INFORME

Anàlisi internacional d'aplicacions de rastreig de contactes en el context de la pandèmia de COVID-19

VERSIÓ	2.0
ESTAT	Versió final
DATA	18/01/2021
NOM DOCUMENT	Anàlisi internacional d'aplicacions de rastreig de contactes en el context de la pandèmia de COVID-19
TIPUS DOCUMENT	Informe
NIVELL DISSEMINACIÓ	Públic

Contingut

1.Glossari de termes

API: *Application Programming Interface*. Es tracta d'una interfície de programació que permet la interacció d'usuaris amb un servei d'una companyia, un hardware específic o un servidor (back-end). Es comporta com una caixa negra: no cal saber com funciona internament i el sistema està protegit contra usos malintencionats. En un context de servidors, l'API permetria la interacció amb el back-end.

APP: Referit a aplicacions mòbils dels sistemes operatius iOS i Android. Les aplicacions són les que poden utilitzar APIs per realitzar els seus objectius. En el context del Contact Tracing cada país pot desenvolupar una aplicació, i amb el permís de Google i Apple, acreditant-se com autoritat sanitària d'aquell país, podrien utilitzar la seva API per obtenir la informació que necessiten sobre els contactes detectats per Bluetooth. En aquest cas, l'APP depèn de la transparència de l'API per conèixer més detalls sobre aquests contactes.

Back-end: El back-end és el nom que rep l'estructura d'una aplicació o programari relacionada amb servidors, gestió de dades i computació. Es defineix en combinació a un altre concepte: el front-end. El front-end és la part d'una aplicació o programari amb la qual un usuari de perfil general té contacte. El back-end actua de fons, sense que l'usuari hi pugui tenir cap intervenció, a vegades com una caixa negra. Usualment els desenvolupadors ofereixen una API que permet la interacció entre l'aplicació i els serveis de back-end.

Beacon: Missatges que envien els telèfons mòbils a través de BLE a mode de notificació. Aquests missatges no tenen un destinatari concret: s'utilitzen per descobrir-se entre ells o per oferir un servei.

BLE: *Bluetooth Low Energy* és una tecnologia Bluetooth enfocada en l'estalvi d'energia i àmpliament utilitzada per els telèfons mòbil i dispositius wearables. Està suportada a partir de la versió 4.0 de Bluetooth (2010). Aquesta tecnologia permet l'enviament de beacons per al descobriment de dispositius propers sense el cost d'establir una connexió i és la base de les solucions de detecció de contactes (Contact Tracing) implementades en telèfons mòbils.

Claus d'exposició temporal (TEK, *Temporal Exposure Key*): Aquesta explicació és vàlida en el context de la utilització de GAEN. El TEK és un identificador aleatoris que s'utilitza per identificar un usuari i que es renova diàriament. A partir d'aquesta clau, es generen els identificadors pseudoaleatoris (RPI) que es publiquen per BLE i que canvien cada 15 minuts.

Claus de diagnosi: En el context GAEN, quan una persona és diagnosticada com a positiva en COVID-19, les claus d'exposició temporal (TEK) d'aquell dia i dels últims 14 dies associades al seu usuari passen a dir-se claus de diagnosi, i es comparteixen, amb el permís de l'usuari, amb el back-end.

Codi QR: *Quick Response (QR)* és un codi de barres de dues dimensions. Es pot utilitzar la càmera del telèfon mòbil i una aplicació per interpretar-ho.

Contact Tracing: S'utilitza l'anglicisme Contact Tracing per referir-se al traçament de contactes.

Distància de risc: Aquesta és la distància a partir de la qual les autoritats epidemiològiques de cada país defineixen que existeix un risc elevat de contagi.

DP-3T: *Decentralized Privacy-Preserving Proximity Tracing* és un protocol dissenyat per simplificar i accelerar el procés d'identificació de persones que han estat en contacte amb una persona infectada assegurant la privacitat dels usuaris. El disseny d'aquest protocol s'ha dut a terme per un consorci internacional de tecnòlegs, experts en lleis, enginyers i epidemiòlegs.

GAEN: *Google Apple Exposure Notification [21] [22]* és el nom que rep formalment l'API de Google i Apple. El servei que han posat disponible en els sistemes operatius de iOS i Android s'anomena *Exposure Notification* i, combinat amb les aplicacions de Contact Tracing, proporciona informació sobre el risc d'exposició que ha tingut un usuari al llarg dels últims dies.

GUID: *Globally Unique IDentifier* o també *Universally Unique IDentifier* (UUID) és un identificador de 128 bits (32 dígits hexadecimals) generat aleatòriament amb un algoritme que assegura amb una alta probabilitat de que l'UUID generat és únic universalment.

Identificador Aleatori: Quan es parla d'un identificador aleatori, es fa referència a una seqüència de dígits generada de manera totalment aleatòria.

Identificador Pseudoaleatori: Quan es parla d'un identificador pseudoaleatori, es fa referència a una seqüència de dígits generada aleatòriament a partir d'un valor de referència, que pot fer-se servir per recuperar la seqüència.

Identificador/pseudònim efímer (RPI, *Rolling Proximity Identifier*): En el context GAEN, els RPI són els pseudònims efímers (identificadors pseudoaleatoris) que es deriven de les claus d'exposició temporal (TEK) i que varien cada 15 minuts. Aquests són els que s'envien per BLE i que s'emmagatzemen als telèfons mòbils per registrar els contactes. Amb la clau original (TEK) és possible recuperar tots els identificadors RPI que s'hagin generat a partir d'ella. Aquesta clau no conté informació sobre la identitat de l'usuari.

OPSEC: Seguretat operativa. Procés i conjunt de tècniques que permeten analitzar la informació i identificar vulnerabilitats o riscos. La finalitat és trobar mesures per protegir la informació i prevenir davant de possibles amenaces.

PEPP-PT: *Pan-European Privacy-Preserving Proximity Tracing* és una iniciativa europea per definir les bases d'una solució comuna de traçabilitat de contactes que asseguri la privacitat dels usuaris. Es tracta d'una proposta alternativa al DP-3T que s'enfoca en l'ús d'un model centralitzat.

ROBERT: *ROBust and privacy-presERving proximity tracing protocol* [19] és un protocol que implementa el PEPP-PT. El protocol està desenvolupat conjuntament pels centres *Inria* i Fraunhofer AISEC (*Applied and Integrated SECurity*). És la base de l'aplicació de Contact Tracing francesa. Aquest seria un protocol alternatiu al protocol GAEN.

Temps de contacte: El temps de contacte està definit per les autoritats epidemiològiques de cada país i consisteix en el temps mantingut en contacte proper a partir del qual el risc d'haver-se contagiat és elevat.

Trilateració: És un mètode matemàtic per determinar la posició d'un objecte en relació a una espai de referència conegut. S'utilitza la localització dels punts de referència i la distància mesurada entre l'objecte a localitzar i cada punt de referència.

UWB: Ultra Wide Band. Reben aquest nom les tecnologies que fan ús d'un espectre molt ample (de més de 100MHz). Com a resultat d'utilitzar espectres tan amples es poden manegar senyals temporals molt curtes que son aptes per la mesura de temps de propagació del senyal radio.

2.Introducció

Arrel de la pandèmia decretada pel SARS-CoV-2, molts dels estats han enfocat part dels seus esforços en trobar eines digitals que els permetin afrontar de forma més eficient la pandèmia de COVID-19 i utilitzar aquestes eines per reduir la propagació de la malaltia. A banda de les Apps informatives, la veritable revolució durant aquesta pandèmia han estat les aplicacions que permeten als governs obtenir dades precises sobre les zones de contagi o sobre les persones que han tingut contacte amb persones infectades.

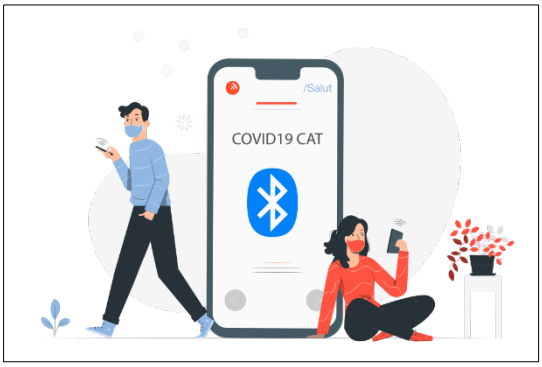
La Fundació TIC Salut i Social, juntament amb la Fundació i2cat, i per encàrrec del Departament de Salut, ha analitzat les aplicacions desenvolupades per diferents governs internacionals que tenen com a principal objectiu realitzar el rastreig de contactes (*Contact Tracing Mobile Applications*) de COVID-19 a través del telèfon mòbil i notificar al usuari si ha estat en contacte amb persones exposades a la malaltia. L'objectiu d'aquestes aplicacions és identificar nous riscos de contagi que permetin aplicar les mesures adients per tal d'interrompre la propagació de la malaltia i, d'aquesta, manera fer front a la situació actual.

3.Objectiu

L'anàlisi efectuada ha consistit en realitzar una revisió de les aplicacions i eines digitals posades al mercat en els últims mesos per diferents governs internacionals per tal d'abordar la traçabilitat de contactes diagnosticats amb COVID-19. La finalitat del projecte és presentar un seguit de recomanacions i aspectes a tenir en compte a l'hora de desenvolupar una aplicació d'aquestes característiques que permeti fer front a la pandèmia de COVID-19 desencadenada en els darreres mesos.

Aquesta anàlisi permetrà tenir una visió global i general de quina és la tendència que estan tenint els diferents governs a l'hora d'apostar per aquestes tecnologies i saber com són adoptades en els seus territoris. Apartats com la privacitat de les dades, la seguretat, la usabilitat i la interoperabilitat entre d'altres, són alguns dels aspectes rellevants que s'han revisat en el desenvolupament de la present anàlisi.

Objectiu de les aplicacions de rastreig de contactes



El rastreig de contactes permet detectar els **contactes no coneguts** d'un usuari que voluntàriament desitja fer ús d'aquest tipus d'aplicacions. L'aplicació **registra** aquests contactes mitjançant uns identificadors pseudonimitzats. Aquests identificadors es guarden durant **14 dies** i en el cas de detectar algun contacte diagnosticat de COVID-19, el telèfon realitza un avís al usuari indicant el **nivell de risc** al qual ha estat exposat.

4.Metodologia

La metodologia que s'ha seguit en el desenvolupament de la anàlisi ha estat la següent:

En primer lloc, s'ha realitzat una revisió complerta de les **aplicacions existents** en els diferents països i regions, per tal de veure quines són les principals funcionalitats que incorporen, les característiques tecnològiques i els protocols que utilitzen, entre d'altres.

A continuació, s'ha analitzat de forma experimental el funcionament de la **tecnologia Bluetooth Low Energy (BLE)** que fan servir les aplicacions a l'hora de traçar el possible contacte entre usuaris. D'aquesta manera es pot estimar la distància entre dos telèfons mòbils sense necessitat de conèixer la posició absoluta (geolocalització) dels mateixos. Per a evitar que es pugui identificar o traçar als usuaris, es fan servir identificadors generats de forma pseudoaleatòria que van canviant cada poc temps.

Per altra banda, s'ha realitzat una anàlisi complerta dels protocols utilitzats en aquest tipus d'aplicacions, com **l'API de Google i Apple** i el protocol Robert, entre d'altres.

Paral·lelament, s'han analitzat els dictàmens i informes procedents de les autoritats de protecció de dades dels diferents estats membres, com la d'Itàlia i Alemanya, així com la documentació publicada per el Comitè Europeu de Protecció de dades i el Supervisor Europeu de Protecció de dades.

Finalment, s'han analitzat les especificacions tècniques necessàries per tal d'assegurar la **interoperabilitat** entre les aplicacions de traçabilitat de contactes existents a diferents països. Aquest és un aspecte clau per aconseguir un èxit clar en el desenvolupament d'aquest tipus de tecnologies, ja que els ciutadans que les utilitzaran es mouran dins dels estats i l'aplicació caldrà que continuï transmeten la informació de manera fiable i consistent garantint la correcta interpretació de les dades recollides.

5.Circuit funcional de les aplicacions de rastreig de contactes

Un dels objectius d'aquestes aplicacions és preservar la salut pública dels ciutadans sense renunciar a perdre la seva privacitat. Les aplicacions segueixen patrons similars, i la majoria d'elles disposen de tres moments clau: I) ***Activació del Bluetooth*** en el dispositiu mòbil per iniciar el rastreig de contactes; II) ***Reportar els diagnòstics positius*** a través d'identificadors pseudoanimitzats i; III) ***Notificar a un usuari*** del nivell de risc al que ha estat exposat.

El circuit funcional d'aquestes aplicacions segueix quatre punts elementals, com es pot apreciar a la ***Figura 1***:

1. Establir la **configuració inicial** d'acceptació de condicions (Set-up).
2. **Habilitar la funcionalitat** de rastreig de contactes activant el Bluetooth.
3. **Registre i verificació de les proves** de test realitzades per identificar els casos positius.
4. **Notificació del nivell de risc** al qual ha estat exposat el usuari.

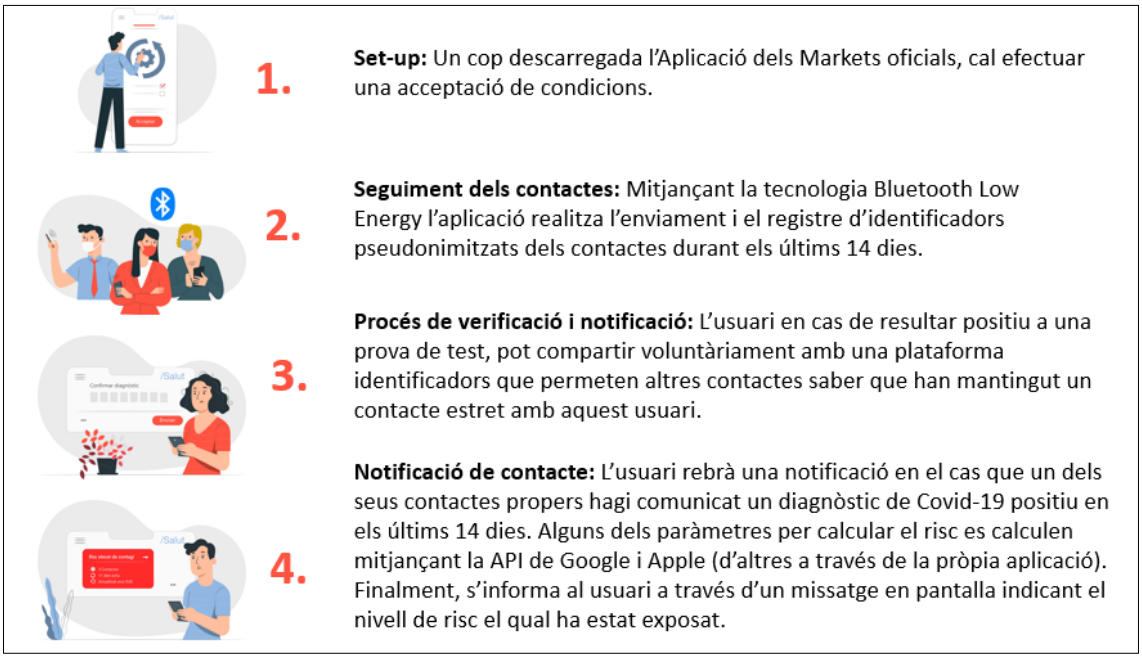


Figura 1. Circuit funcional que segueixen les aplicacions de rastreig de contactes

6.Aplicacions que s'han desenvolupat a nivell mundial per fer front a la pandèmia de COVID-19

Durant les darreres setmanes s'han revisat les aplicacions següents desenvolupades en diferents governs (Itàlia, Alemanya, Letònia, França, Regne Unit, Irlanda, Noruega, Singapur, Suïssa i Austràlia, entre d'altres). El detall complert de les funcionalitats, el protocol utilitzat i el model que segueixen aquest tipus d'aplicacions es pot consultar a *l'**Annex I*** del present document.

A mode de resum s'ha dissenyat la ***Taula 1*** per explicar millor les principals diferències i aspectes rellevants de cadascuna de les aplicacions més destacables analitzades.

Com es pot observar a la taula, aplicacions com **Immuni**, del govern italià o **Corona Warn-App** del govern alemany, segueixen patrons de funcionament similars, integrades amb l'API de Google&Apple. En ambdós casos, fan servir un model descentralitzat on la major part de la informació (tals com l'identificador dels contactes, el temps de contacte i les estimacions de proximitat) queda emmagatzemada al telèfon mòbil de l'usuari durant un temps limitat. Únicament en el cas de trobar un usuari positiu en COVID-19, aquest enviarà, a través de l'aplicació i de forma voluntària, els identificadors BLE que hagi fet servir durant els últims dies al servidor. El servidor és l'encarregat de compartir aquestes dades amb la resta d'usuaris; de forma que l'aplicació als seus mòbils pugui determinar si són contactes de risc o no. Per tant, el model de decisió del risc de contagi s'executa al propi terminal de l'usuari.

D'altres aplicacions, com l'App francesa, **Stop Covid**, segueixen models totalment diferents pel que fa al registre de dades, seguint un model centralitzat i aplicant el protocol Robert. En aquest cas, un usuari que doni positiu en COVID-19 pujaria al seu terminal tota la informació que ha

recollit sobre possibles contactes en els últims dies (identificadors, temps de contacte i estimació de proximitat). El servidor serà el que aplicarà el model de decisió de risc de contagi i el que s'encarregarà de notificar als usuaris en risc.

Altres governs com el del **Regne Unit** i el de **Noruega** han hagut de retirar les seves aplicacions del mercat, degut a problemes tecnològics o bé per no compliment de la normativa de protecció de dades dels usuaris. Entitats com Amnistia Internacional posen en dubte algunes d'aquestes aplicacions per la utilització de models que no garanteixen els drets i llibertats de les persones. Segons la revista Life in Norway, l'App noruega va ser retirada per generar un consum elevat de la bateria dels terminals i per la facilitat amb la que es podien falsificar els missatges SMS d'alerta.

Durant l'anàlisi efectuada cal destacar l'aplicació d'Alemanya, **Corona-Warn-App**, entre la resta per està dissenyada preservant la privacitat dels usuaris amb aspectes a destacar com: processar les dades mínimes possibles, no identificar l'usuari ni fer perfilatge del mateix, no recollir cap dada que permeti inferir la identitat de l'usuari, el seu estat de salut o geolocalitzar-lo i abstenir-se expressament d'usar sistemes de rastreig que permetin saber com utilitza l'usuari l'App. Així com per disposar d'un bon circuit funcional per establir els càlculs de risc de contagi, mantenint una bona experiència d'usuari a l'hora de transmetre la informació cap al ciutadà. Per aquest motiu s'ha aprofundit en l'estudi del mètode de càlcul de risc de l'aplicació, així com en l'arquitectura en què està constituïda. A l'***Annex II***, es pot trobar el detall de com realitza el càlcul de risc de contagi i el detall de l'arquitectura de l'aplicació alemanya.

App	Immuni	Corona-Warn-App	Stop Covid	Apturi Covid	SwissCovid	TraceTogether
País	**Itàlia**	**Alemanya**	**França**	**Letònia**	**Suïssa**	**Singapur**
Model	Descentralitzat	Descentralitzat	Centralitzat	Descentralitzat	Descentralitzat	Centralitzat
Descàrrega ***Android***	+1M*	+5M*	+1M*	+50K*	500K*	+1M*
Publicada	Publicada	Publicada	Publicada	Publicada	Publicada	Publicada
Protocol	API Google&Apple	API Google&Apple	ROBERT	API Google&Apple	API Google&Apple	Bluetrace
Beacons enviats[1]	200 per minut	200 per minut	480 per minut	200 per minut	No avaluat	No avaluat
Identificadors	Vàlids cada 15 minuts	Vàlids cada 15 minuts	Vàlids cada 15 minuts	Vàlids cada 15 minuts	Vàlids cada 15 minuts	Vàlids cada 15 minuts
Distància de risc	< 2 metres	< 1.5 metres	< 1 metre	< 2 metres	1.5 metres	< 2 metres
Avaluació d'impacte	SI. Amb el OK de l'autoritat de PD previ consideracions	SI. L'autoritat de PD assumeix la supervisió del funcionament	SI. Amb el OK de l'autoritat de PD previ consideracions	No trobada avaluació d'impacte. Només hi ha el Ok de l'autoritat de PD	No trobada avaluació d'impacte. Només prova de seguretat Centre Nacional de Ciberseguretat (NCSC)	No trobada
Funcionalitats destacades	No identifica l'usuari Recull dades analítiques	No identifica l'usuari Codi QR per registre de prova i call center	Pseudònim temporal Codi QR per registre i amb identitat de la persona. Recull dades estadístiques	No identifica l'usuari Codi únic per compartir id de contacte. I transfereix el tfn a l'autoritat perquè contacti amb el contacte.	No identifica l'usuari Al introduir el codi, en ser positiu, l'aplicació notifica automàticament a altres usuaris. Es comparteix la data de quan has sigut contacte.	No identifica l'usuari Recull dades analítiques

Taula 1. Taula resum de les aplicacions de rastreig de contactes més destacades que s'han revisat. (*Data actualització taula: 27 de Juliol de 2020*)

[1] Basat en els missatges rebuts a curta distància a un sol canal fent servir un sniffer BLE. Els beacons s'envien per tres canals BLE. Un alt número de missatges pot repercutir amb un consum més elevat de la bateria del dispositiu mòbil.

7.Marc Tecnològic

7.1. Mètodes de detecció a l'exposició al risc de contagi

La detecció a l'exposició al risc de contagi dependrà de la solució de rastreig de contactes que s'implementi. En termes generals, es fan servir les aplicacions mòbils i la tecnologia Bluetooth per detectar la proximitat entre contactes. Per exemple, en el cas del protocol de Google i Apple, cada usuari utilitza una clau d'exposició temporal per generar i publicar uns identificadors pseudoaleatoris. Aquests identificadors són substituïts cada 15 minuts per millorar la privacitat del usuari. Al mateix temps, tots els usuaris poden rebre missatges (tot i que en unes finestres temporals més petites) i emmagatzemen els identificadors que escolten.

Per altra banda, els usuaris que es realitzen un prova de test i resulten positius en COVID-19, poden decidir indicar-ho al sistema i pujar la seva informació per a permetre la identificació dels possibles contactes de risc. Per tal d'evitar falsos positius, cal realitzar un procés de verificació de les dades. La forma de verificació i el mode en que els usuaris són notificats com a positius variarà segons la solució. Per exemple, en el cas de l'aplicació alemanya s'incorpora un sistema de notificació i verificació basat en codis QR i, de forma alternativa, un sistema de notificació telefònica. En aquest cas, l'usuari positiu rebria un codi per pujar les seves claus d'exposició (també anomenades claus de diagnòstic) dels últims 14 dies al servidor de l'aplicació. Aquestes dades es verifiquen i s'emmagatzemen de forma segura a una base de dades central, i es posen a disposició dels usuaris per a que puguin consultar-les, baixant-les als seus terminals i desxifrant-les per calcular el nivell de risc.

Pel que fa al càlcul del nivell de risc, el valor obtingut estima quina és l'exposició que pot haver patit una persona al virus. Es calcula a partir de les següents variables sobre un contacte:

- **Proximitat:** Derivat de l'atenuació del senyal dels missatges rebuts a través de BLE.
- **Duració:** En passos de 5 minuts i fins a 30 minuts.
- **Dies des del contacte:** Fins el límit màxim de 14 dies.
- **Risc de transmissió:** Valor individual que s'associa individualment segons el risc de transmissió propi o el risc de transmissió dins de la regió. Aquest risc de transmissió es podrien associar als següents factors (en el cas de que es puguin conèixer): si la persona és simptomàtica o asimptomàtica o el temps transcorregut des de tenir símptomes o des del contagi. A [24] es pot consultar un estudi sobre el paràmetre de risc de transmissió.

Les ponderacions d'aquestes variables van a càrrec de l'aplicació que implementi l'API, i en el cas de l'aplicació d'Alemanya estarien recolzades per un institut epidemiològic (Robert Koch-Institut).

Els mecanismes de càlcul de risc venen definits per l'API de Google i Apple que l'aplicació fa servir. La notificació final que es realitza a l'usuari dependrà de l'aplicació. En el cas de l'aplicació d'Alemanya, per exemple, l'usuari final rebrà una notificació sobre el seu nivell de risc (alt, baix o desconegut), el nombre de coincidències amb contactes positius i el temps des de l'últim contacte.

Es destaca que la següent explicació del càlcul de risc es conforme a la versió 1.0 de la API de Google i Apple i és la que fan servir a data d'avui aplicacions de Contact Tracing com la d'Alemanya. Tot i així, al Juliol Google i Apple van treure una nova versió de la API, la v.1.5, que modifica el procediment del

càlcul de risc i dona més llibertat/responsabilitat a les aplicacions de Contact Tracing. A l'apartat ***7.3*** es descriuen les diferències entre ambdues versions.

7.2 Descripció de les tecnologies utilitzades en el rastreig de contactes

7.2.1Tecnologia Bluetooth

La tecnologia utilitzada per les aplicacions a l'hora de traçar els contactes és la tecnologia Bluetooth Low Energy (BLE), que consisteix en l'enviament de missatges (beacons) des d'un terminal i la recepció i anàlisi del nivell de senyal dels mateixos en l'altre terminal per estimar la proximitat entre els usuaris.

