The Ministry of Health

The Centre for Disease Prevention and Control

DESCRIPTION OF TECHNICAL SOLUTION

v.1.0

RIGA 2020

Content

The Centre for Disease Prevention and Control (hereinafter, the CDPC) in cooperation with the Latvian ICT sector has developed the Apturi Covid app (hereinafter, the App) to provide support to the public in limiting the spread of Covid-19 (hereinafter, the Disease or Covid-19). The technical solution of the App was made possible as a result of public engagement according to the Memorandum on Public Engagement in Limiting Covid-19[1] and these developers: country's largest mobile operator – LMT; software development companies MAK IT, Autentica, and Zippy Vision; software testing service TestDevLab; and IT security testing and consultancy IT Centrs.

To ensure continued operation of the App, active participation of each and every user and his/her awareness of the risk of the Disease are of utmost importance, as only if the CDPC and the public act together it will be possible to protect each and every individual. The App aims to increase the epidemiological safety to mitigate any threat to the public health posed by the consequences of Covid-19 spread. The App will help the CDPC discover and investigate Covid-19 cases faster, organise implementation of precautionary measures and improve the public and User awareness that, in turn, will decrease the overall risk of spreading Covid-19.

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

1. Technologies and OS support

Exposure notification API developed by **Google** and **Apple** was used to develop the App, and the most recent copy of its documentation is available on the official sites of Google and Apple[2].

Preconditions for installing the App:

- iOS smartphone that supports 13.5 iOS, **or**
- **Android** smartphone that supports at least Android 6.0 OS and Google Play Services v20.18.17., **and**
- Access to Bluetooth Low Energy (hereinafter, the BTLE).

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

2. Description of Contact Recording Activity

When the contact discovery functionality is activated, the user confirms his/her consent to activating notifications concerning exposure to Covid-19 (Exposure Notification): it allows to exchange contact keys, and carry out contact risk verification of the user who has the Disease. Every time the App is operated, activation of the said consent is verified: if it is not activated, a respective notification is displayed.

In Android devices:

- Exposure notification about a contact with a Covid-19 case developed by Google is activated;
- Bluetooth functionality is activated;
- Location services functionality of the device is activated: it is needed to discover any nearby Bluetooth devices, but the App does not access and does not use the location tracking of the device.

In iOS devices:

- Exposure notification about a contact with a Covid-19 case developed by Apple is activated;
- The User has to activate the Bluetooth manually, as iOS does not allow access to the Bluetooth module, and the App does not have a right to activate it.

The User is invited to enter his/her phone number in the App for the CDPC to contact the User and provide advice about further action, if there is a suspected exposure. In this case, verification of the phone number takes place (See Fig. 3, Flow 1). The User may choose not to provide his/her phone number or to enter the phone number at any other time, and start the verification process.

For each User who confirms participation in the contact tracing programme, once a day a unique Temporary Exposure Key (hereinafter, the TEK) is created in a protected area of the phone that is not accessible to apps. If the User is confirmed to have the Disease, keys collected during the last 14 days, as well as the starting time of their validity period are sent to the CDPC server. By means of the TEK, once per 10-15 minutes a Rolling proximity identifier (hereinafter, the RPI) and an encryption key that protect the meta data are created. The RPI and the encoded meta data required to quantify the infection risk by means of the BTLE broadcasting packages are periodically transmitted from the device. The type of BTLE broadcasting protocol data unit is ADV_NONCONN_IND, and it informs that is not possible to connect to the device. The transmission does not have a noticeable effect on the consumption of energy from the phone’s battery. Other nearby devices receive these packages, and if the receiving device is registered for the contact tracing programme it saves the received RPI in its protected memory. These data are not available to the App.

If the user has fallen ill, he/she is asked to transfer the TEK keys collected during the last 14 days to the CDPC that will publish them on a public server. Thereafter, the TEK may no longer be retrieved from the protected memory. In addition, to protect the privacy, the TEK of the current day may not be retrieved.

