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

Deliverable D5.4

Developed Mobile App for Vulnerable Citizens

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

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**ulnerabl**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 Mobile App for Vulnerable Citizens
Work Package	WP5
Date of the document	31/08/2023
Version of the document	04
Responsible Partner	RINISOFT
Reviewing Partner(s)	CBRNE, ETICAS, DB, UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	01/08/2023	First draft sent to consortium for review
02	11/08/2023	Draft with comments from reviewing partners
03	21/08/2023	Final Draft
04	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

List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Server
CBRNe	Chemical, Biological, Radiological, Nuclear, and explosive
CSAB	Civil Society Advisory Board
CCS	Crisis Communication System
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
MoSCoW	Must have, Should have, Could have, Won't have
MVC	Model-View-Controller
MVP	Model-View-Presenter
MVVM	Model-View-View-Model
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

Executive summary

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

The development focused on ensuring 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 for vulnerable citizens helps to improve the efficiency of the communication between LEAs, Policy Makers and Citizens, including those who may be vulnerable, with a particular focus on information sharing and usability. 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 CCS, which may interact by pushing/pulling information to or from the PROACTIVE CCS.

Input from WP1, WP2, WP3, WP4, WP6 and WP8 has been reviewed to determine the needs and gaps of the users in terms of current public perceptions relating to CBRNe incidents & mobile apps. The research completed in WP1 fed into the key engagement tasks in WP2 and WP3, while technical development of the PROACTIVE CCS took place in WP4 & WP5. The CCS was then tested in WP6. Feedbacks received from the three PROACTIVE field exercises helped to improve the developed CCS, 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 emphasis was made to ensure compliance with "Secure by Design" requirements.

The developed mobile app for vulnerable citizens will remain active and usable for the 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

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, the PROACTIVE project 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 project.

One of the tools resulted from the PROACTIVE project is a CBRNe Crisis Communications System (CCS), 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; and
- a Mobile App for Vulnerable Citizens.

This PROACTIVE CBRNe Mobile App for Vulnerable Citizens was developed within WP5 of the project.

1.2. Objectives of WP5

The main objectives of WP5 were defined in the original project proposal and are dedicated to the development of one essential component of the PROACTIVE CBRNe CCS: the toolkit for civil society organisations, which includes a mobile app adapted to various vulnerable citizen categories and pre-incident public information material. These provide valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRN activities and help consolidate the EU Action Plan to enhance preparedness for CBRN threats. As an integral part of these activities, the objectives of WP5 also included:

1. Content selected and adapted for use in the PROACTIVE guidance toolkit.
2. Pre-incident public information materials for CBRNe terrorism designed, developed, and tested during the PROACTIVE field exercises.
3. A clearly specified mobile app for vulnerable citizens, designed to reduce inequalities and address the specific requirements of vulnerable citizens. While key accessibility

functionality will be ensured for vulnerable citizens, the App will be targeted at civilians.

4. Develop the comprehensive technological components supporting the PROACTIVE CBRNe Crisis Communications System.

5. Design the complete PROACTIVE CBRNe Crisis Communications System (set of tools and supporting technologies), ensuring modularity, flexibility adaptability, scalability, usability and robustness,

6. Build technological tools facilitating communication and cooperation between LEAs and vulnerable citizens during CBRNe crisis, exploiting the use of mobile technologies and bi-directional communication.

7. Integrate, test and validate the developed mobile app for vulnerable citizens.

1.3. Objectives of D5.4

The key objective of D5.4 is to report on the design, development, implementation, testing and validation of the PROACTIVE CBRNe mobile app for vulnerable citizens. 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 Vulnerable Citizens is the main output of D5.4.

While this deliverable focuses specifically on the development of the Mobile App for Vulnerable Citizens, it is important to note that the app is one component of the overall PROACTIVE Crisis Communication System (CCS). 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 the PROACTIVE project in consultation with all potential stakeholders:

- **User Experience**: The CCS should be designed with the user in mind, with an intuitive and user-friendly interface. The user should be able to easily navigate the CCS, access information, and complete tasks.
- **Functionality**: The CCS should have all the necessary features and functionalities, such as account management, and access to content and services.
- **Security**: The CCS should be designed with security in mind, with measures in place to protect user data and prevent unauthorised access. This includes using encryption, secure authentication mechanisms, and other security features.
- **Compatibility**: The CCS should be compatible with different devices and operating systems, and should work seamlessly with both iOS and Android devices.
- **Scalability**: The CCS 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 CCS can handle increasing traffic and usage.
- **Market Appearance**: The CCS 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. INTERACTIONS WITH OTHER WORKPACKAGES

Design and development of the PROACTIVE CBRNe Mobile App for Vulnerable Citizens was predominantly the responsibility of WP5.

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 WP3, 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 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 Practitioners and the Web Collaborative Platform (WP4);
- 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.

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

Figure 1 below provides graphical illustration of the collaboration and interaction of WP5 with other WPs of PROACTIVE project.

