NOTA VOOR EERSTE DISCUSSIE IN DE INTERMINISTERIËLE CONFERENTIE OVER EEN CONTACTOPSPORINGSAPP – 25 MEI 2020

CONTACTOPSPORING: MOGELIJKE METHODEN

Experten zijn het erover eens dat een epidemie maar onder controle kan gebracht worden met een combinatie van testen, contactopsporing en quarantaine. Door contactopsporing identificeert men burgers die in contact zijn geweest met een besmet persoon om deze burgers aan te moedigen om in quarantaine te gaan plaatsen en/of zich te laten te testen. Contactopsporing is een belangrijk element in een controlestrategie, maar het is geen wondermiddel. Slechts 5% van de risicovolle contacten zouden leiden tot een besmetting, wat betekent dat – zelfs als de contactopsporing op zich goed zou werken – 95% van de testen na contactopsporing negatief kunnen zijn. Daarnaast kan contactopsporing geen infecties via oppervlakken detecteren[1].

Manuele contactopsporing op basis van interviews werd recent geïmplementeerd in België. Deze aanpak is onderhevig aan een aantal beperkingen: het vraagt veel tijd en middelen, het steunt op het geheugen van de besmette personen en het is niet geschikt om contacten op te sporen met onbekenden (bv. op het openbaar vervoer of op restaurant).

Er zijn sterke indicaties dat een contactopsporingsapp een positieve rol kan spelen bij het onder controle brengen van een epidemie. Een app biedt belangrijke voordelen inzake snelheid en efficiëntie van contactopsporing. Een dergelijke app moet gezien worden als een oplossing die complementair is aan manuele contactopsporing: beide oplossingen zijn nodig. Een app kan bijvoorbeeld geen contacten detecteren met burgers die de app niet gebruiken en het kan moeilijker zijn voor een app om sommige risico-contacten goed in te schatten. Ook beschermt de app de gebruiker niet direct tegen besmetting maar hij kan wel de verspreiding van het virus helpen afremmen.

Gedurende de voorbije maanden zijn een groot aantal technologische oplossingen voorgesteld voor contactopsporing. Deze oplossingen verschillen in gebruikte technologie, bescherming van privacy en veiligheidseigenschappen. Er is een consensus in de wetenschappelijke wereld dat de aanpak met het meeste kans op succes steunt op het gebruik van een smartphone app gebaseerd op Bluetooth (beschikbaar in 95% van de smartphones).

Het is van belang dat een contactopsporingsapp het vertrouwen geniet van de burger: dat betekent dat hij vrijwillig wordt gebruikt, niet onnodig persoonsgegevens verwerkt en enkel gebruikt kan worden om burgers na een risico-contact te waarschuwen en om hen aan te moedigen om zich te laten testen en/of in quarantaine te gaan. Burgers moeten ervan overtuigd kunnen zijn dat ze op geen enkele manier enig nadeel zullen ondervinden als gevolg van het gebruik van de contactopsporingsapp.

[1] De US CDC stelt dat « It may be possible that a person can get COVID-19 by touching a surface or object that has the virus on it and then touching their own mouth, nose, or possibly their eyes. This is not thought to be the main way the virus spreads, but we are still learning more about how this virus spreads. », https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html

KRITISCHE EISEN VOOR EEN APP

Een eerste vereiste is dat de app voldoende **nauwkeurig** is. Dit betekent dat de app enkel contacten van minstens 15 minuten op een afstand van 1,5 meter of minder registreert. Dit moet voldoende nauwkeurig gebeuren, d.w.z. met een optimale tradeoff tussen valse positieven (contact registreren die geen risico vormen) en valse negatieven (gemiste contacten). De nauwkeurigheid van de app kan verbeterd worden door de burger de mogelijkheid te bieden om bepaalde perioden (waarbij men bv. afgeschermd is door plexiglas) de app te deactiveren.

Een tweede eis is dat men **valse of incorrecte rapportering** van besmettingen kan vermijden: rapportering van een infectie kan enkel na een positief testresultaat of een vaststelling door een arts. Dat betekent dat men geen zelf-rapportering mag toelaten en dat een autorisatie nodig is om gegevens op te laden.

