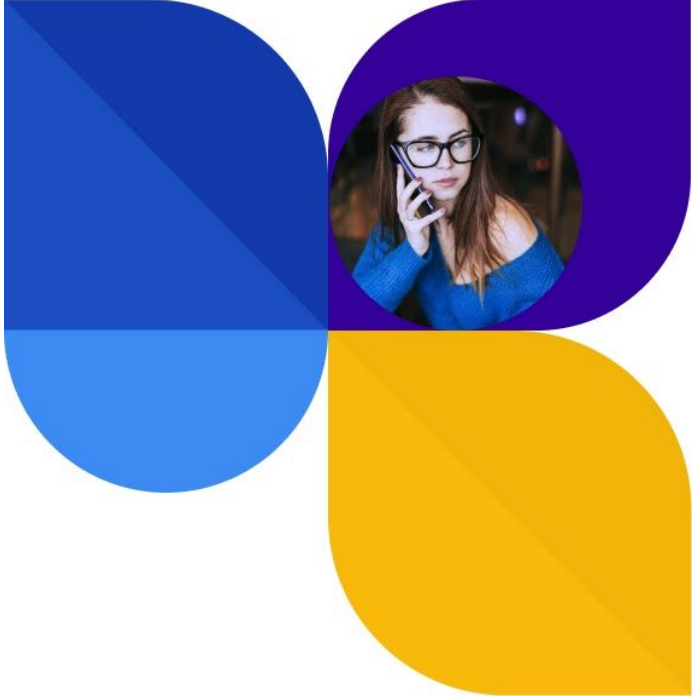


LEMON

The COVID-19 Tracing-App

High-Level Tech Overview

10/09/20

Product Overview

The new COVID-19 Tracing-App "**LEMON**" wants people to be safe while protecting life and data equally. The promise of our App: **We only trace the virus, not humans.**

Its goal is to simplify and accelerate the process of identifying people who have been in contact with an infected person, thus providing a technological foundation to help slow the spread of the SARS-CoV-2 virus. The system aims to minimise privacy and security risks for individuals and communities and guarantee data privacy.

The app offers several functionalities:

- **COVID-19 location and risk of exposure tracing**: The app uses a device's Bluetooth in order to trace contacts with other app users. An external system called DP-3T is used for this process that has been accepted by multiple countries across Europe as a privacy-preserving system that traces COVID-19 exposure risk. In summary, the system works by logging all contacts between users and storing them on the device. Should a user test positive and the user gives consent to notify other users, these contacts are sent to the server anonymously. Each device regularly pulls all contacts with contagious users from the central server and checks to see if any of them correspond to their unique identifier. For more information on this process read up on DP-3T documentation that can be found here.
- **Symptom tracking**: Users can track their symptoms, whether they are tested positive or unsure about their current status. This information can be shared anonymously, to help educate the medical community about spread and developments of symptoms, COVID-19 and support epidemiological models. In addition, the age as well as the date of occurrence of the first symptoms and the date of a positive test result are collected and can be shared anonymously.
- **Information and statistics**: The app provides key statistics on the developments of COVID-19 globally and in the country of the user. Furthermore, the app provides tips on social distancing, hygiene and when to seek medical advice as well as the contact number to do so.

Documents

Full documentation on the project can be found here. Otherwise, see below for links to useful project documentation.

- **Architecture Overview**: AWS Project Architecture
- **Mobile Application Flow**: User flow stories

- **Open Feature Roadmap**: Roadmap
- **Data Diagram**: Data Flow Diagram

Tech Architecture

See below for details on the technical architecture of the application.

Phase 1

This details some of the technical architecture that has been proposed for phase 1 of the application.

Mobile Application

- **Framework**: React Native (iOS, Android)
- **Storage**: SQLite and encrypted file storage
- **Analytics**: Crashlytics (Mobile error logging and reporting)
- **Build Pipeline**: Fast Lane (build and release manager)

Backend Application

- **Framework**: .NET CORE 2.2 Web API
- **ORM**: Entity Framework with MS SQL DB
- **Error** Logging: Sentry
- **Push Notifications**: Firebase Cloud Messenger (FCM)
- **Authentication**: RSA key pairs with AES session keys
- **Build Pipeline**: AWS CodeDeploy
- **Documentation**: Postman and Swagger

Infrastructure

- **Provider**: Amazon Web Services (AWS)
- **CDN**: CloudFront
- **Hosting**: Elastic Beanstalk (EB)
- **Database**: Relational Database Service (RDS)
- **Key Storage**: Key Management Services (KMS)

Tech Principles

Privacy by design

Privacy by design requires that the user's privacy is taken into account throughout the whole engineering process.

