

History of Changes

Version	Date	Source	Change Description
		Comment from ESR However it is not clear why the deployment of the hidden human detector tool (not required by the topic) is included in the Proposal.	Section 1.3.4b/ "Hidden Human Detection Technology": Explanation provided on the rationale for the concept of Hidden Human Detection technology.
		Comment from ESR. However the case study on refugees on the Greek/Serbian/Hungarian land borders is not sufficiently contextualised and it causes confusion -the proposal establishes a link between the arrival of refugees in recent months in this region and the iCROSS technological solution but does not adequately acknowledge the fluidity of current and unfolding refugee situation in Europe.	Section 1.3.1: Explanation added.
		Comment from ESR However, providing wi-fi hotspots for connecting to the system is technically trivial, but the rationale for its uptake is not sufficiently demonstrated.	Section 1.3.4b/ "Wireless Technologies for Border Check Process": Explanation Added.
		Comment from ESR One shortcoming is that the affordability of the technology is not adequately explained.	The relative analysis will be considered in the WP 7. A relative statement has been added in the WP description.
		Comment from ESR Some of the resources that are not sufficiently detailed, for example the pilot train case, avatar, consumables and equipment.	Section 3.2/ "Resources to be committed"/ "Justification of resources and budget"/ "C. Equipment", "D. Consumables" & "F. Other costs": Relevant explanations are provided.
		Comment from ESR However, the proposal heavily relies on automated deception detection which poses certain risks that are not adequately addressed.	2 more risks have been added in the risk table in Part A.
		Comment from Ethics committee Include Ethics requirements and relating description of action	Section 5, Section 3.2/ "Project Bodies and main Roles": Ethics requirements, relating deliverables and description of action have been added.
		Comments from Scrutiny committee	Section 6, Section 3.2/ "Project Bodies and main Roles": Comments by Scrutiny committee have been added.
		Comment from Financial Officer	Section 3.2/ "Resources to be committed"/ "Justification of resources and budget": Tables have been added/updated for more detailed justification of costs

Contents

SECTION 1.	EXCELLENCE.....	3
1.1	OBJECTIVES.....	3
1.2	RELATION TO THE WORK PROGRAMME.....	6
1.3	CONCEPT AND APPROACH.....	8
1.4	AMBITION.....	25
SECTION 2.	IMPACT	34
2.1	EXPECTED IMPACTS	34
2.2	MEASURES TO MAXIMISE IMPACT.....	38
A.	DISSEMINATION AND EXPLOITATION OF RESULTS.....	38
B.	COMMUNICATION ACTIVITIES	44
SECTION 3.	IMPLEMENTATION	48
3.1	WORK PLAN — WORK PACKAGES, DELIVERABLES AND MILESTONES.....	48
3.2	MANAGEMENT STRUCTURE AND PROCEDURES	52
3.3	CONSORTIUM OVERVIEW - INDUSTRIAL INVOLVEMENT AND VALUE CHAIN COMPLEMENTARITY.....	55
3.4	RESOURCES TO BE COMMITTED	57
SECTION 4:	MEMBERS OF THE CONSORTIUM.....	60
SECTION 5:	ETHICS AND SOCIETAL IMPACT	98
SECTION 6:	SECURITY	127
6.1	SECURITY ASPECT LETTER	127
6.2	SECURITY CLASSIFICATION GUIDE.....	127
6.3	SECURITY STAFF.....	127
6.4	OTHER PROJECT-SPECIFIC SECURITY MEASURES	128
ANNEX.....		129

Section 1. Excellence

1.1 Objectives

The main objective of iCROSS is to **enable faster and thorough border control for third country nationals crossing the land borders of EU Member States (MS), with technologies that adopt the future development of the Schengen Border Management.**¹ iCROSS includes software and hardware technologies ranging from portable readers and scanners, various emerging and novel subsystems for automatic controls, highly reliable wireless networking for mobile controls, and secure backend storage and processing. **iCROSS designs and implements a comprehensive system that adopts mobility concepts and that consists of a two-stage-procedure, designed to reduce cost and time spent per traveller at the border crossing station.** The project envisages an optimal mixture of an enhanced but voluntary form of a Registered Traveller Programme (RTP) and an auxiliary solution for the Entry/Exit System (EES) based on involving bona fide travellers.

Continuous traffic growth, combined with the increased threat of illegal immigration, is putting nowadays border agencies under considerable pressure. Slow border crossings impact traveller satisfaction, business and trade. According to the Cockfield Report in 1980, the estimated income from abolishing controls on internal borders gave a rise as much as 2.5% of the annual GDP of the Member States. Calculating with figures from 2011, this means 232 billion EUR annually. A smaller, but still considerable rise in the EU GDP can be achieved through better facilitating border checks – and so, commercial traffic – at external borders. At the same time as making the border clearance process as streamlined as possible, the authorities need to make checkpoints safe and secure but also consider the limitations coming from human resources. Border checks become increasingly more challenging due to increased international trade, more complex supply chains and more sophisticated criminal activity. They also need to do all this at lower cost.

iCROSS focuses on the land border crossing points: road, walkway, train stations. It addresses the better facilitation of thorough checking required for third country nationals that intend to cross EU borders. To this respect, iCROSS specific objectives are:

- To **significantly increase the efficiency in terms of traveller throughput** at the border as well as security in terms of significantly fewer successful illegal crossings;
- To achieve greater comfort, **reduced time at the border** by utilising the portable traveller devices and portable units;
- To utilize **pre-registration step** as a means to better inform travellers of their rights, the procedures they will have to go through for their travel, the data collected and how they are analysed as per EU and national legal requirements and to obtain, where necessary, an informed consent from the traveller.
- To **reduce the subjective control and workload of human agents and to increase the objective control** with automated means that are non-invasive and do not add to the time the traveller has to spend at the border;
- To **create of a fifth tier** for the four-tier access control model of the Integrated Border Management System involving bona fide travellers, especially regular travellers into a Schengen-wide frequent traveller programme including a reward system based on number of successful crossings and trouble-free stay.

As mentioned above, iCROSS system consists of a two-stage procedure that includes the following:

First Stage (1) the registration before the travel to **gather initial personal, travel document and vehicle data, perform a short, automated, non-invasive interview with an avatar, subject to lie detection** and link the traveller to any pre-existing (at the authorities) data. Utilizing advanced multifactor analytics and risk based approach the data registered by the traveller is processed but also correlated with publicly open data (i.e. social media profile, google search etc.) or external systems such as the Schengen Information System (SIS II). Processing will need the travellers consent and they will be granted access to SIS II data related to their person and belongings as set in EU legislation and national law (exercising the fundamental right of freedom of information).²

Second Stage (2) the **actual control at the border** that complements existing (pre-registered) information with results of security controls that are performed with a **portable, securely wireless connected, iCROSS unit** that can be used inside buses or trains or at any other point. Multiple technologies check validity and authenticity of various parameters within travel documents, visa, face recognition between traveller and passport picture; real-time automated non-invasive lie detection in interview by officer, etc. The wealth of data and links collected are encrypted,

¹ See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP) - COM/2013/096 final - 2013/0060 (COD)

² Articles 41-43 in Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). For national legislation please see example of 26.§ of the Hungarian Act No. CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System.

securely transferred and analysed in real time, providing an automated decision support system for the border control officers.

These procedures are separated based on two important criteria:

- (i) Information that the traveller can easily provide to the system with commonly available equipment of the portable devices or home based office equipment (scanner, photo camera, etc.) and
- (ii) estimated needed time for the integrated system to capture and process the necessary information i.e. capturing of video-audio conversation with an avatar for deception detection requires at least a few minutes conversation that should not delay the actual border control.

The two stage procedure enables multiple processing and cross-correlation of data and consultation with external systems without the pressure of delaying people, or vehicles from continuing their journeys. Travellers crossing the border with their own vehicle have to register their vehicle information.

Travellers' legal rights are addressed both at the European as well at the relevant national levels when collecting, storing and processing relevant data through the iCROSS legal framework. It is underlined that the participation in is not compulsory, it works on a voluntarily basis, offering ease of control for travellers willing to cooperate with authorities to speed up the border control.

The process incorporates novel mobility concepts, including the use of traveller's personal computing devices and sensors built into them to collect data at the pre-registration stage and dedicated secure devices at the border crossing to validate and further assist border guards in their decisions. These include face pictures, scans or pictures of all available and relevant travel documents and other data. The traveller will be informed about other documents to be requested at the border crossing (e.g. marriage certification, work contract, certificate of admission to school etc.). The traveller may also provide travel plan (time and place of entry), so that the authorities can better manage resources and diminish waiting time.

Based on the above, iCROSS addresses the main and specific objectives by research which has a dual focus:

- (a) **theoretical**, in terms of defining legal and functional requirements, novel border control concepts – for example a fifth tier to the four-tier access control model³ - and technologies as well as the controlled parameters and their contribution to the dynamic, intelligent, integrated risk assessment module enhancing the Common Integrated Risk Analysis (CIRAM) model currently in use. In particular risk factors will be defined to address the cumulative (based on multiple automated tools) estimated degree of malicious intent, involvement or intention of illicit activity, and real time detection of falsified, invalid, or mismatching of traveller travel documents, empowering the human agent to make more accurate decisions during border control operations, and
- (b) **applied**, whereby the technologies will be developed, integrated, deployed and validated with relevant robust quantifiable risk factors to ensure reliability, effectiveness and speed of border checks.

iCROSS integrated system provides automation of multiple key border control tasks which are organised in the following steps:

- A. A **pre-arrival registration and preliminary check of entry and stay requirements** where the traveller has to provide certain information before travelling and includes two phase:
 - (a) the registration of traveller related information (i.e. personal identification, travel documents),
 - (b) answer a set of questions about how they obtained their documents and their travel intentions, and
 - (c) the registration of trip related information (i.e. e-tickets, visa, etc.).

Registration must be personal, as from 2006 the one-travel-document-per-holder is a general policy (see EC Regulation 2252/2004 Art. 4, section 3).

The pre-arrival check results into a risk classification of each traveller that ranges from low to high. The travellers receive a personal notification (i.e. QR code) to their mobile device to facilitate the actual control to fast and easily retrieve the processed information and guide the next steps at the border crossing station.

- B. The **humans border control at the crossing station**. In line with the Schengen Border Code regulations, all travellers have to undergo border control when crossing the external borders of the Schengen Area. EU citizens and their family members undergo a minimum check, while third country nationals undergo a thorough check that complement the preregistered information. The personal code, generated at pre-arrival control phase, is used for fast retrieval of the traveller's processed information at the crossing point and guides the next procedural controls necessary. The minimum additional control will need just one biometric authentication and travel document scanning to verify that the person is the one that is holding the travel documents at hand, while the maximum control will use all the control functions offered.

³ The four tiers of the model are:

- ☐ activities in third countries, countries of origin and transit
- ☐ bilateral and international cooperation (cooperation with neighbouring countries)
- ☐ measures at the external borders
- ☐ activities inside the territories. (Council 2002a: 11)

C. Traveller's **vehicle control**. Currently during actual border control vehicles have to be checked for being illegally transported or stolen with manual check for condition (damages, missing parts, tires, the vehicle's cabin (passenger cab), trunk and the engine bay, with additional option of searching the entire vehicle (including partial disassemble) for drugs and illicit goods. On the other hand for cargo trains specific respective control procedures are dictated as well. However, in the majority of the cases and depending on traffic flows, vehicles or trains (passengers or cargo) are not systematically checked for hidden humans. The vehicle control also includes a search for vehicle identification (type, colour, VIN, number plate) in the Schengen Information System, verification of vehicle insurance and driving license of the driver, which could be part of the iCROSS vehicle pre-registered control. In some countries, the vehicle is also registered in the national entry/exit system. In this context, complementing the vehicle pre-registered control, during actual border control the iCROSS project provides the additional option the vehicles or compartments (e.g. in trucks or cargo trains) to be checked for hidden people with portable or deployable modules (based on radar and acoustic/sound sensors). This option is meant to test and prove integration ability and operation applicability; paving the way for future inclusion of potentially portable devices of other technologies used both for hidden humans or illicit goods detection.

Direct interaction between the authorities and the pre-registered travellers is enabled during all stages to exchange information (notifications about upcoming checks, waiting time, rewards and honours, rights and obligations in destination country, remaining days of stay etc. This system also facilitates notifications and alarms for the authorities as well for the traveller allowing the traveller to act in time, (i.e. when a traveller visa expires, etc.), thus avoiding a wasted journey through refused entry or expulsion. It also enables a deep interview with the traveller before travelling, enabling better specialization for border guard personnel and less waiting time at border gates for *bona fide* travellers.

[REDACTED]

[REDACTED] Furthermore the following systems are included:

- I. A **securely accessible web interface** will be provided for travellers to register and guide them to provide the required information for the pre-arrival control. This will be presented in the form of workflow that shows the steps and the progress in the procedures and is executed at the backend by cloud infrastructure with enhanced security.
- II. A **portable hardware iCROSS unit will be devised including:**
 - a) **dedicated portable travel document scanners** to capture the travel documents (e-tickets, passports, ID cards, etc.) State of the art and off-the-shelf document readers and scanners with advanced features such as UV scanning will be integrated etc.
 - b) **biometric scanners** that capture state-of-the-art biometrics such as fingerprints, faces, veins, etc.
 - c) **portable modules** based on radar and acoustic sensors **to facilitate hidden human detection (HHD)** within vehicles, trucks or closed compartments triggering a more thorough inspection on a secondary level
 - d) **body mounted cameras**, based on those currently in use by police officers to monitor compliance with professional standards, **in this case to capture and process non-verbal features required for lie detection at the crossing point.**

- e) **the battery pack** which supplies electricity for all set elements. It can be also considered as a back-up power while working in the operating area.
- f) **touch screen** showing **information obtained** in the course of border control.
- III. **Automatic Deception Detection System (ADDS)**, which analyses Non-Verbal Behaviour (NVB) will provide an estimated level of deception based on analysis of the video-recorded question-answer session. Questions will be unpredictable by the traveller will target issues based on the traveller's data and profile analyses. For example questions will target assessing deception attempts by third country nationals entering the EU as economic migrants and engaging in terrorism, human trafficking and drug smuggling. These risk factors will also be passed to the human border agent, who will be supported by ADDS at the border crossing.
- IV. **Document Authenticity Analytics Tool (DAAT)**, which performs straightforward verification of travel documents. Building on top of existing systems (iFADO) the aim is improve response speed and efficiency.
- V. The provision of **Biometric Analytics (BIO)** that process the biometrics captured by the related devices of the portable hardware unit, etc., already included in the e-Passports of many countries, but also emerging and promising ones that enhance the security of the procedures (iris, vein, etc.)
- VI. The **Face Matching Tool (FMT)** that captures the face of the traveller at each stage and correlates it with the one in the travelling documents to estimate the probability that the travel document belongs to the traveller and that the same person completed the pre-arrival registration stage. With e-passports increasingly adopted this matching is further facilitated and addresses more efficiently variations and discrepancies such as aging, lighting, occlusion due to glasses or facial hair, etc.
- VII. **Vehicle Control Module (VEHC)** which will control and process the vehicle registration against cloning, alteration, theft and unauthorized use as well as status of international insurance bond.
- VIII. The **iCROSS integrated automated border control Risk-Based Analytics Tool (RBAT)**, will utilize state of the art risk based approaches to intelligently fuse all data collected and risk estimated and classify travellers to facilitate the human agent task.
- IX. A **human border control portable Agent User Interface (AUD)**, to visualise in real time the quantified metrics resulted from the sub-system analytics, guide the processing required and allow the agent to correlate the result with his own perception of the traveller.
- X. **Intelligent Border Control Analytics Tool (BCAT)** that performs analyses utilizing advanced computational intelligence based approaches in order to evaluate the performance of iCROSS systems discovering key patterns in the data that would help quickly identify False accept or false rejects of travellers based on the data collected in the Pilot study. The BCAT will use advanced algorithms based on machine learning, neural networks as well as statistical approaches to determine the confidence in the produced results.
- XI. **Wireless connectivity with ensured QoS will be provided through a high reliable radio network, involving wireless mobile and satellite access techniques**, by addressing respective Physical layer and Radio Resources Management challenges, with Optimum synergetic radio networks design, including scenarios with high speed vehicles (bus, trains, etc.), Analytical end-to-end models for the evaluation of cooperative transmission techniques and Development of a new unified resource management framework as well as relevant algorithmic solutions for coordinating and optimizing user access to ultra-dense networks.

Legal and ethical issues will be systemically considered to enable legal compliance with privacy, non –disclosure of sensitive information related to current and potentially future border control procedures, and legal training in issues related to the use of automated systems involved in border control tasks.

Real life experimental evaluation with both border guards and travellers across 4 European countries iteratively, covering a large scale of diverse requirements for land border control (bus, train, vehicles, pedestrian, etc.) with human border control experts and travellers will enable the validation of the proposed technology. Key performance metrics will not only focus on *False Accept rate* and *False Reject Rate of illegal travellers* but also on monetary (acquisition and maintenance), time, effectiveness and reliability associated with each task.

Dissemination of the project outcomes to key stakeholders, including border control and policing institutions, key policy makers and researchers in border control related issues and **to facilitate further research and new market opportunities** towards the border control research community.

1.2 Relation to the work programme

The following table lists how each of the presumed border control abilities as listed in the call topic BES-05 is addressed in the iCROSS Platform proposed solution:

BES 5 topic	iCROSS Platform proposed solution
Border control is likely to face increasing demands for efficiency, implying need for	iCROSS focuses on enhancing operational conditions at the border crossing stations in terms of:

<p>technical systems that are user friendly and reliable in operational conditions.</p>	<ul style="list-style-type: none"> • efficiency and accuracy, reducing time needed at the border crossing stations due to the iCROSS secure agent mobile system that allows faster and more accurate processing of the required information and the inclusion of pre-arrival control phase. This supports the efficient use of border control personnel by empowering them to utilize state of the art technologies to perform their duties while reducing subjectivity and human errors. • user-friendly human empowerment, is ensured by the use of web technologies familiar to the traveller, with a user friendly intuitive web interface to get informed about their rights, provide consent and provide data. The border agent portal will share on the same design and technology benefits but will be protected through a secure intranet system empowering agents by: <ul style="list-style-type: none"> ○ Providing direct access to traveller data ○ Providing decision support based on advanced analyses of traveller data including targeted issues the traveller needs to be further examined for. ○ Providing metrics derived from specific components of traveller's data. ○ Providing overall metrics for border crossings, including number of travellers expected to cross based on predictions derived from pre-registration information and correlation with past similar occurrences. • the incorporation of pre-arrival control for reducing actual border control, the portable control unit that removes the burden of getting out of vehicles and delays in travelling times, the possibility of continuous interaction between the traveller and the authorities, and the reward system, shaped after the current trend of gamification, transforming traveller risk analysis into a special treat, making frequent and benevolent travellers proud of their achievement. • reliability in operational conditions is ensured by the iCROSS scalable design and that a large part of the control, which burdened the operational IT infrastructure, will be done in advance, saving operational resources. Furthermore the ability of the system to warn in advance border control authorities of border crossing traffic will further help better manage resources.
<p>... use technology from adjacent markets such as mobile or satellite telecommunications, could help the costs of processing down to a minimum. In particular, the use of passengers' personal mobile devices is expected to enable efficient and reliable identity checks through the application of biometric technology...</p>	<p>With the iCROSS Platform, travellers will mainly use their own devices for pre-arrival check, saving resource in terms of operational lifetime of border guard equipment, which can accumulate to a significant saving in money, corresponding to the entire Schengen Area.</p> <p>Deployment of state-of-the-art biometric technology and the ADDS will result in reliable identity checks and efficient traveller risk assessment.</p> <p>Furthermore the prescribed QoS of the wireless connectivity will be guaranteed using, in an optimum combined and synergetic way, the transmission capabilities and the technological advances that are offered from mobile and satellite telecommunication networks. More specifically, iCROSS addresses this issue through the efficient and cost effective design of the radio network by taking advantage of the radio environment (propagation conditions, switching between technologies, optimum installation of radio relay nodes, antenna diagram and power allocation optimization, cooperative strategies etc.) and finally by minimizing the total energy consumption.</p>
<p>The ability to automatically and rapidly detect document forgeries is also expected to be further improved.</p>	<p>Several novelties are proposed for the automated and rapid process of document forgeries. Documents not only concern the official travel documents (passports, visa, etc.) but also other documents, such as tickets, vehicles ids, etc. There is the two stage procedure that allows multiple checks and cross-correlation with external systems. Furthermore, the integration of the FMT to calculate the probability the passport holder is the person depicted in the passport. Connected to the iFADO software, the DAAT will be able to detect forgeries initially at pre-arrival phase with the use and control of visible security features (MRZ checksums, OVI, iris printing etc.) and more detailed with reduced needed time at the crossing point in a mobile version with improved features in accuracy and time. The RBAT elevates the process and security to new levels, by calculating a cumulative risk factor for each specific traveller.</p>
<p>...novel concepts relying on the use of traveller's personal mobile devices, and/or border</p>	<p>iCROSS is designed by involving border control experts who, after reviewing current procedures and requirement studies, as well as the state of the art on how to address each requirement using novel technologies, incorporated these technologies into the iCROSS platform. The technologies make use of personal web accessible mobile devices at the</p>

<p>authorities' specific mobile equipment, for high security level passengers' identity control. ...biometric identification of travellers inside vehicles (cars, bus, trains as well as pedestrians. Portable Automatic Border Control (ABC) gate for land boarder (could be used at lanes outside the terminal)</p>	<p>pre-registration phase expanding the data availability per subject and enabling especially in the case of no risk frequent travellers the quick crossing while highlighting both the high risk travellers as well as the reasons for that assessment. With this new approach we engage bona fide travellers and ease their border crossing as well as creating an individual traveller risk assessment method never seen before.</p> <p>The iCROSS secure mobile agent unit will be developed incorporating secure wireless connection with guaranteed quality of service (QoS) allowing the agent to perform the complete additional check and have access to all pre-existing traveller information and decision support inside vehicles (buses, trains, cars, or for pedestrians) without delays and procedures requiring people disembarkation, manual processing. Advanced biometric sensors will be built into the unit (body mounted camera for face and deception recognition, fingerprint, palm vein) to enable the mobile collection of data empowering the agent to make quick and accurate decisions. A specific use case for the train travel will demonstrate how the control can be executed during the actual train travel without stop between the two train stations that connect the border.</p>
<p>Novel technological solutions and procedures to manage relevant associated workflows (to be validated by border guards in a realistic operational scenario)</p>	<p>iCROSS is designed around the existing border control workflows expanding relevant nodes with state of the art technology. The entire system results in a complete re-engineering of the procedures enabling robust automated border control, that includes steps for the traveller to provide requested information starting from the pre-arrival phase, dialogues to engage in video-audio conversion providing higher security levels, and procedures that decide and guide the border control at the crossing station based on cumulative risk from the traveller. The process involve all the steps and procedures that guide the work of the agent. They will be validated in real operational scenarios depicting the variety of cases (train, vehicle, pedestrian, etc.) in 4 EU countries with border to countries outside EU.</p>
<p>Legal, ethical or social implications must be taken into account</p>	<p>iCROSS solutions will be developed in line with the European Charter of Fundamental Rights, the Schengen Border Code, the Visa Code, the Schengen Best Practice Handbook for Border Guards (through inputs from our end-users) and the Code of Conduct for Border Guards (issued by FRONTEX). Data protection legislation will be taken into account as well, including the Prüm Convention for facilitating data exchange between MS law enforcement agencies. Specific partner (LUH) is responsible to ensure that the system is designed to address all legal, ethical and social issues.</p>
<p>New opportunities for European leadership in European, international markets</p>	<p>iCROSS provides the opportunity for the partner industries to develop necessary solutions and products which have the ability to provide competitive advantage for European industrial partner internationally. Europe will rely on own technological expertise and will need not to adopt technologies from abroad.</p>

1.3 Concept and approach

1.3.1. Rationale

“The story began in 1985, when five EU states decided to abolish internal border controls – the Schengen area was born. On a continent where nations once shed blood to defend their territories, today borders only exist on maps. A Europe without internal borders brings huge benefits to the economy as well, which shows how tangible, popular and successful the Schengen achievement is and the importance it has for our daily lives and for our societies. We need to preserve and reinforce this common achievement.”⁴

Similar advantages can emerge from the efficient, harmonised and secure border crossing of external borders of EU. According to an EC General Directorate of Migration and Home Affairs publication⁵, as a whole non-EU residents contributed €271 billion to the economy when travelling to the EU in 2011, most of them being business travellers, workers, researchers and students, individuals with close family ties to EU citizens or living in regions bordering the EU. Every year, more than 700 million⁶ external border crossings take place at the EU borders out of which about a third are made by third country nationals. Moreover, these figures are continuously rising as a result of an increasingly interconnected world.

