Teched
CONSULTING SERVICES

Law Enforcement Criminal Intelligence System

Highlights

- Supports operational work of law enforcement organizations
- Provides support in conducting covert criminal and analytical investigations
- Linking of objects that are the subject of operational, criminal or analytical investigations, such as people, vehicles, mobile phones, weapons etc.
- Need-to-know, and right-to-know security policies built into the system
- Display and analysis of geospatial data such as the location of the incident, traffic accidents, the location of a mobile phone etc.
- Management and analysis of phone call records
- Management of secret surveillance of telecommunications devices, support for listening and processing of phone calls, export of phone call data for the Court and the archiving of data
- Support for data analysis tools (Business Intelligence) such as Microsoft Excel for producing statistics and trends
- Integration with external analytical tools such as the IBM Analyst Notebook for analysts

Criminal Intelligence plays an important role in the fight against serious and organized crime, particularly due to the increasing complexity and sophistication of organized crime.

Introduction

Criminal Intelligence plays an important role in the fight against serious and organized crime, particularly due to the increasing complexity and sophistication of organized crime. If operational and intelligence capacities of a law enforcement organization are insufficient, investigators will not get timely information to help them solve crimes, apprehend perpetrators and detect illegal activities of organized crime groups. Having such problems, law enforcement organizations cannot plan a long-term law enforcement strategy.

The operational work of conducting criminal, analytical and related investigations requires many resources, and can often end up inefficient. Common problems include holding some data only on paper, unintegrated and unstructured information resources, the lack of efficient access to the overall knowledge base, as well as slow, inefficient and unsafe exchange of classified information.

In order to increase operational efficiency and productivity and to address the need for integration of available information, applications and services, as well as the requirement for national availability and secure access to all relevant data, the LECIS (**Law Enforcement Criminal Intelligence System**) was developed. **LECIS** is a **specialised system, designed to provide informa-**

