Flying 2.0

Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors.

This work takes place in the context of ENISA's Emerging and Future Risk programme.

Contact details

This report has been edited by Barbara Daskala.

e-mail: RiskManagement@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

LIST OF EXPERTS AND CONTRIBUTORS

This report was produced by the ENISA editor using input and comments from a group selected for their expertise in the subject area and in the areas of assessment (security, privacy, social, legal) including industry and academic experts. It should be noted that group members participate as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and does not in any way bind group members when dealing with the issues it covers in other contexts.

The contributors are listed below in alphabetical order:

- **Alessandro Bassi**, Hitachi Europe SAS, France
- **Jim Clarke**, Researcher, Waterford Institute of Technology, Ireland
- **France Charles de Couessin**, Executive Partner, ID Partners, France
- **Sotiris Ioannidis**, Associate Researcher, Institute of Computer Science, Foundation for Research and Technology (FORTH), Greece
- **Eleni Kosta**, Legal Researcher, K.U.Leuven - Interdisciplinary Centre for Law & ICT (ICRI), Belgium
- **Paul McCarthy**, Research Fellow, Lancaster University, UK
- **Huang Ming-Yuh**, Program Manager, Strategic Information Assurance, The Boeing Company, US
- **Eurico Neves**, CEO, INOVA+ Serviços de Consultadoria em Inovação Tecnológica SA, Portugal
- **Dennis Nilsson**, Consultant at Syncron Japan KK, Tokyo, Japan
- **Milan Petkovic**, Philips Research, The Netherlands
- **Pawel Rotter**, AGH University of Science and Technology in Krakow, Automatics Department, Poland
- **Markus Tiemann**, Human Factors and Cabin/Cargo Operations, AIRBUS Operations, Germany
- **David Wright**, Managing Partner, Trilateral Research & Consulting LLP, UK

In the delivery of technical risk assessment and identification of the implemented controls, we have been assisted by the following risk assessment experts from Ernst & Young, Greece:

- **Sotiris Papiotis, CISSP, CISA, CBCP, CIA,** Executive Director, Advisory Services
- **Panagiotis Koumousis,** Advisory Services, Ernst & Young,
- **Charalampos Melegos**, Advisory Services, Ernst & Young,

In addition, the following ENISA experts participated in the work (in alphabetical order):

- **Ingo Naumann,** ENISA
- **Panagiotis Saragiotis,** ENISA

1 EXECUTIVE SUMMARY

ENISA undertook the task to identify and assess emerging and future risks of a particular IoT/RFID scenario, also in the context of ENISA's role in this specified in EC Communication "*Internet of Things – An Action Plan for Europe*" [9]. The "Internet of Things" (IoT), sometimes referred to as ubiquitous networking or pervasive computing environments, is a vision where all manufactured things can be network enabled, that is connected to each other via wireless or wired communication networks. The Internet of Things is envisaged to bring many benefits, but it also poses many new challenges and risks.

Thanks to the advancement of ICT technologies, the number of different ordinary devices that increased their capabilities well beyond their original purpose is dramatically rising. These smart devices, which are the bricks needed to realize an IoT are poised to create significant impact on many areas of our lives, and will be illustrated in detail within this report in a case scenario of air travel. While IoT will inevitably play a major role in improving future air transportation, as it will in many other areas as well, there are critical issues to be identified and considered in depth. Smaller form factor and portability encourages mobility, which leads to frequent interaction between devices, sensors, and network infrastructures. The movement of travellers, airport/airline personnel, and luggage creates an increasing amount of continuous interaction between devices. As the result of these interactions, significant amounts of sensitive information will be generated and shared. The aspects of system security, safety, data sensitivity, usage and management all require further investigation and require addressing in any implementation of IoT environments.

For an Internet of Things / RFID vision to realise the benefits envisaged, the challenges and risks it poses should be identified and addressed in a proactive way. These risks do not always have to do with the technology per se but with the way we use it.

For the purposes of this work, an expert group was assembled to carry out a risk assessment on a complex scenario involving Internet of Things (IoT) / Radio Frequency IDentification (RFID) technologies in future air travel. Amongst the technologies, applications and devices considered in this scenario, in addition to RFID, are smart phones, netbooks and location-based services (LBS). The power of these technologies is greatly leveraged by their convergence and interoperability. The air travel scenario was selected to illustrate the convergence of these IoT technologies and the issues that arise as a result of this convergence and interoperability.

This report contains the result of this work. The risk assessment involved extensive detailed identification and measurement of the vulnerabilities and emerging threats for the entire scenario. Moreover, the report also includes appropriate recommendations to address the risks identified.

This report explains how potentially this technology can be used in an air travel scenario; in the scenario we look at the benefits of this technology and environment, particularly in future air travel, and we identify the major security risks. We also cover the privacy, social and legal implications. Finally, we make concrete recommendations on how to address the risks, so as to maximise the benefits.

The intended audience of this report is:

- European Commission and European policymakers, to assist them on setting research policy (to develop technologies that mitigate risks) and to assist them in deciding on appropriate policy and economic incentives, legislative measures, awareness-raising initiatives, etc. vis-à-vis IoT/RFID technologies and applications; and in particular, on air travel;
- Industry, to encourage them to secure their technologies and services, to make transparent to citizen-consumers their purposes and practices in collecting and processing personal data and to identify any third parties with whom they share such data;
- Air transport stakeholders, such as airports, Airport Council International (ACI) and IATA;
- Individuals or citizens, to enable them to evaluate the costs, risks and benefits of using the consumer version of these applications.

1.1 RECOMMENDATIONS

In order to mitigate the risks identified, appropriate recommendations were presented in the report. The recommendations were made for the various stakeholders, including technology and policy, research, legal and European Commission. The following contains a summary of the top recommendations identified within the report. Further details on the recommendations can be found in Chapter 6.

POLICY RECOMMENDATIONS

Rethink existing business structures and introduce new business models. It is recommended that air transportation businesses and agencies (e.g. airlines, airports, air cargos/logistics, and government aviation security agencies) proactively plan, design and stay alert on the introduction of new business models.

User-friendliness of devices and procedures / be inclusive. The usability of the smart technical applications / devices has to be considered thoroughly. Processes have to be clear and comprehensible, and user interfaces have to be designed in such a way that the corresponding systems will be easy to use by their target groups.

RESEARCH RECOMMENDATIONS

Data protection and privacy. It is recommended to carry out research to examine the issues in relation to IoT deployments and to further extend security and privacy solutions.

Usability. It is recommended to investigate the issues related to usability of security and privacy technologies, and consequently research and development in the related technical fields including human-device interfaces and assisted privacy policy (consent) specification and management.

Managing trust. In a future IoT environment, trust should be a central consideration; an enterprise should identify and understand its own trust framework in order to be able to deal with the IoT challenges. It is also recommended to focus particularly on the appropriateness and the compliance aspects of trust policies into the IoT applications.

Multi-modal person authentication. It is recommended to further investigate and develop biometric procedures for person authentication.

Proposing standards of light cryptography protocols. It is recommended to set up light cryptography standards and give some time to the scientific community to test them before wide implementation.

LEGAL RECOMMENDATIONS

Support for Users. It is recommended that sufficient support is provided to data subjects so that they get adequate information relating to the processing of their personal data and they can better exercise their rights.

Placing a high value on information and data. It is recommended that the entities that process personal data, including any governmental or commercial entity, such as electronic communications providers, road infrastructure providers, airline companies or any other entity in the air transport sector, shall value highly the security of the personal data of the data subjects and shall take all the necessary technical and organisational measures to ensure it.

Harmonisation of data collection by airport shops. It is recommended that there be further harmonisation of the current practice and efforts be made to raise awareness among travellers as to the collection and processing of data when purchasing items from shops.

RECOMMENDATIONS TOWARDS THE EUROPEAN COMMISSION

Enforcement and application of the European regulatory framework. It is recommended that the Commission prepare guidelines on the better enforcement and application of the European regulatory framework, especially in view of the challenges posed by technological developments.

Alignment of research with industrial and societal needs while promoting the participation of industry, and in particular SMEs in research activities as FP7. It is recommended that the Commission reinforce pilot activities in the line of the present CIP ICT-PSP programme with more ambitious targets and measures for participation of SMEs.

Ethical limits research. It is recommended that the Commission encourage more (and better) research at EU level on the ethical limits of private data capture and circulation, and on the societal implications of developments in this regard, e.g. under the Science and Society programme of FP7.

Need for impact assessment and trials of new technologies before deployment: *privacy and security by design*. To avoid rushed decisions and roll out of technologies that might create more security problems then they fix, it is recommended that any decision on the introduction of new technologies and new procedures should be taken only after a privacy and technology impact assessment and by a joint panel with representatives comprising all stakeholders (industry, civil society organisations, legislators, technology experts, health experts, data protection authorities etc.), which are truly tested and adopted jointly by all Member States. It is recommended that the European Commission appropriately endorse and steer such a process.

1.2 TOP RISKS

The most important risks discussed in this report are the following:

Failure of reservation, check-in and boarding procedures – Procedural / operational failures and other organisational interruptions; passengers and airlines may be unable to perform automated reservation, check-in, and boarding procedures due to procedural or operational errors, ill-designed procedures, introduction of erroneous data or even resource shortages from unexpected interruptions such as industrial action (e.g. strikes etc.). For more information, please refer to [**R1**].

Problems in issuing / controlling electronic visas – The risk of states' inability to issue and control the usage of electronic visas arises from system failures, procedural incompatibility, equipment failures, cyber attacks, identity theft or usage of erroneous data. As a result, citizens/passengers are unable to obtain an electronic visa for their travel. For more information, please refer to [**R2**].

Loss / violation of citizen/passenger privacy – The natural characteristic of IoT environment is the prevalence of devices, sensors, readers, and applications which have the potential to collect a multiplicity of data types of individuals as they move through such environments. Many citizen data will be generated and collected for example, as well as other forms such as location, purchasing habits, as well as other preferences stored for ease of use in systems. This leads to concerns over the potential compromising of citizen's privacy via collecting/surveillance/profiting of traveller's activity. For more information, please refer to [**R6**].

Compromise and abuse of state-owned citizen/passenger databases – States provide and collect citizen/passenger data throughout the air transport process; these data may also detail citizens' mobility patterns and as such open the possibilities for abuses through practices such as profiling, unwarranted monitoring or data in governmental databases being compromised due to accidental loss, fraud or other illicit or criminal activity. Of particular concern here would be corruption or unavailability of the state-owned citizen air transportation databases. Moreover, any inaccuracies of data may mean that citizens may be inaccurately identified as 'suspicious' (false positives), while perpetrators may not be appropriately detected (false negatives). For more information, please refer to [**R7**].

Repurposing of data / mission creep – The risk here is that data will be used for purposes in addition or other to those originally specified. Repurposing of data can be in the cards even before data collection begins, e.g., law enforcement authorities or intelligence agencies may seek access to data collected by others for specified purposes. This is not just in relation to the violation of individual rights to privacy but also may impact on wider social and public acceptance. For more information, please refer to [**R8**].

Health process-related concerns – It is expected that the "Internet of Things" will create significant impact to future delivery of healthcare. However, high dependability on the IoT technologies in e-Health creates significant security and privacy risks; particularly with respect to patient identification and reliability of collected information. For more information, please refer to [**R9**].

User frustration and low user acceptance – The sometimes complex procedures and sophisticated devices may overwhelm users, the travellers that are not IT friendly or even airport / airlines personnel can be potentially included in this category of persons. For more information, please refer to [**R11**].

Aggressive profiling and social sorting leading to social exclusion – In a highly interconnected environment as IoT is**, t**he collection of data and profiling are both facts and not necessarily negative per se. However, excessive data collection and profiling, will inevitably lead to social sorting practices for commercial or other purposes, leading to exclusion of people from accessing services. Like

repurposing of data and mission creep, social sorting in an increasing temptation with increasing data collection. For more information, please refer to [**R12**].

Legislation lagging behind rapid technological advancements – The rapid advance of technology is at variance with the slower pace of the legislative processes, which may lead to serious legal gaps in a future environment of Internet of Things, particularly in the context of air travel. These gaps pose a big challenge to Member States and the European Institutions to tackle, since inadequate legal protection may have severe negative impacts on the everyday lives of European citizens. For more information, please refer to [**R17**].

Non-compliance with data protection legislation – Currently there is a strong data protection legislative framework in place, which is likely to be adapted by 2015 to better deal with the challenges posed by the technological developments, such as the Internet of Things. Nevertheless, there are certain concerns and risks relating to the processing of personal data. Some of them arise from the challenge of assuring compliance with the legislation, since as we experience every day it is not something easily achieved. For more information, please refer to [**R18**].

CONTENTS

2 INTRODUCTION

2.1 BACKGROUND

The "Internet of Things" (IoT), sometimes referred to as ubiquitous networking or pervasive computing environments, is a vision where all manufactured things can be network enabled, that is connected to each other via wireless or wired communication networks. While there is no single definition for the Internet of Things, a commonly accepted one is the ITU-T definition from 2005, arguing that the development of item identifications, sensor technologies and the ability to interact with the environment will create an Internet of Things. The Internet of Things is envisaged to bring many benefits, but it also poses many new challenges and risks.

In view of this, ENISA undertook the task to identify and assess emerging and future risks of a particular IoT/RFID scenario, also in the context of ENISA's role in this specified in EC Communication "*Internet of Things – An Action Plan for Europe*" [9].

This report contains the result of an extensive risk assessment effort on a comprehensive scenario involving IoT and RFID usage in the context of air travel. The assessment involved extensive detailed identification and measurement of the vulnerabilities and emerging threats for the entire scenario. Moreover, the report also includes appropriate recommendations to address the risks identified.

2.2 OPPORTUNITIES OF IOT/RFID IN THE FUTURE – A CASE SCENARIO

The Conferences[1] "On RFID: The Next Step to the Internet of Things" held in Lisbon during the Portuguese Presidency on 15-16th November 2007, and subsequently the Conference on "*The Internet of Things Europe 2009: Emerging Technologies for the Future*" in May 2009 concluded with a consensus for Europe to analyse, assess and develop common strategies for optimising the shift of RFID technology into the "Internet of Things", whilst safeguarding sensitive information and protecting the privacy of individuals.

In parallel, thanks to the advancement of ICT technologies, the number of different ordinary devices that increased their capabilities well beyond their original purpose is dramatically rising. These smart devices, which are the bricks needed to realize an "Internet of Things" (IoT) are poised to create significant impact on many areas of our lives, and will in this be document be illustrated by the case

[1] http://ec.europa.eu/information_society/policy/rfid/index_en.htm

scenario of air travel. It is clear that Airlines already improved significantly their operational efficiency by utilising Internet check-in, electronic boarding passes, RFID-enabled luggage handling, as well as e-enabled airport check-in and boarding. The adoption and deployment of smart devices is bound to improve their efficiency even further. Similarly, border control and airport security agencies can make use of these technologies to achieve a more accurate and efficient screening process. From the passengers' perspective, improved convenience comes from reducing or even eliminating the need to carry and manage various pieces of documents, certificates and other sensitive assets.

While IoT will inevitably play a major role in improving future air transportation, as it will in many other areas as well, there are critical issues to be identified and considered in depth. Smaller form factor and portability encourages mobility, which leads to frequent interaction between devices, sensors, and network infrastructures. The movement of travellers, airport/airline personnel, and luggage creates an increasing amount of continuous interaction between devices. As the result of these interactions, significant amounts of sensitive information will be generated and shared. The aspects of system security, safety, data sensitivity, usage and management all require further investigation and require addressing in any implementation of IoT environments.

Moreover, the overall system vulnerability landscape is not the mere sum of the vulnerabilities of single devices. As different components start to interact, seemingly minor vulnerabilities of one (e.g. malware on a smart phone), could potentially trigger a major risk of another (e.g. avionic system safety) and amplify the overall risk level. Because of this, new "emerging" vulnerabilities are created (i.e. A + B = A + B + Emerging Risks). The future air transportation processes must therefore address these compound emerging risks, as well as be in a position to predict them and manage them effectively in robust risk management procedures.

2.3 WHY AN IOT/RFID AIR TRAVEL SCENARIO?

In the context of our work in WPK3.1[2], identification of emerging and future risks, we carried out an exhaustive risk assessment on a complex scenario involving Internet of Things / Radio Frequency IDentification (RFID) technologies in future air travel. Given that we are already seeing the introduction and use of smart technologies and applications in air travel (e.g., RFID-enabled passports, electronic boarding passes sent using SMS and displayed using cell phones, etc.), we consider this as a representative, realistic yet emerging, showcase scenario within which we can identify and highlight important risks and challenges posed by IoT technologies. Amongst the technologies, applications and devices considered in this scenario, in addition to RFID, are smart phones, netbooks and location-based services (LBS). The power of these technologies is greatly leveraged by their convergence and

[2] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa_wp_2009.pdf

interoperability. The air travel scenario was selected to illustrate the convergence of these IoT technologies and the issues that arise as a result of this convergence and interoperability.

2.4 TARGET AUDIENCE

The intended audiences of this report are:

- The European Commission, EU Institutions and EU Agencies (e.g. EASA), to assist them on setting research policy (to develop technologies that mitigate risks) and to assist them in deciding on appropriate policy and economic incentives, legislative measures, awareness-raising initiatives, etc. vis-à-vis IoT/RFID technologies and applications; in particular, on air travel;
- Industry, to encourage them to secure their technologies and services, to make transparent to citizen-consumers their purposes and practices in collecting and processing personal data and to identify any third parties with whom they share such data;
- Air transport stakeholders, such as airports Airport Council International (ACI) and IATA;
- Shop owners and vendors who operate in airports;
- Individuals or citizens, to enable them to evaluate the costs, risks and benefits of using the consumer version of these applications.

2.5 SCOPE AND OVERVIEW OF THE SCENARIO

This scenario is explorative and is set in the future, approximately five years from now in the year 2015. It follows three passengers of different citizenships (EU, US, Japan) flying from European airports. The scenario depicts emerging automated procedures typically used in normal air travel, such as check-in and boarding. Different criteria have been used to select the passengers starring in the scenario, namely:

- **Nationality**: Richard is a US citizen, Elena is Spanish and Akira is Japanese
- **Age**: Richard, Elena and Akira, belong to different age groups: 52, 39 and 20 years old respectively.
- **Health**: Richard is a diabetic and has serious heart problems, Elena is healthy overall, but has an allergy condition and Akira is healthy
- **IT "literacy"**: While Richard and Akira are familiar with technology; Elena faces some basic problems with the use of technology and finds it quite overwhelming following the air travel procedures using smart devices.

