NTNU | Norwegian University of Science and Technology

# Smittestopp dissekert

Tjerand Silde – 20. September, 2022

# Personvern

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson.

Innebygget personvern:

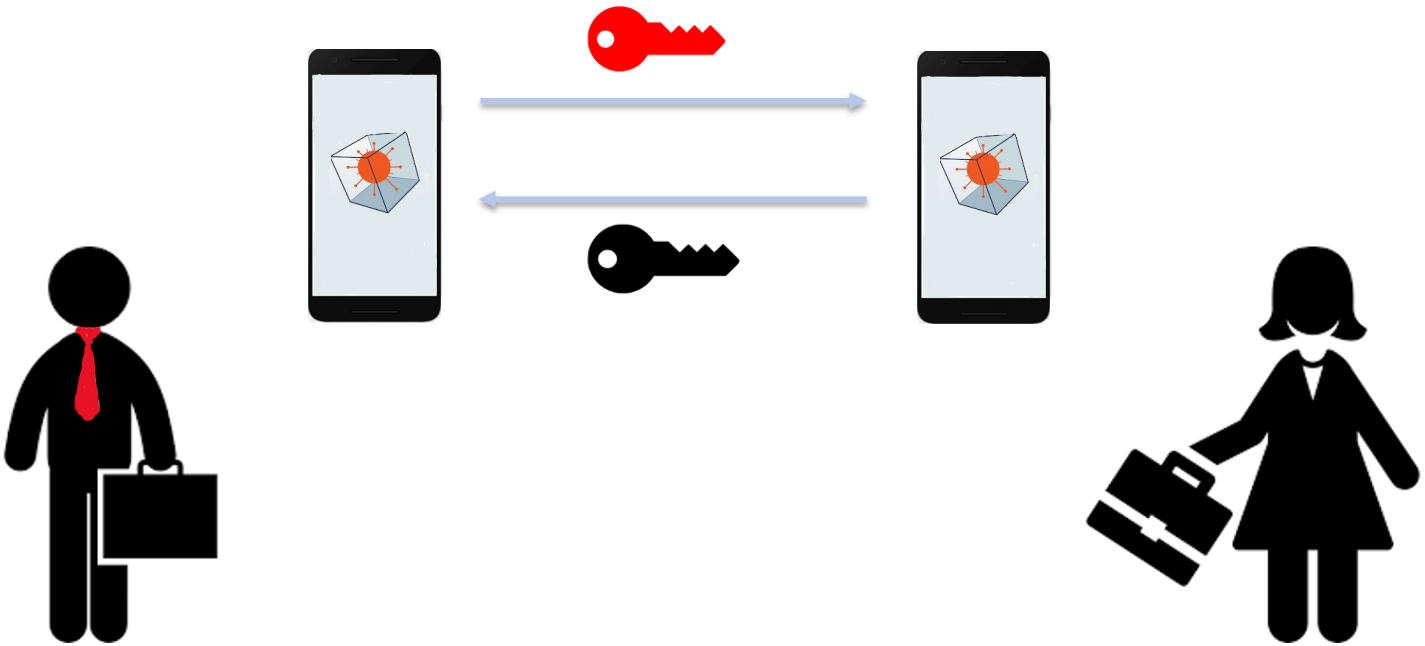
1. Vær i forkant, forebygg fremfor å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