Decentralised Storage

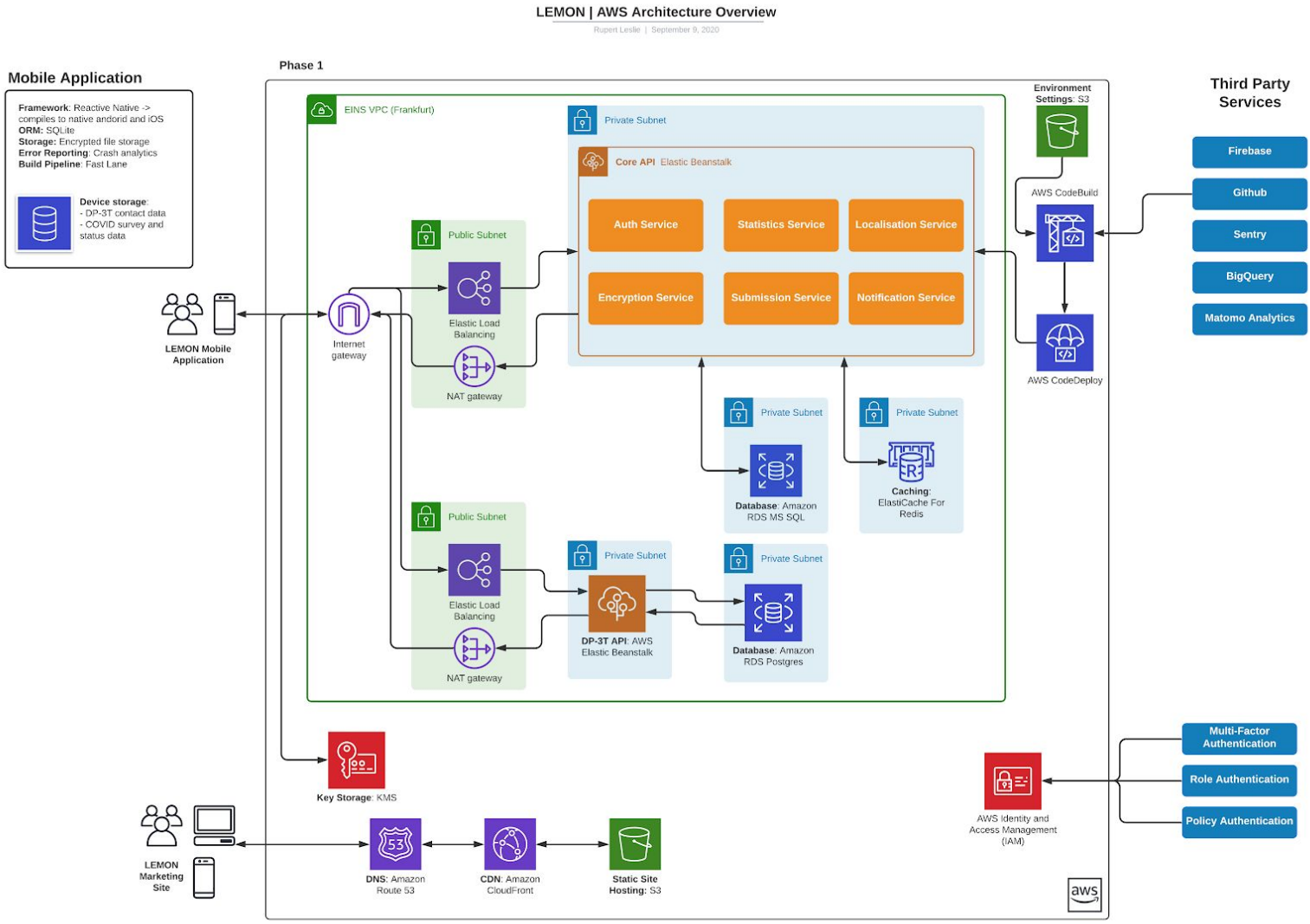
All sensitive information is stored on an LEMON user's device, offering both improved privacy and security.

