 2020

H2020 – BES – 5 – 2015

Research Innovation Action

Intelligent Portable Control System

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626

D4.2 Second version of the iBorderCtrl software platform

Report Identifier:	D4.2 Second version of the iBorderCtrl software platform		
Work-package, Task:	WP4	**Status – Version:**	V1.00
Distribution Security:	CO	**Deliverable Type:**	R
Editor:	ED		
Contributors:	STR		
Reviewers:	ICCS, STR		
Quality Reviewer:	ED		
Keywords:	Software, Development, Prototype		
Project website: www.iborderctrl.eu			

Table of Contents

List of Tables

List of Figures

Abbreviations

BCAT	Border Control Analytics Tool
BGUA	Border Guard User Application
BMUA	Border Manager User Application
EES	Entry/Exit System
ELSI	External Legacy and Social Interfaces
RBAT	Risk Based Assessment Tool
SIS	Schengen Information System
TUA	Traveller User Application
UMF	Universal Messaging Format
VIS	Visa Information System
WP	Work Package

Executive Summary

In this deliverable the final and complete versions of the individual components of the iBorderCtrl software platform are presented as the conclusion of WP4. This deliverable submitted at month 24 follows the delivery of D4.1: First version of the iBorderCtrl software platform, delivered at month 18 that presented the on-going progress of the Development of the iBorderCtrl software platform and related interfaces.

The three main iBorderCtrl software tools namely the Risk Based Assessment Tool (RBAT), the External Legacy and Social Interfaces (ELSI) and the Border Control Analytics Tool (BCAT) and their final functionalities are presented in the deliverable. For each sub-system, a technical description overview is provided including a brief description of the final system and deviations from the functionality presented in D4.1 (if any). Moreover, further information on the risk score calculation and the criteria and methodology used per subsystem is provided. The final functionality of each subsystem using respective descriptions and/or screenshots is explained while additional implementation details, code or GitHub actions (where applicable) are provided. In addition some performance test results are apposed to show/measure the readiness level, the subsystem performance, the results and outcomes of the development and implementation including exemptions, experiments and respective metrics.

It should be noted that in the present deliverable, the three user interfaces, namely the Traveller User Interface, the Border Guard User Interface and the Border Manager User Interface are not included in order to avoid repetitions as they were thoroughly described in D4.1 with a focus on the graphical implementation with screenshots of the current versions and implementation details. However, the respective iBorderCtrl user applications (Traveller User Application (TUA), Border Guard User Application (BGUA) and Border Manager User Application (MBUA)) are thoroughly presented in D5.2: Early version of the integrated prototype (limited functionality) demonstrating at the same time the integration of the applications under the iBorderCtrl platform.

1 Introduction

The final versions of the major software systems developed in iBorderCtrl are presented in this deliverable; these are the RBAT, ELSI and BCAT modules. Each sub-system is presented in terms of final technology functionalities. Furthermore additional information are included per sub-system, such as the risk scores calculation methodology, additional implementation details (code, available services) and performance test results.

The functionality of RBAT is presented through screenshots and explanations demonstrating how the Border Managers would interact with in order to take advantage of the full functionality that RBAT has to offer. This very detailed analysis could be used as a user manual facilitating the familiarization of Border Managers (non-experts) with the tool.

A technical description overview is presented for ELSI. A detailed explanation of how legacy databases (SIS, VIS and EES) and which fields exactly are going to be utilised in the risk score calculation is also included.

BCAT is presented through respective screenshots as a scientific workflow that will perform the meta-analyses of collected data. BCAT enables the combinatorial analyses of all data collected in iBorderCtrl database utilizing statistical, machine learning and data mining approaches to discover new patterns and knowledge that can be used through the RBAT tool to enhance the performance of the system. Furthermore, the tool will be used to evaluate all modules in iBorderCtrl through the analyses of data collected as part of the pilot phase.

2 Risk Based Assessment Tool (RBAT)

2.1 Technical description overview

RBAT is designed to cover the necessity of calculating and managing traveller related risks in the Border check procedure in an easy and effective way. Its goal is to provide a robust, user friendly and flexible tool in order to support the decision making process of the Border Authorities.

RBAT will be accessible from the Border Manager User Application and will offer additional functionality to the Border Managers. The Border Managers will be able to author rules using RBAT's rule authoring environment. A rule allows the Border Managers to perform complex queries with specific criteria combining information from:

a. Law Enforcement Agencies directives such as Europol, FRONTEX, etc.
b. black lists, wanted persons lists, missing persons lists (i.e. as the ones contained in SIS) etc.
c. identified risk patterns (outcomes of the BCAT module)

In case there is a match or a hit on the authored rules, RBAT will automatically produce risk indicators and provide suggestions to the border guards on the actions to be followed per case.

The risk indicators produced after the pre-registration phase will be available for (optional) evaluation by the Border Managers who can accept, reject or modify the risk indicators before they will be available to the border guards. The risk indicators produced during the border crossing phase will be available to the Border Guards (along with the pre-registration risk score and the overall risk score) to alert or notify them on the hit/match and assist their final decision on the admission approval or rejection.

The Risk Based Assessment Tool (RBAT) will calculate the pre-registration risk score for each traveller and the overall risk score.

The preregistration risk score for each traveller who has used TUA to register a new trip will be calculated based on:

a) the individual risk scores produced by other iBorderCtrl modules/tools during the pre-registration phase
b) the risk score from the latest trip of the same traveller (if available)

The overall risk score for each traveller crossing the borders will be calculated based on:

a) the individual risk scores produced by other iBorderCtrl modules/tools during the border crossing phase
b) the pre-registration risk score

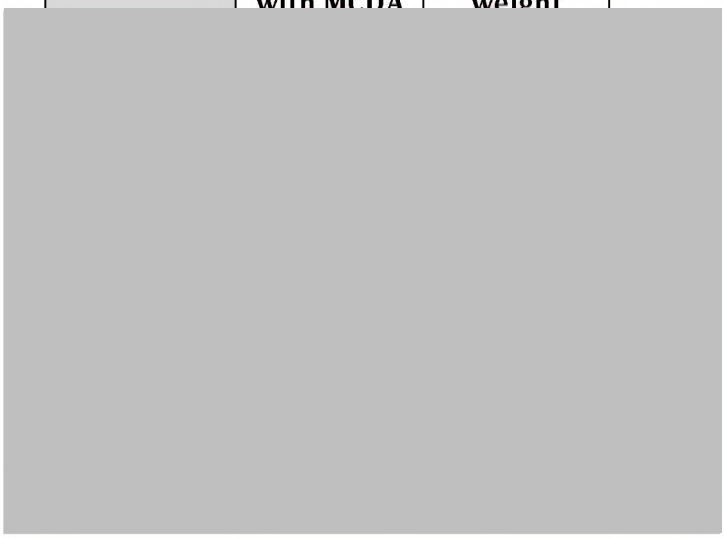
2.2 Risk calculation explanation

Based on the Multi Criteria Decision Analysis (MCDA) technique and the steps for the "weight" determination of each iBorderCtrl module that was described in detail in D4.2, the final weights per module and per phase (after normalisation) are shown in the tables below.

Table 1 Pre-registration Phase Module Weights

Table 2 Border Crossing Phase Module Weights

Border Crossing		
	Weight determined in D4.2 with MCDA	Normalised weight



In both phases, each tool is going to provide their own risk score in a range of 0-100 (value 0 represents 100% refusal to pass and value 100 represents 100% admission). In order to combine the weights and scores for each tool to derive an overall risk value, a weighted average of the risk score for each module will be calculated providing the total risk score.

Each module, except from the risk score, is going to provide some additional information to be presented to the Border Guard and could clarify the overall risk score calculated by RBAT. For example if the risk score is low (suggestion to deny entry), then the Border Guard should have all information available in order to understand the reason or the subsystem/s behind that low score (i.e. problem with the passport watermark, high deception detected, hit on a legacy database etc.). More specifically, in case that there is a very low value coming from DAAT, then the Border Guard will be able to see the area of the passport that was problematic and led to the low score: e.g. watermark on the bottom left side of passport was incorrect.

In the tables below, the additional information to be provided to the Border Guard by phase and per module along with specific examples are presented. It should be noted that in case that there is nothing important to be presented to the Border Guard, i.e. the passport was found genuine and the risk score is 100 no additional information will be included.

Pre-registration phase (PRE)	
	Additional information that might be of interest to the Border Guard and will be included in the json
DAAT	OCR results in case a problem is detected. For example: • *The first (or/and last) name entered in the Traveller User Application does not match the first (or/and last) name in the MRZ of the passport* • *The passport will not be valid throughout the duration of the trip because the expiration date is before the declared return date.*
FMT	There is no matching score between the person doing the interview and the registered traveller. For example: • *No face detected in the images sent from the interview* • *The quality of the images sent from the interview is not good enough* • *Is the first time the traveller uses the system*
RBAT	Risk indicators (hits from rules authored by the Border Managers). For example: • *The specific traveller has a vehicle with a suspicious license plate. Please check thoroughly for hidden humans* • *You should stop and thoroughly check this traveller because the destination country and last name match to a wanted person*
ELSI	Additional information regarding the legacy system hit or related to the social media account (twitter). For example: • *Name of the legacy system or DB that the hit was identified* • *The alert linked to the missing or wanted person* • *Posts on Twitter indicating illicit activity*
Border Crossing Phase (BCP)	
	Additional information that might be of interest to the Border Guard and will be included in the json
DAAT	a) Problematic area of passport (based on Regula validation results); for example: " *The watermark on the right upper corner of the passport is not correct*" b) HTML content that describes the passport security features; for example: *https://www.consilium.europa.eu/prado/en/GRC-AO-03003/index.html*
BIOF	In this case there is no relevant information beside the match / no match information. We have included the matching score as the risk, but for the border guards will be a yes or no (like they have already in their systems)
BIOPV	There will be no additional information included beside the match / no match information.
FMT	No further information beside the matching score in the three comparisons we made

HHD	There will be no additional information included beside the confirmation or not of hidden human detection.
RBAT	Risk indicators (hits from rules authored by the Border Managers): same as the ones in the table above

2.3 Final technology functionalities

In this section, the functionality of RBAT is going to be described through respective screenshots of the application. RBAT treats risk management as an interactive process in which information is continuously updated, analysed, acted upon and reviewed.

More specifically the RBAT module:

- Calculates the overall risk score of each traveller (Weight based risk calculation) taking into consideration a) the pre-registration phase risk, b) the individual risk scores provided by each module. It should be noted here that the pre-registration phase risk is calculated based a) on the individual risk scores provided by each module (that take part in the pre-registration phase and b) the overall risk score from the latest previous trip;
- Identifies and presents risk indicators that deserve further investigation stemming from the rules that the Border Managers have previously authored;
- Supports the decision making process of the Border Authorities;
- Provides all the necessary measures to limit the likelihood of risk occurring (Risk Indicators, Random Selection, Weight based risk calculation).

In summary, RBAT provides Border Authorities with strategies and structures to ensure that illegal crossings are kept to the minimum possible. RBAT not only promotes the ability of Border Authorities to detect high-risk cases, but also enables Border administrations to improve their controls along the land borders.

RBAT functionality can be summarised to the following:

- **Authoring:** A complete point and click graphical environment that allows the Border Manager to author rules through the use of structured, non-technical expression of logical interactions between the "Risk Objects» identifying Travellers that deserve further investigation
- **Evaluation:** Is the process of applying the rules onto incoming data (traveller data in an .xml form) to produce "Risk Indicators", together with the identified risks scores and a suggestion for further actions
- **Assessment:** Review of the Risk Indicators by the Border Managers, resulting in the final Risk Assessment
- **Optimization:** BCAT risk patterns identification leads to the authoring of new rules or improvements (optimisations) on the active ones

In the sections below the respective screens of RBAT are going to be presented along with the functionality per screen.

