Veselības ministrija

Slimību profilakses un kontroles centrs

APTURI COVID

RISINĀJUMA TEHNISKAIS APRAKSTS

v.1.0

RĪGA 2020

Saturs

Slimību profilakses un kontroles centrs (turpmāk – SPKC) sadarbībā ar Latvijas IT uzņēmumiem un profesionāļiem ir izveidojis lietotni “Apturi Covid” (turpmāk – Lietotne), lai sniegtu iedzīvotājiem atbalstu slimības Covid-19 (turpmāk – Slimība vai Covid-19) ierobežošanā. Lietotnes tehniskais risinājums ir tapis, pateicoties sabiedrības iesaistei saskaņā ar Memorandu[1] sabiedrības līdzdalībai Covid-19 ierobežošanā un šādu uzņēmumu dalībai tehniskajā izstrādē: Latvijas Mobilais Telefons, MakIT, TestDevLab, IT centrs, Autentica, Zippy Vision.

Lietotnes darbībā ikviena Lietotnes lietotāja līdzdarbošanās un sapratne par Slimības radīto risku nopietnību ir nozīmīga, jo, tikai SPKC un sabiedrībai darbojoties kopā, ir iespēja aizsargāt ikvienu iedzīvotāju individuāli. Lietotnes mērķis ir veicināt epidemioloģisko drošību, lai mazinātu sabiedrības veselības apdraudējumu, ko izraisa Covid-19 izplatības iedarbība. Lietotne palīdzēs SPKC ātrāk atklāt un izmeklēt Covid-19 iespējamos saslimšanas gadījumus, organizēt piesardzības pasākumus, kā arī uzlabos sabiedrības un arī Lietotāju informētību, kas savukārt mazinās kopējos Covid-19 izplatības riskus.

[1] https://apturicovid.lv/memorands

1. Izmantotās tehnoloģijas un operētājsistēmas atbalsts

Lietotnes izstrādē tika izmantots **Google** un **Apple** izstrādātais **"Exposure notification"** API, ar kura aktuālo dokumentāciju ikviens interesents var iepazīties Google un Apple oficiālajās vietnēs[2].

Priekšnoteikumi, lai Lietotāji varētu instalēt Lietotni:

- iOS viedtālrunis, kas atbalsta 13.5 iOS operētājsistēmu **vai**
- **Android** viedtālrunis, kas atbalsta vismaz Android 6.0 operētājsistēmu un Google Play Services v20.18.17. **un**
- pieejams *Bluetooth Low Energy (*turpmāk – BTLE*)*.

[2] https://www.apple.com/covid19/contacttracing, https://www.google.com/covid19/exposurenotifications/

2. Kontakta fiksēšanas darbības apraksts

Aktivizējot kontakta fiksēšanas funkcionalitāti, lietotājs apstiprina atļauju aktivizēt paziņojumus par saskari ar Covid-19 (*Exposure Notification*), ar kuras palīdzību var apmainīties ar kontakta atslēgām un veikt Slimības skartā lietotāja kontakta riska pārbaudes. Katru reizi darbinot Lietotni, tiek veikta pārbaude, vai lietotājs ir apstiprinājis šādu atļauju, ja nē, tad tiek attēlots paziņojums par šādas atļaujas apstiprināšanu.

Android gadījumā:

- Tiek ieslēgts Google izstrādātais paziņojums par saskari ar Covid-19;
- Tiek ieslēgta Bluetooth funkcionalitāte;
- Tiek ieslēgta ierīces atrašanās vietas funkcionalitāte, kas nepieciešama, lai noteiktu tuvumā esošas Bluetooth ierīces, taču Lietotne nepiekļūst un neizmanto ierīces atrašanās vietas noteikšanu.

iOS gadījumā:

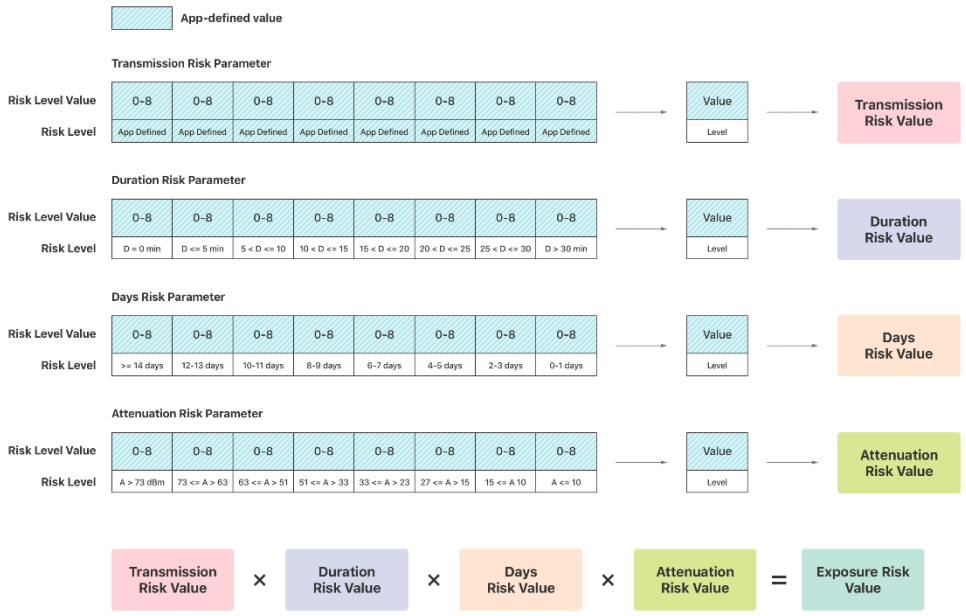
- Tiek ieslēgts Apple izstrādātais paziņojums par saskari ar Covid-19 (*Exposure Notification*);
- Lietotājam pašam ir jāieslēdz Bluetooth, jo iOS liedz piekļuvi Bluetooth modulim un Lietotnei nav tiesību ieslēgt to.

Lietotājs Lietotnē ir aicināts ievadīt savu tālruņa numuru, lai SPKC iespējamā kontakta gadījumā varētu sazināties un sniegt konsultācijas par nākamo rīcību. Šajā gadījumā notiek tālruņa numura apstiprināšanas (3.att. 1.plūsma) process. Lietotājs var izvēlēties neievadīt tālruņa numuru un jebkurā brīdi var izvēlēties norādīt savu tālruņa numuru un uzsākt tālruņa numura apstiprināšanas procesu.

Katram lietotājam, apstiprinot dalību kontakta fiksēšanas programmā, reizi dienā tālruņa aizsargātā apgabalā, kas nav pieejams lietotnēm, tiek izveidota unikāla pagaidu ekspozīcijas atslēga (*Temporary Exposure Key*, turpmāk - TEK). Ja lietotājam tiks apstiprinātas pozitīva diagnoze, atslēgas par 14 pēdējām dienām kopā ar to derīguma sākumlaiku tiks nosūtītas SPKC serverim. Izmantojot TEK, reizi 10 līdz 15 minūtēs tiek veidots mainīgs attāluma identifikators (*Rolling proximity identifier*, turpmāk - RPI) un šifrēšanas atslēga, kura aizsargā metadatus. RPI un šifrētie metadati, kas nepieciešami inficēšanās riska noteikšanai ar BTLE apraides paketēm, tiek periodiski raidīti no iekārtas. BTLE apraides protokola datu vienības tips ir *ADV_NONCONN_IND*, kas norāda, ka uz iekārtu nav iespējams pieslēgties. Šāda raidīšana būtiski neietekmē tālruņa baterijas patēriņu. Citas apkārtesošās iekārtas uztver šīs paketes un ja uztverošā iekārta piedalās kontakta fiksēšanas programmā, tad iekārta saglabā savā aizsargātajā atmiņā saņemtos RPI. Šie dati nav pieejami lietotnei.

Saslimšanas gadījumā lietotājam tiek palūgts pēdējo 14 dienu TEK atslēgas nodot SPKC, kas tās publicēs uz publiska servera. Pēc šīs darbības lietotāja TEK otru reizi vairs nav iespējams izgūt no aizsargātās atmiņas. Papildu privātuma aizsardzības nolūkos, tekošās dienas TEK nav iespējams iegūt.

