NTNU

Kunnskap for en bedre verden

Anonym Smittesporing

Henrik W. Moe (Bekk),
Tjerand Silde (NTNU),
og Martin Strand (FFI)

BEKK

FFI Forsvarets forskningsinstitutt

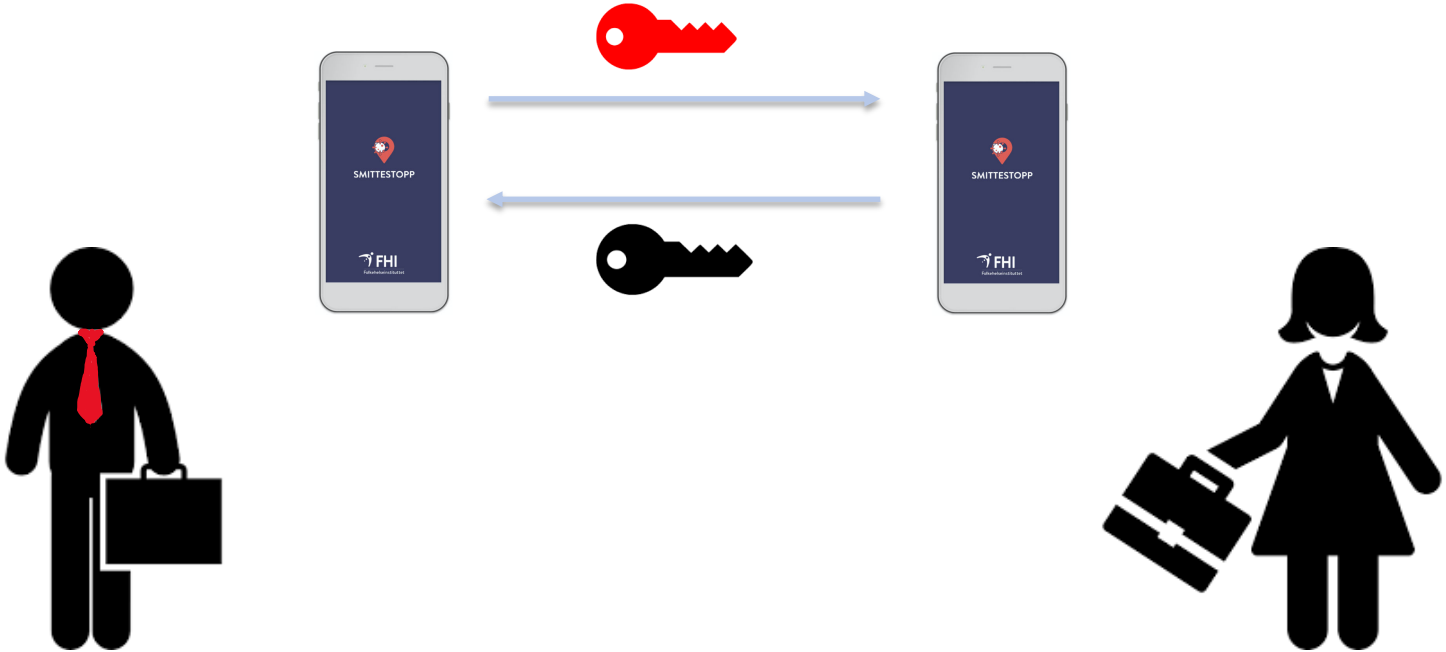
Bakgrunn

FHI ønsker digital smittesporing som komplement til tradisjonell smittesporing.

Appen varsler nærkontakter dersom noen tester positivt. Dette kan fange opp personer man ikke trodde eller visste var nærkontakter.

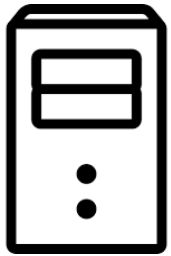
Appen varsler også nærkontakter som myndighetene ikke får tak i på tradisjonelt vis.

