Near border information exchange procedures for law enforcement authorities

Jyri Rajamäki, and Jouni Viitanen

***Abstract*—**European integration has increased organized crime, e.g. the transport of illegal goods in Europe. This means that the transmitting of tracking and other status information between nations and their Law Enforcement Authorities (LEAs) should become an everyday business. The goal of this paper is to find possible bottle necks in international cooperation between LEAs and to find possible solutions for them. The following area can be considered as a part of the MACICO (Multi-Agency Cooperation In Cross-border Operations) Celtic Plus research project. The target of the paper is to present administrative and technical solutions to improve multi-organizational tracking solutions. Namely, the goal is to make it possible to create a timely situational picture in joint multinational and interagency operations. This paper will provide guidance for preparing appropriate plans and doctrine proposals for joint operations and training. Also technical solutions and bottlenecks are briefly covered in this paper.

***Keywords*—**Cross-border operations, Emergency communications, Law enforcement, Law enforcement authorities, Public key infrastructure, Public safety.

I. Introduction

Organized crime is a real threat around the globe. Law Enforcement Authorities (LEAs) are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organizations. Organized crime is an international business whereas operational LEAs are mostly national organizations. This creates a pressure for improved cooperation between LEAs. However, LEA organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared to empower joint responses to threats and crisis in an increasingly interconnected network, but also LEA organizations have to benefit from interoperability functionality in their day-to-day work.

Multi-Agency Cooperation In Cross-border Operations (MACICO) is the Celtic-Plus project with nine partners from Finland, France and Spain [1]. The duration of the project is Dec 2011 – May 2014. It develops a concept for interworking for security organizations in their daily activity. It deals with cooperation of security organizations that do not use (in their day-to-day job) the same radio network, but in some missions could take benefit from a sharing of their respective infrastructure. Use cases such as pursuit of criminals across a border, close support of vehicles going through a border, and disaster relief operations require security organizations from both countries to communicate together and to continue to communicate with their control room.

A. Administrative Challenges

When an illegal incident has come to a law enforcement official's knowledge, (s)he must act, and omitting to act may result in legal actions. Failing to obtain or share information from or with the partners, however, is mostly a volunteer action, although this information could prevent something unwanted. Furthermore, information sharing is often a complicated legal issue. Therefore, exclusion of information sharing is a much easier and safer choice for the officers' own well-being.

During crisis situations, the information exchange between people from different organizations is often done informally. These contacts are not institutionalized but are set up on a personal basis. Information is shared more easily with people that one knows and trusts [2]. If the information exchange is based from beginning to end on personal contacts, technology can create only limited help. Another disadvantage is a dependency of key persons. Absenteeism or loss of any individual should not be a threat to public safety. For these reasons, it is not acceptable that real-time information sharing in law enforcement between parties is based on personal contacts.

At the EU-level, law enforcement organizations are exchanging information. EUROPOL is the European law enforcement organization which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organized crime [3]. EUROPOL's task is to handle criminal intelligence. EUROPOL works mainly on a political level because, at the operational level, the pursuit of Europol is simply too slow. Therefore, additional principles agreed to beforehand are needed. Currently, the change of information between LEA organizations helps just in the case of investigation or in statistics, but not at the operational level.

B. Target of the Paper

The ICT services supporting LEAs' surveillance operations

This work was supported in part by EUREKA Celtic Plus programme and Tekes—the Finnish Funding Agency for Technology under the MACICO (Multi-Agency Cooperation In Cross-border Operations) project.

J. Rajamäki is with the Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland (phone: +358 40 7642 750; e-mail: jyri.rajamaki@laurea.fi).

have usually been developed by national agencies, although some commercial devices are nowadays more widely in use. Many of the solution providers offer integrated systems, where sensors and mapping software are combined. Traditionally these systems are designed to be standalone services with no built-in way to communicate with other mapping systems. If some interface and protocol exists, the possibility to send properties and status information, so-called metadata, is still missing. Differences between devices, protocols and background systems have caused problems for international cooperation, simply due to lack of commonly agreed operational procedures and technical interfaces [4].

This paper discusses what challenges borders brings to LEAs. It also presents a system how LEAs can exchange and share critical information. The paper answers how to provide efficiency and consistent Public Key Infrastructure functionality. The main question is how LEAs can identify the counterparty player securely. A LEA organization must be able to trust outputs and inputs.

