Yleiskuvaus

Käyttötarkoitus

Hankkeen tavoitteena on tukea ja tehostaa tartuntatautien jäljitystyötä terveydenhuollossa ja tartuntaketjujen katkaisemista mobiiliteknologiaan perustuvaa sovellusta hyödyntämällä. Yksityisyydensuojaa tulee kunnioittaa ja sovelluksen käytön tulee olla vapaaehtoista.

Tavoitteena on kansalaisille maksutta puhelimeen ladattavan sovelluksen avulla

- Tavoittaa tartuntataudille altistunut henkilö
- Antaa altistuneelle henkilölle toimintaohjeita yhteydenottamiseksi terveydenhuoltoon tarkempien ohjeiden ja mahdollisesti karanteenipäätöksen saamiseksi sekä tarvittaessa testaukseen hakeutumiseksi.

Reunaehdot

Euroopan komissio on antanut ohjeistuksensa. Tiivistetysti näistä merkittävimmät ovat

- Sovellusten pitää toimia koko EU alueella.
- Sovelluksen käyttäjän identiteettiä ei ilmaista viranomaisille, mutta käyttäjä voi halutessaan antaa tiedon viranomaisille.
- Tieto altistumisesta välitetään muille sovelluksen käyttäjille ja vain mahdollisesti viranomaisille.
- Palvelimille mahdollisesti tallennetun tiedon tulee olla salattua ja noudattaa täysin EU:n tietosuojasäännöksiä.

Sosiaali- ja terveysministeriö (STM) on antanut linjauksena
- Ensimmäisessä vaiheessa sovellus toteutetaan hajautetun mallin mukaisesti jota täydennetään asiakkaan vapaaehtoisella ilmoituksella terveydenhuoltoon.
- Sovellukseen liittyvien integraatioiden määrä pidetään mahdollisimman vähäisinä, paitsi
    - Avauskoodin saaminen ammattilaiselta
    - Altistuneen pitää pystyä tekemään soittopyyntö sovelluksen avulla
- Kontaktienseuranta saa perustua vain Bluetooth-teknologiaan ja seurannassa ei saa hyödyntää tai tallentaa muuta paikkatietoa.
- Sovelluksen tulee toimia vähintään suomeksi ja ruotsiksi.

Järjestelmä yleisellä tasolla noudattaa kansainvälistä DP3-T -mallia ja käyttää Apple/Google-rajapintoja. Työssä on huomioitava Googlen ja Applen asettamat reunaehdot jäljityssovelluksille.

Liittymät muihin järjestelmiin

Avauskoodin saaminen terveydenhuollosta

Osana totetusssuunnitelmaa on kuvattava, millaiset järjestelyt terveydenhuollossa tarvitaan, jotta terveydenhuollon ammattihenkilö pääsee antamaan avauskoodin.

Avauskoodi voidaan toimittaa todetulle tapaukselle esim. laboratoriotuloksen, eristys- ja hoito-ohjeiden sekä kontaktien kartoituksen yhteydessä.

On varmistettava, ettei avauskoodeja voi tuottaa muut kuin terveydenhuolto.

On varmistettava, ettei avauskoodia syötetä toisen kuin varmistetun tapauksen puhelimen sovellukseen.

Altistuneen tekemä soittopyyntö

Henkilön on mahdollista välittää sovelluksella omat yhteystietonsa (nimi, puhelinnumero ja kunta) terveydenhuollon tietojärjestelmään.

Toiminnalliset vaatimukset

Yleiskuvaus järjestelmän toiminnasta

Hajautetun mallin mukaisesti altistuneiden tavoittaminen toteutetaan mobiililaitteiden Bluetooth-teknologiaa hyödyntämällä siten, että laitteeseen tallentuu tiedot henkilöiden laitteiden kohtaamisista. Mobiiliratkaisu perustuu henkilöiden vapaaehtoisesti käyttöön ottamiin sovelluksiin, jotka tallentavat vahvasti salatut kontaktitiedot hajautetusti käyttäjien mobiililaitteisiin. Sovellus ei tallenna tunnisteellista henkilötietoa, vaan yksilöllisiä pseudonymisoituja tunnisteita, jolloin yksittäiset, lähikontaktissa olleet henkilöt eivät ole tunnistettavissa.