Per tal d'avaluar els missatges que s'envien des de l'aplicació i analitzar el funcionament del BLE s'ha fet servir un equip sniffer BLE connectat a un PC que permet monitoritzar els missatges que l'aplicació instal·lada al telèfon envia a través de Bluetooth Low Energy. D'aquesta manera s'ha pogut analitzar el nivell del senyal rebut a diferents distàncies (que serveix per derivar la proximitat entre els usuaris), la freqüència d'enviament dels beacons (que tindrà impacte en el consum de bateria i en la fiabilitat de la solució) i el format de les trames (que impactarà en la interoperabilitat).

Després de realitzar les proves, s'ha pogut observar les següents característiques i aspectes a tenir en compte a l'hora d'utilitzar la tecnologia Bluetooth:

Dependència del dispositiu mòbil de l'usuari

Les solucions de Contact Tracing es basen majoritàriament en la utilització del telèfon mòbil d'un usuari. Tot i que això facilita la implementació, s'ha de tenir en compte que requereixen que l'usuari porti el telèfon a prop i que existeixen alguns col·lectius sensibles que possiblement no tindran accés a l'aplicació (per exemple, gent gran o persones sense recursos). Un altre aspecte a tenir en compte és que potser no tots els terminals seran compatibles amb les aplicacions de Contact Tracing degut a limitacions tecnològiques. Algunes propostes, com Tracetogether, han implementat solucions basades en equips específics (braçalets Bluetooth) que puguin fer-se servir per detectar contactes propers.

Precisió de l'estimació de proximitat mitjançant BLE

Com s'ha comentat anteriorment, estimar la proximitat d'un usuari a partir del nivell del senyal de missatges BLE pot comportar riscos de "falsos positius" causats per la variabilitat que pot experimentar el nivell de senyal segons el tipus de terminal, la orientació del telèfon, la ubicació del terminal (a la mà, a la orella o a la butxaca), les condicions de l'entorn o el nivell de potència. Tots aquets factors fan que sigui difícil estimar amb precisió la distància entre dos usuaris. Algunes solucions proposen la implementació de millores per tal de minimitzar el número de falsos positius. Per una banda, Google i Apple inclouen informació sobre la potència transmesa. Per altra banda, algunes iniciatives proposen de fer servir la informació d'altres elements del mòbil, per exemple els inercials, per derivar informació sobre la orientació i la ubicació. També es proposa tenir en compte el temps de contacte com un factor important que ajudi a eliminar falsos positius (per exemple, contactes degut a mesures errònies del Bluetooth). Un altre factor a tenir en compte és que per minimitzar el consum de la bateria dels dispositius mòbils o l'espai d'emmagatzematge necessari, aquests no estaran escoltant la radio BLE de forma continua, sinó durant unes finestres de temps definides. Això podria fer que alguns contactes curts però importants (una encaixada de mans) no es poguessin detectar.

Consum del dispositiu d'usuari

S'ha vist que aquestes aplicacions envien un número de missatges BLE (beacons) força elevat (proper als 400 paquets per minut), per tant, suposaran un augment del consum de la bateria dels terminals. Aquest consum vindrà determinat per la freqüència d'enviament dels missatges mitjançant BLE i també per el temps en que el telèfon està esperant rebre missatges d'altres terminals. Un altre factor important per al consum serà el fet de que l'aplicació pugui funcionar en segon pla (background) per a que no requereixi tenir la pantalla activa. Per tant, a l'hora d'implementar una aplicació de Contact Tracing, s'haurà de buscar un compromís entre el consum i el temps mínim que es requereix per assegurar que es puguin detectar tots els contactes rellevants. A mode de referència, s'ha vist que el consum de les aplicacions basades en l'API de Google i Apple (que permeten fer servir l'aplicació en segon pla) suposaria un 1-2% del total de la bateria; per tant, en aquests casos, no es consideraria un factor limitant.

7.2.2 Tecnologia Ultra-WideBand

UWB (Ultra-WideBand) és una tecnologia sense fils basada en el estàndard IEEE802.15.4a[25] que es considera interessant per a la seva utilització en aplicacions de localització. Aquesta tecnologia és robusta a interferències, té rangs d'abast que podrien arribar als centenars de metres i permet realitzar mesures de distància entre dos terminals amb precisions de centímetres. Aquestes mesures es realitzen a partir de la mesura del temps de vol dels missatges enviats. Per tant, fent servir un sistema de localització basat en la instal·lació de diferents referències UWB amb una localització fixa (referides àncores) seria possible derivar la posició de objectes o usuaris que portin un localitzador (o "tag") a partir de la trilateració de les seves distàncies respecte a les àncores. Donat que la solució requereix de la instal·lació d'uns elements fixes, seria un sistema més adient per entorns acotats (per exemple, edificis o zones delimitades que es pugui cobrir fàcilment). Actualment, seria necessari que els usuaris portessin un dispositiu específic per a la localització; tot i així, alguns fabricants de telèfons mòbils com iPhone ja han començat a incloure aquesta tecnologia a alguns dels seus terminals.

Es pot també mesurar la distància entre dos dispositius sense infraestructura, però es necessiten un nombre elevat de missatges que fan que la solució no sigui escalable a molts usuaris i amb localitzacions freqüents.

7.2.3 Altres

L'aplicació NOVID de Carnegie Mellon University fa servir ultrasons per localitzar amb precisió. L'aplicació utilitza la tecnologia Bluetooth per a detectar dispositius propers amb els que comunicar-se i fa servir el micròfon per detectar polsos d'alta freqüència i calcular així la distància respecte a altres usuaris. Aquesta alternativa presenta limitacions de privacitat addicionals al necessitar permís dels sistemes operatius dels telèfons mòbils per utilitzar el micròfon per escoltar missatges sonors i té limitacions en el nombre d usuaris.

Algunes altres solucions fan servir la localització per satèl·lit o GNSS (Global Navigation Satellite System), o de forma comú conegudes com a GPS. Aquestes solucions nomes funcionen en exteriors i tenen una precisió que no permet fer traçabilitat de contactes. Les aplicacions que ho fan servir ho fan bàsicament per geolocalitzar als usuaris i fer control de confinament.

7.3. API Google i Apple per fer front a la pandèmia de COVID-19

Google i Apple han llençat una iniciativa (protocol GAEN) per proporcionar una funcionalitat que permet als usuaris rebre notificacions relacionades amb possibles exposicions davant el COVID-19 entre usuaris propers a través de Bluetooth Low Energy. Aquesta funcionalitat està disponible tant per telèfons mòbils iPhone com Android a nivell de sistema operatiu i les notificacions són totalment voluntàries i poden ser inhabilitades en qualsevol moment. S'ha definit una API per a que les aplicacions de rastreig de contactes puguin utilitzar aquest sistema de notificació d'exposició afavorint així la interoperabilitat entre solucions.

En el dispositiu mòbil apareix un missatge de "*Notificación de Exposición*" quan s'ha estat en contacte amb exposició del virus com es pot veure a la ***Figura 2***.

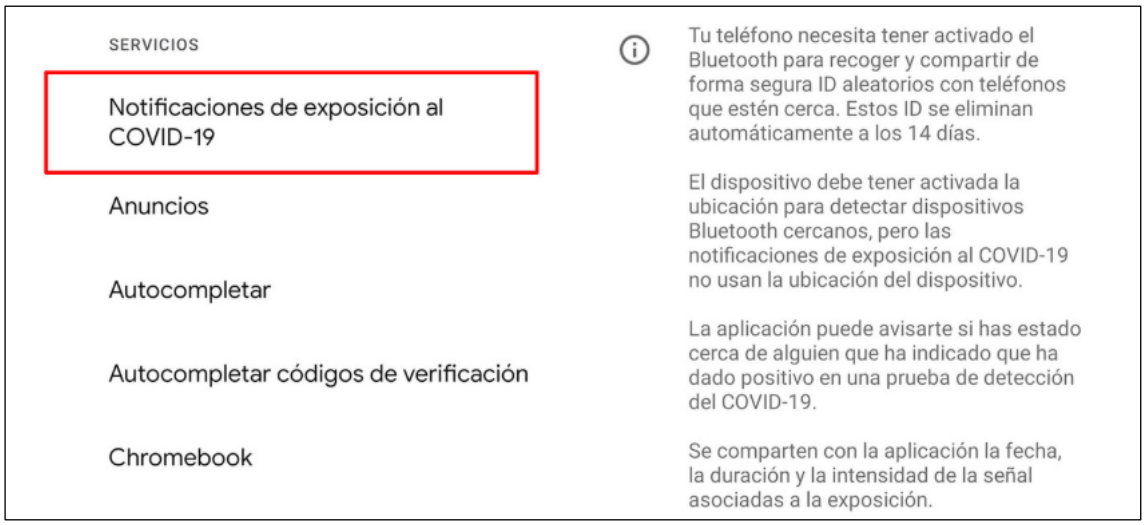


Figura 2. Pantalla de Notificació d'Exposició al COVID-19

El sistema no recopila dades d'ubicació del dispositiu si l'usuari no ho desitja, ja que les notificacions es poden habilitar o deshabilitar. A més a més el sistema utilitza claus d'exposició que es generen de forma aleatòria i la encriptació de les metadades associades al tràfic de Bluetooth.

Segons fonts de Google i Apple aquesta funcionalitat només es mantindrà activa quan sigui necessari i no serà una funcionalitat que es mantingui de manera permanent en el terminal.

Per tant, utilitzar l'API de Google i Apple suposa els següents avantatges:

- Permet que l'aplicació pugui funcionar en segon pla en Android i iOS. D'aquesta manera l'usuari no requereix tenir l'aplicació oberta i a la pantalla tot el temps. Això facilita la usabilitat i també redueix notablement el consum requerit per l'aplicació.
- Facilita la interoperabilitat entre aplicacions, ja que es defineix un tipus de missatge comú que altres aplicacions poden implementar i interpretar.
- Incorpora informació sobre la potència transmesa als missatges enviats. Aquesta informació es faria servir per a una millor estimació de la proximitat (distància) dels possibles contactes.
- Inclou aspectes de seguretat per millorar la privacitat de l'usuari. Per una banda els identificadors de BLE canvien freqüentment. Per altra banda, els identificadors i les metadades del missatge (per exemple, la informació de la potència rebuda) van xifrats; de forma que un usuari maligne que

estigui escoltant els missatges enviats per BLE no pugui fer-les servir per derivar informació sobre usuaris propers.

- Permet que l'usuari pugui habilitar o deshabilitar l'ús de les aplicacions de Contact Tracing des de les opcions de configuració del telèfon. D'aquesta manera l'usuari té un major control i transparència sobre el procés de traçabilitat de contactes.

A la ***Figura 3*** es mostra un exemple de com és possible tenir varies aplicacions de Contact Tracing instal·lades i controlar individualment les aplicacions, desactivar les notificacions d'exposició o suprimir els identificadors des de la pantalla de configuració de notificacions COVID-19 del sistema operatiu Android.

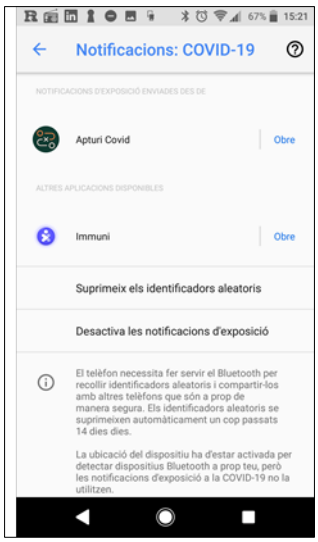


Figura 3. Pantalla de control de notificacions COVID-19 del sistema operatiu Android

Durant les primeres setmanes de juliol s'ha anunciat una nova versió de l'API de Google i Apple, la versió 1.5. Fins ara la versió que suportaven les aplicacions era la v1.1. Aquesta nova versió introdueix nous canvis que es centren en donar més llibertat a les aplicacions per calcular el risc d'exposició. Amb aquesta nova versió s'assegura compatibilitat bidireccional amb la versió 1.1, de forma que les aplicacions actuals podran seguir funcionant encara que s'actualitzi el sistema operatiu.

En comptes de realitzar un càlcul de risc internament, la nova versió de la API de Google i Apple proporcionaria a l'aplicació tota la informació necessària per a prendre la decisió sobre el risc d'exposició de l'usuari. Aquesta informació es referida com a la Finestra d'exposició o "Exposure Window"[21] .

La nova versió de la API contempla la incorporació de nous paràmetres (alguns d'ells encara pendents d'implementació). Concretament els paràmetres serien els següents:

- **Tipus de diagnosi.** Permet distingir la fiabilitat d'un diagnòstic positiu segons el procés d'obtenció del mateix: 1) El resultat d'un test (més fiable); 2) El diagnòstic mèdic en base a simptomatologia (sense realitzar el test) i 3) Una autodiagnosis (menys fiable).
- **Informació de cal·libració BLE**. Aquest paràmetre està previst per a noves actualitzacions. Permetrà derivar la fiabilitat de les mesures d'atenuació (proximitat de contactes) segons la qualitat de la informació de cal·libració de la que es disposi. Per exemple, si la cal·libració de

la potencia de transmissió s'ha realitzat conforme a dades obtingudes amb el mateix model de terminal de l'usuari això proporcionarà una major fiabilitat.

- **Capacitat d'infecció.** Aquest paràmetre està previst per noves actualitzacions. Permetrà donar informació sobre la capacitat de contagi d'un usuari positiu en base a als dies que fa de l'aparició dels seus símptomes.

Per altra banda, per la informació publicada, sembla que el protocol de Apple i Google podria reduir els períodes d'escolta (actualment aquests serien de 5 minuts). Això permetria millorar la capacitat de detectar contactes breus. I també, es redueixen de 20 a 6 el nombre de descarregues de claus de diagnosi per dia.

Com a limitacions, s'ha de tenir en compte que l'API no funciona en tots es telèfons mòbils. Concretament, el servei no seria compatible amb els següents terminals i versions de sistema operatiu:

- iPhones amb iOS 13.5 o posteriors [22]
- Versions Android anteriors a la versió 6.0 [21]
- Models de telèfons mòbils que no tinguin la possibilitat d'utilitzar els Google Mobile Services (GMS), com per exemple els nous models de Huawei produïts després de maig del 2019.

Aquesta limitació suposaria una major dificultat d'implantació ja que depenent dels països podria arribar a deixar fora a un 10% o més dels usuaris de terminals mòbils. No obstant, Huawei ha desenvolupat la HMS (Huawei Mobile Services) Contact Shield API (Juny 2020) que podria donar una opció de compatibilitat en un futur. Concretament, a [23] s'anuncia que l'aplicació alemanya Corona Warn App es suportarà als mòbils Huawei, tant per als dispositius HMS (no compatibles amb Google Mobile Services) i GMS (Google Mobile Services), tot i que no s'indica una data en la que aquesta opció estaria disponible.

7.4. Model del servidor

Les aplicacions de rastreig de contactes existents es basen en dos tipus de models de funcionament: descentralitzat i centralitzat.

Les principals diferències entre un model centralitzat i un descentralitzat es basen, per una banda, en la funció del servidor utilitzat, en on es realitza l'emmagatzematge de la informació recollida i en la pressa de les decisions efectuades.

7.4.1.Model de dades centralitzat

El **model centralitzat** és el que segueix, per exemple, el protocol ROBERT (proposat per la iniciativa europea PEPP-PT). En aquest cas el servidor genera i proveeix els pseudònims (identificadors efímer) que faran servir els usuaris. Els usuaris infectats per COVID-19 tenen la opció de compartir amb la base de dades els pseudònims dels contactes detectats (a partir de les mesures BLE) i el temps. Amb aquesta informació, el servidor pot deduir aspectes com el temps d'exposició i és el que s'encarrega d'aplicar els models de detecció de risc pertinents per determinar quins usuaris estan en risc per contacte.

Quan un altre usuari es posa en contacte amb el servidor (diferents cops al dia per enviar els seus identificadors), el servidor compara el seu identificador personal amb els publicats. En el cas que hi hagi algun identificador coincident i en base als paràmetres de risc establerts, l'aplicació informa a

l'usuari que ha estat en contacte amb una persona infectada. Per tant, el servidor s'encarrega de fer arribar aquesta informació als usuaris afectats.

A [20] es pot trobar una infografia que explica aquest model de forma senzilla.

Un dels punts a favor d'aquest tipus de models és el fet de que no es publica l'identificador de la font de contagi i, per tant, seria més difícil de rastrejar. Per altra banda, donat que en aquest cas el servidor és el que genera els identificadors seria fàcil controlar usuaris maliciosos. No obstant, el servidor és un punt sensible de seguretat, ja que tindria informació dels usuaris i dels seus contactes de risc.

Finalment, aquest model permet que les autoritats sanitàries puguin recollir informació interessant per als epidemiòlegs (al tenir informació sobre els contactes (identificadors i temps d'exposició) d'una persona infectada).

7.4.2.Model de dades descentralitzat

El **model descentralitzat** està recolzat per diferents iniciatives tals com DP-3T[20] , TCN o l'API de Google i Apple [21] i per les recomanacions de la Comunitat Europea[13] . Concretament, aquest model es considera més adient des del punt de vista de la privadesa i seguretat de les dades de contactes, ja que la informació que s'emmagatzema al servidor seria mínima (identificadors dels usuaris que han notificat ser positius en COVID-19, dates i informació del país al que ha estat l'usuari). La resta de informació clau estaria al telèfon del propi usuari i seria responsabilitat de l'aplicació i del protocol utilitzat que aquesta es mantingui i emmagatzemi de forma segura i per un temps limitat. Per tant, aquest tipus de model el servidor no necessita identificar l'usuari, és el propi telèfon de l'usuari el responsable de generar els identificadors pseudoaleatoris.

Quan un usuari ha estat infectat, decideix voluntàriament pujar les dades dels seus pseudònims al servidor. Aquest les publicarà per a que la resta d'usuaris puguin comprovar si han tingut algun contacte de risc. Per tant, la decisió de si s'ha establert aquest contacte o no es realitza en el propi terminal a partir dels models de decisions corresponents. En aquest model no és necessari l'enviament d'informació sobre el temps d'exposició al servidor.

Particularment, tot i seguir un model descentralitzat, el protocol DP-3T contempla la compartició d'algunes dades amb els epidemiòlegs per a la realització de gràfiques d'anàlisi de contactes.

7.5. Interoperabilitat entre països

Donat que per ara no es pot esperar que hi hagi una única aplicació o un únic protocol de Contact Tracing definitiva sinó diverses iniciatives provinents dels diferents països, s'hauria de valorar la implementació de solucions que permetin interoperar amb diferents aplicacions i que permetin la compartició d'informació entre els diferents servidors (backends). La migració cap a solucions basades en el ús de la API de Google i Apple o en solucions de codi obert seria recomanable per afavorir la interoperabilitat.

Per altra banda, el 13 de maig, en el marc de les accions previstes per la Comissió Europea, els Estats Membres de la xarxa *eHealth* Network van adoptar unes guies d'interoperabilitat [16] per ser implementades en les aplicacions mòbils de traça de contactes. Un dels punts destacables és que cada país membre ha de disposar d'un sol servidor interlocutor amb el EU FGS (*Federated Gateway Service*).

No es descarta, tot i que no és necessària la comunicació P2P entre servidors backend dels països membre.

8. Consideracions relatives a la protecció de les dades

Per tal de destacar els aspectes bàsics des del punt de vista de la normativa de protecció de dades pel que fa a les App's de gestió de contactes, s'han de tenir en compte els següents documents publicats per l'EDPB (*European Data Protection Board*), la Comissió Europea i el Consell Europeu en relació a l'ús d'aquest tipus d'aplicacions mòbils en el context del Covid-19:

- Carta de l'EDPB, de 14 d'abril de 2020, adreçada a la Comissió Europea en relació a l'esborrany de recomanacions sobre l'ús d'Apps en el context de lluita contra el Covid-19[2].
- Recomanació (UE) 2020/518 de la Comissió de 8 de abril de 2020 relativa a un conjunt d'instruments comuns de la Unió per la utilització de la tecnologia i les dades a fi de combatre i superar la crisis del COVID-19, en particular, pel que respecte a les aplicacions mòbils i a la utilització de dades de mobilitat anonimitzats[3].
- Full de Ruta Europeu conjunt del Consell Europeu sobre les mesures de contenció del Covid-19, de 15 d'abril de 2020[4].

8.1. Naturalesa de les dades tractades

El seguiment dels contactes d'una persona a través de Bluetooth, en la mesura que permeti la identificació directa o indirecta d'aquesta persona o de les persones amb les quals entra en contacte, constituiria un tractament de dades personals.

En aquest cas, cal tenir en compte, a més a més, que la identificació d'aquestes persones podria donar lloc a la revelació de dades relacionades amb la seva salut, incloent no només els usuaris diagnosticats positius, sinó també els contactes que resultin alertats per estar en situació de risc d'haver-se contagiat. El RGPD (*Reglament General de Protecció de Dades*) considera com a dada relacionada amb la salut, qualsevol informació sobre l'estat de salut física o mental, present, passada o futura, entre d'altres, el risc de patir malalties (considerant 35).

A priori, l'objectiu d'aquestes Apps de rastreig de contactes, no és identificar els usuaris, ni tampoc recollir dades de localització, tot i que les Apps poden arribar a recollir més informació[5], deixant oberta aquesta opció a les autoritats nacionals. A través d'aquestes aplicacions es transmeten i es reben codis

[2] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

[3] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H0518&from=ES

[4] https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

[5] DP-3T White Paper Decentralized Privacy-Preserving Proximity Tracing

aleatoris que s'allotgen o bé al dispositiu de l'usuari (descentralitzada) o bé al servidor central de l'administració (centralitzada).
Advertir que la informació que recullen les aplicacions només es podria considerar correctament anonimitzada si es pot assegurar que no existeix una probabilitat raonable de reidentificació, per qualsevol mitjà disponible que permeti l'associació del codi amb el número de mòbil o amb qualsevol altra dada que permeti identificar l'usuari del mòbil, atenent als factors objectius, els costos i el temps necessari per a la identificació.

A les dades anònimes no els hi és d'aplicació el RGPD, però cal ser conscients de la dificultat que pot suposar en determinats casos, garantir que el procés d'anonimització s'ha realitzat correctament i que no és possible reidentificar. Per això, davant qualsevol dubte és aconsellable tenir en compte les normes i garanties de la normativa de protecció de dades, i aplicar-la com si es tractés de dades pseudonomitzades.

8.2 Finalitat del tractament

Identificar de manera clara quina és la finalitat que es persegueix amb l'ús d'aquest tipus d'aplicacions és un aspecte important a tenir en compte i sembla ser que hi ha un consens generalitzat en els diferents estats de la UE i així ho reconeix la Comissió Europea, sobre l'important paper que poden jugar aquest tipus d'aplicacions en el rastreig dels contactes, a l'hora de limitar la propagació de la transmissió de la malaltia i interrompre les cadenes de transmissió. En concret, poden ser especialment importants per proporcionar informació sobre el nivell de circulació del virus, avaluar l'eficàcia de las mesures de distanciament físic i confinament i orientar estratègies de desescalada.

No obstant, a banda de permetre als usuaris informar-los de forma ràpida que han entrat en contacte estret amb un subjecte positiu de COVID-19, aquest tipus d'aplicacions proporcionen recomanacions sobre el comportament i hi ha casos que conviden a l'usuari a consultar amb el seu professional de la salut.

Per tant, cal tenir especialment cura de les dades que es recullen dels dispositius dels usuaris (dades analítiques) amb finalitats de salut pública i que contribueixen a millorar el funcionament del sistema d'alertes.

8.3. Licitud: base jurídica legitimadora

La traçabilitat dels contactes a través de Bluetooth dels dispositius mòbils personals es troba subjecte a la descàrrega voluntària per part del usuari i per tant, és el mateix usuari qui realitza l'acceptació del tractament de les seves dades personals.

Ara bé, com apunta l'EDPB, el fet que l'Autoritat Sanitària pugui recollir i tractar les dades personals d'aquests usuaris no necessàriament ha de basar-se en aquest consentiment.

La posada d'aquest servei a disposició de la ciutadania, i el tractament de les dades per part de l'autoritat sanitària podria justificar-se en el marc de les mesures de contenció de la propagació del coronavirus sobre la base d'una missió realitzada en interès públic en l'àmbit de la salut pública amb

la finalitat de supervisió i d'alerta o de prevenció i control de malalties transmissibles i altres amenaces greus per a la salut. (art. 6.1.e) en relació amb l'art. 9.2.g) i) RGPD).

El punt 1 de la disposició addicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades i garantia dels drets digitals disposa que estan *emparats en les lletres g), h), i) i j) de l'article 9.2 del Reglament (UE) 2016/679 els tractaments de dades relacionades amb la salut que regulin, entre d'altres, la Llei 14/1986, de 25 d'abril, general de sanitat, i la Llei 33/2011, de 4 d'octubre, general de salut pública, així con les seves disposicions de desenvolupament.*

La Llei orgànica 3/1986 de mesures especials en matèria de salut pública, preveu que **les autoritats competents en matèria de salut pública puguin, per tal de controlar malalties transmissibles, *"adoptar les mesures oportunes per al control dels malalts, de les persones que estiguin o hagin estat en contacte amb els mateixos i de l'entorn immediat, així com les que es considerin necessàries en cas de risc de caràcter transmissible*."**(art. 3)

Per altra banda, l'article 9 de la Llei 33/2011, de 4 d'octubre, general de salut pública estableix que *"1. Les persones que coneguin fets, dades o circumstàncies que puguin constituir un risc o perill greu per a la salut de la població els han de posar en coneixement de les autoritats sanitàries, que han de vetllar per la protecció deguda a les dades de caràcter personal."*

El decret *203/2015,* de 15 de setembre, pel qual es crea la Xarxa de Vigilància Epidemiològica i es regulen els sistemes de notificació de malalties de declaració obligatòria i brots epidèmics, preveu a l'article 16.2 que els metges sota la direcció dels metges del servei de vigilància epidemiològica, puguin adoptar les mesures necessàries que s'hagin de dur a terme pel que fa a la persona malalta i el seu entorn més immediat, per al control de malalties notificades.

