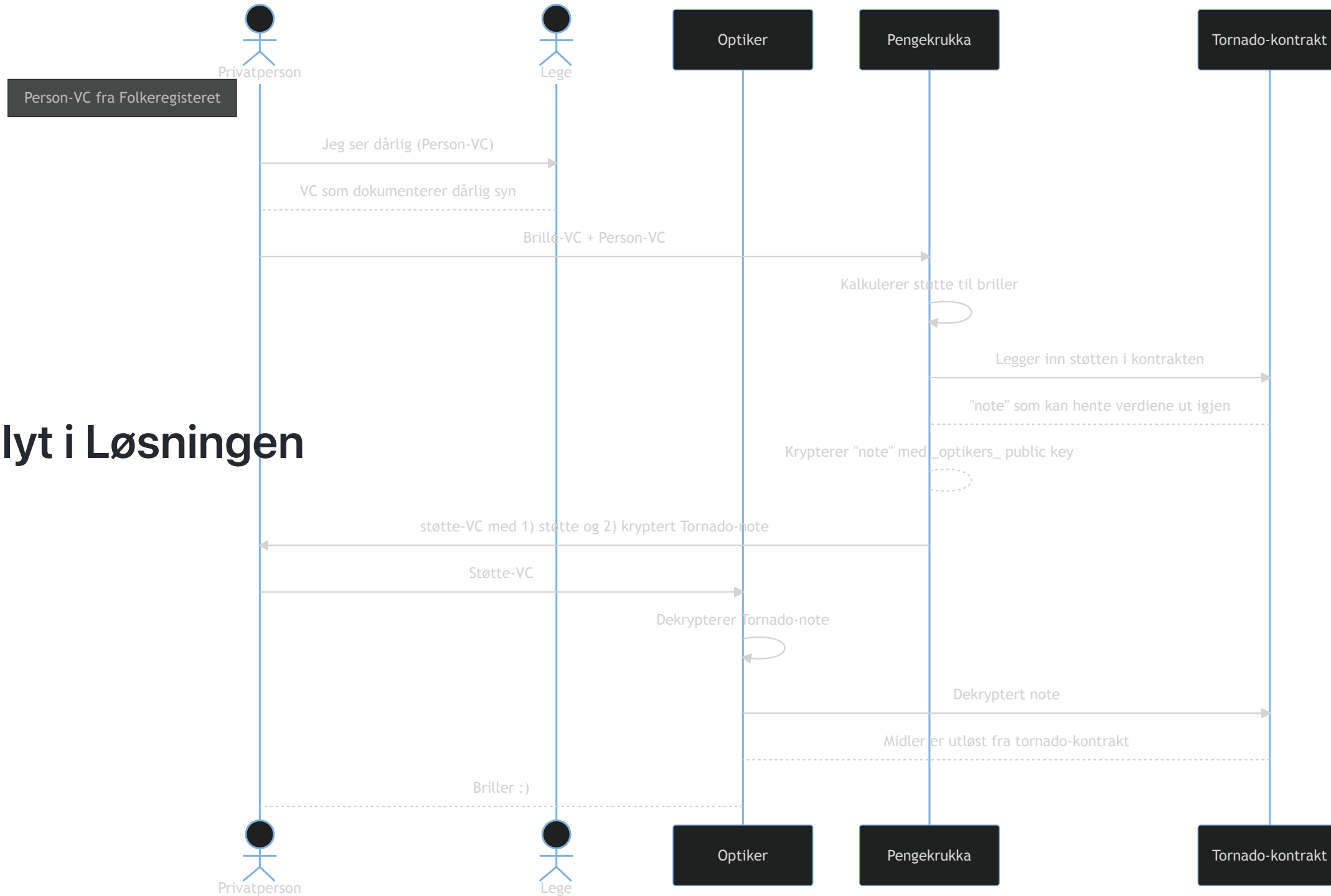
Om Oss

- Asbjoern Riddervold
- Olav Sundfør
- Frilansere
- Lære! Og har lært.
- Samfunnsnyttige

Pengekrukka

- utbetaling fra det offentlige
- fokus på bevaring av personvern
- bygger på Verifiable Credentials og Zero Knowledge Proofs
- betalinger via blokkjeden

