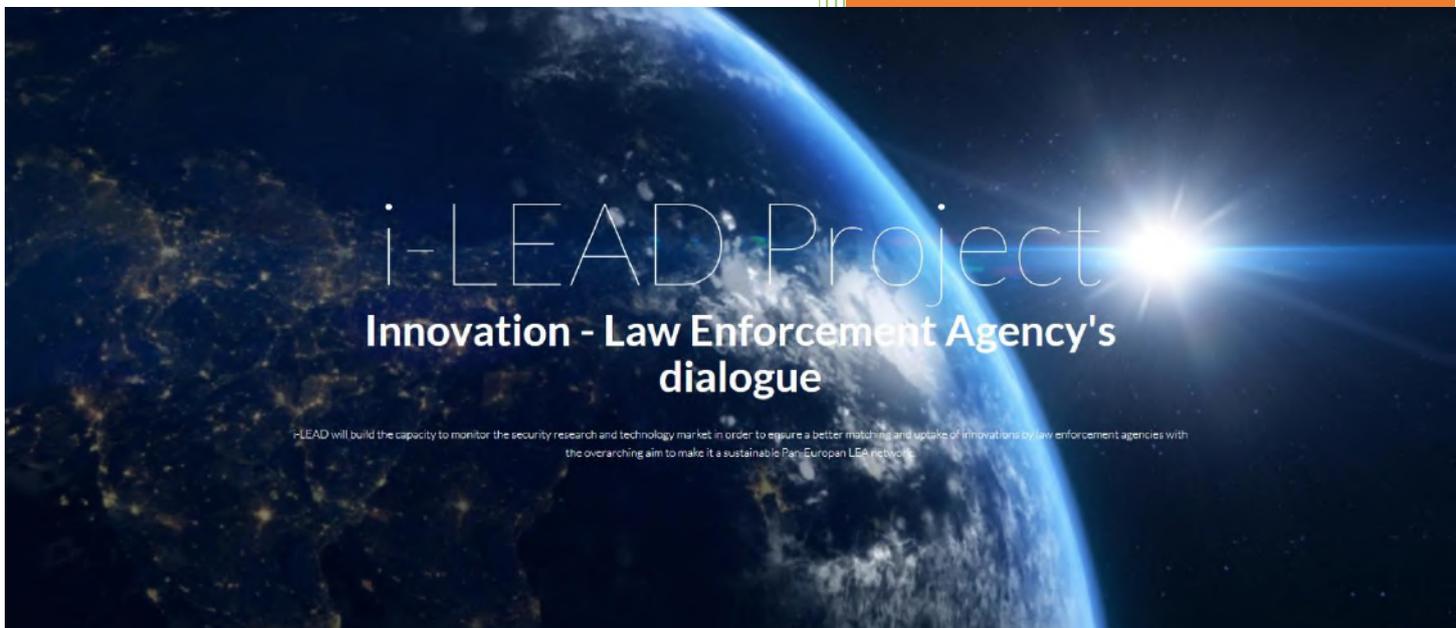




innovation - law enforcement agency's dialogue

2020

**WP4 Reports - Recommendations on Standardisation and Procurement**



**in the areas of**

**Crime Scene  
Recording and  
Documentation**

**Digital Investigation**

**Crime as a Service**

**Vehicle Mitigation**



i-LEAD is funded by the European Union's Horizon 2020 - Research and Innovation Framework Programme, under grant agreement no 740685

## Table of Contents

<b>1. I-LEAD abstract.....</b>	<b>2</b>
<b>2. WP4 description.....</b>	<b>2</b>
<b>3. Crime Scene Recording and Documentation.....</b>	<b>3</b>
<b>4. Digital Investigation .....</b>	<b>5</b>
<b>5. Crime as a Service.....</b>	<b>7</b>
<b>6. Vehicle Mitigation .....</b>	<b>10</b>

## 1. I-LEAD abstract

The I-LEAD, (Innovation – Law Enforcement Agencies Dialogue) is a coordination and support action project funded by the European Commission through Horizon 2020 Programme. The main aim of the project is to develop a Pan European Network of practitioners and other actors in the field of security to:

- 1) Monitor research and innovation projects with a view to recommending the uptake or the industrialisation of the results.
- 2) Express common requirements of Law Enforcement Agencies (LEA's) with regards capability gaps and determine innovative and fit for purpose solutions to address the gaps and improve future performance.
- 3) Indicate priorities as regards domains requiring more standardisation.

