UiO : Universitetet i Oslo

Tillit i mobilapper som samler inn sensitive data

Software 2017

Dagfinn Bergsager, USIT

Tjenester for sensitive data

- Sikker forskningsplattform for UiO og andre offentlige forskningsinstitusjoner.
- Alle prosjekter får sin egen sikre server
- Lagt opp til analyse av data inne i TSD
- Mulig å få inn data fra åpne skjema på nett
- 282 aktive prosjekt 15.feb 2017
- http://www.uio.no/tjenester/it/forskning/sensitiv/

Datainnsamling til forskning

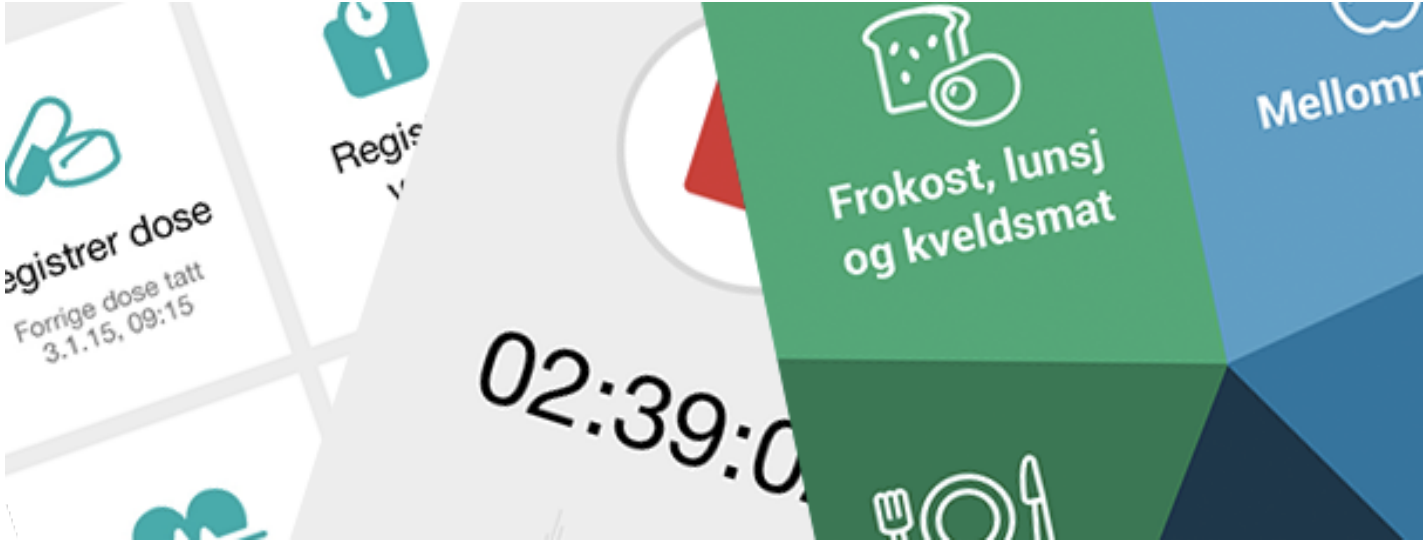
- Samles inn fra egenutviklet skjemaløsning: https://nettskjema.uio.no
- Data sendes asymmetrisk kryptert til prosjektetserver i TSD
- Kun forsker har tilgang til data (ikke driftsavdelingen)
- Løsningen sikkerhetsvurderes fortløpende og utvikles stadig

Dagens løsning: Høy tillit i sektoren

- Lang og stabil drift
- Ingen lekkasjer
- Klarer levere løsninger ingen andre har
- Tilgjengelighet
- Skalerbare standardløsninger med mange brukere

