EINS

High-Level Tech Overview

April 20th 2020

Product Overview

The new Covid-19 Tracing-App **"EINS"** 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 the user's geolocation in a private by design logging method to save the past location of the user on the user's device. Once a user tests positive for the virus, they are given the opportunity to share their past location data. People with symptoms can then use the app to compare these data points with their own range of action. Based on an algorithm, the App calculates a risk of exposure for each user.
- Symptom Tracking:
  Users can track their symptoms, whether they are tested positive or unsure about the current status. This information can be shared anonymously, to help educate the medical community about spread & 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 & Key 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

Architecture Overview: Diagram Link

These two documents give an overview of all user-orientated data flows within the first version of EINS:

Text: EINS - Data flow user stories

Diagram: Data diagram

Open feature roadmap: Link

Tech Architecture

Phase 1

Mobile Application

- **Framework**: React Native (iOS, Android)
- **Storage**: SQLite and encrypted file storage
- **Analytics**: Crash Analytics (Mobile error logging and reporting)
- **Location**: Google location API
- **Build Pipeline**: Fast lane (Build and release manager)

Backend Application

- **Framework**: .NET Core 2.2 Web API
- **ORM**: MS SQL, NoSQL DB
- **Location Service**: Google location API
- **Error logging**: Sentry
- **Push notifications**: FCM (Firebase)
- **Authentication**: RSA Keypairs
- **Build Pipeline**: Github pipeline
- **Documentation**: Postman / Swagger

Infrastructure

- **Provider**: AWS (Switched to another provider in progress)
- **CDN**: CloudFront
- **Hosting**: EB
- **Database**: RDS