- **Language skills**: Elena does not speak German and has difficulties in communicating even in English. The others two can both speak English and Richard German as well.

The scenario takes into account current work being carried out by Airport Council International (ACI) and the Simplifying Passenger Travel (SPT), an international interest group comprising of representatives from governments, security agencies, professional organisations, technology vendors, airports and airlines, which is driven by the International Air Transport Association (IATA), the international syndicate of airlines. The scenario considers the IATA-SPT Ideal Process Flow (IPF) [*see Figure 1*] and shows how new technologies such as smart phones, RFID and LBS can contribute to improving the flow of passengers through airports and onto the aircraft and thereby cutting costs for airlines, airports and other stakeholders while, at the same time, improving security.

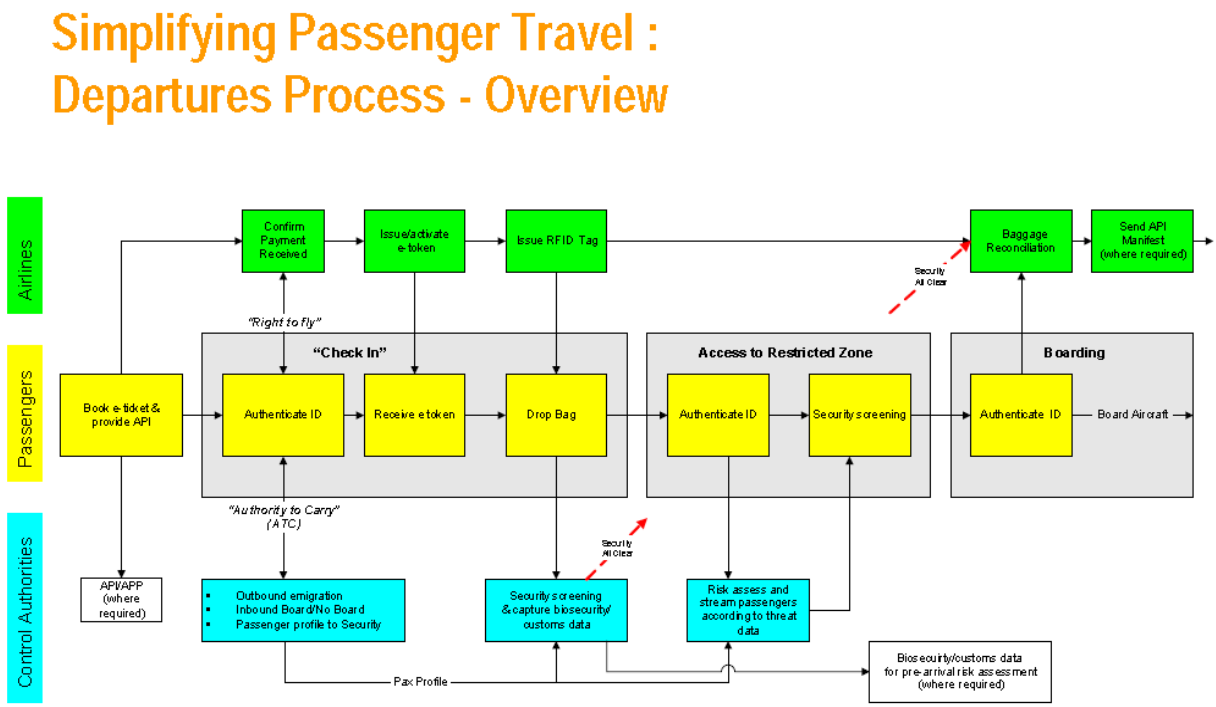


Figure 1 – The technology response to the growing demand from airlines and airports for passenger automation.[3]

[3] See IATA: http://www.iata.org/NR/rdonlyres/31BD66A2-4446-4514-A911-3EA9DDAC7CAA/0/IPF_V20_FINAL.pdf

In the context of the current and emerging procedures for handling passengers, the scenario also examines how the Internet of Things could be a pervasive element within future air transportation from the perspectives of industry and consumer stakeholders.

The scenario tracks and is divided into several phases based on the air travel process and involves the following:

2.5.1 GETTING TO THE AIRPORT AND PRE-FLIGHT ARRANGEMENTS

On the day of travel, there are multiple ways of getting to the airport – personal vehicle, buses, taxis, trains and shuttles. Smart IoT devices interact with various established services in helping passengers get to the airport safely, on time and cost effectively. These services can include on-line selection of travel options based on current position, traffic road conditions, flight schedules and updates, car-pools and airport parking assistance.

2.5.2 GETTING READY TO FLY: AIRPORT CHECK-IN, BOARDING, SECURITY CONTROLS

As a result of IATA's Simplifying the Business (StB) program[4], most carriers (99 per cent) have now adopted electronic ticketing (e-ticketing) measures, to replace costly paper boarding passes. Passengers are invited to check-in from home or at special airport counters and kiosks using electronic ticket codes. While carriers and airports are planning to implement more and more efficient self-service kiosks, there is still a long way to go to fully implement a process based entirely on smart devices.

AIRPORT CHECK-IN

In future air travel, we envision that much, if not all, of the check-in process will be conducted via the Internet. A large percentage of the check-in process will involve IoT smart devices. The passengers will receive a token in the form of a 2D barcode or raw data depending on the capabilities of their devices and the transport medium. As a matter of fact, several airlines already give travellers the option to retrieve the electronic barcode directly on their cell phone. With this scheme, the travellers can simply display the barcode image on their cell phone to a reading device. Consequently, the barcode gets scanned and decoded, making the contained data available to the connected IT systems without the need of airport personnel processing paper copies.

[4] http://www.iata.org/stb/index.htm

SECURITY AND BORDER ACCESS CONTROLS

The scenario does not examine security and border access controls in great depth, only briefly for completeness purposes, since these are an important phase in the air travel process, and cannot be left out of the scenario.

Within the scenario, accompanying friends and family members are limited to the check-in zone of the airport. Only passengers and necessary personnel (e.g. crew members, airline agents, service personnel, restaurant and shop clerks) are allowed to enter the restricted zone for security reasons. Measures for the access control to the restricted zone are being accomplished in two steps:

- **Identification and authentication:** Individuals are identified by comparing their physical traits (face, height, age, etc.) with those documented on a valid official identification document (e.g. passport, national ID card, crew pass, personnel pass).
- **Authorisation:** This is the process of determining whether an authenticated entity is allowed to enter the restricted zone. For passengers, it is done by means of a boarding pass, valid for a flight in the current timeframe. The data on the boarding pass are communicated through 2D barcodes displayed on smart devices, printed on a paper strip or transmitted by near field communication (NFC)[5] and verified by the departure control system of the airline. For the crew and service personnel, authorisation is granted based on a valid crew or airport personnel pass. If they contain a photo, valid passes often also support authentication.

Passengers travelling within the Schengen area[6] are normally exempt from passport checkings and visas required of non-Europeans. There is limited or no border control within the Schengen area.

[5] Near Field Communication (NFC) is a short-range high frequency wireless communication technology which enables the exchange of data between devices over about a 10 centimetre distance. An NFC device can communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices. NFC is primarily aimed at usage in mobile phones. [This definition has been adapted from Wikipedia]

[6] The Schengen Agreement of 1985 established an area where the free movement of persons is guaranteed. The signatory states to the agreement have abolished all internal borders in lieu of a single external border. Here common rules and procedures are applied with regard to visas for short stays, asylum requests and border controls. Simultaneously, to guarantee security within the Schengen area, cooperation and coordination between police services and judicial authorities have been stepped up. Schengen cooperation has been incorporated into the European Union (EU) legal framework by the Treaty of Amsterdam of 1997. However, the European Union and the Schengen area are two different zones: not all EU countries participate in the Schengen area and vice versa: http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm.

A number of fast-track programs have enabled automated border controls based on e-passports. However, there is currently no standard technology used for automatic gates. Most of the systems are based on either fingerprints, with a prior enrolment in a government database, or face recognition based on the match between the passenger and the digital picture in her passport. Furthermore, some airports (e.g., London Heathrow) give travellers the option of using special gates that implement biometric checks (iris scans). Another example can be found in Amsterdam Schiphol airport, where travellers can register for the Privium service program. This is designed for frequent flyers who wish to travel without unnecessary delays. Within Privium, an iris scan is stored on the Privium card[7]. The traveller submits to an iris scan that is compared to the one on the card for a quick pass through the security checks. The iris scan even works when wearing glasses or contact lenses.

The scenario highlights the automatic authentication of passengers by means of their biometric features (e.g., fingerprints and facial image of citizens[8]) stored in their passport as part of EU border control. The scenario does not enter into much detail about this authentication process.

The implementation of an EU passenger name record (PNR) program is scheduled to enter into force from 2010, which will enable travellers to fill in Electronic Travel Authorisation (ETA) forms online 48 hours before departure. The scenario assumes that this has taken place but refers to generic systems instead of specific named ones thus far mentioned in EU documents. We likewise make assumptions that the characteristics of this system will mirror those outlined currently, with the caveat that we accept there might changes in the manner and method of its implementation. This is particularly dependent on currently ongoing consultations between the European Parliament and the Commission on these systems. At many airports, a security check comes immediately after access to the restricted zone and before the passport and immigration control. The scenario depicts performance of security checks in smart corridors equipped with metal detectors, explosive detection systems (EDS) and liquids and gels (LAG) detectors to identify prohibited items such as weapons, liquids and explosives.

WAITING TO BOARD

Passengers often spend a lot of time waiting to board either due to flight delays or simply because they arrive earlier than necessary to avoid the risk of being late for the flight because of delays at security check points. Airports and several Commercial Services saw an opportunity in this and they

[7] http://www.schiphol.nl/Travellers/AtSchiphol/PriviumIrisscan.htm

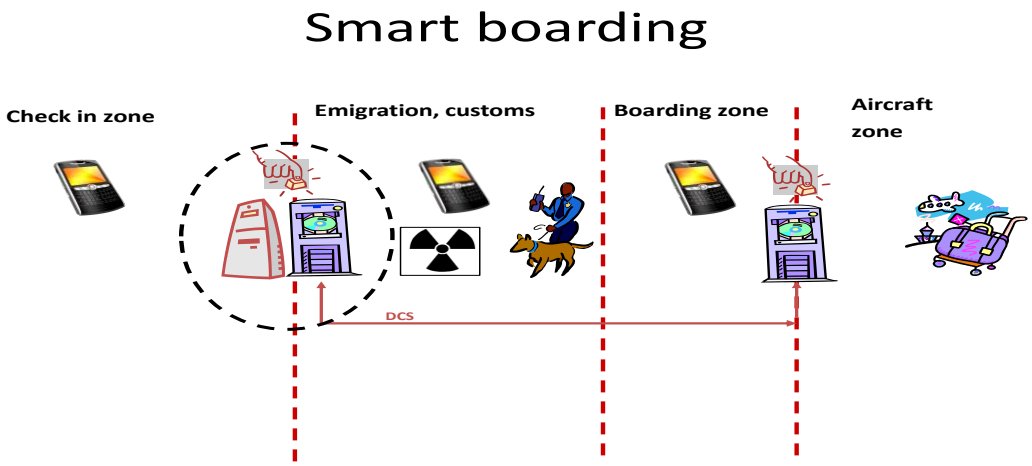
[8] Council Regulation EC 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L385/1, 29.12.2004. For EU Member States, Art 1(2) of the Council Regulation EC 2252/2004 obliges the storage of the e-passport holder's facial image in the RFID-enabled chip and include fingerprints in interoperable formats.

sought to turn this time gap into an advantage. Duty-free shops, kiosks, restaurants and information services compete to attract travellers' attention and their intention to buy. Passengers often are interested in buying souvenirs, food, entertainment, network access and other services, while airports are increasingly happy to accommodate increased consumer spending as reflected in the design of airport retail space. The interesting challenge here is matching consumers to suppliers effectively (finding the right customer as well as the right product), efficiently (since time is relatively limited) and unobtrusively (not an open market). IoT smart devices could play a major role enabling the future of this environment. They also have the capability to unobtrusively provide direction-related assistance, e.g. for locating gates, stores, restrooms, kiosks, police desks, wheel chair stations, access gates for people with reduced mobility (PRM) and airline service desks.

Airport security may also monitor abnormal behaviour of passengers, e.g. lingering around in sensitive areas using localisation-enabled smart devices. They may also wish to identify potential emergency situations, e.g. of disabled passengers needing help, by detecting people not having moved for an excessive time.

BOARDING

The scenario depicts a seamless "smart" boarding process aiming at enabling efficient and secure passenger management. This process is based on the same principle that is used at the check-in stage, namely verifying 2D barcodes or tokens and biometrically authenticating passengers to prevent the exchange of boarding passes.



By smart boarding, we mean that the passenger is already identified based on the link established between the check-in system and the ultimate boarding control via the departure control system (DCS)

of the airline. The concept is quite straightforward: the passenger has completed the check-in using any technology – e.g. Internet printing of the boarding pass, PDA validation of an electronic code, NFC interaction with a sensor.

Several airlines have already implemented such a system to speed up boarding procedures. This requires a prior negotiation with data protection authorities, as private companies are not allowed to access the biometric data stored in the e-enabled passports. For these reasons, these airlines have launched proprietary systems, as Air France has done for flights between Paris and Amsterdam Schiphol[9,10].

2.5.3 IN FLIGHT

Combined with the increasing prevalence of "Internet in the air" services, smart devices will have significant impact to both airlines and passengers. Broadband wireless communication will enable the download of flight and in-flight entertainment (IFE) data for travellers. During their flights, passengers will have access to the Internet via their netbooks, smart phones or the IFE screen. If desired, movies can be uploaded before the aircraft departs.

2.5.4 ARRIVAL AND TRANSFER

Upon arrival, passengers claim their luggage and proceed to local transportation to head toward their final destinations. IoT and smart devices are expected to further facilitate this process and, in particular, enhance services related for example with assistance on local arrangements for visitors. Also, from the local perspective, the arrival of a new passenger creates business opportunities (e.g., ground transportation, lodging or tourist services); is envisaged that IoT devices will facilitate the the exploitation of such opportunities.

For passengers transferring to another flight, IoT devices can assist in providing connection and flight information and locating the correct gate. Therefore, another round of "waiting to board" scenarios is

[9] Most of the carriers take advantage of government automated border control programs for international flights. But in the case of domestic/ intra-Schengen flights, they consider managing their own fast track system as a competitive advantage to increase their market share on highly competitive routes. This is the case of Air France for their ADP/ Schiphol flights; and same for Air France in their competition against the high speed train: Paris / Marseille / Nice, Toulouse, etc. But as the carriers are not allowed to control the biometrics of the passports, they need to launch their own system in agreement with local Data Protection Commissioners. This means that we might see different proprietary systems for intra-Shengen flights in parallel to government's Automatic Border Management systems should the Data Protection Commissioners not allow the carriers to access the passports' biometrics.

[10] See http://www.theregister.co.uk/2009/03/19/france_fingerprint_cards/

played out in the gateway airport. In particular, for passengers who miss their connection, IoT devices can assist in flight re-booking, wherever required (some airlines, e.g. Delta airlines, currently provide automatic re-booking) and, if necessary, lay-over lodging and hotel transportation. Some airlines have systems already in place that re-book delayed passengers onto the next available flight and, in the future, passengers will receive the up-to-date information on rebooked flights automatically on their devices when they arrive at the airport.

After leaving the aircraft, at the arrival gate, and particularly in big airports, passengers may be offered additional guidance if needed, through the arrival process and to the final destination by personal electronic devices, as well as airport infrastructure such as information kiosks and guidance systems. Moreover, booking applications may be available for taxis, public transportation or further travel-related services. Data may be exchanged between flight information systems, the passengers' personal devices and those services in order to update schedules and to ensure seamless and comfortable transportation.

2.6 WHAT'S OUT OF SCOPE

The following fall outside the scenario's scope:

- National security issues were not considered: as ENISA worked in first pillar activities of EU[11] at the time when this project was first conceived, it was not possible to enter into issues of national security that fell within the third pillar. For this reason, border control issues fall out of the scope of this assessment. Any border control mentioned in the scenario is only for completion purposes, as this is an inherent part of the air travel process, and we want to keep the scenario realistic.
- The focus is mainly on passengers. Due to limited time and resources, the scenario does not consider in detail security personnel, airline crew and other airport personnel, who may have different access requirements.
- Aircraft security and general aviation maintenance, repair and overhaul (MRO) procedures are not considered, as they would considerably increase the complexity of the scenario.

[11] For more information on the three pillars of EU, please refer to http://europa.eu/scadplus/glossary/eu_pillars_en.htm. It is noted that although the pillar structure have been abolished in the new Constitutional Treaty of Lisbon, at the time when this project was conceived in 2008, the pillars were still in effect and their restrictions had to be considered and respected.

3 CAUTIONARY TALES – FLYING 2.0 – A 'SMART' IOT/RFID AIR TRAVEL SCENARIO

ENISA convened a group of independent experts to develop and analyse a scenario, the context of which was the use of new smart technologies, notably IoT technologies, in air travel. Once the scenario was reasonably stable (it went through several iterations), the group then analysed the scenario using ENISA's methodology, in particular to identify assets, vulnerabilities, threats, risks and remedial actions as well as eventually recommendations to policy-makers and other stakeholders.

Thus, the scenario is the foundation on which everything else is built. The scenario developed by the group can be found in Annex II.

This section presents three cautionary tales, based on the somewhat longer scenario script. The cautionary tales are in two parts. The text in the right-hand column presents a streamlined scenario script, while the left-hand column provides some commentary, notably on possible risks arising from the actions taking place in the scenario script. Also in the left-hand column are some [R xx, where xx represents a number] which refers to the specific risks identified in section 5.2 of this document.

