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

Quick Response for Operational Centers

D3.4 – QROC Standing Operational Procedures

WP number and title	WP3 – European Operational Centers Cross Border Communication
Lead Beneficiary	IGPR
Contributor(s)	EUC
Deliverable type	Report
Planned delivery date	31/08/2020
Last Update	31/08/2020
Dissemination level	PU

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	05/08/2020	Draft	Ionuț Eduard Staicu (IGPR)	First draft
V0.2	12/08/2020	Draft	Jacques van Wersch (DITSS)	Contribution to all sections
V0.3	13/08/2020	Draft	Ionuț Eduard Staicu (IGPR)	Section 5
V0.4	23/08/2020	Draft	Floor Lams and Sander Donceel (Campus Vesta) Gerry Obrien (Garda)	Review and contribution to sections *Executive summary*, 1,2,4 and 6
V0.5	26/08/2020	Draft	Ionuț Eduard Staicu (IGPR)	Sections 1,2,4
V0.6	31/08/2020	Draft	George Kioumourtzis (DITSS), Jacques van Wersch (DITSS)	Corrections, final review and Quality assurance
V0.7	16/10/2020	Draft	Patrick Padding (DITSS)	Request for a second review to include feedback of participating LEAs
V0.8	10/11/2020	Draft	Ionuț Eduard Staicu (IGPR)	New version with the LEAs feedback
V1.0	16/11/2020	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
PMC	Project Management Committee
PCG	Project Coordination Group
QC	Quality Control
NGO	Non-governmental Organization
NPO	Non-Profit Organization
RTO	Research & Technology Organization
SME	Small- and Medium-sized Enterprise
UNI	University
GDPR	General Data Protection Regulation
DSA	Data Sharing Agreement
MDM	Mobile Device Management
LDAP	Lightweight Directory Access Protocol
SSL	Secure Socket Layers
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman
TIG	Technology Interest Group

Table of Contents

Executive summary

The present document is a result of all the previous work conducted in the project and is intended to give a clear view of the way the information sharing process will be performed.

QROC Standing Operational Procedures for Information Sharing aims to help the partners to agree on the conditions for cross border information sharing. The main objectives of the deliverable are to establish when, for what purposes, and how the new capabilities of selected technologies will be used.

The document reviews the activities performed so far, that set up the base for the QROC Standing Operational Procedures for Information Sharing.

The main sections of the document are:

1. Introduction
2. Procedure overview
3. When and for what purpose LEAs should share information
4. How the new capability selected technologies will be used
5. Data protection
6. Conclusions
7. References

The procedures for information sharing depend very much on the particular legislation of every LEA. A key element of the procedure is the new tool that will cover the needs of the process. Testing and the usage of the new tool in the forthcoming stages of the project will add up the main directions of the procedure.

The present document aims to regulate *when, why and how* information sharing will be realized as part of the whole process.

1 Introduction

1.1. Purpose and Background of the agreement (review)

Purpose

The Quick Response for Operational Centre's (hereinafter referred to as QROC) project is an initiative of the Core group of the European Network of Law Enforcement Technology Services (ENLETS) and is funded by the Internal Security Fund of the European Commission. It runs from October 2019 until September 2021.

The general objective of the project is to provide all EU member states National Operational Centre's (hereinafter referred to as NOCs) with an increased level of response capability to protect the public and public spaces against terrorist attacks and CBRN-E threats by:

1. Implementing a Pan European communication capability that connects member states NOCs, enabling them to exchange indispensable needed operational data related to a terrorist (and CBRN-E) attack to steer their preparedness and Command and Control Decision making process to protect the Public and Public places.

2. Enabling access to innovation and sharing best practices for Operational Centre's (hereinafter referred to as OCs) to handle data flows for Command and Control Decision making in OCs for public protection, specifically regarding 5G, autonomous drones, surveillance video and data management technologies, and where relevant integrated with the aforementioned international communication capability. This knowledge will also be shared using the PISP of the I-LEAD project.

3. Incorporating the aforementioned priorities, providing education and training based upon three real case scenarios; man hunt, Public Protection management and CBRN-e threats with the objective to exchange best practices and to improve the capabilities of National Operational OCs in public protection.