Pārējās iekārtas regulāri ielādē šīs atslēgas no SPKC servera. Lietotne šīs atslēgas visas kopā nodod *Exposure Notification* API, kurš uz ierīces pārbauda vai aizsargātajā atmiņā neglabājas fiksēts kontakts ar kādu no šīm atslēgām. Ja tiek atrasts kontakts, tad *Exposure Notification* API uz ierīces veic riska aprēķinu, balstoties uz konfigurācijas parametriem. Konfigurācijas parametri veidojas pēc 1.att redzamās formulas. Konfigurācijas parametri tiek pieprasīti no SPKC servera.[3]



1.att. Kontakta riska aprēķina formula[4]

Par katru fiksēto kontaktu API atgriež fiksētā kontakta kopsavilkumu (*Exposure Summary*) informāciju, ja lietotājs ir bijis kontaktā ar kādu saslimušo. Fiksētā kontakta kopsavilkums par katru no kontaktiem satur:

- diena (bez laika), kad ir noticis kontakts;
- kontakta ilgums: 5, 10, 15, 20, 25, 30 (garāki kontakta ilgumi tiek noapaļoti uz 30);
- BTLE signāla traucējumu līmenis, kas ļauj noteikt aptuvenu distanci;
- aprēķinātais inficēšanās risks.

Lietotne nevar noskaidrot ar kuru konkrētu TEK lietotājs ir bijis kontaktā, līdz ar to, nav iespējams noskaidrot precīzi ar kuru saslimušo ir būts saskarē. Lietotņu apstiprināšanas

[3] https://apturicovid-files.spkc.gov.lv/exposure_configurations/v1/android.json un https://apturicovid-files.spkc.gov.lv/exposure_configurations/v1/ios.json
[4] https://developer.apple.com/documentation/exposurenotification/enexposureconfiguration

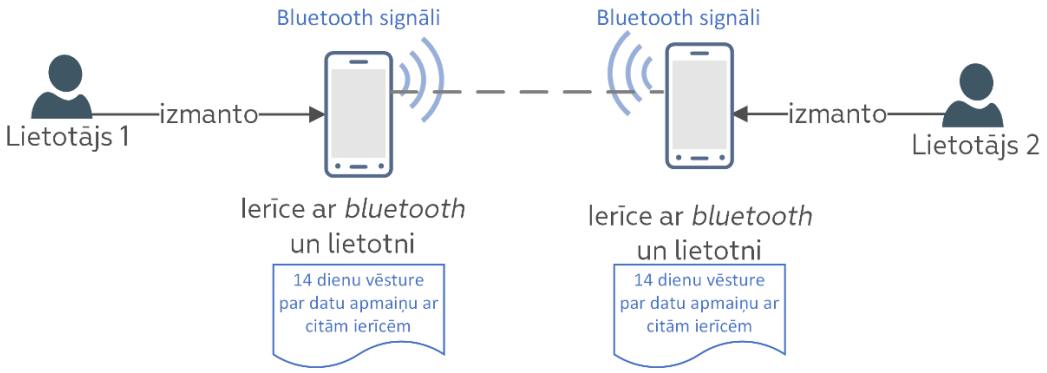
process nodrošina, lai lietotne nemēģinātu identificēt saslimušos, piemēram, nododot tikai vienu vai dažas TEK atslēgas API.

2.1 Kontakta fiksēšana

2.att. attēlota kontakta fiksēšana, kur Lietotājs 1 un Lietotājs 2 ar viedierīcēm, uz kurām uzstādīta Apturi Covid lietotne un aktivizētajām atļaujām, aptuveni 2 m attālumā vismaz 15 min ilgumā, apmainās ar RPI. Tāpat tālrunī tiek saglabāts:

- kontakta fiksēšanas datums,
- ilgums un
- BTLE signāla parametri, kas indikatīvi norāda uz fiksēto attālumu.