Kun sovelluksen ladanneet henkilöt kohtaavat, sovellukset tallentavat toistensa yksilölliset tunnisteet. Teknisesti sovellukseen määritellään terveysviranomaisen arvioon perustuen, mikä on Covid-19-viruksen lähikontakti eli kontaktin etäisyys ja kohtaamisen kesto (tämän hetkisen tiedon valossa esim. 2 metriä ja 15 minuuttia). Kontaktin etäisyys tulee Bluetooth BLE tekniikan kantomatkasta, joka on vain muutamia metrejä eikä siihen voi vaikuttaa eikä sitä mitata. Sen sijaan kontaktin minimiaikaraja voidaan asettaa ja se tulee parametreista.

Sovellus seuraa terveydenhuollon taustajärjestelmän kautta julkaisemia infektoituneiden henkilöiden sovellusten pseudotunnuksia. Jos sovellus huomaa olleensa lähikontaktissa infektoituneen pseudotunnuksen kanssa, ilmoittaa sovellus käyttäjälle altistumisesta.

Jos sovelluksen käyttöönottaneella henkilöllä vahvistetaan positiivinen Covid-19-testitulos, hän saa terveydenhuollolta yhteydenoton muuten kuin sovelluksen kautta. Sovelluksen kautta ei tule yhteydenottoa, koska terveydenhuollolla ei ole sovelluksen yhteystietoja.

Käyttötapaukset

Sovelluksen asennus

Sovellus asennetaan samoista sovelluskaupoista kuin muutkin Android ja IOS sovellukset.

Lähikontaktin tunnistaminen

Kun sovelluksen ladanneiden henkilöiden laitteet kohtaavat, niiden sovellukset tallentavat toistensa yksilölliset tunnisteet. Teknisesti sovellukseen määritellään terveysviranomaisen arvioon perustuen, mikä on Covid-19-taudin

lähikontakti eli kontaktin etäisyys ja kohtaamisen kesto (tämän hetkisen tiedon valossa esim. 2 metriä ja 15 minuuttia). Tämä määrittely on parametri.

Tartuntataudin varmistaminen

Jos sovelluksen käyttöönottaneella henkilöllä vahvistetaan positiivinen Covid-19-testitulos, hän saa terveydenhuollolta avauskoodin omien tietojensa välittämiseksi taustajärjestelmään. Tällöin vain hänen oman sovelluksensa pseudotunniste välitetään taustajärjestelmään . Erityisesti on huomioitava, ettei sovellukseen tallentuneita kontaktitietoja eli muiden käyttäjien pseudotunnisteita luovuteta taustajärjestelmälle. Hän myös syöttää sovellukseen oireiden alkamispäivän (oireinen tapaus) tai näytteenottopäivän (oireeton tapaus), minkä avulla mahdolliset altistuneet määritellään.

Altistumisesta ilmoittaminen

Sovellus ilmoittaa käyttäjälleen varoituksen mahdollisesta altistumisesta Covid-19 virukselle kerätyn läheisyystiedon ja taustajärjestelmästä hakemiensa tartuntatietojen ja parametritietojen perusteella. Altistuneet henkilöt saavat tiedon omaan sovellukseensa ja heille annetaan toimintaohjeet. Altistunut henkilö voi vapaaehtoisella luovutuksella sovelluksen avulla luovuttaa oman nimen, puhelinnumeron ja kunnan terveydenhuollolle. Altistunut henkilö voi itse jakaa tiedon edelleen terveydenhuollon toimivaltaisille viranomaisille (kunnan tartuntatautilääkäri). Ilmoituksessa tulee olla linkki Omaolo-oirekyselyyn, jonka kautta oireinen altistunut voi saada toimintaohjeita.

Saadessaan tiedon altistumisesta, altistunut henkilö jättää halutessaan oma-aloitteisesti sovelluksen kautta yhteydenottopyynnön terveydenhuoltoon.

Sovelluksen käytön päättäminen

Sovelluksen käyttö on kansalaisille vapaaehtoista ja sen voi poistaa puhelimesta milloin vain, jolloin sovelluksen tallentamat tiedot ja sovelluksen asetukset tuhoutuvat. Bluetooth-yhteyden voi myös halutessaan kytkeä pois päältä.

EI-toteutettavat toiminnat

Ei tallenneta sairastuneen karanteeni- ja eristämispäätöksiä tai seurata niiden noudattamista.

Ei seurata käyttäjän sijaintia.