Background of the agreement

In June 2016 ENLETS had organized a cross border exercise, testing the member states capacity in an emerging cross border threat. It was proven that OCs in surrounding member states are "blindly waiting" when an attack occurs, whilst a terrorist is on the run and an immediate information exchange is needed. The follow-up took place in 2017 when an ENLETS Technology Interest Group (TIG), named 'National Operational Centre's' started within the ENLETS Security and Technology Program (ESTP). Results of the TIG indicated that during the incidents 'golden hour', there is a lack of common capabilities to directly share (push) information between member states. During the 'golden hour' it is absolute essential that information can be shared swiftly between Law Enforcement Agencies, with the least possible delay, in order to increase the detection and detaining of the suspect(s) and stopping the incident. No data such as photos, video's, surveillance record, GPS data or other information could be exchanged, as law enforcement is depending on radio systems (Tetra, Tetrapol) or Pan-European information systems, such as the Schengen information system, unable to process swiftly and directly data which holds other formats or of large sizes. In addition, the extended possibilities for exchanging cross-border information based on European treaties, between member states and frameworks, has not always led to exchanging cross-border information partly caused by the lack of knowledge, lack of trust and lack of a common agreed approach. Despite these facts, there was broad consensus among OCs that there is a need of a pan European approach to establish fast cross border data exchange. The development of a common approach should also take into account the way in which the OCs are anchored organizationally and procedurally within the Member States. Operators of different channels can be geographically separated. This can affect the development of a cross border exchange mechanism.

1.2. Purpose of the procedure

In this activity the LEA partners will agree on the conditions for cross border information sharing, respectively when, for what purpose, and how new capabilities of selected technologies will be used and tested.

The information sharing process will take place in certain situations which have determined the present project, these are: terrorist threats and attacks, CBRN-E threats, and similar situations. In such situations, there are multiple time frames for taking action, each one with its particularities. The most important interval of time is the reaction time in the *golden hour*, meaning the time before an imminent event and the time immediately after it happens. The procedure should offer the framework and the tools to communicate and efficiently share information in order to get the best possible results.

Clearly the main purpose is to raise the level of response and of the results of LEAs in the situations mentioned above.

How the capabilities are to be used is the third main objective of the procedure. This section should establish and clarify the technical instruments and means and the judicial framework needed for this process.

2 Procedure overview

The effective cross-border exchange of LEAs information and intelligence is of great importance for preventing and combating crimes. It is therefore necessary that LEAs are able to share information and intelligence in fast and effective ways.

In the current context, when a terrorist is on the run" the *days of working in isolation should be gone''*, collaboration between LEAs is the only way to address terrorist acts that threaten Europe. An integrated policy is critical to reach the goal commonly shared by EU countries, to prevent terrorist activities that damage our collective sense of security.

Right now, all LEAs find themselves with disparate communication systems that are unable to share critical data.

There are considerable challenges in enabling information to be fully and promptly exchanged. These challenges include technical IT capabilities, availability of encrypted information networks and common or mutually understood security classifications. Workflows within LEAs are different for a number of good reasons, depending mainly on national structures.

In addition to legal instruments, communication channels, workflows and human factors also need to be taken into account. Significant cultural and working practice differences exist within the LEAs and these differences often have an impact on the approaches and attitude to cross-border information exchange.

The main goal should be harmonization and gaining synergies without affecting each state sovereignty.

3 When and for what purpose LEAs should share information

When making decisions about what information to share, after verifying the information, we should consider the relevance of the information in relation with the event.

Only information that is relevant and adequate to the purpose should be shared. Also, information should be of the right quality to ensure that it can be understood and relied upon.

Information should be accurate and up to date and should clearly distinguish between fact and opinion.

There are multiple situations when sharing information is vital in case of terrorist threats or attacks. In each situation there are different stages and critical moments that require different approaches. The present procedure aims to set up the right ways to act in each situation and each timeframe of an event or threat.

The procedure should clarify what actions are to be taken before an imminent event when certain information leads to this conclusion, during the event or in the aftermaths.

Information should be shared in a timely fashion to ensure the:

1. Prevention of crime and disorder;
2. Maintaining of public safety;
3. Apprehension of offenders;
4. Detection of crime.

The purpose of the information exchange is to prevent the predictable unpleasant events and also to react in order to apprehend the offenders in case of events.

To reach these goals the process of information exchange must be quick, relevant and adequate.

4 How the new capability's selected technologies will be used

In the matter of how the information exchange will take place, the most significant aspects are the instruments that are going to be used and also the data sharing agreement that the members will conclude on.

Based on the previous documentation in this project, the most suitable information exchange tool at the moment is the Stashcat application, which has been selected. Stashcat is being used in an attempt to show that cross border communication could be unified, using one system.

