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

Deliverable D5.3

Requirements of the Mobile Application for Vulnerable Citizens and revised technical specifications

Due date of deliverable: 31/10/2020

Actual submission date: 30/10/2020

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

Rinisoft Limited

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 – 30/04/2022
Duration	36 Months
Coordinator	UIC – Grigore Havarneanu (havarneanu@uic.org)

Document details

Title	Requirements of the Mobile Application for Vulnerable Citizens and revised technical specifications
Work Package	WP5
Date of the document	30/10/2020
Version of the document	V5
Responsible Partner	RINISOFT
Reviewing Partner	WMP, ETI, CBRNE, UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	04/09/2020	First Draft
02	06/10/2020	Technical Content Added
03	12/10/2020	Formatted for Submission to Reviewers
04	22/10/2020	Draft reviewed by WMP, ETI, CBRNE, UIC
05	30/10/2020	Final Submission incorporating reviewers' comments

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	RINI	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	PHE	DEPARTMENT OF HEALTH	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 architecture design specifications specific to the Mobile Application for Vulnerable Citizens is the main output of Deliverable 5.3 (D5.3). The purpose of the architectural design specification in this case is to ensure consistency with the Law Enforcement Agencies (LEAs) toolkit (D4.1) in addition to ensuring a modular, flexible, extensible, scalable, robust and secure system. The design process focuses on facilitating the ability of vulnerable citizens to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The Mobile Application for Vulnerable Citizens aims to improve the efficiency of communication between all citizens, including those more vulnerable and the LEAs and Policy Makers involved in the operational aspects of the CBRNe incident, with a particular focus on information sharing (Task 5.1). The technology, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by mobile technologies and, to support the users in overall decision-making processes. The provision of 'other applications' (3rd party) has also been addressed and refers to the 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.

Input will be required from WP4, where the extensive list of requirements are documented in D4.1, which will be adapted as required to suit the functional requirements specific to vulnerable citizens. WP1 and WP3 will provide input in terms of the needs and gaps of the users, specifically relating to the current public perceptions of CBRNe incidents. The research completed in WP1 will feed into the key engagement tasks in WP3, and by default will provide key feedback for the Mobile Application for Vulnerable Citizens in WP5. The work carried out in WP5, will in parallel to WP4 feed primarily into the exercises in WP6, whether they are in person or virtual and will create a feedback loop enabling an iterative approach to the development of the Mobile Application for Vulnerable Citizens.

As referenced in D4.1, the initial end user requirements were derived from the Description of Action, and the experience of Rinisoft, which provided a baseline for the minimal functionality of the system, including the web collaborative platform, and Mobile Applications. The full list of the overall proposed requirements, which can be found in D4.1, were discussed with all consortium members during Progress Meetings 3 and 4. From this, the core requirements were agreed and the initial designs were implemented, detailing the graphic user interface and the key functionalities in relation to the exercises originally proposed, scheduled for M18 in Rieti. However, due to the ongoing COVID-19 pandemic, and the proposed exercise being postponed, further feedback has been sought through network partners and planned webinars, most recently the Civil Society Advisory Board (CSAB) webinar held on 1st October 2020.

The Mobile Application for Vulnerable Citizens will be developed based on an iterative approach in line with the 3 exercises planned during the lifetime of the PROACTIVE project. This deliverable documents the requirements captured prior to the 1st exercise utilising the access we have to the end users within the consortium and the existing CSAB network. Future iterations of the system development are expected to be customised in relation to the exercises planned; initially focus will be placed on the CSAB requirements, then the Practitioner Stakeholder Advisory Board (PSAB) and the final exercise will amalgamate the two. To date, the development has focused on the core

functionality, which will span across the exercises aiming to gather end user feedback to feed into the development loop. The next phase of the development will be to incorporate the current available content (Task 5.1), effectively showcasing the usability and purpose of the system during and post mid-term conference. Further requirements will be documented in D5.4.

Due to the proposed iterative development of the PROACTIVE system, we realise further requirements will be identified, particularly in relation to customisation for the project scenarios. Further requirements will therefore be documented in D5.4 respectively, which is due in M36.