A – RICHARD

Introducing Richard… and his gadgets: a pace-maker, a sensor implant and a smart phone *He depends on the reliability of his technologies and the communications' infrastructure [R9], [R13]*	Richard is a 52-year-old US citizen who has been working in Frankfurt and now is flying back to Atlanta, with German Air (GA), for his vacation. He has had two heart surgeries over the years and carries a pace-maker. He also has a chronic diabetes condition for which his doctor has implanted an in-body blood sugar level monitoring sensor. The monitoring system can communicate with his doctor in case of an emergency using Richard's smart phone as a gateway. This system is also capable of announcing itself to the surrounding environment and other devices (e.g., body scanners or smart corridors) in case they might disrupt his pacemaker or body area network.
He similarly depends on the security of government	As a non-EU citizen resident in Germany, Richard has enrolled in the registered traveller (RT) program at the German Ministry of Interior

databases	offices in Frankfurt.
… and of industry databases and service providers [R10], [R9]	He has recently bought a new smart phone with NFC functionality in order to use a personal healthcare service while he is on the move. The smart phone is able to collect data from his implanted blood sugar level sensor and forward its measurements to a "steady-sugar-level" diabetes service to which Richard has subscribed. The service monitors Richard's blood glucose level and provides him advice on his diet and activity.
Richard's details are on his airline's database, so he depends on its security and it not being shared without valid reasons, but government agencies have such access [R6]	Richard, who is an "Elite frequent flyer" member of his airline's program, confirmed his flight and selected his seat 24 hours in advance with his smart phone. To do this, he logged in with his frequent flyer number and his PIN code and then selected the online check-in menu. This check-in menu is accessible via both computer and personal digital assistant (PDA). As a result, he received and stored in his smart device a token for his check-in data, as well as information and alerts on his calendar. This token is used as his boarding pass. When registering as a frequent flyer member, Richard registered his fingerprints to the airline. When the token is issued, it is encoded with his fingerprints to prevent someone else from using his token.
The RFID tags could become detached from the luggage, either by accident or on purpose. Richard could also lose his smart phone and, if so, would lose the RFID tag's number [R5].	During the check-in process, Richard asked for a luggage service, which picks up passengers' luggage from their homes. When the service personnel arrive at his house, Richard communicates his boarding pass data from his smart phone to their mobile device which include RFID printers. The driver prints RFID-enabled luggage tags and attaches them to Richard's luggage. These tags contain Richard's passenger and flight data as well as other relevant data such as weight, priority handling and insurance. Richard is also reminded to point his smart phone at the tags to record their number, and then the driver takes the luggage to the airport. This enables Richard to get a receipt, stored in his smart phone, of the luggage tags, to be on the safe side.

It is not clear who is retaining the data on the tag and what they do with it. [R6, R7]	Throughout the travel, the RFID tags will be read by scanners at various locations in the luggage transportation chain, and the data they contain will be stored on the relevant system.
Richard has no insight about what happens to his PNR, who gets the data and what they do with it [R7, R10].	Richard has also filled in, 24 hours in advance, the passenger name record (PNR) form at the German Airlines website, where he provided personal information including his name, date of birth, nationality and passport issuance data. These data were then processed and validated by the German Passenger Information Unit (PIU) and then forwarded to the US Department of Homeland Security which then further disperses the data to other US agencies.
Richard does not consider any risks arising from third party access to his smart phone [R14, R15].	As Richard has no luggage to carry, he decides to travel to the airport using Diamond Airport Shuttle Express. He is a subscriber to a web-based travel service called "WhereToGo", which books the shuttle for him based on his departure time. Acting like a secretary, WhereToGo places the shuttle reservation, pick-up time and fare information into the electronic calendar on Richard's smart phone.
Everything works smoothly as long as Richard does not lose his smart phone.	German Air announces an unexpected three-hour delay in the departure of Richard's flight. WhereToGo immediately re-books the shuttle, updates his calendar and sends Richard a voice mail alert. Unperturbed, Richard uses the extra time to respond to e-mails and review some reports. As his pick-up time finally approaches, WhereToGo sends him a reminder about where he has to go to meet the shuttle. The shuttle service uses car-to-roadside communication to continuously update its route and time planning to ensure on-time arrival at each pickup location and at the airport. After picking up Richard, the shuttle bus receives information from roadside units (RSU) at an intersection ahead about a car accident blocking traffic. The shuttle bus takes an alternative route to avoid the traffic accident and they arrive at the airport on time. Before arrival, the shuttle driver requests payment and Richard pays

	the meter plus tip using his smart phone, which has an e-cash purse application (among many others).
Richard's identity does not have to be revealed to make a payment.	
If someone had stolen Richard's smart phone [R15], that someone could get past this first security check. Fortunately, there is no failure in the process of checking in and boarding [R1]	Upon arrival in the airport, Richard checks his smart phone for the latest flight status information. He uses his smart phone with the received token during check-in in combination with the smart phone's near field communications (NFC) capability to gain access to the restricted zone. He also has to put his finger on a reader which reads his fingerprint and confirms that the token is issued to him. If his phone were to be stolen, the token would not be usable without his fingerprints. The scanner is linked to the departure control system (DCS), which has the data on Richard's travel on the German Air flight to Atlanta. He is allowed to enter the restricted zone.
The choice of a fingerprint or iris scanner is meaningless for some disabled or older passengers who may not be able to confirm their identity by either means [R17]. Legislation lags technology developments such as full body scanning [R17].	Since Richard is leaving the Schengen area, he needs to go through the automated passport control. He proceeds to a border control booth and places his passport near the reader to activate the authentication process. The passport reader verifies his passport. Richard has to use a fingerprint or iris scanner which confirms him as the rightful owner of the passport based on biometrics stored in it. He is then subjected to a full body scan, which he clears after officials see that his pacemaker and implant are non-threatening. (Not all airports are using full body scans yet, partly because of the cost and partly because of a lack of legislative authorisation.) Access to the security control zone is authorised after the automated passport/immigration control system accesses the Passenger Information Unit (PIU) at the German Ministry of the Interior, which delivers an electronic travel authorisation (ETA), based on the

clearing of his PNR data.

By agreeing to this service, Richard potentially exposes himself to a lot of location-based spam [R18]. So far, it hasn't been a problem.

Richard can then enjoy various airport facilities, such as connecting to the GA Elite Frequent Flyer free Wi-Fi network. When he buys goods from duty free shops, he confirms his flight by communicating his token through NFC. While Richard is browsing, a location-based service (LBS) identifies his presence to a neighbouring duty-free shop or, at least, the presence of someone who has indicated his interest in certain products. Based on his LBS' preferences, the shop automatically transmits a message to Richard's smart phone, recommending that he checks out its offer on silk scarves. Richard visits the store and buys two scarves for Helen, his wife.

Richard believes that his electronic purchase does not leave any digital traces of personal data (which could result in identity theft [R14])… and he may be right in this case

Richard feels hungry. He goes to the "Food Corner" to grab a sandwich. His smart phone has an application which enables Richard to detect RFID-labelled products which are compatible with his restricted diet. As he pays for the item using his smart phone's e-purse function again, he receives an alert from German Air calling him to his boarding gate. A few minutes later, he retrieves the check-in token again and authenticates himself at the gate as he did at passport control.

…but on-board, he is less sure. Perhaps the airline monitors his health status too, linking that data with the data they already have about him…[R9].

Richard boards his German Air plane which is equipped for "physically challenged passengers". The aircraft has special seats embedded with pressure and temperature sensors, which unobtrusively monitor passengers for early warnings such as lack of movement or agitated movement during long flights. The aircraft also has an onboard wireless network which allows Richard to transmit signals from his body area network to terrestrial networks and on to his health subscription service which can detect any early signs of health problems.

nor can he be sure about whether his communications are monitored [R18].

The aircraft's satellite communications service, although expensive, allows Richard to connect with the Internet and to check his e-mails.

Richard's service provider also knows where he is and, unbeknownst to him, could be sharing his whereabouts with third parties [R6].	Since Helen, Richard's wife, said she would collect him from the airport upon arrival, Richard ensures his smart phone's position determination function is on, so she can monitor his progress through the airport and meet him at the exit.

B – ELENA

Introducing Elena, who is not very IT-literate [R11]	Elena**,** a 39-year-old Spanish language professor, was visiting her 25-year-old niece Cristina in Frankfurt, but now is returning to Madrid with Aerolíneas Españolas. Elena does not speak German nor is her English very good. Moreover, she is not 'IT-literate'. She does not travel much and finds the automated air transport procedures a bit overwhelming and difficult to follow. She owns an old mobile phone with limited features. Elena's only smart device is her allergy bracelet (she suffers from gluten intolerance) which alerts her when by vibrating/flashing.
Elena did not misplace her paper ticket, although she is a bit forgetful, but she could have done so [R4].	Cristina bought a paper flight ticket for Elena at a travel agency, and she now drives her to the airport with the help of her car's computer, which is equipped with GPS and a telematics module. Cristina subscribes to a vehicle safety and efficiency service (which is also a location-based service, LBS) which is available to all cars equipped with such modules. The service automatically selects the optimal route based on Cristina's current location (which is determined by her GPS and/or intelligent sensors in her car interacting with roadside sensors), traffic conditions and local weather information communicated by the service. While the traffic information is downloaded in real time and displayed on the digital map shown on her car's computer, Cristina's location is revealed to her cell communication provider as well as her LBS provider. Airport staff, city administration and private companies share and co-ordinate traffic data in order to minimise potential disruptions on roads to the airport.
There are always trade-offs. The service to which Cristina subscribes offers more automotive efficiency but it also has a record of how fast she drives and where [R6].	
Has Cristina agreed to their sharing her data? [R6, R8] Does she understand what	Cristina earns points with the latter service when she uses specific

they are doing with her data?

facilities and services, such as the airport parking lot, or when she buys from a specific store. So, upon entering the airport access road, the automobile's licence number is captured by several digital video cameras. The video record is shared between commercial service providers as well as the airport security service. The LBS invites Cristina to use a specific airport parking and when she accepts, the garage parking assistance application guides her to the specific lot.

As expected, they arrive at the airport on time. However, Cristina must attend an urgent business meeting, so she can only help Elena with her luggage to the airport entrance where they part company.

The VID is a life-saver for Elena, otherwise she would have had some problems checking in and making her way to her departure gate [R1], but its capabilities are limited to only the official languages of the EU. Slim chance, but still how would Elena cope if she only spoke Basque or one of the other minority languages? [R11]

Elena must find her own way to the Aerolíneas Españolas check-in counter. As soon as she enters the airport, Elena approaches an information kiosk to ask for more information on how to proceed next. As she doesn't speak German or English very well, the assistant gives her a visual interface device (VID) which is location sensitive, with voice instructions in all EU languages. Elena selects the Spanish language and follows the instructions towards a manned check-in desk to drop off her luggage and collect a boarding pass, including the luggage tag receipt. At the check-in counter, the attendant asks her for the VID and keys in, as the final destination, the gate from which Elena should board. The VID provides her spoken and visual information on her location inside the airport and how to get to the gate where she is to board. It will also alert her when boarding actually starts. The attendant tries to explain to her, with a lot of body language, that she will need to leave the device with an assistant at the boarding counter.

Elena's language difficulties hamper her check-in, but she manages. Her difficulties would be greatly compounded if there were an operational failure or disruption [R1]

With more gesturing, the attendant asks Elena to press a finger against a scanner, which registers her fingerprint features and encodes them in a 2D barcode which he prints off as part of her boarding pass. This prevents Elena's boarding pass from being used by another person. He gives her the boarding pass and VID. Following its instructions, she proceeds to the security check, and then on to her gate. She's relieved to see that she made it with less trouble than she feared.

As she still has plenty of time before her flight departs, she decides

to go window-shopping. She loses track of time, until her VID alerts her that her flight is about to start boarding, so she rushes back to the gate. When she presents her boarding pass, the airline attendant asks her (in Spanish, whew!) for the VID, which she hands over. Airline staff will return it in due course to one of the information kiosks.

Elena depends on the reliability of her allergy bracelet to avoid a risk to her health [R9]. And what if she has chosen to eat the pretzels despite of the alarm in the bracelet?

Apparently, Elena is frustrated with her bracelet… What if she stops using it? [R11]

Having boarded the plane without incident, Elena is safely ensconced in her seat when, after take-off, the flight attendants begin distributing drinks and snacks. They hand her a bag of pretzels with an RFID chip imprinted on the bag. Elena's allergy bracelet recognizes the rice gluten content via communication with the chip containing the product code and alerts her by vibrating/flashing; it is also supposed to deliver a SMS on her phone and/or an alert through the Bluetooth connection; however, Elena has her phone switched off, and the alert fails to be delivered. Elena chooses to ignore the vibration: the bracelet many times has vibrated even if the food was OK for her to eat, and she is rather annoyed with it. She does, however, decline the snack, because she does not feel like eating pretzels. The flight attendant offers her some fresh fruit as an alternative.

As the flight heads south to Spain, Elena tries out the e-book reader in the seat-back pocket, a recent novelty introduced by the airline. Elena has never used one before, but her positive experience with the VID has encouraged her to try out this new technology. She selects one of the titles in Spanish. The device is intuitive and easy to use. The day's excitement has made her a bit weary so she plugs in the accompanying earphones and turns on the e-book's text-to-speech function. This is wonderful, she thinks to herself.

The LBS operator and taxi company both retain copies of Elena's response in case they wish to offer her a similar service in future. Elena does not know that they retain her data indefinitely in contravention

The flight lands on time at Madrid's Barajas airport. Now, back on familiar ground, even if she is not a frequent traveller, she can easily find her way around. She switches on her mobile phone as goes to collect her luggage. Since her niece had subscribed her to the LBS service before, so that she can find a taxi right away, Elena immediately receives an SMS asking if she needs a taxi, and as she feels tired, she replies "Yes". Her response and GSM-based coordinates are transmitted to an LBS operator which also serves a

of data protection legislation [R18]	taxi company. As she exits the terminal, she receives a multi-media messaging service (MMS) photo of the car which is waiting a few metres away from her.

C – AKIRA

Introducing Akira *Akira managed to get a visa, but there could be a risk for individuals wanting a visa if there is a failure in the system [R5]. There could also be a risk if an evil-doer succeeds in getting a visa [R7], [R14], [R15].*	Akira, a 20-year-old Japanese architecture student, is returning to Tokyo, with Nihon Airlines, after studying on a scholarship at the University of London. Before he left Tokyo a year ago, he was registered on the new Entry Exit system managed by the European Commission's Directorate General for Justice, Freedom and Security (DG JFS) and received a one-year visa for the time he was to spend in the UK. The entry system authenticates the visa holder by matching his fingerprints against the templates stored in the chip of his visa, somewhat like biometric passports. The entry system records his name, date and place of entry.
The system could be a problem for people without fingers or with worn fingerprints (e.g., many old people) [R3]	Complying with travel regulations, Akira has filled out, 24 hours in advance, his passenger name record (PNR) form, which he did online and which he sent to the UK Home Office. The latter positively matched the PNR against his Global Entry registration data.
The airline acquires more data about Akira's tastes and interests [R6].	Still online, Akira visits the airline's duty-free section and buys a few gifts for his parents. The airline attaches RFID tags to the items indicating that Akira is the rightful owner. The items will be loaded onto the correct airplane based on his boarding pass information and given to Akira when he is in mid-air.
Akira does not know how secure the card is, nor how secure is TfL's storage of his personal data, nor whether third parties have access to it. [R10]	Akira takes the Underground to Heathrow. He pays for the journey using his RFID-embedded Oyster card. Transport for London (TfL) maintains a record of Akira's payments as well as all the travels he has made using the card.

The system works well as long as all individual components, nodes and links work as they are supposed to, but they could fail [R3]. If communications with the Home Office go down (e.g., because of a fire), the whole system may crash [R13]

As Akira has not checked in yet, he goes to a kiosk in the departure terminal where he uses his Nihon Airlines frequent-flyer card to check in. He presents the RFID-embedded card to one of the designated RFID readers. He is also asked to put one of his fingers on the scanner, which compares it with the fingerprint features stored on his frequent flyer card, a procedure designed to prevent someone other than Akira from using his frequent flyer card with his boarding pass. The reader transfers information about Akira's flight, seat number, etc., to the frequent flyer card and to the RFID tag embedded in his suitcase. Now Akira can use his card as a boarding pass. When he displays his card to the reader, which is linked to the airline's departure control system, it confirms that he is indeed booked on the flight to Narita. At the same time, it updates the Passenger Information Unit (PIU) at the Home Office, which delivers an electronic travel authorisation (ETA), based on the processing of his PNR. He would not be issued an ETA if he had overstayed his visa period. This check-in procedure allows Akira to enter the restricted area.

Is there a fall-back system for people without fingerprints? [R3], [R4]

What happens if Akira is mistakenly on one of the various watch-lists maintained by EU border authorities? [R2]

At the self-check in kiosk, the machine also adds Akira's flight details to the RFID tag embedded in his suitcase. The luggage tag receipt is then stored on his frequent flyer card. Akira can then drop off his suitcase at the nearest baggage drop. Akira puts the luggage on a conveyor, which dispatches it to the Tokyo flight containers for his flight.

He then proceeds to the restricted zone, which he enters by presenting his frequent flyer card to an RFID reader and pressing a finger against a scanner which confirms that the card containing his boarding pass belongs to him.

As he is leaving the Schengen area, he is directed to an automated passport/immigration control. The combined biometric data from both his visa and passport are checked to verify that he is the rightful owner and that he has not overstayed his time in Europe.

People like Akira can be fed faked information via social networking applications

After passing the security check, he proceeds to his gate. He is registered on a Japanese professional network site (*JP-professionals-unite.com*) and is interested in making new connections with

and, potentially, be exposed to fraud or other crime [R10], [R15].

architects and interior designers, since he will be looking for a job in Japan. At the boarding gate, the application on his smart phone detects someone from Tokyo Architects Ltd waiting to board the same plane. Akira sends a message, which the other accepts; they agree to identify themselves and soon they are chatting face to face.

Akira places trust, perhaps unwisely, in others whom he does not know

On board and in the air, Akira turns on his notebook and soon forms a peer-to-peer ad-hoc network with 15 other passengers who share interests in travel to exotic places. Akira also connects to the Nihon Airline's flight entertainment system's free movie section and browses the movies but cannot find anything that he likes. However, he does find a couple of interesting documentary films, published under Creative Commons, about travels to South America which a fellow passenger shares on his video server. Akira spends some enjoyable hours viewing these. Akira reciprocates with some of the content and services on his notebook.

Akira exposes himself to behavioural advertising [R8]

Akira also uses his notebook to select a Japanese dinner from the Nihon Airlines in-flight service menu website.

and again [R8]

One of the in-flight attendant's brings Akira the duty-free items he had previously purchased via the airline's website. A match is made between the RFID tags on Akira's boarding pass and on the tagged items. As an afterthought, he connects to the in-flight duty free shopping menu from his notebook and decides to buy a heavily discounted Swiss watch for his girlfriend.