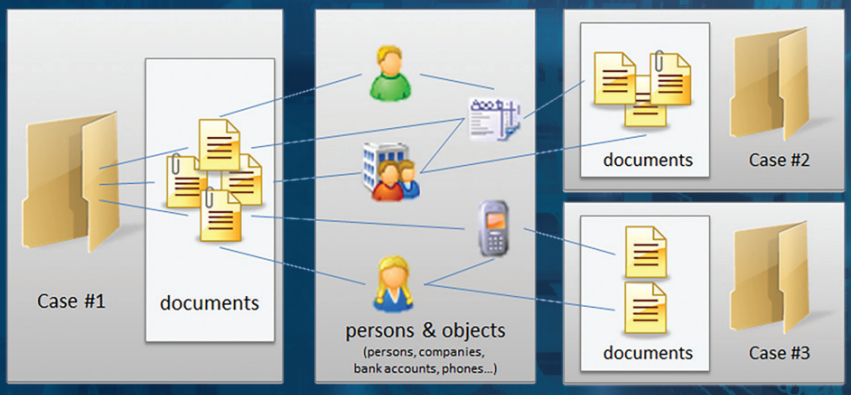


Figure 1. Intelligence Led Policing concept

Product Sheet

Law Enforcement Criminal Intelligence System

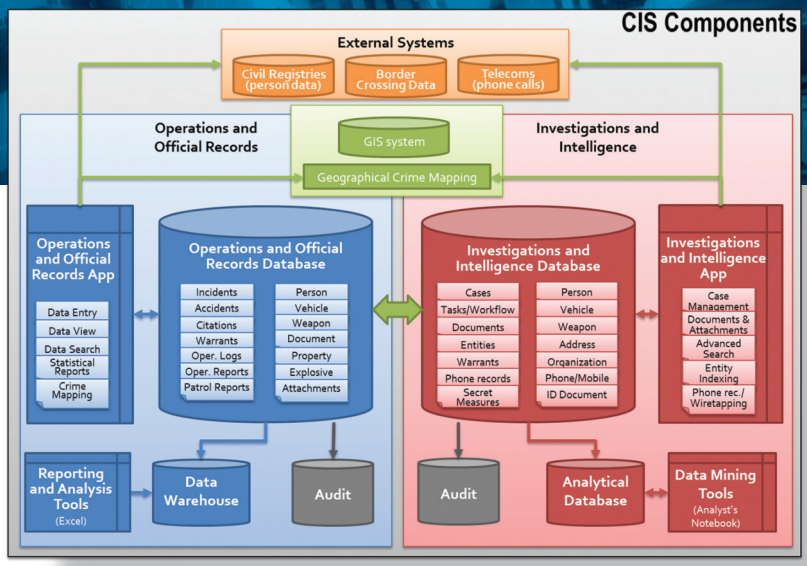


Figure 2. LECIS components

tion support for operational, criminal and analytical investigations, that enables controlled sharing of classified information stored in the system. Access permissions are given based on the need for information and the right to know, providing timely access to information. The purpose of LECIS is to **significantly speed-up the discovery of possible solutions for fighting serious and organized crime**, using state of the art intelligence and surveillance technology and monitoring of criminal activities, combining criminal intelligence and criminal investigation processes. Implementation of LECIS allows access to the required intelligence data, using **Intelligence-Led Policing principles**, which is implemented as one of the key system functionalities. At the same time, the highest international standards of quality and compliance with national and European legal requirements are maintained.

Basic features of the system

The LECIS solution is a specialized solution to provide **information support for the operational activities and tasks of law enforcement organisations, particularly when conducting criminal and analytical investigations**, although it can also be used for any type of investigation and intelligence processing. LECIS can be integrated with existing information systems and brings a whole new set of possibilities to the tasks of processing, searching and analysing data. Implementation of this system, built specifically for the needs of criminal intelligence, can significantly increase the capacity and efficiency of any law enforcement organization.

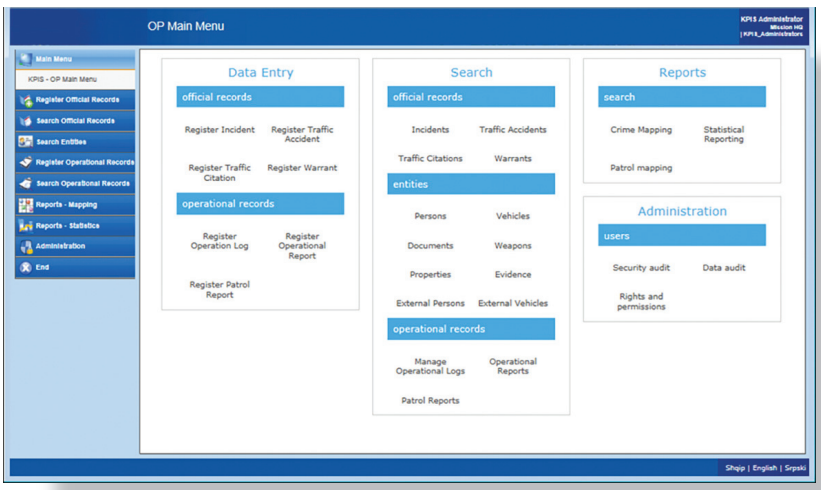


Figure 3. Module for operational records of daily events

The LECIS information system consists of independent, but linked, modules covering specific segments of the business processes followed by law enforcement organizations. The modules are:

- **a module for operational recording of daily events** (e.g. incidents, accidents, offences and traffic fines, orders for arrest);
- **a module for managing criminal and analytical investigations**;
- a **module for managing ob-**

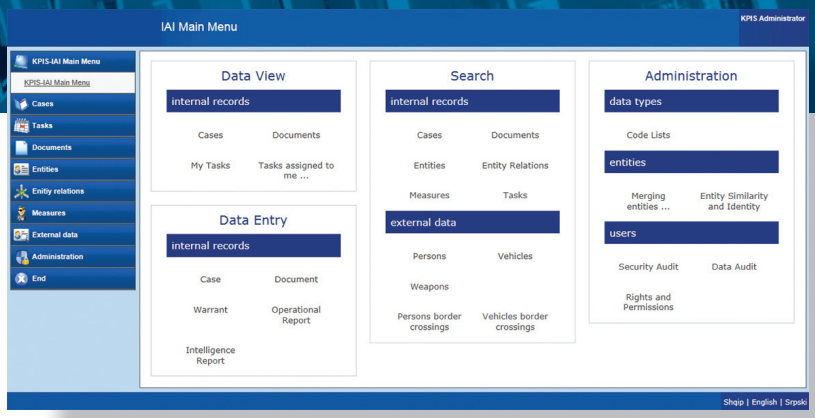


Figure 4. Module for criminal and analytical investigations

jects that appear in such daily events and criminal cases (e.g. people, vehicles, communication devices, weapons, etc.);