Self-Sovereign Identity

The principles of self-sovereign identity (SSI) intend to put the ownership of a user's online identity directly in their own hands. This can be done in various ways and consists of many sub-approach processes. More recently, the introduction of decentralised ledger technology (such as blockchain technology) which provides a trustless verification of identities (including pseudonyms identities) and fully secure data encryption and ownership offers a path to implement and make use of self-sovereign identities.

Platform Overview

The platform is structured as shown in the diagram below:



DP-3T Integration

A key part of the application is the contact-tracing functionality provided by DP-3T. For simplicity and security, this integration between the LEMON and DP-3T system was kept as simple as possible. There are two parts to the DP-3T system that must be integrated to LEMON:

- DP-3T app software development kits (SDKs)
- DP-3T Server

DP-3T SDK Integration

The DP-3T SDK code and documentation can be found here for IOS and here for Android. Essentially this side of the DP-3T system is where the majority of the functionality comes from. It is responsible for the actual activation and monitoring of Bluetooth signals, the ephemeral Id generation and other security measures. All of this functionality takes place within the SDK itself, the LEMON application simply wraps some of the SDK methods in order to ease the SDK usage.

Some minor configuration is required on the SDK. This simply involves pointing it to the LEMON hosting of the DP-3T backend server and specifying the public key that corresponds to the LEMON backend server key pair in order to establish secure communications.

DP-3T Server Integration

As specified by DP-3T, each application using the contact tracing system will have to set up its own backend. This backend is simply used as a central data store for any contacts recorded by the mobile application. The mobile application simply pulls information from the DP-3T backend and searches for any contacts involving its own ephemeral Ids.

Therefore, as displayed in the architecture diagram above, the DP-3T backend is completely independent of the LEMON backend API. They are hosted within the same virtual private cloud (VPC), however, these two systems do not communicate in any way with each other. Due to the nature of the DP-3T system, there is no need for the two servers to communicate directly with each other, this includes both communications to the mobile application as well as interoperability between different DP-3T servers.

In terms of configuration, all that was required was to update the server key pair to ensure complete security of the system.

Interoperability

In order for the contact tracing to function effectively, it is crucial that a critical mass of the population is using some form of contact tracing. Restricted access to required tracing APIs from

Google Apple Exposure Notification (GAEN) service and isolated strategies across countries have provided barriers and restricted parts of the population from onboarding onto a unified high-tech contact tracing solution.

In addition to this , as the world attempts to return to some sense of normalcy, we will see an increase in travel for both business and leisure reasons. This renders current tracing apps effectively inept due to the current lack of interoperability between apps largely due to the inability to reach a consensus around a number of factors.

The LEMON application aims to overcome this by pulling tracing information from as many different locations as possible to provide our user with the most comprehensive tracing experience possible. For initial release this will include pulling tracingkeys from the following countries:

- Switzerland
- Germany
- Italy
- Austria
- Spain
- Latvia
- Denmark
- Poland

In order to stick to its core ideal of privacy by design, LEMON is taking a decentralized approach to interoperability between different countries. This means that the LEMON application on the device is responsible for managing this interoperability, rather than a central server that pulls the various keys.