Akira arrives at Narita airport and proceeds to the luggage reclaim, where an automated system returns all pieces of luggage exactly to their owners upon request. Akira approaches such a station and presents to a reader his frequent flyer card, which contains his luggage tags receipt. Within a few seconds, the system automatically moves his suitcases to the appropriate reclaim station, where Akira collects them.

The airport allows collaboration with other third party service providers, raising questions about data

As he does so, he receives a message from a well-established Japanese online dating service, to which Akira had been a subscriber and which is integrated with the LBS service of Narita airport:

sharing [R8], [R18]	"Dear Akira-san, welcome back. We hope you had a good journey. It is our greatest pleasure to offer you this opportunity to meet Sakura-san, a young lady of exceptionally fine matching attributes based on your "Hazukashi Nain" (Shy Not) social network profile. Sakura-san is not far from your current physical location and is willing to communicate with you. Please push this button for an instant audio/video connection." But Akira has a girlfriend now and no longer wishes to receive such invitations. He wisely clicks on the "ignore" button and moves on towards the exit where his girlfriend and parents await him.

4 ENISA EFR FRAMEWORK AND RISK ASSESSMENT METHODOLOGY

The European Network Information Security Agency (ENISA), has undertaken the development of a framework for the analysis and reporting of emerging and future risks in the area of information security. ENISA defines emerging risks as those that may have an impact between one and five years in the future; and future risks as those that may have an impact more than five years in the future.

4.1 THE EFR FRAMEWORK: CONCEPT AND PURPOSE

The EFR Framework is based around the use of predictive, narrative "scenarios". The concept behind scenario planning is essentially simple: it facilitates the telling of realistic stories about possible (or probable) future events, based on extrapolation from present trends.

In the EFR Framework , the use of scenarios, rather than any other form of analysis, is intended to ensure that the extrapolations are both realistic and can be understood and appreciated by the decision makers. When building the scenario, a single technology, or prospective use of that technology, is selected for consideration. This is then built into a unique scenario that describes a situation in the future; in which that technology, or its functionality, has been deployed.

Once an area of EFR interest has been selected; a narrative story or "scenario" is written. The concepts underlying the story are then subjected to a risk assessment process, more information on which you may find in the next section. This looks at the technology and its use, as described in the narrative, in order to identify possible threats and vulnerabilities. From these, the assessment deduces the potential risk to the assets mentioned by the narrative.

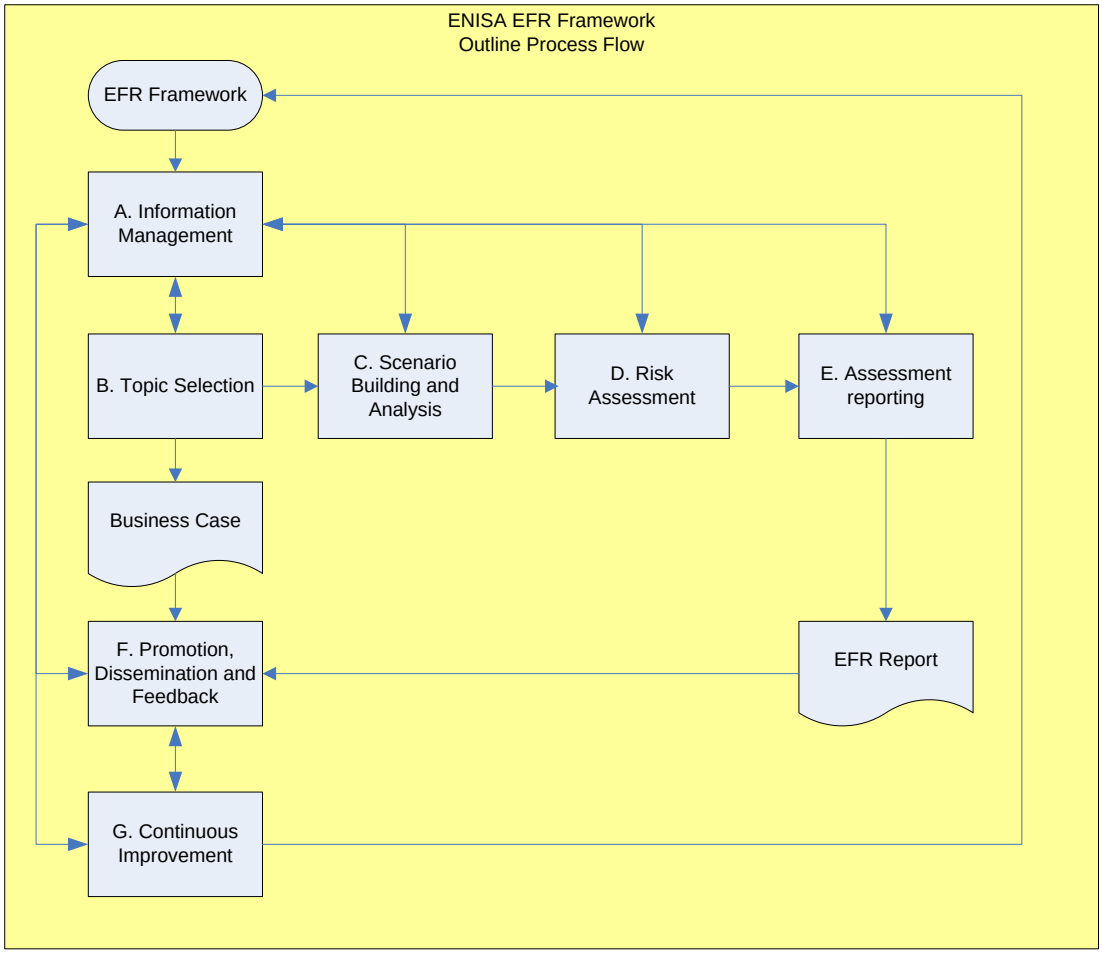
The purpose of the ENISA EFR Framework is similar to that of classical scenario planning; in that it alerts those reading the report to possible future outcomes of current trends. However, the EFR Framework is both more narrowly targeted and more structured; in that it delivers a reasoned assessment of the risks inherent in the technology and its use.

EFR assessment reports should be read by appropriate target audiences in order to ensure that the risks (both positive and negative) inherent in a technology and its use are recognised and understood. If considered necessary and appropriate, comprehension of the risks will enable decision makers to take appropriate steps to manage and mitigate them, where possible.

At figure 1, below, is a simplified, outline flow diagram showing the processes of the EFR Framework. These are as follows:

A. Information Management

B. Topic Selection
C. Scenario Building and Analysis
D. Risk Assessment
E. Assessment Reporting
F. Promotion, Dissemination and Feed-back
G. Continuous Improvement.



For more information on the EFR Framework, please refer to the *ENISA EFR Framework – Introductory Manual* [16].

4.2 RISK ASSESSMENT METHODOLOGY

The methodological approach used in this project to identify and assess emerging and future risks was based on the standard **ISO/ IEC 27005:2008 Information technology — Security techniques —**

Information Security Risk Management [25]. In this endeavour, the ENISA team was supported by a group of external risk management specialists from Ernst & Young Greece.

The evaluation scales and metrics have been customised to fit the project's requirements.

The following major steps were performed in the process of assessing the emerging and future risks:

- Assets identification and valuation
- Vulnerabilities identification and assessment
- Threats identification and assessment
- Identification of existing / implemented controls
- Identification of final risks

4.2.1 IDENTIFICATION AND VALUATION OF ASSETS

In this step, we identified the major assets to be protected in the scenario and we estimated their value.

For the purposes of our analysis, asset identification was performed at the composite asset level, meaning that personal and other type of data was identified as part of a physical asset (e.g. a smart device, a health monitoring device, a database etc.) and not as a separate asset. As such, the estimation of the value of the physical asset considered also the value of the data that resides on this asset.

To estimate the asset value, we identified and considered the certain impact areas. Using a scale from 1 to 5 (Very Low to Very High), we estimated the impact in each area for each asset. The final asset value was the maximum of these values.

4.2.2 IDENTIFICATION AND ASSESSMENT OF VULNERABILITIES

The purpose of this stage was to identify and assess vulnerabilities of the assets. A "vulnerability" refers to an aspect of an system / process (the assets) that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that are likely to be threatened. These vulnerabilities are independent of any particular threat instance or attack.

In the evaluation of the vulnerabilities, a scale from 1 to 5 (Very Low to Very High) was used and the following attributes were considered:

- **Severity**: The severity of impact that will be incurred if the particular vulnerability is exploited. This includes the scope of the impact and the escalation potential (e.g.: where the exploitation of the particular vulnerability would subsequently lead).
- **Exposure**: The ease of exploiting the particular vulnerability through physical or electronic means (required know-how, required resources).

It should also be noted that the vulnerability value was assigned when related to a specific asset, since the same vulnerability had different value in different assets. The vulnerability assessment also considered possible existing / implemented controls identified or assumed in our scenario.

4.2.3 IDENTIFICATION AND ASSESSMENT OF THREATS

This stage involved the identification and assessment of possible threats that could exploit the vulnerabilities of the assets identified. It should be noted that threats exist regardless of the vulnerabilities, and there are two major categories of threats to be considered: **man-made** and **natural** threats, namely threats due to humans (either accidentally or intentionally) and threats due to natural events (e.g. adverse weather conditions).

Using the same scale of 1 to 5 (very low to very high), the threats are evaluated, considering the following parameters, especially for man-made threats:

- **Capability**: The amount of information available to the threat agent (knowledge, training, technological sophistication etc.) and the availability of the required resources.
- **Motivation**: The threat agent's perception of attractiveness of the assets, danger of apprehension, and in general motive to violate standards and procedures

Please note that the function of these two parameters provides the **likelihood** of this threat to occur.

4.2.4 IDENTIFICATION AND ASSESSMENT OF IMPLEMENTED CONTROLS

As controls we identified measures for protection and effective operation of the assets such as: policies, procedures, organizational and technological manual or automated mechanisms. Controls can be categorised as:

- Preventive controls
- Detective controls
- Deterrent controls

- Corrective controls
- Containment and recovery controls

As our scenario is plausible, existing (implemented) controls have been identified in the form of assumptions in the scenario development.

The expert group considered existing controls in the evaluation of vulnerabilities and threats. The values of which have been decreased in some cases due to the existence of these controls.

4.2.5 Risk identification and Assessment

According to ENISA's risk analysis methodology, the final risk and its value are a function of the three elements namely:

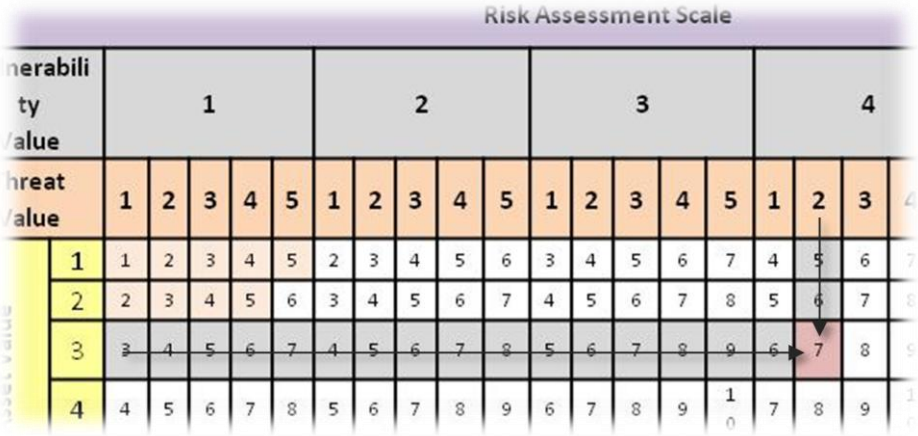
Risk = f(Asset, Vulnerability, Threat)

In practice, after identifying and assessing the vulnerabilities for every asset, the group followed these steps:

- **Mapping threats to vulnerabilities**: In this step, the group identified possible threats that could exploit each vulnerability of each asset. It is the unique pairs of vulnerability and threat for a certain asset that produces a risk for this asset.
- **Risk value**: As mentioned above, the value of the risk is a function of the asset, vulnerability and threat values. The asset values, and the threat and vulnerability levels, relevant to each type of consequence, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 1 to 13. The values are placed in the matrix in a structured manner [25].

Risk Assessment Scale																									
Vulnerability Value		1					2					3					4					5				
Threat Value		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Asset Value	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
	2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
	3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
	4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
	5	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13

According to the standard, for each asset, the relevant vulnerabilities and their corresponding threats are considered. In principle, if there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk [25]. Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the vulnerability value and the threat value. For example, for an asset with a value of 3, with a vulnerability valued at 4, which can be exploited by a threat valued at 2, the final risk produced is estimated at the value of 7, as shown in the figure below:



All of the steps presented above have been performed and are documented in an Excel file, which can be found in the attached Annex III of this report. The results for each step are presented in the relevant worksheet tab.

4.2.6 RISK MITIGATION – IDENTIFICATION OF CONTROLS AND RECOMMENDATIONS

Following the identification and assessment of risks, to the group ranked the risks from very high to very low. Therefore, as the next step, the group identified possible controls and safeguards that could reduce those risks. For the purposes of this analysis, the risk mitigation step has been limited to the recommendation of potential controls to mitigate the risks identified. For example, acceptance levels have not been identified, as is the case in a usual risk mitigation exercise.

5 RISK ASSESSMENT RESULTS

This chapter presents the results of the risk assessment are presented.

5.1 ASSETS – WHAT ARE WE TRYING TO PROTECT?

This section identifies the assets that we wish to protect against the risks identified in the previous section. Within the IoT/RFID air transportation context, can be tangible or intangible as well as be owned by various stakeholders such as passengers, states, airlines, or airport shops. Assets may include hardware, software, systems, data, business processes, buildings/facilities, equipment, or infrastructure. The values of the assets are different for different entities. For example, passport and ID cards are extremely important for passengers, because without them air travel would be almost impossible. On the other hand, passport and ID cards are not that pertinent for airport shops. Another example would be RFID and barcode readers. In 2015, this equipment will likely be extremely important to the airlines to enhance further the efficiency of check-in, boarding and baggage handling processes. Nevertheless, from a passenger's perspective, these processes are transparent and, as such, the value propositions of such equipments are relatively low. Asset values also change over time. An after-flight boarding pass can still be valuable for frequent flyer mileage validation, but it is not as critical as it is a pre-flight one.

Assets have vulnerabilities that could potentially be exploited. These vulnerabilities expose assets to various risks. For example, future air transportation will depend heavily on computer network infrastructure for both data communication and system control. This heavy dependency on networking infrastructure exposes air transportation to the risk of network unavailability rendered by, for example, power failure.

During a meeting in Brussels in November 2009, experts used the IoT/RFID air travel scenario as a framework to identify assets likely to be owned by various stakeholders. After the discussions, the group agreed upon the following set of assets as significant within the 2015 air transportation context:

INTANGIBLE ASSETS

A1 – AUTOMATED RESERVATION, CHECKING-IN AND BOARDING PROCEDURES

This is a collection of business processes for remotely accepting and admitting flight bookings, checking in passengers for flights, controlling their entry into the restricted area of an airport and, finally, boarding the airplanes. Each airport and each airline has its own processes. These processes are largely similar but they also contain procedures unique to the process owners (different airlines). In an

airport, together with the state-operated screening processes, they constitute the overall air transportation airport business process. The expert group considered the value of this asset as high.

A2 – **ELECTRONIC VISA ISSUING PROCESS**

This is the state-owned process of issuing electronic visas to foreign visitors. This process also includes making available the status of visas to the air transportation check-in, security screening and border control processes. This asset has a high value

A3 – **LUGGAGE AND GOODS HANDLING PROCESS**

Owned by airlines, airports, service providers and airport shops, this is the logistic process of moving goods to and from and within the airport. The goods include passenger luggage, airport shop merchandise and airport facility supplies. In a larger context, it can also include logistic processes of airplane maintenance. The value of this asset is considered high.

A4 – **AUTOMATED ROADWAY TRAFFIC MANAGEMENT AND ASSISTANCE SYSTEMS**

IoT will also facilitate getting to the airport in 2015. In the context of our scenario, an automated traffic management system could provide applications such as smart routing or automated re-scheduling of passengers when there are flight delays. The value of this asset is considered high.

TANGIBLE ASSETS

A5 – **PASSPORT AND NATIONAL ID CARDS**

Owned by state agencies issuing these IDs and by the citizens, these are the new generation IoT smart IDs with embedded RFID, digital photos, and biometric information (e.g. fingers prints and iris patterns). The value of this asset is considered high.

A6 – **MOBILE "SMART" DEVICE**

Smart mobile personal devices owned by the passengers, such as cell phones and PDAs, will play a major part in the automation of future air transportation processes. These small computing devices will allow for the transmission of voice as well as data. Functions integrated in one device usually include those of a mobile phone, digital camera (working also as 2D barcode reader), NFC reader/tag, Bluetooth interface, LCD (2D barcode can be displayed), GNSS receiver, PDAs, laptops, e-book reader, etc. The devices may store the following data:

- Personal data
- Personal preferences
- Location data

- Electronic boarding passes
- Electronic visa
- Electronic luggage tags

They may also store and/or generate:

- Non-personal data
- Passports and national ID cards
- Passenger name record (PNR) data.

The value of this asset is considered high.

A7 – **HEALTH MONITORING DEVICES**

Owned by passengers, and possibly by airlines or airports, these implants and/or biosensors are critical assets in monitoring citizens' health. Examples include a body area network for blood pressure monitoring, allergy bracelet and seat-embedded motion sensors to detect lack of motion or over-agitated physically-challenged passengers. The value of this asset is considered to be very high.

A8 – **TRAVEL DOCUMENTS ON PAPER**

Owned by the travellers as well as the airlines, airline tickets and boarding passes may be printed on paper. It is also possible that an RFID tag can be imprinted on or in paper. The value of this asset is considered medium.

A9 – **RFID TAG, RFID READER AND BARCODE READER**

Depending on the nature of the document or device to which it is attached, the RFID could be owned by travellers solely, airlines, states, shop vendors, or suppliers. An RFID tag can be on a card or imprinted on papers (e.g., boarding passes or luggage tags). Readers are typically owned by establishments such as airlines, airports or airport shops to authenticate boarding passes in performing business transactions or detecting customer browsing behaviours. Readers could be at automatic check-in kiosks, security control points, airport shops/shelves, as well as within the smart devices owned by citizens or passengers. The value of this asset is considered medium.