On the other hand, illegal human trafficking has constituted one of the major challenges to the affected EU member states and organs in charge of EU border security. EUMS & Schengen Associated Countries reported more than

⁴ EC leaflet “Europe without borders: The Schengen area”, Directorate-General for Migration, Home Affairs and Citizenship

⁵ http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm

⁶ “EU Border Security”, Government Gazette, March 2013

280,000 detections of illegal border crossing⁷, which was twice as many as the previous record of 140,000 detections in 2011, the year of the Arab Spring. Out of these numbers, only in 2013, there were around 9,800 detections of migrants using document-fraud to enter the EU or Schengen area illegally⁸. Approximately 224,000 refugees and immigrants have arrived in Europe passing through the Mediterranean Sea since the beginning of year 2015, as announced quite recently (first week of August) by the United Nations High Commissioner for Refugees (UNHCR)⁹. Given the explosive increase of around 300% (in the first half of 2015 vs. same period of 2014) of the number of immigrants who entered illegally in Greece, the official reports evidence an “arrival” in Athens by an average of 1,200 immigrants per day. It is absolutely clear that the ultimate goal of all the above categories is the entrance to European and Schengen countries through the Greek land and train borders between Greece / FYROM and Bulgaria. Especially, the Greek / FYROM borders (Eidomeni/Geygeli check points of Greek/FYROM land and train borders) tends to be, recently, vastly crowded. And this goes further, more intensified, in the land borders of FYROM / Serbia and Serbia / Hungary forming a pathway of tragedy especially when a country has extensive land borders or uneven and hard geomorphology. This pathway is given in the following frame, in order to absolutely justify the selection of the specific pilot sites by the iCROSS project (described later in further detail).

Given the size of the conflicts along North African and Middle East, the numbers previously given are quite modest considering what’s next in respect to the size of the problem. *“It is clear that we need a new, a more European approach”* pointed out in a joint statement the relevant EU Officers, France Timmermans, first vice President of EC, Federica Mogherini Responsible for Commission’s foreign policy and Dimitris Avramopoulos, Commissioner of Immigration. The correct balance is inevitably needed for protecting and promoting mobility and travel on one hand, and on the other hand, the need to preserve a safe and secure area within the EU while respecting the highest standards of human rights. The “smart border” initiative is part of the EC agenda since 2008, where a more modern and efficient border management is proposed, in order to speed-up border crossing for regular travellers but also facilitate and reinforce border check procedures for foreigners travelling to the EU using the external borders.

It is obvious that the EU needs now, more than ever, new, user-friendly, mobile and reliable technologies to be adopted and customised accordingly for the border check process, so as to simplify life for foreigners frequently travelling to the EU and to better monitor third-country nationals crossing the borders. Mobile technologies and cloud-based services are rapidly changing the IT landscape, are assumed to be robust technological components and therefore can be taken under serious consideration when designing novel border management services. The same stands for the growing computational power and the low-cost mobile devices, smartphones, etc. *“the world is home to 7.2 billion gadgets, and they’re multiplying five times faster than we are”*¹⁰ - which can make new border management tools increasingly accessible to nearly every traveller and border agent, around Europe and the world.

Most EU countries apply the same border control rules to non EU-citizens coming to the EU. Common rules make it easier for people coming to the EU. They are also important for the EU’s border-free travel zone throughout which authorised travellers can move freely without passport controls between EU countries.

To this end, having in mind that nowadays border control is like looking for a needle in a haystack and that most people crossing a border are law abiding and honest, iCROSS aims to implement a novel but “light-touch” processing for these people going through land borders. iCROSS combines portable and security-driven technologies to speed-up and automate the procedures, ending up finally to a robust mechanism for “moving the hay aside so that the needle is easier to find”.

Refugees’ pathway through Greek / Serbian / Hungarian land and train borders

The refugees in their vast majority arrive by bus or taxi from Athens at the border with FYROM in Eidomeni and Evzoni land borders. Illegal transfer was enormous in previous years, since they lodged in the forests and fields of the Greek borders waiting for the chance to enter the neighbouring country or were falling victims of exploitation and trafficking, paying handsomely for entering FYROM.

Thus, the illegal manner of the transfer was reduced due to governmental policies and political reasons and not because of technical aids and systems that could help a better classification; holistic systems like airport check points or technical aids of such character in some cases and in certain countries simply do not exist at the land borders. Buses and taxis disembark refugees in the neutral zone, a short distance from the station Eidomeni, where the Greek trains (TRAINOSE) running route from Thessaloniki to Belgrade enters the territory of FYROM in sealed wagons, so if during the journey identify illegal passengers. However, in any case, the control is small, if

⁷ FRONTEX *Annual Risk Analysis 2015*

⁸ FRONTEX *Annual Risk Analysis 2014*

⁹ «Η ΚΑΘΗΜΕΡΙΝΗ της ΚΥΠΙΑΚΗΣ» Greek largest Sunday newspaper, printed and online editions of 9/8/2015, following press releases of the UNHCR and the Hellenic Police. <http://www.ekathimerini.com/>

¹⁰ The Independent article “There are officially more mobile devices than people in the world”, Zachary Davies Boren, 7-Oct-14

¹¹ “Η ΚΑΘΗΜΕΡΙΝΗ της ΚΥΠΙΑΚΗΣ” Greek largest Sunday newspaper, printed and online editions of 9/8/2015, <http://www.kathimerini.gr/826645/article/epikairothta/ellada/maxh-gia-mia-8esh-sta-trena-ths-fyghs> Article “Battle for a seat in the trains of great escape”, Stavros Tzimas, 9-Aug-15, <http://www.ekathimerini.com/>

at all, limited only to visual inspection by guards, occasionally or indicatively, due to the volume of people and the lack of technical aids that would help a smooth and fast operation.

Railway Station Gevgelija, a few hundred meters from the Greek border Eidomeni, refugees are struggling to board the train covering local routes to Skopje and Kumanovo on the other side of FYROM on the border with Serbia. Up to 500 people are packed into three or four old and small wagons on a route that in previous years had only a few passengers if anyone at all. Nowadays however, the "trains of the great escape" are carrying thousands of Syrians, Iraqis, Kurds, Afghans, on their journey to salvation. About 1,500 passengers travel daily into the city of Skopje and Kumanovo in the north, where they hope that they will pass secretly across the border into Serbia. Crews of Slav-FYROM police record them, providing a residence permit of 72 hours on the territory and transfer them through bus to the small railway station Gevgelija, to board the trains. Others, those who can pay "well", find coach or taxi to Serbia at Kumanovo in FYROM-Serbia borders. However, the passage in Serbian territory through wooded areas is not easy, as the authorities of the country follow a stricter policy, having developed strong police forces assisted by armed detachments of Hungarian, German and Austrian police and having set up "reception centres" in the Presevo Valley. Serbs, unlike Greece, FYROM and Bulgaria, do not follow policies facilitating transit flows for the additional reason that the refugees end up trapped at the Serbian – Hungarian borders. The borders with Hungary are the gateway to the final destination in West Europe and this time are considered to be the most "hot" zones of Europe in the refugee issue. Despite the strict measures there, thousands of people of all ages arrive (with the help of unscrupulous traffickers) near the town of Subotica, in order to go to Hungary. The fear of forests and plains of Vojvodina possibly being flooded with refugee crowds of Syrians and Iraqis scares both Serbs and Hungarians with the latter working feverishly to raise a steel fence of 170 km length in order to confront attempts of violent invasion, similar to that in Calais, France.



The situation described in the passage above, shows that the way of the refugees from Greece to western Europe includes the train trip through Eidomeni station. The train pilot was conceptualised to address this problem. According to preliminary analysis of requirements it was indicated that two issues arise during train trips:

1. the majority of people that want to travel through the borders illegally they board on the trains and hide there, since they don't possess all the papers for proper border check.
2. Those who do not hide and go through the process legally, follow the existing procedure of checking the papers within the train. The train stops at the border and the border police agent is boarding on the train and collects all papers and passports. He is bringing them to his office to check. When done he brings them back to the train and gives them to the passengers.

1.3.2. Project positioning in terms of Technology Readiness Level

The following figure illustrates the TRL of iCROSS technological components.

Project results in relation with TRL	TRLs at project start	TRLs at project end
Integrated cloud iCROSS system	-	5
ADDS	5	7
RBAT	6	7
DAAT	7	8
Biometrics (face, fingerprint)	7	8
Biometrics (vein..., iris)	4	5
Portable HW unit	-	5
Portable HHD unit (radar & acoustic sensors)	3	5

Fig 1: iCROSS TRL illustration

1.3.3. Previous research and innovation activities linked with the project

The project is well positioned in terms of the State-of-the-art, defined by research projects at European and international level, which have already been taken into account for their concepts and published results, and goes beyond national and international research projects with concrete opportunities for synergy or adoption of projects results, because of the existing contacts from the consortium which are listed below:

Project	Description	iCROSS relevance
FASTPASS FP7 SECURITY	FastPass establishes and demonstrates a harmonized, modular approach for ABC gates. Fastpass will serve both demands at the same time to keep security at the highest level while increasing the speed and the comfort for all	iCROSS goes beyond the results of FastPass by improved traveller identification technologies, such as new biometric modules, the ADDS, the portable HW and HHD units, the

	legitimate travellers at all border control points aiming at a minimum of privacy intrusion.	risk based approach, etc., will increase the security of the process and minimize spoofing.
ABC4EU FP7	ABC4EU identifies the requirements for an integrated, interoperable ABC system, respectful of citizens' rights, at EU level, taking account the future needs derived from the Smart Border and other EU and national initiatives and paying very special attention to citizen rights, privacy and other related ethical aspects. ABC4EU focuses in the need for harmonization in the design and operational features of ABC Gates, considering specially the full exploitation of the EU second generation passports and other accepted travel documents.	The ABC4EU system is of particular interest for iCROSS, and particularly its deployment in the real-life scenarios (not yet implemented), but goes further by introducing the pre-arrival phase, where much query time is preserved. Furthermore, innovative tools, such as the Avatar which, working with ADDS, will detect human stress and deception through face analyses, are adapted.
MOBILEPASS FP7	MOBILEPASS focuses on research and development towards technologically advanced mobile equipment at land border crossing points. Border control authorities can check European, visa-holding and frequent third country travellers in a comfortable, fast and secure way. The mobile solution incorporates new technologies needed in mobile scenarios and embeds them in the actual border crossing workflow to speed up control procedures.	iCROSS will consider this project results and will integrate any suitable approach. However, iCROSS goes far beyond by providing an integrated comprehensive environment, of which MOBILEPASS maybe an interesting component.
EFFISEC FP7 project	EFFISEC delivers to border authorities more efficient technological equipment for identity and luggage control of pedestrians and travellers inside vehicles, at land and maritime checkpoints, while maintaining or improving the flow of people crossing borders and improving work conditions of border inspectors, with more powerful capabilities, less repetitive tasks, and more ergonomic equipment.	iCROSS will consider the results of this project and will integrate any suitable approach, especially regarding to human/goods detection component and envisages of a more complete, integrated solution that will deal with all aspects of land border control.
TABULA RASA FP7 project	Analyses weaknesses of biometric identification process software in scope of its vulnerability to spoofing, diminishing efficiency of biometric devices. The goal is to provide more resistant systems and standards for protection of biometric devices against spoofing.	iCROSS will use results of TABULA RASA to protect the planned solutions against spoofing or impersonation.
eGate External Borders Fund, Hungary	The pilot deployment of an ABC system financed of Schengen External Borders Fund in Hungary at Budapest Liszt Ferenc International Airport in 2014.	HNP will share lessons learned, experience and results on use of ABC gates by travellers and time to pass compared to manual minimum check with other iCROSS members.
Next Generation VIS, Hungary	Supported by External Borders Fund, With the deployment of fingerprint readers for TCN control, this new system allows first line officers to check visa holder's identity with biometrics. HNP was participant of the pilot project aimed at testing the innovation for all MS.	HNP will share lessons learned, experience and results on use of new VIS technology including deployment experience to facilitate pilot deployment for iCROSS.
BEAT - Biometrics Evaluation and Testing SEC-2011.5.1-1	The BETA project implements a framework of standard operational evaluations for biometric technologies with an online and open platform to transparently and impartially assess biometric systems against validated benchmarks, create protocols and tools for vulnerability analysis, and develop standardization documents for Common Criteria evaluation. Moreover, the project deals with the legal implications connected with biometric devices. In addition, because of the influence of the results on the standards, decision-makers and officials will be kept up-to-date with the progress made in the field of biometrics.	iCROSS will consider the BETA project's results in the area of technology assessment. Particularly relevant will be the issue of arising legal implications with regard to state-of-the-art biometric systems, which can be taken into consideration in the iCROSS project.

1.3.4. The overall approach and methodology

a. Legal Compliance and legal Policy Makers synergy

Art. 7 and 8 of the European Union's Charter of Fundamental Rights declare the right to respect someone's private life and the protection of personal data as fundamental rights for everyone in the European Union. Data Protection and Respect to private life are therefore core values within the European Union. The importance of data protection and privacy of individuals have been further strengthened during recent years in particular through two judgements of the European Court of Justice. The first one declared the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) invalid.¹² *The Court takes the view that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.*¹³

The second one declared (some kind of a) right to be forgotten against search engine operators. The data subject can demand that a search engine has to delete links to the data subject.¹⁴ Especially the judgment regarding the Data Retention directive shows that the processing of personal data through state authorities is not per se and necessarily compliant with fundamental rights in any case, even if it is foreseen to fight terrorism and crime. Nevertheless, the right to privacy can also be limited to ensure other (fundamental) rights which might be afflicted, like in the context of iCROSS the Right of Liberty and Security declared in Art. 6 of the Charter. Such limitations of the right for privacy or the protection of personal data could be set in relevant EU and member state legislation concerning border control measures, e.g. limitations to freedom of information in the Prüm Convention¹⁵. In a rather recent case, the CJEU declared the usage of digital fingerprints in identity-cards and passport-control scenarios as in principle compliant with European primary law and stated that national law does not necessarily have to exclude secondary usage of biometric data (CJEU, C-446/12 to C-449/12).

The use of technologies at the borders of the European Union, as proposed in iCROSS, enables state authorities to collect and process personal data, in the way that data subjects cannot deny the collection and processing of their data if they want to enter or leave the territorial of the European Union. Due to these circumstances, the proposed data processing cannot be justified on a basis of informed consent, but only on a legal basis which allows it. Systems like video and audio surveillance or additional data collection from other resources like social media without the knowledge of the traveller affect the rights of privacy and protection of personal data. Especially the collection of personal data by state authorities without the knowledge of the traveller, e.g. social media content, might not be allowed in every single member state based on its current laws. This might not be decisive in cases of publicly accessible profiles, as this kind of information might not fall within the scope of data protection regulations, but at the same time suggests new issues to be regarded, such as fake profiles which might affect the value of the information contained. Also state authorities may have specific restrictions and requirements concerning the use of hard- and software, like the use of cloud services. Therefore the project will investigate whether measures proposed by the project can be legally justified with the goal of improving cross border travelling as well as the work of border agents. It is understood that the project takes place in between the conflicting priorities of data protection and the need for national security, consequently between fundamental rights of individuals and the need to protect the general public. On these grounds, the project will firstly demonstrate the legal system of the EU and the implementation of relevant EU law by its member states. This will be followed by an analysis of the legal framework at European level and their transposition into the relevant member state law. Furthermore the relevant future legislations like the proposed Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union (COM(2013) 95 final) will be considered. This will be done in close cooperation with other European projects on crime prevention LUH was or is actively involved in such as CITYCOP, SMART and RESPECT.

Depending on these results requirements of a possible future legislation concerning the use of such proposed techniques will be evaluated and a conclusion given. A starting point will be an examination of the judgements of the European Court of Justice concerning the Data retention directive and the regulation to store fingerprints on travel documents. Furthermore there are several regulations and jurisdictions as well as bylaws on international and national level that will be assessed in respect to data protection and data security, for instance the Schengen acquis¹⁶, which

¹² ECJ, 8.04.2014, C-293/12 and C-594/12.

¹³ ECJ, Press release, curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

¹⁴ ECJ, 13.05.2014, C-131/12.

¹⁵ "Police Robots and the Prüm Convention - Compliance ..." 2015. 10 Aug. 2015

<http://www.academia.edu/10208625/Police_Robots_and_the_Pr_Convention_Compliance_Study_on_Police_Robots_and_Freedom_of_Information>

¹⁶ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33020>

has been concluded in order to create a safe situation in an area of open borders.¹⁷ Schengen area is now part of the legal and institutional framework of the EU. It is therefore an area of parliamentary and judicial scrutiny, and attains the objective of free movement of persons enshrined in the Single European Act of 1986.¹⁸ It has been founded by several Treaties, such as the Accession Treaty¹⁹, the Implementation Treaty²⁰ and the Prüm Convention that will be evaluated. Further the Schengen Border Code²¹, Visa Waiver Regulation, Visa Code, FX Regulation, European Border Guard Teams, EUROSUR Regulation, Biometric passport regulation and the directive on free movement will be analysed. Additional on these findings technical requirements will be proposed to protect personal data to comply with existing legislation and to minimize possible intrusions in the right to protect personal data and privacy.

iCROSS's Data Protection Framework will guarantee that the system development as well as the system deployed will work as privacy-benchmark in the area.

The project's data protection and data security framework will guarantee the non-disclosure of personal and/or other sensitive information related to current and potentially future border control procedures. In addition, legally sound best practices in the use of automated decision support systems in border control will be presented. Legal systems often require (in their data protection laws) that final decisions having an impact on citizens' rights are taken by a human and not a machine. iCROSS will allow a machine-human interaction that supports maximum efficiency without jeopardising the data subject's right to be subject of human decision-taking. iCROSS will build on work already undertaken in SMART²² and RESPECT²³, making use of the model laws developed there.

b. Technical approach

[REDACTED]

[REDACTED]

[REDACTED]

¹⁷ *Hufnagel, Harfield, Bronitt*, Cross Border Law Enforcement, Regional Law Enforcement Cooperation- European, Australian and Asia – Pacific Perspectives, p.112, Abingdon, Oxon 2012.

¹⁸ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33020>, last viewed at August 12th 2015.

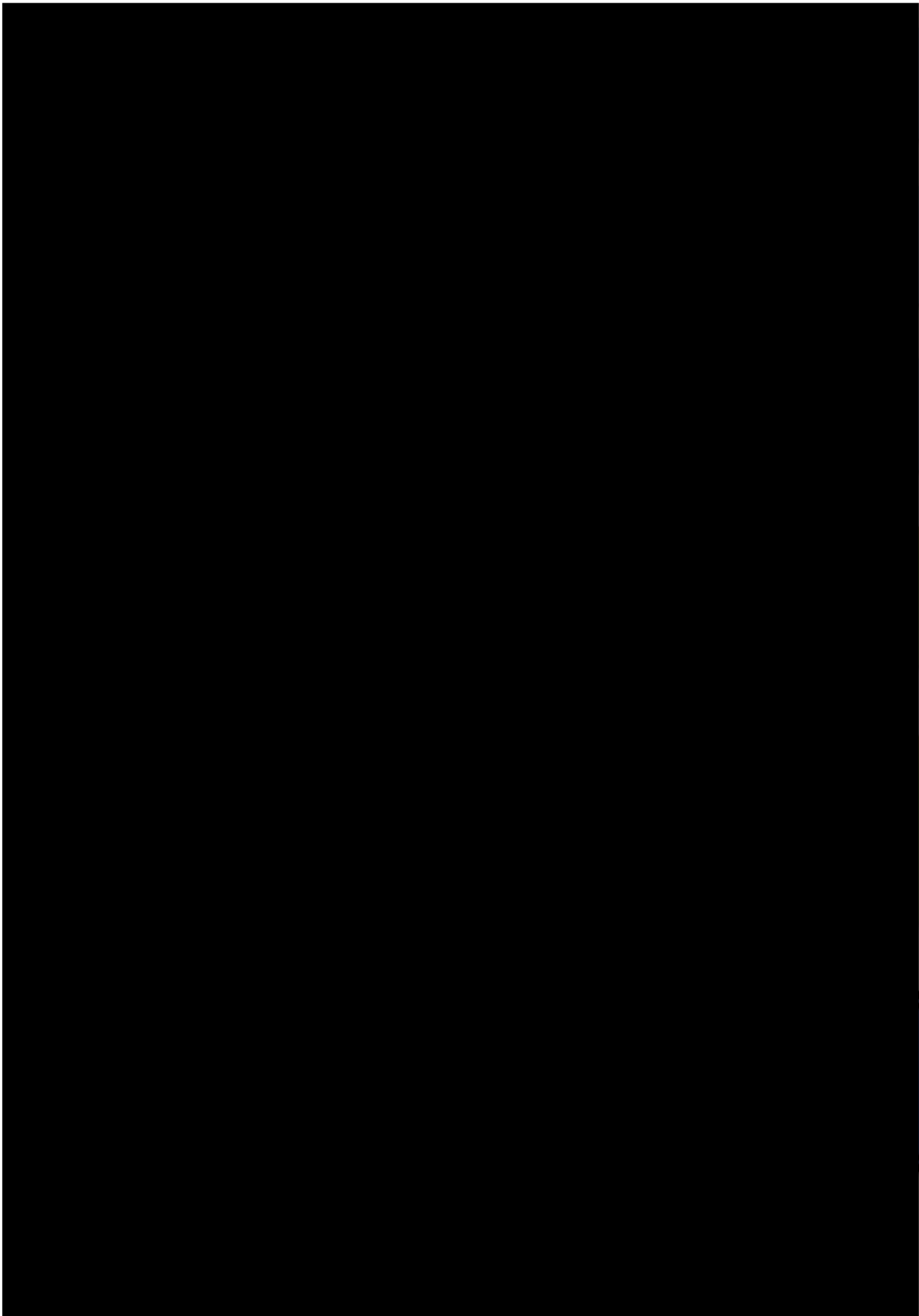
¹⁹ "EUR-Lex - 42000A0922(04) - EN - EUR-Lex." 2014. 10 Aug. 2015

²⁰ EUR-Lex - 42000A0922(02) - EN - EUR-Lex." 2014. 10 Aug. 2015

²¹ Regulation (EC) No 562/2006 - EUR-Lex - Europa." 2006. 10 Aug. 2015

²² http://smartsurveillance.eu/index.php?option=com_content&view=article&id=69&Itemid=64

²³ http://respectproject.eu/index.php?option=com_content&view=article&id=46&Itemid=73



The border agent avatar

Border control officer's tasks rely on bilateral human interaction such as border control agents interviewing an individual using verbal and non-verbal communication to both provoke response and interpret the traveller's responses. ADDS is powered by Silent Talker, a system capable of semi-automating that process by quantifying the probability of deception from the part of the interviewee. However, to maximize the potential impact of ADDS the border crossing, it would be beneficial to utilize this system not only to provide support to a human border control agent but also to collect data completely automated on the potential of deceitful behaviour by a traveller. To achieve this, an advanced verbal and non-verbal communication border control agent avatar will be created. This will be instantiated per traveller and will be personalized to correctly communicate with the traveller including utilizing subtle non-verbal communication cues to gauge response to them. The avatar will potentially improve performance in certain situations compared to a human agent because it will be able to correctly adapt to the travellers profile as well as be able to target specific interview topics of high relevance to specific travellers based on analyses of data available on them. Furthermore, completely automating parts of the interview questions will enable to shift some of those to the pre-crossing phase thus resulting in considerable time and monetary savings while increasing security. As part of the iCROSS evaluation the use of the avatar will be evaluated so that it can be determined what type of questions and to which travellers it responds better especially at the pre-crossing phase. This will ensure that full automation is only deployed when meaningful to do so while still enabling pre-crossing collected data.

The border control Agent User Interface AUI

Multiple visualization ways will be provided in order to manage the data captured by iCROSS platform, including both the pre-arrival as well as the border crossing phase. They will additionally present the results that the specific tools generate in order to assist border agents with interpreting and accessing the data in real time within their procedures during decision-making. Visualization of risk estimate that support decision of the human agent will provide a discreet output clearly visible and readily interpretable only by the agent.

The system aims to support queries and statistics extraction, that is particularly useful in case the agent needs to further investigate the reasons that automated risk estimations were high, or during special investigations. Finally, the system will incorporate and visualise information that are being recalled by external assisting databases, either the existing ones like SIS/VIS, credit/debit cards status, etc. or databases that will be available in the future, maybe by Interpol, Europol, etc.

Mobile Application

Mobility is one of the characteristics that iCROSS aims to adopt in its application. Therefore, it is of great necessity to reflect the interaction of the travellers and the border agent through iCROSS platform in a **mobile application**. This application will enable the travellers to rapidly recall information already uploaded to the system and will acknowledge them with the next steps or any parallel information needed before, through and after the border check procedure.