2.3.1 Monitoring screen

In the Monitoring screen the Border Manager is able to view the produced risk indicators based on the rules he/she has previously authored. The Border Manager may review (modify, delete, add comments) the risk indicators, resulting in the final ones that are going to be sent to the Border Guards to be taken into consideration for the final decision. It should be noted here, that the Border Manager can view and evaluate only the risk indicators produced from the pre-registration phase because

there is some time until the traveller reaches the borders. The risk indicators produced during the border crossing phase are automatically sent to the border guards (without review from the Border Managers as the Border Guard must take a direct decision for the traveller's admission or entry refusal).

The figure below presents an example of a list of produced risk indicators (hit/match from a previously authored rule) that the Border Manager has at his disposal for manual overview. The system displays the QR code number related to the risk indicator, the phase involved and an indication of the level of the risk for each category. These indications are available for possible manual interventions to all the Border Managers that have access to the specific result sets. The Border Manager may select a risk indicator, modify the proposed action and justify this alteration. The system provides a list of available physical controls and the Border Manager is able to suggest more than one type of physical controls for each result as it will be described in the next sections.

Figure 1 Monitoring screen

The final risk indicators derived either from the automated Risk evaluation process or from manual intervention by the Border Manager remain in the RBAT data repository and are communicated to the Border Guards. Certain parameters depict the time limit that the Border Manager has in order to complete the overview of the risk indicators (Timeout parameter) and the time that the risk indicators will be available to be communicated to the Border Guards during the border check (Risk timestamp parameter). By default RBAT will forward the results after the expiration of a dedicated and configurable time or right after the Border Manager's manual intervention.

RBAT supports the decision making process providing full access to the Border Manager to all risk related data (rules, dynamic registries, risk indicators, etc.). The Border Guards can view the risk indicators produced from the pre-registration phase (reviewed or not by the Border Managers) and the border crossing phase. RBAT keeps history of every change on the automatic results and the manual adjustments (tracking) on the risk indicators.

2.3.2 Rule Authoring screen

RBAT facilitates high level analysis by offering to the Border Managers a point and click graphical environment to author rules through the use of structured, non-technical expression of logical interactions between predefined "Risk objects" executing "what-if" scenarios. RBAT also provides the option to test new rules and criteria in real time without affecting RBAT's functionality by using the test category rules allowing the results to be available only for test purposes (described in section 2.3.5). The Border managers will be able to define Risk Categories, set rule conditions and rule actions.

The following figure presents the rule authoring environment. A rule expresses a query based on information that are available to the Border Manager such as a) directives received by Law Enforcement Agencies (e.g. Europol, FRONTEX, etc.), b) known lists (i.e. wanted, missing persons, black lists) and c) risk patterns that have been identified by BCAT. The rule expresses the proposed action (ACTION (Then) on the definition of the rule) when the declared conditions (CONDITIONS (If) on the definition of the rule) are fulfilled.

By unifying all these disparate data and information sources and by providing a simple interface to combine them, RBAT empowers the Border Manager and allows him to focus on the actual risk identification process rather than spending valuable time and resources on low level manipulation of data.

Figure 2 Rule Authoring screen

Below, the procedure to be followed in order to author a simple rule is presented in steps and an example is provided.

Figure 3 Rule Authoring screen: Specify Entity

For the specific rule example to be presented, let's assume that the Border Manager has selected the "Traveller" entity. As depicted in the Figure below RBAT displays a list of the available properties (risk objects/database fields) that have been assigned to the specific entity. The user can select any of the available properties (risk objects) and express any type of comparison (conditions).

Figure 4 Rule Authoring screen: Specify Entity Property

The authoring environment provides a wide array of logical operators and comparisons. The system recognises the data type of the loading data (i.e. string number etc.) providing the appropriate operators. RBAT also provides the ability to organise the rules into logical groups for efficient maintenance.

The Figure below presents the available conditional operators in order to perform a comparison (condition). The selected property is the "residence country" with data type "String" and RBAT adjusts the operator list showing only the operators related to this data type.

Figure 5 Rule Authoring screen: Specify Conditional Operator

In the figure below a simple rule example is presented:

Figure 6 Rule Authoring screen: Simple Rule example

More specifically, this rule checks if a Traveller exists who has:

a. declared as residence country the United Kingdom and
b. his first name is "James" and
c. a travel exists for this person with the declared origin country to be either Syria or Afghanistan and

Figure 7 Rule Authoring screen: Specify actions

Now that the conditions of the rule are set, the proposed actions in case of a match/hit should be defined. When a rule is triggered and the conditions are satisfied, the action that has been declared to the "ACTIONS (then)" part of the rule is added to the produced risk indicators. The part "ACTIONS (then)" is totally user defined as described in section 2.3.7.6.

Summarising, a rule expresses a query combining the input data and expresses the proposed action. If this rule fires the system produces a risk indicator and alerts the Border Guard based on the specified actions. In this specific example, if there is a hit/match then a risk indicator is produced with "red" severity (the highest one), the origin of this rule is specified (the traveller is black listed) and the proposed action is mentioned ("deny entry") as depicted in the figure above.

More complex rules can be authored based on the information and/or risk patterns available to the Border Manager. An example of a more complex rule in presented in the figure below.

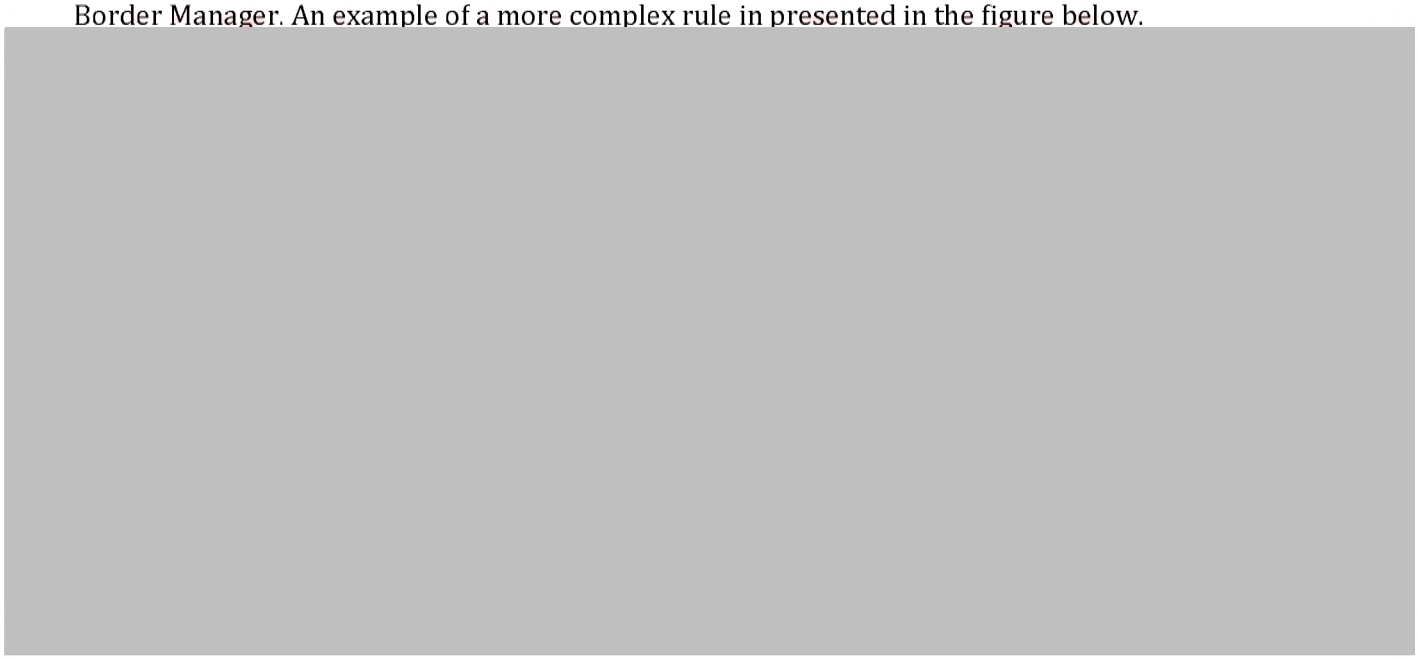


Figure 8 Rule Authoring screen: Complex rule example

This rule checks if a travel document exists having expiration date from 3 months after a specific date and 4 months before another specific date. If there is a hit/match then a risk indicator is produced with "red" severity (the highest one), the origin of this rule is specified (falsified document) and the proposed action is mentioned ("second line check") as depicted in the figure above.

2.3.3 Registry Management screen

Specific provisions have been made to accommodate often used data sources such as wanted or missing persons' lists contained for example in SIS database and similar intelligence related data. A flexible mechanism is provided to seamlessly integrate such data into the system.

The inherent dynamic nature of RBAT allows the on the fly definition of various data sources, e.g. Law Enforcement Agencies directives and the near instantaneous exploitation of them. The Border Manager by using Dynamic Registries as a flexible data structure combined with the ease in defining Rules, can turn information into rules at the moment they are known.

RBAT allows the definition of the Dynamic Registries through a user friendly and intuitive interface without the need for development support. Once a Dynamic Registry is created, it is available to be used in the Rule Authoring environment. Using the mechanisms of Dynamic Registries, it is possible

to integrate into RBAT any number of external ad-hoc or predefined parameters to be used throughout the Risk Assessment process.

The system provides a number of actions to support the operations of maintenance and administration of the Dynamic Registries. The Border Manager is able to add a new Dynamic Registry, edit or delete existing ones, copy/import/export the definition of the registries and manage their data.

The figure below presents the definition of a Dynamic Registry. The Border Manager creates a new Dynamic Registry, called "Wanted Persons list" which has the columns that are necessary to store the desired information, such as name, surname, country, address. The system provides the ability to define any constraint that needs to be checked during the loading of the data for the declared registry. For example the Border Manager is able to define that a column of the registry has to be unique. The system during the loading of the data for the specific registry, checks the uniqueness of the column and does not allow duplications. The logs about the handing of the data are available to the Border Manager with detailed information regarding how many records have been processed successfully, how many records have failed to load and the reason of failure.

External data sources can be easily accommodated through the provided functionality of importing arbitrary excel files which can be manipulated on the fly and incorporated into RBAT at real time. This means that the information from external legacy systems or urgent directives can be automatically translated as rules through the dynamic registries functionality.

The Border Manager has full access on the Dynamic Registries and their data. The system allows the actions of edit, delete, copy or export both for the definitions of the registries and their data.

