D2.5 Multinational risk based cooperation

Document Date: 11/12/2020

Work Package 2: Risk based border crossing points

Document Dissemination Level: Public
Abstract

The goal of TRESSPASS is to develop, demonstrate, and validate a single cohesive risk-based border management concept for air, maritime, and land border crossing points. As part of this goal, this document describes existing mechanisms for information exchange in the context of border control, what kind of information is involved in the implementation of risk-based border control in air, land and sea modalities and how the required information exchange was defined within the TRESSPASS project.

Chapter 2 presents background information along with the definition of information flows and benefits and challenges that might emerge in the border control context. In order to establish a ground for further technical descriptions, different levels and patterns of information exchange are introduced, including the publish/subscribe pattern of information exchange utilised within TRESSPASS.

Chapter 3 focuses on information flows with relevance for risk-based border management. It presents what data gathering possibilities exist for air, land and sea modalities and how various pre-enrolment technologies can be used to aid risk assessment based on traveller data. The chapter furthermore describes current key mechanisms in national and international information exchange and their relevance for multi-national, multi-level and multi-stage risk-based collaboration.

Chapter 4 delivers a description of key components and mechanisms developed within TRESSPASS to enable efficient data exchange within and between border crossing points and the entities responsible for them. After a short introduction of TRESSPASS risk-based border management information exchange principles, the different information exchange levels and components involved in the information exchange are described, followed by information on key aspects of information exchange in the TRESSPASS pilots.

Chapter 5 concludes with a summary of key aspects and recommendations for multinational risk-based cooperation.
# Project Information

<table>
<thead>
<tr>
<th>Project Name</th>
<th>robust Risk basEd Screening and alert System for PASSeengers and luggage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Acronym</td>
<td>TRESSPASS</td>
</tr>
<tr>
<td>Project Coordinator</td>
<td>National Center for Scientific Research “Demokritos”, EL</td>
</tr>
<tr>
<td>Project Funded by</td>
<td>European Commission</td>
</tr>
<tr>
<td>Under the Programme</td>
<td>Horizon 2020 Secure Societies</td>
</tr>
<tr>
<td>Call</td>
<td>H2020-SEC-2016-2017 (SECURITY)</td>
</tr>
<tr>
<td>Funding Instrument</td>
<td>Innovation Action</td>
</tr>
<tr>
<td>Grant Agreement No.</td>
<td>787120</td>
</tr>
</tbody>
</table>

# Document Information

<table>
<thead>
<tr>
<th>Document reference</th>
<th>D2.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title</td>
<td>Multinational risk based cooperation</td>
</tr>
<tr>
<td>Work Package reference</td>
<td>T2.5</td>
</tr>
<tr>
<td>Delivery due date</td>
<td>30.11.2020</td>
</tr>
<tr>
<td>Actual submission date</td>
<td>11.12.2020</td>
</tr>
<tr>
<td>Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Author(s)</td>
<td>Silvie Hrbková, Johanna Müller, Curdin Brändli, Slavtcho Groshev (CASRA)</td>
</tr>
<tr>
<td>Contributor(s)</td>
<td>Dirk J. Stolk, Jeroen van Rest, Mark van den Brink (TNO), Emmanouil Kermitsis, Konstantinos Apostolou (KEMEA), Paola Fratantoni (Z&amp;P), Elisa Orrù (ALU-FR), Manolis Kaliorakis (ED), Dimitris M. Kyriazanos (NCSR)</td>
</tr>
<tr>
<td>Document Review Status</td>
<td>☐ Consortium</td>
</tr>
<tr>
<td></td>
<td>☒ WP leader</td>
</tr>
<tr>
<td></td>
<td>☒ Technical Manager</td>
</tr>
<tr>
<td></td>
<td>☒ Quality and Risk Manager</td>
</tr>
<tr>
<td></td>
<td>☐ Ethical Advisory Board</td>
</tr>
<tr>
<td></td>
<td>☐ Security Advisory Committee</td>
</tr>
<tr>
<td></td>
<td>☒ Project Coordinator</td>
</tr>
</tbody>
</table>
List of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>Automated Border Controls</td>
</tr>
<tr>
<td>API</td>
<td>Advance Passenger Information / Application Programming Interface</td>
</tr>
<tr>
<td>BCP</td>
<td>Border Crossing Point</td>
</tr>
<tr>
<td>C2</td>
<td>Command &amp; Control</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-circuit television</td>
</tr>
<tr>
<td>CISE</td>
<td>Common Information Sharing Environment</td>
</tr>
<tr>
<td>CTG</td>
<td>Counter Terrorism Group</td>
</tr>
<tr>
<td>DBT</td>
<td>Design Basis Threat</td>
</tr>
<tr>
<td>DFA</td>
<td>Data Fusion &amp; Analytics</td>
</tr>
<tr>
<td>DMS</td>
<td>Distributed Messaging System</td>
</tr>
<tr>
<td>DRAS</td>
<td>Dynamic Risk Assessment System</td>
</tr>
<tr>
<td>DSC</td>
<td>Document Checking Service</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECRIS</td>
<td>European Criminal Records Information System</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EES</td>
<td>Entry-Exit System</td>
</tr>
<tr>
<td>EIF</td>
<td>European Interoperability Framework</td>
</tr>
<tr>
<td>EIS</td>
<td>Europol Information System</td>
</tr>
<tr>
<td>EIXM</td>
<td>European Information Exchange Model</td>
</tr>
<tr>
<td>EMSA</td>
<td>European Maritime Safety Agency</td>
</tr>
<tr>
<td>ETIAS</td>
<td>European Travel Information and Authorisation System</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EURODAC</td>
<td>European Asylum Dactyloscopy Database</td>
</tr>
<tr>
<td>EUROSUR</td>
<td>European Border Surveillance System</td>
</tr>
<tr>
<td>Eu-LISA</td>
<td>European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice</td>
</tr>
<tr>
<td>GDS</td>
<td>Government Digital Service</td>
</tr>
<tr>
<td>GNIBIS</td>
<td>Garda National Immigration Bureau Information System</td>
</tr>
<tr>
<td>IAPI</td>
<td>Interactive Advance Passenger Information</td>
</tr>
<tr>
<td>IAS</td>
<td>International Alert System</td>
</tr>
<tr>
<td>IBM</td>
<td>Integrated Border Management</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>LEAs</td>
<td>Law Enforcement Authorities</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>LSI</td>
<td>Legacy Systems Interface</td>
</tr>
<tr>
<td>MS</td>
<td>Member State</td>
</tr>
<tr>
<td>PIU</td>
<td>Passenger Information Unit</td>
</tr>
<tr>
<td>PKD</td>
<td>Public Key Directory</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Record</td>
</tr>
<tr>
<td>PPA</td>
<td>Privacy Protection Act</td>
</tr>
<tr>
<td>PWGT</td>
<td>Police Working Group on Terrorism</td>
</tr>
<tr>
<td>RBBM</td>
<td>Risk-based border management</td>
</tr>
<tr>
<td>RI</td>
<td>Risk indicator</td>
</tr>
<tr>
<td>SIS</td>
<td>Schengen Information System</td>
</tr>
<tr>
<td>SitCen</td>
<td>Situation Centre</td>
</tr>
<tr>
<td>SLTD</td>
<td>Stolen and Lost Travel Documents Database</td>
</tr>
<tr>
<td>SPA</td>
<td>Security Personnel Application</td>
</tr>
<tr>
<td>TDAWN</td>
<td>Interpol Travel Documents Associated with Notices database</td>
</tr>
<tr>
<td>TIEN</td>
<td>TRESSPASS information exchange network</td>
</tr>
<tr>
<td>TLC</td>
<td>TRESSPASS Light Client</td>
</tr>
<tr>
<td>TRA</td>
<td>Traveller Registration Application</td>
</tr>
<tr>
<td>TRESSPASS</td>
<td>robust Risk based Screening and alert System for PASSengers and luggage</td>
</tr>
<tr>
<td>TRIP</td>
<td>Traveller Identification Programme</td>
</tr>
<tr>
<td>VIS</td>
<td>Visa Information System</td>
</tr>
</tbody>
</table>
4.4 Horizontal Information Exchange Between Stakeholders Using the TRESSPASS System 41
4.5 Functional Information Exchange Using the TRESSPASS System 43
4.6 Benefits of the TRESSPASS Information Exchange Architecture 44
4.7 Information Exchange in TRESSPASS Pilots 44

4.7.1 Pilot in the Netherlands (Air Pilot) 45
4.7.2 Pilot in Poland (Land Pilot) 46
4.7.3 Pilot in Greece (Sea Pilot) 47

5 Conclusion 48

References 49

List of Figures 54

List of Tables 55
1 INTRODUCTION

1.1 Background

TRESSPASS aims to design, demonstrate and validate a single cohesive risk-based border management concept in support of the European Integrated Border Management. All tiers of the four-tier access control model are to be addressed, namely (1) measures undertaken in, or jointly with third countries or service providers, (2) cooperation with neighbouring countries, (3) border control and counter-smuggling measures and (4) control measures within the area of free movement.\(^1\) Risk-based border management is about using border control as a risk management measure against specific threats. The objective of Work Package (WP) 2 is the development of the risk-based border management concept, specifically with regards to border crossing points (BCPs). Risk methods, algorithms, border crossing point designs and information exchange are key factors to account for. Naturally, multinational risk-based cooperation must rely on functioning information flows. The types of information exchanged, the recipients and the timing of the information exchange must be well understood. The relevant scope covers not only information going to a particular BCP but also information flows between BCPs within a given country and information flows between BCPs situated in different countries.

1.2 Aim of this document

This document aims to describe the information flows within risk-based border management with a description of the solution approach of TRESSPASS. This includes the type of information, who needs to receive this information and when. This is not limited to sending various pieces of information to a certain BCP (or its data analysis centre), but also about information flows (including risk assessments) between BCPs (e.g. between different types (air, land, sea) of BCPs within one country, between bordering countries, within Schengen, Europe, between EU member states and external states). Lessons learnt in the maritime domain are incorporated and the role of Advance Passenger Information (API) and Passenger Name Record (PNR) systems described. A detailed description of the functional information exchange between border crossing points and the organisations that are responsible for these BCPs is thus presented in support of risk-based border management concept implementation.

Readers external to the project can expect to gain a better understanding of the information flows within risk-based border management and the TRESSPASS approach to facilitating them.

1.3 Input / output relevant for this document

Central inputs to this document were derived from:

- D1.2 Risk-based border management concept
- D1.4 Analysis of the legal and regulatory framework
- D2.1 Method for Design Basis Threat
- D2.3 Risk assessment methods
- D3.7 Interfaces to external systems
- D3.8 Exchange Service Model
- D5.1 System Architecture

\(^1\) For more information see: [https://ec.europa.eu/home-affairs/content/european-integrated-border-management_en](https://ec.europa.eu/home-affairs/content/european-integrated-border-management_en)
ICAO TRIP Guide on Border Control Management
CISE Architecture

The document can serve as input to WP4, WP5 and WP6, in particular whenever a description of the information flows between TRESSPASS nodes needs to be referenced, and in particular for D6.4 Framework for future implementation and validation of the TRESSPASS solution including post-project.

1.4 Methodology

The document consists of two main parts with different research methodologies. For sections 2 and 3, online resources were utilised for a selective search, in which the search terms presented in Table 1 were combined.

**TABLE 1: SEARCH KEYWORDS**

<table>
<thead>
<tr>
<th>Theme</th>
<th>Search term</th>
</tr>
</thead>
</table>
| **Information** |  ◦ Information exchange/flow/sharing  
◦ Types of information  
◦ Recipients of information |
| **Border**   |  ◦ National borders  
◦ Between borders/countries  
◦ Air/land/sea  
◦ In EU  
◦ Risk-based border management |
| **Institutions** |  ◦ Institutions for information exchange  
◦ CISE |

Parts of section 3 and especially section 4 describe concepts and functionalities described and developed within TRESSPASS, thus drawing information primarily from project deliverables and project partners.

---

2 For more information see https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20on%20BCM%20Presentation-May%202018.pptx
3 For more information see http://www.emsa.europa.eu/technical-specifications.html


2 INFORMATION EXCHANGE AND FLOWS

In this section, a theoretical introduction on information exchange is given, divided into several sub-chapters. While taking into consideration that information sharing can take place as a unilateral action without information given back in exchange and information exchange is a bi- or multilateral process between two or more entities, the two terms will be individually clarified, but for the purpose of this document, they are used interchangeably. In our understanding, sharing and exchanging of information constitutes an information flow.

