Ketju-hankkeen loppuraportti

Versio 1.1, 18.6.2020

Alustava jakelu

Sitra
Vaasan sairaanhoitopiiri
2M-IT Oy
Fraktal Oy
Futurice Oy
Reaktor Innovations Oy

1. Johdanto, taustaa ja hankkeen osapuolet

Laajat eristystoimet COVID-19-pandemian rauhoittamiseksi ovat kalliita ja raskaita sekä taloudellisesti että inhimillisesti. Viranomaisten tavoite on päästä purkamaan eristystä tavalla, joka estäisi viruksen liiallisen leviämisen, mutta sallisi yhteiskunnan mahdollisimman normaalin toiminnan.

Jäljitä testaa eristä hoida -malli on valittu Suomessa osaksi kansallista strategiaa viruksen torjunnassa. Tässä yhteydessä yritetään parantaa manuaalista jäljitysprosessia mm. teknologisin keinoin. Suomen itsenäisyyden juhlarahasto Sitra teki huhtikuun alussa rahoituspäätöksen, jonka avulla Vaasan sairaanhoitopiiri pilotoi puhelinlaitteiden keskinäistä läheisyyttä aistivaa mobiilisovellusta omalla henkilöstöllään toukokuun aikana. Puhelinten keskinäinen läheisyys havaitaan Bluetooth-teknologialla, ja sovellus perustuu ns. hajautettuun jäljitysmalliin. Pilotin tavoitteena oli testata Bluetooth-teknologian toimivuutta laitteiden keskinäisen etäisyyden mittaamisessa sekä sovelluksen toimivuudesta ja käytöstä arkielämässä.

Hankkeen alkuvaiheessa arvioitiin erilaisia maailmalla kehitettyjä ja kehityksessä olevia Bluetooth-protokollia sekä jäljitysmalleja. Monet teknologioista olivat uusia ja sekä teknologiat että lainsäädäntöön ja yksityisyydensuojaan liittyvät yksityiskohdat muuttuivat nopealla tahdilla hankkeen alkuvaiheessa. Osa Bluetooth-ratkaisuista ja jäljitysmalleista suljettiin arvioinnin jälkeen pois, koska ne eivät sopisi Suomen tai EU:n ympäristöön (mm. Singaporessa käytössä ollut keskitetty ratkaisu Bluetrace sekä Euroopassa kehitetty keskitetty ratkaisu PEPP-PT). Huhtikuussa pilottiin valittiin silloin lupaavimmaksi osoittautunut, Euroopassa kehitetty DP-3T-protokolla.

DP-3T on hajautettu, sovelluksen käyttäjien tietosuojaa ja -turvaa painottava malli, jossa sovelluksen käyttäjän on mahdollista pysyä halutessaan täysin anonyymina.

Pilotin käynnistäjänä, rahoittajana ja koordinoijana on toiminut Suomen itsenäisyyden juhlarahasto Sitra; lisäksi hankkeeseen osallistuivat Vaasan sairaanhoitopiiri sekä IT-alan yritykset 2M-IT, Fraktal, Futurice, Columbia Road ja Reaktor. Sovelluksen tietoturvaan ja -suojaan liittyen hankkeen aikana informoitiin tietosuojavaltuutettua sekä konsultoitiin Kyberturvallisuuskeskusta.

2. Hankkeen aikataulu

Hankkeen aikataulua ei pystytty lyömään lukkoon hankkeen alkuvaiheessa, koska teknisen toteutuksen aikataulu riippui merkittävästi eri Bluetooth-protokollien julkaisusta ja teknologioiden kehityksestä hankkeen aikana. Voidaan kuitenkin todeta, että hanke toteutettiin nopealla aikataululla ja hankkeen sisäisesti päätetty aikataulu pilotin toteutuksesta pääosin toukokuussa toteutui.

Päivämäärä	**Hankkeen vaihe**
24.3.2020	Esivalmistelu ja toteutusvaihtoehtojen vertailu toimittajien kesken aloitettiin
8.4.2020	Hankkeen aloitus, eri protokolla-vaihtoehtojen arviointi, tekninen toteutus
30.4.2020	Pilotin suunnittelun aloitus, tekninen toteutus
4.-15.5.2020	Pilottiin osallistuvien informointi ja tekninen testaus, pilotin tarkempi suunnittelu
18.5.2020	Pilottikäyttö alkoi
5.6.2020	Pilottikäyttö päättyi
15.6.2020	Hankkeen loppuraportti valmis

Taulukko 1: Hankkeen aikataulu

3. Tuotettu tekninen ratkaisu ja sen toiminnan pääperiaatteet

Sanasto

Hankkeessa toteutettu sovellus sisältää useita eri käsitteitä, jotka ovat spesifejä käytettyyn teknologiaan ja valittuun toimintaratkaisuun. Tässä sanastossa on kuvattu merkittävimmät käsitteet.

Kättely on yksittäinen hetkellinen havainto kahden toisiaan riittävän lähellä olevan laitteen välillä.

Kontakti tarkoittaa jäljityksen yhteydessä laitteen hetkellistä pidempää havaintoa toisesta laitteesta. Kontakti muodostuu riittävästä määrästä kättelyitä. Havainto voi olla yksipuolinen, ja sen on täytettävä etukäteen määritellyt kriteerit signaalinvoimakkuudelle sekä ajalliselle kestolle.

Altistuminen on kontakti, jonka katsotaan vahvuutensa (aika, välimatka) vuoksi johtavan riittävän todennäköisesti virusaltistukseen. Virusaltistuksen kriteerit ovat alun perin epidemiologisia, mutta ne on sovelluksessa määritelty teknisiksi kriteereiksi.

Anonymisointi tarkoittaa käyttäjän kuvaamista sinänsä merkityksettömällä, yleensä arvotulla merkkijonolla, jota ei voida liittää käyttäjän todelliseen identiteettiin ilman ulkopuolista tietoa. Tämä tieto voi olla implisiittisenä käyttäjän puhelimessa ja jaettuna ulkopuolisille vasta jälkikäteen (tai ei koskaan), tai tallennettuna ulkoiseen tietokantaan.

Tunniste tarkoittaa tässä kontekstissa yllä kuvatun mukaista anonymisoitua merkkijonoa, joita sovellukset vaihtavat ja joiden perusteella sovellukset voivat tunnistaa olleensa kohtaamisessa toisen sovelluksen kanssa, mikäli tunniste yhdistetään myöhemmin diagnosoituun covid-19 tapaukseen.

Keskitetty jäljitysmalli sisältää tietokannan, joka paljastaa tarvittaessa käyttäjien identiteetit heistä itsestään riippumatta.

Hajautettu jäljitysmalli ei sisällä käyttäjien identiteetit paljastavaa tietokantaa. Sairastumisen tai altistumisen yhteydessäkään käyttäjän identiteetti ei paljastu, vaan kohtaamistiedot toisten käyttäjien kanssa pysyvät anonyymeina.

Hybridi jäljitysmalli ei sisällä käyttäjien identiteetit etukäteen paljastavaa tietokantaa. Käyttäjä voi kuitenkin vapaaehtoisesti ilmoittautua havaitun altistumisen yhteydessä, jolloin jakamalla

hänet altistaneen kontaktin tunnisteen muodostuu altistumisketju. Jos käyttäjä ei altistumisen jälkeen ilmoittaudu, hän jää anonyymiksi.

Käytännössä ero keskitetyn ja hajautetun mallin välillä ei ole yksikäsitteinen. Näiden mallien väliin jääviä hybridiratkaisuja on useita mahdollisia.

Pilotissa käytetyn jäljitysprotokollan valinta

COVID-19-pandemian levitessä keväällä 2020 alettiin monissa maissa suunnitella ja kehittää mobiilisovelluksia ja niiden perustana olevia jäljitysprotokollia altistumisten havainnointiin. Ratkaisut hyödynsivät laitteiden välistä Bluetooth-yhteyttä sekä etenkin sen tarjoamaa mahdollisuutta kantaman sisällä olevien laitteiden etäisyyden arviointiin signaalin vaimeneman avulla. Uusien jäljitysprotokollien julkaisu lähes viikottain aiheutti huhtikuun aikana hankkeessa useita eri evaluointikierroksia ennen lopullisen protokollavalinnan tekemistä.

Singaporessa valtiollisesti kehitetty BlueTrace oli maaliskuun 2020 lopulla ensimmäisiä julkisuuteen tulleita jäljitysprotokollia, jonka lähdekoodi julkaistiin lopulta huhtikuun puolivälissä. BlueTrace vaikuttikin tuolloin käytännössä ainoana vaihtoehtona varsin valmiilta ja käyttökelpoiselta tekniseltä rungolta Ketju-sovelluksen pohjaksi, jonka mukaisesti Ketju-sovellusta alettiin suunnittelemaan. Keskitettynä protokollana se tarjosi mahdollisuuden myös tartuntaketjujen muodostamiseen terveydenhuollon viranomaiskäyttöä varten.

Huhtikuun alussa Keski-Euroopassa Saksan johdolla kehitetty PEPP-PT-jäljitysprotokolla tuli julkisuuteen nauttien heti laajaa yhteiseurooppalaista kiinnostusta sekä tarjoten vielä kehitysasteella olevan lähdekoodin halukkaiden käyttöön ennen BlueTrace-koodin julkistamista. PEPP-PT-protokollassa huomioitu keskinäinen yhteensopivuus eri maiden toteutusten välillä vaikutti arvokkaalta lisältä Euroopassa.

Pian tämän jälkeen kuitenkin Sveitsin johdolla PEPP-PT:n kehityksestä erkaantunut tutkijaryhmä julkaisi oman käyttäjien tietosuojaa ja anonymiteettiä painottavan hajautetun DP-3T jäljitysprotokollan, jollaista osa tutkijajoukosta oli jo PEPP-PT-protokollaksi ehdottanut. Kasvava huoli jäljityssovellusten yksityisyydensuojasta julkisessa keskustelussa sai katseet kääntymään DP-3T:n suuntaan myös Ketju-sovelluksen protokollan valinnassa. Lisäksi DP-3T:n hyvin avoin ja nopeasti etenevä kehitystyö nähtiin parannuksena BlueTracen ja PEPP-PT:n erittäin suljettuun kehitykseen nähden. Anonyymin hajautetun lähestymistavan kääntöpuolena oli kuitenkin varsin rajoitetut mahdollisuudet viranomaisten tekemän manuaalisen jäljitystyön tehokkaaseen avustamiseen.

Lopulta huhtikuun loppupuolella iso kansainvälinen tutkijajoukko ilmaisi avoimessa kirjeessä huolensa keskitettyjen jäljitysprotokollien palvelimille tallennetun käyttäjätiedon yksityisyydensuojasta ja väärinkäytön mahdollisuuksista. Viimeistään tämän seurauksena suurin osa PEPP-PT:n tukijoista siirtyi DP-3T-protokollan taakse.

