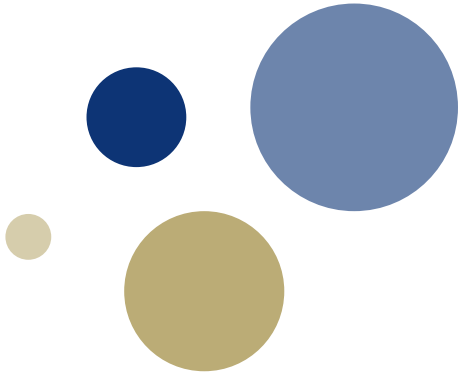
NTNU

Kunnskap for en bedre verden



Anonyme Tokens & Privat Smittesporing

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

BEKK

FFI Forsvarets forskningsinstitutt

Innhold

Anonym kommunikasjon

Digital smittesporing

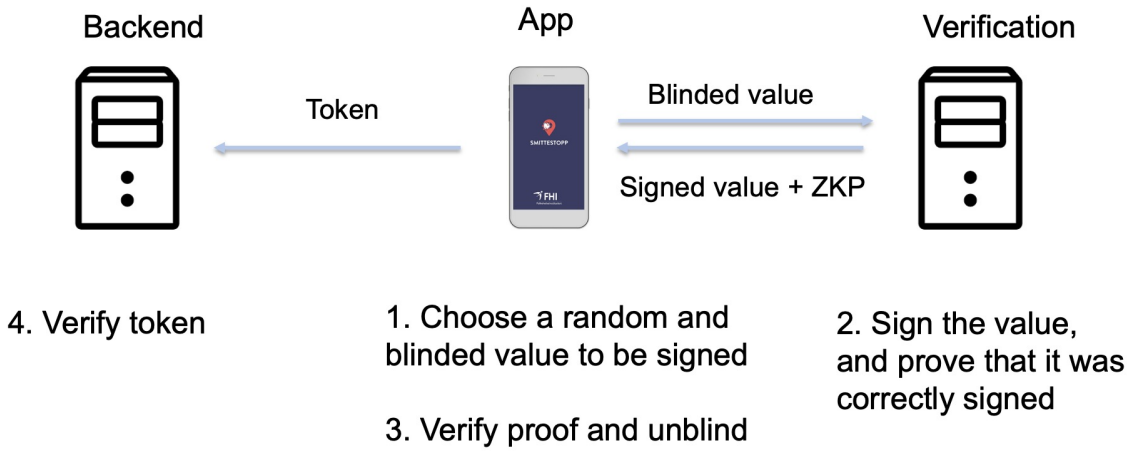
Smittestopp 2.0

Kryptografi

Protokollen

Videre arbeid

Ressurser



Anonym kommunikasjon

Mange muligheter i litteraturen: anonyme engangs-token, blinde signaturer, attributt-baserte attester, …

Egenskaper: kobling, forfalsking, offentlig eller designert verifisering, revokering, effektivitet, …

Underliggende primitiver: faktorisering, (elliptisk kurve) diskrete logaritmer, bilineære paringer, …

Anonym kommunikasjon

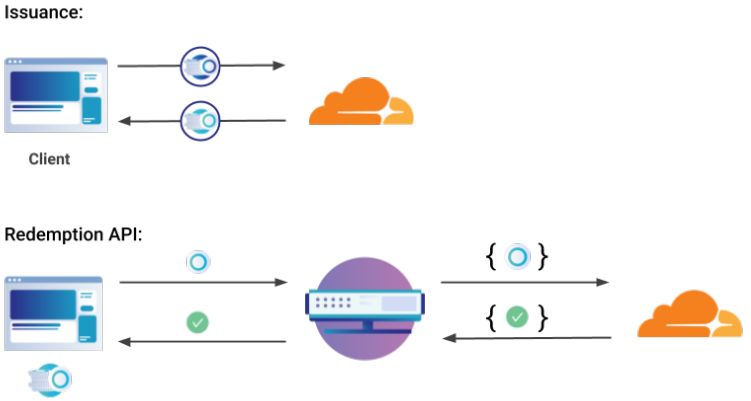
Eksempel: Privacy Pass

Utviklet av Cloudflare.