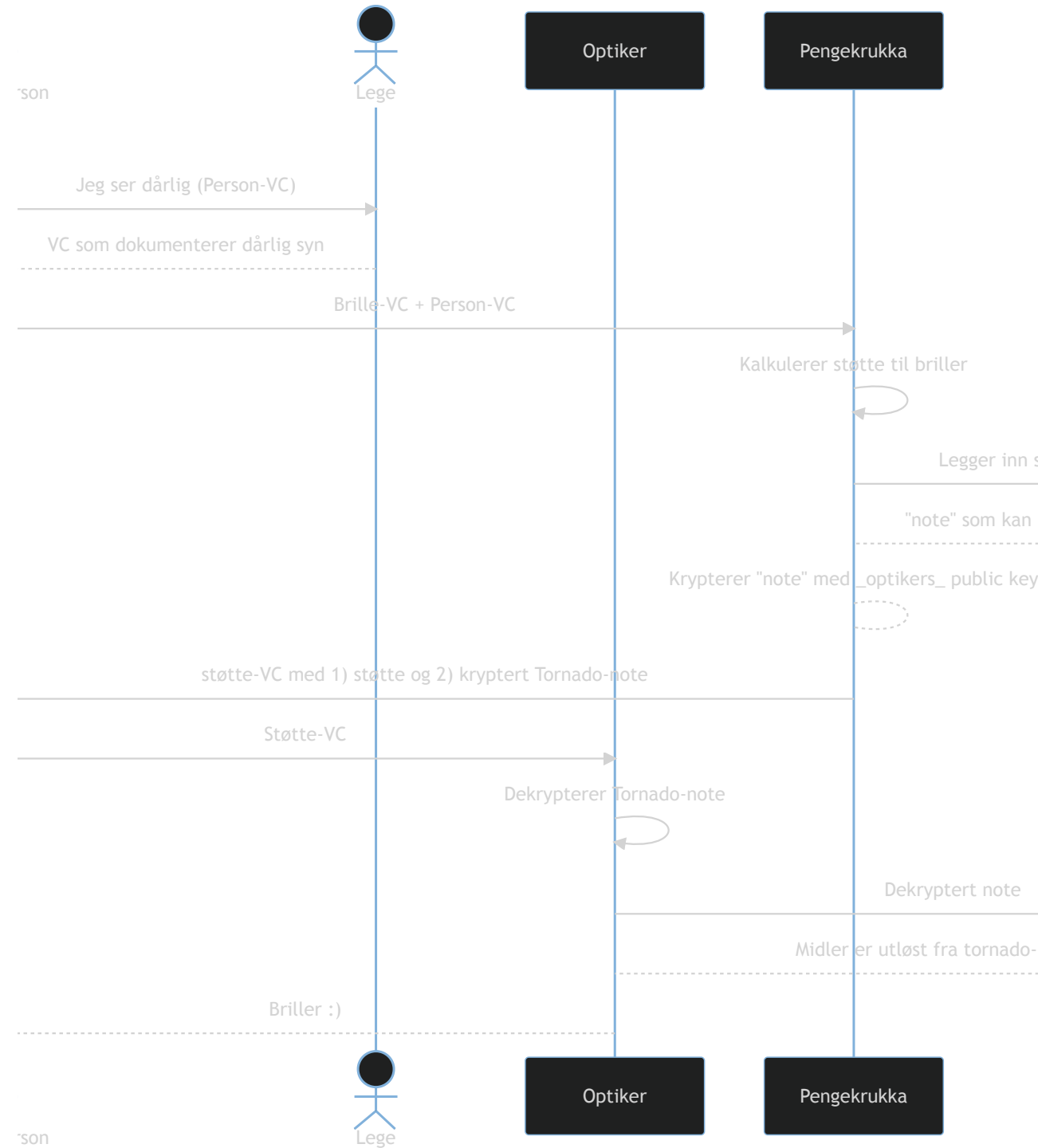
Flyt i Løsningen



Tanker bak 1/3

- ivaretar personvern
- både digital og fysisk

FIXME: Bakgrunn

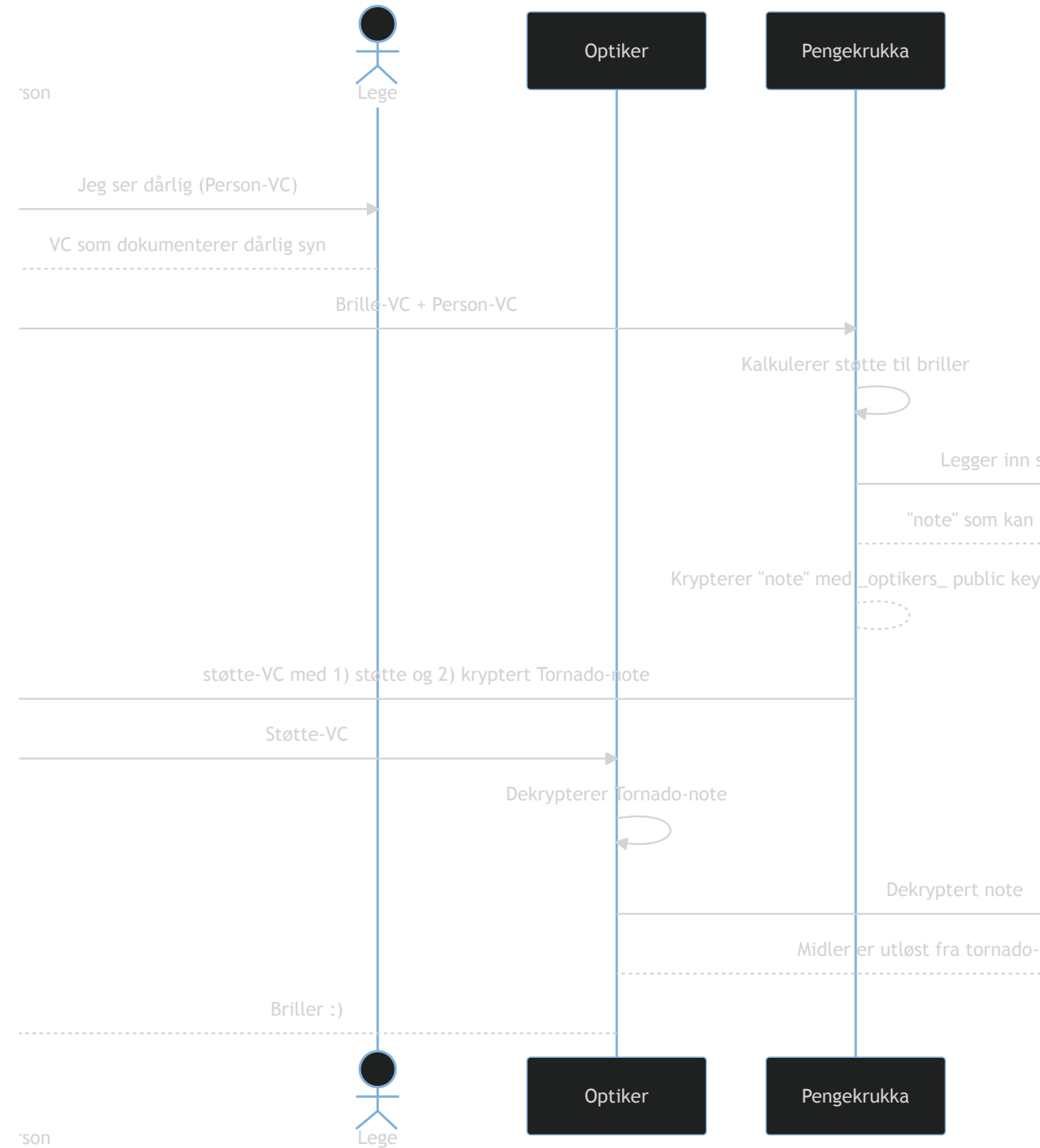


Tanker bak 2/3

Verifiable Credential

- Litt som en seddel (vannmerker - > digitale signaturer av utsteder)
- kun et standardisert JSON-objekt
- kan like så gjerne være et fysisk ark med QR
- standardisert gjennom EUs ID-prosjekt
- Forskning (Song et al 2022) peker paa dette som veien fremover