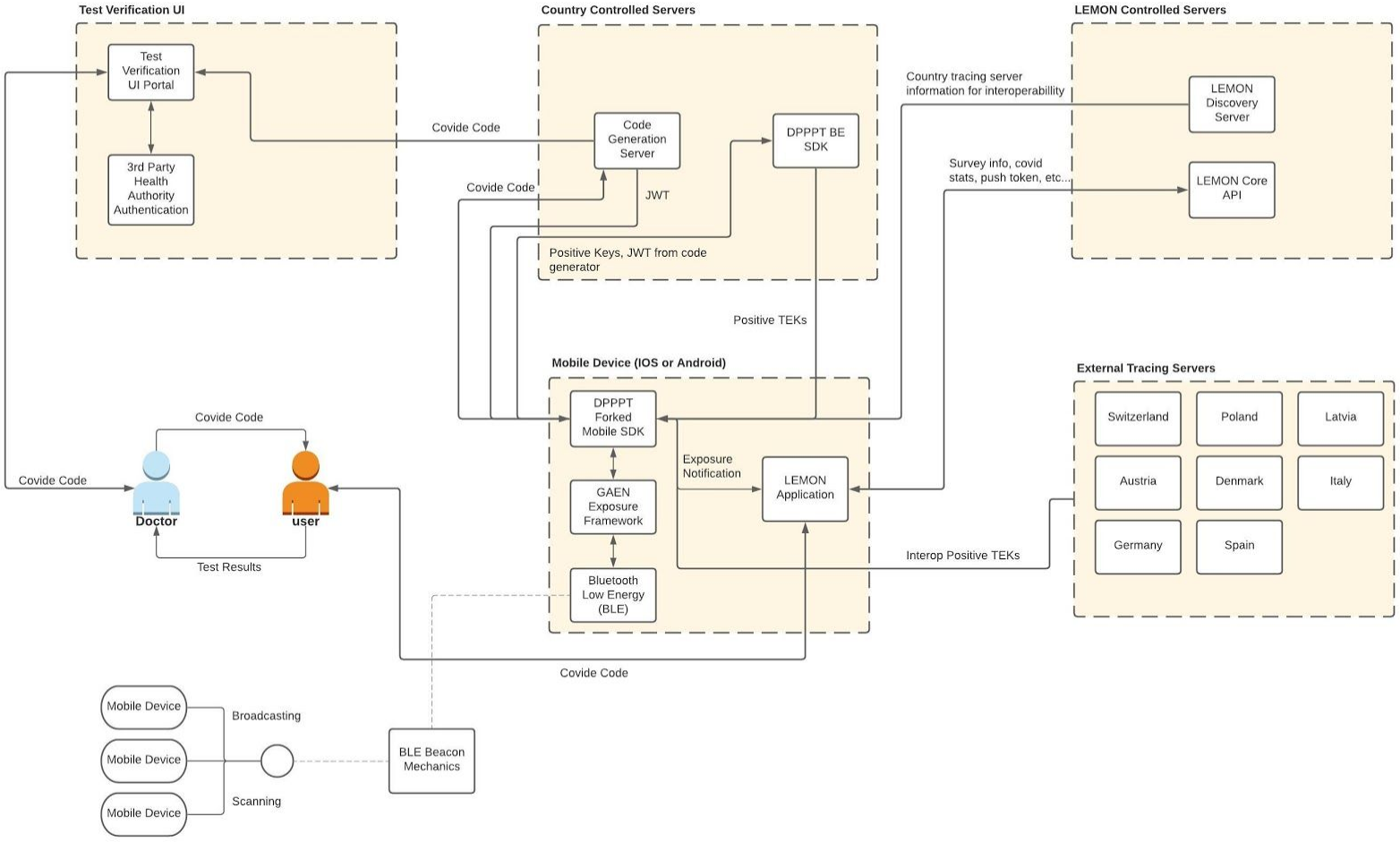
Test Verification

In order to launch in Switzerland it is crucial that the test verification process stipulated by the government is included into the LEMON application. This means that LEMON has to interface with the CovideCode System run by the Swiss application.

Based upon this, it was decided that integration with Swiss DP-3T would be the most effective strategy in achieving test verification functionality in Switzerland as well alongside this test verification. This means that LEMON will not only pull positive tracing keys from the Swiss server for interoperability, but also upload positive keys should a user successfully verify their positive status.

