Council of the
European Union

**Brussels, 11 November 2020**
**(OR. en)**

**11824/20**

**LIMITE**

**IXIM 101**
**JAI 817**
**COMIX 462**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Working Party on JHA Information Exchange (IXIM) / Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein) |
| No. prev. doc.: | WK 6096/20; 10429/20 |
| Subject: | Roadmap for standardisation for data quality purposes |

## INTRODUCTION

Today, and in the years to come, as a result of the evolving terrorist threats and continuous migratory pressure, the European Union will be facing a dual challenge:

- One the one hand, to ***remain open to the rest of the world***, since the world has never been smaller than it is today. Countries, businesses, organisations and people are more interconnected and interdependent than ever before.

- On the other, to ***stay secure***, since security and safety are one of the major concerns of the European citizens.

Internal security, border management and migration are crucial elements of the response to this challenge. However, today they are a challenge on their own as well. In an increasingly globalised world, economic prosperity relies on the free movement of goods and people, but if those flows are not monitored and controlled the result can be smuggling, trafficking and irregular migration. Moreover, with them come organized crime and terrorism. How can we reconcile these contradictions and make internal security, border management and migration more efficient and agile?

To answer this question we have to recognise that internal security, border management and migration are going through a fundamental transformation:

- First, they are information driven and today **information is the most valuable asset**;
- Second, their efficiency is totally **dependent on digital technologies**, infrastructure and large-scale IT systems;
- Third, there is a rapid process of **convergence** between border management, migration management and internal security.

Therefore, there is a need for **paradigm shift** from them being built on **physical assets** to being built on **digital assets,** and from a **silo-based approach** to **integration and information exchange**.

Digital technologies will be a key enabler and success factor of this change. However, the information, operational and technical **silos** created in the past **are no longer fit for purpose**. There is a **need** for a **new integrated information architecture** for internal security, border management and migration. It should consolidate the capabilities of digital technologies and available information and provide an extended and powerful tool for practitioners, increasing the efficiency of their daily work.

This need has been clearly recognised by the EU. In recent years, a crucial element of its response to it is the efforts to address existing information gaps and to strengthen and develop further information exchange and management.

With these objectives in mind, in recent years the EU has launched a number of new initiatives, in particular:

- The European Entry/Exit System (EES);
- The European Travel Information and Authorisation System (ETIAS);
- The European Criminal Records Information Systems – Third Country Nationals (ECRIS-TCN);
- Interoperability architecture for the large-scale IT systems in the JHA domain.

These initiatives aim to make information exchange and information management in the European Union more efficient and comprehensive and to deploy a **new information architecture for internal security, border management and migration in the EU.** However, once deployed, the ability of this new information architecture to deliver its anticipated policy objectives and operational benefits will depend largely on the quality of the data fed into it and timely and efficient access to the information extracted from that data. For this reason, alongside with its implementation EU needs deployment of a **new eco system** of devices and solutions for the acquisition of raw data and access to information for the purposes of internal security, border management and migration as well as the further strengthening of cybersecurity**.**

Development and implementation of the interoperability architecture, as outlined in the Interoperability Regulations[1], will substantially reduce the currently existing information gaps and will consolidate and streamline access to information available in the already existing[2] and the new[3] information systems for border management and internal security. However, two preconditions must be fulfilled in order to achieve maximum effect from the interoperability architecture, once it is deployed. First, the data entered in the systems needs to be of very high quality. Second, end-users should have timely, secure and comprehensive access to information derived from the data stored in the systems.

[1] Regulation (EU) 2019/817 and Regulation (EU) 2019/818.

[2] Schengen Information System (SIS), Visa Information System (VIS) and the European Asylum Dactyloscopy Database (Eurodac).

[3] Entry/Exit System (EES), European Travel Information and Authorisation System (ETIAS) and the European Criminal Records System for Third Country Nationals. (ECRIS-TCN).

Therefore, to maximise the operational benefits of the new information architecture for the Member States in parallel with its deployment, an essential element is the development, endorsement and implementation of common standards (where relevant) in key areas.

At the initiative of the Croatian Presidency and followed up by the German Presidency, within the framework of the Working Party on JHA Information Exchange (IXIM), the need for a Roadmap with a comprehensive set of actions has been agreed. The purpose of the Roadmap is to address gaps pertaining to data quality and access to information by way of the development, endorsement and implementation of common standards in the following areas: quality of biometric data; quality of alphanumeric data; devices for the acquisition of raw biometric data; mobile devices and solutions for access to the information available through the new interoperability architecture; and cyber security.

This document contains the Roadmap with targeted short- and medium-term actions, as well as long-term directions aimed at enhancing data quality and access to information through the interoperability architecture in the JHA area. The Roadmap builds on the activities carried out during the recent years[4], and takes into account the outcome of the recent discussions within the scope of the IXIM WP meetings on 26 February[5], 3 June[6] and 16 July 2020.

The development and implementation of the Roadmap, as well as the monitoring of the results, reviewing and updating it when the need arises, requires a coordinated approach from the relevant stakeholders, including the Council and Member States' authorities, the Commission, and the relevant JHA agencies. The Roadmap provides a comprehensive approach and a coherent framework for improving data quality, data acquisition and access to data. It includes an analysis of the key challenges linked to data quality, data collection and access to data in the JHA area from the perspective of the Member States and other stakeholders, as well as an overview of the actions taken so far. The Roadmap also defines key principles for the implementation, monitoring and follow-up of the actions defined in the Roadmap (Chapter 1). The key elements of the Roadmap are the lists of actions proposed for implementation in each of the thematic areas:

[4] E.g. the 'Final Report of the High-level expert group on information systems and interoperability'; the 'Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area'.

[5] 5924/20.

[6] 7125/20.

- Data quality standards and processes for biometric and alphanumeric data (Chapter 2);
- Creation of a reference catalogue of devices and solutions for the acquisition of data and access to information (Chapter 3);
- Cyber security (Chapter 4).

## 1. State of play, overall framework and key principles

### 1.1. State of play

This Roadmap builds on the work that has already been done in the area of data quality concerning data stored in the large-scale IT systems in the JHA area at Member State and EU levels. Within the scope of this Roadmap, the Presidency circulated a questionnaire proposed by eu-LISA in order to collect information from Member State authorities on the challenges they face concerning data quality and the actions already taken at Member State level to tackle those challenges. In their responses, Member States indicated that a wide range of actions have been and are being implemented.