II. Cross-border Challenges for LEAs

LEA use more tracking technology than ever before. Early systems applied point-to-point technology, in which the surveillance team was receiving the information through point-to-point radio communication. Today's systems are TCP/IP-based and law enforcement officers can send and receive the information basically anywhere. Many cross-border joint ventures are targeted at some big incidents, although smaller separate cases together are creating the biggest flow. This means that all the cases cannot go through the same hierarchical command system, because the huge number of cases.

Unfortunately, borders create delays for LEA as discussed in [5] and shown in Figures 1. Therefore a proactive crime preventing work will often change into reactive investigations [4]. "0 Situation at first" on the top of Figure 1 presents a normal real-time tracking situation, where the local LEA is getting the target's position in near real-time, only with a few seconds delay. "1 Point of caution" presents the point when the LEA starts to be worried that the target might go across the border, but the tracking is still near real-time. A border is a very thin line, and if LEA officers want to be successful, they need timely information about both sides of the border. Border guards are very seldom responsible for tracking, so in many cases they do not have the information. After the target crosses the border ("2 Bureaucratic challenges"), the trouble starts. The target's timeline is still straightforward, but now the LEA starts to use time in discussions with superiors to find out how to proceed in the new situation. There is still no information on the border or on the other side. The exchange of information with people from other organizations during crisis situations is often done informally. These contacts are not institutionalized, but are established on a personal basis. Information is shared more easily with people that one knows and trusts. Is it acceptable that real-time information sharing in law enforcement between parties is based on personal

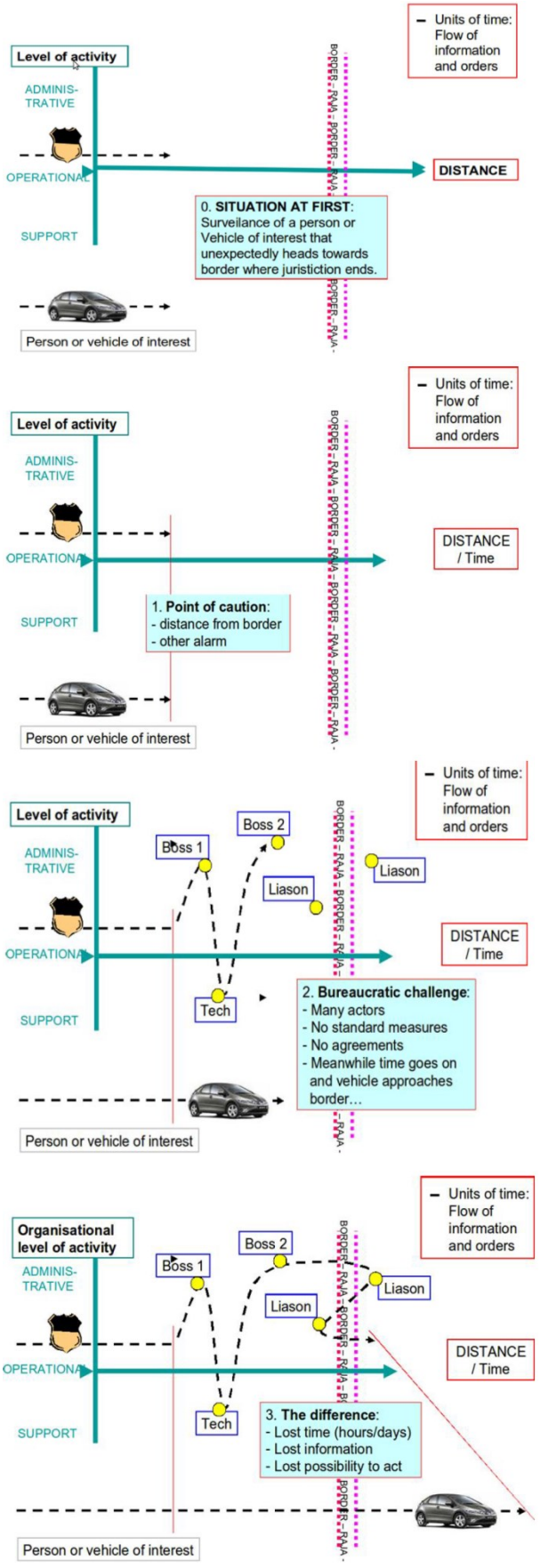

Figure 1. Flow of information and movements of target at the border crossing situation (adapted from [4])

contacts? Nowadays it is commonly the only way to change metadata about the properties and status of the target. If the information exchange is based completely on personal contacts, it is clear that technology can create only limited help. Another disadvantage is dependency of the key persons. Absenteeism or loss of a key individual who cannot be readily replaced should not be a threat to public safety. The real-time tracking might be still on, but the target is over the border and the information stays on the wrong side of the border as seen on the bottom of Figure 1.

