This report was funded by the European Union's Internal Security Fund — Police under grant agreement n° 861716

Quick Response for Operational Centers

D 3.3 – Technology assessment

WP number and title	WP3 – European Centers Cross Border Communication
Lead Beneficiary	MIR-ES Spanish National Police
Contributor(s)	DITSS
Deliverable type	Report
Planned delivery date	31/08/2020
Last Update	11/09/2020
Dissemination level	Public

Disclaimer

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The QROC Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	DUTCH INSTITUTE FOR TECHNOLOGY, SAFETY & SECURITY	DITSS	NPO	NL
2	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	RTO	NL
3	THE NATIONAL POLICE OF THE NETHERLANDS	NPN	LEA	NL
4	AEORUM ESPANA S.L.	AEORUM	SME	ES
5	POLICEJNI PREZIDIUM CESKE REPUBLIKY	PPCR	LEA	CZ
6	MINISTRSTVO ZA NOTRANJE ZADEVE REPUBLIKE SLOVENIJE, POLICIJA	MNZRS	LEA	SI
7	MINISTERIO DEL INTERIOR	MIR-ES	LEA	ES
8	INSPECTORATUL GENERAL AL POLITIEI ROMANE	IGPR	LEA	RO
9	HELLENIC POLICE	HP	LEA	GR
10	EUROPEAN UNIVERSITY CYPRUS	EUC	UNI	CY
11	STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO	PPBW	NGO	PL
12	POLICE GRAND-DUCALE	PL	LEA	LU
13	AN GARDA SIOCHANA	GARDA	LEA	IE
14	AUTONOOM PROVINCIEBEDRIJF CAMPUS VESTA	VESTA	GOV	BE
15	POLIISIHALLITUS	FINPOL	LEA	FI
16	COMMUNICATION AND INFORMATION SYSTEMS DIRECTORATE	BGPOL	LEA	BG
17	CYPRUS POLICE	CYPOL	LEA	CY
18	MINISTRY OF DEFENSE / KMAR	MINDEF	LEA	NL

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	30/07/2020	Draft	MIR-ES Jose Francisco López	A first overview of the findings to be reviewed.
V0.2	31/08/2020	Draft	MIR-ES Jose Francisco López	Second draft
V0.3	07/09/2020	Draft	MIR-ES Jose Francisco López	Third draft to review
V0.4	11/09/2020	Draft	George Kioumourtzis (DITSS), Jacques van Wersch (DITSS)	Corrections, final review and Quality assurance
V1.0	14/09/2020	Final	Patrick Padding (DITSS)	Final approval and submission

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
QROC	Quick Response for Operational Centers
LEA	Law Enforcement Agency
OC	Operational Centers
IM	Instant Messaging
SMS	Short message service
GPS	Global Positioning System
DC	Data Center
DNS	Domain Name System
API	Application Programing Interface
API REST	Application Programing Interface Representational State Transfer
HTML5	Hyper Text Markup language, version 5
MDM	Mobile Device Management
LDAP	Lightweight Directory Access Protocol
DDos	Denial of Service

Table of Contents

List of Tables

Executive Summary

This report describes the QROC instant messaging applications benchmarking. Within QROC previous deliverables the desirable attributes for an information sharing system have been identified according to QROC purposes.

There are three main Key points that the IM systems must offer, as identified in QROC D3.1 "Oversight of operational data and formats":

1.- Support the exchange of different data formats (text formats, audio and video formats, photo formats, live video…),

2.- Ability to be easily integrated in OCs platforms allowing us to interact with our internal applications and automated OCs internal processes

3.- Implement all the security measures and features in order to guarantee information management system security in use by LEAs.

Instant Messaging is the best technology to share operational information between OCs across EU territory anytime and anywhere. Instant messaging Apps have many benefits and advantages, as well as a high level of security to ensure the secure storage and transmission of operational and confidential information. In this document we will analyse in which level do the main IM market solutions meet the QROC key points and requirements.

