This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 832981

Deliverable D4.3

Developed Modular App for Practitioners

Due date of deliverable: 31/08/2023

Actual submission date: 31/08/2023

George Kolev[1], Garik Markarian[1], Nataly Polushkina[1]

Laura Petersen[2], Grigore Havârneanu[2]

1: RINISOFT 2: UIC

The document reflects only the author's views and the Commission will not be liable of any use that may be made of the information contained therein. The use of the content provided is at the sole risk of the user.

Project details

Project acronym	PROACTIVE
Project full title	**PR**eparedness against CBRNE threats through c**O**mmon **A**pproaches between security pra**CTI**tioners and the **V**uleranbl**E** civil society
Grant Agreement no.	832981
Call ID and Topic	H2020-SU-SEC-2018, Topic SU-FCT01-2018
Project Timeframe	01/05/2019 – 31/08/2023
Duration	52 Months
Coordinator	UIC – Grigore Havarneanu (havarneanu@uic.org)

Document details

Title	Developed Modular App for Practitioners
Work Package	WP4
Date of the document	31/08/2023
Version of the document	06
Responsible Partner	RINISOFT
Reviewing Partner	ETICAS, CBRNE, UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	01/07/2023	First Draft
02	16/07/2023	Second Draft
03	24/07/2023	Third Draft
04	01/08/2023	Fourth Draft
05	30/08/2023	Final Draft
06	31/08/2023	Final Version

Consortium – List of partners

Partner no.	Short name	Name	Country
1	UIC	UNION INTERNATIONALE DES CHEMINS DE FER (COORDINATOR)	France
2	CBRNE	CBRNE LTD	UK
3	PPI	POPULATION PROTECTION INSTITUTE (MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC)	Czech Republic
4	DB	DEUTSCHE BAHN AG	Germany
6	UMU	UMEA UNIVERSITET	Sweden
7	DHPOL	DEUTSCHE HOCHSCHULE DER POLIZEI	Germany
8	RINISOFT	RINISOFT LTD	Bulgaria
9	WMP	WEST MIDLANDS POLICE AND CRIME COMMISSIONER	UK
10	ETICAS	ETICAS RESEARCH AND CONSULTING SL	Spain
11	SESU	STATE EMERGENCY SERVICE OF UKRAINE	Ukraine
12	UKHSA	UK HEALTH SECURITY AGENCY (DEPARTMENT OF HEALTH – PUBLIC HEALTH ENGLAND)	UK
13	SPL	STATE POLICE OF LATVIA	Latvia
14	AGS	AN GARDA SÍOCHÁNA – NATIONAL POLICE FORCE IRELAND	Ireland
15	FFI	FORSVARETS FORSKNINGSINSTITUTT	Norway
16	NPH	KOMENDA GŁÓWNA POLICJI	Poland

Executive summary

The purpose of this deliverable (D4.3) is to provide detailed description of the co-creation, testing and verification process used throughout the project to develop the PROACTIVE mobile App for Practitioners. The PROACTIVE mobile App is one of the three components of the PROACTIVE Crisis communication system that aims to facilitate communication between practitioners and citizens both before and during a CBRNe incident. The other two components of the system are the collaborative web platform (described in D4.2) and the mobile App for vulnerable citizens (D5.4).

The development focused on ensuring that all the requirements, as defined in PROACTIVE policymaking toolkits, were met. This involved facilitating Law Enforcement Agencies (LEAs) and Security Policy Makers ability to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The developed mobile App helps to improve the efficiency of the communication between LEAs, Policy Makers and Citizens, with a particular focus on information sharing and usability by vulnerable groups (T5.4). The technology, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by mobile technologies, as well as modern data analytics capabilities to support users in overall decision-making processes. The provision of ‘other applications’ (such as Twitter, Facebook) has also been implemented, covering potentially any application outside of the PROACTIVE system, which may interact by pushing/pulling information to or from the PROACTIVE system.

Input from WP1, WP2, WP3, WP5 and WP8 has been reviewed to determine the needs and gaps of the users in terms of current public perceptions relating to Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) incidents. The research completed in WP1 fed into the key engagement tasks in WP2 and WP3, and by default provided key feedback for the Toolkits in WP4 and WP5. The work and deliverables completed in WP4 were utilised during the exercises in WP6. Feedbacks received from 3 PROACTIVE exercises helped to improve the developed mobile App, while inputs from WP8 and WP10 were utilised for evaluation of ethical and legal compliances. In addition, even though this was beyond the original scope of the PROACTIVE project, special emphases were made to ensure compliance with “Secure by Design” requirements.

The developed mobile App will remain active and usable for forceable future after the completion of the project. RINISOFT will continue maintenance of the developed software, ensuring that the whole PROACTIVE Crisis Communication System (both the web platform and apps) are still available on relevant third party servers and can support communication between practitioners and citizens beyond the life of the project.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Server
CBRNe	Chemical Biological, Radiological, Nuclear, explosive
CSAB	Civil Society Advisory Board
D	Deliverable
DSDM	Dynamic Systems Development Method
FR	First Responders
GDPR	General Data Protection Regulation
GIS	Geographic Information System mapping
GUI	Graphic User Interface
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol Address
IPR	Intellectual Property Rights
LEAs	Law Enforcement Agencies
MA	Mobile App
MoSCoW	Must have, Should have, Could have, and Won't have
MVC	Model-View-Controller
MVP	Model-View-Presenter
MVVM	Model-View-ViewModel
PSAB	Practitioner Stakeholder Advisory Board
QA	Quality Assurance
REST	Representational State Transfer
SOP	Standard Operating Procedure
SQL	Structure Query Language
TLS	Transport Layer Security
UAT	User Acceptance Testing
WP	Work Package

1. INTRODUCTION

1.1. Project Summary

In line with the EU Action Plan to enhance preparedness against Chemical, Biological, Radiological Nuclear and explosive (CBRNe) security risks and the overall Security Union approach to fight crime and terrorism, PROACTIVE aimed to enhance societal CBRNe preparedness by increasing Practitioner effectiveness in communicating and managing large, diverse groups of people in a CBRNe environment.

This was achieved by delivering new PROACTIVE tools and providing innovative recommendations for Policy Makers and Safety and Security Practitioners. Liaising with the eNOTICE H2020 project, three joint exercises were conducted with special emphases on roles play by volunteers recruited by PROACTIVE and evaluation of the developed tools. These exercises helped to evaluate the acceptability and usability of existing procedures and test new tools developed within PROACTIVE,

One of the tools resulted from the PROACTIVE project is a CBRNe Crisis Communications System, which includes three core components:

- a Web Collaborative platform with database scenarios for LEAs and Security Policy makers
- an innovative response tool in the form of a Mobile Application for Practitioners
- a Mobile App for Vulnerable Citizens.

This PROACTIVE CBRNe Crisis Communications System was developed within WP4 of the project.

1.2. Objectives of WP4

The main objectives of WP4 were defined in the original project proposal and can be summarised as follows:

- Develop the comprehensive technological components supporting the PROACTIVE CBRNe Crisis Communications System;
- Design the complete PROACTIVE CBRNe Crisis Communications System (set of tools and supporting technologies), ensuring modularity, flexibility adaptability, scalability, usability and robustness,
- Build technological tools facilitating communication and cooperation between LEAs and security-based policy makers in an efficient and effective way, exploiting the use of mobile technologies and bi-directional communication;
- Develop restricted access rich visualisation and reporting tools for LEAs and coordinating entities assisting security monitoring of communities; assessing risks, threats, vulnerabilities and incidents; allocation of resources and decision-making;
- Integrate, test and validate the Toolkit.

1.3. Objectives of D4.3

The deliverable D4.3 is an integral part of the overall deliverable from WP4 and is concerned with the developed PROACTIVE Mobile App (MA) for practitioners and general public. The key objective of D4.3 were defined during the proposal preparation phase and were constantly reviewed and updated as the project execution was progressing. These objectives can be summarised as design, development, implementation, testing and validation of PROACTIVE CBRNe mobile App for LEAs and Security Policy makers. This deliverable outlines the key results obtained throughout the project and documents these results for future use after the project completion.

2. PURPOSE OF THE DELIVERABLE

The PROACTIVE CBRNe mobile App for practitioners and general public is the main output of D4.3.

While this deliverable focuses specifically on the development of the web collaborative platform, it is important to note that the web platform is one component of the overall PROACTIVE Crisis Communication System. The PROACTIVE Crisis Communication System is made up of a:

- Web collaborative platform, with an intend end-users of LEAs and Security Policy Makers (this deliverable),
- Mobile App for Practitioners (D4.3) and
- Mobile App for vulnerable citizens (D5.4).

Hence, since the start, all three components have been developed in a harmonised way and all tools share common denominators as expressed in the initial architectural design documents. As shown in D4.1 & D5.3, the core structure of the system is the same across all three so as to enable consistency and bi-directional communication, while allowing customisations for specific groups of users (e.g., LEAs, Policy Makers, Citizens). They all aimed to ensure a modular, flexible, extensible, scalable, robust and secure system. The PROACTIVE Crisis Communication System, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by digital technologies, as well as modern data analytics capabilities to support the users in overall decision-making processes. Accessibility, in particular, is a key focus across the system as a whole. This is principally important for vulnerable communities or communities that are more difficult to reach; deaf, visually impaired, religious, children, elderly, etc. It is also important to ensure that the tools are accessible for all CBRNe practitioners. The provision of ‘other applications’ (for example Twitter, Facebook) has also been addressed and allows integration with third party applications, this covers any application outside of the PROACTIVE system, which may interact by pushing/pulling information to or from the PROACTIVE system.

The PROACTIVE CBRNe Crisis Communication System was developed based on the bellow requirements defined by PROACTIVE project in consultation with all potential stakeholders:

- ***User Experience:*** The MA should be designed with the user in mind, with an intuitive and user-friendly interface. The user should be able to easily navigate the MA, access information, and complete tasks.
- ***Functionality:*** The MA should have all the necessary features and functionalities, such as account management, personal profile set up, and access to content and services.
- ***Security:*** The MA should be designed with security in mind, with measures in place to protect user data and prevent unauthorised access. This includes using encryption, secure registration and authentication mechanisms, and other security features.
- ***Compatibility:*** The MA should be compatible with different devices and operating systems, and should work seamlessly with both iOS and Android devices.
- ***Scalability:*** The MA should be designed to handle growth and increased usage over time. This includes using scalable architecture, such as cloud-based servers and databases, to ensure that the MA is compatible with the developed PROACTIVE CBRNe collaborative platform developed in D4.2 and can handle increasing traffic and usage.
- ***Market Appearance:*** The MA architecture should be generic, ensuring that it could be easily adapted for other market applications.

The Mobile App for Practitioners and the Mobile App for Vulnerable Citizens are available as one single app, with the target end-user (practitioner or vulnerable citizen) being differentiated by access rights.

