ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-MOPV010

WORKING UNDER PANDEMIC CONDITIONS: CONTACT TRACING MEETS TECHNOLOGY

E. Blanco Viñuela*, T. Previero, E. Matli, B. Copy, S. Danzeca,
R. Sierra, R. Losito, Ch. Delamare, A. Masi
CERN, Geneva, Switzerland

Abstract

COVID-19 has dramatically transformed our working practices with a big change to a teleworking model for many people. There are however many essential activities requiring personnel on site. In order to minimise the risks for its personnel CERN decided to take every measure possible, including internal contact tracing by the CERN medical service. They performed manual procedures which relied on people's ability to remember past encounters. To improve this situation and minimise the number of employees who would need to be quarantined, CERN approved the design of a specific device: the Proximeter. The project goal was to design a wearable device, built in a partnership with industry (*Terabee* and CERN), fulfilling the contact tracing needs of the CERN medical service. The proximeter records other devices in close proximity and reports the encounters to a cloud-based system. The service came to operation early 2021 and more than 8000 devices were distributed to CERN members of personnel. This publication reports on the service offered, with emphasis on the overall workflow of the project under exceptional conditions and the implications data privacy imposed on the design of the software application.

INTRODUCTION

COVID-19 has dramatically modified working conditions hence affected largely to global economies and enterprise businesses. However, during the pandemic situation essential activities still required personnel on site. In order to keep production stability but ensuring workers safety there was an increased focus on finding solutions to comply with COVID-19 social distancing recommendations [1].

Initially, most of CERN activities adapted and were executed remotely (teleworking), but still some critical activities required work on site. The Health, Safety and Environmental (HSE) unit at CERN introduced a series of measures following the recommendations issued by the Host States. Social distancing and contact tracing have been some of the measures implemented. Contact tracing is defined as the capability of identifying persons who have been in the vicinity of an infected person so their isolation would avoid the spread of the virus. This tracing process was manually conducted by the medical service and required a large effort to keep up with the rate of infection. The process was mostly relying on memories of the infected individuals who should remember with whom they may be in close contact hence does not guarantee perfect traceability.

Two main challenges appeared: (1) help individuals in keeping a **social distance** and (2) timely **identify individuals** who were in close contact with an infected person, the so-called contact tracing.

To tackle the mentioned challenges CERN approved the design of a specific device: the proximeter. The overall project goal was to design a wearable device able to record other devices in close proximity. Additionally an application provides only the close contacts under the request of the medical service.

This publication reports on the service offered, with emphasis on the overall workflow of the project under exceptional conditions and the implications data privacy imposed on the design of the overall service.

THE PROXIMETER

First of all, the definition of two essential terms representing key events widely used during this publication is introduced here: **encounter** as the event of two individuals being within 2 meters distance for more than 30 seconds and **close contact** as the event of an encounter lasting more than 15 minutes which must be traced if required by the medical service.

The device was created with two main objectives: (1) **warning**: so the users are warned once they are not keeping the expected social distancing (2) **contact tracing**: timely provide potential close contacts in case of a positive appears.

Several similar devices with these characteristics were available on the market, but none presenting at the same time the desired precision, scalability to 10000 and more devices, timely data availability and more importantly adaptability in order to protect the sensible data collected at all moments of use and transfer. CERN decided then to issue a competitive tender with those specific requirements.

The company that was awarded the contract, *Terabee* [2], adapted one of its products, the *Terabee mobile robotics positioning system*, to comply with the specifications. In particular, for the connection to the CERN infrastructure *Terabee* implemented the CERN's *miniIoT* (Internet of Things) technology, under licence from CERN, while using its own technology for the encounters tracking based on the accurate Ultra Wide Band (UWB) radiofrequency.

Then, *Terabee* engineered a device that CERN called the **proximeter** (Fig. 1) which become a commercialised wearable product in *Terabee*'s portfolio [3].

* Enrique.Blanco@cern.ch

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-MOPV010

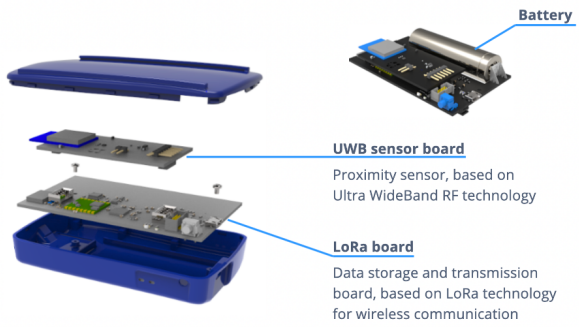

Figure 1: The proximeter device.