A10 – **CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS**

Owned by the passengers or the issuing institutions, these cards may be with or without embedded RFID. Passengers use these assets to conduct transactions at various locations (e.g., check-in counters, airport shops, online purchase via smart devices). The value of this asset is considered high.

A11 – **OTHER RFID-ENABLED CARDS**

Owned by the passengers or the issuing institutions, these include transportation (e.g., metro/subway), frequent flyer and small purchase RFID-based cards. The value of this asset is considered medium.

A12 – **SCANNERS AND DETECTORS**

Owned by the airport or states, these assets refer specifically to security screening equipment such as liquid and gels (LAG) detectors, body scanners, etc. The value of this asset is considered high.

A13 – **NETWORK INFRASTRUCTURE**

Owned by the society and service providers, as well as airlines and airports, a computer network infrastructure provides the backbone of future air transportation operations. These include, but are not limited to, Wi-Fi, WiMax, conventional broadband, ZigBee, smart dust, mesh and ad-hoc networks, etc. The value of this asset is considered high.

A14 – **STATE DATABASES**

State databases contain data on passengers, including information originally created by states (e.g., in passports or visas) or later collected by the states during the air travel process (e.g., border entry/exit, citizen location information, citizen travel patterns, etc.). The value of this asset is considered high.

A15 – **COMMERCIAL AND OTHER DATABASES**

These databases contain passenger data held by businesses and entities other than state agencies. Many business functions such as market analysis or consumer pattern discovery drive the creation and collection of these potentially privacy-sensitive data. Such databases may contain the original raw passenger data or the further processed data sets. Both are considered important commercial assets in this future air transportation context. The value of this asset is considered high.

A16 – **ELECTRONIC AIRPORT GUIDES (AKA VISUAL INTERFACE DEVICE, VID)**

Owned by the airports or airlines, these devices are given to passengers who need help in navigating the airport and/or in translation functionality. Since these devices are likely to be location-enabled, the passenger's location data can be exposed through these assets as can be the fact that the passenger needs such a device. The value of this asset is considered low.

A17 – **LUGGAGE AND GOODS**

These items include passengers' luggage, airport shop merchandise, supplies for airport facilities (e.g., offices, restrooms) and, in a larger context, aircraft maintenance operation parts, tools or supplies. The value of this asset is considered medium.

A18 – **CHECK-IN INFRASTRUCTURE**

The infrastructure owned by the airlines and airports to facilitate passenger check-in. It comprises kiosks, desks, counters, luggage conveyer belts, flight status displays, etc. The value of this asset is considered high.

A19 – **AIRPORT FACILITIES**

These include all physical airport facilities such as garages, buildings, shops, stands, information desks, elevators, escalators, etc. The value of this asset is considered medium.

A20 – **CARS / VEHICLES**

This asset includes the cars and other vehicles used in the scenario to transport citizens. The value of this asset is considered high.

As mentioned in the methodology section above, the valuation of assets was based on the **impact areas** identified. The group agreed upon the following impact areas:

I1 – HEALTH / LIFE: Refers to the physical and psychological condition of an individual; his/her physical and psychological well-being and absence of disease.

I2 – TIME: refers to the time needed to get to the airport, check-in, clear security controls and board the aircraft.

I3 – HUMAN RIGHTS AND SOCIAL VALUES: include privacy, autonomy, non-discrimination, dignity, social inclusion, trusted human relationships, etc.

I4 – MOBILITY OF INDIVIDUALS: refers to the ability and potential of people to move across countries.

I5 – FINANCIAL / ECONOMICAL FACTORS: include costs for airlines, airports, companies and individuals

I6 – COMFORT, CONVENIENCE AND EASE OF ACCESS: refer to the extent to which services are provided and procedures followed without difficulties.

I7 – INTEROPERABILITY: refers to the interoperability between networks, sensors, devices, organisations, passengers and users. An IoT-like network will depend on a high level of interoperability between all of the different contexts and situations in which devices will need to communicate. Interoperable networks carry with them significant risks and issues, such as privacy, access controls, access to data, secondary and primary uses of data and data “shelf” life. In addition to these risks are technical problems such as standardisation in network protocols. Interoperable networks may also provide more room for fraud or other criminal activity in that compromising one part may allow

unauthorised access to another. The same is true if interoperability extends to interdependency in the case of failures and problems.

I8 – TRUST: is essential in all aspects of the scenario. Passengers must trust the information on their devices. Operators must trust personal data provided, and information provided to them by other operators. Trust is also needed in the automated procedures by airlines and airport operators. And border authorities must likewise trust in the systems to perform.

I9 –BUSINESS ACTIVITIES: includes all those activities performed by product vendors and service providers to generate revenues and earnings. Specifically, this impact refers to all non air transport related commercial activities within the scenario; these refer to commercial operations within the airport, such as duty free retail areas as well as those external to the airport such as commercial transportation entities.

5.2 MAJOR RISKS

Major risks have been categorised as follows:

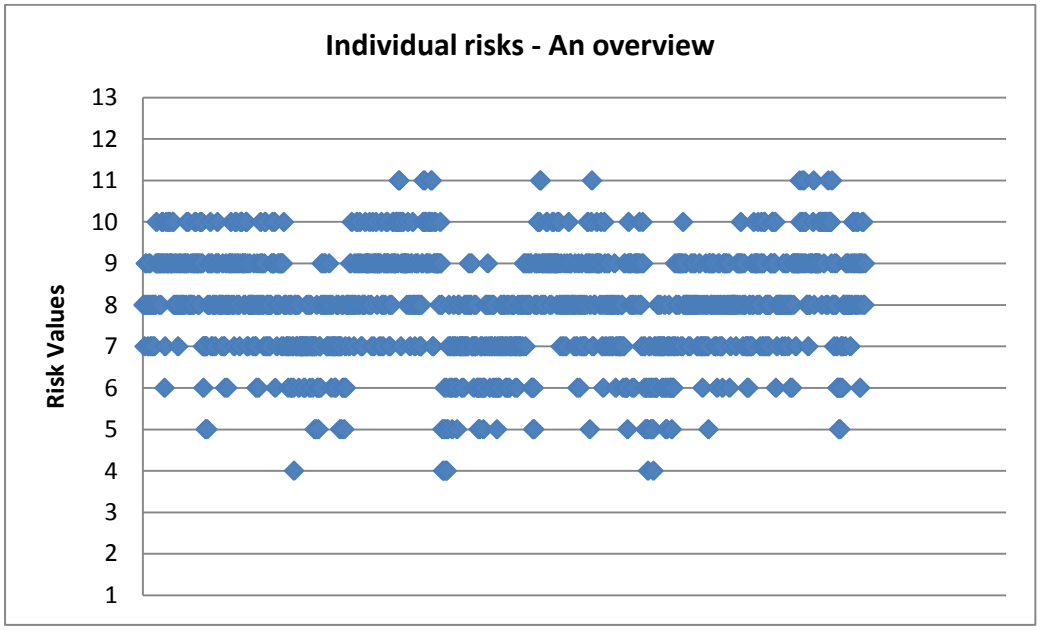
- Organisational and policy risks
- Socio-economic risks: including privacy issues
- Technical risks
- Legal risks

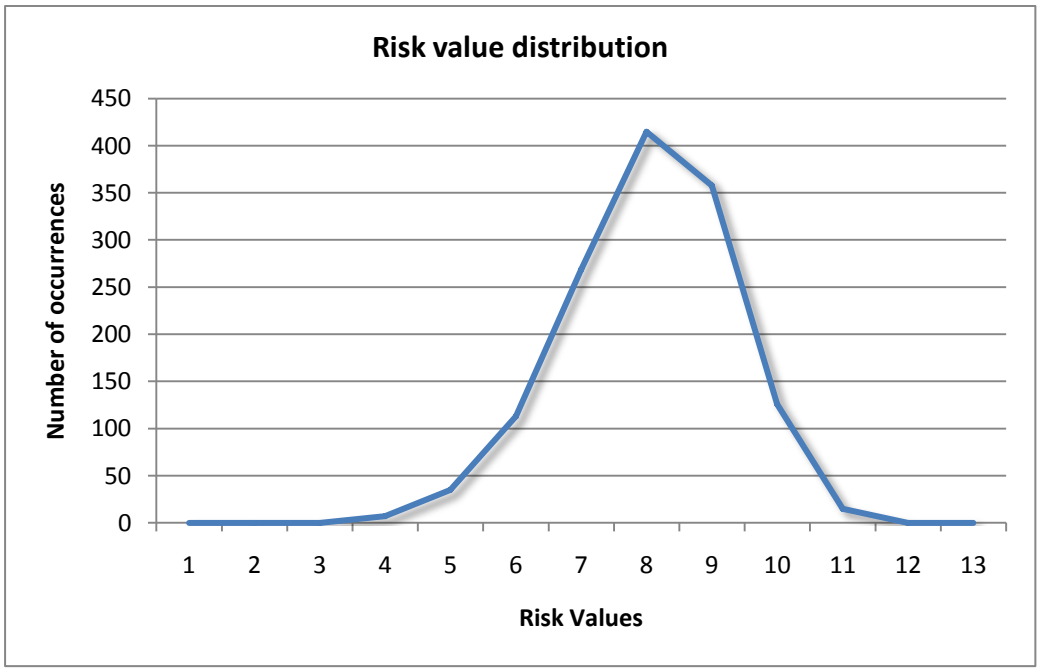
Within each category, risks are ranked according to their severity levels as indicated by the colour scale below.

Information Security Risk Measurement Scale												
Minimum Risk												Maximum Risk
1	2	3	4	5	6	7	8	9	10	11	12	13
VERY LOW		LOW			MEDIUM			HIGH			VERY HIGH	

Based on our detailed analysis which you can find in the excel spreadsheet of Annex III (*Risk Assessment*" tab), we have identified a total of 1306 individual risks. In the graphs below you can see an overview of the values of the risks identified (first graph) and a distribution of the individual risks (second graph); from the second graph, we can see that the majority of the risks of the risks identified

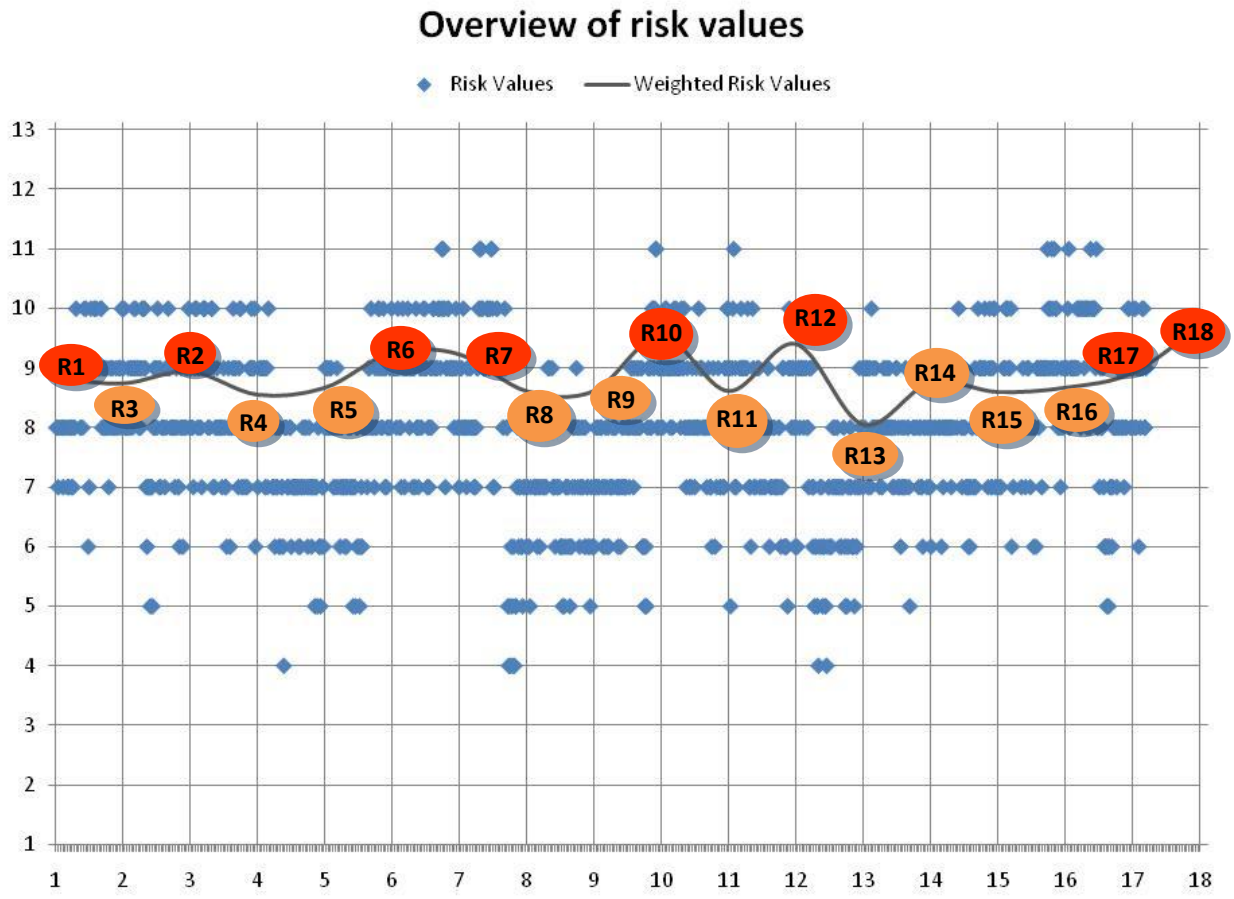
are ranked as **Medium** to **High;** it is noted however that there are individual risks that are considered Very High, and which you may find at the "Risk Assessment" tab of the excel spreadsheet of Annex III.





For presentation purposes, we have grouped these individual risks into 18 major compound risks, for which we have calculated a weighted risk value. All of the weighted risks also range from Medium to

High. The following figure gives a graphical representation of the risk values of the individual risks (*blue scatter dots*) and of their weighted values (*grey line*) for the 18 compound risks identified in this report, and which are indicated on the line: the reader can navigate to the risks in this document by clicking on the respective risk number, indicated on the graph.



In addition to a short description of the risk, the following items are identified for every risk in a table:

- **The affected assets** : as those have been identified in the previous section
- **The relative vulnerabilities and threats**: you can click on each item to navigate to Annex I for more information
- **Reference to other risks**: most of the risks identified are highly inter-related, so specific reference to other relevant risks is made. Again you may click on the item to navigate to the corresponding risk inside the document.

- **The risk level**: as mentioned above, since the risks identified here are a high level grouping of all the individual risks identified in our analysis (see the detailed analysis in the spreadsheet of Annex III), a weighted risk level is estimated and included in the risk description.

Organisational and policy risks

R1. Failure of reservation, check-in and boarding procedures: procedural / operational failures and other organisational interruptions

Affected assets	A1 – Automated reservation, checking and boarding procedures A5 – Passports and national ID cards A6 – Mobile "smart" devices A8 – Travel documents in paper A9 – RFID, RFID reader and barcode reader A12 – Scanners and detectors A13 – Network infrastructure A18 – Check-in infrastructure A19 – Airport facilities
Vulnerabilities	V1, V2, V3, V4, V5, V6, V7, V8, V9, V10, V11, V12, V13, V14, V15, V16, V18, V19, V20, V21, V22, V23, V24, V25, V26, V27, V28, V29, V31, V32, V33, V35, V36, V37, V38, V39, V40, V41
Threats	T1, T2, T3, T4, T5, T6, T7, T8, 1.1.1.1.1T9,T10,T11, T12, T13, T14, T15, T16, T17, T18, T19, T20, T21, T22, T23, T24, T25, T26, T27, T28, T29, T30, T31, T32, T33, T34
Related risks	R4, R7, R11, R13, R14, R15
Risk level [weighted average]	**HIGH**

Passengers and airlines may be unable to perform automated reservation, check-in, and boarding procedures due to procedural or operational errors, ill-designed procedures, introduction of erroneous data or even resource shortages from unexpected interruptions such as industrial action (e.g. strikes etc.). Some of these risks can be alleviated by means of technologies such as facial recognition, fingerprint scanning, but the overall effectiveness still depends on the original design as well as the operation and management of the screening processes.

R2. PROBLEMS IN ISSUING / CONTROLLING ELECTRONIC VISAS

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE "SMART" DEVICES A9 – RFID, RFID READER AND BARCODE READER A13 – NETWORK INFRASTRUCTURE A14 – STATE DATABASES A19 – AIRPORT FACILITIES
Vulnerabilities	V1V10V12V14V15V16V18V19V2V20V21V28V3V35V36V37V4V38V5V6V7V8V 9V40V41V34V31V23V39V11V24V25V26V27V22V31V13, V33
Threats	T6, T8, T11, T12, T13, T14, T27, T1, T22, T25, T28, T9, T10, T30, T2, T3, T5, T7, T16, T23, T26, T24, T4, T19, T20, T29, T15, T17, T18, T21, T31, T33, T32, T34
Related risks	R1, R4, R6, R7, R11, R8, R18
Risk level [weighted average]	**HIGH**

The risk of states' inability to issue and control the usage of electronic visas arises from system failures, procedural incompatibility, equipment failures, cyber attacks, identity theft or usage of erroneous data. As a result, citizens/passengers are unable to obtain an electronic visa for their travel.

R3. SECURITY SCREENING FAILURE

Affected assets	A9 – RFID, RFID READER AND BARCODE READER A12 – SCANNERS AND DETECTORS A13 – NETWORK INFRASTRUCTURE A19 – AIRPORT FACILITIES
Vulnerabilities	V1, V2, V3, V4, V5, V6, V8, V9, V10, V11, V14, V16, V19, V20, V21, V22, V23, V29, V30, V31, V32, V36, V37, V39, V41
Threats	T6,T8,T11, T12, T13, T14, T27, T1, T2, T5, T22, T24, T25, T28, T30, T10, T9, T7, T16, T19, T20, T29, T18, T31, T32, T33, T23, T3, T15, T17, T21, T4, T26, T34

Related risks	R6, R7, R9, R11, R13, R14, R15
Risk level [weighted average]	**MEDIUM**

This risk involves failure and compromise of passenger security screening process to detect weapons, explosives, liquids and gels due to malfunction of scanners, inconsistent procedures, malicious power failures, jamming, cyber infrastructure attacks, malicious insiders, and low social acceptance.

