NTNU
Kunnskap for en bedre verden

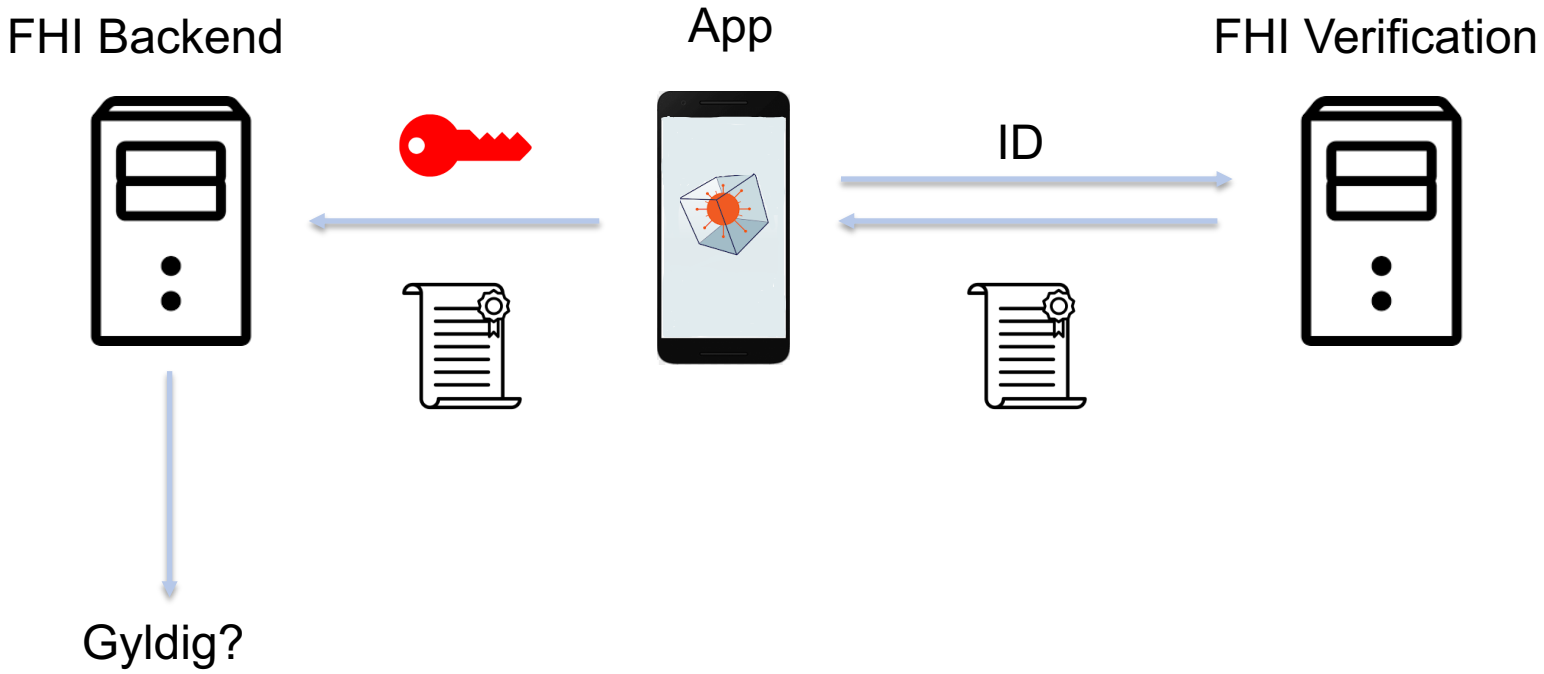
FFI Forsvarets forskningsinstitutt

BEKK

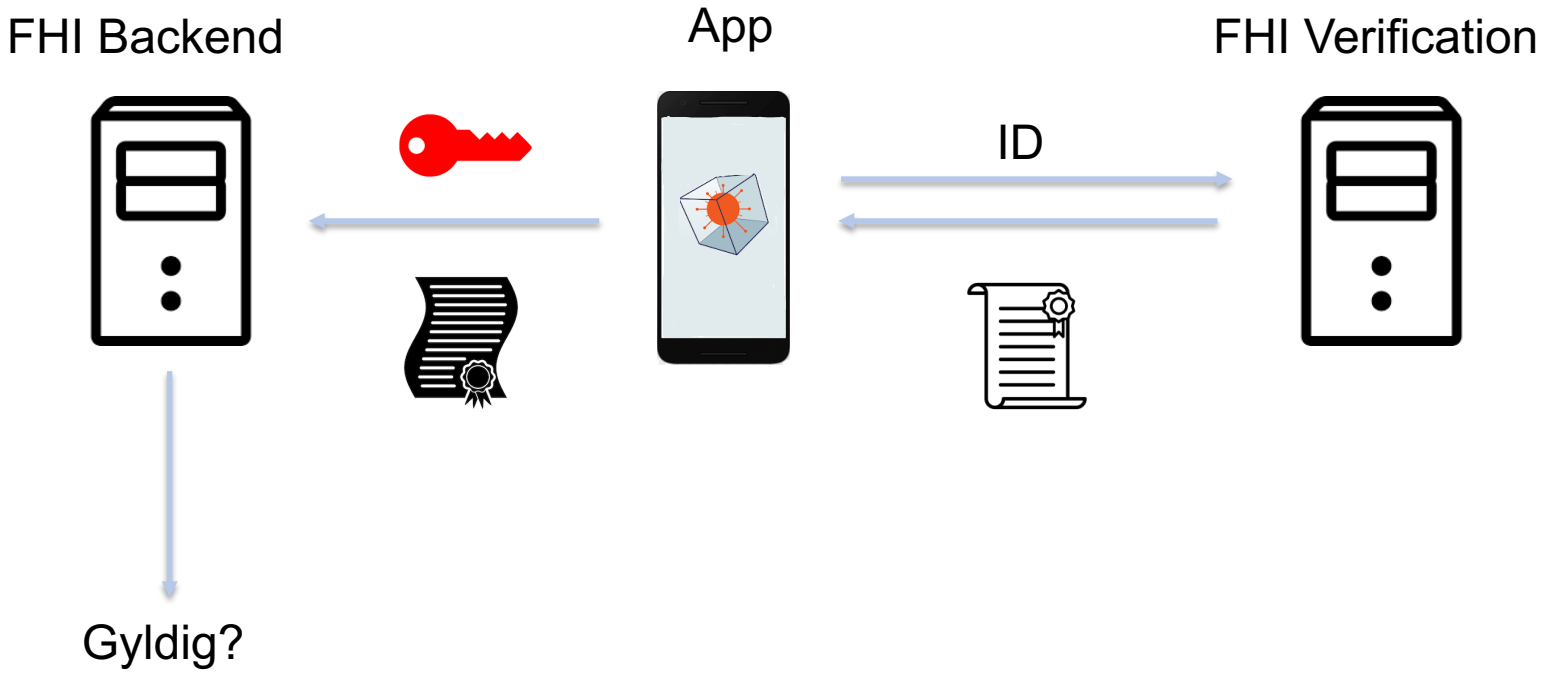
Anonyme attester i Smittestopp

Henrik Walker Moe (Bekk)
Tjerand Silde (NTNU)
Martin Strand (FFI)

Opprinnelig Smittestopp



Anonymitet i Smittestopp



Merverdi til Smittestopp

Prinsipielt:

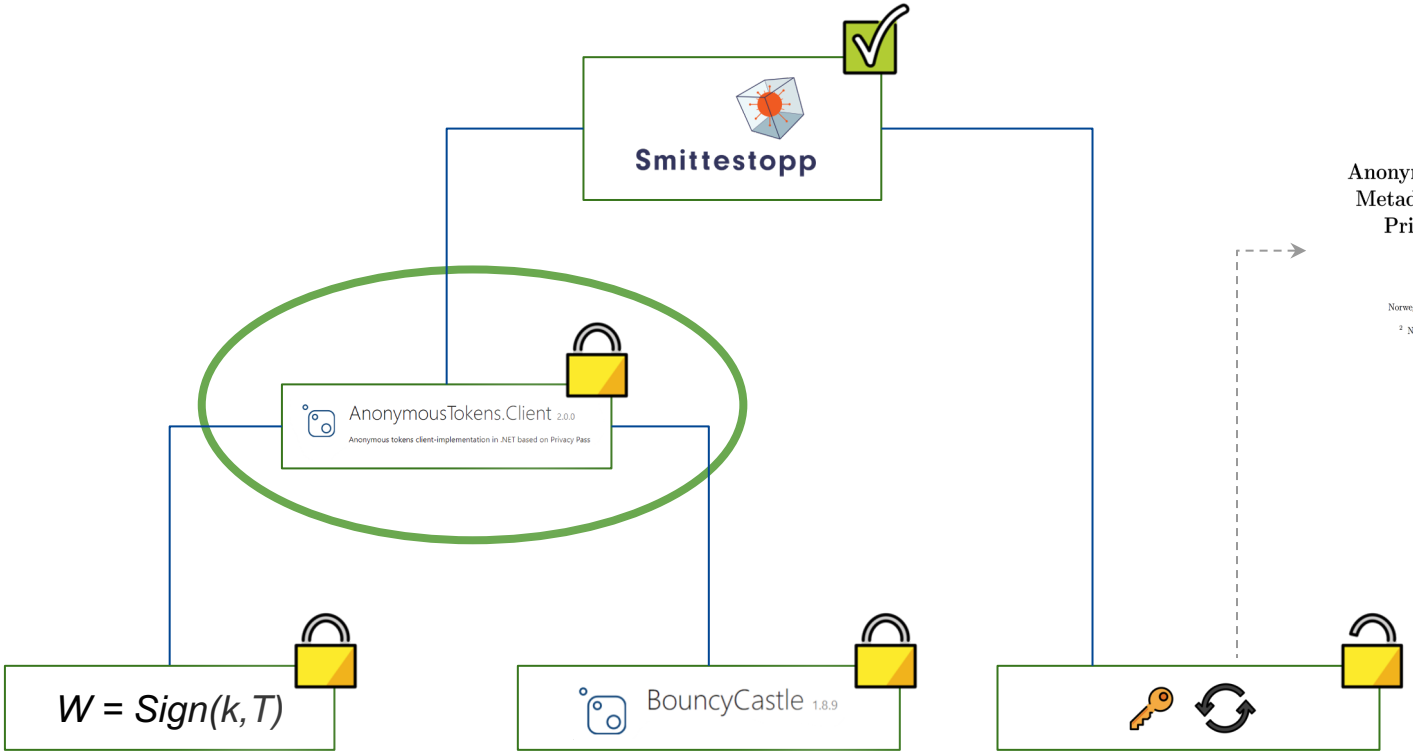
- En attest fra FHI Verification er entydig knyttet til en identitet
- FHI Backend trenger ikke identiteter for å gjøre jobben sin
- Vi framtvinger at det blir sånn

Logger kan lekke de smittedes lokasjonsgraf og sosiale graf.
Anonyme attester sørger for innebygget personvern og dataminimering.

Fare med logging:

- Formålsutglidning eller endring av lover
- Hacking fra tredjeparter, sporing i offentlig rom

Sårbarhetsanalyse



Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing

Tjerand Silde[1] and Martin Strand[2]

[1] Department of Mathematical Sciences, Norwegian University of Science and Technology – NTNU, tjerand.silde@ntnu.no
[2] Norwegian Defence Research Establishment – FFI, martin.strand@ffi.no

Andre anvendelser

Privacy Pass:

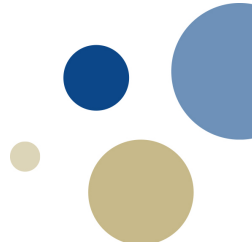
- TOR-brukere kan løse en CAPTCHA én gang hos Cloudflare, og få mange attester som lagres i nettleseren
- Når brukeren kommer tilbake senere, kan han løse inn en attest istedenfor å måtte løse enda en CAPTCHA

Facebook PrivateStats:

- FB driver utstrakt logging. Anonyme attester gjør loggene fullstendig anonyme, men gir fortsatt FB nyttige driftsdata

Smitte|stop:

- Samme modell i den danske appen som i Smittestopp



Anonyme periodebilletter

Foto: Ruter As / CatchLight Fotostudio AS

Kjøp/gjenoppretting: Generer tilstrekkelig mange anonyme attester, og last dem inn på telefonen

- Metadata: Utløpsdato, billettype

Bussreise: Skanne med NFC eller strekkode

- Automaten verifiserer gyldighet og melder tilbake til telefonen som da sletter attesten
- Automaten rapporterer inn attester som er brukt, samt metadata for statistikkformål

Oppsummert

- Kort vei fra idé til god implementasjon
- Læringspunkt: Hvordan selge inn en funksjon som er basert på antagelsen om at man ikke skal stole på systemeieren?
- Sterkt personvern uten å ofre funksjonalitet – dette kan vi oppnå mange andre steder også!
- Forskningsarbeidet følges opp internasjonalt og går rett inn i en eksisterende standardiseringsprosess

Takk! Spørsmål?

GitHub-repo: HenrikWM/anonymous-tokens