At first, we define information sharing and provide context on its importance. Then, the benefits and challenges of information exchange are discussed, taking into account technical, organisational and political aspects. Different types of information exchange are distinguished as well as various patterns of information flow, elaborated on in sections 2.2 and 2.4. A theoretical introduction to the concept of interoperability closes this chapter.

2.1 Information exchange

2.1.1 Definition and context

Gil-Garcia, Chengalur-Smith, & Duchessi (2007) define information sharing as “building systems, instituting formal standards, and changing business processes to allow organizations to share data and information with many other organizations” (p. 1). Information sharing aims at regulating and standardising an “efficient and rapid flow of information and effective documentation” (European Commission, 2010, p. 47). Information sharing furthermore enables cooperation across boundaries (Navarrete A. et al., 2009). The implementation and connection of information systems has become crucial in modern global governance, not only on national but also on international levels. Prins, Broeders, Griffioen, Keizer, & Keymolen (2011, p. 133) state that “[i]nformation-sharing is important, after all, not only for security reasons; inside the external borders of Europe, it is also helping to complete the internal market and administrative cooperation in many different forms.”

By means of sharing information, EU Member States (MS) can deal with issues that would have been unmanageable otherwise, such as e.g. a common, streamlined migration policy based on data in European migration databases. A basic premise of information sharing is that the more data is exchanged between European governments, the better they can deal with the challenges facing them. Prins et al. (2011) see the protection of Europe’s citizens against the threat of terrorism as a main challenge (more information on this in section 2.1.4).

Two policy principles of information sharing can be distinguished (Scholl, 2005, p. 2; Dawes, 1996, p. 392):

- “Information stewardship”: the government acts as a responsible caretaker of accurate and useable information
- “Information use”: agencies are given incentives to responsibly provide and share accurate information

Furthermore, four components of cross-boundary information sharing are discussed in research (Gil-Garcia, Pardo, & Sutherland, 2016, p. 347; Navarrete A. et al., 2009, p. 7):

- “Trusted social networks”: social actors who know and trust each other
- “Shared information”: sharing of knowledge - both formal (e.g. documents) and informal (e.g. informal talks, e-mail messages, text messages, etc.)
“Integrated data”: integration of data at the level of data element standards or industry/community standards (e.g. Extensible Markup Language (XML))

“Interoperable technical infrastructure”: systems that can communicate with each other at the hardware or operating system level

2.1.2 Benefits and challenges of inter-agency information exchange

Inter-agency information exchange describes, in general, the sharing and exchanging of information between two or more agencies. Benefits of and barriers to information exchange are briefly described here from a technical, organisational and political perspective.

From a technical perspective, information sharing can help improve the management of data and technical infrastructure, as with more information being shared, infrastructure systems are required to develop further to be able to accommodate the increased information flow (Scholl, 2005). At the same time, with a new, convenient communication tool becoming available (e.g. online push messages) more information will likely be shared through it. Streamlined data management ideally avoids duplicated data collection, processing and storage, increases productivity and thus reduces costs, with the development of information infrastructure furthering development of technical standards, data centres and telecommunication networks (Dawes, 1996). On the other hand, incompatible hardware, software and communications along with mismatched data structures can be considered as some of the main barriers of information sharing. Different agencies may have (besides different software systems) conflicting data definitions and structures, which complicates successful information sharing.

From an organisational perspective, the use of information sharing as a tool for problem solving can allow agencies to benefit from improved quality, quantity and availability of data. Comparing data with external information can enhance the validity of one’s own data and compiling data from different sources can result in more comprehensive and accurate information for problem solving. Information sharing additionally can lead to broadened networks of professional contacts, often being the currency of such relationships (Dawes, 1996). However, individual organisations usually only participate in information sharing when it is beneficial in some way. Thus, organisational self-interest can act as a potential barrier for information sharing. Dominant professional frameworks and their ethical standards play a crucial role in whether or not information is (or can be) shared between organisations. Furthermore, lack of trust, security reasons, legal restraints and lack of awareness of each other’s information needs might serve as barriers for information sharing.

As far as the political perspective is concerned, the sharing of information can enable a better coordination of services and improved accountability in the public domain (Scholl, 2005). With a collective information database, agencies can use a broader economic and demographic context for achieving policy goals. With more information available, more alternatives can be taken into account for taking decisions. Importantly, making information publicly available can allow for more accountability, as governments can be forced to explain decisions using the available information. Lastly, sharing information can also lead to more integrated planning and service delivery and improved program evaluation (Dawes, 1996). However, organisations can thus be forced to share decision-making powers with other actors, which means there are external influences over decision-making acting as possible barriers. Agencies can be reluctant to share information, because it is a source of power and a symbol of authority in decision-making. This power of agency discretion and the “primacy of programs” (government activity being mostly defined through legislation assigning responsibility for programs to specific agencies) can act as further political barriers.
2.1.3 Information sharing in the border control context

Navarrete A., Mellouli, Pardo, & Gil-Garcia (2009) studied information sharing at national borders and developed a framework incorporating information sharing with various contextual factors of border regions. Collaboration within national border regions was described as potentially challenging due to “diverging national, as well as state, provincial, and local agendas, different legislation and regulation systems for providing services, accessing, and sharing both citizen and government information, cultural differences (e.g. language barriers, resistance to technological innovation), and technological problems related to the integration of the deployed systems” (Navarrete A. et al., 2009, p. 1). Examples of complicating factors for information sharing between entities include “incompatible infrastructures, heterogeneous communication networks, complex web of information systems, diverse database designs, and variable data quality” (p. 5) along with different institutional, personnel and technological capacities, as well as political instabilities. Thus, the political, social, cultural and economic environment of each border control entity could be a barrier to interactions and information sharing.

For an effective and efficient information exchange, information and communication technologies, organisational structures, as well as the policy environment and jurisdictional authorities play a crucial role. Furthermore, governments require “high levels of interoperability of policy, management and technology systems including standardization” (Navarrete A. et al., 2009, p. 2). While effective information sharing provides many benefits, there are also potential risks related to privacy and further rights. This is especially highlighted in the EU regulation 2016/679 (GDPR) regarding the protection of personal data, which emphasises the risks accompanying cross-border flows of personal data along with the legal rights and duties deriving from them, as a result of modern social and economic integration along with rapid development in technologies and globalisation.

2.1.4 Information sharing across EU countries to combat the threat of terrorism

Before the terrorist attacks of September 11th, 2001 in the United States of America, cooperation in counter-terrorism was informal and not officially a part of the institutional structure of the European Community (Wensink et al., 2017). After the bombings of July 7th, 2005 in London, the EU adopted the “European Union Counter-Terrorism Strategy”, facing challenges related to coordination, coherence and consistency in this policy area. Then, in 2015, the “European Agenda on Security” was launched in order to enhance security in MS by improving information sharing and prevention of radicalisation. One year later, after the attacks in Brussels (March 2016), a “Security Union” was launched, further emphasising the need to improve the sharing of information (Wensink et al., 2017).

Crucially, Wensink et al. (2017) point out that “[s]haring more information is not necessarily a good thing as it can produce data overflow. Of more importance in this respect is the capacity for analysis in the Member States to process the information” (p. 54). This can be challenging, since the degree of collaboration among agencies (police, intelligence, security service, judicial) in the EU MS varies⁴, and agencies are bound by legal mandates when it comes to what information can be shared and with whom.

The most important information sharing platforms for intelligence and security services, as well as for police forces are informal non-EU structures, such as the Counter Terrorism Group

---

⁴ For more information on the specific set-up of the mentioned agencies in the different countries see https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf, p. 54 and 55.
Another element in the EU’s internal-external security network is the EU Joint Situation Centre (SitCen), observing developments on a 24 h basis. Members of European security and foreign intelligence services evaluate information they receive from national intelligence sources, making the results available to decision makers in the Member States (Roell, 2011). The following advantages of SitCen are noted (Roell, 2011, p. 7):

- Bundling of information from a range of EU domestic and foreign intelligence services
- Improvement of the overall level of information
- Joint monitoring of security threats
- Support of common working standard and political decision making

SitCen cooperates, among others, with Europol (see section 3.3.3.4).

In the past few years, several steps have been undertaken to enhance the collection and exchange of data within EU countries for national security, namely the PNR Directive, the Schengen Information System (SIS) as well as the European Criminal Records Information System (ECRIS and ECRIS-TCN). In order to use existing and future databases more efficiently, proposals were issued by the European Commission (EC) on the interoperability between EU information systems. Intended to be operational after 2023, the new interoperability architecture aims at providing “border guards and law enforcement authorities with a single interface for their searches, as well as a biometric matching service to facilitate identification” (Innenkamp et al., 2019, p. 8).

Enhanced information sharing across EU countries can result in various improvements of the protection of citizens against terrorism, ranging from “cutting the financing of terrorism, tackling organised crime, and strengthening border controls to addressing radicalisation and improving police and judicial cooperation on tracing suspects and pursuing perpetrators” (Terrorism in the EU since 2015, 2019). In addition, Europol (see section 3.3.3.4) has been given additional powers, allowing it to set up specialised units more easily, as was done with the European Counter Terrorism Centre set up in January 2016, and to exchange information with private companies where needed (Terrorism in the EU since 2015, 2019). As criminals and terrorists often use false identities in order to evade border guards and police, the importance of effective information sharing between relevant authorities is further highlighted (How to Stop Terrorism: EU Measures Explained (Infographic), 2019).

2.2 Types of information exchange

The Guidelines for Integrated Border Management (IBM) (European Commission, 2010) distinguish between three types of cooperation where information exchange plays a crucial role, namely intra-service (within organisations), inter-agency (between organisations) and international cooperation (between organisations of different countries).

---

5 The CTG (as part of the informal Club de Berne) acts as the interface between representatives of the intelligence services and state protection authorities from 30 Schengen countries (Closer Cooperation with the Counter-Terrorism Group, 2019) on terrorist matters, and provides a forum for experts to develop practical collaboration and an understanding of the terrorist threat (“Club de Berne” Meeting in Switzerland, n.d.).

6 The PWGT, established in 1979, allows for the exchange of police information on terrorist threats in Europe (PWGT, n.d.; Wensink et al., 2017).


8 For more information see: https://www.europol.europa.eu/
2.2.1 Intra-service cooperation and information exchange

The operational staff of a border management entity should have relevant and current information to enhance knowledge of relevant risks and situational awareness and support focused operations that successfully fulfil their duties. Within each border management agency, information flows need to be horizontal and vertical. These are defined as follows (European Commission, 2010, p. 47):

“Horizontal flow is the exchange of information between different individuals, departments or units at the same organisational level. This should take place at all organisational levels of an agency: at headquarters, regional centres and local units.

Vertical flow is the exchange of information between different individuals, departments or units at different organisational levels.”

Ideally, the system of information exchange is described in operational instructions, including standardised templates for the reporting of data and information. A harmonised system of data collection facilitates data sharing with other services. Data protection has to be ensured at all times, regardless of the information exchange system in place. The established IT system should have the following capabilities (European Commission, 2010, p. 48):

- Ensure automated information exchange and communication within the border management agency through a unified system, for example, through database, intranet and emails;
- Provide for a system of collecting, processing and distributing data and information with real-time access for authorized users;
- Allow for data flow management;
- Allow for identification of users based on the access rights and passwords;
- Include a central alert system;
- Include the possibility of creating statistical/analytical summaries (it must be specified who has the right to create these);
- Ensure security and integrity of the system, e.g. through fire walls and cryptography;
- Allow links to electronic border protection equipment (sensors, radars, stationary thermal cameras, etc.) where feasible;
- Be interoperable with the IT systems of other relevant public authorities considering protection of personal data.”

2.2.2 Inter-agency cooperation and information exchange

For inter-agency communication, three levels are distinguished (European Commission, 2010, p. 58):

- Local: Shift managers/leaders in daily contact; BCP chiefs meeting regularly (e.g. on a weekly basis) and ad hoc (e.g. early warning or to deal with unforeseen cases);
- Regional: Heads of regional office conducting regular (e.g. monthly) meetings and ad hoc;
- Central: Representatives of all agencies meeting regularly, for example on a monthly basis as well as ad hoc; representatives of the IBM inter-agency working group meeting on a regular basis (e.g. twice yearly).”