Some of the key requirements of the product and the solutions provided are shown in Table 1.

Table 1: Main Requirements and Solutions Given

Requirements	Solutions
Precise detection	UWB technology
Warning features	Buzzer and visual LEDs
Easy to use	Wearable device
Autonomy	Large capacity battery
Encounters accessibility	IoT networking: LoRaWAN®
Privacy	Encryption and no geotagging

The proximeter only knows where it is with respect to other proximeters. It does, however, know that specific information to an accuracy far better than that of mobile-phone-based apps, which makes it very good at telling its holders when they are getting too close, while keeping their whereabouts confidential.

The proximeter device [4] is a twofold design (Fig. 1): it is composed of a mainboard and a sensor-board. The sensor-board hosts a Ultra Wide Band (UWB) sensor. The sensor-board communicates with the mainboard via an SPI bus, that is shared with the LoRa® transceiver. The board is powered by a rechargeable Li-Ion battery rated at 3350mAh. The device also provides a red LED, which is used to assess the charging state, an RGB status LED, and a vibrator motor, which warns the user in case of an encounter is detected.

When the device is powered on, it joins the LoRaWAN® network and sends encounters that were not transmitted, if present. At the end of each encounter, the recorded information is saved in a flash memory and is used to compose the LoRaWAN® packets to be transmitted. Every 15 minutes, the device checks the encounters that have not yet been sent and empties the queue via LoRaWAN®. The communication between the device and the LoRaWAN® network is encrypted via AES-128.

THE IoT INFRASTRUCTURE

As already introduced the device uses LoRaWAN® to exchange the encounters. The LoRaWAN® specification [5] is a Low Power, Wide Area (LPWA) networking protocol designed to wirelessly connect battery operated 'things' to local or global networks, and targets key Internet of Things (IoT) requirements.

LoRaWAN® is the default IoT protocol for CERN [6] and it has been used in other projects in the last years. The choice of the proximeter for using this network was made in base of the experience already acquired with other devices, the existence of the *miniIoT* platform developed at CERN and the important requirements of coverage, power consumption and confidentiality. The network offers extremely **long-range data** links which allows to exchange data all around the campus (around 60 km2) with minimal deployment. The proximeters are battery-powered and LoRa has a reduction in **power consumption** by a factor of 10 compared to Wi-Fi. LoRaWAN® parameters are only known by the LoRaWAN® network administrators, not even the owner of the device knows them, and all communications are **encrypted** from the device up to the application.

The CERN IT department offers the infrastructure of the network together with a complete architecture which allows to host the device transmitted data.

THE SERVICE

CERN imposed the use of the proximeters as part of the efforts to respond to the challenges posed by COVID-19. To date, more than 8000 people received the wearable device with a goal to minimize potentially harmful encounters and provide contact tracing information in case of need.

Setting up such global service was a non trivial task as the service must take care of different aspects as distribution, asset management, support, data collection and, finally, provide the relevant close contacts to the medical service. All these must be done under strong requirements on personnel safety and privacy. To succeed in this task a diverse team of people in different technical and organisational fields was assembled.

Distribution

Distributing such amount of devices as fast as possible during the pandemic situation constituted the first challenge. Put in practice this demand required a fast and organised distribution mechanism which guaranteed the users safety as crowds had to be avoided.

A dedicated web-based appointment mechanism was set up. Users could reserve a slot to pick up their proximeters at their convenience (location and time). This ensured the safety for the team delivering the devices and the users themselves.

The response of the CERN personnel collecting the devices was extremely good (Fig. 2) considering that the majority of them were teleworking from their homes. This mechanism gave additional trust which indeed allowed a general recall campaign to deal with the release of a newer firmware version (mid February 2021) improving safety features deployed on the first firmware version. The distribution started with a pilot of 950 devices in December 2020 which

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-MOPV010

confirmed their effectiveness, successfully reporting violations of the two-metre rule with an accuracy of up to 90%. The full scale roll out officially started early 2021 and the use of the proximeter became mandatory from 1st of March 2021 when the number of 5000 devices distributed was successfully reached.