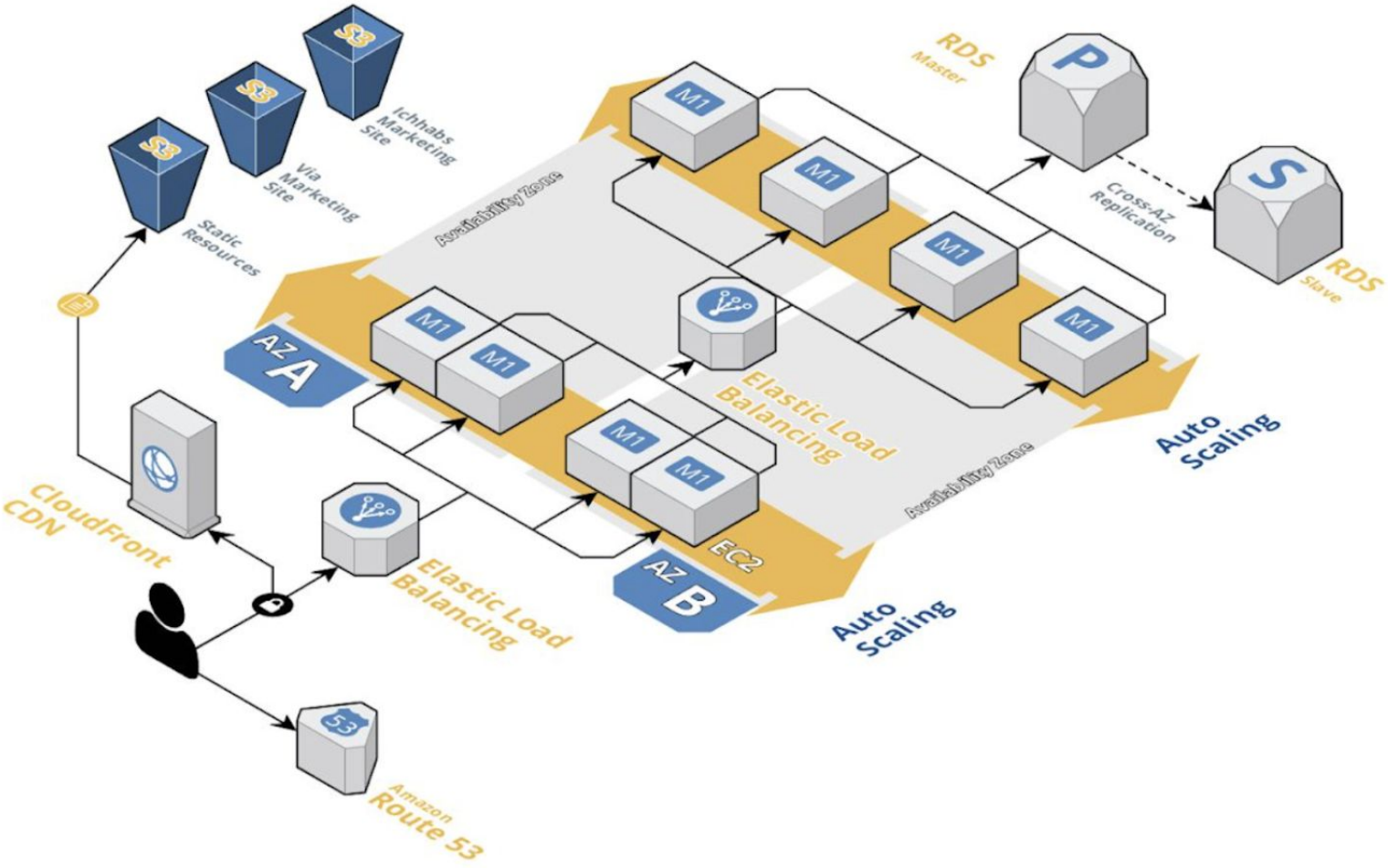
System Diagram

Based upon the above information. The LEMON system will be set up as follows:



Infrastructure Overview

The project infrastructure is set up using Amazon Web Services (AWS). The infrastructure is laid-out as detailed below:



Third-Party Overview

Overview of all third parties involved in data processing or providing tech services.

External Data Processing Services

Name	Sensitive	Location	Service Type	Data Passed	Data Affected
Sentry	Yes	Google Cloud (unclear)	Error logging	Non identifying datasets Stack traces from backend	Anonymised Stripped Error logs
AWS	Yes	Europe	Cloud Hosting		See Architecture Document for data in databases on AWS.

Other Services

Name	Sensitive	Location	Service Type	Data Passed	Data Affected
Firebase	No	Can select Europe	Push notification service	Push token	Hashed App instance Id
Github	No	Mostly US	Source Control	None	See Architecture Document for data in databases on AWS.
Big Query	No	Can select Europe	COVID-19 statistics	COVID-19 Statistics	None
Crashlytics	No	Can transfer to US and other operating countries	Mobile error reporting	Device Id, Crash specifics	Hashed App instance Id

Self-Sovereign Identity Overview

The use of self-sovereign identity will further enhance the privacy and functionalities around identity that LEMON can offer in the future. SSI's will permit LEMON users to issue proof of certain

events or facts to other ecosystem stakeholders for verification without compromising their privacy. It, therefore, permits for zero-knowledge proofs whereby stakeholders can disclose certain information without giving away further information in the process.