Integraatiot laboratoriotulosten tai potilaskertomusmerkintöjen tuottamisessa käytettäviin tietojärjestelmiin tai Kanta-palveluihin eivät sisälly järjestelmään. Ehdotuksissa saa kuitenkin esittää jatkokehitysmahdollisuuksia ominaisuuksista, joilla järjestelmä voidaan myöhemmin sovittaa sujuvasti hoito- ja jäljitysprosesseissa toimivien ammattilaisten toimintaan.

Optiot

Yhteentoimivuus EU alueella.

Tiedon vapaaehtoiseen antamiseen perustuva kontaktitietojen luovutus eli kohdattujen muiden henkilöiden pseudotunnisteiden luovutus taustajärjestelmälle. Tällöin jäljitystoimintaa voidaan tehdä myös taustajärjestelmässä ja terveydenhuoltohenkilökunnalla on näkyvyys altistusketjuihin.

Käyttäjä voi ilmoittaa sovellukselle perustiedot oireista (onko Covid-19-sairauteen liittyviä oireita, milloin alkavat). Tätä tietoa käytetään riskiarvion laskennassa niin, että huomioidaan osa sellaisistakin kontakteista, jotka normaalisti ohitettaisiin.

Muut kuin toiminnalliset vaatimukset

Ohjelmisto

Ohjelmiston ja sen lähdekoodin tulee olla tilaajan omistuksessa. Tilaajalla on oikeus julkaista ohjelmiston lähdekoodi tilaajan valitsemalla lisenssillä. Tästä syystä ohjelmiston käyttöön ja kehittämiseen tarvittavat työkalut ja kirjastot tulee olla open sourcea tai muuten avoimesti maksutta saatavissa koko sopimuskauden ajan ml. optiokausi.

Käytettävyys

Yhdenvertaisuuslain 5 §:n mukaisesti viranomaisten on edistettävä yhdenvertaisuutta. Yhdenvertaisuuden kannalta merkityksellisten hankkeiden valmistelussa on arvioitava niiden yhdenvertaisuusvaikutukset.

Koska jäljityssovelluksella tuotettaisiin turvaa vakavaa terveydellistä riskiä koskien, on edellä viitattu yhdenvertaisuuslain velvoite huomioiden varmistettava, että asian lisävalmistelussa riittävästi arvioidaan suunnitelmaan liittyvien toteuttamisvaihtoehtojen yhdenvertaisuusvaikutuksia

Esimerkiksi ikään (erityisesti lapset ja ikääntyneet), kieleen ja vammaisuuteen liittyvät näkökohdat on huomioitava ja pyrittävä valitsemaan mahdollisimman hyvin yhdenvertaisuutta edistävät toteuttamistavat. Lopullisessa suunnitelmassa, laadittavassa laissa, toteuttamisbudjetissa, THL:ltä edellytettävissä toimenpiteissä sekä sopimuksessa palveluntuottajan kanssa on riittävällä tasolla turvattava arvioinnissa havaitut relevantit yhdenvertaisuusnäkökohdat. Myös mahdollisen käyttöönoton aikana sovelluksen toimintaa on arvioitava tästä näkökulmasta.

Etenemistä koskevan muistion mukaan (s. 4) ”Sovelluksen kehityksessä on tavoitteena ottaa huomioon myös sellaiset väestöryhmät, joilla ei ole mahdollisuutta käyttää älylaitetta edellyttäviä sovelluksia. Esteettömiä tapoja jäljityssovelluksen hyötyjen toteuttamiseksi ovat erilaiset kansainvälisissä malleissa toteutetut puettavat tai mukana pidettävät välineet.”.

Valtuutetun näkemyksen mukaan asian jatkovalmistelussa on tarkennettava ja lisäselvitettävä edellä todettuja seikkoja. Jäljityssovelluksen valmistelussa, kehityksessä, budjetissa ja mahdollisen käyttöönoton jälkeisessä seurannassa on varmistettava esteettömyyteen ja saavutettavuuteen liittyvät näkökohdat. Valtuutetun näkemyksen mukaan yhdenvertaisuuslain 5 § huomioiden mahdollinen sovellus ja sitä koskeva tiedotus ja opastus tulisi suomen ja ruotsin kielen lisäksi toteuttaa myös riittävästi muilla kielillä (arvioitavaksi valmistelussa esimerkiksi Suomessa yleisimmin käytetyt kielet mukaan lukien perustuslain 17 §:ssä mainitut kielet), jotta sovelluksesta voivat saada tietoa ja sitä käyttää myös muut kuin kansalliskieliä osaavat henkilöt.