Bruksområde: Brukere kan benytte Tor uten å måtte løse CAPTCHAs hele tiden.

Sikkerhet: Kan ikke tillate sporing av brukere, og må forhindre DDOS angrep.

Utfordring: Revokere tokens.



Anonym kommunikasjon

Eksempel: PrivateStats

Utviklet av FaceBook.

Bruksområde: Brukes til å innhente anonyme telemetri data fra WhatsApp.

Løser revokering ved å oppdatere den offentlige nøkkelen deterministisk daglig.

Utfordring: Mye data må sendes.

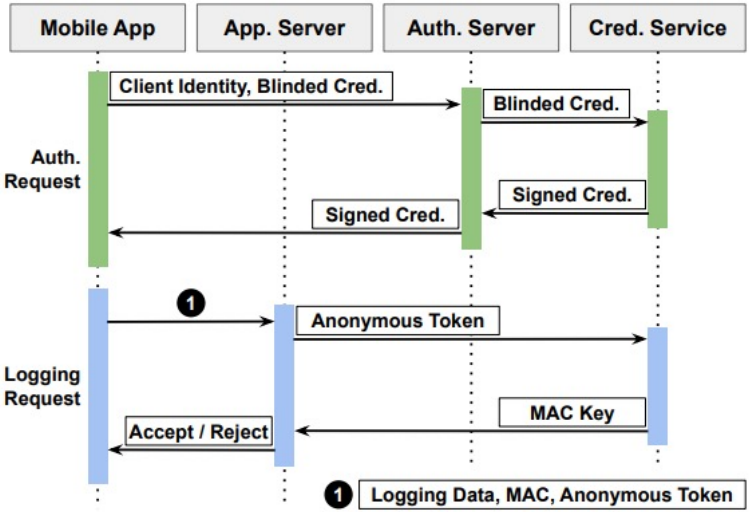


Fig. 1: Protocol flow diagram.

Digital smittesporing

FHI ønsket 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.

