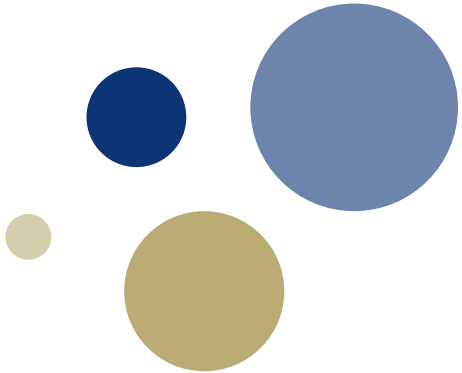
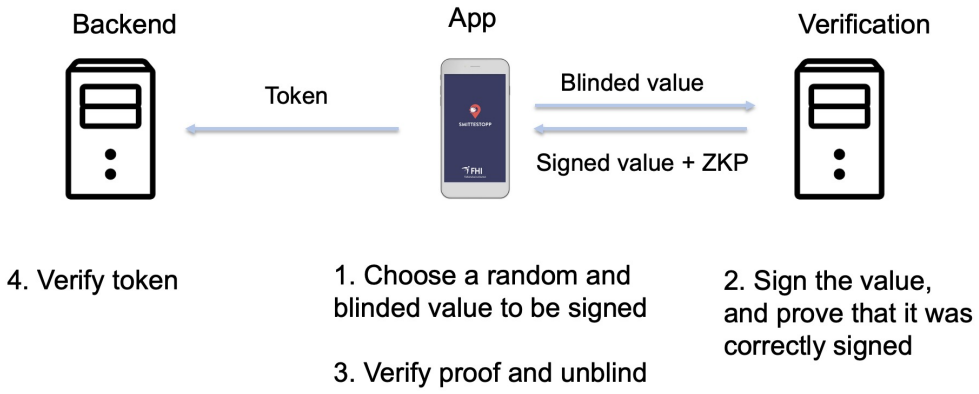


Private Contact Tracing and Anonymous Tickets

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

Content

- Digital Contact Tracing
- The Smittestopp Contact Tracing App
- Ongoing Research & Anonymous Tickets
- Resources



Digital Contact Tracing

The Norwegian Institute of Public Health has developed an app to supplement traditional contact tracing.

The app sends you a notification if you have been close to someone that has tested positive for Covid-19.

The hope is this may be faster, and can notify contacts that you forgot or didn’t know about.

