Cross-border Information Exchange between Law Enforcement Authorities

JYRI RAJAMÄKI
Service Innovation and Design, Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
jyri.rajamaki@laurea.fi http://www.laurea.fi/en/leppavaara

Abstract: - The nature of crime has internationalized. Therefore the transmitting of tracking and other status information between Law Enforcement Authorities should become an everyday business. The goal of this paper is to present a solution for international cooperation between law enforcement authorities. The proposed solution is based on Public Key Infrastructure operation model built for the financial sector companies.

Key-Words: - Cross-border operations, Law enforcement, Law enforcement authorities, Public key infrastructure, Public safety

1 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.

1.2 Administrative Challenges

When an illegal incident has come to the knowledge of a law enforcement official, (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 voluntary 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 own well-being of the officers.

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 at 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 exchange of information between LEA organizations helps just in the case of investigation or in statistics, but not at the operational level [4].

1.3 Target of the Paper

The ICT services supporting LEAs' surveillance operations 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 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.

2 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 [5], 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. [6] 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 [7] 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.

2.1 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 1 shows a possible 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 the data source of another LEA organization 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.

2.2 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 2. All these processes 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

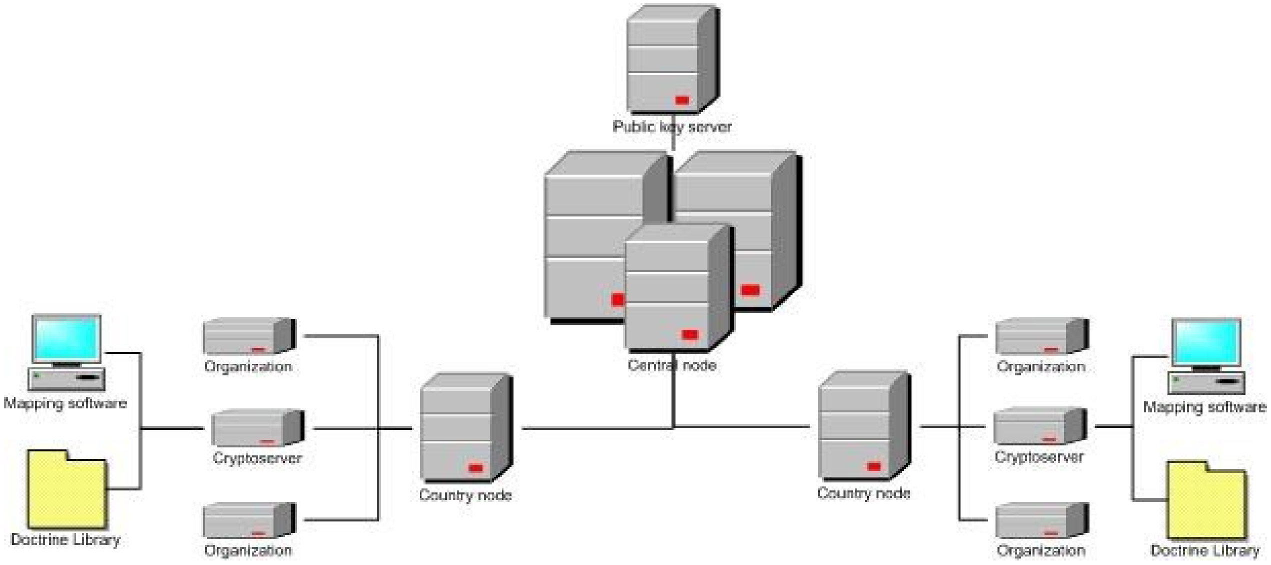

Fig. 1 Network Topology

process. First time an organization must build this document, it might be a large undertaking for the organization. However, in the next project this process is only applied to updating valid policies.

Everything starts from the LEAs operational needs. It is important that the operational part is leading this conversation. IT management and Risk management support 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. The model is PKI project best practices. This is the reason why all processes are described as separate processes. All phases give advice on what must be done and what should be done. In the end it is 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 which they follow or they can follow the PMBOK guide [8].

Operational case phase is a regular operational process case. This process should come from the own operational environment of the LEA. 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. An important question is how to estimate what is really needed so that future projects do not build extra secure or fully automated environments without any benefit.