Table of contents

Table of Figures

Table of Figures

Table of Acronyms

LEAs -	Law Enforcement Agencies
CBRNe -	Chemical Biological, Radiological, Nuclear, explosive
WP -	Work Package
PSAB -	Practitioner Stakeholder Advisory Board
CSAB -	Civil Society Advisory Board

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 aims to enhance societal CBRNe preparedness by increasing Practitioner effectiveness in managing large, diverse groups of people in a CBRNe environment.

This will be achieved by testing common approaches between European Practitioners such as Law Enforcement Agencies (LEAs) and First Responders. These will be evaluated and validated against the requirements of civil society, including vulnerable groups of citizens reflected in the European Security Model. A Practitioner Stakeholder Advisory Board (PSAB) and a Civil Society Advisory Board (CSAB) will extend the representation of both sides in several surveys, focus-groups, workshops and field exercises. A benchmark study between LEAs will identify common approaches in assessing CBRNe threats and the protocols and tools used to help citizens. Liaising with the eNOTICE H2020 project, three joint exercises will include role play volunteers recruited by PROACTIVE. They will evaluate the acceptability and usability of existing procedures and test new tools developed within PROACTIVE to provide innovative recommendations for Policy Makers and Safety and Security Practitioners.

PROACTIVE will result in toolkits for CBRNe Practitioners and for Civil Society Organisations. The toolkit for Practitioners will include a Web Collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a Mobile Application. The toolkit for the Civil Society will include a Mobile Application adapted to various vulnerable citizen categories and pre-incident public information material. These will provide 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.

1.2. Interaction with other Work Packages

Designing and developing the Mobile Application for Vulnerable Citizens will be included as one of the key responsibilities of WP5. Input will be required from WP4, where the extensive list of core requirements are documented in D4.1, this will be adapted as required to suit the functional requirements specific to vulnerable citizens. WP1 and WP2 will provide input in terms of the needs and gaps of the users, specifically relating to the current public perceptions of CBRNe incidents. The research completed in WP1 will feed into the key engagement tasks in WP2, and by default will provide key feedback for the Mobile Application for Vulnerable Citizens in WP5. The work carried out in WP5, will in parallel to WP4 feed primarily into the exercises in WP6, whether they are in person or virtual and will create a feedback loop enabling an iterative approach to the development of the Mobile Application for Vulnerable Citizens.

1.3. Objectives of WP5

The main objectives of WP5 can be summarised as follows:

- Content selected and adapted for use in the PROACTIVE guidance toolkit;
- Pre-incident public information materials for CBRNe terrorism designed, developed, and tested;
- A clearly specified mobile app for disabled 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 as a whole.

1.4. Objectives of D5.3

The key objective of D5.3 will be to document the architectural requirements of the Mobile Application for Vulnerable Citizens. The core system development will be documented in D4.1 and referenced where necessary. The deliverable will highlight the core requirements identified to date but will then further address the specific adaptations to suit the needs of the vulnerable citizens.

2. PURPOSE OF THE DELIVERABLE

The architecture design specification for the Mobile Application for Vulnerable Citizens is the main output of D5.3. The purpose of the architectural design specification in this case is to ensure consistency with the LEAs toolkit in addition to ensuring a modular, flexible, extensible, scalable, robust and secure system. The design process focuses on enabling vulnerable citizens' ability to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The Mobile Application for Vulnerable Citizens aims to improve the efficiency of the communication between all citizens, including those more vulnerable and the LEAs and Policy Makers involved in the operational aspects of a CBRNe incident, with a particular focus on information sharing (T5.1). The technology, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by mobile technologies and, to support the users in overall decision-making processes. The provision of 'other applications' (3rd party) has also been addressed and refers to 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 architecture herein presented promotes customisation to fit the needs of each user group, while sharing common denominators expressed in this architectural design document. Although further information relevant to LEAs and Security Policy Makers will be documented in D4.1, it is inevitable the core structure of the system is the same across all stakeholder groups to enable consistency and bi-directional communication. Accessibility, in particular will be a key focus across the system as a whole, as this is principally important for vulnerable groups and communities that are more difficult to reach: deaf, visually impaired, religious, children, elderly etc.