Kaikkien eri Bluetooth-jäljitysprotokollatoteutusten haasteena oli kuitenkin etenkin iOS-käyttöjärjestelmän osalta varsin rajoittunut tai jopa estynyt toiminta jäljityssovelluksen ollessa tausta-ajossa. Ehkä osin tästä syystä Apple ja Google päätyivät kehittämään oman hajautetun Exposure Notification -protokollansa, joka otti hyvin paljon vaikutteita DP-3T protokollasta. Protokolla voitiin toteuttaa Applen ja Googlen toimesta käyttöjärjestelmätason palveluna ratkaisten edellä mainitut ongelmat tausta-ajossa sekä mahdollistaen myös kohtaamisdatan tallentamisen suojatummin. Vaikka protokolla julkaistiin jo huhtikuun puolivälissä, lupailtiin toteutusta saataville vasta toukokuussa, joka oli jo liian myöhään Ketjun pilottivaiheen ajoitusta varten. Näin pilotissa käyttöönotetuksi jäljitysprotokollaksi valikoitui DP-3T.

Tämän lisäksi Apple ja Google myöntävät oikeuden Exposure Notification -protokollan käyttöön erittäin tiukoin ehdoin, vaatien valtion terveydenhuoltoviranomaisten mandaatin ja yksinoikeuden valitulle jäljityssovellustoteutukselle kussakin maassa.

Tutkittujen jäljitysprotokollien keskeisimmät ominaisuudet:

BlueTrace

- Käyttöönotossa tallennetaan käyttäjän yhteystiedot keskitetylle palvelimelle.
- Vaihtuvat kohtaamistunnisteet haetaan palvelimelta.
- Kohtaamistiedot tallennetaan aluksi vain paikallisesti.
- Sairastumisen yhteydessä käyttäjä voi halutessaan jakaa kohtaamistietonsa terveysviranomaisille, jolloin voidaan muodostaa altistumisketju keskitetyn palvelimen tietojen avulla ja altistuneisiin henkilöihin voidaan olla yhteydessä.

PEPP-PT

- Vastaavat ominaisuudet kuin BlueTrace-protokollassa.
- Mahdollisuus yhteistoimintaan eri maiden sovellusten välillä.

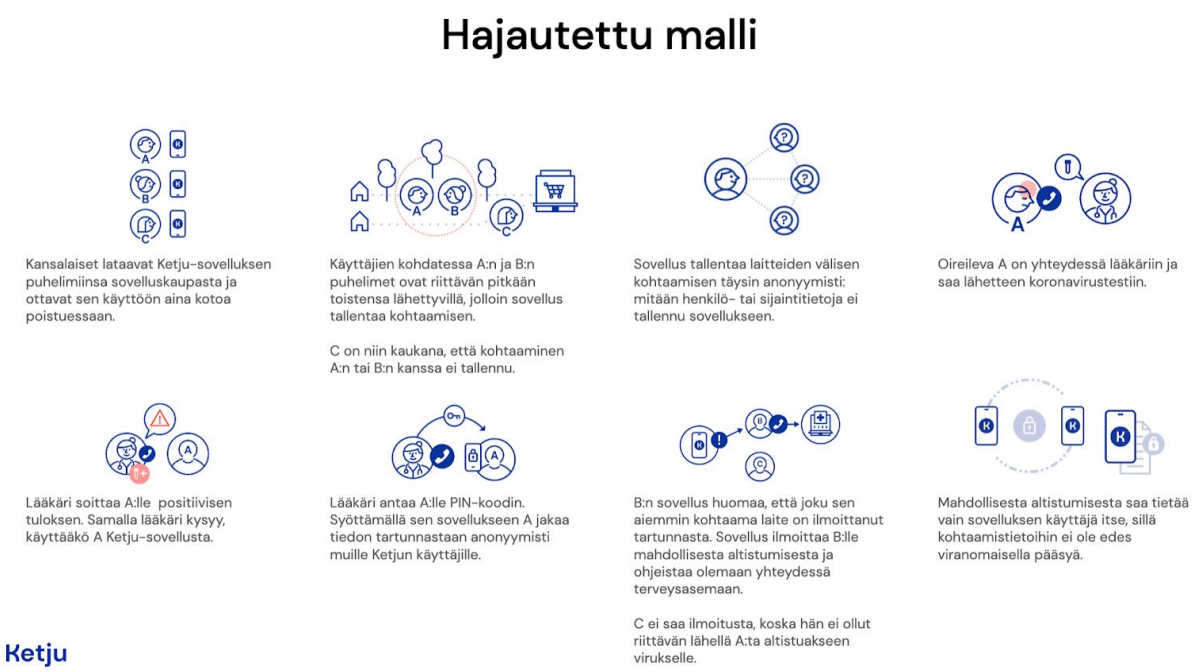
DP-3T

- Käyttöönotossa ei vaadita mitään henkilötietoja eikä edes minkäänlaista teknistä rekisteröitymistä taustajärjestelmään.
- Vaihtuvat kohtaamistunnisteet luodaan paikallisesti.
- Kohtaamistiedot tallennetaan vain paikallisesti.
- Sairastumisen yhteydessä käyttäjä voi halutessaan jakaa anonyymisti käyttämänsä kohtaamistunnisteet, joiden avulla toisten käyttäjien sovellukset voivat paikallisesti tunnistaa omasta kohtaamishistoriastaan mahdolliset kohtaamiset näiden tunnisteiden kanssa ja todeta näin altistumisen ja varoittaa siitä käyttäjää.

Apple ja Google Exposure Notification API

- Vastaavat ominaisuudet kuin DP-3T-protokollassa.
- Muihin protokolliin nähden oletettavasti parempi toimivuus tausta-ajossa etenkin iOS-käyttöjärjestelmällä.

Pilottiratkaisun toimintaperiaate



Kuva 1: Sovelluksen toiminta pääpiirteissään

Ketju-sovelluksen käyttämän DP-3T:n, kuten muidenkin tutkittujen jäljitysprotokollavaihtoehtojen, toiminta perustuu langattoman Bluetooth-yhteysteknologian käyttöön muiden lähietäisyydellä olevien samaa jäljityssovellusta käyttävien mobiililaitteiden havainnointiin.

Sovellukset lähettävät jatkuvasti omia 15 min välein vaihtuvia lyhytaikaistunnisteita, joita johdetaan paikallisesti tietyn kryptografisen määritelmän mukaisesti päivittäin vaihtuvista salaisista avaimista. Nämä salaiset avaimet taas johdetaan aina edellisen päivän avaimesta, alkaen käyttöönoton yhteydessä arvotusta ensimmäisestä satunnaisesta salaisesta avaimesta. Lyhytaikaistunnisteet vaikuttavat ulkopuolisesta satunnaisilta eivätkä ne paljasta käyttäjän identiteettiä. Ulkopuolinen taho ei myöskään pysty ennustamaan käyttäjän seuraavia tai edellisiä lyhytaikaistunnistetta nykyisen tunnisteen perusteella, estäen näin käyttäjän pidempiaikaisen seurannan Bluetooth-liikennettä havainnoimalla.

Laitteen Bluetooth-yhteyden kantaman alueella olevat toiset laitteet kuuntelevat ja tallentavat näitä lähetettyjä lyhytaikaistunnisteita sovelluksen sisäiseen tietokantaan kättelyiksi, sisältäen lisäksi ajanhetken sekä vastaanotetun signaalin voimakkuuden ja lähettävän laitteen

ilmoittaman lähetystehon. Jälkimmäisten erotuksena voidaan laskea signaalin vaimenema laitteiden välillä ja tästä taas saadaan arvio etäisyydestä.

Riittävästä määrästä yksittäisiä kättelyitä saman väliaikaistunnisteen kanssa voidaan koostaa kohtaamisia, joilla on tietty ajallinen kesto sekä keskimääräinen signaalinvoimakkuus, josta voidaan tehdä arvio kohtaamisen keskimääräisestä etäisyydestä kohtaamisen aikana.

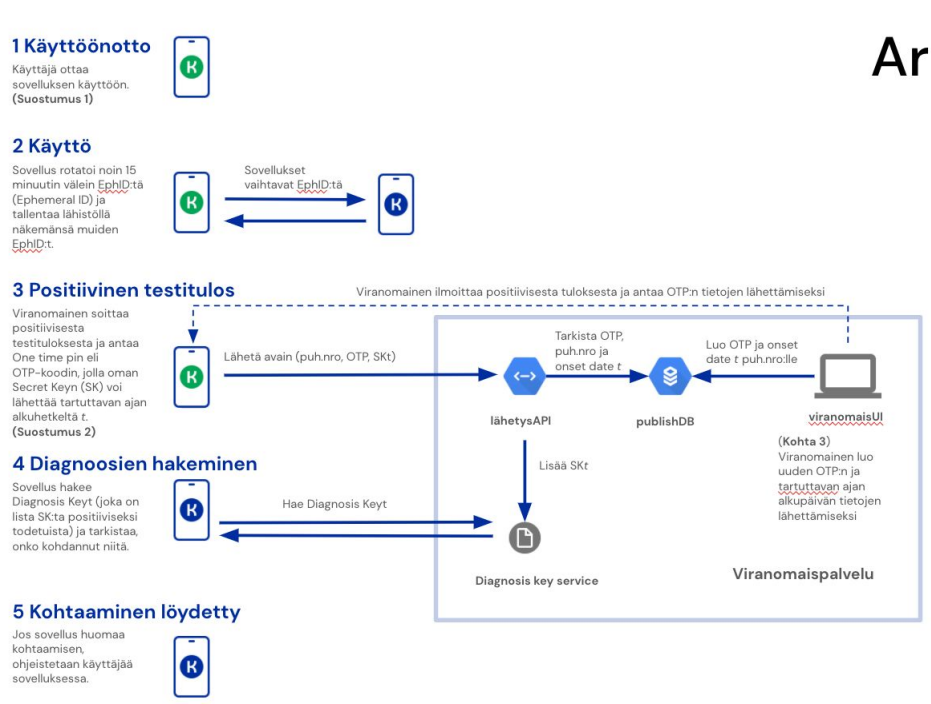
Käyttäjän sairastuessa ja saadessa positiivisen COVID-19-diagnoosin hän voi halutessaan jakaa tiedon sairastumisestaan muiden sovelluskäyttäjien kesken ja mahdollistaa näin hänen altistamiensa käyttäjien varoittamisen sovelluksen kautta. Teknisesti tieto sairastumisesta jaetaan julkaisemalla sovelluskäyttäjän oletetusta ensimmäisestä tartuttavuuspäivästä alkaen käyttämät salaiset avaimet, joista muut sovellukset voivat johtaa kaikki päivän väliaikaistunnisteet ja verrata niitä itse tallentamiinsa kohtaamisiin. Jos käytössä olevan altistumisen määritelmän mukaisen minimietäisyyden ehdot täyttäviä kohtaamisia löytyy päivän ajalta yhteensä vähintään altistumiseen vaadittavan minimikeston verran, voidaan todeta altistumisen tapahtuneen. Tässäkään tapauksessa altistaneen käyttäjän identiteetti ei paljastu eikä myöskään tieto altistumisesta paljastu kuin altistuneelle käyttäjälle itselleen.

