Council of the European Union

Brussels, 29 January 2019
(OR. en)

5574/19

LIMITE

DAPIX 16
ENFOCUSTOM 16
COSI 4
ENFOPOL 20
FRONT 19
SIRIS 14
JAI 47

NOTE

From:	Commission services
To:	Delegations
No. prev. doc.:	15142/18
Subject:	Assessment report of practitioners - Interoperability of security and border management systems with customs systems

Delegations will find in annex an 'Assessment report of practitioners' from the Commission services concerning the Interoperability of security and border management systems with customs systems.

ANNEX

Interoperability of security and border management systems with customs systems

Assessment report of the practitioners

Legal Notice

The final report by the high-level expert group on information systems and interoperability, set up under Commission Decision C/2016/3780 of 17 June 2016, invited and recommended the Commission to organise an expert meeting with security, border management and customs experts on the options of promoting interoperability across their respective systems.

The opinions and recommendations expressed in this document are those of this expert group and do not necessarily represent the views of the European Commission.

1. Background

This paper assesses several aspects of potential interoperability of security and border IT management systems with customs' IT systems.

In May 2016, the Commission set up a high-level expert group ('HLEG') on information systems and interoperability.[1] The HLEG, in its final report of May 2017[2], highlighted among others the potential added-value of interoperability between the customs and Justice and Home Affairs (JHA) systems. The final report recognised that customs authorities are also a crucial actor in the multi-agency cooperation at the external borders. They have various systems and databases that contain data on movements of goods, identification of economic operators and risk-related information that can be used to reinforce internal security. The HLEG group considered it necessary to create synergies and convergence between information systems and their corresponding infrastructures for both EU border management and security and for customs operations.

[1] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435
[2] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

The final report invited and recommended the Commission to organise an expert meeting with security, border management and customs experts on the options of promoting interoperability across their respective systems. The report recommended that the experts should consider the technical, operational and legal feasibility of establishing interoperability across the relevant systems.

The Commission was also invited to launch a feasibility study to explore further the technical, operational and legal aspects of interoperability with customs systems.

In its conclusions of 14 June 2017[3], the Council endorsed the HLEG recommendations and invited the Commission to "continue to develop the import control system and undertake a feasibility study to further explore the technical, operational and legal aspects of interoperability of the security and border management systems with customs systems, and present its findings for discussion by the Council by the end of 2018".

The need for improvement of interagency cooperation and information-sharing between customs and other authorities, in particular other law enforcement and security agencies at the national and EU level is also one of the core principles and objectives of the EU customs risk management strategy and action plan endorsed by the Council in year 2014.[4]

Coordination of different actors involved in border management is also one of the objectives of the Commission's work on the Governance of the Customs Union[5] aiming to implement the European Agenda on Security and to an effective and genuine Security Union.

[3] http://data.consilium.europa.eu/doc/document/st-10151-2017-init/en/pdf
[4] COM(2014) 527 final, 21.8.2014
[5] Communication on Developing the EU Customs Union and Its Governance COM(2016) 813 final 21.12.2016

The Council, in its conclusions on developing the EU Customs Union and its governance[6], invited the Commission and the Member States to "*improve the coordination and the cooperation of customs with other law enforcement authorities and other agencies, particularly those involved in border management, and develop possible synergies and co-operation models, such as with Europol and European Border and Coast Guard Agency (Frontex), with the aim of further incorporating customs priorities, including, where possible, via the interoperability of their IT systems*".

2. Objective of interoperability between customs and JHA information systems

EU information systems for security, border and migration management in the JHA area support controls of **persons at external borders or within the EU territory.** They are aimed at ensuring effective border and migration management and at preserving a high level of internal security within the EU. Information systems in the customs domain collect and contain information on **goods** crossing the EU external borders, including on economic operators and persons involved in offences linked to security risks. The customs systems support customs authorities in performing their risk-based controls at the external borders, which are, among others, also aimed at detecting and preventing the trafficking of goods posing security or safety risks. Currently, customs and JHA information systems are not interoperable. This leads to blind spots at both sides.