# SMITTESTOPP V1

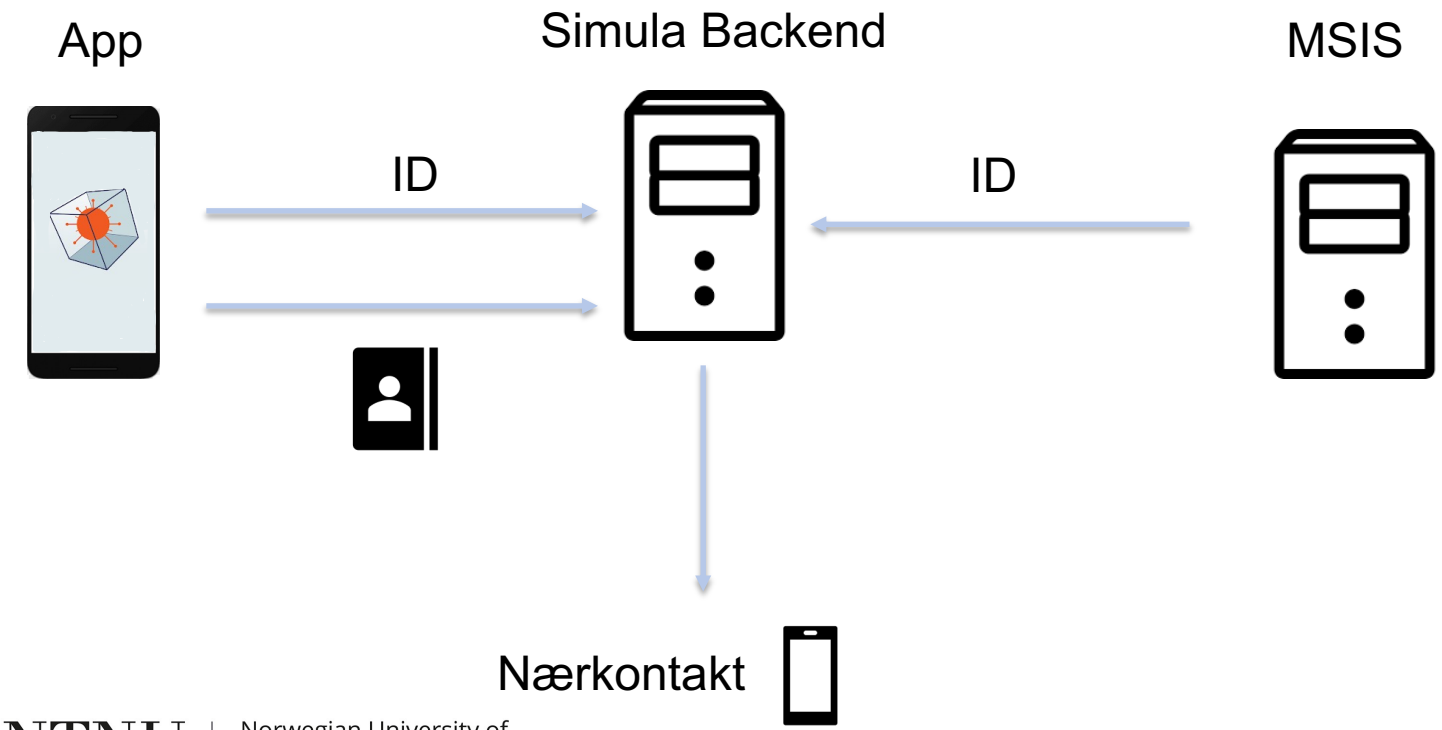
# Utfordringer

- Digitale smittesporingsverktøy eksisterte ikke
- Vi var i starten av en kaotisk pandemi
- iPhone satt BLE på pause i bakgrunnen

# Smittesporing ved hjelp av mobiltelefoner



# Opprinnelig Smittestopp



# Identifisering av brukere

1. Hver brukes identifiseres ved registrering
2. Brukerne får tilegnet en unik bruker-ID
3. Appen kringkaster bruker-ID kontinuering
4. Appen laster kontinuering opp mottatte ID-er
5. Appen laster kontinuerlig opp GPS-koordinater
6. Positiv test: Et skript kjøres for å finne kontakter
7. Varsling: Nærkontakter får tilsendt en SMS

# Identifisering av brukere

1. Hver brukes identifiseres ved registrering
2. Brukerne får tilegnet en unik bruker-ID
3. Appen kringkaster bruker-ID kontinuering
4. Appen laster kontinuering opp mottatte ID-er
5. Appen laster kontinuerlig opp GPS-koordinater
6. Positiv test: Et skript kjøres for å finne kontakter
7. Varsling: Nærkontakter får tilsendt en SMS

# Sporing av brukere


KAN BRUKES TIL SPORING: Smittestopp-appen kan i øyeblikket brukes til sporing av personer. Foto: Heiko Junge