In the analysis of technical requirements the organization should follow known standards such as the ISO 27000 or PCI. A good example is the best practices in [9]. It is important to go through all in the analysis stage as an 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 on costs and time. Also, if environment is outsourced it helps environment deployment.

Governance support, such as 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. The model gives basic knowledge for governance support but this is normally dependent 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 detailed information on how to evaluate real impacts. This phase needs a check list for the actors. There is always something that must be taken into consideration, which is the reason why a best practice check list is needed.

Projecting phase is a standard stage in the projects. This phase should give more detailed information on where the 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 built. This phase is more technical than the others. It is important that technical personnel of the project are participating.

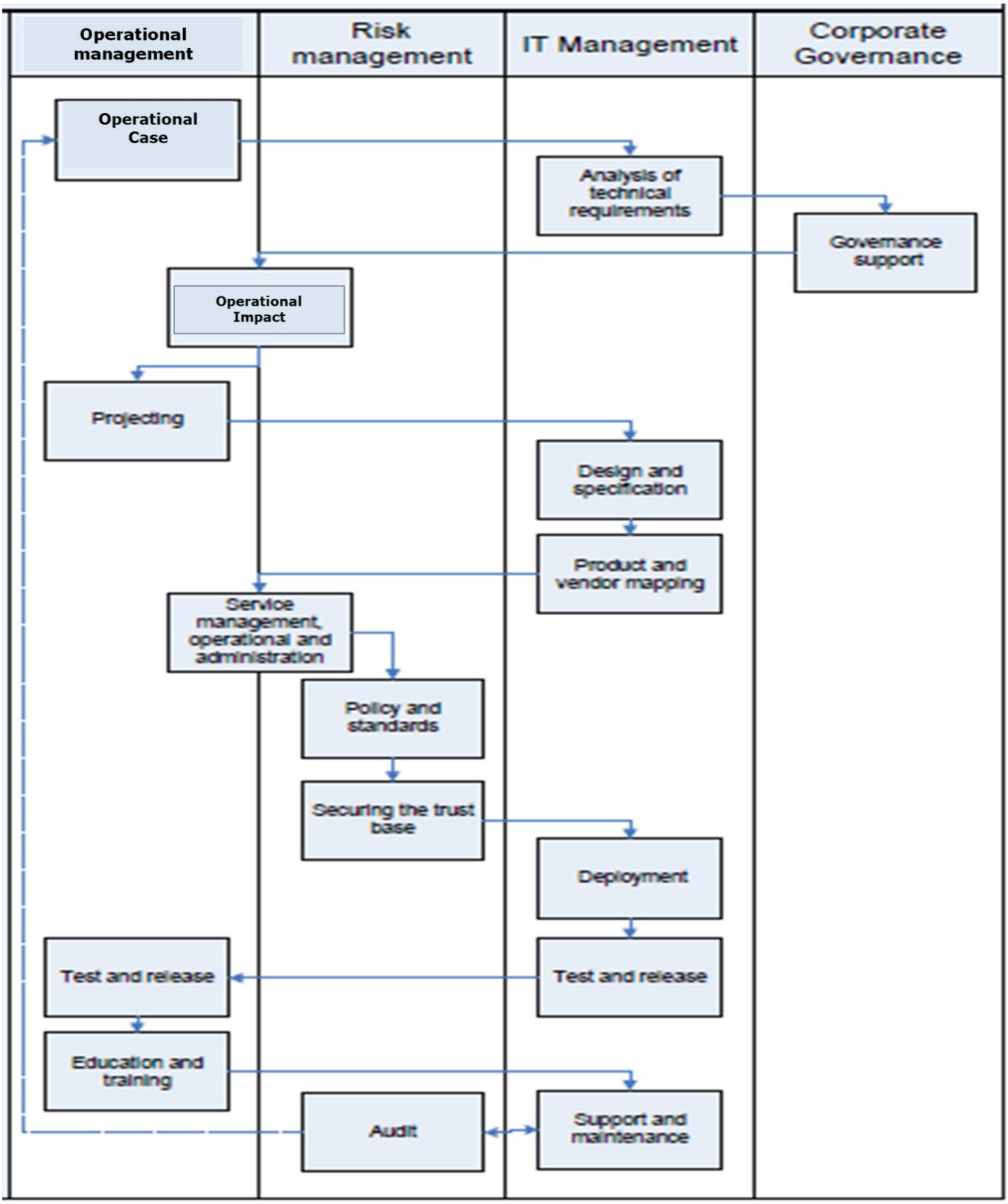

Fig. 2 PKI Operations Model (modified from [10])

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 the decisions on what service provider or program the company is using. This phase needs more information from e.g. ITIL; the project can find correct 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. Some special detail for PKI or security can be found. Generally speaking, these processes are almost same for the entire IT sector. The model should follow ITIL process steps with PKI information.