This mobile application is referring to all travellers, from different countries, different ages and cultures and should therefore understand the current practices and the desires of potential users, as well as the ways in which people experience or would like to experience life. A novel methodology for the design process will be followed, based on innovative research and literature printed out by the MIT²⁴, exploring the traditional user-centred design procedure, which is based on the user observation in their real context of use. iCROSS's new agile methodology will take into account the inability of mobile devices to observe users in many of their daily use of mobile applications and will travel far above the user-centred design procedure, by using creative methods in order to "analyse" users' interactions such as generative research²⁵ and structured interviews. **The ultimate goal is to create an entirely new experience with better communication and interaction.**

Document Authenticity Analytics Tool (DAAT)

The proposed DAAT will be built on top of an existing system, the ED's False and Authentic Documents Online (FADO) and its public version (PRADO). This system will be repurposed and customised to explore the knowledge and experience to provide an added value to fluent, fast and secure border crossings while ensuring security Schengen Handbook. The focus will be on increased performance for a more rapid and straightforward verification of travel documents in short time durations, especially during the check phase process. The implementation will take place in two stages, both in the pre-arrival/registration phase, as well as in the check phase.

[REDACTED]

[REDACTED]

[REDACTED]

²⁴ Bentley, E. Barrett, "Building Mobile Experiences", MIT Press, 2012

²⁵ "Communicating with mobile technology" class, Massachusetts Institute of Technology

²⁵ It is research that takes place in the form of discussion with end users in an approach to generate new design ideas (see above MIT references).

[REDACTED]

iCROSS tools will have the capability to interface in the future with national/international authorities', Europol's, Interpol's newly or future developed databases using the travellers' personal information, such as name, date-of-birth and nationality and thus may result in criminal detection of individuals attempting to carry out transactions using identity documents; real-time law enforcement notification; increased border agent safety by enhancing identity protection measures to reduce criminal activity and attacks.

Automatic Deception Detection System (ADDS)

A single, real-time, Silent Talker (ST) classification system will be developed for both pre-arrival and border crossing interviews. Based on existing (ST) architecture, this component will be re-engineered in a 6-phase procedure, as following:

[REDACTED]

Biometrics

Fingerprints

iCROSS intends to adopt fingerprint technology to improve the flow of travellers at border crossing in Europe. The overall approach is to integrate this technology within the iCROSS portable device used by every agent to check people's identity. Most travellers belonging to the EU and from developed countries are issued an e-passport which has an embedded RFID chip that carries digitally signed biometric information (our fingerprints normally, however they are incorporating palm vein data). Obviously, travellers coming from underdeveloped countries doesn't have their fingerprint registered on their passports, so this additional measure of security at border controls is orientated to speed up the flow of travellers owning the mentioned e-passports. When the people don't have the necessary biometrics integrated document, other ways will be used, such as to capture them from the visa issuing or the visa documents.

Palm vein

The BioSec palm vein based biometric identification system relies on the fact that the blood stream in the veins absorbs near IR light and the complete vein pattern becomes visible for the IR optics. The image created will be digitized immediately within the sensor and the image will be deleted irrevocably and an encrypted HASH code will be created. Any direct connection between the person and the biometric template will be terminated. The benefits of a HASH code is that is it always changing, is according to actual mathematical knowledge irreversible. In opposite to other biometric authentication methods the palm vein recognition based biometric identification uses an "inner" ID, therefore the palm vein pattern cannot be seen from outside, cannot be copied or reproduced, like fingerprint. In order to avoid identification, fingerprints can be burned off with e.g. acid or tricked with spoofing. In order to avoid palm vein identification, you have to cut off your hand, which is less likely. Each time the matching procedure is a several step identification/verification procedure to ensure the FAR rate of 0,00008% (certified by BSI in Common Criteria 2 certificate).

The benefit is also the disadvantage, namely that palm vein based identification cannot be used for fight against crime, since you do not leave a trace, therefore palm vein identification forms an ideal combination with fingerprint and/or face recognition, since palm vein recognition has a better FAR and FRR rate and is ideal for primary

authentication but registering fingerprint and/or face templates create valuable databases for law enforcement organisations.

The largest reference for BioSec palm vein recognition based mass identification is the Groupama Arena, where the access control system is equipped with biometric authentication and the BioSec system can identify 23000 people within ~90 minutes at 36 gates. Successful matching takes place within 1 second. The importance of this reference is, since it proves that the system can be used by all types of people (young, old, male, female etc.) and the system does not slow down even in stress situation just like a mass entry before a soccer game. Right now more than 55 000 people are registered in the database and last year more than 250 000 entries have been managed without any security or system issue in outdoor conditions in the winter or summer.

Face Matching Tool (FMT)

The FMT System shown in Fig. 8 consists of 2 stages: pre-arrival and border crossing. At the **pre-arrival phase (where the person is at home or similar)**, two inputs will feed the check phase: (1) sample facial images of the traveller obtained during the interaction with the avatar/ADDS and (2) the passport that the traveller uploaded to the system. Therefore, a first “**offline**” verification will take place to compare the sample facial images of the person who talked with the avatar and the uploaded passport, to check whether it is the same person or not. Following that, at the **check phase (where the person is physically at border controls)** a second “**online**” verification will take place. It will consist of capturing facial images of a traveller and retrieving and comparing with the photo from the traveller’s documents, either stored in electronic version or scanned from the passport photo page. A high resolution camera detects and captures the facial image of the traveller in quality resolution for processing. A passport scanner scans the photo on the passport and an e-passport reader retrieves the electronic file of the photo stored (in the case of e-passport). Finally, before the result of “Match” or “No Match”, a **last verification** is done to check whether the person attempting to cross the border controls is the same person that talked with the avatar in the pre-arrival phase.

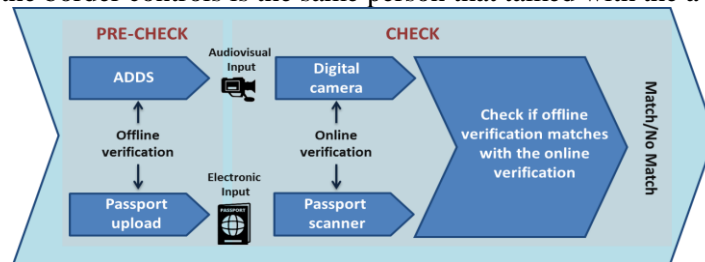


Fig 5: FMT System and Architecture

The first core of the **FMT Engine** compares the photos between uploaded, scanned and stored in the case of an e-passport to detect forgeries or mismatches between them. The different or reduced quality of the scanned image compared to the original photo image will be considered in the matching process, which extracts some start-of-the-art **invariant facial features** such as shapes, local patterns and biologically inspired features from the images.

The second core of the FMT Engine extracts both global and local **facial features** from the sample facial images obtained in the ADDS and from the high resolution images as well as facial features such as eyes, nose and mouth. Parallel matching processes take place between captured image and stored photo (or scanned in case of conventional passport) in global and local scales. The **global matching** provides a holistic verification including shape and geometrical information, while **local matching** further enhances the confidence of the matching with matched facial features.

The third core accounts for the tolerated **natural variations** in lighting, aging, expression and facial marks, built on training thousands cases. These changes are described by smooth, nonlinear **manifolds** extracted from the training samples. These changes exist in both global and local features and are treated coherently. Mostly importantly these changes are different from the discrepancies between subjects and are thus modelled differently to differentiate **the pixel and manifold differences**. The ability to recognise the manifold changes are the key to the robustness of the FMT System. The sensitivity of the system is influenced by the pixel difference, though other differences can help make informed judgement on the differences between the subject and the photo.

Finally the **Fusion** core of the FMT System synergises the matching in various scores and different levels and provides an overall matching score of the traveller and the passport photo. With a pre-set confidence level (set by the border controls), this overall score will translate to either “Match” or “No match” output to the Border Control System.

Regarding to where will the FMT engine is implemented at border controls, the overall concept is to integrate it in all traditional security cameras present as well as – a more innovative concept – to provide every agent with a shoulder-mount camera. This way, agents will not depend on traditional cameras, which are more orientated for monitoring and support, and will have their own camera to capture specific sample facial images of the traveller.

Cloud-based storage, processing and data protection

The processed information from all technological components (both during the pre-arrival and check phase) will be collected to a centralized cloud-based application that will allow the analysis and evaluation of travellers' risk, uploaded data and timestamped interviews. Moreover, the cloud based application will host the real-time statistics analysis tools. Border agent specific statistics will include login/logout time, location and terminal ID, number of passports and number of falsified passports found. Traveller specific statistics will include date/time of arrival, expected departure based on above, number of visits, frequency of visits, categorization of visits, and country of origin and destination country.

Processed information is securely stored and processed in the cloud, while complying to the **European data protection guidelines** and following industry best practices on **privacy and security**.

Secure access and secure transfer of the data from the cloud to border devices and vice-versa. An architectural decision will be made to determine the appropriate method to protect data when it is being transmitted. The most common options available are Virtual Private Networks (VPN) or a Secure Socket Layer (SSL) / Transport Layer Security (TLS) model. SSL 3.0 and TLS 1.2 for the web application and API is selected. At a minimum, all of the following should be followed:

- Require SSL for all pages. Non-SSL requests to these pages should be redirected to the SSL page.
- Set the 'secure' flag on all sensitive cookies
- Configure the SSL provider to only support strong (e.g., FIPS 140-2 compliant) algorithms
- Ensure that every SSL or TLS service uses a certificate that is valid, not expired, not revoked, and matches all domains used by the site. We should also schedule renewal of all certificates before they expire to ensure the services remain secure
- Backend and other connections should also use SSL or other encryption technologies
- Use SSL or TLS throughout the entire domain in order to reduce complexity. Remember that any included content such as images, JavaScript or CSS should also be provided over SSL or TLS in order to avoid 'mixed content' warnings in users' browsers
- Obtain an Extended Validation (EV) certificate

Secure Application Programming Interfaces. APIs are integral to security and availability of services. These interfaces must be designed to protect against both accidental and malicious attempts. Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities will be avoided at all times.

Access Right Management System and Relevant Policies

Authentication. The traditional form of security tokens like username/password used to access online services are prone to phishing attacks and hence do not provide complete security. Identity will be protected with directory integration, groups, as well as Single-Sign-On (SSO) integration. Authentication controls will include Two Factor Authentication (2FA), and session expiration.

Secure Management Interfaces. Command and control facilities are understood and secured. SSL will be used to encrypt all transactions.

The cloud-based system will follow a "Privacy by Design" principle in order to promote privacy and data protection compliance from the start. The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs ²⁶), 'privacy by default' settings and the necessary tools to enable better protection of personal data (e.g., access controls, encryption). The principle of 'Privacy by Design' should be binding for technology designers and producers. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems.

Measures to improve **platform security** include:

Transport Layer Protection. The most common options available are Virtual Private Networks (VPN) or Transport Layer Security (TLS) model.

Prevention and Detection of SQL Injection.

Access Right Management System and Relevant Policies.

Authentication. The traditional form of security tokens like username/password are prone to phishing attacks and hence do not provide complete security. Instead iCROSS will use **Two Factor Authentication** (2FA), adding an extra layer of security that is known as "multi factor authentication". Users are required not only a password and username (single-factor authentication) but two out of three types of credentials before being able to access an account.

Auditing. Auditing is the security concept in which privileged and critical business transactions are logged. At a bare minimum, audit fields that include who (user or process) did what, where (file or table) and when (created or modified

²⁶ Going beyond the secure storage and communication of data, Privacy Enhancing Technologies (PETs) now exist with counterintuitive capabilities such as anonymous communication across the public Internet; electronic cash that mirrors the anonymous nature of money in the physical world; and anonymous credentials that prove an individual has permission to access specific resources without revealing their identity.

timestamp) along with a before and after snapshot of the information that was changed must be logged for all administrative or critical transactions as defined by the business.

System Documentation. Documenting system components, networks, services, and software should provide for a bird's-eye view needed to thoroughly cover and consider security concerns, attack vectors and possible security domain bridging points. Just as with hardware, all software components should be documented, since this can assist in understanding total system impact due to a compromise or vulnerability of a specific class of software. A network topology should be provided with highlights specifically calling out the data flows and bridging points between the security domains.

Configuration Management. Configuration management allows avoiding the many pitfalls inherent in building, managing, and maintaining complex infrastructures. Tools will always be used to automate configuration and deployment. It is important that network devices, operating system, database, firewalls as well as software configurations are monitored on regular basis to ensure that their configuration is not changed by any unauthorized user.

Patch Management. Patch management is to manage the implementation of fixes in order to resolve the defects/problems identified.

Methods to improve **data protection** include:

Sanitisation of tenant data when program ends;

Encryption to protect sensitive information in transit and storage. For data in transit end-to-end encryption should be applied. It must be ensured that personal data in transit is protected against active (e.g. replays, traffic injection) and passive attacks (e.g. eavesdropping), thus ensuring data integrity²⁷.

The encryption keys should not be used by, or be accessible to anyone others than the border agency and the cloud service provider.

Storage encryption adds an additional layer of protection that will continue protecting the data even if an attacker subverts the database access control layer.

Backup is the most important means to keep the data from being lost due to intentional or unintentional access. It is also important to encrypt the up-to-date backups. Backup is easiest and the most familiar process for most situations

Data destruction, by effectively deleting personal data from disks and other storage media. Measures include immediate overwriting with random data²⁸, destroying/demagnetising the storage media, physically destroying the media so that it can no longer be used, usage of secure deletion software.

Interface with Social media

Border control processes today include the consideration were applicable of publicly available information. Such information may be that conference agendas and published papers for example of travellers to a scientific conference, similarly for athletes travelling to an athletic event, or representatives of merchants attending an expo, news and other. Social platforms can also shed light on travellers' affiliations and interests that will in turn guide some of the interview questions. iCROSS will develop search tool to perform preliminary search on public information and social media analytics to consult about the validity of the information at the pre-arrival stage, i.e. To check matching photo of the person with the name and nationality, etc. It will be developed in synergies with other research projects, especially IO-FACT on Digital Forensic Investigations and RUBICON on planning of border check processes, where partners participate or adoption of publicly available open source tools and will interface with iCROSS RBAT.

Integrated Border Control Analytics Tool (BCAT)

The underlying technical approach for the implementation of the BCAT is based on the utilization of all results produced by all the tools implemented in the project to perform post processing analyses in order to achieve two goals:

- a. Evaluate the performance of the each proposed task and compared its effectiveness to the human border control agent.
- b. Discover key patterns in the data associated with either False accept or false rejects of travellers based on the data collected in the Pilot study (but also applicable in the event of wide adoption of the iCROSS platform)

The analyses tools will be broken up into two categories, (a) the statistical analyses and modelling tools, and (b) the data mining-computational intelligence tools. The statistical analyses and modelling tools will reveal complex statistical models that will attempt to utilize the results of each implemented tool to improve on the system's overall effectiveness.

The data mining – computational intelligence tools will be targeted towards the identification of novel patterns in the intermediate, or final results of all the analyses tools applied to travellers that are associated with specific classes of travellers, for example travellers that are falsely accepted, or falsely rejected by human border control

²⁷ Integrity may be defined as the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission.

²⁸ Special software tools that overwrite data multiple times in accordance with a recognized specification should be used.

agents or by specific automated tools. Dimensionality reduction algorithms will be implemented to help identify which automated tool's results, or intermediary results do not contribute significantly to the final outcome of a traveller's accept or rejection decision for border control while feature selection algorithms will be implemented to identify the specific intermediary or final results of tools that tend to be strongly associated with the outcome of border controls of travellers. Various clustering approaches (hard, fuzzy, hierarchical) will be investigated to enable unsupervised identification of groups of travellers that share common characteristics in their collected data (honest/lying to the same questions, similar document authenticity results etc) as a method of identifying specific cases where either the human agents, or the proposed automated tools tend to consistently fail.

Furthermore, experimental workflows will be defined, sequences of analytic steps to be applied at regular intervals to provide descriptive statistics as to the performance of the iCROSS platform and the human border control agents. As an example consider performing document authentication first, and using the output of that analyses to guide the Avatar on asking questions related to his/her identity or how he/she was issued those documents.

Risk Based Assessment Tool (RBAT)

The RBAT module will act as an "automated decision-maker" on the data extracted during the iCROSS procedure. It will support the decision-making process of the application backend towards the end-users of the application (in this case the border-agents), while providing all the necessary measures to ensure that the appropriate information reaches the relevant group of users. This module can be developed on the basis of an ED existing tool.

More particularly, a complete point and click graphical environment allows authoring rules through the use of structured, non-technical expression of logical interactions between the "Business/Target User Objects". The administrator will have the capability in a very simple manner, which will not require prior knowledge of difficult programming languages, to author the appropriate conditions/rules in order to determine, according to the European/international laws, national regulations, "trends/tendencies" of the particular time-period, etc., the security level during the border check process and the risk-threshold that will classify accordingly the traveller and the customised procedure he/she will have to go through.

Some highlights of the RBAT module are:

- *User defined Criteria*
 - Easy, human-friendly and efficient compilation of logic involved
 - Completely User-Defined, loosely coupled with proprietary in-house IT Systems
 - Adaptable to new requirements or amendments
 - Natural language oriented Rule Based System and /or Algorithmic while the combination of both is supported
- *Rules.* A rule allows users to perform complex queries with specific criteria combining available data. The RBAT module is based on a full version control system that is explicitly bound to the decision making process. The complete history of the classifications made at a point in time is stored along with the rules that were used to arrive at each conclusion and all relevant data. The administrator is responsible for the maintenance of the rules that s/he created. The system provides a number of actions over the rules, such as add, edit, delete, copy allowing the performance of any desired adjustment.
- *Scoring schema.* RBAT provides scoring schema based on user-defined scoring mechanism. The user can assign a scoring value to each rule which depended on the type of the operator that performed in the evaluation process, i.e. exact match, contained, phonetic match. The scoring schema is tuned by the administrator of the system. *Definition of the scoring schema* is an entire research effort that will take place in collaboration with the end users and requires thorough validation to ensure that the risks are correctly assigned based on the data that result in their calculation. Several parameters contribute to the estimation of risk: the origin of risk parameter indicating whether it is coming from a reliable source as opposed to on publicly available data, the reliability of the source indicating whether it is based on reliable data and calculation or fuzzy methods (i.e. the INTERPOL list of criminal is a reliable source as opposed to an article listing criminals in a news web site), the degree of uncertainty in the calculation (the FMT gives more certain result than the ADDS), etc.

Hidden Human Detection Technology (HHD tool)

This tool has been suggested to solve an existing problem that is reported at the border control. In many cases the illegal travellers hide themselves in busses, cars or trains, since they don't possess the necessary travel documents. The authorities have to detect them and they do so, without appropriate tools to support them. This is the case highlighted in the pictures below. The portable HHD is proposed to facilitate this work.

As a secondary target, iCROSS will attempt to provide detection of people crossing land borders hidden inside vehicles or trucks and trains containers or open cargo wagons. The land border staff has often confronted "peculiar" situations with people hiding literally inside car seats, small closets or even suitcases. However, relevant checks are not performed routinely, especially when traffic flow across the check points increases; instead they are made occasionally or indicatively, unless dictated by official warnings, relying mostly on visual inspection and staff's

experience and perception. Thus, a need for portable devices is revealed, especially when more advanced equipment requiring large installations (i.e. x-rays for trucks and containers) is considered too expensive.

To this respect, iCROSS proposal aims at providing a portable radar prototype for the detection of hidden people, exploiting the Doppler frequency shift in E/M waves caused by breath or slight movements. iCROSS Hidden Humans

Detection (HHD) tool, lies upon a life detector CW radar for detecting trapped alive humans under building ruins, already developed by ICCS²⁹; an early version of which has already been tested in Athens earthquake (1999) assisting rescue teams, while three lab prototypes have been achieved in the meantime (one of them is tri-band in P, S and X-band). However, the situation in land borders concerning hidden humans is quite different than alive persons under collapsed buildings.

Although the basic concept remains more or less the same, several advances are in order to meet iCROSS needs. In the foreseen scenarios, the HHD tool will be carried and operated by customs officers or border staff. Thus, the range towards the “target” is smaller; resulting in compact portable module without loss of performance, with lower

transmitted power and smaller batteries. Based on the existing experience, frequencies of operation will be thoroughly investigated. As it seems, the lower microwave band (2.5 & 1.15GHz) is the best candidate for the relevant cases, combined with slot-type antennas instead of large horns. Other solutions will be also explored (i.e. UWB) while P/UHF and X-band will be sustained for flexibility and increased detection probability. In order to finally decide performance parameters, dual or tri-band modes will be used combined with alternative implementations and through measurements and testing in

both real and simulated cases for advanced performance.

Apart from open air use (vehicles and passengers trains or open wagons), for penetration through metallic containers or closed compartments, attempts of combination and data fusion with acoustic sensors (using sound echo signal) will be made (B version), based on quite recent advances³⁰ in high-power acoustic sensors technology. Sound penetrates metallic walls; thus, the acoustic sensor is an excellent complement to the radar one, due to its sensitivity to small and slow motions, allowing detection of stationary persons by breathing motion alone. Moreover, FFT and digital signal processing will be made locally with the use of smartphone or tablet, that will act as a CPU and, with a mobile-type app, enabling data local visualization and transmission to the iCROSS platform. On successful detection, the user will experience a beep alarm signal, triggering an in-depth inspection at a secondary level.

Therefore, HHD module will consist of two main units (sensors and tablet) resulting in a portable device complying to the iCROSS concept. Attractive features are also targeted: high-resolution, near-real-time data processing and display, low development cost and user-friendliness. In terms of the overall iCROSS platform and the TRL5 approach, the HHD tool is considered as a module to test and prove the technology, the integration ability and the applicability of operation and will be tested in vehicles and in the passengers / cargo train pilot

Wireless Technologies for Border Check Process

The wireless technologies requirement was imposed by the fact that at border checking the new technologies require specific Quality of Service (QoS) at border crossing station, within trains, or busses that is not guaranteed given their remote or mobile nature. This state-of-the-art technology supports this requirement.

The iCROSS project aims at speeding up and facilitating the land border control operations in automated manner. Travellers control envisages a two stages border check process including the pre-arrival registration and the reduced time actual control at the border, the implementation of which cannot exist without highly reliable, available, efficient and secure wireless communication systems. In order to provide a reliable, secure and user-friendly environment for the users, the wireless technologies that will be employed should meet specific needs and requirements: high-availability even in remote/rural areas, mobility requirement focusing on improved system performance in high speed scenarios and of course reliability and safety requirements.

The radio link availability depends primarily on the radio coverage of the wireless network that could be a cellular or a satellite system. Obviously, in case of the on-board check (and potential pre-arrival registration) scenarios, the requirement of high-availability is a challenging task due to the complexity of the scenario’s environment; if, for example, the users travel by train, their route may include bridges, tunnels and viaducts. Vehicle’s high speed may prevent a datalink connection due to the extremely short interval for handovers between cellular nodes. Moreover, in many cases, the vehicles travel through rural areas where cellular coverage is inadequate.

²⁹ M. Bimpas, N. Paraskevopoulos, K. Nikellis, D. Economou and N. Uzunoglu “Development of a Three Band Radar System for detecting Trapped alive humans under building ruins”, Journal Progress In Electromagnetics Research, PIER 49, 161–188, 2004

³⁰ Franklin Felber “Demonstration of novel high-power acoustic through-the-wall sensor”, Proc. SPIE 9456, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement XIV, 945603 (May 14, 2015); doi:10.1117/12.2084056

A reliable, cost-effective and easily deployed solution that can be employed is the satellite communication. Particularly, using the Ka band satellite technologies, the border security personnel (customs officers, border agents) or travellers can connect with a reliable, high-speed satellite link to the internet and send the required digital information to the control border centre while they are on the move. In case of trains, the trajectories are constant, consequently, proactive fade mitigation techniques may be applied (adaptive coding and modulation, and diversity techniques) in order to increase the availability and the reliability of the system.

Scenarios of on border crossing points and potential On Board checks

As discussed in the previous sections, during the pre-arrival registration stage, the traveller provides initial digital information to the iCROSS platform. Then, in the border crossing point the actual border control takes place by the security agents. Depending on the technological capabilities of pedestrians or travellers inside vehicles (cars, buses, trains etc.) the following wireless connectivity scenarios are foreseen: In the *first basic scenario*, on the border crossing point, iCROSS foresees the wireless connection via the portable iCROSS unit, of the border officers conducting the security controls to the iCROSS platform. In parallel the registration of those travellers that did not have the ability to pre-register may also take place. The *second scenario*, which is potentially more advanced, is basically meant for the border agents when in trains; since, in many cases the border agents move on-board the train from one country border to the other and vice versa, conducting passport and security checks and then return back on the next train. However depending on the facilities available, iCROSS may also facilitate even traveller's "on-board" registration; the traveller can provide certain information *during* his travel and before actually reaches the border crossing point, although being close to it (i.e. an hour distance). The relevant facilities require an *a priori* internet connectivity and wireless access to the iCROSS platform, provide that this is available; i.e. by the traveller's mobile devices while quite many applications nowadays involve existing internet availability through Wi-Fi in buses, shuttles or trains.