By promoting interoperability between the centralised customs and JHA systems, the aim is to enable sharing information in a systematic and automated way and in real-time that could help support competent authorities with the information they need.

The objective of interoperability between customs and JHA systems is thus to contribute eliminating blind spots in order to help customs and other law enforcement authorities improving detection and prevention of security and safety risks linked with goods and persons moving across external borders.

[6] Standing Committee on Operational Cooperation on Internal Security (COSI) Document 7585/1/17 REV 1

3. Mandate of the practitioners' project group

As a first step, the Commission services, in line with the recommendations of the HLEG final report and the two Council conclusions mentioned above, set up an expert group with practitioners bringing together relevant operational knowledge and experiences on security, border management and customs operations.

The mandate of the group was to map the different customs and JHA systems in the area of security, border and migration management and to analyse the data and information for which compatibility may exist. The aim was to identify - through practical scenarios - the information, processes and systems for which interoperability could enhance external border management and/or internal security. The work of the expert group at this first stage was exclusively focused on identifying potential added-value of cross-checking relevant goods and persons' data or information without looking into technical, operational or legal aspects.

The group met twice (4/5 October and 14/15 November 2018). This paper summarises the main conclusions of their work. In the annex, these conclusions are supported by some concrete examples/scenarios where the practitioners identified potential added-value of interoperability.

In a second phase, the Commission intends to use these conclusions to define the scope of a feasibility study to explore further any technical, operational or legal aspects, including potential hurdles, problems and restrictions as - among others - data protection implications.

4. Scoping of the interoperability between customs and JHA systems

The starting point of the scoping exercise by the practitioners[7] was to establish a common view and understanding of what 'interoperability' in this specific context means.

Building on the way interoperability was addressed in the Communication on Stronger and Smarter Borders[8] ("the ability of information systems to exchange data and to enable the sharing of information"), the practitioners considered that not all the different dimensions on interoperability defined in that Communication were applicable between customs and JHA Systems. The dimension that is likely to lead to operational results according to the practitioners is the one where it is defined as "*interconnectivity of information systems where data registered in one system will automatically be consulted by another system on a real-time basis*". In this context, provision of access by competent authorities to the relevant information stored in the system of another authority for further human intervention and decision making would only happen following an automated process which would result in the 'match' of comparable data/information stored in two or more systems.

Under this scope, interoperability between customs and JHA systems could allow the identification and real-time tracking of goods received by persons or economic operators posing security or safety risks. In practical terms, the aim is to help ensuring effective identification by the authorities of risky movements of goods across the EU borders.

This approach differs from, and falls out of the remit of the interoperability package inside the JHA environment that is currently under discussion in the Council, which goes beyond automated real-time cross matching of data. Moreover, it also differs from potential case-by-case investigative queries from law enforcement authorities in the historic repository of customs systems collecting data on entry, import, transit or export of goods, which is not a real-time cross matching of data. From an investigative point of view this access to data could make sense, but this should be rather subject to a policy discussion.

---

7 The meetings gathered among others staff from the relevant Commission services and agencies (Europol, Frontex) together with customs officials from several member states, police and border enforcement.

8 Communication on Stronger and Smarter Information Systems for Borders and Security COM(2016) 205 final 06.04.2016

In this sense the scope of interoperability is also distinct from other methods of data sharing and data exploitation, such as data mining. It is acknowledged that several parallel initiatives are ongoing on data mining, or other data and information sharing arrangements between various authorities at national and EU level.

Finally, the scoping exercise by the practitioners was to analyse the EU's different information systems in the JHA and customs domain that collect and store information **in a centralised way** in line with the established principles of interoperability initiative for border management and security.