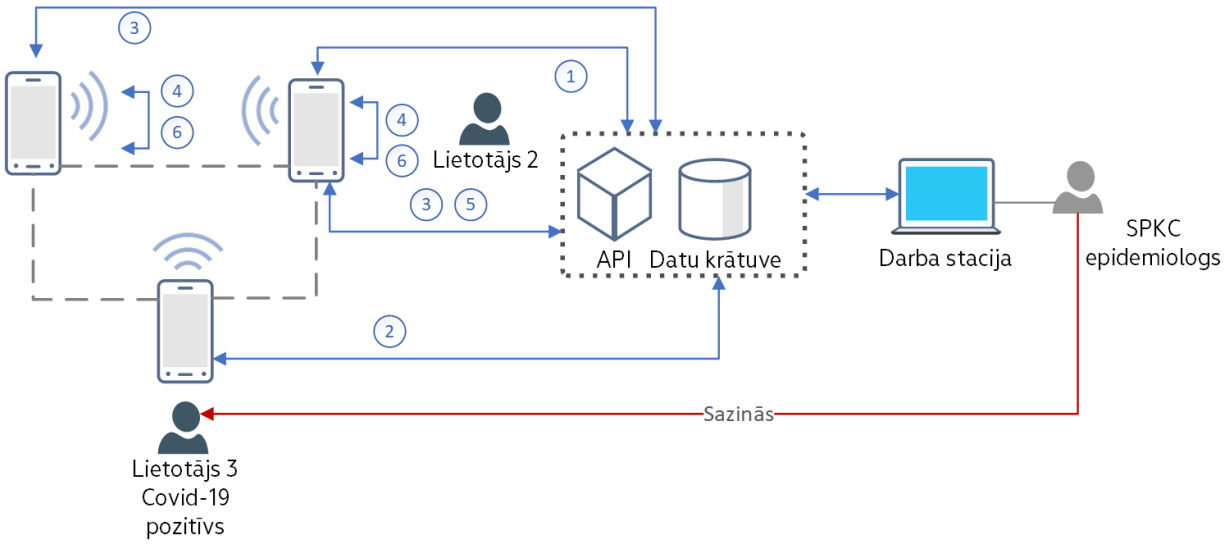
Šie dati glabājas tālruņa datu krātuvē 14 dienas, pēc kurām tie tiek dzēsti. Izstrādes gaitā notika testi gan uz dažādām ierīcēm, gan dažādiem attālumiem, kā arī tika sagatavoti vairāki testēšanas scenāriji, lai pārliecinātos par BTLE kalibrācijas pietuvinājumu pēc iespējas reālākai dzīves situācijai, kas šobrīd ir veikta optimālā līmenī un tiks turpināti testi, lai ieviestu BTLE kalibrācijas uzlabojumus.



2.att. Bluetooth kontakta fiksēšana

2.2 Lietotāju apziņošanas process

Apskatīsim **3.att**. lietotāju apziņošanas process par kontaktu ar Covid-19 gadījumu, kur pieņemsim, ka Lietotājs 1 ir palicis anonīms, Lietotājs 2 brīvprātīgi ievadījis savu tālruņa numuru, bet Lietotājam 3 ir laboratoriski apstiprināta saslimšana ar Covid-19. Visiem trim lietotājiem 14 dienu laikā ir ticis fiksēts kontakts savā starpā.



3. att. Paziņojums par saskari ar Covid-19 gadījumu

1. plūsma – Telefona numura apstiprināšanas process

Telefona numura apstiprināšanas process norisinās sekojoši:

1. Lietotājs 2 Lietotnē ievada savu tālruņa numuru, kas to nosūta to uz SPKC API.
2. SPKC API lietotājam atgriež parakstītu un šifrētu JSON Web Tokens[5] marķieri (turpmāk – JWT token), kas ļauj sistēmā tālruņa numuru dzēst. Šifrēts JWT token sevī ietver telefona numuru un exposure_token. Šifrēšanas atslēga un exposure_token tiek glabāti uz servera, bet pats JWT token uz servera netiek saglabāts. Papildus tiek izsaukts SMS nosūtīšanas serviss, kas nosūta lietotājam 8 ciparu kodu. Kods ir derīgs ne ilgāk kā 30 min.
3. Saņemot SMS, lietotājs kodu ievada Lietotnē. Uz SPKC API tiek nosūtīts pieprasījums verifikācijas apstiprināšanai. Pieprasījums sastāv no JWT token un SMS koda.