With regard to the quality of biometric data, several Member States have indicated that they have implemented a national ABIS/AFIS system with automatic quality control, as well as having procured new hardware and software for biometric enrolment and identification with the possibility of controlling the quality of biometric samples at the hardware and software levels. In addition, the majority of the Member States responding to the questionnaire indicated that continuous training of the end-users of biometric equipment is performed in order to address the human factor. Member State authorities have also taken action on improving the quality of alphanumeric data, such as the definition of business rules in the systems at national level, as well as integration with other systems at national level, such as population registers, for data verification purposes[7].

[7] For a more comprehensive overview of Member States' responses to the questionnaire, please consult Annex I.

CRRS[8] will be an important technical component enabling effective and efficient reporting, including reporting on data quality. It will replace the reporting systems currently in place in each of the systems. CRRS will remove the need for direct access by eligible authorities to information in the systems, enabling the consistent analysis of anonymised data and streamlined reporting, including reporting on data quality and the functioning of the systems through the following functionalities:

- Reporting and statistics on the business use of the systems, mainly used by stakeholders regarding developments in the JHA area;
- Reporting and review of data quality and operational accuracy[9], which will be used by the data owners at Member State level;
- Reporting on the functioning and the use of the systems, which will be mainly used by eu-LISA for analysis and development of the systems' performance and infrastructure.

CRRS will bring important changes to the data handling processes related to reporting, including automation. Review of data input processes, current data quality analysis methods and ways of dealing with data quality issues are the basis for a new approach. As the amount of data will grow both with the general increase in the use of the systems and with the launch of the new systems, the common approach can then be developed into the most appropriate automated solutions.

Data quality has to be ensured not only by technical means (e.g. appropriate database structures) but also by putting in place appropriate quality management processes and procedures at organisational level. The criteria for assessing data quality are therefore not only related to the completeness of a record but are part of a wider approach including data gathering, use, analysis and reporting. Addressing data quality issues will therefore require a detailed assessment of the business processes and procedures in place across Member States and relevant stakeholders.

[8] Central Repository for Reporting and Statistics.

[9] Specifically with regard to the shared Biometric Matching Service accuracy calculation tool.

To support the above, the draft Commission Implementing Decision, pursuant to Article 37(4) of Regulations (EU) 2019/817 and 2019/818 contains general requirements for data quality control mechanisms and procedures, as well as detailed specifications for data quality control and reporting. In particular it refers to the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in EES, VIS, ETIAS, SIS, ECRIS-TCN, sBMS[10] and CIR[11].

In addition, the draft Commission Implementing Decision contains a set of minimum data quality indicators, which will be applicable to input data, in accordance with the rules applied by each EU information system and interoperability component. These indicators are: completeness, accuracy, consistency, timeliness and uniqueness. The accuracy indicator for biometric data also specifically includes resolution.

With regard to access to information, key challenges have been identified already within the scope of the Smart Borders Pilot[12], the Report of the Working Group on ICT solutions for the MS with external land and sea borders[13] and the Progress Reports on the implementation of hotspots in Greece[14] and Italy[15]. These challenges include, among others, the following: wireless network coverage, especially in case of remote land and sea border crossing points and when operating inside trains and vessels; capturing of biometric data in non-optimal conditions; availability of mobile equipment and its interoperability in the context of joint operations. In addition, access to information is affected by other challenges, such as lack of common standards with regard to data representations (e.g. common ontologies) that are applicable to data used in the JHA area, siloed systems (to a significant extent addressed by interoperability), and lack of harmonised processes at Member State level.

[10] Shared Biometric Matching Service.

[11] Common Identity Repository.

[12] Technical Study on Smart Borders, Final Report (https://www.eulisa.europa.eu/Newsroom/News/Pages/Smart-Borders-Report-Publised-Today.aspx

[13] Entry/Exit System (EES) Working Group on ICT Solutions for External Borders (sea/land) Report.

[14] 15399/15.

[15] 15402/15.

### 1.2. Overall framework and key principles

The implementation of the new ecosystem for interoperability requires coordinated efforts from many actors. In this respect the guiding principles for implementation of the Roadmap will be:

- Complementarity;
- Consolidation;
- Stakeholder integration and synergies between the relevant actors.

eu-LISA, as the Agency responsible for the operational management of three large-scale systems already in operation and for the development and implementation of the new large-scale systems as well as the interoperability architecture, is an essential focal point for coordination of implementation of the Roadmap.  However, a broad range of stakeholders will need to be involved.

Considering the variety of the actions and the diversity of actors involved, the next steps towards the further development and implementation of the actions will need careful consideration and extensive interaction with stakeholders. The involvement of relevant decision-making bodies (e.g. Advisory Groups and Committees) will be an essential part of the process. Considering that this Roadmap is intended as a living document, further prioritisation of the actions and the definition of additional actions will be done in the process of implementation of this Roadmap, on the basis of continuous discussions with all relevant stakeholders.

In addition, in order to ensure effective and efficient implementation of the actions identified in the Roadmap and the fulfilment of the objectives set, appropriate resources will need to be allocated to each entity responsible for the implementation of the actions (this concerns both eu-LISA and other JHA agencies, as well as Member State authorities). To support this, a comprehensive resource plan, including possible funding sources, will have to be defined, discussed and agreed upon as part of further planning of this Roadmap.

Governance is needed to keep the implementation and application of actions according to this Roadmap present. The IXIM WP was established with the aim to ensure a comprehensive and cross-cutting overview on tasks and challenges of the revised JHA information architecture on Council side. The IXIM WP is therefore predestined as monitoring instance for this Roadmap.

## 2. Improving the quality of biometric and alphanumeric data

### 2.1. Review of the current situation

Biometric identification has significant potential; however, it is also one of the most complex technical challenges. eu-LISA provides this service to Member States through its Core Business Systems[16] (CBS) assuring quality and reliability. The main metric that describes the proper running of the biometric systems is the accuracy, which provides a measure of the correct decisions (e.g. correctly verified traveller) over the wrong decisions (e.g. wrong hit). Several factors influence biometric system accuracy (e.g. user interaction or environment) but one of the most relevant is the sample quality.