The official start of the 5-year project was September 2017 and is coordinated by the Dutch National Police and consists of a consortium of 19 partners.

The I-LEAD project will build LEA community networks around 5 specific key Practitioner Groups these being:

- Front Line Policing
- Cross Border Crime
- Cybercrime
- Crime & Intelligence
- Forensics

More information about the project at can be found at: [www.i-lead.eu](http://www.i-lead.eu)

## 2. WP4 description

Work Package 4 - standardisation and procurement (WP4) is viewed as the supporting department for the I-LEAD project. It will liaise with practitioners of the community networks to determine the present situation with regards standardisation, and if relevant and required, put forward recommendations for the development of existing standards or the creation of new standards.

This objective is to support LEA's within Europe to strengthen cross border cooperation in the fight against crime and terrorism via the standardisation of technologies, procedures and processes, in the activities of; criminal investigation, offender detection and the gathering and submission of evidence that is acceptable by courts of law.

Further, EU-wide standards will also enable economy of scale advantages for both LEA's and suppliers (industry and SME's) of technologies, tools, systems and services, as the same product will meet the requirements of each LEA (in most) of the EU Member States. From that reason developing new tools and solutions will be more cost-effective. And finally, common standards will also accelerate pre-commercial procurement (PCP) and public procurement of novel solutions and products.

WP4 is designed to meet the following main objectives:

- Examine the opportunities for standardisation of the results of Practitioner Groups workshops.
- Build the European LEA capacity and knowledge for joint procurement actions
- Accelerate process of joint PCP and PPI projects.

### 3. Crime Scene Recording and Documentation

#### State of the art in the field of Crime Scene Recording and Documentation in terms of standardisation and procurement

There is a lot of activity in the field of forensic sciences, especially in but not limited to the committees ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection" and ISO/TC 272 "Forensic Sciences". Below are the most relevant standards, both published and under development:

- **ISO/IEC 17020:2012**, reviewed and confirmed in 2017: *Conformity assessment - Requirements for the operation of various types of bodies performing inspection.*
  - Specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities.
- **ISO/IEC 17025:2017**: *Testing and calibration laboratories.*
  - Enables laboratories to demonstrate that they operate competently and generate valid results, thereby promoting confidence in their work both nationally and around the world. It also helps facilitate cooperation between laboratories and other bodies by generating wider acceptance of results between countries. Test reports and certificates can be accepted from one country to another without the need for further testing, which, in turn, improves international trade.
- **ISO 18385:2016**: *Minimizing the risk of human DNA contamination in products used to collect, store and analyze biological material for forensic purposes — Requirements*
  - This document specifies requirements for the production of products used in the collection, storage, and analysis of biological material for forensic DNA purposes, but not those consumables and reagents used in post-amplification analysis.
  - Currently, the Technical Committee is voting on whether this standard needs to be reviewed. The vote will end on March 2021.
- **ISO 21043-1:2018**: *Forensic sciences — Part 1: Terms and definitions*
  - This document terms used in the ISO 21043 series of standards.
- **ISO 21043-2:2018**: *Forensic sciences — Part 2: Recognition, recording, collecting, transport and storage of items*
  - This document specifies requirements for the forensic process focusing on recognition, recording, collection, transport and storage of items of potential forensic value. It includes requirements for the assessment and examination of scenes but is also applicable to activities that occur within the facility. This document also includes quality requirements.
- There are three more parts being worked on in the ISO 21043 series. Part 3 on Analysis, Part 4 on Interpretation, and Part 5 on Reporting. These are all expected to be published in 2021.
- **CEN/CWA Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain**
  - This is a document by Horizon2020 project FORMOBILE, which has been set up to establish a complete end-to-end forensic investigation chain that targets mobile devices and includes an appropriate standard. A relevant aspect of this project is, for instance, the seizure of devices and documentation of all investigation steps. It is set to be published in March 2020.