Sensitive information must be kept private and never abandoned the OCs control. This is the reason why ON PREMISE solutions must be required and deployed in OCs Data Centres. The IM solution must also allow OCs administrators to manage and control every security aspect and privacy settings of the network and the information shared.

The infrastructure deployed ON PREMISE must comply and implement all the security measures and recommendations required for these types of systems in order to avoid information interception, DDOs attacks, etc. In order to guarantee high availability for the service in case of catastrophe or attack to one DC, it is interesting to have the option to deploy a second redundant infrastructure of the solution.

The solution must offer an easy integration with the different OCs platforms and systems. These solutions will allow us to integrate our internal applications or even develop new applications from scratch so OCs can interact with on field users in an automated way.

The solution must be multiplatform, allowing users to connect from the main SO devices (iOS, Android, Mac, Windows and Linux). Multichannel capabilities (being able to use the app simultaneously from different devices) are also a desired capability.

Although security and privacy are a must, the IM solution also needs to offer a simple but powerful tool so any user can adopt it with a small learning curve. This means that the user experience within the app should be similar to the most popular IM public Apps and offer similar features to the users. This will guarantee the success of the solution within the organization and the general take up by the users.

These Apps have been classified into two categories, public and professional solutions/Apps.

Public instant messaging solutions like WhatsApp, Telegram do not offer all the required specifications/features for QROC purposes (while Signal meet some of them). The main problem with these public IM tools is a complete lack of control over the information shared, the network and the users. These public IM tools are based in the United States and under US laws, meaning that all the information shared with these Apps will be stored and could be used by the service provider or Government under US laws. In resume, they will make us lose control over our information and communication channels. Instead, professional Apps are installed ON PREMISE with the full system running under the system administrator (e.g. Police). Therefore, LEAs are the owners of the information and have full control over it.

The professional Apps presented in this deliverable are those that are in use by LEAs in Europe, on one side the two with more licenses: StashCat in Germany and IMBox in Spain, both Apps are in use by European Agencies (Stashcat by EU Lisa and IMBox by Europol in test), on the other side Threema (Switzerland) and WhatSU in Belgium. Microsoft Teams also has been included in the benchmarking assessment.

The benchmarking analysis carried out in this report is an assessment based on seven (7) different categories: security, usability, functional features, interoperability, feasibility (integration capacity), compliance and price. Those categories are split in twenty-five sub-categories allowing us to compare both the public and the professional solutions. For obvious reasons the conclusions are mainly focused on the professional solutions instead of in the public IM tools.

The analysis highlights several features that have been identified as important for QROC. Some other features have been classified as desirable due to the extra capabilities that they may give us.

1. Introduction

The overall objective of WP3 within the European “Quick Response for Operational Centres”-project (QROC) is to implement a cross border data exchange between the National Operational Centres and between this OCs and on field officers.

This mechanism needs to ensure user access to centralized operational databases to perform any request and also a direct and immediate communication channel prior-during – and after a terrorist/ CBRN-e threat.

Based on [1] the NOCs need to increase their capabilities in managing different formats of information instantly anytime and anywhere. The number of files formats has increased exponentially, and our current platforms are not able to support all of them. Also, these solutions are not mobile first, meaning that users need to be in front of their desktop in order to check the information instead of checking it on the go. Information is shared via Framed Document Templates which is not powerful enough to share photos, video clips, live video, documents, voice, and spatial information.

Exchange of information between Operational Centres (OC) can be achieved through many communication channels and multiple ICT technologies. New ways of sharing information have emerged as innovative technologies such as Instant Messaging are helping users to stay connected with each other at anytime and anywhere. With the increasing use of mobile phones, laptops and tablets, there is a great opportunity to implement solutions to help Police Officers from different Member States to communicate with each other and share information instantly in an easy manner. New ICT systems should allow Police Officers to exchange any file in a simple way between OCs and operational officers on the field.

Nowadays nearly every person uses one or more public IM tools, mainly WhatsApp and Telegram, but as explained before, these solutions are not designed to cover our exhaustive information security and network control needs.

