Sia Partners - StopC19 App

Design and Development Brief

1 Introduction

Sia Partners has partnered in (10)(2a) with Accenture, SopraSteria and Orange, to build a complete system around "Contact Tracing" principles to enable governments to manage Covid19 lockdown ending.

This project has been driven as a civic initiative, initially to allow the (10)(2a) government to make use of a global set of features (and not only contact tracing capability) that can be activated / deactivated before the launch of the application when lockdown ends. All companies have worked since mid-March and deployed on a pro bono basis a team of 75 senior developers, technical experts (architecture, smartphone platforms, telecom, Bluetooth, security, scalability, testing...), functional consultants and data-scientists with a view to delivering a first release on April 20th. At this date, the solution was deployed on a scalable pre-production environment, enabling testing, audit, and field trials.

Our objective is to deliver all source code to governments who want to start a "Contact Tracing" project and who want to accelerate their project by using our complete platform. Although there are a lot of additional functionalities in the consortium backlog (these features have been anticipated for future development), next steps will consist in demonstrating our system to government experts, disclose source code for external audits, reshuffle our backlog by adding governments modification requests, add releases in our roadmap to develop implement these features with our core-team, and help local teams to customize our package.

As of April 20th, our system and its source code can be reviewed, tested and used by the (10)(2g) government to setup its Contact Tracing project. In the meantime, we will also continue our discussions with (10)(2g) government who tries to develop such a system.

2 Convictions

We have started our project 5 weeks ago, when no requirements were available from neither (10)(2g) nor European governments. We have built our system based on several convictions, and with the objective to manage contact tracing, and not to intervene with digital freedoms and privacy. The aim is to provide healthcare authorities with a decisive investigation tool to prevent any form of resumption of the epidemic by identifying any new cluster:

- Rebuild contamination chain from an individual tested positive for COVID-19 in a systematic, reliable and massive manner
- Record the consent of any individual before tracing its contacts
- Prioritize population tests on exposed individuals.

We have designed the application according to the following design principles:

- Usage of smartphones and on-board Bluetooth functions. Our tests demonstrate a technological robustness and a technical capacity to be deployed in mass, thanks to the use of powerful algorithms;
- Collection an explicit consent from the user of the Smartphone application (opt-in), reinforced in the event of contamination. The mass adoption of this application (target 60% of the population) is an essential criterion of its effectiveness;
- *Privacy by design* for all contact tracing data. All other data should be anonymized. If some health data need to be nominative, only healthcare personnel shall have access to them;
- Opt-out guarantee, individually at any time and globally in the event of the end of an epidemic episode;
- With regard to health data storage, the principles of sovereignty and cybersecurity must apply and data hosting should be organized in a proper cloud;
- End-to-end service, from citizens to healthcare professionals and relevant authorities;
- Modular application, to be able to be gradually deployed;
- Smartphone application should be available in Apple and Google stores a couple of days before lockdown ends, to allow progressive enrollment of citizens in order to maximize the percentage of application deployed on smartphones when lockdown will be over. Contact tracing features can be activated during lockdown for voluntary users in order to constitute a representative sample of contact tracing data to train datascience retracing algorithms;
- Smartphone application could be completed with other electronic wristbband-type devices intended for precarious people, the elderly or minors under 14 years of age, but we have not started to work on these features.

3 The Solution

This application is intended to be transferred and managed by the government or public services, in order to manage the end of lockdown. The goal is to guarantee:

- limited dependence on third-party companies (hardware & OS)
- control of data acquisition, storage and management
- control of security protocols

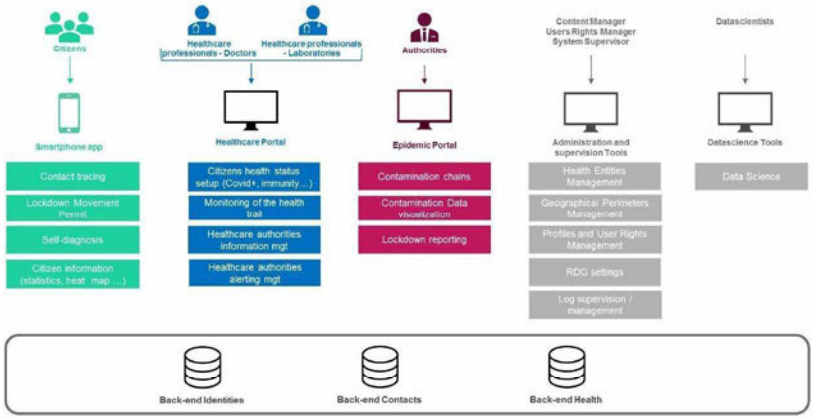
As of today, Intellectual Property is owned by the consortium, but we are ready to transfer all source code and all rights to use and modify it to governments before application is widely deployed. We have not decided to publish it as an open source project for the moment, since some governments may argue they do not want to disclose all security items. As a consequence, open source publication decision will come from discussion with governments.