FIXME: Bakgrunn

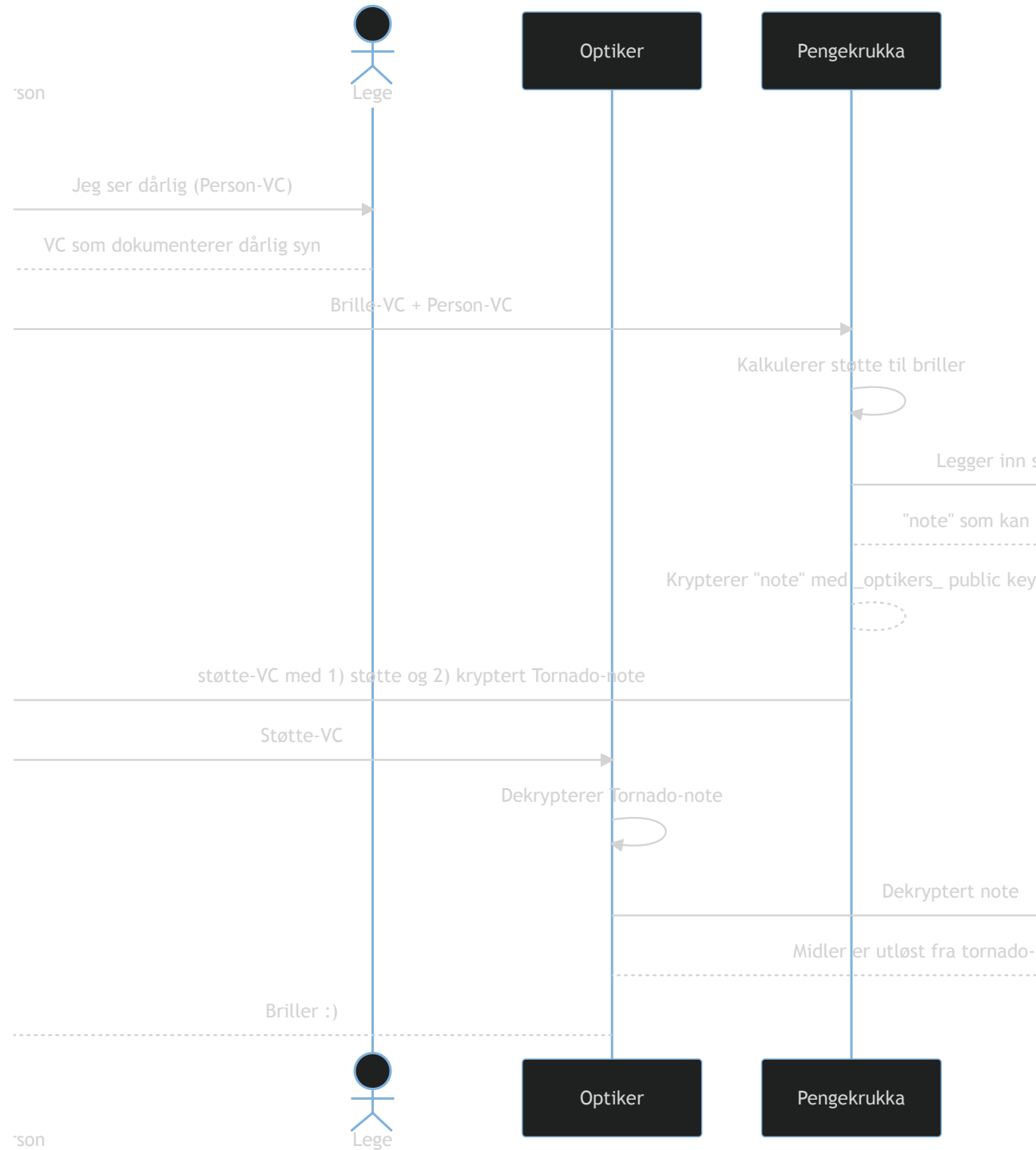


Tanker bak 3/3

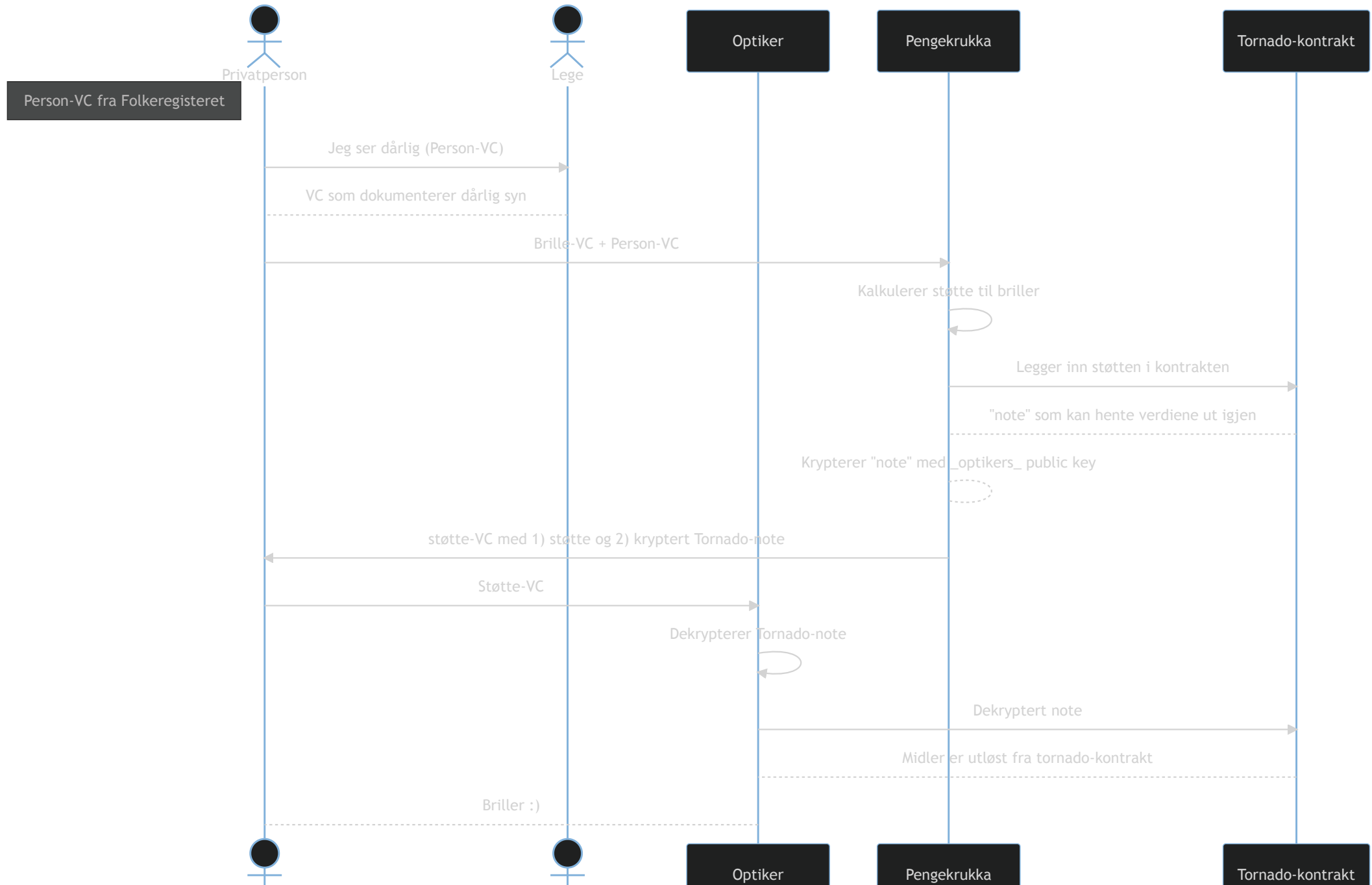
Zero Knowledge Proofs

- kun gi den informasjonen som er relevant
- har nøkkelen-bevise uten å vise det frem
- alt som havner på blokkjeden er anonymt gjennom ZKP

FIXME: Bakgrunn



Private Eye - Eksempel



Demo

- heldigital, men det trenger den ikke være!

Fordeler med denne løsningen

- kan også fungere analogt med minimale tilpasninger
- lav kobling mellom aktørene; vanskelig å sette sammen data
- økt gjennomsiktighet uten å gå på bekostning av den enkeltes personvern
- kan i prinsippet kjøres av hvem som helst i befolkningen
- automatisk øremerket! ingen kvittering/bevisbyrde i etterkant

Ulempler med løsningen

- generering av proofs tar tid og koster mye gas
- fremmed for mange

Ting som kunne gjort det kulere

- implementert validering av VC-er (signerte ID-er i subject osv.)
- anonymisere credentials gjennom hashing
- trenger ikke velge optiker hos Pengekrukka

Avslutningsvis

- Gleder oss til etterpå
- Takk for masse læring!
- FJERN (lære mer i samtaler med dere)
- FJERN (vi ser faktisk etter flere prosjekter om dagen, så vi er åpne for den type samtler også)