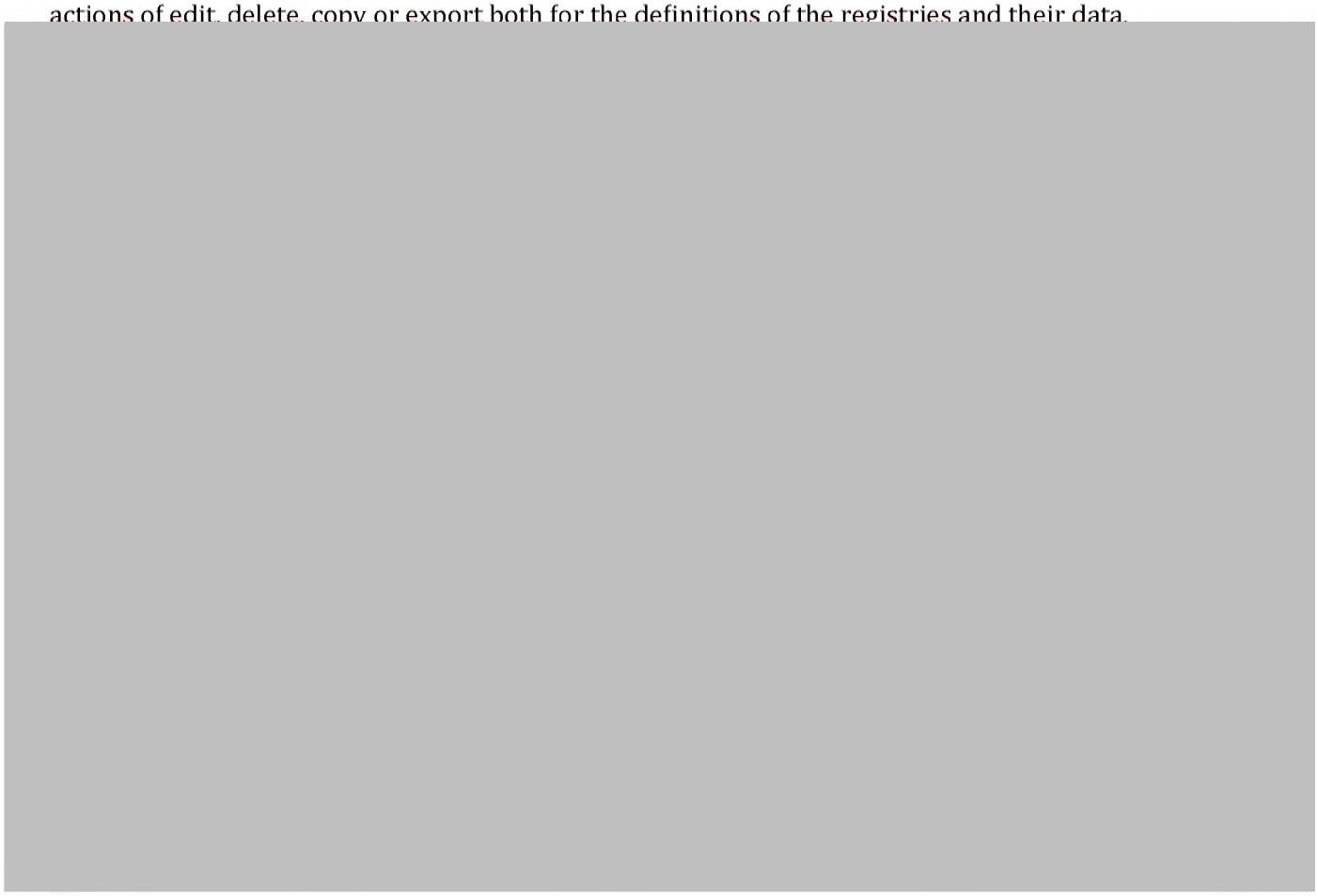


Figure 9 Registry Management screen

2.3.4 Rule Management screen

The rule management screen presents the complete history of the changes performed in a rule and which user (Border Manager) performed the changes along with all relevant metadata. The Border Manager is responsible for the maintenance of the rules that he/she created. The system provides a number of actions over the rules, such as add, edit, delete, copy allowing the user to perform any desired adjustment.

Previous versions of rules can be re-instated and be put into use. This feature allows for parallel execution of multiple rule versions and comparison of results leading to informed decisions about the best approach of use. History management of information covers both system supplied data as well as all user defined ad hoc data that were used at the time of consultation.

Figure 10 Rule Management screen

2.3.5 Manage categories screen

The Manage categories screen provides an overview of the rule categories defined in the Rule Authoring Environment screen. The Border manager can activate or deactivate a category. Risk Category is a means of grouping rules. Rules contained in a specific category are evaluated as a group and the produced result sets are a product of the combination of one or more rules.

RBAT provides a special Risk Category, "Test Category" which is used for the testing of Rules. The result set that is produced from the testing process is ignored by RBAT and no risk indicators are produced by the rules authored in this "test" category (test mode).

Figure 11 Manage categories screen

2.3.6 Manage risk profiles screen

Risk Profiles are objects with specific data structure that contain a number of user defined parameters. Those parameters are evaluated against the input data defining which Risk Categories should be evaluated.

Figure 12 Manage risk profiles screen

2.3.7 System administration

RBAT is equipped with a special system administration functionality for authorised users. With this module, it is possible to perform maintenance and customization tasks on the application and the application modules. Areas that can be tuned and customized include user management, system parameters, special processes automation, special values etc.

The administration functionality provides a complete web-based interface for all administrative and customization functions of the platform. All technical as well as all security-oriented functions of the system are available for customization through a well thought-of set of web consoles specifically tailored to accomplish administrative tasks.

2.3.7.1 User administration screen

User management is a critical part of maintaining a secure and efficient system. Using the Administration services functionality, the system administrator can define the users of the system along with their access privileges and roles. Apart from defining users and user attributes, the administrator is given a well-designed set of tools to identify the state and actions of users logged into the application. The system administrator can also create new users.

Figure 13 User administration screen

2.3.7.2 Parameters screen

The parameters screen activates and deactivates the processing of the dynamic registries excel files.

Figure 14 Parameters screen

2.3.7.3 Define Timeout screen

In the define timeout screen, the time available for the Border Manager to review the produced risk indicators from the preregistration phase and the time when the risk indicators are going to be communicated to the Border Guards can be defined.

Figure 15 Define timeout screen

2.3.7.4 Weight based screen

Weight based is an algorithmic procedure to assess the overall score based in the risk scores provided by iBorderCtrl modules and certain weights identified for each module. In essence, the total risk score is computed for each traveller and for each phase by calculating the weighted average of the risk score provided by each module. The risk score provided by each iBorderCtrl module has a predefined weight. The Weight based limits are used in order to screen all travellers by separating them into high, medium and low risk groups. For each traveller a total risk score according to the risk scores provided by other iBorderCtrl modules is calculated by the system and for both phases (preregistration and border crossing). The adherent risk values are used to calculate the overall risk score by taking into account specific weights as defined using the Multicriteria Decision Analysis technique and

methodology described in D4.1. The weight for each module and for each phase as presented in section 2.2 has been saved in RBAT's weight based screen as shown in the figure below:

Figure 16 Weight based screen

2.3.7.5 Random check screen

The Random Selection is a procedure to identify cases for further analysis based on random sampling or stratified random selection. Random selection can be activated per Border Crossing Point on demand. Moreover, each Border authority office is able to define the required parameters for Random Selection independently from each other. For example, as depicted in the figure below, during the border crossing phase every 30 travellers that pass one of them (random selection) should be thoroughly checked.

Figure 17 Random check screen

2.3.7.6 Manage result codes screen

In this section, the selection options for the proposed actions related to the rules can be defined. For example the proposed actions when there is a hit/match in a rule is to a) stop the traveller, b)

Figure 18 Manage result codes screen

2.3.8 Reports screen

RBAT provides a report extraction functionality. The Border Manager has at his disposal a number of criteria and combinations of criteria, for creating reports and for exporting data. RBAT also provides a search mechanism for all the data that are available to the system such as the Dynamic Registries, the authored rules etc. The available parameters for the search queries are dynamic and adjusted according to the available data fields and their data type. Also the system provides a number of reports that allow the Border Manager to monitor the result sets, the manual interventions, the input data of the system etc.

A query can involve accumulated data (sum, count of, min, max, average) and grouping by different factors (e.g. traveller, border crossing point etc.). Equalities, inequalities and ranges (equal to, less than, more than, between x and y) can apply on quantifiable data. The Border Manager can choose HTML or CSV as an output format.

2.4 Implementation details

The Rule Authoring Environment is an integral part of RBAT. The Rule Authoring Environment module allows Border Managers to define conditionally executed actions based on occurring events while at the same time to take into account past information if necessary.

The rules definition is facilitated through an AJAX based web interface, which by using a simple natural language-like interface allows Border Managers to express all needed rule conditions and actions using familiar domain specific terms. Decisions on the actions to be followed in case there is a hit or a match at a rule, are codified in sequences of simple rules that can be interconnected. Decisions are based on the most current data available to the application as all traveller information stored in

the iBorderCtrl database are pushed through an xml to RBAT for both phases (preregistration and border crossing phase) with special care taken for cases needing to access historical data (traveller risk from previous crossings). The dynamic nature of RBAT's Rule Authoring Environment and ultra-fast execution makes it realistic to be employed in Border checks in order to facilitate the decision of the border guards.

Using the easy, AJAX-based web interface of the Rule Authoring Environment, the rules can be easily updated and kept up to date with minimum effort. Information available only to Border Managers can be quickly transformed into rules enabling rapid adaptation to law enforcement directives or important information that have to be directly translated into rules.

RBAT's dynamic registries functionality, enables the Rule Authoring Environment to incorporate data from various sources (i.e. Law Enforcement Agencies' directives, black lists, wanted persons' lists, missing persons' lists, identified risk patterns from the BCAT module) and to translate them in rules. New rules can be deployed anytime without requiring any kind of server restart and without any downtime.

The administrative module of RBAT provides dedicated modules for logging user actions and system events. The system records who has accessed the system and what operations has been performed during a given period of time. Audit trails and system logs of the offered solution are designed with the purpose of maintaining security, monitor system operation, data recovery assistance and error correction.

The RBAT system is consisted of one service "getApplication" and it is listened to:

method:POST

The "getApplication" service is related to receiving the information that TUA sends through http requests.

More specific TUA system has to send the information in a JSON object with the specific format. Upon the receipt of the request the RBAT system fires the evaluation process of the specific request.

2.5 Performance test results

This section provides information on the RBAT performance testing for both phases. The results of the performance testing are presented in the figure below. Each dot represents a risk calculation request. In the top diagram the time spent for each risk estimation is depicted. By combining the upper and middle diagram, the result is that the average response time per request is equal to 0.7-0.8 sec. In the last diagram at the bottom, the volume of data involved in the risk estimation process are presented.