Other devices download these keys on regular basis from the CDPC server. The App transfers the totality of the keys to the Exposure Notification API that checks the protected memory of the device for any contact with the said keys. If a contact is found the Exposure Notification API quantifies the risk in the device according to the configured parameters. See Figure 1 for configuration parameters. The configuration parameters are requested from the CDPC server.[3]

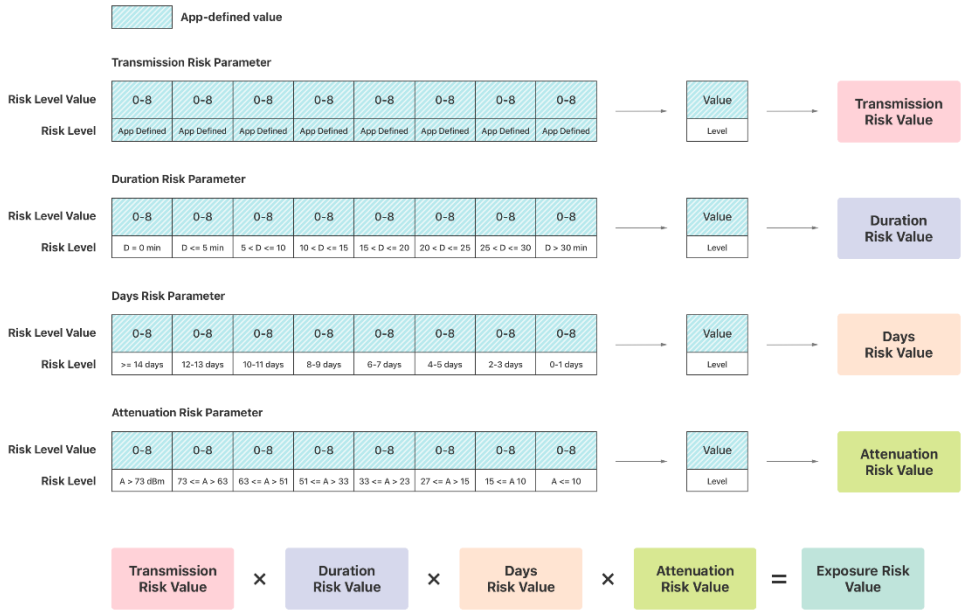

Fig. 1. Exposure risk formula[4]

For each recorded contact, the API returns its Exposure Summary, if the user has had any contact with an infected person. The said Exposure Summary contains the following data:

- Day (no time), when exposure took place;
- Duration of exposure: 5, 10, 15, 20, 25, 30 (if longer, rounded down to 30);
- BTLE signal interference level that allows to establish the approximate distance;
- Quantified infection risk.

The App is unable to determine the exact TEK the user has been exposed to, thus, it is not possible to determine the exact infected person who has been in contact with the user. The App acceptance process ensures that the App does not attempt to identify the infected person, for example, by transferring only one or a few TEK keys to the API.

2.1. Discovery of Contacts

See **Figure 2** for a description of discovery of contacts: User 1 and User 2 have smart devices with the Apturi Covid App and activated consents, they are approximately 2 m apart for at least 15 minutes and exchange the RPI. The phone also records

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

- The date when a contact was discovered,
- Duration of the contact and
- BTLE signal parameters that point to the recorded tentative distance.

These data are kept in the phone's storage for 14 days and then deleted. During the development, testing was carried out with various devices and at various distances, and several testing scenarios were prepared to ensure that the BTLE is calibrated for real-life scenarios as much as possible; currently the BTLE calibration is optimum, and tests will continue to implement further improvements therein.