Recommendations on standardisation and procurement in the field of Crime Scene Recording and Documentation, concentrating on the 'THOR' dimensions ( <i>technical, human, organisational and regulatory</i> )				
	Practitioners' needs and requirements (based on PG meeting)	Standards recommendations	Legislative recommendations	Joint Procurement recommendations
1.	Standardisation of trainings	<p>Unification and implementation of technical training for Crime Scene Investigators (CSIs) and prosecutors. They will allow officers to have the right skillset and knowledge to use the digital elements in their investigation.</p> <p>Awareness raising.</p> <p>A similar project on the establishment of a set of skills for experts has been started in CEN-CLC/JTC 13 "Cybersecurity", a joint Technical Committee of CEN and CENELEC.</p>	<p>EU recommendations in this field might be helpful</p>	-
2.	Data retention rules	-	<p>A need to change law regarding data retention time (e.g. people's DNA and any imagery that was inadvertently captured when conducting 3D scans or from drones). Practitioners stated that the duration often makes it impossible to process all administrative tasks.</p>	-

3.	Data processing and sharing standardisation	Unification of data processing and sharing methods and formats would be beneficial to improve the ability to share data with both national and international LEAs.	EU recommendations in this field might be helpful	A <u>central online sharing platform</u> would allow for faster connectivity and more data sharing between (national/international) partners.
4.	Drones/robotics procurement	-	-	A joint PCP/PPI for enhanced drone or other data collection technologies, allowing easier and also indoor collection of data for the CSIs would be beneficial.
<b>Recommendations for Pre-Commercial Procurement (PCP) / Public Procurement of Innovative solutions (PPI) / Fast Track for Innovation (FTI), regards to Crime Scene Recording and Documentation</b>				
There is a common agreement that an enhanced technology is needed for more efficient crime scene recording and documentation. Practitioners mentioned the desired characteristics and features of such a drone/scanner/ device. Thus the outcomes of the Practitioners Meeting can be a basis for further work on a joint PCP/PPI for the LEAs.				
<b>Additional recommendations and remarks</b>				
<ol style="list-style-type: none"> <li>1. Exchanging technical specification of tools and solutions for Crime Scene Recording would be helpful.</li> <li>2. Training the Crime Scene Investigators and equipment necessary for Crime Scene Recording is expensive therefore buying a service of recording the crime scene could be good solution (outsourcing).</li> </ol>				

## 4. Digital Investigation

<b>State of the art in the field of Digital Investigations in terms of standardisation and procurement</b>
<p>The most relevant standards in the field of Digital Investigation are:</p> <ul style="list-style-type: none"> <li>• <b>ISO/IEC 27037:2012</b>, reviewed and confirmed in 2018: <i>Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence</i> <ul style="list-style-type: none"> <li>○ This document provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value.</li> </ul> </li> <li>• <b>ISO/IEC 27041:2015</b>: <i>Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method</i> <ul style="list-style-type: none"> <li>○ This document provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods, and providing evidence that implementations of methods can be shown to satisfy requirements. It includes consideration of how vendor and third-party testing can be used to assist this assurance process.</li> <li>○ This document is currently under vote for review.</li> </ul> </li> <li>• <b>ISO/IEC 27042:2015</b>: <i>Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence</i> <ul style="list-style-type: none"> <li>○ This document provides guidance on the analysis and interpretation of digital evidence in a</li> </ul> </li> </ul>

manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.