According to the vocabulary standard (ISO/IEC 2382-37:2017) within the ISO/IEC SC 37 – Biometrics, "quality" is defined as "a measure of the fitness of a biometric sample to accomplish or fulfil the biometric comparison decision. Quality is a measure of biometric utility". Taking into account this definition, it is possible to derive two types of quality:

a) Measure of the level of performance of a biometric matching software/service. This metric checks whether the biometric sample contains the characteristics that the biometric system expects and to what extent.

b) Measure of the easiness for a human eye (normally an expert) to identify an individual. In other words it measures how well the characteristics that make individuals different are present in the examined sample (e.g. minutiae in fingerprints or pose in faces).

[16] SIS II, VIS/BMS and Eurodac

Currently, the reference implementations and standardised algorithms related to biometric sample quality take into account both of these quality types. Regarding fingerprint quality, none of the existing eu-LISA CBS are currently providing NFIQ[17] version 2, which is the reference implementation of the *ISO/IEC 29794-4 Biometric sample quality -- Part 4: Finger image data: 2010*. This algorithm provides a score from 0 (worst) to 100 (best), taking into account several parameters which include the two types of quality mentioned above. However, an important development in this respect is that the NFIQ2 will be built into the sBMS by design. Thus, the standard will be used for each eu-LISA CBS (both existing and new systems), which will be connected to sBMS, once in operation.

Facial recognition is becoming increasingly relevant and improving substantially in terms of accuracy and usability. Yet, there is still no clear reference standard to measure face sample quality within a biometric matching system. In this direction, there are sets of best practices, requirements and recommendations to obtain face samples that allow for proper recognition of an individual, included in the following standards: *ICAO 9303* for Machine Readable Travel Documents and the *ISO/IEC 19794-5:2011 Biometric data interchange formats — Part 5: Face image data* (based mainly on the ICAO 9303). Both standards view quality as the second type described above, namely as the degree of easiness of inspection by the human eye. Following the cited standards, eu-LISA is developing a face quality algorithm for the sBMS based on both the ISO/IEC 19794-5: 2011 standard and a proprietary algorithm developed by the sBMS contractor (machine learning based). The sBMS will be in line with the requirements set in the Commission’s Implementing Decision (EU) 2019/329 for EES, requiring both the NFIQv2 and the ISO/IEC 19794-5: 2011 as the reference quality metrics for the EES.

With regard to alphanumeric data stored in the large-scale IT systems, the responsibility for data quality lies with the Member States. Until 2017, due to its restricted mandate, eu-LISA was only committed to providing monitoring capabilities and technical solutions to support Member States in improving the quality of the data inserted in the systems; however, no rules or procedures were implemented in the central systems to ensure data quality. In this respect, data quality was ensured through processes, procedures and rules (if any) in place within individual Member States.

[17] NIST Fingerprint Image Quality

Within the limited mandate of the Agency in this filed, a couple of initiatives were launched upon specific requests from Member States. Regular discussions and exchange of best practice take place within the Advisory Group meetings, and support is provided by eu-LISA when necessary. Given the importance of data quality, eu-LISA has also been organising regular trainings on the subject of data quality.

Data quality has long been recognised as an important issue in context of the central systems. An Action Plan on Data Quality was approved by the Working Party on Information Exchange and Data Protection (DAPIX) on 1 December 2016 in context of the fifth Action List of the revised Information Management Strategy. The Action plan formed the basis for actions on improving data quality included in the final report of the HLEG[18].

## 2.2. Description of the future status

The revised eu-LISA establishing regulation, the regulations on the new systems, and the Interoperability Regulation all address the issue of data quality from the regulatory standpoint. To complement those, the Commission's Implementing Decision on automated data quality control[19], which is currently being drafted by a relevant committee, lays down a broad range of requirements pertaining to data quality, such as:

- General requirements for data quality control mechanisms and procedures;
- Automated data quality control mechanism for data entered and stored in EES, VIS, ETIAS, SIS, sBMS and CIR;
- Procedures for governing the data quality control indicators, standards and mechanisms;

[18] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

[19] Draft Implementing Decision laying down the details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in the EES, VIS, ETIAS, SIS, the sBMS and the CIR, pursuant to Article 37(4) of Regulation (EU) 2019/817.

- Reports on automated data quality control mechanisms and procedures and common data quality indicators according to Article 37(4) of Regulation (EU) 2019/817;
- Annex Section 1: hard rules and soft rules for data to be entered in EES, VIS, ETIAS, SIS, the sBMS and the CIR;
- Annex Section 2: general considerations on the common data quality indicators and minimum quality standards for data to be entered in EES, VIS ETIAS, SIS, the sBMS and the CIR;
- Annex Section 3: Data Quality Classification;
- Annex Section 4: Data Quality Monitoring.

In addition, the draft Implementing Decision sets a number of data quality indicators applicable to all input data in accordance with the rules applied by each EU information system and interoperability component: completeness, accuracy, consistency, timeliness, uniqueness. These actions, when implemented, will address the data quality issues identified earlier to a significant extent.

Focusing on biometric data quality, eu-LISA is determined to the application of the best-known metrics published on the standards in order to guarantee transparency and interoperability. Therefore, eu-LISA will continue applying reference implementations such as the NFIQv2. In case of facial recognition, as there are still no reference metrics, eu-LISA will actively stay up to date regarding the subsequent ISO SC37 standards and study the application of future metrics.

The future will bring a wider range of biometric modalities in the areas of border control migration and security. Palm prints are already part of the SIS II recast, while other modalities, such as iris, are likely to become part of the technology landscape in the JHA domain along with significant improvements in technologies or the acceptability criteria. Factors such as touchless and less intrusive technologies will play an important role in the future. These developments need to be considered by Member States and EU Agencies in context of the evolution of relevant EU legislation and systems.

Biometric sample quality is highly relevant for accuracy but it has also relevance within the system security domain. In recent times, presentation attack[20] has come to be considered one of the crucial topics within the biometrics community as it has been proven in the past that biometric systems in general were not prepared against forgeries. This is the point where the biometric quality analysis plays an important role as part of the Presentation Attack Detection (PAD) techniques[21]. This Roadmap outlines a set of actions aimed at further improvement of both biometric and alphanumeric data quality.

[20] Presentation attack is the use of presentation attack instruments, such as photographs, masks, fake silicone fingerprints, in order to subvert a biometric system.