Nevertheless, we can take advantage of professional solutions that have been designed to meet LEAs needs such as IMBox, Threema, WhatSU, Microsoft Teams and Stashcat. While Whatsapp and Telegram (even Signal) store messages and files in their own cloud (US servers), professional solutions must guarantee the possibility to implement an ON PREMISE deployment of their technology.

Nevertheless, the biggest challenge will be to connect users from different Member States with a common solution or doing independent solutions interoperable. Some problems may arise such as where to deploy the servers, or who will administrate the network. Therefore, the solutions should be flexible enough to allow creating different networks within a server or even allowing us to deploy independent and geographically separated but interconnected infrastructures between Member States.

The aim of this document is to compare the most popular IM solutions. We will compare the two main public IM tools (Whatsapp, Telegram and Signal), the main professional tools used by law enforcement at an EU level (IMBox, Stashcat and WhatSU) and Threema and Microsoft Teams

This report, however, does not constitute an overall benchmark and technology scan due to:

1- Not all Apps used in the EU have been benchmarked, only those known and experienced by some LEAs have been included in the report
2- Most of the information included in the report was found in internet with few contacts with some providers, so in some rare cases information may not be correct.

2. Messaging Applications

Instant Messaging Applications allow users to share messages and files with each other through an Internet connection.

The increasing market share of smartphones together with a poor, and in some countries expensive communication system based on SMS, paved the ground for companies like WhatsApp to rapidly expand their user base worldwide surpassing the use of SMS to send text messages.

The ease of use, the ability to send any type of file, the ability to easily create and manage group chats, etc. helped these solutions to become very popular in very short time.

Nowadays, every smartphone user has at least, one IM solution to share messages and files with their family, friends and co-workers. The number of messaging Apps have increased significantly over the last years, and the devoted Apps focusing more on specific formats, like Skype in video, have boosted the number of followers.

Even though the formats supported by most of them are similar, other features of messaging Apps, like security in communications, have even increased their popularity in the general public. The encryption of communications, the architecture of the systems, the access to personal information, the place where the servers are located, the owners of the information we are transmitting, became a desired attribute that professionals increasingly are looking for.

This new trend (the use of public IM tools to share sensitive information) has helped new companies offering new professional IM solutions. These companies offer all the features of a public IM solution to the final user while giving companies and organizations control over their information and communication channels.

2.1. Messaging Applications features: the most relevant to QROC

After analysing dozens of Instant Messaging features, we have selected those considered most important for the project purposes:

- **Supported formats**: text messages, photo, video-clips, live voice and video call, spatial information, pdf files, word, excel and power point files are the formats identified in [1] as the most useful for information exchange.
- **Security**: Shared messages and files should be encrypted in transit and at rest. Although all Apps encrypt the communications while in transit, some of them do not encrypt the information at rest. Also, depending on how the communication protocol is implemented, the information shared can be exposed malicious third parties.
- **Architecture**: Most of them are Client/Server applications using real time standard protocols or proprietary protocols for communications. The solution must be deployed ON PREMISE in OCs DCS. Geographically separated redundant systems are also valuable.
- **Data storage**: Secure data storage is a key element for QROC purposes. We need to know and understand what kind of data is stored, for how long and hold the certainty that we are the sole owners of the information transmitted through the service.
- **Multiplatform and multichannel:** In order to use the app in the OCs, the App should be able to be installed in any type of device (mobile, tablet or PC) and OS (Android and iOS for mobile devices and tablets, Windows/Mac/Linux for the desktop versions). Also, users should be able to use their account simultaneously in different devices (multichannel capabilities).

- **Functional features**: The App must offer the same features as those offered by the most common public solutions (WhatsApp and Telegram) and implement a similar look and feel to help users adopt the solution with ease.
- **Metadata**: The transmission of information is complemented with no visible information that depending on the application is able to provide valuable information from the operational point of view. Metadata information is important to be able to comply, if needed, with European auditing regulations. This metadata may include information of the user IP address, message date and time, mobile device type, etc.

2.2. Instant messaging applications to benchmark

The IM solutions analysed are divided in public and professional solutions and have been selected based on their popularity.