R4. INABILITY OF PASSENGERS TO TRAVEL DUE TO LOSS OF PAPER DOCUMENTS OR OTHER DELAYS / FAILURES IN CHECK-IN / PASSENGER IDENTIFICATION

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A3 – LUGGAGE AND GOODS HANDLING PROCESS A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE "SMART" DEVICES A8 – TRAVEL DOCUMENTS IN PAPER A9 – RFID, RFID READER AND BARCODE READER A12 – SCANNERS AND DETECTORS A13 – NETWORK INFRASTRUCTURE A14 – STATE DATABASES A17 – LUGGAGE AND GOODS A18 – CHECK-IN INFRASTRUCTURE A19 – AIRPORT FACILITIES
Vulnerabilities	V1, V10, V12, V14, V15, V21, V3, V37, V4, V5, V6, V7, V11, V32, V29, V23, V24
Threats	T8, T11, T14, T27, T22, T28, T9, T10, T30, T7, T23, T21
Related risks	R2, R7, R9, R12, R13, R14, R15
Risk level [weighted average]	**MEDIUM**

The risk is an inability to travel resulting from loss or compromise of paper-based travel documents and no back-up for the e-transportation process due to theft, misplacement, identity theft, and fraud.

R5. LOSS / MISHANDLING OF GOODS

Affected assets and value	A3 – LUGGAGE AND GOODS HANDLING PROCESS A9 – RFID, RFID READER AND BARCODE READER A17 – LUGGAGE AND GOODS
Vulnerabilities	V1, V2, V3, V6, V7, V10, V13, V14, V16, V17, V21, V22, V24, V30, V31, V33
Threats	T1, T2, T6, T7, T8, T9, T10, T11, T15, T20, T21, T22, T28
Related risks	R1, R4, R7, R9, R13, R14, R15
Risk level [weighted average]	**MEDIUM**

There are risks associated with the loss of luggage, personal goods, and airport store merchandise due to logistic handling system error, system components (e.g. RFID/readers) failures, social engineering, theft, cyber attacks, and general power failure. Such risks could also result from operation errors (e.g. RFID tags torn from the luggage) or unforeseen events (RF interference).

Socio-economic risks

R6. LOSS / VIOLATION OF CITIZEN/PASSENGER PRIVACY

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A3 – LUGGAGE AND GOODS HANDLING PROCESS A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE "SMART" DEVICES A7 – HEALTH MONITORING DEVICES A8 – TRAVEL DOCUMENTS IN PAPER A9 – RFID, RFID READER AND BARCODE READER A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS A11 – OTHER RFID-ENABLED CARDS A12 – SCANNERS AND DETECTORS A14 – STATE DATABASES A15 – COMMERCIAL AND OTHER DATABASES
Vulnerabilities	V1, V14, V18, V20, V21, V37, V4, V7, V9, V40, V41, V24, V31, V13, V22, V11, V3, V5, V23, V39, V33
Threats	T11, T12, T13, T2, T3, T10, T26, T15, T17, T18, T19, T20, T29, T31, T33, T32, T1
Related risks	R1, R2, R3, R4, R5, R7, R9, R8, R12, R14, R15, R17, R18
Risk level [weighted average]	**HIGH**

The natural characteristic of IoT air transportation is the prevalence of devices, sensors, readers, and applications which have the potential to collect a multiplicity of data types of individuals as they move through such environments. Many citizen air transportation data will be generated and collected for example as well as other forms such as location, purchasing habits, as well as other preferences stored for ease of use in systems. This leads to concerns over the potential compromising of citizen's privacy via collecting/surveillance/profiting of traveller's activity. Given the assumptions of an IoT scenario in terms of automation, interoperable networks, devices and databases as well as the proliferation of sensors we consider the risks to be high in this regard.

- Electronic passport/visa issuing data.

- Ticket purchase/check-in/travel pattern/partner/time/price travel data.
- Baggage handling data.
- Credit/debit/payment e-card and e-wallet transaction data.
- Citizen's air travel and commercial transaction patterns.
- Locations and correlation between location data of passengers.
- Health monitoring data, sharing of these data to potentially conflict-of-interest entities such as health insurance establishments.
- Correlation of travel data to all other online citizen data.
- Spamming and undesirable exposure to solicitations brought upon by services such as LBS.

R7. COMPROMISE AND ABUSE OF STATE-OWNED CITIZEN/PASSENGER DATABASES (ALSO AN *ORGANISATIONAL AND POLICY RISK* AND *TECHNICAL RISK*)

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A5 – PASSPORT AND NATIONAL ID CARDS A8 – TRAVEL DOCUMENTS IN PAPER A9 – RFID, RFID READER AND BARCODE READER A13 – NETWORK INFRASTRUCTURE A14 – STATE DATABASES
Vulnerabilities	V1, V2, V3, V4, V7, V9, V10, V11, V14, V16, V18, V19, V20, V21, V24, V27, V28, V31, V34, V35, V36, V37, V38, V39, V40, V41
Threats	T1, T2, T3, T6, T7, T9, T10, T11, T12, T13, T15, T24, T30, T31, T32, T33, T34
Related risks	R5, R6, R9, R8, R12, R13, R14, R15, R17, R18
Risk level [weighted average]	**HIGH**

Citizen/passenger data are generated, and can also be potentially collected, starting from the very beginning of ID/passport issuing stage all the way through to visa application, ticket purchase, check-in, security-screening and boarding, as well as border/immigration control processes. States provide

and collect these data to facilitate the future air transportation process. However, these data also detail citizens' mobility patterns and as such open the possibilities for abuses through practices such as profiling, unwarranted monitoring or data in governmental databases being compromised due to accidental loss, fraud or other illicit or criminal activity. Of particular concern here would be the storage and collection of biometric data. Linking identity to biometrics has often been raised as being problematic due to the risks of such data being compromised. While passwords or pins can be changed this is not true if an identity is compromised utilising biometrics. Subsequently, there are different types of risks associated with the databases owned by the states regarding citizens' air transportation activities.

- Upon the compromise, corruption or unavailability of the state-owned citizen air transportation databases, the authorities will not be able to issue travel credentials, authenticate validity of the IDs in providing critical support like boarder control, security screening and airline check-in processes.
- Via the collection of citizen travel data, states potentially will gain enhanced ability to perform citizen surveillances via both real-time monitoring, as well as offline travel pattern analysis. This surveillance could be legal or illegal depending on the local and EU laws. Misuse and abuse of the citizen data could also come from state employees or people with privileged system access in performing criminal activities, such as illegal substance trafficking, extortion, or sale of the privileged data for commercial gains.
- Cross compilation with various open and limited (secure) databases opens the possibility of gaining a capability for additional citizen surveillance.
- Malicious perpetrators can also mislead state surveillance by feeding intentionally fake and erroneous data. A potential distributed denial-of-service (DDOS) can also be launched via the sensory infrastructure.
- There is a risk of sharing and sale of personal data by commercial entities such as LBS providers who hold passengers' location data.
- Loss or compromised biometric data represents unique and potentially highly damaging risks in terms of identity theft.
- Inaccuracies in data may mean that citizens may be inaccurately identified as 'suspicious' (false positives), while real perpetrators may not be appropriately detected (false negatives). Automated procedures utilising biometrics in checking databases may not be the ultimate panacea for identity related problems issues.

R8. REPURPOSING OF DATA / MISSION CREEP

Affected assets	**A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES** **A2 – ELECTRONIC VISA ISSUING PROCESS** **A5 – PASSPORT AND NATIONAL ID CARDS** **A6 – MOBILE "SMART" DEVICES** **A7 – HEALTH MONITORING DEVICES** **A9 – RFID, RFID READER AND BARCODE READER** **A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS** **A11 – OTHER RFID-ENABLED CARDS** **A14 – STATE DATABASES** **A15 – COMMERCIAL AND OTHER DATABASES**
Vulnerabilities	V10, V11, V14, V16, V18, V19, V20, V21, V34, V35, V37, V39, V40, V41
Threats	T3, T8, T11, T12, T13, T26, T31, T32, T33, T34
Related risks	R6, R7, R9, R12, R15, R17, R18
Risk level [weighted average]	**HIGH**

The more data is collected, the more likely it is that data controllers and others will dream up ways in which the data can be repurposed. It is an almost inevitable tendency for people to maximise opportunities and minimise costs (by spreading costs over a wider range of missions). Usually ideas for these new opportunities for repurposing data occur only after the collection of data has begun. Thus, the risk is that data will be used for purposes in addition to those originally specified. Repurposing of data can, however, also be in the cards before data collection begins, e.g., law enforcement authorities or intelligence agencies may seek access to data collected by others for specified purposes. In some cases, the repurposing may seem relatively innocuous, for he massive collection of data, might result in the data used for other purposes that they were initially intended for. To provide an example, Richard's dietary habits or requirements might end up being used as a basis to provide personalised advertisement to him or even by insurance companies to negotiate the amount of premiums, etc. The point is, however, that such repurposing is without the user's consent and contravenes the provisions of the Data Protection Directive. Repurposing is one of the most insidious activities against privacy and data protection. It undermines trust and confidence.

This represents a critical risk for IoT enabled environments. This is not just in relation to the violation of individual rights to privacy but also may impact on wider social and public acceptance. To draw

parallels with other ICT developments 'spam' or junk mail remains one of the most negatively perceived impacts of increased internet access and usage by individuals. If IoT devices are all potentially areas where targeted or personalised messages can be received by individuals then 'spam' will take on whole new connotations. The proliferation of sensors recording data likewise is problematic in this regards. It remains unclear as to how privacy can be maintained and how practices of profiling and data mining can be curtailed. A pessimistic glance at the situation today often reveals flagrant disregard on the part of companies, and governments, for the privacy of individuals either accidentally or with specific intent.

R9. HEALTH-PROCESS RELATED CONCERNS

Affected assets	A6 – MOBILE "SMART" DEVICES A7 – HEALTH MONITORING DEVICES A9 – RFID, RFID READER AND BARCODE READER A13 – NETWORKS A15 – COMMERCIAL AND OTHER DATABASES
Vulnerabilities	V1, V2, V3, V4, V5, V6, V7, V8, V9, V10, V11, V13, V18, V19, V20, V21, V22, V23, V24, V26, V27, V28, V31, V33, V37, V38, V39, V40, V41
Threats	T1, T2, T5, T6, T8, T9, T11, T12
Related risks	R6, R7, R9, R8, R12, R14, R15, R18
Risk level [weighted average]	**HIGH**

Rapid advancement of ICTs has led to an increasing number of portable devices and sensors (Internet of Things) that enable various e-Health scenarios such as remote patient monitoring. It is expected that the "Internet of Things" will create significant impact to future delivery of healthcare. However, high dependability on the IoT technologies in e-Health creates significant security and privacy risks. For example, in the case of Richard, his medical data is not collected by healthcare providers in a controlled medical environment using certified medical devices, but by his own devices while he is on the move or devices in the airplane. This creates several significant risks related to the quality of the healthcare he receives, as his healthcare relies very much on the IoT technology. In particular, there are risks with respect to patient identification and reliability of collected information. It is important that: (i) the patient is properly identified (for example by the airplane sensors/devices which is related to V32 and V36) so that the measurements done by external sensors are associated with the right

person, and (ii) the measurements are taken with a reliable, certified sensor/device and that they are not modified on the way to the healthcare service (related to T10, T22, V7, V31, V33).

Another group of related risks are concerned with patient privacy. Once sensitive information about an individual's health is uncovered and social damage is done, there is no way to revoke the information or to compensate the individual appropriately for this damage. Next to that, the modern eHealth solutions based on IoT are heading towards open, interconnected environments which collect and rapidly exchange sensitive data making the problem more difficult. There are several threats (such as T3, T5, T8, T12), as well as vulnerabilities (V9, V19, V33, V38, V39) that can be exploited to endanger patient privacy, compromise his health records or misuse his health information for non-legitimate purposes (e.g. marketing, see also risk R8). Furthermore, there is a risk that the patient/consumer is not in control on how his data is shared and used due to the lack of proper end-to-end security mechanisms, not usable policy/consent specification techniques and the lack of respect to the transparency principle.

R10. COMPROMISE AND ABUSE OF COMMERCIALLY-OWNED CITIZEN/PASSENGER DATABASES (ALSO AN *ORGANISATIONAL AND POLICY RISK*)

Affected assets	A6 – MOBILE "SMART" DEVICES A7 – HEALTH MONITORING DEVICES A9 – RFID, RFID READER AND BARCODE READER A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS A11 – OTHER RFID-ENABLED CARDS A13 – NETWORK INFRASTRUCTURE A15 – COMMERCIAL AND OTHER DATABASES
Vulnerabilities	V1, V2, V3, V4, V5, V9, V10, V11, V13, V18, V19, V20, V21, V24, V27, V28, V33, V34, V35, V37, V38, V39, V40, V41
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T13, T15, T16, T18, T20, T22, T24, T25, T27, T28, T31, T32, T33, T34
Related risks	R1, R5, R6, R7, R8, R12, R13, R14, R15, R17, R18
Risk level [weighted average]	**MEDIUM**

There are also different types of risks associated with the databases owned by commercial entities that collect and generate citizen/passenger data in future air transportation. These entities include,

but are not limited to, airlines, shuttle services, parking garages, baggage handling third-party companies, airport stores and various wired and wireless air transportation relevant service providers (e.g., travel planning, LBS-enabled travel assistance). Commercial interests such as operational efficiency, market analysis, consumer profile (anonymous or not) identification, are the major motivation behind such databases. Subsequently, there are also different types of risks associated with these types of databases.

- The compromise and unavailability of these databases will render the intended business activities ineffective. In the case of airlines, without the passenger register/ticketing/check-in databases, the entire flight processes will be severely impacted. For shuttle services, similar passenger database failure will also significantly impact their passenger transportation process.
- Similar to the state-owned databases, these commercial databases also contain passenger travel patterns. Additionally, consumer and personal activities such as airport store purchases, travel partners, hobbies and interests, interactions with other people, time of travel, dietary preferences and health conditions can all be collected. As such, these databases are open to potential abuses by commercial entities, hackers and malicious insiders with privileged accesses.
- Cross compilation with other online Internet databases to gain additional consumer behaviour knowledge is a risk.
- Similar to the state-own databases, erroneous and fake data could also be purposely generated by the malicious perpetrator to compromise the integrity of the database for devious commercial purposes.
- It is unclear how such databases will be regulated within existing or future data protection regulatory frameworks. The challenges of data chopping, data mining and data outsourcing are already on the agenda for European Data Protection authorities and respective national organisations. In an IoT environment risks expand exponentially due to the ease with which data can be collected, stored and moved around.
- Unobtrusive collection of data, while offering benefits to commercial operators (such as highlighting Richard's preferences discreetly in the scenario) raise critical questions in relation to consent. It would appear that in many IoT scenarios consent is assumed in relation to data sharing and data collection, yet this is against the provisions of data protection directives where consent must be explicitly given for the collection of data and its processing clearly explained to data subjects.
- Likewise by expanding the commercial scope and value of transactions within an IoT environment then the value of being able to illicitly gain access to individuals data and credentials increases. It can be expected, just as with increased internet use has led to the emergence of identity theft as a

major source of criminal activity, that new or refinements of existing methods of criminal activity will emerge.

Some of these risks could be alleviated by using the digital anonymous technology to avoid, for example, Richard's revealing his identity while paying for the shuttle service which takes him to the airport. As such, the implementation and design of the systems and their integration play a big part in the mitigation of these risks.

R11. USER FRUSTRATION AND LOW USER ACCEPTANCE

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A3 – LUGGAGE AND GOODS HANDLING PROCESS A4 – AUTOMATED ROADWAY TRAFFIC MANAGEMENT AND ASSISTANCE SYSTEMS A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE "SMART" DEVICES A7 – HEALTH MONITORING DEVICES A8 – TRAVEL DOCUMENTS IN PAPER A9 – RFID, RFID READER AND BARCODE READER A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS A11 – OTHER RFID-ENABLED CARDS A12 – SCANNERS AND DETECTORS A16 – ELECTRONIC AIRPORT GUIDES A17 – LUGGAGE AND GOODS A18 – CHECK-IN INFRASTRUCTURE A19 – AIRPORT FACILITIES A20 – CARS / VEHICLES
Vulnerabilities	V1, V2, V3, V4, V5, V6, V7, V9, V10, V11, V12, V14, V17, V18, V19, V20, V21, V22, V23, V24, V27, V28, V29, V30, V32, V33, V34, V35, V36, V38, V39, V40, V41
Threats	T1, T2, T5, T6, T7, T8, T9, T10, T11, T13, T14, T15, T20, T22, T23, T24, T30, T31, T33, T34
Related risks	R1, R2, R4, R5, R6, R7, R9, R8, R12, R9, R13, R14, R15, R16, R17, R18

Risk level [weighted average]	MEDIUM

The sometimes complex procedures and sophisticated devices may overwhelm users, the travellers that are not IT friendly or even airport / airlines personnel can be potentially included in this category of persons. This might result in errors in procedures or even failure to use them at all, but it may also result in serious user frustration, which may be further intensified when devices fail to work properly (e.g. give many false positives etc.). This may further raise the risk of low acceptance of the new technologies and applications. As it stands there is little large scale independent empirical research upon which to infer any conclusions as to how publics will interact or engage with IoT enabled environments. Linked to this is the observation that outside of research documents, or scenarios like these, little to no work has been undertaken in terms of raising public awareness or engaging with publics on the proposed developments that IoT will bring.

The scenario assumes that technologies are relatively widely used and that they are acceptable for most, even to the extent of helping Elena navigate the confusing (to her) process of boarding her plane. Yet this remains a substantial assumption. Likewise Elena while having difficulties with IT may have had further problems compounded by disability, age, a nationality other than European all of which would further complicate her time in the airport. A level of refusal to use any IoT enabled services must also be considered [though unlikely if assumptions in the scenario such as with PNR and entry/exit automated systems occur]. Providing an opt-out solution for individual citizens from these environments must be considered and can represent a significant challenge for states, airports as well airline operators.

