'WIQAYTNA', THE MOROCCAN COVID-19 EXPOSURE NOTIFICATION APPLICATION

WHITE PAPER

June 9, 2020

AUTHORS:

Mohamed Guenoun, Mohamed Benmansour, Zouheir Lakhdissi, Nasser Kettani, Youssef Dahbi

Changelog

9/6/2020:

Initial Public Release

Contact information

Website: www.wiqaytna.ma

E-mail : contact@wiqaytna.ma

GitHub repository: https://github.com/Wiqaytna-app

Contents

Introduction

In its fight against the worldwide pandemic like the one generated by the outbreak of Coronavirus-SARS-V2, known as "Covid-19", the Government of the Kingdom of Morocco sponged a multi-facets plan including but not limited to health, economics, solidarity, security, information and awareness and of course innovation. The Country gathered as ONE including government, private sector, academia, innovators, and NGOs to address the challenge.

The Kingdom used digital technologies across several of its initiatives to fight the pandemic. One of which was the development of an application, "Wiqaytna" (our prevention), to help the health experts in early detection of potential cases in their backtracking effort as well as monitoring the pandemic, and better planning for testing.

The Moroccan authorities felt it will be good practice to share its experience and technical challenges and how it was able to address them. It is also releasing the source code of the application as Open Source to the community. Other innovators and countries who want to embark on a similar journey can reuse and improve this code and learn from the Moroccan experience.

1. Context

Helping health authorities, doctors, and nurses to fight the epidemic in Morocco and save lives is paramount and the Government took every step possible to do so, including preparing hospital capacity, science, research, medical treatment, … But most importantly, the Government took important measures to slow down and stop the outbreak and spread of the virus across the country using smart and efficient early testing, by back-tracking, through medical interviews, people that have been exposed to Covid-19+ patients.

As the country prepares for lockdown easing, the Government decided to use digital technologies to help improve and streamline this early detection process. Hence, "Wiqaytna", an exposure notification mobile application will help detect potential cases exposed to Covid-19 and alert them depending on the risk identified by health authority. Its main objective is to help protect Moroccan citizens by helping the staff of the Ministry of Health to quickly find people who have been in contact with a patient confirmed positive for Covid19, test them and take health measures to save lives.

The team benchmarked the various platforms and solutions that existed at the time of the start of the project and decided to not develop Wiqaytna from scratch, but to reuse the Bluetrace protocol and some of the code that was made available by Singapore with the Opentrace project. The code was enhanced to meet the very needs and constraints of the Moroccan context, enriched with various enhancements and optimizations on the front side, and on server side including risk parameters estimation, and the Bluetooth calibration that is presented in this white paper.

2. General principle

There were 3 main principles driving the design of Wiqaytna:

1- Design a system that fits the needs of health authorities within the current level of the pandemic and provide a tool to support health authorities without changing their processes.

2- Provide a smooth experience to citizens that fits their way of living and smartphone technical constraints.

3- Respect data privacy.

The application stores anonymous Bluetooth identifiers on the phone in an encrypted format, which are exchanged with the phones of other contacts having the application as well.

Patients tested positive by the Ministry of Health are invited to upload the list of anonymous encrypted identifiers on a voluntary basis. This operation is protected by a secret code sent by the Ministry of Health to avoid accidental uploading of this information.

A back-office application allows the Ministry of Health to view the list of anonymized Bluetooth contacts with the risk parameters associated with each contact, and to notify contacts that show average to high exposure risk.

Main Technological Choices

1. Hybrid Architecture

Three architectures were proposed by different countries to handle contact tracing mechanisms. The architectures are based on what kind of data is stored, where and who handles the declaration of positive cases.

- Centralized architecture: All contacts data are stored in the mobile phone and synchronized to the backend frequently. The Ministry of Health is in charge of declaring positive cases.
- Decentralized architecture: All contacts data are stored locally in the mobile phone and never sent to a server. The patient declares the result of his tests which can be confirmed through a health authority. Positive cases IDs are sent to all mobile phones to allow them to be notified if they were in contact with a positive case during last days and weeks.
- Hybrid architecture: All contacts data are stored locally in the mobile phone. When a patient is declared Covid-19 positive, he or she is notified by the health authority and asked to share willingly his contact data by introducing a confirmation code and pushing a button in the application.