We are ready to support modification and maintenance of this system.

3.1 Functional overview

The system we built is an end-to-end digital service, comprising:

- an application for iOS (v11+) & Android (v5+ - api21) smartphones
- a robust and secure and scalable back-end
- dedicated web portals for healthcare professionals and authorities.



3.2 Smartphone Application features

- **Onboarding:** after download from Apple or Google stores, at first launch of the application, the user is requested to validate Terms of Use of the application to create a unique account/device Id in the Identities back-end. This procedure is fully anonymous (no phone number, no name, no login requested) and protected by a captcha mechanism to limit the risk of multiple device registration (other mechanisms could be implemented like *WhatsApp* enrolment – transmitting user phone number and protected by a SMS confirmation. This alternative ensures maximum protection but request a user identification that is considered in France as no more anonymous, even if back-end storage is dedicated and independent).
  Identities back-end acknowledge the enrolment (Json Web Token) and transfers to the smartphone the hardware dependent parameters it should use for contact tracing feature.

- **Contact tracing:** *this functionality is described in detail in a separate chapter.* Two functionalities are accessible to the user:
  - 3 Level-Consent management:
    - user doesn't want any contact tracing. No contact data will be collected by the smartphone (and of course no data sent to any back-end server)
    - user allows contact tracing data transmission to the back-end only when he has been tested as Covid positive, and allows to be alerted by the app when he has had a contact with a Covid+ user. Bluetooth will be automatically enabled (this mode should be the most used)
    - user allows to send every day his contact tracing data to help algorithms improvement (useful for testing and field trial)
  - Contact tracing dashboard: displays the number of contacts (of contact tracing) of the user on a daily basis, measuring the number of all kind of contacts (Covid+ or not, with no distinction). This dashboard based on smartphone data is refreshed every day (to avoid retracing of Covid+ contacts). This feature is according to us a must-have in case we want to maintain some social distancing recommendation after lockdown, since it will help users monitoring the effects of their behavior)

- **Covid testing follow-up:** Contact Tracing has no sense if the retracing algorithm is not triggered by a Covid+ information. Our conviction is that this information cannot be entered by the user himself, since it will allow a group of hundreds ill-intentioned people to generate country-wide panic, just by declaring themselves Covid+.

  Our system relies on healthcare professionals – and only healthcare professionals – to update Covid test (or immunity test) results. This action will be performed through our system Healthcare Portal. (We can also connect to an existing healthcare system through webservices, if such a system exists (it's not the case in France for small laboratories, nurses, doctors) and if the existing system is compliant with anonymization and privacy requirements).
  Our system proposes a fully anonymous testing result transmission:
  - When a citizen goes to a laboratory for a Covid test, the laboratory assistant connects on our Healthcare portal, which generates a one-time "medical key" (with a control character to avoid typing mistakes). No other information (name, id) is collected by the laboratory. This key is stored in the Healthcare back-end (storage of health data in a relevant cloud). This back-end is not connected to Identities nor Contact back-ends and has no key to enable cross-referring (event for database administrators)
  - The citizen enters this key in its smartphone. Starting from this point, the smartphone will start a polling mechanism of the Healthcare database till it finds a test result in front of its key (we do not use notification mechanism for better reliability but also to avoid connection between device Id and medical key)
  - When the test result is entered by the laboratory in the Healthcare portal, the smartphone will get it through this mechanism and will display it to the user. (several medical keys can be generated on a single smartphone, for multiple tests, but they can also be used to collect test results from children or relatives without smartphones)
  - If the test delivers a Covid+ result and if the user has enabled contact tracing (level 2 or 3), the smartphone starts the contract tracing process (see below)

- **User profile definition:** the user may enter some personal data that will be kept an encrypted in his smartphone (they are never transmitted to the back-end):
  - Name
  - Date of birth
  - Address
  - Children or relatives

  This information is useless (and not used) for contact tracing but is mandatory to issue a Lockdown Movement Permit as designed by French authorities.

- **Lockdown Movement Permit:** during lockdown in [redacted], non-Covid positive people may move from their lockdown location to go to their office (if no home-office), to go to medical appointments, to buy food and first necessity products, or perform short sport activities. This functionality generates the QR code that could be requested by police officers.

- **Individual Lockdown Instruction (next release):** after lockdown, free movement authorization, lockdown instruction (in case of Covid+ testing), warning (covid testing and lockdown recommended, after contamination suspicion through contact tracing process).

- **Covid Autodiagnosis:** link toward government autodiagnosis page (app v1 – April 20th), that will be replaced by a dedicated tool in next release.

- **Covid Dashboard:** data visualization of daily epidemics statistics collected from healthcare authorities.

