EKT

Strategija. Efektyvumas. Vertė

Prepared for:

Ministry of the Interior of the Republic of Lithuania

Promotion and development of coordination, cooperation and mutual understanding among law enforcement agencies and other authorities by implementing integrated information system of penal process (IISPP)

IISPP development strategy

Prepared by:

Ekonominės konsultacijos ir tyrimai Ltd and

Investment Development Agency Ltd.

2015

UAB „Ekonominės konsultacijos ir tyrimai“, J. Jasinskio g. 16B, Vilnius LT- 01112, T. (8-5) 252 6225, F. (8-5) 252 6226, ekt@ekt.lt, www.ekt.lt

CONTENT

List of pictures

List of tables

Terms used

Project Strategy development Project under the contract „Promotion and development of coordination, cooperation and mutual understanding among law enforcement agencies and other authorities by implementing integrated information system of penal process (IISPP)“.

Abbreviations used

EIXM	European Information Exchange Model
EIS	Europol Information System
EU	European Union
IISPP	Integrated Information System of Penal Process
IS	Information system
IPS	Information System of Prosecutors
LITEKO	Court Information System
MOI	Ministry of the Interior of the Republic of Lithuania
RPRE	Register of Police Registered Events
SPOC	Single Point of Contact
SIRENE	Supplementary Information Request at the National Entry

INTRODUCTION

The Commission's Directorate-General Home Affairs (DG HOME) mandated Ministry of the Interior of the Republic of Lithuania , as a request for services under the tender No HOME/2009/ISEC/ AG/209 to conduct a project "Promotion and Development of Coordination, Cooperation and Mutual Understanding among Law Enforcement Agencies and Other Authorities by Implementing Integrated Information System of Penal Process (IISPP)".

General objective of the project is to promote and develop coordination, cooperation and mutual understanding among law enforcement agencies (LEA) in Lithuania, Latvia and Estonia.

Integrated IISPP will allow optimizing the pre-trial investigation process by enabling an effective exchange of pre-trial criminal proceeding between the main institutions involved (Police, General Prosecutor's Office, National Court Administration, and Prisons Department).

Among the IISPP project deliverables falls development of a strategic document, which provides foresights for the further development of IISPP taking into account technical and economic factors, the EU Union's recommendations and legislation. The main objective of the project is to determine all technical and legislation means leading to the better cooperation between Lithuanian Latvian and Estonian LEA.

For the development of the strategic document The Ministry of the Interior selected service providers consortium of JSC "Economic Consulting and Research" (ECR) and JSC „Investment Development Agency (IDA)".

The contract for the project "International Cooperation Strategy for Integrated Information System of Penal Process for Promotion and Development of Coordination, Cooperation and Mutual Understanding among Law Enforcement Agencies and Other Authorities" was signed in 2014. December 31st. Period of four months was estimated for the provision of services.

Scope of the strategy

The strategy document constitutes the report on the further development directions of IISPP and presents the following sections:

Section 1:

Assumptions for the development of strategy.

Section 2:

Assessment of the current situation:

- IISPP description;
- Short overview of IISPP implementation.

Section 3:

Review of EU information exchange:

- General provisions;
- Issues regarding information exchange in EU;
- The development of new tools and evaluation of existing ones;
- Legal framework for European cross- border information exchange model.

Section 4:

IISPP strategic development directions:

- IISPP as a part of EIXM;
- New partnership opportunities between Lithuanian, Latvian and Estonian LEA;
- IISPP development direction in the national context;
- IISPP development direction in the EU context.

Section 5:

Conclusion and recommendations.

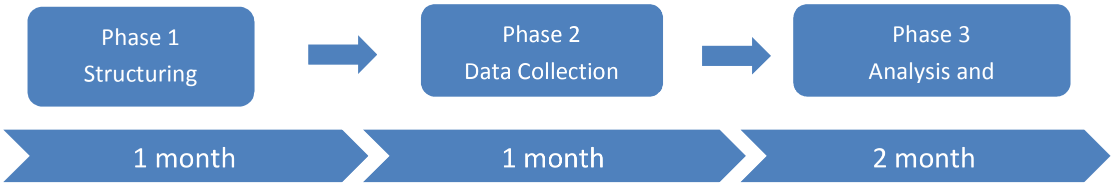
Project methodology

The strategy development process is carried out in three phases:

- The Structuring phase allowed the team of experts to structure the strategy development process according to specific research questions to be answered by Lithuanian, Latvian and Estonian LEA according to general objectives stipulated in the Terms of Reference (ToR). This phase ended with the submission and validation of the **Interim Report.** This phase mainly served to develop the methodology tool that will be used to structure all assignment, namely Analytical Framework. The Analytical Framework was hence used as the backbone of the project delivery.

- The study‘s Data gathering phase aimed to collect data to respond to the research questions developed in the Interim Report and was carried out through the research activities detailed in our project plan, including data collection from Latvia, Lithuania and Estonia LEA, IISPP project manager, and consortia of private companies responsible for IISPP development and implementation.
- The analysis, judgement and reporting phase is horizontal in that relevant activities occur at different times during the project implementation. The project team analysed data both during and after completion of each research activity. A final analysis and judgement took place at the last phase of the assignment to produce the **Final Report** including experts' conclusions and recommendations for future actions. This consisted of going back to the Analytical Framework to ensure that we have met each objective and given an answer to every research question. This exercise was crucial to the analysis and ensures that conclusions and recommendations, based on a triangulation, were strictly evidence-based.

Picture 1. Project flow and description of Project execution stages



Phase 1
Structuring

Phase 2
Data Collection

Phase 3
Analysis and

1 month

1 month

2 month

- Kick off meeting
- First meeting with national LEA representatives
- Preliminary desk research
- Refine methodological approach
- Interim report

- Meeting with national LEA and MOI representatives
- Web based survey of EU legislation
- Web based survey of National legislation
- Meeting with IISPP project manager and development company
- International workshop with LEA representatives
- Development of list of research questions for Latvian and Estonian LEA

- Presentation of the research results in the international conference
- IISPP development directions and validation with Latvian and Estonian LEA
- Draft of Final Report
- Final report meeting
- Final report

It should be noted that during the drafting of the IISPP development strategy the IISPP has been at the final implementation stage, therefore to assess the IISPP functionalities in the production environment during strategy development stage was not possible.

One of the major objectives of the project was to screen information and data exchange improvement between Latvian and Estonian law enforcement authorities, however limited participation of these countries' in the Project, feasibility and availability of information, resulted the accuracy of the project results.

IISPP Project background

The goal of penal process is to perform investigation and disclose criminal activity in the shortest possible time period. However before the IISPP project was initiated the law enforcement agencies that execute penal process faced several problems of ineffective collaboration steaming from the lack of institutions' IT systems integration. At that moment it was rather problematic to gather, accumulate, store and effectively use penal process information for the investigations and prevention of criminal activities because development level of information systems of law enforcement agencies was very different and systems were not integrated. Data about penal process in Lithuania was stored in not interrelated databases that have been managed by various institutions. The majority of investigation data was stored only on paper; part of statistical data was managed on paper cards; a lot of formalized messages between pre-trial investigation institutions used to be sent in paper form. These cases create condition for ineffective cooperation, usage of human and financial resources executing disclosure and investigation of criminal activities.

Therefore the Police department of Lithuania initiated feasibility study in order to find the best solution for above mentioned problems and needs. The final report of the study concluded that the major needs seeking to improve coordination, cooperation and mutual understanding among law enforcement agencies in Lithuania and other authorities abroad are: accelerate decision making process; eliminate duplications; transfer process data to electronic files; automate creation of penal process document, statistical reports and data transfer to other information systems and registers; establish IT control, deadline control, reminders; suggest several levels of paper documents refusal.

IISPP project content

Integrated Information System of Penal Process (IISPS) will be a sophisticated instrument for supporting implementation of Prüm, namely improving information exchange and developing law enforcement information management capacity. IISPS project will definite promote and develop coordination, cooperation and mutual understanding among law enforcement agencies starting from

Lithuania, then Latvia and Estonia, and later EU member states. Feasibility study conducted by Police Department under the Ministry of Interior shows that there is a great need for integrated environment which will be beneficial not only in organizational and functional aspects, but also will save up to 5 times of operational costs of law enforcement agencies in 10 years comparing to primary investment.

The IISPP project will complement such activities currently done in EU member states, e.g. Latvia: Development of the Database "Victims of Criminal Offences" (project number JLS/2007/ISEC/414), Sweden: European Statistical Database on Lethal Violence (project number JLS/2007/ISEC/434), Germany: Development and implementation of a web-based database for online requests (project number JLS/2007/ISEC/FPA/C1/014) and others. The IISPP project will also complement an information exchange among Latvia, Lithuania and Estonia that was started on July 15, 2008. The IISPP project will have a great multiplier effect on the public not only in Lithuania at first and then in the Baltic States, but also later in all European Union. The IISPP project will give a reasonable solution to common routine problems that many Law Enforcement Agencies of other EU member states are more or less facing with.

The main innovation, brought by IISPP is freely customizable integrated environment supporting electronic document management, processing and e-signature authentication. IISPP allows to store and effectively exchange data (criminal event, started pre-court investigation, pre-court investigation data files, court decisions and convictions, important penal process information starting from criminal activities and ending with expiration of conviction, informational and administrative practise investigating violation of law) between institutions at both national and international level. The project is one of the first steps towards integrated information systems of penal process in all EU.

Results achieved:

- implemented Integrated Information System of Penal Process in six Lithuanian institutions;
- prepared strategy aimed at international cooperation between Lithuanian, Estonian and Latvian authorities based on IISPP to achieve the goals of information exchange improvement, sharing of best practices and education, development of law enforcement information management capacity.

1 ASSUMPTIONS FOR THE STRATEGY DEVELOPMENT

The main aim of the strategy is to define possible IISPP development directions, allowing closer cooperation between law enforcement authorities internationally.

In assessing the potential use of IISPP for closer and smoother co-operation between Member States law enforcement authorities, it is important to define the current projected range of applications of the IISPP. From the initial design stage through to its deployment IISPP was (is) the national (Lithuania) IS for institutions involved in criminal proceedings (currently IISPP scope is limited to pre-trial investigation).

This system is primarily designed for police and prosecutorial professionals, but can also be used by courts and other institutions involved with the relevant authorities and actors. IISPP purpose is to ease and simplify the criminal process execution, creating a seamless system, which makes it possible to place and receive all information relating to the investigation. This system also includes task management. IISPP architecture and technical possibilities in more details is presented in paragraph 2.1.

While assessing IISPP possible development directions, it is necessary to define the essential factors that imply the spectrum and intensity of potential development directions. Essential factors are:

- IS, its purpose, technical possibilities and usability;
- The documents regulating international co-operation and exchange of information at EU level and the EU's position on the future of cooperation in this field;
- National and international legal regulation in the field of information Exchange.

2 ASSESMENT OF CURRENT SITUATION

2.1 IISPP description

Ministry of the Interior implements the European Commission-funded project that seeks to develop an integrated information system of criminal procedure, in order to promote and develop law enforcement and other authorities, mutual understanding, coordination of these institutions. The project aims to develop an integrated information system of criminal procedure, which would contain data about the event, initiated an investigation, pre-trial proceedings, data, data about the court made the order, judgments and other court records, move to cyberspace criminal proceedings to ensure the full criminal process information supply store, manage and deliver the criminal proceedings related information and legal probative value of electronic documents, exchange of information and criminal procedure legal probative value of electronic documents to national law enforcement authorities in the promotion and development of law enforcement and other authorities, the mutual understanding these bodies coordination. IISPP will automatically generate the structure of criminal cases, procedural documents, forms, statistical recording cards in one place all the institutions involved in the investigation of actions by officers and information relating to the investigation of criminal offenses from its registration until publication of the judgment.