Serveris pārliecinās, ka pieprasījums nāk no reālas ierīces, izmantojot SafetyNet[6] un DeviceCheck[7] API. Serverim ir uzstādīti pieprasījumu skaita ierobežojumi no vienas ierīces.

2. plūsma – TEK diagnozes atslēgu (diagnosis key) nodošana serverim

Brīdī, kad Lietotājs 3 ir nodevis laboratoriskās analīzes uz Covid-19 un rezultāts ir bijis pozitīvs, SPKC atbilstoši normatīvajiem aktiem no laboratorijas saņem pacienta

[5] https://jwt.io
[6] https://developer.android.com/training/safetynet/attestation#quota-monitoring
[7] https://developer.apple.com/documentation/devicecheck

personas datus un kontaktinformāciju. SPKC potenciālo kontaktu izpēte sākas ar pacienta interviju, kuras laikā tiks noskaidrots vai pacients lieto Lietotni, kā arī citiem jautājumiem. Šajā gadījumā SPKC risinājuma saskarnē uzģenerē astoņu ciparu kodu un inicializē SMS izsūtīšanu Lietotājam 3. Kods ir derīgs ne ilgāk kā 30 min.

Lietotājs, ievadot šo kodu Lietotnē, no Exposure Notification API iegūst TEK diagnozes atslēgas par pēdējām 14 dienām un nosūta tās SPKC serverim. Reizi dienā visi iesūtītie TEK tiek apkopoti un ievietoti publiskā reģistrā[8]. Uz servera pieejamas tikai tās atslēgas, kas nav vecākas, kā divas dienas pirms konkrētā saslimšanas datuma.

3. plūsma – Aktuālo diagnozes atslēgu paņemšana

Serverī jaunas atslēgas tiek augšupielādētas reizi dienā. Lietotne pieslēdzas pie servera vairākas reizes dienā, lai lejupielādētu aktuālās TEK diagnožu atslēgas. Lietotne lejupielādē tikai tās atslēgas, kuras iepriekš netika lejupielādētas.

4. plūsma – TEK diagnozes atslēgas pārbaude uz tālruņa

Lietotnē ir izstrādāti OS (operētājsistēmas) līmeņa fona uzdevumi, kas periodiski pārbauda vai starp kādām no aktuālajām TEK atslēgām ir kāda, kura pēc Exposure Notification API specifikācijā noteiktā algoritma aprēķina rezultāta sakrīt ar uz tālruņa aizsargātajā atmiņā saglabātajām RPI atslēgām.

Ja Exposure Notification API aprēķina rezultāts sakrīt un lietotājs ir verificējis telefona numuru, tad inicializējas fiksēto kontaktu kopsavilkuma (Exposure Summary) nodošana serverim.

5. plūsma – Fiksēto kontaktu kopsavilkuma nodošana

Tikai Lietotāja 2 fiksēto kontaktu kopsavilkuma dati tiek nodoti kopā ar JWT token. Sistēmā tiek pārbaudīts vai JWT token ir derīgs, salīdzinot datubāzē saglabāto exposure_token ar JWT token esošo.

6. plūsma – Paziņojums par kontakta ar Covid-19 izplatīšana

TEK diagnozes atslēgas pārbaudes (atbilstoši 4. plūsmai) un rezultātu sakritības gadījumā lietotne paziņo par to, ka ir bijis kontakts ar Covid-19 nenorādot nedz potenciālo kontakta vietu, nedz lietotāju vai tā kādus identificējošus datus.