The architectural definition process focused on the following four principle objectives:

- To clearly present a description of the PROACTIVE system and how it addresses stakeholder needs, (including LEAs, Security Policy Makers and citizens, including those that are vulnerable);
- 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 Tasks 4.2, 4.3, 5.2 and 5.3 that will use this architecture design as a baseline input.

3. END USER REQUIREMENTS

The core functionality of the PROACTIVE system is the same across the web-based platform and both Mobile Applications. As referenced in D4.1, the initial end user requirements were derived from the Description of Action, and the experience of Rinisoft, which provided a baseline for the minimal functionality of the system, including the web collaborative platform, and Mobile Applications. The full list of the overall proposed requirements, which can be found in D4.1 were discussed with all consortium members during Progress Meetings 3 and 4. From this, the core requirements were agreed and the initial designs were implemented, detailing the graphic user interface and the key functionalities in relation to the original proposed exercise, scheduled for M18 in Rieti. However, due to the ongoing COVID-19 pandemic, and the proposed exercise being postponed, further feedback has been sought through network partners and planned webinars, most recently the CSAB webinar held on 1st October 2020. This deliverable will focus on the Mobile Application for Vulnerable Citizens and due to the proposed iterative development of the PROACTIVE system, we realise further requirements will be identified, particularly in relation to customisation for the project scenarios. Further requirements will therefore be documented in D5.4, which is due in M36.

3.1. Core Requirements

Table 1 Core Requirements, highlights the high-level core requirements identified in preparation for the initial version of the web platform and Mobile Applications for both the LEAs/Security Policy Makers and Vulnerable Citizens, a more detailed list of core requirements specific to vulnerable citizens can be found in Annex A, which will be referenced for future development as required. It is important again to highlight the core requirements will not differ between the Mobile Applications for the LEAs Security Policy Makers and Vulnerable Citizens, the way they are used may however vary. Also, a key element of the Application for vulnerable citizens is ‘Accessibility’. For consistency, the PROACTIVE system as a whole is being developed with the concept or accessibility at the forefront, therefore ensuring all methods of communications are available across the user groups.

During the design phase Rinisoft discussed elements of security, ethical procedures and legal requirements with consortium partners involved in WP8 and in particular with the WP8 leader ETICAS to ensure the system is compliant with all these important requirements. The PROACTIVE tools will be integrated into a system adapted to the needs of LEAs and other Practitioners. This system comprises therefore many functionalities and involves the management of citizens' data by different actors with different responsibilities, which makes necessary the establishment of clear protocols for its use.

Table 1 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 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)

3.2. Functional Requirements – First Field Exercise

The consortium agreed it would be beneficial to have the first iteration of the system, available for testing during the exercise in October 2020. The system would have limited functionality as per *Table 2 Functionality for* to enable users to provide initial thoughts on usability and content. As the exercise

is no longer happening in M18, the app will now be presented at the mid-term conference on the 28th October. Future updates of the Mobile Application for Vulnerable Citizens will be included in D5.4.

The Rieti exercise has now been proposed for the 28th April 2021 and will focus predominantly on the CSAB stakeholders. Following discussions with CBRNE, the Mobile Application for Vulnerable Citizens will be the primary focus for feedback, however to enable this, the functionality for the web-based platform and Mobile Application for LEAs and Security Policy Makers will have to be developed in parallel to support information sharing and bi-directional communication. Allowing for the additional time, the intention is to further develop the functionality to include some features in *Table 3 Access* , in particular the forum capabilities to enable the exercise to gather feedback during and following the event.

Table 2 Functionality for the first field exercise

Functionality - Rieti	
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 lessons learnt.
Links to Available National Apps	Countries with existing Apps for crises events will have the link signposted in the PROACTIVE portal
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, creating 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.