- This document is currently under vote for review.
- **ISO/IEC 27050 series: Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence**
  - Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. This document provides an overview of electronic discovery.
  - There are currently three parts: Part 1 "Overview and concepts", Part 2 "Guidance for governance and management of electronic discovery" and part 3 "Code of practice for electronic discovery"
- **CEN/CWA Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain**
  - This is a document by Horizon2020 project FORMOBILE, which has been set up to establish a complete end-to-end forensic investigation chain that targets mobile devices and includes an appropriate standard. A relevant aspect of this project is, for instance, the seizure of devices and documentation of all investigation steps. It is set to be published in March 2020.

**Recommendations on standardisation and procurement in the field of Digital Investigations, concentrating on the ‘THOR’ dimensions (technical, human, organisational and regulatory)**

	<b>Practitioners’ needs and requirements (based on PG meeting)</b>	<b>Standards recommendations</b>	<b>Legislative recommendations</b>	<b>Joint Procurement recommendations</b>
1.	Standardisation of trainings	Unification and implementation of technical training for LEA are necessary. They will allow officers to have the right skillset and knowledge to use the digital elements in their investigation. Awareness raising.	EU recommendations in this field might be helpful	-
2.	Standardisation of procedures	Standardisation of Digital Investigation procedures covering all aspects of investigation – from the scene to the courts	EU recommendations in this field might be helpful	-
3.	Data sharing standardisation	Unification of data sharing methods and formats would be beneficial to improve the ability to share data with both national and international LEAs.	EU recommendations in this field might be helpful	A <u>central online sharing platform</u> would allow for faster connectivity and more data sharing between (national/international) partners.

4.	Cryptocurrency technology	-	-	Practitioners underlined that there is a growing need to procure cryptocurrency analysis tools which could identify, track and analyse any suspicious transactions and quickly identify the parties to the transaction.
5.	Cloud storage access technology	-	EU recommendations in this field might be helpful	Practitioners stressed out that there is a need to have a tool allowing the analysis of individuals cloud storages.
6.	Data retention rules	-	A need to change law regarding data retention time. Practitioners stated that the duration often makes it impossible to process all administrative tasks.	-
<b>Recommendations for Pre-Commercial Procurement (PCP) / Public Procurement of Innovative solutions (PPI) / Fast Track for Innovation (FTI), regards to Digital Investigation</b>				
The need for an effective cryptocurrency analysis or cloud storage analysis tool could be a basis for joint PCP or PPI.				
<b>Additional recommendations and remarks</b>				
-				

## 5. Crime as a Service

### State of the art in the field of Crime-as-a-Service in terms of standardisation and procurement

#### Relevant standards:

- **ISO/IEC 27001:2013**, reviewed and confirmed in 2019: *Information technology — Security techniques — Information security management systems — Requirements*
  - This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.
- **ISO/IEC CD 27032**, *Information Technology — Cybersecurity — Guidelines for Internet Security*
  - This document is under development and expected late 2021.
- **ISO/IEC 27035 series**, *Information technology — Security techniques — Information security incident management*
  - This series provides basic principles for information security incident management (Part 1), Guidelines to plan and prepare (Part 2), Guidelines for response operations (Part 3) and

Coordination (Part 4)

- Part 1 and 2 are currently being reviewed, Part 3 has only recently been published, Part 4 is now being developed.
- **ISO/IEC 27042:2015: Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence**
  - This document provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.
  - This document is currently under vote for review.
- **ISO/IEC 27043:2015, reviewed and confirmed in 2020: Information technology — Security techniques — Incident investigation principles and processes**
  - This document provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence.
- **ISO/IEC TR 27103:2018, Information technology — Security techniques — Cybersecurity and ISO and IEC Standards**
  - This document provides guidance on how to leverage existing standards in a cybersecurity framework.