Smittestopp

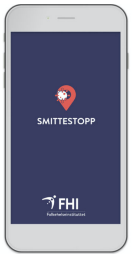


Smittestopp

FHI - Backend

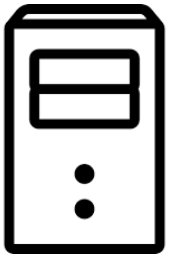


App



ID

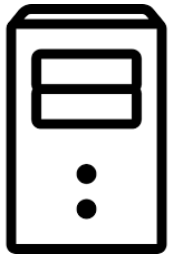
FHI - Verification



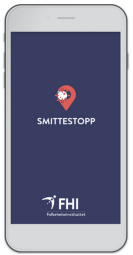
Meld Smitte

Smittestopp

FHI - Backend

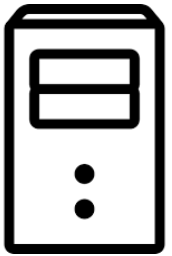


App



Bekreft Smitte

FHI - Verification

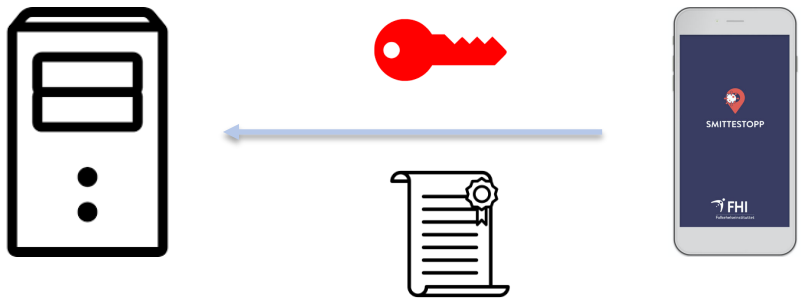


Smittestopp

FHI - Backend

App

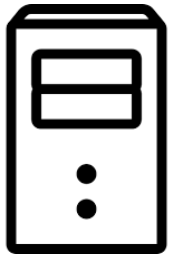
FHI - Verification



Send Smittenøkler

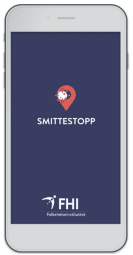
Smittestopp

FHI - Backend

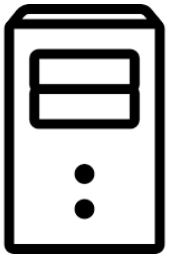


Gyldig?

App



FHI - Verification

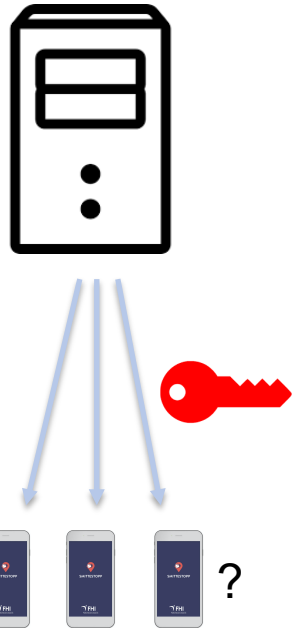


Smittestopp

FHI - Backend

App

FHI - Verification



Dersom man har sett noen av nøklene tidligere,
så bør man teste seg og gå i karantene.