3.3. Functional Requirements – User Categories

Initial discussions with the end users in the consortium highlighted a number of differences related to functionality in terms of access rights for different user groups, which inevitably affects the way the system will be used by each group. *Table 3 Access Levels,* highlights the core features identified

in Section 3.1/ 3.2 broken down to address the features which will be available to Vulnerable Citizens. For perspective, the access levels for LEAs and Security Policy Makers have also been included. The level of access for Security and Policy Makers and will be reviewed during each of the planned exercises.

Table 3 Access Levels

Functionality	LEAs	Security Policy Makers	Vulnerable Citizens
Display EU flag and Grant Number	Yes	Yes	Yes
Privacy Policy, data protection and access to potential data, consent form and disclaimer	Yes	Yes	Yes
Register/ Login (only email addresses) Option to subscribe to additional information (tick box)	Yes - mandatory	Yes – mandatory	Yes – not mandatory
Link to 'About PROACTIVE' Page	Yes	Yes	Yes
Contacts Page (LEAs/ Policy Makers/ Hospitals/ Health Advisors etc)	Yes	Yes	Yes
Link to Direct Messaging	Yes	Yes - will vary per scenario	Yes - will vary per scenario
Link to Forums	Yes	Yes	Yes
Link to CBRNe Information	Yes (to include operational and policy information)	Yes (to exclude operational information if confidential)	Yes – only public facing information
Link to Available Support Tools (Existing Apps/ websites)	Yes	Yes	Yes
Link to push notifications (automated early warnings)	Yes (multiple data formats)	Receive only (multiple data formats).	Receive only (multiple data formats).
Link to available News Channels	Yes	Yes	Yes
FAQ page (pre, during and post incident)	Yes	Yes	Yes

4. REVISED TECHNICAL SPECIFICATIONS

4.1. System Functionality

Following a technical analysis of the user requirements, the following section outlines the non-functional requirements, whereby the user requirements are reviewed to determine the systems operational functionality. This covers areas such as the legal, ethical, security, accessibility, scalability, usability and deployment. The system will be made up of two main components:

4.2. ASP.NET Core 3 Stateless Web Service

- Hostable on traditional on-site or cloud servers
- Hostable as a stateless Lambda service on AWS or Azure
- Backed by Postgres 13 SQL server

4.3. Angular 9 Reactive Web Application

- Reactive design supports all device sizes, smart phone, tablet & pc.
- Available as a Progressive App on iOS and Android
- Designed as an accessible application with simple UI
- Supports screen readers and other accessibility tools.

Figure 1 Linux Based Server shows the logical topology of an example single server deployment of the Proactive Application. The top half of the diagram shows the supported devices & web browsers (Safari, Firefox & Google Chrome), which allow the users to connect to the Server via a secure HTTPS connection. The bottom half of the diagram shows the connections & relationships between the installed components on the server:

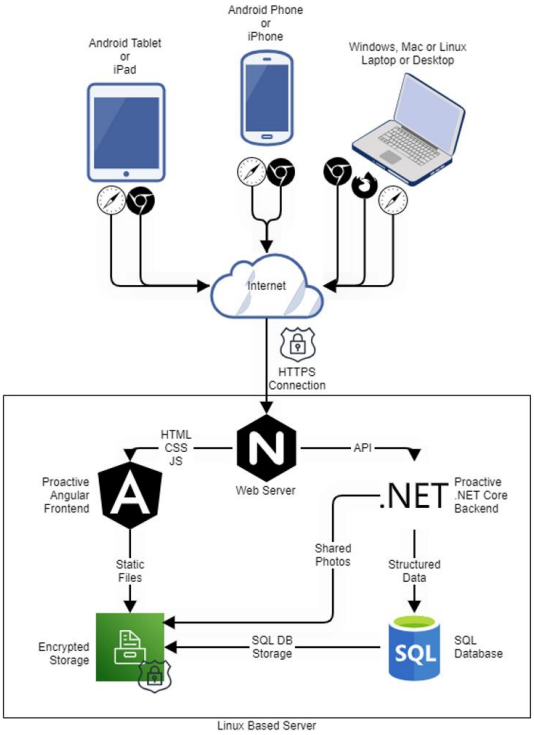

Figure 1 Linux Based Server

4.4. System Security

The system will enforce the following security protocols:

- SQL Data Protected by Full Drive Encryption: aes-xts 256;
- Client-Server communication protected by Transport Layer Security (HTTPS);
- System access is controlled by application level authorisation. Unauthorised users (not logged in) and members of the public may not view sensitive information or edit publicly accessible information directly. In addition, API Key authorisation will be available for external integrations.

4.5. System Interoperability

- The PROACTIVE platform exposes a secure REST API that allows for external systems to integrate;
- The integration API can be used by authorised partners to push data into the system in real time;
- The home page has links to external applications and resources.

4.6. Graphic User Interface

The PROACTIVE portal's GUI is an Angular 9 Reactive web application that provides users with an accessible user interface to carry out the main functional interactions required of the PROACTIVE platform. The GUI is designed to cater for a diverse range of users and devices, supporting:

- Landscape and Portrait aspect ratios;
- Screen sizes from 10cm to 50+cm;
- iOS phones and tablets;
- Android phones and tables;
- Laptop & Desktop browsers; Chrome, Firefox, Edge, Opera and more;
- Screen readers & accessibility tools;
- Progressive Web app to provide offline functionality and asynchronous file uploads.

4.6.1. PROACTIVE Portal Login and About Us Pages

Allows registered users and site admins (LEAs) to log into the portal and access application features not available to unregistered users. It is not however mandatory to login to the portal, information on CBRNe issues will be available without registering. Project information for members of the public; this page details the grant agreement information in addition to the purpose of the project. Should users require further details they will have the option of requesting further information through the PROACTIVE email or via the website.