- **Useful information**

- **User Settings management:**
  - account & data deletion
  - app notification enablement

- **Statistical data for epidemics follow-up:** apart from contact tracing feature, that has a dedicated user consent recording, user may allow (or not) the transfer of anonymous daily data for epidemics follow up (number of contacts per day – if contact tracing is enabled, Covid status, age – if indicated in user profile, zip code – if indicated in user profile)

3.3 Back-Office web applications features

- **Administration Web Portal:** connection is secured (2 factors) and restricted to system administrators:
  - Users rights management: enables to give healthcare professionals ad authorities the relevant user rights combining habilitation to a functionality x Entity (to which the user belongs) x geographical perimeter (on which the user may act)
  - Parameters and system Rules setup
  - Log management and supervision

- **Healthcare Web Portal:** connection to this portal is secured (2 factors) and restricted to registered healthcare professionals (in France, healthcare authorities publish a daily list of registered professionals):
    - Covid Test Management (available in April 20th release) as explained in smartphone section
    - Patient follow-up for doctors (next release)

- **Epidemics Web Portal:**
    - Epidemics dashboard based on collected anonymous statistics and tracing data analysis
    - Lockdown follow-up (next release)

3.4 Contact Tracing

Contact tracing feature is implemented in both smartphones and server side to maximize anonymization and privacy. Following explanation is done when consent level 2 has been set by the user (user allows contact tracing data transmission to the back-end only when he has been tested as Covid+).

We consider that a "contact moment" is represented by a Bluetooth signal reception, with a sufficient level, during a sufficient time lapse.

Each smartphone is generating a periodic ID that will be recorded by a neighboring smartphone when net level (RSSI reprocessed thanks to transmission power) is greater than a threshold (depending on smartphone model, set up at onboarding) and a duration greater than a threshold (set up at onboarding). [*Mechanism are very different in iOS and Android contexts and app in foreground and background*]. Data are stored in the smartphone during 21days, deleted after dans never sent to the back-end at this stage.

When a smartphone A triggers contact tracing process, it sends to the Contacts back-end the list of its periodic IDs + the one of smartphones with which it had a "contact moment" (with timestamps and also other parameters like signal levels...). A back-end algorithm filters then the "contact moment list" sent by A to create a smaller "risky contact list".

In the meantime, all smartphones B, C, D... are polling the "risky contact list" (with some data transfer optimization mechanisms) and download it on their respective smartphone. Contact back-end has thus no idea who called be the smartphones represented by the contact periodic IDs given by A.

Locally, B smartphone analyze the risky list and alerts its user in case it finds one of its periodic ID in the downloaded list.

3.5 Datascience tools

- Datascience tools and algorithms are used for suspicious risky contacts detection from contact tracing data
- Machine Learning is used to tune contact tracing parameters (server side and smartphone side)
- Datascience and data-visualization tools are available to analyze tracing and statistical data (with a specific Analytics and Datascience back-end)

3.6 Data storage

On smartphone side :

- All data are stored encrypted in Android devices
- User + personal data are stored encrypted in iOs devices
- Contact tracing data (just composed of anonymous periodic IDs that nobody can retranscript except the mobile who has generated it) are not crypted in iOS devices, since encrypted data cannot be used when app is running in background

All data exchanges between smartphones and servers are encrypted.

On back-end side, all operational data are stored in 3 different back-ends (Identities, Healthcare, Contacts) with no cross-referring key between them. All these back-end are today hosted in Outscale cloud (Dassault Systems) with development, test and pre-production environments. Healthcare data are in a specific "health data" cloud (even if they are fully anonymous up to now, just in case tomorrow someone wants to add no anonymous medical data).

4 Product development & project management

4.1 Project Team

We have created a dedicated project team to build this system, composed of functional teams and development teams, for back-end, back-office, smartphones and datascience. Of course, all project was using Agile methodology.

All software developments have been executed by Accenture, SopraSteria and Orange experts. Development environments are within their VPN architecture and on Dassault System Outscale cloud, with highest level of security.

All these companies are certified ISO9001 and ISO27001.

The team size is 75 people:

- 6 project management
- 6 UX / UI
- 8 functional consultants
- 15 smartphone developers (native iOS & Android codes)
- 7 contact tracing bluetooth experts and smartphone developers
- 15 back-end architects and developers
- 3 security experts
- 4 data protection & GPDR experts
- 4 testers (functional, security, load & performance) (tests also done by functional team)
- 5 datascientists

4.2 Launch strategy

Our system is today finishing qualification and will be in pre-production on Monday, April 20th, for French context. It needs to be customized for the context of the Netherlands and add / remove / modify the existing framework. Depending on your requirements, it can take a couple of days or a couple of weeks.

We propose to perform a regional field trial to train and optimize datascience and contact tracing algorithm. This can be performed from our pre-production environment (which is scalable to a full production environment).

For production, we recommend you select a sovereign cloud.