## Har funnet sikkerhetsrisiko i Smittestopp-appen – kan brukes til å spore andre

**Smittesporingsappen gjør det mulig for datakyndige å spore dem som bruker appen. Det viser undersøkelsene til datautvikler Hallvard Nygård. Det utgjør en potensiell sikkerhetsrisiko for regjeringsmedlemmene, som nesten alle lastet ned appen umiddelbart.**



vg.no/nyheter/innenriks/i/y3dwae/har-funnet-sikkerhetsrisiko-i-smittestopp-appen-kan-brukes-til-aa-spore-andre

# Lagring av data

To formål: smittesporing og forskning

All data lagres på en sentral server
Serveren er hos Microsoft i Irland
Data består av GPS-koordinater og ID
All data lagres for 30 dager

Denne type data kan misbrukes
Dette er en gullgruve for hackere

# Brudd med personvernprinsipp

Samfunn

## Personvernråd i EU mener norsk app bryter med viktig personvernprinsipp

Skrevet av Øyvind Bye Skille 16. april 2020 135


Skjermbilder av den norske appen Smittestopp. Illustrasjon: FHI/NRKbeta

# Krav om smittesporing fra EU

I samsvar med EUs datasikkerhets- og personvernregler

Implementeres i samarbeid med offentlige helsemyndigheter

Benytte de nyeste teknologiske løsningene som ivaretar personvernhensyn, ikke ved sporing av lokasjon

De bør baseres på anonymisert data

De bør være kompatible med hverandre i hele EU



datatilsynet.no/personvern-pa-ulike-omrader/korona/en-eu-tilnarming-til-kontaktsporingsapper

# Brukervennlighet, batteri og testing


**En Google-bruker**

16. april 2020

91

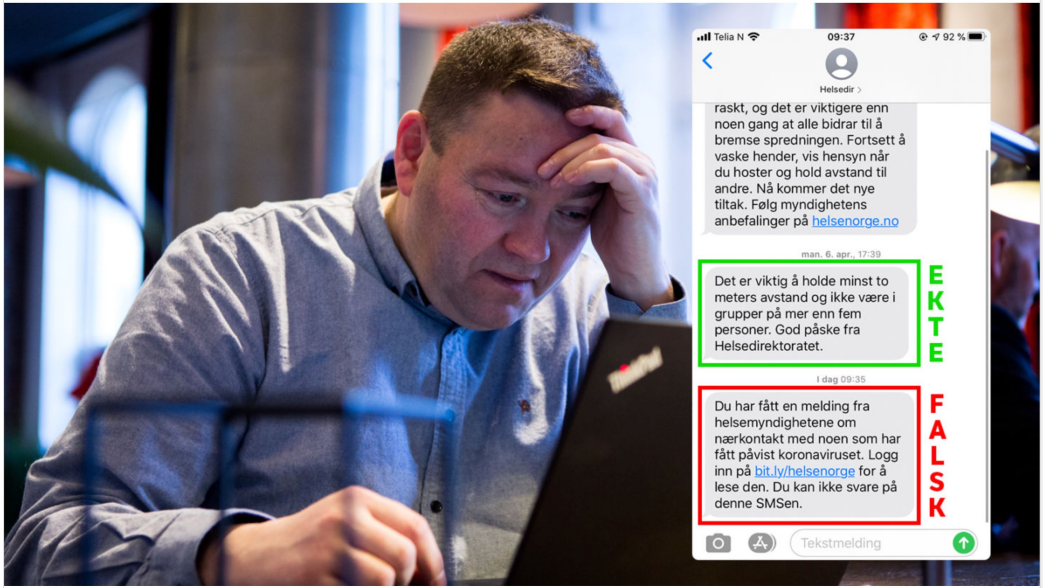
Viktig å bidra ja, men da må det jo fungere. Registrering bare henger. Første gang (og senere) kom det feilmelding: The custom error module does not recognize this error. Stiller som flere her spørsmål m behov for GPS hele tiden og strømforbruk.