The required capacity and internet connectivity will be achieved through agreements (SLAs) with either fixed, or mobile or satellite operators. The rest radio network will be fully designed by iCROSS team.

[REDACTED]

iCROSS impact Assessment

iCROSS's integrated estimation of deceptiveness and suspect behaviour will be compared with the established border control procedures. Data about today's procedures will be collected to derive metrics that will indicate improvement or not of the task, based on multivariable analysis, aiming at the overall improvement of the procedures. A comparative approach of the data collected before and during the pilots will take place to help with the evaluation of the performance of iCROSS. Specific metrics will be set such as % correctly classified as truthful or deceptive. Contingency tables can be used to identify bias (i.e. high accuracy with classifying one category, low with the other).

Implementation approach

The iCROSS implementation approach follows the well-known V-model approach, focusing on a top to down way for the architecture design and iterative validation with end users of intermediate prototypes. The figure below highlights the workflow all along the project.

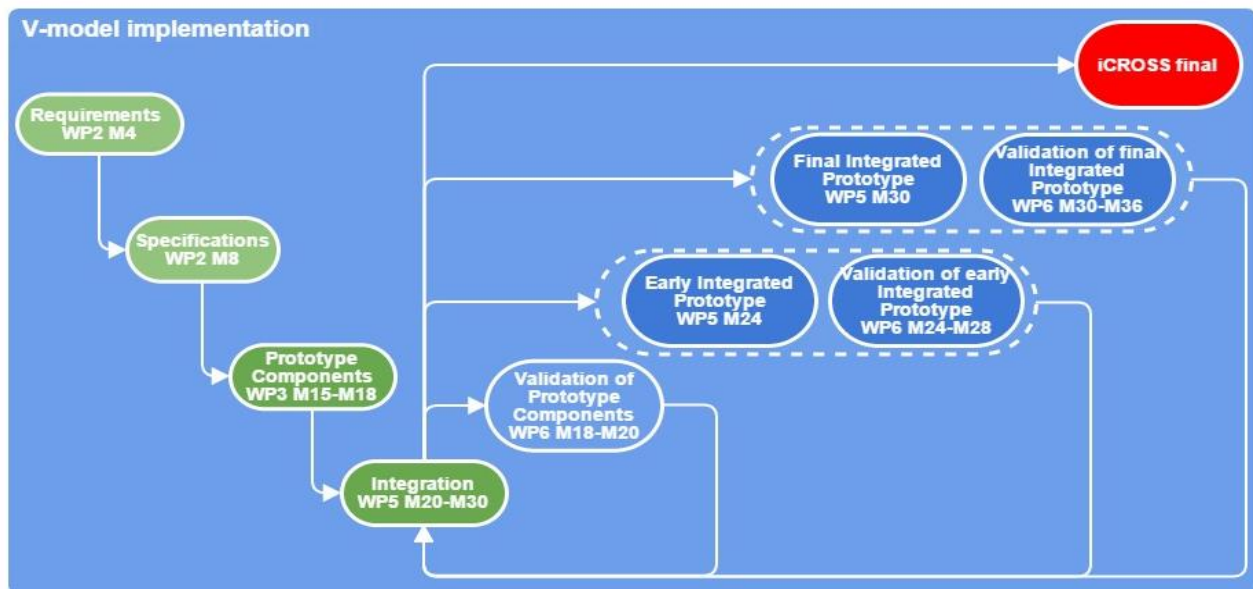


Fig 7: iCROSS V-model implementation approach

1.3.5. Sex/gender issues

With respect to the research topics addressed, the technology is essentially gender neutral. Regarding the consortium, it comprises of a well-balanced team with representatives of both genders, working together in an effective and productive way. Additionally the coordinator and technical manager are females but also leadership and relevant responsibilities are distributed to researchers of both genders. In that way, the iCROSS consortium promotes the successful collaboration of the two genders.

User friendly mobile application for the traveller and the agent

_____.

FADO/PRADO created by ED for EC served as a European system for the exchange by computerized means information concerning genuine and false legal and travel documents and contained -among others- images of false and forged documents, images of genuine documents, summary information on forgery techniques as well as information on security techniques. Ever since many systems have been developed, including both software and hardware (hardware is fundamentally based on existing technology devices, e.g. IR/UV scanners, etc.), for document authentication, but their application is mostly “limited” to banks, casino groups, car-hire companies, etc. They have not yet adequately been utilized to support border control operations in real time.

Automatic Deception Detection System (ADDS)

[REDACTED]

(b) [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(c) [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]

(d) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic such as: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data take an innovative step forward to **replace personal information (ID cards)** in order to ensure a faster and more secure and feasible verification of people's identity. Biometric templates cannot be reverse-engineered to recreate personal information and neither cannot be stolen and used to access personal information. Using a unique, physical attribute

URL=http://www.frontiersin.org/Journal/Abstract.aspx?s=537&name=human_neuroscience&ART_Doi=10.3389/fnhm.2013.00016

³³ Wojciechowski J, Stolarski M, Matthews G (2014) Emotional Intelligence and Mismatching Expressive and Verbal Messages: A Contribution to Detection of Deception. *PLoS ONE* 9(3): e92570. doi:10.1371/journal.pone.0092570

of your body, such as your fingerprint or iris, to effortlessly identify and verify that you are who you claim to be, is the best and easiest solution in the market today. Biometrics have been around for many years and recent modern advances in this innovative technology coupled with big reductions in cost makes it available and affordable to almost everyone: consumers, small business owner, larger corporations and public sector agencies.



Fig 8: Biometric symbol in e-passports

Nowadays, biometric information (i.e. fingerprints, palm vein data, iris recognition, etc.) is being incorporated in passports, known as **e-passports**. They are a combination of paper and electronic passport that contains the necessary information (included in an embedded RFID chip – effectively a contactless smartcard) to establish one's identity. To prevent wireless reading of the passport content without the owner's consent, passports can use a mechanism called Basic Access Control (BAC): to access the smartcard one must visually read some information printed in the passport. Subsequent communication between passport and reader is then encrypted to prevent eavesdropping. All EU passports implement BAC. However, it is expected that Supplemental Access Control (SAC) replaces BAC in the future due to the weaknesses detected among BAC. Other protection mechanisms are implemented in the contactless chip such as: (1) Passive Authentication, to detect any possible modifications of the chip and (2) Active Authentication, to prevent people from cloning the passport chip. Moreover, another protection mechanism is being implemented to protect fingerprints and palm vein data, which is: Extended Access Control (EAC). It simply consists in verifying that the chip and the terminal reader are not a falsification. All these features makes e-passports ideal, fast and secure for checking people's identity. The advantage of this technology is its fast extension within member states and therefore, most people already possess an e-passport. According to a report from Ryan Clary³⁴, the International Civil Aviation Organization (ICAO) reported that by 2011, 93 out of 193 United Nations (U.N.) member states, were issuing e-passports, with additional 21 countries ready to deploy the technology in the following years. The ICAO estimated that by July 2011, these 93 states had issued more than 345 million e-passports, of which at least 45 of them included fingerprints and 14 of them were planning to include fingerprints by the end of 2011. This report also mentions an IMS Research prediction of 90% e-passport domination by 2016. iCROSS is thus well positioned in time, since is now the time of implementing biometric verification systems at border controls.

Face Matching Tool (FMT) Ambition

Face recognition (FR) is by far the most convenient biometric means. Although face recognition has started to appear on many applications, especially under controllable environments, such as computer login, entrance and gaming devices, and has been piloted at several airports for checks and passport controls, there are still challenges to be addressed for a robust deployment. The biggest challenge comes under unconstrained environments where illumination variability and poor image quality are by far the most problematic issues for reliable applications in large-scale public services³⁵.

Ever since Turk and Pentland's seminal paper on eigenfaces³⁶, there have been tremendous progress in making face image based biometrics a practical tool. Worldwide laboratories and researchers have been competing to further advance the field with the notable methods such as, Fisherfaces³⁷, Features and Templates³⁸, Active Shape Model³⁹⁴⁰, Active Appearance Models⁴¹, Morphable Model⁴² and Local Binary Patterns⁴³. The Face Recognition Vendor Test (FRVT) 2006 is an independent evaluator for face recognition systems and largely represents the state-of-the-art performances with the best results achieving accuracy 99% under high resolution and controlled environment and 80% under unconstraint conditions, respectively. This provides a benchmark on FR system performances and indicates that reliability is expected between 80% and 99%. In order to enhance the system performance to the upper bound, natural variations (e.g. aging⁴⁴ ⁴⁵, expression, limited pose) and environment factors (e.g. lighting, ambient) must be addressed and integrated into the recognition models.

³⁴ <http://www.secureidnews.com/news-item/e-passports-spread-to-half-the-globe/>

³⁵ N. Firth, "Face recognition technology fails to find UK rioters", p.19, 20 August 2011, New Scientist.

³⁶ M. Turk and A. Pentland, "Eigenfaces for recognition," J. of Cognitive Neuroscience, vol. 3, pp. 71-86, 1991.

³⁷ P.N. Belhumeur, J.P. Hespanha, D.J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, 1997.

³⁸ R. Brunelli, T. Poggio, "Face recognition: Features versus templates," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 15, pp. 1042-1052, 1993.

³⁹ T.F. Cootes, C.J. Taylor, D.H. Cooper, J. Graham, "Active shape models-their training and application," Computer Vision and Image Understanding, vol. 61, pp. 38-59, 1995

⁴⁰ A. Lanitis, C.J. Taylor and T.F. Cootes. Automatic Interpretation and Coding of Face Images, Using Flexible Models. IEEE Transactions of Pattern Analysis and Machine Intelligence, Special Issue in Face and Gesture Recognition Vol 19, no 7, pp 743-756, 1997.

⁴¹ T.F. Cootes, G.J. Edwards and C.J. Taylor: "Active appearance models. IEEE Trans. on Pattern Analysis and Machine Intelligence, 23(6), pp 2001, 681-685.

⁴² V. Blanz and Th. Vetter, "A morphable model for the synthesis of 3D faces," SIGGRAPH'99, pp.187-194, 1999.

⁴³ T. Ojala, M. Pietikäinen and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 24, pp. 971-987, 2002.

⁴⁴ A. Lanitis, C.J. Taylor and T.F. Cootes. "Toward Automatic Simulation of Aging Effects on Face Images". IEEE Transactions of Pattern Analysis and Machine Intelligence, Vol 24, no 4, pp 442-455, 2002.

⁴⁵ G. Panis, A. Lanitis, N. Tsapatsoulis, T.F. Cootes, Overview of research on facial ageing using the FG-NET ageing database. IET Biometrics, 2015

Various approaches addressing these variations and discrepancies in facial images appear in literature, among them, manifolds or dimensionality reduction methods are making great impact. The dimensionality reduction (DR) process and effect has been linked with the Deep Neural Networks⁴⁶, which has become a de facto architecture for solving complex cognitive tasks. They can be used to model and capture nonlinear variations among facial and lighting changes. Various DR methods and manifolds have been derived recently, Kernel PCA, Local Linear Embedding (LLE), ISOMAP, Laplacian eigenmap, Locality Preserving Projection (LLP), Self-Organising Map (SOM) and ViSOM, and their performances in aiding the FR have been evaluated⁴⁷ and results show that certain adaptive neural methods can make significant improvement on the performance. When further coupled with the efficient LBP and gradient based methods, they can boost the performance under unconstrained conditions to within 2-3% of the upper bound⁴⁸.

In iCROSS FMT will enable seamless interaction with both the traveller mobile device hardware that will be in the pre-arrival as well as the body mounted camera at the human agent interview.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

The **integrated Border Control Analytics Tool (BCAT)**

The BCAT tool will be implemented enabling combinatorial analyses using statistical modelling and data mining approaches of all available data. During the pilot phase of the project, this will enable the support of the real time analytic algorithms by enabling the integrated analyses of their final or intermediate results. However, the biggest value of this tool will be the ability to use novel approaches to re-analyse using the Pilot case data collectively:

- 1: The performance of each individual tool will be calculated by univariate analyses tools. Through this the validity, sensitivity and specificity of each tool will be compared against the human border control agent performing the task.
2. Any potential interaction effects between the results of multiple tools (subjects found to be marginally deceitful on question 1 and have marginal similarity with the picture on their travel documents, are strongly associated with travellers using invalid documents that human agents fail to identify correctly)
3. High (to include) or low (to exclude) performing automation tasks that contribute greatly to the final decision making support of the status of a traveller. These analyses will be implemented through data mining techniques such as feature selection and dimensionality reduction.
4. Finally, automated pattern discovery will enable the automated discovery of key patterns in the data of travellers matching the same outcomes. This could include intermediary results of analyses from some tools, and will have the advantage of helping discover new patterns. In this regard iCROSS envisages advancement of clustering approaches (particularly fuzzy) and distributed association rules to be of value in identifying relationships within the data.

HHD tool: Hidden Humans / Illicit Goods Detection in Land Borders

The detection of hidden humans and illicit goods in borders security, is a challenging whole project by itself, incorporating extensive multidisciplinary research; technology for the easy fast and effective detection of humans hidden in a variety of vehicles (cars, trucks, containers, trains etc.) is still not available to customs and border guard services. Current commercial solutions mainly involve high energy x-rays detectors; however, in land borders the whole vehicle, truck or cargo container should be subject to x-rays and large commercial vendors⁴⁹ offer integrated systems finding hidden contraband through more than a foot of steel. However, such technology solutions are either too expensive or difficult to deploy in all border control scenarios, requiring demanding installations which reduce applicability especially for extended border lines.

⁴⁶ G.E. Hinton and R.R. Salakhutdinov. "Reducing the dimensionality of data with neural networks," Science, vol. 313.5786, pp. 504-507, 2006.

⁴⁷ H. Yin and W. Huang, "Adaptive nonlinear manifolds and their applications to pattern recognition," Information Sciences, vol. 180, pp. 2649-2662, 2010.

W. Huang and H. Yin, "On nonlinear dimensionality reduction for face recognition," Image and Vision Computing, vol. 30, pp. 355-366, 2012.

⁴⁸ W. Huang and H. Yin, "Binary gradient correlation pattern for robust facial representation," submitted to IEEE Trans. On Pattern Analysis and Machine Intelligence, 2014.

⁴⁹ Rapiscan Systems <http://www.rapiscansystems.com/>, SmithsDetection Inc. <http://www.smithsdetection.com/>, Leidos Inc.

Although for illicit goods, mostly explosives, portable or desktop trace detectors exist commercially, this is not the case for hidden humans; profiling and detection dogs have proven to be the most effective. Moreover, for rising cross-border flows with high throughput, time is limited for in-depth controls, therefore vehicles and containers are not systematically checked. FP7 Security Calls addressed the issue while the following solutions can be highlighted among the Security Research projects⁵⁰: artificial sniffers based on human perspirations/CO₂ (SNOOPY), olfactory sniffers (HANDHOLD, SNIFFER) with bio-mimicry biosensors and linear ion trap mass spectrometry, Terahertz technology - THz (TERASCREEN). Other technologies include heartbeat detectors, mm-waves, laser distance measurement, telescopic inspection mirrors/cameras, EM field detection and chemicals.

In past years, several researchers suggested Non-ionizing EM radiation using CW Doppler radar as Life Detector of trapped persons within collapsed buildings, through their breath or slight movements^{51,52}; penetration depth and spatial resolution are the main trade-offs for iron loaded concrete. Quite recently, similar concept's NASA/JPL's Finder module⁵³ helped saving lives in Nepal earthquake (April 2015). Nowadays, the relevant interest has increased for patients' vital signs contactless monitoring, and for high security requirements i.e. see-through-wall radar, airport and entrance security monitoring, border patrol etc. Although in the 1980s, relevant microwave systems focused at the X-band (10 GHz), it turned out that it cannot penetrate difficult material. Other systems at UHF (450 MHz) and at lower microwaves are better, with 2.5GHz and 1150 MHz⁵⁴ penetrating easier metallic wire mesh concrete. More recent advances use UWB pulses radars⁵⁵ showing high penetration capability, immunity against multipath interference and large bandwidth for better separation between target and clutter.

Millimetre (mm-) wave passive and active imaging offers rapid remote detection of metallic and non-metallic objects and contraband concealed beneath clothing⁵⁶, enabling "through-the-wall imaging systems (TWIS)" and humans' remote observation for military and law enforcement personnel, but not through metal walls. Passive mm-wave (PMMW) radars are much better for outdoor detection of concealed weapons in human body⁵⁷, while THz technology⁵⁸ is also an emerging candidate for concealed non-metallic weaponry. Multifrequency microwave radars⁵⁹ detect human movements and gestures through micro-Doppler signals, at short (S-Band, through-wall, up to 3m) or long ranges (W-Band, mm-waves, up to 100m in free space) through wideband noise or continuous single tone.

iCROSS HHD tool aims at a simple, portable solution, exploiting already gained knowledge on the field through ICCS's legacy life detector module. Although in natural disasters timing and exact location is everything for the survival and rescue of victims, this is not the case herein. Increased accuracy in location or in-depth screening are not absolutely targeted in iCROSS scenarios; but rather a small-range alert tool, enabling the use of electromagnetism coupled with newest achievements in acoustic sensors (sound echo) for tracking people also behind metal walls. EM waves cannot penetrate metallic structures and this is a real challenge especially for the cargo containers scenario; however, these are not EM shielded and leakage through their walls or doors may reach a highly sensitive receiver. Higher frequencies (X-band) show excellent spatial accuracy of detecting very slight movements (i.e. breath acquired in front of a human) but penetration depth is limited and vice versa; lower frequencies (VHF/UHF bands) have much higher penetration depth but can detect only large motions (i.e. an intensive hand movement). Thus, acoustics sensors are better solution for the metal walls case.

Summarizing, the iCROSS HHD radar aims to further advance the humans' detection technology when hidden in vehicles/closed compartments with portable, easy to use, contactless and reliable characteristics, tailored to the land borders security staff everyday procedures and working activities. Considering that the final outcome will be an advanced lab prototype, the aim is to contribute as possible to the iCROSS overall concept for effective portable devices. Above all, to prove that such modules could be successfully integrated in holistic systems of broader applications and to pave the way for potential integration of other similar research or commercial devices in the future (i.e. illicit good detectors that could also be optional for the open iCROSS platform).

⁵⁰ Work Programme 2013 Cooperation Theme 10 SECURITY, <http://cordis.europa.eu/search/result>

⁵¹ Chen, et al., "An X-band M/W life-detection system" IEEE Trans. Biomedical Eng., Vol. BME-33,697–701, July 1986.

⁵² Aggelopoulos, Karabetos, Constantinou and Uzunoglu, "Mobile microwave sensor for detection of trapped human beings" Journal of Int. Measurement Confeder., Vol. 18, No. 3, 177–183, July 1996

⁵³ Article: <http://www.jpl.nasa.gov/news/news.php?feature=4578>, Media Contact, E. Landau, NASA's Jet Propulsion Laboratory, Pasadena, CA.

⁵⁴ Changzhi Li, et al., "Radar Remote Monitoring of Vital Signs", IEEE Microwave magazine, February 2009, pp 47-56

⁵⁵ Ossberger et al, "Non-invasive respiratory movement detection and monitoring of hidden humans using UWB pulse radar", Joint Intern. Conf. on UWBST & IWUWBS. 2004

⁵⁶ G. Richard Huguenin, "Millimeter-wave concealed weapons detection and through-the-wall imaging systems" Proceedings of SPIE - The International Society for Optical Engineering 1997 (1997).

⁵⁷ Xiang et al, "Development of passive mm-wave imaging for concealed weapon detection indoors" Microwave and Optical Technology Letters Volume 56, Issue 7, pages 1701–1706, July 2014 (2014).

⁵⁸ Tribe Kemp et al, "Hidden object detection: security applications of THz technology", THz and GHz Electronics and Photonics III, Proc. of SPIE, Vol. 5354 (SPIE, Bellingham, WA, 2004) pp 168-176

⁵⁹ Narayanan, et al, "A Multifrequency Radar System for Detecting Humans and Characterizing Human Activities for Short-Range Through-Wall and Long-Range Foliage Penetration Applications" International Journal of Microwave Science and Technology Volume 2014 (2014).

Radio Communication Networks

The iCROSS project aims at exploiting wireless and satellite communication technologies to speed up and facilitate the land border control operations in an automated manner. Nevertheless under the framework there will be some important advances in the field of wireless and satellite communication technologies in various aspects such as physical layer and channel modelling, cooperative and relaying techniques, in radio resources management techniques and spatial distribution and connectivity evaluation.

[REDACTED]

Description of operations at the pilot sites

A. Hungarian Border

The external Schengen border in Hungary is about 1139 km long, consisting of border sections to: Croatia (EU), Serbia, Romania (EU) and Ukraine. Currently, with a 175 km section in the main migration route, the border between Hungary and Serbia can be considered as a hotspot. Protected by a 4 m high fence enhanced with NATO barbed wire, temporarily set up along the green border on the Hungarian side, it is not only interesting because of push of the

⁶⁰ A. D. Panagopoulos et al, "Satellite Communications at Ku, Ka and V bands, Propagation Impairments and Mitigation Techniques", IEEE Communication Surveys and Tutorials, 3rd Quarter, pp.1-13, October 2004.

⁶¹ K. P. Liolis, et al, "On the Combination of Tropospheric and Local Environment Propagation Effects for Mobile Satellite Systems above 10 GHz", IEEE Transactions on Vehicular Technology, Volume: 59, issue: 3, pages: 1109-1120, March 2010.

⁶² P. D. Arapoglou, et al, "Railway Satellite Channel at Ku Band and Above: Composite Dynamic Modelling for the Design of Fade Mitigation Techniques", International Journal of Satellite Communications and Networking, Jan. 2012.

⁶³ K. P. Liolis, et al. "On the Applicability of MIMO Principle to 10-66GHz BFWA Networks Capacity Enhancement through Spatial Multiplexing and Interference Reduction through Selection Diversity", IEEE Transactions on Communications, vol.57, Issue 2, pp. 530-541, Feb 2009.

⁶⁴ V. K. Sakarellos, C. Kourogiorgas, A. D. Panagopoulos, "Cooperative Hybrid Land Mobile Satellite-Terrestrial Broadcasting Systems Outage Probability Evaluation and Accurate Simulation", Wireless Personal Communications, July 2014.

illegal migration,⁶⁵ but also facing a huge wave of passenger traffic. This direction is also the route of the Eastern-European and Asian workers employed in the EU and travelling home for holiday every year. This means a wave of traffic between mid-June and mid-September is huge at this border section, it can be up to 10 000 vehicles per day with an average of 3000 vehicles per day, usually each with families of 3-5 or larger groups (mini-, midi-, and large buses). This daily pressure counts up to ~580000 vehicles exiting and about the same number (~588000) entering the Schengen Area at this section.



[REDACTED]

[REDACTED]

[REDACTED]

B. TRAINOSE-Greek border

TRAINOSE will host a train border-check pilot case, using as test-field the Eidomeni (GR) – Gevgelija (MK) border stations. The above mentioned border stations were selected due to the initial passage from an EU member country (Greece) to an Non-EU / Non-Schengen member country (FYROM) and vice versa. For this demonstration, two different cases will be examined; one will deal with a passenger train, whereas the other will employ a freight train.

CASE A: Passenger train

[REDACTED]

⁶⁵ Crossing the green border without permission is an offence in Hungary, therefore who commits it has no right to stay in the country, its presence is illegal.

⁶⁶ <http://www.cit-rail.org/>

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

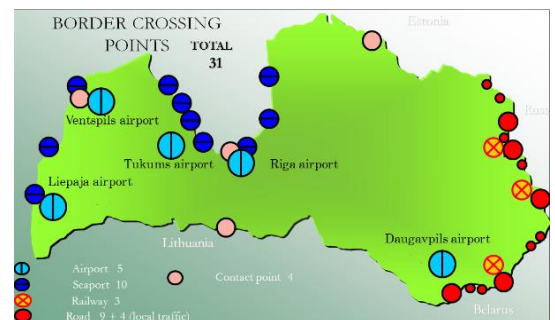
C. Borders of the Republic of Latvia

State Border Guard of the Republic of Latvia (SBG) is a direct administration State institution, under the supervision of the Ministry of the Interior. On issues of guarding and control of the State border, as well as on issues, which are associated with the control of the observance of the entry, residence, exit and transit of aliens and stateless persons regulations, and other issues within the competence.