Key IISPP architecture principles:

1. IISPP multilevel architecture (multi-tier, N-tier), consists of a minimum of three hierarchical levels (user actions, operational control logic, data manipulation and management).
2. IISPP has a unified data structures.
3. IISPP design supports integration with standard open database management systems.
4. IISPP architecture and design supports a collaborative work organization approach.
5. IISPP implements institutional hierarchy, subordination and substitution functionalities.
6. IISPP has configuration options:
    6.1. Document approval requirements (review conformation, approval, digital signature, physical signature);
    6.2. Process completion requirements (set of tasks to be completed to close the process);
    6.3. Integrity of physical documents and signature into overall system based process;

6.4. Individualised desktop per user role;

6.5. Workflow, based on institution, case type etc.

IISPP consists of the following modules and subsystems:

1. The data exchange module – to ensure smooth, reliable, data loss-less, secure, real-time exchange of data between the IISPP, its internal components, other information systems and registers.
2. Document and task management module – enterprise level task and documents management solution enriched with functionality supporting completely digital business process organization featured integration with national e-governance infrastructure and featuring e-documents, e-signature and e-identity recognition.
3. Search module – integrated module in all the IISPP system modules providing the extremely fast possibility to search and filter not only structured and indexed data but also unstructured information stored in the IISPP system storage with results presentation to the IISPP end-user in few seconds.
4. Reporting module – featuring standard and custom reporting on all different steps of Criminal Procedure processes, types of the cases, user groups or other user formation.
5. Classification module – centralized classifiers management implementation delivering single place to maintain all system classifiers, their versioning and in part delivers information validation based on the structures defined.
6. Audit module – delivers logging and auditing functionality for all the IISPP end-user actions to ensure maximum transparently and control while delivering access to the system storing all national pre-trial information.
7. Pre-trial process execution subsystem – ensures pre-trial process execution covering institutional, cross-institutional and cross-country process actors, their duties, process steps, due dates, approval structures, information access organization and other Criminal Procedure process related regulations defined in Lithuanian laws.
8. Pre-trial process control subsystem – delivering functionality for the pre-trial process monitoring, automated issue identification and escalation to the responsible end-users of the competent authorities of Lithuania.
9. Pre-trial process execution for pre-trial judges' subsystem – delivering functionality of all the pre-trial judge actions and ensuring relevant access to the information related to the case.

10. End-user administration module – implements multi-institutional organization structure, organization hierarchies, user groups, user roles, user authorization levels, related system actions, information access rights and required administration tool-set for centralized end-user management.

IISPP physical architecture consists of 3 servers to implement virtualization platform, 3 servers to secure the data exchange with the relevant authorities, 2 repositories for storing IISPP data processed, one of which is used as the primary and the other is used as a reserve designed to back up IISPP data. IISPP technical infrastructure implemented virtualization platform, which is distributed over two server rooms. The data stored in the data warehouse is dubbed. The copies of the data have to be made in a tape library. Information systems hardware architecture is designed to ensure system reliability, security, performance and flexibility.

Embedded in each institution be equipped with data exchange server operating networked services (Eng. Web Services) technologies for realization of links with the authorities of internal information systems (databases).

Virtualization platform provides for the following virtual servers:

1. Database Management,
2. The application,
3. Document and task management subsystem,
4. Data exchange,
5. Analysis and reporting.

IISPP is developed applying the following system-to-system integrations:

1. Prosecutor's Office's Information System (IPS). Information from the IPS to the IISPP:
   a. Complaints registered in the IPS, even those that are already started, with all associated data, including scanned versions of paper documents.
   b. Requests received for legal assistance from foreign countries with all associated data and the documents required.

Backwards integration from the IISPP to the IPS:

c. pre-trial case information;
d. information about criminal offences;
e. information about the actors involved: suspects, victims, witnesses;
f. procedural actions and decisions;

g. related electronic documents.

2. Lithuanian courts information system LITEKO. Information from the LITEKO to the IISPP:

a. data about judges, including the pre-trial judge;
b. judges and other participants in the process of employment, in order to introduce the appropriate IISPP hearing on pre-trial action date and time is a must;
c. details about the hearing location and time of enabling the entered prosecutor taking part in the hearing, details;
d. data on court decisions taken in the process, the process of decision;
e. court decision related electronic documents or electronic copies.

Backwards integration from the IISPP to the LITEKO:

f. formed electronic pre-trial documents in the file together with the indictment, the statement on the order of application of the criminal and all related data;
g. data required by the LITEKO for statistical process tracking and reporting.

3. Register of Police Registered Events (RPRE). Information from the RPRE to the IISPP:

a. data about the event (including documents created in the Police Registered Events IS), that requires a decision on investigation initiation;
b. information related to the event, and activities performed.

Backwards integration from the IISPP to the RPRE:

c. data about the pre-trial case initiation decision;
d. pre-trial case status information to be reported back to the incident reported parties.

4. Suspects, defendants and convicts register (ĮKNR). Information from the ĮKNR to the IISPP:

a. data and documents on the natural persons, suspected of having committed a criminal offense;
b. reports on the legal person suspected of committing a criminal offense;
c. resolutions;
d. pre-trial judge orders;

Backwards integration for the IISPP to ĮKNR:

e. suspects related data obtained during the trial rulings and the criminal data;
f. data about the citizens of the Republic of Lithuania convictions in the EU Member States and Third countries.

5. Arrest or fixed-term imprisonment of ex-offenders identification tags departmental registers (AŽŽR) to collect all related data and backwards integration to provide the person identification

data, data tags and other relevant information helping to identify the person in other LEA processes.

6. Wanted Persons, Unidentified Bodies and Unknown Helpless Persons system (IAR) to collect the data on:
   a. data of the person wanted;
   b. search of the investigation data on bodies,
   c. search related identifiers
   d. European arrest warrant and related data.

7. Criminal offenses departmental register (NVŽR) to exchange statistical information required for statistical forms.

8. Fingerprint data register for the exchange of dactyloscopic data card, the unique identification number and fingerprint files.

9. DNA data registers (DNRDR) for the exchange of DNA data and the related identification code.

10. Wanted and found, numbered and those with individual attributes register of documents and objects (INDR) for the data exchange to avoid the usage of a document and objects or a possibility of setting them invalid.

11. Register of Legal Entities for the data exchange on legal entities, actors.

12. National addresses register for the address and geo reference data exchange on actors (individuals and entities), event place and other geo related information.

13. National Register of Legal Entities (JAR) for the data exchange on legal entities, actors.

14. National Address Register (AR) for the address and geographical reference data exchange on actors (individuals and entities), event place and other geographically related information.

15. National Residents' Register (GR) for the data exchange on pre-trial cases and investigation process participants.

16. National Property Seizure Acts Register (TAARS) for the data exchange on seized assets, property and documents on distrain.

17. National Wanted Vehicle Register (ITPRO) for the exchange of the data on the wanted vehicles.

18. National Wanted Weapons Register (IGR) for the exchange of the data on the wanted weapons and related data.

19. National Preventive Measures Register (PPPTR) for the exchange of the data on preventive measures, impact of preventive measures, applicable to persons and other related relevant data.

20. Lithuanian National Schengen Information System (NSIS) for the information exchange on the persons and vehicles wanted and the related data.

Security issues

IISPP requirements these software security measures:

1. IISPP documents (electronic documents, scanned documents, not to sign the documents) files in file systems must be stored in encrypted form, so that system administrators can have access to these documents.

2. IISPP functions are to be available only with a valid user name and password.

3. Connect and work with IISPP using a web browser to:

3.1. Encrypt communication between the system and the user's computer SSL (. Secure Socket Layer) encryption or other equivalent means;

3.2. SSL must be approved by a qualified certificate (VeriSign or equivalent);

4. The consumer must be able to change your password periodically.

5. IISPP function modules must be linked to the rights which the consumer must be able to fulfil them.

6. IISPP modules with the end user's computer to communicate in an encrypted https protocol.

7. All users of the ancillary systems to be audited user actions audit module.

8. IISPP System Module technical realization must be resistant to unauthorized use. Every architectural layer must be protected by a separate safety level: the user interface, software interface, business logic components - each of them must be installed on the safety checks.

9. IISPP communication systems to be used for secure data transmission networks.

10. IISPP servers and internal networks from unauthorized access must be protected by firewalls.

Audit

All the IISPP users actions are processed by an auditing component that transforms the end-user (and/or system) generated action data and send it to the centralized national auditing service. The information from all national IS will be collected on a number of end-user (and/or system) action events and all the related data available will go to the Ministry of Interior AUDIT III IS. Auditing component is also covering reporting on the end-user action and automated system actions. All the audit related information from the IISPP system to the AUDIT III system is delivered via the asynchronous information exchange mechanism and does not impact IISPP performance. The number of audit events also includes messages sent, scans, validations performed, processes steps and any records made to the AUDI III database by itself, sent messages, scans, validates, processes, and records made to the AUDI III database subsystem.

General non-functional requirements

IISPP must be designed and built to:

1. Could have at least 2,500 users online at the same moment;
2. Conventional forms of presentation of data retention, data revision operations (except for the loading of scanned documents and representation);
3. 90% of the time it would take no longer than 5 seconds;
4. It takes no longer than 10 seconds to perform a search action in 90% of cases;
5. It take no longer than 5 seconds to generate the case document in 90% of cases;

Requirements for systems architecture

1. IISPP should have a common database structure.
2. The system architecture should be multi (multi-tier, N-tier); it must consist of as a minimum of three hierarchical levels (end-user system layer, system operating logic layer, data manipulation and storage layer).
3. The system should be designed so as to be able to be used in conjunction with a standard open database management system that satisfies the following requirements:

   - the possibility to work in multi-user environments;
   - the possibility to work in heterogeneous networks;
   - the possibility for different end-users workstation platforms to work in parallel;

- the possibility to integrate with other database systems, data exchange platforms;
- the protection of all data from unauthorized access;
- the reliable and integral storage;
- the ability to use the national alphabet according to the following standards;
- the possibility to use unstructured data types;
- the possibility to coexist and integrate with distributed architecture databases
- the possibility to maintain local and remote database administration tools to carry out standard IS maintenance functions.

Requirements for the user interface:

1. End-user workplace must be an internet browser based and support all main internet browsers;
2. Connect and operate with the IISPP using a web browser using (Secure Socket Layer) SSL encrypted communication channel between the system and the end-user's device or secure encryption implemented other equivalent means;
3. Data IISPP user interface to be updated in real-time mode;
4. IISPP must be possible to upload these files formats:

    - Office document formats (Word, Excel, Adobe Acrobat, etc.);
    - Graphical image formats (JPEG, BMP, GIF, PNG, etc.);
    - Audio and video formats (mp3, wav, avi, mpeg, etc.);
    - HTML, XML;
    - Other analysis to determine the required format.

5. IISPP must allow the system to store, view the stored photographic images and video files directly in your browser;
6. IISPP must allow putting note in all end-user forms, and at the same time adding to the system a few or more other files.

2.2 Short overview of IISPP implementation

Intensive digitalization on the institutional level - national digital registers, institutional information systems, digitalization of documents, secure network and communication channels of Law Enforcement Agencies (LEA) - in the period of past two decades created preconditions for further improvements exploiting the benefits of information technologies (IT). The unique initiative of the IISPP is a significant break point from the public services management perspective – moving from the functional management to the process centric management. It is one of the first implementations in EU of full pre-trial process in one single system, uniting all process actors.

Key figures, describing the scope of the Project:

- 2 years of development and implementation;
- Over 50 000 development hours;
- Planned scope:
    - 85 000 pre-trial investigations per year;
    - over 1 000 000 documents in the first year;
    - over 5 TB of data per year;
- Number of users: over 5000;
- Types of users: police officers, investigators, prosecutors, judges, administration and management;
- Integrations with 15 registers and/or other IS

Main implementation challenges:

- Resistance to change – a new tool for a large number of existing users, the migration from institution level IS to cross-institutional level;
- Legal basis – a vast amount of changes in national legislation had to be prepared, fine-tuned and implemented even before the system was launched, legitimation of e-standard;
- While digitalising paper based process scenario still must be maintained;
- Several versions and flexible data structures – the migration of legacy data, the transition from current to structured data, the preparation for strict data structure rules in the future;
- Differences in IT, project management, processes, organizational maturity levels across institutions and geographical regions.