Sekä positiivisen COVID-19-diagnoosin että ensimmäisen tartuttavuuspäivän määrittelee kuvatussa ratkaisussa terveydenhuollon viranomainen.

Tekniset tiedot ja arkkitehtuuri

Mobiilisovellukset on toteutettu nk. natiivisovelluksina käyttäen kullekin käyttöjärjestelmälle tyypillisiä teknologioita ja käytäntöjä. Ohjelmointikielinä käytettiin Swiftiä (iOS) ja Kotlinia (Android). Varsinainen jäljitystoiminnallisuus otettiin käyttöön valmiina avoimen lähdekoodin DP-3T-ohjelmistokirjastona, johon tehtiin testikäyttäjien identiteetin paljastavia muutoksia tallennettavaan kättely- ja kontaktidataan pilottitestausta varten, jotta kerättyä kohtaamisdataa voidaan verrata manuaalisiin havaintoihin teknisen toiminnan varmistamiseksi.

Taustajärjestelmä on toteutettu käyttäen moderneja teknologioita (TypeScript, Node.js, PostgreSQL) ja sen infrastruktuuri on sijoitettu Google Cloud Platformin Haminan datakeskukseen.



Kuva 2: Ratkaisun arkkitehtuuri pääpiirteissään.

4. Sovelluksen suunnittelun pääperiaatteet - käyttöliittymä ja visuaalinen ilme

Ketju-sovelluksen käyttöliittymän, ulkoasun ja käyttökokemuksen suunnittelutyötä ohjasivat sekä alalla hyväksi todetut käyttäjäkeskeisen suunnittelun periaatteet että projektissa erikseen määritellyt tavoitteet. Koska sovelluksen perusta on hyvin tekninen ja oletettava käyttäjäkunta on laaja ja sisältää eri tasoilla teknologiaa ymmärtäviä käyttäjäjoukkoja, suunnittelun pääperiaatteina pidettiin selkeyttä, saavutettavuutta, helppokäyttöisyyttä, luotettavuutta ja inhimillisyyttä. Tämä tarkoitti mm että:

- vakiintuneita toimintatapoja (konventioita) hyödynnettiin käyttöliittymällisiä toimintoja suunnitellessa
- tekstin luettavuus varmistettiin mm. huomioimalla riittävä tekstikoko ja kontrasti
- varmistettiin, että esimerkiksi näkövammaisten käyttäjien ruudunlukuohjelmat tai muu avustava teknologia pystyy tulkitsemaan sivun sisältöä oikein ja käyttäjä pystyy hyödyntämään sovelluksen toiminnallisuuksia
- suunnittelussa huomioitiin eri ruutukokoot, puhelinmallit sekä -käyttöjärjestelmät
- näkymien tuli olla rauhallisia, käyttöä ohjaavien tekstien napakoita ja ohjekuvien yksiselitteisiä
- yleisilmeen tuli olla visuaalisesti viimeistelty, tasapainoinen ja johdonmukainen. Esimerkiksi kaikki sovellukseen liittyvä viestintä ja ohjeistus tuli olla tunnistettavaa ja määritellyn brändin mukaista.
- vaikka kyseessä on yhteiskunnallisesti kriittinen, tärkeä ja virallinen sovellus, tulee sen suunnittelutyössä ja toteutuksessa huomioida tietty inhimillisyys ja lähestyttävyys

Kuva 3. Esimerkki visuaalisesta ilmeestä.

5. Tietoturva ja -suoja

Jo hankkeen alussa tiedettiin, että kohtaamisten jäljittämiseen tarkoitetut sovellukset voivat avata yksilön kannalta merkittäviä tietoturva- ja tietosuojariskejä, mikäli näitä riskejä ei hallita riittävästi sovellusten arkkitehtuureissa, toiminnoissa, ja teknologiavalinnoissa sekä varmistamalla sovelluksen laadukas toteutus. Ketju-hankkeen osapuolille oli hankkeen aikana keskeistä, että pilotoitava sovellus suunnitellaan yksilön kannalta turvalliseksi. Tietosuojavaltuutettu pidettiin informoituna sovelluksen toteutuksesta.

Sovelluksen tietoturvaa ja tietosuojaa ohjattiin sisäänrakennetun ja oletusarvoisen tietosuojan vaatimus huomioiden muodostamalla hankkeen alussa tietosuojaa ja tietoturvaa ohjaavat periaatteet. Tietoturvauhkiin varauduttiin tunnistamalla ja hallitsemalla uhkaskenaarioita osana jatkuvaa prosessia toteutuksen aikana.

Ohjaavat periaatteet

Ketju-järjestelmän tietoturva- ja tietosuoja-arkkitehtuuria ohjasivat seuraavat periaatteet.

Käyttäjien keskinäinen anonymiteetti

Sovellus ei saa sisältää tapaa, jolla käyttäjän identiteetti paljastuisi toiselle käyttäjälle. Ketju-mobiilisovellukset vaihtavat tilapäisiä tunnisteita. Mobiilisovellukset uusivat tunnisteet itse useita kertoja vuorokaudessa. DP-3T:n mukaisessa algoritmissa tilapäiset tunnisteet johdetaan matemaattisesti kunkin sovelluksen sisäisestä yksilöivästä tunnisteesta. Tämä tapahtuu tiivistealgoritmeilla, jotka eivät mahdollista sisäisen yksilöivän tunnisteen päättelemistä tilapäisen tunnisteen perusteella.

Kun sovelluksen käyttäjä saa viranomaisen vahvistaman koronavirusdiagnoosin, hän voi vapaaehtoisesti lähettää oman tunnisteensa taustajärjestelmään. Muiden käyttäjien sovellukset hakevat näitä tunnisteita säännöllisesti. Tällä tavoin sovellukset voivat ilmoittaa muille käyttäjille, jos he ovat tallentaneet tartunnan saaneen henkilön tunnisteen. Käyttäjien keskinäinen anonymiteetti ei vaarannu tässä mekanismissa, sillä henkilötietoja tai kohtaamisen tarkkaa ajankohtaa ei kerrota käyttäjille altistumisilmoituksen yhteydessä.

Käyttäjien anonymiteetti ylläpitäjille

Sovellus ei myöskään tarjoa järjestelmän omistajille tai ylläpitäjille tapaa kytkeä identiteettejä sellaisiin tunnisteisiin, joiden haltijat eivät ole ilmoittautuneet vapaaehtoisesti.

Ketju-mobiilisovellukset keräävät, käsittelevät, ja tallentavat tiedot itsenäisesti. Mobiilisovellukset eivät päivittäisessä käytössä lähetä mitään tietoa taustapalveluun.

Mobiilisovellukset ovat säännöllisesti yhteydessä taustajärjestelmään noutaakseen diagnoosin saaneiden käyttäjien yksilöivät tunnisteet. Vertailu näihin tunnisteisiin tapahtuu mobiilisovelluksen sisäisesti.

Tietojen käsittelyn minimointi

Sovellus käsittelee vain niitä tietoja, jotka ovat tarpeen käyttäjien keskinäisten kohtaamisten keston ja etäisyyden arvioimiseksi.

Kunkin sovelluksen keräämät kohtaamistiedot sijaitsevat vain tuossa kyseisessä sovelluksessa ja päätelaitteessa. Mobiilisovellus ei hyödynnä tai kerää sijaintitietoa esimerkiksi satelliittien (GPS) tai wifi-paikannuksen avulla. Poistettaessa sovellus mobiililaitteesta kyseisen sovelluksen tiedot tuhoutuvat eikä niitä ole mahdollista palauttaa mistään taustajärjestelmästä.

Kohtaamistietoja tallennetaan sovelluksessa ja päätelaitteessa vain ennalta määrätty aika (DP-3T toteutuksessa 3 viikkoa), jonka jälkeen sovellus tuhoaa niitä automaattisesti. Tällä varmistetaan se, ettei sovellukseen kerry mahdollisten tartuntaketjujen selvittämisen kannalta tarpeetonta historiaa kohtaamisista. Lisäksi pilottisovellukseen sisäänrakennettiin mekanismi, joka lopettaa sovelluksen toiminnan viimeistään 1.7.2020, mikäli pilottikäyttäjät eivät poista sovellusta pilotin päätyttyä.

Käyttäjää ei ole mahdollista harhauttaa paljastamaan mitään tietoja kohtaamisistaan, sillä sovellus ei tarjoa tapaa avata tai kopioida niitä.

Käyttäjä on yksilöity vain pseudonymisoidun tunnisteen avulla. Kuten yllä on kuvattu, käyttäjän identiteetti voidaan kytkeä tunnisteeseen vain käyttäjän itse niin halutessa.

Tunnistetut uhkaskenaariot

Järjestelmän suunnittelutyössä kiinnitettiin merkittävää huomiota erilaisten tietoturvaa ja tietosuojaa vaarantavien uhkien ja haavoittuvuuksien mahdollisuuteen. Oheinen luettelo kuvaa tiivistetysti uhkia, jotka hankkeen aikana tunnistettiin. Kukin uhka voisi toteutuessaan johtaa joko luottamuksellisen tiedon paljastumiseen, tiedon muuttumiseen, tai tiedon tai palvelun käytön estymiseen. Uhkia hallittiin monipuolisilla toimenpiteillä, kuten tietoturvaa tukevalla arkkitehtuurisuunnittelulla, teknologiavalinnoilla, sekä ohjelmointi- ja testauskäytännöillä.

Matkapuhelinsovellukseen kohdistuvat uhkat

Matkapuhelinsovellukseen tai päätelaitteeseen liittyen tunnistettiin seuraavia tietoturvauhkia.

- Luvattoman tahon pääsy sovellukseen, kun päätelaite ei ole lukittu.
- Luvattoman tahon pääsy sovelluksen tarvitsemiin toimintoihin, kuten mahdollisuus kytkeä Bluetooth pois toiminnasta.
- Sovelluksen takaisinmallinnus ja toiminnan muuttaminen, kuten verkkotoimintojen muutokset, tai tunnisteiden väärentäminen tai kopioiminen päätelaitteista toisiin.
- Sovelluksen sisäisten tietojen vuotaminen.
- Sovelluksen muodostamien käyttölokien ja analytiikan luottamuksellisuus.
- Käyttäjän harhauttaminen tietojen luovuttamiseksi tai muuttamiseksi.

Viestintään kohdistuvat uhkat

Matkapuhelinsovelluksen ja taustajärjestelmän väliseen viestintään, sekä matkapuhelinsovellusten väliseen viestintään voi kohdistua seuraavia tietoturvauhkia.