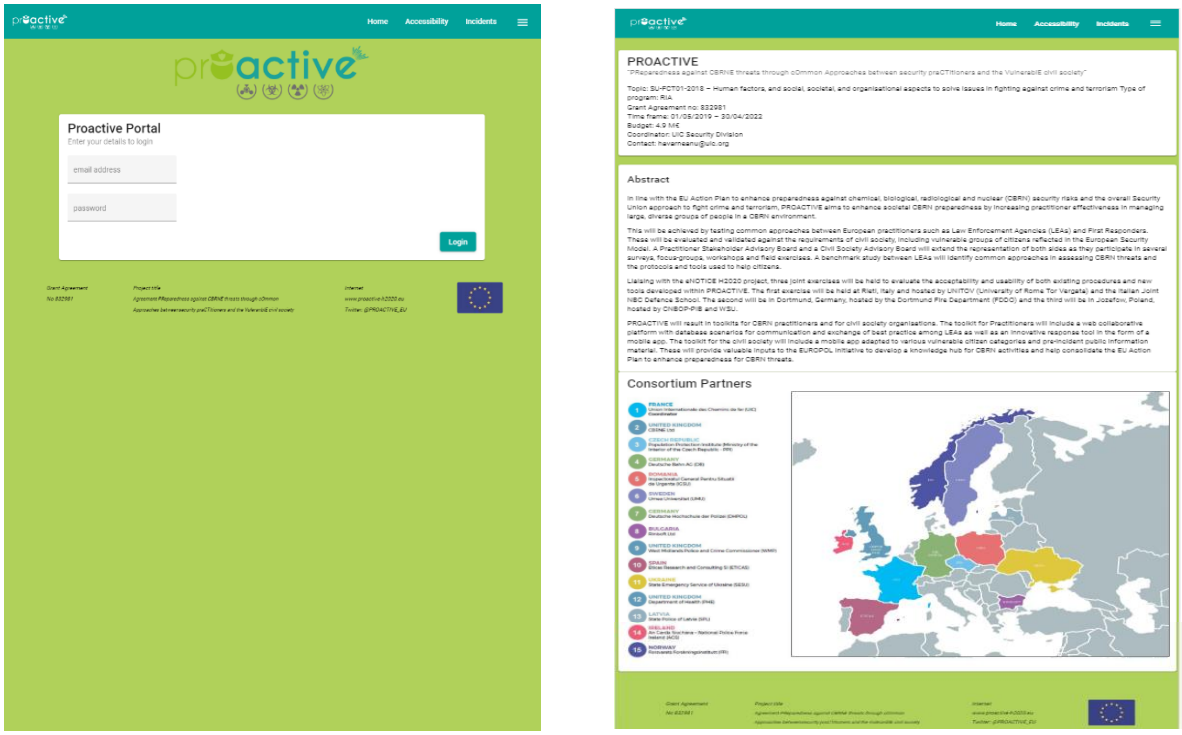

Figure 2 Registration and About Us Pages

4.6.2. Portal Home Page and Key Contacts

A landing page for users containing up to date notifications and news feeds along with links to external information sources and contacts. This will act as the central hub for the technology, enabling users to navigate to the relevant areas of interest. This page will also act as a main notification page, providing users with live updates either directly through the PROACTIVE Mobile Application or through link to national systems and news channels.