Sobre la base d'aquestes previsions, l'Autoritat Sanitària estaria legitimada per recollir i tractar les dades de salut necessàries de les persones diagnosticades positives i també les dades de les persones amb les que s'ha pogut estar en contacte per alertar-los.

En aquest cas però, es tracta de posar al servei dels ciutadans una aplicació tecnològica que rastreja els contactes. El rastreig es defineix com la cerca d'una persona o cosa seguint el seu rastre o senyal. De fet, el que pretenen aquestes aplicacions és poder identificar (encara que es faci a través de codis aleatoris) i alertar les persones que han estat en contacte amb persones diagnosticades positives (i per tant amb risc d'haver estat contagiades).

El tractament massiu de dades de salut per part de l'Autoritat Sanitària sobre la base de l'execepció prevista a l'article 9. 2.i) RGPD, requereria de l'aplicació de mesures adeqüades i específiques per protegir els interessos, drets i llibertats de les persones afectades.

L'EDPB, apunta a la necessitat que siguin les normes legals internes les que promoguin l'ús d'aquest tipus d'App, i ho facin sense obligar ningú i sense cap conseqüència negativa per a les persones que decideixen no utlitizar-la. La Comissió Europea també fa referencia en les seves recomanacions a que siguin els diferents estats els que adoptin disposicions legislatives que ho regulin. Per exemple, l'aprovació d'una llei que reguli aquest fet.

Una possible alternativa seria que es regulessin les garanties específiciques d'aquesta App en el marc d'un decret llei en el qual s'abordessin també altres solucions tecnològiques previstes en el context del COVID-19 (incloent-hi l'App STOP COVID-19 que ja està en marxa). Un exemple clar seria doncs, el cas d'Itàlia, on s'han regulat les directrius pel funcionament del sistema de gestió de contactes amb el Decret llei del 30 d'abril de 2020, n. 28 [6], dictat posterior als informes de l'Autoritat de Protecció de Dades del país.

Un altre exemple seria la proposta de llei publicada al Regne Unit i liderada pel professor Lilian Edwards (Universitat de Newcastle)[7], amb una regulació de mesures que garanteixin els drets i llibertats de les persones en el tractament de dades a través de diferents solucions tecnològiques en la lluita contra el coronavirus.

D'aquesta proposta, cal assenyalar alguns punts que destacables:

- Ningú hauria de ser penalitzat per no tenir un telèfon, sortir de casa sense un telèfon, sense carregar el telèfon, i conductes similars.
- Ningú està obligat a instalar una aplicació de rastreig en el seu dispositiu mòbil.
- Les dades recollides per una aplicació no seran compartides fora del sistema públic de salut i de les persones involucrades en el seguiment del COVID-19, excepte amb el consentiment previ i lliurement atorgat, i sempre que el nou tractament compleixi concretament amb els principis de tractament lícit, necessari i proporcional.
- Les dades recollides per aquesta aplicació han de ser suprimides o anonimitzades el més aviat possible i com a màxim després de sis mesos.

8.4. Avaluació d'impacte

Amb independència de la base jurídica en que es fonamenti el tractament, hi ha altres elements que tant l'EPDB com la Comissió Europea assenyalen com a necessaris. La realització d'una **avaluació d'impacte** sobre els drets i llibertats de les persones que reculli com a mínim els aspectes següents:

- Valoració de la idoneïtat, la necessitat i la proporcionalitat en l'ús d'una aplicació de rastreig de contactes
- Minimització de les dades recollides
- Implantació de mecanismes de privacitat des del disseny i per defecte

8.4.1. Valoració de la idoneïtat, la necessitat i la proporcionalitat en l'ús d'una aplicació de rastreig de contactes

8.4.1.1. Idoneïtat

Cal demostrar que, a criteri dels experts en epidemiologia i salut pública, la solució tecnològica que s'ofereix a la ciutadania compleix amb la finalitat que es pretén amb la seva implantació.

La Comissió Europea fonamenta l'ús d'aquestes Apps de rastreig en el fet que poden detectar amb rapidesa a tots els contactes d'un pacient confirmat de COVID-19 per tal de demanar-los que

[6] https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg
[7] https://osf.io/preprints/lawarxiv/yc6xu/

practiquin l'autoaïllament, i en cas de desenvolupar símptomes, realitzar-los les proves i aïllar-los de forma ràpida.

Sense posar en dubte que aquestes Apps poden ser un mecanisme molt útil per a què les autoritats sanitàries efectuïn el rastreig dels contactes, el cert és que la seva eficàcia pot dependre de molts factors, entre d'altres, el percentatge de població que utilitza dispositius mòbils, i dins d'aquest grup, el percentatge de la població que acabi descarregant-se i utilitzant l'aplicació.

A més a més, l'aplicació ha de ser robusta pel que respecta al compliment dels nivells de seguretat per tal de que es donin les garanties pertinents pel que respecte a la no reidentificació de l'usuari.

8.4.1.2. Necessitat

Cal demostrar que l'ús per part de la ciutadania d'aquesta aplicació i l'objectiu que pretén és rellevant i que no existeix una altra mesura menys intrusiva per a la consecució d'aquest propòsit i amb igual eficàcia.
La valoració sobre la necessitat s'ha de fer amb criteris de salut pública. El propòsit de l'App és identificar contactes amb persones positives de COVID-19, però ha de ser l'autoritat sanitària qui determini que s'entén per contacte estret (distància, temps), així com els criteris i els procediments de seguiment.

8.4.1.3. Proporcionalitat

Cal fer un judici de ponderació i preguntar-se quin són els beneficis obtinguts per l'ús d'aquesta tecnologia i si aquests pesen més que els seus efectes negatius.

Per exemple, que l'avís o alerta que es genera a un usuari per haver estat amb contacte amb una persona amb positiu de COVID-19 podrien, a banda de generar una preocupació al usuari, ser un fals positiu. Aquest fet, provocaria que l'usuari es veiés obligat a autoconfinar-se, sense saber, ni on, ni qui, ni quan ha pogut contactar amb un positiu. Per tant, l'App no pot ser una plataforma que generi alarma social o doni lloc a que es produeixi cap tipus d'estigmatització.

8.4.2. Minimització de les dades

Les dades personals que es tractin han de ser les mínimes necessàries per a la consecució de l'objectiu o finalitat que es pretén amb el tractament. L'EDPB assenyala dos elements a tenir en compte:

1. Les Apps de rastreig de contactes no necessiten recollir dades de localització dels usuaris. El seu objectiu no és seguir els moviments de les persones o imposar restriccions. La seva principal funció es detectar contactes amb persones diagnosticades positives. La recollida de dades de localització suposaria la violació del principi de minimització i l'augment del risc per a la seguretat i privacitat dels usuaris.

2. S'ha de ponderar com es realitzarà l'emmagatzematge de les dades, descentralitzada en els dispositius dels usuaris o centralitzada. Ambdues alternatives poden ser vàlides, però s'ha d'atendre el principi de minimització.

8.4.3. Implantació de mecanismes de privacitat des del disseny i per defecte.

El desenvolupament d'aquestes aplicacions ha de complir amb la privacitat des del disseny i per defecte. Adoptant les mesures de seguretat adequades per minimitzar els riscos.

L'App ha de complir amb els requisits de seguretat efectius per a protegir la disponibilitat, autenticitat, integritat i confidencialitat de les dades.

8.5. Intervenció de l'APDCAT

És imprescindible, i així ho apunten tant l'EDPB com la Comissió Europea la intervenció de l'autoritat de protecció de dades abans de prendre qualsevol decisió respecte aquest tema.

8.6. Limitació de la finalitat i limitació temporal de l'ús d'aquest tipus aplicacions

Cal limitar estrictament el tractament de dades personals a la finalitat que persegueix el rastreig de contacte a través de l'App i vetllar per a que les dades personals no s'utilitzin per a altres finalitats, com la coerció o amb finalitats comercials.

Una vegada finalitzada la crisi, aquest tipus d'aplicacions no hauria de fer-se servir, i les dades recollides haurien de ser eliminades o anonimitzades.

8.7. Transparència /Informació a l'usuari de l'App i a la ciutadania en general.

Aconseguir que aquesta App de rastreig de contactes sigui efectiva com a mesura de contenció de l'epidèmia dependrà bàsicament del grau d'acceptació de la ciutadania, que és qui ha de decidir si s'instal·la o no l'aplicació al mòbil. Es tracta en definitiva de fer que la gent se senti partícip i col·labori amb l'autoritat sanitària i amb els científics en la lluita contra la pandèmia, i per aconseguir això caldrà generar confiança.

La confiança de la ciutadania en les decisions i mesures que s'adoptin obliguen l'autoritat sanitària a ser transparent, i a difondre tots els aspectes i detalls relacionats amb la finalitat i el funcionament d'aquesta App. L'EDPB fa esment a la necessitat d'acompanyar les mesures legislatives que s'adoptin amb activitats de comunicació que promoguin l'ús de l'App per part dels usuaris.

A més a més, els usuaris haurien de conèixer abans d'instal·lar-se l'App, quines dades es recullen, el període de retenció, la descripció dels sistema que s'utilitza per generar l'alerta i la manera com es realitzarà aquesta alerta o avís a les persones que han mantingut contacte amb positius en covid-19.

L'EDPB assenyala, a més a més, que el codi font de l'App hauria de ser disponible públicament per tal que pugui ser sotmès a escrutini de la comunitat científica.

9. Riscos i amenaces

A continuació es presenten aspectes relacionats amb els riscos o amenaces associats a la traçabilitat de contactes.

9.1. Taxonomia dels riscos

La idea bàsica del rastreig de proximitat digital mitjançant aplicacions mòbils és utilitzar senyals Bluetooth Low Energy (BLE) per estimar la proximitat física entre dos telèfons intel·ligents. L'única funcionalitat que necessita proporcionar una aplicació és informar als contactes d'una persona infectada que podrien haver estat exposats al virus a través d'un contacte físic de rang proper. És de rellevància destacar que des de el punt de vista de la privacitat dels individus i seguretat inherent que el sistema no necessita revelar a ningú amb qui va tenir contacte el contacte contagiós, ni quan i on va passar.

Respecte als riscos s'identifiquin de tres tipus:

- Riscos inherents que s'apliquen a tots els sistemes de traça de contactes
- Riscos genèrics que s'apliquen als sistemes que utilitzen BLE
- Riscos derivats de la informació exposada per la xarxa

La ***Figura 4*** proporciona una visió dels riscos inherents per a la traçabilitat de contactes segons *[27]* . Per a cada tipus de sistema, la taula mostra si els sistemes específics presenten aquest risc ("✓") i si es pot pal·liar el risc ("(✓)"). Les notes a sota de les marques de verificació especifiquen, si s'escau, el mecanisme d'atac que comporta el risc

	All PT systems	BLE-based PT systems	Systems sharing infected identifiers	Systems sharing observed identifiers	
			Decentralised	Decentralised	Centralised
	Section 2.1	Section 2.2	Section 3.2	Section 3.4	Section 3.5
Identify					
Infected individuals (IR 1)	✓ Multiple accounts	✓ Multiple accounts	✓ Eavesdropping	✓ Injection	✓ Multiple accounts
Locations with infected people present (GR 3)		✓ Multiple accounts	✓ Eavesdropping	✓ Injection	✓ Multiple accounts
Prevent notification (IR 2)	✓	✓	✓	✓	✓
Cause false alarms					
Through range extension (GR 1)		✓	✓ Injection	✓ Eavesdropping	✓ Eavesdropping
Through active relay (GR 2)		✓ Bi-directional	✓ Uni-directional	✓ Uni-directional	✓ Uni-directional
Disrupt contact discovery (GR 4)		✓	✓	✓	✓
Track a BT enabled device (GR 5)		(✓)	(✓)	(✓)	(✓)
Reveal app usage (GR 6)		✓	✓	✓	✓

Figura 4. Visió general dels riscos inherents i genèrics dels sistemes de traça de proximitat digitals [27]

9.2. Dispositiu com a vector de l'atac

El model de "Bring your own Device" aplicable a aquest tipus d'escenari impacta en aspectes com:

1. No tenir control de versions de hardware, firmware ni Sistema operatius del dispositiu.
2. No tenir control de l'estat (routed/unblocked) del dispositiu final.
3. No tenir control de l'estat de millores de seguretat aplicades.
4. No tenir control de versions de hardware i firmware Bluetooth al dispositiu.

Per exemple, el protocol DP-3T (Decentralized Privacy-Preserving Proximity Tracing) és vulnerable a la descoberta de l'algorisme generador d'entropia utilitzat per generar els EphID (Ephemeral IDs), L'obtenció de clau mestra o la injecció d'una EPHI/RPI persistent permetria reidentificar els usuaris.

S'ha de tenir en compte, que aquest atac requereix l'accés al dispositiu i un coneixement de la tècnica per extreure dades d'aquest.

9.3. BLE com a vector de l'atac

La tecnologia BLE conté riscos de seguretat degut a la natura sense fils del protocol. A mode d'exemple a [29] es demostra com es podria arribar a identificar als usuaris i traçar el seu moviment.

Per això es requeriria instal·lar un nombre important de dispositius actuant com a sniffers BLE (rebent els beacons que s'envien a través de l'aire) a diferents llocs coneguts. Per altra banda, faria falta un dispositiu compromès capaç d'utilitzar una aplicació oficial de traçament de contactes que permetés interceptar i desxifrar les claus de diagnòstic positives que l'aplicació descarrega dels servidors de les autoritats locals de salut. Finalment, faria falta un servidor que rebés els identificadors captats a través de l'aire (RPIs) i els identificadors obtinguts del dispositiu piratejat.

Amb aquesta informació seria possible arribar a traçar als usuaris infectats que s'haguessin mogut per la zona on estan desplegats els sniffers; com es mostra a la següent figura. A la ***Figura 5*** s'il·lustra un exemple del funcionament de l'atac [30]. En aquest cas, les dades no pertanyen a un atac real a cap dispositiu, sinó que s'ha emulat el funcionament del protocol de Google i Apple.

Figura 5. Traçabilitat de contactes a partir d'escolta passiva BLE i un atac al dispositiu/aplicació [27]

9.4 Recomanacions addicionals (OPSEC)

En el context actual és important considerar a mode de bones pràctiques la incorporació de mecanismes de seguretat a les aplicacions de seguiment de proximitat per garantir que les propietats de seguretat i privadesa proporcionades pels protocols no siguin minades per altres components del sistema.

En particular proporcionem recomanacions per prestar atenció i protegir:

- Les Comunicacions sensibles entre aplicació i servidor i així assegurar que el trànsit de xarxa associat amb informació sensible (estat positiu COVID, usuaris notificats) no pugui ser reconegut per observadors passius.
- Les Comunicacions entre back-end i els telèfons intel·ligents. És necessari considerar mecanismes de verificació de la integritat dels Sistemes Operatius dels dispositius clients. És

important assenyalar que aquesta verificació augmenta la dependència dels components de codi tancat i pot no estar disponible a tots els telèfons.

- Protecció de metadades al servidor. Es requereix un anàlisi de quina informació podria recopilar un servidor i proporcionar recomanacions sobre aspectes de registre i emmagatzematge.
- Validació de notificacions. Incorporació d'un mecanisme que permeti validar que quan un usuari afirma haver rebut una notificació sigui a través del dispositiu pel qual l'aplicació ha generat realment notificacions.

9.5. Tendències en curs

Grups de hackers, com APT29 es troben treballant de manera activa en detectar vulnerabilitats de tipus ZERO DAY (vulnerabilitats encara desconegudes) que afectin a aquests sistemes.

També estan treballant en la creació de malware (programari maligne) que exploti aquestes vulnerabilitats per obtenir dades sensibles d'usuaris infectats per COVID.

Es sospita que aquests grups de hackers podrien estar finançats per governs i disposarien de pressupostos molt elevats.

Factors com la falta de control dels dispositius, els problemes de seguretat de BLE i l'alt valor de la informació (infectats de COVID) fa que la probabilitat tenir atacs exitosos pugui créixer en un futur proper.

10. Conclusions

Per tant, a mode de resum s'indica que hi ha un consens generalitzat en els diferents estats de la UE i així ho reconeix la Comissió Europea sobre l'important paper que poden jugar aquest tipus d'aplicacions en el rastreig dels contactes, **limitar la propagació de la transmissió de la malaltia i interrompre les cadenes de transmissió**. Aquestes Apps també poden ser especialment importants per proporcionar informació sobre el nivell de circulació del virus, avaluar l'eficàcia de las mesures de distanciament físic i confinament, i orientar estratègies de desescalada.

La Comissió Europa aposta clarament per un **model descentralitzat** basat en DP-3T, així com la utilització de l'**API de Google i Apple** en aquest tipus d'aplicacions.

L'aplicació d'Alemanya sembla un bon exemple pel que fa a garantir la privacitat dels usuaris, processant un conjunt mínim de dades personals necessàries per la finalitat de la mateixa. També presenta una bona experiència d'usuari i una integració robusta dins del seu sistema de salut.

Pel que fa a la anàlisi de la tecnologia **Bluetooth Low Energy** (BLE) efectuada, cal destacar:

- La **dependència del dispositiu mòbil** de l'usuari (*tenir el dispositiu a prop per funcionar*)
- **Precisió de l'estimació** de proximitat mitjançant BLE (*variabilitat en el nivell del senyal en funció d'on duem el telèfon mòbil*)

- **Consum del dispositiu d'usuari** (Tot i que el número de missatges BLE (beacons) enviats és força elevat (proper als 400 paquets per minut) el consum de bateria del terminal no representa més d'un 2% en un dia d'ús normal.

A nivell funcional i a banda de les consideracions relatives a la seguretat i protecció de les dades o al potencial d'interoperabilitat entre els diferents països, cal destacar el potencial que tenen aquestes Apps per oferir altres serveis. La major part de les aplicacions ofereixen, ja sigui en el moment de la instal·lació o en algun submenú, recomanacions higièniques i de comportament. Només l'App de Letònia ofereix informació relativa a l'evolució de la malaltia a nivell local, amb dades del nombre de test, casos nous, morts i percentatge d'infectats. En el cas de l'App Immuni, d'Itàlia, destaca el seu disseny i la senzillesa d'ús com a punts forts.

D'altre banda, sembla imprescindible millorar la comunicació respecte els termes legals i les condicions d'ús que aquest tipus d'aplicacions proporcionen als seus usuaris. Podria ser interessant treballar en l'adaptació d'aquets apartats i defugir d'introduir simplement un document que sovint és molt difícil de llegir en un dispositiu mòbil.

12. Recomanacions

En el cas que es vulgues posar en marxa una aplicació de traçabilitat de contactes i després de realitzar la anàlisi de les aplicacions que han desenvolupat diferents regions es recomana:

- Utilitzar un model de **servidor descentralitzat**
- Aplicar **l'API de Google i Android** en la implementació de la solució
- Implementar un **backend** que resolgui la integració amb els laboratoris/l'autoritat sanitària i la interoperabilitat entre les solucions dels diferents països. També s'hauria d'encarregar de gestionar la verificació dels usuaris i la transmissió de les claus de diagnòstic.
- Incorporar **mecanismes per ajustar el càlcul de risc** d'exposició de forma dinàmica segons evolucionin les recomanacions epidemiològiques.
- El **model de l'aplicació d'Alemanya** sembla que resolt molt favorablement els aspectes de privacitat i protecció de dades dels ciutadans. A banda, de ser una aplicació amb una bona experiència d'usuari, senzilla d'interpretar i que disposa molts dels components de l'arquitectura (aplicació i backend) en codi obert. El fet de definir diversos servidors independents (servidor de verificació i servidor de l'aplicació) permet que les dades es puguin gestionar de forma segura i privada, a més a més l'aplicació no interacciona en cap moment amb els servidors dels laboratoris. A l'Annex II es pot consultar com es calcula el risc d'exposició i els elements de codi lliure utilitzats en l'arquitectura de la solució

Per altra banda, caldria tenir en compte els següents aspectes des del punt de vista de la normativa de protecció de dades:

- Utilitzar aquest tipus d'aplicacions ha de ser totalment a **voluntat de l'usuari.**
- Els mecanismes i garanties específiques dels drets i llibertats s'haurien d'establir preferiblement mitjançant **normes en rang de llei.**
- Realitzar i documentar una **avaluació d'impacte** sobre els drets i les llibertats dels ciutadans.

- Comptar amb la intervenció de **l'Autoritat de protecció de dades.**
- La implementació de disseny en aquestes aplicacions s'ha de preveure des de diversos àmbits i **experts** (seguretat, privacitat, legal, ètic i salut pública).
- Cal que es determini de manera clara quina és la **finalitat** que es persegueix amb l'ús d'aquestes aplicacions.
- La **base de legitimació** de la posada d'aquest servei a disposició de la ciutadania, i el tractament de les dades per part de l'autoritat sanitària podria justificar-se en el consentiment i el marc de les mesures de contenció de la propagació del coronavirus sobre la base d'una missió realitzada en interès públic en l'àmbit de la salut pública amb la finalitat de supervisió i d'alerta o de prevenció i control de malalties transmissibles i altres amenaces greus per a la salut. (art. 6.1.e) en relació amb l'art. 9.2.g) i) RGPD).
- **Limitar els terminis** d'ús d'aquestes Apps i **eliminar les dades** tant aviat com sigui possible un cop finalitzada la situació excepcional de crisis sanitària actual.
- **Transparència i informació** a l'usuari de l'App i a la ciutadania en general. Cal generar confiança i un grau d'acceptació alt entre la ciutadania per tal d'aconseguir que l'App sigui efectiva com a mesura de contenció de l'epidèmia.
- A banda d'aquests aspectes, en el cas que es vulgui desenvolupar una aplicació d'aquestes característiques, caldrà que es faci tenint en compte, **la privacitat en el disseny i per defecte.**

13. Referències

[1] Yasaka TM, Lehrich BM, Sahyouni R. **Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App**. *JMIR Mhealth Uhealth*. 2020;8(4):e18936. Publicat el 7 d'abril de 2020. doi:10.2196/18936. Disponible article complert: https://mhealth.jmir.org/2020/4/e18936/pdf

[2] Abeler J, Bäcker M, Buermeyer U, Zillessen H. **COVID-19 Contact Tracing and Data Protection Can Go Together**. *JMIR Mhealth Uhealth*. 2020;8(4):e19359. Publicat el 20 d'abril de 2020. doi:10.2196/19359. Disponible article complert: https://mhealth.jmir.org/2020/4/e19359/pdf

[3] OSF. 2020 Mar 26. **Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy**. Disponible a la següent URL: https://osf.io/7vgq9/

[4] Government Digital services of Singapore. 2020 Mar 27. **App TraceTogether**. Disponible a la següent URL: https://www.tracetogether.gov.sg/

[5] Cellan-Jones, R.2020 Mar 31. Coronavirus: UK considers virus-tracing app to ease lockdown

[6] *BBCC News*. Consultat l'1 d'Abril de 2020. Disponible a la següent URL: https://www.bbc.com/news/technology-52095331

[7] Kim, M.S. 2020 Mar 6. South Korea is watching quarantined citizens with smartphone app. MIT Tecnology Review. Consultat el 27 de Març de 2020. Disponible a la següent URL: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/

[8] Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS). 2020 Apr. **Avaluació de la traçabilitat de contactes ("Contact tracing") per Bluetooth en el marc de la pandèmia de COVID-19**. Disponible l'informe complert a: http://aquas.gencat.cat/web/.content/minisite/aquas/publicacions/2020/avaluacio_tracabilitat_contact_tracing_bluetooth_covid19_aquas2020.pdf

[9] Portal documental de **l'App Immuni**. 2020 June. https://github.com/immuni-app/immuni-documentation

[10] Agència Italiana de protecció de dades. 2020 June. **App "Immuni": via libera del Garante privacy**. Disponible a la següent URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356588

[11] Agència Italiana de protecció de dades. 2020 June. **Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni". Disponible a la següent URL:** https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9357972

[12] IDAC. 2020 June 5. **Privacy in the Age of COVID: An IDAC Investigation of COVID-19 Apps**. Disponible a la següent URL: https://digitalwatchdog.org/wp-content/uploads/2020/06/IDAC-COVID19-Mobile-Apps-Investigation.pdf

[13] eHealth Network. 2020 May 13. **Interoperability guidelines for approved contact tracing mobile applications in the EU**. Disponible a la següent URL: https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

[14] European Data Protection Board. 2020 Apr 21. **Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak**. Disponible a la següent URL:

[15] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[16] eHealth Network . 2020 June 16. **eHealth Network Guidelines to the EU Member States and the European Commission on interoperability specifications for cross-border transmission chains between approved apps**. Disponible a la següent URL: https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf

[17] European Comission. 2020 Apr. **Joint European Roadmap towards lifting COVID-19 containment measures**. Disponible a la següent URL: https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

[18] eHealth Network. 2020 Apr 15. Common EU Toolbox for Member States. **Mobile applications to support contact tracing in the EU's fight against COVID-19**. Disponible a la següent URL: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[19] Github. 2020 Apr 18. **Infografia sobre el protocol ROBERT**. Disponible a la següent URL: https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-infography-EN.pdf

[20] Github. 2020 Apr. **DP3T – Descentralized Privacy-Preserving Proximity Tracing**. Disponible a: https://github.com/DP-3T/documents

[21] Documentació de la API de Google i Apple (Android). https://developers.google.com/android/exposure-notifications/exposure-notifications-api

[22] Documentació de la API de Google i Apple (iOS).https://developer.apple.com/documentation/exposurenotification/building_an_app_to_notify_users_of_covid-19_exposure

[23] Suport Huawei per l'aplicació Corona-Warn-App. https://consumer.huawei.com/ae-en/community/details/New-Corona-warning-app-for-all-Huawei-smartphones/topicId_109122/

[24] CWA Team. June 2020. **Epidemiological Motivation of the Transmission Risk Level**. Disponible a: https://github.com/corona-warn-app/cwa-documentation/blob/master/transmission_risk.pdf

[25] UWB. **Estandard IEEE 802.15.4a.** https://web.archive.org/web/20150705092920/http://www.decawave.com/technology/ieee802154a-standard

[26] Aplicació NOVID. https://techxplore.com/news/2020-07-novid-accurate-app-contact.html

[27] The DP-3T project. April 2020. **Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems**. Disponible a : https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf

[28] **BLE contact tracing sniffer PoC**. Disponible a: https://github.com/oseiskar/corona-sniffer

[29] Baumgärtner, Lars et al. June 2020. **Mind the GAP: Security & Privacy Risks of Contact Tracing Apps.** Disponible a: https://www.researchgate.net/publication/342093921_Mind_the_GAP_Security_Privacy_Risks_of_Contact_Tracing_Apps

[30] The DP-3T project. April 2020. **Security and Privacy Analysis of the document 'PEPP-PT: Data Protection and Information Security Architecture'**. Disponible a: https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architechture%20-%20Security%20and%20privacy%20analysis.pdf

[31] Leopold, George. May 2020. **COVID-19 Contact Tracing Apps Attracting Hackers**. Disponible a: https://www.enterpriseai.news/2020/05/27/contact-tracing-apps-attracting-hackers/

[32] Starks, Tim. June 2020. **Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better.** Disponible a: https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601

[33] MIT Technology review. July 2020. **Russian hackers have been accused of targeting covid-19 vaccine researchers**. Disponible a: https://www.technologyreview.com/2020/07/16/1005336/russian-hackers-have-been-accused-of-targeting-covid-19-vaccine-researchers/

Annex I. Aplicacions de traçabilitat de contactes

A continuació es detallen les aplicacions revisades de traçabilitat de contactes en el context de la pandèmia de COVID-19. Les aplicacions més destacades són:

AI.1 Itàlia

Nom: Immuni

Immuni és una aplicació que s'ha desenvolupat per ajudar-nos a combatre l'epidèmia de la COVID-19. L'aplicació es serveix de la tecnologia per avisar els usuaris que han estat exposats a el risc, encara que siguin asimptomàtics.