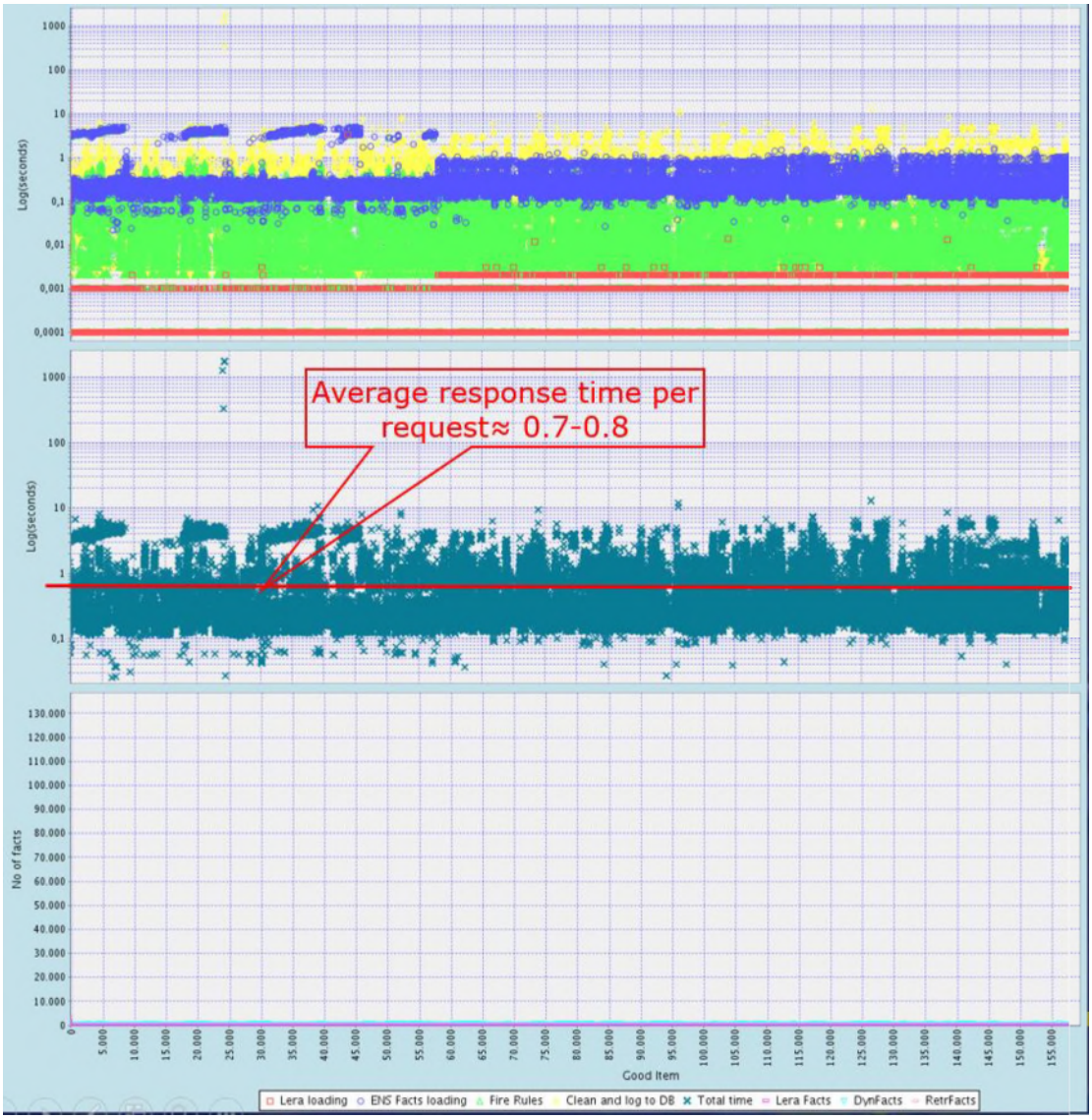


Figure 19 RBAT performance test results

3 External Legacy and Social Interfaces (ELSI)

3.1 Technical description overview

ELSI is tasked with linking in, and calculating risks based on external to iBorderCtrl databases. To achieve these tasks ELSI has two distinctive roles, and two implementations.

- The Border Control institutional systems giving access to databases across countries.
  - VIS: Visa Information System – the database stores information about issued visas.
  - SIS2: Schengen Information System – the database stores information about verifications in the Schengen zone.
  - RTP-EES: Registered traveller program – Entry/Exit System – the database stores information about crossings of Schengen borders by citizens of third countries.
- The social media component, responsible for linking publically accessible information about the traveller from their social media account, ***provided they consent to it and there's clear legal scope to allow for the tests***

For VIS, SIS2 and RTP-EES implementation details were outlined in great detail in Deliverable 4.1. As a summary, as VIS and SIS2 are all highly secure systems with strict governance by policing institutions at national and international levels getting access to the real system for piloting purposes was outside of the scope of the project. We did try however in hopes that perhaps we would be given at least access to test systems, however we were unsuccessful as it was considered possible to simply re-develop the systems for the needs of our project rather than expose existing ones to the potential risk a prototype system would expose. As such we relied on information from various official sources to understand the protocols involved, with great interest given to the fields and schema of databases within this systems and the communication protocol that relied on the Universal Messaging Format (UMF, following Europol's SIENNA application). We implemented each of the systems for piloting purposes of the project and are able to populate the databases with traveller's information relevant to the showcases and pilots of the project.

ELSI provides risk assessment based on each system's information, correlated to the information collected at pre-registration about a traveller or at the border if it is re-invoked. Specifically it checks:

- VIS: If a visa claimed to be issues by a traveller at pre-registration indeed exists, and all relevant information from that visa (Name, country of birth, etc) are indeed the same as those of the traveller registering to cross the border.
- SIS: Identifies if the traveller is listed in the Schengen Information system of any country, essentially identifying if the traveller is linked to an alert as a missing or wanted person, or listed as related to criminal offences. If a hit is identified then all relevant information is copied onto the dataset in conjunction with the high risk score to provide instant feedback to authorities that the traveller should be accordingly processed on arrival by appropriate policing stuff.
- RTP-EES: Is capable (as EES system is on the design phase, and expected to go live in the next years) of identifying if the individual is listed in EES. If he is listed in EES, then checks to identify past infractions are considered, for example if the traveller has exceeded the number of days he is allowed to stay in the country, if the visa number in the EES is the same as the one he is registered under to travel, and correlation of all personal information between the pre-registration information and the EES system.

3.2 Risk Calculation Explanation

3.2.1 VIS risk calculation

If a visa claimed to be issued by a traveller at pre-registration, indeed exists in the VIS of that country, in VIS then all relevant information from that visa (Name, country of birth, etc.) will be cross validated with the information they provided at registration. This will identify cases of people using valid visas that are however not issued to them and instead attempt to cross under someone else's ID. The Risk score generated by ELSI will not consider fingerprint or face picture as that will be taken care of by other tools in iBorderCtrl, however ELSI does facilitate the acquisition of biometrics (fingerprints and Face image) to those tools.

Risk calculation is estimated by checking if the information in the VISA used at pre-registration by the traveller indeed is valid, and contains all information as provided by the traveller in the iBorderCtrl app. If there are any mismatches related to the identity of the individual, the RISK will immediately be increased to the maximum risk as that would imply an attempt to misrepresent or alter the VISA. Some variables that may not be considered as critical may result in minor increases in risk simply to ensure that the border guard takes a look at them and makes a decision on escalating the traveller check or not.

Specifically, the Fields checked include:

Column name	Description	Process Method
VisNumber	Primary visa numer	Used to retrieve VIS field for fields validation with the i BorderCtrl database
VisOtherNumber	Secondary visa number	Checked if it's the same as the one inputted at pre-registration. If not risk is increased 100%
EndDate	Expiration date of visa	Checked if it's the same as the one inputted at pre-registration. If not risk is increased 100%.
LengthOfStay	Maximum allowable duration of stay in the country	Checked to see if the expected duration is within the allowable limit. If not Risk is made 100%.
State	Visa status	Checked to see if VISA is still valid.
TripReason	Reason of entering the country	The information is pushed on to the iBorderCtrl database.
FirstName	First name	Checked if it's the same as the one reported in the pre-registration, if not risk is set at 100% and the information is passed to the iBorderCtrl database to be presented to the guard.
LastName	Last name	Checked if it's the same as the one reported in the pre-registration, if not risk is set at 100% and the information is passed to the iBorderCtrl database to be presented to the guard.

BirthDate	Date of birth	Checked if it's the same as the one reported in the pre-registration, if not risk is set at 100% and the information is passed to the iBorderCtrl database to be presented to the guard.
Sex	Sex	Checked if it's the same as the one reported in the pre-registration, if not risk is set at 100% and the information is passed to the iBorderCtrl database to be presented to the guard.
FingerPrints	Number of acquired fingerprints	Information made accesible to the iBorderCtrl system through ELSI to enable their check by other modules.
Photo	Photo identifier	Information made accesible to the iBorderCtrl system through ELSI to enable their check by other modules
Subject	Fingerprints identifier	Information made accesible to the iBorderCtrl system through ELSI to enable their check by other modules
FingersNotNeeded	Are fingerprints required?	Information made accesible to the iBorderCtrl system through ELSI to enable their check by other modules

3.2.2 SIS risk calculation

SIS identifies if the traveller is linked to an alert as a missing or wanted person, or listed as related to criminal offences. If a hit is identified then all relevant information is copied onto the dataset in conjunction with the high risk score to provide instant feedback to authorities that the traveller should be accordingly processed on arrival by appropriate policing stuff.

Column name	Description	Process Method
Number	Document number/Traveler personal id	Used to check if the person is listed. If yes RISK is set to 100%
OriginCountry	Identifier of the country signalling warning about the document	Passed to the iBorderCtrl Database.
Type	Identifier of the warning type	Passed to the iBorderCtrl Database.
Reason	Identifier of the reason for signaling warning	Passed to the iBorderCtrl Database.
Action	Action identifier	Passed to the iBorderCtrl Database.

3.2.3 RTP-EES risk calculation

RTP-EES: Identify if the individual is listed in EES. If he/she is listed in EES, then checks to identify past infractions are considered, for example if the traveller has exceeded the number of days he is allowed to stay in the country, if the visa number in the EES is the same as the one he is registered under to travel, and correlation of all personal information between the pre-registration information and the EES system.

VIS Column name	Description	Process Method
DocumentId	Document identifier	Used to retrieve the VISA as provided in the pre-registration.
PersonId	Person Identifier	Used if DocumentId fails to retrieve the VISA as a way to check if an individual holds one with a different number.
DenyReason	Reason for denying the visa application	Individuals who are found to have been denied Visas, are identified through the VISA number, or through their ID number result in immediate 100% RISK score and the DenyReason field is pushed to the iBorderCtrl database to enable reporting this key information to authorities.
Rejection Reason	Reason for rejection	If this information exists it results in immediate 100% RISK score and the Rejection Reason field is pushed to the iBorderCtrl database to enable reporting this key information to authorities.

3.2.4 Social Media risk calculation

A key challenge with processing social media or other web based public information about travellers in ELSI for the purposes of iBorderCtrl is the challenges imposed by the GDPR. This isn't to say that GDPR disables the planned functionality, in a way it provides a clear justified exception to policing, however, iBorderCtrl as a project is involved in a technology platform development, not policing. Therefore the exception for the activities of the project isn't considered applicable. Following recommendations by the Legal partners some of the functionality although developed will not be tested to ensure strict adherence to GDPR in the piloting. However we are presenting and disseminating the capability, in an effort to introduce the potential impact of these technologies to policing authorities and relevant policy makers who may, though policy changes decide to adopt some of these technologies.

The key risk calculation of ELSI for social media was done through twitter. Travelers are asked to optionally provide their twitter account as well as consent to processing public information they make available through it to help determine their traveller risk. The plan was to motivate travellers to provide their twitter accounts to benefit from the potential identification of their status as a bona fide traveller, while enabling ELSI to map travellers to social networks identifying potential links of the travellers to known accounts associated with illicit activity. Such illicit activity may include accounts linked to terror attacks, drug / smuggling/ human trafficking activities etc. Risk is calculated by providing a list of accounts and groups linked to an associated risk score for the traveller who follows them, or is followed by them. Risk could also be calculated to 2nd degree contacts (i.e., followed by followers). The clear violation of privacy here is that even though the individual traveller may have provided consent to have their twitter account analysed, the followers, groups etc., did not. Therefore for this type of risk calculation to take place, new policy needs to be adopted.

Therefore twitter risk is for the time being limited to risk scores derived from postings and account settings of the individual traveller with no consideration of his network. We process these tweets and push them onto the database to allow the border guard to have access to them for review and potentially to use as part of an interview. We can perform also some checks, to see if the country of residence on social media matches what is reported in TUA, user's gender, and other information; however we expect this to be of minimal impact to the overall risk as this data is self-reported, users primarily complete it when they initially make the account, and many users complete the information on social media intentionally wrong as they perceive it as a way to protect their privacy.

By pushing the latest tweets onto the database we also enable follow-up analyses using text data mining through the BCAT tool to identify rules associated with specific illicit activity in the future that may be deployed through RBAT. This may include mentioning of specific words that may stand as abbreviations linked to illegal activity.

3.3 Final technology functionalities

ELSI is implemented as a virtual machine, it incorporates access to VIS, SIS2, RTP EES (legacy databases) systems that were implemented from scratch duplicating the ones in each country for VIS and SIS2. This is to enable quick re-instantiation of the system to address potential issues with Countries or organizations needing to set up their own instance of VIS, SIS2, or EES and all the relevant modules of ELSI. For the purposes of this project the iBorderCtrl instantiation is accessible at elsi.stremble.com.

To enable the pilot phases to be executed using the VIS, SIS2 and RTP EES databases developed for evaluating ELSI by all partners a set of APIs was developed supporting communication with these systems as well.

Finally to enable setting up of specific travellers in the legacy databases a procedure is set up, as this is not the appropriate method to be used in real life deployment, we relied primarily on setting up entries using simple SQL tools directly on the server.