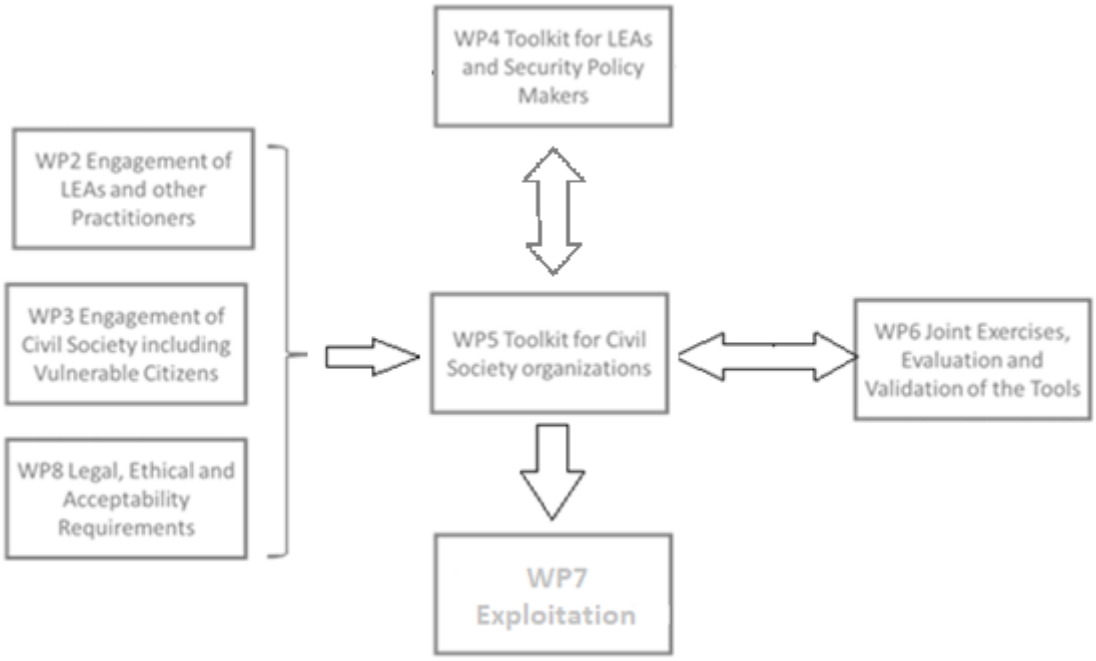

Figure 1 WP5 Collaboration and Interaction With Other WPs of PROACTIVE

As it follows from this figure, for the purpose of this deliverable D5.4, research completed in each of the highlighted Work Packages, has been reviewed and analysed from the perspective of the PROACTIVE Mobile App for Vulnerable Citizens.

Thanks to this iterative, co-creation process with many feedback loops and interactions with other WPs, 20 versions[2] 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).

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

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 for Vulnerable Citizens was developed and released for initial testing and verification by the PROACTIVE consortium as a web application. 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 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 CCS (and therefore the Mobile App for Vulnerable Citizens 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 Workshop 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 PROACTIVE CCS quality perception within each group of users and provide

a baseline for how the rating is going to change over time. These results also set a benchmark for the developers, with am aim to improve the overall rating at the end of the project.

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

In addition to the two workshops 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 Functional Requirements

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

Once gathered, the MoSCoW findings were translated to PROACTIVE CCS 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. MoSCoW findings Categorised as Universal Design Principles

The concept of universal design takes into account the fact that the general public is a diverse group of people, including vulnerable groups, and is based on seven principles as elaborated by Connell et al. (1997): equitable use, flexibility in use, simple and intuitive use, perceptible information, tolerance for error, low physical effort and size and space for approach and use. In Petersen et al., 2022 [5], the MoSCoW requirements from the CSAB were categorised as belonging to one or several Universal Design principles, and are reproduced here as Table 5.

Table 5 CSAB MoSCoW requirements categorised by Universal Design Principle

Universal Design / MoSCoW	**Equitable use**	**Flexibility in use**	**Simple and intuitive use**	**Perceptible information**
Must have	• Audio information • Colour blind compatibility • Compliance with international standards for accessibility (e.g., WCAG 2.1) • International Sign Language • Text-to-speech	• Ability to zoom while ensuring high image quality • An Easy Read option • A high contrast option • Translation	• A less chaotic interface • An uncomplicated structure • Bigger text (font size) • Bigger buttons, icons and symbols	• Ability to zoom while ensuring high image quality • An Easy Read option • Audio information • Basic wording • Bigger text (font size) • Bigger buttons, icons and symbols • A high contrast option • Pictures, pictograms • Specific information on what is happening and how to act Translation

				• Text-to-speech
Should have	• Less text	• Less reliance on maps	• Less confusing icons (e.g., contact icon should be an envelope, not an arrow) • Links to other useful apps • A search button • Ways to contact relatives/loved ones	• A search button
Could have			• Social media integration (post information to a given social media account)	

Overall, the iterative, co-creation process has allowed for the Mobile App to consider 4 out of the 7 Universal Design principles, and solutions for the remaining three have also been implemented.

In order to achieve the Universal Design principle of equitable use, the PROACTIVE app has been designed as a single app for all users (meaning that there aren't different versions to download to accommodate any given vulnerability). This has been done by ensuring that the app uses basic wording and less text. This increases accessibility for those with intellectual disabilities and children as well as any citizen who might use the app during a CBRNe incident and have a functional need support. The app applies a colourblind friendly colour palette, ensuring compliance with text-to-speech readers, avoiding flashing images, and has information materials that are supported with audio. As such, users who are colourblind, blind or partially sighted, epileptic or hearing-impaired can all use the app equitably. For compliance with text-to-speech readers, the formatting of headings, lists, graphics and logos, sequences and hierarchies was completed. Compatibility was tested using a screen reader and a keyboard. When it comes to content, the data, whether that be pre-incident information materials or a list of local hospitals, is available as plain text built into the web page as well as a downloadable document.

Flexibility in use has been achieved in the app redesign by embedding colour contrast ratios in the HTML coding in order to provide a high contrast option. Furthermore, the reliance on the interactive

map to find and report incidents has been reduced and alternative options for using these features have been implemented.

Simple and intuitive use has been achieved through the homepage reorganisation, as described above. Many of the updates in the app redesign that are relevant for the universal design principles of equitable use and flexibility of use overlap with the principle of perceptible information.

The principle of tolerance for error is addressed via the “back” and/or “undo” buttons/controls. To ensure low physical effort, the PROACTIVE app has minimised clicks (part of the requirement less chaotic interface) and has ensured compatibility with assistive technologies (part of requirement text-to-speech). Similarly, the principle of size and space for use is being addressed by ensuring that the app is compatible with multiple devices and is available as both a web-platform and a smartphone application, aka the PROACTIVE CCS. This allows the end-user to choose the size and space of the device.