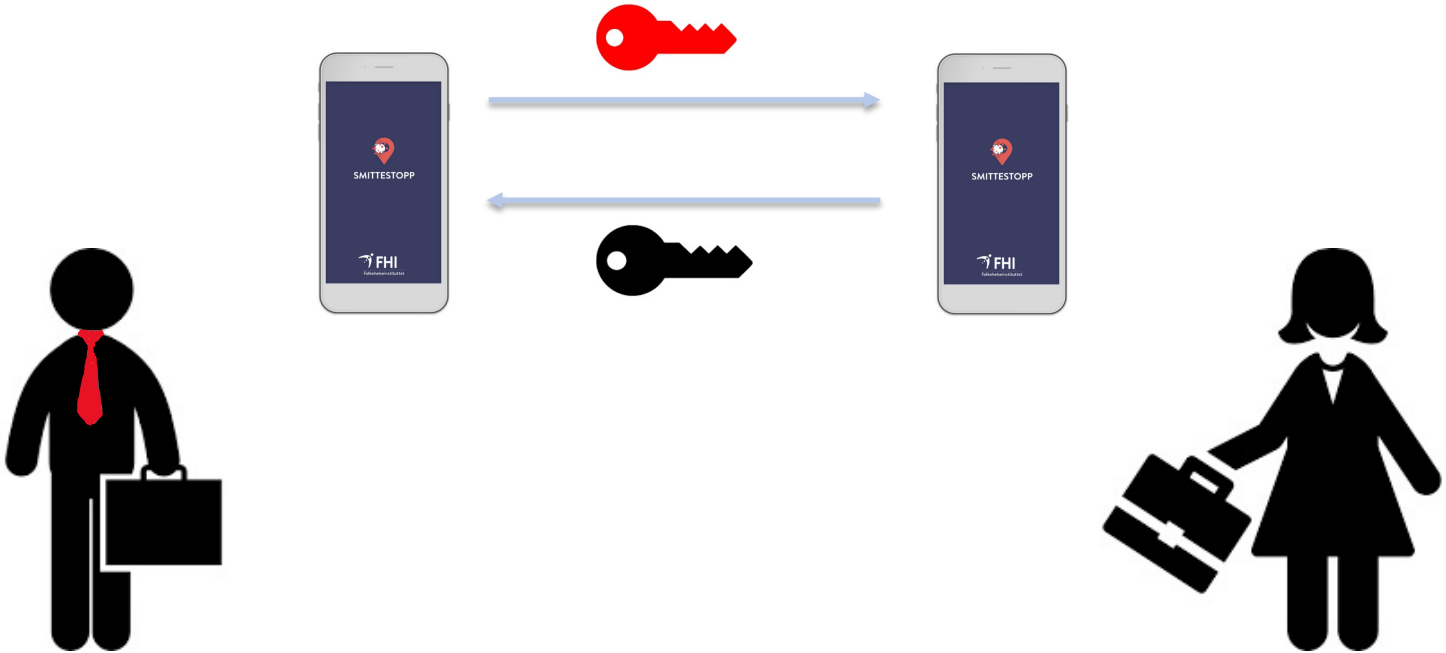
Digital Contact Tracing

All data is stored on the user's phone. It uses Bluetooth for communication with other phones, but no GPS tracking.

You only identify yourself to report a positive test, and then you upload the "infection keys" anonymously to the server.

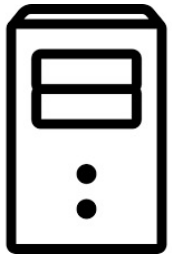
The other users check locally if they have been in touch with someone who has uploaded their keys.

Smittestopp



Smittestopp

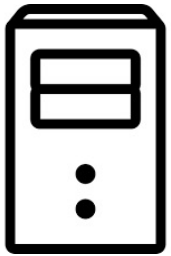
Backend



App

ID

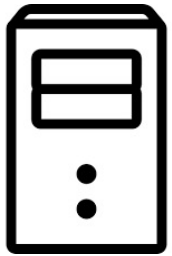
Verification



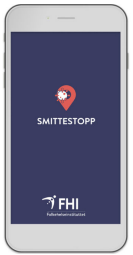
Report Infection

Smittestopp

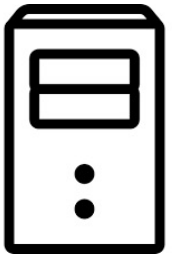
Backend



App



Verification



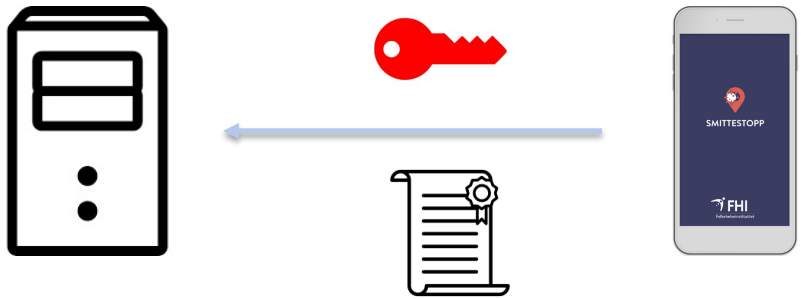
Confirm Infection

Smittestopp

Backend

App

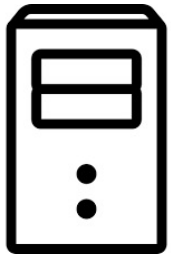
Verification



Send Infection Keys

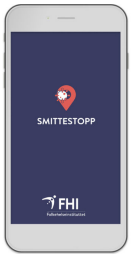
Smittestopp

Backend

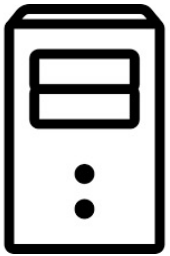


Valid?

App

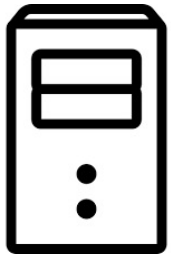


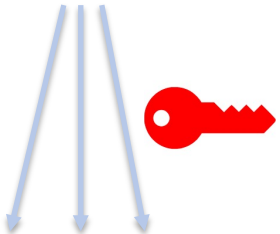
Verification



Smittestopp

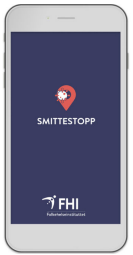
Backend



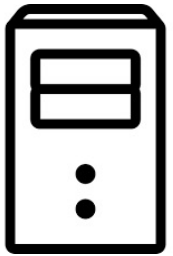


?