Lessons learned:

- Correct combination of expertise in process, organization, legacy environment, technologies in use and project management is crucial for the implementation of such a complex project.
- Political will and support is critical to insure the continuity of such a long lasting project.
- Small project team member’s rotation during the whole project implementation period is important to ensure focus, knowledge accumulation and commitment.

- Mapping of expectations, requirements and the priorities of different institutions at the early stages and maintenance of agreements through the whole project is essential.
- Management of risk of changes in technology, legislative environment, organizational structures and the common infrastructure becomes very important and should be addressed separately while implementing such a large scale and long lasting projects.
- Organizational and compatibility related issues raise more challenges and disputes than the technology related issues but the attention drawn at the project development stage is usually the opposite.
- Difficulties in resolving complex organizational, process, management conflicts tend to be transferred to excess technological solutions.

3 REVIEW OF EU INFORMATION EXANGE

3.1 General provisions

3.1.1 European Commission Communication on the Overview of Information Management

In 2010, the European Commission published a Communication concerning an overview of information management in the area of freedom, security and justice[1].

The Communication provides a synthesis of EU-level measures regulating the management of personal information and proposes a set of principles for the development and assessment of such measures in order to make the approach to the exchange of information more coherent.

The Communication covered information exchange instruments that facilitate the exchange of personal data and were at that time (1) either currently in force, under implementation or consideration, or (2) set out in the Stockholm Programme Action Plan.

3.1.2 Means and channels of EU data exchange

There are three main EU and international channels used for cross-border information exchange, i.e.: (1) SIRENE, (2) the Europol channel, and (3) the Interpol channel. Bilateral or regional channels are used in addition to these channels, such as the regional PCCCs:

- **SIRENE (Supplementary Information Request at the National Entry) Bureaux** – offices SIS alert. You can get additional information from the State party, which registered alert. Offices operate 24/7 (twenty-four hours, seven days a week) in accordance with relevant procedures as defined in the Sirene user manual. At present, the exchange of information takes place through a system called SISNET, which from 2013 changed SIS II network.

- **Europol National Unit (ENU) / Europol National Units (ENUs)** exchange information with Europol. They are also used to exchange information on crime, which falls outside

[1] COM(2010)385, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF

the limits of the powers of Europol under bilateral agreements. NEP can exchange information directly or through Europol liaison officers, who belong to the NEP, but deployed Europol's headquarters. Secure communications tool used - SIENA (Secure Information Exchange Network Application) has been developed and Europol for the exchange of information between Europol and between Member States (in 2011, using the walls were exchanged 222,000 reports, of which 53% were submitted and Europol).

- **Interpol National Central Bureaus**: working 24/7 for the exchange of information with Interpol as well as between countries on a bilateral basis, excluding Interpol. The national central offices of exchange of information use I-24/7 communication tool that is designed to Interpol.

- **Other channels, including bilateral liaison officers (Liaison Officers)** are deployed in other member states and is generally used in more complex cases, the Police and Customs Cooperation Centres (set up in neighbouring Member States and support for the exchange of information and operational cooperation between the border regions).

3.1.3 Relevance of existing systems and tools

Large majority of EU Member States greatly underuse the capacities of the Europol and Interpol information system .This is not due to legal constraints, but to a lack of motivation and national capacity to provide information which may be of use to other EU Member States. Criminal investigation information is, by its very nature, sensitive so there are good reasons to exchange this information with caution. However, legal and technical safeguards exist and can be strengthened further. Providing access to national police information is an investment that provides benefits to other EU Member States and, understandably, such investments are not seen as a priority in most EU Member States. EU-level financing schemes might be useful in this regard. Existing legal obligations alone, such as the obligation to upload information to the Europol Information System (EIS) have not been an effective motivator so far.

Financial, technical or political obstacles aside, police officers throughout the EU need timely, accurate and relevant information. They do not need empty or low quality (existing or new) databases.

Some experts have stressed the need for greater access to different types of data or information systems; such as EURODAC, EU-PNR and, in particular ECRIS (Criminal records information system) data. Interpol is also considered a very useful system allowing access to data from non-EU countries. However, four EU systems seem to offer the most potential to address the need of law enforcement authorities to identify whether information on a certain person is held in (an) other EU Member State(s). The following table provides an overview of these systems.

Table 1. Relevant Systems overview

System /tool	*Purpose Definition*	*Data stored*	*Access to data*	*System limitations*
EIS	To support MS' competent authorities in preventing and combating **organised crime, terrorism and other forms of serious crime** affecting two or more MS	Data on persons **suspected of crimes** falling under Europol's mandate (personal data including biometric identifiers, convictions, and organised crime links)	**3516 users**; this number is expected to increase in the coming years, because only since the beginning of 2012 it is possible to make the EIS available to competent authorities on a hit/no hit basis	**1. System underused** (not equivalent amount and quality of data per MS) **2.Limited scope** of Europol mandate **3.Limited access** and the possibility to query the system in MS
SIENA	To provide a **secure way** to manage the exchange of **operational and strategic crime-related information**	Serves MS as a relay and messaging service between MS **without storing** the content of the information	**Around 3000** users with increased extension to competent authorities and the direct access for strategic and operational cooperation partners	**1.** Currently offered as a web based form that **cannot be integrated easily** in MS systems (also due to EU RESTRICTED accreditation) **2.** Most activities necessary for EPRIS' purposes require **a manual intervention**
SIS II	To **ensure a high level of security** within the Schengen area, including the **maintenance of public security, public policy and the safeguarding of security.** Also to apply provisions relating to **the movement of persons** within the Schengen area using information communicated via the system	Alerts on **wanted/missing/sought persons and objects** and on **persons and objects** posing **threats to public security**	**Large group of users:** MS authorities responsible for border control and other police and customs checks; by extension - national judicial authorities. In case of a hit, the local SIRENE office is involved in each country (10-60 people per MS). Also, authorised staff of Europol and	**1.** Sometimes erroneously perceived as simply a border control/migration instrument although this is not borne out by the legal instruments, nor by the information within the SIS which is largely law enforcement based. **2.** Lack of data on **persons or objects**

			national members of Eurojust and their assistants	**known**, if they are not currently wanted/missing/sought or presenting a threat to public security
Prium	To improve cooperation between EU police and judicial authorities **to combat terrorism and cross-border crime more effectively**	Anonymous DNA and FP, VRD information on **individuals suspected of criminal offences**	**Limited group of users:** contact points transmit requests; domestic access is governed by national law	**1. Not operational** in all MS **2. Lack of person/object related data other than** DNA/FP and VRD

3.1.4 EIXM legal instruments

This section is an introduction to the formal aspects and main features of the legal instruments which are the focus of this study:

- The Swedish Framework Decision; and
- The Prüm Decisions.

The Swedish Framework Decision

In the light of the terrorist attacks in Madrid and London, in 2004 and 2005, Sweden proposed an initiative to simplify the exchange of information and intelligence between law enforcement authorities[2]. The so-called Swedish Framework Decision (SFD)[3], adopted in 2006, sets out common rules on procedures according to which information may be exchanged between Member States' law enforcement authorities.

The essence of the Decision is that Member States must ensure that the conditions applied to providing and requesting information and intelligence to or from competent law enforcement authorities from other countries are not stricter than those applicable at national level (Article 3). This is referred to as the principle of equivalent access, which is considered as a major step forward

[2] *C.f. http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.*

[3] *Framework Decision 2006/960 JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:EN:PDF.*

in cross-border law information exchange[4]. By establishing relevant conditions for the provision of information and intelligence, the Swedish Framework Decision partly implements the principle of availability established in The Hague Programme[5]. Notably, Article 4 stipulates time limits for providing information[6]. If the time limits cannot be kept to, the Member State receiving the request is required to provide reasons for not being able to comply. In addition, the Decision seeks to promote information exchange with Europol and Eurojust for crimes that fall within their mandates[7].

While Member States are obliged to share relevant information with other Member States, there are certain limits are enshrined[8] in the Decision. In particular, the Decision does not include an obligation for Member States' law enforcement authorities to collect information in order to be able to answer queries from other national or EU bodies. Moreover, information may be used as evidence as part of a judicial procedure[9] only if the source Member State has given its consent (Article 1). In addition, the SFD provides grounds to refuse information, for example on the grounds of national security interests (Article 10).

Finally, the SFD incorporates **forms** which may be used by law enforcement authorities for the exchange of information. Annex A of the SFD contains a form to be used for transmitting requested information and Annex B contains a form to request information

The Prüm Decisions

The cooperation that started as a multilateral treaty between Austria, Belgium, France, Germany, Luxembourg, the Netherlands and in 2005, i.e. the Prüm Convention, was shifted to EU level with Council's Decision 2008/615/JHA51 and the related provisions for its implementation 2008/616/JHA52 (the two 'Prüm Decisions').

[4] *C.f http://www.eumonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vj6iponbr3yj/f=/14755_1_12_rev_1.pdf.*

[5] *C.f. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:053:0001:0014:EN:PDF.*

[6] *Accordingly, urgent requests shall be responded to in eight hours, Non-urgent cases shall be responded to within one week. In all other cases, information shall be provided within 14 days*

[7] *Cf. Article 6(2) SFD*

[8] *In practice, these forms are rarely used and their added-value has been questioned by a number of stakeholders. This is discussed in section 4.1.1.2 Operational compliance with the Swedish Framework Decision's legal requirements*

[9] *It is noted that the recent adoption of the European Investigation Order (Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters) will influence the judicial aspects of law enforcement information exchange, as further explained in this section*

The Prüm Decisions set out provisions regarding:

- Automated search of data;
- Supply of data in relation to major events;
- Supply of information in order to prevent terrorist offences; and
- Other measures for stepping up cross-border police cooperation.

They include the obligation to establish databases related to automated DNA analysis files, automated dactyloscopic (i.e. fingerprint) identification systems53, and vehicle registration data54, as well as procedures and modalities for Member States' access to each other's databases in the context of cross-border law enforcement.

Bilateral or regional channels are used in addition to these channels, such as the regional PCCCs.

3.1.5 Processes and practical aspects of Information exchange (EU overview)

The Single Points of Contact (SPOCs)

The 2008 Manual of Good Practices concerning the International Police Cooperation Units at National Level underlined the advantages of setting-up a "one stop shop" unit for international police cooperation, with a multi-agency organisation within each Member State. The Manual emphasised that setting up such a unit was a matter of national competence, which had to take account of each Member State's legal situation and law enforcement structures. Nonetheless, it stressed the advantages stemming from adopting such a set of recommendations and the general efficiency of EU police cooperation exchange as a whole.

The purpose of this institution is to make cross-border police cooperation more effective by subsuming into it the competencies of different national offices or contact points. These involve:

- The Europol National Unit (ENU);
- The Interpol National Central Bureau (NCB);
- The SIRENE Bureau;

- The contact point for national liaison officers posted abroad and foreign liaison officers posted in the Member State;
- The contact points designated pursuant to the "Swedish Framework Decision" and the "Prüm Decisions" (step 2 – exchange of additional information following a hit for DNA, fingerprints and VRD); and
- If any: the contact point for the regional and bilateral offices.

With respect to the SPOC concept, the 2012 EIXM Communication invited Member States to: Create, if not already existing, a Single Point of Contact (SPOC) covering all main channels, available 24/7, bringing together all law enforcement authorities, with access to national databases.

Ensure that information exchanged through Police and Customs Cooperation Centres is where appropriate passed up to national level, and where relevant to Europol. Establish cooperation between SPOCs and EUROSUR NCCs.

3.1.6 Application of the Single Point of Contact concept in the Member States

In June 2013, the European Council mandated the future Presidencies to start discussions on the future strategic guidelines in the area of freedom, security and justice with a view to its June 2014 meeting.