You can find below a comparison between the three architectures:

Characteristics	Centralized	Decentralized	Hybrid
Privacy	Low	High	High
User control	Low	High	High
Health Authority Involvement	High	Low	High
Phone Storage space	Very Low	High	Low
CPU and battery usage	Low	High	Low
Data usage	High	High	Low

In Morocco, four considerations were key in the choice of the Hybrid Architecture:

- The use of the application cannot be enforced, and privacy needs to be totally ensured in order to guarantee high adoption.
- The Ministry of Health is gradually increasing the capacity of tests. It is important for the ministry to prioritize the suspected cases that need to be tested depending on risk parameters of the suspected cases and on test capacity evolution.
- The majority of smartphones have low storage capacity and low CPU power.
- The application's main objective is to help the ministry of health improve their existing manual contact tracing.

2. Choice of Bluetooth Protocol

The choice of Bluetooth Low Energy (BLE) technology, was driven by two main criteria:

- The battery consumption of this technology is optimal
- Data privacy is easily taken into account, as no personal data is exchanged between devices

As a result of a benchmark study of existing Bluetooth based protocols, the project team recommended the use of the BlueTrace protocol.

This protocol that was designed to:

- enhance data privacy: by issuing crypted temporary ids valid only for a short period (15mn), to be used in the exchanges between the phones
- prepare interoperability: if the protocol is adopted by different countries and implemented in each local solution

The Open Source approach was also an important criterion for the team's choice. It allows to build on an existing base instead of starting from scratch and to benefit from future fixes and enhancements.

3. Architectural Principles

Phone devices exchange information by taking on central and peripheral roles. Peripherals advertise Services, and Centrals scan for Peripherals' advertisements

to connect to their Services which are a collection of encrypted data with a limited lifespan of less than 15 min.

Wiqaytna works as a blend of decentralized proximity data collection with a centralized notification capability. Data is uploaded to the health authorities central servers only if the app user is diagnosed COVID-19 positive.

Wiqaytna includes enhanced features at the phone application level as well as the back-end infrastructure level.

At the application level, the power consumption has been highly optimized. Test results show that the app uses less than 3% during 24 hours of activity.

Furthermore, data stored locally is compressed to optimize disk space.

At the backend level, we implemented serverless functions for high volume scalability. We also built algorithms to calculate the distance between contacts from the signal power RSSI, the frequency and the duration of the encounter.

The backend application is built with Node.JS and it is split into two sides: Mobile application back-end and Data Analytics backend.

In the mobile application backend, Serverless functions are implemented to connect the mobile application with a NoSQL Database that hosts encrypted information about the handshake devices in a JSON format. When compared to relational databases, NoSQL databases are more scalable and provide greater performance, and their data model addresses several shortcomings of the relational model. The main serverless functions that interact with the mobile application are: GenerateTempID, GetOTPCode, and Upload.

GenerateTempID is the serverless function that generates the temporary IDs that are exchanged between two phone devices during Bluetooth handshake. To protect users' privacy, these messages do not reveal users' identity. In addition, these messages do not contain static identifiers, to prevent users from being tracked over time by third parties. Each TempID comprises a UserID, created time, and expiry time encrypted. Only the health ministry holds the secret key to encrypt and decrypt TempIDs which have a short lifetime. This helps to mitigate the impact of DOS attacks. In order to ensure that devices have a supply of valid TempIDs even when the internet connection is unstable, phone devices pull batches of forward-dated TempIDs from the back-end service each time. This function has been programmed to be called up every couple of days for each phone device.

GetOTPCode is the second serverless function that is called up in the authentication process of the application. It calls a local SMS gateway that sends a verification code to the phone devices using the telecom networks to save cost and improve latency. This function is called every time a user downloads the mobile application.