App

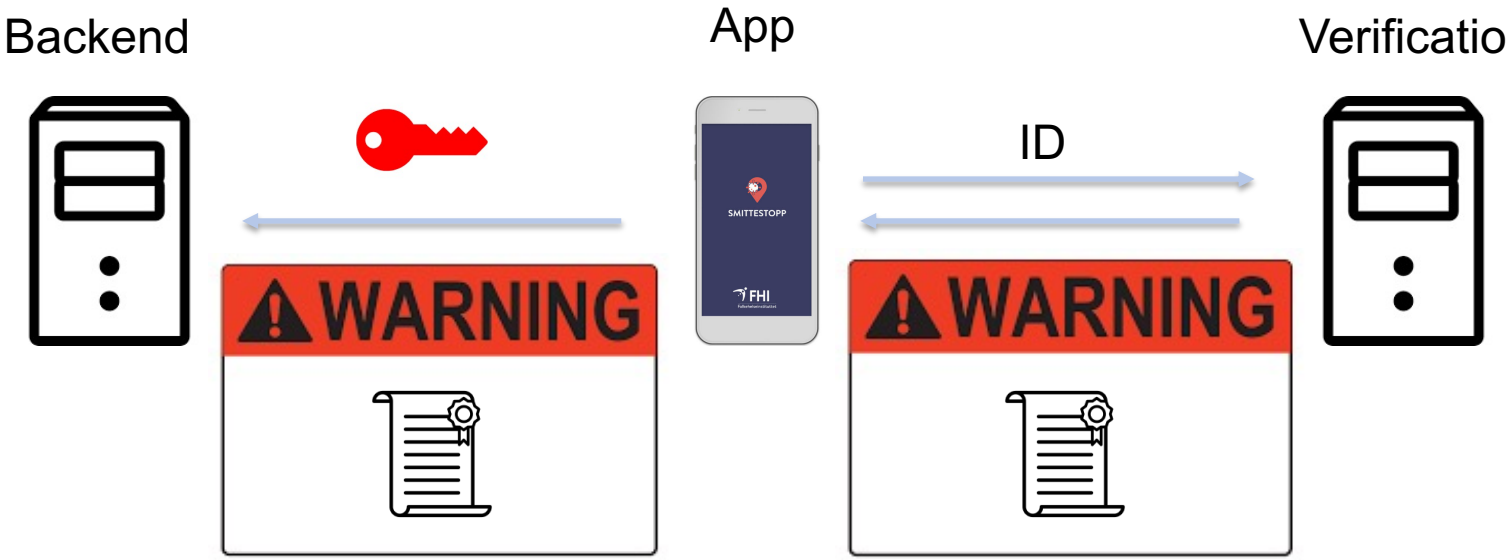


Verification



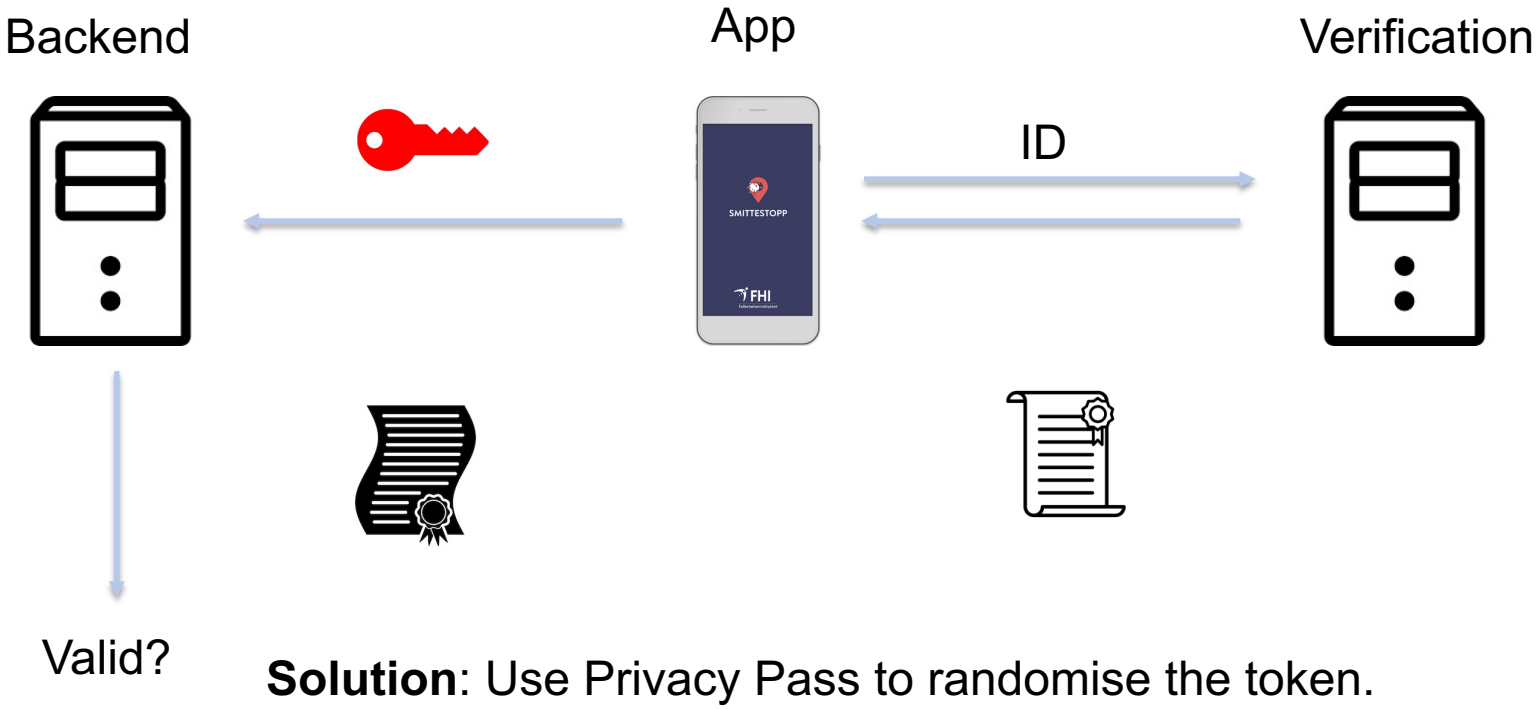
If the phones have seen the keys earlier: alert the users.