- a **module for managing information** (e.g. evidence, operational and analytical reports, documents, etc.);
- a **module for statistical reports**;
- a **module for displaying and analysing geo-data** (GIS);
- a module for integration with **external analytical tools** (eg. IBM Analyst Notebook).

The system also includes additional modules for managing intelligence in the field of signal intelligence (SIGINT):

- **TELint** - module for the management and analysis of phone call data;
- **KOMint** - module for processing and analysis of surveillance of telecommunications (listening in to suspects).

All modules are based on a common security module that supports individual assignment of permissions as needed (need-to-know) as well as permissions based on the role that person has in the organization (right-to-know).

Security in LECIS

The security module in LECIS is based on the premiss of granting specific permissions to individual users or groups of users (roles) in the system, also taking into account the **specifics of the organizational hierarchy, whether geographical or lineal**, of the law enforcement organization. In this way, the implicit access permissions such as "a senior officer must always have the permission to access information produced by subordinate employees" or "a line manager must be able to see all information produced in his line of work" are converted into explicit permissions managed by the security module, and, thus, at any moment it is known who can access particular protected information.

Permissions to access objects in the LECIS can be granted or denied based on:

- The **position that person holds**

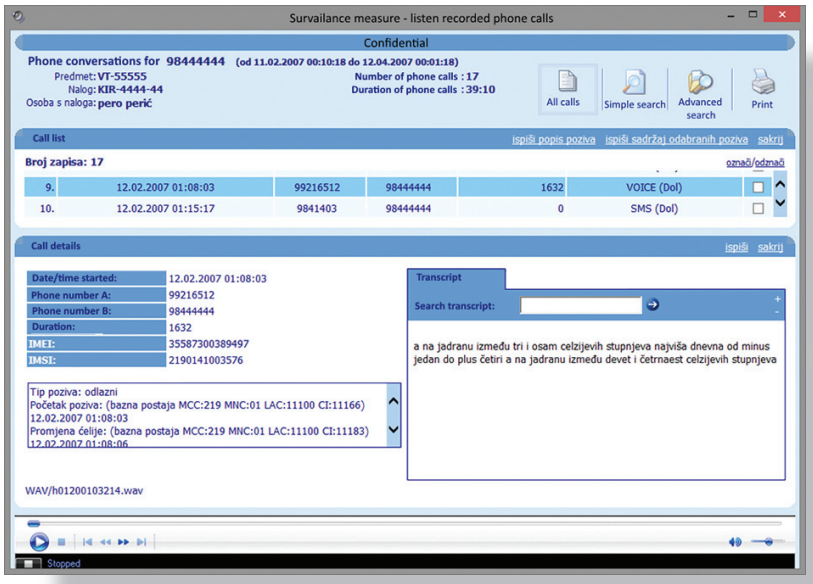


Figure 5. Offline application for calls exported from KOMint: audio, fax, SMS, MMS