Upload is the third serverless function that is used to upload the handshake messages only when a diagnosis of covid-19 is made. The handshake message is a JSON format that is represented as bellow :

{
"id": 1,
"modelC": "Redmi Note 8T",
"modelP": "SM-J810F",
"msg":
"Xf0i7ZDu6alUMQJpWgsCWISKEt7
2s96PoArDLk131+EMOVWbwEStQi
g5VUJCtUJPS5ikENe+bXy3TyFSG
w==",
"org": "MAR",
"rssi": -80,
"timestamp": 1586953969,
"v": 2
}

In the data analytics backend, we put in place an asynchronous process to perform data analytics. The semi-structured data (JSON format) is pulled from MongoDB and inserted into a column-oriented DBMS (Database Management System) for optimum data visualization usage.

4. Privacy by Design

As the team embarked on the project, they assigned a DPO and developed a DPIA (Data Protection Impact Assessment); they took a holistic approach to privacy:

1- Design the whole application with privacy in mind from the outset
2- Work with the data protection authority (CNDP) to make sure we meet the obligation of the Moroccan Law 09.08 on data privacy.

These are some of the privacy principles that were implemented:

- Download of the application is not mandated; it is on a volunteer basis.

- Clear and easy to read Privacy Policy is provided in the application in 2 languages. Additional FAQ is provided on a responsive web site to provide more transparency to users.
- Minimal PII data capture: we capture only the Phone Number of the user to then be able to alert in case the health authority needs to. These phone numbers are stored encrypted and provide anonymity as we don't cross this platform with other Telco platforms such CDRs or BTS localization.
- We capture user activity data (such as Bluetooth handshakes) and keep them on the phone. A detailed technical description of that process is provided below
- We keep the data on the phone only for the duration required by the health authorities.
- When there is a need to upload the data from the phone to the backend as decided by the health expert (when a person is tested Covid-19 positive), the user is asked to do so on a voluntary basis.
- There is no technology provided in the backend to allow to export this data (for example, in separate files, …).
- Notification of handshake contacts is done automatically by the system to avoid human access to phone numbers. In case a health specialist needs to call a contact, the platform will temporarily decrypt the phone of that contact solely.
- A clear data governance process is defined based on solid authentication; an identity management is in place to make sure that back-end users have access to only what they need, depending on their role etc …
- Limit the usage of the data only to the management of the pandemic, nothing else.
- Close up the system when health authorities declare the end of the pandemic. Data in the backend will then be 100% anonymized and kept for purpose of science and research.

Main Enhancements

1. Specific Moroccan Constraints

In the Moroccan smartphone and telecom market there are some characteristics that create challenges for a large public mobile application. These characteristics make it different from Asian, European and American markets and at the same time very close to African market constraints:

- Android have more than 90% market share
- The handsets are very diverse with more than 8 brands in the top 20 Mobile phones
- Entry level android phones dominate the market with low storage capacity and CPU power
- Low storage and tendency to uninstall big applications in order to free space is very common
- Data bandwidth in some areas is slow and access to data is not permanent for some users (some users deactivate data in order to save cost) and some users rely on Wi-Fi access
- Mobile phones time and date are not commonly synchronized with network or Internet

These specific constraints created some key challenges in developing the Wiqaytna applications and led us to different optimizations to the Bluetrace protocol and design of the application.

2. Main Optimizations performed

In order to make the application compatible with the maximum number of devices in Morocco different optimizations were conducted.

- Optimizing the size of the application for Android: The challenge was to have an application in the store with a size lower than 5 Mo to reduce download time and increase installation.
- Optimizing battery usage to the minimum (less than 3% of battery time) by reducing CPU usage and number of connections to the backend
- Optimizing data usage by reducing overheads in exchanges with the backend server and frequencies of updates.

- Allowing tracing even if a user phone is not connected to the internet for a long period by increasing the number of TempId downloaded in a single call.
- Allowing the tracing even if the system time is not synchronized with the network by allowing the first TempId to be valid even for few hours before the current server time
- Adapting the application and fine tuning it to more than 100 devices that were tested during the test phases

Some other optimizations are still being tested and will be implemented in the next updates depending on the feedback after the launch of the application.