# Usikker varsling

Samfunn

## Så enkelt er det å forfalske SMS-er fra Smittestopp

Skrevet av Martin Gundersen og Øyvind Bye Skille 20. april 2020 66




Sikkerhetsekspert Per Thorsheim mener man ikke kan stole på SMS. Foto: Martin Gundersen

# Fare for formålsutglidning

Det finnes allerede eksempler på at personvernbestemmelser må vike dersom politikerne anser det som viktig nok. I 2014 ble en mann fra Tsjetsjenia dømt, og dermed ble det lagret DNA av ham i politiets DNA-register. Dette registeret skal bare brukes til straffesaker, ifølge lovverket som regulerer registeret. Senere fikk kvinnen han var gift med lov til å bruke DNA fra dette registeret til å avgjøre en farskapssak, som altså ikke er en straffesak. Høyesterett mente da at barneloven skulle få forrang foran politiregisterloven.



agendamagasin.no/kommentarer/bekjempe-pandemi-finnes-app

# Ekstern analyse

## FHI-appen Smittestopp gjennomgås nå av sikkerhetseksperter

Målet er at appen for digital smittesporing skal lanseres over påske i et utvalg kommuner. En ekspertgruppe satt ned av Helsedepartementet ser nå over datakoden for oppdage sikkerhetsproblemer før appen lanseres.

DIGITAL SMITTESPORING: Målet er at apper skal gjøre det mulig å digitalt «markere» en person i bybildet som smittet.
ILLUSTRASJON: TORE MEEK / NTB SCANPIX (FOTO), NRK (MONTASJE)

Øyvind Bye Skille
@Byeskille
Journalist

Publisert 8. apr. 2020 kl. 20:14
Oppdatert 9. apr. 2020 kl. 11:07

Artikkelen er mer enn to år gammel.

nrk.no/norge/fhi-appen-smittestopp-gjennomgas-na-av-sikkerhetseksperter-1.14977918

# Anbefalinger

1. Forskrift og anonymisering
2. Dele opp formålene
3. Fjerne all data man ikke trenger
4. Implementere «differential privacy»
5. Gå over til en distribuert modell
6. Tilgjengeliggjør kode
7. Sørg for regelmessig evaluering



regjeringen.no/contentassets/88ec3360adae44a1a9635fd6c1a58fca/200520_rapport_ekspertgruppa_smittestopp.pdf

# Overvåking av enkeltpersoner

**Simula vil beskytte personvernet:** Simula ønsker ikke at ukjente aktører skal få tilgang til en kildekode som har potensiale i seg til å misbrukes ved å overvåke enkeltpersoner. Dersom appen skal deles med andre, mener Simula at dette skal gjøres av norske myndigheter i samråd med Simula.



kode24.no/kodenytt/derfor-vil-ikke-simula-apne-kildekoden/72324506

# Rapport fra Amnesty

## Bahrain, Kuwait og Norge har de verste korona-appene

Det er ikke nok å sette Smittestopp-appen på pause. Hvis den ikke endres drastisk, bryter den med personvern og menneskerettigheter.

# Veien videre for FHI

Alternativene som har vært vurdert er:

- Alternativ 0: Avvikle helt og velge bort nasjonal automatisert digital sporing
- Alternativ 1: Endre Smittestopp innenfor eksisterende løsning, innføre to samtykker i appen
- Alternativ 2: Ny app basert på ENS-rammeverket, utelukkende for digital smittesporing
- Alternativ 3: To apper, en basert på ENS for digital sporing, i tillegg til ny versjon av Smittestopp utelukkende for innsamling av data til analyseformål


fhi.no/contentassets/4f79542c8a544edbaaf004d07242777a/rapport-oppdrag-hod-hurtigutredning---videre-plan-for-applikasjonen-smittestopp-v1.0-150920.pdf

# SMITTESTOPP V2

# Exposure Notification Service

1. Når du installerer appen trenger du ikke å registrere noen personopplysninger

2. Når appen kjører kringkaster den identifikatorer. Disse identifikatorene byttes med noen minutters mellomrom

3. Appen tar vare på alt den har “sagt” og alt den har “hørt”

4. Om du blir smittet kan du velge å laste opp det du har “sagt” til en “oppslagstavle”

5. Alle laster ned oppslagstavla daglig og sammenligner med det de har “hørt”

6. Om det er en match varsler telefonen brukeren om at de kan være smittet



kode24.no/artikkel/historien-om-smittestopp-fra-innsida-personvern-handler-om-tekniske-valg/77012938