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

Securing the trust base phase tells the 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 everything is done as in the defined policy. The PKI policy is an inclusive guide, ranging from technical to legal issues. Therefore this phase needs time to pass.

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

Test and release phase is where the project needs more hands-on personnel because there are many different tasks. In a normal situation an organisation has its own test and release processes. If not, the organization should follow some known standard or best practice like ITIL. ITIL has already solved the basic problems with this phase. This implementation model should follow the ITIL process more. These basic ITIL processes need various 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 organisation to know what this project focuses on. An organisation should have its own security education and training program. This training program should be only one part of the phase. The project has massive work to do if an organisation does not have any training program of its own. This must be taken care of in the project time table.

The support and maintenance phase is important for continuity. LEAs should have already working support and maintenance processes. This is only for PKI implementation to those. Also this is lighter if services are outsourced because some services are provided by the vendor. LEAs should follow ITIL processes if the company does not have already these processes in place. During this phase the 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 the LEA should have an audit process in place, such as specification audits and environment audits. Normally these are added to the own project processes of the target organisations. During the audit phase the LEA should use COBIT models.

3 Discussions and Conclusions

The result of this paper is the artifact of a Public Key Infrastructure operations model. This model offers the first steps on what must be done in a PKI project. It provides a partial answer to how to develop faster, more efficient, and safer PKI services. The results of the paper 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 2 are not at the same operational level. Some phases are light business/operational decisions and so are detailed technical assignments. The model needs some kind of estimation about the timetable. Every phase should have its own estimated duration. Also, the model needs an estimate on what phases can be done at the same time and what phases are dependent on each other. It also needs the actors. Every phase should have information concerning who is responsible for that phase and who must participate in that phase. The 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.

ACKNOWLEDGMENT

The author would like to acknowledge all the participants of the MACICO project [1], EUREKA and Tekes—the Finnish Funding Agency for Technology.

References:

[1] CELTIC-Plus, MACICO Project Information, http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp

[2] Muhren, W., Jaarva, M.-M., Rintakoski, K. & Sundqvist, J., "Information sharing and interoperability in national, cross-border and international crisis management", Crisis Management Initiative, Tilburg University, Crisis Management Centre Finland & Elisa Ltd., June 2008. http://www.cmi.fi/files/Interoperability_report.pdf

[3] EUROPOL, the European Police Office, http://www.europol.europa.eu

[4] Viitanen, J., Happonen, M., Patama, P. & Rajamaki, J., "Near Border Procedures for Tracking Information", WSEAS TRANSACTIONS on SYSTEMS. Issue 3, Volume 9, March 2010.

[5] Park, S. & Yi, W., "The Evaluation Criteria for Designation of Critical Information Infrastructure", in Proceedings of the 8th WSEAS International Conference on EActivities, Information Security and Privacy (ISP), Puerto de la Cruz, Spain, December 2009, pp. 77-83.

[6] Patriciu, V.-V.& Furtuna, A. C., "Guide for Designing Cyber Security Exercises", in Proceedings of the 8th WSEAS International Conference on E-Activities, Information Security and Privacy (ISP), Puerto de la Cruz, Spain, December 2009, pp. 172-177.

[7] National Marine Electronic Association, http://www.nmea.org

[8] A Guide to the Project Management Body of Knowledge (PMBOK Guide), Project Management Institute, 4th Edition 2008.

[9] Barker, E., Barker, W., Burr ,W. & Polk ,W. & Smid, M., Key Management Inserts for Security Plan Templates. 2002.

[10] Ruohomäki, P. Public Key Infrastructure operations model, Master thesis. Theseus. Espoo: Laurea. 2012.