III. Proposed System

Operational procedures should be as follows: Decisions should be taken at the lowest appropriate level with coordination at the highest necessary level. The doctrine and training describe the way in which people, processes and technology combine to enhance decision making through the use of a common operating picture that provides mission critical information available to appropriate staff.

When building up LEAs' multinational sensor data exchange system, increased costs are minor when compared to benefits of international cooperation of authorities. Shared data should be considered critical information, and therefore appropriate data protection is required. More and more information and communications have become network-based, and accordingly the number of cyber-security incidents has increased. Although some nations have already established critical information infrastructure protection (CIIP) laws [6], international legislation is still missing.

When an information infrastructure is installed and all functions are tested, the system should be tested against external and also internal cyber-attacks to find possible vulnerabilities. Protection against external attacks and alternative routing with different IP addresses should be tested to provide necessary reliability for the system. Ref. [7] is one useful aid for planning security tests.

Suitable ways for exchanging and sharing information between LEAs with no delays should be found; certain protocols and operational procedures are needed. The possibility to adopt already existing methods, for example from military organizations, should be considered. Currently the National Marine Electronics Association (NMEA) protocol [8] is used in some international situations, but for real-time surveillance it is not sufficient. For example, the NMEA protocol does not provide the possibility to send metadata.

A. Network Topology

The lack of a transmission protocol is not the only issue in developing a multinational LEA network; also the network topology has to be agreed. Figure 2 shows a high-level network topology, in which all data transfer is encrypted and protected with a virtual private network (VPN). If the data should be encrypted inside VPN, the easiest way is to use a common Public Key Infrastructure (PKI) solution. All the public keys should be stored in one server connectible via VPN.

When a connection to another LEA organizations' data source is needed, the transmitting server acquires needed public keys from the dedicated server, then encrypts and sends messages to the receiver. When the receiving server gets a new encrypted message, it automatically decrypts the data.

Also, reliable ways to exchange additional information during cross-border operations is needed. This so-called metadata contains necessary information about the target and therefore should also be transmitted to the foreign LEAs. Metadata can include details about the target vehicle, possible risks of the target (e.g. armed) and preferred actions against the target. Like always, all data should be encrypted. All metadata should be sent along with the spatial information.

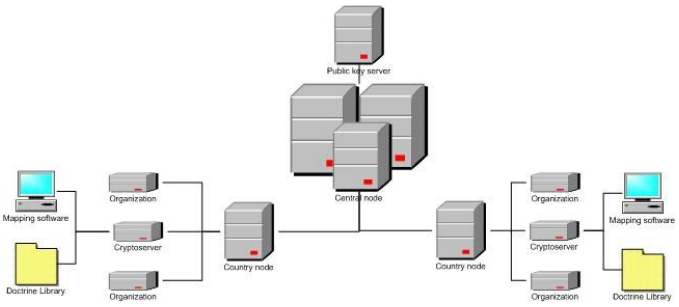

Figure 2. High-level Network Topology [9]

Figure 2 is a high-level description, and too general for practical implementations. The mapping server should relay information to the right units utilizing metadata status and properties. Also, the sub-systems of Figure 2 are of a different level; for example, real time data is not applicable in all command and control rooms, and they should get data in the right formation and at the right speed. However, data should be exchanged from the LEA of one country to the LEA of another country, so that the national requirements for digital evidences will be fulfilled.

B. Metadata status and properties

In social sciences people are frequently classified according to their behavior, preferences or similar needs. The classification of similar objects into groups is also important in LEAs. The methods and resources ordered to a case vary very much depending on the case. A small scale weed smuggler doesn't get as much resources as a terrorist group aiming to attack a nuclear plant. Also the dealing with these two cases usually belong to two totally different units or departments.

It's not possible to create efficient information exchange for LEA before there is a commonly agreed cluster or some other similar system to classify crime, criminals and their preferences. There cannot be an automated information exchange for LEA before there are commonly agreed ways to describe the status and properties.