All participating agencies should have a formal agreement clarifying which information will be shared and with whom, as well as how the information exchange should take place. Possible methods are briefings and meetings, nomination of contact points within each agency, hard-copy as well as electronic reports and data, sharing of information from databases or common databases (European Commission, 2010, p. 58). Ideally, joint systems would be created to facilitate the authorised exchange of information.
2.2.3 International cooperation and information exchange

For international cooperation and information exchange, the IBM proposes “to set up effective external communication mechanisms in order to create functional interfaces between border management agencies in different countries” (European Commission, 2010, p. 73). In doing so, there should be an emphasis “on neighbouring countries, countries of origin of significant flows of migrants, strategically relevant exporting and importing countries, industry representatives within these countries as well as relevant international organisations” (European Commission, 2010, p. 73).

Regular meetings between representatives of border management agencies from different states serve as a platform for information exchange on various developments regarding legislation, institutions and organisations, as well as operations of each agency and the challenges they each face. Heads of border posts should maintain contact and establish working relations with their counterparts at an operational level, and exchange data and intelligence based on relevant agreements. The IBM guidelines further suggest a systematic exchange of national reports on a weekly or monthly basis, allowing a monitoring of the border situation in a region and an exchange of statistical data with authorities of neighbouring states. On a yearly basis, an analysis of BCP operations should be prepared, so neighbouring countries could discuss key findings on shared BCPs and assess their cooperation as well as discuss operational changes in order to harmonise border procedures.

In addition, it is described as beneficial to pursue memberships of relevant international networks, “as these fora also provide opportunities for formal and informal information exchange and the development of a contact network with counterparts in other states and agencies” (European Commission, 2010, p. 73).

2.3 Information flow

Information flow, a concept already mentioned, can be defined as the “path data takes from its original setting to its end users” (Business Dictionary: Information Flow, n.d.) and further as the “movement of information between people and systems” (8 Types of Information Flow, n.d.). Barwise and Seligman (1997) developed four principles that characterise information flows that are briefly summarised here.

The first information flow principle (Barwise & Seligman, 1997, pp. 8-9) is that “information flow results from regularities in a distributed system”. Distributed means divided into parts, so that the information flows from one part to another. The system is made of different components located in different places and/or machines that coordinate their activities. The presence of regularities is what links the parts of a system together so that the flow of information is possible. Usually, the regularities that ensure the uniform behavior of a system are of electrical or mechanical nature (e.g. a computer). However, “the behavior of the system need not be entirely predictable for information to flow. […]. Yet, as a general rule, the more random the system the less information will flow.”

The second principle of information flow is that “information flow crucially involves both type and their particulars” (Barwise & Seligman, 1997, p. 27). Particulars or “tokens” carry information in the form of types, so “a ‘token’ is something that is being classified, and a ‘type’ is something that is used to classify something else” (Mantri & Feng, 2010, p. 5). As an example, tokens could be instances of a traffic light, types the occurrence of red, green and yellow lights (Mantri & Feng, 2010).

The third principle by Barwise and Seligman (1997) is the following: “It is by virtue of regularities among connections that information about some components of a distributed
system carries information about other components” (Barwise & Seligman, 1997, p. 35; Kent, 2016, p. 11; Mantri & Feng, 2010, p. 8). Thus the traffic light tokens from the previous paragraph act as traffic light system component connections. Mantri & Feng (2010, p. 7) describe that a “traffic light’s colour is responsible for the Instructions to the Traffic in some way at a time if this kind of correspondences between them happens by the two of them being part of, say, a single traffic light system”. This kind of correspondence enables one of them to carry information about the other.

Finally, the fourth principle of information flow reads as follows (Barwise & Seligman, 1997, p. 43; Kent, 2016, p. 13): “The regularities of a given distributed system are relative to its analysis in terms of information channels”.

2.4 Patterns of information flow

In the following sections, different information flow patterns are described, building upon insights from the maritime domain in Europe.

2.4.1 Sender and receiver

In a communication context, a sender is considered to be the originator of a message on a particular occasion. Within information processing, senders encode information and transmit data, via a channel, to one or more observers or receivers. A receiver is in turn the audience that receives the message from the sender. Often, the receiver gives feedback to the sender to confirm message retrieval. In common communication patterns, the sender and receiver roles are interchangeable (Oxford University Press, 2020). The effectiveness of the data exchange depends critically on the information structure. When incomplete and/or asymmetric information flows exist between a sender and a receiver, the sender can limit the receiver’s perceptions of their knowledge and reduce the knowledge transfer (Lin et al., 2014).

2.4.2 General pattern of information flow

Depending on the perspective on information exchange, authorities who share data can take both the role of information sender and information receiver at consecutive points in time. For example, Authority A can act as a sender when sending a traveller’s information to Authority B to cross-check against a national database containing a watch list. Authority B is the receiver at first and then becomes the sender when returning the result of the database check to Authority A. This principle is shown in a basic schematic illustration in Figure 2-1.

![Figure 2-1: Basic Information Exchange](image-url)
2.4.3 Common Information Sharing Environment (CISE)

The Common Information Sharing Environment (CISE)\(^9\) by the European Maritime Safety Agency (EMSA) distinguishes five communication patterns for information flow between CISE stakeholders, summarised as follows:

**Pull**: the consumer knows the provider and asks for information, made available only if and when possible (asynchronously) (Figure 2-2).

**Pull unknown**: the consumer asks for information to all possible providers, as they do not know who will provide them with the specific information they need. Information is made available only if and when possible by one or several providers (asynchronously) (Figure 2-3).

**Push**: the provider knows a consumer who could be interested in information and sends it to him (synchronously) (Figure 2-4).

**Push unknown**: the provider does not know who could be interested in the information but sends it (synchronously) to all possible consumers of a certain profile (Figure 2-5).

---

Publish/subscribe: the consumer subscribes to a type of information from the provider. As soon as this information is available from the provider, it is sent to all consumers which have previously subscribed (Figure 2-6).

FIGURE 2-6: PUBLISH/SUBSCRIBE PATTERN OF INFORMATION EXCHANGE (CISE Architecture, n.d., p. 2)

With regards to communication practices and information exchange between customs and border guards, four similar categories of information exchange are distinguished, namely “on request”; ‘ad hoc’; ‘periodic’; and ‘continuous exchange through joint databases’” (Practices and Forms of Cooperation between Customs and Border Guards in the European Union, 2011, p. 3).

2.5 Interoperability

Interoperability is defined as “the ability of diverse systems and organizations to work together i.e. to inter-operate” (ISO 22397, n.d.). It is considered a shared value of a community and multilateral by nature. A broader definition provided by the European Interoperability Framework (EIF) is the following (European Interoperability Framework (EIF) for European Public Services, 2010, p. 1):

“Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.”

The EIF distinguishes four aspects of interoperability, namely legal (align legislations of collaborating countries), organisational (coordinating processes), semantic (preserve meaning of information) and technical (equipment and ICT systems).

Interoperability is crucial to an efficient delivery of European public services, as it addresses the need for (European Interoperability Framework (EIF) for European Public Services, 2010, p. 2):

› cooperation among public administrations with the aim to establish public services;
› exchanging information among public administrations to fulfil legal requirements or political commitments;
› sharing and reusing information among public administrations to increase administrative efficiency and cut red tape for citizens and businesses.”

As a result, public service delivery can be improved by facilitating a “one-stop-shop delivery of public services” (European Interoperability Framework (EIF) for European Public Services, 2010, p. 2) and thus lowering costs for public administrations.
3 INFORMATION FLOWS WITH RELEVANCE FOR RISK-BASED BORDER MANAGEMENT (RBBM)

This chapter focuses on information flows with relevance for risk-based border management. It aims to illustrate how data gathering would need to be adapted for air, land and sea modalities and how various pre-enrolment technologies could be used to address the concept of risk assessment based on traveller data. Current key mechanisms in national and international information exchange are also discussed, concluding with a multi-national, multi-level and multi-stage overview of information flows with relevance for RBBM.

3.1 RBBM overview

The current decision-making process prevalent at BCPs currently is primarily rule-based. This means that travellers who want to cross the border at a BCP are checked indiscriminately, according to the same rules. An extension of this rule-based approach is intelligence-led decision making, which is currently in use at certain BCPs (especially airports). This approach includes collecting and screening certain additional information on travellers (e.g. provided by carriers) before they actually arrive at the BCP. However, with both these approaches the actual checks remain the same, and the flow-rate (throughput) of travellers at BCPs is expected to decrease in the long-term due to growing traveller volume. RBBM offers a potential solution through tailored checks proportional to the risk profile of a traveller. This means that minimal checks are conducted if possible, and more stringent checks applied when needed. In order to achieve this, “the type of checks should be based on a situational threat assessment of each individual traveller, based on actual information on threats and vulnerabilities” (D1.2, p. 38).

To this end, RBBM requires (multi-)national policy decisions to determine threats that have to be counteracted by border control as well as risk acceptance levels (seeing as risks cannot be completely eliminated), allowing national strategic formulations of threat scenarios and associated risk profiles (D2.3)\(^\text{10}\). Risk profiles are defined through combinations of characteristics related to behaviour, identity, mental state and capability that could plausibly lead to the manifestation of risks if a traveller is allowed to pass a BCP. In turn, risk indicators are the indicative signs that suggest that a particular threat has been encountered as a result of screening and/or checks (D2.1, p. 14). The set of risk profiles and corresponding risk indicators of a particular BCP can and need to be adjusted based on situational assessments. For travellers and belongings that match specified low-risk profiles, the number and extent of checks at BCPs can be reduced. On the other hand, travellers and belongings that match higher-risk profiles will receive more extensive checks at BCPs.

Figure 3-1 illustrates how the risk-based border management approach manifests at a given BCP. A (contactless) screening of each traveller is performed in advance of their arrival and at the BCP. This screening data is combined and matched with data from further information sources and compared against risk profiles. Based on this risk assessment, the type of check(s) for each traveller is determined. Assuming that the vast majority of travellers do not present a threat and that it is possible to accurately assess the threat for most travellers, a central

---

\(^\text{10}\) See the first TRESSPASS Newsletter for an overview: https://mailchi.mp/8d0500c53df0/tresspass-project-newsletter
expected outcome of applying RBBM is fewer and shorter interruptions in the flows of travellers and their belongings.

**Figure 3-1: Risk-based Border Management Approach at BCPs (D2.3, p. 9)**

Information exchange can be considered as one of the core elements of RBBM. Risk-based decision making requires more and other types of information than rule-based decision making, e.g. information for a situational risk assessment to determine the types of risks that an individual BCP is facing. The following sections discuss key stakeholders and current and planned approaches to information gathering and exchange with relevance for RBBM.

### 3.2 Information flow overview between RBBM stakeholder levels

One important pre-condition for RBBM is facilitation of interaction at various management levels between all involved organisations (D1.2, p. 85). Figure 3-2 depicts a schematic overview of public stakeholders and their relations in border management, distinguished by intra-service, inter-agency and international collaboration. The illustration distinguishes between five hierarchical levels (D1.2, p. 18):

- **The EU policy level**, where the EU and governments of MS make agreements on border management in Europe and on how they operate (in agencies like Frontex and Eurosur).
- **The national policy or governmental level**, where each MS decides on the implementation of border management within its country in alignment with EU policies, and where bi-lateral agreements with countries inside and outside the EU are established.
- **The strategic level**, where national authorities and services (a) command and control their respective agencies at tactical level (intra-service) and (b) coordinate their activities with their colleague agencies at strategical level within their country (inter-service) and with other countries (international).
- **The tactical level**, where command, control and coordination at BCPs and at the green and blue borders takes place.
- **The operational level**, where border control (at BCPs) and border surveillance (at green and blue borders) actually is executed.
3.2.1 Vertical information flow

RBBM requires that government stakeholders at European and national level commit to definitions of threats and the acceptance of associated residual risk. The strategic level role is to then further elaborate threat scenarios and risk acceptance details relevant in the context of the national BCPs, along with initial risk indicators. This level ensures that the threats established on the national level are sufficiently mitigated by border control at BCPs. At BCPs, the tactical level personnel need to maintain detailed risk indicators lists so that a regular situation assessment and a targeted risk assessment of travellers can be performed. This level also maintains risk profiles and verifies whether they are still adequate and up-to-date. Staff on the operational level (e.g. field border guards) finally perform the screening and checks of travellers to assess their conformance or non-conformance with risk profiles (D1.2, p. 79).