R12. AGGRESSIVE PROFILING AND SOCIAL SORTING LEADING TO SOCIAL EXCLUSION

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE "SMART" DEVICES A7 – HEALTH MONITORING DEVICES A9 – RFID, RFID READER AND BARCODE READER A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS A11 – OTHER RFID-ENABLED CARDS A14 – STATE DATABASES A15 – COMMERCIAL AND OTHER DATABASES
Vulnerabilities	V1, V4, V7, V10, V14, V18, V19, V20, V21, V34, V35, V37, V39, V40, V41
Threats	T3, T8, T9, T10, T11, T12, T13, T26, T31, T32, T33, T34
Related risks	R6, R7, R8, R9, R17, R18
Risk level [weighted average]	**MEDIUM**

Since we are talking about an Internet of Things scenario, the collection of data and profiling are both facts and not necessarily negative per se. However, excessive data collection and profiling, will inevitably lead to social sorting practices for commercial or other purposes, leading to exclusion of people from accessing services. Like repurposing of data and mission creep, social sorting in an increasing temptation with increasing data collection. It may seem at first glance that social sorting enables governments to more efficiently provide services and to better target citizens who might be at risk, but closer examination shows that social sorting often comes with evils, consumers who are targeted because they offer better commercial prospects inevitably means that other consumers are ignored or marginalised. Social sorting enables insurance companies, airlines and many enterprises to provide some deals to their valued customers and not to others. Even fast-tracking in airports is a form of social sorting. In the long run, social sorting risks damaging notions of equality and democracy.

Some examples of this can already be seen in the increasing proliferation of 'trusted traveller' schemes where for a financial premium people can avoid the normal queues and delays associated with other types of travellers at European airports.

Other technologies referred to in the scenario, such as for example, biometric related devices may even just exclude by the nature of how they function. In this instance both the very old, the young may have problems with fingerprinting or iris scans [eye disease etc].

Profiling and data mining within an IoT scenario such as the one described is massively increased as a potential harm to individuals due to the ease to which data can be collected, stored, shared and analysed. Over reliance on the content of databases [such as security related ones] may likewise be problematic in instances where mistakes are made. The recent attempted bombing of a flight bound from Schiphol to Detroit in December 2009[12] also illustrates, by virtue of the fact that would-be bomber's status on a no-flight list was not updated and highlights the difficult balancing act between individual rights to privacy and the requirements of security that will exponentially increase as databases become ever larger and more sophisticated within IoT environments. Individual access to remedy incorrect data being stored on them should be seen as a key goal yet it represents a challenge given the wide range of potential databases that might be in existence with the widespread implementation of IoT technologies and systems.

Technical Risks

R13. Air transportation process rendered unavailable: overall computing network infrastructure failure (hardware and device failures, natural and environmental causes)

Affected assets	A13 – Network infrastructure A18 – Check-in infrastructure A19 – Airport facilities
Vulnerabilities	V2, V3, V8
Threats	T1, T28, T22, T24
Related risks	R1, R3, R2, R4, R6, R11, R14
Risk level [weighted average]	MEDIUM

[12] http://blog.newsweek.com/blogs/declassified/archive/2009/12/26/why-bombing-suspect-may-have-been-absent-from-u-s-no-fly-list.aspx

This risk involves computer and network infrastructure failure that leads to major paralysis of the overall automated air transportation process. This includes both the wired and wireless infrastructure as well as critical components (e.g. servers, routers, software services). Many of these sensors and readers require wired or wireless infrastructure to deliver their data. Additionally, the whole system may require network access to backend servers. The current internet infrastructure is an integral part of providing future IoT air transportation. Depending on the degree of computing network infrastructure failure, the impact to air travel could be severe.

An important factor that makes this failure even more severe and more likely is the excessive reliance on the technological infrastructure that is characteristic of this new environment. There may be an over-reliance on passengers' smart devices as the foundation of future air transportation, which becomes apparent in the event of an overall system failure due to compromise of these smart devices and loss of functionality due to wireless/IT infrastructure failure, equipment/reader malfunctions, theft, devices' weak access control, jamming, social engineering or cyber attacks.

Over-reliance may also become apparent with paralysis and interruption of the air transportation process resulting from malfunction of critical technology components such as barcode scanners, RFID tags and RFID readers due to electro-magnetic interference, vibration and age. As in the case of passenger authentication via biometric authentication, fingerprint and iris scanners may be ineffective to certainly aged passenger or people with finger injury or damage[13]. Such risks arise from non-malicious "malfunction" of biometric sensors and are facts of technology limitations. Manual processes can be devised to address them.

Hard failures could result from hardware (e.g., kiosks, terminals, readers, RFID) malfunctions, virus attacks, denial-of-service/flood attacks or drive-by downloads of malicious code. Also, for portable devices, the battery could be discharged rendering the device useless.

Airport facilities such as garages, driveways, check-in halls, screening/border-controls areas, restrooms, lighting, HVAC (Heat, Ventilation, and Air Conditioning), plumbing, elevators/escalators, gates, public address systems are all critical parts of the future air transportation process. Many of these facilities can and will be integrated with IoT of the future – for example, HVAC (as well as plumbing systems) can be integrated with various temperature, vibration or pressure sensors at strategic locations. Data from these sensors could be read or accessed through mobile RFID readers or smart phones. Under such circumstances, the physical failure of the facilities is tightly linked with the

[13] However, it should be mentioned that the percentage of people that cannot be fingerprinted due to insufficient quality of fingerprints is by some sources estimated as about 2%, however this number seems exaggerated; for a detailed discussion see the NIST report [24]

management of the IoT devices, in addition to risks arising from structural, electrical or terrorist causes.

R14. ELECTRONIC IDENTIFICATION FAILURES AND IDENTITY THEFT

Affected assets	A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE 'SMART' DEVICES A9 – RFID, RFID READER AND BARCODE READERS
Vulnerabilities	V1, V10, V12, V14, V15, V16, V18, V19, V2, V20, V21, V28, V3, V35, V36, V37, V4, V38, V5, V6, V7, V8, V9, V40, V41, V24, V31, V13, V22, V25, V26, V27, V11, V31, V32, V29, V34, V23, V39, V17, V33, V30
Threats	T6, T8, T11, T12, T13, T14, T27, T1, T22, T25, T28, T9, T10, T30, T2, T3, T5, T7, T16, T23, T26, T24, T4, T19, T20, T29, T15, T17, T18, T21, T31, T32, T33, T34
Related risks	R1, R2, R3,R5, R6, R7, R9, R11, R9, R13, R15
Risk level [weighted average]	**MEDIUM**

This risk involves compromise, loss of function and theft of RFID-embedded passport and national ID cards due to system, device or equipment malfunction, identity theft, social engineering, RFID cloning, cyber attacks and lack of remote revocation process. Identity theft poses a risk not only to those whose identities are "stolen", but to commercial and governmental undertakings as well, for example, fraudulent use of another's identity may impact banks and credit card companies as well. Identity theft creates a social burden, for example, on law enforcement authorities who try to combat such fraud as well as policy-makers who are obliged to divert time and resources from more socially productive uses. Hence, identity theft is a drag on our societies and economies as well as deleterious to the individuals directly affected.

R15. REALISATION OF MALICIOUS ATTACKS (THEFT, COMPROMISE OF SYSTEMS ETC.)

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A6 – MOBILE "SMART" DEVICES A9 – RFID, RFID READER AND BARCODE READER A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS A11 – OTHER RFID-ENABLED CARDS A12 – SCANNERS AND DETECTORS

	A13 – NETWORK INFRASTRUCTURE A14 – STATE DATABASES A15 – COMMERCIAL AND OTHER DATABASES A19 – AIRPORT FACILITIES A20 – CARS / VEHICLES
Vulnerabilities	V1, V2, V3, V4, V5, V9, V10, V11, V13, V14, V16, V21, V24, V25, V26, V27, V28, V31, V33, V38
Threats	T1, T2, T4, T5, T6, T7, T8, T9, T15, T16, T17, T18, T19, T20, T21, T24, T25, T29
Relation with other risks	R2, R3, R6, R7, R9, R11, R9, R13, R14, R16
Risk level [weighted average]	**MEDIUM**

This risk involves inconveniences and failure to conduct air transportation business transaction processes due to the loss, theft, unauthorised access, rogue cards and/or readers, attacks, spoofing and incompatibilities of both RFID and non-RFID embedded credit, debit and/or payment e-cards and e-wallets. This risk is, of course, directly linked with others, for example, realisation of malicious attacks on the infrastructure and systems might render the services unavailable or it might lead to identify theft.

R16. FAILURE OF VEHICLES AND GROUND TRANSPORTATION INFRASTRUCTURE

Affected assets	A4 – AUTOMATED TRAFFIC MANAGEMENT A6 – MOBILE "SMART" DEVICES A9 – RFID, RFID READER AND BARCODE READER A20 – CARS / VEHICLES
Vulnerabilities	V2, V3, V4, V5, V6, V10, V12, V13, V17, V24, V22, V31, V33, V37, V38
Threats	T9, T22, T1, T2, T5, T7, T17, T18, T19, T20, T24,T28
Related risks	R11, R15
Risk level [weighted average]	**MEDIUM**

Ground transportation is an important feature in the future IoT air transportation scenario. Getting passengers and goods in and out of the airports, garage parking and effective traffic control all require cohesive integration of vehicles and ground transportation infrastructure. Faults and malicious attacks (e.g., blocking, jamming, side channel attacks, rogue readers and RFIDs, physical RFID destruction) could significantly impact air transportation, creating traffic jams and accidents. Vehicle systems as well as communication infrastructure are evolving and are useful to improve the efficiency and robustness of ground transportation systems, but at the same time, if failing or manipulated, they may induce new risks. Standards and designs of these systems and how they could integrate with the future air transportation process need to be managed effectively to minimise any consequent risks.

Legal Risks

R17. Legislation lagging behind rapid technological advancements

Affected assets	A1 – Automated reservation, checking and boarding procedures A2 – Electronic visa issuing process A5 – Passport and national ID cards A6 – Mobile "smart" device A10 – Credit cards, debit cards, payment cards, e-wallets A11 – Other RFID-enabled cards A12 – Scanners and detectors A14 – State databases A15 – Commercial and other databases
Vulnerabilities	V21, V37
Threats	T2, T3, T5, T6, T7, T8, T9, T10, T11, T12, T13, T14, T16, T17, T18, T19, T20, T23, T25, T28, T29, T31, T26, T29, T30, T32, T33, T34
Relation with other risks	R6, R12, R18
Risk level [weighted average]	**HIGH**

The rapid advance of technology is at variance with the slower pace of the legislative processes, which may lead to serious legal gaps in a future environment of Internet of Things, particularly in the context of air travel. These gaps pose a big challenge to Member States and the European Institutions to

tackle, since inadequate legal protection may have severe negative impacts on the everyday lives of European citizens.

R18. NON-COMPLIANCE WITH DATA PROTECTION LEGISLATION

Affected assets	A1 – AUTOMATED RESERVATION, CHECKING AND BOARDING PROCEDURES A2 – ELECTRONIC VISA ISSUING PROCESS A4 – AUTOMATED ROADWAY TRAFFIC MANAGEMENT AND ASSISTANCE SYSTEMS A5 – PASSPORT AND NATIONAL ID CARDS A6 – MOBILE "SMART" DEVICE A7 – HEALTH MONITORING DEVICES A9 – RFID, RFID READER AND BARCODE READER A10 – CREDIT CARDS, DEBIT CARDS, PAYMENT CARDS, E-WALLETS A11 – OTHER RFID-ENABLED CARDS A12 – SCANNERS AND DETECTORS A14 – STATE DATABASES A15 – COMMERCIAL AND OTHER DATABASES A19 – AIRPORT FACILITIES A20 – CARS / VEHICLES
Vulnerabilities	V18, V19, V20, V39, V40, V41
Threats	T2, T3, T4, T6, T7, T8, T9, T10, T11, T12, T15, T21, T23, T25, T29, T30, T31, T32, T33
Relation with other risks	R6, R7, R9, R12, R17
Risk level [weighted average]	**HIGH**

Currently there is a strong data protection legislative framework in place, which is likely to be adapted by 2015 to better deal with the challenges posed by the technological developments, such as the Internet of Things. Nevertheless, there are certain concerns and risks relating to the processing of personal data, as seen from the vulnerabilities and threats presented in the table above. Some of them arise from the challenge of assuring compliance with the legislation, since as we experience every day it is not something easily achieved.

5.3 IMPLEMENTED CONTROLS IN SCENARIO 2015 – *ASSUMPTIONS MADE*

The following table presents existing controls envisaged in the scenario that is assumption of controls implemented at the time the scenario takes place. Notably, assuming that these controls are in place decreased the value of some of the vulnerabilities identified that would have been higher if this assumption was not made.

It is therefore noted he identification of these envisaged controls was considered necessary so as to make the scenario more reality-checked: a certain level of protection had to be assumed. In view of this, what makes the presentation of this control very important is that these assumed implemented controls may also serve as **indirect recommendations** of the IoT/RFID group, since they have been deemed as a *sine-qua-non* in such an environment. Additional recommendations to address the risks that are identified even after the application of these measures, are presented in the next chapter.

Control description	Control category	Control nature	Affected assets	Explanation of control
Multiple ways of getting to the airport (personal vehicle, buses, taxis, trains etc): intermodality	Containment and Recovery	Semi Automated	A1. Automated reservation, checking and boarding procedure	Modern airports are served by a variety of infrastructure methods, including rail, bus, and car. Should passengers have difficulties in arriving at the airport utilising one means of transport, other means can be expected to function as replacements. Further improvements in managing traffic flows using different types of transport can by 2015 be expected to have improved utilising IoT based technologies and improvements in co-ordinated traffic management systems. This will allow for effective contingency plans for passengers in cases of emergencies as well as maintain a range of choices in transport that passengers can exercise. It will also allow airports to manage traffic flows to and from the airport through predicting passenger numbers based on pre-booking information, and for example ensuring extra buses are in operation at busy times.

Control description	Control category	Control nature	Affected assets	Explanation of control
Comparison of individuals physical traits with those documented on a valid official document (passport, national ID card, crew pass, personnel pass) for identification and authentication purposes	Preventive	Manual	A1. Automated reservation, checking and boarding procedure	Passports, even biometric ones, continue and will continue to contain traditional means of identifying individuals such as photographs. Likewise for other forms of identification, such as ID cards biometrics may not be included or used, either as they are legacy forms of identification or biometrics were deemed not to be a requirement. Some airports have already issued biometric personnel passes and this trend can be expected to continue through to 2015. There will though it is assumed here be a continued need for some individuals to be checked manually by airport staff, for individuals lacking a biometric form of identification and in cases of problems with automated biometric identification. Examples here might include very young children, who while having passports would not be in possession of viable biometric forms of identification.
Automatic authentication of passengers by means of their biometric features	Preventive	Automated	A1. Automated reservation, checking and boarding procedure	Automated biometric gates are an increasing feature of airports currently, examples include the Privium system at Schipol as well as automatic gates at Heathrow's terminal 5. Biometric identification refers to authenticating and verifying individuals by means of a unique physiological feature (biometric) such as iris, face or fingerprint. By 2015 it is assumed that biometric recognition will be in widespread use at airports. Increased effectiveness in their ability to correctly identify people is also

Control description	Control category	Control nature	Affected assets	Explanation of control
				assumed to be achieved by 2010. This system will ensure efficient management of passengers proceeding through the boarding process and reduce risks of unauthorised persons gaining access to areas (through automated barrier gates etc). For airports the control will allow for labour efficiencies and reduce queues associated the manual checking of ID at points throughout the airport.
Authorisation of passengers by a paper boarding pass and verified by the airline personnel	Preventive	Manual	A1. Automated reservation, checking and boarding procedure	Current practice in airports is for at least two manual checks by airline personnel of passengers boarding cards (at departure gates and at the entrance of the airplane). While the scenario assumes an automatic boarding procedure it is expected that manual checking can still be implemented in cases of system failure or problems with passengers utilising the automatic procedures. This will be aimed at preventing passengers boarding the wrong plane, unauthorised persons who are flagged by the automatic systems to be further investigated as well as assisting passengers who may have difficulties with the automatic process.
Authorisation of passengers by electronic boarding pass verified by the departure control system of the airline	Preventive	Automated	A1. Automated reservation, checking and boarding procedure	Automatic checking of boarding cards at some points of the check in procedure are a feature of some airports already (Heathrow, Manchester). It is assumed that with the introduction of a DCS system this practice will supplant manual checks other than those required by system failures or problems encountered by passengers in utilising

Control description	Control category	Control nature	Affected assets	Explanation of control
				the automatic process. An alarm mechanism is incorporated into various parts of the DCS to ensure manual checking where problems occur. Automated gates and doors will refuse to open and an alarm sound when unauthorised individuals are detected. Ideally, for passengers that lose their way or that find themeselves in the wrong place spoken commands or messages delivered to their smart devices will direct them to their proper departure gate. Continued sounding of the alarm will result in a notice for airline or airport personnel to attend the incident.
Valid crew or airport personnel pass with digital photo	Preventive	Automated Manual	1. Automated reservation, checking and boarding procedure	Automatic face recognition technology is assumed to have advanced by 2015 to be a suitable method of screening valid crew and airport personnel. However as with other existing forms of identification crew or airport personnel passes may not be biometric based. Although biometric forms of ID are increasing in use at airports, visitors to airports for work purposes (perhaps contract work which cannot be performed by existing staff) or temporary workers for whom biometric enrolment may not be practical on economic grounds for airports may continue to utilise non-biometric forms of identification such as passes incorporating digital photos. It is assumed here that automatic checking will occur at entry/exit points to the airport, to prevent unauthorised access

Control description	Control category	Control nature	Affected assets	Explanation of control
				to non-public areas and within departure areas. Alarm mechanisms are incorporated in order to detect and alert airport staff to problems or unauthorised access.
Security checks in smart corridors with metal detectors, EDS and LAG detectors	Detective Preventive	Automated	A1. Automated reservation, checking and boarding procedure	Security checks are a critical feature of modern airports. Currently a mixture of manual and automatic procedures are performed in most settings. It is expected that by 2015 that the security check process will be almost wholly automated in terms of scanning and screening passengers. Corridors are equipped with alarm systems, where objects are detected which are hazardous or otherwise prohibited these alarms will sound and security personnel can intervene in order to perform thorough checks on the individual involved. Such alarms can be silent, being a message communicated solely to security staff in certain instances to reduce the risk of individuals committing dangerous acts or being a hazard to others. It is assumed that devices within smart corridors comply with data protection legislation as well as other relevant legislation (such as security procedures).
Airport security monitoring and emergencies identification through the usage of smart devices	Detective Corrective	Automated	A1. Automated reservation, checking and boarding procedure	It is assumed in the scenario that a network of sensors will be in place to detect and allow responses to emergencies on the part of airport personnel. Within the reservation, checking and boarding procedure the system will focus on the detection of unauthorised passengers, flag potential