3. INTERACTION WITH OTHER WORK PACKAGES

Design and development of the PROACTIVE CBRNe Web collaborative platform for LEAs and security policy makers was predominantly the responsibility of WP4. Inputs for this work were provided from WP1, WP2, WP3, WP7 and WP8, determining the needs and gaps of the users in terms of current public perceptions relating to CBRNe incidents. The outcome of the research completed in WP1 contributed into the key engagement tasks in WP2, and by default, provided key feedback for the PROACTIVE Web Based platform in WP4. These interactions were laid out in D4.1 [1]:

- Since the publication of D4.1 in March 2021, the following new interactions have occurred:
- Development and approval of the objective technical criteria for performance evaluation of the development PROACTIVE Crisis Communication System with PROACTIVE consortium members during Progress Meetings;
- Multiple workshops with targeted end-users carried out as part of WP2 and WP3:
  - Online PSAB Workshop on 25 February 2021 (details are reported in Section 4.1);
  - Online CSAB Workshops on 26 February 2021 (Section 4.1);
  - Data Breach workshop on 4 March 2021 (details are reported in Section 4.2 & D8.2);
  - Online CSAB Focus Groups on 12 May, 26 May and June 2021 (Section 4.3);

    - The Joint CSAB-PSAB Workshop held in-person on 6 – 7 April 2022[1] (Section 4.5);

- Integration with the Mobile App for Vulnerable Citizens (WP5);
- Testing and verification of the PROACTIVE Crisis Communication System during the three field exercises organised as an integral part of WP6:
    - Contributions to the development of the Observer Guide questionnaire and its analysis;
    - Dedicated sessions during the Pre-Exercise Online Briefings to help Observers download and install the app;
    - Monitoring and analysing technical performance;
- Ensuring sustainability and market uptake of the Crisis Communication System in tandem with WP7;
- Participation and contribution to WP8 activities:
    - Involvement in the Social Impact Assessment and translating these recommendations into technical requirements for implementation in the PROACTIVE Communications System;
    - Evaluation of the Secure by Design concept and ensuring that PROACTIVE Communications System is compliant with these requirements.

Figure 1 below provides graphical illustration of the collaboration and interaction of WP4 with other WPs of PROACTIVE project.

[1] https://uic.org/com/enews/article/proactive-eu-project-holds-its-11th-consortium-meeting-and-a-joint-workshop

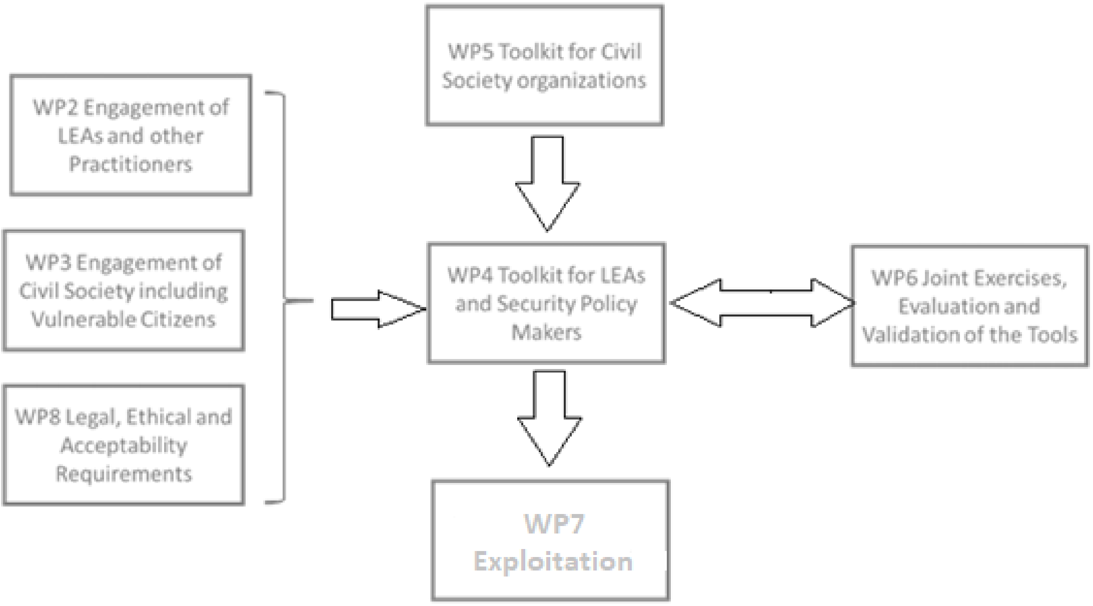

WP5 Toolkit for Civil Society organizations
WP2 Engagement of LEAs and other Practitioners
WP3 Engagement of Civil Society including Vulnerable Citizens
WP8 Legal, Ethical and Acceptability Requirements
WP4 Toolkit for LEAs and Security Policy Makers
WP6 Joint Exercises, Evaluation and Validation of the Tools
WP7 Exploitation

Figure 1 WP4 Collaboration and Interaction with other WPs of PROACTIVE

As it follows from this figure, for the purpose of this deliverable D4.3, research completed in each of the Work Packages highlighted in **Error! Reference source not found.**, has been reviewed and a nalysed from the perspective of the PROACTIVE Mobile App.

Thanks to this iterative, co-creation process with many feedback loops and interactions with other WPs, at least 20[2] new versions of the PROACTIVE Crisis Communication System (made up of the Mobile App(s) and web collaborative platform) were released, which goes beyond the original amount of versions as laid out in the project Description of Action (DoA).

4. END USER REQUIREMENTS COLLECTED PRIOR TO THE FIELD EXERCISES

Based on the requirements set out in D4.1 & D5.3, the first prototype of PROACTIVE CBRNe Mobile App was developed and released for initial testing and verification by the PROACTIVE consortium. Following these tests, it was suggested to engage PSAB and the CSAB for further testing and advise from user perspective. It needs to be emphasised that this work was not originally planned in the

[2] Including the version released after the last field exercise in Ranst, taking into account the end-user feedback collected.

original DoA. However, the benefits of such an evaluation were obvious so a decision was made to spend additional efforts on these extra tasks.

Even though this activity was not in the original DoA, the prototype was then tested with the PSAB & the CSAB during numerous workshops and focus groups organised by the UIC; details on the stakeholder engagement model are described in Havârneanu et al., 2022 [2]. However, Covid-19 pandemic affected all ways of life Globally and PROACTIVE project was not exempt from it. However, consortium members quickly adapted to a new reality and under the leadership of UIC new ways of project execution were introduced. One of the core components of this new approach was continued engagement with PROACTIVE stakeholders through online workshops and focus groups, organised by UIC, even though this was additional workload. One of the main challenges that needed to be overcome was to ensure that critical mass of practitioners and stakeholders will participate in the workshop in challenging conditions of Covid-19 pandemic. The project successfully recruited members from the advisory board to participate in all engagement activities.

Following the workshops, the PROACTIVE Crisis Communication System (and Mobile App as an integral part of this system) was redesigned, putting recommendations from the stakeholders as the key requirement (including the redesign of collaborative web platform and a first development of the Mobile App). Two additional factors contributed to this decision:

- PROACTIVE project extension due to Covid-19 pandemic.
- Iterative development process accepted by the PROACTIVE project.

The decision wasn't an easy one as it required a lot of additional work efforts which were not originally planned. This was complicated by the fact that RINISOFT lost a few development engineers who left the company and moved to other countries after Covid-19 pandemic. But all the additional efforts paid off as the new and revised version of the Crisis Communication System, developed based on direct specifications from the end users, eventually ensured successful use during the field exercises.

During the workshops and focus groups, feedback was collected and analysed using the MoSCoW methodology and a refined set of requirements were laid out. MoSCoW is a prioritisation technique commonly used in project management and software development to classify requirements or features based on their importance and urgency. The MoSCoW prioritisation technique was first introduced by Dai Cleggin in 1994 [3]. He developed this approach while working on the Dynamic Systems Development Method (DSDM), an agile project management framework. MoSCoW became a fundamental aspect of DSDM and has since been widely adopted in various project management methodologies, including PROACTIVE, particularly in the field of software development. It provides a structured approach for prioritising requirements and making informed decisions about project scope and deliverables. The acronym stands for Must have, Should have, Could have, and Won't have. Each category represents a different level of priority for the project or product being developed.

4.1. PSAB & CSAB Workshops Requirements

There were two consecutive workshops and the first workshop was conducted with 18 PSAB participants representing all categories of CBRNe practitioners on the 25 February 2021 [4]; and the second one involved 10 CSAB members representing mainly experts or researchers on the 26 February 2021 [5].

The workshops took the form of an incident-based discussion followed by a presentation of the PROACTIVE CBRNe Mobile App and then a live questionnaire. Participants were provided a fictitious CBRNe scenario, involving a suspected chemical attack set on a train carriage, and asked questions about their reactions to such situations. The live questionnaire asked questions specifically concerning the App functionality, design and accessibility. The incident-based discussion and live questionnaire allowed for the further elaboration of the requirements. First of all, we collected detailed feedback on the usefulness of existing features. These are shown in Table 1.

Table 1. Feedback on the existing features collected during the first workshop

Must have	Should have	Could have	Won't have
• Live alerts during an incident • Pre-Incident Information/ communication materials • Possibility to share information, including location and images	Contact details of LEAs and Vulnerable Citizen Organisations	Forum and/or Direct Messaging between LEAs and Citizens	Not applicable (N/A)

These workshops created foundation for closer engagement with PROACTIVE stakeholders and CBRNe practitioners. Further, these two workshops allowed us to collect new input, including additional features that the app must, should or could have. These are shown in Table 2. UIC, who organised the workshop, tried to keep interactive workshop format even though these workshops were organised online. To achieve this, live evaluation sessions were introduced and during these live evaluation sessions of the workshops, when asked to rate the web platform out of five stars, the PSAB workshop participants gave it 4 stars while the CSAB participants gave it 3. This symbolic exercise has demonstrated the importance of user engagement and was used to give an overall impression about the MA quality perception within each group of users and provide a baseline for how the rating is going to change over time.

Table 2 Additional features collected during the workshops.

Must have	Should have	Could have	Won’t have
• Better accessibility features, including: • Text-to-speech • Translation • Big text • Basic wording • Uncomplicated structure • Pictures, pictograms • Big buttons, icons and symbols • Color blind mode for images/mapping • Specific information on what is happening and how to act	• Less text • Mental health support message • A symptoms checklist • Hospital lists • Links to other useful apps	• Social media integration (post information to a given social media account) • Ways to contact relatives/loved ones • Proof of decontamination	• Live camera feed to App for transmission to First Responders

4.2. Data Breach Workshop Requirements

Therefore, in addition to two workshop explained in the previous section, the PROACTIVE Data Breach Tabletop Exercise (TTX) took place on 4 March 2021 and had 10 participants, including security experts from law enforcement agencies and ethics experts. It was a scenario-based discussion in the format of a focus group. This workshop allowed for the development of requirements related to the prevention and mitigation of data breaches which are summarised in the Table 3 below. Full details of the data breach workshop were reported in D8.2 [6].

Table 3 Requirements related to the prevention and mitigation of data breaches

Must have	Should have	Could have	Won't have
• A means to secure the integrity and confidentiality of personal data • Anonymisation, pseudonymisation and encryption • A means to provide information about the potential source of the data breach and data subjects involved • The ability to communicate the breach to the supervisory authority based on data regulations and, in some cases, also the data subjects (the citizens) • The functionality to preserve the leak's circumstances, as preservation is a key aspect of digital forensics	• Ability to switch off the false data source • Ability to detect if the data breach is human error, misuse or an intentional attack • A tool within the App to rapidly report leaks to users • The protocol to be followed in case of data leaks	• Include a system to catalogue received information according to the source in some way; • A way to register logs to the system integrated into the platform • A data breach communication protocol	• Direct integration with other apps

4.3. Focus Groups with the CSAB

The discovered format of stakeholder engagement was well accepted by all the participants and a decision was made to enhance this programme until travel restrictions are removed. Therefore, three online Focus Groups with CSAB members were held in May-June 2021 in the following order:

- 12 May 2021 with 4 participants representing the blind/visually impaired, autistic, and mobility restricted;

- 26 May 2021 with 9 participants representing the blind/visually impaired, the deaf/hard of hearing, the LGBTQ-community, and the mobility restricted; and
- 8 June 2021 with 6 CSAB members representing the homeless, pregnant women, senior citizens, visually impaired guide dog users, and immigrants.