Tech Principles

Privacy by Design

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

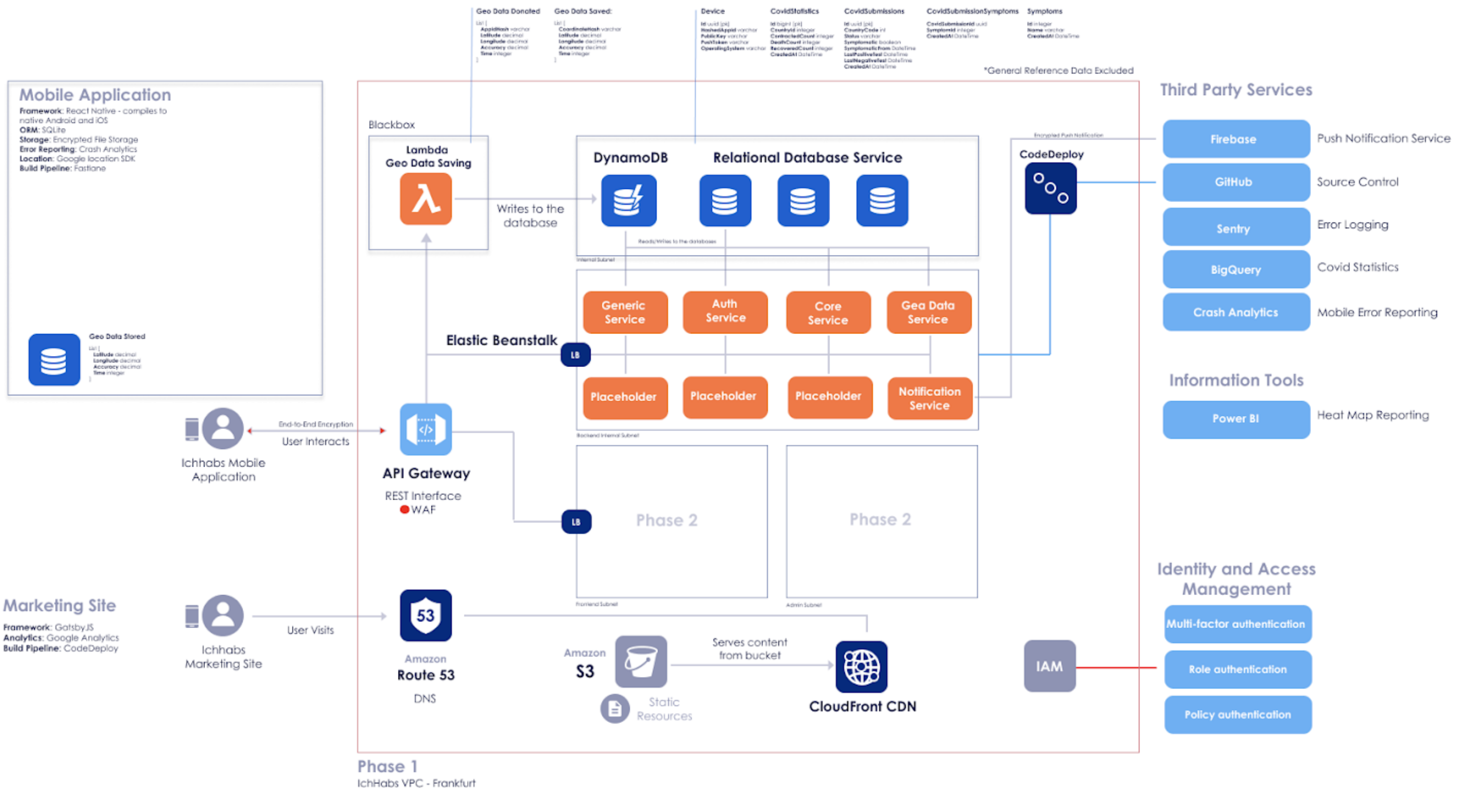
Decentralised Data Storage

Decentralised data storage enables EINS users to store their geolocation data on their own devices, offering both improved privacy and security.

Self-Sovereign Identity

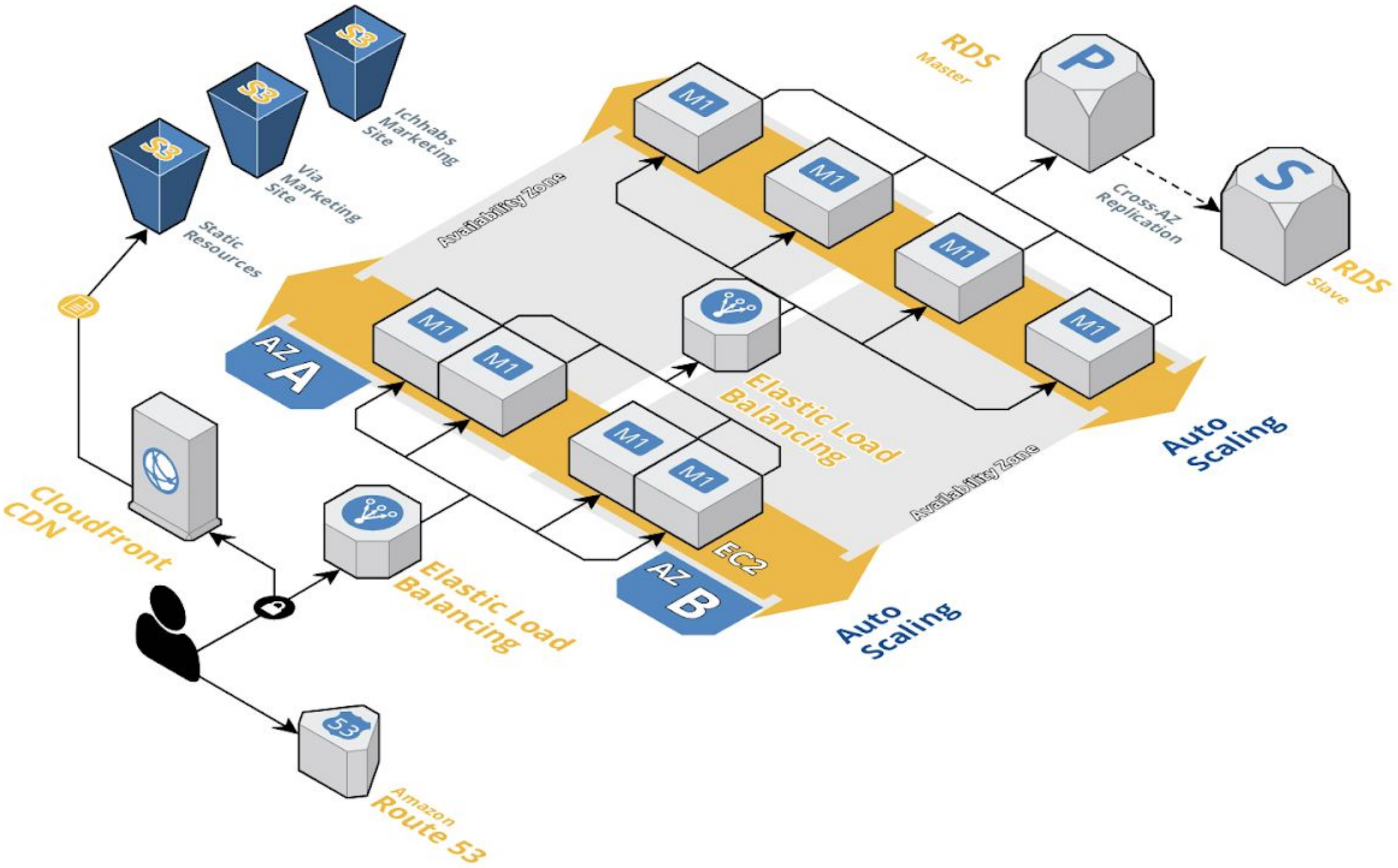
The principle of self-sovereign identity (SSI) intends to put the ownership of a user's online identity directly in their own hands. This can be done in various ways and consists of many sub- approach processes. More recently, the introduction of decentralised ledger technology (such as blockchain technology) 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