Yleisesti valtuutettu vielä toteaa, että koska kaikilla suomalaisilla ei ole käytössään älylaitteita – esimerkiksi ikään, terveyteen tai vammaisuuteen liittyvien taikka sosioekonomisista syistä johtuen – on mahdollisen sovelluksen ohella Covid-19 -jäljitystyössä tehokkaasti käytettävä ja kehitettävä myös muita kuin sovellukseen nojaavia menetelmiä.

Ylläpidettävyys

Parametrien kautta tapahtuva helpompi muunneltavuus, ilman että sovellusta tarvitsee päivittää, kun tieto lisääntyy ja sovelluksen toimintaa tai viestejä halutaan muuttaa. Parametrit on kuvattu tarkemmin Taustajärjestelmän kohdalla.

Laajennettavuus

Sovellusta tullaan mahdollisesti laajentamaan seuraaviin suuntiin, jotka tulisi huomioida jo perusvaiheen teossa niin, ettei laajennusten tekeminen riko tai aiheuta suuria muutoksia olemassa olevaan toimintaan.

- Omien tietojen ilmoittaminen appista taustajärjestelmään terveydenhuollolle tarkkuudella nimi, kunta, puhelin.
- Oman pseudotunnisteen ilmoittaminen appista taustajärjestelmään ja siten oman identiteetin kytkeminen siihen.
- Taustajärjestelmän integraatioita.

Rakenne

Järjestelmä koostuu mobiilisovelluksesta sekä taustajärjestelmästä.

Tietoturva

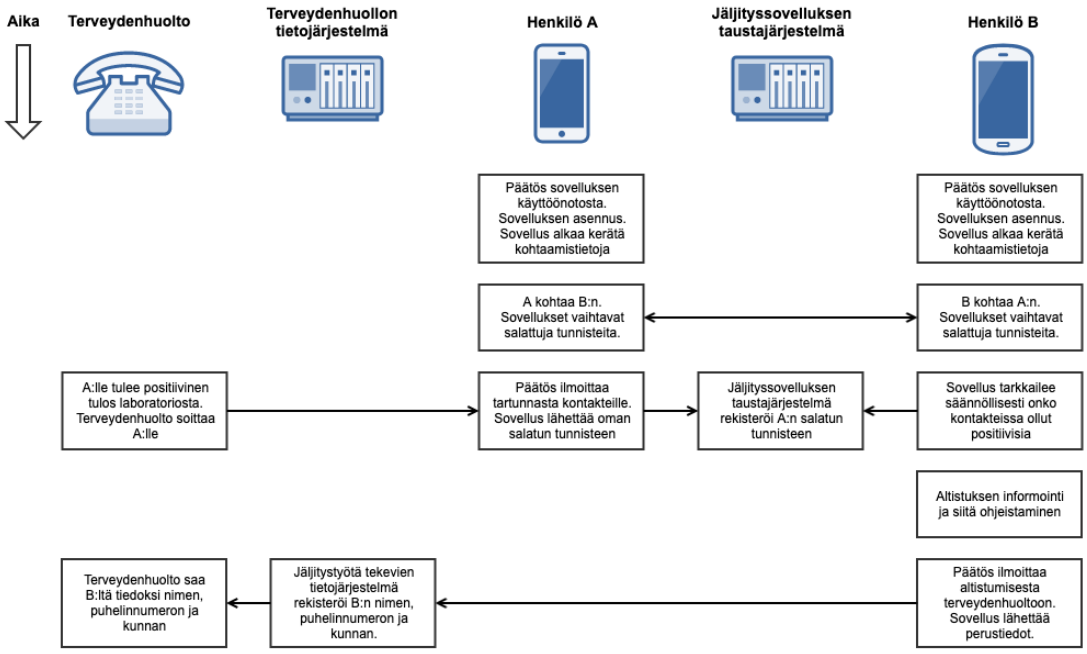
Ohjelmiston suunnittelussa ja toteutuksessa tulee noudattaa tietoturvallisia käytäntöjä siten, että niiden noudattaminen pystytään osoittamaan.

Kyberturvallisuuskeskus arvioi tai hyväksyy lopputuloksen. Arvioinnissa nojaudutaan erityisesti sellaisiin Katakri- ja Pitukri-kriteereihin, joita voidaan soveltaa kehitettävään ratkaisuun.