Smittestopp



ID can be tied to infection keys when uploading!

Smittestopp



Solution: Use Privacy Pass to randomise the token.

Smittestopp

Problem: Users should not hold onto tokens and upload later.

Solution: Rotate key-material every 3 days via public API.

Problem: Signer and verifier needs to share key-material.

Solution: Share a seed and generate new time-based keys.

Problem: Still possible to correlate identities with “infection keys” if the servers are logging IP-addresses and timestamps.

Solution: …

Ongoing Research & Anonymous Tickets

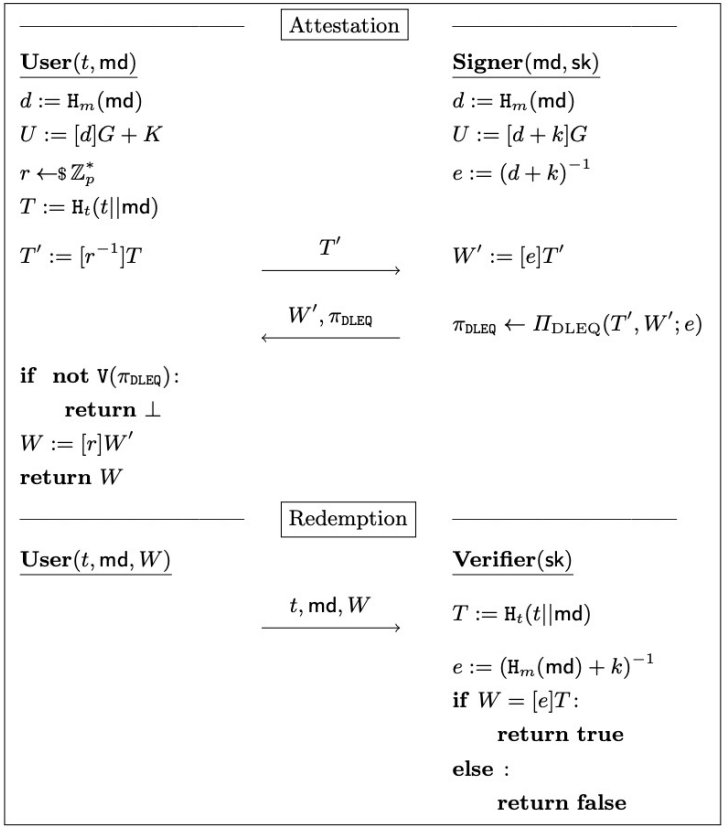
Martin Strand and I designed a new anonymous token protocol with public metadata and public verifiability.

Based on ECC, avoids pairings.
Public verification with pairings.

Revocation based on metadata.

A PoC is currently being implemented by interns at the Norwegian Defence Research Establishment.

Paper is available at: ia.cr/2021/203



Ongoing Research & Anonymous Tickets

New application: Anonymous Tickets

Every ticket holder receives anonymous tokens with public metadata about validity.

Ticket company can validate tickets and log traffic patterns but avoid tracking their users.

A PoC is currently being implemented by interns working at Entur and Bekk.

Foto: Ruter As / CatchLight Fotostudio AS

Resources

- An open-source C#/.NET library for anonymous-tokens:
- https://github.com/HenrikWM/anonymous-tokens
- Documentation for our anonymous tokens library: https://github.com/HenrikWM/anonymous-tokens/wiki
- Blog-post about anonymous tokens for private contact tracing:
- https://security.christmas/2020/22
- Blog-post about anonymous tokens with public metadata: https://world.hey.com/tjerand/anonymous-tokens-with-public-metadata-1253024d

Thank you! Questions?

Slides: tjerandsilde.no/talks

Twitter: @TjerandSilde