Een derde eis is **internationale interoperabiliteit:** men kan verwachten dat de grenzen in de EU opnieuw zullen openen. Het zou dan zeer nuttig zijn dat het Bluetooth deel van de app in een zo groot aantal mogelijk landen bruikbaar is en dat ook informatie over besmettingen tussen landen op anonieme wijze kan gedeeld worden.

Tot slot zijn er nog een aantal praktische vereisten. Om een praktische bijdrage te kunnen leveren moet de oplossing **schaalbaar** zijn naar miljoenen gebruikers (of zelfs honderden miljoenen gebruikers) en beschikbaar zijn binnen een **redelijke termijn** (5-6 weken). Op dit moment kan de Bluetooth op iOS[2] enkel maar effectief[3] gebruikt worden via de speciale interface voor contactopsporing (Exposure Notification API) die door Apple en Google ter beschikking is gesteld vanaf 20 mei 2020.

Tenslotte moet de app de **privacy van de gebruikers** waarborgen, wat betekent dat het ontwerp moet gebaseerd op “dat minimisatie” en “privacy by design”, zoals o.a. aangegeven in de aanbevelingen van de EDPB (European Data Protection Board)[4]. Dit moet worden afgetoetst in een Privacy Impact Assessment. Dit betekent onder meer dat:

- geen locatie-informatie mag gebruikt worden (dergelijke informatie kan enkel maar gepseudonimiseerd worden of geanonimiseerd worden door aggregatie, en aggregatie kan hier niet);
- er zo weinig mogelijk informatie wordt vrijgegeven over wie door wie besmet is, waar en wanneer, en er geen contactinformatie wordt vrijgegeven over wie niet besmet is;
- er zo weinig mogelijk informatie centraal opgeslagen wordt;
- het systeem uitgeschakeld kan worden en alle opgeslagen informatie verwijderd kan worden aan het einde van de epidemie;

[2] Marketaandeel van Apple smartphones in België is 30-35%.

[3] Zonder deze API kan een contactopsporingsapp op iOS maar werken als ze draait in de voorgrond en het scherm niet gelocked is; dit leidt tot een hoog batterijverbruik, is niet gebruiksvriendelijk en zelfs onveilig.

[4] https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en

- het niet mogelijk is om het systeem of de gegevens voor andere doeleinden te gebruiken (bv. sanctioneren wie de quarantaineregels niet gevolgd heeft).

Het gebruik van de app mag **niet verplicht** worden en mag zeker geen aanleiding geven tot discriminatie. Zelfs nadat een burger een positief testresultaat ontvangt, mag hij of zij beslissen om de app niet te gebruiken om andere burgers te verwittigen.

Er moet **maximale transparantie** nagestreefd worden zowel inzake de technologie als de genomen democratische waarborgen. Meer specifiek gaat het dan over de architectuur van het systeem en de werking van de app en backend. De broncode van de app en backend moeten vrij beschikbaar zijn (**open source**). Daarnaast moet het Data Protection Impact Assessment gepubliceerd worden. Tot slot moet er transparantie zijn over het beleidsproces achter de ontwikkeling en over de opvolging en evaluatie van het systeem.

De werking van het systeem moet op regelmatige basis **gemonitord, geëvalueerd** en **bijgesteld** worden door een interdisciplinair en onafhankelijk orgaan. Als zou blijken dat het systeem niet effectief is, moet het systeem gestopt worden.

Een contactopsporingsapp kan tenslotte maar succesvol zijn als het brede publiek voldoende **vertrouwen** heeft in de oplossing. De hierboven vermeldde voorwaarden zijn daarvoor essentieel.

Het is zeer moeilijk vooraf te bepalen welk percentage van gebruik nodig is: dit hangt af van het aantal besmettingen, maar ook of gebruikers geconcentreerd zitten in specifieke sociale netwerken (bv. grote ondernemingen of universiteiten).

INTERNATIONAAL EN EUROPEES KADER

Heel wat landen hebben een contactopsporingsapp ingevoerd of overwegen er één in te voeren. Grosso modo kan in de onderliggende technologie een onderscheid worden gemaakt tussen

- apps gebaseerd op locatiegegevens verkregen via GPS of GSM, waarbij het bewegingsgedrag van alle gebruikers in kaart wordt gebracht op een centrale server, die risicoberekeningen uitvoert;
- apps gebaseerd op het opsporen van de nabijheid van personen via Bluetooth, waarbij de anonieme sleutels worden opgeslagen op een centrale server, die de risicoberekeningen uitvoert (bv. PEPP-PT-NTK, Robert, DESIRE)
- apps gebaseerd op het opsporen van de nabijheid van personen via Bluetooth met een decentrale opslag van de anonieme sleutels zolang de persoon niet heeft gemeld dat hij is besmet (bv. DP-3T).