Most popular public applications in EU are:

- WhatsApp
- Telegram
- Signal

Identified professional applications for LEA are:

- Stashcat
- IMBox
- Threema
- WhatSU
- Microsoft Teams

Unlike the public IM solutions, finding information for some of the professional solutions analyzed has not been an easy task. We might however confirm some of the conclusions with the different providers in order to double check our findings and give them the opportunity to clarify any aspect they may not agree with.

3. Benchmarking criteria

This section identifies and defines the variables used to compare the different solutions.

3.1. CRITERIA

a. <u>**SECURITY**</u>: QROC is looking for a private, secure and controlled instant messaging and file sharing application to exchange information between Operational Centres (OCs) and mobile users in the field with a secure, quick and easy to use solution. Security is the key issue.

   Security criteria is defined through different parameters:

- **Encryption**: information should be encrypted in transit and at rest (when stored in the servers). Information must be encrypted and secured while is travelling from the server to the client, from client to server or from client to client (in case of end to end encrypted video calls). Strong encryption and well designed and implemented secure communication protocols should be implemented for all those transmissions.

  Also, information shared can be stored in the servers or in the user's mobile databases. Both, the servers and the user's mobile databases need to be encrypted. Apart from the default OS encryption of the device (if an access code or biometric control is enabled), the messaging App must also encrypt the client database itself to secure the information in case of lost or stolen devices. Any other features allowing administrators to manage user's mobile databases (such as remote deletion of the database, ability to block file downloads to the user's device, etc) are also valuable.

  The level of encryption is not going to be assessed in this report.

  Encryption sub-categories compared in the analysis are: **file and message encryption**, **mobile device database encryption**, **server database encryption** (As stated before, the information must be encrypted at rest in the IN HOUSE servers) and **IP voice and video calls encryption** (Does the app offer secure end to end encrypted voice and video calls?)

- **Secure file storage in the private cloud**: One of the main painful points for the users is the mobile device storage capacity. Many users have storage capacity issues as they use the device to take and share operational photos and videos that need to be stored locally. This also means that these users store sensitive information in their devices. Offering users a private cloud does not only allow them to store files in the cloud and regain storage capacity in the device but also allow us, as an organization, to block the download button functionality so sensitive information is never stored locally in the user device.

  The files will be securely stored in in-house servers and linked to the user. The way these files are stored and the security implementations of the servers is important (ideal architecture of the system):

  1. They should be encrypted while stored at rest.
  2. The infrastructure should implement all the security measures available to avoid third party access (example: firewall configuration)
  3. Redundant servers containing all the information should be deployed. This way, if one server goes down or its destroyed, there is a backup server in place.
  4. Geographically distributed infrastructures. The geographic redundancy guarantees the maximum availability for users. If one full DC is down or even attacked, there is another up

to date infrastructure elsewhere that will continue to give service instantly with zero information loss if both had been in constant communication before the attack or catastrophe.

5. DNS redundancy. If the provider loses control of its domain (xxxx.com), a malicious user could redirect its clients' traffic to an external server. To minimize this risk, providers Apps could resolve 3 independent DNS hosted on 3 independent and use a quorum strategy, that is, they follow the majority (2 out of 3) in case of dispute. A malicious user would have to gain access to 2 providers simultaneously to get a quorum and redirect traffic. Does the provider offer DNS redundancy in its platform?

- **MDM Integration**: MDM is useful to remotely manage and control user devices, remotely set different security policies to the mobile devices, easily deploy an app to thousands of devices, force application updates to the users, avoid ransomware, etc. The integration of MDM in the mobile device allow better security polices and settings. Does the app integrate with the different MDM solutions in the market?

- **Other security features**: could be the use of biometric access control systems through face recognition or fingerprint detection to access the app. Two factor authentications to log in from a different device, the ability to set specific security policies for the messaging network, etc. are also valuable.

b. **USABILITY**:

- **Multiplatform: T**he app should be available for Android, iOS, Windows desktop, macOS and Linux.