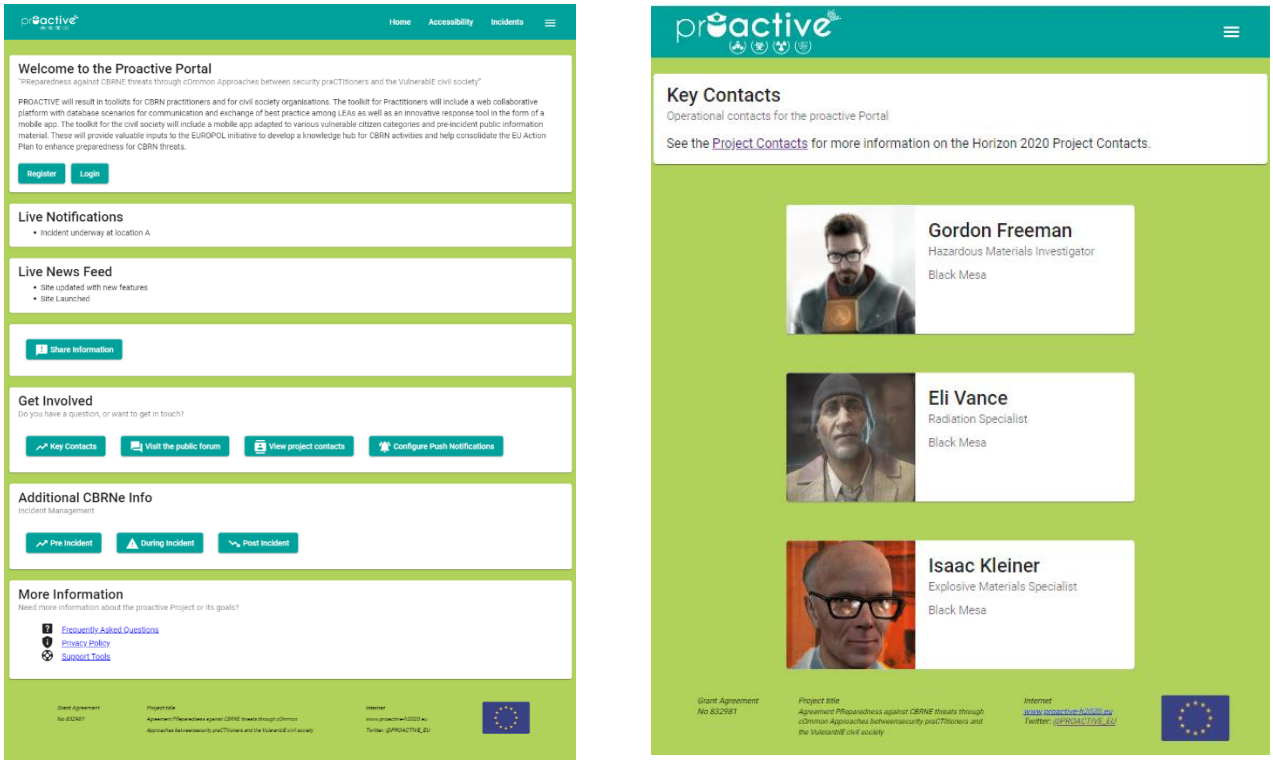

Figure 3 Home Page and Key Contacts

4.6.3. Information Sharing

Live updated map of current incidents along with a summary of incident status. Registered users will have the capability to notify of an incident in their area. Basic details including date logged, the status and type of incident will be required in addition to the location. All incidents will be moved to a holding queue, in which LEAs will have direct access to the review and verify the incident. Once validated the LEA can then choose to release an update on the incident utilising the map functionality available in the Mobile Applications. Furthermore, LEAs will have the option to monitor and update the incident using the live notifications functionality once the incident has been investigated.