Onderscheiden organen van de Europese Unie hebben zich ook uitgesproken over contactopsporingsapps. Hierbij kan worden verwezen naar

- de Aanbeveling (EU) 2020/518 van de Commissie van 8 april 2020 over een gemeenschappelijke toolbox voor het gebruik van technologie en gegevens om de Covid19-crisis te bestrijden en te boven te komen, met name wat mobiele applicaties en het gebruik van geanonimiseerde mobiliteitsgegevens betreft;
- de gemeenschappelijke EU Toolbox voor de Lidstaten van het eHealth Network van 16 april 2020;

- de mededeling van de Commissie van 17 april 2020 inzake de Richtsnoeren in verband met gegevensbescherming voor apps ter ondersteuning van de bestrijding van de COVID-19-pandemie;
- de resolutie van het Europees parlement van 17 april 2020 over gecoördineerde EU-maatregelen ter bestrijding van de COVID-19-pandemie en de gevolgen ervan;
- de Guidelines 04/2020 van de European Data Protection Board van 21 april 2020 'on the use of location data and contact tracing tools in the context of the Covid-19 outbreak'
- de Interoperabilty Guidelines van het eHealth Network van 13 mei 2020.

Uit een analyse van de Europese documenten blijkt een absolute voorkeur voor apps gebaseerd op het opsporen van de nabijheid van personen via Bluetooth met een decentrale opslag van de anonieme sleutels zolang de persoon niet heeft gemeld dat hij is besmet, en gebaseerd op een wettelijk kader.

VOORGESTELDE TECHNISCHE OPLOSSING: DP-3T ARCHITECTUUR MET GOOGLE/APPLE AP

DP-3T[5] is een samenwerkingsverband van onderzoekers uit heel Europa die hun krachten hebben gebundeld om een open technische oplossing voor contactopsporing te creëren voor de COVID-19-epidemie die de privacy respecteert. De DP-3T oplossing voldoet aan de hogervermelde vereisten.

De meest recente open source implementatie steunt op de Google/Apple API[6]. De specifieke integratie met de gezondheidsinfrastructuur moet voor elk land afzonderlijk ontwikkeld worden; hiervoor zijn ook modellen voorzien. Meer details zijn beschreven in Appendix 1.

Het DP-3T consortium ligt aan de basis van de app die in Zwitserland zal gebruikt worden.[7] Inmiddels hebben 21 andere landen of staten besloten om een oplossing gebaseerd op de Google/Apple API te kiezen, wat de mogelijkheid biedt tot interoperabiliteit; tot deze lijst behoren Denemarken, Duitsland, Estland, Finland, Ierland, Italië, Letland, Nederland, Oostenrijk en Spanje.

De DP-3T oplossing is **gedecentraliseerd**, wat betekent dat informatie over contacten lokaal op de smartphone bewaard blijven en de beslissing of de burger een risico loopt op de smartphone zelf genomen wordt. Er is een centraal register dat enkel willekeurige sleutels en een geldigheidsperiode bevat. Het gebruik van een gedecentraliseerde architectuur is een noodzakelijke voorwaarde om toegang te krijgen tot de Google/Apple API.

Hieronder wordt op de oplossing bondig beschreven.

[5] https://github.com/DP-3T/documents

[6] Application Programming Interface: definieert de interacties tussen meerdere software componenten.

[7] Testfaze van de rollout is begonnen op 25 mei 2020.

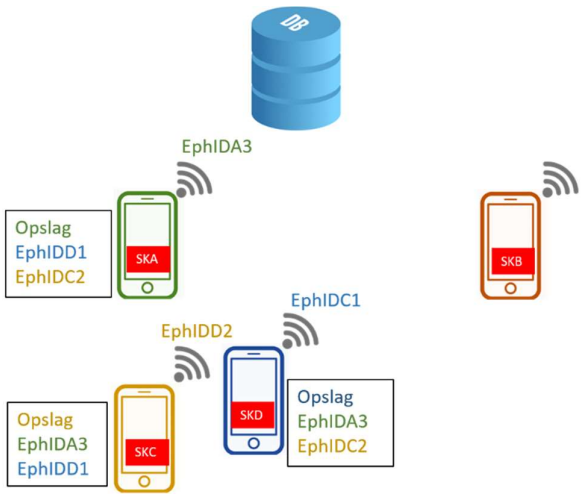
INSTALLATIE

De burgers installeren de app in de Google of Apple appstore[8]. De app genereert elke dag een geheime sleutel. Op basis van deze sleutels worden dan Bluetooth tokens (random getallen van 128 bits) gegenereerd.