Quan l'aplicació avisa els usuaris d'un possible contagi, aquests es poden aïllar per evitar posar en risc a altres persones. D'aquesta manera, ajuden a contenir l'epidèmia i contribueixen a que tornem a la normalitat com més aviat millor.

A més, com reben un avís immediatament, els usuaris poden contactar amb el seu metge de capçalera i reduir així el risc de complicacions.

Figura 1. Captura de pantalla de l'aplicació Immuni.

Nom: Immuni
Versió: 2.2.0
Data de llançament: 02/06/2020
Enllaç de descarrega:
https://play.google.com/store/apps/details?id=it.ministerodellasalute.immuni&gl=ES

Itàlia va publicar el dia **2/6/2020** la **App Immuni**, la primera aplicació oficial en el marc de la UE **de traçabilitat de contactes** oferta al públic que utilitza el sistema de "notificació d'exposicions al COVID-19" d'Apple i Google. La App està disponible per descarrega gratuïta i disposa de la traducció a l'espanyol.

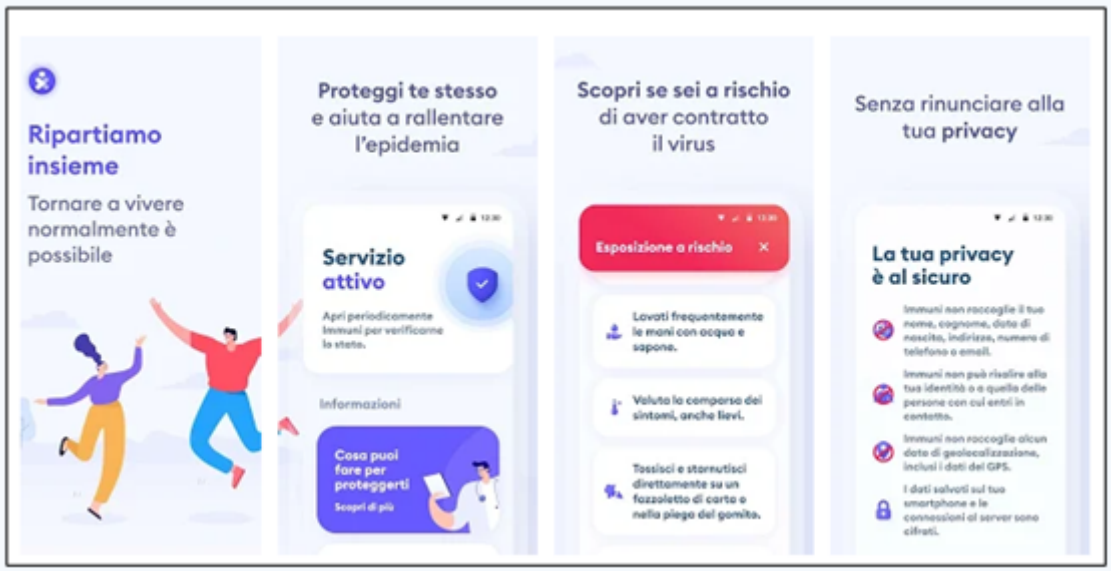


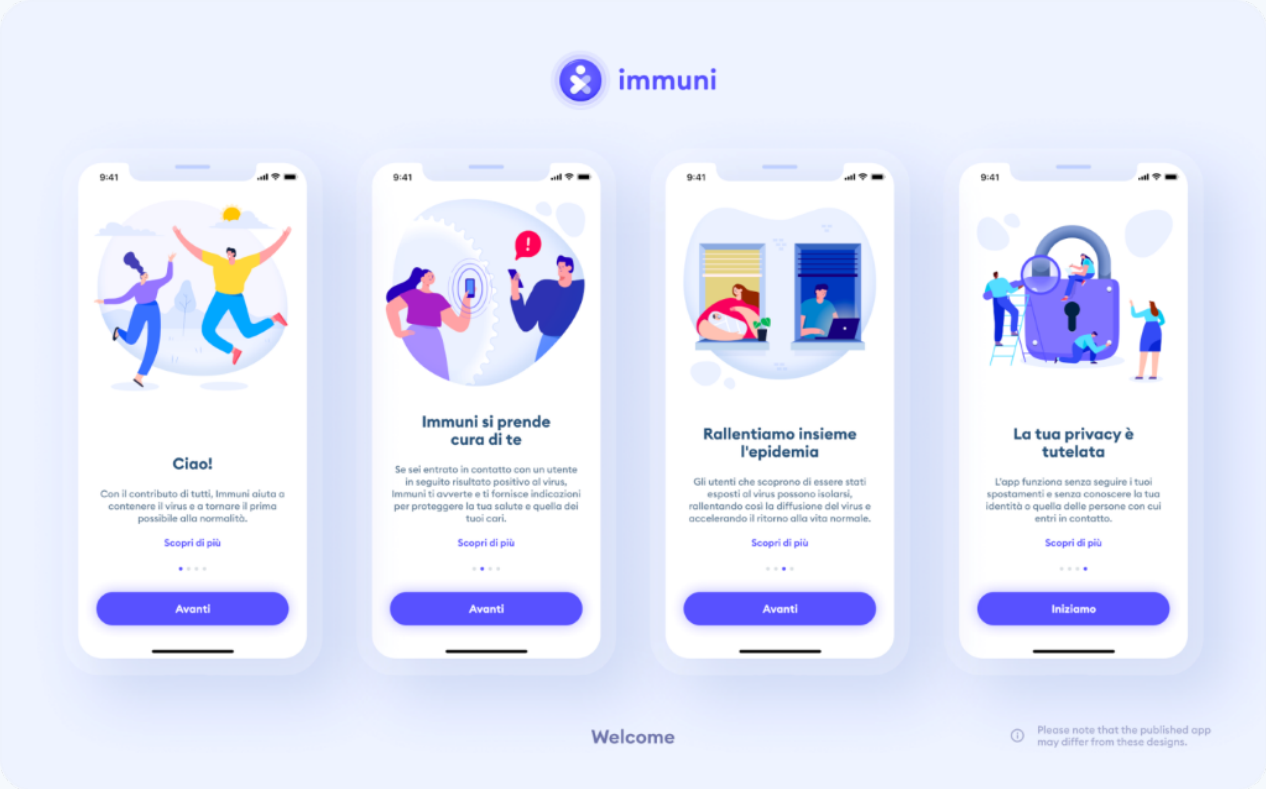
Figura 2. Captures de pantalla de Apple Store de l'App Immuni

Pots descarregar Immuni des de qualsevol part de món.

No obstant això, per raons de seguretat, hauràs d'estar a Itàlia per poder pujar les teves dades en cas que donis positiu en la prova de virus. En els dispositius iOS, l'intercanvi dels codis aleatoris es desactivarà si et trobes a l'estranger.

Un cop més a causa de motius de seguretat, no podràs establir connexió amb el servidor que et permet descarregar els codis aleatoris dels usuaris que han donat positiu si estàs fora del territori europeu.

De moment, Immuni només detecta els contactes amb altres usuaris de l'aplicació. A nivell europeu, s'està treballant per permetre que les diferents aplicacions nacionals de rastreig de contactes, inclosa Immuni, es comuniquin entre si. Gràcies a aquesta col·laboració, també els estrangers que viatgin per Itàlia i els italians que viatgin a l'estranger podran fer ús del sistema de rastreig de contactes sense haver de descarregar-altres aplicacions.



Font: Immuni

Pel que fa al servei, s'informa a l'usuari dels següents aspectes pel que fa a la privacitat:

- No recopila el teu nom, cognoms, data de naixement, direcció, número de telèfon ni correu electrònic.
- No pot rastrejar la teva identitat ni la de les persones amb les que entres en contacte.
- No recopila cap dada de geolocalització, incloses les dades de GPS. No es realitza cap seguiment dels desplaçaments de l'usuari.
- Les dades desades en el telèfon intel·ligent i les connexions contra el servidor estan xifrades.
- Per ajudar al Servei Nacional de Salut (SSN), l'aplicació envia al servidor del Ministeri de Salut la següent informació:
    - La província a on resideixes
    - Si l'aplicació funciona correctament
    - Si has rebut un avis d'un contacte de risc
- Les dades es desen en un servidor d'Itàlia, són administrades per entitats públiques i les supervisa el Ministeri de Salut.

- Totes les dades desades s'eliminaran quan deixin de ser necessàries i, en qualsevol cas, el 31 de desembre del 2020 com a màxim.

Una altra dada interessant pel que fa a la privacitat, és que l'aplicació té bloquejada l'opció d'efectuar captures de pantalla, per evitar que dades com el codi aleatori surtin del propi terminal.

En aquest sentit l'Autoritat Italiana de Protecció de Dades Personals ha autoritzat al Ministeri de Salut per iniciar el tractament de dades relatiu al sistema d'alerta Covid-19. A partir de l'avaluació d'impacte transmesa pel Ministeri, el tractament de les dades personals realitzades dins del Sistema s'ha considerat proporcional, ja que s'han previst mesures per garantir el respecte suficient pels drets i llibertats dels afectats, que mitiguen el riscos que es puguin derivar del tractament.

Dades d'ús

Número de descàrregues	Notificacions enviades	Positius registrats a l'APP
10.004.204	81.200	6.380
12/12/2020	*12/12/2020*	*12/12/2020*

AI.2 Corea del Sud

Potser és un dels països modèlics en la contenció i tractament de la malaltia. Probablement l'epidèmia de MERS que els va afectar anys enrere és la principal responsable de que el govern Coreà ja estigues preparat en molts sentits. Entre altres coses ja tenien en vigor una legislació que els hi permet recopilar dades de posició dels mòbils dels ciutadans amb la finalitat de lluitar contra aquest tipus d'epidèmies.

En aquest cas el govern de Corea ha utilitzat l'App **"Self-quarantine app"**, que permet monitoritzar la localització de les persones afectades per la malaltia, dels que encara no estan diagnosticats però tenen símptomes i de les persones de fora del país. L'aplicació requereix de descarrega per part del ciutadà i també haurà d'atorgar els permisos corresponents perquè l'aplicació funcioni. (Kim, 2020)

Com a funcionalitats principals podem destacar:

- Enviament d'alertes a la població
- Geolocalització per control de les quarantenes.
- Localització de punts per fer-se la prova del COVID-19

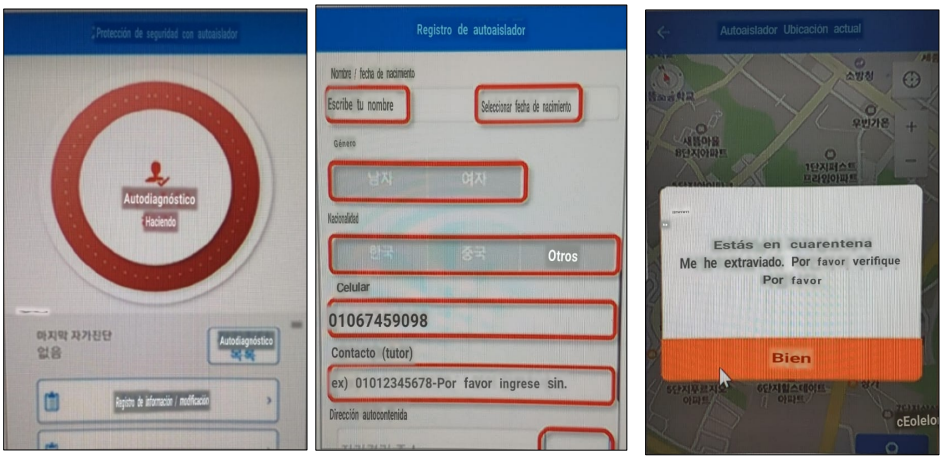


Figura 3 . Captures de pantalla “Self-quarantineapp” (traduïdes del Coreà)

També s’ha posat a disposició de la ciutadania una App anomenada Corona plus que permet conèixer espais on s’han diagnosticat casos positius de Covid19.

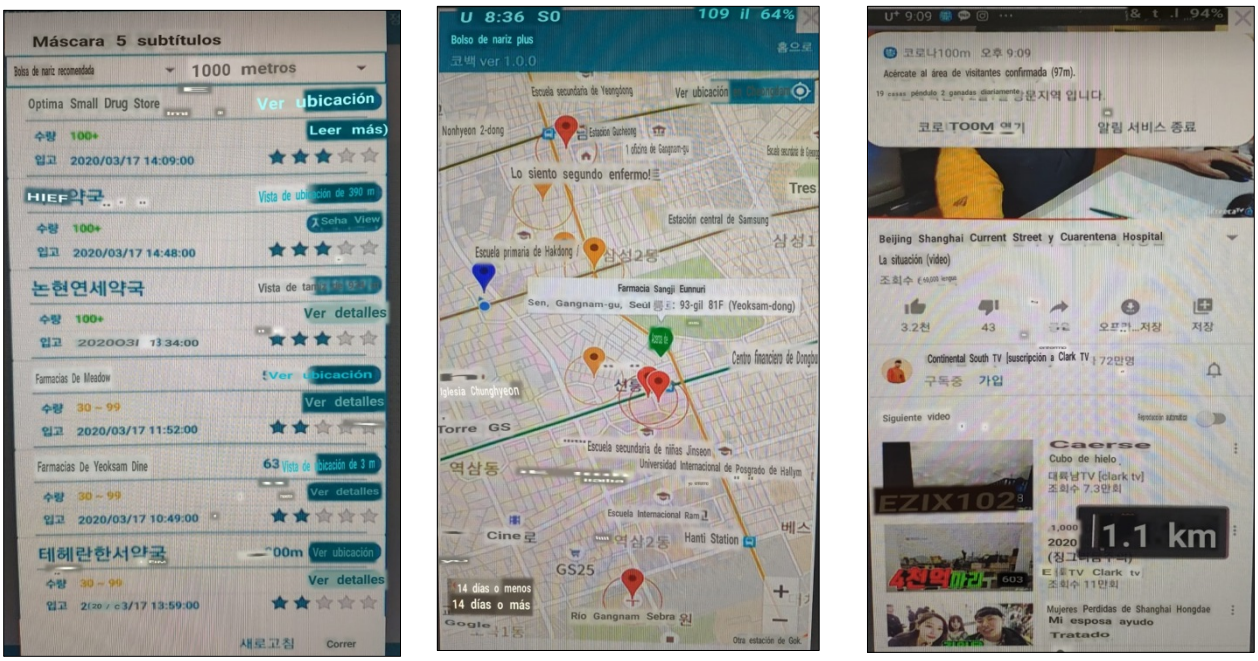


Figura 4. Captures de pantalla “Coronaplus” (traduïdes del Coreà)

AI.3 Singapur

El punt de partida de Singapur es força avantatjós per dos motius principalment. En primer lloc com molts països asiàtics ja va patir en 2002 i 2013 les epidèmies de SARS i MERS fet que podem remarcar com a rellevant a l’hora de tenir establerts protocols, mesures de contenció i una població altament conscienciada. En segon lloc Singapur compta amb els sistema de salut que més esta apostant per la tecnologia aplicada a la promoció de la salut de les persones amb el seu “Health Hub”.

Trace together

El cas de Singapur l'App **"Trace together"** està molt enfocada al seguiment minuciós i gairebé quirúrgic del procés d'infecció. Aquesta aplicació dissenyada per l'agència de tecnologia del govern es basa en la tecnologia Bluetooth i concretament en el protocol Bluetrace per determinar si dos ciutadans han estat a menys de 2m de distancia durant més de 30 minuts. Els creadors asseguren que totes les dades son emmagatzemades en local y pertinentment xifrades. (Goverment Digital services, 2020)

La característica més important d'aquesta aplicació es que permet saber si has estat en contacte amb alguna persona infectada en els últims 21 dies i ser avisat per part de les autoritats competents.

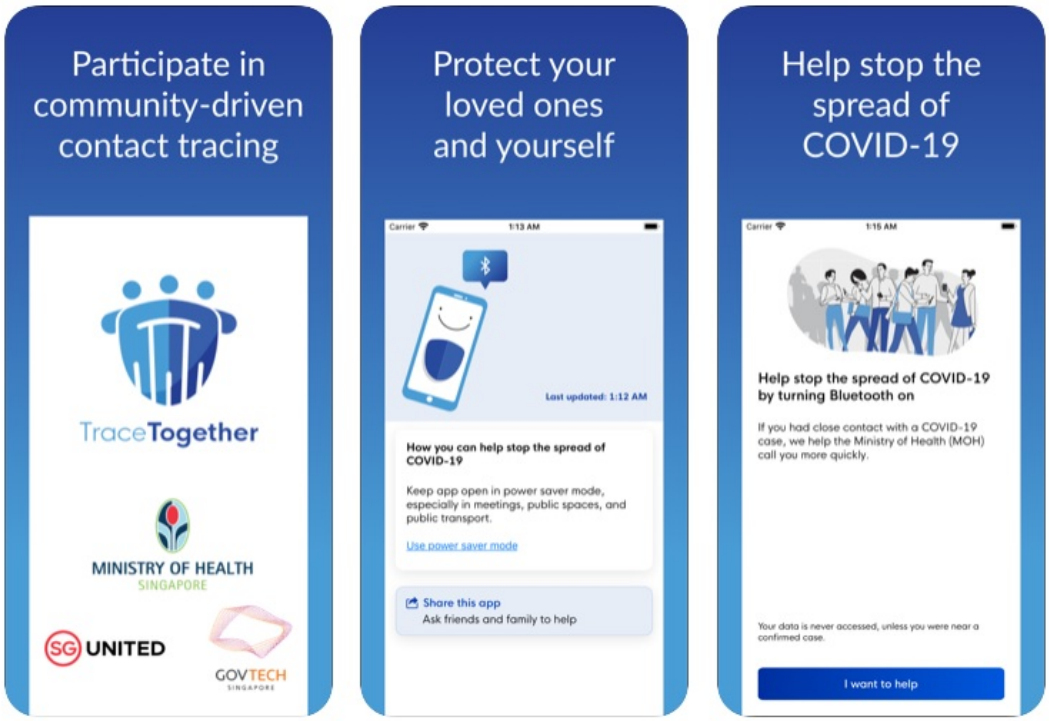


Figura 5. Captures de pantalla de l'App TraceTogether

Tot i així, l'aplicació **no va apostar pel sistema de notificació d'exposició** del COVID-19 de Apple i Google, i va tenir certs problemes ja que a iOS no és possible l'escaneig de Bluetooth en segon pla.

L'aplicació ha tingut un total de **1,5 milions de descàrregues** el que representa un **20-25% de la població de Singapur**. Les dades que tenen més de 25 dies s'eliminen automàticament del telèfon i en cas de d'haver de disposar de les dades de contacte, aquestes podran ser utilitzades per un grup reduït autoritzat pel Ministeri de Salut del país.

Polseres rastrejadores

Una altra mesura que està adoptant el govern de Singapur és el repartiment de polseres rastrejadores a la població (***uns 5,7 milions de residents***) per fer front a la propagació del virus i, d'aquesta manera,

poder conèixer quins han estat els contactes i quins són els focus de contagi. Aquest projecte es troba en fase de proves i encara no se'n coneixen més detalls.

Figura 6. Informació de les polseres rastrejadores de Singapur

El wearable estarà basat en tecnologia Bluetooth, i no serà necessari que els ciutadans disposin d'un telèfon mòbil per poder-ho utilitzar. L'aplicació TraceTogether no funciona igual de bé amb tots els sistemes operatius i per aquest motiu no la van poder fer d'obligat ús a tota la població.

Aplicació SafeEntry

A banda d'aquests projectes, Singapur també ha realitzat una altra mesura pel que fa al desconfinament. Es tracta del sistema **SafeEntry**, **d'obligat compliment per tota la població** que es va posar en funcionament el 23 d'abril.

SafeEntry és un sistema de registre digital a través del dispositiu mòbil que exigeix a tots els negocis i comerços realitzar un **registre del nom, DNI telèfon i hora de tots els visitants quan entren i surten de la botiga**.

L'aplicació **SafeEntry** consisteix en realitzar tres passos:

1. A la pantalla principal apareix el codi QR necessari escanejar per accedir a l'aplicació
2. S'escull si s'està entrant (*Check-in*) o sortint (*Check-out*) de la botiga.
3. El sistema sol·licita les dades requerides a través d'un formulari (nom complert, número de passaport o NRIC i el telèfon mòbil). Aquestes dades poden ser introduïdes manualment, o a través de l'aplicació SingPass.