This format was selected deliberately as the goal was to separate the CSAB into smaller working groups and collect their inputs separately once they had a hands-on experience with the web platform during an incident-led discussion. Discussions within the focus groups concentrated on accessibility and ease-of-use of the app, which led to the following requirements (Table 4). Moreover, the focus groups gave the App a rating of 2.6 stars out of 5 on average. Detailed results are reported in Petersen et al., 2022 [5].

Table 4 Accessibility requirements collected during the 3 focus groups

Must have	Should have	Could have	Won't have
• Compliance with international standards for accessibility (e.g., WCAG 2.1) • Accessibility features, including: • Translation • Ability to zoom for the partially sighted • A high contrast option • Audio information • International Sign Language • An Easy Read mode A less chaotic interface	• A search button • Less confusing icons (e.g., contact icon should be an envelope, not an arrow) Less reliance on maps	N/A	N/A

4.4. Translation of MoSCoW findings into design and functional requirements

Let's go through each MoSCoW category in more detail:

Once gathered, the MoSCoW findings were translated to PROACTIVE Crisis Communications System design and functional requirements, promoting the customisation elements needed to address the demands clearly explained during the workshops by each user group. This selected method ensured a core set of key functionalities are helped to build the overall system architecture ensuring a modular, flexible, scalable, robust and secure system is built. The architectural definition process focused on the following four principal objectives:

- To clearly present a description of the PROACTIVE system and how it addresses the stakeholder needs (including LEAs and vulnerable citizens);
- To provide a clear description of the critical aspects that need to be taken into consideration to ensure the system is modular, flexible, extensible, scalable, robust and secure;
- To provide enough details to allow technical teams to build instances of the system that share a common structure and consequently are interoperable by design;
- To ensure consistency for the MoSCoW findings by using this architecture design as a baseline input.

Concretely, this meant, for the MoSCoW requirement of “a less chaotic interface”, the collaborative web platform homepage was redesigned to have a less complicated structure and a more ergonomic interface. For example, the “report an incident” button is now a standalone button, no longer under the heading of “get involved,” and has been coloured as a different colour (in this case red) and shade (lighter) than the other buttons to demonstrate its importance.

To meet the Must have requirement of better accessibility features, the web platform was updated to use larger font sizes, bigger buttons and bigger icons.

“The PROACTIVE platform is your one-stop hub for all things Communication in relation to CBRNe incidents. The terms CBRNe refers to any Chemical, Biological, Radioactive, Nuclear and Explosive incidents and through the platform you can:

- Report and receive live notifications about ongoing incidents in your area;
- Access pre-incident information on incidents;
- Interact with Law Enforcement Agencies and Civilian Organisations.”

Another example is that the contact icon was depicted as an arrow and has now been replaced with an envelope, the icon which the participants felt best depicted the idea of contact. Furthermore, the exclamation mark by share information made it seem that one would receive information and not report it to the police, so this was removed.

4.5. Release of the Mobile App at the Joint CSAB-PSAB Workshop in Paris

Up till April 2022, all engagement activities (workshops, focus groups) with the PROACTIVE Advisory Boards describe in the above sections and feedback sessions with PROACTIVE Consortium members during Progress Meetings were carried out using a prototype web collaborative platform.

Starting at the Joint CSAB-PSAB Workshop in Paris and continuing on to the three field exercises, end-user requirements were collected based on the Mobile App[3]. Indeed, all the end-user requirements collected regarding the prototype collaborative web platform were also applied to the mobile app, which debuted during the Joint CSAB-PSAB Workshop. However, it is important to note that just in the case of the requirements collected via testing of the web collaborative platform being applicable to the Mobile App, all requirements collected in regards to the Mobile App were also applied to the web collaborative platform.

A key example of this can be taken from the development of the now entitled CBRNe Library. Since its inception, one aspect of the PROACTIVE Crisis Communication System was to foster CBRNe incident preparedness through stocking relevant CBRNe preparedness materials (including but not limited to the PROACTIVE Pre-Incident Information Materials developed in D5.2 [7]) in a dedicated repository. In the original web collaborative platform prototype this area was called “CBRNe Information” and so was transferred as such to the Mobile App. During the Paris Workshop, it became clear that this was confusing to participants, with many thinking that if they clicked on the “CBRNe Information” button, they would find out information about the on-going CBRNe Incident. At the suggestion of the targeted end-users, the verbiage was changed to better reflect its actual purpose (that of a repository and not of informing about ongoing incidents): CBRNe Information became CBRNe Library. This change was not applied only to the Mobile App but was also applied to the web collaborative platform.

5. MOBILE APP DEVELOPMENT

5.1. General Approach

The PROACTIVE CBRNe MA was developed based on an iterative approach in line with the three field exercises completed during the lifetime of the PROACTIVE project. Numerous iterations of the developed system were implemented as a feedback loop for system optimisation as shown in below diagram.

[3] Regarding the mobile app(s), while the DoA distinguishes between a Mobile App for Practitioners and a Mobile App for Vulnerable Citizens, this is in actuality the same app, differentiated by user groups (admin rights for Practitioners, and both a registered user and non-registered user for (vulnerable) citizens). See D4.3 & D5.4 for more.

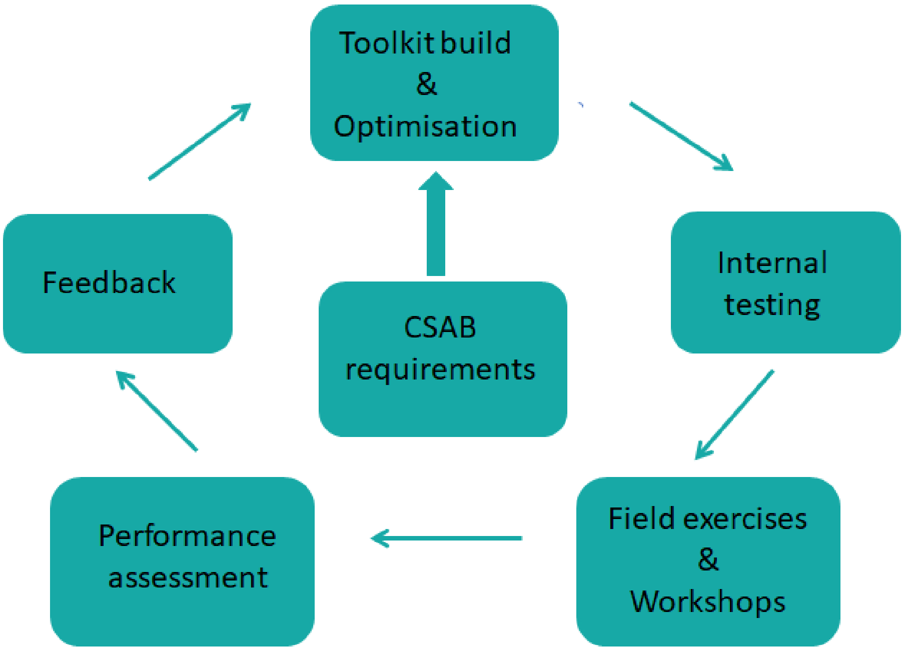


Figure 2 Iterative approach to Mobile App development

As it is shown on this figure, initially focus of MA development was placed on the CSAB requirements, then the PSAB and the final exercise will amalgamate the two. The final phase of the development was dedicated to incorporation of the currently available content, effectively showcasing the usability and purpose of the developed MA during and post exercises, which produced recommendations for further optimisation, as an integral part of the overall iterative process.

5.2. Architecture

As mentioned earlier, the PROACTIVE CBRNe MA is an integral part of the PROACTIVE CBRNe Communications System therefore the development of MA was closely correlated with the development of the overall communications system. Figure bellow illustrates the block diagram of the overall communications system and highlights the interaction of the MA with all components of the overall system.

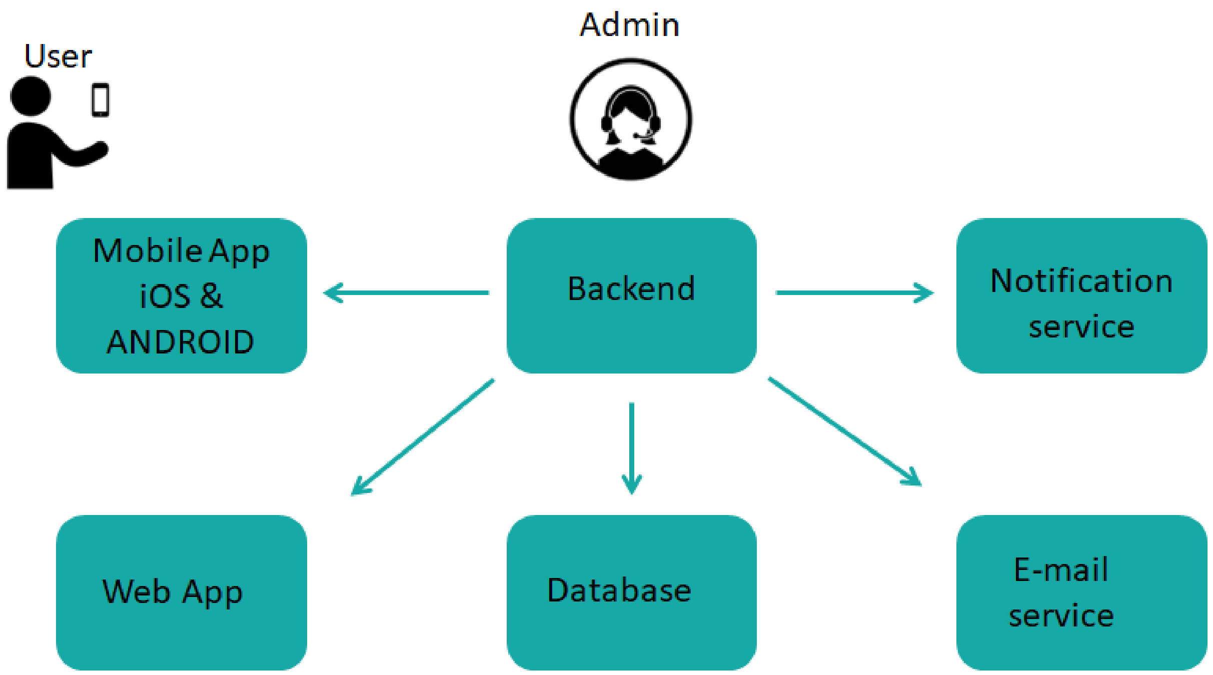


Figure 3 MA as an Integral part of the PROACTIVE CBRNe Communications System

As it follows from this diagram, the PROACTIVE CBRNe MA is a key component enabling bi-directional communications between the users and the administrators of the overall PROACTIVE CBRNe Crisis Communications System. When developing the PROACTIVE MA, RINISOFT understood that there isn't a single "*most advanced*" mobile App architecture, as the choice of architecture depends on the specific requirements, complexity, and goals of the application. Therefore, when starting the development, the following approaches to MA design were considered:

- ***Model-View-Controller (MVC):*** MVC [8] is a classic architecture that separates an application into three components: the Model (data and business logic), the View (user interface), and the Controller (mediates between the Model and the View). While MVC has been widely used, it is considered less advanced compared to more modern architectures.
- ***Model-View-Presenter (MVP):*** MVP [9] is an evolution of MVC, where the Presenter acts as the middleman between the Model and the View. The Presenter handles the business logic and interacts with the View and Model to update the UI and process user input.
- ***Model-View-ViewModel (MVVM):*** MVVM [10] separates an application into three components: the Model (data and business logic), the View (user interface), and the ViewModel. The ViewModel acts as a bridge between the View and the Model, providing data and commands to the View and handling UI-specific logic. MVVM is often used in conjunction with data binding frameworks.
- ***Clean Architecture:*** Clean Architecture emphasises the separation of concerns and decoupling of components. It consists of multiple layers, including the Presentation layer (UI), Domain layer (business logic), and Data layer (data access). Each layer has its own responsibilities and dependencies are directed inward, ensuring that higher-level layers are not dependent on lower-level ones.