According to [1], Stashcat offers the capabilities and resources to perform the information exchange in the most effective way based on a previous assessment in [2], as follows:

The most critical aspect of the information exchange software is unification. Europe is composed of 27 member countries, having one information exchange tool amongst LEAs for Europe ensures a high volume of users and therefore high data. It increases the possibilities of preventing unwanted outcomes through a unified effort of information exchange. Since Stashcat is being used by the German LEAs and paid for by the I-Lead project [3], choosing a different software would go against the goal of unified information exchange. Using a tool that others are using in the same domain is Management by example and paves the way for others to join. Moreover, depending on the policy of member states and their willingness to give access to a dedicated and secure server, Cloud solutions are also possible for storage and exchange. Maintenance and further development are based on the number of the people that are using the software, if the volume of users increases, maintenance will follow. Finally, Stashcat provides functionality, as it fulfils our project's needs of information exchange without compromising security and by providing a user-friendly platform [4].

There are some technicalities involving the level of dissemination, referring to the police officers installing the application on their professional phone in a secure way and having access to their police data. Stashcat has a mobile device management system which allows for access to network and data from personal devices, regardless of the location. Since Stashcat provides mobile access; a lot of server related issues could be solved by using additional software, an example of which is Projectplace where you can access the data when logging in. However, as it is not available for all devices, communication will be restricted only to those who use the devices that Stashcat is designed for. Stashcat runs on all mobile and stationary devices that use Android, iOS and for Desktop or mobile. According to [5], this software can support the various formats in use, such as photo sharing, documents, video clips, live videos, voice recordings (Voice over IP is currently being developed) and spatial information.

Stashcat was selected as the **Permanent Information Sharing Platform** (PISP) in the I-Lead project. The purpose was to increase the sharing of information among Law Enforcement Agencies. To achieve this, separate channels were created, covering the five key areas of law enforcement: **Front Line Policing, Cross Border, Cybercrime, Crime and Forensics**. These channels serve as the knowledge and experience transfer of the I-LEAD main working areas.

Stashcat has the following features:

1. Single chats
2. Channels
3. Calendar
4. File storage
5. Survey tool
6. Georeferencing
7. Other features such as:
    a. Branding
    b. MDM

c. LDAP
d. Guest access
e. Folder synchronization
f. Broadcast lists
g. Phone and video conferences
h. Voice over IP technology

How the selected technology will be integrated as the instrument of information exchange among LEAs is a result of a process that requires time and resources such as: training, procurement and testing.

According to the QROC forecasted activities [6], D3.5 provides the following stages of implementation:

> *1. Phase 1- Procurement: In this phase within the new EU-LISA mandate and with the support of EU-LISA, the project **will procure licenses for all project LEA partners** to use the new capabilities.*
>
> *2. Phase 2- Implementation: This is the implementation phase where the project will install related solutions on the EU-LISA servers.*
>
> *3. Phase 3– Testing: In this phase, all LEA partners in the consortium will test the new capability as part of the training scenarios within WP5, including also the tabletop exercises. Results will be reported in [6] and [7] and if successful, a formal request will be initiated from the QR-OC members to the Commission services and EU-LISA for a final implementation.*

Only after using and testing the communication instruments, the procedure of effective information sharing can be completed.

5 Data protection

The General Data Protection Regulation (GDPR) entered into force on the 24th May 2016 and took effect on the 25 May 2018. Processing of personal data for "law enforcement purposes" is not covered by the GDPR but by the Law Enforcement Directive, which replaced the European Council Framework Decision 2008/977/JHA. The directive was enforced on 5 May 2016 and EU countries had to transpose it into their national law by 6 May 2018.

Effective Information sharing among Law Enforcement Agencies has become a critical aspect in their ability to detect, prevent and respond to their daily tasks. Information systems are used to capture data and make it broadly available to authorized users in a timely and secure manner. In the case of cross-border communications, this proves challenging for technical and other reasons.

All information should be stored in a registration system and, in doing so, should abide the rules for protecting human rights.

This deliverable will be used to ensure that sharing information is carried out in an accurate, adequate, timely and lawful manner.

In order to reach the objectives, the LEAs will:

1. Ensure that all the information will only be used for the reasons it has been obtained, considering the rights of the individual and the law;
2. Ensure that all the information is shared in a secure and confidential manner;
3. Establish appropriate management and administrative practices to facilitate the information sharing;
4. Ensure that all staff are supported in understanding their responsibilities when sharing information;
5. Ensure that all shared information is recorded, reasons should be cited including what information has been shared and with whom.

Data protection and security depends not only on the procedures, but also on the quality and performance of the instruments used for communication. Regarding that, D2.4 Cross Border Knowledge Base treats this subject in detail:

Due to the sensitive nature of the information passed, security remains a top priority for the successful exchange of information. The deployment of Stashcat takes place centrally on encrypted, redundant servers, which are operated by a private company in a high-security center in Munich, Germany. The company places huge efforts for the protection of the data centers and moreover provide summaries about technical and organizational activities regarding the protection of data, which are available to every client [4].