[21] When referring to presentation attacks, we implicitly include also morphing attacks. Reference standard for PAD is ISO/IEC 30107, in particular ISO/IEC 30107-3:2017 - Biometric presentation attack detection, Testing and reporting.

### 2.3. Overview of key stakeholders

Implementation of the actions aimed at improving the quality of biometric and alphanumeric data will require the involvement of a wide range of stakeholders. eu-LISA as the Agency responsible for the operation of the large-scale IT systems in the JHA area, is a key stakeholder when it comes to ensuring data quality. eu-LISA will therefore play an important role in the coordination of implementation of this Roadmap. From the biometric sample capture, the Member States are key actors in ensuring that the data capture process is performed in accordance with the EU legal basis and best practices. Several Directorates General of the European Commission should be involved. DG HOME should be engaged with the focus on policy aspects related to the improvement of alphanumeric data. DG CNECT should be engaged as a key stakeholder responsible for standardisation in the area of information and communication technologies. DG DIGIT, in particular Unit D2, should be involved due to their specific expertise with regard to interoperability of information systems and their work on data modelling to ensure data quality. Relevant JHA agencies (e.g. Europol and Frontex/EBCGA) should be involved in the implementation of specific actions, considering their role in defining measures at operational level. Relevant international stakeholders playing an important role in defining standards or requirements for alphanumeric data should also be involved where relevant (e.g. ICAO; IATA). Service providers developing means to control the entire biometric process, as well as optimising the biometric sample capture and therefore the sample quality. As mentioned above, standardisation committees, such as the ISO SC37 or the CEN WG18[22], make significant efforts to deliver high quality standards that can be applied by Member State authorities, eu-LISA, and other relevant JHA agencies.

[22] CEN is the European Committee for Standardization, an association that brings together the National Standardisation Bodies of 33 European countries. Biometric technologies are considered in the Working Group WG18 “Biometrics”, a part of the Technical Committee TC224 “Personal identification, electronic signature and cards and their related systems and operations”.

### 2.4. Improving the quality of biometric and alphanumeric data: Implementation[23]

| N0 | Objective | Action | Responsible Party(ies) | Stakeholders | Implementation timeline | Monitoring |
|---|---|---|---|---|---|---|
| **Focusing on biometric data** | | | | | | |
| **1.** | To ensure high biometric sample quality across all systems using biometric data. | Drawing up of shared good practices and definition of standard processes and workflows to ensure acquisition of high quality biometric data. | eu-LISA<br>Europol<br>Frontex/EBCGA | Member State authorities<br>EC DG JRC | 2021-2022 | IXIM WP |
| **2.** | To ensure high biometric sample quality across all systems using biometric data. | Adoption of good practices and standardised processes and workflows for biometric data acquisition by the relevant Member State authorities. | eu-LISA<br>Europol<br>Frontex/EBCGA | Member State authorities<br>EC DG JRC | 2022-2023 | IXIM WP |
| **3.** | To ensure high biometric sample quality across all systems using biometric data. | Drawing up of common staff trainings for the end users of biometric equipment for enrolment, identification and verification. | eu-LISA<br>Europol<br>Frontex/EBCGA<br>CEPOL | Member States authorities<br>EC DG JRC | 2022-2023 | IXIM WP |
| **4.** | To ensure that the quality of equipment used by the MS authorities and relevant EU agencies is sufficient to comply with the requirements of the central systems. | Campaigns for updating obsolete equipment for biometric data acquisition at Member States' level. | Member State authorities | eu-LISA<br>Europol<br>Frontex/EBCGA | Regular campaigns without a specific timeline | IXIM WP |

[23] Control points and reassessment will be set at the time of implementation.

| | | | | | | |
|---|---|---|---|---|---|---|
| **Focusing on alphanumeric data** | | | | | | |
| **5.** | To further develop the UMF into the standard message format for data exchange in the JHA area. | Interoperability Regulations define UMF as a standard that shall be used in the development of EES, ETIAS, the ESP, the CIR and the MID[24].<br>Currently UMF serves the purpose of data exchange for law enforcement purposes.<br>To ensure that UMF can be universally applied for data exchange in the JHA area, it needs to be further extended to include data categories and data fields used in border management and migration. | eu-LISA<br>Europol | Bundeskriminalamt (DE),<br>EC DG HOME,<br>Frontex/EBCGA,<br>Member State authorities,<br>Interpol.<br>EC DG DIGIT (D2) | 2021-2023 | IXIM WP |
| **6.** | To improve the knowledge and skills of the staff responsible for data input into the central systems. | Since 2017, eu-LISA has been organising training activities on data quality issues pertaining to the systems currently in place. Nevertheless, this effort needs to be continued and extended to cover the new systems and the components of the interoperability architecture.<br>As part of its training mandate, eu-LISA will continue the development and provision of relevant training events focusing on improving data quality to the staff of the Member States' authorities and JHA agencies. | eu-LISA<br>Frontex/EBCGA | JHA agencies,<br>Member State authorities. | Continuous | IXIM WP |

[24] Multiple Identity Detector.

| | | | | | | |
|---|---|---|---|---|---|---|
| **7.** | To improve the quality of data provided through manual input. | Manual data entry is one of the key challenges related to the quality of alphanumerical data entered into the central systems. To address this, development, endorsement and implementation of standardised solutions is necessary. Those include:<br>• Adoption of standardised transliteration schemes and/or standardised automated solutions for transliteration across Member States' authorities.<br>• Application of standards to certain data fields;<br>Development of common approaches to data input/validation rules within interfaces, standard architectures and/or devices.<br>With regard to manual input of data, ETIAS is a special case because data input will be performed by the traveller into the central system. Possible data quality issues should be prevented or limited by reinforcing automated data quality control mechanisms in the central system, as well as communication tools for communication with the traveller via the public website (e.g. FAQs) and/or traveller helpdesk. | eu-LISA | JHA agencies, Member State authorities.<br>EC DG DIGIT (D2) | 2021-2023 | IXIM WP |

| | | | | | | |
|---|---|---|---|---|---|---|
| **8.** | To improve the quality of data in order to ensure high quality data analytics. | The Common Repository for Reporting and Statistics will be used in a number of processes as defined in the relevant regulations. One of such processes is the development of risk indicators for automated processing of applications in ETIAS and potentially in the VIS.<br>Screening solutions based on artificial intelligence will be used in order to ensure efficient and effective automated screening of applications. However, high performance of solutions relying on artificial intelligence depends on high quality of input data.<br>In this context, development and deployment of solutions for data quality evaluation and control will be necessary, including on the level of Member States. | eu-LISA | Frontex/EBCGA, Member State authorities. | 2021-2023 | IXIM WP |

## **3. Creation of a reference catalogue of devices and solutions for the acquisition of data and access to information**

### 3.1. Review of the current situation

Procurement of technological solutions and equipment necessary for the implementation of the EU legislative acts in the areas of border management, migration and internal security on side of the end users is performed at Member State level. Procurement of such solutions is done taking into account the requirements defined in the relevant Implementing Acts; however, procurement is not coordinated across Member States and no specific guidance regarding the performance of solutions and devices and compliance with the set requirements, is provided centrally. This may potentially have deleterious effect on the quality of data submitted to the central systems.