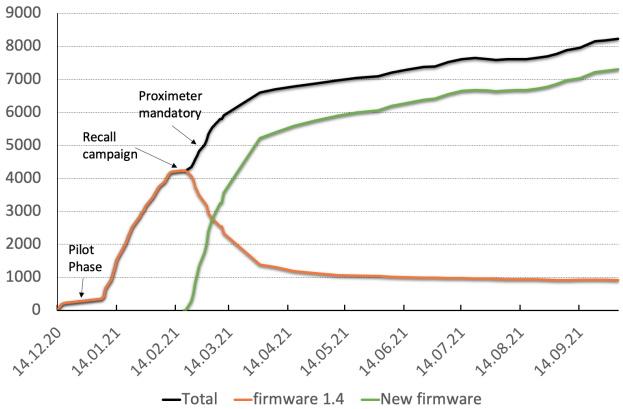

Figure 2: Distribution of the proximeters.

The distribution of the devices was executed by the registration service initially in different sites (e.g. experimental areas, restaurants...) and then centralised in a single location. Additional staff was required to deliver such amount of devices in parallel.

Asset Management

This activity started with the procurement of the devices themselves which were configured with the required encounter parameters (distance: 2 meters and time: 30 seconds) at the factory (*Terabee*). The CERN procurement and supply chain teams worked together to handle the equipment providing them to the distribution point.

All the devices were registered in the computerised maintenance system available at CERN: *InforEAM*®. This allowed proper asset management to cope with the administration of spares and to handle the dysfunctional or lost devices while also playing an essential role on the data protection as will be explained later. The support of this activity was done by the asset and maintenance management team.

Proximeters Support

The success of the project resided on the adoption of the wearable device by the users.

The device is not complex to use as it only requires to switch it on. However users need, both, to understand the different status modes and, more importantly, what and how the personal data shared is exploited. To cope with the first need, a complete user manual was created, distributed with the device and also made available online. To respond to the second need, a comprehensive online training course was created on the learning hub at CERN. This became essential in explaining the goals of the project and showing the kind of data collected together with their potential use by the medical service providing total transparency on personal data use. Moreover the information about the proximeter project was regularly reported to the CERN personnel.

The support of the users was made by a team of experts on different domains (e.g. electronics, software, architecture, data protection...). All support was centralised in the CERN ticketing support service: *ServiceNow*® where a functional element was created to provide the CERN-wide support for the proximeter device. Diverse technical teams were involved in this support. The proximeter functional element provided a central point of support with links to a comprehensive set of the project information, online courses, frequently asked questions, manuals and the privacy notice.

During the current year (project activity) and until mid-September, there have been 216 incident requests and 131 general requests. These figures are considered to be low with respect to the number of deployed proximeters and they corroborate the quality and the ability of the device to be operational.

Data Collection

The proximeter stores the encounters locally with the following data (see example of Table 2): Peer device (*RefTag ID*), own device (*myTag ID*) starting time of the encounter (*Date*) and duration (*NUM*). The last representing the total number of 30 seconds slots of the whole duration of the encounter. Data is regularly sent via the LoRaWAN® network and then stored in a database as records.

Table 2: Data Records Transmitted and Archived

RefTag ID	myTag ID	NUM	Date
24500	12893	32	01-MAR-21 10:26:00
22382	12893	3	01-MAR-21 10:51:00
53019	12893	7	01-MAR-21 10:58:00

The data is kept for a maximum of 14 days which is the time window when the tracing of close contacts may be of interest, then it is deleted. The IDs serve to identify the proximeter involved in the encounter. By design, the proximeters can not register the *geolocation* of the devices, so user's whereabouts remain confidential.

Tracing Exercise

The ultimate phase is the ability of the medical service to trace people in close contact with a tested positive case or a person showing disease symptoms. The medical service is the only service allowed to perform this activity.

A complete software suite, the *proximeter portal* was designed. It allowed the medical service to query the records with the name of a person and to get back the close contacts list. This software suite represents the core of the service as it provides not only this feature but also handles the distribution and management of the devices by the registration service. Figure 3 shows the functionality given when tracing people. The example shows the identification of a close contact with

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-MOPV010

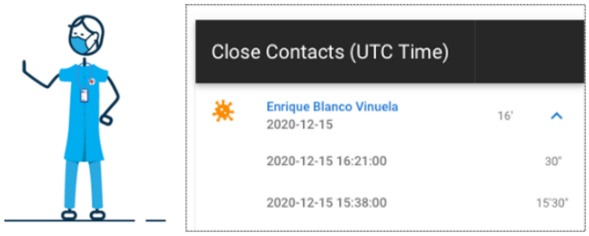

Figure 3: Close contacts from a contact tracing request.

two encounters of 30 seconds and 15 minutes and 30 seconds respectively.