Security is achieved through encryption, more specifically, end-to-end encryption across all transmission paths[8]. Frequent, automatic online backups take place, to avoid the loss of data through hardware failure, virus attacks or act of nature. All relevant data is secured through the latest SSL encryption methods where protection takes when the date is on the way to the servers and encrypts the data exchange between the server and terminal device. Encryption on the user's terminal device takes place where the data is encrypted through a combination of AES and RSA algorithms. Every user has a public and a private key to communicate via Stashcat. The private key is encrypted by a password chosen by the user. The private key is encrypted by a password chosen by the user. When a conversation is created, a random key is generated. The keys are generated with a cryptographically secure random generator. This way, users can be sure that neither unauthorized third parties nor the Stashcat team itself can decrypt or access any data. All relevant data is thus transmitted encrypted on the way to and from the server and stored there also encrypted. Encryption

applies to all types of data [9]. Moreover, it is a GDPR-compliant messenger platform which is necessary to maintain secure and efficient data management practices by providing enhanced capabilities for data analysis, data quality and data handling [8].

6 Conclusions

The overall objective of WP3 is to implement a cross border data exchange mechanism between the National Operational Centres, to share operational data peer to peer and to ensure a direct and immediate response after a terrorist attack/ CBRN-e threats.

This new Capability Package (CP) mechanism will exist out of, among others, an EU-LISA portal that will be accessible 24/7, for Operational Centers to share the information of an (ongoing) incident. Integrated with an application for mobile phones (Stashcat), the capability can be used anywhere, anytime, therefore connecting operational officers from several member states.

This capability will not replace any other formal EU data exchange, but it is based on a need & gaps analysis done by various EU ENLETS members. The conclusion of the ENLETS Operational Centers TIG is that a direct, modern exchange and secure mechanism is necessary. Innovative solutions, allowing a swift and highly secure exchange of data, have been considered and analyzed concluding that Stashcat is at present time the most suitable. In the future, at the moment of the communication instrument purchase, a new market research shall be done, to find the best provider and application.

Information sharing enables early intervention and preventative work to safeguard and promote welfare, as well as for wider public protection.

The procedure for information sharing is a critical part of the entire framework. At the present time of the project, the procedure is subject to additions, correction and improvements, especially in the forthcoming stages of implementation and testing.

The present deliverable sets up the guidelines and the frame for the detailed procedure, that is aimed to include judicial parameters of each member, the specific experience and also the results of the testing stages.

The results of the project, the future actions and also the restrictions on the exchange of information will be subject to the law of each partner of the agreement.

References

[1] QROC D2.4 “QROC Cross border knowledge base”.

[2] QROC D3.2 “Data sharing agreement between QROC OCs”.

[3] Innovation – Law Enforcement Agencies Dialogue “I-LEAD”, available online at: http://i-lead.eu/

[4] "Emergency Communication", Stashcat.com, 2020. [Online]. Available: https://stashcat.com/en/emergency-communication. [Accessed: 12- Jul- 2020].

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

[6] QROC D3.5 “Implementation report”.

[7] QROC D3.6 “Testing results”.

[8] Frequentis AG", Stashcat.com, 2020. Available: https://stashcat.com/en/references/partner-frequentis. [Accessed: 20- Jun- 2020].

[9] Stashcat Encryption Technologies” can be provided upon request.

ANNEX I. EXPLANATORY NOTES

According to the QROC forecasted activities, D3.4 – QROC Standing Operational Procedures is supposed to be subject to the partners agreement on when, for what purposes, and how the new capability selected technologies will be used. Therefore, an agreement on the conditions for the cross-border information exchange was formally requested through a questionnaire sent to each participating LEA. Following this final stage of the activity the feedback on the procedure was collected and integrated, resulting the final form of the deliverable.

The final form of the D3.4 deliverable was agreed on by four LEAs, without any remarks, respectively:

- POLICEJNI PREZIDIUM CESKE REPUBLIKY
- MINISTRSTVO ZA NOTRANJE ZADEVE REPUBLIKE SLOVENIJE, POLICIJA
- AN GARDA SIOCHANA
- COMMUNICATION AND INFORMATION SYSTEMS DIRECTORATE

Remarks and suggestions were provided by the following LEAS:

- THE NATIONAL POLICE OF THE NETHERLANDS
- HELLENIC POLICE
- POLIISIHALLITUS

All their observations were taken into account and have been used to update the deliverable.

Four other LEAs did not send any answer or remarks and we conclude they agree with the procedure.