- Mobiilisovelluksen ja taustajärjestelmän välisen tietoliikenteen salakuuntelu ja muuttaminen.
- Mobiilisovellusten BT-viestinnän salakuuntelu, muuttaminen, toistaminen ja välittäminen.
- Mobiilisovellusten sijainnin ja liikkeiden ristipaikannus BT-viestinnän perusteella.

Taustajärjestelmän rajapintoihin kohdistuvat uhkat

Taustajärjestelmän rajapintoja koskien tunnistettiin seuraavia tietoturvauhkia:

- Yritys korruptoida järjestelmän tietosisältöä.
- Järjestelmän tarkoituksellinen kuormittaminen (palvelunesto).
- Henkilöitä koskevien tietojen paljastuminen, kuten henkilötiedot, saatu diagnoosi, diagnoosin ajankohta, tai altistuneet henkilöt.

Terveydenhuollon käyttöliittymään kohdistuvat uhkat

Terveydenhuollon käyttöliittymää koskien tunnistettiin seuraavia tietoturvauhkia.

- Luvaton pääsy käyttöliittymään ja sen esittämiin tietoihin.
- Henkilötietojen tarpeeton katselu.
- Tietosisällön luvattomat muutokset.

Sovelluskehitykseen ja sovellusjakeluun kohdistuvat uhkat

Sovelluskehitykseen käytetyn välineistön tai sovellusjakelun tietoturvapuutteista voi aiheutua seuraavia tietoturvauhkia.

- Riippuvuudet 3. osapuolen sovelluskomponenteista.
- Lähdekoodin luvattomat muutokset.
- Käännettyjen komponenttien muutokset.

- Valesovelluksen jakelu.

Taustajärjestelmän hallintaan kohdistuvat hyökkäykset

Ketju-sovelluksen taustajärjestelmät toteutettiin pilotissa Google Cloud Platform -julkipilvipalveluilla Haminan datakeskuksessa. Palveluiden hallintakerrokseen liittyen tunnistettiin seuraavia tietoturvauhkia.

- Luvaton pääsy resursseihin kuten tietokantaan.
- Pilviresurssien luvattomat muutokset kuten resurssien ja tietojen tuhoaminen.

Vertailu viranomaisten suosituksiin

Euroopan komissio ja Euroopan tietosuojaneuvosto ovat julkaisseet keväällä 2020 omia suosituksiaan COVID-19-pandemian torjuntaa tukeville sovelluksille.

Hankkeessa arvioitiin Euroopan komission ja tietosuojaneuvoston julkaisemat suositukset sekä soveltuvan lainsäädännön (kuten EU:n yleinen tietosuoja-asetus ja suomen kansallinen lainsäädäntö) asettamat vaatimukset sovellukselle. Hankkeessa tehdyn arvioinnin perusteella Ketju-sovelluksessa toteutettu arkkitehtuuri, toiminnot, ja tietojenkäsittelyn periaatteet ovat soveltuvan lainsäädännön sekä viranomaisten antamien suositusten mukaiset. Kansallinen sovellus voidaan valituista toimintaperiaatteesta riippuen toteuttaa niin, että se täyttää soveltuvan lainsäädännön vaatimukset ja siihen mahdollisesti tehtävät päivitykset.

Tietosuojaa koskevien oikeuksien toteutuminen

EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) takaa rekisteröidyille henkilöille tietyt tietosuojaa koskevat oikeudet. Hankkeessa tehdyn arvioinnin perusteella Ketju-sovellus mahdollistaa näiden oikeuksien toteutumisen. Käyttäjä voi myös itse hallita tietojaan esim. poistamalla sovelluksen mobiililaitteestaan, jolloin kyseisen sovelluksen tiedot tuhoutuvat eikä niitä ole mahdollista palauttaa mistään taustajärjestelmästä.

6. Viestintä

Selkeä, innostava ja luottamusta herättävä viestintä on avainasemassa tartuntaketjuja jäljittävän sovelluksen levityksessä ja käyttäjähankinnassa. Ketju-sovelluksen pilotin viestinnällä oli kaksi tärkeää kohderyhmää: pilottiin osallistuvat sovelluksen käyttäjät sekä laajemmin Suomen kansalaiset, jotka kuulivat hankkeesta median kautta. Tavoitteena oli kertoa, miksi tartuntaketjujen digitaalinen tunnistaminen on tärkeää sekä vakuuttaa kohderyhmä siitä, että sovellus täyttää tiukat turvallisuus- ja yksityisyysvaatimukset.

Vuorovaikutuksessa sovelluskäyttäjien ja median kanssa korostuivat kansalaisten huolet koronasovellusten yksityisyydensuojasta ja tietoturvasta. Esiin nousi erityisesti muutama keskeinen kysymys, joihin viestinnässä vastattiin toistuvasti eri kanavissa:

- Näkevätkö sovelluskäyttäjät oman tai toistensa kohtaamishistorian?
- Tarkkaileeko tai tallentaako sovellus käyttäjän sijaintia?
- Mitä tietoja sovelluskäyttäjistä näkyy viranomaisille?
- Kuluttaako sovellus erityisen paljon puhelimen akkua?
- Kuinka paljon käyttäjiä tarvitaan, että sovelluksesta on hyötyä epidemian hillitsemisessä?

Usein kysyttyihin kysymyksiin vastattiin sekä pilottikäyttäjille suunnatussa sisäisessä viestinnässä, mediassa että ketjusovellus.fi-verkkosivustolla.

Sovelluskäyttäjille suunnatussa viestinnässä ilmeni erityinen haaste Bluetoothiin ja sijaintitietoihin liittyen. Ketju-sovellus ei tarkkaile eikä tallenna käyttäjän sijaintitietoja, mutta Android-käyttöjärjestelmässä Bluetoothin käyttäminen vaatii sijaintitietojen yleisen sallimisen, eikä sovellustasolla ollut mahdollista pyytää lupaa spesifimmin. Oikeuksia tietoihin piti selventää käyttäjille suunnatuissa materiaaleissa. Viestinnässä on tärkeää huomioida, että viestit ovat linjakkaita sekä sovelluksessa, markkinointimateriaaleissa että mediassa. Tätä silmällä pitäen oli tärkeää seurata tarkkaan mitä mediassa kirjoitettiin aiheen tiimoilta ja pyrkiä vaikuttamaan siihen, että medialla on saatavilla ajantasaisin tieto mahdollisimman kattavasti — vaikka aihealue on riippuvuuksineen erittäin laaja. Sovelluksen lähettämät notifikaatiot ovat nekin osa viestintää, ja ilmoituksista syntyvät mielikuvat oleellisia.

Koska pilotin osallistujat oli sovittu etukäteen, varsinaisesta käyttäjähankinnasta (user acquisition) ei hankkeessa saatu kokemusta.

7. Pilotti - kuvaus, havainnot ja tulokset

Pilotin järjestelyt

Pilottiin osallistui 33 vapaaehtoista käyttäjää Vaasan Keskussairaalan päivystyspoliklinikalta sekä Vaasan Sairaanhoitopiirin johtaja. Osallistujat työskentelivät pääosin normaalin rutiinin mukaan kolmessa vuorossa samoissa tiloissa maanantai 18.5.2020 – perjantai 5.6.2020 välillä. Käyttäjien käytössä oli useita erilaisia iPhone- ja Android-laitteita eri käyttöjärjestelmäversioilla.

Neljä osallistujaa teki lisäksi manuaalista kirjanpitoa työvuoron aikana tapahtuneista kohtaamisista. Pilotin aikana näiden neljän käyttäjän simuloitiin “sairastuneen”, jolloin voitiin seurata, milloin tieto altistumisesta päätyi muille pilottikäyttäjille sovellusten kautta, ja miten sovellukset ilmoittivat altistumisesta. Sairastumiseen johtava kohtaaminen pilotissa eli altistumisraja oli asetettu vähintään 15 minuuttiin alle 4,5 metrin etäisyydellä päivässä.

Pilottisovellus pohjautui hajautettuun malliin ja DP-3T-protokollaan, joka käyttää kohtaamisten havaitsemiseen Bluetoothia ja tallentaa kohtaamiset hajautetusti ja anonyymisti vain käyttäjien omille laitteille. Tästä johtuen pilottikäyttäjät lähettivät kertyneet tiedot säännöllisesti kehitystiimille omista sovelluksistaan.

Tulosten analysoinnin helpottamiseksi pilottisovelluksen DP-3T-toteutus oli debug-tilassa, jossa jokaisesta kohdatusta laitteesta tallennettiin samana pysyvä, laitekohtainen tunniste. Tämän ansiosta pilotin datasta oli mahdollista nähdä kaikki käyttäjien väliset kohtaamiset, jolloin voitiin verrata laitteiden havaintoja toisiinsa sekä käsin kirjattuihin kohtaamisiin. Tuotantotilaisesta DP-3T-toteutuksesta olisi saatu tieto vain altistumiseen johtaneista kohtaamisista, ja niistäkin vain päivän tarkkuudella.

Pilotissa käytössä olleet laitevariaatiot

iPhone (18 kpl)

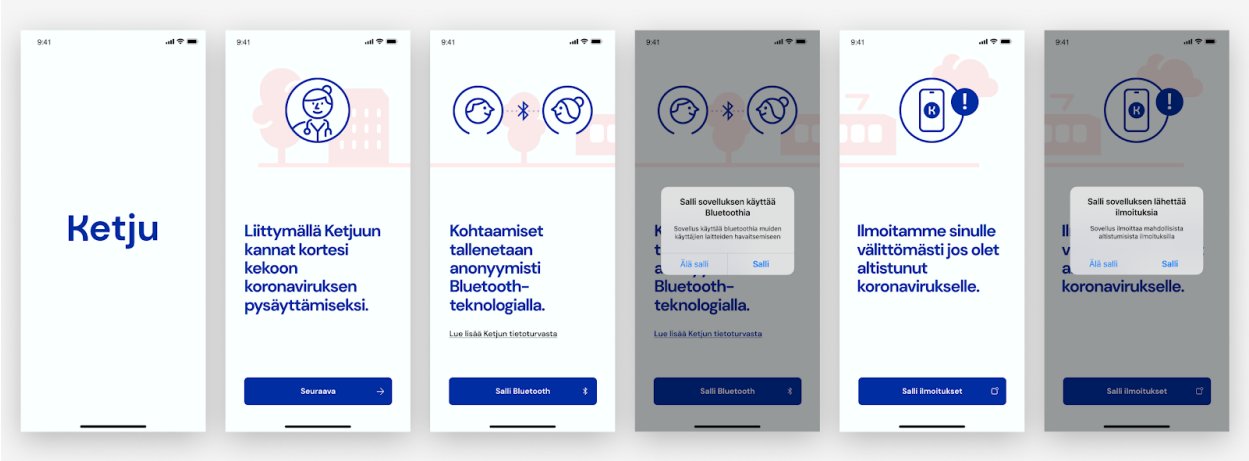
- mallit 6, 6s, 7, 7plus, 8, XS, XR, 11
- käyttöjärjestelmätasot 12.4.5, 12.13, 13.3.1, 13.4, 13.4.1