4.6. 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. 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 FOR VULNERABLE CITIZENS DEVELOPMENT

5.1. General Approach

The PROACTIVE CBRNe Mobile App for Vulnerable Citizens was integral part of the PROACTIVE CBRNe Crisis Communications Systems development. The core of the development was 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.

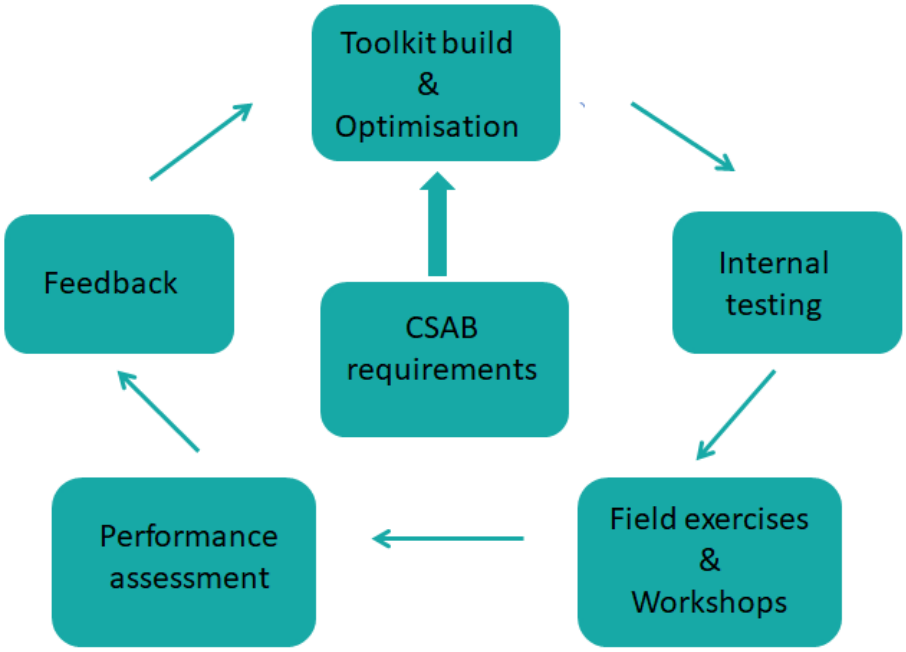

Figure 2 Iterative approach to development

Similar to the Mobile App for Practitioners as described in D4.3 [9], initially the Mobile App for Vulnerable Citizens development was focused on the CSAB requirements, then the PSAB and then the final exercise amalgamated the two. The final phase of the development was dedicated to the incorporation of the currently available content, effectively showcasing the usability and purpose of the developed app during and post exercises. This produced further recommendations for optimisation, as an integral part of the overall iterative process.

5.2. Architecture

As mentioned earlier, the PROACTIVE CBRNe Mobile App for Vulnerable Citizens is an integral part of the PROACTIVE CBRNe CCS, therefore its development was closely correlated with the development of all three components of the CCS. Figure 3 below illustrates the block diagram of the

overall communications system and highlights the interaction of the Mobile App with all components of the overall system.

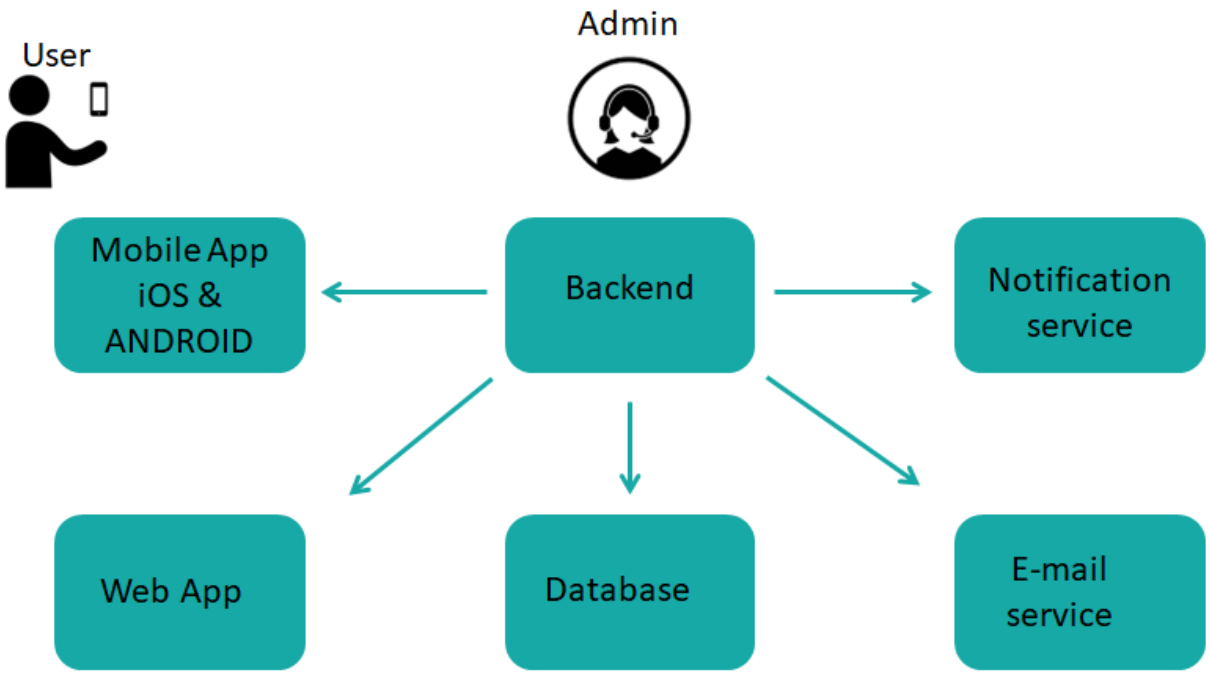

Figure 3 Mobile App as an Integral part of the PROACTIVE CBRNe Communications System

To ensure that the Mobile App is accepted and used by the community, Table 6 below outlines the most important design principles which RINISOFT applied when developing this Mobile App.