Main tasks of the State Border Guard are Border checks of persons and means of transport at BCP, surveillance of the land and sea border between BCP, control of foreigners residence into the country and expulsion of illegal migrants (immigration control), investigation of criminal cases on illegal crossing of the state border and people illegal movement, identification of asylum seekers and documents' expertise.

Total border length of Latvia is 1878 km including land border - 1380 km and sea border - 498 km. Latvia has border with Estonia (EU) - 343 km, Lithuania (EU) – 588 km, Russia – 276 km and Belarus – 173 km.

There are totally 31 border crossing points (airport -5, seaport -10, railway -3, road -13)



[REDACTED]

[REDACTED]

D. Polish borders

Poland has an external EU/Schengen land border of 1163.25 km with non-EU/Schengen countries (state borders with Russian Federation, Republic of Belarus and Ukraine) along with 418 km external EU/Schengen sea border. Specifically, the whole Polish borderline is about 3512 km long, consisting of 440 km sea border and 3072 km land border: 210 km with Russia, 104 km with Lithuania (EU), 418 km with Belarus, 535 km with Ukraine, 541 km with Slovakia (EU), 796 km with the Czech Republic (EU) and 467 km with Germany (EU) as seen in the map below. Thus Poland is actually an EU external border and considering the presence of one main airport and 10 regionals in the country, the necessity to improve tools and methods in the context of automated border control systems, esp. [REDACTED]



Source: study of Border Management of Headquarters of Polish Border Guard

PBG - Polish Border Guard is the main Polish organization for the conductance of border checks and traffic control, and the protection against illegal immigration.

Border Guard Regional Units	Check Points			Border crossing points					
	Overall	External	Internal	Totally	Land	Railway	River	Sea	Air
	93	89	17	72	19	14	1	13	20
Warmińsko-Mazurski Regional Unit	11	10	1	8	4	3	—	—	1
Podlaski Regional Unit	18	13	3	9	4	4	1	—	—
Nadbużański Regional Unit	20	20	—	12	7	4	—	—	1
Bieleszowski Regional Unit	14	14	—	9	4	3	—	—	2
Morski Regional Unit	8	9	—	21	—	—	—	18	3
Nadwiślański Regional Unit	6	5	—	6	—	—	—	—	6
Śląsko-Małopolski Regional Unit	7	2	5	2	—	—	—	—	2
Nadodrzański Regional Unit	11	3	8	5	—	—	—	—	5

Source: study of Border Management of Headquarters of Polish Border Guard

Section 2. Impact

2.1 Expected impacts

Expected impacts listed in the workprogramme

Expected impact list from the call	Expected impact – iCROSS
..lead to novel mobility concepts for land border security	<p>iCROSS expected impact has the potential to become the fifth tier added to the access control model of the Integrated Border Management: in addition to embassies, Schengen cooperation, border control and measures within territory (in-depth checks), benevolent frequent travellers will begin to contribute to the effectiveness of the Schengen System, providing advance passenger information (API) on their free will, forecast traffic and generate feedback.</p> <p>Furthermore, iCROSS elevates the land border security with several new concepts, technologies and procedures that aim to improve speed and increase accuracy and reliability. A combination of novel and existing technologies will be integrated into a coherent and user driven system to ensure that the requirements of future land border control are met and proofs are provided.</p> <p>The integrated analytics tools that provide novel insights and intelligence and contribute in novel ways in identifying threats and vulnerabilities will contribute to frame the way risk scores are allocated as components for better planning and decision making for the border operations as well as for future predictive analytics across real-time border transactional data, better situational awareness and more targeted intervention.</p>
enabling authorities to achieve higher throughput at the crossing points whilst guaranteeing high security level	<p>With the use of the pre-arrival checks, average processing time is expected to drop by one third per traveller and authorities will be able to focus on risky passenger categories and individuals, achieving a higher security level. Furthermore, with increasing numbers of people and vehicles crossing borders every year there exists a strong demand for new ways of performing biometric recognition whereby throughput is increased, security is maintained or increased and all processing is performed in a legally and ethically compliant manner. Therefore iCROSS provides significant potential to deploy advanced technologies and analytics to enable border guards to perform enhanced risk assessment as for example, to detect attempts to evade identity checks, or choosing a particular moment to enter the border zone because the traveller believes that when increased numbers of travellers are passing through the identity checks will be less thorough. These tools collect information and enable border conformance checks and reporting and the detection of anomalous behaviour, focusing on optimization of traveller flow.</p>
Enabling fast processing of passengers within vehicles or pedestrians	<p>iCROSS expectation is, that average processing time of a third country national will drop by at least 30%. According to the recommendation of the Schengen Evaluation Committee, the average time for a thorough check shall be around 3 minutes, while a minimum check is 45 seconds. We are aiming at shrinking the time of the thorough check to the duration of minimum check, but taking into consideration, that not everybody will register and the penetration of internet connection and mobile devices is at low rate in certain countries, we set a reachable target with aiming at a least 30% drop in average (including non-registered travellers). This drop will result from the decrease in the number of steps the border guard has to carry out manually during thorough check. According to the Schengen Border Code, travel document validity (holder identity, expiration, date of issue), visa (if required), purpose and means of stay, existence of an alert on refusing of entry has to be checked and the traveller shall not pose a threat to public health, public security or international relations of the MS. The detailed list for HNP border guards, how to carry out these checks consist of 17 elements. With the use of iCROSS, only part of document validity (including identification of holder) has to be checked at the first line, the rest will be already assessed by iCROSS and results will be provided for the border guard. So time taken for thorough check of a low-risk third country national will take no more time than a minimum check for an EU citizen without relaxing border checks meaning level of security will be maintained continuously.</p>
improving the efficiency of passengers flow management	<p>Using the statistical module of the system and risk-based approach that deploys effective scanning and inspection technologies, border crossing points can be informed of expected numbers of travellers in advance, as travellers complete their pre-arrival check on the platform. Furthermore the portable units can detect and prevent illicit crossings of people and goods. Previously this was mainly available at airports and harbours; with iCROSS concept it can become a reality at road BCPs in wider extent.</p>

<p>Harmonization of requirements across Member States and Associated Countries (and standardization) is expected to also automatically greatly improve affordability</p>	<p>iCROSS is an effort to establish common procedures and assessment criteria and mutual approaches for identifying, classifying and addressing risks at the land borders. It is an approach that includes 4 EU member states end users (3 of them governmental authorities) that will define, develop and evaluate integrated start-to-end procedures and rules.</p> <p>The iCROSS analytics tool in addition to the risk based approach is expected to contribute to collaboration and coordination across border controls and enhance the SIS, EES and RTP with more information from land border not so far considered. Agreed and common risk model and standardized types of information collected and specified processes can improve communication between them. This is the beginning of an era where LEA can exchange information about travellers and goods, to organize public and private stakeholders to activities that can strengthen security and efficiency.</p> <p>Standardizing procedures and data not only save effort, by sharing and exchanging important information, but also generate savings resulting from streamlining and stimulating border security operations. With standardised procedures vertical, national implementations that increase costs can be replaced to achieve economies of scale. iCROSS contributes a step towards a more integrated and harmonised border control in EU area. An added bonus to this effort in standardization is the fact that it would ease the integration of new technologies and procedures across all the member states and associated countries reducing the costs of including innovative solutions to border control. Development of integrated mobile system for border control concept, will use the experiences with the operational work of the Border Guard in different EU countries. The acquired competence in this area, along with the knowledge obtained during the iCROSS project work will help to define the recommendations hardware and design of system to meet the requirements set for full functionality useful in the performance of duties by Border Guard officers. Providing connectivity for the mobile border control system with national databases connected to VIS, SIS II, EES will allow for immediate verification of a person crossing the border. This will increase the reliability of border control work carried out in the field and improve the procedures for the elimination of risk of penetration into the EU of unauthorized persons, or who use someone else's identity.</p>
--	--

Meeting Needs of European and global markets

According to the World Tourism Organization⁶⁷, the number of international arrivals shows a growth from a mere 25 million international arrivals in 1950, to 806 million in 2005, to a staggering 1.087 billion in 2013. The Organization forecasts a further growth in international tourist arrivals of between 4% and 4.5% in 2015 and by 2030; they expect the number of **people crossing international borders to exceed 1.8 billion per year**, which will undoubtedly increase the strain on border control.

Enabling smooth and fast border crossing for travellers, while ensuring an adequate level of security, is a challenge for many Member States. Currently, the Schengen Borders Code requires a thorough check at entry of all travellers crossing the external border; the system is largely depending on the human agent and its ability to capture the deceptive and illegal behaviour. The same checks are applied to all third country nationals, regardless of the level of risk associated with them or their frequency of travel. Although there are already measures and tools available at EU border crossing points, such as the Schengen Information System (SIS)⁶⁸ and Visa Information System (VIS), none is comprehensive enough and tackle the entire procedure from start-to-end, to ensure appropriate border crossings within the EU territory. The SIS is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area, in particular to carry out checks on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. The main purpose of the VIS is to allow the verification of a traveller's visa application history and, at entry level, verify whether the person presenting the visa at the border is the same person to whom the visa has been issued. None of them can consult in real time about suspects that are not yet listed. From the above it gets clear that the border control operations and their security lies in the centre of the Europe's political agenda as indicated by already existing and complementary European initiative (Smart Border Initiative).

Additionally, the European Commission has proposed the allocation of €3.5 billion from the €4.7 billion Internal Security Fund 2014–2020 to external borders and visas, including large-scale IT systems. The priorities for the fund are “The further development of an integrated border management system by improving, replacing, and upgrading

⁶⁷ <http://mkt.unwto.org/en/barometer>

⁶⁸ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm

equipment/infrastructure for visa and borders according to new technological developments. This would in particular include enhancing the operational capabilities of the member states within the framework of EUROSUR standards.”⁶⁹ Furthermore, in July 2010, in “The Global ePassport and eVisa Industry Report”⁷⁰, it was projected that ePassports become mainstream and significant penetration has been achieved; therefore the next logical step would be the proliferation of ABC solutions. In 2014, the ABC eGates began to gain significant traction in the global marketplace. In another report by Acuity, it was estimated that for Airport, Land Border and Sea Port, the overall systems’ deployment were counted to be 75,000 units worldwide (both fully automated as well as partially automated), which proves a still limited market size that will certainly be further developed.

According to EU statistics⁷¹ “In 2013, around 325 000 non-EU citizens were refused entry at the external borders of the EU28. More than 70 % of these cases were recorded in Spain (192 775) and Poland (40 385). In 2013, 12.4 % of the total number of EU-28 refusals were recorded by Poland, due largely to the high number of entry refusals (97 %) from Russia, Ukraine, Georgia, Belarus, Armenia. The preliminary check on entry and stay requirements will be able to significantly decrease this number by informing travellers on lack of entry and stay conditions (meaning a refusal) in advance. With checking travel document, visa, means and purposes as well as the SIS II alert on refusing entry, taking the same year, 119 195 travellers would have been informed in advance, meaning 36% less refusals, thus less administration work and staff effort for border guards.

	2008		2009		2010		2011		2012		2013	
	Refusals	%	Refusals	%	Refusals	%	Refusals	%	Refusals	%	Refusals	%
EU-28	634 975		499 640		394 800		343 005		316 015		324 840	
Belgium	1 170	0	2 055	0	1 855	0	2 730	1	2 390	1	1 535	0
Bulgaria	4 060	1	3 030	1	3 070	1	2 810	1	3 070	1	2 550	1
Czech Republic	255	0	380	0	330	0	360	0	190	0	310	0
Denmark	70	0	60	0	80	0	115	0	95	0	140	0
Germany	7 215	1	2 980	1	3 550	1	3 365	1	3 820	1	3 845	1
Estonia	2 325	0	915	0	1 665	0	2 205	1	1 915	1	1 400	0
Ireland	5 260	1	3 560	1	2 790	1	2 545	1	2 205	1	1 935	1
Greece	2 055	0	3 000	1	3 805	1	11 160	3	9 415	3	6 995	2
Spain	510 010	80	387 015	77	290 045	73	227 655	66	199 830	63	192 775	59
France	16 695	3	14 280	3	9 840	2	11 100	3	11 310	4	11 745	4
Croatia (*)											10 015	3
Italy	6 405	1	3 700	1	4 215	1	8 635	3	7 350	2	7 370	2
Cyprus	895	0	670	0	685	0	575	0	545	0	430	0
Latvia	875	0	670	0	815	0	1 230	0	1 820	1	2 050	1
Lithuania	2 210	0	1 750	0	1 965	0	2 215	1	2 215	1	2 865	1
Luxembourg	5	0	0	0			0	0	5	0	0	0
Hungary	5 530	1	7 700	2	10 475	3	11 790	3	9 240	3	11 055	3
Malta	120	0	140	0	130	0	80	0	200	0	300	0
Netherlands	3 160	0	2 500	1	2 935	1	3 500	1	2 515	1	1 990	1
Austria	2 715	0	645	0	400	0	445	0	245	0	360	0
Poland	16 850	3	26 890	5	23 015	6	20 225	6	29 705	9	40 385	12
Portugal	3 600	1	2 565	1	2 060	1	1 795	1	1 240	0	810	0
Romania	8 920	1	4 595	1	4 750	1	3 620	1	3 340	1	3 410	1
Slovenia	7 565	1	7 895	2	7 845	2	7 970	2	7 665	2	4 780	1
Slovakia	1 540	0	855	0	840	0	595	0	595	0	435	0
Finland	1 775	0	1 300	0	1 185	0	1 420	0	1 640	1	1 735	1
Sweden	55	0	35	0	90	0	155	0	155	0	180	0
United Kingdom	23 640	4	20 460	4	16 365	4	14 720	4	13 300	4	13 435	4

Fig 9: Non-EU citizens refused entry at external borders, by EU Member State⁷²

In the Hungarian border it is estimated an average checking time for persons enjoying the right of free movement and stay (EU families) is no more than 10-15 seconds per person, and up to 3 minutes for checking third country citizens. The estimated average of 3.5 million persons crossing the border every year and estimated third country citizen rate is 48% (~1.7 million). According to official statistics the last five years averagely 32 million foreigners crossed the Hungarian borders every year. Annual total passenger flow for Schengen borders is estimated between 490-585 million border crossings per year.

The challenge of iCROSS is to bridge and complement the market needs, the efforts and initiatives of the EU and provide additional IT tools to improve the planned services in EU and globally wide.

Target Markets and Size

As iCROSS challenges are valid for all European and Schengen Territories border control authorities, these constitute the target market, but also territories beyond Europe can be addressed by partners. Indicators of the investments and interest is evidenced by the following:

Automated Border Control (ABC) solutions are fundamentally transforming the global travel experience. From Australia’s SmartGates and US Global Entry to the hundreds of eChannel gates at Hong Kong land and sea crossings, to the Automated Passport Control Kiosks rolling out across North America, and the nearly 200 eGates planned for deployment in the UK and Germany next year, ABC technology is driving the development of the 21st century international transportation infrastructure.

⁶⁹ “Borderline, The EU’s New Border Surveillance Initiatives”, A study by the Heinrich Böll Foundation, June 2012

⁷⁰ <http://www.acuity-mi.com/index.php>

⁷¹ http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_enforcement_of_immigration_legislation

⁷² http://ec.europa.eu/eurostat/statisticsexplained/index.php/File:NonEU_citizens_refused_entry_at_external_borders,_by_EU_Member_State,_2008%E2%80%9C2013_V1_1.png

According to a market report⁷³, published by Transparency Market Research, the global homeland security market was valued at USD 245.72 billion in 2013, growing at a CAGR of 5.6% from 2014 to 2020 to account for USD 364.44 billion in 2020.

The major factor driving the growth of homeland security market is several government initiatives undertaken to restrict increasing terrorist threats and cross border insurgency. In addition, rising cases of illegal immigration, drug smuggling and human trafficking are compelling the governments of various countries to invest heavily in procurement of homeland security products.

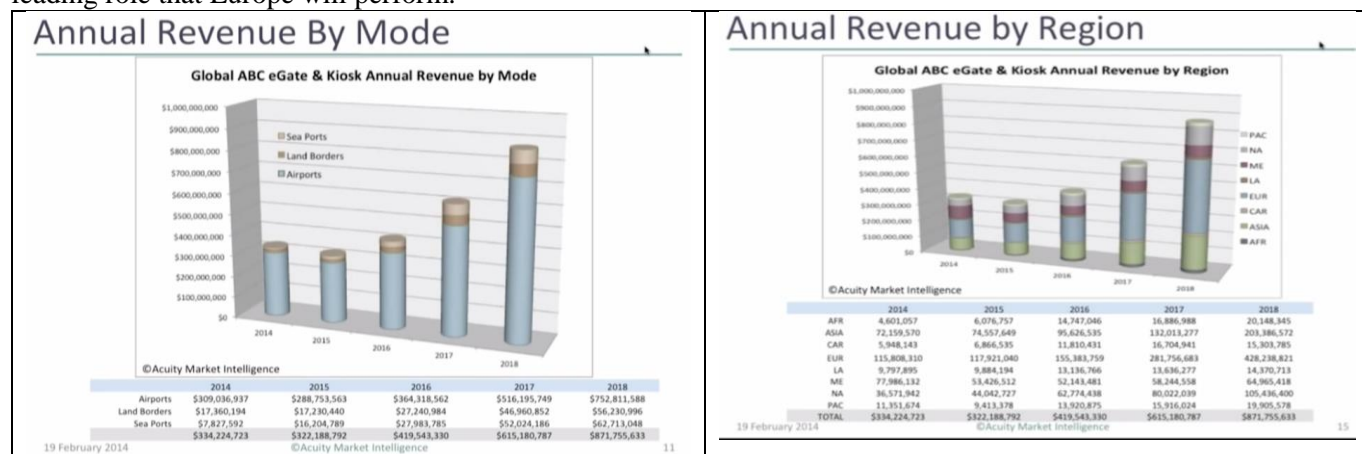
More particularly, and as far as Automated Border Control (ABC) is concerned, Acuity Market Intelligence reports⁷⁴ that the rapidly evolving ABC eGate and kiosk market will generate more than \$1.2 billion dollars in annual revenue by 2020. The total number of ABC eGates deployed as fully automated replacements for border control stations is projected to exceed 6,000 by 2020. An additional 33,000 specialized immigration self-service kiosks and eGates will be deployed at check-in, baggage drop, arrival halls, and boarding gates at airports, land borders, and seaports worldwide.

Nearly 50% of the total number of eGates deployed at all airports, seaports and land borders are in Asia. Europe leads in airport deployments with nearly 40% of global units. eGates are estimated to increasingly be used at land borders; today they just represent 4.7% of all eGates deployed.

Europe will be the largest market for ABC eGates and kiosks representing a 47% total revenue market share from 2014 to 2020. Asia will follow with 22.5% revenue market share over the forecast period.

Airports are, for the time-being, the dominant sector in the ABC eGate and kiosk marketplace, nevertheless by 2020, they will cede ground to land borders and seaports.

Indicative numbers are presented in the following figures, clearly showing the increase in land border needs and the leading role that Europe will perform.



Other impact (Environmental, social, etc.)

Efficient border control operations has a variety of **social impacts** primarily in ensuring that borders remain under surveillance and are controlled.

Border Management is a challenge but comes together with a great opportunity since it will help contribute towards **an increased amount of security for all citizens** with more **secure borders**.

This supports tourist activity, and also helps to ensure safety for all by:

- Reducing the number of illegal immigrants who enter country borders undetected
- Increasing internal security as a whole by contributing to the prevention of cross border crime
- Increasing internal security as a whole by contributing to the prevention of cross border terrorism
- Reducing the traffic of drugs, weapons and illicit substances
- Preventing deaths of illegal immigrants entering countries

Barriers to achieving the expected impact

A number of persistent barriers can be identified, which the project's design has considered and should be overcome:

- Initial Investment:** The investment needed to research, design, implement and commercialize a tool like this will discourage most stakeholders. iCROSS is meant to be a foundation stone where they can build upon.
- Procedures and Technology reform:** The adoption of iCROSS implies important reframing and adjustments to border control processes and infrastructures as well as the daily work of border control authorities. Thus final adoption in everyday practice underlines central decisions, financial support, education and training, etc., which the nations have to adopt.

⁷³ <http://www.transparencymarketresearch.com/homeland-security-market.html>

⁷⁴ http://www.acuity-mi.com/ABCair_Report.php

- iii. **Critical mass of End users and Policy regulators:** iCROSS is integrating and improving psychological factors research and technological tools of diverse nature to improve border control operations. Due to its nature, the future adoption is only guaranteed with a critical mass of policy regulators, end users and stakeholders, which adopt and participate in the initiative and promote it further.

2.2 Measures to maximise impact

a. Dissemination and exploitation of results

The iCROSS dissemination & exploitation strategy in line with the innovation management approach consists of several policies, intended for the transfer of project achievements and lessons learnt and mainly to commercialise project results. The planning of dissemination policies, which is a *horizontal* procedure along the overall project lifecycle, will start immediately with the start of the project. In general, dissemination & exploitation policies will be based on the following:

Dissemination to European Industry	<p>The industrial partners and public bodies will disseminate the usage of iCROSS within their companies and organisations, out of the department or unit in charge of iCROSS participation and through their networks. Dissemination will be produced by means of the following mechanisms:</p> <ul style="list-style-type: none"> • Informal knowledge dissemination within each organisation, through internal websites or newsletters. • Meetings of iCROSS related staff with other personnel out of the project (in order to identify synergies). • Dissemination to related Business Interest Group (BIG) - the following indicative potential target groups for dissemination of non-confidential information iCROSS vision and innovations are initially identified: <ul style="list-style-type: none"> ○ Border control/face recognition technology tools/Sensors/Document recognition hardware and services suppliers (Business domain): iCROSS will share non-confidential information about the potential and the progress of the project for potential translation to other fields of interest, further exploitation of the results. ○ ICT applications suppliers and Industrial Community (Technological domain): iCROSS frontend and backend environment in terms of software and cloud-based applications/platforms and their technology will be demonstrated together with its publicly available documentation so that it can easily be the basis for many other applications for other target groups and even other application domains. Partner [REDACTED] are active in the provision of IT and commercial solutions in the private and public sector in sensors/tools/data integration and other domains and will disseminate the project results to their channels.
Dissemination to the scientific community	<p>The iCROSS consortium is strongly motivated for providing technological and scientific results that will be of major importance and interest for the scientific and industry communities. These results will be communicated in iCROSS website, at scientific, ICT and Security society meetings, submitted for publications in peer-reviewed journals and in press releases for popular and sectorial magazines, and newspapers. Efforts will be made to promote Open Access policies.</p> <p>In addition, the Scientific Council of the Hungarian National Police intends to host scientific and press events to present the project to the public, as follows:</p> <ul style="list-style-type: none"> ▪ 3-day national workshop for border guard, legal, technical and human rights experts in Hungarian, to generate significant input for relevant WPs; ▪ 3-day international workshop for experts to elaborate relevant findings in WP6; ▪ 2-day national conference to present results in Hungarian; ▪ 2-day international conference to present results of the project, inviting Central and East Europe Border Guard and Police authorities, foreign representatives, the Frontex, the Borderpol, the Ceuol and the Europol, EU-LISA. <p>Prior to each event, a press release will be released by the police and press will be invited to the last day of the events where there will be a press event and the consortium will give interviews in Hungarian and in English. Conferences will be broadcasted live and also recorded. Presented papers will be published in a peer-reviewed publication with ISBN number in both (English and Hungarian) languages.</p>
Dissemination of Knowledge to the wider	<p>Many of the partners involved in the iCROSS project are heavily engaged in collaboration projects concerning Security and e-borders/e-customs on a national and international scale. These collaborations allow these partners to transfer knowledge, and also to extract new challenging problems that require research to achieve new knowledge. ED is a major provider of IT solutions and services in 27 countries for the public sector and will thus disseminate the project knowledge and results through its activities and partnerships. [REDACTED] and</p>

	The iCROSS project intensifies this mutual insemination. It is an invaluable advantage for the partners to be able to produce experience with collaboration that has led to excellent research results and at the same time produced significant commercial impact. Periodic plenary and thematic/work package meetings will be held and involve all relevant public and industry partners.
Dissemination to policy makers and reform	iCROSS results will be disseminated to policy makers to the extent that this technology needs to be integrated in several border control facilities, aiming at the public sector. Thus information as illustrated in the sections below will be accessible to national policy makers. Private confidential meetings with European reimbursement agencies, European regulatory offices or notified bodies will be organized whenever requested, for advices and recommendations for the development of iCROSS intelligent border security system. The Hungarian National Police intends to bring results to European and national stakeholders with presenting results at 1) the Frontex Management Board, 2) Annual International Border Guard Conference 3) to Borderpol (an international NGO of border guards around the globe).
Commercial exploitation	Recognized by iCROSS consortium as the key driver for any future commercial success. The commercial exploitation plan is always based on a study that shall deal with the Background and Foreground Rights, the Patents, trademarks and IPR issues, which will be in the base of the future iCROSS product, taking account of EU policies, including those to foster the transfer of technology to SMEs, and promoting the use of generic, non-proprietary technologies, as well as the overall European security framework. In order to design a successful Exploitation strategy, the exploitation document will be developed taking as a reference the <i>Business Model Generation</i> (proposed by “Osterwalder&Pigneur” in 2010).
Educational use	As the research/academic/public authorities institutions engaged in the iCROSS project have teaching duties, the results of the project will place them in a position, where new alleys in the education of students or trainees can be exploited. The results of the iCROSS project will be used to provide students/trainees, research fellows and several companies with teaching and consultation services. These services will entail the transfer of knowledge and know-how to interested entities in the fields of: biometrics, sensors, IT platforms/databases, data fusion, and borders security.