3. Bluetooth Challenges

The Bluetooth protocol was initially designed for simple use cases, such as connection to audio devices, or for the exchange of photos between 2 devices for example.

The use of a Bluetooth protocol in the context of applications similar to Wiqaytna revealed a number of technical challenges to which we have tried to provide solutions and workarounds.

3.1 Background mode

Apart from the case of the iPhones which was already identified in the whitepaper of OpenTrace, we noted that certain manufacturers of Android smartphones have adapted their OS for a more important optimization of the battery and deactivate several functionalities for the applications which are in background, including Bluetooth.

Work with the various manufacturers, and the feedback obtained is being integrated into a personalized Wiqaytna onboarding screens for certain models to indicate to the end user certain settings to be made manually.

3.2 Difficulty estimating distances

The calibration data published in particular by Singapore is not sufficient in the case of Morocco.

Indeed, each model of each manufacturer has a particular behavior linked in particular to the parameter Txpower (Transmission power), to the Bluetooth chip and to the antenna which is mounted on this model.

4. Exposure risk parameters estimation approach

A person carrying the Covid 19 Virus is considered contagious:

- 2 days before the onset of symptoms
- or 2 days before the test date for asymptomatic carriers

The parameters defined by the Ministry of Health to assess the risk of exposure to the Covid-19 virus are as follows:

- **Distance between the carrier of the virus and the exposed persons:** the closer the distance, the higher the risk. The risk is maximum below 1m.
- **Duration of meetings:** the longer the duration, the greater the risk
- **Frequency of meetings:** the higher the number of meetings between the carrier and an exposed person, the greater the risk of contagion.

Initially, the selection process will be based on these parameters by providing the Ministry of Health with simple filters that allow targeting of people at risk who must be notified and then taken care of.

The evaluation of these various parameters is based on data from Bluetooth handshakes recorded on the phone of the carrier of the Covid19 virus and uploaded to the server. Each handshake collected contains standard information defined in the Bluetrace protocol, as shown in the following example:

{
"id": 1,
"modelC": "Redmi Note 8T",
"modelP": "SM-J810F",
"msg":
"Xf0i7ZDu6alUMQJpWgsCWISKEt7
2s96PoArDLk131+EMOVWbwEStQi
g5VUJCtUJPS5ikENe+bXy3TyFSG
w==",
"org": "MAR",
"rssi": -80,
"timestamp": 1586953969,
"v": 2
}

4.1 Reconstitution of meetings from handshakes

An algorithm has been designed to infer the notion of meeting from unitary handshakes.

Each meeting includes a set of successive Handshakes. The algorithm is based on the notion of a window without Bluetooth exchange between the phone of the virus carrier and that of the contact. We were able to observe that in Foreground mode exchanges are frequent, of the order of a minute.

This period between 2 handshakes is influenced by several parameters:

- Period between 2 scans: this parameter is set to 40s
- Blacklist validity period: This parameter is intended to avoid scanning the same phone every time if it is nearby. It is positioned at 100s In Background mode

4.2 Estimated duration and frequency

The notion of meeting which was introduced in 4.1 simplifies the estimation of these 2 parameters.

So, the frequency is simply equal to the number of meetings that have been reconstructed.

For each encounter, the duration is calculated by the difference between the timestamp of the last Handshake and that of the first Handshake.

In the case of meetings with a single Handshake, the duration is positioned with the value of the period between two scans which is 40s.

The filters used to select those at risk are based, among other things, on the minimum duration, the maximum duration and the average duration of meetings between 2 people.

4.3 Estimated distances:

The relevant information for the estimation of the distance is the field "RSSI 'or" Received Signal Strenth Indicator "which gives the signal strength received by the phone which performs the scan.

We started by adopting and implementing a distance calculation formula widely used in literature, which is presented as follows:

$d = A * (r / t) ^ B + C$

Where r is the value of the RSSI read, and t is the Txpower (Transmission Power) specific to the telephone model, and where A, B and C are constants specific to each model which must be determined by linear regression from the measurements which must be done outdoors, in a space free of any obstacle within a radius of 50m, for different distances: 0.25, 0.5, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 , 14, 16, 18, 20, 25, 30.