Ratkaisun toteuttamisessa on noudatettava liitteen 5 (tietoturvavaatimukset) mukaisia vaatimuksia.

Arkkitehtuuri

Prosesseista on laadittu prosessikuvaukset, jotka ovat saatavana erikseen. Alla on yleiskuva ja sen jälkeen tapahtumakohtaiset yksinkertaistetut kuvaukset.



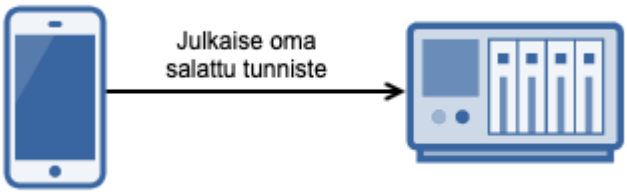
Kohtaaminen

Käyttäjän sovellus vaihtaa tietoja toisen puhelimen sovelluksen kanssa, jos kohtaaminen ylittää kestoltaan annetun aikarajan. Mitään henkilökohtaista tietoa ei siirry. Vaihdossa siirtyy vain salattu tunniste, josta ei käy ilmi mitään henkilötietoja. Tieto kohtaamisesta säilytetään käyttäjän laitteella korkeintaan 14 vuorokautta.

Sairastunut

Hajautetussa järjestelmässä viranomaispalvelussa on ainoastaan vahvistettujen tartuntojen osalta sovellusten salatut tunnisteet, jos käyttäjät ovat ne antaneet. Tunnisteen antaminen on vapaaehtoista. Viranomaisilla ei ole tietokantaa, siitä kuka on kohdannut kenet, tai milloin tapaamisia on tapahtunut.

Käyttäjä voi julkaista oman salatun tunnisteensa ainoastaan viranomaisen pyynnöstä ja silloin tiedon oikeellisuus tarkistetaan vertaamalla julkaisun ja pyynnön yhdistävää tilapäistä avainta. Kukaan ei voi väittää saaneensa tartuntaa ja siten häiritä järjestelmää.

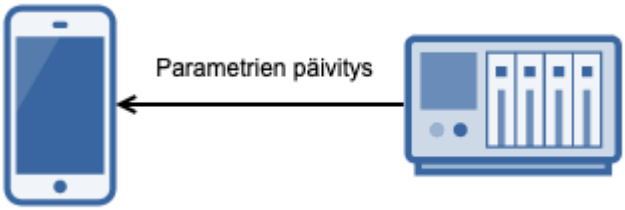


Oireeton

Sovellus tarkistaa väliajoin, onko tullut se kohdannut sairastuneita siten, että kohtaaminen on kestänyt yli annetun aikarajan. Jos näin on käynyt, sovellus ohjeistaa miten toimia. Sovellus ei lähetä tietoja eteenpäin.

Päivitykset

Epidemian aikana voi tarkentua ohjeet siitä, miten toimia tai mihin ottaa yhteyttä. Samoin kieliversiot teksteistä voivat muuttua tai kriteerit joilla kohtaaminen rekisteröidään. Sen sijaan että nämä olisivat kiintesti osa sovellusta, ne voidaan ladata parametreina palvelimelta, jolloin niiden päivitys on helppoa.



Käyttöliittymä

Appiin tarvitaan ainakin seuraavat sivut tai toiminnallisuudet:

- Status: Onko yhteydet kunnossa ja onko tiedonkeruu muista appeista toiminnassa
- Altistuminen: Altistuminen havaittu aiemman kohtaamisen perusteella, ohjeet mitä tehdä.
- Positiivinen tulos: Omien tietojen vapaaehtoinen jako terveydenhoitohenkilökunnalle
- Suostumus 1: Saako jakaa pseudonymisoituna id:n muille kohdatuille appeille
- Suostumus 2: Omien tietojen jakaminen terveydenhoitohenkilökunnalle

Osajärjestelmät

Mobiiliappi

Mobiiliappien tulee toimia sekä Android että IOS laitteilla.

Ohjelmointikieli appille tulee olla yleisesti saatavilla ja samoin käytettävä kehitysympäristö. Ohjelmiston jatkokehitystä ja siihen tehtäviä muutoksia tulee tilaajan pystyä käytännössä jatkamaan myös muun kuin alkuperäisen toimittajan kanssa.