Android (17 kpl)

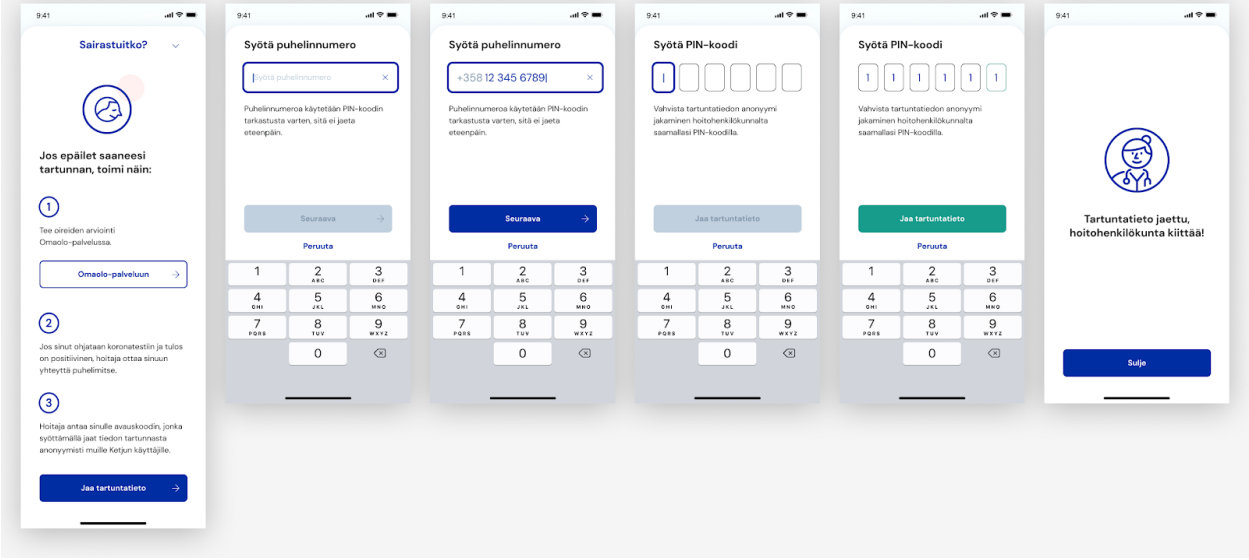
- mallit Samsung Galaxy A50 / J5 / S8+ / S10e, Nokia 8, OnePlus 5 / 6T, Huawei P30 lite, Huawei Nova 3
- käyttöjärjestelmät Android 6, 8.0, 9, 10, OxygenOS 9.0.11

Pilottisovellus

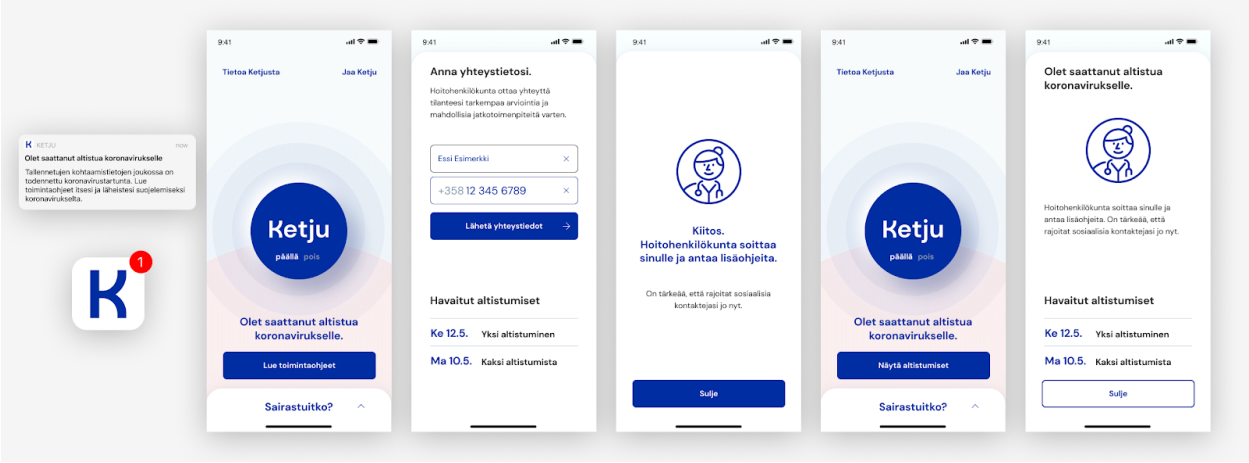
Kuvista 4-6 ilmenee pilotissa käytetyn mobiilisovelluksen toimintalogiikka pääpiirteissään.



Kuva 4. Kun sovellus avataan ensimmäisen kerran, käyttäjä ohjataan antamaan lupa bluetoothin ja ilmoitusten käyttöön.



Kuva 5. Tieto positiivisesta koronatuloksesta jaetaan muille sovelluksen käyttäjille anonyymisti kohdasta "Sairastuitko?". Pilotin tukitiimi toimitti “sairastuneille” PIN-koodin, jonka tavallisesti saisi hoitohenkilökunnalta positiivisen testituloksen yhteydessä. Puhelinnumeroa käytetään vain PIN-koodin tarkastukseen; sitä ei jaeta tai tallenneta.



Kuva 6. Mahdollisesta altistumisesta ilmoitetaan käyttöjärjestelmän ilmoituksella sekä viestillä sovelluksen sisällä. Käyttäjä ohjataan antamaan yhteystiedot, jotta hoitohenkilökunta voi arvioida tilanteen.

Havaintoja ja tuloksia

Pilotista tulosten yleistämisessä kannattaa ottaa huomioon pilotin pieni koko, testausympäristön erityislaatu ja etenkin valitut teknologiat ja jäljitysmalli. Pilotin ajoituksesta johtuen pilottisovellus ei käyttänyt myöhemmin kehitettyä DP-3T:n versiota, joka hyödyntää Googlen ja Applen omaa APIa. Niinpä tulokset koskevat ainoastaan DP-3T:n oman Bluetooth-toteutuksen päälle rakennettua hajautetun jäljitysmallin sovellusta.

Kertyneet mittaukset:

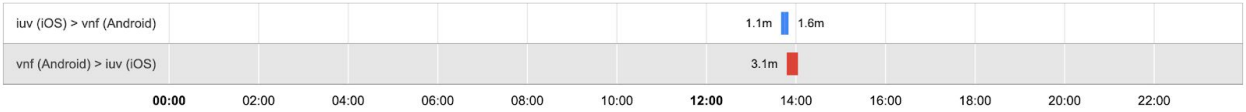
- Sovellus toimi käytössä ja kaikkien osallistujien sovelluksiin kertyi hyvin dataa.
- Pilottiin osallistui 33 henkilöä Vaasan Keskussairaalan päivystyspoliklinikalta sekä VSHP:n johtaja.
    - Kahdella käyttäjistä oli mukanaan kaksi eri laitetta (iOS, Android) koko pilotin ajan. (Kaksoislaitteet on tarpeellisin osin poistettu analyyseista.)
    - Päivystyspolin kahvihuoneessa oli lisäksi toimivuuden testaamista varten ylimääräinen puhelin, jossa sovellus oli jatkuvasti päällä.
    - Lisäksi yksi hankkeen kehitystiimin jäsen vieraili Vaasassa kahden eri puhelimen (iOS, Android) kanssa, joihin kertyi myös tietoa kohtaamisista vierailun aikana.
- Pilotin osallistujat lähettivät kehitystiimille 240 datalähetystä.
- Pilotin aikana kertyi yhteensä yli 6200 kontaktia laitteista.
    - Kahta puhelinta kantaneiden henkilöiden puhelinten välisiä kontakteja oli noin 1400.
    - Kahvihuoneessa olleen puhelimen kanssa oli noin 850 kontaktia.
    - Pilottikäyttäjien välisiä kontakteja oli noin 4000.

- Neljä käyttäjää piti lisäksi käsin kirjaa kaikista kohtaamisista, jotka olivat käyttäjän arvion mukaan vähintään 10 min alle 5 metrin etäisyydellä, joita myöhemmin verrattiin sovellusten kirjaamiin kohtaamisiin.
    - Käsin kirjattuja kohtaamisia oli noin 250.

Tuloksia

- Kuvista 7–12 saa intuitiivisen käsityksen kohtaamisdatan luonteesta.
- Puhelinten havainnot toisistaan olivat kirjavia:
    - Puhelinparien havainnot toisistaan voivat sosiaalisessa kohtaamisessa jäädä yksisuuntaisiksi. Yksisuuntaisten havaintojen suhteellinen osuus on hyvä mittari kohtaamisten rekisteröinnin epätarkkuudesta, mutta se riippuu kontaktin ajallisesta rajauksesta. Myös iOS-laitteiden vähyys pilotissa ja iOS-tausta-ajon toimimattomuus sekoittaa kokonaiskuvaa. Tiukimmalla viiden minuuten aikakriteerillä Android-puhelinten havaitsemista kohtaamisista yksisuuntaisiksi jäi n. 37%; loput 63% oli onnistuneesti havaittu molemmin puolin. Molemminpuolisten osuus kipuaa n. 70–75%:iin löysennettäessä kohtaamisen ajallista asynkroniaa järkevälle 0.5–1 tunnin tasolle. iOS-puhelinten keskinäiset kohtaamiset rekisteröityvät ehkä ainakin yhtä hyvin, mutta tapahtumia on liian vähän varmoihin johtopäätöksiin (kuva 14).
    - Käyttöjärjestelmien välisten kohtaamisten rekisteröintiä haittasi luultavasti iOS-tausta-ajon puute pilottisovelluksessa, joten niitä kertyi vähemmän kuin esimerkiksi Android-Android kohtaamisia (kuva 14).
    - Laitekohtaiset tulkintaerot signaalinvoimakkuuteen perustuvista kohtaamisetäisyyksistä olivat joskus suuria, esimerkiksi 1 metri vs. 4 metriä (kuva 15). Näiden huomioiminen laitekohtaisilla kalibraatioilla olisi erittäin työlästä laitekirjon laajuuden vuoksi. Saman puhelinmallin puhelimissakin voi olla erilaisia valmistuseräkohtaisia komponentteja ja asetuksia.
- Ns. väärät positiiviset kohtaamiset esimerkiksi seinien läpi eivät nousseet merkittäväksi ongelmaksi pilotin aikana. Voidaan kuitenkin todeta, että tämän kaltaisen järjestelmän kehityksessä tehdään aina kompromissi ylimääräisten haamukohtaamisten (väärät positiiviset) ja huomaamatta jääneiden kohtaamisten (väärät negatiiviset) välillä: vähentämällä toisia lisätään toisia. Tasapainoilu näiden kahden välillä tehdään kohtaamis-kriteeristön raja-arvoilla, jotka täytyy päättää kehittämisen aikana.
- Akun kulutuksen lisääntyminen ei tuntunut olevan ongelma testikäyttäjillä.
- Bluetooth-yhteyksissä muihin laitteisiin (urheilukellot, auton radio) esiintyi jonkin verran ongelmia sovelluksen ollessa päällä.
- Sovellus ei aina lähettänyt ilmoitusta altistumisesta sen ollessa tausta-ajossa.
- Käyttäjät eivät välttämättä huomanneet sovelluksen lähettämää altistumisilmoitusta.
- Pilottisovellus ei kerännyt kontakteja, jos käyttäjä ei ollut antanut oikeuksia käyttää sijaintiaan Android-puhelimessa. Toiset laitteet näkivät tällaisen laitteet normaalisti.