Figuur 1 Installatie

WERKING

Op geregelde basis stuurt elke smartphone met de contactopsporingsapp een Bluetooth token uit in broadcast mode. Elke 10-20 minuten wordt een ander token uitgestuurd om te beletten dat deze tokens kunnen gebruikt worden om een gebruiker te volgen. Deze tokens kunnen worden opgevangen door elke smartphone in de buurt. Elke smartphone met de contactopsporingsapp luistert ook of het Bluetooth tokens hoort (gedurende 4 seconden elke 5 minuten). In dat geval slaat het dit token op, samen met de dag en de signaalsterkte. Deze tokens worden bewaard gedurende 14 dagen en dan verwijderd.

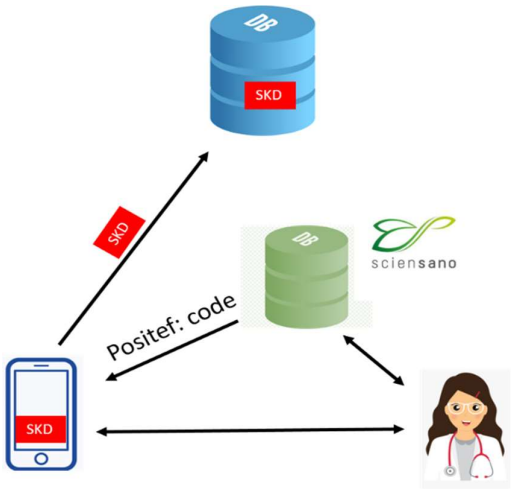


Figuur 2 : werking

[8] 97% van de smartphones in België gebruikt Android of iOS als besturingssysteem.

BESMETTING

Als een burger symptomen heeft, laat hij zich testen bij een arts. Hierbij deelt de burger zijn INSZ[9] en zijn mobiel nummer mee aan de arts. Ook wordt de datum vastgesteld van wanneer hij besmettelijk was. Als het testresultaat positief is, wordt de burger gecontacteerd en krijgt hij een autorisatietoken. Met behulp van dit autorisatietoken laadt de burger de geheime sleutels van de besmettelijke dagen met de bijhorende data op in een centrale database (de loglijst). Deze sleutels worden na 14 dagen uit deze database verwijderd. Aangezien de burger in quarantaine moet gaan zolang hij besmettelijk is, moet de app na het opladen van de sleutels verwijderd worden, zodat er geen nieuwe risico's meer kunnen worden gedetecteerd.



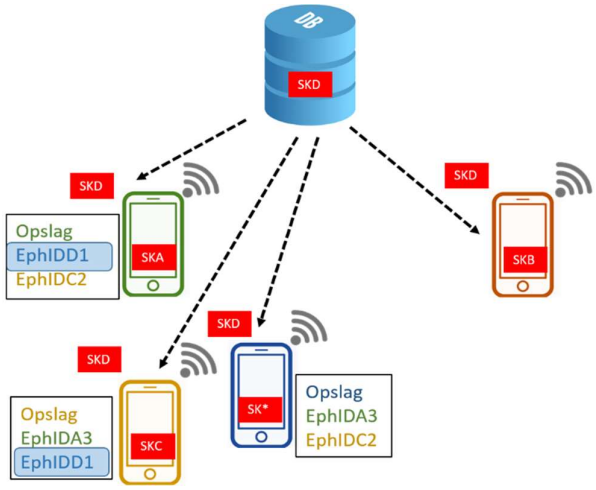
Figuur 3 Testen

OPSPOREN CONTACTEN

Op geregelde tijdstippen contacteert de app de centrale database en downloadt de app de sleutels en de bijhorende besmettelijke dagen van alle besmette gebruikers. Hiermee kan de app nagaan of de smartphone in de voorbije 14 dagen voldoende lang en voldoende dicht bij een besmet persoon is geweest. Als de app een risico detecteert, informeert de app de gebruiker over de aanbevolen acties

[9] IdentificatieNummer Sociale Zekerheid

(quarantaine, contact met huisarts, …). Merk op: deze notificatie gebeurt niet in real-time, omdat dit de privacy van de besmette persoon zou schenden.