In particular with regard to strengthening the cooperation of MS' law enforcement authorities, MS stressed that the exchange and management of information should be considered in a systematic manner. Full advantage should be taken of all opportunities, at technical and organisational level, created over the past years for gathering, analysing and exchanging information. In this context, some MS mentioned the merits of a single point of operational contact (SPOC) in order to cope with the increase of cross-border information exchange.

The Presidency recommends to thoroughly examine the use of SIENA III as the prime tool for exchanging operational and strategic intra-EU crime related information and intelligence, both with regard to the Europol mandate and to bilateral information exchange between Member States.

Europol currently aims at a further enhanced interoperability between the national case management system and SIENA by expanding the interaction between both interfaces allowing more SIENA actions to be performed directly from the case management system such as searches, task assignment and national workflow definition of incoming and outgoing SIENA messages.

In June 2014, the Council adopted the SPOC Guidelines for international law enforcement information exchange. As a new element, a section was added on the SPOCs' case management system, which defines a "circle of criminal intelligence" (receipt-evaluation-distribution) and provides a proposed classification of urgency.

The vast majority of Member States have an international police cooperation structure that at least partly complies with the criteria set by the EIXM Communication and the subsequent SPOC Guidelines. At the same time, many national systems are currently under review and in a process of transformation.

A detailed distinction among and typology of the different versions of SPOCs is in fact made redundant by the different national ways of working and the different institutional set-ups in the Member States. The understanding of which level of the relevant structure actually qualifies as a SPOC seems very different. Some interviewees understand as 'SPOC' only the front office (or 'communication centre'); for others, it means the entity housing the three channels (Europol, Interpol and SIRENE) together. The definition of yet another set of interviewees has the largest scope, in which in addition to all these elements the SPOC also contains further strategic and support services. Some Member States do not yet have a SPOC at all.

Case example: establishment of a SPOC

Greece is currently in the process of setting up a SPOC according to the guidelines. First, the Interpol department will move into the same location as the other channels. Then, a common operational centre will be created, which will be the single point of entrance. After that, a new technical infrastructure, including case-management system and archiving system, needs to be developed.

Regarding the possible future development of the concept, we note here that there are some plans in Finland for developing the current front office into a Situation Centre with analysts and intelligence.

Application of SPOC concept in member states

Our assessment below on the application of the concept of SPOC in the Member States looks at it from the following perspective:

- Implementation of the EIXM Communication criteria;
- Implementation of the SPOC Guidelines criteria;
- Different models of the functioning of the SPOC; as well as
- Added value, difficulties and limitations.

a) Implementation of the EIXM Communication criteria

The specific **criteria** for SPOCs in the **EIXM Communication** are: covering all main channels, available 24/7, and bringing together all law enforcement authorities, with access to national databases.

Covering all main channels seems to be generally accepted as a prime condition for a SPOC, **normally all three main channels** (i.e. Europol, Interpol, SIRENE) **are covered** by Member States' SPOCs. However, SIENA is in many cases not used to a significant extent. Furthermore, in most countries not all SPOC staff members can use all channels, especially in those countries where there are different teams designated to work in the front and in the back office. SPOCs are **available 24/7**, except that most Member States do not monitor SIENA outside office hours. As also highlighted on the choice of channel, "the nature of SIENA" not to be fed at night and, in the absence of an actual legal obligation to do so, MS do not work with it then either as they do not see any communication coming in on.

Regarding the criterion of implementing a **multi-agency model**, less than half of the Member States seem to have such a system in place. The most typical law enforcement authority other than the police (or gendarmerie) to be present in a SPOC is customs. Some Member States also have finance or coast guard staff working in the SPOC.

In terms of the criterion of SPOCs' access to **national databases** no issue was reported during our interviews.

Most Member State SPOCs do not have a **manual** for the choice of channel. This is particularly interesting in view of our observation reported under section 4.3.1.1, i.e. that SPOC officers do not in general receive hands-on on boarding training.

b) Implementation of the SPOC Guidelines' criteria

The June 2014 **SPOC Guidelines** set criteria in addition to those defined by the EIXM Communication. Our assessment of the current implementation of these is presented in the Table below.

Table 2. Application of the SPOC Guidelines' criteria in the Member States

SPOC Guidelines' criteria	Assessment
The SPOC has **one phone number and one e-mail address** for all international police cooperation requests sent at central level.	SPOCs in most Member States
Ideally, the SPOC houses its different sections in the **same building**.	There is a mixed picture in this respect for Member State SPOCs. We also note that some sections of the SPOC, even though they are in the same building, can sometimes be housed on separate floors
Its staff - includes interpretation or translation capacities; - is trained and equipped/mandated to deal with all kinds of tasks.	Translation capacities do not seem to be present in all structures. As mentioned in section 4.3.1.1, staff on boarding training is limited
Every investigating police officer knows the basic services provided by the SPOC.	Interviewees and our web-based survey results reveal ample space for improvement in this respect
A **request** is sent through **one channel only**.	Due to the diversity of national preferences for the choice of channel, duplication still remains
The SPOC has access to a **case management system** that evaluates, classifies and disseminates the information originating from all cooperation channels and national authorities.	Not all Member States have a case management system for the SPOC.
Staff is able to communicate orally and to have good written skills in the most relevant	There is room for improvement in most Member States.

foreign languages for this country. Operators all speak **English**.	

As the table above shows, for the most part the criteria of the SPOC Guidelines are not yet implemented in practice.

c) Different models for the functioning of the SPOC

Overall, almost all interviewees considered the SPOC concept as **highly useful** and conducive to facilitating information exchange. Some even consider it the main element establishing information exchange among Member States. In addition, many highlighted that, besides providing a contact point for international contacts, having a convergent point for international cooperation in this form is also useful for coordination within the country.

However, apart from the definition of the SPOC (detailed above), the understanding and implementation of its *modus operandi* also varies across Member States. We note in particular diversity over:

- Functioning as a coordinating office (civilian staff) versus a more prominent overview role (where staff has substantial subject matter expertise).
- Designated separate front office and back office teams versus a mixed model where staff can have an overview of both roles.

Different level of empowerment of field officers. This can result in, for example:

- some SPOCs using the channel that their requesting investigators indicate they prefer while others make this choice independently; or that
- field officers in some Member State have direct access to SIENA.
- The extent to which law enforcement agencies other than the police are involved.

We observe that these different models entail different levels of efficiency in facilitating information exchange, and are also closely linked to the national traditions and the national landscape of law enforcement institutions. Nevertheless, based on our interviews and expert panel, we observe that overall, establishment of a SPOC seems to depend mostly on **political will**. In this respect the adoption of the Guidelines seem to have inspired reflection in some Member States on how to adapt the organisation of their SPOCs, but this process still is voluntary and hence remains limited in scope.

d) Added value, difficulties and limitations

In general, our interviewees and expert panel participants perceived that there is substantial **added value** in having a SPOC. It is felt that the SPOC plays an important role to avoid duplication. Furthermore, the SPOC is also believed to be in place to ensure quality of messaging, and to have an overview function (which is the reason why it is seen as important by many that the SPOC is involved in all exchanges.

Expert panel participants also highlighted that SPOCs can mitigate the controversy on the choice of channels – *provided* all channels are available to a SPOC and the SPOC is able and ready to use all channels appropriately (including e.g. information sharing with Europol).

Furthermore, some panel participants believed that as a general rule, police officers need the SPOC as a connecting piece between them and another legal system, where they do not know the legal standards and the language. Some interviewees stated that for them it is easier to communicate with a Member State that has a SPOC, because it is more efficient.

Those interviewees, who expressed a view of the subject, believed that the SPOC concept was a good way of maintaining quality of data, as it allows for officers to be better trained in data protection.

In Member States where the SPOC concept is not yet implemented, interviewees reported that there were cases where, without being aware of it, different international police cooperation units were working on the same case, because they received the same request through different channels.

Furthermore, in the absence of a SPOC, there are in some cases no direct connections between e.g. the Europol and the SIRENE units, with officers not being exactly sure what their colleagues in the other unit actually do.

As mentioned above, not all Member States have a SPOC fulfilling the criteria of the EIXM Communication and the SPOC Guidelines. Our interviewee specifically mentioned some **difficulties** with establishing comprehensive SPOCs. Lack of resources can be a difficulty, however we note that once in place, SPOCs can also, via rationalisation of resources, entail savings.

Rigid national organisational structures and resistance to change can pose another difficulty in developing a SPOC. In fact, even once it is there, **as efficient as the SPOC may be, it cannot in itself overcome less efficient ways of working further afield in the national administrations**.

For example, while SPOCs might work with an email-based case management system to sort out and allocate work to its staff, their national “clients” in the field often still use paper files or fax. Inserting and formatting these messages into the SPOC’s system takes resources and these issues have an effect on the response time for requests. Hence we observe that national workflow challenges are exported to the EU level, with some Member States being known among the rest of the Member States as very frequently replying late to requests.

Furthermore, there is often a division or even competition of competence between national entities, which is not overcome by the installation of a SPOC.

As an additional issue, we highlight the question of the **language of communication** among SPOCs. The most common language is English. However, it is not the only language used. In particular, many interviewees highlighted that they use their own language with specific countries that can understood. Although substantial misunderstandings due to language use were not reported, most of our interviews acknowledged that there is still space for improving SPOC staffs’ language skills.

The issue of languages is especially crucial in the front office. Some SPOCs only run reduced language capacities outside of normal working hours.

While, in general, there is wide appreciation among stakeholders for having a SPOC, a few also mentioned what they see as the **disadvantages** of this concept.

While acknowledging that SPOCs bring consistency in the way requests are treated, some nevertheless believed that incoming requests are interpreted according to the national law of the requested state. This can relate to national rules regarding deadlines for response, the national approach to only limiting the reply strictly to the information requested, as well as specific national data protection rules.

As another limitation, some interviewees mentioned the fact that due to the alertness needed and the shifts they work in, staff switching between shifts in both front and back office can be overworked.

In those Member States where the SPOC has a strict coordinating role, some interviewees saw it as a limitation that this obligatory involvement of the SPOC actually prolongs the distance (and hence the time elapsed) between information source and end use.

Conclusions

The vast majority of Member States have an international police cooperation structure that at least partly complies with the Single Point of Contact (SPOC) criteria set by the EIXM Communication and the subsequent SPOC Guidelines.

Those not having a SPOC face difficulties with optimising their workflow which is constantly increasing as cross-border information exchange expands.

The concept of the SPOC is considered as highly useful and as clearly facilitating information exchange. However, application of the SPOC concept varies across Member States and there is no common understanding of what constitutes a SPOC and how to assess whether different features exist.

The adoption of the Guidelines seem to have inspired reflection on how to adapt the organisation of the SPOCs organisation, but this process still is voluntary and hence remains limited in scope.

Recommendations

The SPOC Guidelines need to be transposed into the national context by the individual Member States. The application of the Guidelines' in the Member States should be evaluated by the Commission in two years from now.

Consideration should be given to establishing a network consisting of SPOC staff and/or heads of SPOCs with a view to exchanging good practices and lessons learned, as well as identifying issues related to the application of the SPOC Guidelines and in particular to the choice of channel.

Member States are invited to facilitate, with the support of Commission funding, the use of all channels equally by establishing electronic case management systems for their SPOC. More specifically, without prejudice to relevant data protection standards, a national interface could be created that makes it easy to use all different channels.

Integrated solutions should be adopted where officers in the field do not have to choose the information channel, but it is built into routines and national systems.

SIRENE manual and good practices should, where appropriate, be taken into account when shaping the setup of SPOCs.

Member States should also ensure that the workflow is clear between the SPOC and the PCCCs.

As it is not sufficient only to improve the SPOCs, in cases where the national workflow outside the SPOC lacks efficiency, attention should be also paid to optimising workflow from field officers to the SPOC.

In order to ensure timely implementation, a peer evaluation mechanism should be devised for Member States' SPOCs.