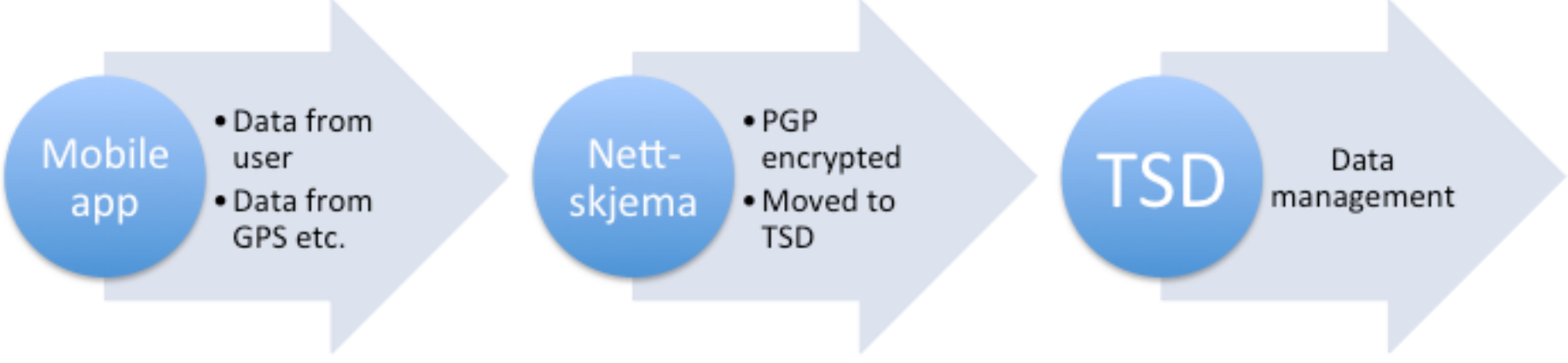
Mobilappene kommer!

- Forskere får bedre data
- Mulighet til å tidsstyre når respondent skal svare
- Flere funksjoner og tilpasninger for svaring



Teknisk design for datainnsamling

- Data leveres fortløpende fra telefonen



Nye utfordringer med mobilapper

- Mobilappen må lagre noe data
  - Når du leverte data sist
  - ID på hvem som har levert svaret
- At du har installert appen kan kobles til at du har en diagnose
- Dersom appen mister nett, kan det være behov for å legge data i kø
- Data på mobiler blir ofte sikkerhetskopiert til apple/google

Lagring av data i appen

- Risikovurdert for hver app hvilke data som kan lagres i appen
- Pinkode
- StudieID håndteres som passord (Keyring)
- Bilder og lyd legges kryptert i kø dersom nett mangler
  - Data i kø er ikke lesbare i appen

”Hemmelige” apper (Kliniske)

- Må ha gyldig studieID for å starte appen første gang
- Ikke mulig å lese ut av appen hva den gjør
- Nøytrale PopUp-meldinger
- Nøktern beskrivelse i AppStore og GooglePlay

”Hemmeligere” og mer kompliserte apper

- Vi kjøper inn iPads
- iPads styres med AirWatch
- Tømmes for data med gitte intervaller
- Setter pinkode og unngår backup til Apple
- Rutiner for iPads på avveie
- GPS-tracking
  - Eks.: iPads som forlater sykehuset tømmes for data og banditt blir bedt om å returnere den til UiO (ellers kommer vi og henter den)

Anonyme apper

- Vanskelig med digital anonymitet…
- Anonyme undersøkelser med sensitive data behandles på samme måte som ikke-anonyme prosjekter
- Forsker kan ikke koble svar og respondent (IP-adresse)
- Drift har ikke tilgang til svarene

Prioriteringer for all utvikling

1. Sikkerhet og personvern
2. Bruksopplevelse for den som skal levere data
3. Funksjonalitet for den som samler inn data

-Vi skal alltid være best på sikkerhet!

Åpenhet!

- Vi forteller om sikkerhetstiltak og arkitektur
- ROS-analyser sammen med involverte
  - Tar med sikkerhet og personvern
  - Gjenbruker eksisterende ROS (trenger kun 1 time)
- Kun åpen kildekode
- Åpne Jiraprosjekter og GIT-repo
- http://www.uio.no/tjenester/it/forskning/mobil-app/

Demo…