With full respect of the Member States' autonomy, including the applicable regulatory framework, the current exercise is not intended to change the procurement procedures applied by the Member States. The general belief is, however, that the acquisition of devices for the collection of high-quality data, capable of supporting all associated operational business processes, could be supported on a central level by creating a reference catalogue of verified equipment/solutions that would

- enable the operational business process as intended for the specific end-user, and
- ensure the data quality required for the global functioning of the respective European large-scale IT systems.

Some initial work in this direction is already being done by the Member States and EU agencies. For the time being, the evaluation results of any tests, field trials, benchmarking exercises, or procurement procedures and/or technical reports made either by agencies or the Member States are being documented and made available for future reference.

Important work in this direction has already been initiated, in particular by Frontex/EBCGA in collaboration with experts from the Member States, the Commission and eu-LISA. The work focused on the development of technical standards for border control equipment that meet requirements set by the central Entry/Exit System based on a range of operational scenarios. These activities performed by Frontex/EBCGA will lead to the establishment of an Innovation Lab, which will embed activities related to the testing and accreditation of the performance of border control equipment[25]. Close coordination of activities between eu-LISA and Frontex/EBCGA concerning testing and conformity assessment of relevant equipment would therefore be essential to maximise the benefits and avoid overlaps in carrying out these activities.

### 3.2. Description of the future status

This conceptual proposal of eu-LISA would entail three general phases, which would be sequentially introduced and later coexist after their implementation. An overview of the three phases is provided below.

**Phase 1:** The first phase will include the definition and adoption of a set of technical and user requirements that equipment needs to meet in order to be included in the catalogue. These requirements will be defined per business area (e.g. visa issuance, border management, migration management and law enforcement) and based on the work already done by the Advisory Groups, eu-LISA working groups (e.g. Biometric WG), Frontex/EBCGA and the respective Member State authorities. Where relevant, these requirements shall include the criteria already set in relevant legal acts (e.g. Implementing Acts). One of the key objectives is to ensure compliance of devices with the business processes on the level of Member States and related to the central systems (i.e. EES, ETIAS, VIS, etc.)

[25] Regulation (EU) 2019/1896 (Frontex/EBCGA Regulation) calls for the Agency to establish technical standards for equipment in the area of border control. The work on technical standards is extended to testing and conformity assessment of devices to be included in the technical equipment pool.

**Phase 2:** The second phase will entail the collection of data on equipment or devices that are already either in use, have been tested, or otherwise proven to be fit for purpose by the EU agencies or Member State authorities. The results of this exercise will serve as a baseline for the initial reference catalogue of solutions and devices.

**Phase 3:** The third phase would be a long-term objective for the European JHA community targeting to professionalise the process of conformity assessment, as well as mitigating the financial and resource burden that such a process creates over time.

The third phase would build upon the data collected in the first two phases to develop a conformity assessment process, which would be implemented within the scope of a testing lab established e.g. at eu-LISA, in order to provide facilities to the Member States to test conformance of equipment (e.g. biometric devices, mobile devices used at BCPs) as well as solutions for biometric identification/matching. The testing lab could be set up in two stages:

- First, a virtual testing facility would be set up to allow for independent testing of solutions, against the associated operational business processes provided by commercial vendors;
- Second, a physical testing environment could be set up in order to enable the testing of equipment.

In order to support the testing lab, in particular with regard to testing of devices and solutions, a dedicated Expert Network could be set-up on a permanent basis. The expert network would include technical and business experts from relevant MS authorities, JHA agencies, in particular Frontex/EBCGA focusing on the testing of border control equipment, and the Joint Research Centre (JRC), and would facilitate the exchange of experience, adoption of standards and sharing of good practices.

Different modalities are possible for conformity assessment of relevant equipment. One modality is fee-based, in which case vendors of hardware and software solutions would pay for the certification of equipment. This modality would allow to at least partially cover the costs of establishing and maintaining the testing lab. An alternative option would be to implement the lab using EU funding, in which case the lab would provide independent performance validation services for equipment (both HW and SW) procured by the Member States.

Depending on the preferred modality and other considerations, conformity assessment of equipment for the use in context of the central systems could be either voluntary or mandatory. In case such conformity assessment would be considered mandatory, eu-LISA would commit to take the devices included in the reference catalogue into account in future updates to the systems, re-test them against changes and cooperate with the manufacturers regarding the provision of necessary firmware updates to the respective devices in preparation of system-changes. When developing the conformity assessment processes, relevant standards and regulations setting criteria for equipment to be assessed will be applied, along with relevant standards for performance testing of relevant equipment/systems (e.g. ISO/IEC 19795 Biometric Performance Testing and Reporting). Last, but not least, relevant standards on quality management will be applied (e.g. ISO 9001 family) to ensure consistent quality of conformance testing and trust of both suppliers and end-users.

The reference catalogue and testing lab for conformity assessment will not perform certification of devices/systems/technologies with regard to cybersecurity in order to avoid possible overlap with the work performed in this domain by ENISA[26]. It is important to stress that the reference catalogue should be public and available for reference for Member State authorities, EU agencies and private sector vendors.

[26] European Union Agency for Cyber Security.