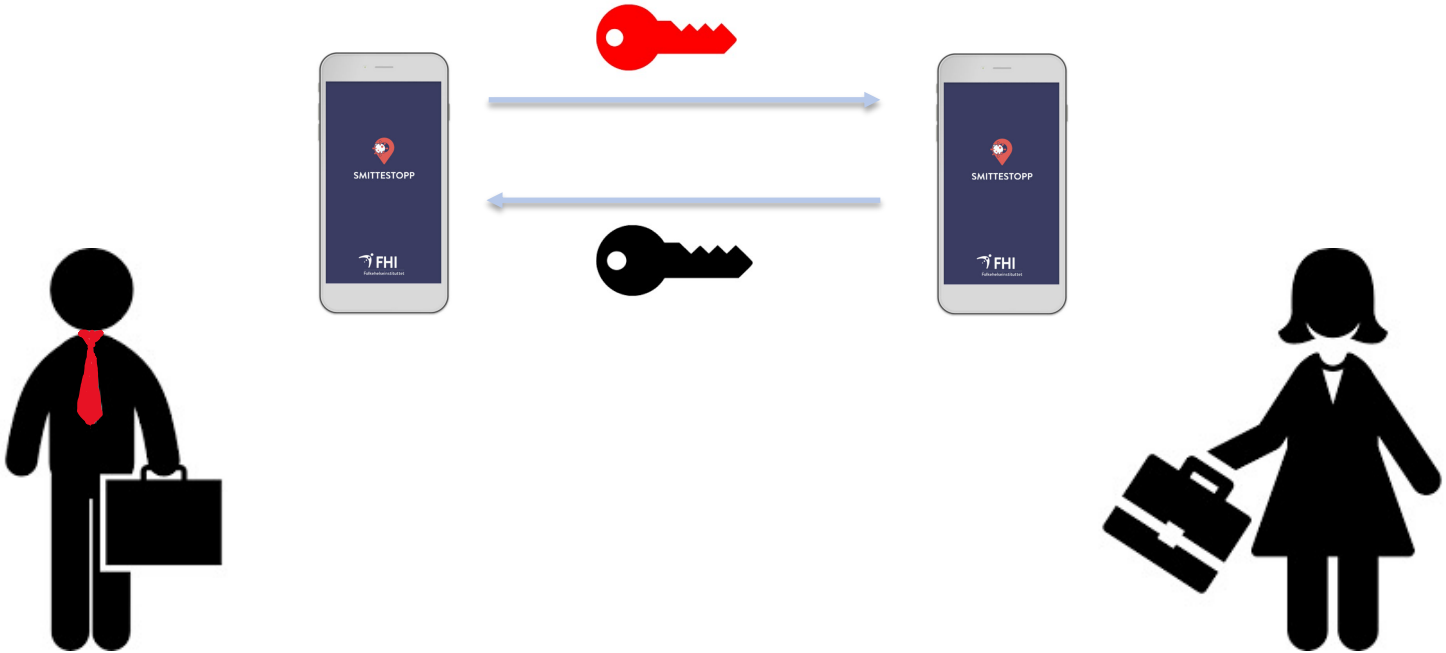
Digital smittesporing

Roterende smittenøkler gjør det er umulig 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.

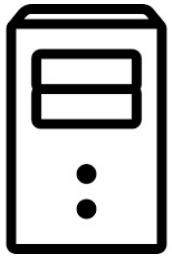
Appen sjekker lokalt dersom den har vert i kontakt med noen som har lastet opp smittenøkler på serveren.

Smittestopp



Smittestopp

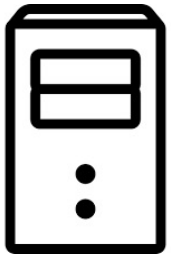
Backend



App

ID

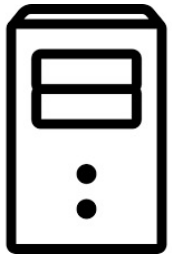
Verification



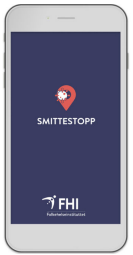
Rapportere smitte

Smittestopp

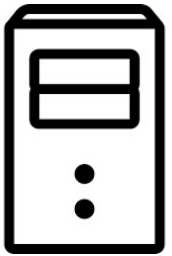
Backend



App



Verification



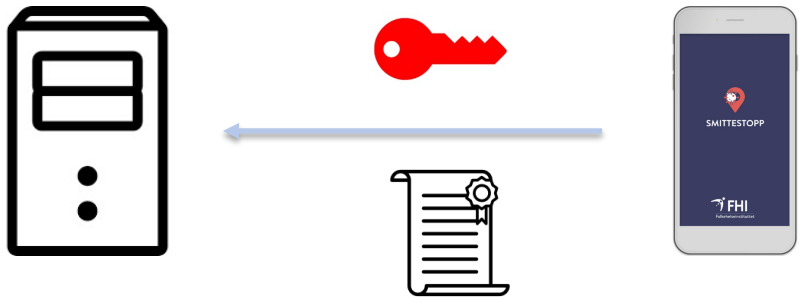
Bekrefte smitte

Smittestopp

Backend

App

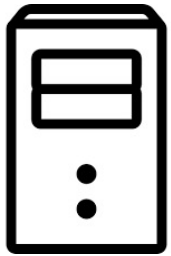
Verification



Sende smittenøkler

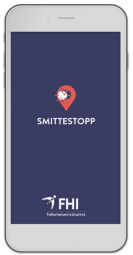
Smittestopp

Backend

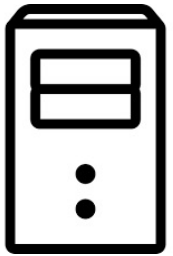


Gyldig?