Figuur 4 Opsporen contacten

STOPZETTEN SYSTEEM

Als er geen besmettingen meer zijn, worden er geen nieuwe sleutels opgeladen in de centrale database. Aangezien sleutels na 14 dagen verwijderd worden, zal deze database 14 dagen na de laatste besmetting automatisch leeg zijn. Als het einde van de epidemie wordt vastgesteld, kunnen de servers ontmanteld worden en zullen Google en Apple de API niet langer ondersteunen. De gebruikers zullen op dat moment gevraagd worden om de app te verwijderen.

JURIDISCH KADER

Een juridisch kader voor een contactopsporingsapp overeenkomstig de hogervermelde architectuur is uitgewerkt en voorgelegd aan het advies van de Gegevensbeschermingsautoriteit. Het ligt voor in de Belgische Kamer van Volksvertegenwoordigers in de vorm van een wetsvoorstel betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking[10]. Het is in overeenstemming met de hogervermelde Europese aanbevelingen. In dat kader wordt voorgesteld om de gegevensbank met de anonieme sleutels van besmette personen te laten beheren door Sciensano.

PLANNING EN BUDGETTEN

PLANNING

Een **contactopsporingsapp** en de bijbehorende **serverinfrastructuur** kan beschikbaar zijn binnen 5-6 weken na het nemen van de beslissing. In een eerste fase moeten de specificaties gefinaliseerd worden

[10] https://www.dekamer.be/FLWB/PDF/55/1251/55K1251001.pdf

(voornamelijk interface met gezondheidsinfrastructuur), gevolgd door ontwikkeling van de eindgebruikersapp en de installatie van de serverinfrastructuur. Bij de ontwikkeling van de eindgebruikersapp kan maximaal gebruikt worden van open source apps die vandaag reeds bestaan in andere landen. Hiervoor zal beroep worden gedaan op gespecialiseerde ontwikkelaars aangetrokken op basis van een overheidsopdracht uitgeschreven in gemeenschappelijk overleg tussen de onderscheiden overheidsniveaus of op basis van een reeds bestaande raamovereenkomst afgesloten op basis van een vroegere overheidsopdracht.

Na een functionele en security review kan een lokale test gebeuren (met een duizendtal gebruikers) gevolgd door de roll-out. In parallel moet ook met EU-partners worden samengewerkt aan afspraken en interfaces voor interoperabiliteit.

Tegelijk kan er gewerkt worden aan de **contractuele en juridische** aspecten en de **processen en interfaces** voor testers en voor de beheerder Sciensano, aan de draaiboeken voor testen, en aan de processen voor monitoring en audit.

Om de aanvaardbaarheid van de app bij de bevolking te maximaliseren is het van belang om zo **transparant** mogelijk te zijn gedurende alle stappen van de uitrol. Een belangrijk element hierbij is parallel met de ontwikkeling een publieke consultatie te organiseren. Een ethische commissie kan worden ingesteld om het gebruik van de app mee op te volgen.

BUDGET

Er is al heel wat open source code beschikbaar voor de app (SDK, Google/Apple API) die de ontwikkeling van de app gevoelig kan versnellen. Ook bij de serve infrastructuur kan ten dele gesteund worden op de beschikbare code, maar hier zal meer integratie nodig zijn. De totale ontwikkelingskost (m.i.v. security audit) wordt geschat op 350 kEUR en de operationele uitgaven (beheer van software, servers) op 40 kEUR/maand. Het toevoegen van interoperabiliteit op Europees niveau zou een meerkost van ongeveer 25% vragen.

De publieke consultatie moet uitgevoerd worden door een organisatie met ervaring in dit domein; dit vraagt een beperkt budget (20 kEUR). Er is ook voldoende budget nodig voor communicatie: het is van essentieel belang om de boodschap goed te definiëren en om de juiste partners te vinden om de app bij het bredere publiek ingang te doen vinden. Ook moet gedacht worden aan crisiscommunicatie om effectief op te kunnen treden bij mogelijke incidenten. Dit wordt bij voorkeur gedaan door een extern communicatiebureau.