General recommendations for staff recruitment and training

- Staff is experienced in dealing with international cases and main EU and international tools of police co-operation.
- Staff has knowledge of issues such as intelligence and criminal investigative techniques, as well as of the national legislation.
- ▪ Staff is able to communicate orally and to have good written skills in foreign languages.
- Operators speak English. Basic knowledge of one or two other languages is an asset,
- especially of those languages most used in the international cooperation cases of their

- Member State (based on geographical, economic or historical reasons or on criminal phenomena).
- Staff has enough computer skills to fulfil its desk duties.
- Staff receives regular training, both about EU and international cooperation mechanisms (*i.a.*via CEPOL) and about national developments.

Specific requirements for the Head of the SPOC

- The head of the SPOC has a broad background in law enforcement.
- He/she has a suitable ranking to require additional information from national competent authorities and / or to speed up and ensure the follow up of requests within the time frames.

3.2 Circumstances shaping further development

Today a list of topicalities can be identified while discussing the IISPP and other LEA IT solutions development options of a similar nature at different levels:

- New national and international IS, registers and platforms are being developed and implemented;
- Introduction of new standards in EU;
- The issue balancing between human rights, private data protection and security measures;
- Numbers of international criminal offences are growing, as well as the needs for international cooperation;
- The issue balancing national security risks and international openness, equality and cooperation;
- Despite of common Europe initiatives, tools implemented and directives, the human factor and institutional will related challenges still determine various process inefficiencies:
    - 65% of international requests are left unresponded due to a large volume of manual work, which leads to the avoidance of submitting potentially essential requests[10];
    - Failure to comply with time limits;
    - Duplication of information;
    - Wrong choice of information channels;
    - Different interpretations of criminal offenses in different Member States (MS);

[10] Source: Council of the European Union, Working group on Information Exchange and Data Protection (DAPIX). Subject: EPRIS / ADEP: Automation of the data exchange process. Date: 15 October 2012, Brussels

  - Lack of competence / process clarity and its regulation;
  - Setting priorities, sequencing.
- Diversity in the European countries;
  - Issue of different legal bases, regulations, process organizations;
  - Issue of multilingualism;
  - Issue of different information structuration;

Addressing the topicalities listed, EU set's major suggestions for a further development of cross-border information exchange:

- Implementation of the National Single Point of Contact (SPOC) concept which would include police, prosecution service, customs and border;
- Implementation of Hague Program and Stockholm Program by the European Information Exchange Model (EIXM);
- Full scale implementation of Swedish Framework Decision (SFD) and Prüm Decisions;
- Purposive use of communication channels;
- Recommendation to use existing EU centralised IS, instead of originating new ones;
- Reduce the influence of human factor via automatisation.

Each member state is free to choose their own strategy and roadmap of national LEA IT tools and measures based on their priorities, maturity level, EU recommendations, geographical and crime specifics and resources. Despite the national specifics, all MS should follow general principles embedded in EU recommendations for LEA cross-border information exchange. Lithuania considers IISPP as a significant accomplishment leading towards a smoother information exchange.

3.3 Presumptions of further development

The further development of the IISPP is determined by several important aspects. First of all it is the nature and primary mission of the system. IISPP was developed as a national cross-institutional IS. Technologically IISPP can be expanded to national LEA Single Point of Contact (SPOC) or international information exchange platform (EXIM). However other than technological issues should be addressed:

- mitigation of national security risk;
- protection of sensitive national data;
- limited information scope, provided by IISPP.

It is foreseen that at this stage of development, IISPP should remain as a national cross-institutional pre-trial process execution solution, which provides preconditions for the digitalized cross-border information exchange.

The next important aspect of the further development of IISPP is the European perspective. Reacting to new criminal trends EU has agreed to set new international LEA cooperation strategic development directions. The objectives set, requires improvements towards more interoperable, smoother and more secure information exchange between different EU MS LEA's and the implementation of next generation National SPOC's. IISPP implementation and further development establish major preconditions to face the future needs and challenges:

- Providing a single environment for all the digitalised data regarding all pre-trial investigations carried out in Lithuania it eliminates the necessity of information distribution knowledge across national institutions and IS.
- Information is stored in a structured form based on predefined classifiers, the information gets more accurately searchable, more focused and can be interpreted with minimal or without translation.
- IISPP establish technological base for the minimization of human participation in cross-institutional and cross-border information exchange processes leading to process automation benefits, scalability, service availability, the reduction of human factor related risks, resource optimization.

In order to address the listed presumptions the IISPP is planned to be developed in two strategic directions:

- Further developments for improving criminal procedure at the national level;
- IISPP as a tool to improve the cross-border exchange of information.

4 STRATEGIC DEVELOPMENT DIRECTIONS OF THE IISPP

The analysis of further development IISPP direction clearly has two main areas. IISPP can be further developed in the national and international contexts. However, exact needs and further development definitions will be revealed when all institutions will be using IISPP for a while. Nevertheless, already at this stage it is possible to distinguish certain further development directions:

- Though, it was not the first priority and not so actual due to lack of basic functionality, - one of the key aspects for the future extension is: developments, integrations and improvements towards wider and more automated cross-institutional and cross-border cooperation, information access, delivery and exchange.
- Wider, more detailed and more structured digital information related to panel process that can lead to more structured, more defined, better controlled, more transparent and more automated process management.

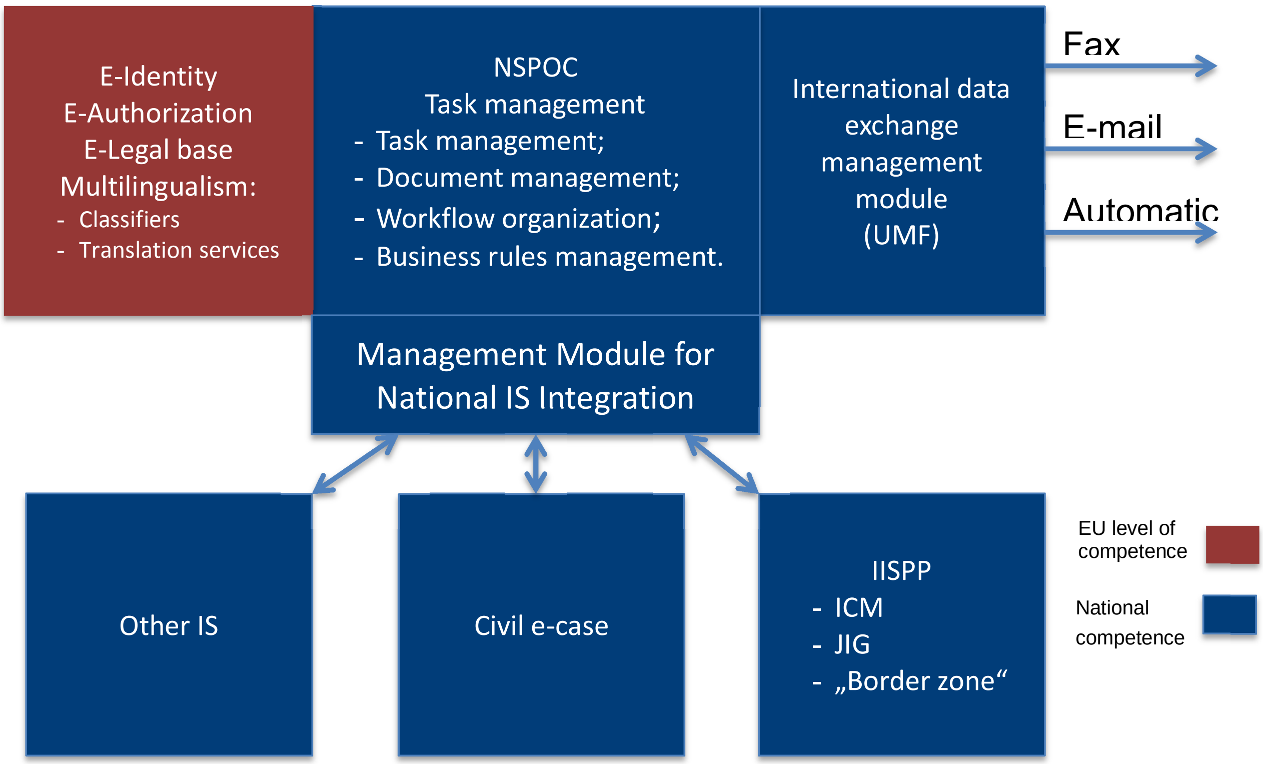
4.1 IISPP as part of the international information exchange

In the context of international cooperation, current IISPP functionality only partially realizes information exchange. Prior to full international collaboration process implementation such a system as IISPP was required to be developed and implemented. Only now, when all national panel process information and processing is accessible via centralized and unified one-stop-shop solution – IISPP, it is possible to deliver automated, menless international collaboration functionality and service. Considering the fact that collaborative solutions demand for similar readiness of all process participants, vision for the further developments must be formed in progressive manner.

The vision regarding IISPP role in international cooperation:

“Omit the human factor in international data exchange among EU MS and move towards a fully automated process”

Picture 2. IISPP role in the context of international cooperation development



National SPOC. To meet all requirements addressed to the NSPOC and assure effective operations a single, but separate IS should be implemented. Considering all recommendations and key functions addressed to the NSPOC solutions, the core of it must be based on the task management IS. However, investigating the reasons, why EU MS are struggling to meet the requirements set it is necessary to highlight additional features, mandatory for successful NSPOC implementation:

- Development of EU MS national LEA IS's was not homogeneous and is based on several technological, architectural, procedural, normative standards. It would be too naive stating that it is possible and demanding from all EU MS moving towards one single standard in a big bang approach. It will be required some transition period and some transition solutions to reach the goal.
- At the same time it is expected that NSPOCs must be single unit for all international cooperation regardless from geopolitical position (is it EU MS, some other alliance or international cooperation based on the *good will* principles). In that perspective NSPOCs' IS design must foresee several ways of process organization with different level of authorization, automatization, self-service possibilities and technical standards.

- Managing associated risks and at the same time implementing process back-up scenario, as well supporting low-tech countries integration it is required to leave the possibilities for manual process organization using old-school technological stack – paper based documents processed via fax or post based communication channels.
- A high standard for e-identification is pre-requisite for process automation. It will be always the question on mutual (mis-) trust for process automation and cross-border access to LEA information organization via processes design based on self-service principles.
- Auto-stop ruleset must be implemented in order to assure adequate level of risk mitigation considering possible information security infringements.

International data exchange management module. The module is a technical solution to ensure the support of all types of information exchange technologies, architectures, formats (e.g. UMF 2.0, 3.0), channels (e-channels, fax, post), standards, and security requirements.

EU centralised components. As the compatibility of different aspects is one of the main obstacles for automated cross-border information exchange, mapping and harmonising of those differences is of a critical importance:

- **Identity -** to ensure reliable identity conformation – national and cross-border eID;
- **Authorization level -** to harmonise where it is possible and map authorization structures across different institutions and different EU MS. Different EU MS have different regulations and it is often the question of request interpretation – does the inquirer not exceed its mandate, is the inquirer mandate enough for authorization, what are the limits for classified or sensitive information to be applied, etc.
- **Request validity -** to verify and validate legal basis of any request issued, - is it approved, actual, up to date, legal for international matters. E-case validation infrastructure in every MS and EU interoperability network.

Management module for national IS integration. There is and always will be several national IS storing and managing LEA activities related information, developed asynchronously, using different technologies, based on a different architecture. It creates a necessity to have national interoperability solutions supporting the following key functions required for a smooth and automated international information exchange:

- mechanism recognising the primary data source, in accordance to the request type;
- the tool-set and rule-set for the request and response data transformation into the formats and structures supported by the target national IS;

- transformation mechanism, that provides the international authorization and authentication confirmation tickets into the technical formats supported by national IS;
- feedback mechanism to report back the status – steps completed, on-going activity progress, due dates and related information.