- Muistiinpanojen tekeminen kohtaamisista käsin riittävän tarkalla tasolla osoittautui vaikeaksi käyttäjille: mihin aikaan kohtaaminen tapahtui, kestikö se riittävän kauan ja keitä oli paikalla.



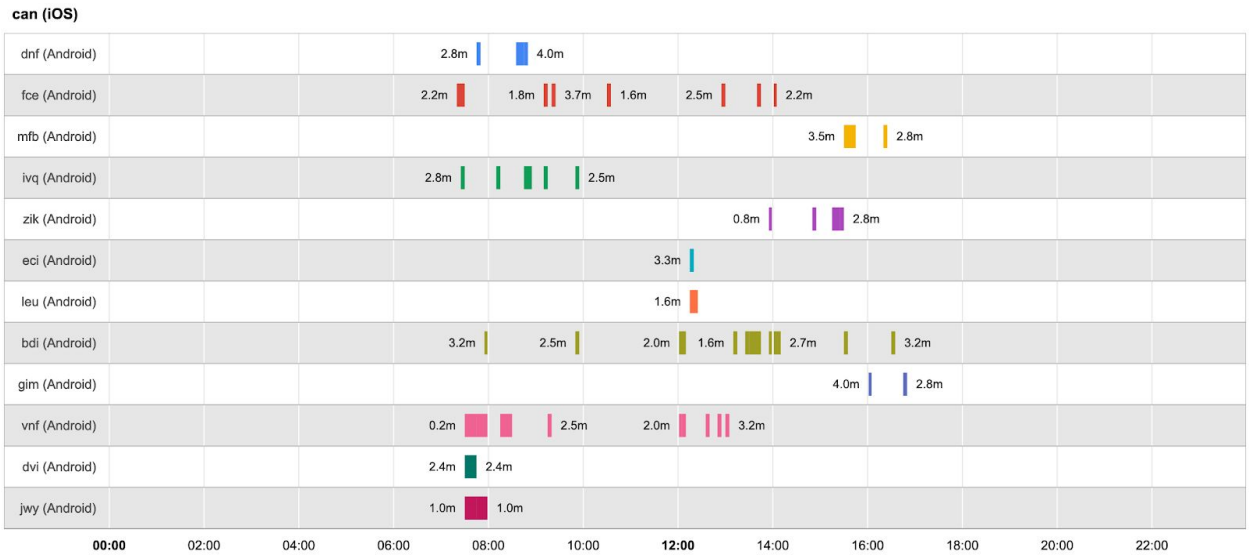
Kuva 7. Molemminpuolinen kontaktihavainto, pieni ajallinen asynkronia (vrt. kuva 14).

Kuva 8. Parittomia ja molemminpuolisia kontakteja.

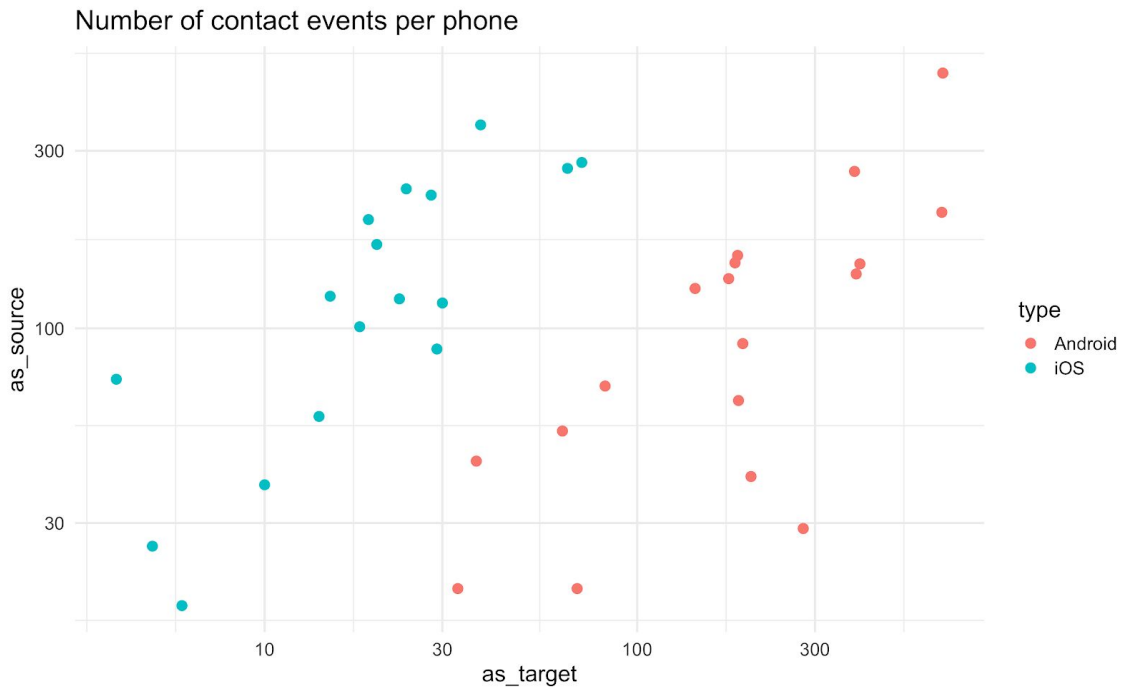
Kuva 9. Android-laite näkee iOS-laitteen harvemmin kuin iOS näkee Androidin (ks. myös kuva 13). Tämä liittynee iOS-sovelluksen tausta-ajon puuttumiseen pilottisovelluksesta.

Kuva 10. Parittomia iOS-kohtaamisia on runsaasti: iOS on nähnyt Androidin, muttei päinvastoin (toinen aikajana puuttuu, koska se olisi tyhjä).

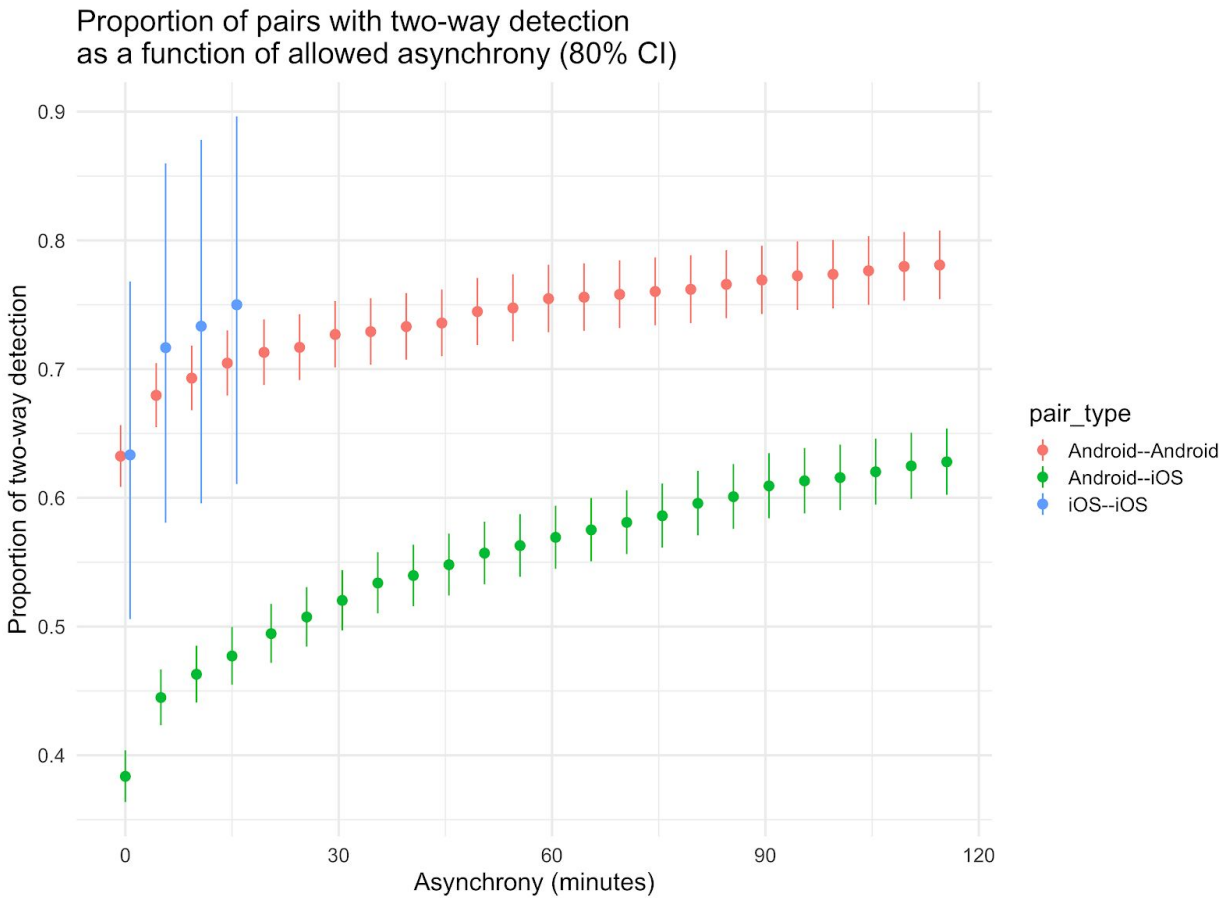
Kuva 11. Todennäköinen väärä positiivinen (keskimmäinen rivi).