Relevant TCs:

- ISO/IEC JTC 1/SC 27: 'Information security, cybersecurity and privacy protection'

**Recommendations on standardisation and procurement in the field of Crime-as-a-Service, concentrating on the 'THOR' dimensions (technical, human, organisational and regulatory)**

	<b>Practitioners' needs and requirements (based on PG meeting)</b>	<b>Standards recommendations</b>	<b>Legislative recommendations</b>	<b>Joint Procurement recommendations</b>
1.	Crime reports standardisation	A setting of reporting schemes and common agreement on boundary reporting fields and areas would be helpful for the investigation and data collection purposes.	EU recommendations in this field might be helpful	-

2.	Standardisation of exchange of information with private insititutions	Unification of data and information exchange and regulations is necessary for LEA to effectively combat CaaS. This relates mostly to the communication with Internet Service Providers.	EU recommendations in this field might be helpful	-
3.	Standardisation of data formats and gathering methods	<ul style="list-style-type: none"> <li>- Unification of data sharing methods and formats would be beneficial to improve the ability to share data with both national and international LEAs;</li> <li>- The Cloud (see procurement ideas) could also summarize, calssify and link the cases inputted by LEA.</li> </ul>	EU recommendations in this field might be helpful	
4.	Joint platform for the major ISP	-	-	Procurement of a joint platform for all LEA and Internet Service Providers that would allow asking for data and the standardization of the request process.
5.	Harmonisation of law/harmonisation of LEAs procedures as the crimes outreach single jurisdiction	Standardisation of procedures covering all aspects of investigation – from the scene to the courts	EU recommendations in this field might be helpful	-
6.	Standardisation of trainings	Unification and implementation of technical training for LEA are necessary. They will allow officers to have the right skillset and knowledge to use the digital elements in their investigation. Awareness raising.	EU recommendations in this field might be helpful	-

7.	PCP/PPI of technologies that would allow efficient CaaS fighting	-	-	Practitioners underlined that there is a growing need to procure cloud tool to allow common data gathering and classifying the cases. Moreover a tool for real-time decryption is needed.
<b>Recommendations for Pre-Commercial Procurement (PCP) / Public Procurement of Innovative solutions (PPI) / Fast Track for Innovation (FTI), regards to Crime-as-a-Service</b>				
There is a common agreement that an enhanced technology is needed for more efficient cloud repository tool to allow common data gathering and classifying the cases Thus the outcomes of the Practitioners Meeting can be a basis for further work on a joint PCP/PPI for the LEAs.				
<b>Additional recommendations and remarks</b>				