- ***Flutter's Provider Architecture*:** Flutter, a popular cross-platform framework, utilises an architecture based on the Provider package. It follows a reactive approach, where data flows from providers to consumers. The Provider Architecture leverages InheritedWidgets and ChangeNotifier to manage the state of the application and handle updates efficiently.
- ***Redux:*** Redux is an architecture pattern that originated in web development but has gained popularity in mobile App development, especially with frameworks like React Native. Redux stores the application state in a single, immutable store. Actions trigger state changes through reducers, and UI components subscribe to the store to update based on the state changes.

As it follows from the best practice of MA design, the choice of architecture should align with the project's needs, maintainability, scalability, and the development team's familiarity and expertise. Therefore, taking into account all the above and recommendations from the PROACTIVE stakeholders, MVP architecture was adopted for PROACTIVE CBRNe MA. The generic block diagram of the MVP architecture is shown in the figure below

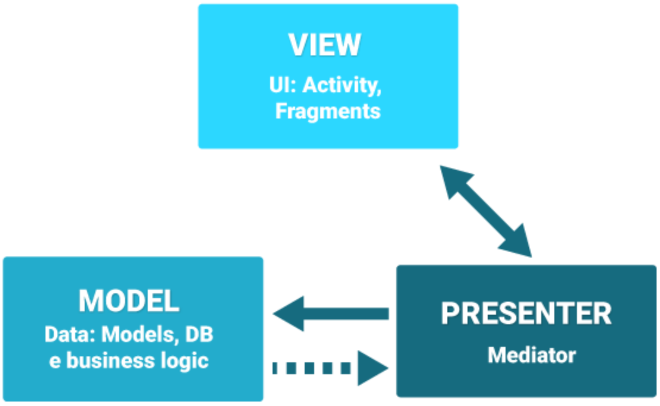


Figure 4 Generic Diagram of the MVP architecture

The key component of this diagram are as following:

- ***Model:*** The Model represents the data and business logic of the application. It encapsulates data retrieval, manipulation, and storage operations. The Model component is independent of the GUI and communicates with the Presenter to provide data for display or to perform business logic operations.

- ***View:*** The View component represents the user interface and is responsible for displaying information to the user. It can be implemented as an activity, fragment, or a custom GUI element, depending on the platform and framework being used. The View is passive and should not contain any business logic. It communicates user actions to the Presenter and receives updates to refresh the UI.

- ***Presenter:*** The Presenter acts as an intermediary between the View and the Model. It receives user input from the View and processes it accordingly. The Presenter retrieves data from the Model and formats it for display in the View. It handles the business logic of the application, such as validation, data transformation, and coordination between the View and Model. The Presenter also notifies the View of any updates or changes that need to be reflected in the GUI.

The flow of data and events in MVP follows general steps shown in Figure below:

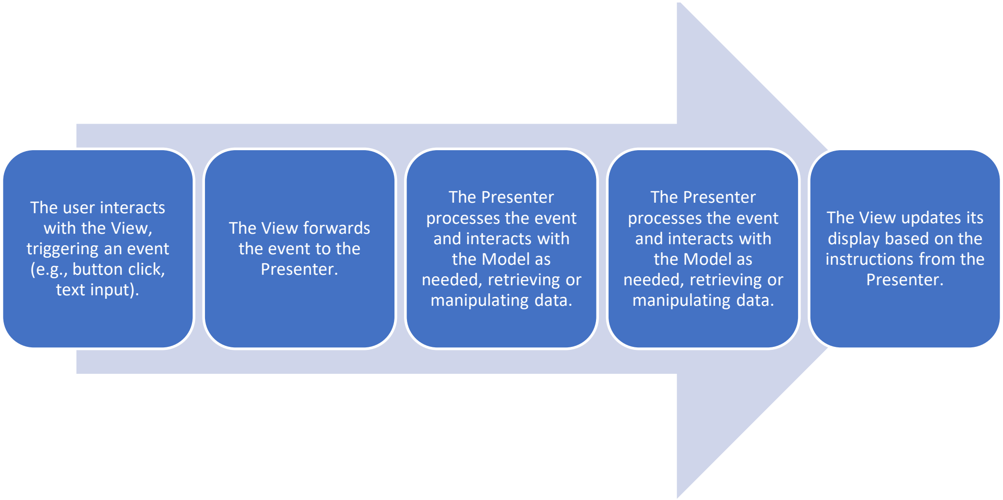

The user interacts with the View, triggering an event (e.g., button click, text input).
The View forwards the event to the Presenter.
The Presenter processes the event and interacts with the Model as needed, retrieving or manipulating data.
The Presenter processes the event and interacts with the Model as needed, retrieving or manipulating data.
The View updates its display based on the instructions from the Presenter.

Figure 5 Flow of Data and Events in MVP

The MVP pattern helps to separate concerns and maintain a clear separation of responsibilities between the components. This separation makes it easier to test individual components independently, as business logic resides in the Presenter, and the View can be mocked or replaced for testing purposes.

A key factor in selecting MVP is the fact that MVP is widely used in various platforms and frameworks, including Android, iOS, and web development, which was one of the core technical requirements for PROACTIVE MA.

When developing the PROACTIVE CBRNe MA we envisaged the worst case scenario when no public communications infrastructure will be available during a CBRNe incident. Therefore, the developed MA (being integral part of the PROACTIVE Communications System) is designed with unique feature to support reliable and robust operation of PROACTIVE CBRNe communications system over private and restricted networks, such as mesh networks established by the First Responders as an integral part of incident response [11]. ***This feature makes the developed MA unique in comparison with the possible existing solutions (WhatsApp, Facebook, etc), which require INTERNET connectivity for their operations.***

5.3. Development Tools

As mentioned earlier, throughout the PROACTIVE project lifespan, over 20 versions of MA were developed and released, utilising iterative development process adopted by the project. When developing PROACTIVE MA using the MVP architecture, RINISOFT considered and used various tools and frameworks to aid in the development process. As the developed MA was required to work on both the ANDROIND and iOS, and taking into account plans for post-project commercialisation, the decision was made to de two separate independent developments (for both the Android and iOS) using 2 parallel set of development tools listed below:

- *Java:* Programming language widely used for Android App development with libraries and frameworks compatible with MVP.
- *Swift:* Programming language for iOS App development that allows implementation of MVP on Apple platforms.
- *Android Jetpack:* Offers a set of libraries and tools from Google, which can facilitate the implementation of the MVP pattern in Android apps.
- *iOS UIKit:* Apple's UI framework for iOS App development, which provides essential components for building user interfaces in MVP-based applications.
- *Dagger (for Android):* A dependency injection framework for Android that assists in providing dependencies to the Presenter and other components in the MVP architecture.
- *Swinject (for iOS):* A lightweight dependency injection framework for Swift that helps manage dependencies within the MVP architecture.
- *Espresso (for Android):* A testing framework specifically designed for Android, which enables GUI testing and interaction verification in MVP-based applications.
- *XCTest (for iOS):* Apple's testing framework for iOS apps, supporting unit testing and GUI testing in MVP architectures.
- *Android Studio:* The integrated development environment (IDE) for Android App development, offering a range of tools for coding, debugging, and testing Android MVP applications.
- *Xcode:* Apple's IDE for iOS development, providing features for building, testing, and debugging iOS applications following the MVP architecture.
- *Git:* A distributed version control system that helps manage source code changes, collaborate with a team, and track project history for both the ANDROIND and iOS versions of the MA.

These tools provided support for developing MVP-based PROACTIVE MA across different platforms, helping to streamline development, improve code quality, and enhance productivity.

5.4. System Functionality

The key component in the development of the PROACTIVE MA was to develop a methodology and procedure for technical evaluation of the functionality of the developed App utilising the selected MVP architecture. This development included the following steps:

- ***Understand the Requirements:*** Thoroughly understand the functional requirements of the MA, including the core features, user interactions, and expected behaviour of the application.
- ***Identify Use Cases:*** Split the app's functionality into specific use cases or user scenarios where each use case represents a specific task or action that a user can perform within the app.
- ***Map Use Cases to Components:*** Associate each use case with the relevant components in the MVP architecture and determine which components (View, Presenter, Model) are responsible for handling the specific use case and its associated functionality.
- ***Test the View:*** Verify that the View component correctly displays the user interface elements and responds to user interactions, ensuring that the UI elements are correctly rendered, transitions between screens work as intended, and user inputs are properly captured.
- ***Test the Presenter:*** Evaluate the Presenter's functionality by simulating user actions and verifying that the Presenter handles those actions appropriately.
- ***Test the Model:*** Assess the Model's functionality by verifying that it correctly handles data retrieval, manipulation, and storage operations.
- ***Test Interaction between Components:*** Evaluate the interaction and communication between the View, Presenter, and Model and verify that data flows correctly between components and that updates or changes made in one component are reflected in the others as expected.
- ***Conduct Use Case Testing:*** Execute the identified PROACTIVE user scenarios, systematically testing each one to ensure that the App functions as intended.
- ***Test Edge Cases and Error Handling:*** Perform testing with various edge cases, boundary conditions, and error scenarios, ensuring that the App handles these situations gracefully, providing appropriate error messages or fallback behaviour.
- ***Gather User Feedback:*** Once functional testing is complete, gather feedback from PROACTIVE MA users, and optimise any areas that may require improvements or enhancements.

By developing and applying these steps, RINISOFT was able to provide technical evaluation of the developed PROACTIVE MA and set up objective technical criteria for continuous improvements.

5.5. Security

As mentioned in D4.2 the PROACTIVE CBRNe Crisis Communications System is designed to be compliant with the concept of "*Secure by Design*[4]" [11]. As PROACTIVE MA is an integral part of the communications system, the same approach was adopted to the design the MA. The main principles of the "*Secure by Design"* concept are outlined in the table below:

Table 5 Main Principle of Secure by Design

Principle	Implementation
Minimising attack surface:	This principle involves reducing the opportunities for attackers to exploit vulnerabilities in a system by reducing its attack surface. This can be achieved by implementing only necessary functionality and limiting access to sensitive data.
Layered defence:	This principle involves implementing multiple layers of defence to provide a more robust security posture. This can be achieved by using a combination of security controls such as firewalls, intrusion detection systems, and encryption.
Principle of least privilege:	This principle involves giving users and processes only the minimum level of access necessary to perform their tasks. This can help reduce the risk of unauthorised access and limit the potential damage that can be caused by a compromised account.
Secure default settings:	This principle involves implementing secure default settings for all systems and applications. This includes ensuring that all passwords are strong and not easily guessable, and that all default configurations are secure.
Fail-safe defaults:	This principle involves ensuring that systems and applications fail safely in the event of an error or security breach. This can help prevent attackers from exploiting vulnerabilities to gain unauthorised access or cause damage.