[8] https://apturicovid-files.spkc.gov.lv/dkfs/v1/index.txt

3. Privātuma aspekti

Izstrādājot lietotni tika ievēroti šādi galvenie privātuma aspekti:

- Lietotnes uzstādīšana un izmantošana ir **bezmaksas** un **brīvprātīga**. Lietotājam pēc savas izvēles ir iespēja izmantot visas piedāvātās Lietotnes funkcijas vai arī tikai kādu daļu no tām. Lietotnes neizmantošana nerada papildu saistības un vienlaikus nemazina personas tiesības un pienākumus attiecībā uz normatīvajos aktos paredzētajiem epidemioloģiskās drošības pasākumiem.
- Lietotnes neizmantošana var mazināt vai paildzināt Lietotāja iespējas uz savlaicīgu informācijas saņemšanu, īpaši, ja Lietotājs ir atradies nejaušā vai neapzinātā kontaktā ar personu, kam ir konstatēts Covid-19, vai arī ja ar Covid-19 saslimusī persona neatceras visas personas, ar kurām ir bijusi tuvumā.
- Lietotājs var uzsākt un pārtraukt Lietotnes lietošanu, kā arī mainīt izvēlei pieejamos Lietotnes iestatījumus pēc sava ieskata. Lietotāja veiktās izmaiņas Lietotnes iestatījumos tiek attiecinātas uz Lietotnes turpmāko funkciju pieejamību un neietekmē apstrādi, kas veikta līdz izmaiņu veikšanai.
- Lietotne nereģistrē un attiecīgi nevar atklāt Lietotāja un personu, ar ko Lietotājam ir bijis kontakts, galiekārtu ģeogrāfiskās koordinātas (atrašanās vietas datus).
- Lietotne neievāc un neapstrādā datus, kas nav nepieciešami Lietotnes darbības mērķa sasniegšanai.
- Jebkuri lietotāju dati tiek izmantoti tikai sabiedrības veselībai un nav pieejami jebkādiem citiem valsts, pašvaldību vai komerciāliem mērķiem.
- Lietotne darbojas, ievērojot cilvēktiesības, un atbilstoši Eiropas Savienības normatīvajam regulējumam un vadlīnijām attiecībā uz datu apstrādi un drošību.
- Plašāk ar Lietošanas nosacījumiem var iepazīties šeit: https://apturicovid.lv/lietosanas-noteikumi un privātuma politiku https://apturicovid.lv/privatuma-politika.

4. Drošības testēšanas pārskats

Risinājumam izvirzītajām drošības prasībām, par pamatu tika izmantoti labās prakses principi, ISO 27002 standarts, Ministru kabineta noteikumi 442, kas nosaka valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģiju minimālās drošības prasības[9].

Risinājuma izstrādes gaitā iteratīvi noritēja drošības testēšana, kuru veic speciālisti no šādām organizācijām: IT Centrs SIA, LATVIJAS MOBILAIS TELEFONS SIA, TestDevLab SIA, kā arī CERT.LV. Drošības testiem tika izmantotas OWASP Testing Guide v4[10], OWASP MASVS L1 metodikas un citi OWASP ieteikumi par drošu lietojumu izstrādi.

Gala drošības testēšanā tika konstatēts sekojošais:

Lietotnes informāciju par lietotnes avārijām un darbības kļūdām, kas satur viedtālruņa modeli un kļūdas tehnisko informāciju, anonīmi, bez lietotāja identifikācijas un bez lietotāja ievadītā satura nosūta un apkopo, izmantojot *Firebase Crashlytics* pakalpojumu. Ņemot vērā, ka lietotne darbojas autonomā režīmā ar minimālu lietotāja iesaisti un ir jānodrošina lietotnes optimāla darbība apjomīgam lietotāju skaitam ar dažādu ražotāju iekārtām, lietotnes uzturēšanai ir būtiski nepieciešams uzzināt par lietotnes avārijām un darbības kļūdām. Tas dod iespēju atklāt lietotnes tehniskās problēmas, lai varētu operatīvi veikt lietotnes uzlabojumus un nodrošinātu lietotnes drošību.

[9] https://likumi.lv/ta/id/295995-grozijumi-ministru-kabineta-2015-gada-28-julija-noteikumos-nr-442-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas
[10] https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf

5. Lietotnes koda caurskate

Koda caurskates rezultātā atrasto problēmu atklāšanā, lūdzam, ievērot atbildīgu ievainojamību atklāšanas labo praksi - https://cert.lv/lv/par-mums/atbildiga-ievainojamibu-atklasana.