Table 6 Design Principles for Mobile App Development

Principle	Implementation
Accessibility	Ensure that the app is accessible to users with disabilities. This means providing support for screen readers, offering adjustable font sizes and colour contrast, and implementing keyboard navigation for those who may have difficulties using touch gestures.
Simplicity and Intuitiveness	Keep the app design simple and intuitive, with clear and straightforward navigation. Avoid cluttering the interface with unnecessary elements and use easily recognizable icons and symbols.
Clear and Readable Text	Use plain language and clear, easy-to-read fonts. Avoid jargon and complicated terminologies. If the app provides important information, ensure it is presented in a digestible format.
Large Tap Targets	Consider users who may have motor skill impairments or use larger tap targets that are easy to tap. This reduces the risk of accidental taps and improves overall usability.

Flexibility in Input Methods	Accommodate different input methods, such as touch, tap, voice commands, or keyboard input, to cater to users with varying abilities.
Feedback and Confirmation	Provide clear and concise feedback when users perform actions, such as button clicks or form submissions, to assure them that their input has been received.
Personalisation	Allow users to customise the app to their preferences, such as font size, colour schemes, or settings for notifications. This helps accommodate individual needs.
Safety and Security	For vulnerable users, data privacy and security are crucial. Clearly explain how user data will be used and stored and implement robust security measures.
Offline Functionality	Consider users who may have limited access to the internet or face connectivity issues. Ensure essential features of the app can be accessed offline if possible.
Testing with the Target Audience	Involve the target user group in the design and testing process. Conduct usability testing with representative users to gather feedback and make improvements.
Training and Support	Include clear instructions and onboarding processes to help users understand how to use the app effectively. Additionally, offer accessible customer support channels if users encounter issues.
Collaboration with Advocacy Groups	Collaborate with organisations and advocacy groups that focus on vulnerable populations. Their insights and feedback can be invaluable in improving the app's design.

As emphasised throughout this report, when developing the Mobile App, RINISOFT aimed to minimise the complexity of the overall CCS. Therefore, block diagram of the Mobile App for Vulnerable Citizens was selected to be the same as for the Mobile App for Practitioners, aligning 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, a MVP architecture as described in D4.3 [9] was adopted for the Mobile App for Vulnerable Citizens. The generic block diagram of the MVP (Model-View-Presenter) [8] architecture is shown in Figure 4.

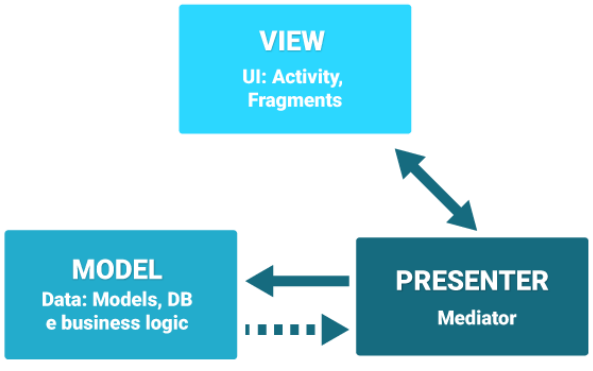

Figure 4 Generic Diagram of the MVP architecture

The key components of this diagram are as follows:

- **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 from 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 the MVP follows general steps shown in Figure 5, below.

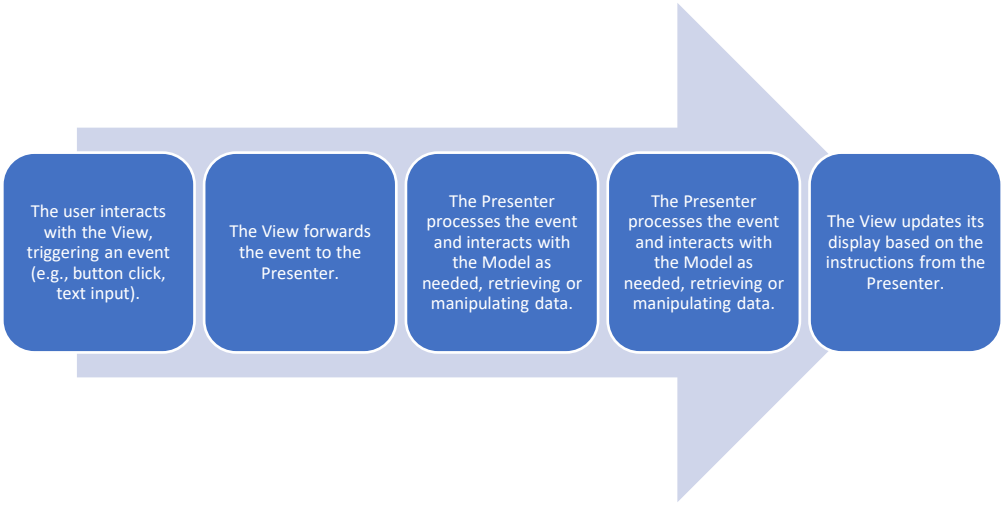

Figure 5 Flow of Data and Events in the MVP

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 imitated 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 the PROACTIVE CCS.