# Personvernvennlig løsning

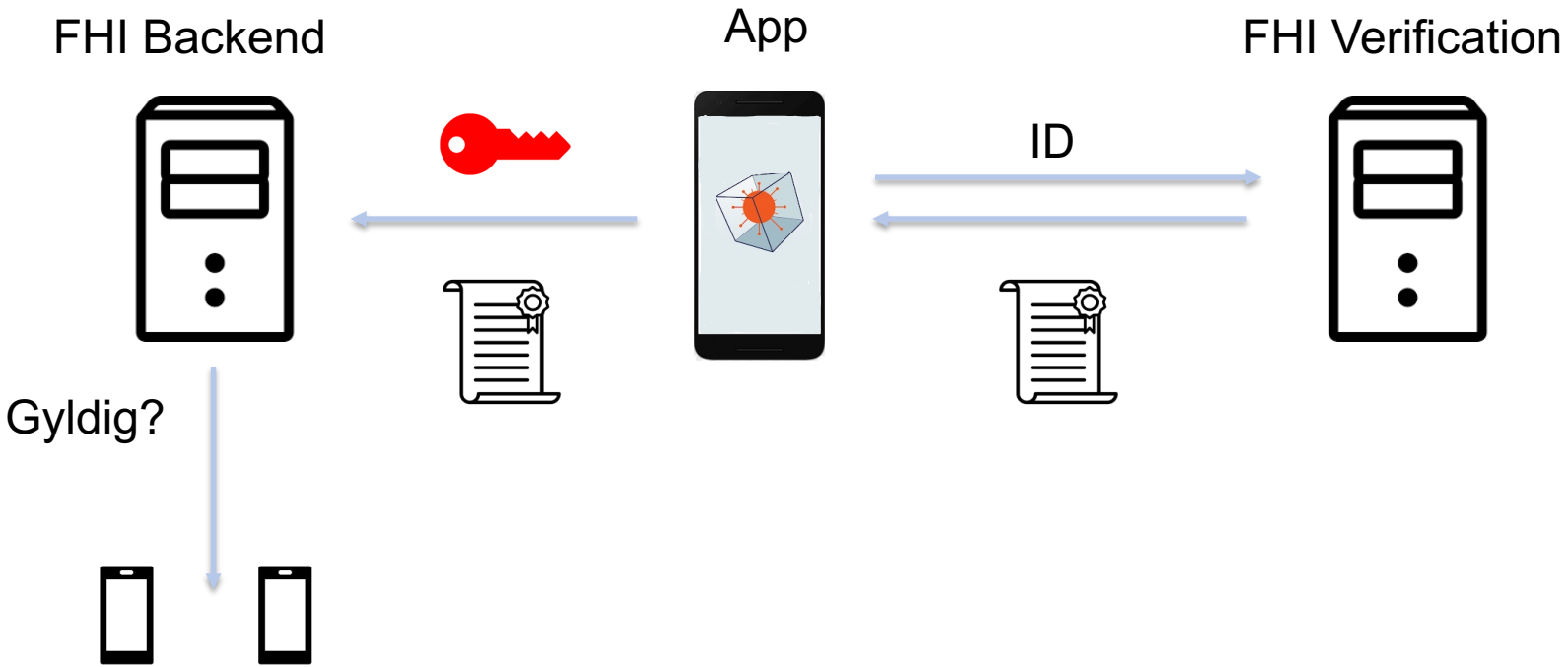
Den nye Smittestopp-appen er en helt ny teknisk løsning, og skiller seg ifølge FHI fra den gamle på flere måter:

- Den nye appen lagrer alt på din telefon, og laster ikke opp informasjon til et sentralt register slik den gamle gjorde.
- Den nye appen benytter kun Bluetooth og ikke GPS eller annen satelittposisjonering. Dermed lagrer den ikke hvor du har vært.
- Den nye appen brukes kun til smittesporing, og ikke analyse eller forskning.
- Den nye appen samler ikke inn data der du kan identifiseres, og dermed er det heller ikke noe å få innsyn i.
- Den nye appen bruker mindre batteri enn den gamle.