App

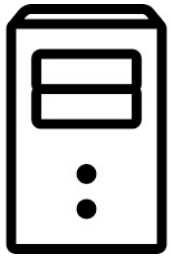


Verification

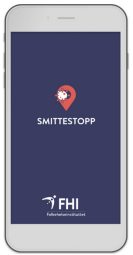


Smittestopp

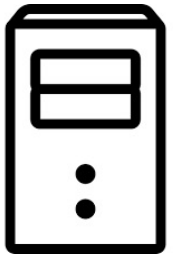
Backend

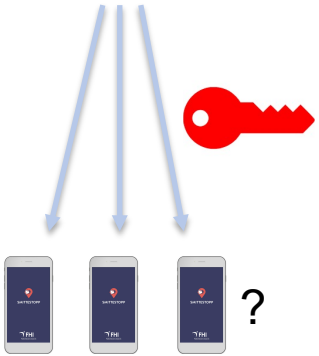


App



Verification

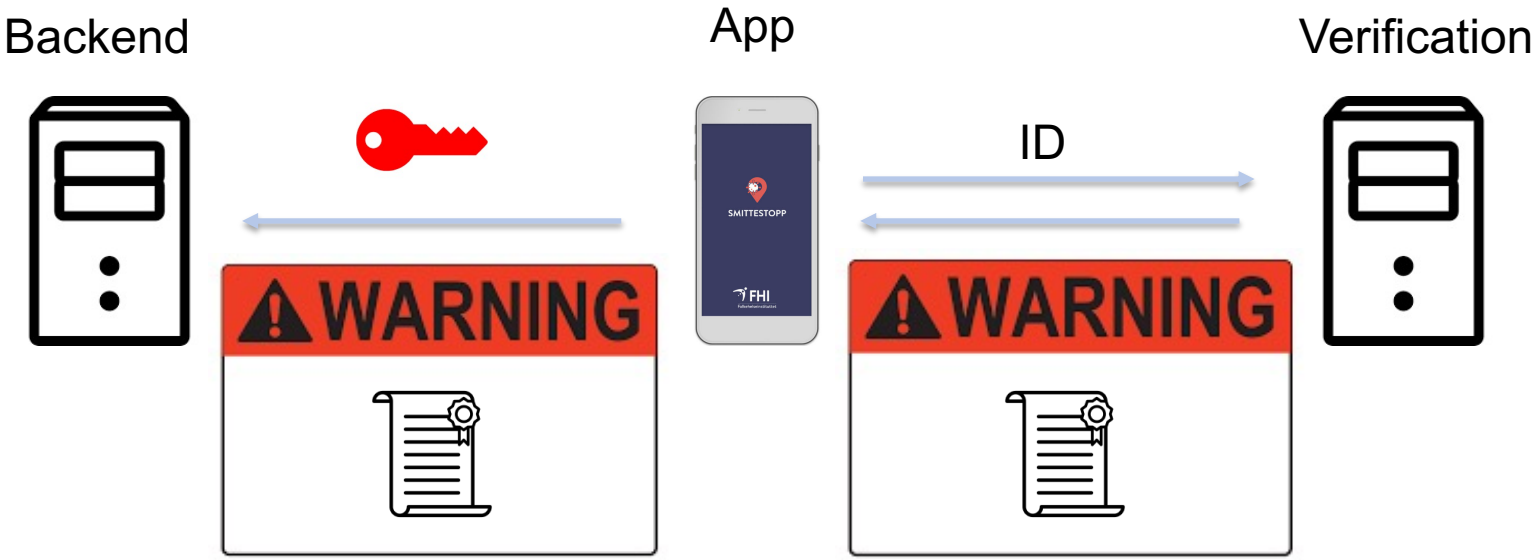




?