When developing the PROACTIVE CCS we envisaged the worst-case scenario when no public communications infrastructure will be available during a CBRNe incident. Therefore, the developed Mobile App is designed with a unique feature to support reliable and robust operation of the

PROACTIVE CCS over private and restricted networks, such as mesh networks established by the First Responders as an integral part of incident response (D4.2). **This feature makes the developed CCS unique in comparison with other existing solutions (WhatsApp, Facebook, etc), which require an INTERNET connection for their operations.**

5.3. Development Tools

As mentioned earlier, throughout the PROACTIVE project lifespan, over 20 versions of the Mobile App were developed and released, utilising the iterative development process adopted by the project. When developing the PROACTIVE Mobile App[3] using the MVP architecture, RINISOFT used various tools and frameworks to aid in the development process. As the developed Mobile App was required to work on both ANDROIND and iOS, and taking into account plans for post-project commercialisation, the decision was made to have two separate developments (for 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 managing 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.

[3] Both for practitioner and vulnerable citizens

- *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 managing source code changes, collaborating with a team, and tracking project history for ANDROIND and iOS versions of the MA.

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

An important component of the design process was testing various versions (releases) with targeted end-users. Following the recommendations from these advisory groups, the following additional testing steps were incorporated within the development process:

- **Usability Testing with Vulnerable Users**: Involve members of the vulnerable population for which the app is intended in usability testing. Observe how they interact with the app, gather feedback, and make necessary improvements based on their feedback.

- **Accessibility Testing**: Conduct accessibility testing with individuals who have disabilities to ensure that the app can be used by people with varying abilities. Check for compatibility with screen readers, keyboard navigation, and other assistive technologies.

- **Cognitive Testing**: Assess the app's cognitive load on users with limited cognitive abilities or conditions like dementia. Ensure that the app's navigation and interfaces are clear and straightforward.

- **Language and Literacy Testing**: As the Mobile App targets users with limited literacy skills, validate that the language used is simple, and instructions are easily understandable. Conduct testing with individuals representing different literacy levels.

- **User Interface (UI) and User Experience (UX) Testing**: Evaluate the app's UI and UX design to ensure that it is intuitive, consistent, and engaging for vulnerable users.

- **Feedback Mechanisms**: Implement feedback mechanisms within the app to allow users to provide comments, suggestions, or report issues easily.

- **Performance and Reliability Testing**: Verify that the app performs well and is reliable even on devices with limited resources or unstable network conditions.

- **Security Testing**: Ensure the app incorporates appropriate security measures to protect users' data and privacy.

- **Inclusive Language and Visuals**: Review the app's content and visuals to ensure they are inclusive and respectful to all users.

- **Error Handling and Recovery**: Test how the app handles errors and guide users through the recovery process in a clear and supportive manner.

- **Testing in Real-World Contexts**: Test the app in real-world scenarios to see how it performs in environments where vulnerable users are likely to interact with it.

- **Compliance Testing**: Verify that the app adheres to all relevant regulations and standards, particularly those related to data privacy and accessibility.

- **Continuous Iteration**: Based on user feedback and testing results, iterate and improve the app to better meet the needs of users.

5.4. System Functionality

The key component in the development of Mobile App 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 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 the Presenter handles those actions appropriately.

- Test the Model: Assess the Model's functionality by verifying it correctly handles data retrieval, manipulation, and storage operations.

- Test the Interaction between Components: Evaluate the interaction and communication between View, Presenter, and Model and verify 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 the app functions as intended.

- Test Edge Cases and Error Handling: Perform testing with various edge cases, boundary conditions, and error scenarios, ensuring the app handles these situations gracefully, providing appropriate error messages or fallback behaviour.

- Gather User Feedback: Once functional testing is completed, gather feedback from PROACTIVE end-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 Mobile App and set up objective technical criteria for continuous improvements. Despite all the restrictions imposed by COVID-19, the developed Mobile App was tested during all three field exercises. This involved representatives from the vulnerable population and their feedback was used in the PROACTIVE project iterative process. Testing with real users from the target audience was invaluable in identifying issues and making the PROACTIVE Mobile App more effective and inclusive. When developing the Mobile App, we took a more challenging but rewarding approach when designing an Mobile App for vulnerable people where a one-size-fits-all approach does not always work, as the needs and abilities within this group can be diverse. Throughput the project we engaged with the relevant groups and asked for their feedback as an integral part of PROACTIVE iterative development approach. By iterating and improving the app based on user input and emerging accessibility standards, we are pleased to report that it was well accepted by the vulnerable groups participating the final exercise.

5.5. Security

The PROACTIVE CBRNe CCS is designed to be compliant with the concept of “Secure by Design.” Although many steps in ensuring compliance of the developed Mobile App with the “Secure by Design” concept were similar to the processes described in D4.2 for the Web Collaborative Platform [11], ensuring compliance with "Secure by Design" principle in an MVP PROACTIVE Mobile App involved additional security practices in the development process, which are elaborated in D4.3 [9]. The same process that was used for the Mobile App for Practitioners (D4.3) was applied to the development of the Mobile App for Vulnerable Citizens.

5.6. Interoperability

Once the Mobile App for Vulnerable Citizens was developed and tested, the development process still wasn’t completed as the developed Mobile App needed to be integrated with the PROACTIVE CBRNe Web Collaborative Platform (D4.2) and with the Mobile App for Practitioners (D4.3). This required a thoughtful approach to ensure a seamless and inclusive user experience for all users. In addition, RINISOFT wanted to ensure the developed PROACTIVE Crisis Communications System could be easily supported during the commercial exploitation phase. Therefore, at the core of our technical development we adopted the Universal Core Functionality (UCF) approach, which represents a conceptual idea of essential and foundational capabilities commonly found in various software applications. These functionalities are considered crucial, enabling the basic operations and interactions within various domains. The UCF is a result of collaborative efforts and continuous

innovation from the technology community, aiming to make computing systems more capable, reliable, and efficient. These functionalities are listed in Table 7, below.