All access APIs for the different services are presented in detail in **Appendix A.**

4 Border Control Analytics Tool (BCAT)

4.1 Technical description overview

BCAT is based on a scientific workflow analytics platform that allows the creation of new analytical workflows to build purpose designed solutions to today's border control problems, as well as making it easy to expand these functionalities to future problems. The functionality is split into three categories, the first category are iBorderCtrl technical algorithms needed to integrate with the platform, (link to databases, filtering and trip/traveller selection), the second includes the **generic algorithms** widely used in statistics and data mining to solve complicated analytics challenges, and the second workflows, where we solve specific Border Control problems by designing **analytical workflows** that include analytical steps with the algorithms in the system parameterized to the specific problem at hand.

The generic algorithms are standardized, well established, robust algorithms that solve strict primarily mathematical/computational problems with a wide range of applications across many domains including border control, and we split these into 2 further categories, those based purely on statistical approaches, and those based on data mining approaches including machine learning algorithms. The statistical methods are targeted towards testing specific hypothesis including but not limited to hypothesis related to the performance of each modules in iBorderCtrl.

The final and most interesting type are **analytical workflows,** these are designed to solve specific problems in the border control domain utilizing the generic algorithms. They enable the systematic analyses of new trips as time progresses, and the potential discovery of new patterns in trips and travellers. These can be developed by experienced analysts easily right in BCAT and tested using all the data in iBorderCtrl from past trips and once finalized can be released to be used by all users, with documentation, support and simple clear visualizations build right into the platform to enable border managers with no background in analytics other than what is expected of them for their positions to utilize these workflows to meet challenges in their day to day operations.

4.2 Meta-analyses explanation

BCAT provides a platform and tools to perform analyses on all data collected through iBorderCtrl, including upcoming trips, past trips and all registered travellers whose data is still in the system. The goal is to provide BCAT as a tool that allows the re-use of old data to discover knowledge that will help make border control adaptable to the evolving challenges and attempts of illicit crossings. To demonstrate the potential of such a platform it was essential to consider specific known challenges of border control today, and utilize BCAT to deliver analytical workflows that are easy to use by border managers to solve key tasks that are either now not possible, or require a lot of effort making them inefficient and expensive.

The selection of algorithms to include in BCAT was done through a review of the requirements analyses as part of iBorderCtrl, as well as through follow-up structured and unstructured interviews and meetings with the end-users of the project that revealed current capacities, as well as needs. BCAT inevitably does replicate some of the existing capacities, however most importantly is that it goes beyond those capacities and meets current gaps in the information extraction potential of knowledge form database that is designed to:

- maximize the cost reduction to time and resources needed to perform an investigation
- automate meta-analytics that need to be executed routinely on the metadata collected across all EU borders to identify trends and patterns of behaviour linked to illicit activities and the people/vehicles performing them.

- provide forecasting solutions to traffic, risk, and behavioural patterns to allow the border guard authorities to become quickly adaptive and predictive empowering them to meet their objectives with greater efficiency.

Complete detailed lists of algorithms coupled with explanations were presented in previous deliverables, most extensively on D4.1. There has been no deviation from the plan and all planned algorithms are available generating the relevant tables, and visualizations expected. Thus in this Deliverable we focus on the user interface. Note that although the system is up and running and communicating with the iBorderCtrl database, the only data in the database are sample trips and travellers details/ profiles that different consortium partners were inputting to perform their own alpha testing as they were developing the system. Thus the presented screenshots include these data as output. There is a plan to completely clean all data from all databases in iBorderCtrl before Pilot trials begin, and at the end of those we expect meaningful analytics to be possible to take place. As most modules were completed at the same time, only testing data was available in the database that is fake, and in no way matches distributions or nature of real data, leaving the demonstration of the system to the deliverables that will report on the end-user pilots.

4.3 The user interface

Bellow you can see a screen shot of BCAT. The underlying platform of BCAT is based on the Galaxy Project, a scientific workflow platform initially developed for Bioinformatics that has been reused here as well as other projects primarily due to it's

- open source nature,
- it's ability to quickly and effortlessly provide scalable analytics to high performance computing
- It's ability to be instantiated independently for different projects.
- It's ability to form scientific workflows that utilize multiple algorithms in sequence or parallel to achieve specific problem objectives.
- It's expandability as we have done in iBorderCtrl that allowed us to expand the code easily to support the link to the iBorderCtrl database and other modules.
- The ease of creating workflows, were users with expertise in analytics can develop scientific workflows that are problem specific, and share these with others who may not have the knowledge of the inner process of the analytical methodologies used, but can simply through point-and-click in the platform use them focusing on setting up the options (input, parameters), and output.

In the figure below you can see the user interface (UI), it's split into the top bar (dark blue) that contains links to the various screens; these provide access to previous stored by the user, or shared with the user by others, databases, workflows and visualizations. It also holds the link to administration options, help and support documents and user accounts settings.

The remainder of the UI is split into 3 columns, on the left we have the links to "Tools", these are small algorithms implemented through the Galaxy platform to be inter-locking with each other, so you could run them in any sequence in the same piping the output of one algorithm as input to the next. Bellow them are "Workflows, these may be developed by a single user and shared with others, or they may be developed by any user for their own investigations. Stored workflows may still be parameterized, for example you may define a workflow that attempts to identify patterns in travellers limited to the country of origin and date-range of trip, you could define a workflow were the algorithmic steps are fixed, but once instantiated the user is to provide the date range, and country of origin.

The middle column is the workspace, here you will see the screen of the tool you are currently working on. In the figure belowFigure 20 you see the tool that pulls data from the iBorderCtrl database. This is

also the space you receive notifications, status updates, and were results will appear once analyses is completed after you select for specific outputs to be visualized in the right hand column.

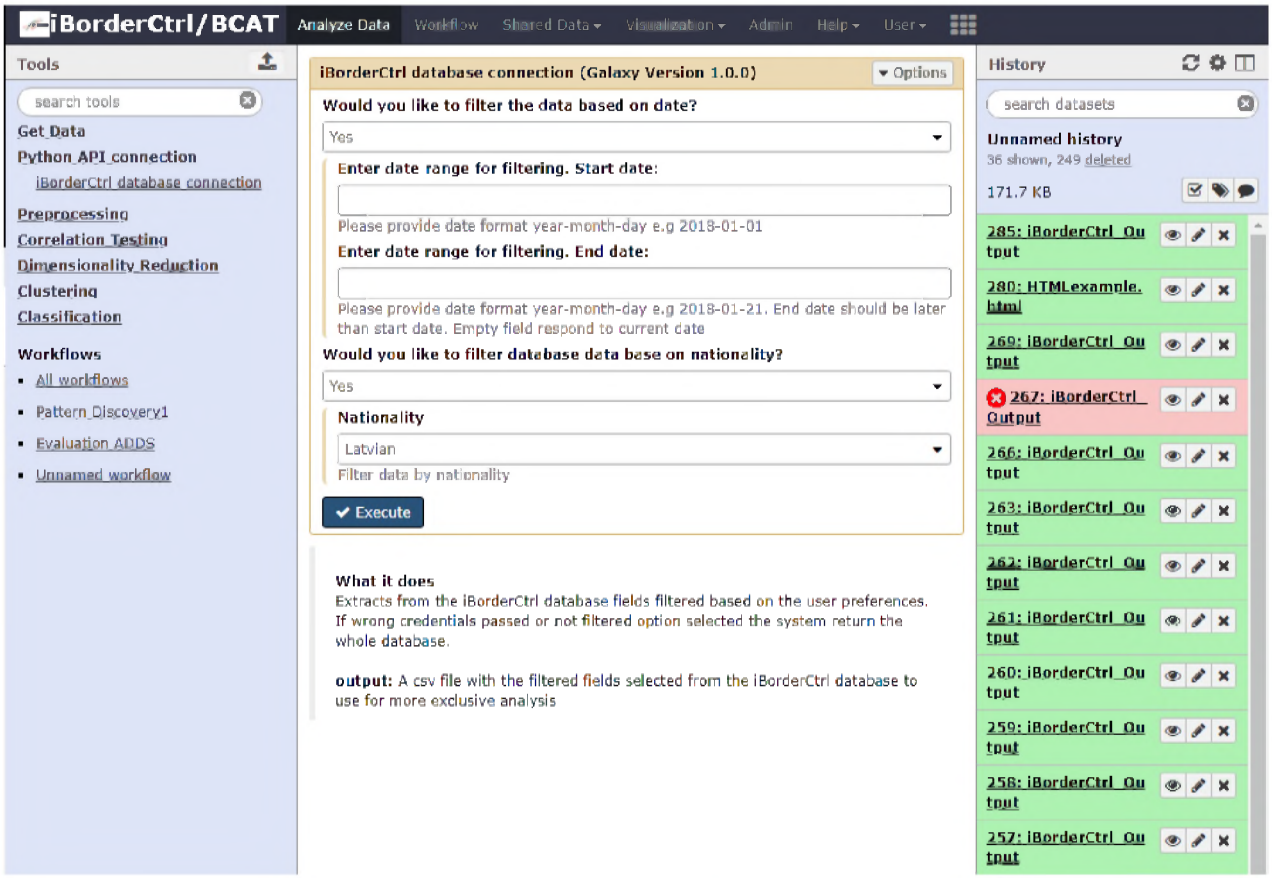


Figure 20 The BCAT platform, Get data.

This brings us to the last area, the third column that is the right-most one. This one contains each procedure instantiated, whether it's a single tool, or workflow. Each instantiation can have 3 colours, green if it's complete and ready, Red, if it encountered any error, in the example, operation 267 is red, on closer inspection the database returned an error because there were no travellers matching the conditions set in that instantiation. Or it can be yellow, that indicated a tool or workflow is still running. Finally it may also be grey if a tool's execution is scheduled pending the completion of another tool that is linked to it through a workflow. The figure belowFigure 21 is a screenshot that follows a simple tool execution for getting data from the iBorderCtrl database from Jan 1st 2018, to 1st of May 2018. As you can see there are some testing data that are returned in a tabular format

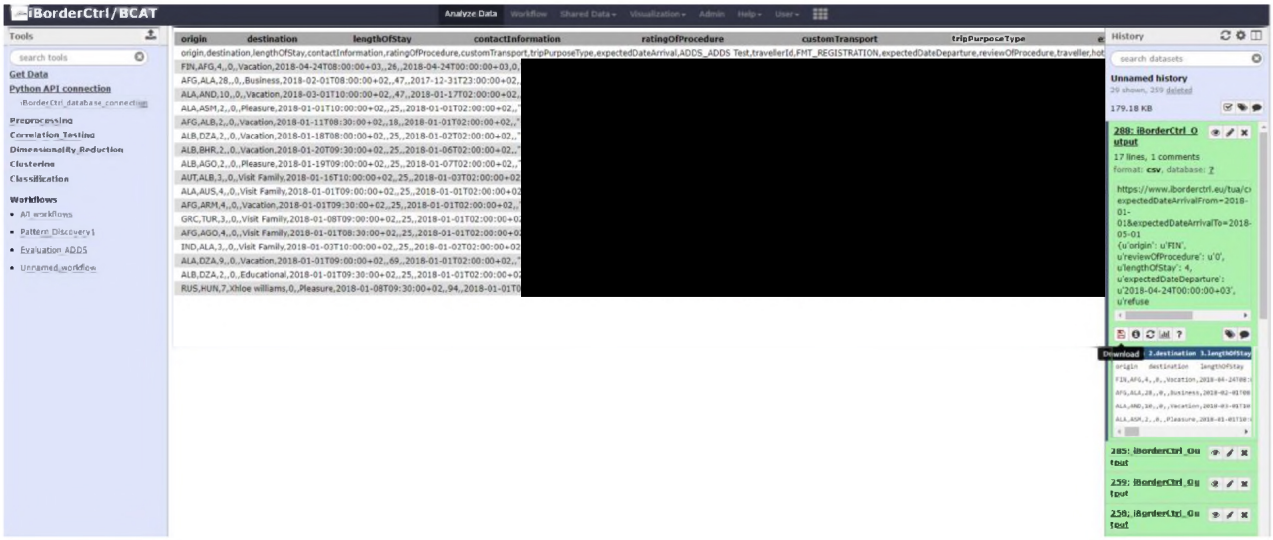


Figure 21 Tool Instantiation output, Table output from database

. The table is viewed by clicking on the eye  icon in the right hand column for the tool instantiation of interest, and by clicking on it it expands as shown in the figure to also provide options  moving from left to right for "save as" that in this case will generate a comma separated value (csv) file output for this output that itself is directly loadable to the vast majority of other software designed to process tables, as an example in the figure belowFigure 22 shows the outputted file opened in excel. The next icon provides information on the tool executed to produce the output, and any specific parameters used, the next icon that looks like a bar chart, provides the ability to produce plots from a number of options from the table outputted in the last tool. In the figure belowFigure 23 you can see a plot generated that is a pie-chart of the trip duration of travellers planning to travel in a specific range of days.