4. Totes les dades són emmagatzemades al núvol de l'aplicació i són consultades només per personal autoritzat.

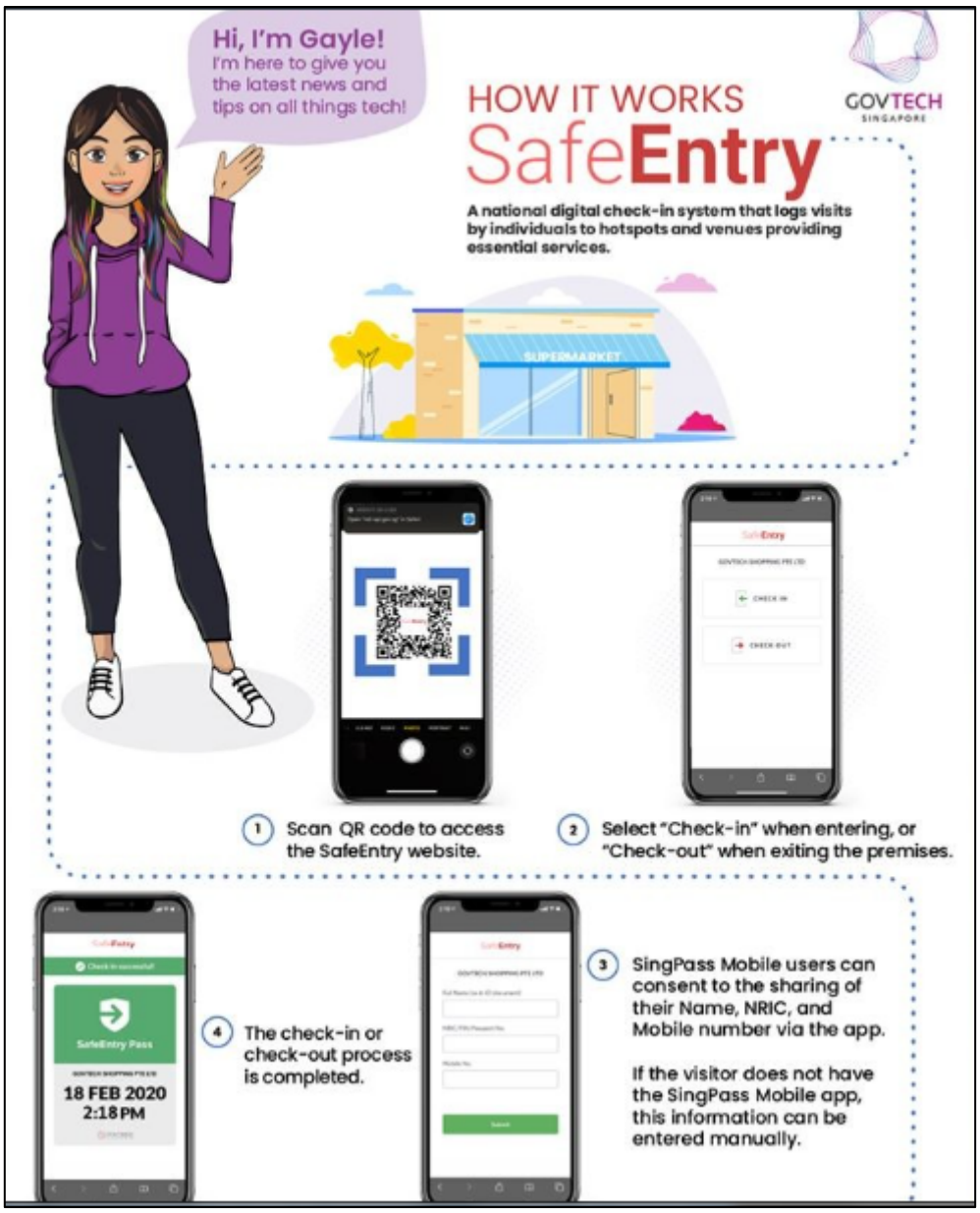


Figura 7. Diagrama funcional de l'App SafeEntry (*captura extreta de xataka*)

AI.4 Letònia

El govern de Letònia, va publicar el 29 de maig del 2020 l'App oficial d'enregistrament de contactes de COVID-19, l'App **Apturi Covid.** L'aplicació no registra la ubicació, les dades només s'emmagatzemen al dispositiu i se suprimeixen automàticament al cap de 14 dies. Si s'escull proporcionar un telèfon de contacte, el servei només rebrà aquesta dada.

L'aplicació notifica als contactes en el cas que un d'aquests contactes estigui notificat com a contacte malalt de COVID-19, sense revelar la identitat del remitent ni el destinatari. També aporta informació sobre la malaltia i indicacions de què fer en cas de ser notificat.

L'aplicació utilitza l'API de notificació d'exposició d'Apple per a la privadesa i seguretat.

Àrea de Descàrrega a AppStore: https://apps.apple.com/us/app/apturi-covid-latvia-spkc/id1513573144

Àrea de Descàrrega a Google play: https://play.google.com/store/apps/details?id=lv.spkc.gov.apturicovid

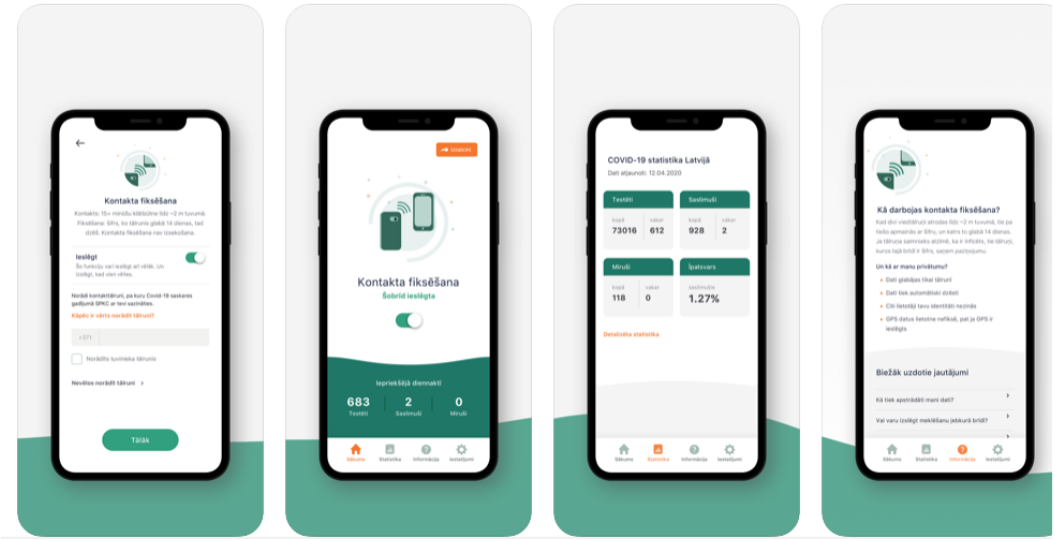


Figura 8. Captures de pantalla de l'App Apturi Covid (*captures extretes de AppStore*)

AI.5 Israel

En el cas d'Israel no podem dir que tinguessin experiència prèvia en la contenció d'epidèmies víriques com les que van afectar l'Àsia. Tot i això el govern del país ha desenvolupat una aplicació denominada **"Hamagen"** que permet als usuaris que la descarreguen comprovar si han tingut contacte amb alguna persona infectada per Covid19.

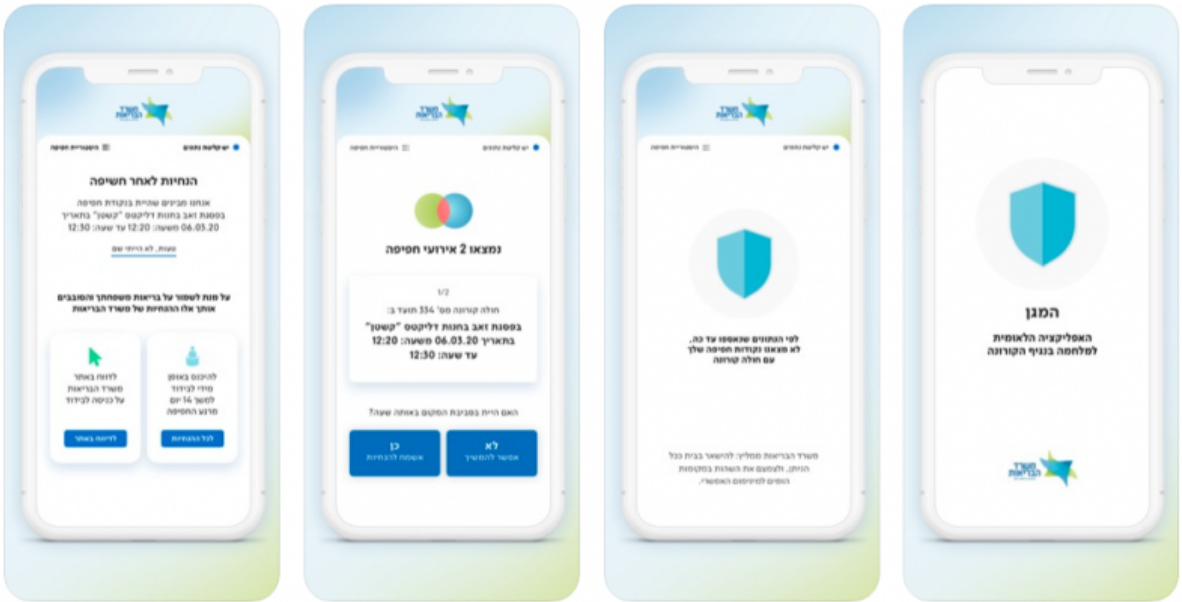


Figura 9. Captures de pantalla de l'App Hamagen (*captures extretes de AppStore*)

Els desenvolupadors recullen a la descripció de l'aplicació que els seu funcionament es basa en recollir la posició GPS de l'usuari per fer una comparació amb la posició d'aquelles persones que han estat diagnosticades amb COvid19. Es realitza un creuament d'aquestes dades i s'avisa de possibles contactes de risc.

AI.6 Hong Kong

En el cas de Hong Kong a la mesura de gestionar una o diverses Apps que garanteixi el confinament dels ciutadans s'ha optat per incorporar una polsera que registri possibles canvis d'ubicació. Per reforçar la unió de la persona amb el dispositiu mòbil s'ha optat per una polsera senzilla que està en contacte permanent amb l'App en cas de que es trenqui la comunicació entre la polsera i el mòbil o que l'individu es tregui la polsera, es produeix un avís cap a les autoritats del país. (News.gov.hk, 2020).

AI.7 Vietnam

Concretament a la capital Hanoi, s'ofereix a la població l'aplicació "SmartCity". Aquesta aplicació esta especialment pensada per les persones a les que se'ls hi ha decretat confinament o totes aquelles que resten en quarantena. Aquesta App utilitza també sistemes de geolocalització per advertir a les autoritats i als veïns més propers quan alguna d'aquestes persones se salta el confinament o la quarantena decretats.

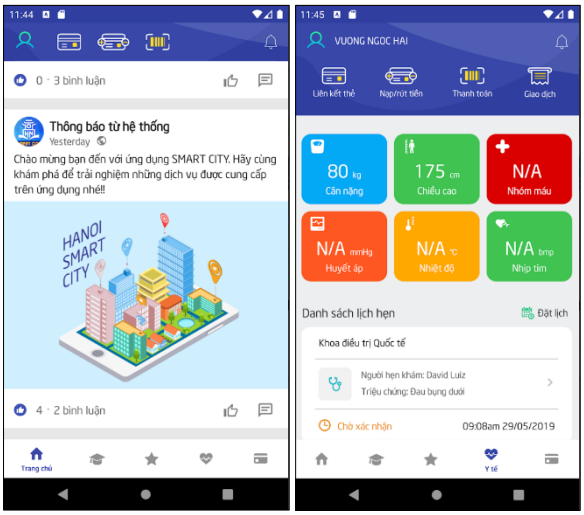


Figura 10. Captures de pantalla de l'App SmartCity (*captures extretes de AppStore*)

AI.8 França

Nom: TousAntiCovid

TousAntiCovid és una aplicació que permet participar a tothom en la lluita contra l'epidèmia. És un gest de barrera addicional que activem en tot moment quan hem d'estar molt atents: als restaurants, al menjador, quan anem a un gimnàs, quan participem en un esdeveniment professional, quan hi ha té el risc que tothom no respecti els altres gestos de barrera.

TousAntiCovid complementa l'acció dels metges i l'Assegurança de Salut, encaminada a contenir la propagació de virus detenint les cadenes de contaminació el més ràpid possible.

Nom: TousAntiCovid

Versió: 2.2.0

Data de llançament: 22/10/2020

Enllaç de descàrrega Google Play:
https://play.google.com/store/apps/details?id=fr.gouv.android.stopcovid&hl=en_US&gl=US

El principi és el següent: prevenir, garantint l'anonimat, les persones que han estat al voltant d'una persona que ha donat positiu, perquè puguin acudir a fer-se la prova i ser atesos el més aviat possible.

També permet estar informat sobre l'evolució de l'epidèmia i sobre les accions a prendre i així romandre alerta i adoptar les accions adequades.

Proporciona un fàcil accés a les altres eines disponibles per als ciutadans que desitgin participar en la lluita contra l'epidèmia: DepistageCovid, que ofereix un mapa dels laboratoris propers i els temps d'espera, i el consell d'MesCovid, que brinda consells personalitzats per a protegir-se a si mateix i als altres.

La instal·lació de l'aplicació TousAntiCovid es realitza de forma voluntària.

-Per què va reemplaçar StopCovid per TousAntiCovid? Quines novetats porta l'aplicació TousAntiCovid?

En un context de major acceleració de l'epidèmia, el govern ha reafirmat l'estratègia nacional de lluita contra el virus "Prova, Alerta, Protegeix".

Les eines digitals estan a el servei d'aquesta estratègia.

TousAntiCovid és una versió enriquida i interactiva de la primera aplicació StopCovid que li va permetre ser alertat i alerta en cas de proximitat a una persona que va donar positiu. Aquesta alerta permet que l'usuari sigui avaluat com una prioritat, a l'igual que una persona de contacte identificada pels metges o l'assegurança mèdica.

L'aplicació TousAntiCovid també porta els canvis següents:

- un entorn visual optimitzat i ergonomia amb accés instantani a totes les funcionalitats de l'aplicació;
- un centre d'informació, que li ofereix informació sobre la situació epidemiològica a França, així com notícies relacionades amb la lluita contra l'epidèmia (exemple: mesures posades en marxa per les autoritats nacionals i locals);
- major transparència amb la publicació automàtica i periòdica de xifres sobre l'ús de l'aplicació;
- accés a DépistageCovid, el mapa actualitzat dels centres de detecció amb informació sobre els temps d'espera informats pels usuaris;
- accés a MyCovidAdvices per assessorament personalitzat;
- accés més fàcil al certificat de viatge excepcional.
- L'aplicació seguirà enriquint periòdicament amb nova informació i nous serveis.

-Com puc instal·lar l'aplicació en el meu telèfon?

Descarrego l'aplicació buscant "TousAntiCovid" a Play Store si tinc un telèfon Android o en App Store si ús un iPhone.

També puc escanejar el codi QR amb el meu telèfon. L'aplicació és gratuïta i no li demana que ingressi informació personal. Si escaneja un codi QR, assegureu-vos que l'enllaç ho enviï a l'aplicació governamental TousAntiCovid.

Activi el Bluetooth. Autoritzi l'aplicació a utilitzar Bluetooth. Per defecte, les aplicacions s'actualitzen en segon pla en el seu telèfon intel·ligent. Si té un iPhone i no ha permès que les aplicacions s'actualitzin, ho ha de fer a Configuració> General> Actualització en segon pla.

Si ja ha descarregat l'aplicació StopCovid, no la desinstal·li: s'oferirà una actualització automàticament.

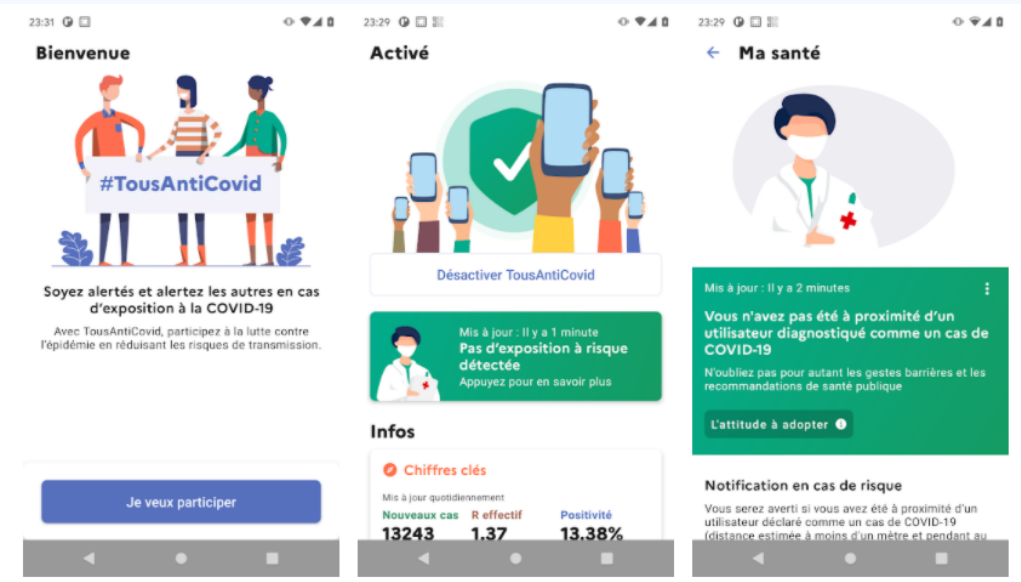


Figura 11. Diferents captures de pantalla de l'aplicació TousAntiCovid

-Com funciona?

Quan dos telèfons es creuen durant al menys 15 minuts dins d'un metre, cada un guarda a l'altre en el seu historial d'aplicacions de forma encriptada. Això permet de forma retrospectiva que, quan una persona es declara positiva en l'aplicació, s'adverteix a tots els usuaris de TousAntiCovid que s'ha trobat. Els telèfons han d'estar prop durant al menys 15 minuts a una distància de menys d'un metre. Aquests criteris són definits pel Ministeri de Solidaritat i Salut i poden canviar amb el temps depenent de el coneixement de l'epidèmia.

Quan una persona dóna positiu, se li dóna un codi únic amb el resultat de la prova. Si ho desitja, pot utilitzar aquest codi per indicar a l'aplicació que ha donat positiu.

Es convida a les persones alertades per l'aplicació a aïllar-se i realitzar una prova de detecció.

La tecnologia utilitzada és només Bluetooth. El Govern ha decidit no utilitzar tecnologies que utilitzin la geolocalització de persones.

-Quan he activar l'aplicació?

La funcionalitat per a ser alertat en cas de contacte o poder alertar a les persones creuades en cas d'una prova positiva requereix JavaScript Bluetooth i no tancar l'aplicació.

És útil comprovar que la teva aplicació està activada quan et trobes en una situació de risc, quan no es garanteix l'ús de màscara o el respecte de les distàncies, en llocs concorreguts o reduïts. Es recomana encaridament, per exemple, activar l'aplicació en les següents situacions:

- En transports públics;
- En restaurants, bars, cantines i restaurants universitaris;
- En botigues;

- En pavellons esportius i clubs;
- Quan estic amb persones fora de casa (amics, companys), ja sigui en espais públics o privats.

L'objectiu és poder rastrejar ràpidament les cadenes de contaminació si una de les persones dóna positiu en la prova.

Dades d'ús

Número de descàrregues	Notificacions enviades	Positius registrats a l'APP
8.560.750	11.613	46.613
16/112/2020	*16/11/2020*	*116/11/2020*

AI.9 Irlanda

Nom: Covid Tracker

Versió: 1.0.1.44

Data de llançament: 17/07/2020

Enllaç de descàrrega: https://play.google.comom.covidtracker.hse

Descàrregues: 500K a Andorid

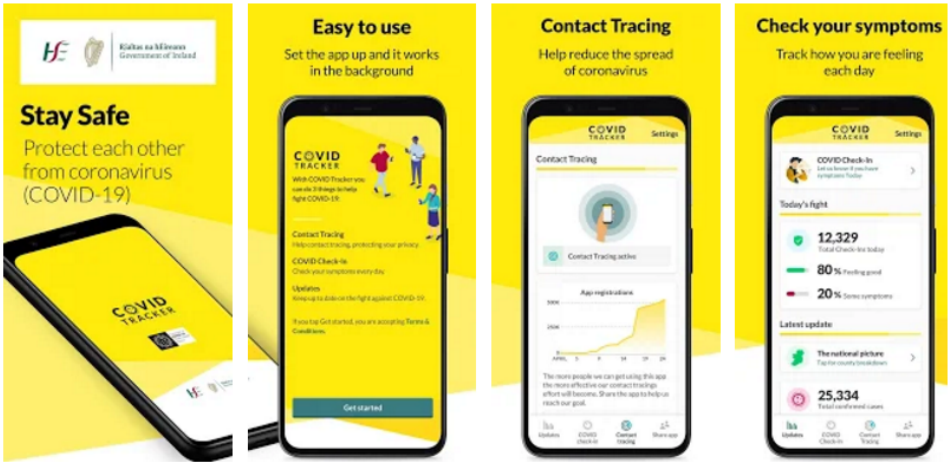


Figura 12. Captures de pantalla de l'App CovidTracker

Irlanda, també a posa't a l'abast de la ciutadania una aplicació per al rastreig de contactes. Actualment un 30% de la població amb terminals compatibles ja ha descarregat el software. El govern Irlandès ha apostat de forma decidida per la transparència en aquest projecte. Han optat per un model descentralitzat i per la API de Google i Apple. Respecte a funcionalitats cap a destacar.

L'element més destacat és la donació del codi que ha fet el govern irlandès a la Fundació Linux. Actualment el codi de l'aplicació està sota Llicencia Apache 2.0 i es pot trobar en el repositori de Github que gestiona la mateixa Fundació, anomenat Covid Green.

AI.10 Suïssa

Nom: SwissCovid app

L'aplicació **SwissCovid** per a telèfons mòbils (Android / iPhone) contribueix a contenir el coronavirus. Complementa el rastreig de contactes convencional dut a terme per les autoritats per rastrejar les noves infeccions. Així, les cadenes de transmissió es poden trencar més ràpidament. L'aplicació SwissCovid està disponible a l'Apple Store i a Google Play Store.

L'ús de l'aplicació SwissCovid és voluntari i gratuït. Com més gent instal·li i utilitzi l'aplicació, més eficaç ens pot ajudar a combatre el nou coronavirus.

Quan es troben dins del rang de Bluetooth, els telèfons mòbils en els quals s'instal·la l'aplicació SwissCovid o aplicacions compatibles intercanvien identificacions aleatòries (codis d'identificació) entre si. Aquests identificadors romanen emmagatzemats als telèfons mòbils durant 14 dies i, posteriorment, se suprimeixen automàticament.

Les aplicacions compatibles amb l'aplicació SwissCovid són aplicacions similars d'altres països (per exemple, l'aplicació alemanya Corona-Warn). Actualment s'emmagatzemen els identificadors aleatoris dels que tenen aplicacions d'altres països, però igualment no és possible rebre notificacions d'aquestes altres aplicacions similars.

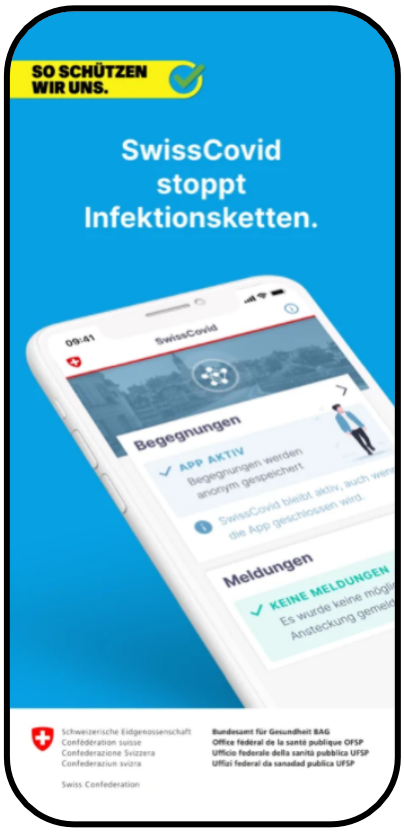


Figura 13. Captura de pantalla de l'aplicació SwissCovid.

Nom: SwissCovid

Versió: 1.3.0

Data de llançament: 27/05/2020

Enllaç de descarrega: https://play.google.com/store/apps/details?id=ch.admin.bag.dp3t

Suïssa ha creat SwissCovid, una aplicació de traçabilitat de contactes que acumula una mica més dos milions vuit-centes mil descarregues. Ha estat la primera App en incloure la API de Google/Apple. Actualment es pot descarregar i utilitzar-la sense restriccions.

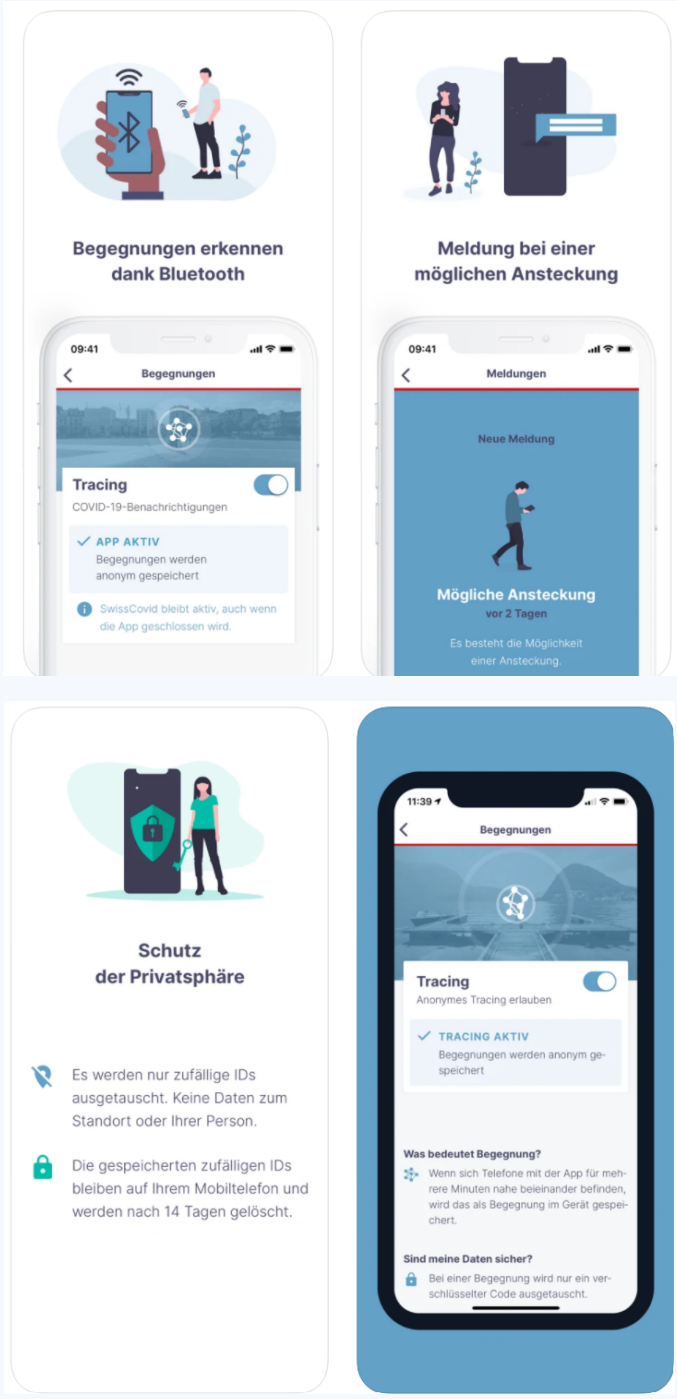


Figura 14. Captures de pantalla de l'App Swiss Covid

El govern Suïs va ser el primer en publicar una App en versió beta, que fes servir les APIs de rastreig de contactes promogudes per Google i Apple. El seu us es va testar amb membres de l'exercit i personal d'emergències.