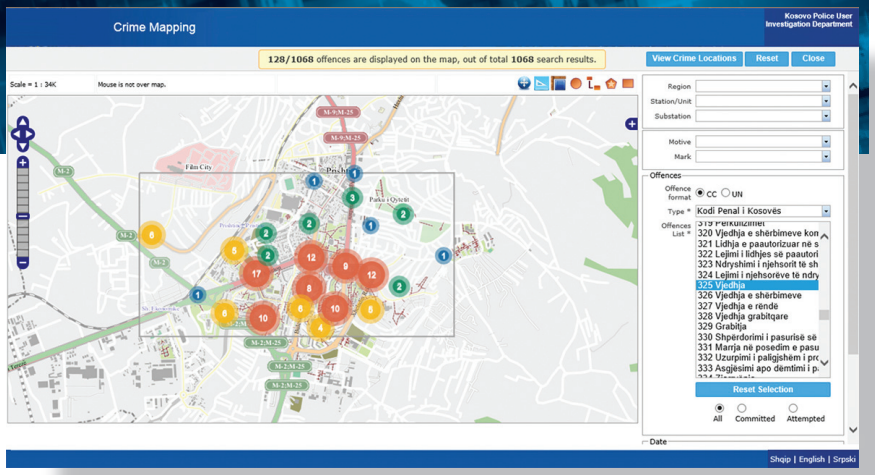


Figure 6. Analysis of geographical data - incidents, traffic accidents, mobile phone location

in the organizational structure (e.g. all employees in an organizational unit will have an initial permission to access certain information created in that organizational unit and all subordinate organizational units);

- **Assignment of a person to an investigation** (e.g. all officers who work on a specific case will have permission to access all information within that case);
- **Individual**: permission to certain information may be granted or denied to a particular user of the system, independently of the role of the person in the system or case the person is working on.

In addition to checking the rights and permissions in the system, **the security module records all actions which users perform in the system. Audit records are created when data is created, read, modified or deleted**.

TELint

Phone call records can provide valuable information for carrying out criminal and analytical investigations. Since there is usually a large amount of available phone call records data, it is necessary for the system to provide functionality for analysing the collected data. The main purpose of TELint tools are to enable the import of data to the intelligence database and to analyse the phone call records. TELint module supports an efficient and fast analysis, enabling users to **store and process hundreds of millions of phone call records** as well as maintaining the high performance of the system.

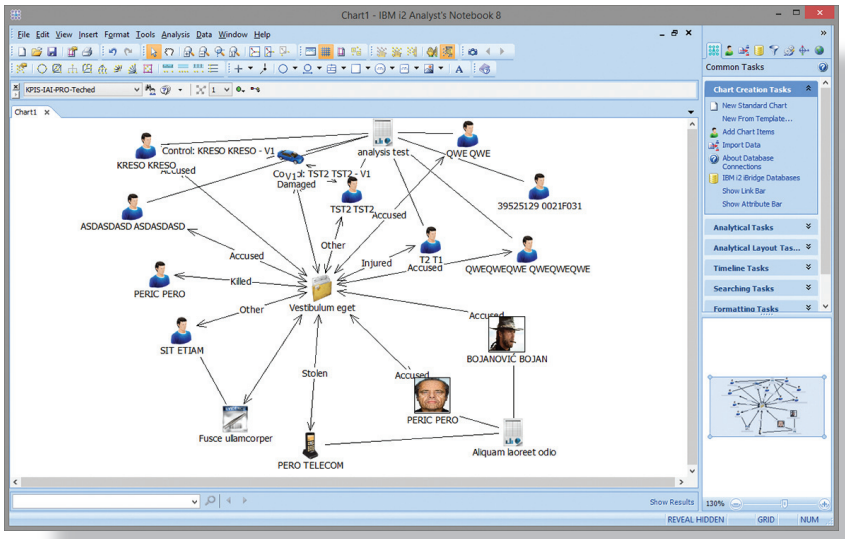


Figure 7. Integration with external analytical tools - IBM Analyst Notebook

KOMint

Telephone surveillance of suspects are of extreme importance to analysts and operatives during the course of investigations and during the apprehension of suspects. **KOMint module provides users with a way to listen to suspect phone calls as soon as possible after the end of the conversation, using streaming technology**, in any organizational unit in the country, even those with a lower capacity of network links. KOMint provides information during the course of the conversation, such as the position of the suspect, on the basis of base stations of mobile networks. Such information is used to locate a suspect's whereabouts, which is particularly important during operative actions such as the apprehension of suspects.