3.2.2 Horizontal information flow

RBBM involves particular additional types of information that would need to be exchanged for effective multi-national and multi-level risk-based cooperation, e.g. (D1.2, p. 85):

- **Residual risk:** Participants in international agreements may plausibly want to reach agreements on taking on less or additional risk under specific conditions in light of specific benefits.
- **Risk-based concepts:** Novel risk-based concepts may very well be developed on national level that are applicable and valuable to be shared with other countries.
Risk profiles: Border guard agencies will periodically update distinguishing features between illegitimate and legitimate travellers and accordingly design and update risk profiles for their BCPs. These profiles could very well be relevant to be shared with other BCPs, whether in other modalities or even other countries.

BCP records: Travellers may pass through multiple BCP during their journey, providing new risk-related information at every BCP that will most likely be relevant for the next.

3.3 National and international collaboration systems

As described above, the IBM distinguishes between three types of collaboration within public agencies, intra-service (within organisations), inter-agency (between organisations) and international (between organisations of different countries). IBM, and with it the three ‘pillars of collaboration’ should be understood as (European Commission, 2010, p. 23): “national and international coordination and cooperation among all the relevant authorities and agencies involved in border security and trade facilitation to establish effective, efficient and coordinated border management, in order to reach the objective of open, but well controlled and secure borders”.

A number of databases are currently in use to facilitate information exchange in border control related to travellers and their belongings. Key drivers behind the internationalisation of information flows are the various systems put into place for tackling the threats of irregular migration, cross-border crime and international terrorism (Prins et al., 2011). For national law enforcement authorities, timely access to up-to-date information and intelligence is crucial for the task of successfully preventing, detecting and investigating criminal activities (Information Exchange, n.d.). With the Hague Programme11 (2005-2010) the principle of “availability” was introduced, as “the guiding concept for law enforcement information exchange”, establishing that throughout the EU, information available to law enforcement authorities of one MS should also be made accessible to law enforcement authorities of other MS (Information Exchange, n.d.). The later introduced Stockholm Programme12 (2010-2015) emphasised the need to continuously develop law enforcement cooperation within the EU.

Such existing information systems serve as an important source of information that can be utilised for the risk assessment of a traveller.

3.3.1 Domains of main information systems

In Figure 3-3, the main information systems for border management and law enforcement are depicted in a summary overview, distinguishing between border management information systems and law enforcement information systems.

---


This division is used in the rest of the subchapter, where a brief discussion of the main EU information exchange systems, as well as further, complementary information exchange systems is provided. The discussion describes the types of information that the systems provide and that might be employed by RBBM, as well as the accessibility of this information to different authorities.\(^{13,14}\)

### 3.3.2 Border management systems for information exchange\(^{15,16}\)

The three main border management information systems with relevance for RBBM are the Schengen Information System (SIS), Visa Information System (VIS) and European Asylum Dactyloscopy Database (Eurodac) (European Commission, 2016, p. 5). In addition to these systems, the Entry-Exit System (EES)\(^{17}\) is expected to be operational in the first half of 2022 to capture entry, exit and refusal data on third-country nationals crossing the external borders (European Commission, 2016).\(^{18}\) Furthermore, the European Travel Information and

---


15 Consider also D1.4 (chapter 3.3) with more information on the legal aspects of the various information exchange and operational cooperation systems in the EU.


Authorisation System (ETIAS)\textsuperscript{19,20} is expected to be in place by the end of 2022 to help keep track of visitors from countries that do not need a visa to enter the Schengen Zone (ETIAS – European Travel Information and Authorisation System, 2020). In the following table (Table 2) we provide an overview of the accessibility of these main information exchange systems to different authorities. This information will be further discussed separately for individual databases in the following subchapters.

**Table 2: Who can access which database? (“EU INFORMATION SYSTEMS SECURITY AND BORDERS,” 2019)**

<table>
<thead>
<tr>
<th>Accessible to</th>
<th>SIS</th>
<th>VIS</th>
<th>Eurodac</th>
<th>EES</th>
<th>ETIAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa authorities (consular posts) and immigration authorities</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Border controls authorities (border guards)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Asylum authorities</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Police authorities</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customs authorities</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Judicial authorities</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vehicle, boat and aircraft registration authorities</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carriers*</td>
<td>●</td>
<td></td>
<td>●</td>
<td>(1)</td>
<td>(2)</td>
</tr>
</tbody>
</table>

* Carriers will only have access to a limited web service in order to confirm that the traveller holds a valid visa or ETIAS authorisation.

### 3.3.2.1 Schengen Information System II (SIS II)

The Schengen Information System (SIS) is used by law enforcement authorities to consult alerts on wanted or missing persons (in particular children) and objects (such as money, cars, firearms, identity documents), inside the EU and at the EU’s external borders. In 2013, a more advanced version of the SIS, the Schengen Information System II (SIS II)\textsuperscript{21} was launched “with enhanced functionalities such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system” (Second Generation Schengen Information System (SIS II), n.d.). In 2015, it was upgraded to facilitate information exchange on terrorist suspects as well as to reinforce MS efforts “to invalidate travel documents of persons suspected of wanting to join terrorist groups outside the EU” (Information Exchange, n.d.). The SIS II allows for information exchange between national border control authorities and is used by 25 EU MS\textsuperscript{22}, four


\textsuperscript{22} Austria; Belgium; Bulgaria; Croatia; Czech Republic; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Italy; Latvia; Lithuania; Luxembourg; Malta; the Netherlands; Poland; Portugal; Romania; Slovakia; Slovenia; Spain; Sweden
associated countries\(^\text{23}\) and the United Kingdom (SIS II - Second Generation Schengen Information System, n.d.). Thus, SIS II supports authorities in ensuring the internal security of the EU, while respecting data protection requirements. It contains the following information on persons (or objects) for whom (or which) an alert has been issued (Regulation (EC) No 1987/2006, n.d., p. 13):

- Identity of person: surname(s), forename(s), name(s) at birth, aliases, specific physical characteristics, place and date of birth, sex, nationality/ies
- Photographs and fingerprints
- Reason for alert and links between alerts plus authority issuing alert
- Whether person is armed, violent or has escaped
- Alerts on persons wanted for arrest or sought to assist with a judicial procedure
- Alerts on persons or vehicles, boats, aircraft and containers for checks in order to prosecute criminal offences
- Alerts on objects sought for seizure

Within SIS II, national offices called *Supplementary Information Request at the National Entries (SIRENE)*\(^\text{24}\) Bureaux are acting as the contact points between a MS creating an alert and one receiving the match, thus assisting in obtaining supplementary information for SIS II. The SIS II can be accessed by visa authorities, border control authorities, asylum, police, customs and judicial authorities as well as vehicle, boat and aircraft registration authorities. However, carriers do not have access to the SIS II. Under certain conditions, Europol, Eurojust\(^\text{25}\) and the European Border and Coast Guard Agency (Frontex) can as well access the SIS II. A match between an identified person and an alert in SIS II would be an immediate red flag in the context of RBBM.

3.3.2.2 Visa Information System (VIS)

The Visa Information System (VIS) enables the exchange of visa data between EU countries and associated countries applying the common visa policy. With the VIS “the examination of applications for short stay visas and decisions on extending, revoking and annulling visas, as well as the checks on visas and the verifications and identifications of visa applicants and holders are facilitated” (VIS Regulation, n.d.).

In the VIS, the following data are recorded:

- Alphanumeric data on the applicant and on the visas requested etc.
- Photographs and fingerprints
- Links to previous visa applications and to the application files of persons travelling together

A search in the VIS serves the purpose of verifying the identity of a person and / or the authenticity of the visa and / or whether a certain person meets the requirements for entry, stay or residence within a national territory. If data of the visa holder is found in the VIS, the relevant authorities can consult certain data of the application file (VIS Regulation, n.d.). For the VIS, access is granted to visa/immigration authorities as well as border control authorities, and also asylum and police authorities. In addition, carriers can as well access this information system, and under certain conditions other national authorities, Europol and the European

---

\(^{23}\) Iceland; Liechtenstein; Norway and Switzerland


Border and Coast Guard Agency (Frontex). The identification of a traveller followed by the verification that they were granted a visa will likely lower their risk score within RBBM substantially.

3.3.2.3 **Eurodac system**

Eurodac is an EU-wide biometric database containing fingerprints of asylum applicants and third-country nationals (entering the EU) for comparison between EU countries. Eurodac aims at making it easier for EU countries to “determine responsibility for examining an asylum application by comparing the fingerprints of asylum applicants and non-EU/EEA nationals against a central database” (Eurodac: European System for the Comparison of Fingerprints of Asylum Applicants, n.d.). Furthermore, law enforcement authorities should be enabled to consult Eurodac for the investigation, detection and prevention of terrorist or serious criminal offences. Countries are obliged to take fingerprints of “all asylum applicants and those apprehended while trying to cross a border irregularly (e.g. non-EU/EEA nationals or stateless persons entering without valid documents) over the age of 14 and, within 72 hours” and then transmit it to Eurodac (Eurodac: European System for the Comparison of Fingerprints of Asylum Applicants, n.d.). Thus, if an asylum seeker or third-country national is illegally present in the EU, the respective EU country can consult Eurodac in order to determine whether that person has previously applied for asylum or tried to unlawfully enter the EU. Eurodac is accessed by border control, asylum and police authorities, and could be accessed under certain conditions by Europol, the European Border and Coast Guard Agency as well as the European Asylum Support Office26. A match between an identified person and a negative Eurodac entry would be an immediate red flag in the context of RBBM.

3.3.2.4 **Entry-Exit-System (EES)**

The planned Entry-Exit-System, part of the Smart Borders package27, will apply to non-EU nationals crossing the EU’s external borders for a short stay and to travellers who are from visa-exempt non-EU countries (and allowed to stay up to 90 days in a 180-day period). It is an “automated IT system for registering entries and exits of travellers from non-EU countries at the external borders” (Smart Borders: EU Entry/Exit System, n.d.). With EES, it will be possible to detect overstay and undocumented persons in the Schengen area (European Commission, 2016). The date, time and place of entry and exit of non-EU nationals crossing EU borders will be recorded and stored, together with data on identity, travel documents, as well as biometric data. The system will also automatically calculate the duration of authorised stay and generate alerts to EU countries upon expiry of the stay. It will also record data of non-EU nationals whose entry for a short stay was denied. EES will be operational at the external borders of the EU in the first half of 2022, fulfilling the following conditions (Smart Borders: EU Entry/Exit System, n.d.):

“[…] which apply the Schengen acquis28 in full and at the borders of EU countries which — at the time the system will start its operations — will not yet apply the Schengen acquis in full, but will have successfully gone through the Schengen evaluation procedure29 and

---

26 For more information see: [https://easo.europa.eu/](https://easo.europa.eu/)
28 For more information see [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922%2802%29](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922%2802%29)
The stored data will be accessible to border authorities, visa-issuing authorities and authorities responsible for monitoring whether or not a non-EU national fulfils the conditions for entry or residence. Designated law enforcement authorities and Europol can also request the consultation of EES data (Smart Borders: EU Entry/Exit System, n.d.). A match between an identified person and an EES alert would be an immediate red flag in the context of RBBM.

3.3.2.5 European Travel Information and Authorisation System (ETIAS)

ETIAS, expected to be operational by the end of 2022, will gather information on all non-EU nationals travelling visa-free to Europe and ensure that possible security and irregular migration concerns are identified before travel to the Schengen area. As citizens of countries who do not need a visa for travelling to the EU (for up to 90 days) do not need to go through a visa application process, ETIAS aims to make sure that these travellers are not a security threat. Citizens from 62 countries will need to get ETIAS authorisation once the system is in place. ETIAS is to be accessed by border control authorities and carriers and would provide first inputs for traveller risk assessment in the context of RBBM.

3.3.2.6 Stolen and Lost Travel Documents database (SLTD)

The Stolen and Lost Travel Documents database (SLTD) “helps police to catch terrorists and criminals who often use fraudulent travel documents to cross borders” (Stolen and Lost Travel Documents Database, n.d.). It allows law officers around the world to check the validity of a travel document. The database contains around 84 million records of lost, stolen and revoked travel documents (passports, identity cards, visas and UN laissez-passer, as well as stolen blank travel documents). Countries can submit records of lost or stolen documents to the database only if it was issued in the respective country. Then, law enforcement officials at border crossings can check the passports of travellers internationally against the SLTD and determine if the document has been reported as lost or stolen. A match with a SLTD entry would be an immediate red flag in the context of RBBM.