The software suite will be technically introduced later but its functionality appears along this publication in many aspects: e.g. distribution, data privacy, and user interface allowing CERN personnel to consult their own generated data.

THE DATA PRIVACY

CERN collects and uses **Personal Data** related to people who interact with the organisation in carrying out the mission. CERN is committed to respecting the security and confidentiality of the Personal Data for which it is responsible, in accordance with its Data Privacy Protection Policy[1]. CERN processes only such Personal Data as is required for the proper functioning of the Organization. A privacy notice for the proximeter device was created.

Data privacy has been the central concern on the proximeter project, therefore the design of the service including the tools, architecture and the software providing the main functionalities (i.e. assignation, asset management and tracing) have followed strong principles to protect the users privacy.

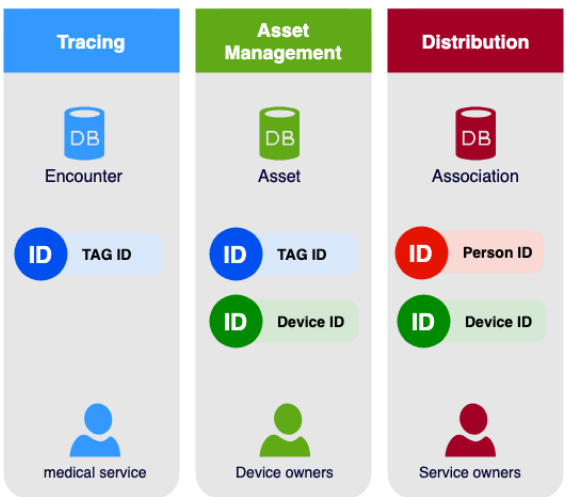

Figure 4: Global architecture based on scattered databases.

Three distinct databases were designed and deployed for that purpose: (1) Encounter, (2) Asset and (3) Association. Figure 4 shows the databases, the team having access and their main function. Access to the databases is only granted to specific teams with a clear purpose: e.g. medical service only has access to the Encounter DB, device owners only has access to the Asset DB and the registration service only has access to the Association DB.

An access to an individual database is not enough to relate the identity of a person and his/hers assigned proximeter guaranteeing anonymity. Also it shows the main identifiers (IDs) allowing a data pseudonymization which permits the data records be less identifiable while remaining suitable for the traceability (Table 3).

Table 3: Data Pseudonymization with Identifiers (IDs)

ID	Function
Person ID	CERN person identification number
Device ID	Proximeter visible identification number
TAG ID	Proximeter internal identification number

The CERN office of data protection (ODP) played a central role in the validation of the choices made. It particularly advised about the final solution providing users with the ability to consult their personal data kept at all times. To comply with this requirement the software suite added a new functionality called *self-service* to allow people to see their encounters. Obviously the data provided to the users listed the encounters of the person without the identification of the peers to ensure their anonymity.

Another aspect which was also looked at carefully was the security. The software suite together with the infrastructure was provided to the IT security team who run a complete audit to identify the robustness of the solution with respect to any possible data leak.

THE PROXIMETER PORTAL

The design of the software application was driven by the requirements of the contact tracing but also with the idea of minimising resources by employing services already provided by CERN. The data scattered in different databases imposed several constraints on the design of the software increasing the complexity and making difficult the diagnostics in case of any technical issue. A second concern was to make a software suite in the shortest possible period of time to provide the application to the medical service as soon as possible.

The software suite ensures functionality to manage the proximeters by the registration service: i.e. assignment, lost&found and relinquish (REGISTRATION, STATUS and FOUND), the self-service (MY DATA) allowing all users to consult the personal data retained (encounters) and the tracing (TRACKING) of close contacts for the use of the medical service (Fig. 5).

The portal application is based on web technologies and split in a front-end and a back-end. The web application back-end is based on *Java™ 11*, *Maven*™ and *Spring®*

[1] The Processing of Personal Data at CERN (OC11)

ISBN: 978-3-95450-221-9 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2021-MOPV010

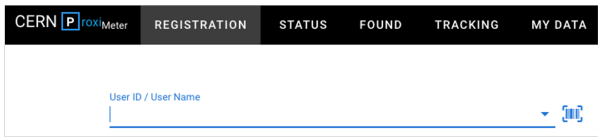

Figure 5: Proximeter portal main interface.