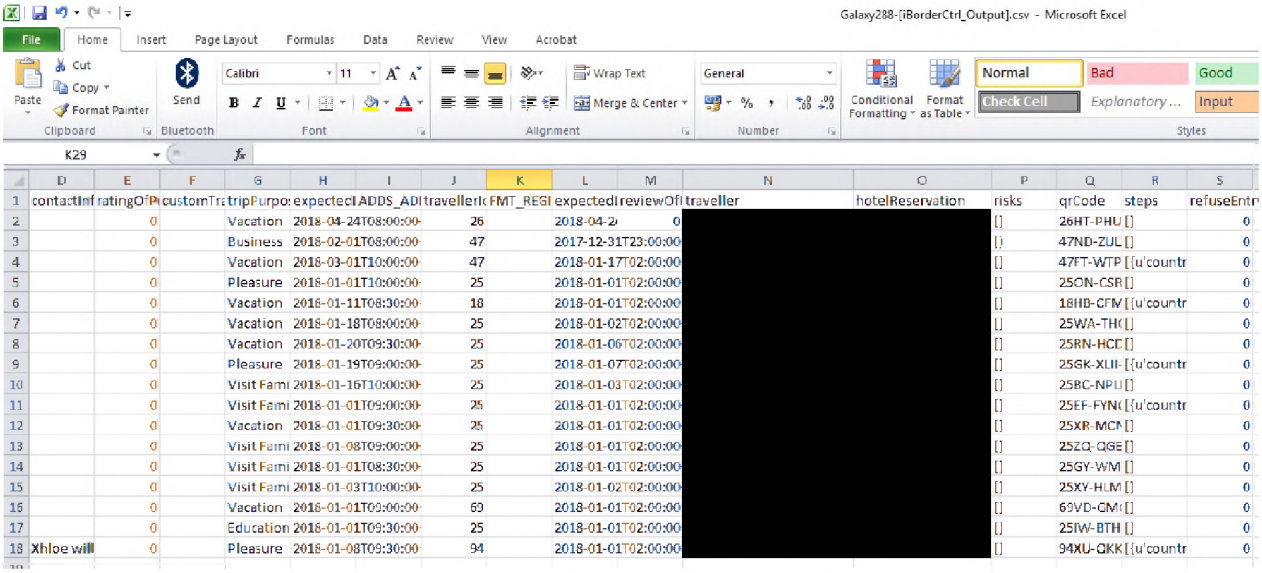


Figure 22 csv File output from BCAT opened directly with excel without any pre-processing.

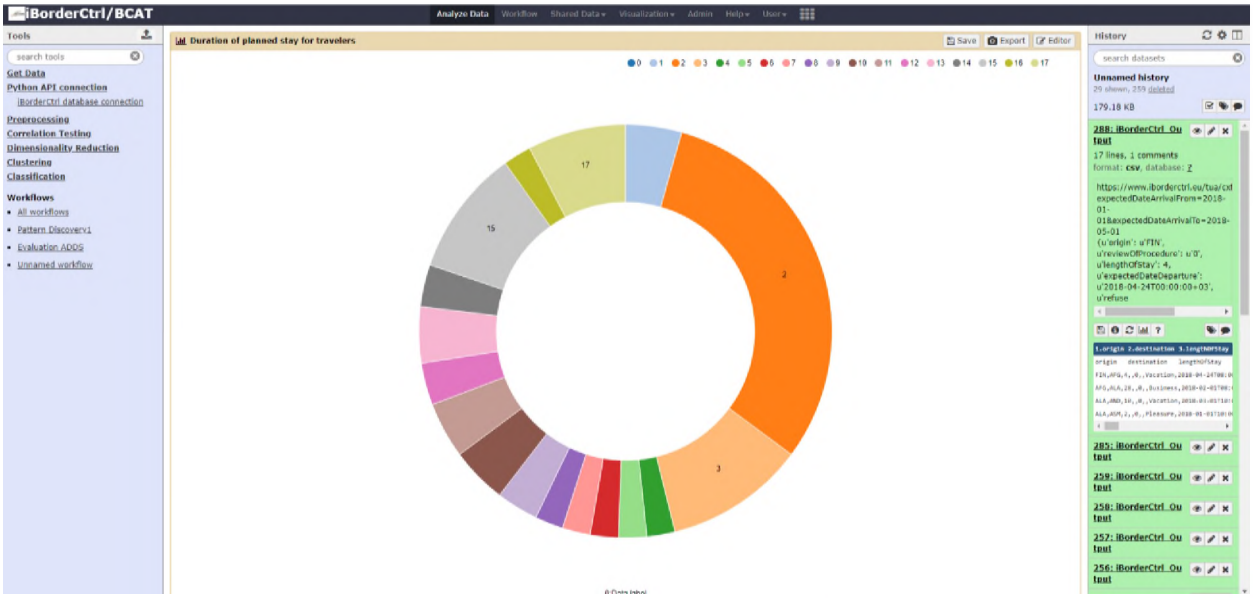


Figure 23 Pie Chart visualization with the distribution of travellers and the number of days they plan to stay in their destination country

4.4 Workflows

Workflows are powerful tools, and the key ability of the underlying open source platform chosen for BCAT (the Galaxy Project). They allow the utilization of analytical tools in any sequence, and even the parallel deployment of algorithms that are either competing, or are tasks with different objectives but rely on the same input data. The figure below captures a complicated workflow, designed to demonstrate the capability of the system. This would have been designed by an experienced analyst, but would be deployed by any border manager. There is no need to view, or configure the view by the end-user, the view on this figure is meant for the designer not the executor. This workflow is designed to achieve multiple objectives, and attempt to meet each one through independent sub-workflows that may be parameterized and optimized to the specific situation. Specifically it takes as input the metadata from the iBorderCtrl databases that can be filtered for country, and data range for the planned trip. IT will then perform analyses that will meet the following objectives, the final algorithms are listed in each objectives so the reader can follow back and identify the different sub-workflows that will all be executed to meet the same objective.

- Pattern identification from all metadata inputted (Hierarchical Clustering)
- Pattern Identification from all metadata inputted with optimization at pre-processing stage to improve performance if the database grows large, and the data range is wide requiring some intelligent optimization (HSIC Lasso->Hierarchical Clustering, as well as Principal Component Analyses ->Hierarchical Clustering)
- Identification of the most informative variables ordered based on their predictive power for crossing rejection (Random Forest)
- Clustering of travellers with a simple view to identify travellers exhibiting similar behaviour (k-means)
- Build intelligent predictive models that prognoses the border control outcome of a traveller/trip based only on the pre-crossing available data provided by the TUA and processed through the various modules in iBorderCtrl (FMT, ELSI etc.), (Support Vector Machines)

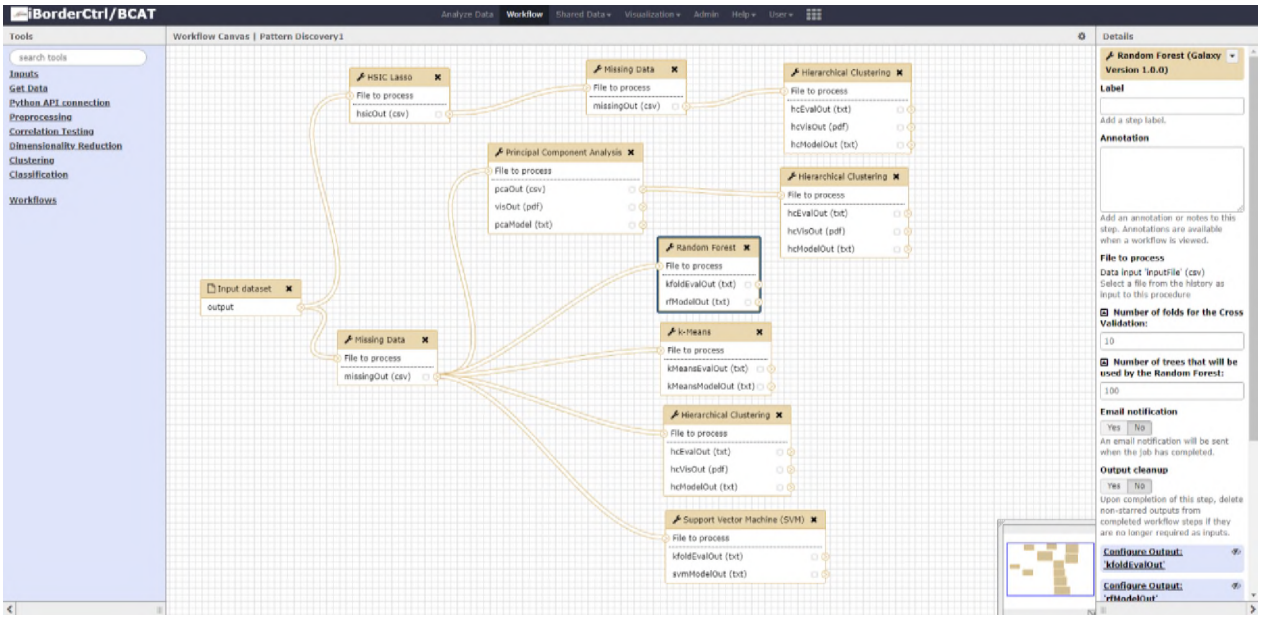


Figure 24 Creating a workflow

Once a user selects a workflow (right hand column "Tools" section, selecting Pattern Discovery 1 inputting a data range for trips to be considered and hitting execute). Each intermediary tool will appear on the right column either yellow or grey, yellow indicating they are executing, and grey indicating that they are pending execution on the completion of the previous step. Each tool that completes becomes green and its outputs are available for viewing. Workflow designers have access to intermediary results. However users with access only to the workflow and not its design will be able to monitor the execution process, but all intermediary databases will be eliminated from their view with only key visualizations, tabular views and automatically generated reports made available to them.