- **Synchronization platform** (multichannel): The solution must allow users to connect and use the app from different devices simultaneously. Arguing security reasons, some applications do not allow the use of the same user account in different devices at the same time. To solve this problem, a double factor authentication process can be implemented to guarantee security while offering the multichannel feature. Not offering this feature could be an obstacle in the day-to-day operations. Does the app allow the users to simultaneously use their account in more than one mobile device? Can the administrator of the network define the maximum number of devices allowed to be used simultaneously?

- **Access to platform: Administrator web control panel and access security:** The solution must offer a web control panel allowing the administrator/s to configure the security policy settings for each OC network (password policy of the network, maximum number of wrong access attempts, block/unblock file downloads to user devices, messages and files expiration date, block the possibility to share some kind of files by mime type or by size, etc.). On the other hand, the access to the user account should be protected. The most common access method is via user and password, but new ways of secure access are also important (biometric access control via face recognition or fingerprint detection).

- Usability with regards to **interface and management (look and feel and user experience):** Users are familiar with WhatsApp and Telegram ease of use and features. Implementing similar interfaces and features is important to guarantee a general adoption of the solution.

- **LDAP integration**: It is to know if a client/server application allows access to the directory, what is useful to find information in databases in a network environment. It is really useful to manage user registrations or deny subscriptions. Does the app integrate with LDAP?

- **Branding customizable**: The app should be able to adapt its colours, terms and conditions, point of contact, language, etc. to the specific needs of the EU State Members. Does the app allow changing the language, colours, terms, contact info, etc. to match the country specifications?

c. <u>**FUNCTINAL FEATURES**</u>: Administrators of the network should be able to easily manage and control the system at the network level (password policy, access control, file and messages retention policy, etc) and at the user level (create and delete users, create and manage group chats and distribution lists, etc):

- **IN HOUSE infrastructure**: The solution must be fully or partially deployed in house. Public solutions like WhatsApp and Telegram do not allow ON PREMISE deployments. Signal, as an open source solution, may be implemented IN HOUSE. Professional solutions generally allow ON PREMISE deployments but some of them use third party servers for different purposes. This approach should be analysed to understand what kind of information is shared with third party server providers and why.

- **Chat groups**: Chat groups allow users to send messages to one or more users in a chatroom. This is very interesting to coordinate field operations. All benchmarked applications have this feature implemented. The difference is in the number of groups that can be created, if users can create groups from the app or if groups must be created centrally by the network administrator.

- **Distribution lists**: Distribution lists are like chat groups but are READ ONLY for its members. In these lists only the creator and administrators of the list are able to send messages and files while the rest of users can only read. The app should allow the creation of distribution lists to broadcast information.

- **Group and list without limit of members**: The solution should allow the creation of groups or distribution lists with no limit on members. Can we create a group with 100.000 users or is there a limit?

- **Guest access**: We might need to invite external users temporarily to the network as guests. Does the solution allow us to invite external users to our network as guests?
- **User and groups managing interface** (control panel): Having a quick and flexible way of creating groups can make the difference while coordinating a group of users when in a man hunt scenario. Users must be able to create group chats directly from the app. On the other hand, administrators

must also have an easy way to quickly create these groups of users from a web control panel and instantly send them a message or even manage and control the groups created by users. Does the solution offer a web control panel to easily create and manage users and groups?

- **Surveys**: Although this feature is not important for QROC objectives, some applications offer the possibility to launch surveys within the app. The users answer these surveys and the results can be integrated in any other system. Does the app allow us to create and send surveys to the users?

- **Calendar integration**: calendar integration is not a key feature for QROC objectives either, but it is also a feature offered by some of the Apps. Does the app allow users to send and accept/reject meeting appointments that are then integrated with the device calendar application?

- **Location module**: The number of mobile devices in the hands of LEA personnel in the operational field is increasing exponentially. The use of geo positioning systems to visualize and track police officers on the field and interact with them can be an important tool when conducting on field operations. This tool can facilitate the coordination of operations across borders and help us anticipate events and speed up the decision-making process.