## 6. Vehicle Mitigation

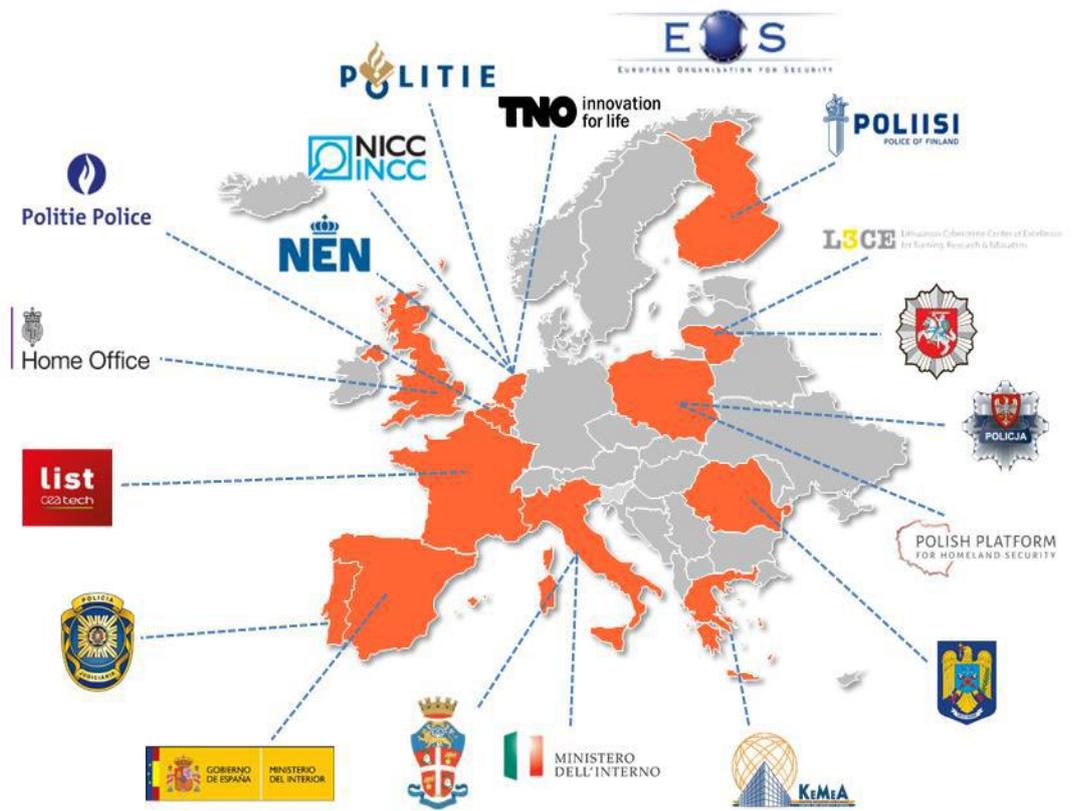
<b>State of the art in the field of Vehicle Mitigation in terms of standardisation and procurement</b>				
There have been no relevant standards or Technical Committees identified, apart from the ISO IWA 14 standard related to vehicle security barriers, which is more of a side standard than the core element of PG meeting. Therefore, there is an opportunity to attract discussion on new standardisation and procurement fields for standardisation bodies.				
<b>Recommendations on standardisation and procurement in the field of Vehicle Mitigation, concentrating on the 'THOR' dimensions (technical, human, organisational and regulatory)</b>				
	<b>Practitioners' needs and requirements (based on PG meeting)</b>	<b>Standards recommendations</b>	<b>Legislative recommendations</b>	<b>Joint Procurement recommendations</b>
1.	Standardisation of internal and external LEA communication	-	-	There is a need for technology allowing quick and efficient internal and cross-border communication and data exchange e.g. on the ANPR, facial recognition effects etc. The software needs to ensure interoperability and swift data processing.

2.	Harmonisation of law on vehicle mitigation	-	Currently different LEA have to follow different national legal provisions e.g. if police is allowed to touch the vehicle, technologies and action means that are allowed to use, GDPR provisions incorporations differ. This makes it harder to standardise procedures or procure technology.	-
3.	Joint adoption of existing standards/Dissemination action for existing standards	In order to harmonise the procedures, it was suggested to adopt the ISO IWA 14 standard, which is an impact test standard detailing the method and means of measuring the performance outcome for impact tested vehicle security barriers (VSB).	EU recommendations in this field might be helpful	-
4.	Standardisation of trainings and good practices sharing	Unification and implementation of technical training for Vehicle Mitigation. They will allow officers to have the right skillset and knowledge to use the digital elements in their actions.	EU recommendations in this field might be helpful	-
<b>Recommendations for Pre-Commercial Procurement (PCP) / Public Procurement of Innovative solutions (PPI) / Fast Track for Innovation (FTI), regards to Vehicle Mitigation</b>				
The practitioners agreed that a joint procurement of vehicle mitigation technology would be beneficial to all EU LEA. The talks focused mainly on a safe stop system (radio pulse disabling electronics, invisible to suspects, working on all vehicles, accessible and smaller than what is available now). There is a potential for PCP or PPI in this field.				
<b>Additional recommendations and remarks</b>				
-				



# i-LEAD

innovation - law enforcement agency's dialogue



[www.i-lead.eu](http://www.i-lead.eu)