We quickly abandoned this approach following the first results which showed that the value of the distance obtained is very approximate compared to reality. Indeed, this measurement varies significantly depending on several factors including the phone model, knowing that each manufacturer for each of its models can choose different Bluetooth chips and antennas that make the behavior of this particular model different from other models from the same manufacturer and also from other manufacturers.

So, we decided to opt instead for distance ranges based on a calibration of rssi thresholds for each of the most used phone models in Morocco. For non-calibrated models, we have provided default thresholds.

The procedure and the results of the Bluetooth calibration tests are described in Chapter 4.

The distance ranges used are as follows:

- Very close (0-1m)
- Close (1-2m)
- Far (Beyond 2m)

An Ad hoc configuration has been implemented at the Backend level, as well as a matching process for the value of the rssi for each handshake with the thresholds configured for the model in question.

The distance range that is chosen for a meeting is the smallest among the handshakes available in this meeting.

Testing approach

In order to assure application's utility and compatibility with most Android versions, and phone operating systems, a series of tests and trials were conducted:

- Functional tests and quality assurance
- Cross-device tests
- Bluetooth tests with different methodologies, emulating real-life scenarios.
- Security tests to assure privacy and application's immunity to known exploits.
- large-scale tests with more than 1000 volunteers.

The main aims of these trials are:

- Making mobile app compatible with most used phones and operating systems in Morocco.
- concluding a distance estimation model through low energy Bluetooth recorded RSSI values taking into consideration different factors that affect its propagation.
- guaranteeing a consistent interface between phone models.
- Pentesting application's security to exploits that might affect user privacy, mainly replay attacks.
- Experimenting how environmental factors such as phone orientation, physical, and interference with other signals (WIFI and GSM features) might affect RSSI values.

1. Cross-device tests

Due to the diversity of mobile devices and platforms, compatibility testing for mobile apps has been identified as one urgent and challenging issue.

The main objective of compatibility testing was to validate whether the mobile application can be installed and run on different mobile devices and environments, and whether it is compatible with expected mobile platforms, device features and native APIs, etc."

In fact, due to differences in API, scheduling and operation mechanism of mobile platforms, some faults/bugs could appear when application install or run on some special mobile platforms. In particular, open-source android platform may be

customized and modified by some manufacturers of mobile device, which will result in serious android fragmentation problems.

Another objective is to test device hardware compatibility, in fact mobile devices have many hardware components (CPU, RAM, Screen, Bluetooth, etc). Each has some different feature values, for examples, there are different screen sizes, such as: 5.5 inches, 5 inches, 4.5 inches, 4 inches, etc. The difference of hardware features may lead to compatibility problems of mobile application.

For example, some mobiles may have layout and display faults due to different screen sizes and resolutions.

The cross-devices tests were applied to a fleet of more than 140 phones, targeting most used phone models taking into consideration variation in operating systems, phone models, and manufacturer-specific implementations.

To make sure that the mobile App will run smoothly on different devices, an analysis of the market allowed us to draw up a list of the most used devices in Morocco.

A series of functional tests were conducted to test the application on those most used phones, some fixes and improvements were applied to make the application compatible.

2. Large-scale Trial

To effectively test the reliability and performance of the application, a large-scale trial was conducted with the help and support of OCP Group, a national mining company (A world leader in the phosphate industry and the world's first producer of phosphate-based fertilizers)

The main objectives were as follows:

- To observe app performance and stability in different settings;
- To compare the effectiveness of our interpreted data with real contact-tracing procedures.
- To validate how our implementation was used by actual users and identify potential areas for improvement.

2.1 Outline of the entire Trial

Identify areas of interest

Prior to the trial, we did a survey on the location in which the trial would be conducted. We identified areas where participants would typically congregate during the course of their daily routines.

Also we tried to mix between indoor and outdoor environments to test several factors that impact the Bluetooth tracking (Multipath fading, Environmental factors such as surface textures, geometry, and physical layout, Phone placement on a person, e.g. in a hand, in a pocket, Device-specific characteristics such as chipset, antenna layout, and OS configurations).