Additional functionality provided by the KOMint system is the ability to **export all processed phone calls to external storage**

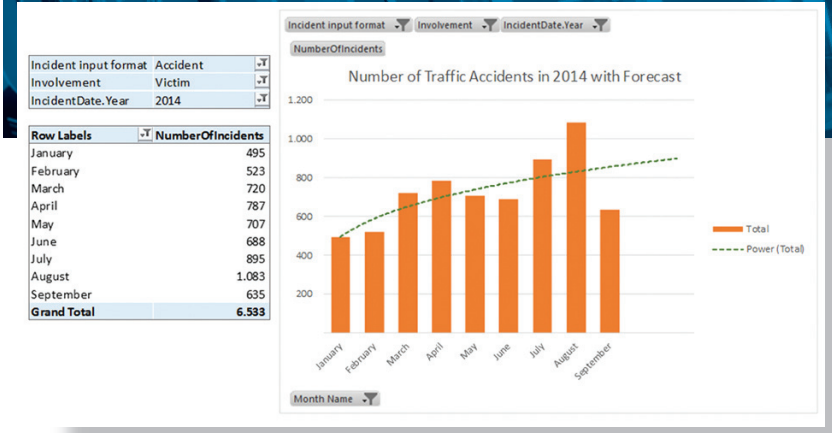


Figure 8. Data mininig and business intelligence with forecast analysis

(CD, DVD, etc.) A linked application allows users to view this data off-line, to run simple and advanced searches and to print the data. **Such external storage can serve as evidence in a court case**, thus eliminating the need to print phone calls to paper and deliver them in paper format.

GIS

A lot of data stored in LECIS may be associated with geographical coordinates. Examples include incidents, accidents, location of mobile phones, etc. LECIS includes a **module for display and analysis of this geographic data**. Given the sensitivity of information in the system, prior to displaying them on the map, data are filtered according to the search parameters and the access permissions so that at any time a user sees only the data he/she is authorized to see.

External analytical tools

Analysts in law enforcement organizations need to detect or 'extract' hidden knowledge from the collected data, in a simple and effective way, using analytical tools. Such tools can provide better information, presented in the most suitable way for these analysts.

With special software interfaces built into the system, LECIS becomes a source of information for external analytical tools that may already be present in the law enforcement organization. LECIS has procedures to synchronize data between its central analytical database and the analytical databases of individual police departments, thus enabling an effective analysis of data in remote locations, spreading the load on system resources and ensuring efficient and secure carrying out of investigations and analysis of the available data.

LECIS prepares data in such a way that it can be used by the most popular analytical tools, including IBM Analysts Notebook, one of the best known and most widely used analytical tools in law enforcement organizations.

Statistical reporting and BI

LECIS allows users to use standard, predefined statistical reports (such as number of incidents in a given time period, list of traffic citations, etc.) and en-

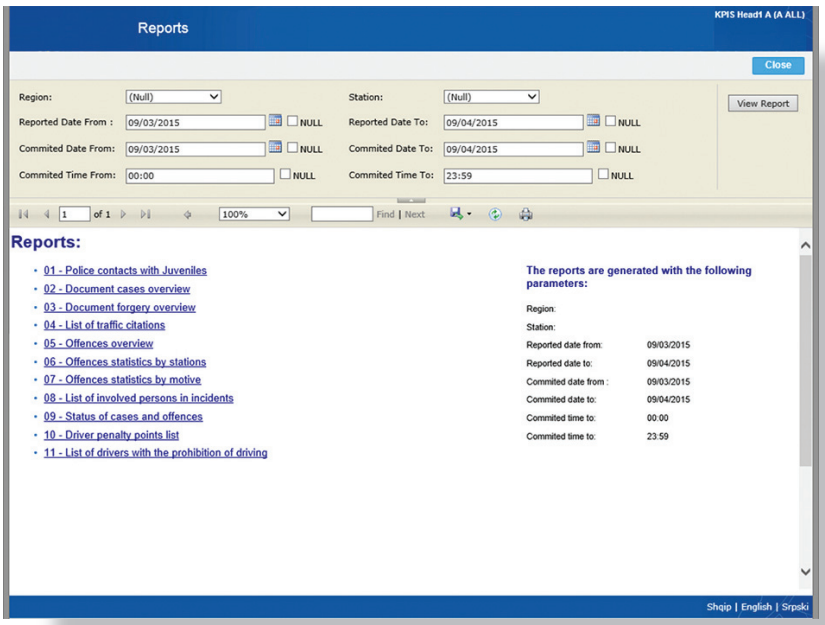
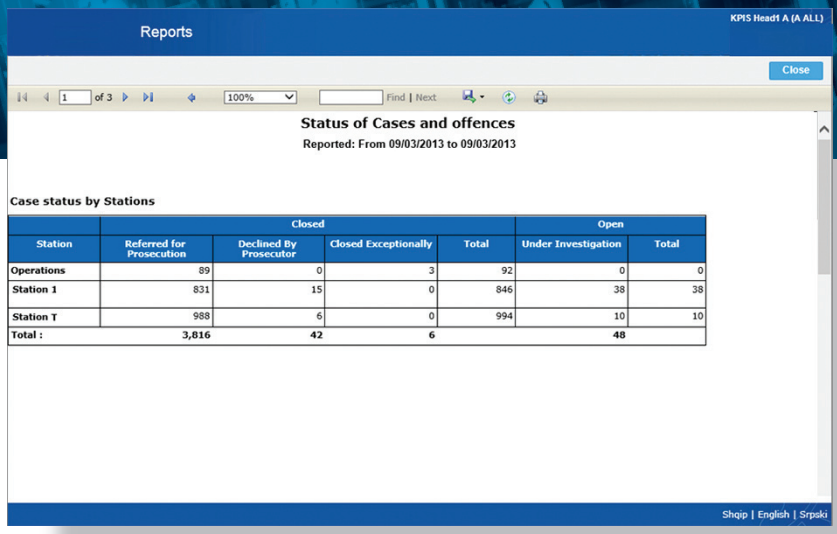