- **SIM card no needed**: Does the user need a SIM card to register or to use the application?

d. **<u>INTEROPERABILITY</u>**: Blackberry Messenger failed to maintain his market position as a leader because they did not make the solution interoperable between different operating systems. In our case, interoperability between users from different countries is key to guarantee a quick and coordinated response to terrorist attacks or other type of events. The IM solution must allow LEA users from different countries to find and communicate quick and easily with each other. QROC needs a solution that is offering users a quick access to a central directory. Users will be able to find and chat with any user just by searching him by name, last name or even by his job description/position with no need or having his telephone number or email address. This feature will allow users and operators to establish communications quickly with anyone in the network offering a quick response tool to coordinate events. In summary, the solution must allow users and operators to easily access a centrally managed database, quickly create group chats and invite users to join and allow network federation (**compatibility between different networks)** so a Police Officer from Poland can connect with a German Police officer even if they are users from different networks. The IM application must facilitate the interoperability between similar applications deployed in several EU Member States.

e. **<u>FEASIBILITY (integration capacity)</u>**: the solution should be integrated with other internal systems to automatically send predefined messages and alerts after a trigger event take place:

- **API should let integrate the systems and internal procedures easily** (API REST). Does the solution offer a complete and easy to use API to integrate the IM solution with our internal systems/Apps? e.g. when new information about a terrorist suspect person is uploaded to our databases by any Member State, can this trigger and automatic alert message via the IM solution and distribute a PDF with the information to one or more users instantly?

- **HTML5 lets the user integrate the app with new open functionalities.** Integrated HTML5 Apps can be interesting to allow us to easily create and distribute simple Apps within the users' solution. This Apps can, for example, give webcam access to designated users from their device or even allow users, via a simple form, to introduce a citizen ID and instantly receive a PDF with his/her information from a central database. Does the solution offer a development framework to create HTML5 Apps that integrates within the messaging app?

f. **COMPLIANCE**: Certification and accreditation of the app is a need in some countries, not all Apps meet the security requirements, furthermore, the compliance with privacy and data protection is paramount to procure this software by public administration in order to not compromise the privacy and security of the systems.

   In order to comply with potential court obligations or data protection laws, the solution must offer "auditing capabilities" of the user activity and allow us to extract information to be able to respond to these possible future legal demands (**auditing capabilities in case legal compliance)**.

g. **PRICE**: Compares the price per user/month of the different solutions.

4. Benchmarking

Applications benchmarked in this report are those known by LEAs participating in QROC project. QROC is aware that there are more vendors in the market, especially in the covert domain, but also at national level. This report is not a technology scan, it is a comparison between Apps base on few criteria meeting some QROC purposes.

Information to benchmark has been obtained from internet in the case of Stashcat, Threema, WhatsApp, Microsoft Teams, Signal and Telegram, on the other side, from direct contact to IMBox and WhatSU providers.

There is a slight possibility that some of data in the next table are not accurate. In order to get accurate data to conduct a technology assessment, it is needed to contact directly with the Apps providers in order to get precise content about the main features of the solutions filling the criteria defined by QROC project.

Therefore, it is recommended for the reader to perform a deeper analysis or further study on instant messaging solutions.

	Stashcat	IMBox	Threema	WhatSU	Microsoft Teams	WhatsApp	Signal	Telegram
File and messages encryption	✓	✓	✓	✗	✓	✓	✓	✓
Mobile device data base encryption	✗	✓	✓	NA	✓	✗	✓	✗
Server data base encryption	✓	✓	NA	✗	✓	NA	✓	✓
IP Voice and video calls encryption	✗	✓	✓	NA	✓	✓	✓	✓
Secure file storage	✓	✓	✓	✗	✓	✓	✓	✓
Multi data centre for IN HOUSE System	✗	✓	✗	✓	✗	✗	✓	✗
MDM integration	✓	✓	✓	✓	✓	✗	✓	✗
Multi device (one account in several devices running at a time)	✗	✓	✗	✓	✓	✗	✓	✓
Admin panel for managing security settings	✓	✓	✓	✓	✓	✗	✗	✗