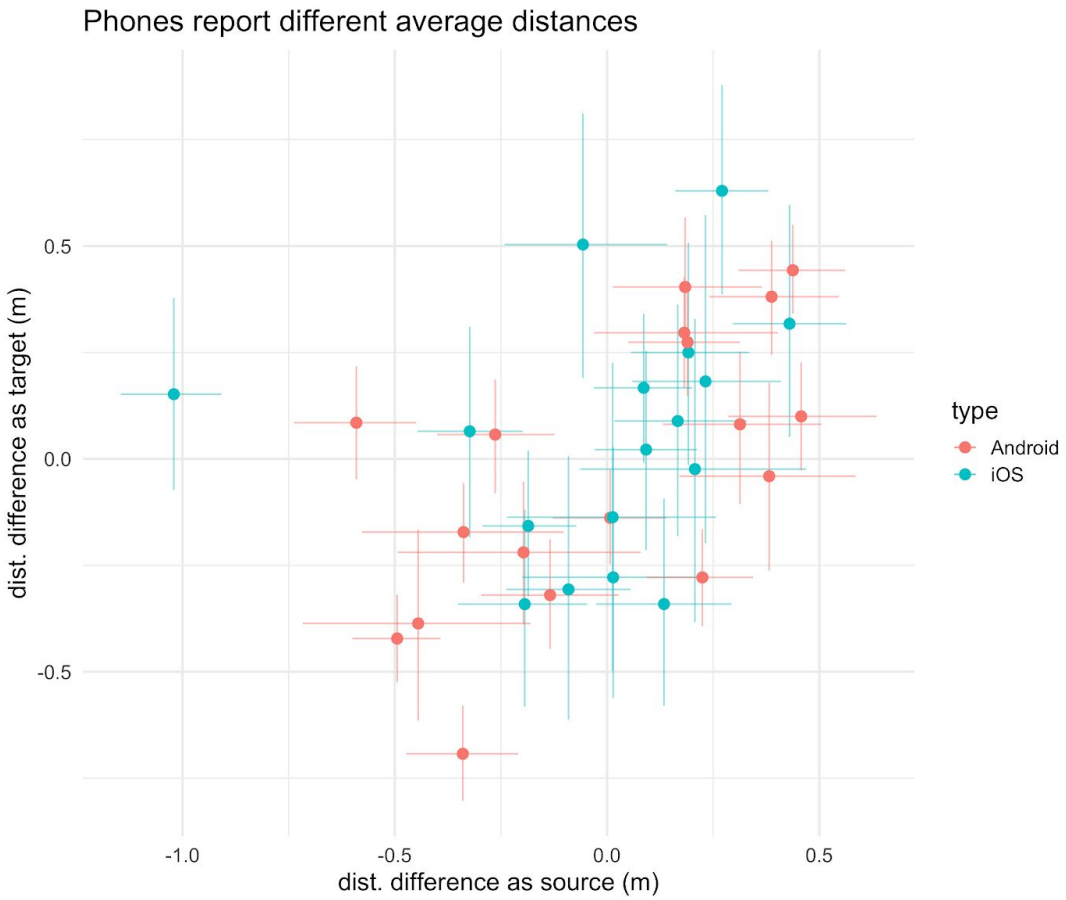
Kuva 12. Yksittäisen käyttäjän kohtaamisia vuoron aikana



Kuva 13. Yksittäisten puhelinten rekisteröimät kontaktitapausten määrät vaihtelivat huomattavasti (akselit ovat logaritmisia). Tämä kontaktimäärien vino jakauma kuvannee osin antennien herkkyyseroja ja muita teknisiä yksityiskohtia, mutta lienee pääosin ihmisten tyypillistä käyttäytymistä. iOS nähtiin kohteena harvemmin koska iOS-tausta-ajo ei toiminut (x-akseli). (iOS-sovellus kyllä näki päällä ollessaan yhtä hyvin kaikenlaiset laitteet, y-akseli.)



Kuva 14. Kontaktissa molempien puhelinten pitäisi havaita tilanne symmetrisesti. Havaintojen epäsymmetriaa voidaan pitää epätarkkuuden indikaattorina (esim. kuva 8). Toisaalta ihmisten liikkuessa vapaasti ei kontakti ole ajallisesti selkeästi määritelty tapahtuma (vrt. kuva 7). Kuvassa kaksisuuntaisten havaintojen osuus kaikista pariin liittyvistä havainnoista, x-akselilla sallittu aikaero havaintojen välillä. Aivan samanhetkisesti (mittausgranulariteetti 5 min) n. 63% Android–Android-pareista havaitsee toisensa kumpaankin suuntaan, loput n. 37% havainnoista jää yksisuuntaiseksi. Kaksisuuntaisten havaintojen osuus nousee jos kaksisuuntaisuudelle sallitaan ajallista epätarkkuutta. iOS–iOS-pareja on liian vähän, jotta niistä voisi sanoa mitään varmaa. Käyttöjärjestelmien sekaparit tunnistavat toisensa Android–Android-pareja selvästi huonommin. Luottamusvälit on laskettu tapausmääristä; käyttäjätason klusteroitumisen takia todellinen epävarmuus tuloksissa on suurempaa.



Kuva 15. Puhelimien raportoimat etäisyydet toisiinsa eivät olleet keskimäärin samoja, mutta käyttöjärjestelmien välillä ei ollut eroa. Osin erot johtuvat puhelinten teknisistä ominaisuuksista ja tavoista kantaa ja säilyttää puhelinta (tasku, käsilaukku, käsi, pöytä), mutta ne voivat osin johtua myös käyttäjiensä tavoista ylläpitää fyysistä etäisyyttä sosiaalisissa kontakteissa. (Luottamusvälit 80% on laskettu hierarkisesta regressiomallista, viime kädessä tapausmääristä ja puhelinten samankaltaisuudesta.) Ilman mittausvirheitä puhelin näkyisi kohteena ja lähteenä yhtä hyvin, jolloin pisteet kuvassa olisivat nousevalla diagonaalilla.

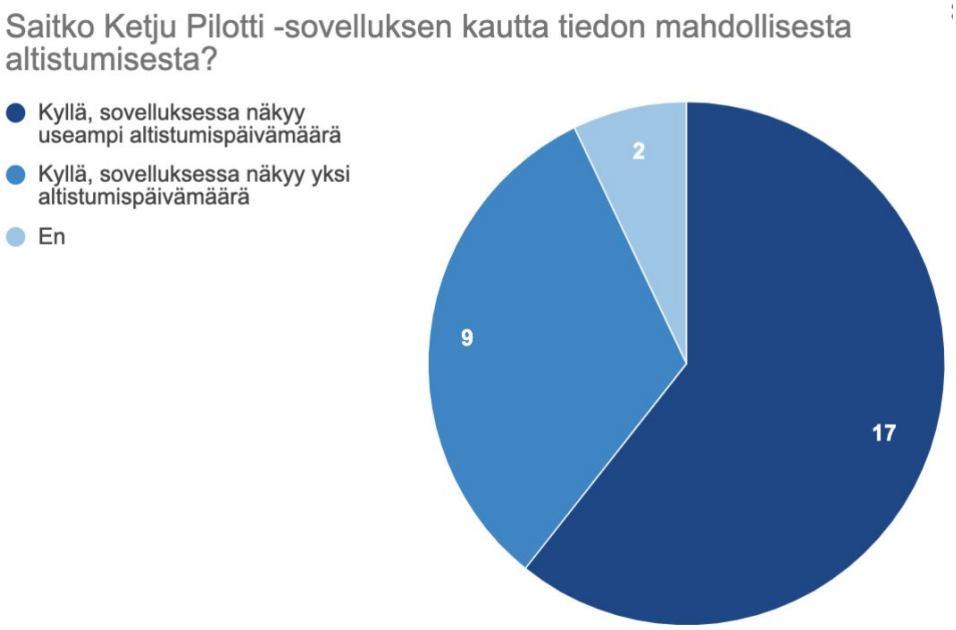
Pilotin osallistujien kokemukset

Hankkeessa tuotettiin lopuksi palautekysely pilotin osallistujille ja 33 osallistujasta 28 vastasi kyselyyn.

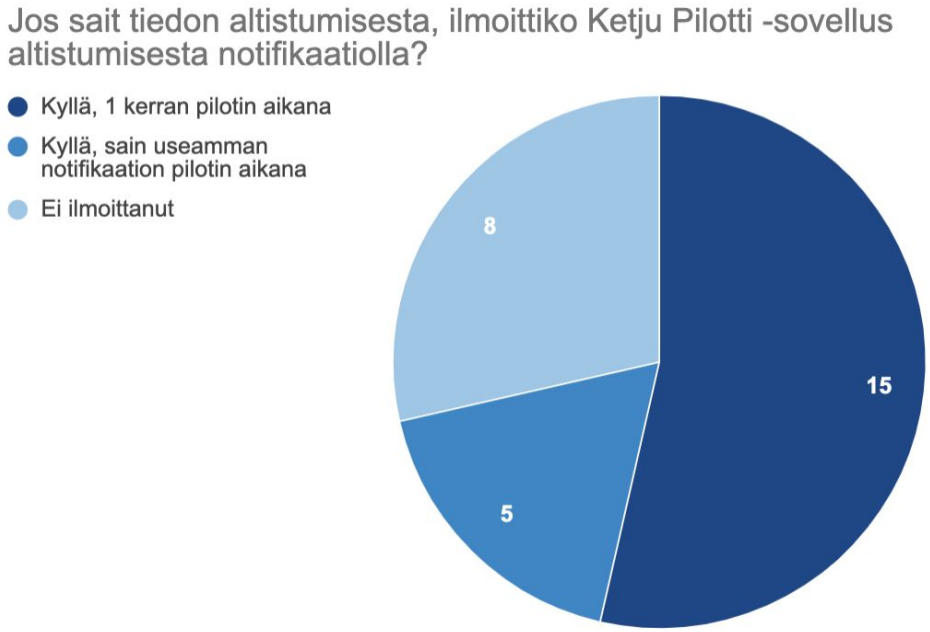
	Kuinka helpoksi koit Ketju Pilotti -sovelluksen käytön? (vastausten keskiarvo skaalalla 1-5, jossa 5 on todella helppoa)	**Kuinka koit Ketju Pilotti -sovelluksen vaikuttavan akun kulutukseen?** (vastausten keskiarvo skaalalla 1-5, jossa 5 on todella helppoa)	**Vaikuttiko Ketju Pilotti -sovellus jotenkin puhelimen käyttöösi?**	**Vaikuttiko Ketju Pilotti -sovellus jotenkin puhelimeen yhdistettävien lisälaitteiden käyttöön?**
Android	4.6	3.5	4/28 Vastasi myöntävästi	1/28 Vastasi myöntävästi
Apple iOS	4.8	4.4	2/28 Vastasi myöntävästi	4/28 Vastasi myöntävästi

Kuva 16. Pilotin lopussa kysyttiin, miten sovelluksen käyttö vaikutti yleiseen puhelimen käyttöön, akun kulutukseen ja lisälaitteiden käyttöön.

iOS-sovelluksen käyttäjät kokivat sovelluksen käytön keskimäärin helpommaksi. (Mutta ero vastauksissa on niin pieni, että se mahtuu otoksen satunnaisvaihteluun; tämän ja muiden alla olevien tulosten tilastollista merkitsevyyttä ei ole testattu.) Lisälaitteiden käytössä oli enemmän haasteita kuin Android-sovelluksen käyttäjillä. Android-sovelluksen käyttäjät kokivat sovelluksen vaikutuksen akun kulutukseen suuremmaksi, ja kokivat että sovelluksen käyttö vaikutti heidän normaaliin puhelimen käyttöönsä.