Path towards commercialization

Dissemination and exploitation efforts and materials are to be generated and their viability, integrity, complementarity, and consistency are supervised in WP7. iCROSS exploitation and commercialisation depends upon:

- Privacy regulations which are based on international and European regulations but may vary in each country, and thus require to be addressed in order to be commercialisable and ensure its wider acceptability and use.
- The modernisation of working processes and workers’ management procedures, equipment and software that facilitates border monitoring and security and support of the facility management of the public sector authorities and the promotion of this plan within the public workers.

A stepwise approach to ensuring maximal exploitation of project results will be pursued:

Step 0: Understanding the full value chain and building the value creation, and the business /use case early in the project which will be achieved in line with the project’s innovation approach.

Step 1: Investigation of all relevant market segments and further potential application areas, including legal, financial issues, competition and business planning taking into account of marketing studies and socio-economic research and carrying out complementary primary research where required. This activity will be mainly performed by marketing departments of iCROSS industry partners, in order to understand the possible threats and defining the proper wordings to be used in internal product leaflet in order to respond to the regulations in Europe and rest of the World.

Step 2: Analysis of complementary and competitor services and equipment in the market and wider community; identification of emerging best practice across the border security management internationally.

Step 3: Develop the deployment and business scenarios, market and business models for individual exploitation and joint exploitation, specifying collaboration roles, costs and revenue flows thus enabling calculation of net return over time for each type of market player, commercial and/or public; Identification of exploitation paths including the product roadmap, certification accreditation, commercial licence, etc. This will involve the socio-economic analysis of the solution and its impact.

Step 4: Organisation, planning and execution of wide impact dissemination activities to create full awareness of iCROSS activities and approach in the academic community, the Security, the ICT and general RTD community.

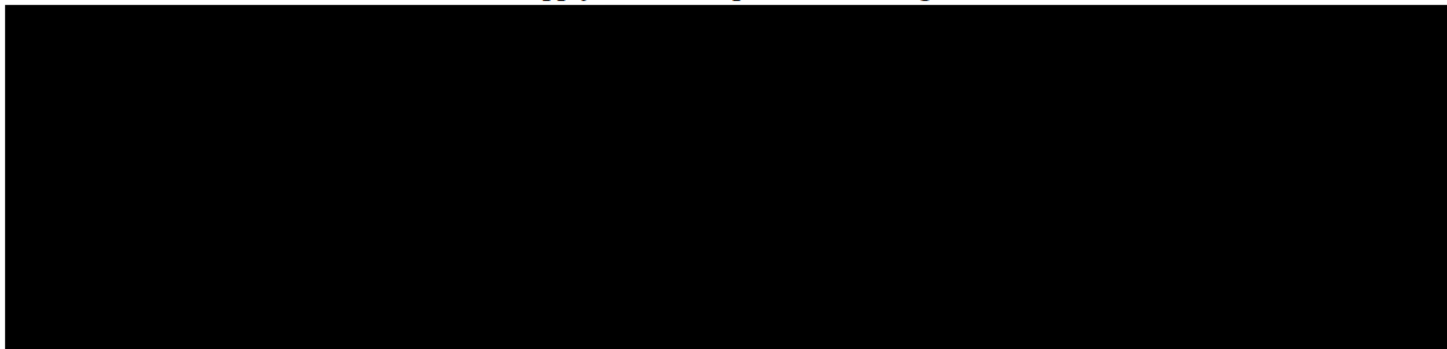
Step 5: Regular review, revision and refinement of partner-specific exploitation plans and joint/collaborative business plans in the light of interim project results; formalisation of service level and other appropriate agreements for joint exploitation among partners and third parties including possible creation of new legal entities (joint venture).

Step 6: Development and publication of a short evidence document outlining the experience and results of deploying iCROSS in real life scenarios, to be used for convincing new adopters of iCROSS solutions.

In general, if the project is successfully completed, it is expected that sufficient interest may have been raised from the market to enable initialisation of commercialisation procedures. However, commercialisation will require small additional investment and will not take very long after the completion of the project. The following key standards will be though foreseen to comply with during and after the project commercialisation:

Early joint exploitation plan

iCROSS consortium covers the whole supply chain as explained in the figure below:



The consortium intends to commercialize the outcomes of the project through **alliance agreements** with the partners led by ED, a well-established and respected corporation in the ICT market with multiple successful products and services on the market.

. This alliance exploitation agreement will outline the commercial cooperation roles-responsibilities and costs-revenues among the partners which developed system components and will be developed at the middle of the project when more is known about the exploitation plans.

An alternate method of capitalization on the iCROSS project's outcome for all its members is by exploiting the expertise they will gain in border control automation. Currently due to the limitations associated with border control (closed environment, classified procedures, hard to acquire realistic data) specific research is difficult to perform and the unique blend of consortium partners in this project will enable everybody to benefit from the added expertise, and network expansion that will be maintained through the established iCROSS alliance.

Exploitable results

The exploitable results are the entire platform but also the partial results of the individual tools and scientific research that will be the result of iCROSS. The following figure outline the main results, the exploitation paths and the partners interested in each of them.



Commercialisation model

iCROSS is a fully scalable system that is by design inter-operable and based on a scalable architecture; thus can be easily deployed in all EU countries' points of external entry. iCROSS platform with its mobile units and novel concepts for land crossing will be commercialised as a whole as well as partially by:

- Protecting the IPR of the relevant consortium partners for specific tools found to be successfully deployed and meeting expectations through the Pilot study making it available through a licensing scheme to border control authorities

- Developing the iCROSS platform and its tools can be offered to public authorities by answering to specific tenders by partners led by [REDACTED] and in alliances to offer the complete or partial solutions as required in each case. The platform will be offered in terms of license costs in addition to services to install, customize the tools and train the end users in the various countries. [REDACTED].
- Providing consultancy services that will built upon the expertise of the partners and the iCROSS experience.

Individual exploitation & use plans

ED is a leading innovative IT company, acting internationally, which is always interested to enlarge its current activities. ED has proven in its long history that it can successfully launch new products and services in the international market, and this is proven by the number and the importance of its clients (see profile). [REDACTED]

ICCS is a very active non-profit, Academic, Research Institute, addressing multi-disciplinary fields, being at the forefront of knowledge-intensive competitiveness, representing the dynamic academic Greek [REDACTED]

STR Stremble Ventures is a research and development company focused heavily on further developing its portfolio of services and technologies. The core of STREMBLE is its multi-disciplinary team of scientists that come together to tackle challenging and often complicated tasks requiring inter-disciplinary expertise and cooperation. [REDACTED]

[REDACTED]

MMU

[REDACTED]

ITTI

[REDACTED]

EVR is a multinational group born in Spain with a commercial network around the world that provides global solutions for critical systems in the fields of Aeronautics, Space, Defense, Security and Emergency, based on engineering developments and innovative technologies developed both in-house and by third parties. EVERIS AD does provide the most leading technology, developed by ten Spanish companies which make up the group, taking advantage of the flexibility and speed in R&D and innovation processes.

Everis has a broad experience in working with biometric technology [REDACTED]

BIOSEC is an R&D company specialized on developing biometric authentication solutions based on palm vein recognition especially in the field of IT security, mass identification and access control. BioSec's major goal is to further widen the portfolio of services and products through system integrations with third party systems.

[REDACTED]

[REDACTED]

LUH

HNP, PBG, TRA, BSG [REDACTED]

IPR Strategy

IPR management is crucial when developing complex software as it requires certainty as to the property of IP and a perfect understanding of the features, consequences and effects of the licenses accepted and/or used. Key developers and managers need explicit rules on how to access pre-existing know-how and foreground knowledge and qualitative and practical information support on how to ensure the protection of intellectual property as well as the ability to address legal issues with licensing experts.

The IPR management strategy will be the responsibility of the Project's Steering Committee and will be explicitly supported in the Consortium Agreement. It will include:

- raising participants awareness regarding IP issues
- contributing to the resolution of disagreements between participants
- assisting in the drafting of the plan for the use and dissemination of foreground
- tracking down results that should be protected and advice the individual partners on the means of protection
- assisting the participants in evaluating their contribution to the jointly owned foreground and establishing their respective shares
- deciding regarding third parties joining the consortium with the intention to receive the ownership of the Foreground of a specific Party.

	<ul style="list-style-type: none"> • Present the concept, objectives and expected results 	the target market of iCROSS <ul style="list-style-type: none"> • Demonstrate early results (components and early technical validation results) 	<ul style="list-style-type: none"> • Demonstrate more advanced results (components and intermediate and final validation results)
ACTIVITIES	<ul style="list-style-type: none"> • iCROSS logo validation • iCROSS project web-site • Event, literature, research source identification • Press release • Project leaflet • Select events for attendance and start attending 	<ul style="list-style-type: none"> • Refine web-site with more concrete results and news • Social media and online promotion, such as news about early results in Twitter, Facebook, etc. and newsletter • Publish brochure, press release with intermediary results • Distribute marketing material • Attend events • Create YouTube videos showcasing components and intermediary results • Publish scientific papers in conference journals 	<ul style="list-style-type: none"> • Refine web-site with news, videos, photos, public deliverables and partial results • Social media and online promotion, such as about early results in Twitter, Facebook, etc. and newsletter • Publish brochure, press release and newsletter to registered parties and partners' relevant contacts • Distribute marketing material • Attend events • Workshops • Issue final press release • Create YouTube videos showcasing the system in trials and users' opinion • Publish scientific papers in conference journals • Demonstrations and feedback of trials evaluation
Target Groups			
Public workers and wider public Public workers, facility managers, working conditions advisors, IT engineers, Students, Researchers and the general public	Funders and policy making bodies Policy makers in government, ministries and Regulators-Managers etc. Donors, Grants providers and Development partners, Representatives from international and national development cooperation agencies	Enterprise and Industry Industry stakeholders, Private sector: Intelligent Border/Security suppliers companies, electronics and sensors manufacturers, mobile, web and IT developers.	

The project will aim at four levels of communication: awareness, understanding, action and participation. The target groups of each level have been identified and are presented in the table above. *Awareness* will mainly involve delivering the main message of the iCROSS project in relation to its aim and objectives, while *understanding* will require the providing of more detailed information on the project purposes, methods and deliverables. Involvement in both of these two stages will provide the basis for communication for *action*, where the project products will be delivered for further use. Communication of information is particularly necessary when targeting stakeholders likely to participate (in supporting the project), namely those who will offer financial, administrative and technical support within the project duration.

Efficient communication during the project will make use of a variety of dissemination tools. This will include:

Development of iCROSS visual identity

A **visual identity** will be developed for the project comprising a logo and style guidelines for on-line and off-line publications including at least the following applications:

- The project logo and website; Online banners; Social media accounts (project's online 'persona'); a Wikipedia entry; PowerPoint presentations; Exhibition stands; Project leaflet and other promotional material. A consistent look but also consistent written communication, a set of standard project descriptions and key messages will be provided.

iCROSS website and operation

An interactive and accessible project web site will be developed by ED and made available before *Month 1* of the project. The website will be referred to in all iCROSS public documents and presentations, as well as its QR code for easy reference. An easy and convenient content management will be provided making use of the open source content management software "Drupal". The public section of the iCROSS website will provide:

- a brief project summary in journalistic style highlighting the objectives, the contents and the structure of iCROSS
- a short profile of each partner and link to each site
- access to the project Public Deliverables and abstracts of selected non-Public Deliverables;
- publications and presentations at external conferences in various formats (pdf, MSWord, etc.);
- events section, promoting the events that the iCROSS consortium participates or (co-)organises.
- interactive features, such as questionnaires and/or FAQ, allowing for periodical online activation to be used for collecting end-users input whenever this is need, i.e. Towards the requirements analysis,
- visible links to the social media accounts of the project
- technical & scientific information (e.g. white papers) and user-oriented information;
- Relevant web sites of interest for the project such as companies, institutions, etc.
- Factsheets, reference materials and results produced within the project itself, including deliverables.
- Contact us section

A counter of visitors and other statistical tools will be used (including a visitors' feedback form), to monitor the usability and interest created by the web site and the project. The goal is to have a continuously increasing average number of web visits at monthly level.

The content of the website will be managed by: ED (general); the IP Management Team for the technical and scientific content.

Electronic newsletters

Short electronic newsletters, or e-newsletters and YouTube videos, informing key stakeholders of project developments will be developed

- The e-newsletter is issued on a six-month basis in English, so the frequency of publication must be maintained at all times whereby regular intervals are respected.
- The e-newsletter must be short.
- Each piece of news must be short, and concluded by a hyperlink that will invite the reader to get more information through the website.

The newsletter will include details of the project (Basic description of the project; description of the partners; description of the methodology and indicators), updates on its phases, a description of the preliminary technological enablers, summarization about the progress of the implementation of the specific technological enablers within the prototype, reports on the project's participations in events, proposed topics for the workshops, conclusions of the workshops, relevant media coverage, interviews and / or quotes from stakeholders' opinions regarding the necessity of the project, description of the final conclusions of the project;

Social media and online promotion

Facebook, Twitter and Google+ accounts will be set up for the project, with the aim to foster more accessible communication. YouTube channel will be set up, for easy upload of footage from the workshops, demo clips and other. The icons will be integrated in the website, for the audience to be aware of the availability for "conversation" of the project.

Publications and Participation in workshops, conferences and events

Participation of the project to up to 30 relevant European or international events (workshops, conferences and exhibitions) taking place within the European Union mainly (but not limited) to promote the project and its results. iCROSS events will be chosen taking into account the objectives set out in the project communication plan. Indicatively, a list is presented but will be further updated during the course of the project with more actual information. A detailed proposal for such events with the associated timing and objectives will be included in the communication plan to be presented on Month 6. The goal is to have at least 10 presentations and Demos in Conferences each project year. Key to the traditional dissemination strategy is to focus on a number of scientific and business publications outlining key technical achievements or business potential. The following provide indicative list:

will specifically target the following journals:

- IEEE Intelligent Systems
- Expert Systems With Applications
- Computers & Technology
- Information & Management
- IEEE Transactions on Neural Networks and Learning Systems
- International Journal of Neural Systems
- Journal of Nonverbal Behaviour
- ACM Transactions

and the following conferences:

- EASST – European Association for the Study of Science and Technology
- EMAC - European Marketing Association Conference
- ECIS - European Conference on Information Systems
- International Conference on Information Fusion
- EURO ID exhibition
- World e-ID congress
- SDW – Security Document World Exhibition
- SMi Border Security Conference
- IEEE International Conference on Artificial Neural Networks
- IEEE World Congress on Computational Intelligence
- Smart Borders Conference 2015
- European Day for Border Guards (FRONTEX)

In addition, some results of the project and announcements for iCROSS workshops and conferences will be disseminated through:

- Practitioner (trade) conferences such as ACI (Airports Council International), MMU have lots of experience with mass media – this contributes to acceptance by public
- Press releases and media interviews since i.e. MMU has a good track record in TV/radio interviews (whenever it is relevant);
- The websites of other thematically-related EU projects;

Preparation of publication and promotional material

iCROSS promotional video

A Promotional video will be prepared that will illustrate, in eloquent and business oriented style, the overall results of the iCROSS project and its success stories. This video will be promoted at the project web site, but also at YouTube. Leaflets and Posters Flyers: 2.000 copies, A4 recto verso, full colour, and posters: 200 copies, A1, full colour will be produced in two stages:

- By end of month 6, focusing on project objectives, challenges, and expected benefits for the project stakeholders, with aim to attract interest and involvement of stakeholders and SMEs in the pilot actions
- By end of month 20, focusing on project objectives, challenges, and results achieved, with aim to widely promote the project achievements and expected impact for customs and taxation across the EU and beyond.

The quantity for each material in each of the two phases will vary in function of the project needs and objectives, according to the expected distribution number which will be identified in the Communication Plan and limited by the maximum quantities proposed.

Participation in workshops, conferences and events

Participation of the project in up to 20 relevant European or international events (workshops, conferences and exhibitions) taking place within the European Union mainly (but not limited) to promote the project and its results. iCROSS events will be chosen taking into account the objectives set out in the project communication plan. Indicatively, a list is presented but will be further updated during the course of the project with more actual information. A detailed proposal for such events with the associated timing and objectives will be included in the dissemination plan to be presented. The goal is to have at least 10 presentations and Demos in Conferences each project year.

Collaboration with other projects – iCROSS will collaborate with other relevant projects aiming at exploiting synergies and impact increase. The envisaged fields of activity include joint activities for exchange, dissemination and training and coordination of standardisation efforts.

Section 3. Implementation

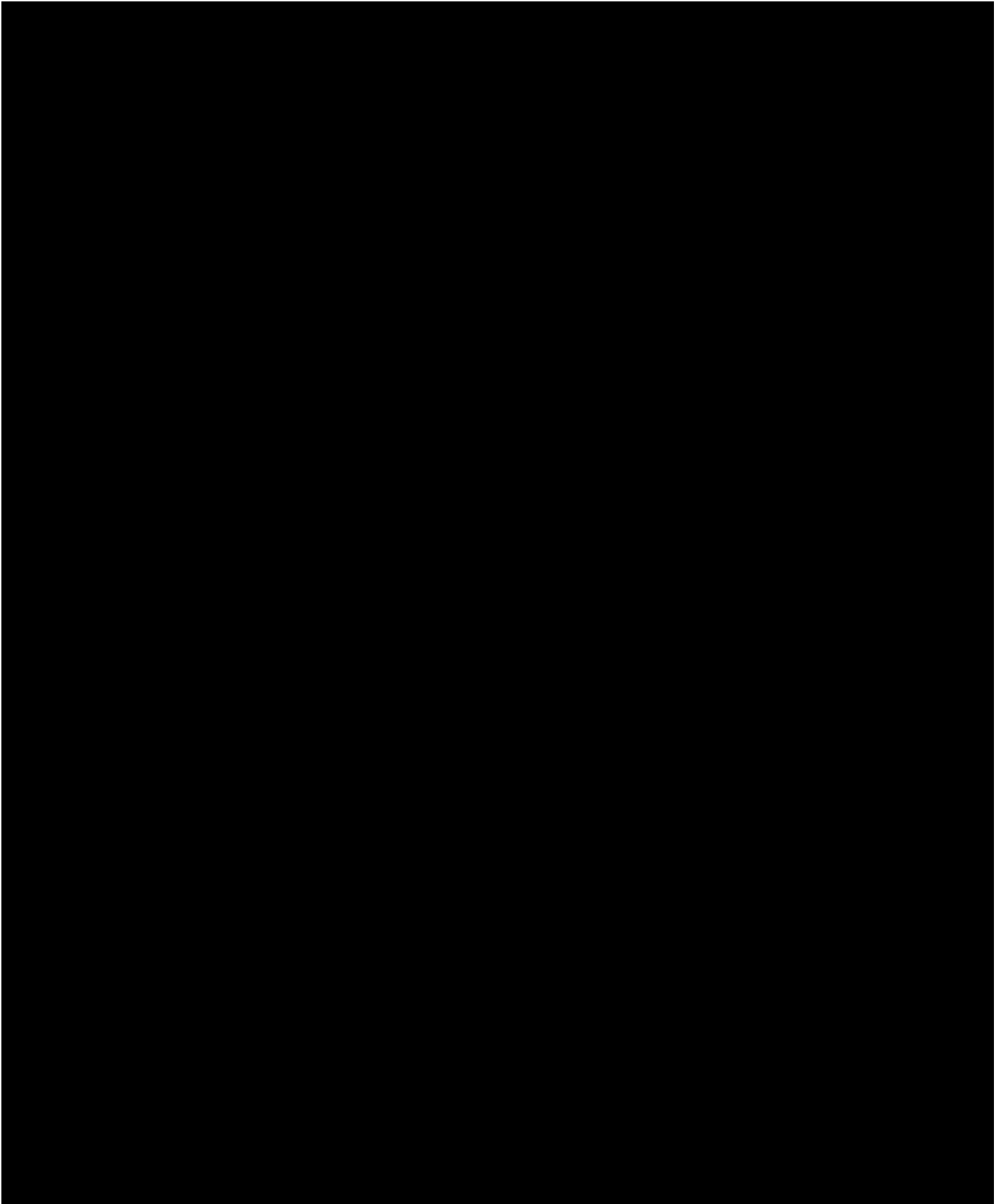
3.1 Work plan — Work packages, deliverables and milestones

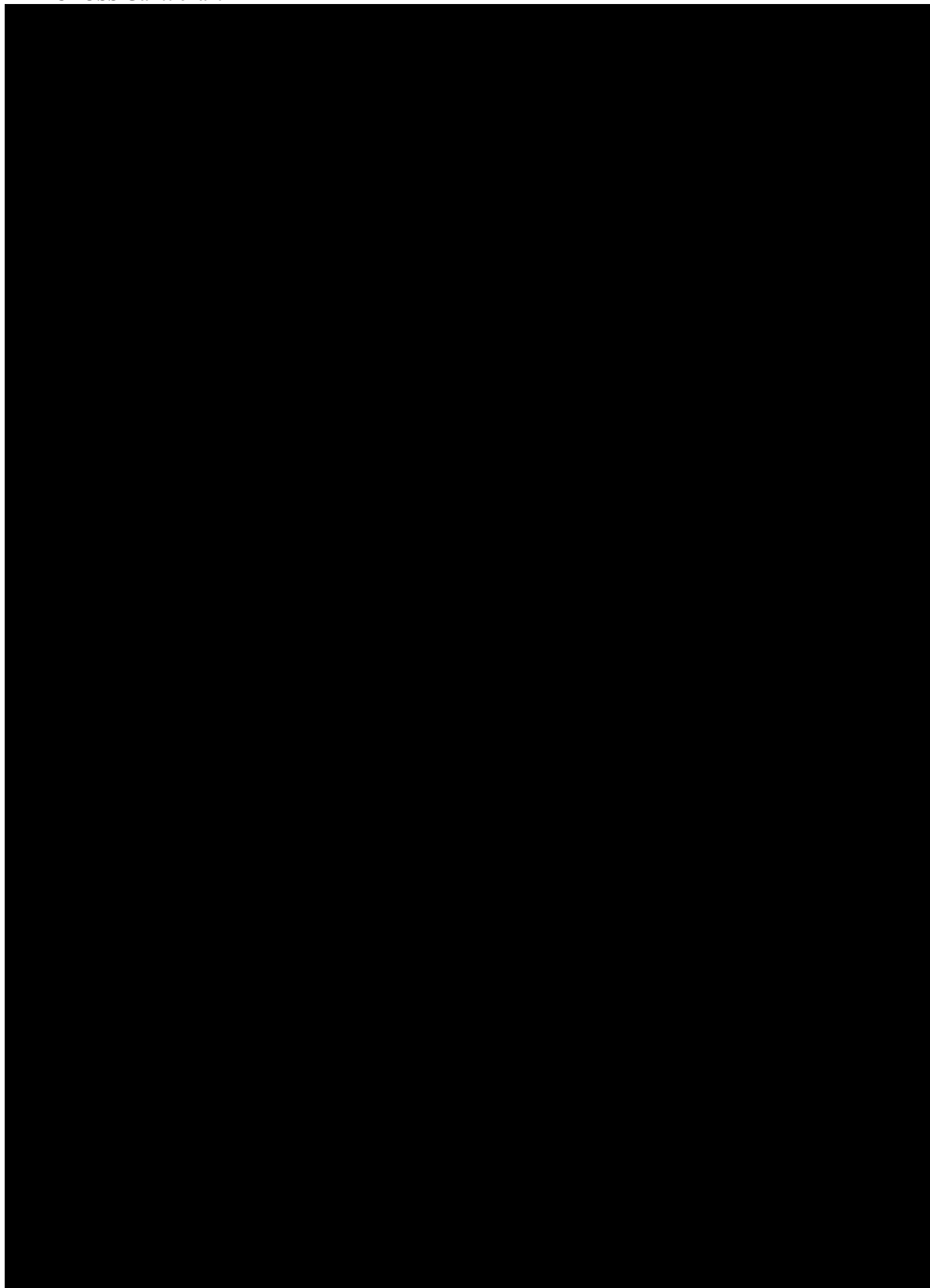
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[illegible][illegible]