LDAP integration	✓	✓	✓	✓	✓	✗	✗	✗
Branding customizable	✓	✓	✓	✓	✓	✗	✓	✗
IN HOUSE System	✓	✓	✗	✓	✗	✗	✓	✗
Chat groups	✓	✓	✓	✓	✓	✓	✓	✓
Distribution list	✓	✓	✓	✓	✓	✗	✓	✓
Groups and lists without limit of members	✗	✓	✗	✗	✓	✗	✓	✓
Guest access	✓	✓	✓	✓	✓	✗	✓	✗
Users and group managing interface (panel)	✓	✓	✓	✓	✓	✗	✗	✗
Surveys	✓	✗	✓	✗	NA	✗	✓	✗
Calendar integration	✓	✗	✗	✗	✓	✗	✗	✗
Location module	✗	✓	✗	✗	NA	✗	✗	✗
SIM card no needed	✓	✓	✓	✗	✓	✗	✓	✓
Compatibility with several independent networks	✗	✓	NA	✓	✗	✗	✓	✗
API REST	✓	✓	✓	✓	✓	✗	✓	✓
Integrated applications/forms and services	✗	✓	✗	✗	✓	✗	✗	✗
Auditing capabilities in case of legal compliance	✓	✓	✗	✓	✓	✗	✗	✗
PRICE	3.90	0.5	1.3	0	5-20	0	0	0

Table 1: Benchmark table

Price per license per month is the last variable of the analysis. Public Apps are free of charge as their business model comes from using the user information for advertising purposes.

On the other hand, professional applications are not interested in our information and their business model is a service-based license fee. These companies have a maximum price and then volume price discounts are applying. The price benchmarking above is the price that each provider has when not applying volume discounts.

5. Conclusions

Public applications (WhatsApp and Telegram) should not be used to share sensitive information because:

1. Public solutions have not been designed to cover Security Forces needs and fail to guarantee the exhaustive privacy and security requirements of the information and the minimum control capabilities of the network. For example, the mobile database in Telegram and WhatsApp is not encrypted.
2. Public solutions do not allow us to create a private network, establish custom policy settings and manage users, groups, control access policies, etc.
3. Last but not least, public applications store the information in their own servers (mainly in the United States) and cannot be deployed ON PREMISE. When sending messages and files, uploading your phone agenda or even when sending your location, there is an international data transfer as this information travels and is stored in the company servers in the United States losing complete control over our information.

Unlike public solutions, professional applications are designed to cover the specific security requirements and needs of organizations in terms of security, architecture of the systems, usability, and interoperability. They are user friendly, offer lots of features and give tools for developers to integrate corporate systems within the messaging application.

To better understand our conclusions, the differences in regards with the architecture of the systems should be noted. There are three different architectures:

- Stashcat, IMBox, Threema and WhatSU with full architecture in premises (servers are in house with full control over information and communications)
- Signal offers a mixed architecture system, where information is stored in Signal servers (encrypted) but an IN-PREMISES server is stored all metadata of the communications. Both servers are used to store data.
- Microsoft Teams allow only the use of Microsoft cloud (Office 365) to store data and communication (we don't have any control over the data, even when data is totally encrypted. It does not allow full audits).

Stashcat, IMBox, Threema and WhatSU fulfil better the requirements to be implemented in QROC. While Signal does it partially, but as it is an open source application allow us to develop new features and developments.

We are to focus more on the first four mentioned applications (Stashcat, IMBox, Threema and WhatSU) with some references to Signal and Microsoft Teams.

In terms of security features WhatSU has currently less features than the rest of the professional tools even though they have most of them under development.

As stated before, security of the information in transit and at rest is one of the most important aspects when comparing professional Apps. Although all of them have the servers in premises, regarding high availability and catastrophe protection architecture, IMBox and WhatSU have both multi-data centre implementations. Stashcat and IMBox architecture seems more appropriate to guaranty the security of communications and storage of data, due to the fact that communications and server's storage are encrypted.