Appien käyttämät kirjastoversiot ja ominaisuudet tulee valita siten yleisiksi, että appi on kyseisen ympäristön (Android / IOS) suomalaisista käyttäjistä noin 95 % käytettävissä.

Taustajärjestelmä

Taustajärjestelmä on toteutettava seuraavassa taulukossa kuvatuilla teknologioilla.

Teknologiavaatimuksen osa-alue	**Vaatimus**
Rajapinnat	REST (suositus) tai SOAP. Rajapintasuojauksiin käytettävä OpenID connect -teknologiaa.
Ohjelmointikieli	Java, OpenJDK versiot 11-14. Käyttöliittymän kehitykseen on käytettävä ReactJS.
Käyttöjärjestelmä	Redhat Linux.
Ajoympäristö	Spring Boot, OpenShift.
Tietokannat	PostgreSQL.
Tietoliikenne	Toimittajille järjestetään pääsy tarvittaviin taustajärjestelmiin Kelan osoittamilla tavoilla. Taustasovelluksien on toimittava Kelan valitsemien varmentajien (CA) varmenteilla.
Kokoonpanohallinta	Maven. Valmius asennuksiin Jenkinsin kautta.
Kirjastot ja middleware-ratkaisut	Käytettävä maksutta saatavia valtavirtaratkaisuja (open source), joihin on saatavissa enterprise-tason tukipalvelu. Mikäli taustajärjestelmän toiminta edellyttää muita kuin maksutta saatavia kirjastoja

Teknologiavaatimuksen osa-alue	Vaatimus
	tai alustaan, ajoympäristöön tai muihin middleware-ratkaisuihin liittyviä komponentteja, tarjouksessa on kuvattava tarvittavien lisenssien ja tukipalvelujen kustannukset sopimuskauden ajalta ml. optiokausi.
Tuotantovalmiudet	Tekniset ratkaisut on dokumentoitava siten, että niiden avulla voidaan ylläpitää, kehittää ja asentaa tarvittavat taustajärjestelmät. Taustajärjestelmän komponentit ovat skaalattavissa. Palvelut oltava kahdennettavissa ja hajautettavissa useampaan konesaliin. Sovelluksien on tarjottava valvontarajapinnat. Järjestelmän on tuotettava riittävät käytön- ja sovellusvalvonnan ominaisuudet.

Infektoituneiden tietokanta
Kaikki keskustellut mallit, myös hajautettu malli, tarvitsevat infektoituneiden pseudotunnusten tallentamista ja appeille jakamista varten terveysviranomaisten ylläpitämän palvelun. Jos tämä puuttuisi, ei appilla olisi luotettavaa mahdollisuutta kertoa käyttäjälle altistuksesta.
EU Komission vaatimusten mukaan tietokanta on salattu. Tähän riittää se, että tietokanta sisältää pseudotunnisteita, jotka ovat itsessään salaisia eikä niitä voi yhdistää käyttäjiin, elleivät nämä ole erikseen antaneet lupaa sovelluksessa. Tietokantaa ei itsessään tarvitse salata.

Aktivointikoodin generointi
Infektoituneelle todennäköisesti soittamalla toimitettavan koodin luonti, jolla appi voi luotettavasti ilmoittaa taustajärjestelmän Infektoituneiden tietokannalle oman pseudotunnuksensa.

Sovelluksen parametrikanta
Parametrikannan avulla Tilaaja voi itse ylläpitää ja muuttaa sinne sovittuja parametreja, jotka sovellus hakee väliajoin parametrikannasta ja näin päivittää toimintaansa. Jos parametrikanta on helposti käytettävissä esimerkiksi SQL lausein, ei sille tarvitse rakentaa erillistä käyttöliittymää.
Tunnistetut parametrit
- Käyttäjälle annettavat viestit eri tilanteissa kuten altistuksen havaittaessa. Viestit annetaan eri kieliversioilla suomi ja ruotsi.
- Altistuksen minimiaikaraja, joka tarvitaan lähikontaktin rekisteröintiin. Tätä ajallisesti lyhyempiä lähikontakteja ei huomioida.
- Tartuntamisikkunan aikaraja, eli kuinka paljon ennen

Jäljitystietokanta
Toteutuksena on hajautettu malli täydennettynä altistuneen vapaaehtoisella ilmoituksella, jolloin käyttäjän salliessa lähettää terveydenhuollolle nimen, kunnan ja puhelinnumeron.