There is no use to transmit only the position information forward. What can you do if you have couple of dots on the map but you don't know, what those dots present and what their threats and preferences are. Only when you know that,

you can start allocating the right LEA resources to the case.

If the metadata is still exchanged as before, using personal contacts and by telephone or e-mails, you will lose the benefits of an automated system. However, in this paper we don't go deeper into this metadata clustering problem, but we are planning to do further research of the subject.

C. *PKI Operations Model*

Public Key Infrastructure operations model idea is based on ISF (Information Security Forum) best practices and modified for a financial company. The model idea is that it serves as a basic package to new PKI projects. The model is divided to 16 different processes as shown in Figure 3. All these processes

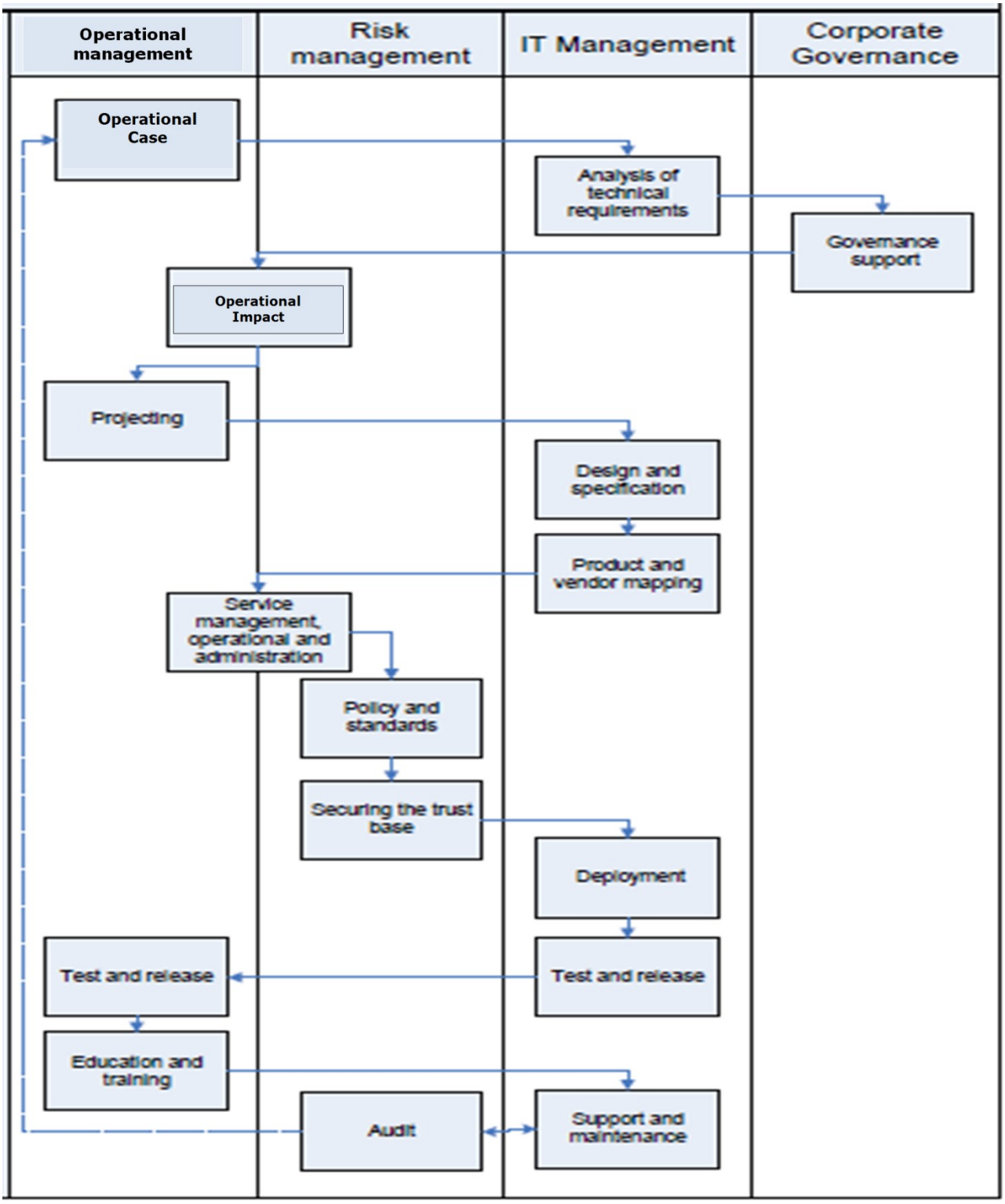

Figure 3. PKI Operations Model (adapted from [[10])

have their own role and owners. Process owners have divided to four different roles. Sometimes process significance might be trivial, other times the process might prove vital for the project. Good example is the Policy and standard process. First time an organization must build this document, it might be a large undertaking for the organization. However, in next project this process is only applied for updating valid policies.