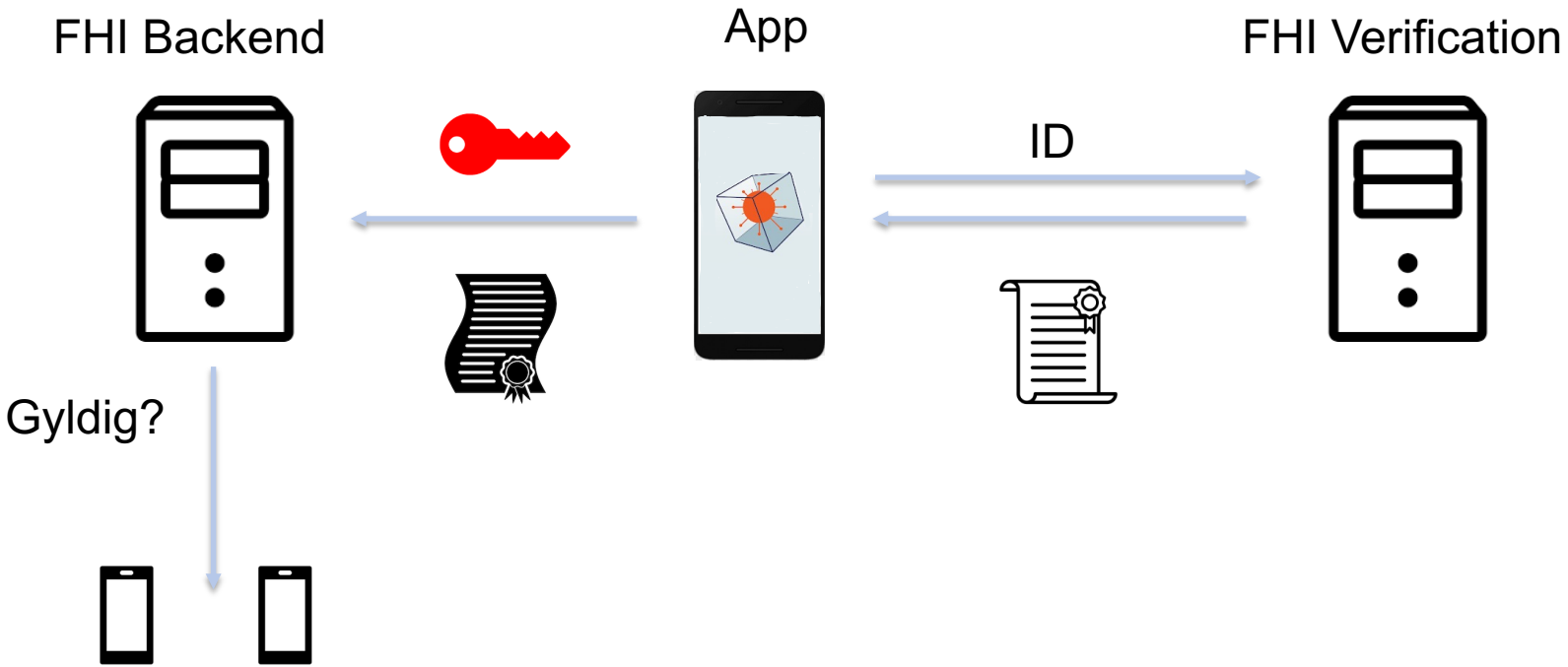


datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-smittestopp-lansert

# Utgangspunkt Smittestopp v2



# Anonymitet i Smittestopp v2



# Merverdi til Smittestopp

Prinsipielt:

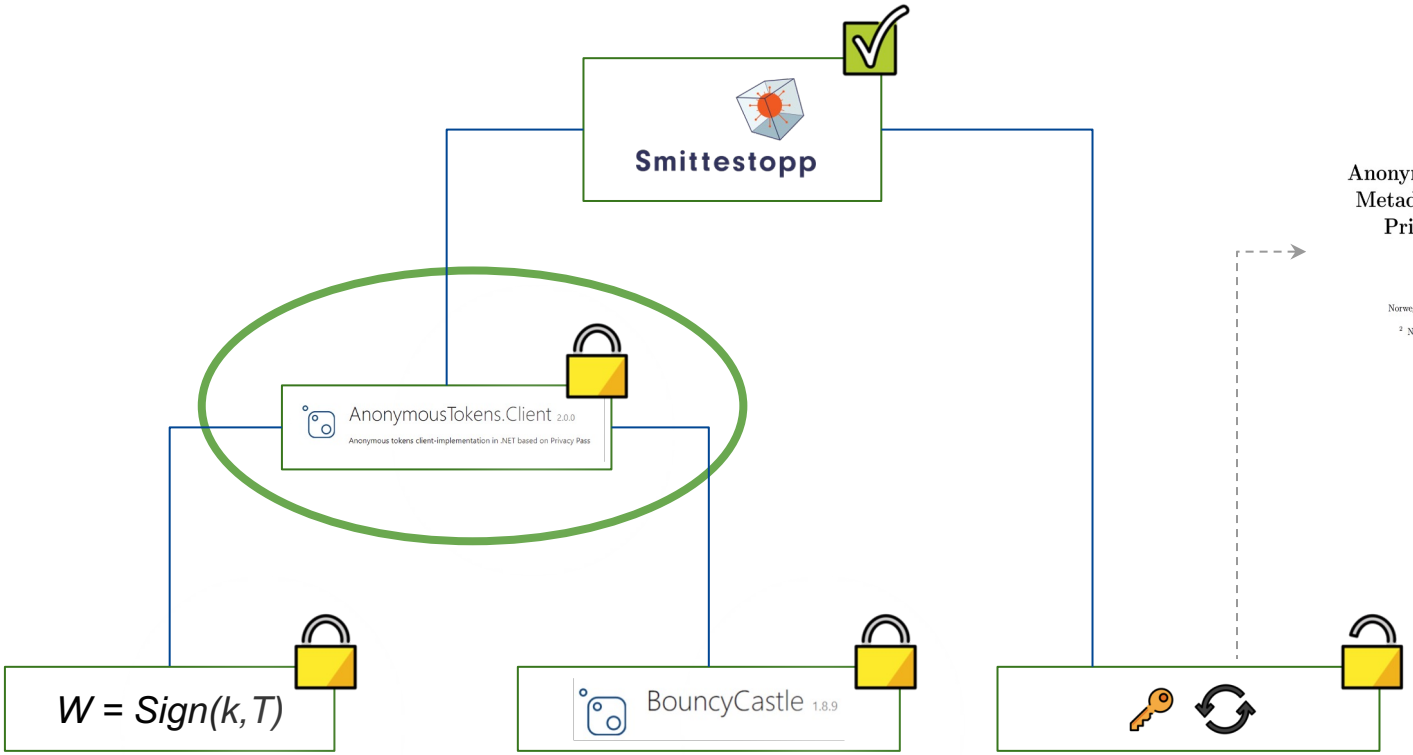
- En attest fra FHI Verification er entydig knyttet til en identitet
- FHI Backend trenger ikke identiteter for å gjøre jobben sin
- Vi framtvinger at det blir sånn

Logger kan lekke de smittedes sensitive 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

# Penetrasjonstest

## 1.1 OPPSUMMERING AV DE VIKTIGSTE FUNNENE

| | |
|---|---|
| POSITIVT | Pålogging til appen krever sikker autentisering med ID-porten. Det ble ikke funnet svakheter i autentiseringsflyten. |
| POSITIVT | Det lyktes ikke å injisere noe ondsinnet kode i appen eller gjennom API-ene. |
| POSITIVT | Personvern for brukerne er godt ivaretatt gjennom personvernerklæring og sikker lagring av personsensitive data. |

## 1.2 IMPLEMENTERTE TILTAK UNDERVEIS I PENETRASJONSTESTEN

- Cookie for lastbalanserer er deaktivert på Backend-server, da denne ikke var i bruk.
- Støtte for TLS1.0/1.1 deaktivert på vl-op.ss2.fhi.no
- Tiltak mot forfalsking av e-post er implementert på smittestopp.no.
- Omdirigering fra smittestopp.no til helsenorge.no/smittestopp



fhi.no/contentassets/93841455d6554ccb869f3a2fe362b9f6/vedlegg/presentasjoner/pdfer/penetrasjonstest---smittestopp-sammendrag.pdf