- [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]
 ■ [REDACTED]

[illegible]

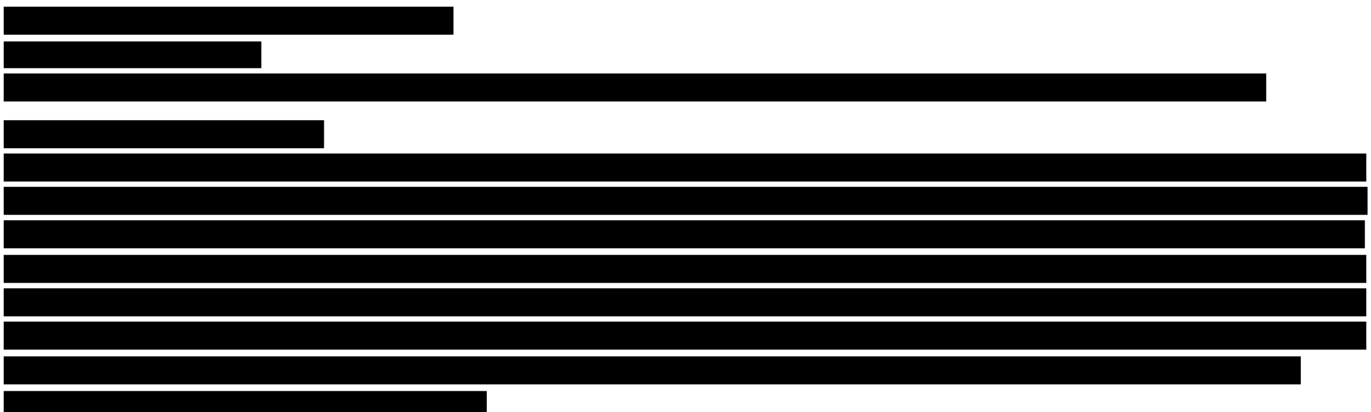
[REDACTED]

[REDACTED]

- 1. [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- 2. [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]




[REDACTED]	[REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

57

Section 4: Members of the consortium

4.1. Participants

1. European Dynamics Luxembourg SA

NAME:	 European Dynamics Luxembourg SA.				
Short Name:	ED	Country:	Luxembourg	Partner #:	1
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>EUROPEAN DYNAMICS SA (ED) is a leading European software vendor and Information and Communication Technologies (ICT) services provider, operating internationally through its offices and antennas in Alicante, Athens, Berlin, Bonn, Brussels, Frankfurt, London, Luxembourg, Nicosia, Stockholm, Tunis, etc. The company designs, develops, supports and promotes software ICT applications using integrated, state-of-art technology to governments, public organizations and private enterprises in more than 27 countries in the world. Customers include government institutions, multinational corporations, public administrations and multinational companies, research and academic institutes. ED has an extended expertise in the areas of e-Government (they include Taxation, Customs, Statistics, Intellectual Property, Trade Marks, Patents, Pharmaceuticals, Health, Justice, etc.), e-Business, e- Procurement, e-Collaboration, groupware and workflow, content, document and knowledge management, communications middleware, ICT security. Own software products and tools have been developed in these domains. All the products and services are offered for web, intranet and Internet environments and are based on open architectures and state-of-the-art technologies.</p> <p>ED is an ISO 9001:2008 and ISO 27001:2005 certified company and holds a NATO and EU security clearance (secret).</p> <p>ED has expertise in the provision of SaaS, e-business (B2C, B2B, B2E, B2G, G2G, etc.), BroadBand Services, e-collaboration and workflow management, developing its own software applications and products, offered for web, Internet and portable devices, relying on open architectures. Its activities include the:</p> <ul style="list-style-type: none"> • successful delivery of a large number of IT complex projects to international organisations, such as the European Parliament, the European Court of Auditors, Interpol, the European Environment Agency (EEA) , the European Medicines Agency (EMA) , the Office for the Harmonisation of the Internal Market (OHIM), the European Police Office (EUROPOL) , the Publications Office of the European Union (POEU) , the European Centre for the Development of Vocational Training (CEDEFOP) , the European Chemicals Agency (ECHA) , the European Centre for Disease Prevention and Control (ECDC) and national administrations in Austria, Cyprus, Germany, Finland, Belgium, Bulgaria, The Netherlands, Italy, Switzerland, etc. • design and implementation of integrated ICT systems, e-Records warehousing, web interfaces, semantic and ontology support, “Object oriented” and n-tiers architectures including web services, SOA, ESB, etc., software total quality management, information systems security audit & design <p>██████████</p> <p>██</p> <p>██</p> <p>██</p> <p>██</p>				

	<div></div> <div></div>			
Key Project personnel	<div></div>			
	<div></div>	<div></div>	<div></div>	
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	<div></div>			
	Publications Products, Services	<i>List of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i>		
		<u>Commercial projects in the security domain</u> include:		
		<ul style="list-style-type: none"> <div></div> <div></div> <div></div> 		
<ul style="list-style-type: none"> <div></div> <div></div> <div></div> <div></div> <div></div> 				
<ul style="list-style-type: none"> <div></div> <div></div> 				

General description of the org.	<p>The Institute of Communication and Computer Systems (ICCS) (www.iccs.gr/eng/), established in 1989, is a non-profit Academic Research Body associated with the School of Electrical & Computer Engineering (SECE) of the National Technical University of Athens (NTUA) under the auspice of the Hellenic Ministry of Education. ICCS carries research and development activities in the fields of all diverse aspects of telecommunications, computer systems and techniques and their application in a variety of areas. ICCS personnel consists of a number of Senior Researchers and associated scientists, substantially supported by SECE University Professors. ICCS involves many Research Groups and Laboratories very active in National and European funded research projects.</p> <p>In iCROSS proposal, ICCS participates through the RF/Microwaves Wireless & Satcom Group, an active Research Group of the Microwave and Fiber Optics Laboratory (MFOL) of ICCS/NTUA. MFOL (http://mfol.ece.ntua.gr/), established in 1985 as one of the NTUA Laboratories and a research unit of ICCS, holds a long-standing track record on basic and applied research, design & development, testing and measurements of RF/microwave units and systems covering almost the entire electromagnetic spectrum. The RF/Microwaves Wireless & Satcom Group of MFOL owns extensive experience in the related fields and is involved in many National and EU projects. The Group's staff consists of 1 ICCS Senior Researcher, 3 Professors, 2 postdoc senior researchers and PhD students.</p> <p>The most important areas of R&D activities performed or supported by the Group involve design and development of: RF & microwave systems, remote sensing, radar, life detectors and sensors, satellite communication and wireless radio networks, antennas front-end and wireless systems and subsystems up to millimeter waves, signal processing, as well as applications relevant to telecom, satcom and broadband wireless networks with the development of many dedicated prototypes. The Group has significant expertise and know-how in wireless and satellite communication systems design, digital communications, radio network dimensioning and planning, radio coverage measurements, radio channel modelling, RF systems design, interference studies and measurements, spectrum management and radio protocols design. Finally, the Group owns a broad experience in Lab and on Site / Field measurements along with conductance of EMC/EMI tests (conducted/radiated emission / immunity tests, STANAG standards etc).</p> <p>The Group's staff are active members of the research community having published more than 500 publications in International Journals and Conferences in the above subjects. Members of the Group have been involved in more than 60 R&D projects funded either from EC or the Greek Public/Private Sector such as: E-SPONDER (FP7 SECURITY), Jason, WiSepon, Emosic and Maribrain (Cooperation I & II), NexGenMiliwave, EU-FP7 HIRF, FP7 interactIVe, FP6-RURAL WINGS, SATNEX I (FP6 IST), SATNEX II (FP6 IST), SATNEX III (ESA), MIMO-NPI, (ESA-NPI), Flame, MIMOSA and COST Actions.</p> <p>[REDACTED]</p>														
	<p>[REDACTED]</p>														
Key Project personnel	<table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr></table>			[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]													
[REDACTED]	[REDACTED]	[REDACTED]													
[REDACTED]	[REDACTED]	[REDACTED]													
[REDACTED]	[REDACTED]	[REDACTED]													

[illegible]


[illegible]

General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>The Manchester Metropolitan University (MMU) is one the largest Universities in the UK, hosting 34,000 students and employing 4,300 staff. It is amongst the best performing ‘new universities’ for research. MMU has experience of participating in, and managing a range of European funded research projects including a number supported by previous Framework Programmes. The School in which the team are based (Computing, Mathematics and Digital Technology) currently co-ordinates the Framework 7 projects BACTOCOM, COBRA and TRUCE.</p> <p>MMU’s contribution will be led by the <i>Intelligent Systems Group (ISG)</i>. ISG has expertise in using computational intelligence techniques (specifically artificial neural networks) to monitor and analyze visual non-verbal behaviour in human subjects. MMU holds a patent on technology in this area relating to the system Silent Talker (Publication number WO2002087443 A1, Application number PCT/GB2002/001806), which learns patterns of microgestures which can be used to detect deception. The group also has extensive experience in the development of Conversational Agents and Conversational Intelligent Tutoring Systems. It has conducted pioneering work in the development of short text semantic similarity measures (STSS) that has led to the development of semantic conversational agents and in addition the Multi-lingual STSS in Arabic, Urdu and Thai. Recent work in this area also includes the design of highly computationally efficient algorithms for classifying Dialogue Acts based solely on small vocabulary (function word) features. Members of the group also have extensive knowledge of computational intelligence techniques including computing with words, fuzzy logic and evolutionary algorithms and natural language Interfaces for database information retrieval systems.</p> <p>The project team will also have access to specialised facilities and equipment including a usability lab within MMU which incorporates a range of tools and techniques (eye tracking, sensing equipment, video recording and Noldus Observer XT10 behaviour analysis software) to analyse human behaviour.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>								
Key Project personnel	<p><i>A CV or description of the profile of the persons, including their gender, who will be primarily responsible for carrying out the proposed research and/or innovation activities</i></p> <table border="1" data-bbox="304 1541 1366 1621"> <tr> <td data-bbox="304 1541 488 1581">[REDACTED]</td> <td data-bbox="488 1541 624 1581">[REDACTED]</td> <td data-bbox="624 1541 1235 1581">[REDACTED]</td> <td data-bbox="1235 1541 1366 1581">[REDACTED]</td> </tr> <tr> <td data-bbox="304 1581 488 1621">[REDACTED]</td> <td data-bbox="488 1581 624 1621">[REDACTED]</td> <td data-bbox="624 1581 1235 1621">[REDACTED]</td> <td data-bbox="1235 1581 1366 1621">[REDACTED]</td> </tr> </table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]						
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]						

	<p>Investment Programme on CBRN) as well as Action Grant CIPS II and NATO Industrial Advisory Group studies. The company has also been active in some Polish applied research projects. Recently, ITTI has been also involved in the European Space Agency projects. In R&D activities the company cooperates closely with numerous universities and research institutes based in Poland as well as around Europe. Moreover, ITTI is an institutional member of the Public Safety Communication Europe Forum, Integrated Mission Group for Security (IMG-S) and ITIC Group - International Telecommunications and IT Consultants. ITTI is also one of the co-founders of Polish Space Industry Association and participates to Wielkopolska ICT Cluster. In the recent years ITTI was awarded the prestigious “Cristal Brussels Prize 2013” for the most active and successful Polish company participating in FP7, while in 2009 ITTI received the reward for high performance in R&D projects for the European Defence Agency awarded by the Polish Ministry of Defence.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>									
Key Project personnel	<p>[REDACTED]</p> <table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr></table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td></td><td>[REDACTED]</td><td></td></tr></table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]								
[REDACTED]	[REDACTED]	[REDACTED]								
	[REDACTED]									


	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <table border="1" style="width: 100%;"> <tr> <td style="width: 33%; background-color: black; height: 15px;"></td><td style="width: 33%; background-color: black; height: 15px;"></td><td style="width: 33%; background-color: black; height: 15px;"></td></tr> <tr> <td style="background-color: black; height: 15px;"></td><td style="background-color: black; height: 15px;"></td><td style="background-color: black; height: 15px;"></td></tr> </table> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div>						
Publications Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i> N/A						
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i> <ul style="list-style-type: none"> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> ▪ <div style="background-color: black; height: 15px; width: 100%;"></div> 						
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i> ITTII possesses the standard IT environment (i.e. workstations, servers, software tools). ITTI owns standard office equipment (laptops, computers, phones) and conference facilities (inter alia GoToMeeting licence). ITTI has also servers that can be used for testbeds. In ITTI there is also a team of software developers and programmers. ITTI has also long experience in development of software solutions in R&D projects at national and international level.						
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A						

6. Everis Aerospace and Defence

NAME:	 Everis Aerospace and Defence				
Short Name:	EVR	Country:	Spain	Partner #:	6
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> EVERIS AEROESPACIAL Y DEFENSA is a multinational group born in Spain with a commercial network around the world that provides global solutions for				


	<p>critical systems in the fields of Aeronautics, Space, Defense, Security and Emergency, based on engineering developments and innovative technologies developed both in-house and by third parties. EVERIS AD does provide the most leading technology developed by ten Spanish companies which make up the group, taking advantage of the flexibility and speed in R&D and innovation processes.</p> <p>Those capabilities materialise in a comprehensive portfolio of Services Lines: Engineering; Embedded and real-time systems; Unmanned Aerial Vehicles (UAVs); Certification & Airworthiness; Terrestrial systems; CBRN defense; Emergency management; Protection of critical infrastructure; Border surveillance and protection; Surveillance and security; Intelligence systems; and Information and Communication systems.</p> <p>EVERIS AD has a broad experience working in cooperative EU funded projects (such as OPTIMI, SafeCity, INSEC, CIPHER, ARGOS, etc.) undertaking a wide range of activities that include project coordination and management, definition of functional requirements, business and exploitation plans, etc.</p> <p>Additionally, EVERIS AD is fully backed by Everis Group, a multinational group born in Spain with offices in Europe, United States and Latin America that offers business solutions, strategy, development and maintenance of technology applications and outsourcing. The company, which operates in telecom, financial entities, industry, utilities, energy, banking, insurance, public administration, media and healthcare sectors, reached €591 million turnover at the end of last fiscal year, and build a workforce of over 10,000 professionals all over the world. The key to this performance stems from the commitment of its professionals, resulting from a human resource model that sets it apart from other companies and generates client trust. This, in turn, is bolstered by two main pillars: innovation and entrepreneurial capability.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>													
Key Project personnel	<p>[REDACTED]</p> <table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr></table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td></td><td></td><td></td><td>[REDACTED]</td></tr></table>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]				[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]												
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]										
[REDACTED]				[REDACTED]										

7. BioSec Group Ltd.

NAME:	 BioSec Group Ltd.								
Short Name:	BIO	Country: Hungary	Partner #: 7						
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>BioSec Group Ltd. has been established by four private people with the only goal to develop biometric identification solution based on palm vein recognition. Positioned as R&D company, BioSec has created own software and hardware development infrastructure. Using indirect sales strategy, BioSec is represented in 13 countries all over the world and is specialized within biometric recognition in mass identification and IT security. Based on R&D experience since 2008, BioSec became one of the leading development companies for developing palm vein recognition based solutions. Number of employees is in total 19.</p> <p>Specialist areas of expertise of BioSec can be summarised as follows:</p> <ul style="list-style-type: none"> ▪ software development in C#, specialized in biometric recognition ▪ data encryption ▪ creating physical security systems ▪ hardware development for mobile devices ▪ mass handling ▪ planning and implementing large scale security systems ▪ system integration <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p>								
Key Project personnel	<p>[Redacted]</p> <table border="1" data-bbox="304 1384 1356 1429"> <tr> <td data-bbox="304 1384 721 1429">[Redacted]</td> <td data-bbox="721 1384 1235 1429">[Redacted]</td> <td data-bbox="1235 1384 1356 1429">[Redacted]</td> </tr> </table> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <table border="1" data-bbox="304 1704 1356 1787"> <tr> <td data-bbox="304 1704 721 1787">[Redacted]</td> <td data-bbox="721 1704 1235 1787">[Redacted]</td> <td data-bbox="1235 1704 1356 1787">[Redacted]</td> </tr> </table> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p>			[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]							
[Redacted]	[Redacted]	[Redacted]							


	<div> <div></div> <div></div> <div></div> </div>
	<div> <div></div> <div></div> <div></div> <div></div> </div>
Publications Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i>
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i> <ul style="list-style-type: none"> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div>
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i> As R&D company, BioSec has its own highly developed and equipped laboratory for testing software and hardware elements. Technical equipment includes: <ul style="list-style-type: none"> software laboratory <ul style="list-style-type: none"> simultaneous software testing stress testing vulnerability tests hardware laboratory <ul style="list-style-type: none"> simulation of outdoor conditions stress testing
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A

8. JAS technologie sp z o.o. (Ltd)

NAME:	 JAS technologie sp z o.o. (Ltd)				
Short Name:	JAS	Country:	Poland	Partner #:	8
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> JAS technologie Sp. z o.o. (Ltd) is dynamically growing technology company, operating in telecommunication and security. The company is owned in 100% by Polish capital. The company works closely with equipment manufacturers, Polish Government, Polish Air Navigation Services Agency, Research & Development organizations and Defense				

	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: black; height: 15px; width: 30%;"></div> <div style="background-color: black; height: 15px; width: 40%;"></div> <div style="background-color: black; height: 15px; width: 10%;"></div> </div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div>
Publications Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i>
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 60%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 85%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 30%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 45%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 55%;"></div>
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i> <p>As part of its work in R & D projects the company has made purchases of biometric hardware and dedicated software for the tasks. JAS also has adequate facilities to support the IT hardware programming work. In the implementation of tasks in R & D projects as well as commercial projects, JAS cooperates with many equipment suppliers in Poland and abroad.</p>
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A


9. Gottfried Wilhelm Leibniz Universitaet Hannover

NAME:	 <div style="background-color: #005596; color: white; padding: 5px;"> Leibniz Universität Hannover </div>				
Short Name:	LUH	Country:	Germany	Partner #:	9
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> <p>The Institute for Legal Informatics (IRI), being part of LUH's School of Law, was established in 1983 and is the first Institute dedicated to scientific research on all issues of Information and Communication Technologies at a German University.</p>				


	<p>With currently more than 40 people staff IRI is one of Europe's largest institutions in the field and is actively involved in about 10 European research projects with a focus on data protection, data security and intellectual property. Nikolaus Forgó has been leading IRI in cooperation with Prof. Dr. Heinze since 2014. The L3S Research Centre, also part of LUH, focuses on fundamental and application-oriented research in all areas of Web Science and has a focus on computer science. L3S researchers develop new methods and technologies that enable intelligent, seamless access to information via the Web; link individuals and communities in all areas of the knowledge society, including academia and education; and connect the Internet to the real world. Since 2008, the L3S has been involved in 12 EU projects as part of the EU's Seventh Framework Programme, four of them (LivingKnowledge, Okkam, EUWB and EERQI) integrated projects, as well as the STELLAR Network of Excellence.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>															
Key Project personnel	<p>[REDACTED]</p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]														
[REDACTED]	[REDACTED]	[REDACTED]														
[REDACTED]	[REDACTED]	[REDACTED]														
[REDACTED]	[REDACTED]	[REDACTED]														
[REDACTED]	[REDACTED]	[REDACTED]														
Publications Products, Services	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p>															

	<p>1. Betrieblicher Datenschutz Rechtshandbuch [Handbook operational Data Protection] (Nikolaus Forgo, Marcus Helfrich, and Jochen Schneider (editors)), Munchen: Beck 2014, 1035 pages</p> <p>2. Dealing with Data Safety and Security in Translational and Personalized Medicine (together with Norbert Graf, Yvonne Braun, Elias Neri, Brecht Claerhout et al), in: Pediatric Blood & Cancer 2013, vol. 60, no. 3; doi: 10.1002/pbc.24719</p> <p>3. Security Issues in research projects with patient's medical data (together with M. Goralczyk, and Constantin Graf von Rex), in: Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, 11-13 November 2012, pp. 541-546</p> <p>4. Legal issues in clouds: towards a risk inventory (together with K. Djemame, B. Barnitzke, M. Corrales, M. Kiran, M. Jiang, D. Armstrong and I. Nwankwo), in: Philosophical Transactions of the Royal Society A, A 2013 371, 20120075</p> <p>5. Assuring Data Privacy in Cloud Transformations (together with Corrales, Nwankwo and others), in: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on Digital Object Identifier, pp. 1063 – 1069</p>
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i>
Equipment	<p><i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>N/A</p>
Any other documents	<p><i>Any other supporting documents, if specified in the work programme for this call</i></p> <p>N/A</p>

10. Országos Rendőr-főkapitányság (Hungarian National Police)

NAME:	 <p>Országos Rendőr-főkapitányság</p>			
Short Name:	HNP	Country:	Hungary	Partner #: 10
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>The Hungarian National Police is the only police agency in Hungary, with more than 42,000 sworn members. It undertakes all policing duties within Hungary, including criminal investigation, patrol activities, traffic policing and border control. It is led by the National Police Commissioner under the control of the Minister of the Interior. The body is divided into county police departments, with a further subdivision into regional and town police departments. County police departments and some special units are affiliated legal entities. It is also the agency which operates the 112 national emergency response system, called the ESR. (The Hungarian Border Guard was integrated into the HNP in 2008.)</p> <p>Border control duties are coordinated by the General Department of Border Control and carried out by 67 Border Police Outposts and 85 BCPs along the external border as well as inland alien policing units, consisting of 3500 uniformed professionals in total.</p>			

Any other documents	Any other supporting documents, if specified in the work programme for this call N/A

NAME:	 Karpacki Border Guard Support Center of Polish Border Guard - Headquarters of Polish Border Guard				
Short Name:	PBG	Country:	Poland	Partner #:	11
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>Border Guard, in accordance with Art. 1 of the Act of 12 October 1990 on the Border Guard, is a unitary, uniformed and armed formation.</p> <p>Polish Border Guard within its duty carries out tasks aimed at:</p> <ul style="list-style-type: none"> • Organising the border checks to ensure fluidity movement of people and means of transport across the state border taking place in accordance with the law, while maintaining high efficiency detection of crimes and offenses in this area, • protection of the state border on land and sea, • organizing and carrying out border traffic control, • Recognition, prevention and detection of offenses and prosecution of their perpetrators, within the jurisdiction of the Border Guard, in particular: <ol style="list-style-type: none"> 1. offenses related to crossing the state border in compliance with the provisions related to the reliability of documents entitling to cross the state border, 2. crimes against public safety and security, offenses in communication in connection with the performance of air transport 3. cooperation with other authorities and services in the field of recognizing the risk of terrorism and countering any of these threats, 4. the gathering and processing of information for the protection of the state border-entry, and exchanging of those information with the competent authorities of the state, 				

5. Border Guard carries out tasks under the law of the European-Union and international agreements on principles and scope set out in them,
6. cooperation with other Member States and the Community joint ventures within the working groups
7. Striving to undertake many actions financing from EU funds and bridging funds.

According to Order No. 1 of the Border Guard Commander in Chief of 14 January 2014 on the establishment of the Karpacki Border Guard Support Center (KBGSC) in Nowy Sacz, our unit performs tasks throughout the country on behalf of other units of the Polish Border Guard. KBGSC is an entity having the potential of human resources and organizational - logistics to carry out the Project BES-6-2015 under the Horizon 2020 Programme. Supporting character of the KBGSC in Nowy Sacz allows to carry out a nationwide recruiting of the officers from different units of the Border Guard performing tasks on different state borders sectors (land, air and sea), and subsequently, will coordinate all implemented tasks of the Project.

Due to the fact that Poland is an external border of the European Union and the length of the land border is 1163.25 km (state border between Poland and Russian Federation, Republic of Belarus, Ukraine) with the one main airport and ten regional, the necessity to improve tools and methods for border control with the implementation of biometric technologies, i.e. in the context of automated border control systems is the main objective of the development strategy for Polish Border Guard.

PBG closely associated with the implementation of research projects under the National Center for Research and Development.

PBG set up within its structure a scientific-technical council that compile thematic issues that are referred to consider innovation.

Works within the National Center for Research and Development enable active participation of PBG in the development process as an adviser/expert.