Although many steps in ensuring compliance of the developed MA with the "Secure by Design" concept were similar to the processes described in D4.2 [11], ensuring compliance with "*Secure by Design*" principle in an MVP PROACTIVE MA involves additional security practices in the development process. These are summarised in the table below:

[4] https://cordis.europa.eu/project/id/826293

Table 6 Ensuring Compliance of PROACTIVE MA with "*Security by Design*"

Principle	Implementation
Identify Security Requirements	Understand the specific security requirements for PROACTIVE MA, consider factors such as data privacy, authentication, authorisation, encryption, secure communication, input validation, and protection against common vulnerabilities
Threat Modelling	Perform a thorough threat modelling exercise to identify potential security risks and vulnerabilities in PROACTIVE MA, identify possible attack vectors and assess their impact and likelihood.
Design Secure Architecture	Ensure that each component (View, Presenter, Model) adheres to security best practices.
Apply Secure Coding Practices	Emphasise concepts like secure file handling, proper error logging (without revealing sensitive information), and avoiding hardcoding sensitive data (e.g., passwords, API keys).
Implement Authentication and Authorisation specific for PROACTIVE MA	Incorporate strong authentication mechanisms or biometric authentication, to verify the identities of users, implement authorisation controls to ensure that users have appropriate access privileges and cannot perform unauthorised actions.
Secure Data Storage and Communication	Implement secure storage mechanisms, such as using encryption algorithms, secure key management, and avoiding storing sensitive data unnecessarily. Use secure communication protocols (e.g., HTTPS) to protect data transmission between the App and backend servers.
Input Validation and Sanitisation	Implement robust input validation and sanitisation techniques to prevent common security vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Validate and sanitise user inputs before processing or displaying them to prevent malicious inputs from compromising the app.
Regular Security Testing	Conduct regular security testing and vulnerability assessments to identify and address any weaknesses in PROACTIVE MA, perform security code reviews, penetration testing, and security scanning to uncover vulnerabilities and address them promptly.
Keep Software Dependencies Up to Date	Regularly update the software dependencies used in PROACTIVE MA, including frameworks, libraries, and SDKs.
User Education and Awareness	Educate PROACTIVE MA users about best practices for using the App securely.

By following these steps, RINISOFT integrated security measures into the design and development of the PROACTIVE MA, helping to ensure compliance with "Secure by Design" principles and safeguarding MA users' data and privacy. Additionally, staying updated on the latest security practices and adapting to emerging threats will help you maintain the security of your App over time.

5.6. System Interoperability

Another unique feature of the developed PROACTIVE CBRNe communications system is interoperability with the existing legacy systems. Furthermore, the developed communications system is designed as future proved, allowing integration of systems which could be introduced in the future.

To ensure interoperability between the PROACTIVE MA and legacy systems RINISOFT applied careful planning and consideration of integration techniques, ensuring compliance with requirements developed during the engagement with the end users. The process started analysing the architecture, protocols, and data formats used by the legacy systems. RINISOFT identified limitations or constraints that may affect the integration process and mitigated the risks by seeking input from the team members s familiar with the legacy systems. This was followed by the definition of the specific integration requirements between the PROACTIVE MA and the legacy systems, including identifying the data exchange needs, authentication mechanisms, and workflows that need to be supported.

To ensure the most appropriate integration approach based on the requirements and capabilities of both the PROACTIVE MA and the legacy systems, the following integration techniques were applied:

- APIs of legacy systems to establish communication and data exchange between the PROACTIVE MA and the legacy systems.

- Transformation of the data formats used by the PROACTIVE MA and the legacy systems to convert data between the formats.

- Utilising message-oriented middleware to enable asynchronous communication between the PROACTIVE MA and the legacy systems to ensure adequate performance when dealing with high volumes of data or real-time events.

These techniques, combined with an iterative approach adopted by the PROACTIVE allowed to establish incremental progress and enabled early identification of any challenges or complexities. By following these steps, RINISOFT ensured interoperability between the PROACTIVE MA and legacy systems, enabling seamless data exchange and functionality.

This interoperability was tested during the last 2 field exercises where PROACTIVE CBRNe communications system was linked and integrated with Twitter and LinkedIn social media platforms.

5.7. Description of the PROACTIVE Mobile App for Practitioners

5.7.1. Installation

As required, PROACTIVE MA was developed for both the Android and iOS and as such, was published on both the app stores. To ensure seamless localisation and installation of the PROACTIVE App on mobile devices, special QR-codes were produced and provided to all users. These codes are illustrated in figure below.

a) b) c)

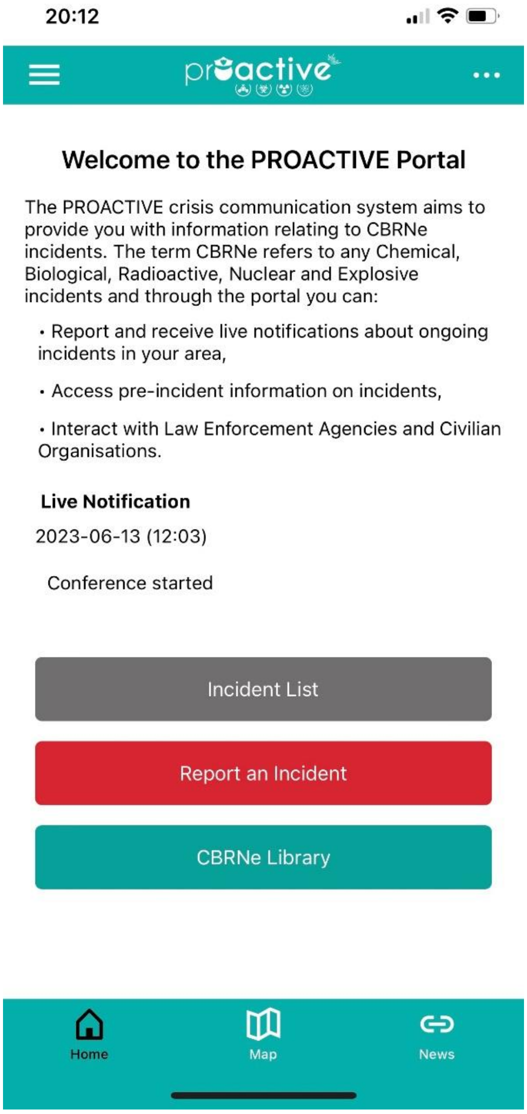
Figure 6 QR Codes for PROACTIVE MA

a) GooglePlay b) AppleStore c) Universal

After downloading the MA, the users will require to register with the PROACTIVE platform, providing their e-mail details. Once the address is verified, the user get access to the PROACTIVE MA. This allows registered users and site admins (LEAs) to access application features not available to unregistered users.

5.7.2. Graphic User Interface

The GUI starts with the following landing page[5]



Welcome to the PROACTIVE Portal

The PROACTIVE crisis communication system aims to provide you with information relating to CBRNe incidents. The term CBRNe refers to any Chemical, Biological, Radioactive, Nuclear and Explosive incidents and through the portal you can:

- Report and receive live notifications about ongoing incidents in your area,
- Access pre-incident information on incidents,
- Interact with Law Enforcement Agencies and Civilian Organisations.

Live Notification

2023-06-13 (12:03)

Conference started

Incident List

Report an Incident

CBRNe Library

Figure 7 Landing Page for PROACTIVE Mobile App

As requested in initial requirements, the developed GUI supports:

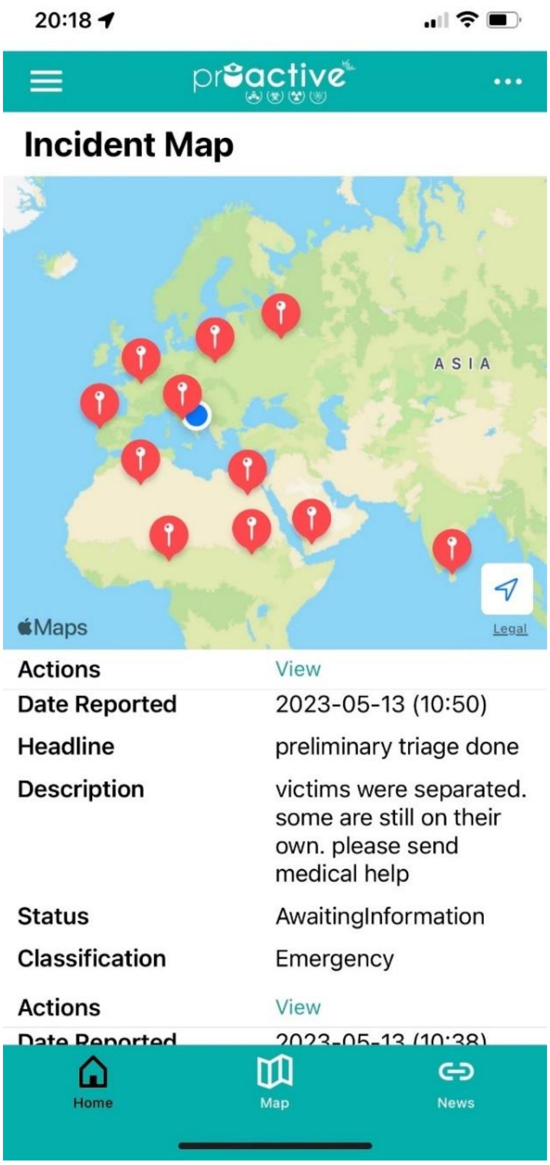
- Landscape and Portrait aspect ratios;

[5] There were a number of versions for the landing page but eventually after discussion with the stakeholders the current version was adopted.