Tilastodata
Tässä kuvataan ne tietotarpeet, joita on taustajärjestelmästä saatava ulos. Tämä voidaan toteuttaa erillisenä osana, tai jos tiedot ovat SQL kannassa tai vastaavassa, niin riittänee määritykset sille kuinka nämä tiedot saadaan haettua.
Taustajärjestelmässä on infektoituneiden pseudotunnuksia ja tilapäisiä OTP tunnuksia jotka on annettu käyttäjille. Näistä tarvitaan tilastollista seurantaa varten kappalemäärät, aikasarja eli aktiivisuuden eteneminen ajassa, ja osuus kuinka moni OTP tunnuksen saaja antaa tietonsa ja kuinka moni kieltäytyy. Tieto on aggregoitua koko maata koskevaa.
Jos hajautetun mallin lisäksi toteutetaan käyttäjältä suostumuksella pyydetty nimen, puhelinnumeron ja kunnan kerääminen, tulisi aggregoida tästä osuudesta kunta, päiväys ja kappalemäärät. Jos lisäksi kerätään muuta tietoa, tulisi myös se aggregoida sillä tasolla, ettei yksilöä tunnisteta.
Lisäksi tulee tietää asennettujen sovellusten määrä. Tähän voidaan käyttää parametrikannasta tehtyjä päivityshakuja siten, että aggregoitaisiin päivätasolla päivitystä pyytäneiden sovellusten lukumäärät. Tällöin tiedetään aktiivisten sovellusten määrät aikasarjassa.

Elinkaari

Mobiilisovellukset

Jakelu

Sovellukset jaellaan Androidin ja Applen sovelluskaupoista. Sovellukset toteuttaa ja sovelluskauppoihin toimittaa Toimittaja, joka on myös sovelluskauppojen edellyttämien sopimusten osapuoli. Toimittaja on velvollinen jakeluun koko sopimuskauden ml.optiokausi ajan ellei Tilaaja toisin ilmoita. Sovelluskaupoissa sovelluksen tulee olla maksuton eikä saa sisältää maksullisia lisäominaisuuksia. Sovelluksesta ei saa tehdä muita versioita kuin mitä Tilaaja on erikseen pyytänyt.

Päivitykset

Toimittaja korjaa ja julkaisee uuden mobiiliversion sovelluskauppihin, jos paljastuu sellainen merkittävä toiminnallisuutta heikentävä seikka, jota ei voida parametrien muutoksilla korjata. Kaikista päivityksistä tulee sopia Tilaajan kanssa.

Käytön lopettaminen

Kun Tilaaja ilmoittaa sovelluksen käytön lopettamisesta, Toimittaja poistaa sovellukset molemmista sovelluskaupoista.

Taustajärjestelmä

Ajoympäristö

Taustajärjestelmää suoritetaan Tilaajan määrittämässä paikassa.

Päivitykset

Toimittaja päivittää taustajärjestelmää, jos tulee sellainen muutostarve, jota ei voida parametrien päivittämisellä korjata, kuten uuden parametrin käyttöönotto.

Uuden kieliversion (suomen ja ruotsin jälkeen) käyttöönotto tulisi kuitenkin huomioida sovelluksessa jo valmiiksi niin, että taustajärjestelmän parametreihin lisätty uusi kieli voidaan ottaa sovelluksessa käyttöön ilman sovelluksen päivitystä sovelluskauppoihin.

Uhkamallinnus

Toteutukseen liittyviä mahdollisia tietoturvariskejä on lueteltu seuraavassa taulukossa.