IISPP and other national IS. The layer that represents all national LEA IS, - internal IS, registers, national interoperability solutions, institutional and cross-institutional IS, registers and databases. In particularly further IISPP developments requires international inquiries support:

- **International communication model** – a separate operational model featuring different processes design, information structures, authorization schemas and rulesets to maintain international cooperation rules, cases classifications, authorization and validation requirements, notary approvals, translations, due dates, etc.

- **Joint Investigation Teams (JIT)** – for more complex and long lasting cases often Joint Investigation Teams are established. It requires a special functionality implemented into national LEA IS's to support cross-country case setup – maintaining JIT case and local case simultaneously. Currently, in most of the countries, JIT case setup is organized as manual process and de-facto takes months to establish. Often, the timing is the reason for the case to be moved to local investigation, in that manner loosing full scale investigation potential. If the process would more automated and faster to initiate, much more panel processes would be organized using the JIT instrument.

- “**Border zone**” **-** the EU requirements for the Private Data protection and LEA IS security requirements demands for the “Privacy by Design” and “Security by Design” principles implementation:
    - no direct access to the databases storing sensitive personal information,
    - information cannot be collected into a single storage,
    - no super roles implementing single access to all type of the information,
    - All actions must be logged, even though it is „view only“ access to the data,
    - All access permissions must be time framed.

It leads to the implementation of semi-demilitarized area for information exchange, where the inquiry related information can be uploaded by source and downloaded from inquirer without direct access to the original sources.

Based on the IISPP implementation experience the vision for the future development of similar solutions can be formed in the following perspectives:

- it will be always two-dimensional
  - National, process-centric, single-standard, automated IS,
  - International, multi-standard, interoperability IS.
- The technological dimension is not a challenge any longer. All required tools, IT solutions, equipment is already available.
- Key challenge to resolve is the organizational, common process and common standards related questions leading to agreements that would facilitate EU MS mutual trust and goodwill development.
- Mutual trust is the key to omit the human factor related issues, in international data exchange among EU MS and move towards a fully automated process.

4.2 Possibilities of closer cooperation with institutions from Latvia and Estonia

During the evaluation of international cooperation in criminal proceedings between Lithuania, Latvia and Estonia LEAs', the following points must be discussed:

1. **Cooperation between national electronic communication centers.** It is necessary to create electronic communication centers for the exchange of documents and data for international cooperation in criminal proceedings. As of this moment there are no functioning communication centers in Lithuania, Latvia or Estonia, therefore this particular method for communication is to be evaluated only in the long-run. Currently, it is not possible to draw conclusions regarding the technological and organizational solutions to be used in national electronic communication centers' integration.

It is possible to define general conceptual aspects related with the exchange of documents and data itself via national electronic communication centers. Firstly, the means for authentication of sent and received documents. There are two possible models for this:

1. The cooperating countries may agree between themselves that all the documents travelling via integrated system are to be considered official, valid and law-binding documents.

2. Only exchanging documents that are digitally signed with electronic signature. In this way, the acceptance of electronic documents' containers and e-signatures would be important.

Secondly, there is a conceptual question of the methods for transferring information and documents – whether the direct system integration will be used or communication is to take place via third-party information networks.

2. Given the fact that this strategy is dedicated to discuss the concepts of possible issues regarding the development of platform designed for Lithuanian law enforcement authorities to cooperate with other countries, one can specify other communication with foreign countries (namely, Latvia and Estonia) methods.

2.1. The first method for communication is creating the possibility for authorized foreign countries‘LE agents to directly connect to the Lithuanian LEAs‘ international cooperation platform for criminal proceedings. However, in this case it should be dealt with these problematic issues:

a) The choice of tools for Latvian and Estonian institutions‘authorized personnel authentication. These measures must ensure that only authorized personnel from a foreign country (Latvia, Estonia) would be able to login and only after properly identifying his or hers identity.

b) Usage of foreign language. The question of languages used within the platform would have to be solved, if the access to the platform were granted for the authorized personnel of a foreign country (Latvia and Estonia, in this case). Naturally, working in Lithuanian-only environment would be unacceptable for foreign country's LEA officers. For this reason, there would be demand to provide foreign countries' LEA officers with an opportunity to work in a different language. Therefore, a decision must be made whether allow each country to choose its own national language (Latvian or Estonian), or to use English, which has become a standard in international cooperation.

It is held that if the access to the aforementioned platform is given to authorized members of different countries, adapting the whole system to their national languages is unreasonable and does not qualify in terms of economic benefit. It could be stated that in all the cases functionality of the system related with end-user interaction must be presented and available in most commonly used international languages (i.e. English, French).

During the evaluation of possibility to incorporate the members from foreign countries LEAs‘ into development the international cooperation platform for criminal proceedings, one more aspect must be taken into consideration. Since this platform is to be considered an official national electronic communication center of Lithuania, the authorized institutions of foreign countries should be able to provide the documents and data they have. This document and data exchange would satisfy all the judicial requirements to organize the communication of international cooperation via central institutions. Therefore, officially, the connection to the platform should be granted only to the authorized personnel of foreign countries’ central institutions.

2.2. **Another form of communication on the international scale** would be developing an integrated interface between the international cooperation in penal process platform and specific foreign countries’ information systems where all the information, which is related to penal processes and their phases, is handled. This evaluation should be oriented towards a realistic estimation of the current situation, therefore, during the analysis of communication with Latvian and Estonian institutions via integrated interface, one should discuss about the information systems these foreign countries are using.

2.2.1. Latvia

Currently, there are two important information systems in Latvia that store and handle the data related with penal processes:

1. **Criminal Procedure Information System** (lat. Kriminālprocesa Informācijas sistēma). This system stores and handles the following data:

- information about all pre-trial investigation procedural documents except those that require special attention to information data security;
- information about registered criminal activities;
- information about officers assigned to the case;
- information about people who have a right to defence;
- information about legal persons on which behalf individuals committed criminal offences;
- information about victims;
- information about that the person was recognized as a victim;

- information about the criminal offence, the damage done and its nature;
- victims' representatives (the date when were granted the relevant status);
- other information relation with the investigation.

It should be noted that this system is used for managing and handling pre-trial investigation processes. Therefore, it could be stated that the possible integration interface between Latvian Criminal Procedure Information System and the platform for international cooperation in penal processes could work only in the context of pre-trial investigation, meaning that the documents and data should be related with investigations in Latvia.

2. **Courts'information system**. This system manages and handles all the information about procedural actions and received documents. In the context of potential integrational interface what would be relevant are the data concerning the pre-trial investigations and criminal proceedings. Therefore, this integration would be oriented towards the exchange of data and documents during the stages of judicial proceedings.

During the assessment of the possible integration of international cooperation system and information systems used by the Latvian authorities, the attention should be drawn to the fact that in order to meet the legal requirement to organize the communication only via central bodies, authorized Latvian authorities should have access to the information systems and be able to receive and send data and documents. This would mean that there might be a demand to modernize the informational systems of Latvian LEAs' for to be compatible with the platform for international cooperation.

2.2.2. Estonia

In Estonia, the following systems store data related to criminal proceedings:

1) Police information systems
2) Administrative register of criminal proceedings;
3) Courts' information system
4) E-file (E-toimik)

E-file system is already integrated with other systems on the list. Therefore, in Estonia's case, one could discuss the possibility creating integration not with different information systems, but only with one – the E-file.

Summarizing the overview of the current situations in Latvia and Estonia, it is possible to distinguish two strategic directions. First, there is a short-term strategic direction in international cooperation. This direction would focus on the factor that there are no functioning national electronic contact centers in Latvia or in Estonia. For this reason, a decision should be made between creating a secure login platform for authorized Latvian and Estonian institutions (while taking in consideration the problematic questions described before) and possible integrational interfaces between the platform and information systems of foreign countries, where the data relevant for international collaboration is stored. It could be stated that since this solution sooner or later will have to be changed to the one which is proposed in the long-term strategy one must choose a solution that is the quickest and the most economically efficient.

In the long-term strategy, the focus should be on a decision to use the integrational interfaces that are to be created by national electronic contacts centers. Since the aforementioned platform would function as Lithuanian national electronic contacts center, this factor would presuppose the need to take in consideration the future demand to have a possibility to create more integrational interfaces like this. Moreover, during the process of platform development, it must be ensured that IT tools would correspond with standard EU solutions, for example, UMF as a message format, or the accepted standards for e-signature and e-container standards.

4.3 IISPP Development Directions in the National Context

The assessment in the national context shows 4 main possible directions for the further development of the IISPP:

- **Further integration**: further cross-institutional integration with Court, Prosecutors, Prison department, Probation services, Bailiffs and expertise related IS, integration with registers (e.g. traffic accidents register etc.), additional integration to ensure the full information about the court decisions and its execution.

- **New modules in the IISPP**: the system should be enriched by the Module for International cooperation (information exchange), the Module of Handling of physical evidence and other property-related areas. Introducing other than LEA process participants with pre-trial investigation and/or case materials is another area for the further development.

- **Operational and process optimization**: include wide range of improvements, such as calendar management, automated data request and transition from other institutions, not directly involved in the pre-trial investigation, e-complaint, the mobile IISPP workplaces etc.

- **Process management improvements**: automatic workflow organization, provision of data for statistics, integration with strategic indicators and analysis of activities.

All directions are presented in more details further.

4.3.1 Further integrations

Modernization of LITEKO and IPS Integration with IISPP

During the evaluation of the possibilities for creating a platform based on IISPP which would be intended for the management digitalization of the international collaboration in penal process one should also consider the formal aspect of these procedures. In some cases, national and international legislations envision a formal address towards a subject in a foreign country that manages particular information or is able to perform certain actions. This suggests that respective subjects are allowed to provide information or execute actions only after receiving and fulfilling a formal document, which satisfies its formal and content requirements. With regard to the indicated circumstances, a potential platform based on IISPP and designed for the international collaboration processes should be capable of such documentation management as well.

Presently, information systems, which deal with the mentioned data and documentation, are:

1. Judiciary Information System - LITEKO
2. Prosecutor Office’s Information System – IPS

The interaction between these systems and the potential IISPP-based platform should be evaluated respectively. Essentially, each instance should be assessed considering whether the development of the IISPP should be oriented towards a more intimate integration into the aforementioned systems, or adopt their functionalities in the area of international collaboration.

Judiciary Information System (LITEKO)

It must be noted that since May 1, 2015 i.e. since the beginning of LITEKO will have a certain inclusive interface with the IISPP. This interface will include:

- Transfer of the documentation and preliminary investigation material to LITEKO;
- Transfer of the procedural documentation obtained from the institutions not involved in the preliminary investigations to IISPP;
- Transfer of the information about the judge assignment to the particular pre-trial investigation from LITEKO to IISPP.

Besides the available resources, defining the existing needs in the context of the system interface is also relevant. In accordance with the analysis of the regulatory acts some processes of international collaboration can be pointed out:

- Judicial proceedings and documents related to the extradition of person or persons from the Republic of Lithuania (on the basis of European Arrest Warrant), including the processes of appeal;
- Judicial proceedings and documents related to the extradition of person to the Republic of Lithuania (European Arrest Warrant);
- Judicial proceedings and documents related to the applications submitted by foreign institutions and international organizations about the execution (approbation) of procedural acts;
- Judicial proceedings related to the appeal towards institutions of the foreign countries.

Presently, the actions noted are recorded by LITEKO using the system tools. For this reason, it can be stated that the main purpose of the modernization in this area is the evolutionary development of the already existing processes, which are synchronized with the acts of international collaboration during the criminal proceedings digitalized by other institutions.

It is also noticeable that LITEKO and IISPP are unable to offer an opportunity for the system users to perform acts of international collaboration in electronic space. What is more, such integrations have their expansion potential and can serve as basis for creating digitalized management of the judicial institution‘s procedural documents.

According to the IISPP‘s as an international collaboration platform‘s choice of development path- whether it is an expansion of LITEKO integration or adoption of LITEKO functionalities, attention should be drawn to the fact that functionalities mentioned above are relevant to the operation of other LITEKO modules for instance, LITEKO module of statistics. Therefore, a direct transfer of LITEKO functionalities to the IISPP would not be sufficient and therefore would require additionally expanding LITEKO‘s and IISPP‘s integration which would assure the appropriate functioning of the present LITEKO mechanism. This suggests that the design of the international collaboration platform based on IISPP would inevitably relate to the modernizing of LITEKO and IISPP integration.