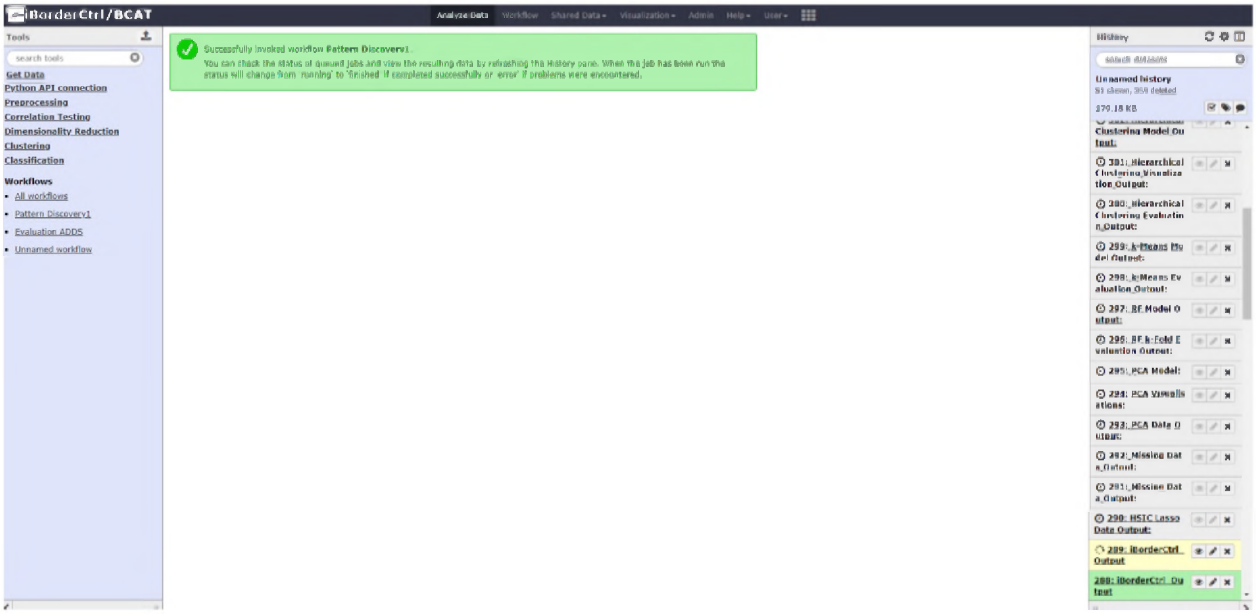


Figure 25 Screen Short post Execution of Workflow

4.5 Performance impact on the iBorderCtrl Platform.

Worth noting this analyses will perform a single get request from the iBorderCtrl database (input dataset tool) and will deploy a high performance computing machine at the premises of Stremble ventures LTD to perform the entire analyses (32 computing nodes 128GB RAM, SSD scratch space and RAID backup storage for all input and output files) thus executing BCAT does not pose any performance impact on the iBorderCtrl platform apart from the single call to the database to provide the data. For future instantiations, existing hardware can be used, and deployed efficiently and quickly as the entire system is built on a virtual machine, or the processing can be deployed to even larger computational resources, such as a computing cloud service.

It's already compatible with any the vast majority of commercial cloud providers such as it supports OpenStack and OpenNebula cloud management protocols enabling it's deployment to amazon web-services, Microsoft Azure etc.

5 Addendum - further legal aspects

The iBorderCtrl project was initially drafted in 2015, with the project starting in September 2016. The system requirements, which formed the backbone of all considerations on how to design the system, were due in M4 of the project, and all subsequent work was aligned with these. At the same time, the European legislator enacted various new pieces of legislation to enhance the quality of border checks. Consequently, the project faced a fast-moving and complex legal situation, where it was crucial to find a proper balance between aligning the technologies proposed in the DoA and the developments in the legal framework happening in parallel to the project.

Within the project lifetime, the prototype was used only to conduct pilot tests. As the purpose for any data processing within the pilot tests was research, it was solely covered by the General Data Protection Regulation (GDPR).[1] The consortium is aware though that, for a possible implementation of the system or parts of it, further changes might be required to reflect legislation specifically applicable to border checks both at the border and in terms of prior access by Member States' border authorities to information systems. In terms of processing of personal data, this will engage inter alia the law enforcement directive and the national laws for implementation. This will require adjustments to the system as and when it is implemented according to the legislative framework covering the concrete circumstances. Thus in some cases, instead of the GDPR, data processing will instead be covered by the law enforcement directive[2]. This approach is also reflected in the latest specific legislation on border crossing such as the EES[3] and ETIAS[4] regulations, whereas the applicability of data protection legislation will depend on the legal nature of authority processing personal data, as well as the specific purposes of processing.[5]

The key new legislative instruments that have been introduced during the lifetime of the project are listed below. A more detailed analyses of their implications for the iBorderCtrl system can be found in Deliverable D5.6.[6]

5.1 Entry-/Exit-System (EES)

5.1.1 Regulation (EU) 2017/2225

This regulation was adopted in November 2017 and mainly amends Regulations (EU) 2016/399 (SBC). Some relevant terms such as: "Self-service system", "e-gate", "automated border control system", and "confirmation of the authenticity and integrity of the chip data" were defined. For example, self-service means "an automated system which performs all or some of the border checks that are applicable to a person and which may be used for pre-enrolling data in the EES." The possibility and legal basis for using self-service systems for pre-enrolling data in the EES is added to Article 8a of the Schengen Borders Code.

[1] Regulation (EU) 2016/679.

[2] Regulation (EU) 2016/680.

[3] Regulations (EU) 2017/2225 and 2017/2226.

[4] Regulations (EU) 2018/1240 and 2018/1241.

[5] In particular, the law enforcement directive will apply to data processing by designated authorities for the the prevention, detection or investigation of terrorist offences or other serious criminal offences.

[6] See especially section 5 of D5.6.

5.1.2 Regulation (EU) 2017/2226

Also adopted in November 2017, this Regulation establishes the Entry/Exit System with the following functionality: it creates a centralised system for the registration of entry and exit data concerning third-country nationals crossing the external borders of the EU Member States for a short stay; calculation of the duration of the authorised stay of such third-country nationals; generation of alerts to Member States when the authorised stay has expired; and recording and storage of the date, time and place of refusal of entry of third-country nationals as well as the authority of the Member State which refused the entry and the reasons for this.

5.2 European Travel Information and Authorisation System (ETIAS)

5.2.1 Regulation (EU) 2018/1240

This Regulation was adopted in September 2018 and seeks to establish a European Travel Information and Authorisation System (ETIAS), which includes a pre-travel authorisation. It applies to visa-exempt travellers, and the key objective is to verify whether a third country national meets the applicable entry requirements before starting their trip to the Schengen area. For this purpose, the traveler is required to submit information prior to his trip via an online application (pre-registration), to enable a pre-travel assessment by the relevant authority.

5.2.2 Regulation (EU) 2018/1241

The main thrust of this Regulation is to amend Regulation (EU) 2016/794 to give Europol the authority to manage the ETIAS watchlist in accordance with Articles 34 and 35 of Regulation 2018/1240, enter data into the ETIAS watchlist related to terrorist offences or other serious criminal offences obtained by Europol, and provide an opinion following a consultation request. Europol shall also enable the European Border and Coast Guard Agency to have indirect access on the basis of a hit/no hit system to data for specific purposes.

5.3 Interoperability regulations

5.3.1 Regulation (EU) 2019/817

The aim of the regulation is to better protect the EU's external borders through improved border management. In this regard, it initiates a system of interoperability between EU level information systems and the various law enforcement systems to eliminate the blind spots. In particular, the collaboration of authorised users such as border guards, law enforcement officers, immigration officers, visa officials or judicial authorities shall be tackled by improving the fragmented architecture of data management for security, border and migration management, where information is stored in separated systems. Prior to the draft, an impact assessment has been conducted.

5.3.2 Regulation (EU) 2019/818

Regulation (EU) 2019/818 also lays down conditions for enhancing interoperability among European databases. While regulation (EU) 2019/817 focuses on providing provisions for EES, VIS, ETIAS and SIS, regulation (EU) 2019/818 focuses on Eurodac, SIS and ECRIS-TCN. In other words, regulation (EU) 2019/817 focuses rather on border checks, whereas regulation (EU) 2019/818 is focused on the field of police and judicial cooperation. However, both fields are closely interlinked with each other.

5.4 ECRIS-TCN (Regulation (EU) 2019/816)

Another regulation released together with the aforementioned interoperability regulations is regulation (EU) 2019/816 on establishing a centralised system providing for access to conviction information on third-country nationals and stateless persons (ECRIS-TCN) held by Member States. This supplements the European Criminal Records Information System and amends Regulation (EU) 2018/1726. In this regard, it also provides the conditions under which the system shall be used.

5.5 Regulation on strengthening ID-cards (Regulation (EU) 2019/1157)

In June 2019, the European parliament and the Council released a regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. The regulation is intended to strengthen the security standards applicable to identity cards issued by Member States to their nationals and to residence documents issued by Member States to Union citizens.

6 Conclusions

The implementation of the iBorderCtrl software platform has progressed as planned and there were no deviations. This deliverable is the final report on the second version of the iBorderCtrl software platform and related subsystems developed as part of WP4 and combined with the information included in D4.1 justify the fulfillment of the WP4 objectives.

The Risk based Assessment tool (RBAT), the External Legacy and Social Interfaces (ELSI) and the Border Control Analytics Tool (BCAT) functionalities are presented in detail. This deliverable includes screenshots, schematics and visualizations throughout the document to demonstrate the final status of each module and the progress of development with regards to the work progress presented in D4.1 (M18), with the expectations envisaged at the end of each task of WP4 (M24).

This deliverable demonstrates that the development of the iBorderCtrl software platform and related interfaces is completed on time at M24. Furthermore, considerations of the system -as a whole- were planned to minimize any risk to the in parallel ongoing integration phase of the project. The main iBorderCtrl integrated applications (TUA, BGUA, BMUA) are described in D5.2: Early version of the integrated prototype (limited functionality).

Appendix A

VIS access API

The vis component can be called with the following API

[redacted]

alternatively if access is through a new instantiation.

{IP}:3000/elsi/VIS/{id}

Or with a Get request on the same IP and port with VisNumber as a key: and as a value: 1 and header :

" Content-Type: application/x-www-form-urlencoded"

Where {id} is to be replaced with the string that represents the Travelers VIS Id number. This will be stored in VIS databases as either visNumber or VisOtherNumber. In the case of a new instantiation of the ELSI virtual machine the path will need to include the instantiated machine's IP number as part of the URL as indicated. Instantiations can support HTTPS or HTTP protocol.

The returned information is shown below for a hypothetical traveller with ID 2142314231. Note however that ID's will be populated based on pilots and only valid ID's will return a successful user, otherwise " a message will be returned.


```
{
  "Data": [
    {
      "Id": 1,
      "VisNumber": "23213214",
      "VisOtherNumber": "2142314231",
      "IssueDate": "2018-02-04T22:00:00.000Z",
      "IssuingCountry": null,
      "StartDate": "2018-02-22T22:00:00.000Z",
      "EndDate": "2018-02-28T22:00:00.000Z",
      "LenghtOfStay": 7,
      "State": 1,
      "Type": 1,
      "DocType": 0,
      "DocNumber": "",
      "DocEndDate": "0000-00-00",
      "TripReason": 0,
      "AllowedTerritory": null,
      "TravelLimit": null,
      [redacted]
      "BirthDate": [redacted],
      "BirthPlace": null,
      "BirthCountry": 1,
      "Sex": 0,
      "FingerPrints": null,
      "Photo": null,
      "FingersNotNeeded": 0,
```

```
        "Subject": null,
        "Code": "12",
        "Name": "Cyprus",
        "VisaNeeded": 0,
        "PhotoData": null,
        "SubjectId": null,
        "Template": null,
        "ID": null
      }
    ]
}
```


SIS access API

The vis component can be called with the following URL

[redacted]

alternatively if access is through a new instantiation.

{IP}:3000/elsi/SIS/{id}

Or with a Get request on the same IP and port with params as a key: id and as a value: 1 and header :

" Content-Type: application/x-www-form-urlencoded"

Where {id} is to be replaced with the string that represents the Travelers Id number. This will be stored in SIS databases as personId. In the case of a new instantiation of the ELSI virtual machine the path will need to include the instantiated machine's IP number as part of the URL as indicated. Instantiations can support HTTPS or HTTP protocol.