### 3.3. Overview of key stakeholders

Implementation of the actions aimed at establishing a reference catalogue and a certification system for equipment and solutions will require involvement of a range of stakeholders. eu-LISA as the agency responsible for the operation of the large-scale IT systems in the JHA area, is a key stakeholder when it comes to ensuring data quality. eu-LISA will therefore play an important role in the coordination of implementation of this Roadmap. Close coordination with Frontex/EBCGA concerning testing and conformity assessment of equipment will be necessary. The eu-LISA Management Board and eu-LISA Advisory Groups; the European Commission DG HOME for consultation on policy aspects of activities related to evaluation and certification of devices and equipment; DG JRC specifically with regard to their expertise in testing of biometric devices and algorithms; and the JHA agencies. DG CNECT should be involved to ensure coherence with the EU Cybersecurity Act[27] and the Certification Scheme included therein. Effective involvement of JHA agencies, such as Europol, EASO, CEPOL and FRA, will be an essential in this effort, considering their relevant expertise. ENISA should be involved on questions related to cybersecurity certification. Private sector partners will also be considered in the implementation of specific actions where relevant.

[27] OJ L 151, 7.6.2019, p. 15.

### 3.4. Creation of a reference catalogue of devices and solutions for the acquisition of data and access to information: Implementation

| N0 | Objective | Action | Responsible Party | Stakeholders | Implementation timetable | Monitoring |
|---|---|---|---|---|---|---|
| **1.** | To establish a well-structured and coordinated approach for the development of a reference catalogue of devices and solutions for the acquisition of data and access to information. | Definition and adoption of a set of technical and user requirements that equipment needs to meet in order to be included in the catalogue. | eu-LISA<br>Frontex/EBCGA | Europol<br>Member State authorities<br>EC DG HOME and DG JRC | 2021 | IXIM WP |
| **2.** | To establish a well-structured and coordinated approach for the development of a reference catalogue of devices and solutions for the acquisition of data and access to information. | Collection of data on equipment or devices that are already either in use, have been tested, or otherwise proven to be fit for purpose by the EU agencies or Member State authorities. | eu-LISA<br>Frontex/EBCGA | Europol<br>Member State authorities<br>EC DG HOME and DG JRC | 2021-2022 | IXIM WP |
| **3.** | To establish a well-structured and coordinated approach for the development of a reference catalogue of devices and solutions for the acquisition of data and access to information. | Establishing a testing lab for testing of technical equipment and solutions used for the acquisition of data and access to information (including testing of alphanumeric / biometric matching algorithms). | eu-LISA<br>Frontex/EBCGA | Member State authorities<br>EC DG HOME and DG JRC | 2022-2023 | IXIM WP |

| | | | | | | |
|---|---|---|---|---|---|---|
| **4.** | Enable testing of devices and solutions in real-life environments and business processes. | Timely re-engineering of business processes related to the new systems and interoperability components on the level of Member States to enable testing of equipment and solutions in real-life environments and business processes. | Member States | eu-LISA<br>Frontex/EBCGA<br>EC DG HOME | 2021-2022 | IXIM WP |

## 4. Strengthening cyber security

### 4.1. Review of the current situation

eu-LISA’s current security framework ensures that security is transversally addressed in all steps of an IT system from the inception to the design, including the development, implementation, the operation and the maintenance phase in compliance with the respective requirements under the legal base of each CBS.

In this approach, the Agency has identified and continues to work on a list of actions to develop the core elements of the security management framework. In particular, the following actions are currently addressed in order to build and maintain a high level security posture of each CBS under the Agency’s mandate.

1) **Tools in place**

   a. The Agency Security Framework, elaborating on security policies, standards and guidelines.

   b. Information Security Management System (ISMS), including the Security Management, the Security Operations and Response, and the Security Assurance functions according to the Plan-Do-Check-Act (PDCA) cycle.

   c. Security dossiers per CBS, including Security Risk Assessment, Security Plan, Business Continuity Plan and other relevant other security documentation concerning the way security requirements are addressed in system implementation.

   d. Specific Security and Business Continuity recommendations prior to the final implementation of EES and ETIAS, encouraging a common approach on the security design and management of the concerned systems by Member States.

   e. Implementing Acts on model security and business continuity plans as well as common security incident cooperation procedures to support a common approach on security management by eu-LISA and Member States.

### 2) Ongoing actions

All of the actions described above undergo a continuous review and an improvement cycle addressing new points of interest raised through the CBS lifecycle. The following developments are ongoing:

a. The Agency Security Framework is currently under review to address new concerns raised in the domain through interoperability requirements and common services. In the meantime the current ISMS framework and security architecture are undergoing compliance checks from internal and external stakeholders through relevant assessment activities and audits.

b. The ISMS currently in place supports the security management in the ITSM cycle. The improvement of the Security Operations and Response, and the Security Assurance functions is being planned through capability improvements.

c. Continuous review and approval process following a two-year review cycle for each large-scale IT system endorsed by the eu-LISA Management Board.

d. Recommendations for both EES and ETIAS already approved by the EES-ETIAS Advisory Group and communicated to Member States.

e. Implementing Acts are currently under preparation by DG HOME-led activities under the Interoperability and ETIAS framework.

### 3) Operational/governance bodies responsible for the actions

Each of the actions follows a similar governance model where various stakeholders are involved in the preparation and approval process. In particular:

For actions 2a and 2c - eu-LISA security function is responsible for the preparation, eu-LISA Management Board is responsible for the endorsement;

For action 2b - eu-LISA security function is responsible for the preparation;

For action 2d - eu-LISA security function is responsible for the preparation, the Advisory Groups are responsible for the review and endorsement;

For action 2e - DG HOME is responsible for the preparation of the Implementing Acts.

### 4.2. Description of the future status

With EES and ETIAS, passenger carriers will have access to these two systems for verification purposes: through a web interface in the case of the EES and a carrier gateway in the case of ETIAS. Similarly, ETIAS will be accessible through a web-based service. Exposure of the systems to the internet, even if by way of a gateway, will add additional security risks. As the Interoperability Regulations envisage reusable interoperable components between various CBSs they broaden the security design considerations.

In order to address these points and improve the cybersecurity posture of the systems managed by eu-LISA, future drivers should enforce cybersecurity both in terms of protection, resilience and response but also in terms of collaboration and standardisation.