Kuva 17. Pilotissa simuloitiin positiivisen koronadiagnoosin lähettämistä sovelluksen kautta. Suurin osa pilotin osallistujista "altistui" koronavirukselle pilotin aikana.



Kuva 18. Suurin osa pilotin osallistujista sai ja huomasi sovelluksen lähettämän notifikaation mahdollisesta altistumisesta.

Kuvien 17 ja 18 perusteella saadaan mielikuva altistumistiedotusten toimivuudesta. Suurin osa osallistujista sai sovellukselta tiedon "altistumisesta", kun simuloimme positiivisten koronadiagnoosien lähettämistä. Vaikuttaa kuitenkin että moni pisti merkille ainoastaan ensimmäisestä altistumisesta tulleen notifikaation, ja sen jälkeen sovellus ei joko lähettänyt

ilmoitusta uusista altistumisista tai jos lähetti, ilmoitusta ei huomattu. Kahdeksan vastaajaa sanoi, että ilmoitusta altistumisesta ei tullut lainkaan.

Alla on loppukyselystä saatuja avoimia kommentteja sovelluksen ilmoituksista:

- Notifikaatio tuntui hyvältä keinolta, mutta se tuli vain kerran.
- Notifikaatio tuli vasta kun avasin sovelluksen. Notifikaatiota ei välttämättä myöskään huomaa kovin helposti. Jokin selkeämpi ilmoitustapa olisi parempi ja että se todella toimisi. Jos en olisi avannut sovellusta, en olisi tiennyt altistumisesta.
- Sitä ei huomannut helposti. Jos sen kuittasi kaikkien muiden notifikaatioiden seassa luetuksi, ei sitä nähnyt enää uudelleen.
- Ilmoitus altistumisesta ei tullut. Ketju sovellusta ei kuitenkaan päivittäin avaa ja altistumisen huomaaminen saattaa mennä pitkälle.
- Sain yhden altistumisen, toimi siinä tapauksessa.
- Notifikaatio tuntui hyvältä keinolta. Huomasin tiedon heti kun otin puhelimen käteeni ensimmäisen kerran ilmoituksen saapumisen jälkeen.

Johtopäätökset pilotista

Seuraavaan sovellusversioon on syytä kokeilla Googlen ja Applen kehittämää API:a.

DP-3T:n oma Bluetooth-toteutus osoittautui datan luotettavuuden näkökulmasta haastavaksi. Sitä käytettäessä iOS-sovellukset olivat usein tausta-ajotilassa siten, että eivät lähettäneet omaa signaaliaan säännöllisesti. Tällöin kohtaamisia toisten iOS-laitteiden kanssa jäi havaitsematta.

DP-3T-konsortio on itsekin luopumassa omasta Bluetooth-toteutuksestaan ja siirtymässä käyttämään Googlen ja Applen ratkaisua.

Kohtaamisten luotettava rekisteröinti on haastavaa.

Pilotti osoittaa kuinka merkittävästi laitteiden käsitys etäisyyksistä toisiinsa vaihtelee. Etäisyysmittaus perustuu signaalin voimakkuuteen, johon vaikuttaa laitteen komponenttien ja konfiguraation lisäksi ainakin ympäristö, laitteen asento ja sen sijoittelu. Sovellusta kehitettäessä on hyvä varata riittävästi aikaa kohtaamisten luotettavuuden testaamiselle ja mahdolliselle säädölle.

Luotettavuuteen voi periaatteessa vaikuttaa ainakin laitekohtaisella kalibraatiolla, altistumiskriteerien optimoinnilla ja tekemällä sopivan kompromissin herkkyyden ja tarkkuuden välillä (väärät positiiviset vs. negatiiviset). *Jos* kohtaamisten ja altistumisten kriteereitä pääsee säätämään, ne voidaan yrittää kalibroida joko vallitsevaan epidemiologiseen nyrkkisääntöön, esimerkiksi “vähintään 15 minuuttia enintään kahden metrin etäisyydellä”, tai todellisiin

tartuntoihin. Koska epidemiologiset nyrkkisäännöt ovat jo sinänsä heuristisia ja tuovat oman epävarmuuden kerroksensa, oikeisiin tartuntoihin kalibrointi olisi paras ratkaisu. Mutta on epäselvää voidaanko valitussa hajautetussa mallissa ja etenkin Google-Apple-ratkaisussa tehdä kansallisia säätöjä tai optimointeja. Toisaalta Googlella ja Applella on globaaleina toimijoina mahdollisuus optimoida säädöt itse hyvin.

Kohtaamisten rekisteröinnin luotettavuus vaikuttaa merkittävästi ilmauksiin, joilla sovelluksen kannattaa käyttäjälleen altistumisesta viestiä. Viranomaisen arvioitavaksi jää, mikä on riittävä luotettavuuden taso ja viestinnällinen kulma, kun sovelluksen julkaisupäätöstä tehdään.

Altistumisesta ilmoittaminen on kriittinen osa sovellusta.

Sovelluksen pitää antaa käyttäjälleen riittävän selvä notifikaatio altistumisesta. Pilottisovelluksessa tämä osoittautui hankalaksi, sillä kaikki datan käsittely sekä notifikaation muodostaminen tehtiin paikallisesti käyttäjän laitteesta. Tausta-ajon vuoksi sovelluksen notifikaatio tuli esiin usein vasta käyttäjän valitessa sovelluksen aktiiviseksi. Käyttäjät toivoivat ilmoitusta esimerkiksi sähköpostitse tai tekstiviestillä, mutta tällainen ei olisi onnistunut tausta-ajon eikä sovelluksen hajautetun mallin toimintatavan vuoksi yhtään paremmin. Koska sovelluksella ei ole tietoa käyttäjien identiteetistä, joudutaan ilmoitukset toimittamaan sovelluksen kautta.

Mobiilisovelluksen notifikaatioita käytettäessä on huomioitava, että kukin yksittäinen sovelluksen käyttäjä voi asettaa notifikaatiot näkymään puhelimessaan halutulla tavalla. Tämän vuoksi notifikaatiot voi asettaa myös pois näkyvistä tai ne voivat tulla näkyviin tavalla, jota käyttäjä ei normaalisti puhelinta käyttäessään huomaa. Tähän voidaan vaikuttaa esimerkiksi ohjeistamalla käyttäjiä tarkemmin siitä, miten notifikaatioiden asetukset sovelluksen osalta kannattaa asettaa.

Hajautetun mallin jäljityksestä ei ole merkittävää apua manuaalisessa jäljitystyössä. Tässä mallissa altistusilmoitus voi johtaa ainoastaan käyttäjän omaehtoiseen ilmoittautumiseen, testiin ja karanteeniin. Altistunutta ei tiedetä.

Tartuntaketjujen yksikäsitteinen identifiointi edellyttäisi hybridimallista sovellusta.

Pilottisovellus käytti DP-3T-protokollaa debug-tilassa, jolloin pilotin aikaiset kohtaamiset oli mahdollista yhdistää toisiin käyttäjiin. Tämä oli välttämätöntä, jotta voitiin varmistaa teknologian toimivuus ja luotettavuustaso vertailemalla sovelluksen keräämää kohtaamistietoa käyttäjien itsensä kirjaamiin kohtaamisiin.

Tuotantotilassa, tai käytettäessä Googlen ja Applen Exposure Notification API:a, kohtaamisten yhdistäminen yksittäisiin käyttäjiin ei ole mahdollista, vaan käyttäjä saa ilmoituksen **mahdollisesta** altistumisestaan **noin päivän tarkkuudella**. Jos altistumisesta ei tiedetä tämän tarkempaa ajankohtaa tai keneltä/keiltä se on peräisin, jäljitystyötä tekevän viranomaisen on äärimmäisen vaikeaa liittää altistustieto muuhun tietoon tai käyttää omaa harkintaa. Edelleen,

ilman yksityiskohtaisempaa tietoa altistuksesta lääkäri ei voi määrätä käyttäjää viralliseen karanteeriin joka oikeuttaisi esim. taloudellisiin korvauksiin. Altistumisilmoituksen perusteella käyttäjä voi siis ainoastaan mennä omaehtoisesti testattavaksi ja/tai jäädä vapaaehtoiseen karanteeniin.

Näin vahva anonyymius on manuaalisen jäljitystyön kannalta hankalaa myös, koska sovellus tuottaa väistämättä vääriä positiivisia altistumia tilanteista jotka eivät todellisuudessa ole altistumisriskejä. Hajautetun mallin vahva tietosuoja (ei tarkkaa aikaa, ei altistumislähdettä) estää tilanteiden yksikäsitteisen tunnistamisen ja niiden tarkemman evaluoinnin esimerkiksi infektiolääkärin toimesta.

Jos sovellus toteutettaisiin hajautetun mallin sijaan hydridimallilla niin että tarkemmat kohtaamistiedot saataisiin käyttäjän suostumuksella viranomaisille, altistumiset olisi mahdollista yhdistää muihin sairastuneisiin ja muistettuihin kohtaamistilanteisiin. Haastattelemalla sekä sairastunutta että altistunutta olisi mahdollista selvittää, että altistunut istui sairastuneen kanssa vaikkapa samassa bussissa kasvot eri suuntiin. Tämän tiedon perustella lääkäri voisi arvioida karanteenitarpeen. Hydridimalli ei kuitenkaan ole mahdollinen käytettäessä DP-3T:ta tai Google-Apple-ratkaisua.

Maailmalla on käytetty pidempään keskitetyn mallin pakollisia jäljityssovelluksia, kuten Singaporessa käytettävää Bluetrace-sovellusta, ja tuloksia niiden käytöstä epidemian hallinnassa on saatavilla. Hajautetun mallin sovelluksia ei ole ollut käytössä (tätä kirjoitettaessa) niin kauaa että niiden hyödyistä epidemian hallinnassa olisi saatu näyttöä. Ylipäätään altistuksia havaitsevat sovellukset ovat epidemian hallinnassa manuaalisen jäljitystyön ja muiden toimenpiteiden tuki ja täydentäjä, ei kokonaisvaltainen ratkaisu.

8. Tulosten julkaisu

Hankkeen tulokset julkaistaan hankkeen lopuksi vapaaseen käyttöön Sitran rahoituspäätöksen periaatteiden mukaisesti. Sovelluskoodit julkaistaan avoimena lähdekoodina GitHub-palvelussa.

Lisäksi palvelussa julkaistaan muut hankkeen aikana tuotetut materiaalit helposti saataville, kuten tämä loppuraportti, arkkitehtuurikuva ja kuvasarjat käyttöliittymistä.

GitHub: https://github.com/ketjusovellus