When choosing between the indicated paths of IISPP modernization it should be taken into consideration which of these paths would demand smaller financial investments. Several aspects are important for such assessment:

1. Creation of a functionality which allows the courts to record actions performed while international collaboration during the criminal proceedings would essentially mean mimicking the existing process recording functionalities of LITEKO. In pursue to optimize the development expenses of the international collaboration during the criminal proceedings platform, unmotivated duplication of the already existing functionalities of other information systems should be avoided.

Besides the investments in the development of the new IISPP functionalities, rational use of the human resources should also be considered. Some actions of the international collaboration are performed during the pre-trial period of the criminal case investigation. Records of the criminal case investigation process are managed in LITEKO. Consequently, choosing the path of transferring LITEKO’s functionalities into IISPP would lay down conditions for a situation when actions performed during the same judicial process would be recorded into two information systems: actions related to the criminal case investigation - LITEKO; international collaboration during the criminal proceedings - IISPP. Such situation should be considered as ineffective use of human resources.

2. The indicated economically unprofitable aspect of transferring LITEKO functionalities into IISPP can be compensated if choosing this path would allow avoiding additional expenses for the modernization of LITEKO and IISPP integration. As stated earlier, the transfer of

LITEKO functionalities into IISPP would require building tools for transferring certain information. This means that despite which decision is taken in order to set conditions for the communication in the international collaboration during the penal process platform, the need of LITEKO and IISPP integration expansion is still of high relevance. The choice of LITEKO and IISPP integration expansion path enables more possibilities of using the present integration mechanisms. As already mentioned above, even in the present integration implementation of LITEKO and IISPP, the information systems are exchanging document files. Creation of IISPP based international collaboration platform would enable courts to receive documents of international collaboration from Lithuanian and foreign institutions as well as transfer procedural court documents to the platform. LITEKO and IISPP integration modernization path would require improvement of the present integration functionality, which would allow information systems to exchange a broader range of document file types. In case of transferring LITEKO's functionalities into IISPP, the information which is presently not transferred would be transferred using the integral base of LITEKO and IISPP, which would mean that the integral interface of LITEKO and IISPP should be improved thoroughly.

3. Economical profitability of transferring LITEKO functionalities into IISPP can manifest through lowering the level of information duplication. In case of LITEKO and IISPP integration expansion the same data (documents) of international collaboration during the criminal proceedings would be stored in both information systems. If the functionalities of LITEKO would be transferred into IISPP, the indicated information would be stored in a singular system at the same time lowering the resource use of other information system, in this case, LITEKO.

Every single of the realizations discussed, possess characteristics which suggest their economic profitability. Systematic comparison of these realizations should be based on the estimation, whether the profit gained from the elimination of the information duplication aspect counterbalances the investments necessary for the development of new and unconventional IISPP functionalities as well as fundamental modernization of LITEKO and IISPP's integrated interface. Considering the level of international collaboration processes in the context of LITEKO it can be stated that the economic benefits gained from eliminating information duplication is not sufficient enough for choosing the path of transferring LITEKO functionalities into IISPP. The conditions indicated suggest that in the economic sense, the path of LITEKO and IISPP's integration expansion should be acknowledged as more efficient.

With regards to the existing integrational interfaces of LITEKO and IISPP as well as the courts position in the process of international collaboration during the criminal proceedings, several strategic objectives can be distinguished:

1. With regards to the existing integrational interfaces of LITEKO and IISPP as well as the courts position in the process of international collaboration during the criminal proceedings, several strategic objectives can be distinguished.
2. To modernize LITEKO and IISPP integrational interface in a way which would allow the court's documents and metadata of international collaboration during the criminal proceedings to be transferred from LITEKO to IISPP?

Prosecutor Office's Information System (IPS)

One of the constituents of IPS information structure is judicial help module dedicated for handling the data about cooperation with foreign countries. This IPS module handles the following information:

- Data regarding the process of extradition from the Republic of Lithuania;
- Data regarding the process of extradition to the Republic of Lithuania;
- Data regarding extradition of persons from the Republic of Lithuania while following the European arrest warrant;
- Data regarding extradition of persons to the Republic of Lithuania while following the European arrest warrant;
- Data about the processes regarding prosecution transfer from and to the Republic of Lithuania;
- Republic of Lithuania's legal aid applications and their data;
- Foreign countries' legal aid applications and their data;
- Requests and complaints made by the inhabitants.

As in the case with LITEKO, there must be an integrated interface between IPS and IISPP. This interface would help in:

- All documents and specific metadata registered in IPS would be directly transferred to IISPP;

• Once a new pre-trial case is created, relevant data would be transferred to IISPP.

This situation has many mutual features with LITEKO and IISPP in the case of integrated interface. Therefore, a choice must be made between the transfer of IPS functionality to IISPP, and expansion of IPS and IISPP integration. The choice to modernize IISPP from the cost efficiency point of view is oriented towards the same aspects as in the case of LITEKO.

1. During the creation of new IISPP functionalities, basically, one would make a replication of already working mechanisms implemented in IPS. For this reason, looking from the cost efficiency point of view, it could be argued that this factor legitimizes further integration of IPS and IISPP

   .

   Furthermore, unlike in the case of courts, the use of IISPP in institutions under the Prosecutor’s Office has some specific features. Prosecutor General's Office has an exceptional status in the context international cooperation. The legislation states that Prosecutor General's Office is a central institution in international cooperation, meaning that it is an institution where all the communication with foreign countries must come through. On the other hand, Prosecutor General's Office is not the only with the status central institution. This means that all the functionalities related with performing the functions of central institution must be installed into IISPP. Due to these factors, IPS functionalities must be transferred to IISPP. The modernization of IPS and IISPP integrational interfaces is an insufficient measure to create a platform on the basis of IISPP for international cooperation.

2. Transferring IPS functionality to IISPP does not eliminate the need to modernize the integrational interface of IPS and IISPP. Data from IPS judicial help module is used for generating IPS statistical reports. A modernized integrational interface should be developed after transferring all the functionality of IPS to IISPP while at the same time attempting to keep current IPS functionality. This modernization should ensure the transfer of data required for IPS statistical report module to work properly.

3. The transfer of IPS functionality would provide evident economic benefits since there would be no need to store the data in two different information systems.

Taking in consideration all aspects that were mentioned in the case regarding IPS functionality, a priority in IISPP development could be transferring IPS functionality to IISPP. To sum up, these strategic objectives can be formulated:

• IISPP will have to provide the opportunity for Prosecutor General's Office to perform actions related with functions delegated to it;

• IISPP will have to provide the opportunity for regional prosecutor' offices to perform functions as authorized institutions in the field of international cooperation.

• To modernize IPS and IISPP integrational interface, while at the same time ensuring the transfer of data that is needed for IPS statistic reports module to work properly.

Specific Aspects of International Cooperation in Penal Process Platform

The following aspects are essential for the development of IISPP strategy and the platform for international cooperation in penal process, which would allow managing all the processes associated with related documents:

1. During the adaptation of IISPP to be used in international relations, one must take in consideration that IISPP must provide an opportunity for central institutions to manage these processes (transfer the documents dedicated to international cooperation to the authorized institutions of Lithuania or other foreign countries). Central institutions are Prosecutor General's Office and Ministry of Justice.

In order to create a platform based on IISPP for international cooperation, one must take in consideration the demand to manage the processes associated with documents dedicated for international cooperation. This means that tools must be created for IISPP which allow performing these actions:

1.1. Registration of documents submitted by institutions of foreign countries. Central institutions must have an opportunity to register the received documents, and to indicate related information: the sender of the document, sender's country, etc. This way, central institutions would register all the received documents regardless of in which form – physical or digital – they would be provided. In case there is a demand, this information could be further transferred to other information systems or used to aggregate statistical info.

Since in some cases the documents can be submitted to the authorized institution not via the central institution but directly, corresponding institutions are also to be granted access to documents registration in IISPP.

If a document send by an authorized foreign institution were an answer to the document sent by Lithuanian institution, this document would be associated with the one that was sent, meaning that a relationship between the two would be shown.

1.2. The formation of tasks to the authorized institutions. Lithuanian Republic Code of Criminal Procedure (hereinafter - BSC), Article 67 paragraph 2 provides that Lithuanian Courts, Prosecutor's Office and other investigating bodies, receive the requests from foreign countries and/or international organizations via Ministry of Justice; Prosecutor General's Office, Prosecutor's Office, The Lithuanian Prosecutor General‘ s Office prosecutor (Lithuanian Deputy National Member of Eurojust). With regard to this provision, central institutions must be granted rights to send the registered document to a relevant authorized institution, which then will have to make a decision what to do. The document's transfer would be performed in one of two ways. First, the document and all the related metadata would be sent to the authorized institution's information system via integrated interface (for example, this method would work for when addressing the document to a judicial authority). Second, authorized institution would register their actions inside IISPP; therefore, the sending of documents would be internal.

In case a document would be received in physical form and a decision would be made not to digitalize it, the authorized institution would be obtain information about the document's transfer from central institution to the authorized one and the data about the documents itself.

In the situation described above, when a document for international cooperation would be received and registered by an authorized institution directly, a demand to obtain a legal permission to answer to the legal aid request sent by a foreign country might arise. In this case, the authorized institution must have an opportunity to inform the central institution about a received document.

1.3. Registration of performed actions in IISPP. If an authorized institution does not have a separate information system where all the performed actions are stored, an opportunity to register all actions related with international cooperation documents must be provided in IISPP.

The latter circumstance presupposes a conclusion that in IISPP there must be a feature not only to register actions made by central institutions, but also for authorized institutions that do not have their own separate information systems for monitoring international cooperation processes.

Central institutions should be granted an opportunity when an international collaboration document is received from the authorized institution, to record an instance of permission or prohibition for the authorized institution to carry out documents and to forward information and/or a document about the adopted decision to a particular institution.

1.4. Submission of the international communication documents from authorized to central institutions. For instance BSC Article 66, paragraph 2 envisions that the international collaboration documents should be transferred to the foreign countries through central institutions. For this reason the IISPP development should also include transfer of the functionalities intended for the documents prepared by authorized institutions as well as the transfer of related information to the central institutions. The transfer of the document could be executed in two ways. First, if the authorized institution recorded its actions during the criminal proceedings in IISPP, the transfer of the document would be carried out inside the system, informing a particular central institution about the submitted document. The second approach, if the authorized institution records its actions in a separate information system, the transfer of a particular document should be carried out through the integrated interface between the information system in question and IISPP.

In a case when a document of the authorized institution is prepared according to the document submitted by another foreign country of the international collaboration, IISPP system should record the connection between the received and the transferred document.

1.5. Transfer of the international collaboration document to the foreign country institution. Regardless of international collaboration document transfer methods the fact of the document transfer should be recorded in the system.

Depending on the technological tools of the foreign countries as well as the documents electronically prepared according to the realities of legal provisions and/or signed by the qualified, systemic signatures, the international collaboration documents of Lithuania's authorized institutions with the help of international integration could be transferred to the other country institutions with expertise

2. The application area of the potential IISPP-based international collaboration platform would be more extensive than the one of the present IISPP. Currently, IISPP is designed for recording the actions and managing information of the pre-trial investigation. The potential IISPP-based platform would be used not only in the pre-trial investigation process but also in the process of the case investigation during trial and in the cases when the pre-trial investigation is not yet initiated in the Republic of Lithuania. The system should allow to determine which stage of the criminal investigation is related to an existence of a particular international collaboration document. If the document is related to the pre-trial stage of the investigation, the existence process of the international collaboration document should be associated with a particular pre-trial process. In case of LITEKO's integration with IISPP, the former would store information about the case presently

investigated or already closed, with which a particular international collaboration document is associated: identification numbers (i.e. case number, number of the criminal proceeding).