Link for diagram: Link

Infrastructure Overview



- **Provider**: AWS
- **Content Delivery Network**: CloudFront
- **Hosting**: Elastic Beanstalk: Orchestration service offered by Amazon Web Services for deploying applications which orchestrates various AWS services, including EC2, S3, CloudWatch, autoscaling, and Elastic Load Balancers
- **Data management**
    - Core: MS SQL instance on RDS for core service
    - Location Data: DynamoDB (NoSQL database)

Overview Third Parties

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

Name	Sensitive	Location	Type of Service	Data passed	Data affected
Firebase	No	Can choose Europe	Push Notification Service	PushToken	AppInstanceId
GitHub	No	Mostly US	Source Control	Non	Non
Sentry	Yes	Google Cloud (do not really know)	Error Logging	Non identifying datasets Stack traces from backend	Non Anonymised Stripped
Big Query	No	Can choose Europe	Covid Statistics	Non We use this to query for new Covid Stats per country	Non
Crash Analytics	No	Can transfer to US and other operating countries	Mobile Error Reporting	DeviceId Crash Specifics	AppInstanceId
Power BI	No	Europe	Heat Map Reporting	Lat Long Datetime	Non
AWS	Yes	Europe			See Architecture Document for data in databases on aws.

SSI Overview

The use of self-sovereign identity will further enhance the privacy and functionalities around identity that Ich Habs can offer in the future. SSI's will permit EINS 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.

FAQs

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 EINS app implements many measures to anonymise its users while still giving actionable insights which assist in saving lives. EINS 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 an AppID (which is randomly generated when the app is being installed) which 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, or force the app to do a local contact tracing check.

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. Once a user tests positive, they are given the option to donate and share that data in order to help save lives by notifying others of high-risk areas. The data that is donated and shared is then anonymised further by adding random noise to data attributes such as age. The data is then added into a pool of other donated and shared data without the integrity of a 'path' intact. This makes the reverse correlation of any set of the points to any human much more difficult.

The final measures used for anonymity are applied when a user performs a self-check against the heatmap data. Noise is added to the parameters of the request so that it is not possible to tell which user is requesting which window. The matching is then done on the device, and the results are shown to the user.

How we use data? Wie werden Daten verwendet?

There exist two main areas where EINS interacts with, or stores, data: the user's device and the server. The user's device will store all of the location data of that specific user once the app has been downloaded. This data is solely used for the user to check against the risk heat map that is downloaded from the server. The app will also store the user status and survey data until such a time when the user opts to donate and share their data, once tested positive.

The EINS server only stores data that has been donated and shared, including risk heatmap data from the geo-locations of past positive patients as well as donated survey and status data. The survey data is never used by the apps. However, parts of the heatmap data are downloaded at regular intervals by the app's users tracing their contact. This anonymised heatmap data, as well as the survey data, will be viewable via a data dashboard to authorities if requested and needed.

What happens with the data we collect 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?

The EINS application.