All these factors introduce random noise in estimates of distance.

➔ 3 main areas were identified:

- Company Headquarters (indoor Office Trial)
- JORF LASFAR Industrial Platform (Indoor & Outdoor)
- Mining site in KHOURIBGA (outdoor & indoor)

Design data collection procedure for the Ground Truth

As we did not want to interfere with participant's routine, we had to come up with a way of knowing the Ground Truth without having the participants perform deliberate movements. We identified some volunteers who's in addition of installing and using permanently the app during the test, were given explicit instructions to fill some activity log sheets tracking all their interactions and movements when entering the various areas of interest.

We also realized that some participants may forget to clock their timings and fill the activity log sheet. So, we made a prominent sign to remind them to do so, and periodically sent out reminders via a WhatsApp group chat.

Conduct trial

A briefing to all participants was given before commencing. During the briefing, participants were shown how to install and use the app (Download through QR code or links provided in different communication supports). The trial app was also deployed in company's internal store for all enrolled phones.

Participants had to fill and submit a volunteering form to note their phone number and device model. They were also given explicit instructions to make sure the app is running, and Bluetooth is enabled all the time.

During the course of the trial, we found that some participants had difficulty using the app properly. This is referring to some Android OEMs aggressively suppressing the performance of the app when running in the background, and at times may even kill the service or throttle the Bluetooth hardware (Huawei, Infinix,...).

Establish Ground Truth data from trial

After the trial, we identified a few volunteers as our "infected" cases and asked them to upload their encounter history through a PIN code sent by SMS.

After a tremendous work of consolidation of different activity log sheets provided by volunteers, we started comparing the contacts logged in participant's device against contacts specified in those activity log sheets.

During our analysis, we found that participants interacted with people who were not part of the trial. Effort was required to clean up our contact-tracing data to only include participants, as well as remove other qualitative data irrelevant to the trial.

2.2 Trial Conclusions

The main conclusion of this pilot phase is Bluetooth limitation to assess distances between devices, nevertheless, we could approximate the distance between devices from the radio signal strength intensity RSSI. In this large-scale trial, we found that RSSI values at the same positions vary from device to device and that same RSSI *values can be recorded at different positions.*

To resolve this issue of non-bijection, a series of trial were conducted later to determine the thresholds of each distance interval for most used mobile phones in Morocco.

3. Calibration Tests

Moroccan authorities have come up with some guidelines to determine if someone has been a close contact of a patient – there were 3 defined distance intervals 0-1m, 1-2m and 2-10m each interval will be weighted in the risk scoring algorithm.

As explained earlier, Bluetooth technology was not designed to assess distances between devices, nevertheless, we could approximate the distance between devices from the radio signal strength intensity RSSI.

To resolve the issue of non-bijection, a series of tests were conducted to determine the thresholds of each distance interval.

The main objectives in this trial were the following:

- To test connectivity between various devices over a length of time. In a real-world scenario where there can be many devices near each other (e.g. a crowded train), any device should be able to pick up other surrounding devices within a reasonable time.
- To test for consistency and stability of the app implementation over a length of time. Assuming that devices do not move around, the pairwise RSSI readings should be of a consistent range without much fluctuation.

Acknowledgments

'Wiqaytna' is a national project that brought together a team of Moroccan talents from a variety of backgrounds. Companies involved in this project, have contributed voluntarily.

GOVERNMENTAL DEPARTMENTS

وزارة الصحة
Ministère de la Santé

Royaume du Maroc
Ministère de l'Intérieur

المملكة المغربية
وزارة الداخلية

NATIONAL AGENCIES

#ADD
Agence de Développement du Digital

anrt
agence nationale de réglementation des télécommunications
الوكالة الوطنية لتقنين المواصلات

CONTRIBUTORS

OCP

MEDTECH GROUP

berkeleysystems

dialTechnologies

OMNIDATA

OMNISHORE

1337

VALYANS CONSULTING

abweb

AIOX LABS
AI AS A SERVICE

HIDDEN CLOUDERS

Publikart
Conseil Médias & Relations Presse