KRITISCHE SUCCESFACTOREN

VERTROUWEN VAN HET BREDE PUBLIEK

De waarde van de app moet **correct gepositioneerd** worden: het gebruik van de app helpt in eerste instantie de hele maatschappij sneller uit de lockdown te komen (of een nieuwe lockdown te vermijden) en helpt de gebruiker zelf maar in tweede orde (laat toe om een besmettingsrisico sneller vast te stellen en vermijdt een manuele contactopsporing). Het gebruik is een teken van burgerzin en

solidariteit: als je besmet raakt laat het toe om de mensen waarmee je in contact bent geweest te waarschuwen en de verdere verspreiding van het virus tegen te gaan.

De app is volledig **vrijwillig:** op geen enkele manier mag de app gebruikt worden om mensen te verplichten om het te gebruiken bv. om naar het werk of naar school te gaan, en essentiële goederen of diensten mogen niet ontzegd worden als men de app niet gebruikt.

Er dient een duidelijk **juridisch kader** te zijn dat rechten van burger beschermt en genoeg **democratische waarborgen** voorziet. De app mag niet worden gezien als een tool waarmee de overheid of Google/Apple kunnen spioneren, dus minimale dataverzameling, geen integratie met bestaande databases, geen 'function creep' mogelijk en niet resulterend in discriminatie of toegenomen ongelijkheid in de samenleving.

De app zal **niet langer gebruikt worden dan nodig** en als de app niet effectief zou blijken, zal de infrastructuur ontmanteld worden en zal aan de burgers gevraagd worden om de app te verwijderen.

Essentieel voor het vertrouwen zijn een duidelijke **communicatie** over deze elementen aan de bevolking, samen met een volledige **transparantie** in combinatie met **toezicht** door een ethische commissie op het gebruik van de app.

TECHNOLOGIE EN GEBRUIK

De app moet voldoen aan hoge kwaliteitseisen: eenvoudig te installeren en gebruiken, beperkt batterijverbruik.

De serverinfrastructuur moet voldoen aan hoge kwaliteitseisen: goede performantie, bestand tegen aanvallen. De infrastructuur moet zo snel mogelijk interoperabel gemaakt worden met de infrastructuur in het buitenland.

De app en de serverinfrastructuur moeten zo weinig mogelijke informatie vrijgeven over wie besmet is en door wie en wanneer men mogelijk besmet is.

Integratie met gezondheidsinfrastructuur: minimale overhead bij aanvragen van test, resultaten van een test kunnen eenvoudig aan de app worden meegedeeld.

Communicatie over mogelijke besmetting: duidelijke communicatie over implicaties van risico's en wat de burger moet doen (contacteren huisarts, test, quarantaine).

MEDISCH

Het aantal nieuwe besmettingen per dag mag niet te hoog liggen.

Er moeten voldoende testen beschikbaar zijn en de testresultaten moeten zo snel mogelijk beschikbaar zijn (idealiter binnen de 24u).

MOGELIJKE UITBREIDINGEN

Kwetsbare groepen in de samenleving beschikken niet over een smartphone. Een contactopsporingsapp laat toe om de epidemie te vertragen en sneller uit de lockdown te komen; daardoor heeft ze in eerste orde een positief effect op de gehele bevolking (dus ook op gebruikers zonder smartphone). Het risico bestaat echter dat het besmettingsrisico veel minder of zelfs niet vertraagd zou worden binnen een aantal kwetsbare groepen, waardoor de app de ongelijkheid kan vergroten en een cumulatief nadeel kan creëren voor die groepen. Een mogelijk oplossing is om een klein draagbaar Bluetooth toestel te ontwikkelen met een vergelijkbare functionaliteit – de kostprijs van zo een toestel met een batterijlevensduur van 1 jaar wordt geschat op 5-7 EUR en de ontwikkeltijd zou 2-3 maanden bedragen. Hiervoor zou best op Europees niveau samengewerkt worden.