The returned information is shown below for a hypothetical traveller with ID 3. Note however that ID's will be populated based on pilots and only valid ID's will return a successful user, otherwise " a message will be returned.


```
"Data": [
  {
    "Id": 3,
    [redacted]
    "SpecialFeatures": null,
    "DateBirth": null,
    "BirthPlace": null,
    "BirthCountry": null,
    "Sex": null,
    "IsArmed": 0,
    "IsAggressive": 0,
    "IsFugitive": 0,
    "Reason": 1,
    "Action": 1,
    "Code": "2222",
    "Name": null,
    "IsSchengen": null,
```

```
        "PersonId": 1,
        "DocumentId": 2,
        "NationalityId": 3,
        "Number": [redacted],
        "OriginCountry": 1,
        "Type": 1
      }
    ]
}
```


RTP EES access API

The vis component can be called with the following URL

[redacted]

alternatively if access is through a new instantiation.

{IP}:3000/ees/{id}

Or with a Get request on the same IP and port with params as a key: id and as a value: 1 and header :

" Content-Type: application/x-www-form-urlencoded"

Where {id} is to be replaced with the string that represents the Travelers Id number. This will be stored in EES databases as personId. In the case of a new instantiation of the ELSI virtual machine the path will need to include the instantiated machine's IP number as part of the URL as indicated. Instantiations can support HTTPS or HTTP protocol.

The returned information is shown below for a hypothetical traveller with ID 3. Note however that ID's will be populated based on pilots and only valid ID's will return a successful user, otherwise " a message will be returned.


```
{
  "Data": [
    {
      "Id": null,
      [redacted]
      "BirthDate": [redacted],
      "BirthCountry": 1,
      "BirthPlace": "Cyprus",
      "Sex": 1,
      "Citizenship": 1,
      "PersonId": 1,
      "DocType": 1,
      "DocNumber": "1456565",
      "DocIssueDate": "2018-07-31T21:00:00.000Z",
      "DocEndDate": "2018-08-30T21:00:00.000Z",
      "DocIssuingCountry": 1,
      "DocIssuingAuthority": "1",
      "VisNumber": null,
```

```
        "DocumentId": 1,
        "ReceivingAuthority": "55",
        "ApplicationPlace": [redacted],
        "ApplicationDate": [redacted],
        "SupportingPerson": null,
        "TripReason": 1,
        "HomeAddress": null,
        "Phone": null,
        "ResidenceCardNumber": null,
        "Proffesion": null,
        "ParentsNames": null,
        "State": 1,
        "DenayReason": null,
        "SubjectId": null,
        "PhotoId": null,
        "ApplicationId": 1,
        "EesId": null,
        "GratingAuthority": null,
        "DecisionPlace": null,
        "Date": null,
        "StartDate": "2018-07-31T21:00:00.000Z",
        "EndDate": "2018-08-30T21:00:00.000Z",
        "ExtStartDate": null,
        "ExtEndDate": null,
        "RejectionReason": "Caught with drugs",
        "ExtensionNr": null,
        "RtpId": null,
        "UserId": null,
        "Action": null,
        "PhotoData": null,
        "Template": null,
        "AppId": null,
        "Authority": null,
        "Place": null,
        "CountryId": null,
        "DaysLeft": null,
        "DateLimit": null,
        "Direction": null,
        "Comment": null,
        "Code": null,
        "Name": null,
        "VisaNeeded": null,
        "IsSchengen": null
      }
    ]
}
```


ELSI API to evaluate a traveller's trip.

ELSI can be called with the following URL

[redacted]

alternatively if access is through a new instantiation.

{IP}:3000/elsi/ees/{QRcode}

ELSI will perform all tests for a specific trip and update the web site with the relevant information including all risk scores. These will include module specific risk scores. The travellers QR code is needed to access all of that trip's information from the iBorderCtrl database.

Alternatively ELSI can also be called through a get request, it takes as a parameter the personId and returns as a response all data from EES database where value pass are equal to person Id

The ELSI API only returns either an error if there was an error in processing a request, and the error will represent the technical details (for example the QR code requested was not found in the iBorderCtrl database) or it will return "Finish Successfully". This indicated that all ELSI functionality was executed, individual and overall risk scores calculated and uploaded on to the iBorderCtrl database.

Security issues with ELSI

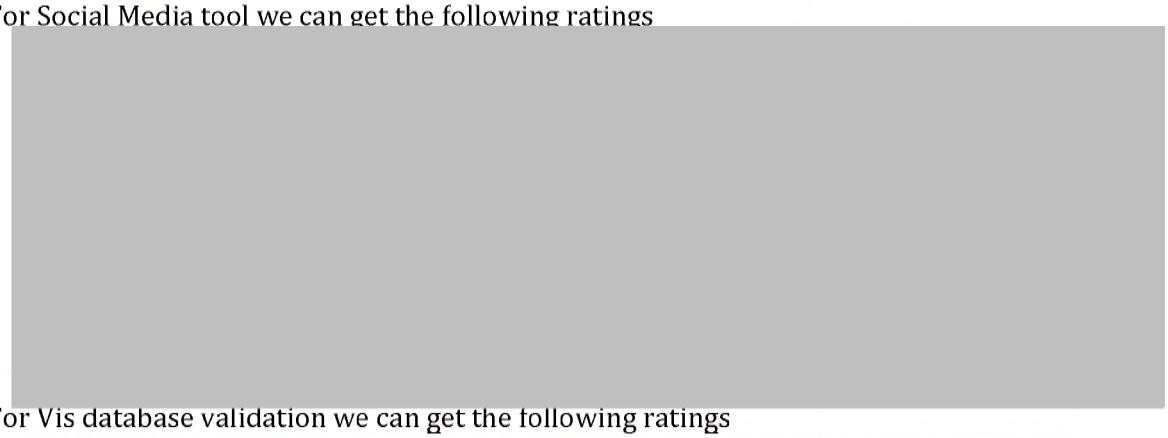
Base64 authorization is supported in ELSI, and if that is implemented in the iBorderCtrl database this can be enabled. Furthermore https is also supported and can be implemented with independent certificate or it's designed assuming more services are provided under the same IP to use the same certificate as the other services to reduce the maintenance load of renewing SSH certificates.

ELSI checks 4 parameters and individually creates a score for each one of the parameters with a text that justifies the reason that led to that score.

All 4 parameters have the same range of score 0-1 that 0 signifies the risk of the current traveller with the unique qrcode is low and 1 that it is high.

More specific follow the way each tool is rating:

1. For Social Media tool we can get the following ratings



2. For Vis database validation we can get the following ratings

An example of no risk for database is the following one. Bcase e.g. :

{ vis_database_score: 1, vis_database_text:[]}

SQL Query for VIS:

```
var query="SELECT LENGTHOFSTAY.LengthOfStay,ENDDATE.EndDate,STATE.State,TRIPREASON.TripReason,BIRTHDATE.BirthDate,SEX.Sex,FIRSTNAME.FirstName,LASTNAME.LastName FROM(SELECT VisNumber ,VisOtherNumber FROM vis WHERE ((vis.VisNumber='"+VisNumber+"')OR(vis.VisOtherNumber='"+VisNumber+"')))AS PersonData LEFT JOIN( SELECT LenghtOfStay AS LengthOfStay, VisNumber ,VisOtherNumber from vis WHERE ((vis.VisNumber='"+VisNumber+"')OR(vis.VisOtherNumber='"+VisNumber+")) and ((LenghtOfStay !="+ LenghtOfStay + ") or ("+ LenghtOfStay+" is null)))AS LENGTHOFSTAY ON ((PersonData.VisNumber=LENGTHOFSTAY.VisNumber) OR (PersonData.VisOtherNumber=LENGTHOFSTAY.VisNumber)) LEFT JOIN ( SELECT EndDate AS EndDate, VisNumber, VisOtherNumber from vis WHERE (((vis.VisNumber='"+VisNumber+"')or(vis.VisOtherNumber='"+VisNumber+")) and ((EndDate NOT LIKE '"+ EndDate + "%') or ("+ EndDate+" is null))))AS ENDDATE ON (PersonData.VisNumber=ENDDATE.VisNumber OR PersonData.VisOtherNumber=ENDDATE.VisNumber) LEFT JOIN ( SELECT State AS State, VisNumber, VisOtherNumber from vis WHERE (((vis.VisNumber='"+VisNumber+"')OR(vis.VisOtherNumber='"+VisNumber+")) and ((State !="+ State + ") or ("+ State+" is null))))AS STATE ON (PersonData.VisNumber=STATE.VisNumber OR PersonData.VisOtherNumber=STATE.VisNumber ) LEFT JOIN ( SELECT TripReason AS TripReason, VisNumber,VisOtherNumber from vis WHERE (((vis.VisNumber='"+VisNumber+"')OR(vis.VisOtherNumber='"+VisNumber+")) and ((TripReason !="+ TripReason + ") or ("+ TripReason+" is null))))AS TRIPREASON ON (PersonData.VisNumber=TRIPREASON.VisNumber OR PersonData.VisOtherNumber=TRIPREASON.VisNumber )LEFT JOIN ( SELECT BirthDate AS BirthDate,VisNumber, VisOtherNumber from vis WHERE (((vis.VisNumber='"+VisNumber+"')OR(vis.VisOtherNumber='"+VisNumber+")) and ((BirthDate NOT LIKE '"+ BirthDate + "%') or ("+ BirthDate +" is null))))AS BIRTHDATE ON (PersonData.VisNumber=BIRTHDATE.VisNumber OR PersonData.VisOtherNumber=BIRTHDATE.VisNumber )LEFT JOIN ( SELECT Sex AS Sex, VisNumber,VisOtherNumber from vis WHERE (((vis.VisNumber='"+ VisNumber +"')OR(vis.VisOtherNumber='"+ VisNumber +")) and ((Sex !="+ Sex + ") or ("+ Sex+" is null))))AS SEX ON (PersonData.VisNumber=SEX.VisNumber OR PersonData.VisOtherNumber=SEX.VisNumber )LEFT JOIN ( SELECT FirstName AS FirstName, VisNumber, VisOtherNumber FROM vis WHERE (((vis.VisNumber= '"+ VisNumber+"')OR(vis.VisOtherNumber= '"+ VisNumber+")) and ((FirstName <> '"+ firstName + "') or ('"+ firstName +"' is null))))AS FIRSTNAME ON (PersonData.VisNumber=FIRSTNAME.VisNumber OR PersonData.VisOtherNumber=FIRSTNAME.VisNumber)LEFT JOIN ( SELECT LastName AS LastName, VisNumber, VisOtherNumber from vis WHERE (((vis.VisNumber= '"+VisNumber+"')OR(vis.VisOtherNumber= '"+VisNumber+")) and ((LastName <> '"+ lastName + "') or ('"+ lastName +"' is null))))AS LASTNAME ON (PersonData.VisNumber = LASTNAME.VisNumber OR PersonData.VisOtherNumber = LASTNAME.VisNumber )";
```

3. For SIS database check control we can get the following ratings

SQL Query for SIS:

```
var query='SELECT document.OriginCountry,document.Type,document.Reason, document.Action FROM document WHERE id IN (SELECT DocumentId FROM documenttoperson WHERE PersonId='+ personId +')' ;
```

4. For EES database check we can get the following ratings

SQL QUERY FOR EES:

```
var query='SELECT CATEGORIZED.RejectionReason, APP.DenayReason FROM application AS APP JOIN (SELECT * FROM rtp WHERE rtp.EesId IN (SELECT ees.Id FROM ees WHERE PersonId='+ personId +'))AS CATEGORIZED ON (APP.Id=CATEGORIZED.ApplicationId)';
```

ELSI Final score:

For final score calculation all 4 parameters score mention above have to be considered and gain the proper weight base on their importance and their credibility. For that the following formula checks is supported.

Beside the standard qrcode, subsystem name and phase on the score string field for each side-tool vis,sis,ees,social_media we report their score as explained previous the way the rating is made and their text that reports the reason of the score if it is high. In other case returns empty, friendly message or latest tweets as in the case of social media.