5. Analysis of the information systems

5.1. Customs systems

Customs authorities need to put in place measures in order to ensure the security and safety of the Union and its residents, where appropriate in close cooperation with other authorities according to Article 3 of the Union Customs Code (UCC). For customs, the focus is on supply chain security, and detection and prevention of serious crimes and terrorism associated with transnational cross border movement of goods, a task of multi-agency concern. Supply chains have a global reach and can provide direct material support, financing and opportunities (transport, infrastructure) for terrorist and criminal acts. The broad range of risks includes dangerous goods such as explosives, drugs and their precursors, firearms and CBRN and unfair and illegal trade in a wide range of goods e.g. counterfeit.

For the Customs Union, the systematic common risk-based customs controls at the external border based is a critical achievement. The EU Common Risk Management Framework (CRMF) allows for the sharing of risk information and intelligence, and enables customs controls based on security risk assessments using common risk indicators. Customs authorities gather in this way many relevant data: details of all movements of goods by different transport means are electronically declared to the import control system (ICS) already from 2011 onwards. These details are available prior to their arrival from third countries at the EU's external borders. The current ICS is however a decentralised system: data are declared in the different member states and not stored in or communicated to a centralised database.

The starting point (opportunity) for interoperability is the development of a centralised EU Advance Cargo Information System (current working name 'ICS2' and hereupon referred as ICS2) planned to replace the current ICS from early 2021 on[9]. It is a completely new generation system for collection of electronic advance cargo information of goods coming to or through the EU customs territory. Advance data is communicated pre-loading/pre-arrival to EU external borders and will be transmitted in the future by additional actors in the goods supply chain (logistic operators, express couriers, postal operators as well as carriers). Conceptually, the advance cargo information system can be compared with the PNR requirement in the JHA area (PNR covers all passengers; ICS2 will cover all goods). This new system will cover all goods intended to enter or pass through the EU customs territory (including transit, transhipment, import). It is estimated to cover more than 300 million cargo shipments (sea, land and air) and between 650 million and 1 billion postal and express courier items (excluding letters) per year. The system will be used by customs authorities to assess security and safety risks of cargo destined to enter the EU territory prior to its arrival at the external border.

This advance cargo information is contained in the electronic Entry Summary Declaration (ENS) and covers the following data categories that are stored in a common repository: data on parties (names, addresses, contacts of private or legal persons involved in sending, selling, transporting, logistics, receiving, buying goods), data on commodities and packing units, data on cargo routing and times and data on means of transport / vehicles.

The risk management and assessment itself is empowered by an electronic filtering of advance cargo transactions data using data analysis techniques and methods such as risk indicators/criteria translated into algorithms (risk rules) or cross-matching of '*knowns'* (i.e. hits on watch-lists, intelligence, past detections and other sources of information), to detect (un)known modus operandi or identify unusual patterns.

[9] The total rollout is planned in 3 releases, starting in 2021 with Postal by Air pre-loading and Air Express pre-loading.

Apart from ICS2, other customs systems and data are used in a broader sense for general customs supervision tasks. The **movement systems NCTS** (customs transit system) **and ECS** (customs export system) also contain real-time information, about goods moving in/out of the EU (as well as info about goods moving within the EU). However, these systems are decentralized[10]. The Container Status Message (CSM) directory contains information on physical movements of any container which will be imported by maritime vessel into the EU[11]. Other systems are centralised systems, but without real-time information (centralised customs databases like Surveillance).

Additionally, the customs authorities use today various sources of information when it comes to known risks, e.g. based on detections they make. On a national level customs authorities cooperate and share information with other law enforcement agencies. This information is input for the national risk analyses in order to enhance internal security on national level. On an EU level customs authorities share their own relevant information among each-other at the EU level via the Customs Risk Management System (CRMS – in the case of risk information for customs control purposes), Anti-Fraud Information system (AFIS – antifraud/investigation purposes) or other more specific customs systems. Information in these customs systems is accessible to and used by all customs authorities for the risk-based external border controls and investigations. [12] However, there is no automatic interconnection between those systems and JHA risk information tools such as SIENA messages and the Europol Information System. This means that customs-relevant alerts sent through JHA systems are not necessarily integrated in customs systems, and conversely.