STRIDE	Tapaus
Identiteettihuijaus	Käytetään väärää pseudotunnusta kun lähetetään taustajärjestelmään infektoituneen oma pseudotunnus terveydenhuollon antaman pin koodin valtuutuksella.
Identiteettihuijaus	Käytetään väärää pseudotunnusta kun vaihdetaan tietoja toisen sovelluksen kanssa
Identiteettihuijaus	Lähetetään väärän henkilön nimi, puhelin ja kunta, kun ilmoitetaan taustajärjestelmään altistumisesta
Identiteettihuijaus	Taustajärjestelmästä jokainen sovellus lataa säännöllisesti infektoituneiden pseudotunnukset. Hyökkääjä voi lähettää omalla muokatulla sovelluksellaan näitä tunnuksia ympärilleen, jolloin järjestelmä kuormittuu ja kokonaiskuva hajoaa.
Tiedon muuttaminen	Lähetetään vääriä tavattuja pseudotunnuksia taustajärjestelmään hybridimallissa
Tiedon muuttaminen	Lähetetään liian pitkä, lyhyt, väärä merkkikoodaus tai muuten rikkinäistä dataa toiselle sovellukselle avaintenvaihto-protokollassa
Tiedon muuttaminen	Lähetetään liian pitkiä, lyhyitä, vääriä merkkikoodauksia tai muuten rikkinäistä dataa taustajärjestelmälle joko viestikokonaisuutena tai yksittäisisssä datakentissä
Tiedon muuttaminen	SQL injektointi-hyökkäys datakenttien sisällössä.
Kiistämättömyys	Sovelluksien pseudotunnusten ajallinen vaihtuminen puhelinten sisällä voi tehdä niiden seurannasta mahdottoman, jos vaihtumisessa tai sen seurannassa on virhe, jolla hukataan tieto aikaisemmista tunnuksista tai tunnuksien luonnissa tapahtuu eri puhelinten kesken törmäämisiä, jolloin luodaan eri puhelimissa samoja tunnuksia.
Tiedon vuotaminen	Voiko puhelimen sovellus vuotaa kohdattujen muiden henkilöiden pseudotunnuksia samassa puhelimessa olevalle toiselle sovellukselle, kun molemmat ovat samassa laitteessa

STRIDE	Tapaus
	ja molemmilla on ehkä oikeudet samaan bluetooth-toiminnallisuuteen ja mahdollisiin lokeihin.
Tiedon vuotaminen	Jos puhelimessa on toinen vähän muokattu jäljityssovellus, niin voiko tämä toinen sovellus hakea taustajärjestelmästä infektoituneiden pseudotunnukset ja hälyttää sillä hetkellä kun havaitsee läheisyydessään tunnetun infektoituneen pseudotunnuksen. Tämä loukkaisi henkilöiden yksityisyyttä vahvasti.
Palvelun esto	Mobiililaitteiden verkkoliikennettä seuraamalla näkee mihin osoitteeseen ne lähettävät tietoa ja mistä hakevat parametreja. Hyökkääjä voi yrittää tehdä samoihin osoitteisiin palvelunestohyökkäuksen.
Käyttöoikeuksien laajentaminen	Puhelimia jailbreakataan ja niihin saadaan ylläpitäjän oikeudet. Voidaanko näitä oikeuksia käyttää sovelluksen käyttämien taustajärjestelmän API-avainten kaappaamiseen tai sovelluksen muistin tutkimiseen siten, että hyökkääjä voi sekoittaa taustajärjestelmän tietosisältöä tai loukata muiden henkilöiden yksityisyyttä esimerkiksi varoittamalla sovelluksen havaitessa infektoituneen pseudotunnuksen läheisyydessään.
Sovelluksen jumiutuminen	Sovellus lataa infektoituneiden pseudotunnukset kerran vuorokaudessa taustajärjestelmästä. Maksimissaan tämä on 5 M kpl. Tiedon koko voisi olla silloin 5 M * 64 B = 320 MB. Tämä voi olla ongelma muistinkulutuksen tai tiedonsiirron kannalta, jos sovelluksen pseudotunnusta vaihdetaan usein, sillä silloin tiedon määrä voi kertautua.
Tartuntaketjun varmistamisen hitaus	Virus voi kulkea useamman henkilön muodostaman ketjun kautta samana päivänä ja siten tartuttaa koko ketjun. Jäljityssovelluksessa jokaisen uuden lenkin lisääminen edellyttää terveydenhuoltohenkilökunnan soittamista infektoituneelle A:lle, infektoituneen suostumusta sovelluksen lähettää oma pseudotunnus taustajärjestelmälle, muiden sovellusten infektointitietojen päivitystä taustajärjestelmistä, sovelluksen ilmoittamista B:lle altistumisesta, B:n laboratoriotestiin hakeutumista, laboratoriotestien tekemistä ja tulosten valmistumista. Tällöin yksittäisen lenkin selvittämisen kesto on ehkä 5 pv kun viruksen siirtymiseen voi riittää 15 min. Täten selvittäminen on pahimmillaan 5 pv/15 min = 480 kertaa hitaampaa kuin leviäminen.