A nivell funcional comparteix les mateixes característiques que altres Apps Europees que utilitzen l'API Google/Apple. Cal destacar que a nivell de disseny s'ha optat per un estil marcadament Suïs molt propi del país i que és l'estil habitual a la major part d'eines digitals promogudes al país helvètic.

Si l'usuari ha instal·lat l'aplicació SwissCovid i ha donat positiu al coronavirus, rebrà un Covidcode (codi de llançament). Els codis Covid poden ser emesos per les autoritats cantonals i els metges que realitzen proves.

El Covidcode permet activar la funció de notificació a l'aplicació, cosa que permet advertir altres usuaris de l'aplicació amb els quals s'ha entrat en contacte durant la fase infecciosa (començant dos dies abans de l'aparició dels símptomes), de manera automàtica i anònima. Les persones que reben alertes no són informades de la identitat de la persona que ha activat la notificació. No obstant això, és possible que algú pugui esbrinar la identitat del contacte en funció de la data.

Es rep una notificació en les dues condicions següents:

En un període de 24 hores, si s'ha tingut contacte amb una persona infectada:

- a una distància inferior a 1,5 metres
- durant almenys 15 minuts

O bé:

En un període de 24 hores, si s'ha tingut contacte amb diverses persones infectades:

- a una distància inferior a 1,5 metres
- durant menys de 15 minuts per persona
- però durant un total de més de 15 minuts en general

<u>Dades d'ús</u>

Número de descàrregues	Positius registrats a l'APP
2.822.148	34.554
10/12/2020	*10/12/2020*

AI.13 Alemanya

Nom: Corona-Warn-App

Corona-Warn-App és una aplicació de seguiment de contactes COVID-19 que s'utilitza per al seguiment digital de contactes a Alemanya. Els experts creuen que el temps estalviat mitjançant l'aplicació pot ser fonamental per millorar l'eficàcia del seguiment dels contactes.

Figura 15. Captura de pantalla de la versió d'Android, que mostra una avaluació de "baix risc" juntament amb orientacions sobre mesures de prevenció com el rentat de mans.

Nom: Corona-Warn-App

Versió: 1.5

Data de llançament: 16/06/2020

La nova versió 1.5 de l'aplicació alemanya Corona-Warn admet el nou servei de passarel·la d'interoperabilitat europea, que permet que les aplicacions nacionals de rastreig i advertència de contactes interaccionin entre elles.

Enllaç de descàrrega: https://play.google.com/store/apps/details?id=de.rki.coronawarnapp

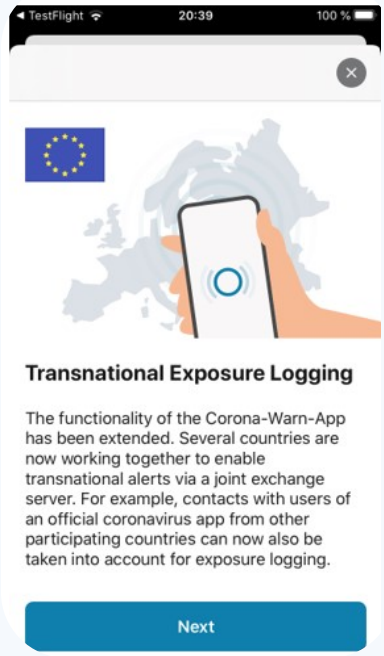


Figura 16. Nou servei de passarel·la d'interoperabilitat europea

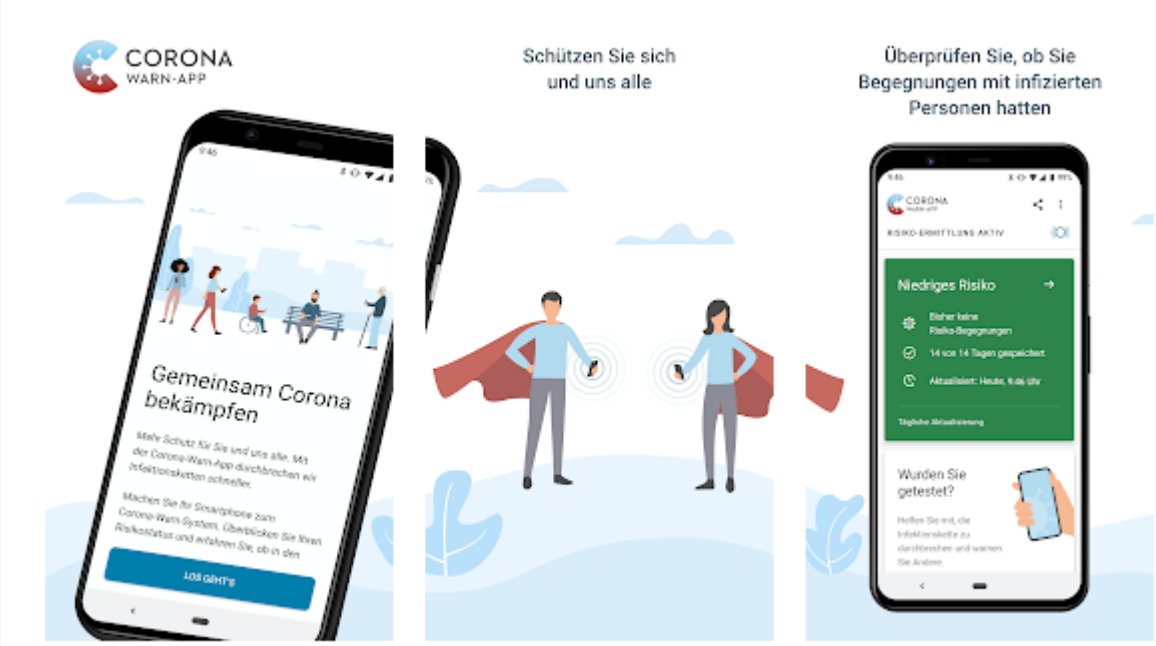


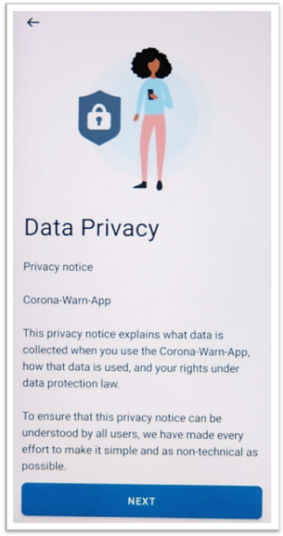
Figura 17. Captures de pantalla de l'App Corona-Warn-App (*captura extreta de l'AppStore*)

Les dades que s'aporten a la pàgina web del projecte i als corresponents repositoris de GithHub, indiquen que és un projecte de codi obert. Expressen la voluntat de l'App de no recollir cap mena de dada personal.

L'App Utilitza les API de Google i de IOS per a fer el seguiment mitjançant Bluetooth. Respecte a la comunicació de positius.

La comunicació de casos positius, es basa en la comunicació proactiva del propi ciutadà dels codis generats durant els últims 14 dies. La App verificarà els resultats del test en el Backend amb els laboratoris alemanys. Un cop verificat el positiu s'utilitzaran els codis lliurats per l'usuari per alertar als possibles contactes.

Procés d'instal·lació.



No requereix cap identificació personal.

L'aplicació realitza un recorregut informatiu en el moment de la instal·lació on s'explica:

Utilitat de l'App

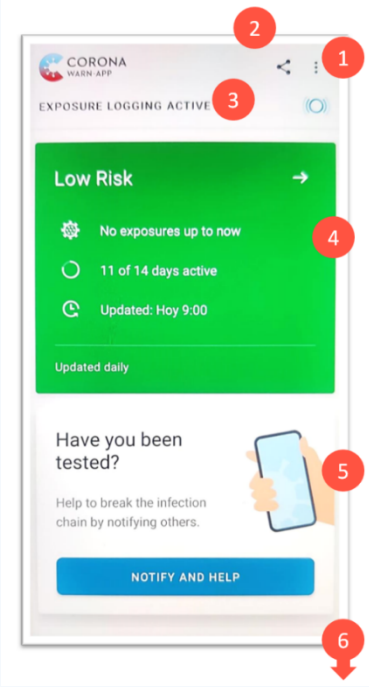
Política de privadesa

Funcionament breument

També es realitza el procés d'activació de la funcionalitat de rastreig per Bluetooth de forma assistida.

**No permet fer captures de pantalla.*

Anàlisis del Continguts:



<u>Pantalla Principal</u>

En la part superior de la pantalla principal trobem les icones de menú i de compartir. (1) (2) Tot seguit una barra d'estat (3) on s'indica si tenim activat el rastreig de contactes.

<u>1-Risc d'infecció:</u> (4) Indica el risc d'infecció calculat per l'App en funció dels contactes i de la seva proximitat que hem tingut en els últims 14 dies.

- Alt Risc
- Baix Risc
- Risc Desconegut

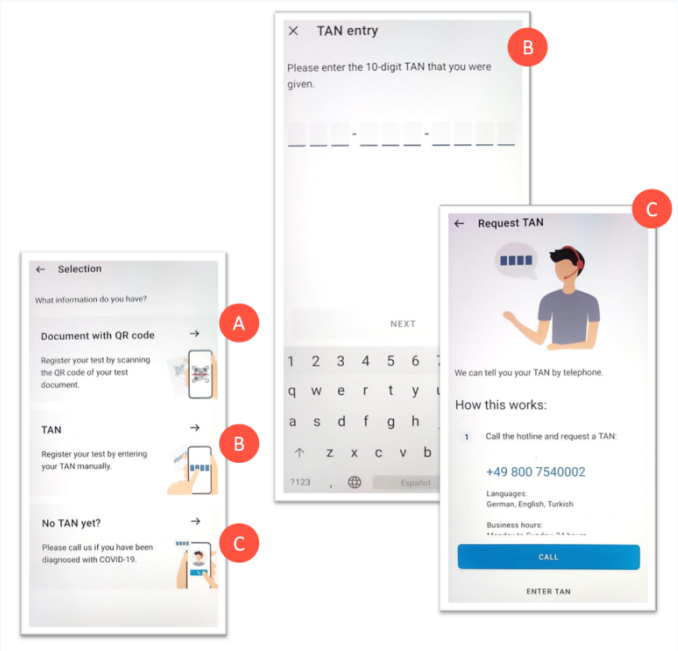
Al final d'aquest apartat es detallen recomanacions higièniques.

Notificació de contagis: (5)

Preguntes Freqüents: (6)

Al final d'aquest apartat es detallen recomanacions com: Rentat de mans, distància, ús de mascareta, etc. Desconeixem si les recomanacions varien en funció del risc detectat. En tot cas seria interessant que aquestes recomanacions s'adeqüessin al risc de contagi de que es mostra en cada moment.

2-Notificació a altres usuaris: En aquesta segona targeta podem trobar la manera de registrar el resultat d'un test de Covid-19. D'aquesta forma notificar-ho al possibles contactes i contribuir a trencar la cadena de contagis.



El procés de comunicació ens informa que només es comunicaran una sèrie d'IDS aleatòries preservant en tot moment el nostre anonimat.

Per tal de registrar el positiu l'App ens dona 3 opcions un codi QR un codi TAN o la possibilitat de demanar la confirmació telefònicament.

- **Codi QR:** Ens sol·licita permís de la càmera per la lectura del codi i ens explica el mecanisme de funcionament dels tests, on els podem visualitzar i com revocar els permisos. (No hem pogut continuar amb el procés) (A)
- **Codi TAN:** Sol·licita un codi de 10 xifres que el ciutadà te i que va associat al test realitzat. (No hem pogut continuar amb el procés) (B)
- **Demanar un codi TAN:** La ultima opció es demanar un codi TAN per telèfon, per després introduir-lo a l'App mitjançant la opció anterior. El telèfon es gratuït i l'atenció es fa en Alemany, Angles i Turc. (C)

3- FAQS: Es tracta d'un enllaç extern a una pàgina web (convenientment indicat) on es fa un recull de preguntes freqüents i les seves corresponents respostes.

- Per què es necessària l'App Corona Warn?
- Que fa l'App Corona Warn?
- Com funciona l'App?
- Quins son els requeriments mínims per poder utilitzar-la?
- Quins criteris utilitza l'App per establir quin risc d'exposició em correspon?
- Com afecta l'ús de l'App al emmagatzematge i a la bateria del meu dispositiu?
- Per què es necessita un servidor central si aquesta es una solució deslocalitzada?
- Com Corona Warn vetlla per la seguretat i la protecció de les meves dades?
- Quina informació personal guarda l'App?
- Existeix interoperabilitat amb altres països Europeus?
- Cobraré la baixa si l'App em suggereix que em confini al domicili?

A banda d'aquestes preguntes també ens ofereix un glossari i un document més extens amb preguntes menys freqüents.

Menú

El menú conté tres opcions diferenciades:

1. Overview: Ofereix una explicació esquemàtica de les funcions que es poden trobar a la pantalla principal. Una explicació gràfica complementada de les funcions complementada amb una definició dels termes més importants que s'utilitzen a l'App.
2. App information: Submenú on es recull tota la informació referent a l'App.

2.1- About the App: Explicació breu del responsable de l'Appp i explicacions respecte aspectes a tenir en compte en el maneig de la situació d'epidemia a abanda de l'ús de l'App.

2.2- FAQS. (Explicat anteriorment)

2.3- Terms of use: En aquest extens apartat es detallen tots i cadascun dels termes i drets d'us de l'App. Cal destacar l'índex en forma de preguntes en alguns casos que facilita molt enfrontar-se a un document d'aquesta magnitud. Tot i això seria recomanable que aquest índex fos clicable per facilitar-ne la lectura.

2.4- Data Privacy Information: En aquest apartat s'exposa tota la informació referent a la privacitat de les dades. Donat que torna a ser un apartat molt extens trobem a faltar un petit índex clicable que ens ajudi a consultar aquelles parts del text que realment tenim interès de consultar.

2.5- Legal Notices: Ens aporta tota aquella informació referent a llicencies de les diferents parts de l'App.

2.6- Techinical hotline: Ens ofereix un telèfon de contacte per tractar qualsevol incidència tècnica. Ens sobta que no s'ofereixi la possibilitat de contactar de forma asíncrona, mitjançant formulari de contacte o correu electrònic.
En aquest mateix apartat també ens ofereixen els telèfons de contacte per qüestions clíniques.

2.7- Publication details: S'explica qui és el responsable de la publicació de l'App i totes les dades de contacte com l'adreça, correu electrònic, telèfon i fins i tot el VAT.

Fora del menú es mostra la versió de l'App que tenim actualment instal·lada en el nostre terminal.

3. Settings: Ens permet controlar i modificar els aspectes tècnics i de funcionament de l'aplicació.

3.1- Expossure Logging: Activa i desactiva el rastreig de contactes. Inclou una petita explicació del funcionament.

3.2- Notifications: Permet activar i desactivar les notificacions de l'aplicació.

- Canvis en el risc d'infecció i l'estat del test de covid-19

Dins d'aquest apartat també trobem la opció de ressetejar les dades d'exposició que s'han obtingut en els darrers dies.

Dades actualitzades

Número de descàrregues	Positius registrats a l'APP
23.800.000	127.765
10/12/2020	*13/12/2020*

AI.14 Croàcia

Nom: Stop COVID-19

Stop COVID-19 és una aplicació que serveix per advertir als ciutadans que es poden trobar en contacte epidemiològicament de risc. Ajuda a prendre la decisió correcta en cas de desenvolupar símptomes: pots proporcionar a l'epidemiòleg informació precisa i clara sobre l'exposició. En cas de no presentar símptomes i l'aplicació adverteix que heu estat en contacte epidemiològicament de risc, per tal de prestar més atenció a la higiene i la distància física.

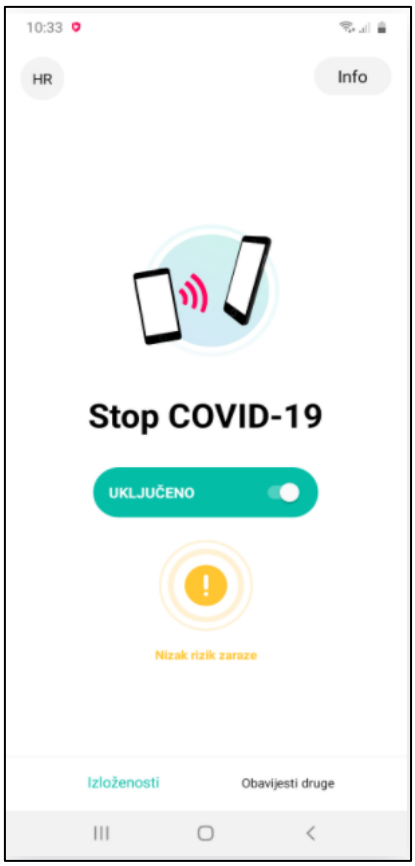


Figura 18. Primera pantalla al inicialitzar l'app Stop COVID-19

Nom: Stop COVID-19

Versió: 2.2.0

Data de llançament: 27/7/2020

Enllaç de descàrrega GooglePlay:
https://play.google.com/store/apps/details?id=hr.miz.evidencijakontakata&hl=en_US&gl=US

L'aplicació COVID-19 es basa en el sistema de "Notificació d'exposició" de Google / Apple. L'aplicació requereix el consentiment explícit de l'usuari, que pot retirar-se en qualsevol moment. L'aplicació és completament voluntària en tots els passos d'ús i l'usuari gestiona completament les dades que desitgi. Els positius de COVID-19 mai han estat identificats per Apple i Google

A mitjans de novembre, l'intercanvi de dades transfronterers entre l'aplicació croata Stop COVID-19 i les aplicacions oficials d'altres estats membres de la UE es va establir com a resultat de decisions i recomanacions de la Comissió Europea i requisits tècnics i de seguretat,. e-salut i altres organismes europeus.

A l'instal·lar l'aplicació, a més d'habilitar la configuració per a l'intercanvi de dades transfronterers, s'assegurarà rebre una notificació d'exposició en cas de viatge a l'estranger o interacció amb usuaris d'altres aplicacions mòbils COVID-19 autoritzades a Croàcia. L'intercanvi de dades transfronterer entre aplicacions nacionals de seguiment de contactes mòbils es defineix en la *Decisió d'Execució (UE) 2020/1023 de la Comissió, de 15 de juliol de 2020.*

Com funciona Stop COVID-19?

L'aplicació assigna claus aleatòries a tots els telèfons mòbils.

Les claus són una cadena de caràcters aleatòria i no contenen informació sobre el dispositiu o sobre dades personals. S'alternen diverses vegades cada hora per mantenir la seva privacitat protegida en tot moment.

Els dispositius mòbils propers estan intercanviant les seves claus aleatòries.

Quan està a prop d'un altre usuari de l'aplicació, els telèfons mòbils intercanvien claus a través de la funció Bluetooth. Per tant, l'aplicació pot rastrejar els contactes realitzats sense identificar l'usuari ni a la persona amb la qual va estar en contacte.

I si l'usuari és positiu?

Els usuaris que reben un resultat de laboratori positiu poden enviar les seves claus aleatòries transmeses en el període anterior, posant-les a disposició d'altres usuaris de l'aplicació. L'enviament de claus aleatòries es realitza ingressant el codi generat per un professional de la salut després de rebre un resultat de laboratori positiu.

Cada mòbil verifica si ha estat en contacte amb les claus que es comparteixen.

L'aplicació comprova periòdicament les claus compartides amb el servidor i les compara amb les claus emmagatzemades al mòbil. D'aquesta manera, l'aplicació pot determinar si l'usuari ha estat exposat a el risc d'infecció.

L'usuari rep una notificació si l'aplicació ha trobat una clau compartida en el seu telèfon mòbil.

Si ha estat en contacte amb una persona que ha compartit les seves claus després d'una troballa positiu, es rep una notificació i instruccions sobre com procedir. L'aplicació no necessita informació sobre on o amb qui ha estat l'usuari, de manera que la seva privacitat està protegida.

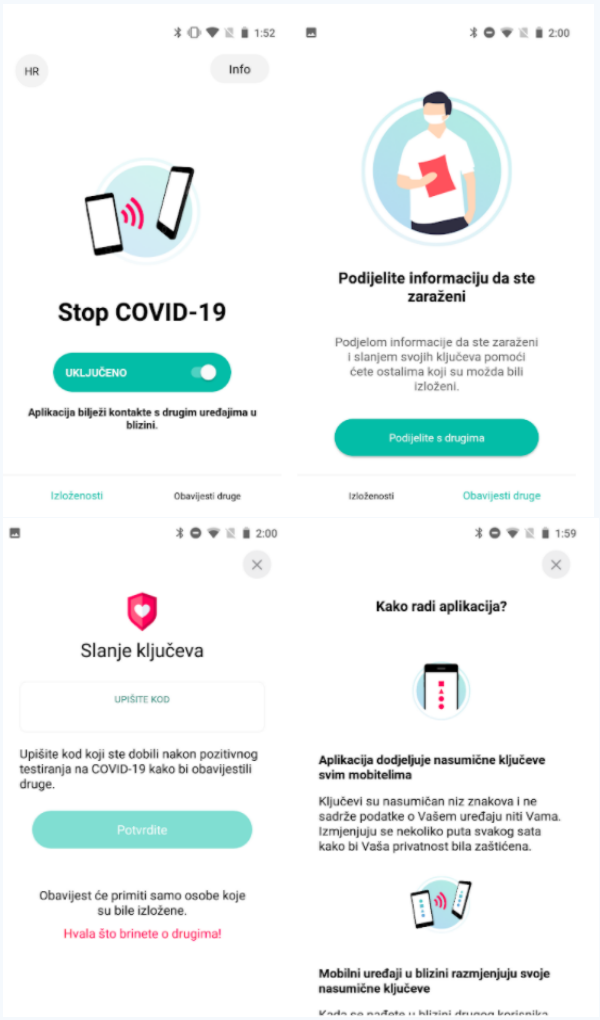
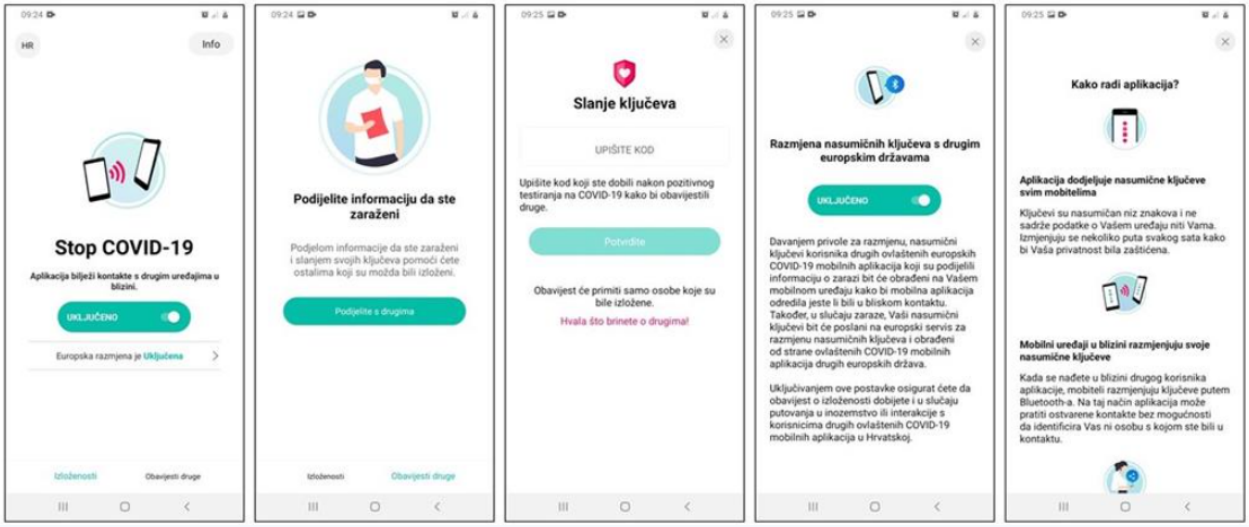


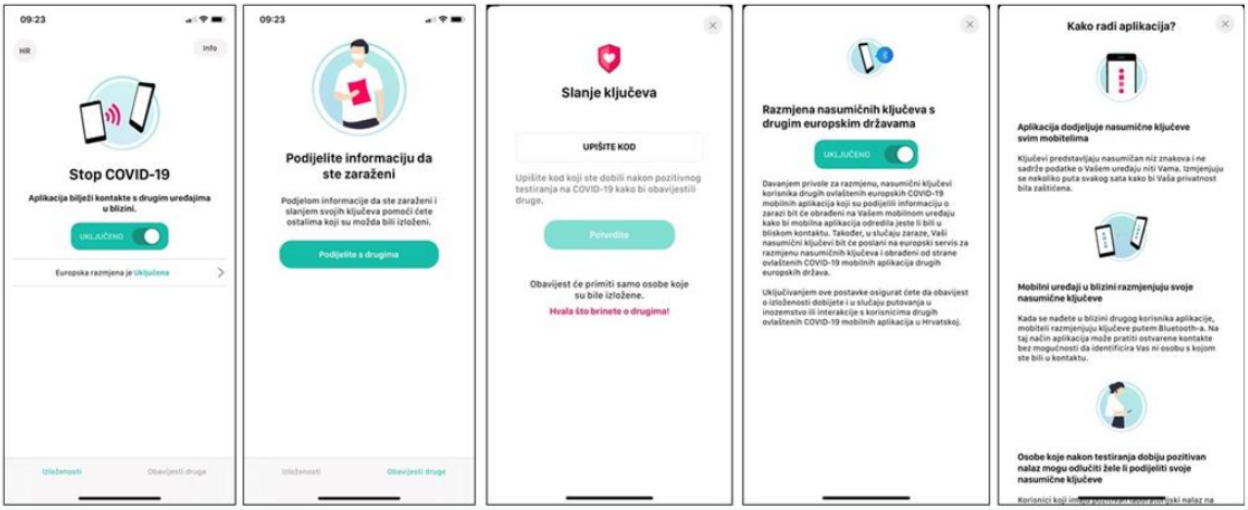
Figura 19. Captures de l'app Stop COVID-19

- **Com s'activa l'opció per compartir també les claus infectades de forma transfronterera?**

Android



iOS



<u>Dades actualitzades</u>

Número de descàrregues	Positius registrats a l'APP
78.799	592
10/12/2020	*11/12/2020*

AI.15 Espanya

Nom: Radar COVID

Radar COVID és l'aplicació dissenyada i dirigida per la Secretaria d'Estat de Digitalització i Intel·ligència Artificial de el Govern d'Espanya per ajudar a evitar la propagació del coronavirus (COVID-19).