---

10 Although these systems are decentralized, the related messages between the MS and/or CTC (Common Transit Convention) partners might be forwarded to a risk management authority, if the necessary legal base to do so is established. OLAF already gets a copy of NCTS messages (the ATIS project). At first sight however, this does not really match with the 'interoperability approach' applied in this project (i.e. interconnectivity of information systems where data registered in one system will automatically be consulted by another system on a real time basis). Nevertheless this is worth further exploring in the feasibility study.

11 This movement information is directly transmitted by the carriers to OLAF. It can be used to verify the origin of a container and, combined with ICS2 data, the completeness and correctness of Entry Summary Declarations (ENS) reported by maritime-operators of containerized cargo. A pilot project was set up between DG TAXUD and OLAF to demonstrate the feasibility of this approach.

12 The Commission services also recognised the potential added value in making interoperable some of the other customs systems, including OLAF systems, with ICS2 and as result with the JHA systems. However, this will be treated as a separate project and needs also further analysis.

Whatever concept will be decided after the feasibility study, it is clear that **ICS2 will play a central role**. As it is the only repository that has **a central overall view of the goods that are entering from third countries into the EU, and this on a real time basis**, which makes it for the moment the most suitable system for interoperability with JHA systems. The feasibility study will have to make clear what, if any, additional systems will be necessary to support correct interpretation of the ENS data (such as central directory of the Container Status Messages – CSM) and if interoperability with data actually gathered in decentralised systems like NCTS or ECS is in one way or another possible or useful. The essential conclusion is the recognition of the need to take the ICS2 as the starting point.

5.2. JHA systems

Practitioners carried out a mapping of the different systems in the JHA environment, essentially taking into account the JHA systems that were subject of the HLEG analysis and coverage. The potential interest of following systems - existing or under development - was examined: Schengen Information System (SIS), Europol Information System (EIS), Passenger Name Record (PNR), European Dactyloscopy (EURODAC), Visa Information System (VIS), Entry/Exit system (EES), European Travel Information and Authorisation System (ETIAS) Interpol's Stolen and Lost Travel Documents (SLTD) and Prüm (vehicle registration data). Each system has its particular role in the EU security architecture, but data are collected and processed in function of that particular role, with specific conditions of data access and data sharing, depending on their legal framework. By reviewing the content of the data and their format, the practitioners together with Commission services, defined where interoperability could add value and enhance the external border and/or internal security.

Regarding **SIS**, it is a system established in 1995 in the signatory Member States of the Schengen Agreement, as a compensatory measure following the abolition of internal border controls. A new legal framework - to be adopted end 2018 - will extent the functionalities, including biometric capabilities to be implemented by 2021. SIS enables competent authorities, such as police, customs and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. An SIS alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. Today, SIS is the largest information exchange platform in Europe containing data on persons and objects (currently it contains about 80 million records, it was accessed more than 5 billion times in 2017). Border control, police, customs, visa and immigration authorities, judicial authorities and vehicle registration services have access to it. SIS contains alerts on wanted persons and several categories of "readily identifiable objects", such as stolen vehicles, trailers, boats, aircraft, containers, industrial equipment and boat engines, stolen, lost, misappropriated or invalidated vehicle registration certificates and vehicle number plates, or stolen, lost, misappropriated or invalidated identity documents, firearms.

The experts concluded that it would be useful to crosscheck the relevant data in ICS2 and SIS in an automated and systematic way in order to ensure that all currently available and relevant information is fully exploited to enhance the external border protection and internal security.