# LÆRDOMMER

# Personvern

«Privacy by design»

Vurdere seg selv som en trussel

Dataminimering

Desentraliserte løsninger

# Sikkerhet ≠ Personvern

Sikkerhet har vært høyt prioritert hele veien, og hensyn til personvern er gjennomgående i utviklingen av appen. Vi har diskutert problemstillinger løpende med Datatilsynet og andre fagmiljøer innen personvern.



vg.no/nyheter/meninger/i/1npvjQ/app-for-smittesporing-nytt-virkemiddel-i-en-vanskelig-tid

# Åpenhet i prosess

## Tirsdag 17. november 2020: Kildekoden er publisert

I ettermiddag publiserte vi kildekoden til Smittestopp, les mer på Nå kan du se kildekoden til nye Smittestopp (fhi.no).

Denne dagen var det også møte i den tekniske delen av fagrådet, se Referat arkitektmøte eksternt fagråd 17.11.2020 (PDF).



## Fredag 13. november 2020: Første workshop i risiko- og sårbarhetsarbeidet gjennomført

FHI holder en workshopserie i forbindelse med risiko- og sårbarhetsanalyse-arbeidet (ROS-arbeidet) for nye Smittestopp. Se presentasjon fra workshopen som ble holdt på fredag på Risiko og sårbarhet workshop 1 13.11.2020 (PDF).

Denne dagen var det også møte i det eksterne fagrådet, som vanlig på fredager. Se Referat demomøte 2 Nye Smittestopp 13.11.2020 (PDF).

# Åpen kildekode

Simulas hovedmål for appen er å lage en løsning som er et godt egnet verktøy for å spore smitte; bidra til å begrense epidemien; være minst mulig inngripende; og ikke skape nye utfordringer for personvern og datasikkerhet.

Simula mener at å gjøre kildekoden til appen åpent tilgjengelig nå ikke bidrar til mer personvern eller bedre sikkerhet.



kode24.no/kodenytt/derfor-vil-ikke-simula-apne-kildekoden/72324506

# Hastverk er lastverk

- Mange tekniske feil hadde vert unngått dersom man hadde tatt seg litt bedre tid (de ble funnet umiddelbart)
- En desentralisert løsning var foreslått ved lansering
- Ny infrastruktur ble bygget på tvers av land og teknologier

# Lytte til ekspertene

## Hundrevis av it-eksperter fra hele verden ut mot sporingsapper som norske Smittestopp

Eksperter går i dag ut mot smittesporingsapper av den typen som innføres i Norge. Norsk professor ønsker ikke at Smittestopp skal gi legitimitet for overvåking i totalitære regimer.


Appen Smittestopp har valgt en løsning som får tydelig kritikk fra et stort antall internasjonale eksperter.
FOTO: STIAN LYSBERG SOLUM / NTB SCANPIX

**Øyvind Bye Skille**
@Byeskille
Journalist

**Martin Gundersen**
Journalist

Publisert 20. apr. 2020 kl. 14:00
Oppdatert 21. apr. 2020 kl. 11:35

Artikkelen er mer enn to år gammel.

nrk.no/norge/hundrevis-av-it-eksperter-fra-hele-verden-ut-mot-sporingsapper-som-norske-smittestopp-1.14988352

# Vær kritisk til teknologi-optimisme

Appen var i bruk fra desember 2020 til august 2022. Funket den?

**Vi vil nok aldri få et definitivt svar på hvor stor effekt smittesporingsapper hadde. Selv om appene ble innført i mange land så gikk pandemien gjennom flere faser med forskjellige responser, smittsomhet og dødelighet. Det er nok vitenskapelig umulig å skille effekten fra appen fra andre tiltak og sykdommens iboende variasjon.**

Men vi må nok innse at det ikke var noen *game changer*.



kode24.no/artikkel/historien-om-smittestopp-fra-innsida-personvern-handler-om-tekniske-valg/77012938

# Takk! Spørsmål?

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