- Screen sizes from 10cm to 50+cm;
- iOS phones and tablets;
- Android phones and tables;
- Screen readers & accessibility tools;

5.7.3. “Incident Map” Page

This is the page on platform which shows geographical location of all the reported incidents and a description for each of the incident provided by the PROACTIVE CCS administrator. The screenshot of this page is shown below:

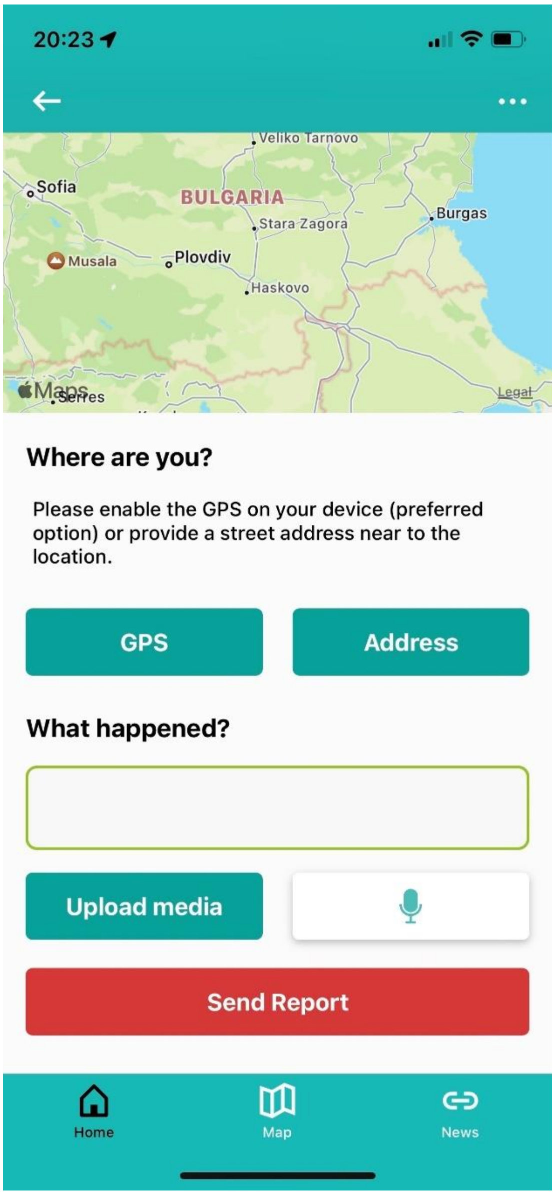


Actions	View
Date Reported	2023-05-13 (10:50)
Headline	preliminary triage done
Description	victims were separated. some are still on their own. please send medical help
Status	AwaitingInformation
Classification	Emergency
Actions	View
Date Reported	2023-05-13 (10:38)

Figure 8 PROACTIVE Mobile App “Incident Map”

5.7.4. “Report an Incident” Page

When a user clicks on “Report an incident” button, he/she will be brought to the page which will allow to report an incident by providing geographical coordinates, address, description of the incident supported by additional video/audio materials. The screenshot of this page is sown in figure below:



Where are you?

Please enable the GPS on your device (preferred option) or provide a street address near to the location.

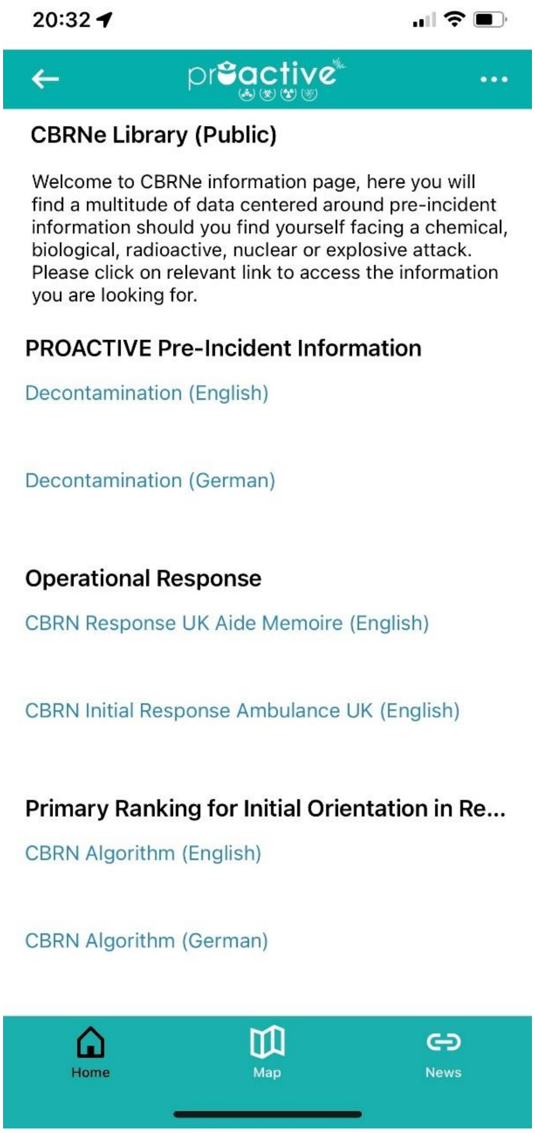
What happened?

Figure 9 Screenshot of the “Report an Incident” Page

Once a report is sent successfully, a confirmation will be sent to the user and it will be now the responsibility of the PROACTIVE CCS administrator to evaluate the report and decide if it should be published for all users.

5.7.5. “CBRNe Library” Page

Similar to PROACTIVE CBRNe Collaborative Platform, PROACTIVE Mobile App also has a dedicated page dedicated to key information required for better preparedness for CBRNe incidents. This page was developed in close cooperation with all stakeholders and includes comprehensive information covering pre-CBRNe, during-CBRNe and post-CBRNe scenarios. Figure bellow show a screenshot of the web platform dedicated to this content. A screenshot of this page is shown in figure below.



20:32

CBRNe Library (Public)

Welcome to CBRNe information page, here you will find a multitude of data centered around pre-incident information should you find yourself facing a chemical, biological, radioactive, nuclear or explosive attack. Please click on relevant link to access the information you are looking for.

PROACTIVE Pre-Incident Information

Decontamination (English)

Decontamination (German)

Operational Response

CBRN Response UK Aide Memoire (English)

CBRN Initial Response Ambulance UK (English)

Primary Ranking for Initial Orientation in Re...

CBRN Algorithm (English)

CBRN Algorithm (German)

Figure 10 PROACTIVE MA “CBRNe Library” Page

The Mobile App has all the information available on PROACTIVE collaborative web platform and is available to all users.

5.7.6. Additional Information

Additional to the pages which are essential for bi-directional communications between the users of the PROACTIVE Mobile App and the First Responders, the developed Mobile App also has numerous pages providing additional supporting information. This information is available through a dedicated menu as shown on a screenshot below.

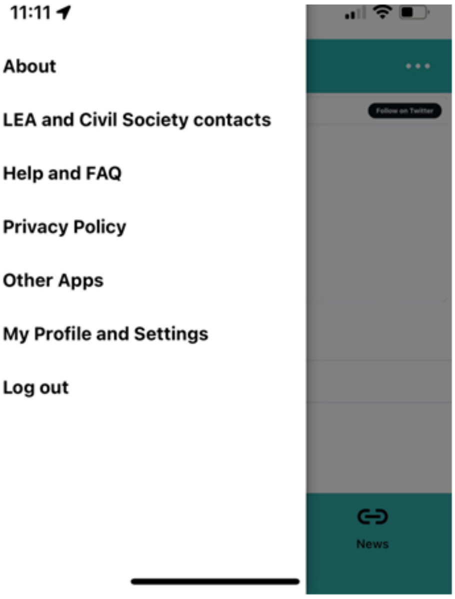


Figure 11 Screen Shot of Menu Page with Additional Information

This information is identical to the information available on PROACTIVE CBRNe Collaborative web platform [11] and is aimed for users who have no access to the platform, ensuring that they are not in disadvantageous position in regards to the information availability.

6. VERIFICATION

6.1. Verification Requirements

Verification and testing of the any software is a key component of any development an PROACTIVE CBRNe Mobile App wasn't exempted from this process. Furthermore, as was requested in the original requirements, the developed Mobile App has undergone 2 independent verifications:

- Objective (technical) verification, which included testing, debugging and collection of objective measurable evidence after every PROACTIVE field exercise;
- Subjective (user) verification through questionnaires, representing subjective views reflecting personal experience from using the developed platform during and between PROACTIVE field exercises.

To ensure fair and comprehensive verification, a set of verification criteria were developed in parallel with the development. To the extend, most of these criteria are similar to verification criteria developed and accepted for verification of PROACTIVE CBRNe Collaborative web platform and are listed below:

Table 7 PROACTIVE MA Verification Criteria

Criteria	Description
Criteria Description Functionality	The App should perform all of its intended functions correctly and without errors. All features and functionalities should be thoroughly tested.
Accessibility	The App should be accessible to users with disabilities, including support for assistive technology and customizable settings to accommodate different needs.
Localisation	The App should be available in different languages and localised to meet the needs of different regions and cultures.
Usability	The App should be easy to use and navigate, with intuitive controls and a clear user interface. The app's design and layout should also be visually appealing and consistent.
Performance	The App should perform well, with fast load times and smooth transitions. The App should not freeze or crash frequently, and should be optimised for battery life and resource usage.
Security	The App should be secure and protect user data from unauthorised access or hacking attempts. The App should use encryption and secure authentication mechanisms to ensure that user data is kept confidential.
Compatibility	The App should be compatible with different devices, platforms, and screen sizes. The App should be tested on a range of devices to ensure that it works well on all of them.
Documentation	The App should have clear and thorough documentation, including user manuals and technical documentation for developers.
Maintenance	The App should be easy to maintain and update, with modular code that is easy to modify and fix. The App should also be tested regularly to ensure that it continues to perform well and meet user needs.
Offline Functionality	In cases where internet connectivity is limited or unreliable, the app should provide offline functionality to ensure users can still access critical features and information.

6.2. Results of Objective (Technical) Verification

As mentioned above, technical (objective) verification of the developed PROCTIVE Mobile App was conducted during the field exercises and included comprehensive measurements of all the key system parameters. To conduct technical verifications, RINISOFT used a dedicated dashboard, embedded within PROCATIVE collaborative web platform, for viewing these parameters in real time, as the exercise evolves. As an example, Figure below shows total number of notifications clicks during the second exercise (Figure 12a) and their distribution between the Android (Figure 12b) and iOS (Figure 12c) users.

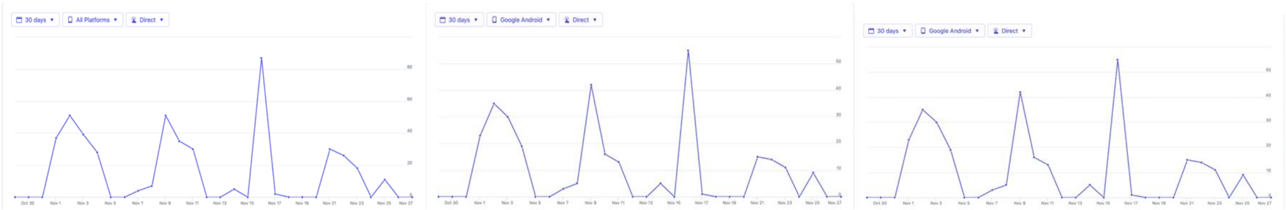
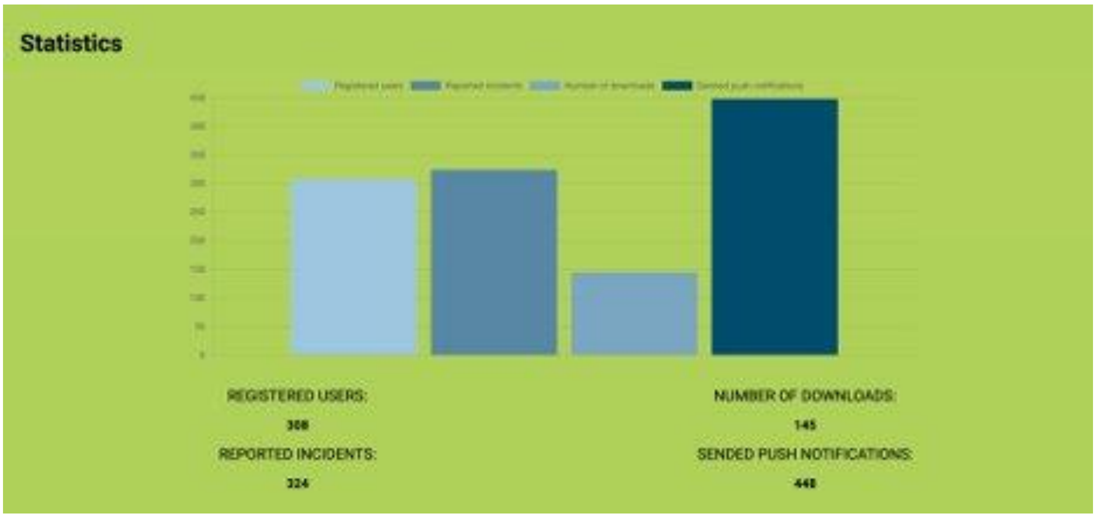


Figure 12 Number of notifications during the second PROACTIVE field Exercise

a) Total Number b) Android users c) iOS users

Figure below represents a screen short illustrating verification summary from the third PROACTIVE field exercise. Some of the results of technical verification from the third (final) PROACTIVE exercise are shown below.