[illegible]

Key Project personnel

[illegible]

Publications Products, Services

12. TRAINOSE METAFORES – METAFORIKES YPIRESIES EPIVATON KAI FORTIOU AE

NAME:	 TRAINOSE METAFORES – METAFORIKES YPIRESIES EPIVATON KAI FORTIOU AE				
Short Name:	TRA	Country:	Greece	Partner #:	12
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>TRAINOSE S.A. was established on 2005 initially as a subsidiary of OSE S.A. group. Since 2007 TRAINOSE S.A. has undertaken the operation and exploitation of all the transportation activities (passenger, freight, etc) and it has been operating as an independent company, being separately managed and organized, according to the provisions of the EU legislation.</p> <p>The company is a member of the International Union of Railways (UIC), the Community of European Railway and Infrastructure Companies (CER), the International Rail Transport Committee (CIT) and the Forum Train Europe; whereas it vigorously continues its effort for international networking, in order to draw valuable and specialized technical know-how.</p> <p>The main scope of the company includes nowadays:</p> <ul style="list-style-type: none"> • The development, organization and exploitation of the urban, suburban, regional, intercity and international passenger and freight railway transportation, as well as all kinds of transportation using fixed track systems. • The development, organization and exploitation of multimodal transportation. • The development, organization and exploitation of urban, suburban, regional, intercity and international passenger and freight bus transportation, nationally and abroad. • The provision of all kinds of logistics services, as well as all related services. • The organization, exploitation and provision of bedding and catering services to passengers. • The provision of consulting services relating to activities in accordance with the scope of the company. <p>Its mission being sustainable development, TRAINOSE S.A. aims to provide its customers with:</p> <ul style="list-style-type: none"> • Reliable transportation • Clean and comfortable trains • On time and reliable information • Experienced and friendly staff <p>R&D activities are coordinated by the Strategic Planning Division of TRAINOSE, and since 2012 the company has been involved as a partner in several EU projects, mainly in the pilot tasks, which subsequently offers as a service to its clients. TRAINOSE emphasizes in the fields of research and technological development for the design, development and implementation of high added value services towards its clients.</p> <p>The active participation of TRAINOSE in EU projects enhances the skills of company staff through the exchange of expertise with other European rail operators, widens the network of associates and increases the company's competitiveness, while supporting the national strategies in the field of rail and combined, multimodal transportation.</p> <p>By now, TRAINOSE has finalized its participation to seven (7) European funded research projects being affiliated to previous EU initiatives, while has just started</p>				

its processes in one more project of Horizon 2020 EU Framework Programme, all of them summarized in the table below:

Project Name	European Initiative	Duration	Budget TRAINOSE SA. (EUR)
██████████ ████	██████████	██████████	██████████
██████████	██████████ ██████████ ██████████	██████████	██████████
██████████	████████████████████	██████████	██████████
██████	████████████████████	██████████	██████████
██████████	████████████████████	██████████	██████████
██████████	████████████████████	██████████	██████████
██████████ ████	████████████████████	██████████	██████████
██████████	████████████████████	██████████	██████████


[illegible]

Key Project personnel

[illegible]

Related projects	[REDACTED]			
	[REDACTED]			
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i>			
	N/A			
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i>			
	N/A			

13. State Border Guard of the Republic of Latvia

NAME:	 State Border Guard of the Republic of Latvia			
Short Name:	BSG	Country:	Latvia	Partner #: 13
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> State Border Guard of the Republic of Latvia (BSG) is a direct administration State institution, under the supervision of the Ministry of the Interior. On issues of			

	<p>guarding and control of the State border, as well as on issues, which are associated with the control of the observance of the entry, residence, exit and transit of aliens and stateless persons regulations, and other issues within the competence.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>						
Key Project personnel	<p><i>A CV or description of the profile of the persons, including their gender, who will be primarily responsible for carrying out the proposed research and/or innovation activities</i></p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]					
[REDACTED]	[REDACTED]	[REDACTED]					
Publications Products, Services	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p>						
Related projects	<p><i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i></p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>						

[illegible]

	[REDACTED]
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A

4.2. Third parties involved in the project (including use of third party resources)

Please complete, for each participant, the following table (or simply state “No third parties involved”, if applicable):

The following table concerns all participants of the iCROSS consortium.

Does the participant plan to subcontract certain tasks (please note that core tasks of the action should not be sub-contracted)	Y
[REDACTED]	
Does the participant envisage that part of its work is performed by linked third parties ⁷⁵	N
[REDACTED]	
Does the participant envisage the use of contributions in kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)	N
[REDACTED]	

⁷⁵ A third party that is an affiliated entity or has a legal link to a participant implying a collaboration not limited to the action (Article 14 of the Model Grant Agreement).

Section 5: Ethics and Societal Impact

During the proposal preparation stage the relevant partners conducted a preliminary ethical requirements collection and platform review to identify any ethical or legal issues relevant to the planned development or deployment of iCROSS. This has resulted in a design for iCROSS that meets and surpasses legal and ethical requirements.

Specifically, the iCROSS consortium includes a partner institution expert in legal informatics, data protection, data security and ethics (LUH) who will lead the EU-wide legal review and legal and ethical compliance task. Any issues identified as part of this task will be addressed, either by incorporating them as requirements that need to be adhered to by the design and implementation of the iCROSS platform or by actions taken as part of this task such as the creation of legal documentation to be developed as part of this task and applied to any of the other tasks in the project. An example of this would be the need to provide informed consent to all Pilot or empirical data collection participants, to communicate with regulatory bodies such as data protection authorities and to report issues directly to the project coordinator and the general assembly.

Ethical privacy concerns are addressed through a privacy-by-design and privacy-by-default approach followed in the iCROSS data collection procedures to ensure that no legal or ethical issues arise in the course of the project execution. Risk management procedures are in place to address any now unforeseen issues. Informed consent materials will be developed as part of the project and will include both informative/educational material relevant stakeholders will go through to understand and be informed of their rights before they provided the consent.

The consortium agrees that proposals for Horizon 2020 need to demonstrate how innovative research can tackle the major societal challenges identified in the Europe 2020 strategy. Social Sciences and Humanities research can play an important and positive role in this process and indeed is uniquely placed to ensure that ethics is central in dealing with the normative dimensions of the themes and topics mentioned in Horizon 2020. Secure Societies targets the area of freedom, security and justice, without internal frontiers, as the European Agenda on Security (released on 28th of April, 2015) underlines

Europeans need to feel confident that, wherever they move within Europe, their freedom and their security are well protected, in full compliance with the Union's values, including the rule of law and fundamental rights. In recent years new and complex threats have emerged highlighting the need for further synergies and closer cooperation at all levels.

It has been noted that:

Horizon 2020 has ambitious aims that not only presuppose empirical claims, e.g., with respect to natural resources, available technologies or existing infrastructures, but also set specific goals, e.g., regarding sustainability, health and well-being, food production, the bio-based economy, and resource efficiency. These goals show that the research themes are not aims in themselves, but means to realising European commitments to human rights and values. These rights and values presuppose normative claims about how humans should treat one another, what makes for good society, and how responsible governments and businesses should behave.

The consortium is also dedicated to ensure full compliance with fundamental rights as required by the Lisbon Treaty – European Charter of Fundamental Rights – which came into force 1st December 2009), provide transparency, accountability as well as providing results compatible with the Prüm framework and the new Europol mandate. To achieve balance within “Liberty and Security” as a single fundamental right, we have decided to set up a sound ethical framework, which is not only essential in fostering responsible research and innovation but also key of providing results able to gain public legitimacy, becoming a widely accepted tool for border traffic control. This section elaborates on how this is operationalised in the iCROSS project.

1. Code of Ethics and Ethics Advisor

In order to ensure that all partners act along the same inline, a Code of Ethics is elaborated, containing rules on general ethics principles, data protection and transparency. It provide rules on the informed consent, procedures implemented for data collection, storage, protection, retention and destruction including confirmation that they comply with national and EU legislation. Legal entities as members of the consortium have to give written informed consent on the Code of Ethics as well as individual researchers participating in the project. The Code of Ethics also contains the Data Protection Rules which has to be applied through the entire implementation (see chapter on Data Protection). An independent Ethics Advisor, who is not employed at any of the consortium members, will be contracted to carry out training, counselling, monitoring and auditing activities in order to ensure that all phases of implementation are in line with the Code of Ethics. The Security Officer will support the work of the Ethics Advisor with taking the role of an internal Data Protection Officer with tasks and responsibilities detailed in the Data Protection Rules. Arbitration over ethics and data protection regulation will be carried out by an Ethics Committee chaired by a Chairman from one of the consortium partners with two members, the Ethics Advisor and the Data Protection Officer (Security Officer). The Committee resolves all cases in written decision and submits a report on ethics and data protection during the reporting period. In case of lack of consent, the Ethical Advisor has the right to write a parallel report.

2. Data Protection

As mentioned in the previous chapter, in general, data protection will be ensured within the frame of the Code of Ethics, in form of Data Protection Rules annexed to the Code. All partners and individuals participating in the research have to give informed consent on data protection rules as well as volunteers participating in the tests.

The procedure of giving informed consent consists of three steps and is coordinated by the Data Protection Officer, who:

- a. informs the persons about the project and the type of data required,
- b. distributes electronic copies of Data Protection Rules and answers all related questions, explains content of the rules as requested,
- c. collects and stores signed forms of informed consent in a searchable format.

It has to be highlighted, that the Hungarian National Police is empowered by law to collect, store and process personal data for the following purposes (Act XXXIV. of 1994 on The Police, 77.):

- a. border control and policing,
- b. crime prevention, fight against crime and terrorism.

For this reason, personal data of third country citizens crossing the border to or from Hungary are collected, stored and processed by the Hungarian National Police for 5 years from the day of border crossing (Act XXXIV. of 1994 on The Police, 91/L. §), affecting the following types of data:

- a. full name
- b. date of birth
- c. nationality
- d. gender
- e. passport number and type
- f. visa number and type

This is also affecting travellers who do not participate in iCROSS tests. If a volunteer revokes its volunteering for participation and informed consent on data processing in the frame of iCROSS, it has to be informed that in case of border crossing to or from Hungary, the personal data listed above will be still processed on the abovementioned legal basis.

All other types of personal data can only be processed on the basis of consent and all other participants can only process those within the frame of the Data Protection Rules. A register will be set up for each

participant by the Data Protection Officer recording data types processed and individuals having access to those data.

For example, capturing of video-audio conversation with an avatar has to be executed only after the user of the device capable of capturing this conversation (eg. laptop with webcam and microphone) has given permission to the relevant software to carry out the capturing sequence. Most operating systems have their built-in procedures to achieve user permission; our solution will use those built-in dynamic linkable libraries and other such tools to ask for the permission of the user. The same applies for other data collection in relevance of the use of the traveller's personal computing devices (eg. GPS data, actual mobile network, handshake with tokens etc.).

After the duration of data process period expires (5 years in total) or the informed consent has been revoked (the sooner applies), all personal and sensitive data has to be deleted from the databases of the consortium with proper software and/or hardware procedures rendering unauthorized restoration impossible (eg. DiskWipe, HDDerase, KillDisk, Format Command Write Zero Option etc.). In case any partner has a parallel, legal bases obligation to further process any kind of data, those partner will further process the data on the given legal basis, while all other partners shall carry out the deletion process. Before deletion, the Ethical Committee has to be notified in due time to be able to observe the procedure and the Security Advisory Board has to be informed on the relevant data to ensure it will be also removed from deliveries (reports). The detailed regulations on storage, process and deletion can be found in the Data Protection Rules (Art. 10.) part of the Ethics Code.

3. Incidental findings

In case the system or the border control personnel detects anything illegal when checking a person participating in the iCROSS as volunteer and crossing the border, two different types of actions may apply depending on the conditions:

- a. the persons shows a Letter of Commission (serialized and registered document with title “Nyílt Parancs” or “Megbízólevél”) issued by the Hungarian National Police, the Hungarian National Protection Service or by the Hungarian Ministry of Interior that he or she has performed the action resembling on an illegal act of the sole purpose of testing the system, and the act committed is exactly as outlined in the commission document, in that case, no actions other than the normal border control has to be carried out with the illegal act ignored,
- b. otherwise, the person has to be handed over to the border police units present who will carry out standard operational procedures determined by regulations on the given case, and all relevant data has to be secured and handed over to the police as evidence, including those who were collected with the perpetrators consent (Act XIX. of 1998 on Penal Procedures 117.§ (2)).

In both cases, the Security Officer has to be informed, and he or she must register the transfer of personal data in the Data Transfer Registry.

Any other incidental findings, not happening at the border and/or in presence of police officers, for example video collected on known terrorist suspects, devices connecting from areas under insurgent control, videos collected on persons known (wanted) as kidnapped or lost, have to be handed over to the Hungarian National Police through the Security Officer.

4. Additional measures on profiling to avoid stigmatization

The main difference between profiling and stigmatization is that a stigma implies the presumption of bad intention or disgrace, while profiling is the act or process of learning information about someone based on what is already known, determining the way how we will check the person. Profiling does not only filters criminals, terrorist or illegal migrants, on the contrary, it has more effect on victims of human trafficking and regular travellers in scope of third country citizens. A recent handbook on human trafficking for example provides clear datasets on from which country which type and age of women are trafficked, how many of them are in one group, what are the main travel destinations. Regular travellers can pass through the border faster as the passport checking personnel already are knowing their profile, a few words on their

language and they already got their passport back, checked and stamped, without any further questioning about purpose of stay, means of stay etc. Sometimes the best profiling is to have clear profiles on regular travellers and filter out everything that is uncommon. However, profiling can also be exploited and misused, like any other tool. To provide additional measures on profiling to avoid stigmatization, we intend to add the following functions into the profiling system:

- a. lapse of scores – both positive and negative scores obtained according to the profiles will diminish with time, in accordance with the legal principle of limitation,
- b. diminishing returns – when travelling many times in very short time period, the basic positive score obtained by successful border crossing will decrease linearly, preventing exploitation of the good scores achievable with travelling regularly,
- c. random score element – a random one-time score with random prefix (positive or negative) will be added each time the profile is checked at the border, the possible values (random interval) will be set to contribute half the score needed for one step change in the control category (minimal, thorough, thorough in a separated place – according to the Regulation 562/2006/EC on the Schengen Border Code),
- d. no manual modification – nobody's score can be modified manually, values apply automatically when the conditional phenomena/case/decision is recorded.

5. False positives

This system does not make decisions on admission or refusal. Its sole purpose is to facilitate border crossing with giving information to both traveller and border guard. Therefore false positives do not have any legal effect, as the final decision is in the hand of the traveller (on travelling or not) and in the border guard (to determine level of control and decide about admission). This is mainly because the international, EU and national law has certain exceptions on persons which are so dynamic that is not programmable. For example once a diplomat from Angola flew to Budapest to participate on a ceremony before she proceeds to Russia to work on the embassy in Moscow, but the database showed she has an alert for refusal on her, because seven years before she was arrested for delivering illicit sexual services in a bar in Budapest. Although the alert was still valid for three more years, the Minister of Interior decided to lift the ban in respect of the change in the status of the person. In another case, a plane full of US soldiers from a non-NATO unit got engine problems and had to spend two days at Budapest Airport with repairs, but the soldiers did not have travel document with themselves. However, the border official in charge decided to let them enter the country and spend the night in a hotel instead aboard of the plane. Therefore iCROSS will tell the traveller, that what he or she can expect at the border, based on the information provided (eg. passport is expired, additional visa is required etc.), but will not tell him or her to travel or not to travel. The same applies for the border guard, iCROSS will only report information gathered, checks already made (eg. passport is valid, the person is identified), profile assessment results (in form of recommended level of control), but will not and is not allowed to tell the policeman what to do exactly, how to control the person and what shall be the decision.

ICROSS

*Code of Ethics
with annexed
Data Protection Regulations
and forms of informed consent*

closed on 02 March 2016

by



Annexes:

1. Data Protection Regulation
2. Declaration of individuals and of legal entities accepting Ethics Code and Data Protection Regulations (forms of informed consent)
3. Data process register and access table

PREAMBLE	104
SCOPE	104
EFFECT	104
RULES OF PARTICIPATION IN THE RESEARCH	104
DEFINITIONS AND PRINCIPLES	105
OBLIGATIONS FOR PARTICIPANTS	106
ETHICAL COMMITTEE	106
ANNEX 1 DECLARATION OF ACCEPTING THE ETHICS CODE	109
I. ANNEXES	112
ANNEX 1 DATA PROTECTION RULES FOR PROJECT ‘ICROSS’	112
<i>Preamble</i>	<i>112</i>
<i>Article 1 Definitions.....</i>	<i>113</i>
<i>Article 2 Principles.....</i>	<i>114</i>
<i>Article 3 Criteria For Making Data Processing Legitimate.....</i>	<i>114</i>
<i>Article 4 Processing Sensitive Personal Data</i>	<i>115</i>
<i>Article 5 Information To Be Given To The Data Subject.....</i>	<i>115</i>
<i>Article 6 The Data Subject's Right Of Access To Data.....</i>	<i>116</i>
<i>Article 7 The Data Subject's Right To Object.....</i>	<i>117</i>
<i>Article 8 Confidentiality And Security Of Processing</i>	<i>118</i>
<i>Article 9 Transfer Of Personal Data To Third Countries.....</i>	<i>118</i>
<i>Article 10 Internal Data Protection Officer</i>	<i>119</i>
<i>Article 11 Other Provisions</i>	<i>120</i>
ANNEX DECLARATION OF ACCEPTING THE ETHICS CODE INCLUDING THE DATA PROTECTION RULE	122

Preamble

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Scope

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

Effect

[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Rules of participation in the research

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

-
- | Row | Bar Length (approx. %) |
|-----|------------------------|
| 1 | 25 |
| 2 | 100 |
| 3 | 75 |
| 4 | 20 |
| 5 | 95 |
| 6 | 45 |
| 7 | 98 |
| 8 | 100 |
| 9 | 30 |
| 10 | 40 |

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Obligations for participants

- [REDACTED]
- [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]

Ethical Committee

[REDACTED]
[REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

Annex 1
Declaration of accepting the Ethics Code
(for individuals and for legal entities, on separate pages)

<Page intentionally left blank>

DECLARATION
on accepting the Ethics Code for individuals

I, <NAME>, born in <POB> on
the <DOB> hereby declare that I have read and accept the Ethics
Code including the data protection rules of the project 'ICROSS' and I understand my rights and
obligations related to the project.

.....
<SIGNATURE>

.....
<DATE>

In witness whereof:

..... <NAME>
.....<ADDRESS>
..... <SIGNATURE>

..... <NAME>
.....<ADDRESS>
..... <SIGNATURE>

DECLARATION

on accepting the Ethics Code for legal entities

Name of Legal Entity:.....

Seat of Legal Entity:.....

Registration number:.....

VAT number:

PIC number:

represented by<NAME and POSITION>

hereby declares that the above mentioned legal entity accepts the Ethics Code including the data protection rules of the project 'ICROSS' of the project 'ICROSS' and understands the rights and obligations related to the project.

.....

<DATE>

.....

<SIGNATURE and STAMP>

I. Annexes

Annex 1

Data Protection Rules for Project 'ICROSS'

Preamble

(1) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

Article 1
Definitions

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 2
Principles

[REDACTED]

- [REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

Article 3
Criteria For Making Data Processing Legitimate

[REDACTED]

- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Article 4
Processing Sensitive Personal Data

[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
■

- [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Article 5
Information To Be Given To The Data Subject

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Article 6
The Data Subject's Right Of Access To Data

[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]

Article 7
The Data Subject's Right To Rectify, Erase or Block Personal Data

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]

Article 8
Confidentiality And Security Of Processing

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

■ [REDACTED]

■ [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

Article 9
Transfer Of Personal Data To Third Countries

[REDACTED]
[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]
[REDACTED]

Article 11
Storage, retention and destruction of personal data

[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 11
Data Protection Officer

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Article 12
Other Provisions

[REDACTED]

- [REDACTED]
- [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Annex
Declaration of accepting the Ethics Code including the Data Protection Rule
(for individuals and for legal entities, on separate pages)
<page intentionally left blank>

DECLARATION

on accepting the Ethics Code including the Data Protection Rule for individuals

I, <NAME>, born in <POB> on
the <DOB> hereby declare that I have read and accept the Ethics
Code including the data protection rules of the project 'ICROSS' and I understand my rights and
obligations related to the project.

.....
<SIGNATURE>

I declare that the ICROSS Consortium processes my personal data with my consent.

.....
<SIGNATURE>

I declare that the ICROSS Consortium processes my personal sensitive data with my consent.

.....
<SIGNATURE>

(Only sign the appropriate declarations!)

.....
<DATE>

In witness whereof:

..... <NAME>
..... <ADDRESS>
..... <SIGNATURE>

..... <NAME>
..... <ADDRESS>
..... <SIGNATURE>

DECLARATION

on accepting the Ethics Code including the Data Protection Rule for legal entities

Name of Legal Entity:.....

Seat of Legal Entity:.....

Registration number:.....

VAT number:

PIC number:

represented by<NAME and POSITION>

hereby declares that the above mentioned legal entity accepts the Ethics Code including the data protection rules of the project 'ICROSS' and understands the rights and obligations related to the project.

.....
.....

<DATE>

.....

<SIGNATURE and STAMP>

DATA PROCESS REGISTER

Name of entity:

Project Name: iCROSS

Numbered list of data types processed:

Start of process period:

End of process period:

Date:

Data Protection Officer

ACCESS TABLE

Mark level in corresponding column (see numbered list above).

Access levels: O=read, I=write, X=admin

Name of person	Access	Revoke	1	2	3	4	5	6	7	8	9	10	11	12	12

(add lists as required)

DATA TRANSFER REGISTER

Transferring Entity	Recipient	Purpose of Transfer	Legal ground of Transfer	Personal Data Transferred	Time of Transfer	Other

Section 6: Security⁷⁶

Activities or results, involved in the project, raising security issues: NO

“EU-classified information” involved in the project as background or results: NO

6.1 Security aspect letter

To be provided by commission service during the Grant Agreement preparation

6.2 Security classification guide

Since the iCROSS platform will collect, analyze, and evaluate only tools that are developed within the project itself without intervening in regular operations to border control. We expect that there will be no need to classify any of the expected deliverables in terms of their security aspects. This is a research and innovation action, and special care was put in the design of iCROSS to focus on automating tasks that border control agents do that are already publically available. To better design iCROSS members of the consortium who were or are directly involved both in relevant policy as well as in border control participate in the project and any tasks of the project that may require a security classification will either be performed by them, or other partners with sufficient security clearance and relevant outcomes of those tasks will not be disseminated to anyone without adequate security clearance. As an extra risk mitigation in the unlikely event that a partner doesn't have sufficient security clearance and is crucial to a task, then that partner will apply to the process to acquire that security clearance, to facilitate this enough time has been allocated from the beginning of the project until the implementation stages to apply and receive clearance.

6.3 Security staff

6.3.1 Project Security Officer

[REDACTED]

6.3.2 Security Advisory Board

A Security Advisory Board (SAB) will be set up with representatives from the consortium and end-users with sufficient knowledge of security issues to assess the sensitivity of the following deliverables prior to publication: D2.1, D2.2, D3.1, D3.2, D3.3, D4.1, D4.2, D6.3 and D6.4. Based on the evaluation of the SAB on deliveries, the dissemination of any content assessed as sensitive will be limited to the consortium on the SABs decision. SAB is empowered to change dissemination level of deliveries to the level justified by the results incorporated (eg. from PU to CO or vica versa). The Security Advisory Board will be led by [REDACTED] who has been assigned with the role of the **Project Security Officer**; whereas representatives from ED (as coordination team), ITTI, EVR, JAS (as tech providers with great

⁷⁶ Article 37.1 of Model Grant Agreement. Before disclosing results of activities raising security issues to a third party (including affiliated entities), a beneficiary must inform the coordinator — which must request written approval from the Commission/Agency; Article 37. Activities related to ‘classified deliverables’ must comply with the ‘security requirements’ until they are declassified; Action tasks related to classified deliverables may not be subcontracted without prior explicit written approval from the Commission/Agency.; The beneficiaries must inform the coordinator — which must immediately inform the Commission/Agency - of any changes in the security context and — if necessary —request for Annex 1 to be amended (see Article 55).

expertise in the field of critical systems for security and emergency), PBG, BSG, TRAINOSE (as end-users) will constitute the Board.

6.4 Other project-specific security measures

As part of work package 2 in iCROSS the security requirements will be established based on both the national, and EU level legislation and border control procedures. Any problems identified, such as the inability of staff without personal security clearance required to access secure premises for the needs of the deployment of the Pilots for example, will be addressed by the partners responsible for each Pilot. Each Pilot will be performed by the same institutions who are responsible for the security of the areas where the Pilots will take place and the pilots themselves will include the use of real border control agents taking part in the project. Since all of them have security clearance in each of the respective Pilot execution sites, we don't anticipate any problem. The Requirements task and the legal compliance task will enable the definition of the requirements that need to be addressed so that border control agents are capable of executing the Pilots, such as user friendly technical set up procedures, stand by telephone technical support by technical experts etc.

Annex

Letter of Support