Boot and exposes data via a REST APIs and serves the static files of the front-end, built with *Vue.js*.

The code is hosted on CERN's *GitLab* and the build of the project, the publishing of the artifacts and the actual deploy of the application is managed through *GitLab's* pipelines. The final artifact resulting from the build process is a Docker image containing the layered *fat JAR* representing the application which is pushed to the project's *GitLab* Container Registry. The image is then deployed on CERN's PaaS (Platform as a Service - *OpenShift®*). The project is completed with metrics collection (*Prometheus*) and visualization (*Grafana*).

In order to provide the web application functionalities, many already existing CERN's resources has been leveraged. CERN's SSO (*Keycloak*) together with its integration with e-groups granted us the possibility to create group of users and give them different roles.

THE STATISTICS

The proximeter portal has been used since early 2021. The distribution of the proximeters reached a notable number of 5000 right before being mandatory at CERN and passed 8000 in September 2021. The only available figure of their real use is the number of those which produce encounters, otherwise the number of proximeters in use is unknown as we intentionally do not check on the proximeters when they connect to the network at their arrival at CERN.

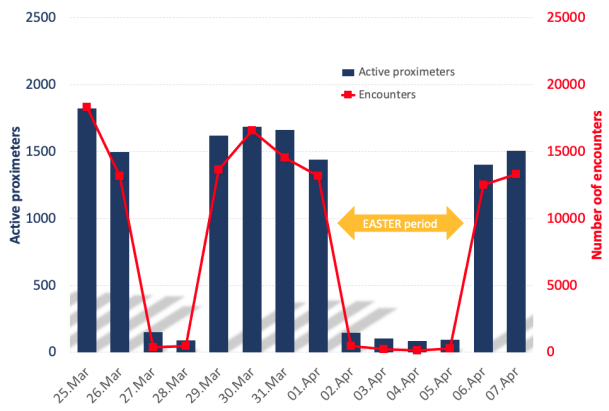

Figure 6: Active proximeters and number of encounters (per day).

During the initial period of the proximeter use (March 2021), the number of unique active proximeters was about 2000 and the number of encounters per working day was approximately of 14500 as average (Fig. 6), note the Easter holidays and week-ends with far fewer encounters. The number of close contacts (encounters with more than 15 minutes) was estimated of approximately 550 per day in average. Note the period shown had a high rate of personnel working from home (teleworking) so a limited number of CERN personnel working on site.

During 2021 the number of positive cases was up to 17 per week (5 per week in average), but the medical service checked on possible close contacts of personnel with compatible disease symptoms. As a reference, in the last weeks of September, the medical service executed approximately 10 extractions per week to find close contacts.

CONCLUSION

CERN invested in performing a rigorous contact tracing as a way to break the chain of infection. The key factor relied on improving the manual tracing executed by the medical service and provided an **immediate report** of close contacts for the medical service. This would minimise the number of employees who would need to be quarantined. The proximeter service revealed itself essential to allow a more precise contact tracing.

The success of this project, allowed by a notable internal cooperation among diverse teams at CERN, was not only based on the device itself but also on providing a service permitting the medical service to fulfil its needs of tracing. The service came to operation early 2021 and more than 8000 devices were distributed to CERN members of personnel who received the device as a protection measure while respecting the personnel privacy.

The software suite handling the proximeters and enabling the contact tracing was designed and engineered reusing all possible resources already available, therefore minimising cost and impact of CERN infrastructure and resources and, always, with the main concern of data privacy. This project indeed reflects well the concept of **privacy by design**.

REFERENCES

[1] WHO, "Contact tracing in the context of COVID-19," in *COVID-19: Surveillance, case investigation and epidemiological protocols*, 2021, https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19

[2] Terabee, https://www.terabee.com

[3] Terabee Proximeter, https://www.terabee.com/shop/covid-products/terabee-proximeter/

[4] C. Merscher, R. Sierra, A. Zimmaro, M. Giordano, and S. Danzeca, "Proximeter CERN detecting device for personnel," in *25th International Conference on Computing in High Energy and Nuclear Physics (CHEP 2021)*, 2021, doi:10.1051/epjconf/202125104025

[5] LoRaWAN® Specification, https://lora-alliance.org/about-lorawan/

[6] R. Sierra and H. Odziemczyk, "Readying CERN for connected device era," in *24th International Conference on Computing in High Energy and Nuclear Physics (CHEP 2019)*, 2020, doi:10.1051/epjconf/202024507015