REGISTERED USERS:
308

REPORTED INCIDENTS:
324

NUMBER OF DOWNLOADS:
145

SENDED PUSH NOTIFICATIONS:
448

Figure 13 Total PROACTIVE MA Statistics

Figure 13 shows overall statistics of the PROACTIVE MA, including total number of registered users, total number of reported incidents, number of MA downloads, etc. When comparing these statistics with verification results from the first and second PROACTIVE exercise, we can see clear increase in user engagement and usability of the developed MA, which indirectly indicates the improved acceptability of the developed MA by the stakeholders.

More details statistics of technical verification are shown on figure below.

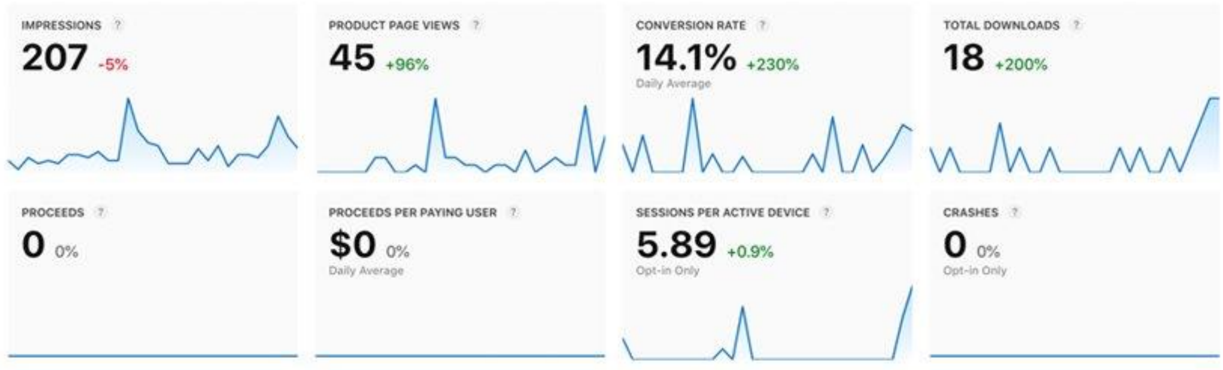


Figure 14 Technical Verification Summary

As it follows from this figures, the developed PROACTIVE Mobile App performed as expected with no technical issues reported during the exercise.

6.3. Subjective Verification

As part of each field training exercise, external Observers were tasked with taking on the role of a witness to the incident who would use the PROACTIVE Mobile App to a) look for information about the ongoing incident and b) report the incident. This is in line with the intended citizen end-user, as research shows that mobile apps are not likely to be used by the victims of a disaster but rather by witnesses.

The Observer Guide questionnaire included a section with roughly 20 questions focused on the app, composed of closed and open questions. The answers to the closed questions were provided on Likert-type scales and were accompanied by open questions which gave the observers the possibility to explain their answers and to give examples. Slight adjustments to the Observer Guide were made over the course of the project, to enhance clarity for example, while ensuring that the questions were similar enough to ensure cross comparison at the end. The full analysis of the Observer Guides is given in the corresponding deliverables (D6.3 [12], D6.4 [13], D6.5 [14]).

Over the course of the three field training exercises, the PROACTIVE Mobile App increased in overall usability and overall usefulness (Table 8). Along those lines, so did the amount of stars the App received. This helps demonstrate the effectiveness of the iterative, co-creation processes, whereby the written feedback provided by the Observers in the Observer Guide was integrated into the version then released/used for the following exercise. By the end of the PROACTIVE project, it can be said that users find the App easy-to-use, are confident when using the App and stat that they would use the App in a real-life incident. Observers overall also agreed that the App enhances situational awareness of the population in regards to CBRNe incidents.

Table 8 Useability, Usefulness and Rating of the Mobile App

Quality/Exercise	Dortmund	Rieti	Ranst
Useable	3.99	4.58	5.04
Useful	3.90	4.64	5.01
Rating out of 5 stars, where 5 stars are the best	2.57	3.53	4.17

7. FUTURE WORK AND DISCUSSIONS

PROACTIVE CBRNe Mobile App has undergone long process of development, optimisations, updates and new releases and eventually performed as required during the final PROACTIVE exercise. However, the better the developed Mobile App was performing the more recommendations and requests for modifications from the stakeholders were received, especially following the final PROACTIVE exercise and the project final conference. Most of these requests and suggestions are constructive aiming to further improve user experience. We acknowledge that this is a normal process for a digital tool which is supposed to be permanently updated and improved. Furthermore, all these recommended modifications are considered in conjunction with the overall PRAOCTIVE Crisis Communication System, of which MA is one of the core components.

7.1. Future Work on PROACTIVE CBRNe CCS

PROACTIVE CBRNe MA undergone long process of development, optimisations, updates and new releases and eventually performed as required during the final PROACTIVE exercise. However, the better the developed platform was performing the more recommendations and requests for modifications from the stakeholders were received, especially following the final PROACTIVE exercise and the Joint Final Conference for EU funded projects[6]. Most of these requests and suggestions are constructive aiming to improve user experience. Talking into account plans for commercialisation of the developed toolkit after the completion of the project, RINISOFT has summarised all the comments and recommendations and these will be discussed with all PROACTIVE partners and communications toolkit stakeholders. The main additional features of PROACTIVE MA that are considered for the implementation in the next release are as following[7]:

[6] Join Final Conference for EU Funded Projects PROACTIVE, eNOTICE and PANDEM-2, 13-15 of June 2023, Brussels.

[7] Some of these are similar to future work planned for PROACTIVE Collaborative Mobile Platform reported in D4.2. This is expected because the two software tools are part of the same PROACTIVE CBRNe Communications System.

- *Differentiation of the incidents on the "Incident List":* Currently all reported incidents on Incidents list are presented with the identical colours, independently of their category (currently there are 4 categories:

    - *Awaiting Information*
    - *Ongoing*
    - Resolved
    - Unknown Status.

  It was recommended to use different colours for different categories of the incidents and this recommendation will be implemented in the next release.

- *Adding time stamps to "Incident List":* currently all reported incidents are permanently presented in the list of incidents, even though these were resolved. It was suggested to modify "Incident List" by splitting it into 2 options: "Past Incidents" and "Ongoing Incidents". From the software development perspective this makes sense and is relatively simple to implement, however, this may complicate the use of the platform. Therefore, we will follow the established procedure and engage with the PROACTIVE CBRNe Crisis Communications System stakeholders asking for their views.

- *Adaptation of the developed PROACTIVE MA for reporting technical issues on railway tracks:* currently inspection of railway tracks in done according to a schedule by dedicated personnel. Enabling public to report any potential issues will improve safety and efficiency of railway infrastructure.

- *Adaptation of the developed PROACTIVE MA for SMART CITY applications:* it was suggested that the developed PROACTIVE MA could be well accepted (after simple modifications) for citizen engagement in SMART CITY operations (reporting issues with roads, public transport, traffic, mass events, etc).

- *Implementing bi-directional communications within the developed system*: current release support return broadcast channel, allowing collaborative platform to send simultaneous messages to all users of the PROACTIVE MA. However, if different user groups are created, having individual bi-directional communications could help in improving response to the incidents (for example special messages could be sent off-duty LEA officers or medical personnel who are in the area of the incident).

- *Implement the developed system with existing legacy systems*: PROACTIVE CBRNe MA is not the first and only communications system developed. There are a number of existing tools on the market, such as National warning systems, other app, proprietary tools, etc. It will be mutually beneficial for both the PROACTIVE and existing legacy toolkits to enable compliance and integration, eventually contributing to the overall safety during the CBRNe.

The above listed suggestions and recommendations for future work are made by the current and potential stakeholders of the developed PROACTIVE MA and as such, they will be taken very seriously. Some of these recommendations are easy to implement technically but may require additional consultations from ethics points of view. Other recommendations (like integration with existing legacy national warning systems) require close cooperation with the owners of these systems and may have admin and organisation challenges. In implementing these recommendations RINISOFT will follow the established procedure of iterative developed process developed during the project and described earlier. This will ensure that well known danger ***"better is enemy of good"*** will be avoided and future releases will be well accepted by PROACTIVE CBRNe stakeholders.

7.2. Integration with Legacy Systems

Integrating a Crisis Communications System (in our case PROACTIVE CBRNe collaborative platform and mobile app) with national information systems can be a complex process that requires careful planning, collaboration, and adherence to data security and privacy regulations. It requires collaboration between relevant stakeholders, including government agencies, platform developers, data protection officers, and legal experts.

The specific steps and considerations may vary depending on the country and the nature of the information systems involved. As an integral part of its activities in PROACTIVE Project, RINISOFT investigated this topic and identified the following guidelines which will be essential to facilitate integration of PROACTIVE CBRNe MA with national information systems [15,16]:

- ***Identify Objectives and Data Requirements***: Clearly define the objectives of integrating the MA with national information systems. Determine the specific data that needs to be exchanged between the MA and the national systems. This may include demographic information, health records, social services data, or other relevant data. Therefore, don't limit your efforts only to technical development and consider ethics and GDPR.
- ***Comply with Regulations and Standards:*** Ensure that the App complies with all relevant national and international data protection and privacy regulations. This includes obtaining necessary permissions and consent from users and implementing robust security measures to safeguard sensitive data.
- ***Establish Data Sharing Protocols:*** Collaborate with the responsible authorities and information system owners to establish data sharing protocols. Determine the data exchange format, API specifications, and authentication methods to be used.
- ***API Integration:*** Create APIs that allow the MA to communicate with the national information systems securely. APIs provide a standardised way for different systems to exchange data.
- ***User Authentication and Authorisation:*** Implement secure user authentication and authorisation mechanisms to ensure that only authorised individuals can access sensitive information.
- ***Data Encryption***: Use encryption protocols to protect data during transmission and storage. This prevents unauthorised access to sensitive information even if intercepted.
- ***Testing and Validation:*** Thoroughly test the integration to ensure data accuracy, reliability, and consistency. Validate the data exchanged between the PROACTIVE CBRNe MA and the national systems to identify and rectify any issues.

- ***Scalability and Performance:*** Consider the potential increase in PROACTIVE CBRNe MA usage and data flow when integrated with national systems. Ensure that the infrastructure can handle increased traffic and maintain optimal performance.
- ***User Education and Training:*** Provide clear instructions and educational resources to help them understand the process.
- ***Monitoring and Maintenance:*** Continuously monitor the MA's integration with national systems to identify and resolve any technical issues promptly. Stay up-to-date with changes in national information system APIs or policies that may affect the integration.
- ***Data Anonymisation and Aggregation:*** Ensure that individual identities are protected through anonymisation techniques.
- ***Secure Data Deletion:*** Implement a mechanism to securely delete user data from the PROACTIVE CBRNe MA and the national systems if users choose to opt-out or if their data is no longer needed.