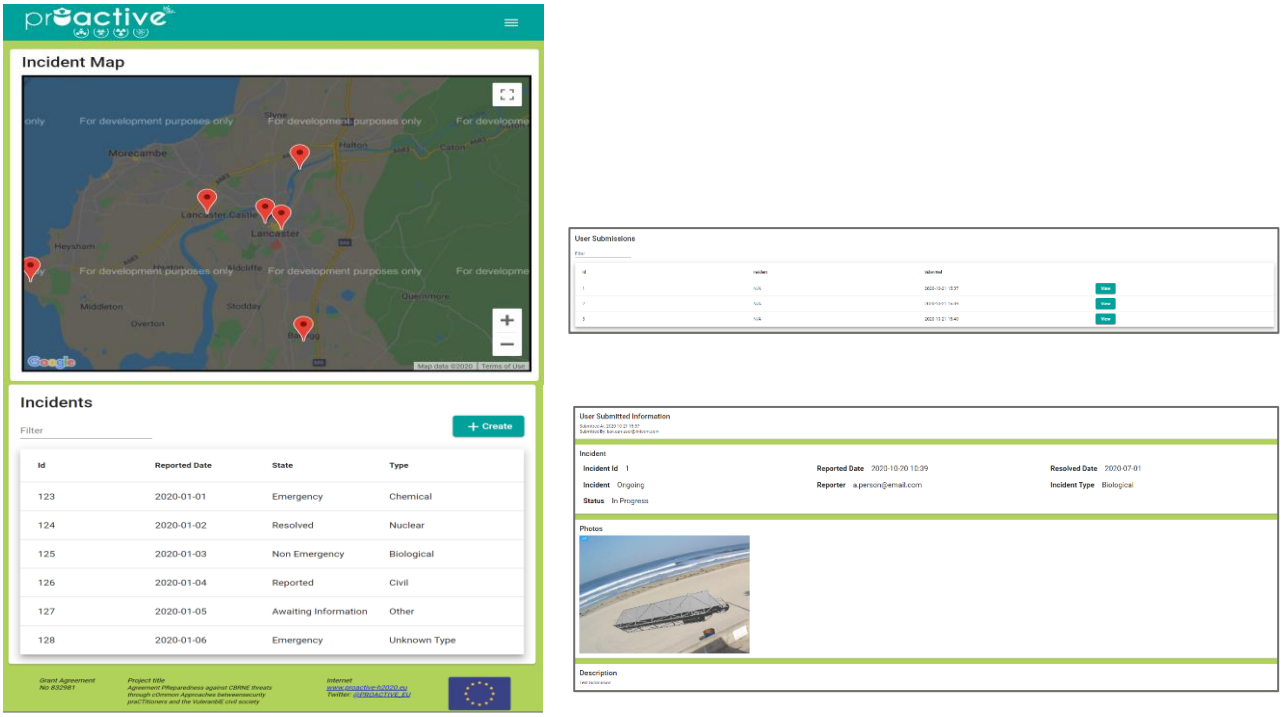

Figure 4 Information Sharing

5. CONCLUSIONS

The Mobile Application for Vulnerable Citizens will be developed based on an iterative approach in line with the 3 exercises planned during the lifetime of the PROACTIVE project. This deliverable documents the requirements captured prior to the 1st exercise utilising the access we have to the end users within the consortium and the existing CSAB network. Future iterations of the system development are expected to be customised in relation to the exercises planned; initially focus will be placed on the CSAB requirements, then the PSAB and the final exercise will amalgamate the two. To date, the development has focused on the core functionality, which will span across the exercises aiming to gather end user feedback to feed into the development loop. The next phase of the development will be to incorporate the currently available content (T5.1), effectively showcasing the usability and purpose of the system during and post mid-term conference. Further requirements will be documented in D5.4.

6. ANNEX A – DETAILED CORE REQUIREMENTS

Mobile Application for Vulnerable Citizens
Documented in Description of Action The Mobile Application for Vulnerable Citizens should incorporate a consistent interface and branding using the PROACTIVE colours Mobile Application for Vulnerable Citizens will allow vulnerable citizens to communicate with other citizens, LEAs and Security Policy Makers Mobile Application for Vulnerable Citizens will provide video (for sign language support), real-time text, text-to-speech features and an intuitive user experience environment, with smart buttons and visual instructions to report emergencies. Mobile Application for Vulnerable Citizens will also be able to receive automated early warnings issued by authorities **Additional Requirements from End Users** The Mobile Application for Vulnerable Citizens static content shall be initially in English (to reflect NATO standards). The static content will be manually changed to Italian, German and Belgian/Flemish for the planned exercises. The Mobile Application for Vulnerable Citizens must allow various settings for accessibility; Font Size & Type, Colour of Screen to support colour blindness, no flashing images to reduce issues with epilepsy, audio options/ voice control for the visually impaired/ or those with dyslexia, and sign language videos for those with limited hearing etc. The sign language used will reflect the languages used in the exercise countries (Italian, German, Belgian/Flemish). The Mobile Application for Vulnerable Citizens is required to reference existing apps (providing links where possible. Integration directly with apps will be avoided to prevents privacy and security issues. The Mobile Application for Vulnerable Citizens should consider novelty, e.g. cartoon characters, pictograms, symbols etc where appropriate to reduce the issue of language barriers. Concept of a system wide avatar to be discussed. The Mobile Application for Vulnerable Citizens will have 2 access levels; Registered User (enables citizens to report emergencies and well as view information) and Non-registered users enables citizens to view information but not report. The Mobile Application for Vulnerable Citizens must be available for cache data in areas where the internet is not available and should be uploaded automatically with it becomes available.

Users of the Mobile Application for Vulnerable Citizens are required to read and verify (tick box) a privacy policy, data protection and access to personal data, consent form and disclaimer electronically before they can access the system.

Users of the Mobile Application for Vulnerable Citizens will only be required to provide a valid email address to use the system, they will receive a response welcoming them to the system. No other personal information.

The Mobile Application for Vulnerable Citizens must provide the ability to report an incident at a specific location using a map. The Application must make it clear in the case of a crisis, the emergency number relevant to that country 112 should be used.

The Mobile Application for Vulnerable Citizens to download data (pdf, videos, images, audio files).

Users of the Mobile Application for Vulnerable Citizens will have the option to subscribe to emails and text notifications. This will be a generic message sent to all users, not targeted to the needs and requirements of the individual as this would require substantial personal data to be collected.

The Mobile Application for Vulnerable Citizens will enable the user to select their preferred location when they log in.

The Mobile Application for Vulnerable Citizens will provide the citizens with useful advice about the website itself or about particular situations in their area via an FAQ page. Included in this page will be a section prompting the information to be provided during an incident (route to incident, medical symptoms etc)

The Mobile Application for Vulnerable Citizens will signpost users to other relevant sites/ contacts for useful information, for example accommodation, help lines, charities etc.

The Mobile Application for Vulnerable Citizens should have the ability to trace family members who may have been involved and will want reassurance that family members and friends are accounted for and safe