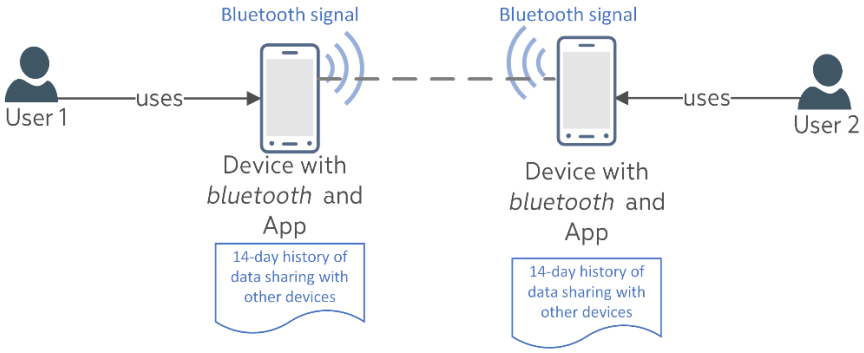

Fig. 2. Bluetooth contact tracing

2.2. User Notification Process

See **Figure 3** for user notification process concerning exposure to Covid-19. Let us assume that User 1 is still anonymous, while User 2 has voluntarily entered his/her phone number, and User 3 has a lab-confirmed Covid-19 infection. For all these users, a contact has been recorded during the last 14 days.

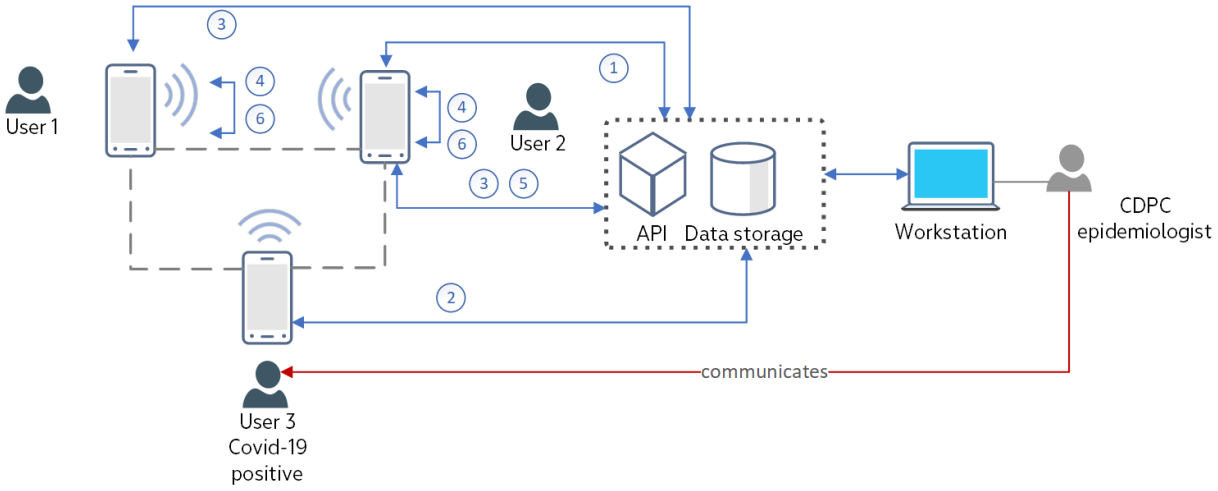

Figure 3. Exposure notification about a Covid-19 case.

Flow 1: Phone number verification process

Verification of the phone number takes place as follows:

1. User 2 enters his/her phone number in the App that sends it to the CDPC API.
2. The CDPC API returns a signed and encrypted JSON Web Tokens[5] token (hereinafter, the JWT token) that allows to delete the number from the system. An encrypted JWT token includes the phone number and the exposure_token. The encryption key and the exposure_token are stored in the server, however, no JWT tokens are stored there. In addition, a text messaging service is requested that sends the user an 8-digit code. The code is valid for no more than 30 minutes.
3. When the text message is received, the user enters the code in the App. A request to confirm verification is sent to the CDPC API. The request consists of the JWT token and the text message code.

By means of the SafetyNet[6] and DeviceCheck[7] API, the server makes sure that the request was received from a real device. The server may process a limited number of requests from one device.

Flow 2: Transfer of the TEK diagnosis key to the server

When User 3 has given his/her material for Covid-19 laboratory tests and the result has been positive, pursuant to the law, the CDPC receives personal data and contact details of the patient from the laboratory. The CDPC starts examination of potential contacts with a patient interview during which it is determined if the User uses the App, and answers to other questions are received. In this case, the interface of the CDPC solution generates an 8-digit number and initiates text messaging for User 3. The code is valid for no more than 30 minutes.