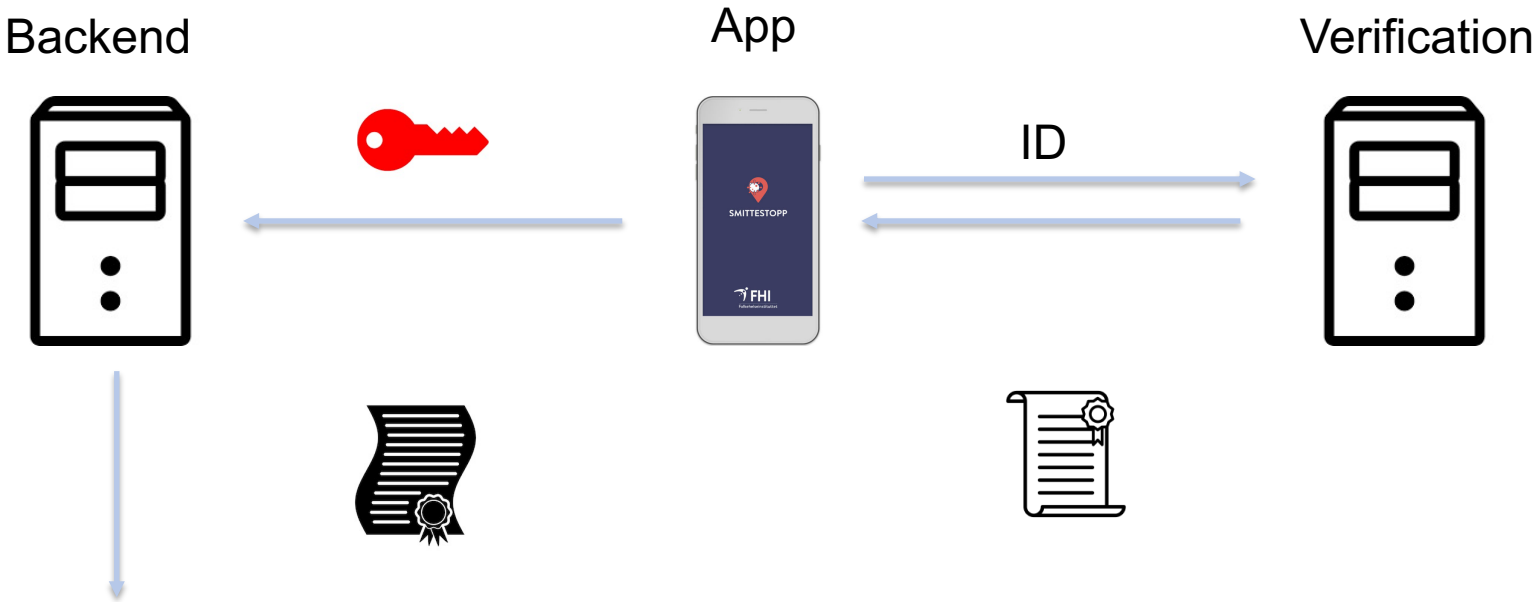
Dersom telefonen har sett nøklene tidligere: varsle brukeren.

Smittestopp



Identitet kan knyttes til smittenøkler ved opplasting!

Smittestopp



Løsning: Appen randomiserer token før den sendes videre.

Smittestopp

Utfordring: Brukere burde ikke ha mulighet til å beholde token og laste opp senere. Vi ugyldiggjør alle ubrukte tokens etter 3 dager.

Løsning: Telefonen må laste ned nye offentlige nøkler fra et offentlig APPI hver gang man skal prate med serveren. Upraktisk.

Merk: Det er fremdeles mulig å korrelere identitet med smittenøkler dersom serveren logger IP-adresser og tidsstempler.

Kryptografi

Hash-funksjon SHA-256

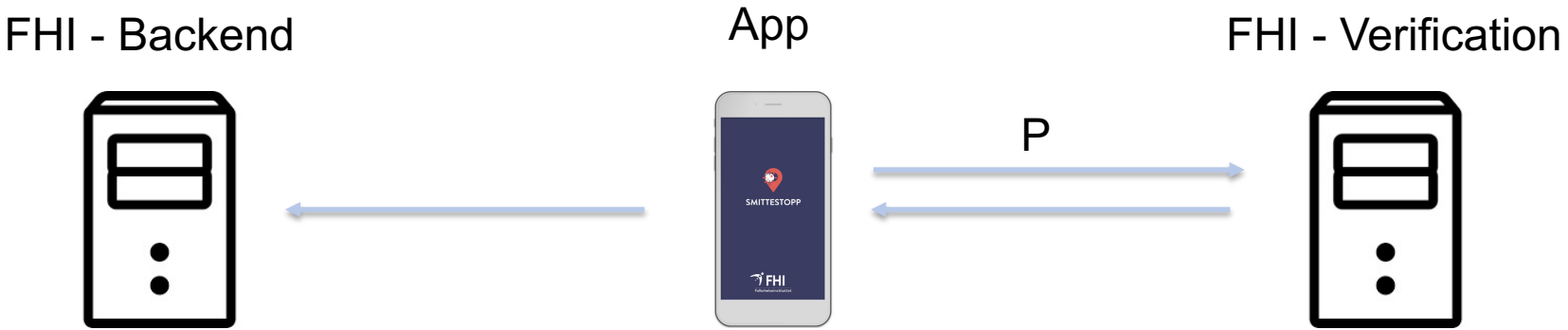
Hash funksjon H slik at:

- 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

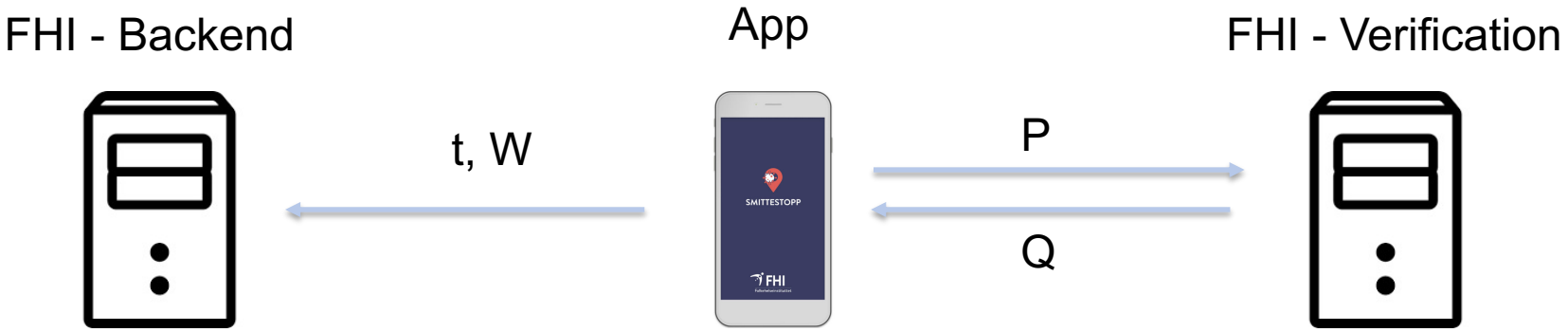
FHI - Backend

App

FHI - Verification

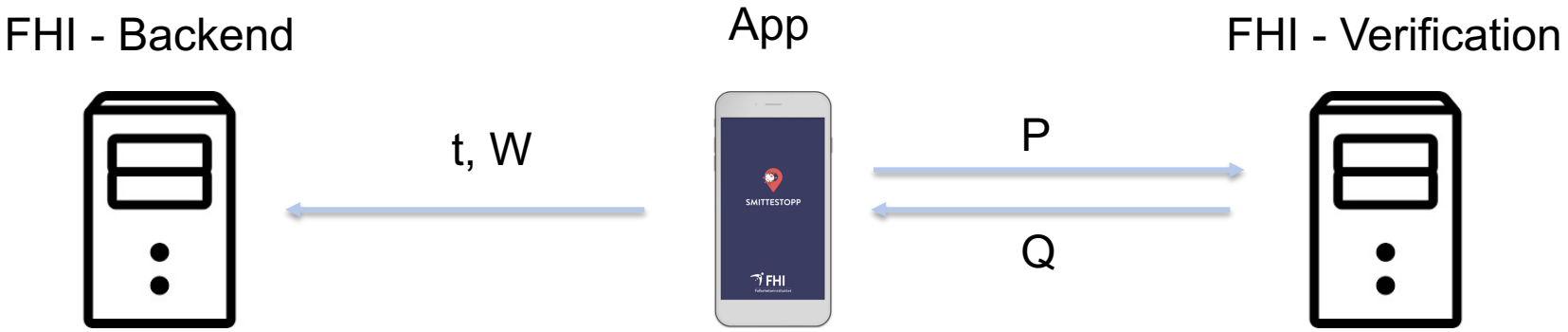
k ← attest-nøkkel
Q = k · P

Protokollen



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

Protokollen



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

Videre arbeid

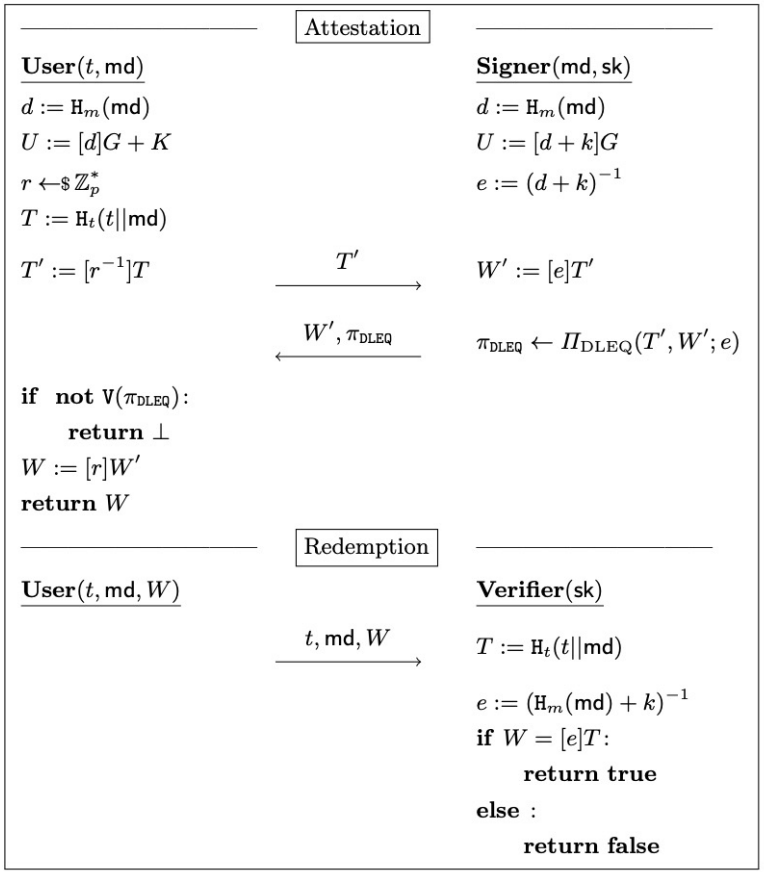
Ny anonym token protokoll med offentlig metadata og offentlig verifikasjon.

Basert på elliptiske kurver.

Revokering basert på metadata.

Ble implementert i sommer av studenter ved FFI på Kjeller.

Artikkelen er tilgjengelig: ia.cr/2021/203



Ressurser

Demo-implementasjon av anonyme tokens i Go:

github.com/tjesi/anonymous-tokens

```go
func main() {

	// Generate private key k,
	// and public key K.
	k, Kx, Ky := KeyGen()

	// Initiate communication.
	// Generate random numbers t and r,
	// and compute T = Hash(t) and P = [r]*T.
	t, r, Px, Py := Initiate()

	// Generate token Q = [k]*P, and create
	// proof (c,z) of correctness, given G and K.
	Qx, Qy, c, z := GenerateToken(Px, Py, Kx, Ky, k)