A key component in planning such an integration includes also planning verification of the developed solution, to ensure that the integration is secure, compliant with regulations, and functions as intended. RINISOFT used best practices developed during PROACTIVE project and suggested the following steps for future integration:

- ***Security Audit:*** Conduct a comprehensive security audit of both the PROACTIVE CBRNe MA and the national information systems. This audit should identify potential vulnerabilities and assess the overall security posture of the systems involved. Since PROACTIVE MA already been evaluated for "Secure by Design", this should make the process of security audit slightly easier.
- ***Data Privacy Assessment:*** Perform a thorough data privacy assessment to identify the types of data that will be exchanged between the MA and national systems. Ensure that the MA complies with relevant data protection regulations and that user consent is obtained where necessary. Since PROACTIVE CBRNe MA already was evaluated by ETICAS for compliance with data protection regulations, this should make this step slightly easier.
- ***API Testing:*** Verify the functionality and security of the APIs that facilitate data exchange between the PROACTIVE CBRNe MA and national systems. Test various scenarios to ensure data is transmitted accurately and securely.
- ***Authentication and Authorisation Testing:*** Test the authentication and authorisation mechanisms to ensure that only authorised users can access the MA and the relevant data within the national systems.
- ***Data Accuracy and Integrity Testing:*** Verify the accuracy and integrity of data exchanged between the PROACTIVE CBRNe MA and national systems. Data should be consistent and error-free to ensure proper functioning of the platform's features.
- ***Performance Testing:*** Test the performance of the MA and the integration under various load conditions to ensure that it can handle the expected user traffic without significant issues.
- ***Compliance Verification:*** Ensure that the integration adheres to all relevant regulations and standards, such as data protection laws and industry-specific requirements.

- ***User Acceptance Testing (UAT):*** Conduct UAT with real users or representatives from the target user group to gather feedback on the platform's usability, accessibility, and overall functionality.
- ***Monitoring and Logging:*** Implement robust monitoring and logging mechanisms to track data exchanges, detect anomalies, and troubleshoot any issues that may arise after deployment.
- ***Disaster Recovery and Redundancy Testing:*** Verify that the integration includes adequate disaster recovery measures and redundancy protocols to minimise the risk of data loss or service interruptions.
- ***Legal Review:*** Seek legal review to ensure that the integration complies with all relevant laws, contracts, and agreements related to data sharing and use.
- ***Documentation:*** Throughout the verification process, document each step thoroughly and address any issues that arise promptly. Collaboration between the MA development team, national system owners, data protection officers, security experts, and legal advisors is crucial to ensure a successful and compliant integration.

The verification process described above typically involves multiple stakeholders with different areas of expertise. These stakeholders are listed in the table below.

Table 9 Stakeholders of Verification Process

Stakeholder	Role in Verification
Development Team	The development team is responsible for ensuring that the App meets the technical requirements for integration. They should conduct security testing, API testing, and data accuracy checks on the app's side of the integration.
Government Authorities and System Owners	The government authorities or agencies responsible for the national information systems are essential stakeholders in the verification process. They oversee the data being shared and must verify that the integration aligns with their system's security and privacy standards.
Data Protection Officers	DPOs play a critical role in assessing and ensuring data privacy compliance. They can review the MA's data privacy policies, consent mechanisms, and data handling practices to verify that user data is appropriately protected.
Security Experts	Independent security experts or security teams within relevant organisations can conduct security audits and penetration testing to identify vulnerabilities and weaknesses in the developed PROACTIVE CBRNe MA and the integration process.
User Representatives	Representatives from the target user group during user acceptance testing
Legal Advisors	Legal advisors help ensure that the integration complies with all relevant laws, regulations, contracts, and agreements related to data sharing and use.
Quality Assurance Team	A dedicated QA team can conduct comprehensive testing, including functional testing, performance testing, and

	regression testing, to ensure the PROACTIVE CBRNe MA functions as expected after the integration
Infrastructure and IT Teams	The IT teams managing the national information systems should verify that the MA's integration aligns with their system's architecture and requirements.

As shown in this section, integration of the PROACTIVE CBRNe MA is desirable but complex task. It requires multi-dimensional scope of activities of which technical development is important but only one of the components. In addition to steps outlined above, one more activity needs to be considered – promotion of the integrated solution to the general public. This requires a well-thought-out marketing and communication strategy which need to be developed jointly with all the stakeholders. The success of integrated PROACTIVE CBRNe MA relies on understanding the needs of the target audience and effectively communicating how the platform addresses those needs. Tailoring the promotion strategy to the specific characteristics and preferences of the citizens will increase the likelihood of PROACTIVE CBRNe MA adoption and usage.

8. CONCLUSIONS

This document has delved into the multifaceted process of creating mobile applications, highlighting the intricate stages from ideation to deployment of the PROACTIVE CBRNe MA. This mobile App was developed as an integral part of the overall PROACTIVE CBRNe Crisis Communication System and allows exchange of best practice among LEAs provides valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRNe activities and help consolidate the EU Action Plan to enhance preparedness for CBRNe threats.

The design and development process required creativity, coding prowess, and user-centred design principles, which utilised the best practice approach, ensuring that the final product meets all the requirements requested by the stakeholders. Throughout this report, we have explored the essential components of mobile App development, including UI/UX design, backend development, testing methodologies, and security considerations. Special emphases were placed on ensuring that the developed web platform meet the need of vulnerable citizens and in "*Secure by Design*".

A key component on the overall design and development process was verification process, which included by objective (technical) and subjective (questionnaire-based) verifications. We are pleased to report that technical (objective) verification showed compliance with the developed requirements while subjective (questionnaire-based) verification shown positive acceptance by the stakeholders.

Constructive recommendations from these verifications will be implemented in the next release of the PROACTIVE CBRNe mobile App as an integral part of the commercial exploitation.

9. REFERENCES

1. PROACTIVE D4.1 – Report on the High-level Architecture design including an interface control document (2021). https://proactive-h2020.eu/wp-content/uploads/2021/04/PROACTIVE_20210312_D4.1_V6_RINI_Report-on-the-high-level-architecture-design_revised.pdf

2. Havârneanu, G.M., Petersen, L., & McCrone, N. (2022). Stakeholder Engagement Model to facilitate the uptake by end users of Crisis Communication Systems. In: G. Markarian, R. Karlovic, H. Nitsch, & K. Chandramouli (Eds). *Security Technologies and Social Implications.* IEEE Press. Wiley. https://doi.org/10.1002/9781119834175.ch8

3. Clegg, Dai; Barker, Richard (1994). *Case Method Fast-Track: A RAD Approach*. Addison-Wesley.

4. Petersen, L., Havârneanu, G., McCrone, N., Markarian, G. (2023). Practitioner Perspectives of the PROACTIVE CBRNe Disaster App. In: Radianti, J., Dokas, I., Lalone, N. & Deepak, K. (Eds) ISCRAM 2023 Conference Proceedings – 20th International ISCRAM Conference. pp 13-19 http://idl.iscram.org/files/petersen/2023/2502_Petersen_etal2023.pdf

5. Petersen, L., Havârneanu, G.M., McCrone, N., Markarian, Burlin, A., & Johansson, P. (2022). CBRNe, a universally designed app for that? In Grace, R., Baharmand, H. (Eds). ISCRAM 2022 Conference Proceedings – 19th International Conference on Information Systems for Crisis Response and Management, p. 836-846, ISSN 2411-3387. http://idl.iscram.org/files/laurapetersen/2022/2459_LauraPetersen_etal2022.pdf

6. PROACTIVE D8.2 – Legal and acceptability recommendations for PROACTIVE toolkit (2021). https://proactive-h2020.eu/wp-content/uploads/2021/04/PROACTIVE_20210315_D8.2_V5_ETICAS_Legal-and-acceptability-recommendations_revised.pdf

7. PROACTIVE D5.2 – Final Pre-Incident Public Information Materials for CBRNe terrorism (2023). https://proactive-h2020.eu/wp-content/uploads/2023/04/PROACTIVE_20230228_D5.2_V4_UKHSA_Final-Pre-Incident-Public-Information-Materials.pdf

8. Davis, I. (2008). What Are The Benefits of MVC?. Internet Alchemy. http://blog.iandavis.com/2008/12/what-are-the-benefits-of-mvc/ Retrieved 2016-11-29.

9. Potel M. (1996). http://www.wildcrest.com/Potel/Portfolio/mvp.pdf

10. Fowler, M. (2004). The Presentation Model Design Pattern. http://martinfowler.com/eaaDev/PresentationModel.html

11. PROACTIVE D4.2 – Developed Web Collaborative platform (2023)

12. PROACTIVE D6.3 Report on the first field exercise and evaluation workshop (2022). https://proactive-h2020.eu/wp-content/uploads/2022/07/PROACTIVE_20220630_D6.3_V4_DHPol_Dortmund-Field-Exercise.pdf

13. PROACTIVE D6.4 Report on the second field exercise and evaluation workshop (2023). https://proactive-h2020.eu/wp-content/uploads/2023/02/PROACTIVE_20230131_D6.4_V5_CBRNE_Rieti-Field-Exercise.pdf

14. PROACTIVE D6.5 Report on the third field exercise and evaluation workshop (2023). https://proactive-h2020.eu/wp-content/uploads/2023/08/PROACTIVE_20230731_D6.5_V5_UMU_Ranst-Field-Exercise.pdf

15. FEMA (2023). Integrated Public Alert & Warning System. https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system (accessed July 2023)

16. CRTC (2014). http://www.crtc.gc.ca/eng/archive/2014/2014-444.htm (accessed July 2023)

10. ANNEX 1A – CORE REQUIREMENTS

Core Requirements	
Graphic User Interface	Simple design reflecting PROACTIVE branding. Accessibility across web collaborative platform and both Mobile Applications
Direct Messaging	The ability for LEAs and Security Policy makers to interact privately. The ability for citizens to send direct messages will vary between scenarios
Forums	Open discussions between all stakeholders
Registration	Not mandatory – registering will increase level of access rights
Legal & Ethical Requirements	Working with ETICAS and CBRNE, GDPR, disclaimers and consent forms will be factored into the system
Notification of Incidents	Notify LEAs of an incident using a map-based system
Data Storage	Secure storage of information input to system
Geo-Location	The ability for the system to recognise the location of an incident(s)
Information Sharing	Ability to share pre-incident information with all users in multiple formats (text, video, audio)
Missing Loved Ones	Ability to locate humans and pets during an incident
Contact Information	List of organisations relevant to vulnerable groups

11. ANNEX 1B – FUNCTIONAL REQUIREMENTS

Functionality Requirements for Field Exercises	
Inter-Agency Information Sharing	The ability to converse directly with relevant stakeholders to discuss operational aspects in terms of information sharing
Pre-Incident Information	Information from T5.1 will be available in the system for users to reference
Post Incident Information	Information post incident to be provided to stakeholders, specific to the scenario exercise as a lesson learnt.
Links to Available National Apps	Countries with existing Apps for crises events will have the link signposted in the PROACTIVE platform
Notification Alerts	Live notifications to be provided by LEAs at all stages of the incident
Existing News Feeds	News feeds from the relevant countries/ areas will be linked to the PROACTIVE Mobile Application, to create a central hub for information
Data Analysis	LEAs will have access to data, specifically number of users on the platform and at what stages the platform was used etc.