Figure 9. Predefined statistical reports

ables **data mining and business intelligence using OLAP client tools (such as Microsoft Excel)**.



Station	Closed				Open	
	Referred for Prosecution	Declined By Prosecutor	Closed Exceptionally	Total	Under Investigation	Total
Operations	89	0	3	92	0	0
Station 1	831	15	0	846	38	38
Station T	988	6	0	994	10	10
Total :	3,816	42	6		48	

Figure 10. Results of predefined reports

Case Studies

Various modules of LECIS have been implemented in the Croatian Ministry of Interior for the Croatian police, in the Kosovo Police and the Office of the Croatian State Attorney. Each implementation has been further adapted to the requirements of the individual organization.

Croatian Ministry of Interior. The system was originally developed for the Ministry of Interior in order to assist them in investigating into serious and organized crime, providing them with state of the art intelligence, for investigating criminal activities, combining criminal intelligence and criminal investigations. Implementation of the system was based on the Intelligence Led Policing model which is the key functionality of the system.

Kosovo Police. The implementation was focused on the collection of key operational information that acts as a record of actions, and can be used for carrying out investigations and for strategic and tactical planning. The system is designed to support the basic operations of the Kosovo Police, and also allows for integration with other databases. The system is multilingual and is implemented in all three official languages. This implementation of the LECIS solution included operations, investigations and intelligence modules.

Office of the Croatian State Attorney. The Office for Combating Corruption and Organised Crime (USKOK) is a specifc office of the State Attorney which is responsible for the prosecution of corruption and organized crime. The office had a need for a new system that would provide support to employees in performing their everyday tasks - with special emphasis on the analysis of data collected during investigations. As a result of these needs, a case management module of LECIS was implemented based on our experience in development and implementation of criminal intelligence systems.

Benefits of implementing LECIS in a law enforcement organization

LECIS combines available information resources, services and systems within an organization and supports the core business processes of a law enforcement organization. At the same time, it pays great attention to confidentiality, integrity and availability of information stored in a central database. Benefits the law enforcement organizations get are:

- Work based on standard processes and procedures built in the system
- Efficient conducting of investigation and case management
- Increased operational efficiency and productivity
- Compliance with the regulations and reduced risk

Contact us

If you would like to find out more about Criminal Intelligence Systems in the field of Law Enforcement based on the Intelligence-led policing model, please contact us.

Teched
CONSULTING SERVICES
Capraška ulica 6/VI
10 000 Zagreb, Croatia
Phone: +385 1 4697 600
Fax: +385 1 4697 615
E-mail: teched@teched.hr
Web: www.teched.eu