Attention should also be drawn to the fact that in the process of criminal proceedings, the actions in the potential IISPP-based platform could be recorded in cases when the collaborating countries are not in the EU. More extensive use of IISPP functionalities is not only possible but rather necessary. Using IISPP only for the management of the documents related to the EU institutions would set ground for a situation where the documents of the international collaboration would be managed using separate tools. Such situation must be considered critically, for it enhances the risk of human error.

Given the indicated aspects of administering the international collaboration documents, strategic IISPP expansion goals can be established:

1. To create opportunities for the central institutions such as Prosecutor General's Office and Ministry of Justice to use tools, designed for managing the international collaboration documents and information about the document related processes.
2. To create opportunities for the authorized institutions, which do not have a separate information systems for recording the international collaboration processes during the criminal proceedings, to record these processes and related documents in IISPP platform.
3. Document management mechanisms in IISPP should be used not only in cases where these documents are related to the pre-trial investigations that take place in Lithuania and are recorded in IISPP but also when the criminal case investigation is ongoing or even if there are no related criminal case investigations processes which are ongoing in Lithuania. Such methods further expand the area where IISPP is applied.

Further integration with existing registers

• IISPP integration with wanted persons register. Integration of people searched for information through integration with IKNR register IISPP.

• Registers of registered traffic accidents through integration with IISPP pegged (EIS ↔ ↔ pegged IISPP).

Additional integration with the court, probation, prisons and the police, to ensure that full information not only about inclusive environment, but the sentence and its execution. Information should include:

- Publication of the judgment of the Court;
- An appeal submission;
- Escalation in penal institutions;
- Penal;
- Parole.

4.3.2 New IISPP modules

Module for international cooperation (information exchange).

In order to support all the specifics of international cooperation, separate functionality must be implemented. Key differences from the national process organization are the following:

- The cases are defined based on the international agreements and laws. 4 different scenario must be implemented in order to support all major aspects of the regulation:
  - Bilateral agreements;
  - EU agreements and directives;
  - International agreements;
  - Other cases handled based on the good faith principles.
- They do have different case structure, processing steps, due periods, responsible authorities and experts involved.
- Representatives and process actors of foreign country can be not known prior to the action and requires different model for the user rights and authorization management.
- Execution workflow is different.
- In most of the cases it involves additional steps for the information translation.

The biggest issues while establishing the communication, information exchange or international penal process case are related with trust:

- How to recognize and validate the identity;
- How to validate case and person authorization level;
- How to provide the access to required information at the same time maintaining high standards of national information security.

Some additional functionality already mentioned above must be implemented in international cooperation layer to resolve these questions.

The international collaboration module by itself must have the functionality supporting:

- Incoming international requests;
- Outgoing international requests;
- JIT cases processing.

Depending on the level of automation we expect from international collaboration model, different standardization levels must be reached, either by implementing common standard or introducing some cross-national mapping standard. Currently, while the international cases in majority number of the countries are processed manually it limits a lot information access time and leaves a lot of place for different appearances of human factor, - mistakes or manipulations.

Handling of physical evidence

Currently in IPPS there is only general information on the case related evidence. There is no separate system national-wide and international-wide centrally storing and managing evidence life-cycle information. It is presumed that due to lack of accuracy in the evidence management continuously LEA are facing additional costs and expenditures. The following problematic areas are recommended to be addressed while assessing further development options:

- Monitoring of movement, maintaining the information about movement history and information about current location of custody. It is not recorded in all of the cases and all process steps. Information gaps appear when the items are transferred from one institution to the other. If the item is provided for additional inspection and/or review, the due dates of the process step related to the action are not controlled in any of the central management systems that potentially can be the reason for item conditional losses.
- Seizure history (when the possessions were taken/returned) and their current status. As seized items are managed separately and mainly manually from overall case, it is possible and sometimes happens, that even after highest court decision, they remain seized (the decision is incomplete). It leads to additional administration, handling and storage costs by LEA. The other aspect of such a situation is that it process-wise very hard to organize additional amendments to the court decision to include seized items as well. It would be a

good solution to have validation rule-set implemented in the IISPP, that could check all aspects of the case before final closure.

- In order to follow best practices, as well to manage real costs of case processing it is recommended in the further development to include integration with accounting and financial management IS. Such an integration would allow to succeed in:
    - Valuable property accounting;
    - Balance monitoring (how many were confiscated, seized, and recovered);
    - Financial management (re-indexing, amortization, etc.);
    - Value management (value adjustment, maintenance, rehabilitation, etc.)

Other property-related areas:

In Lithuanian, asset management in most of areas is centralized and is performed by State Tax Inspectorate. It should be the case that State Tax Inspectorate would handle the asset related processes, such as:

- Right-on-time derelict assets management and handover to State Tax Inspectorate (integration with STI IS)
- Ownership rights management:
    - Announcement of ownership restriction. It appears sometimes, that after ownership rights restriction the owners remain using the asset (especially in cases of real estate). More precise financial management would allow to minimize number of such a process mistakes.
    - Transfer of information about the Decision to other institutions (centre of registers in Lithuania case, as central information management authority), in order to inform other institutions about panel process fact, process decisions, - i.e. banks, insurers, etc.
    - Status of court decision execution and precise management of due dates.

Introducing process participants with pre-trial investigation and/or case materials

Currently IISPP solution is operating in secure LEA network and is not accessible from outside the perimeter zone. That limits some of the process participants (suspects, advocates, etc.) to access case information as well to stay informed and up to date with latest updates. The easiest way would be to introduce temporary access grant to the system part and in that way to fulfil the need, however it is not possible due to the national regulations applied for LEA and security requirements for national level IS. Therefore abovementioned process participants cannot operate in the same system, and – it should be implemented in different manner via separate electronic space (Border zone) where information exchange processes would be handled:

- E-request submission process (saves 1 day)
- Submission and admission of a warrant for E-lawyer advocacy (saves 2-3 days)
- E-invite for questioning (saves 1 day)
- A realized mechanism which is to be used for registration of familiarization act and information submission:
    - Suspects;
    - Penal institutions representatives;
    - By witnesses.

NB! especially for the witnesses, as it gives possibility to register familiarization act remotely, without necessity for travel and daily schedule amendments to fit into working LEA or imprisonment institution hours.

Another advancement of the process that would increase the efficiency of interactive actions with the suspects is integration of video conferences infrastructure. Prisons Department have available infrastructure for the organization of video conference based sessions in most of the imprisonment places. Integration of such a service and infrastructure into IISPP would create the possibilities not only organizing the sessions remotely, but also involve other people into the sessions and scale it up to the real need and at the same time to record all content in the original format minimizing possibilities for defence or offense misinterpretations.

4.3.3 Increasing efficiency of the process

At the same time one of the directions that lot of end-users, systems architects, testers and usability experts are focusing and provide lot of useful insights and recommendations is improvements of existing modules and enrichment of the current functionality. The following areas are presented as most potential for the efficiency improvement:

- Manage calendars of both a prosecutor and an investigator – at the same time giving the ability for other process participants to reserve meeting times. Currently the work organization is based on pre-set time by the prosecutor or investigator. That is pretty big problem in main cities as working hours of most of the people are completely matching prosecutors Office working hours. It demands for the personal and working schedules adjustments to fit into the timeframe pre-set by prosecutor or investigator. E-Calendars will provide more flexibility for the process and at the same time will increase LEA work transparency.
- Integration into the IISPP more e-channels type communication. Currently all information is based on the paper form, even though it is presented in electronic format. More of the e-based communication would allow to decrease the number of paper based printed cases. Additional channels can be used for informing end-users, etc.
- Currently the penal process case and forensic research case are managed in two completely separate systems. It creates some inefficiency, especially in long-lasting investigation cases or cases related to some particular forensic techniques having long forensic examination queues (i.e. computer or digital forensic) where process decisions can revert the need for the forensic investigation or opposite way around -early forensic results can show different view on the case type.
    - Exchange information about the investigation and case progress;
    - Inform about completed or terminated investigation.

Early information on terminated investigation would already create finance benefit for the system, as some of forensic examinations costs are substantial sums.

- Integration with Tax Inspectorate and/or banks IS in order to acquire information about accounts, balance and movement of cash and stop illegal financial transactions or money drain operations in early stages – immediately after the decisions are registered in the IISPP.
- Integration and direct information transfer to the cremation authorities. Manual registration (as it is organized now) causes some delays between actual decision fact and information presence in the corresponding IS. It is potential area for misinterpretations of body status leading to the execution of cremation procedure and loss of evidence (in the cases when the status of the body changes during the panel process execution).
- Transfer of the information to the property seizure register:
    - To this day the information regarding the assets (real estate, vehicles) is not compared against identifiers;

    - Verification against Interpol database.
- More structured electronic message about criminal offences (E-complaint):
    - Implemented only in e-police
    - Now complaints are not well structured
    - Limited capabilities for automated process control
- Remote working place implementation:
    - Registration of remote familiarization and confirmation facts
    - Implementation of e-signing possibility
    - E-templates of procedural statements and complaints\
    - E-invite for questioning
    - Implementation of mobile IISPP workspace
- Technological developments create more possibilities for efficiency and quality improvements. With current technical developments it is possible digitally create 3D reconstruction of crime or event scene using hybrid tools and precise measurement and spacial capturing techniques. Initial assessment shows that such information is valuable not only for the LEA experts but also for the external institutions (for example, insurance companies).

4.3.4 Process management

Current IISPP solution have powerful work-flow organization engine, that can be enriched and rolled out into other cross-institutional processes at the same time providing additional benefits to the end-users and minimizing necessity for vertical communication (involving management and formal request-response pathways):

- Generating work assignments to and from other systems (for example, PRIR)

Other additional features can be summarized as follows:

- Assignments planning and priority setting
- Automatic tasks and workflow management and distribution
- Automatic creation of work assignments

This type of the functionality would enable to create and distribute all incoming cases based on their dimensions. Different setup allows automating not only national cases but also international cases if they pass security and match by information structure.

More precise data structure and process control allows automating some of the monitoring and management functions:

- Alerting on status change – allows to minimize the gap between one step completion and next step start.
- Escalation of work-flow execution issues;

The most wanted feature is historical and statistical data usage for various types of management analytics':

- Integration with IS of LEA strategic indicators and activities analysis;
- Process bottleneck analysis and identification of potential areas for improvement;
- Assessment of best practices for high performance;
- Management of statistic data.

5 CONCLUSIONS AND RECOMMENDATIONS

Assessing the potential use of IISPP for closer and smoother co-operation between Member States law enforcement authorities, requires defining the current and projected IISPP range of applications. From the initial design phase through to its current deployment, IISPP was (is) mostly focused on the national (Lithuania) needs and driven by involved national bodies. It covers main aspects of criminal proceedings panel process. However in order to implement automated and performing international cooperation solution much more institutions must be integrated into this platform (some of them have very little correlation with criminal proceedings and panel process). Otherwise, the process will remain demanding for manual steps execution and will leave the spaces for manipulation.

The SPOC Guidelines need to be transposed into the national context by the individual Member States. The application of the Guidelines' in the Member States should be evaluated by the Commission in two years from now. Consideration should be given to establishing a network consisting of SPOC staff and/or heads of SPOCs with a view to exchanging good practices and lessons learned, as well as identifying issues related to the application of the SPOC Guidelines and in particular to the choice of channel.

Member States are invited to facilitate, with the support of Commission funding, the use of all channels equally by establishing electronic case management systems for their SPOC. More specifically, without prejudice to relevant data protection standards, a national interface must be created that makes it easy to use all different channels. In order to start it working common cross-border platforms must be integrated, - including e-identity, e-authorization, e-signature, e-LEA role verification, e-case verification.

The security and functions required for the international collaboration clearly shows that it is necessary to have separate solutions implemented handling international communication and national case processing. As IISPP is national panel process IS it can be replicated in other countries as national panel process integration platform, but for the cross-border collaboration additional solution must be developed.