Anonymitet

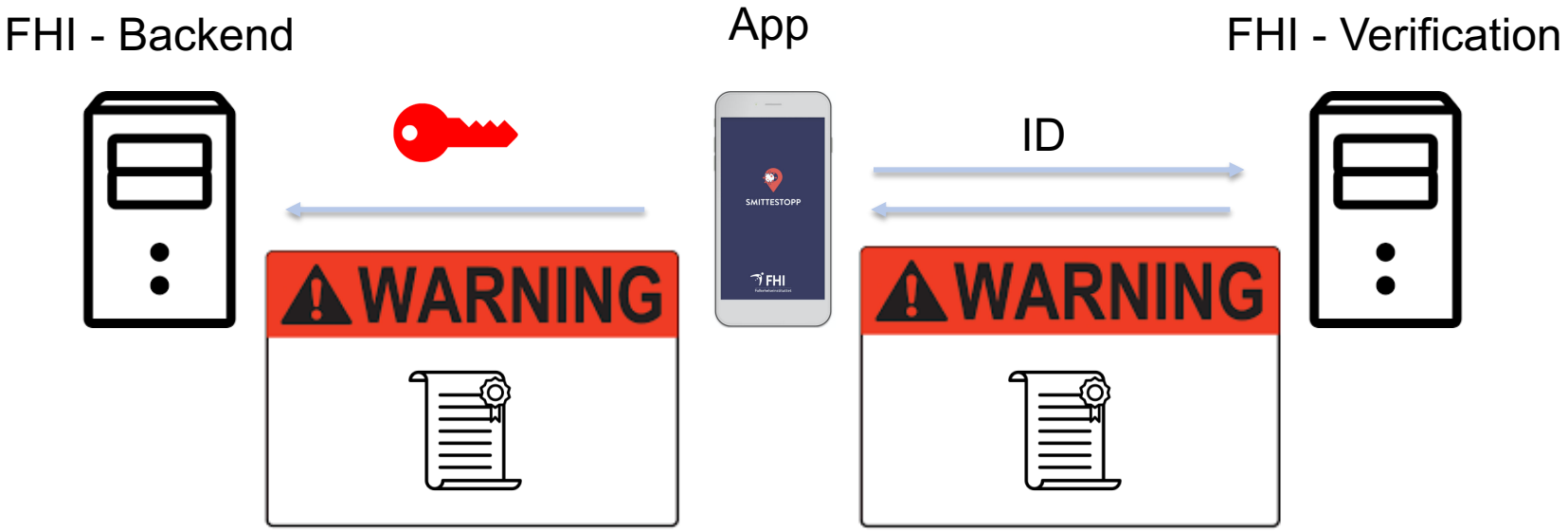
Roterende smittenøkler sørger for at det er vanskelig å følge bevegelsene til en gitt person basert på nøkler man ser.

Data lastes kun opp til en sentral server dersom man har testet positivt, ellers lagres all informasjon kun på telefonen.

Appen sjekker lokalt dersom den har vert i kontakt med noen som har lastet opp smittenøkler på serveren.

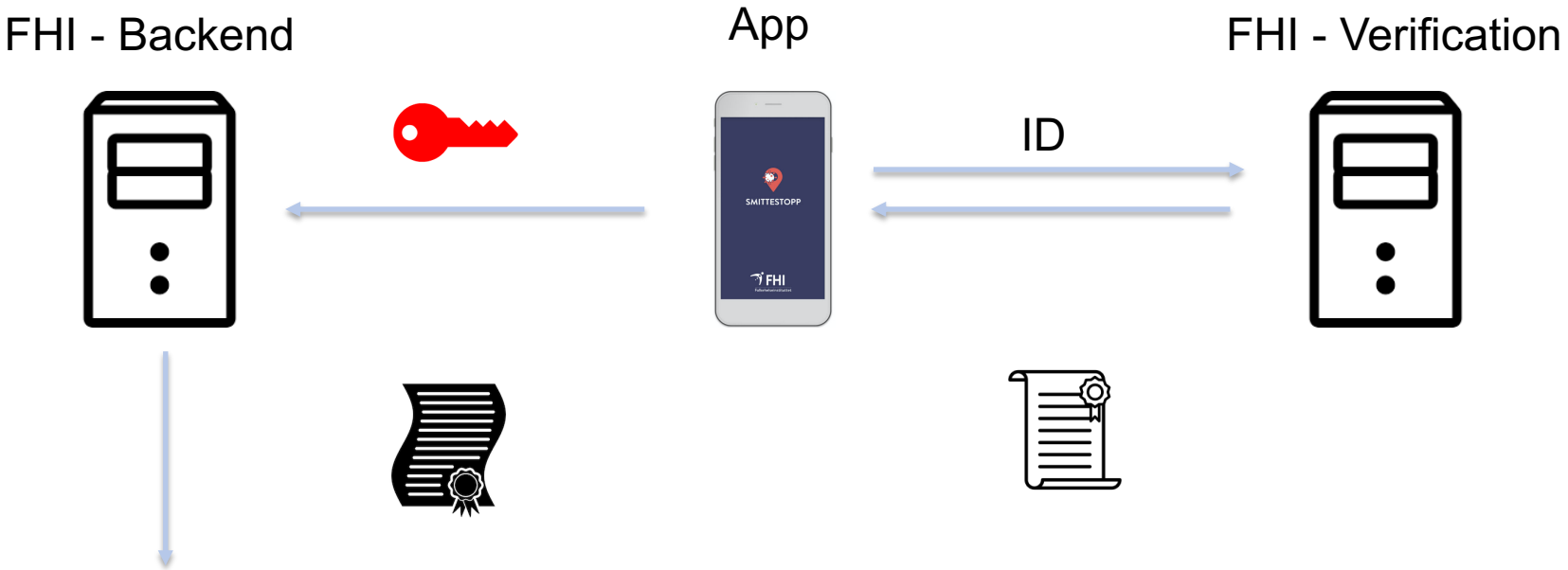
Men....