Radar COVID t'avisa de manera anònima del possible contacte que has pogut tenir en els últims 14 dies amb una persona que hagi resultat infectada utilitzant la tecnologia Bluetooth de baix consum.

Radar COVID a més permet:

- Comunicar de forma anònima teu diagnòstic positiu.
- Comunicar l'exposició de forma anònima a les persones amb les que has estat en contacte

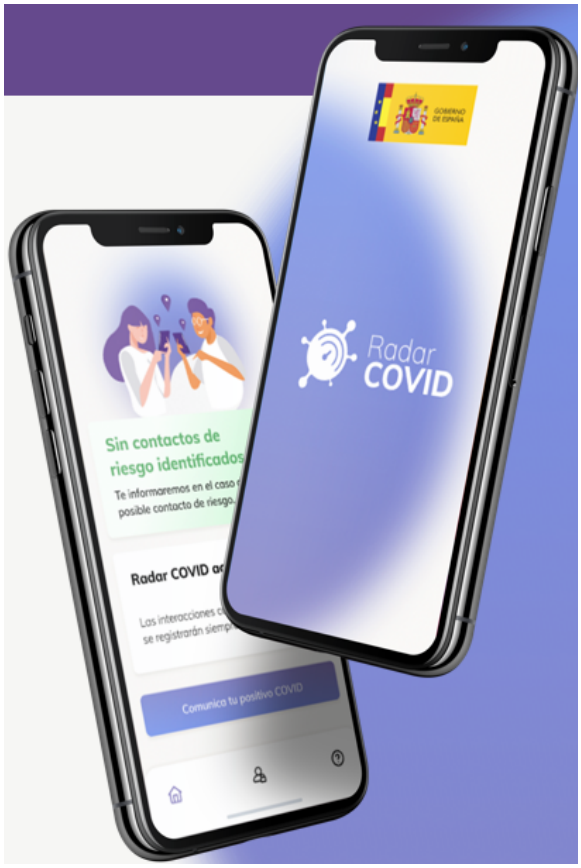


Figura 20. Captures de l'app Radar COVID

Nom: Radar Covid

Versió: 1.2.0

Data de llançament: 10/9/2020

Enllaç de descàrrega Google Play:
https://play.google.com/store/apps/details?id=es.gob.radarcovid&hl=ca&gl=US

Què fa?

Serveix per conèixer si has estat en contacte en els últims dies amb algú que ha estat diagnosticat de COVID-19. És el que es coneix com 'traç automàtic', fonamental per tallar les cadenes de contagi

Què no fa?

- No identifica: mai sabrà qui ets ni amb qui has estat
- No geolocalitza: mai sabrà on has estat perquè no recull dades d'ubicació

Com funciona?

Imagina que surts de casa per anar al treball. Portes el teu mòbil amb tu amb l'app RadarCOVID instal·lada i activa i et trobes amb algú conegut que també porta el mòbil amb el seu app instal·lada activa.

Imagina que esteu parlant més de 15 minuts, a menys de 2 metres de distància. Els vostres mòbils emeten un senyal de Bluetooth que inclou un codi aleatori que no recull cap tipus d'informació personal ni localització. En aquest moment cada telèfon 'recordarà' el codi identificador anònim de l'altre.

Passats uns dies, resulta que no et trobes bé i vas a el metge, on et fan una prova PCR que resulta positiva. El personal sanitari et donarà un codi de diagnòstic anònim perquè, de manera voluntària, el introdueixis en l'app.

Llavors s'enviarà una notificació a tots els terminals que tinguin el teu identificador memoritzat. És a dir, a tota la gent que va estar en contacte proper amb tu. D'aquesta manera estàs protegint als altres: aquesta persona coneguda amb la qual vas estar, i tots els altres contactes que potser no recordis, podran prendre les precaucions necessàries.

Què he de fer?

1. Descarrega l'aplicació

2. Concedeix el permís al Bluetooth i les notificacions
   Radar COVID utilitza només Bluetooth Low Energy per intercanviar codis aleatoris entre dispositius, sense recollir informació personal de cap tipus, ni tampoc la teva ubicació. Aquest sistema, a més de respectar la teva privacitat, gairebé no consumeix bateria del teu mòbil.
3. Mantingues sempre activa perquè funcioni.
   Quan estiguis en contacte amb altres persones, porta sempre el teu mòbil amb el Bluetooth i les notificacions activades per poder registrar contactes de risc.

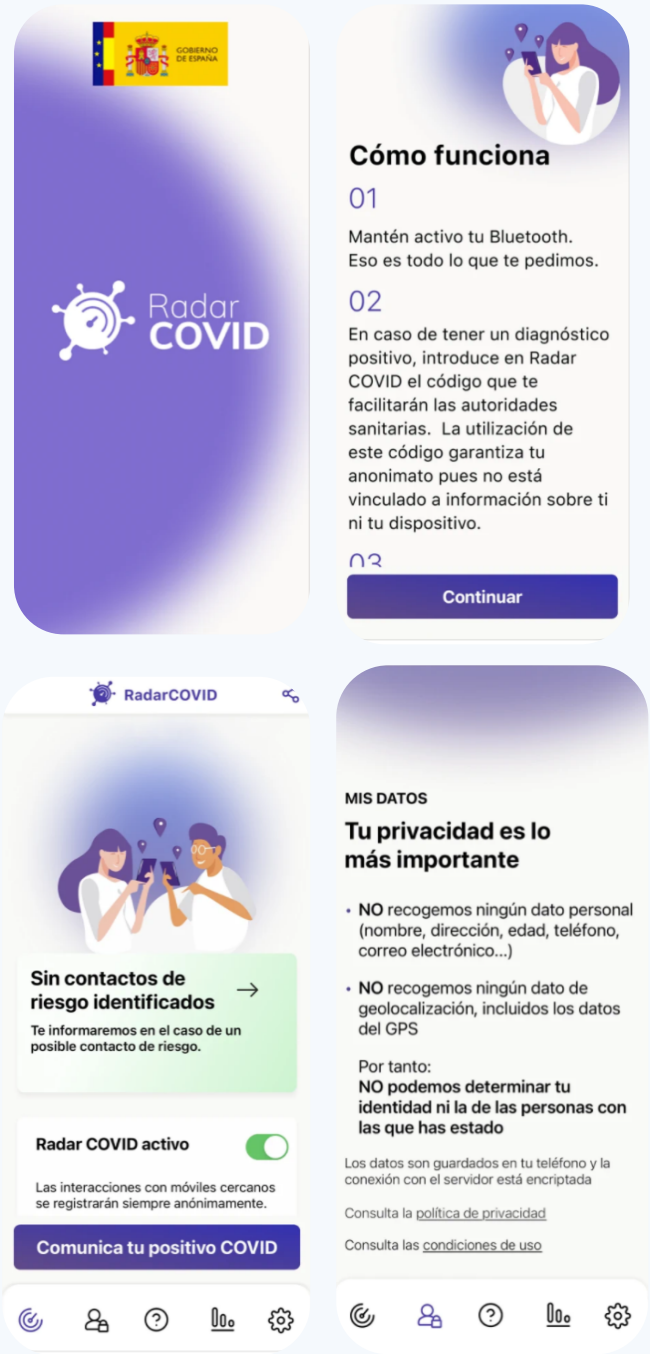


Figura 21. Captures de l'app Radar COVID

Dades actualitzades

Número de descàrregues
4.600.000
19/10/2020

AI.16 Finlàndia

Nom: Koronavilkku

Koronavilkku és una aplicació de localització de contactes produïda per l'Institut Finlandès de Salut i benestar (THL) per ajudar a esbrinar si és possible que un ciutadà hagi estat exposat al coronavirus. Si el ciutadà s'ha fet una prova de coronavirus i ha estat diagnosticat com a infectat, pot utilitzar l'aplicació per compartir-ho de manera anònima amb aquells amb qui hagi estat en contacte estret.

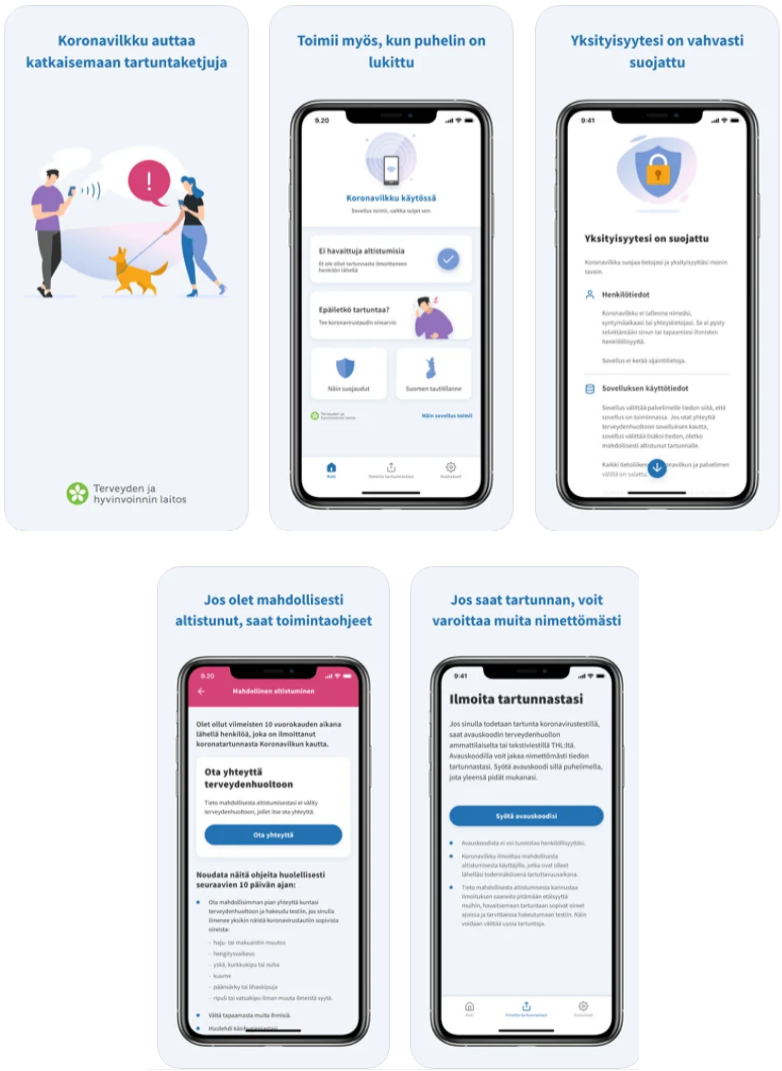


Figura 22. Captures de la plataforma Koronavilkku

Nom: Koronavilkku

Versió actual: 1.3.0+4c5041c

Publicada: 31 August 2020 (idiomes finès i suec)

Actualitzada: 23 de novembre de 2020 (versió llengua anglesa)

Enllaç de descàrrega: https://play.google.com/store/apps/details?id=fi.thl.koronahaavi

Descargues: +2,5 milions

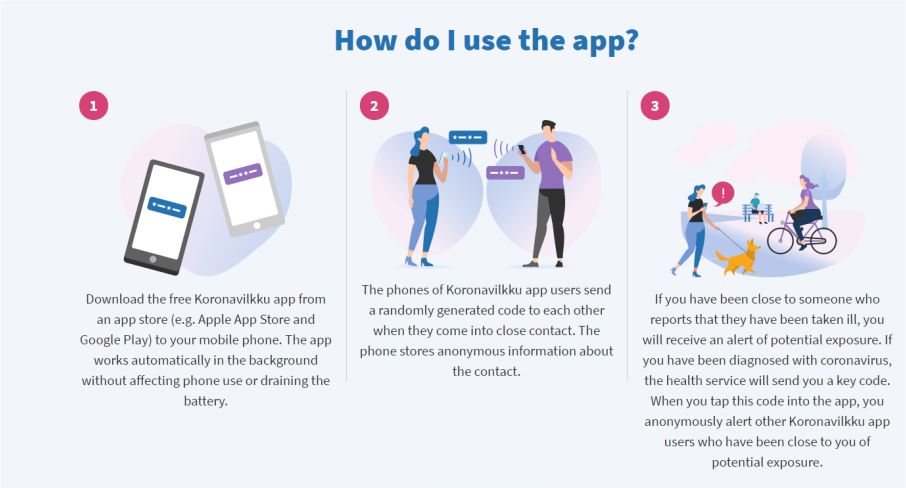


Figura 23. Captures de l'aplicació on es detallen els passos d'ús.

Com funciona?

L'aplicació assigna un codi aleatori a cada telèfon. El codi no conté informació sobre l'usuari ni el seu telèfon.

Quan estan prou a prop l'una de l'altra, les aplicacions intercanvien els codis mitjançant un senyal Bluetooth. La identitat o la ubicació de l'usuari no es desa. L'aplicació conserva els codis durant 21 dies abans de suprimir-los automàticament.

Quan un usuari informa de la seva infecció per COVID a l'aplicació, aquesta envia els codis que ha recopilat a un servidor. Si el contagiat ha estat en contacte estret amb un codi descarregat al servidor, l'aplicació els hi envia una alerta de possibles exposicions.

Si un usuari rep una alerta d'exposició potencial, l'aplicació proporcionarà més instruccions sobre què cal fer.

Per altra banda, en lloc de registrar el contagi l'usuari, si aquest ha donat positiu al coronavirus, un professional sanitari li donarà un codi clau. Quan s'introdueix aquest codi a l'aplicació Koronavilkku, l'aplicació envia els codis que ha recollit al servidor. Totes les persones amb qui l'usuari ha estat en contacte estret seran avisades de possibles exposicions.

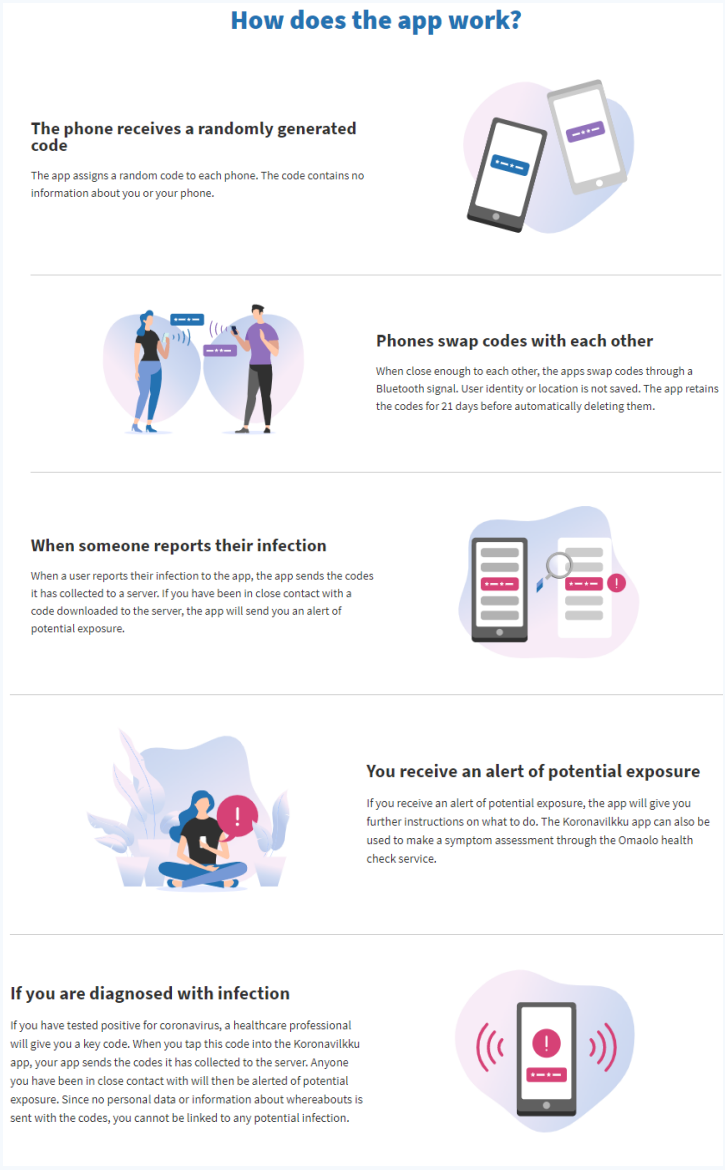


Figura 24. Captures de l'aplicació on es detalla el procés de com opera l'aplicació.

Dades d'ús → impacte

Els usuaris de Koronavilkku van fer un total de **2846 informes d'infecció** a l'aplicació durant els mesos de setembre i octubre.

Això significa que aproximadament el **34,9% de les persones que havien rebut un resultat positiu de la prova van informar la seva infecció a Koronavilkku**, enviant una notificació d'exposició a altres usuaris que podrien haver exposat al virus

Creix el numero de rastrejadors d'infeccions a Finlàndia (+1.000) → Els usuaris informen del seu estat d'infecció amb un codi de desbloqueig d'un sol ús que s'introdueix a l'aplicació. Els usuaris reben el codi de desbloqueig gràcies al paper del rastrejador de malalties infeccioses.

Entre l'1 de setembre i el 15 de setembre de 2020**, el 35% de les persones diagnosticades d'infeccions per coronavirus van utilitzar l'aplicació per informar de la infecció**.

Altres

En altres països com Taiwan s'ha optat per la vigilància mitjançant les antenes de telecomunicacions. Sense el requeriment d'instal·lar cap aplicació el govern directament aplica vigilància sobre les persones que han d'estar en quarantena rastrejant la senyal dels seus telèfons.

Annex II – Arquitectura de la solució Corona Warn App

AII.1 Introducció

En aquest annex s'explica l'estructura i funcionament de la solució de *contact tracing* alemany: Corona-Warn-App.

Des del moment que s'activa l'aplicació, s'intercanvien missatges Bluetooth Low Energy amb altres telèfons mòbils. El sistema de backend només entra en escena quan una persona ha donat positiu en SARS-CoV-2, moment en el que se li demana permís per publicar els seus identificadors al servidor central. A diferència de la majoria d'aplicacions, l'aplicació alemanya comença la relació amb el servidor una mica abans, ja que implementa la possibilitat de realitzar la comunicació del resultat del test a través de l'aplicació.

L'allotjament i administració del backend recau sobre Deutsche Telekom, utilitzant el seu Open Telekom Cloud per allotjar els servidors. El desenvolupament de l'aplicació l'ha realitzat SAP. L'institut Robert Koch proveeix la informació epidemiològica i recomanacions per fer servir l'aplicació. També determina els paràmetres que s'utilitzen per calcular el risc d'exposició.

AII.2 Arquitectura del Backend

La solució arquitectònica [1] proposada té 3 components principals: l'aplicació ("Corona-Warn-App") als telèfons mòbils, el servidor de l'aplicació ("Corona-Warn-App Server") i el servidor de verificació ("Verification Server"). L'aplicació es responsabilitza de registrar els contactes, el servidor de l'aplicació gestiona els identificadors de infectats (claus de diagnosi) i el servidor de verificació es responsabilitza de la veracitat de la identitat de l'usuari.

L'arquitectura de la solució contempla dos casos diferenciats, que depenen de si per rebre els resultats d'un test s'utilitza un servei de notificació electrònica o si en canvi es prefereix rebre la notificació per telèfon. En el primer cas, el pacient rep un codi QR que introdueix a l'aplicació i que associarà el seu usuari amb el resultat del test quan aquest estigui disponible. Aquesta funcionalitat requereix un component addicional respecte l'altre cas: un servidor de resultats de test que relacioni el codi QR amb un resultat. En el segon cas, es fa servir una línia telefònica per comunicar al pacient el resultat del seu test. Si és positiu, se li dona un codi llegible per a que l'introdueixi a l'aplicació. A continuació, es detallen els dos casos.

AII.2.1 Notificació electrònica dels resultats del test

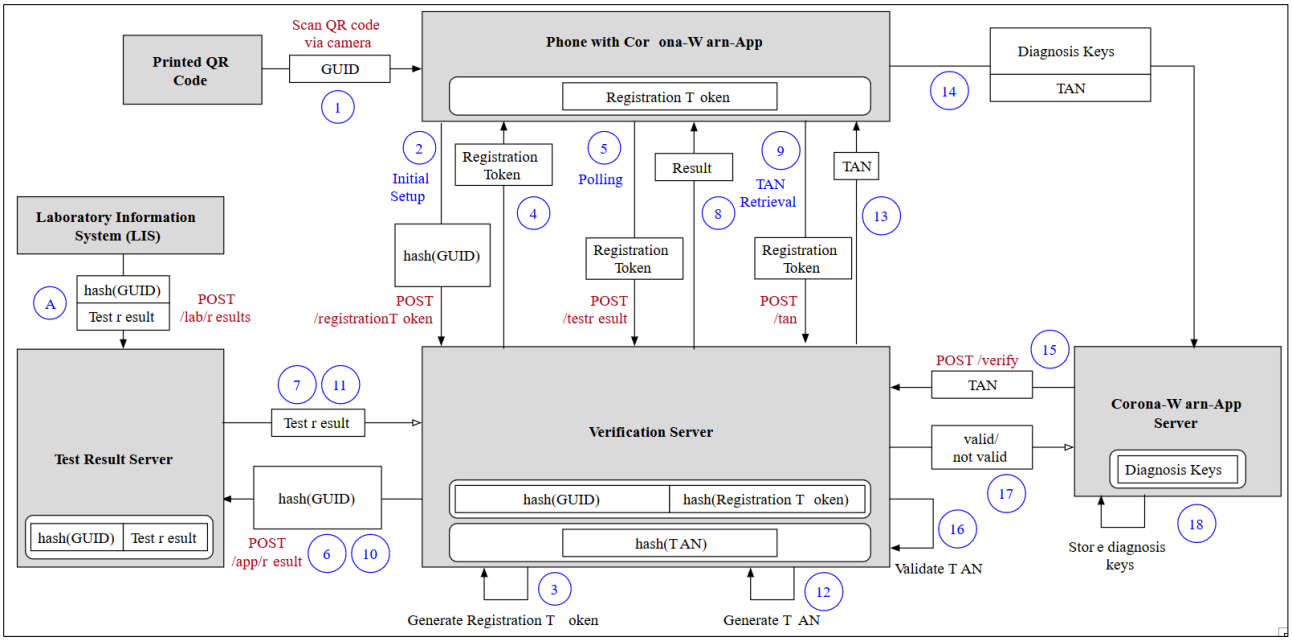


Figura 1: Esquema de l'arquitectura i diagrama del flux del backend amb notificació electrònica dels resultats d'un test [1]

La **Figura 1** descriu el flux que es segueix quan s'accedeix a la notificació electrònica del resultat del test. En aquest cas, el professional mèdic dona al pacient una còpia d'un codi QR generat a través d'un portal web. L'altre còpia li dona als responsables de la realització del test. Aquest codi QR codifica un GUID (*Globally Unique Idenftifier*). Quan el resultat del test està disponible, el laboratori el publica al servidor de resultats juntament amb el GUID del QR. Paral·lelament, l'usuari haurà fet servir l'aplicació per llegir el codi QR. En aquest moment el servidor de verificació crea un número de registre enllaçat al GUID del QR, que identifica l'usuari dins del sistema central. Aquests passos corresponen als punts 1-8 i A de la **Figura 1**.

L'usuari consulta periòdicament si hi ha resultats respecte el seu test. Quan aquests estan disponibles, s'avisa mitjançant una notificació sobre la disponibilitat del resultat. Si el resultat és positiu, es sol·licita a l'usuari que comparteixi els identificadors que ha publicat durant els últims 14 dies. Si l'usuari hi accedeix, verifica la seva identitat amb el servidor de verificació, que comprova si l'usuari que sol·licita pujar els seus identificadors és realment un positiu. En cas afirmatiu, es genera una clau temporal d'un sol ús que es retorna al sol·licitant (TAN). Aquesta clau s'utilitza per identificar-se davant del servidor de l'aplicació, que és el que administra els identificadors. Una vegada més, el servidor de l'aplicació comprova la identitat del sol·licitant amb el servidor de verificació. Si tot és correcte, accepta les claus de diagnòstic i les emmagatzema a una base de dades. Aquests passos corresponen als punts 9-18 de la **Figura 1**.