	// Randomise the token Q, by removing
	// the mask r: W = [(1/r)]*Q = [k]*P.
	// Also checks that proof (c,z) is correct.
	Wx, Wy := RandomiseToken(Px, Py, Qx, Qy, Kx, Ky, c, z, r)

	// Verify that the token (t,W) is correct.
	if VerifyToken(t, Wx, Wy, k) {
		fmt.Println("Token is valid.")
	} else {
		fmt.Println("Token is not valid.")
	}
```

Ressurser

- Alex Davidson - Privacy Pass: Bypassing Internet Challenges Anonymously (https://youtu.be/9DsUi-UF2pM)
- Nick Sullivan - Privacy Pass: A Lightweight Zero Knowledge Protocol Designed for the Web (https://youtu.be/HIqBJKnnHVk)
- Privacy Pass artikkel: https://www.petsymposium.org/2018/files/papers/issue3/popets-2018-0026.pdf
- Dokumentasjon av vår anonymous-tokens bibliotek: https://github.com/HenrikWM/anonymous-tokens/wiki
- Notat om anonym smittesporing: https://github.com/HenrikWM/anonymous-tokens/tree/main/docs
- Blog-post om tokens med offentlig metadata: https://world.hey.com/tjerand/anonymous-tokens-with-public-metadata-1253024d

Takk! Over til Henrik...

Slides: tjerandsilde.no/talks

Twitter: TjerandSilde