3.3.2.7 Advance Passenger Information Systems (APIS)

API, i.e. data contained in travel documents like passports and identity cards, is collected by air carriers during check-in and then transmitted to border control authorities of the destination country. API “enables a risk-based data-driven approach to border security”, as authorities screen passenger data while they are in-flight, and then can expedite the border checks for bona fide travellers, while time and resources can be spent on travellers that need further investigation (European Commission - Evaluation of the EU Policy on Advance Passenger Information (API), n.d.). The main objectives of collecting API data are to combat irregular immigration and improve border control. In the communication from the Commission to the EU Parliament and Council in 2016, it was pointed out that automated cross-checking of API data against SIS II and the SLTD database should be established. Furthermore, it was discussed whether MS should be obliged to require and use API data for inbound and outbound flights, particularly relevant in connection to the implementation of the Passenger Name Record Directive (European Commission, 2016, p. 8). API can serve as a first input for a traveller risk assessment in the context of RBBM.

30 The list of countries where citizens have to get the ETIAS authorization can be accessed here: https://www.schengenvisainfo.com/etias/
3.3.2.8 European Border Surveillance System (Eurosur)

Eurosur, established within Frontex, “is the information-exchange framework designed to improve the management of Europe’s external borders” (Frontex Information Management, n.d.). Its aim is to support MS in combating cross-border crime, tackling irregular migration and preventing loss of migrant lives at sea. At the core of Eurosur is a network of National Coordination Centres (NCCs) established by each MS. The main role of these NCCs is to coordinate the border surveillance activities and serve as an information exchange hub. The NCCs collect information about what takes place at the border, such as illegal border crossings or criminal activities, and then share that information with other MS as well as Frontex (Frontex Information Management, n.d.). None of the information exchanged within Eurosur contains personal data, but this network could plausibly be used for the exchange of risk-based concepts and traveller risk profiles in the context of RBBM.

3.3.3 Law enforcement systems for information exchange

3.3.3.1 European Criminal Records Information System (ECRIS and ECRIS-TCN)

The European Criminal Records Information System (ECRIS), established in 2012, is a decentralised electronic system to exchange information on criminal records between EU Member States. Currently, all EU countries are connected to ECRIS. The system “ensures that information on convictions is exchanged between EU countries in a uniform, fast and compatible way” (European Criminal Records Information System (ECRIS), n.d.). Furthermore, ECRIS provides prosecutors with easy access to information on the criminal history of persons concerned and “removes the possibility for offenders to escape the consequences of their previous convictions in another EU Member State” (European Criminal Records Information System (ECRIS), n.d.). Within ECRIS, it is not possible to easily find information on previous convictions of non-EU nationals. In order to obtain such information, respective EU countries have to be contacted one by one (European Criminal Records Information System (ECRIS), n.d.). For this reason, the proposal for a regulation to establish a centralized ECRIS for third-country nationals (ECRIS-TCN) was presented, expected to be operational in 2022 (other sources mention 2020/2021). In ECRIS-TCN, “[t]he existing procedure remains unchanged for decentralised exchanges of full conviction information on non-EU nationals, after the convicting EU country has been identified through the ECRIS-TCN system” (European Criminal Records Information System (ECRIS), n.d.). The identification of a traveller followed by a match with an ECRIS entry would raise the risk level of a traveller in the context of RBBM.

3.3.3.2 Passenger Name Record (PNR) systems

PNR data is provided by passengers to airlines when they book a flight or check-in for a flight and is stored in airlines’ reservation systems. It contains information such as the passenger’s name, travel dates, itinerary, ticket information, contact details, travel agent, means of payment, seat number and baggage information (New EU Rules on Passenger Name Record (PNR), 2018; Passenger Name Record (PNR), n.d.). The PNR Directive31, adopted in April 2016 regulates the data transfer to MS law enforcement authorities. Within two years, MS had to comply with the directive (Regulating the Use of Passenger Name Record (PNR) Data, 2020).

The processing of PNR data has to ensure full respect for data protection standards.\textsuperscript{32} EU MS are required to establish Passenger Information Units (PIUs) which have the following purposes (Passenger Name Record (PNR), n.d.):

- "Collect" the PNR data from air carriers
- Compare PNR data against relevant law enforcement databases & process them against pre-determined criteria, in order to identify persons that may be involved in a terrorist offence or serious crime.
- Disseminate PNR data to national competent authorities, Europol and PIUs of other Member States, either spontaneously or in response to duly reasoned requests."

### 3.3.3.3 Interpol Travel Documents Associated with Notices database (TDAWN)

This database extracts travel document identifiers from notices to enable authorised users to search them via a query with a Document Identification Number (DIN) of a travel or identity document. The purpose of TDAWN is to detect persons subject to Interpol notices by performing checks on associated travel documents (Di Carlo, n.d., p. 8). A match with a TDAWN entry would be an immediate red flag in the context of RBBM.

### 3.3.3.4 Europol Information System (EIS)

The Europol Information System (EIS)\textsuperscript{33} provides a centralised criminal information database for MS to store and query data on serious crime and terrorism. With Europol’s databases, law enforcement authorities from different countries can work together by identifying common investigations and providing the basis for strategic analysis (Information Exchange, n.d.). Its Secure Information Exchange Network Application (SIENA)\textsuperscript{34} allows an exchange of operational and strategic crime-related information in a swift, secure and user-friendly way among Europol liaison officers, analysts and experts, Member States and third parties with which Europol has cooperation agreements (Secure Information Exchange Network Application (SIENA), n.d.). This network could plausibly also be used for the exchange of risk-based concepts in the context of RBBM.

### 3.3.3.5 European Information Exchange Model (EIXM)

The European Information Exchange Model (EIXM) was adopted in 2012 by the European Commission. Its purpose was to “[...] take stock of the EU information exchanges landscape and recommend [...] concrete steps on how to increase the efficiency and improve the application of existing cooperation instruments” (European Information Exchange Model (EIXM), n.d.). The Prüm Decision (2008/615/JHA) and the Swedish Initiative (2006/960/JHA) are the main legal instruments covered by EIXM. The first (Prüm Decision) states rules for operational police cooperation and introduced procedures for efficient data exchange. It lays down the provisions under which EU MS grant each other access to DNA analysis files, fingerprint identification systems (“hit/no-hit” approach) and vehicle registration data (national

---


\textsuperscript{33} For more information see https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

\textsuperscript{34} For more information see https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena
platforms linked to “EUCARIS”\(^{35}\). The latter instrument under the EIXM, the Swedish initiative, provides a legal framework for the “effective and expeditious exchange of existing information and criminal intelligence between EU Member States' law enforcement authorities” (European Information Exchange Model (EIXM), n.d.). Such established models can arguably facilitate RBBM information exchange through trust building.

3.3.1 **CISE and EUCISE2020**

The purpose of CISE\(^{36}\), an EU initiative, is to make European and EU / European Economic Area (EEA) MS surveillance systems interoperable to provide all concerned authorities from different sectors with access to the classified and unclassified information they need in order to conduct missions at sea (Common Information Sharing Environment (CISE), n.d.). The Maritime CISE is based on five key principles (CISE Architecture, n.d., p. 1):

- CISE connects public authorities in the EU and EEA responsible for maritime surveillance: civil and military, regional/sectorial organisations and EU agencies.
- CISE connects existing maritime surveillance systems.
- CISE promotes a sector-neutral solution: all sectors and systems are important.
- CISE follows a decentralised approach: point-to-point exchange of information.
- Information exchange is voluntary, i.e., not enforced by legislation.

CISE aims at increasing the efficiency and effectiveness of maritime surveillance and it should “address the current legal, technical and cultural barriers in the sharing of maritime data to allow the sharing of available information across the seven [...] User Communities throughout the EU/EEA” (Mendes & Fontaine, 2013, p. iii). Among the seven User Communities mentioned are besides communities in the maritime domain (4) the customs, (5) border control, (6) general law enforcement and (7) defence. With CISE automated exchange of structured information should be facilitated, with information sharing organized in a decentralized manner and built upon User Community systems.

EU CISE 2020 was a security research project under the European Seventh Framework Programme with the aim of pre-operational information sharing between maritime authorities of European states (EUCISE2020, n.d.). Information sharing across seven relevant sectors / user communities (transport, environmental protection, fisheries control, border control, general law enforcement, customs and defence) based on existing and future surveillance systems was to be supported through political, organisational and legal environment creation. A fully operational European Common Information Sharing Environment (CISE) was to follow\(^{37}\). The EUCISE2020 data model consists of seven core data entities (Figure 3-4) (Agent, Object, Location, Document, Event, Risk and Period) and eleven auxiliary ones (Vessel, Cargo, OperationalAsset, Person, Organization, Movement, Incident, Anomaly, Action, UniquelIdentifier and Metadata), which together represent the information exchanged.

---


\(^{36}\) Implemented by the European Maritime Safety Agency (EMSA), for more information see [http://www.emsa.europa.eu/cise.html](http://www.emsa.europa.eu/cise.html)

The EUCISE2020 data model serves as a valuable reference point for data models in the context of RBBM information exchange.

### 3.3.2 Interoperability in the EU

An EU interoperability framework was proposed for the area of border management with the following objectives (Commission Staff Working Document on Establishing a Framework for Interoperability between EU Information Systems, 2017, p. 1):

- Ensuring that end-users have fast, seamless, systematic and controlled access to the information they need to perform their tasks
- Providing a solution to detect multiple identities linked to the same set of biometric data (with the purpose of facilitating identity checks for bona fide travellers and combating identity fraud)
- Facilitating identity checks of third-country nationals on the territory of a MS by authorised officers
- Facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems at EU level where necessary for the prevention, investigation, detection or prosecution of serious crime and terrorism

Thus, the overall interoperability solution was designed as follows\(^\text{38}\) (Figure 3-5):

---

The European Search Portal (ESP) is intended to facilitate the simultaneous query of multiple systems (SIS, Eurodac, VIS, EES, ETIAS, ECRIS-TCN, Interpol Systems and Europol data) via identity data. The ESP does neither process new data nor store any data, but it would query the various systems and return information to which the user has access. With the ESP, the correct and authorised use of each of the existing EU information systems is to be facilitated. The shared Biometric Matching Service (BMS) enables the querying and comparison of biometric data from the central systems (Proposal for a Regulation of the European Parliament and the Council on Establishing a Framework for Interoperability between EU Information Systems (Police and Judicial Cooperation, Asylum and Migration), 2017).

The use of ESP in combination with API and PNR information from PIUs would plausibly form the initial input set for traveller risk assessment within RBBM.

3.3.3 Challenges of international information exchange

If cooperation and coordination between all agencies involved in border control and state border protection can be enhanced, oversight of EU borders can be handled more effectively and efficiently. However, there are some challenges to cooperation and coordination between EU MS that need to be considered. First, the institutional set-up is not the same in all MS. While in some, there are specialised border guard and customs organisations, others provide the police or coast guards with border guard competencies, or the gendarmerie with customs and law-enforcement duties (Practices and Forms of Cooperation between Customs and Border Guards in the European Union, 2011). Competencies of the border guard or customs authorities can also be different from one country to another and vary by type of BCP (land, sea, air) and agencies involved. Depending on that, a country’s location and incident experience, different agencies involved in border checks and border surveillance may have different levels of expertise and operational capacities. In some MS the customs or border guards do not have investigative powers, while “in others they might not have any maritime patrol competencies, or any competencies outside BCPs” (Practices and Forms of Cooperation between Customs and Border Guards in the European Union, 2011, p. 3). A last challenge is posed by the legislative basis varying in MS. While some have comprehensive legislation, others may rely on local or need-based agreements as well as possibly on informal cooperation (Practices and Forms of Cooperation between Customs and Border Guards in the European Union, 2011, p. 3).

Border guards and customs are two central services in charge of border control. Even though common standards for the management of EU external borders have been developing, each MS has the competence to define the forms and range of cooperation between border guard authorities and customs authorities. As a result, some countries have established good institutional cooperation and even merged the two institutions (such as the UK), but in others the relations between the two have been “characterized by either strict division of missions and functions or even in certain cases by distrust, competition and lack of communication” (Practices and Forms of Cooperation between Customs and Border Guards in the European Union, 2011, p. 2).