AII.2.2 Notificació electrònica dels resultats del test

Si l'usuari no accedeix a que se'l notifiqui electrònicament del resultat del seu test, canviarà lleument l'esquema, on intervindrà un sistema de trucades a través del qual es comunicarà a l'usuari tant del

resultat del seu test com d'un codi (que substituirà el GUID) teleTAN que haurà d'introduir manualment a l'aplicació, com es veu a la **Figura** .

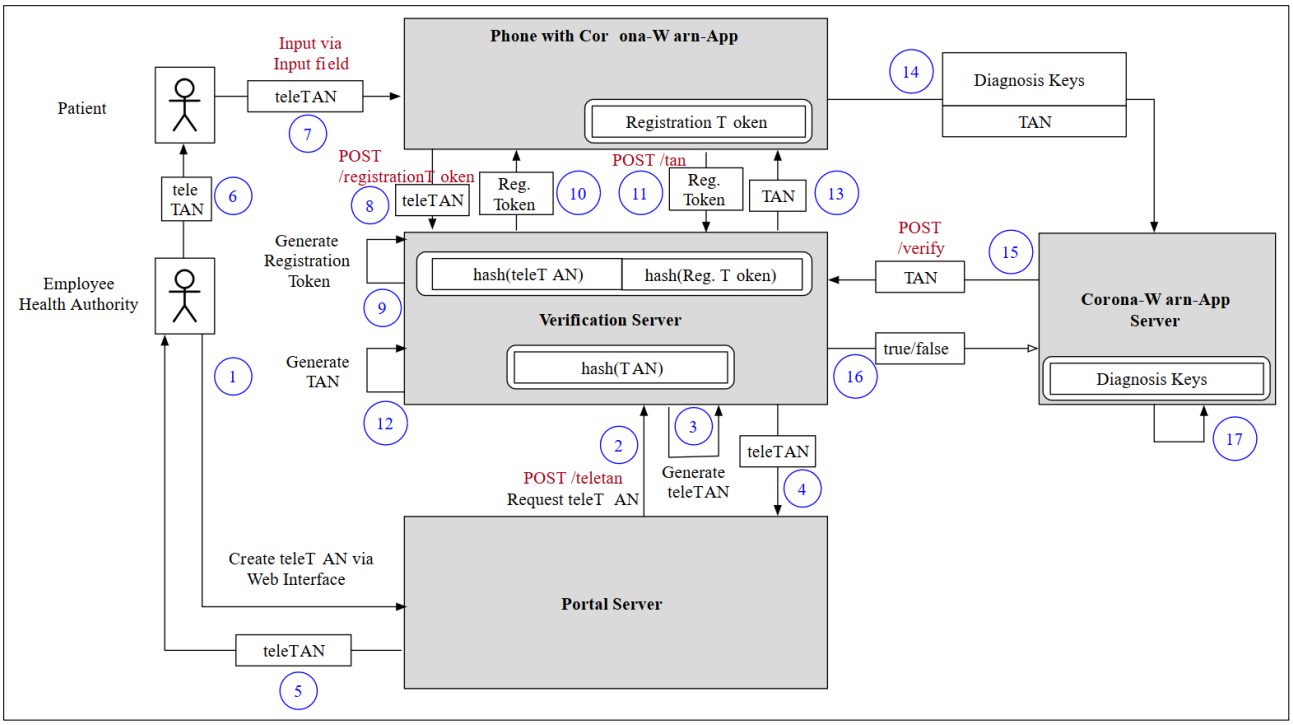


Figura 2: Esquema de l'arquitectura i diagrama de flux del backend sense notificació electrònica del resultat del test [1]

AII.3 Diagrama de flux

Aquest diagrama de flux il·lustra el funcionament de la solució de Contact Tracing d'Alemania. En aquest cas s'assumeix que tots els telèfons implicats utilitzen l'aplicació Corona-Warn-App activament.

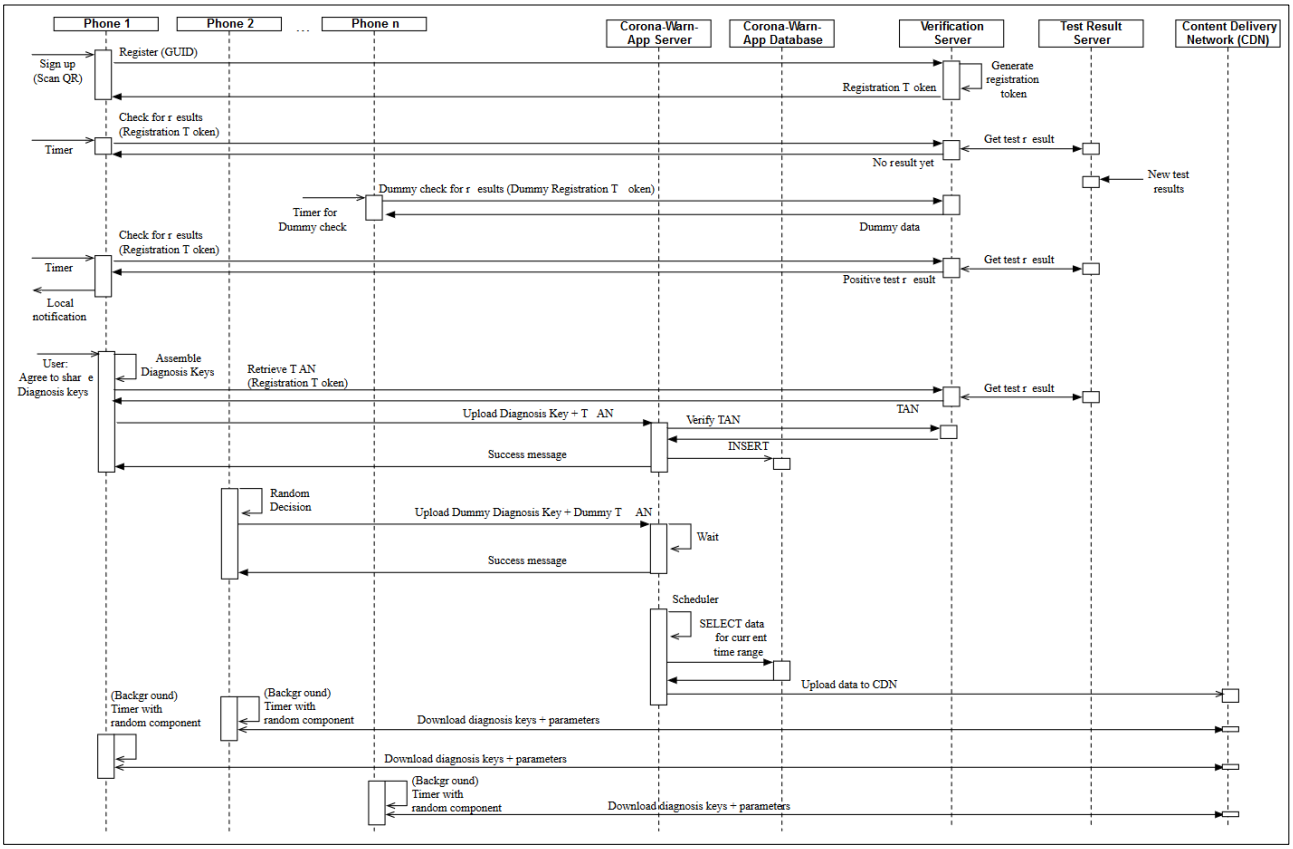


Figura 3: Diagrama de seqüència de l'aplicació; comunicació amb els servidors[1]

A la primera part de la **Figura 3** es defineixen els actors implicats. El Phone 1 interpreta el rol d'un usuari que s'ha fet un test de SARS-CoV-2. Els Phone 2..n són usuaris que ignorem si han donat positiu o no, però que tenen l'aplicació instal·lada i activa. El Corona-Warn-App Server, al que ens referim com a "servidor de l'aplicació" és el servidor que administra les claus de diagnòstic (identificadors de positius). La Corona-Warn-App Database és la base de dades on s'emmagatzemen totes les claus de diagnòstic dels últims 14 dies. El Verification Server és el servidor que verifica la identitat dels usuaris i permet que aquests coneguin el resultat del seu test i puguin pujar les seves claus de diagnòstic. El Test Result Server és el servidor on els laboratoris publiquen el resultat del test i el fan disponible per a la seva consulta gràcies a l'enllaç amb el GUID del QR. Per últim, el Content Delivery Network és una xarxa que facilita als telèfons la consulta de les claus de diagnòstic que es van publicant, que després utilitzen per al càlcul del risc d'exposició.

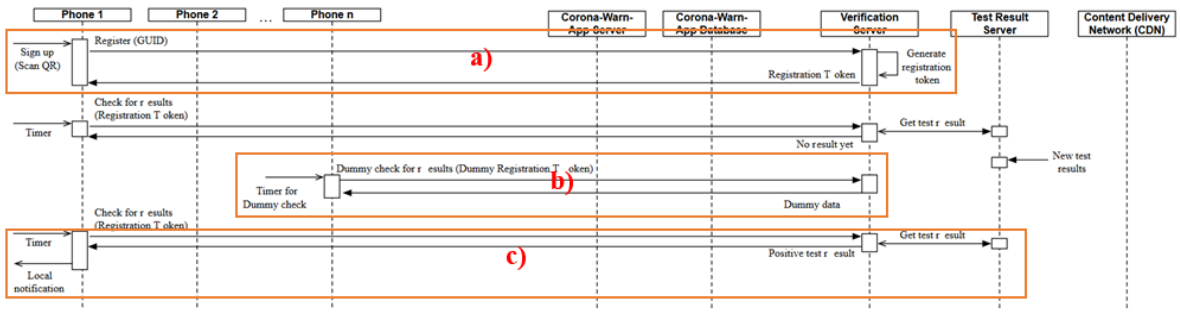


Figura 4: *Primera part del diagrama de seqüència [1]*

A **a)** es representa la comunicació entre un telèfon propietat d'un usuari que s'ha fet un test i ha permès que se'l notifiqui electrònicament. Al escanejar el codi QR que li ha proporcionat l'autoritat mèdica, es registre al servidor de verificació; aquest genera un token de registre associat al GUID del QR. Aquest token s'emmagatzema al servidor i es retorna a l'usuari.

A **b)** es representa un enviament fals. Aquest tipus de missatges es realitzen periòdicament per evitar que es puguin traçar els usuaris que consulten el resultat d'un test, evidenciant que s'han realitzat una prova. El servidor de verificació pot detectar fàcilment aquests enviaments falsos i descartar-los.

A **c)** es representa una consulta real periòdica sobre el resultat del test. S'utilitza el token de registre obtingut durant el registre, que al servidor de verificació s'associa amb el GUID i s'utilitza per consultar el resultat del test al servidor de resultats de test. En aquest servidor el laboratori ha publicat el resultat associat al GUID, que en aquest cas és positiu. Aquest resultat de test s'envia directament a l'usuari. L'aplicació crea una notificació: avisant de que el resultat del test està disponible.

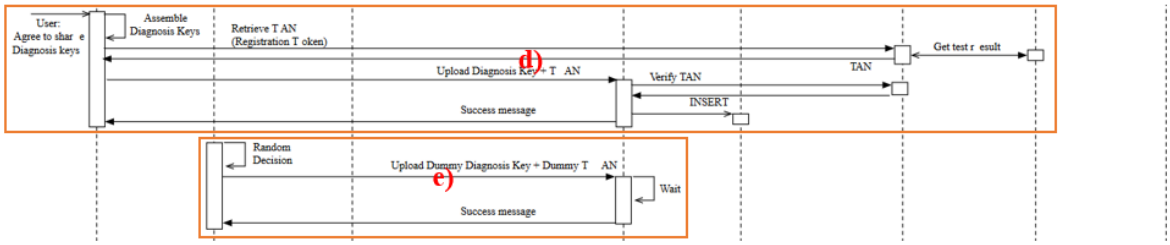


Figura 5: Segona part del diagrama de seqüència [1]

A **d)** es representa que l'usuari accedeix a compartir les seves claus de diagnòstic dels últims 14 dies. Després de preparar el missatge que conté totes les claus, sol·licita al servidor de verificació una autorització, presentant el seu token de registre. El servidor de verificació confirma que el sol·licitant tingui un resultat de test positiu (token de registre → GUID → resultat de test) al servidor de resultats de test i genera una clau temporal d'un sol ús. A continuació, el telèfon utilitza aquesta clau per pujar les dades al servidor de l'aplicació. Aquest, valida la clau temporal d'un sol ús enviant-la al servidor de verificació. Seguidament, inserta les claus de diagnòstic a la base de dades de l'aplicació.

A **e)** es representa una sol·licitud periòdica de càrrega de claus de diagnòstic falsa, per tal d'evitar que es pugui traçar a les persones infectades que pugin les seves claus de diagnòstic. Aquesta sol·licitud és fàcilment detectable al servidor de l'aplicació i és descartada.

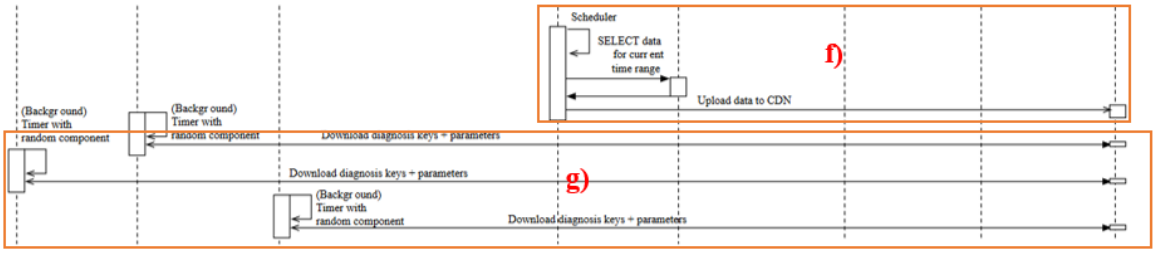


Figura 6: *Tercera part del diagrama de seqüència [1]*

A **f)** es representa un procés que es produeix periòdicament al servidor de l'aplicació, que consisteix en seleccionar de la base de dades les claus de diagnòstic dels últims 14 dies i transferir-les a la xarxa de distribució de contingut.

A **g)** es representen els processos que fan tots els mòbils periòdicament, on consulten a la xarxa de distribució de contingut noves claus de diagnòstic que després utilitzaran localment en el telèfon per calcular el risc de contagi. Quan un usuari rep una notificació d'un possible contagi, se li indica el nivell de risc (baix, mitjà o alt), en base a uns llindars definits per l'aplicació. També se li pot mostrar les variables amb les que es calcula el risc i el dia que va ocórrer la exposició.

AII.4 Elements Open Source de l'arquitectura

La solució alemanya proporciona molts dels components i de les APIs del backend com a codi obert a la seva plataforma GitHub. La següent imatge especifica els elements que estarien disponibles com a "open source".

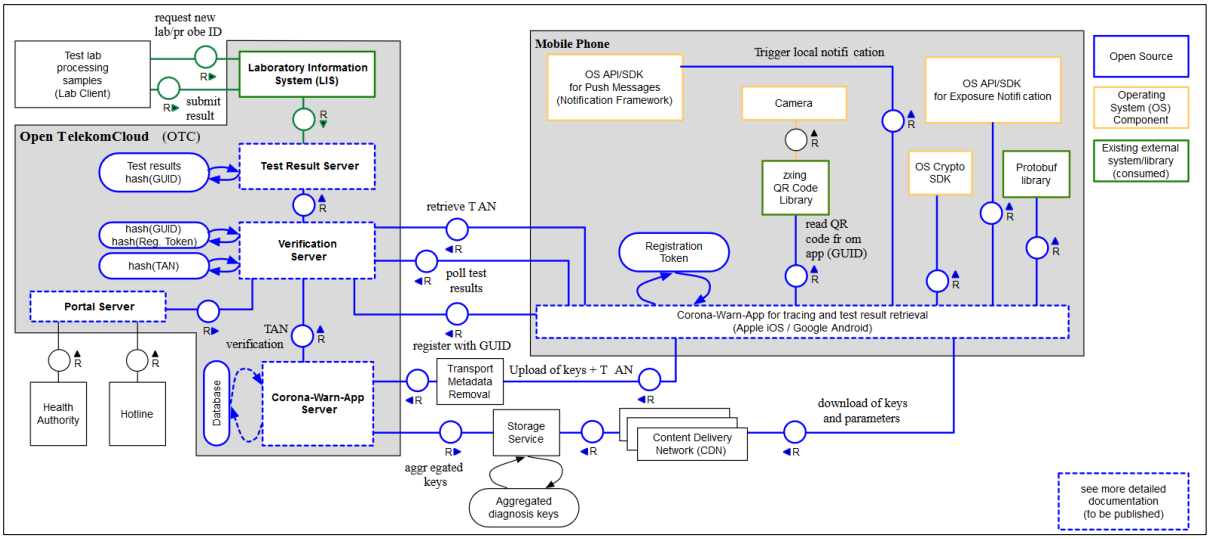


Figura 7: Estructura de la solució. Els elements blaus són de codi obert.

Pel que es veu, la majoria dels elements són de codi obert, a excepció d'alguns que no estan disponibles per raons de seguretat o perquè formen part de la infraestructura del proveïdor del backend (en aquest cas Deutsche Telekom).

AII.5 Càlcul del risc de contagi de l'aplicació Corona Warn

Pel fet d'utilitzar l'API de Google i Apple, el càlcul de risc de contagi a la Corona Warn App [4] [5] depèn de 4 paràmetres: dies des de l'exposició, duració, proximitat (atenuació) i risc de transmissió. Per cada paràmetre s'assignen 8 categories (o subdivisions) i cadascuna d'elles pot tenir una importància específica (de l'1 al 8). Concretament, l'aplicació alemanya defineix els següents valors (en vermell) per defecte per cada categoria:

Figura 8: Taula de ponderacions de les variables utilitzades per l'API de Google i Apple.

Aquests valors estan definits al servidor de l'aplicació i podrien actualitzar-se si es considerés necessari (per exemple, en base a noves indicacions de l'institut epidemiològic). Els valors actuals poden consultar-se a [3]

La configuració actual de l'aplicació aplica el mateix valor a la majoria de categories. Es pot observar com, es descartarien com a risc (valor igual a "0") els contactes de menys de 10 minuts o amb una atenuació de més de 73 dBm (que equivaldria a una distància de 8 metres). A més a més, es considera un pes per a cadascun dels quatre paràmetres. Actualment, la solució alemanya fa servir un pes de 50 per tots els paràmetres excepte els dies des de l'exposició, que tenen un pes de 20. No obstant això, segons els detalls de la documentació proporcionada per Google i Apple, actualment aquests pesos no es fan servir dintre de la API i es reserven per a usos futurs[6] [7] .

El procés del càlcul de risc seria el següent:

- Per a cada RPI amb el que s'ha coincidit al llarg del dia, l'API de Google i Apple suma el temps d'exposició i es calcula una atenuació ponderada. Es descarten:
    - Les exposicions menors a 10 minuts en total.
    - Les atenuacions menors a 73dB.
- L'API calcula el risc total de cada risc d'exposicions (amb un mateix usuari per dia). Per això es multiplica el risc total per exposició per el temps des de l'ultima exposició. Es descarten els riscos inferiors al mínim establert per l'aplicació (11 en el cas de la solució alemanya) i s'extreu el risc màxim de tots els valors calculats.

- Finalment, es calcula el risc combinat de tots els contactes de risc tal com es representa a la següent imatge.

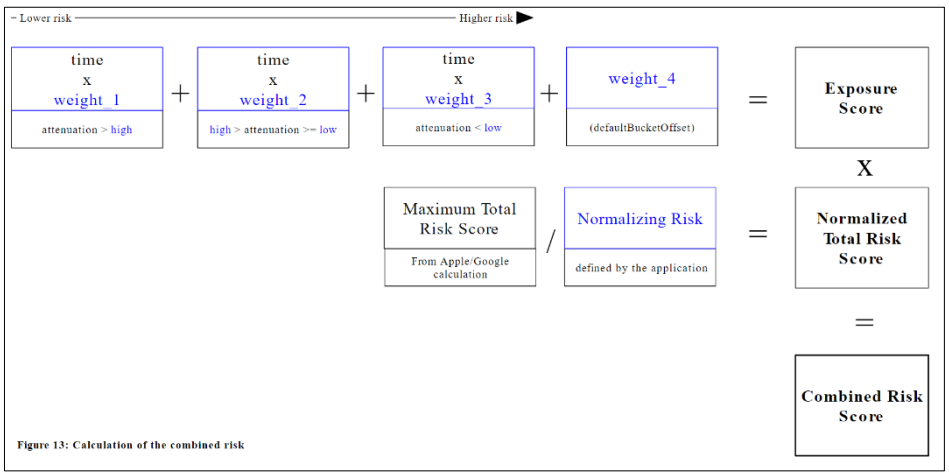


Figura 9: Càlcul del risc combinat.

Per això, es suma el temps de totes les exposicions que hagin ocorregut a una distància curta, mitjana o llarga (segons l'atenuació calculada per l'API i uns llindars definits per l'aplicació) i es multipliquen pel risc màxim normalitzat. Aquests nivells d'atenuació es coneixen com a "attenuation buckets". La solució alemanya defineix un llindar màxim de 63dB (menor risc) i un mínim de 55dB (major risc). També defineix un pes específic per cadascun d'aquests nivells; de forma que els riscos més alts tindrien un pes de "1", els mitjanç un pes de "0.5"(que reduiria el temps d'exposició a la meitat) i els riscos baixos un pes de "0" (es descartarien). Per acabar, es recull el risc màxim que s'ha obtingut del càlcul de la ¡Error! No se encuentra el o rigen de la referencia. i es divideix per un valor normalitzador del risc (25, segons la configuració alemanya) per extreure el risc combinat.

En el cas de l'aplicació alemanya, a l'usuari se li mostren només dos nivells de risc: baix (per a riscos entre 0 i 15) i alt per a valors majors a 15. També se l'informa del nombre de contactes positius amb els que hi ha hagut coincidència i els dies des de l'últim contacte. Finalment, se li faciliten unes recomanacions a seguir.

AII.6 Conclusions

Es destaquen els següents aspectes del disseny de la solució "Corona-Warn-App":

- El fet de definir diversos servidors independents permet que les dades es puguin gestionar de forma segura i privada. D'aquesta manera:
  - L'aplicació de l'usuari no interacciona en cap moment amb els servidors dels laboratoris.
  - El servidor de verificació s'encarrega de la validació dels usuaris com a positius.
  - El servidor de l'aplicació únicament s'encarrega de la gestió de les claus de diagnosi d'usuaris que han estat validats com a positius.
- Es consideren mecanismes d'interacció amb el backend ("falsos missatges") per evitar la traçabilitat d'usuaris que puguin ser positius.

- La solució alemanya facilita molts dels components de l'arquitectura (aplicació i backend) en codi obert.
- Quan un usuari es positiu, puja les claus de diagnosi dels últims 14 dies. A dia d'avui, no s'implementa la opció de que un usuari segueixi pujant identificadors més enllà del dia en que s'obté el resultat del test, ja que tampoc hi ha un procediment per establir quan un usuari ja es podria considerar com a negatiu (per deixar de reportar els seus identificadors). [S'assumeix que un usuari que ha donat positiu i ha reportat les seves dades romandrà confinat durant el temps que estableixi l'autoritat sanitària, i, per tant, no haurien d'esdevenir nous contactes de risc].
- El sistema funciona amb uns identificadors anomenats RPI (*Rolling Proximity Identifier*) que tenen una duració de 15 minuts. Aquests identificadors es deriven d'una clau d'exposició temporal (TEK, *Temporal Exposure Key*) que es substitueix cada dia a les 00:00 UTC. Per aquest motiu, quan un usuari indica que és positiu, pujarà claus de diagnosi en dues ocasions: primer les dels 14 dies anteriors i l'actual quan aquesta sigui substituïda al final del dia.
- El framework de l'API de Google i Apple és una caixa negra per l'aplicació, a la que li entren claus de diagnosi i surt la informació relacionada amb el nivell de risc d'exposició.
- Només es permeten 15 actualitzacions per dia del risc d'exposició. Això protegeix el sistema local d'usos malintencionats. [2]
- El servidor de l'aplicació té un intermediari específic que elimina les metadades de transport (IP) per raons de privacitat.
- Al sol·licitar claus de diagnosi es proveeixen desordenades per a que no es puguin relacionar claus consecutives amb un mateix usuari.
- La consulta de claus de diagnosi noves es fa cada hora.

AII.7 Referències

[1] SAP and Deutsche Telekom, "cwa-documentation/solution_architecture.md." https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md (accessed Jul. 08, 2020).
[2] "detectExposures(configuration:diagnosisKeyURLs:completionHandler:) | Apple Developer Documentation." https://developer.apple.com/documentation/exposurenotification/enmanager/3586331-detectexposures (accessed Jul. 09, 2020).
[3] https://github.com/corona-warn-app/cwa-server/tree/master/services/distribution/src/main/resources/master-config
[4] https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md#risk-score-calculation
[5] https://github.com/corona-warn-app/cwa-documentation/blob/master/cwa-risk-assessment.md
[6] https://developer.apple.com/documentation/exposurenotification/enexposureconfiguration
[7] https://www.google.com/covid19/exposurenotifications/