Anonymitet



ID kan knyttes til Smittenøkler ved opplasting!

Anonymitet



Løsning: Appen endrer attesten før den sendes videre.

Anonymitet

Serverne kan koble ID og smittenøkler via attesten.

Dette kan brukes til å lage kontaktgrafer eller spore brukere dersom tilgang til telefoner eller stasjonære sendere.

Ved å bruke en attest som kan *randomiseres* så unngår vi at ID og smittenøkler kan kobles av serverne.

OBS: det er fremdeles mulig å gjøre koblinger basert på tid.

Protokollen

Hash-funksjon SHA-256

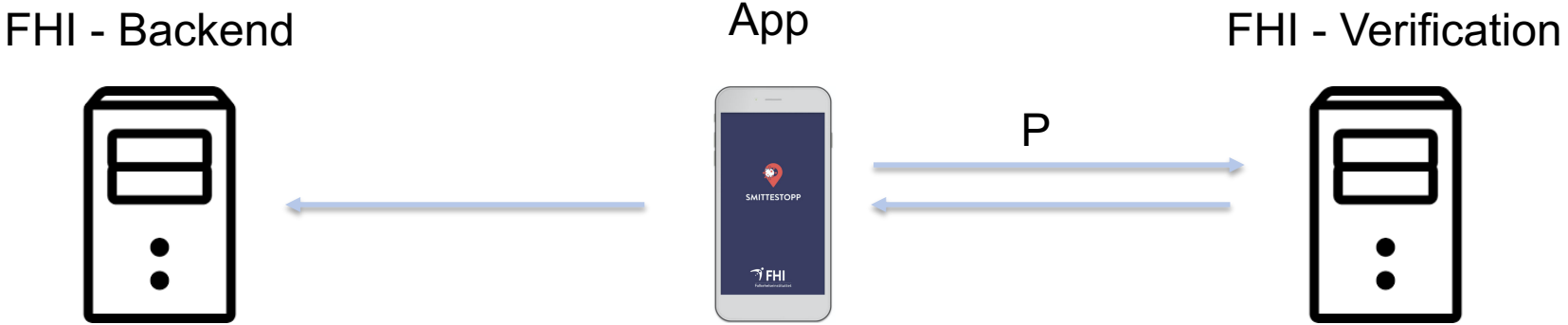
Hash funksjon H slik at:

- Output $y = H(x)$ er tilfeldig
- Det er vanskelig å finne x og y slik at $H(x) = H(y)$
- Transformere t til elliptisk kurve punkt $T = H(t)$

Elliptisk kurve P-256

- Elliptiske kurver gir sikkerhet og effektivitet
- Vanskelig å finne a dersom $A = a \cdot G$
- Randomiserte punkter skjuler all informasjon