I. **Safeguarding the integrity, security and resilience of infrastructures, networks and services** where the protection of core infrastructure is addressed to allow resilience of services in terms of availability and integrity;

II. **Strengthening the ability to prevent, discourage, deter and respond to malicious cyber activities** where operational security in terms of the security monitoring, incident response, threat intelligence and vulnerability management capability is enhanced;

III. **Strategic, operational and technical cooperation between the European and national level** addressing collaboration aspects of the common effort to deal with shared cybersecurity risks;

IV. **Public-private partnership and collaboration** to improve the cooperation and trust level in security market products, and supporting research and innovation while creating networks of cybersecurity communities.

Each of these drivers is implemented through a set of actions that will improve the overall cybersecurity posture in terms of prevention, detection, response and recovery. All actions, in turn, need to be aligned with the Cybersecurity Act, implemented in close coordination with ENISA, in particular taking into account its work on cybersecurity certification.

### 4.3. Overview of key stakeholders

Implementation of the actions aimed at improving cyber security will require the involvement of a range of stakeholders. eu-LISA as the Agency responsible for the operation of the large-scale IT systems in the JHA area, is a key stakeholder when it comes to ensuring data quality. eu-LISA will therefore play an important role in the coordination of implementation of this Roadmap. When further defining and planning the implementation of the actions to augment cybersecurity in the JHA area, activities will need to be coordinated closely with DG CNECT as the DG responsible for cybersecurity policy and ENISA, as the EU cybersecurity agency. Member States authorities shall also be involved through the already existing structures, such as the eu-LISA Management Board, eu-LISA Advisory Groups and the eu-LISA Security Officers Network. Where relevant and necessary, other stakeholders should be involved, including the European Commission DG HOME, the Justice and Home Affairs agencies (i.e. Frontex/EBCGA, Europol, Eurojust, EASO), the European Union Agency for Cyber Security (ENISA) as well as the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU). Private sector partners will also be considered in the implementation of specific actions where relevant.

### 4.4. Strengthening cyber security: Implementation

| N0 | Objective | Action | Responsible Party | Stakeholders | Implementation timetable | Monitoring |
|---|---|---|---|---|---|---|
| **1.** | Safeguarding the integrity, security and resilience of infrastructures, networks and services | Improve resilience and protection of services and infrastructure in terms of enhanced boundary protection, improved resilience of infrastructure through modern compute technologies, improved web service and cloud security and token-based access control mechanisms | eu-LISA,<br>ENISA,<br>EC DG CNECT,<br>EC DG HOME. | Member State authorities,<br>Frontex/EBCGA,<br>Europol,<br>Eurojust,<br>CERT-EU,<br>EC DG HOME. | 2021-2023 | IXIM WP |
| **2.** | Safeguarding the integrity, security and resilience of infrastructures, networks and services | Develop a high common level of security of network and information systems, through the development of standard security architecture models and artefacts, the adoption of common security control frameworks (European Commission Security Policy Framework, NIST 800-53, ISO 27002), the promotion of identities as the new security perimeter enforcing zero trust and continuous validation concepts, incorporating security by default and security by design principles, enhancing the confidentiality of communication infrastructure leveraging standardised encryption mechanisms | eu-LISA,<br>ENISA,<br>EC DG CNECT,<br>EC DG HOME. | Member State authorities,<br>Frontex/EBCGA,<br>Europol,<br>Eurojust,<br>CERT-EU,<br>EC DG HOME. | 2021-2023 | IXIM WP |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| **3.** | Strengthening the ability to prevent, discourage, deter and respond to malicious cyber activities | Enhance Security Operation Centre (SOC) capacity by applying common operational patterns, developing common standard ways to measure and accredit SOC performance. | eu-LISA,<br>ENISA,<br>EC DG CNECT,<br>CERT-EU | Member State authorities,<br>Frontex/EBCGA,<br>Europol,<br>Eurojust,<br>EC DG HOME. | 2022 | IXIM WP |
| **4.** | Strengthening the ability to prevent, discourage, deter and respond to malicious cyber activities | Enhance security incident detection and response capabilities, by developing common standards on incident response through information sharing on situational awareness, improving security monitoring capability, leveraging real time audit and security testing activities (pen testing), improving cyber threat intelligence through common sources (MISP) | eu-LISA,<br>ENISA,<br>EC DG CNECT,<br>CERT-EU | Member State authorities,<br>Frontex/EBCGA,<br>Europol,<br>Eurojust,<br>EC DG HOME. | 2022 | IXIM WP |
| **5.** | Strategic, operational and technical cooperation between European and national level | Develop a common collaborative approach on risk management through the use of common cybersecurity standards and the establishment of common security artefacts | eu-LISA,<br>ENISA,<br>EC DG CNECT,<br>CERT-EU | Member State authorities,<br>Frontex/EBCGA,<br>Europol,<br>Eurojust,<br>EC DG HOME. | 2022 | IXIM WP |
| **6.** | Strategic, operational and technical cooperation between European and national levels | Promote technical cooperation through sharing information on threat intelligence and situational awareness, leveraging the operation of collaborative supporting platforms (Cooperation Platform) | eu-LISA<br>CEPOL<br>CERT-EU<br>ENISA | Member State authorities,<br>Frontex/EBCGA,<br>Europol,<br>Eurojust,<br>EC DG CNECT,<br>EC DG HOME. | 2022 | IXIM WP |

| | | | | | | |
|---|---|---|---|---|---|---|
| **7.** | Strategic, operational and technical cooperation between European level and Member States | Develop cybersecurity awareness and training activities | eu-LISA<br>CEPOL<br>CERT-EU<br>ENISA | Member State authorities, Frontex/EBCGA, Europol, Eurojust, EC DG CONECT, EC DG HOME. | 2022 | IXIM WP |
| **8.** | Public-private partnership and collaboration | Promote EU agencies´ participation in networks of cybersecurity communities by developing research and innovation in the cybersecurity domain, encouraging a high common level of cybersecurity maturity among stakeholders | ENISA | eu-LISA, Frontex/EBCGA, Europol, Eurojust, EC DG CNECT. | 2021 | IXIM WP |
| **9.** | Public-private partnership and collaboration | Build trust on cybersecurity products by defining minimum security requirements of IT products guaranteeing a minimum level of cybersecurity, leveraging cybersecurity certification schemes of IT products, services and processes | ENISA | eu-LISA, Frontex/EBCGA, Europol, Eurojust, EC DG CNECT. | 2021 | IXIM WP |

## 5. Way forward

After endorsement of the Roadmap by the IXIM WP, it will be further broken down into specific activities with respective timeline and owners. The overall coordination of the implementation of the Roadmap will be carried out by eu-LISA in close collaboration with the Member States, Commission and the relevant JHA agencies. Progress with implementation will be regularly reported to the IXIM WP and when relevant to COSI and SCIFA.