As regards the transfer of personal data to recipients outside the EU, Regulation EU 2018/1725 applies. According to this regulation “international transfers may take place when there is an adequate level of protection to the fundamental right of individuals (data

---

39 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)
subjects) to data protection. Adequacy assessments may be carried out by those wishing to transfer data outside the EEA themselves, or by the European Commission” (International Transfers, n.d.). However, information cannot be exchanged outside the EEA without any adequacy decisions or appropriate safeguards in place. Furthermore, even within the EEA, not all countries are connected to all existing information sharing systems and these systems are in turn not all interconnected with each other.

3.4 RBBM information collection across travel modalities

In addition to the information gathered from existing information systems discussed above, RBBM involves additional information to assess traveller risk as discussed in chapter 3.1. Some risk indicators can be constructed from the direct observation of aspects of the traveller upon arrival at the BCP, such as the ones related to what they carry with them (D1.2, p 54). Behaviour detection is another important input for risk profiling (D1.2, p. 57). Predefined behavioural patterns of a traveller could be detected and used for risk evaluation. Other indicators cannot be directly observed, such as indicators related to intent or knowledge. This requires indirect assessment methods based on the observation of related aspects. Plausible intent could potentially be derived e.g. from a check of a traveller’s online presence (D1.2, p 70). Naturally, this requires additional technology, processes and training to collect and interpret the data.

Travel across air, land and sea modalities currently involves different data gathering practices and technologies that could be used to address the concept of risk assessment based on traveller data. From a global perspective, travel can be seen as a continuum, as the same traveller can be in different phases of his journey at the same time when the perspectives of the countries of origin and destination are combined. A traveller in the exit phase from one country is usually simultaneously at the pre-arrival phase of another. Thus, travel is an interdependent system requiring cooperation and information exchange between countries, airlines and further stakeholders (ICAO TRIP Guide on Border Control Management, 2018, p. 12).

3.4.1 Traveller journey via air

Typically, information about travellers (and crew) and their journeys is available to countries before a traveller starts their trip via airplane. A continuous traveller risk assessment can allow states to prevent a traveller from commencing or continuing a journey, conditional on the ability to identify a traveller at a given point throughout their journey. Figure 3-6 illustrates the phases of an air travellers’ journey from the perspective of a destination country, namely pre-departure, pre-arrival, entry, stay and exit. The row marked by the blue arrow shows which tools are available to states to assess traveller information.

---

In national border control systems, various systems, tools and applications (most of which have been described in chapter 3.3.) are currently in use that can support identification and risk assessment across the different travel phases in addition to biographic identity verification (ICAO TRIP Guide on Border Control Management, 2018, p. 21):

- Document readers, Electronic Machine Readable Travel Document (eMRTD) identity verification\(^{41}\), ICAO Public Key Directory (PKD)\(^{42}\)
- National watch lists, international watch lists
- Interpol Stolen and Lost Travel Documents (SLTD) database
- Biometric identity verification

The following systems, tools and applications are applied at specific phases of the traveller journey in addition to liaison officers and primary and secondary examination:

- Pre-departure phase: Visa and Electronic Travel Systems (ETS), Registered Traveller Programmes (RTP), Passenger Name Records (PNR)
- Pre-arrival phase: Advance Passenger Information (API), Interactive Advance Passenger Information (iAPI)
- Entry and exit phases: Entry & exit databases, Automated Border Controls (ABC)

\(^{41}\) See also: [https://www.icao.int/meetings/tag-mrtd/tagmrtd22/tag-mrtd-22_wp24.pdf](https://www.icao.int/meetings/tag-mrtd/tagmrtd22/tag-mrtd-22_wp24.pdf)

\(^{42}\) Public Key Directory: a central repository for exchanging the information required to authenticate ePassports.
See also: [https://www.icao.int/Meetings/TRIP-Symposium-2017/Presentations/Arnaldo%20Cremisini.ICAO-PKD%20Workshop%20Requirements%20Challenges%20Opportunities-final.pdf](https://www.icao.int/Meetings/TRIP-Symposium-2017/Presentations/Arnaldo%20Cremisini.ICAO-PKD%20Workshop%20Requirements%20Challenges%20Opportunities-final.pdf) and [https://www.icao.int/Security/FAL/PKD/Pages/default.aspx](https://www.icao.int/Security/FAL/PKD/Pages/default.aspx)
3.4.1.1 Information on luggage

Luggage that gets checked in is tagged according to messaging standards that have been in place since 1985, with the International Air Transport Association (IATA) Modern Baggage Messaging project working towards a new, sustainable standard for messaging in the area of baggage. A roadmap has been proposed for transitioning the industry towards an XML-based standard under the Airline Industry Data Model (AIDM) over the next few years, including updated luggage security information. As Error! Reference source not found. Figure 3-7 shows, passenger and luggage information along with security screening information is envisioned to be featured, providing valuable risk assessment inputs across the traveller journey.

![Diagram of Bag Logistics Taxonomy of Terms within Events from IATA AIDM]

3.4.2 Traveller journey via land

Pre-enrolment for land travel is more challenging than for air travel, as the ways a land border can be crossed are substantially more diverse (on foot, by car, by coach, by train). The pre-enrolment could be done by means of an application available on a mobile device or a website, allowing the traveller to submit personal and vehicle information in advance (eu-LISA, 2019),

---

43 For more information see: https://www.iata.org/en/programs/ops-infra/baggage/baggagemessaging/#tab-1
44 For more information see: https://airtechzone.iata.org/industry-programs/aidm/#about
45 For more information see: https://www.iata.org/contentassets/6bb095b194bc4ebf851ed73c83266c20/modern-baggage-messaging-roadmap.pdf
as is done within the TRESSPASS project. Other possible approaches for pre-enrolment include:

- For pedestrians: Pre-registration desks/kiosks, Automated Border Control (ABC), Self-Service Systems
- For cars (including lorries/trucks): Pre-registration desk, mobile enrolment (border guard going up the queue of vehicles doing the verification/enrolment)

Additional data can be captured by different devices at the pre-enrolment stage or at the BCP entrance, namely via:

- Terminal devices (document readers, cameras, sensors)
- Access to web services from external systems (SMILE, 2017)

### 3.4.3 Traveller journey via sea

A pre-enrolment phase serving to extract passenger and crew information in advance is already partially established for the sea travel journey for commercial sea transport. Border management is currently being provided with passenger and crew lists obtained by the ship operator before arrival.\(^{46}\) The embarking/disembarking of travellers coming via ship (or boat) can be managed in a similar way as at a land border (using fixed or mobile equipment) depending on the available infrastructure (eu-LISA, 2019). The European PNR Directive (see chapter 3.3.3.2) does not exclude national collection and processing of PNR in additional transportation modes to air travel - if compatible with Union law and after an impact assessment regarding proportionality and necessity. This possibility has been used so far only by a few EU Member States and is still at an early stage of implementation.\(^{47}\) This information can serve as a central first risk assessment input.

### 3.5 Multi-national, multi-level and multi-stage RBBM information flow overview

In the following Table 3, an overview of information flows with relevance for RBBM is provided. It summarises what kind of information the different border management stakeholder levels receive from whom at what stage of a traveller journey, and why. Current challenges for such an information exchange are equally noted.

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Information Type</th>
<th>Sender</th>
<th>Time / Travel Stage</th>
<th>Reason</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU/National level policy entity</td>
<td>Risk-based concept inputs</td>
<td>Other EU/national level policy entity</td>
<td>Periodically</td>
<td>Collaboration on risk-based concept</td>
<td>Mandate, common understanding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>implementation</td>
<td></td>
</tr>
<tr>
<td>UE/National level policy entity</td>
<td>Threat and risk acceptance inputs</td>
<td>Other EU/national level policy entity</td>
<td>Periodically</td>
<td>Collaboration on risk-based concept</td>
<td>Risk appetite divergence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>implementation</td>
<td></td>
</tr>
</tbody>
</table>

\(^{46}\) For more information see: [http://www.imo.org/en/OurWork/Facilitation/FormsCertificates/Pages/Default.aspx](http://www.imo.org/en/OurWork/Facilitation/FormsCertificates/Pages/Default.aspx)

<table>
<thead>
<tr>
<th>Strategic level border management entity</th>
<th>Threat and risk acceptance inputs</th>
<th>Regular intervals</th>
<th>Aid in threat mitigation and residual risk achievement decision making</th>
<th>Mandate, common understanding</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU/national level policy entity</td>
<td>Definition of threats and risk acceptance</td>
<td>Precondition</td>
<td>Threat mitigation and residual risk achievement</td>
<td>Mandate, common understanding</td>
</tr>
<tr>
<td>Tactical level border management entity</td>
<td>Threat scenario and risk profile and indicator detail and trend inputs</td>
<td>Regular intervals</td>
<td>Aid to define, update and assess threats and risks</td>
<td>Mandate, common understanding</td>
</tr>
<tr>
<td>Strategic border management entity</td>
<td>Definition of threat scenarios, initial risk profiles and indicators and risk acceptance details</td>
<td>Precondition</td>
<td>Creating lists of risk indicators and thresholds specific for a BCP</td>
<td>Mandate, common understanding</td>
</tr>
<tr>
<td>Other tactical level border management entity</td>
<td>Threat scenario and risk profile and indicator detail and trend inputs</td>
<td>Periodically</td>
<td>Sharing risk profiles that have proven to be valuable</td>
<td>Mandate, common understanding</td>
</tr>
<tr>
<td>Other tactical level border management entity</td>
<td>BCP records of travellers and alerts</td>
<td>On demand</td>
<td>Cross-border collaboration</td>
<td>Mandate, data privacy, interoperability</td>
</tr>
<tr>
<td>Tactical level border management entity</td>
<td>Risk indicator lists, weights and decision rules</td>
<td>Precondition</td>
<td>Allowing for execution of risk-based screening and checks</td>
<td>Mandate, data privacy, interoperability</td>
</tr>
<tr>
<td>RBBM technology (sensors)</td>
<td>Behavioural indicators</td>
<td>Traveller approaching and at BCP</td>
<td>Risk assessment</td>
<td>Mandate, data privacy, interoperability</td>
</tr>
<tr>
<td>RBBM technology (e.g. Internet search)</td>
<td>Indicators of intent</td>
<td>Pre-travel, traveller approaching and at BCP</td>
<td>Risk assessment</td>
<td>Mandate, data privacy, interoperability</td>
</tr>
<tr>
<td>RBBM technology (pre-travel information)</td>
<td>Personal travel information</td>
<td>Pre-travel</td>
<td>Risk assessment</td>
<td>Mandate, data privacy, interoperability</td>
</tr>
<tr>
<td>Database providers</td>
<td>Information from existing information systems</td>
<td>Pre-travel, traveller approaching and at BCP</td>
<td>Risk assessment</td>
<td>Mandate, data privacy, interoperability</td>
</tr>
</tbody>
</table>

An example of RBBM information exchange with regards to a specific traveller could be described as follows: The traveller is assumed to be a US citizen and CEO of a multinational company with offices in Europe and a broad professional network on LinkedIn. They are a
trusted traveller as they travel to Europe approximately twice a month with a valid passport. Before they began their latest journey, a RBBM concept was established in the destination country in Europe and various risk profiles of mala fide and bona fide travellers specified by tactical border management.

In the pre-travel phase, their administrative assistant booked a business class ticket and the usual hotel at their destination city. The passenger information provided in advance accordingly indicates trusted traveller status, company booking and well-known hotel. A professional social media presence supports a bona fide profile. At the departure airport, the traveller arrives as late as possible and uses the priority lane for check-in and boarding. At the arrival airport, they equally know their way and quickly goes towards the basic e-gate check. Behaviour observation indicates confidence and straightforward movement trajectories and passenger information provided in advance further corroborates a bona fide profile.

The operational BCP management can use the information collected throughout the traveller journey to confirm low-risk traveller status and assign an accordingly minimal check. This process would be facilitated further if the departure BCP record was built using similar information as required by the arrival BCP and could be shared with it.
4 INFORMATION EXCHANGE WITHIN THE TRESSPASS CONCEPT

This chapter aims at describing central information flows within the TRESSPASS concept and how they address challenges presented within chapter 3. A discussion on the TRESSPASS pilots is presented as well.