Everything starts from LEAs operational needs. It is important that the operational part is leading this conversation. IT management and Risk management is supporting this study. This is an important phase because it is here that most of the metrics are defined. In the end these metrics define how successful the project was. Model is PKI project best practices. This is the reason why all processes are described separate processes. All phases give advice on what must be done and what should be done. In the end it's always a company or project decision what to do in the different kind of PKI projects. This is not a model for how to run a PKI project. It does not concern with how to come up with a project budget, or how to keep project meetings. When a certain project adapts this model it assumes that all basic project process practices are defined beforehand. Normally organizations have their own project model what they follow or they can follow PMBOK guide [11].Operational case phase is a regular operational process case. This process should come from LEA's own operational environment. There are no specific PKI demands in the operational case phase. From a security point of view these phases should have their own detailed guide on how to estimate what are the costs to security environment. How to estimate what is really needed so future projects do not build extra secure or fully automated environments without any benefit.

In the analysis of technical requirements the organization should follow know standards like ISO 27000 or PCI. Good example is best practices in [12]. It is important to go through all in the analysis stage as LEA can easily notice if some area, like the physical environment, is missing. Normally projects think only for valid environments. There might be similarities and projects can save cost and time. Also, if environment is outsources it helps environment deployment.

Governance support like senior management support is vital for the security projects. These are persons who can make decisions so projects avoid delays because of lack of decisions. Model gives basic knowledge for governance support but this is normally depended on the manager. E.g., an inside project manager has better connections to senior management. Sometimes this is a good thing and at other times this is a problem.

Operational impact phase needs more detail information how to evaluate real impact. This phase needs a check list for the actors. There is always something what must be taken in the consideration. That is the reason why best practice check list is needed.

Projecting phase is a standard stage in the projects. This phase should give more detail information where project manager can find guidelines and best practices on how to set up a project.

Design and specification phase is what to write so an environment can be done. This is more technical than others. It is important that technical personnel of the project are participating. At this phase all operational needs must be known by the project design group. These specifications should be reviewed with the operational personnel.

Product and vendor mapping phase are decisions what service provider or program company are using. This phase needs more information from e.g. ITIL; the project can find of processes for finding right product and vendor. There should be e.g. specified RFO (Request for Order) and RFP (Request for Proposal) processes.

Service management, operational and administration phase is fully implemented from ITIL. Maybe some special detail for PKI or security can be found. Basically these processes are almost same in all IT sector. Model should follow ITIL process steps with PKI information.

The policy and standards phase is more detailed to PKI and security issues. PKI and security have their own security policies and practice statement models what to follow. During this phase it is always important to remember that organizations have their own security policies what they must follow.

Securing the trust base phase tells company what was the PKI policy state because this phase is based on that. In this phase all the PKI policy stages must be checked so that all is done as in the defined policy. PKI policy is an inclusive guide, ranging from technical to legal issues. So this phase needs time to pass.

Deployment phase is about the technical issues. In this phase all plans are built to use. It is very important to follow specifications so all is done in the right order and in the right way. Normally in this phase it is noticed whether something is not planned. These new specification add-ons must be described and approved by the management. Also it is import calculate new costs.

Test and release phase is where project needs more hands on personnel because there are lots of different tasks. Normal situation an organization has its own test and release processes. If not, organization should follow some known standard or best practice like ITIL. ITIL has already solved basic problems with this phase. This implementation model should follow more ITIL process. These basic ITIL processes need all kind of authorities.

Education and training phase is easiest to drop out from the plans. Yet it is still an important part. This phase is for the new users and for the rest of the company to know what this project focuses on. Company should have its own security education and training program. This should be only one part of that. Project has massive work to do if company does not have any program of its own. This must be taken care of in the project time table.