When the User enters this code in the App, the Exposure Notification API releases TEK diagnoses keys for the last 14 days and sends them to the CDPC server. Once per day, all received TEKs are compiled and entered in a public register[8]. Only those keys that are no older than two days before the onset of the disease are available on the server.

Flow 3: Collection of current diagnosis keys

New keys are uploaded to the server once per day. The App connects to the server several times per day to download the current TEK diagnosis keys. The App downloads only those keys that have not yet been downloaded.

[5] https://jwt.io
[6] https://developer.android.com/training/safetynet/attestation#quota-monitoring
[7] https://developer.apple.com/documentation/devicecheck
[8] https://apturicovid-files.spkc.gov.lv/dkfs/v1/index.txt

Flow 4: Verification of TEK diagnosis keys in the phone

The App has OS level background tasks that periodically check if any of the current TEK keys matches the RPI keys calculated according to the algorithm of the Exposure Notification API specification and saved in the protected memory of the phone.

If the calculation of the Exposure Notification API matches, and the user has verified his/her phone number, transfer of the Exposure Summary to the server is initialized.

Flow 5: Transfer of the Exposure Summary

Only Exposure Summary of User 2 is transferred together with the JWT token. The system verifies that the JWT token is valid by comparing it with the exposure_token saved in the database.

Flow 6: Distribution of Covid-19 exposure notifications

If the verified TEK diagnosis key (see Flow 4) matches the results, the App notifies that the user has been exposed to Covid-19, but does not inform about the place of the potential contact, nor the respective user or any identifying data.

3. Privacy

The following privacy principles were applied during the development of the App:

- Use and installation of the App is **free of charge** and **voluntary**. The User may use the entire functionality of the App or only a part thereof at his/her discretion. Failure to use the App does not result in additional liabilities and does not in any way undermine the rights/limit obligations with regards to the statutory epidemiological safety measures.
- Failure to use the App may limit a User's opportunity to promptly receive information or may extend the time needed to receive information, in particular if the User has been in inadvertent or contingent contact with a person found to have Covid-19, or if the person who has fallen ill with Covid-19 does not remember all persons with whom he/she has been in close vicinity.
- The User may start/stop using the App and change any selectable App settings at his/her discretion. User's changes in the App settings will apply to further availability of App functionality and will not affect any processing completed before such changes.
- The App shall not record and cannot disclose geographical coordinates (location data) of end devices of the User or any persons with whom he/she has been in contact.
- The App does not collect or process data that are not required for its purpose.
- Any user data are used exclusively for public health purposes, and are not available for any national, municipal or commercial purposes.
- The App respects human rights, and complies with the legal framework of the European Union and the applicable guidelines on data processing and security.
- For Terms of Use, see: https://apturicovid.lv/lietosanas-noteikumi/#en and for Privacy Policy: https://apturicovid.lv/privatuma-politika/#en .

4. Security Testing Report

Safety and security requirements of the solution are based on the principles of best practices, ISO 27002, and Cabinet Regulation No. 442 that lays down minimum security requirements for national and municipal information and communication technologies[9].

During the development, experts of the following bodies conducted iterative security testing: SIA IT Centrs, LATVIJAS MOBILAIS TELEFONS SIA, TestDevLab SIA, and CERT.LV. For security tests, OWASP Testing Guide v4[10], OWASP MASVS L1 methodologies and other OWASP recommendation on safe development of solutions were used.

The following was established during the final security testing:

App data on its crashes and failures that contain the smartphone model and technical data on the failure are sent and compiled by means of the Firebase Crashlytics service. The App operates autonomously and requires minimum user engagement, and optimum operation needs to be ensured for a large number of users and many devices produced by various makers. The developers need to know about its crashes and failures. This allows to discover technical problems for the developers to promptly make the necessary updates.

[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. Review of App code

Please abide by the best practice for responsible disclosure of vulnerabilities, when you inform about any problems discovered during the review of the App code: https://cert.lv/en/about-us/responsible-disclosure-policy.