4.1 Introduction of the TRESSPASS system

In the TRESSPASS concept, a number of technical solutions are proposed for deployment at risk-based BCPs. Their role is 1) to gather and combine information relevant for traveller risk assessment in the pre-travel, BCP approach and at BCP phases of a traveller’s journey, 2) provide a secure channel of vertical communication throughout the TRESSPASS system between the tactical and operational border management levels and 3) provide a secure channel of horizontal communication throughout the TRESSPASS system between different BCPs with information exchange services creating a decentralised information exchange network. The policy and strategic border management levels in turn stand to benefits from the availability of a unified tactical and operational RBBM approach. Following the TRESSPASS concept, each (EU) BCP that is part of the TRESSPASS system has solutions available, that are intended to offer enhanced situational awareness for border control practitioners as well as improved risk management coordination and cooperation. In the following chapters, information gathering and exchange within the TRESSPASS concept will be introduced together with the technical solutions that enable it.

It is crucial to note that each TRESSPASS user only has access to data in accordance with a) their authorisation level and b) the TRESSPASS system scope. Thus, while traveller BCP records and profiles along with risk information could be exchanged between TRESSPASS BCPs, information on risk-based concepts and residual risk will still need to be exchanged through different cooperation networks.

4.2 Information sources within the TRESSPASS system

In the following, we provide a brief overview of technical solutions created to gather information processed by the TRESSPASS RBBM system for risk evaluation, as indicated in Table 3: Overview of Multi-national, multi-level and multi-stage RBBM information flow) in chapter 3.5. This information includes pre-registration information, information from existing information systems as described in chapter 3.3 as well as behavioural indicators and indicators of intent.

The TRESSPASS Traveller Registration Application (TRA) provides traveller pre-registration using android and web applications. It enables travellers to enter their personal travel information and enrol in the TRESSPASS system for initial risk assessment.

The Legacy Systems Interface (LSI) is a technical component developed within TRESSPASS to gather data from existing information systems such as VIS, SIS II, PNR and EES (Chapter 3.3). PNR information (e.g. requested from Passenger Information Units (PIUs)) has an important role in the TRESSPASS RBBM concept in that it constitutes a first traveller risk assessment input where pre-registration by the traveller was not undertaken. LSI can be queried automatically (e.g. during passenger entry at BCP) or manually by border control staff. A query using the LSI component involves requesting information based on traveller identification data and a gateway that translates and queries the corresponding information systems, returning the information it receives back. The output of a search request is information used for the population of initial or added risk indicators.
The **Security Personnel Application (SPA)** is a mobile application that can be used by the operational level personnel in field in order to report back observed behaviour of travellers matching an elevated risk profile or other risk related information to the central BCP operation control.

The **Web Intelligence (WI)** component utilises open Internet sources, including social media, to contribute to the calculation of risk indicators.

**TRESSPASS Sensors**, finally, is a collective term for technical components that are installed in BCPs in order to gather information about behavioural indicators and indicators of intent of travellers. These sensors can have diverse functions and their use can and needs to be adjusted to conditions at each specific BCP and modality. The systems used in TRESSPASS span video tracking, real-time behaviour analysis, multi-modal communication analysis, thermal spoofing detection and a traveller and luggage tracking platform.

### 4.3 Vertical information exchange between stakeholders within the TRESSPASS concept

The TRESSPASS concept focuses on facilitating information exchange between the tactical and operational level. The communication with strategic and policy levels is carried out outside of the TRESSPASS technical system, but is a crucial RBBM prerequisite. Figure 4-1 presents an overview of different border management levels and the information they need to deal with to allow for risk assessments of travellers.

![Figure 4-1: Vertical information flow between stakeholders within the TRESSPASS concept](image)

On a national level, **definitions of threats and risk acceptance thresholds** need to be formulated first.

The strategic level in turn elaborates **threat scenarios for BCPs** (the so-called Design Basis Threat (DBT)), **initial risk indicators** (RI) per travel stage, the **required information sources** and **risk acceptance details**.

Risk elements of information include all information gathered by information sources in order to evaluate a traveller’s conformance with a risk profile (see chapters 3.1 and 4.2).

The tactical level at a given BCP management elaborates risk assessment inputs such as **specific RI lists and their weights** and **risk assessment decision rules** that are input into the
TRESSPASS system by configuring the Data Fusion & Analysis (DFA), Dynamic Risk Assessment System (DRAS) and Command & Control (C2) components.

The DFA is a TRESSPASS component that executes data fusion operations in order to allow for the incorporation of information from heterogeneous information sources for the calculation of RI values per traveller based on predefined RI configurations.

The DRAS is the TRESSPASS real-time risk assessment component that provides traveller risk assessments based on RI information it receives from DFA and predefined configurations.

The TRESSPASS C2 component finally serves operational management through overview visualisation and risk status insight on travellers based on DRAS inputs. It provides operators the functionality to monitor risk assessment results live and receive alerts when a risk threshold is exceeded.

The operational level uses the C2 component to aid in the application of rules for screening and checks based on the calculated risk per traveller.

It should be noted that it is the Distributed Messaging System (DMS) that primarily enables other TRESSPASS subsystems to exchange information (D3.8). The DMS enables TRESSPASS components to exchange information based on the publish-subscribe principle (chapter 2.4.3) based on topics that TRESSPASS components can use to consume or produce data. The DMS security relies on the following three principles (D5.1, p. 24):

- Encryption: Information producers and consumers exchange encrypted data.
- Authentication: All partners exchanging information through DMS need to be authenticated in order for their identity to be verified.
- Authorisation: DMS checks access control lists to determine whether or not a particular client is authorised to write or read some topic.

4.4 Horizontal information exchange between stakeholders using the TRESSPASS system

In the TRESSPASS system, two types of horizontal information exchange between organisations responsible for BCPs at tactical and operational level as seen in Figure 4-2 are supported. The first type is information exchange within EU BCPs and the second type is information exchange between EU BCPs and 3rd party (usually country) BCPs (D3.8).

A TRESSPASS system node (software and hardware) installed at an EU BCP is capable of exchanging risk-related information with TRESSPASS nodes at other EU BCPs (either in the
same or a different EU country). For this type of information exchange, the TRESSPASS International Alert System (IAS) is utilised and can support exchange of risk information related to travellers.

Communication between an EU member country and a (non-EU) third country is the second type of horizontal information exchange and is facilitated again by the IAS to enable a safe and secure information exchange. An addition to the previous type is the use of the TRESSPASS Light Client (TLC). In the TLC user interface, data about travellers (from third countries) can be entered and it can be selected with which EU BCPs the information should be shared. The TLC can be used in all travel phases and modalities (air, land and sea). In exchange, third country BCPs can equally receive data about threats and alerts via the TLC.

The TRESSPASS C2 component is the primary access point for BCP operation level control at EU BCPs featuring a front-end (GUI) web application and a back-end data flow application (Figure 4-3). The front-end web application serves operational management at EU BCPs not only to gain risk status insight on travellers, but also the functionality to send push notifications (e.g. security alerts) to TRESSPASS nodes at another EU MS BCPs via the IAS. The back-end of the C2 component is the main TRESSPASS data exchange enabler for EU BCPs, allowing front-end components to connect and consume information based on appropriate authorisation and authentication and also connecting to the DMS (chapter 4.3).

The IAS enables information exchange between TRESSPASS nodes, controlled through C2 in TRESSPASS nodes within EU MS and through TLC in 3rd countries (Figure 4-3). The information exchanged is input through web-based forms that C2 and TLC operators fill when creating alerts of various types. Within TRESSPASS, a common exchange protocol is defined and each node must comply with this protocol in order to be able to share risk-related information. The IAS provides authentication and authorisation over a secure channel (D5.1).

Typical workflows for the IAS would be a C2 operator reviewing the received risk-related information from another TRESSPASS node or in turn propagating risk-related information to a 3rd country (D5.1). Information is exchanged one-to-one between two BCPs, but an operator...
can select multiple BCPs to forward risk information to. Third country BCPs can communicate with TRESSPASS systems inside the (EU) TRESSPASS network but not directly with other third country BCPs.

4.5 Functional information exchange using the TRESSPASS system

The functional information exchange in TRESSPASS is graphically represented in Figure 4-4. As discussed above, BCPs taking part in TRESSPASS can exchange alerts and risk-related data on travellers via the IAS in one-to-one communication. Each TRESSPASS node has its own IAS application and is able to select one or multiple other parties to forward risk information to. Information exchange between two IAS systems can be mutual, so the connection between two IAS systems is depicted by a double-headed arrow.

![Figure 4-4: TRESSPASS Functional Information Exchange](image)

Operational level border management at EU BCPs work primarily via the interface of the C2 component. The C2 interface enables operators to monitor risk assessment results, receive alerts and additional observations reported by field personnel via the Security Personnel Application (SPA) and input alerts. An essential functionality of the C2 component is
information exchange with the IAS and DMS components. Via IAS the C2 component gathers information received from other BCPs and shares it with the operator or (the other way around) information gathered in C2 (from operator, DMS or third IAS system) can be transferred to other BCP’s C2 via the IAS.

The DMS enables communication between TRESSPASS information sources (chapter 4.2), Data Fusion & Analytics component (DFA), Dynamic Risk Assessment System (DRAS) and the C2 component, that presents data about individual traveller risks to the operational level. Traveller risk calculation displayed to operational level via C2 is a result of settings of DFA and DRAS predefined by the tactical level border management.

Third (non-European) countries can use the TLC in order to share and receive information via the IAS.

4.6 Benefits of the TRESSPASS information exchange architecture

As described in chapter 3.1, RBBM requires more types of information to be exchanged than rule-based decision making. The TRESSPASS information exchange architecture provides standardised information collection and exchange capabilities that can be leveraged along the different travel stages as e.g. described in the ICAO TRIP Guide on Border Control Management (chapter 3.4.1 Error! Reference source not found.) and in support of tactical information exchange and cooperation capabilities across BCPs (chapter 4.4 Error! Reference source not found.). The strategic and policy levels stand to benefit from such a standardisation of information exchange when discussing risk indicators per travel stage, required information sources and risk acceptance details (chapter 4.3).

Screening and checking of travellers using current and novel technologies can be leveraged to conduct more proportional checks for each traveller in accordance with their risk profile. The pre-travel and approaching BCP stages can leverage information from traveller pre-registration, existing databases and the Internet, and behavioural patterns can be observed in the BCP area. Within the TRESSPASS concept, a number of sensors can be utilised to observe and analyse traveller’s behaviour in the BCP and the gathered information analysed and compared against risk profiles and risk acceptance thresholds to support border guard decision making (chapter 4.2).

This architecture addresses important challenges of introducing the RBBM concept for BCPs with different institutional set-ups and different border guard and customs authorities by introducing a system that can be adapted to different requirements (chapter 3.3.3). It offers a RBBM approach that can be adapted to different needs and locations, using unified secure information exchange protocols to connect BCPs (Figure 4-4) run by different institutions and operators with different expertise in a streamlined manner.

4.7 Information exchange in TRESSPASS pilots

At this point it is important to note that during the TRESSPASS project no real data from border guards, customs or other law enforcement agencies will be exchanged. Instead, synthetic datasets simulating the structure of the real ones will be used. For the simulation of PIU functionality, the TravelDoc interface by ICTS (ICTS, 2020) will be used with synthetic data. In order for the TRESSPASS process of obtaining information about travellers to be fully compliant with current legal requirements regarding data protection and exchange, the

48 TravelDoc, developed by ICTS, is a software system that verifies passengers’ international travel documentation, including visa requirements. It checks documentation against travel restrictions imposed on a traveller.
processing of personal information within the pilots from volunteers needs to be justified appropriately. It needs to be transparent what data is processed about individuals by whom, how, and why (D1.4 p.97).

Some national legal provisions related to information exchange are covered in this section, with the interested reader being referred to D1.4 for further details. Furthermore, examples and motivation for research questions for the pilots are discussed with an emphasis on information exchange aspects.

4.7.1 Pilot in the Netherlands (air pilot)

Besides the GDPR, for the Netherlands the Dutch laws Wpg (Police Data Act)\textsuperscript{50} and Wiv (Intelligence and Security Services Act)\textsuperscript{51} are of relevance regarding the topic of information exchange. The Wpg is applicable when personal data is processed with regard to all the tasks noted in Article 4 of the Police Act\textsuperscript{52}, except the tasks being carried out under the Dutch Aliens Act\textsuperscript{53}. The following is excerpted from D1.4 (p. 70):

| The provision of police data to entities other than the police and the RNLM is regulated in Articles 16 to 24 of the Wpg. Data may be provided to, for example, members of the public prosecution service, mayors, the Chief of Police, the Board of Procurators General, the Minister of Security and Justice or the Minister of Defense\textsuperscript{54} (Article 16). International bodies, criminal courts, authorities responsible for carrying out police tasks in Europe, as well as third countries may be provided with data for the purposes of prevention, control, investigation and prosecution of serious crime (Articles 15a and 17a). However, an adequate level of protection for data processing must be ensured by the receiving parties. Furthermore, data may be shared with third parties structurally or incidentally for the purposes of prevention and detection of criminal offences; maintaining public order; providing assistance and supervising compliance with regulations (Articles 18 and 19).