Table 7 Main Principles of UFC

Functionality	Description
Data Storage and Retrieval	The ability to store and retrieve data efficiently is fundamental to almost all digital systems. This includes databases, file systems, cloud storage, and any other mechanism that allows information to be stored and accessed.
User Interface	An interface that enables users to interact with the system or application can be graphical (GUI) or text based (CLI) and allows users to input commands or data while receiving outputs or feedback from the system.
Networking and Connectivity	The capability to connect and communicate with other devices or systems, either locally or over a network (e.g., the internet). Networking is vital for sharing data, accessing remote resources, and enabling collaboration.
Processing and Computation	The ability to perform calculations, execute instructions, and process data is the core functionality of any computing system.
Security and Access Control	Ensuring the protection of data, resources, and user privacy through authentication, authorisation, encryption, and other security measures. This functionality is essential to safeguard sensitive information and prevent unauthorised access.
Input/Output (I/O) Handling	Managing the communication between the system and external devices, allows users to interact with the system and receive information through various peripherals.
Error Handling	The capability to identify, report, and manage errors or exceptions that occur during the system's operation. Proper error handling ensures the system can recover gracefully from unexpected issues.
Task Scheduling and Multitasking	The ability to manage multiple tasks or processes concurrently, prioritising and allocating system resources efficiently to ensure smooth operation and responsiveness.
Timekeeping and Synchronisation	The system's ability to keep track of time accurately and synchronise activities, particularly crucial in distributed and real-time systems.
Configuration and Settings Management	Allowing users to customise and configure various aspects of the system or application to suit their preferences and requirements.

We commenced our development of the Mobile App for Practitioners and for Vulnerable Citizens core app with universal functionality catering to the needs of both vulnerable users and the general population. This core app includes essential features and services relevant to all users. Once the core app was defined the following additional points were taken into consideration as summarised in Table 8, below.

Table 8 Additional Points for Consideration

Principle	Implementation
Accessibility Settings	Implement accessibility settings within the app that allow users to adjust various aspects, such as font size, colour contrast, and input methods. This empowers vulnerable users to customise the app based on their individual needs.
User Profiles	Create user profiles within the app, where users can specify their preferences and accessibility requirements. Different user profiles can be established to cater to specific needs.
Role-Based Access:	Implement role-based access control to determine which features and contents are available to different user groups. This allows to provide a personalised experience for vulnerable users while not limiting access to other citizens.
Web Platform Integration:	Develop a web platform that complements the app's functionality. The web platform should mirror the core features of the app and be accessible to all users through web browsers on different devices.
User Accounts and Synchronisation:	Allow users to create accounts that can be used across both the app and the web platform. Ensure user data is securely synchronised between the app and the web platform.
Responsive Design	Ensure both the app and the web platform have a responsive design that adapts to various screen sizes, making them accessible on smartphones, tablets, and desktops.
Data Privacy and Security	Implement robust data privacy and security measures to protect user data, especially when synchronising between the app and the web platform.
Testing and User Feedback	Conduct extensive testing with representatives from both the vulnerable user group and the general population. Gather feedback to make necessary adjustments and improvements.
Continuous Updates and Maintenance:	Regularly update and maintain both the app and the web platform to ensure they remain compatible with evolving technologies and user needs.
Education and Support	Provide clear instructions and educational resources within the app and on the web platform to guide users on how to use the integrated system effectively.
User Outreach and Communication	Utilise various communication channels, including social media, newsletters, and community engagement, to inform users about the integration and its benefits.

Another unique feature of the developed PROACTIVE CBRNe CCS is interoperability with the existing legacy systems. Furthermore, the developed communications system is designed as future proofed, allowing the integration of systems in the future.

To ensure interoperability between the PROACTIVE Mobile App for Vulnerable Citizens 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 familiar with the legacy systems. This was followed by the definition of the specific integration requirements between the PROACTIVE Mobile App for Vulnerable Citizens and the legacy systems, including identifying the data exchange needs, authentication mechanisms, and workflows that need to be supported.

5.7. Installation

As required, PROACTIVE Mobile App 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 Mobile App

a) GooglePlay b) AppleStore c) Universal

After downloading the Mobile App, the users may choose to register by providing their e-mail details. Once the address is verified, the user get access to the additional feature of “Report an Incident” on the PROACTIVE Mobile App.

5.8. Graphic User Interface

5.8.1. Landing Page

The PROACTIVE Mobile App GUI starts with the following landing page, as seen in Figure 7:

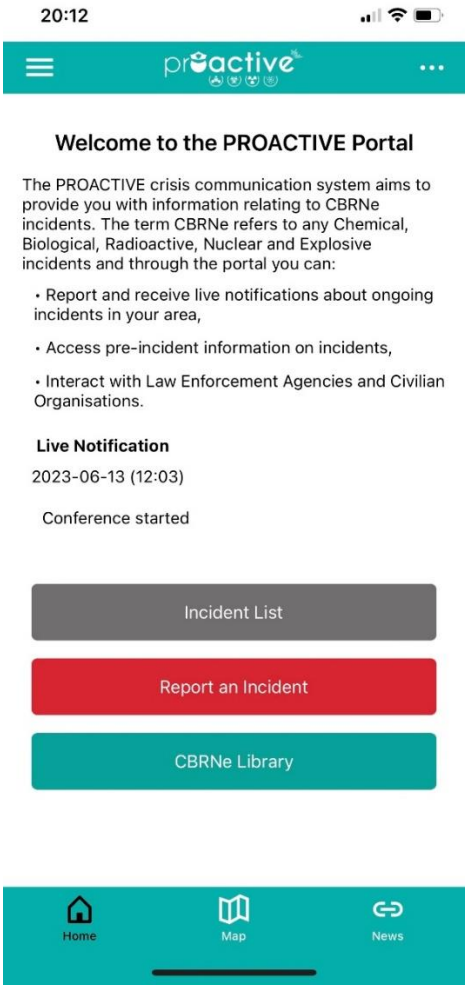

Figure 7 Landing Page

As requested in initial requirements, the developed PROACTIVE CBRNe Mobile App GUI supports:

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

5.8.2. Incident Map Page

This is the page on the app 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, Figure 8:

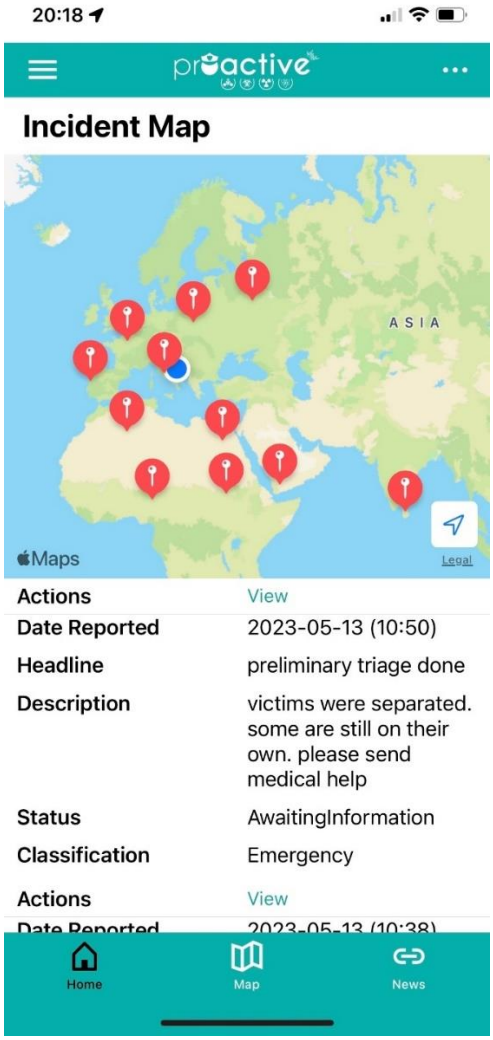

Figure 8 Incident Map

5.8.3. Report an Incident Page

When a registered user clicks on the “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 shown in Figure 9, below:

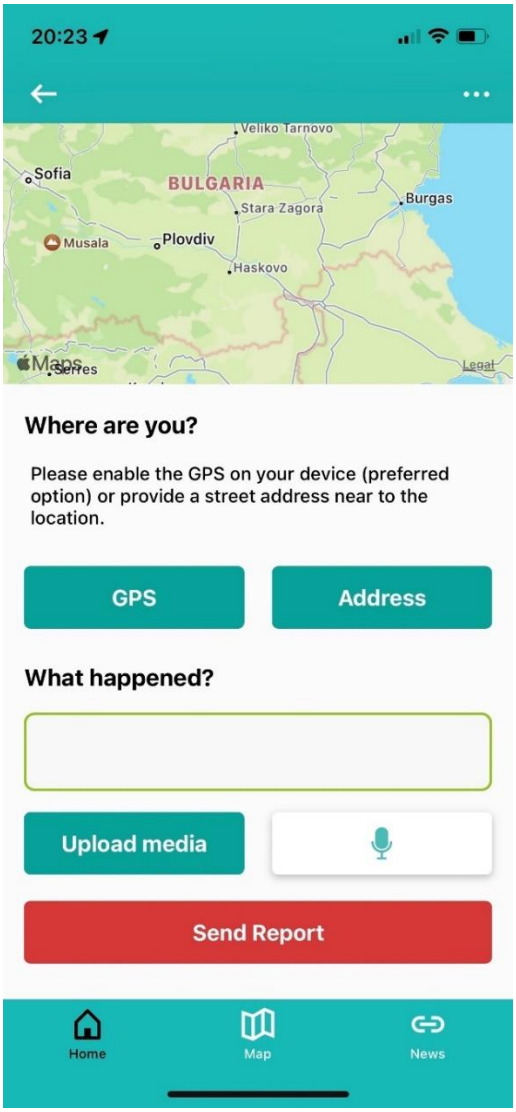

Figure 9 Report an Incident

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

5.8.4. CBRNe Library Page

The 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, seen in Figure 10.