Protokollen



t ← tilfeldige bits
T = Hash(t)

r ← tilfeldig tall
P = r · T

Protokollen

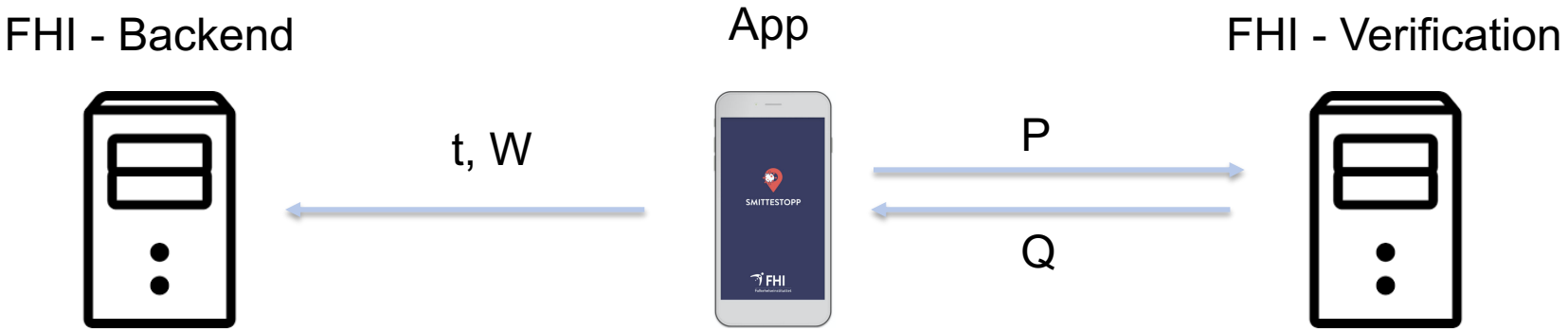
FHI - Backend

App

FHI - Verification

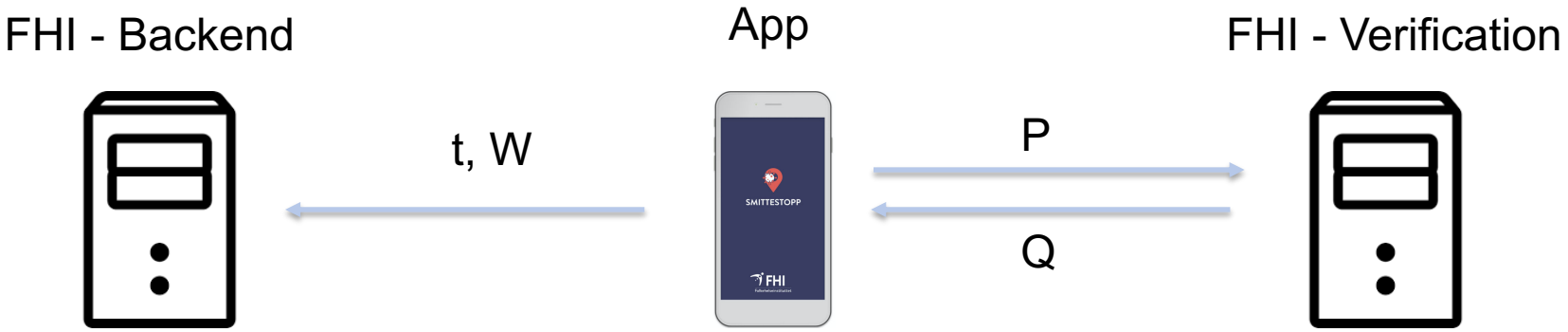
k ← attest-nøkkel
Q = k · P

Protokollen



$$W = (1/r) \cdot Q = k \cdot T$$

Protokollen



k ← attest-nøkkel
T = Hash(t)
W’ = k · T
Er W’ og W like?

Konklusjon

Denne protokollen gjør at vi slipper å måtte stole på at våre kontaktdata ikke vil misbrukes.

Dette minimerer mengden sensitiv data dersom denne skulle komme på avveie f.eks. pga. hacking.

Protokollen kan også benyttes av de andre smittesporing-appene basert på Google / Apple. Kan generelt brukes i systemer som tillater autentisert men anonym tilgang.

Takk! Spørsmål?

Epost: tjerand.silde@ntnu.no
Nettside: tjerandsilde.no

GitHub-repo: HenrikWM/anonymous-tokens