Examples of such proofs (or verified credentials, in this case) would be if a user were to be tested (negative or positive) and then be vaccinated later on. The associated medical professional would attest to the user having undergone the test by scanning their QR code identity within the app. This attestation would then create a credential that is stored in the users' app for them to then show to other stakeholders within the ecosystem. This will allow other stakeholders in the ecosystem to trust that the app user has had a test, what the result was and/or whether or not they are up to date with their vaccinations - all without compromising or revealing any of the person's information.

COVID Test Verification

In order to prevent false positives, it is essential that all users must be verified as having Covid-19 before they can update their status on the application. This process will work using a Covidecode. Essentially this is a unique code that is associated with a positive test result once confirmed by an official testing laboratory.

As of this moment, we are waiting upon the Swiss Government to provide us with authorisation to gain access to this test verification process. Once approval has been granted by the BAG, we will be able to copy the same test verification flow exhibited in the SwissCovid app.

The process can be seen on the public SwissCovid & DP3T repo here: https://github.com/DP-3T/dp3t-app-android-ch/blob/master/documentation/screenshots/en/screenshot3.png.

The user will receive a CovidCode from a health practitioner upon a positive test result being recorded. The user will enter that into the LEMON app when updating their positive status, this will unlock the bluetooth trace data stored on the device, and allow it to be accepted by the contact tracing server.

FAQs

See below to answers for some frequently asked questions.

Who is the app operator / Wer ist betreiber der app?

App operator: Global Citizen Foundation

Data and tech Enabler/Provider: VIA AG

How do we anonymise / Wie wird anonymisiert?

The LEMON app implements many measures to anonymise its users while still giving actionable insights which assist in saving lives. LEMON does not intend to store any direct personal information about its users, such as name or email addresses. The only details that are stored is a Hashed App Instance ID (the instance Id being randomly generated when the app is being installed) and is done to ensure protection against multiple submissions and bad actors. This is also done in order for the push token to communicate with the user.

The core of the anonymisation is centred around a decentralised and private data design architecture where a user's data does not leave their device without them granting permission. There are two areas in which a user can grant permission to share data; through submitting survey information and submitting tracing information.

Survey information may be submitted any time a user completes the form. Should the data be submitted it is completely anonymous and not stored against any identifier. Unfortunately, this does mean that it is not possible for a user to delete this data off of the server once it has been donated.

Should a user test positive, they are given the option to share Bluetooth contact data in order to help save lives by notifying any user that they may have been in contact with. This process follows a strict privacy structure as laid out by DP-3T that maintains the user's complete anonymity.

How do we use data / Wie werden daten verwendet?

There exist two main areas where LEMON interacts with, or stores, data: the user's device and the server.

The user's device is the default store for all application data once the app has been downloaded. The only information stored on the device is the user's status and survey information as well as person to person contacts as detected by the DP-3T Bluetooth system. The survey and status information on the device is not used for any purpose but to display to the user, and for the potential sharing to the server, should the user give permission. This data is not stored for any other purpose and is not used in any other way. The contact tracing information is stored for the sole purpose of sending to the server should a user test positive and they choose to notify other users of a potential infection risk. Should the user choose not to notify other users then this data never leaves the device and therefore is never used.

The only way in which data is sent to the server is if the user gives express permission. As explained by DP-3T, all contact information that is shared has no meaning to any outside entity other than the devices that are involved in the specific contact case. On top of this, all data is

removed after a specified period to ensure that it is not used for any other purposes in the future. All survey data that is submitted is done so completely anonymously such that authorities and epidemiologists can gain further insights into the current state of the COVID-19 pandemic whilst completely protecting the privacy of all users.

What happens with the data collected on symptoms / Was passiert mit den symptom-Daten genau?

The data that is donated and shared from users on their symptoms and test results will form part of their status and survey data. This anonymised data is then viewable via a data dashboard to authorities.

Where is the data stored / Wo werden die daten gespeichert?

All information is stored on the LEMON application on the end-user device. This data is stored securely using cryptographic measures for protection. The contact tracing information is managed by DP-3T software and stored securely on the device separately to the LEMON encrypted information.

Contact tracing information that the user chooses to send to the server is stored within the LEMON infrastructure, on a DP-3T specific database. This database is separate to the LEMON proprietary code and data storage. It can only be accessed by the DP-3T software.

All other related data that the user shares is stored on the LEMON server. This infrastructure, along with the LEMON DP-3T server is stored on an AWS hosted database, located in Frankfurt Germany.