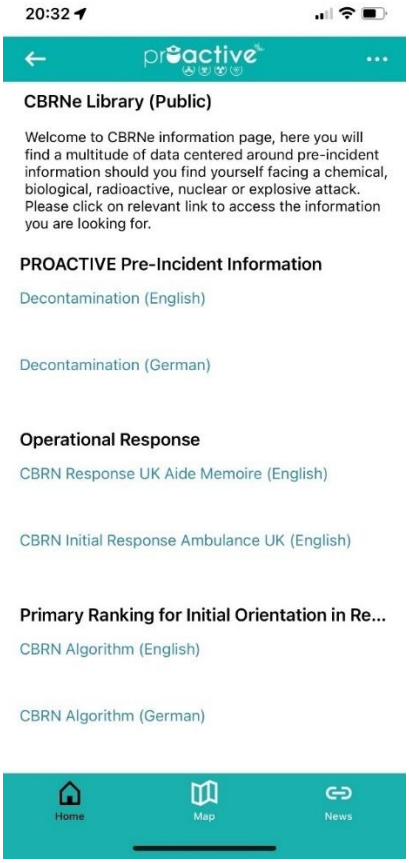

Figure 10 CBRNe Library

5.8.5. Additional Information Menu

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

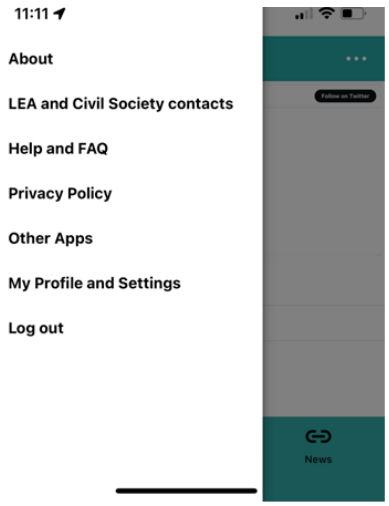

Figure 11 Additional Information Menu

6. TECHNICAL VERIFICATION

6.1. Verification Requirements

Verification and testing of the software are key components of any development but designing mobile apps for vulnerable citizens, ensuring their safety and security is of utmost importance. Verification of such apps involves rigorous testing and evaluation to guarantee they meet specific criteria to protect the users and their data. Therefore, PROACTIVE CBRNe Mobile App wasn't exempted from this process. Furthermore, as requested in the original requirements, the developed app has undergone two 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. Some of these criteria are similar to the verification criteria described in D4.3, however, several additional criteria were utilised to ensure the developed Mobile App for Vulnerable Citizens is acceptable for vulnerable users. These criteria are listed below in Table 9:

Table 9 Additional Verification Criteria

Criteria	Description
Privacy and Data Protection	The app has to have robust privacy measures to protect sensitive user data. It has to comply with relevant data protection laws and provide clear information about data collection, storage, and usage practices. Users must have the option to control their data and give informed consent.
Stability and Reliability	The app should undergo extensive testing to ensure it is stable and reliable. It should not crash frequently or exhibit unexpected behaviour that could negatively impact vulnerable users.
Inclusivity and Diversity	The app's design and content should be inclusive, considering the diverse needs and preferences of vulnerable users. It should avoid promoting stereotypes or excluding any specific groups.
Language and Cultural Considerations	The app should be available in multiple languages and consider cultural differences to cater to a broader audience of vulnerable citizens.
Ethical Considerations	The app should adhere to ethical standards, ensuring it does not exploit vulnerable users or engage in any harmful practices.

6.2. Objective (technical) Verification

The details of the technical/engineering verification are reported in D4.3 [9].

6.3. Subjective (user) 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 [10], D6.4 [11], D6.5 [12]).

Over the course of the three field training exercises, the PROACTIVE mobile app increased in overall usability and overall usefulness (Table 10). 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 10 Usability, 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 DISCUSSION

7.1. Future Work on the PROACTIVE CCS, including the Mobile App for Vulnerable Citizens

The PROACTIVE CBRNe CCS has undergone a long process of development, optimisations, updates and new releases and eventually performed as required during the final PROACTIVE field training 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 Final Conference. Most of these requests and suggestions were constructive, aiming to improve the user experience. Taking into account plans for commercialisation of the developed toolkit after the completion of the project, RINISOFT has summarised all the comments and recommendations. The main additional features that are considered for their implementation in the next release are as following[4]:

1. *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.

2. *Adding time stamps to the "Incident List":* currently all reported incidents are permanently presented in the list of incidents, even those are resolved. It was suggested to modify the "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 opinion.

3. *Adaptation of the developed app for reporting technical issues on railway tracks:* Currently inspection of railway tracks is done according to a schedule by dedicated

[4] These are similarly reported in D4.2 & D4.3, as they all make up the PROACTIVE CCS

personnel. Enabling the public to report any potential issues could improve safety and efficiency of railway infrastructure.

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

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

6. *Implement the developed toolkit with existing legacy systems*: the PROACTIVE CBRNe Mobile App is not the first and only communications toolkit developed. There are a number of existing tools on the market, such as national warning systems, other apps, 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 a CBRNe incident.

The above listed suggestions and recommendations for future work are made by the current and potential stakeholders of the developed PROACTIVE Mobile App for Vulnerable Citizens and as such, they will be taken very seriously. Some of these recommendations are easy to implement technically but may require additional consultations from an ethics point of view. Other recommendations (like integration with existing legacy national warning systems) require close cooperation with the owners of these systems and may have administrative and organisational challenges. In implementing these recommendations RINISOFT will follow the established procedure of an 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 positively accepted by PROACTIVE CBRNe stakeholders.

7.2. Integration with Legacy Systems

Integrating with legacy systems is especially important for practitioners, and without practitioners using the app, citizens won't be able to either. The full details of how we are taking into account integration with legacy systems can be read in D4.3.

8. CONCLUSIONS

This document outlines the major work completed while developing the PROACTIVE CBRNe Mobile App for Vulnerable Citizens. This app was developed as an integral part of the overall PROACTIVE CBRNe Crisis Communications System. The PROACTIVE Mobile App for Vulnerable Citizens fills the gap in a lack of citizen oriented CBRNe disaster apps available on the market today and also minimises the wider "accessibility gap" in emergency management.

The design and development process utilised the best practice approach, ensuring the final product meets the requirements requested by the stakeholders. RINISOFT wanted to ensure the developed PROACTIVE CCS could be easily supported during the commercial exploitation phase. Therefore, at the core of the technical development we adopted the Universal Core Functionality approach, which represents a conceptual idea of essential and foundational capabilities commonly found in various software applications. In addition, special emphasis was placed ensuring the developed CCS meets the needs of vulnerable citizens and is "Secure by Design".

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

Constructive recommendations from these verifications will be implemented in the next release of the PROACTIVE CBRNe CCS 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. Potel M. (1996). http://www.wildcrest.com/Potel/Portfolio/mvp.pdf

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

10. 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

11. 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

12. 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

10. ANNEX 1A – CORE REQUIREMENTS

Core Requirements	
Graphic User Interface	Simple design reflecting PROACTIVE branding. Accessibility across the 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 in the system
Geo-Location	The ability for the system to recognise the location of an incident
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 citizens.

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 a 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 an incident
Existing News Feeds	News feeds from the relevant countries/ areas will be linked to the PROACTIVE MA, 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.