Support and maintenance phase is important for continuity. LEA should have already working support and maintenance processes. This is only for PKI implementation to that. Also this is lighter if services are outsourced because of some services are provided by the vendor. LEA should follow ITIL

processes if company does not have already these processes on place. During this phase LEA must consider whether the PKI services are open always or can the hours be limited to business hours.

The audit phase is compulsory for some sectors. This means that LEA should have an audit process on place like specification audits and environment audits. Normally these are added to LEA's own project processes. During the audit phase LEA should use COBIT models. Company separate full COBIT implementation from project work.

IV. Discussions and Conclusions

The paper discusses about the administrative challenges that occur when non-cooperative target of law enforcement technical tracking crosses the border. When LEAs exchange information, validation and authentication is needed. Credentials should meet a set of requirements to be accepted [13]. This paper presents the artifact of Public Key Infrastructure operations model. This model offers the first steps on what must be done in PKI project. It provides a partial answer on how to develop faster, more efficient, and safer PKI services. The paper results are derived from a real PKI project in the financial sector, but these kinds of projects are comparable with one another.

The model phases in Figure 3 are not at the same operational level. Some phases are light business/operational decisions and so are detailed technical assignments. Model needs some kind of estimation about the timetable. Every phase should have its own duration estimate. Also, the model needs an estimate on what phases can be done at the same time and what phases are depended on each other. It also needs actors. Every phase should have information concerning who is responsible for that phase and who must participate in that phase. Project manager carries the overall responsibility but every phase needs its own responsible person such as the audit risk manager or for technical environment setups the technical architect.

The classification of subjects is an important risk management tool for LEAs. The methods and resources ordered to a case vary very much depending on the case; smuggler doesn't get as much resources as a terrorist group. The creation of an efficient information exchange tool for LEA is impossible before there is a commonly agreed procedure to classify crime, criminals and their preferences. An automated information exchange system for LEAs requires commonly agreed ways to describe the status and properties. For example, transmitting of position information forward is useless, if you do not know what those dots present and what their threats and preferences are. Only when you know these facts, you can start allocating the right LEA resources to the case. If the metadata is exchanged by phone or e-mails, you will lose the benefits of an automated system.

Our main conclusions are that because crime is internationalized, LEAs need automated data exchange systems. However, prior to these systems are possible to create, the metadata clustering problem should be resolved. This needs much further research.

References

[1] L. Drouglazet, J. Rajamäki, J. Tyni and M. Aro, "Multi-agency cooperation in cross-border operations (MACICO) project," in *Proceedings of the 8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14),* 2014, pp. 129-136.

[2] W. Muhren, M. Jaarva, K. Rintakoski and J. Sundqvist, "Information sharing and interoperability in national, cross-border and international crisis management," *Crisis Management Initiative, Tilburg University, Crisis Management Centre Finland & Elisa Ltd,* 2008.

[3] *The European Police Office*. DOI: http://www.europol.europa.eu

[4] J. Viitanen, M. Happonen, P. Patama and J. Rajamäki, "Near border procedures for tracking information," *WSEAS TRANSACTIONS on SYSTEMS,* vol. 9, pp. 223-232, 2010.

[5] P. Kämppi, J. Tyni and J. Rajamäki, "Use cases of the multi-agency cooperation in cross-border operations (MACICO) project," in *Proceedings of the 8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14),* Tenerife, Spain, 2014, pp. 209-212.

[6] S. Park and W. Yi, "The evaluation criteria for designation of critical information infrastructure," in *Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy,* 2009, pp. 77-83.

[7] V. Patriciu and A. C. Furtuna, "Guide for designing cyber security exercises," in *Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy,* 2009, pp. 172-177.

[8] *NMEA*. DOI: http://www.nmea.org/.

[9] J. Rajamäki, "Cross-border information exchange between law enforcement authorities," in *Recent Advances in Computer Engineering, Communications and Information Technology,* Tenerife, Spain, 2014, pp. 205-210.

[10] P. Ruohomäki, "Public Key Infrastructure operations model," Thesues. Espoo: Laurea 2012.

[11] Project Management Institute, "A guide to the project management body of knowledge: PMBOK® guide," 2008.

[12] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, "Key Management Inserts for Security Plan Templates," 2002.

[13] A. FONGEN, "Validation of Inferior Identity Credentials," in *Recent Advances in Computer Engineering, Communications and Information Technology,* Tenerife, Spain, 2014, pp. 49-56.