Stashcat, although encrypting the information stored in the IN-HOUSE servers, does not encrypt the mobile devices database. Threema does encrypt the mobile database but not the IN-HOUSE server's database, as it does not store any information in them. It is remarkable that the data in mobile devices is the minimum to run the applications and all data bases have to be downloaded each time the application is opened, remaining only a few data in the device in case it is lost or stolen. Although WhatSU does not store any information in the mobile database, they do store information in the IN-HOUSE servers that remain unencrypted.

On the other hand IMbox and WhatSU have multi-data centre that allow to have available backup data and get supplementary security through permissions when data is sent or have any type of access. They also offer the chance to implement additional security measures to detect possible attacks; both allow the integration of third party services to avoid DDos, man in the middle attacks, etc. IMbox is the only solution that encrypts the information both at rest in the IN-HOUSE servers and also in the mobile databases. Multi data-centre deployments allow us to deploy IMBox or WhatsU servers in different locations so, if one data centre is down or even destroy, not only the system will continue to work properly but the information will not be lost as it is distributed along different data centres.

Microsoft Teams is mainly a co-working application with an IM module to share information between co-workers. The IM module meets most of requirements than the other Apps but fails in multi data centre for IN PREMISES server.

Regarding network management and control (usability), all four Apps offer similar capabilities for network administrators to manage network security policies and privacy settings.

All of them are multiplatform. WhatSU is currently testing beta versions with several OS, while Stashcat and Threema don't allow users to use the app simultaneously in more than one device (according to their official websites). IMbox and WhatSU do allow multichannel functionality giving users the possibility to start session from different devices at the same time.

Functional features are very similar between Apps (chat groups, distribution lists, guest access, users and group managing interface, etc.) but there is a key difference between WhatSU and the others. While Stashcat, IMBox and Threema don't need a SIM card to be used (they can be used in any device with an internet connection), WhatSU does require a SIM card to function, which limits the use of the app to SIM card devices.

IMBox integrates a mobility/location platform allowing us to remotely coordinate and connect with on field officers while StashCat and Threema don't have this capability. WhatSU doesn't integrate this capability neither, as Belgium Federal Police uses another solution to locate mobile devices running in a parallel application.

Surveys are available in Stashcat and Threema while calendar integration is only available in StashCat.

Regarding group chats, IMBox does not limit the number of members in a group while the rest (Threema, Stashcat and WhatSU) limit the maximum number of users that can be invited to a group.

Interoperability and Integration capacity are key factors for QROC purposes as they will help speed up communications between different countries and also facilitate user access to centralized information databases. Even though all Apps offer an API for integrations (recall that Signal is open source code) and allow users from different countries to communicate, we need to highlight IMBox capabilities in this area because of the interoperability features (creation of different independent, but federal networks and the integration with HTML5 Apps, These Apps are really easy to create, deploy and integrate with OCs systems allowing users to fulfil everyday tasks directly from their mobile device)

All of them, except for Threema, which does not store any information in the servers, have auditing capabilities available. We should ask the providers how we will be able to comply with auditing obligations if required.

The price could become an important aspect depending on the number of users. WhatSU has been developed ad hoc for the Belgium Police so right now is free of charge for them (we need to understand if it will be free for other countries and whether they support thousands of concurrent connections to their servers or not).

WhatSU and Signal are free of charge; the less expensive solution is IMBox, followed by Threema and Stashcat. Microsoft Teams is the most expensive solution of all the Apps analysed.

It is also important to mention that both StashCat and IMBox are already installed in EU Agencies, StashCat in EU Lisa and IMBox in EUROPOL.

In our opinion, IMBox and Stashcat are the best Apps of the market to cover QROC purposes. Although Signal could become a good platform for new developments.

Therefore, our recommendations are:

1. To create a common sharing application based on existing Apps, open enough to be interoperable with other already existing Apps in EU Member States LEAs, in such a way that every country could adopt their own Apps to the common sharing architecture.
2. To use open source code or any existing open programming platform to create a new information sharing system ad hoc, totally compatible to existing OCs platforms.
3. It is also recommended to perform a deeper analysis or further study on IM solutions

References

[1] QROC deliverable D3.1 “Oversight of operational data and formats”.