Within the framework of information-led or risk-based border management, information exchange thus would take place between border police organisations and intelligence services, such as the General Intelligence and Security Service. However, the specific legal obligations and restrictions of the respective laws have to be taken into account.

The air pilot is addressing the challenges of improving BCP throughput without reducing border control effectiveness and increasing digitalization of the border control process. Expected impacts cover maintained or increased border control effectiveness, enhanced border guard decision making, reduced false positive rate and faster and more comfortable journeys for bona fide travellers.\textsuperscript{55}

\textsuperscript{49} Available here: https://www.tresspass.eu/sites/default/files/publications/public/TRESSPASS%20D1.4%20%20Analysis%20of%20the%20legal%20and%20regulatory%20framework.pdf

\textsuperscript{50} Police Data Act. For more information see: https://www.ns.nl/en/privacy/law-on-policedata.html

\textsuperscript{51} Law on intelligence and security services 2017. For more information see: https://pilpnjcm.nl/en/dossiers/bill-intelligence-security-services-act-wiv/

\textsuperscript{52} Police Act 2012. For more information see: https://wetten.overheid.nl/BWBR0031788/2018-09-19#Hoofdstuk2


\textsuperscript{54} the Chief of Police, the Board of Procurators General, the Minister of Security and Justice or the Minister of Defense

\textsuperscript{55} See TRESSPASS website and first newsletter: https://www.tresspass.eu/
The following types of questions will have to be addressed in the context of information exchange accordingly:

› Can border control effectiveness be increased by combining on-site traveller behaviour information with advance travel information like PNR records in the face of fluctuations in the availability and quality of incoming information?

› Can border guard decision making be enhanced through focusing on (changes in) risk categories of travellers arising from continuous information updates over rule execution?

› Can the false positive rate of the BCP be reduced through risk-based classification of travellers as matching bona fide profiles by leveraging multiple existing information sources in combination with behaviour observation?

4.7.2 Pilot in Poland (land pilot)

As for the use case Poland, Article 13 of the Polish Act on foreigners states the kind of data and information concerning a foreigner that may be processed in registers kept under the Act on foreigners (summarised):

name(s) and surname(s); sex; parents name; date, place and country of birth; height in centimetres, colour of the eyes, distinctive features; fingerprints; citizenship, nationality; marital status; education, occupation; national identification number, number of the travel document; identification of the entity ensuring the performance of work; place of residence or stay; phone number, email address; information on criminal records etc.; identification number in the Universal Electronic System for Registration of the Population (PESEL); image of the face; information about residing in the territory of another EU Member State for at least 18 months on the basis of a residence permit issued by that state with an annotation (“EU Blue Card”); data of a host.

As elaborated in D1.4, Regulation OJ 1990 “USTA AWA” about the Border Guard specifies tasks and duties of the Polish Border Guard. Concerning the collection and procession of personal data, border guards may collect and use the following kind of data (Article 10a):

“fingerprints, photographs and personal data for detection and identification purposes, including revealing ethnic origin, religious affiliation and data on health status, people suspected of committing offenses prosecuted against public prosecution, (...) without the consent and knowledge of the data subject”.

D1.4 further specifies the following terms (p. 74):

The data, except for data revealing ethnic origin or religious affiliation has to be kept for a period necessary for the Border Guard to perform statutory tasks and have to be verified at least every 10 years. The Border Guard has direct access to view information on wanted persons, and supplementary information provided by the Police on request (Article 10aa), and can further obtain data which does not constitute content such as telecommunications, postal items etc. (Article 10b).

The land pilot is addressing the challenges of high traffic volumes coupled with evolving cross-border smuggling patterns, document forgery and customs control bottlenecks. Expected

---

57 Polish legislation, obtained by end-user Poland: OJ 1990 No. 78 item 462, “USTA AWA” of October 12, 1990 about the Border Guard
58 Particular rules apply regarding the storage of personal data revealing the ethnic origin or religious affiliation of persons suspected or convicted of committing offenses prosecuted from public prosecution (Article 10a(4, 5)).
impacts cover reliable detection of cross-border smuggling and document forgery, increased capacity and throughput through higher efficiency and facilitated customs control.  

The following types of questions will have to be addressed in the context of information exchange accordingly:

› Can cross-border smuggling and document forgery detection be reliably improved through risk-based checks leveraging multiple information sources and third country collaboration?
› Can resource use efficiency and throughput be improved through classification of travellers in risk categories on the basis of combined information from multiple information sources?
› Can customs checks be substantially sped up through a joint information sharing approach with border control?

4.7.3 Pilot in Greece (sea pilot)

For Greece, Law 4251/2014 (as amended by Law 4232/2015) applies for the topic of personal data collection. However, it does not specify which kind of personal data is collected before or upon crossing the Greek border. In specific cases, personal data such as name, date of birth and passport number are collected (e.g. when hiring third-country nationals for employment, Article 14). Personal data of third-country nationals who reside in Greece are recorded and processed, however the legislation does not specify which kind of data (Article 133). Regulation (EC) No 810/2009 (Visa Code) stipulates in Articles 13 and 14 which personal data are required before crossing the Greek borders.

The sea pilot is addressing the challenges of parallel servicing of embarking and disembarking passengers on a multitude of vessels, direction of non-Schengen arrivals through enhanced infrastructure and facilities and appropriate border control for a large number of cruise passengers. The expected impacts cover better infrastructure and facility use for port operators and border authorities, increased capacity and throughput through higher efficiency and a delay-free cruise passenger processing.

The following types of questions will have to be addressed in the context of information exchange accordingly:

› Can border control effectiveness be maintained and resource use efficiency and throughput be improved by focusing on cruise passenger facilitation based on low-risk profile matching?
› Can maritime PNR provide a common operating picture based on a shared risk-based screening among all involved authorities?
› Can fast border crossing using TRESSPASS on-the-move identification and verification technology within the logic of non-disruptive no-gate border crossing be realised?
› Can the novel technologies and processes be integrated within the current processes compliant with the Schengen Borders Code and data privacy and protection issues taken adequately into account?

59 See TRESSPASS website and first newsletter: https://www.tresspass.eu/
60 Law 4251/2014 Government Gazette 80 / A / 01.04.2014. Immigration and Social Integration Code and other provisions
62 See TRESSPASS website and first newsletter: https://www.tresspass.eu/
5 CONCLUSION

A central aspect of RBBM is screening of travellers in support of risk assessments that allow for more proportional checks for each traveller. RBBM requires threat definition and residual risk acceptance on a (inter-)national policy level to be followed by national strategic formulations of threat scenarios, associated risk profiles and risk indicators (chapter 3.1). An important pre-condition for RBBM is information exchange at various management levels between all involved organisations, which can be considered as one of the core principles of RBBM. General risk-based concepts, residual risk acceptance, distinguishing features between illegitimate and legitimate travellers as well as information on a traveller’s passage through a BCP become central information units to be exchanged (chapter 3.5).

The TRESSPASS information exchange approach presented in chapter 4 describes how information exchange and interoperability on a tactical (where command, control and coordination at BCPs takes place) and operational level (where border control is effectively executed) can be realised. TRESSPASS builds upon existing information exchange structures (chapter 3.3.1) and adds the ability to exchange information with relevance for traveller risk assessment between BCPs in Europe and even third country BCPs within a specified exchange protocol. Central features are rigorous authentication and authorisation schemes that give users access only to information that they are authorised to see, while adhering to privacy by design principles. While the TRESSPASS system does not directly provide functionalities for the policy and strategic levels (chapter 4.3), inputs from and to these levels are essential for the realisation of RBBM and a substantial benefit can arguably be expected from the realisation of a standardised tactical and operational RBBM framework like the one proposed by TRESSPASS. Maintaining integrity and public trust in the risk-based mechanisms will be a crucial element to that end.

Information gathering and exchange developed within the TRESSPASS project is currently challenged by the legislative basis varying in different EU states. While some have comprehensive legislation, others may rely on local or need-based agreements as well as possibly on informal cooperation (Practices and Forms of Cooperation between Customs and Border Guards in the European Union, 2011, p. 3). Currently, information is not allowed to be exchanged outside the EEA if there are no adequacy decisions or appropriate safeguards in place. Even within the EEA, not all countries are connected to all existing information sharing systems (chapter 3.3.3). As part of increasing interoperability on the EU level, it is planned to establish the European Search Portal (ESP) that enables to search various information systems simultaneously (3.3.2). Such possibility could be leveraged by TRESSPASS (chapter 4.2).

However, extensive legislative changes at the EU level will have to occur to facilitate true multi-level, multi-stage and multi-national RBBM collaboration (chapter 3.5). A relaxation of requirements to apply the same minimum checks to all travellers will be needed, conditional on checks being executed in correspondence with clearly defined risk profiles addressing agreed upon threat scenarios and supported by active risk acceptance. More extensive traveller screening and associated cross-border and cross-agency information exchange will be necessary to support the verification of traveller matching against risk profiles. These changes will have to be justified, at the minimum, through positive answers to central research questions addressed by the TRESSPASS pilots (chapter 4.7) and to stand on rigorous and transparent ethical foundations as described by deliverables from TRESSPASS WP9 - Ethics and Data Protection.
# References


Eurodac: European system for the comparison of fingerprints of asylum applicants. (n.d.).
D2.5 Multinational risk based cooperation

Retrieved April 21, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A2A30105_1


**TRESSPASS deliverables:**
- D1.2 Risk-based border management concept
- D1.4 Analysis of the legal and regulatory framework
- D2.1 Method for Design Basis Threat
- D2.3 Risk assessment methods
- D3.7 Interfaces to external systems
- D3.8 Exchange Service Model
- D5.1 System Architecture
LIST OF FIGURES

Figure 2-1: Basic information exchange ........................................................................................................... 16
Figure 2-2: Pull pattern of information exchange (CISE Architecture, n.d., p. 1) ......................... 17
Figure 2-3: Pull unknown pattern of information exchange (CISE Architecture, n.d., p. 2) .... 17
Figure 2-4: Push pattern of information exchange (CISE Architecture, n.d., p. 2) .................. 17
Figure 2-5: Push unknown pattern of information exchange (CISE Architecture, n.d., p. 2) .. 17
Figure 2-6: Publish/subscribe pattern of information exchange (CISE Architecture, n.d., p. 2) ........................................................................................................................................ 18
Figure 3-1: Risk-based border management approach at BCPs (D2.3, p. 9) ...................... 20
Figure 3-2: Schematic overview of public stakeholders and their relations (D1.2, p. 18) ...... 21
Figure 3-3: Schematic overview of the main information systems for border management and law enforcement (European Commission, 2016, p. 6) .......................................................................................................................... 23
Figure 3-4: EUCISE2020 Data Model core data entities (ANNEX B: EUCISE2020 Data Model, n.d., p. 3) ........................................................................................................................................ 31
Figure 3-5: Proposal for EU interoperability framework (Proposal for a Regulation of the European Parliament and the Council on Establishing a Framework for Interoperability between EU Information Systems (Police and Judicial Cooperation, Asylum and Migration), 2017) ........................................................................................................................................ 31
Figure 3-6: Phases of the traveller journey (ICAO TRIP Guide on Border Control Management, 2018, p. 21) ........................................................................................................................................ 34
Figure 3-7: Bag Logistics Taxonomy of Terms within Events from IATA AIDM ...................... 35
Figure 4-1: Vertical information flow between stakeholders within the TRESSPASS concept 40
Figure 4-2: TRESSPASS Data exchange scheme .......................................................................................... 41
Figure 4-3: Information exchange via IAS for TRESSPASS systems at different BCPs using a secure protocol ........................................................................................................................................ 42
Figure 4-4: TRESSPASS Functional Information Exchange ........................................................................ 43
LIST OF TABLES

Table 1: Search keywords.................................................................................................................. 9
Table 2: Who can access which database? (“EU INFORMATION SYSTEMS SECURITY AND BORDERS,” 2019) .................................................................................................................. 24
Table 3: Overview of Multi-national, multi-level and multi-stage RBBM information flows.. 36