De app zou ook via opt-in bijkomende informatie voor epidemiologisch onderzoek kunnen verzamelen. Omdat het gaat over de contactgraaf en niet de sociale graaf en omdat er geen locatie informatie beschikbaar is, denken epidemiologen dat het nut hiervan beperkt is. Anderzijds zou dit een bijkomende server vragen en zou dit – ondanks het opt-in karakter – wantrouwen kunnen opwekken bij de burger. De meeste Europese landen die gekozen hebben voor de DP-3T architectuur hebben besloten om die informatie in eerste instantie niet te verzamelen. Dit is een uitbreiding die kan overwogen worden in een tweede fase.

APPENDIX 1 STRUCTUUR VAN DE VOORGESTELDE CONTACTOPSPORINGSAPP

Deze appendix legt kort uit hoe de contactopsporingsapp is opgebouwd uit bestaande en nieuwe elementen.

GOOGLE/APPLE EXPOSURE NOTIFICATION API (APPLICATION PROGRAMMING INTERFACE)

De kern van de app is een softwarecomponent die ontwikkeld is door Google en Apple en die beschikbaar wordt gesteld voor Android (versie 6.0 en hoger) en iOS (13.5). Het gaat om een component die de geheime sleutels genereert, de Bluetooth tokens genereert en uitstuurt, de Bluetooth tokens ontvangt en deze opslaat samen met de signaalsterkte (RSSI) en de datum. Via een API kunnen deze gegevens opgevraagd worden. Later in 2020 zal deze API ingebouwd worden in Android en ioS als de BLE[11] Contact Detection Service.

DP-3T SDK (SOFTWARE DEVELOPMENT KIT)

Het DP-3T consortium heeft een SDK ontwikkeld die steunt op de Google/Apple API. Deze SDK biedt de volgende functies aan.

- Bepalen van besmettingsrisico: op geregelde basis worden de sleutels en bijhorende data van besmette gebruikers bij de centrale server opgehaald (samen met de parameters van het beslissingsalgoritme). Daarna worden de gegevens over contacten (Bluetooth token, datum, signaalsterkte) opgevraagd via de Google/Apple API. Op basis hiervan wordt nagegaan of de gebruiker een risicocontact gehad heeft in de voorbije periode. Indien ja, zal de gebruiker verwittigd worden.
- Aangeven van een positief testresultaat: in dat geval zal de gezondheidsdienst een autorisatietoken sturen; met behulp van dit token kunnen de sleutels van de gebruiker worden opgeladen in de centrale database.

Steunend op deze SDK heeft het DP-3T consortium[12] een volledige app met gebruikersinterface gebouwd. Op basis hiervan is de Zwitserse contactopsporingsapp ontwikkeld, die geïntegreerd is met de Zwitserse gezondheidsinfrastructuur. Zowel de SDK als de Zwitserse app zijn in open source beschikbaar.

Daarnaast heeft het DP-3T consortium software ontwikkeld voor de serverinfrastructuur en de code hiervan in open source ter beschikking gesteld. Er zijn ook gedetailleerde studies beschikbaar over autorisatiemechanismen en interoperabiliteit. De Zwitserse serverinfrastructuur is ontwikkeld door de Zwitserse overheid.

In samenwerking met het DP-3T consortium zijn Estland en Finland aan een eigen app en serverinfrastructuur aan het werken (steunend op de DP-3T SDK). Deze landen zullen hun code ook

[11] Bluetooth Low Energy
[12] https://github.com/DP-3T/

publiceren. Duitsland is een eigen app en infrastructuur aan het bouwen enkel vertrekkend van de Google/Apple API en zal de code ook publiceren.

Het ontwikkelen van een Belgische app kan steunen op de inspanningen van Google en Apple, het DP-3T consortium en de voorbeelden van Zwitserland, Estland en Finland. De enige aanpassingen die moeten gebeuren zijn de autorisatieberichten (hoe krijgt een app toestemming om de sleutel op te laden na een positieve test) en de gebruikersinterface (wat te doen bij een vastgesteld risico, vertaling). Aan de kant van de serverinfrastructuur moeten er aanpassingen gebeuren bij Sciensano (communicatie na positieve test).

Ook zijn er nog inspanningen nodig om de interoperabiliteit te realiseren: dit vraagt het maken van internationale afspraken en het implementeren van de gemaakte keuzes. Ook moet de app weten welke landen of regio's er bezocht zijn.

Merk op dat Google ter illustratie een app gepubliceerd heeft zonder integratie met een specifieke gezondheidsautoriteit; het is niet duidelijk of deze app nog verder ontwikkeld of ondersteund zal worden.