Regarding Europol systems, Europol has a number of specific tasks and responsibilities such as establishment of a watch list or access to the data in certain systems to support the exchange of information between national police authorities as the EU criminal information hub. Europol provides a centralised criminal information and intelligence database for member states to store and query data on serious crime and terrorism. Europol thus can provide - among others - a quick reference to data on serious international crime available in member states or third parties. On 4 January 2018, the Europol Information System (EIS) contained **1,062,236 objects**. The EIS only contain a small sub-set of data within the Europol databases, but is the current system used for member state direct-access for crosschecking of Europol data. The total number of person objects (suspected, convicted or 'potential future' criminals) in the EIS on 4 January 2018 was **162,376**. A total of **2,478,825 searches** (98% by Member States directly) were performed in the EIS in 2017.

Like the customs information system, Europol databases contain data on suspect, convicted and potential future criminals, companies, telephone numbers, emails, websites, bank details and records, cars and licence plates, locations, etc. The Europol databases can serve both preventive and investigative purposes.

The experts also concluded it would be useful to compare relevant Europol data with ICS2 data because this can enhance the intelligence picture for both law enforcement and customs authorities and can trigger actions of preventive or investigative nature. This should also allow increasing the efficiency and effectiveness of the intelligence gathering and/or operational activities in risk assessment and control.

6. Summary of the practitioners' analysis and proposed next steps

In preparation of the feasibility study the Commission services together with the practitioners identified realistic operational business cases for having relevant customs and JHA systems interoperable with the objective of improving external border and internal security.

For customs risk assessment it is important that intelligence available in the JHA systems is useful to enhance the risk management, while the benefit for the security and border management to know more about the import (or export) activities by people on their watch lists is evident.

The result of the analysis and the conclusion from the practitioners meetings was that in terms of interoperability of security and border management systems with customs systems only SIS and Europol data[13], could add value to enhance the management of security risks. Interoperability of ICS2 data with those in PNR, EURODAC, VIS, EES and ETIAS would have had very limited use, if at all, seen their nature, set-up and/or purpose of gathering.

[13] "Europol data" is also the term used in the HLEG report. It covers the information available in several databases, among other the Europol Information System (EIS).

In addition the experts concluded that direct access for law enforcement authorities to ICS2 data, could be of benefit for investigative purposes. This needs however rather a policy discussion and decision (with consequent legal implications) than a detailed technical feasibility assessment.

Practitioners' analysis of the three systems brought forward certain elements, which will need to be carefully assessed, such as the identification of the relevant data and the limited comparability of certain data (which will require an analysis on data quality). For example, name and surname identification between the ICS2 (names of parties in the advance cargo information) and data in SIS alerts on persons. Also the relevance and manageability of the potential matches need to be assessed.

Further clarification will be needed in terms of identifying operational procedures, including purpose limitation, data access rules, etc. that would follow an automated matching process, taking into account the overall objectives of this initiative and the competences of the different authorities.

Further analysis also has to identify the legal challenges including proportionality and data protection in order to implement interoperability between the different systems.

As regards technical aspects, account should be taken of the interoperability framework under development in the area of border management, immigration and security, such as potential role of the different components of interoperability. This remark is also applicable in a more general way: the systems for which a potential has been identified in terms of interoperability are or still under development (ICS2), or actually evolving (Europol databases and SIS).

Conclusion

Practitioners concluded that there could be a benefit in establishing interoperability of security and border management systems with customs systems as demonstrated by the scenario. Interoperability should be considered between the SIS, Europol data and the ICS2 bearing in mind that the latter is in the process of being constructed. The **Commission will use this preliminary analysis** of systems, data, developed scenarios and conclusions **to further orient the substance of the feasibility study**. That feasibility study is however only a next step and the interoperability of other (potentially relevant) customs' systems will be assessed later in a separate project. Relevant experts from the Member States are requested to continue supporting this process.

Secondly, the Commission services support the idea of examining an additional potential benefit identified by the non-customs law enforcement authorities during the process of practitioners' analysis. This is that in parallel a **discussion should take place to examine the conditions under which other law enforcement authorities could be granted access to ICS2 data** for investigative purposes on a duly justified case-by case basis.