At the same time, considering that some of the activities included in the Roadmap have transversal nature, the IXIM WP will keep the other relevant Working Parties in the Council, such as the Visa WP, COPEN WP, HWP on Cyber Issues and the relevant Commission services (DG HOME, DG JUST, DG JRC) informed on the progress with the implementation of the Roadmap. The operational coordination and reporting on the implementation of the Roadmap will be performed by eu-LISA.

Furthermore, possible synergies with the initiative for establishment of the EU Innovation Hub in the development and implementation of specific actions will be considered, in order to leverage the already existing network and resources. Considering that the roadmap will be a living document, further development, updating and revision of the roadmap should be carried out in coordination with relevant stakeholders, such as the Council, the Commission, the JHA agencies, under the auspices of the IXIM WP.

The implementation of specific actions will be performed by the parties defined as responsible for the implementation of each action, and will be monitored by the relevant governance body and the IXIM WP. Where additional resources (human or financial) are necessary for the implementation of the roadmap, those should be evaluated, and appropriate sources of funding should be identified (e.g. Integrated Border Management Fund, Asylum and Migration Fund, Internal Security Fund, Member States' own resources etc.)

## Annex I: Overview of actions

This overview of actions is based on the responses provided by Member State authorities to the questionnaire circulated within the IXIM WP, as well as Eurodac, VIS, SIS, EES-ETIAS and ECRIS-TCN Advisory Groups in September 2020. This overview is by no means comprehensive and includes only a snapshot of the initiatives in place. A more comprehensive analysis of initiatives in place may be carried out within the scope of the implementation of the Roadmap.

| N0 | Action | Description of action |
|---|---|---|
| **1.** | Improvement of the quality of biometric data by way of a new ABIS/AFIS system. | Several Member States indicated that an ABIS/AFIS system had either been implemented or was being procured. The new ABIS/AFIS includes automatic quality control across a range of biometric data acquisition areas (national systems, Eurodac, VIS, SIS). |
| **2.** | Improvement of the quality of biometric data by way of new hardware and software | Several Member States indicated that they had procured or were in the process of procuring new hardware and software for biometric enrolment, with the possibility of controlling quality at the hardware and software levels, also according to the NFIQ2. Use of Multi Spectrum Imaging scanners to improve fingerprint quality. |
| **3.** | Regular training of end users | Several Member States indicated that regular training of end users was an essential component in the overall effort to ensure quality of biometric and alphanumeric data. |
| **4.** | Provision of User Software Kits for Member State authorities by eu-LISA | eu-LISA provided User Software Kits (USK) for biometric quality assessment in the context of the VIS. eu-LISA has also finalised procurement of the User Software Kits for the use by the Member States in the context of the EES and sBMS. Testing of the USK planned in Q4 2020 with a group of Member States. On the basis of the results of the test, configuration of the sBMS USK will be defined for all MS. |
| **5.** | Definition of business rules/logical restrictions for verification of alphanumeric data inputs | Several Member States indicated that they had put in place business rules to verify alphanumeric data inputs into the national and central systems. |
| **6.** | Checks against national databases | Several Member States indicated that they had put in place processes for verification of data inputs against national databases/registries (e.g. population register), or connection to a unique personal identification number. |

| | | |
|---|---|---|
| **7.** | Comprehensive approaches to ensure data quality | A few Member States indicated the existence of comprehensive approaches to data quality management at national level, with a defined governance structure and coordination mechanisms in place. These also include the systematic exchange of information between authorities in cases where mistakes in registered data are identified. |
| **8.** | Improving access to data | Several Member States indicated that there were actions in place to improve access to data. Those include development and implementation of data warehouse solutions; development of national communications infrastructure; integration with other national systems; procurement/development of mobile units and software for border checks. |
| **9.** | Biometric Working Group established by eu-LISA under the umbrella of the EES-ETIAS Advisory Group | The Biometric WG (BWG) has been established in the context of the interoperability regulation and functions as a platform for exchange of information between stakeholders on the challenges and best practices, with the aim of formulating a set of best practices and recommendations in the area of biometric identification technologies to be used by the Member States. |
| **10.** | Technical Expert Groups for the development of technical standards established by Frontex/EBCGA | Frontex/EBCGA set up two Technical Expert Groups for the development of technical standards for equipment that for some equipment deals with the capture of biometric data: TEG on EES equipment and TEG on Document Inspection Equipment. The TEG are made of MS experts, Agency experts, JRC experts, and in the case of the TEG on EES equipment, experts for eu-LISA. The outcome of the work of the TEG on EES equipment has been shared with the AG EES-ETIAS. These two groups focus on defining technical standards for border control equipment, but not the standard for the quality of the biometric data to be used by systems behind the equipment |
| **11.** | Regular data quality efforts based on data quality reports produced by eu-LISA. | Several Member States indicated that they conduct data quality improvement activities on the basis of data quality reports provided by eu-LISA on a regular basis. |
| **12.** | Travel document authenticity checks. | Two Member States indicated the existence of initiatives at national level aimed at improving the quality of travel document data provided into the national and central systems by way of authenticity checks. |

|  |  |  |
|---|---|---|
| **13.** | UMF3Plus project focusing on further development of the Universal Message Format. | UMF3Plus project aimed at supporting work on the new versions of Universal Message Format (UMF) as the EU data exchange format for law enforcement and the transition to the permanent governance structure, and at supporting the integration of QUEST, SIENA and DATALOADERS (automated uploading & self-data management) in the national systems. The use of UMF results in the improved quality of the data exchanged by removing technical and business ambiguities and enabling the information to become well structured and with consistent formats. |
| **14.** | Europol activities focusing on secure communications | In 2020, at the request of COSI, Europol carried out an assessment of existing solutions, operational requirements and possible gaps in secure communications.<br>Europol also maintains the Virtual Command Post, which is a collaboration solution that leverages real time multi-platform (iOS and Android) communication during operations and emergency responses. The solution enables law enforcement officers in the field to communicate with each other and with Europol in a timely and secure manner. |