Control description	Control category	Control nature	Affected assets	Explanation of control
				passengers for additional screening as well as those who encounter other types of difficulties. A mixture of alarm types is assumed to be used. These may include physical barriers, such as doors refusing to open, messages delivered to passenger's smart devices, sound and silent alarms direct to airport personnel to investigate or spoken commands. The sensors are also assumed to be integrated with other devices such as RFID tags, electronic boarding cards, electronic visas and passengers smart devices to provide an unobtrusive monitoring system.
Airport security monitoring and emergencies identification through the usage of smart devices	Detective Corrective	Automated	A19. Airport facilities	It is assumed in the scenario that a network of sensors will be in place to detect and allow responses to emergencies on the part of airport personnel. Within airport facilities the system will focus on the detection of problems with facilities, detect sensors or devices that are malfunctioning as well as detect other hazardous events, such as fire, electrical faults etc. For emergency incidents which require outside intervention (police, fire, specialist services) networks are interoperable and automatic notices can be sent to request these and inform them of the details of the incident to which they will be responding. A similar system is assumed to also be in place in alerting airline personnel to incidents.
Airport security monitoring and	Detective Corrective	Automated	A18. Check-in infrastructure	It is assumed in the scenario that a network of sensors will be in place to

Control description	Control category	Control nature	Affected assets	Explanation of control
emergencies identification through the usage of smart devices				detect and allow responses to emergencies on the part of airport personnel. Within the check in infrastructure the system will focus on the detection of unauthorised passengers, flag potential passengers for additional screening as well as those who encounter other types of difficulties. It will also be able to detect problems with the physical and digital infrastructure linked to check in, detecting for example faulty boarding gates, issues in network connectivity preventing boarding messages being delivered to passengers. The system incorporates alarm mechanisms to alert airline personnel to problems as well as initiate repair or intervention procedures automatically by providing details and locations of incidents.
Departure Control System (DCS)	Preventive	Automated	A1. Automated reservation, checking and boarding procedure	The scenario assumes that the DCS is an integral element of control within the automated reservation, checking and boarding procedures. The DCS is a centralised system operating within a number of areas in an airport automating and monitoring passengers, crew, and airplanes (in terms of departure, arrival times etc) in order to ensure efficient reservation, check in and boarding procedures. The system will have extensive sensor networks and collect information from a wide variety of settings and devices in the airport (departure lounges, RFID tags in goods, boarding cards, electronic visas). It will be interoperable with other systems, such as traffic management, visa and

Control description	Control category	Control nature	Affected assets	Explanation of control
				other governmental databases, airline networks in order to provide overall management of the reservation, check in and boarding procedure. It is assumed that by 2015 advances in system interoperability will have occurred allowing for complex networks and systems such as the DCS to operate reliably and efficiently. It is assumed that the DCS in handling passenger information will be compliant with data protection and other relevant legislation (such as visa requirements).
Verification of only one person in the booth	Deterrent Preventive	Automated	A1. Automated reservation, checking and boarding procedure	This control measure assumes automatic sensors being in place prior or after passengers entering the booth which can determine the number of people present within the booth at any one time. Such sensors can be CCTV based utilising biometric recognition of the number of bodies present within a booth, alternatively sensors can be configured to detect body temperatures or face which would likewise detect abnormal numbers of people in the booth. Each of these technologies exist presently and it can assumed that refinements in the operational efficiency will have been achieved by 2015. When these sensors are triggered an initial voiced alarm will sound informing users of the booth of the fact that only one person may use it at any time. The booth will refuse to operate until the situation is resolved.

Control description	Control category	Control nature	Affected assets	Explanation of control
				Continual soundings of the alarm will result in a notice being sent to airport personnel so that it can be checked.
Global Entry System authentication for Schengen visa holders using PNR	Preventive	Automated	A1. Automated reservation, checking and boarding procedure	The scenario assumes that a global entry system is in place for Schengen visa travellers which utilises Passenger Name Record data. This system is in place for a variety of reasons. It seeks to prevent passengers who may be on specific watch lists who are not authorised to travel. It establishes the legitimacy of travellers in terms of their Schengen status and screens for those who does not have legitimate visa status. The system is automated at all points, with provisions in place during online check in to determine the status of a traveller as well as providing alerts to border and security personnel for individuals who are on governmental databases. The system may not be directly linked with governmental databases, alarms or hits may trigger a notification being sent from the airport sensors to government databases where staff may then intervene. If the system is linked it is assumed that border and security personnel will have real-time access in determining whether passengers are legitimate Schengen visa holders. Other information it is assumed will also be collated, such as biometric scans, in order to authenticate passengers in linking them to their correct PNR data.

Control description	Control category	Control nature	Affected assets	Explanation of control
Communication of the payment transaction record to the shuttle service operator	Preventive	Automated	A4. Automated traffic management	Before a passenger is able to board the shuttle service it is assumed that reliable communications of transactions is in place within network. This control will allow for efficient scheduling of collection and transport times for passengers to the airport by recording preferences when the transaction is completed. Notices may also be forwarded from the service operator to allow other systems such as the DCS to be aware of estimated passenger arrivals as well as allow for traffic management systems to collate data on predicted traffic flows.
Sharing and co - ordination of traffic data	Deterrent Preventive	Automated	A4. Automated traffic management	This control refers to the automatic sharing of data on traffic flows, congestions etc that is performed between different operators, including transport companies, airports as well as local or national governmental agencies. The sharing of data ensures that traffic to and from the airport can be managed effectively. This system relies on data from train, car, bus and other modalities of transport being generated. Such systems are currently in place in a number of areas (for example monitoring motorway traffic utilising cameras). However advances in efficiencies in monitoring and collecting real-time data will be expected to have occurred by 2015.
Automobile's licence plate number capture by the digital video	Detective	Automated	A4. Automated traffic	This control allows for the identification of automobiles as well as the linked identification of the individual or

Control description	Control category	Control nature	Affected assets	Explanation of control
camera and respective record storage			management	company owning the car. This control will allow for traffic management, recording transactions (such as car parks), prevent unauthorised access to parts of the airport (i.e. by barriers automatically being linked). Records will be kept and such data could be of benefit in crime detection and solution. Such systems are already in place in some countries and more are being proposed. By 2015 it is assumed in the scenario that their use will be wide-spread in airports and that the automatic plate number capture and recognition devices will have increased efficiencies in their operation reducing errors or incomplete captures.
RFID tags on purchased goods for identification of the rightful owner	Preventive Detective	Automated	A3. Luggage and goods handling A17. Luggage and Goods	This control refers to radio frequency identification tags which are designed to link purchased goods to the rightful owner as well as determining where goods are not in the possession of their rightful owner. In this instance the RFID tags are scanned and detected for checked in luggage travelling through the airport infrastructure before being placed on the airplane of the owner. Currently only intrusive manual checking of goods can be used. The system assumes that the integrated networks of sensors and RFID tags within airport will be sufficiently advanced to allow for reliable and effective tracking and linking of goods with passengers.
Reception of purchased goods after	Preventive	Automated	A3. Luggage and goods	This control allows for passengers purchasing goods to indicate their flight

Control description	Control category	Control nature	Affected assets	Explanation of control
scanning the boarding pass on a specific reader inside the plane	Detective		handling A17. Luggage and goods	and have these goods delivered automatically to the correct airplane. It also ensures that passengers have the correct status in purchasing duty-free goods. Currently these checks are conducted manually by shop assistants By 2015 it is assumed that electronic boarding cards will allow for the procedure to be automatic by communicating between airline staff, airport personnel and retail operators in allowing for co-ordination in the delivery of goods which is reliable.
Automated return of unused credit from TfL	Corrective	Automated	A10. Credit Cards/Debit card/Payment cards/'e-wallet'	This control assumes that transport operators have monitoring networks to determine that purchased cards with remaining credit have not been used within 3 months. The control assumes that a record is kept of the financial details of the individual who purchased this credit. Automatic payment systems used by the transport operator will then be able to return credit based on automatic notices being generated that credit is to be returned to individuals.
Flight confirmation during goods purchase	Detective Preventive	Automated	A3. Luggage and goods handling	This control allows for passengers purchasing goods to indicate their flight and allow for airport networks to determine whether passengers are entitled for example to purchase duty free goods. The system is assumed to also be integrated with delivery services by highlighting when and to which airplane goods are to be delivered to. Currently these checks are conducted manually by shop assistants by asking

Control description	Control category	Control nature	Affected assets	Explanation of control
				passengers to display their boarding card. It is assumed in this system that electronic boarding cards utilising RFID tags will enable automatic confirmation of a passengers flight details.
GPI RFID chip	Preventive	Automated	A6. Mobile 'smart' devices	This control refers to protections being placed on RFID chips that prevent them being accessed by unauthorised individuals or organisations. This would for example prevent tampering of RFID tags within shopping areas to prevent theft or fraud. The RFID chip incorporates kill switches to deactivate RFID tags when attempts to hack or other tampering is made. It is also assumed to be able to send alarms, silent or audible to inform other networks and systems, or airline, airport or retail personnel that such an incident has occurred. Resetting of the chip will only be possible by authorised users. This will ensure individuals are not able to misuse RFID tags for financial gain, fraud or gaining access to areas to which they are not authorised to enter.
GA message for boarding	Corrective Preventive	Automated	A1. Automated reservation, checking and boarding procedure	This control refers to targeted messages being sent to passengers to inform that their flight is boarding. Currently such systems a mixture of manual and automatic public announcements conducted over the airport's speaker systems. By 2015 it is expected that messages will be delivered to passengers individually to their smart devices. The sending of messages is managed by the DCS, which identifies which passengers are boarding at any

Control description	Control category	Control nature	Affected assets	Explanation of control
				time and by utilising monitoring networks can determine the respective device for the passenger to which messages should be delivered to. In cases where passengers have not boarded on reception of the first message the DCS can send further messages.
Special seats embedded with pressure and temperature sensors on aircraft	Detective	Automated	A7. Health monitoring devices	The scenario assumes that by 2015 sensor advancements will have occurred allowing for the interaction between airplane seats and other remote health monitoring devices as well as providing a degree of monitoring on passengers. These seats will detect agitated passengers, or provide early warning signs of potential health problems. The control assumes that passengers request such seats due to pre-existing medical conditions where their use would be beneficial. It is assumed here that these seats and their monitoring devices comply with data protection legislation. It also assumes that airline personnel are trained in responding to incidents recorded and flagged by the seats as being a potential problem.
SMS record kept by taxi service as a proof	Detective	Automated	A4. Automated Traffic Management	This control refers to the retention of SMS messages sent to individuals to ensure that the proper individual has used the service, and that payment was made. Recording the time as well will allow for more efficient services for passengers in arriving or leaving airports. SMS records and other data

Control description	Control category	Control nature	Affected assets	Explanation of control
				from taxi services will also it is assumed be integrated with traffic management systems allowing for co-ordination with other methods of transport. Such records will allow for traffic management systems to predict future traffic flows where the taxi has been pre-booked.

6 RECOMMENDATIONS

Given the envisaged opportunities of the IoT, and in order to take full advantage of these, we would need to address the major risks identified in the previous paragraphs. In principle, apart from certain risks that are inherent to the technology of IoT/RFID, as we have seen the majority of the risks posed has to do with the ways the technology is used and is thus not a solely technical matter, so the solutions to address them cannot be only technical either. In this section, we provide some initial recommendations to mitigate those risks; the recommendations are made for the various stakeholders, e.g. industry, academia, research institutions, civil society organisations, ENISA etc, in three areas: policy, research and legal. We have also identified specific recommendation for the European Commission, since one of the objectives of this report is to provide some initial recommendation to the EC on these issues, as specified also in the EC Communication COM(2009) 278 [9].

Policy recommendations

Technology solutions are not and cannot be regarded as the total and only solution. Appropriate processes, including human interaction, always need to be in place. These processes also have to address potential failures of technical systems in the overall risk management design. As long as such processes exist, high-tech dependency is not necessarily by itself a critical risk – given that the probabilities of the breakdowns and relatively low and potential impacts can be managed by appropriate backup procedures with a reasonable effort and workload for the persons involved.

In the case of Richard in the scenario described above, losing his smart phone device due to theft or accidental damage would be detrimental for his air travel if all the necessary e-documents were stored on it. However, if a secure online backup procedure was in place, then the risks could be reduced to a mere inconvenience. In the same sense, in the case of the IT-illiterate Elena, systems must be designed considering usability requirements, so that all potential users will be capable to use them in an adequate manner.

Considering the above, we recommend the following:

Rethink existing business structures and introduce new business models

As we have seen in the scenario, future air transportation is bound to bring in devices/sensors/application that generate data and create business processes integration that was never possible before. For example, sensors and readers at various parts of the airport (check in counter, luggage handling systems, gates, maintenance hangar, or even on the airplane) will provide

visibility and data that can be used for tighter system integrations and, as such, allow for tremendous opportunities for business process improvement. This evolution is also bi-directional. While IoT encourages enterprises to perform vertical business process integration improvement, the process improvement itself also guides the evolution of the IoT implementation (e.g. where to put the sensors, what types of new readers are needed). More importantly, enterprises should regard IoT beyond mere incremental improvement and investigate totally new business models (e.g. new way of air transportation) to achieve strong competitive advantages.

In addition, with the availability of various IoT computing partners, data, and services, air transportation businesses can pro-actively seek the possibility to create new business models that significantly improve future air travel (e.g. via horizontal integration with partners, or existing services).

It is thus recommended that air transportation businesses and agencies (e.g. airlines, airports, air cargos/logistics, and government aviation security agencies) proactively plan, design and stay alert on the introduction of new business models. This is expected to mitigate the following risks identified in this report: R1, R3, R4 R5, R11, R13, R15.

User-friendliness of devices and procedures / be inclusive

As the air transport system is supposed to be operated and used by people having different skills and coming from different cultures, the usability of the technical solutions has to be considered thoroughly. Processes have to be clear and comprehensible, and user interfaces have to be designed in such a way that the corresponding systems will be easy to use by their target groups.

It is recommended that usability studies and investigations be conducted prior to and along with the development of new technologies. New devices and services should undergo a trial period, in which regular end users of the systems shall be involved. This of course could be a research recommendation as well.

Moreover, in order to make the procedures as inclusive as possible and to avoid any discrimination in service provision, alternative check-in and boarding procedures should exist for people who have lost their eyes or are otherwise physically challenged and cannot therefore provide biometrics etc. Also, while recognising the efficiency and efficacy of airlines issuing electronic boarding passes, paper-based boarding passes should continue to exist for those who are digitally challenged.

Raise awareness / educate specialised personnel and citizens

In view of the characteristics of this new environment, it is crucial to increase awareness and promote education of citizens and airports' personnel on the security and privacy risks posed by these new technologies and ways to be prepared, as well as on the use of the new devices / technologies /

applications. As even highly automated processes still require human operators, it is important to develop and provide adequate training and instructions for airline, airport and other ground personnel. The training shall address how to use the new procedures and technologies (e.g. paper boarding passes, smart devices, RFID-enabled frequent flyer cards, RFID-enabled luggage tags) for all relevant processes (e.g. check-in, boarding, luggage check). Also guidelines for handling contingencies (e.g. system failures, emergency or crisis situations) have to be developed.

At the same time it is imperative that the state developed and organised appropriate awareness and educational programmes and activities for citizens, so that they are aware of the security and privacy in terms of security and they face in such an environment. This appropriately complements the recommendation on developing user-friendly and inclusive interfaces for end-users. Both are equally important in a future IoT environment.

By all means the programmes and activities targeted to one or the other should be different in a nature. The education, training and provision of appropriate awareness to specialised personnel should be mainly driven by the industry, organisations and companies, while general awareness campaigns for the citizens and public, should be mainly steered by the states, civil society organisations (e.g. consumer organisations etc.), the European Commission, ENISA etc .

Develop and adopt policies for data management and protection

User data will play an important role in the described air travel scenario, and thus it is imperative that clear policies for their collection, usage, storage and deletion are developed and adopted [see also relevant recommendation in research and legal made below]. Data minimization techniques should be used (collect data based on needs) and proper access control mechanisms need be in use. Policies for gaining users' consent when gathering data and how the data is used need to be developed. Furthermore, the mechanisms for transferring and enforcing these policies should be standardized.

In addition, sufficient support is provided to data subjects so that they get adequate information relating to the processing of their personal data and they can better exercise their rights. In this context, we recommend that:

- signs be posted prominently in airports indicating the presence of CCTV cameras and other surveillance technologies;
- information sheets or leaflets be made available to passengers passing through security checks in airports informing them of the storing of their biometrics (e.g., who is storing the biometrics, for what purpose, for how long, whether any repurposing of the biometric data is expected and whom citizens can contact for further information).

Finally, we would recommend that local authorities and government transport departments put back-up procedures in place in the event of a failure of an intelligent transport system (ITS) (e.g., roads embedded with sensors communicating with passing vehicles).

Research recommendations

IoT technologies involve an increasing number of smart interconnected devices and sensors (e.g. cameras, biometric and medical sensors) that are often non-intrusive, transparent and invisible. Moreover, as the communication among these devices, as well as with related services is expected to happen anytime, anywhere, it is frequently done in a wireless and ad-hoc manner. Next to that, the services become much more fluid, decentralized and complex. Consequently, the security barriers in Internet of Things become much thinner (see the risks on electronic identification failures and realization of malicious attacks, R14 and R15). It also becomes much simpler to collect, store, and search personal information and endanger people's privacy (see the risk on loss/violation of citizen privacy, R6, as well as compromise and abuse of databases, R7 and R8). Moreover, a fear is rising that control over personal information is increasingly getting out of hands of people (see the risks on aggressive profiling and social sorting leading to social exclusion, R11, as well as R10on repurposing of data). Finally, a lot of people might not feel engaged with new technology and even fill irritated with its complexity (see the risk on user frustration and low user acceptance, R9). Obviously, this goes beyond the risks people are used to nowadays, leading to new requirements. Therefore, research related to security and privacy of IoT technologies becomes very important. In particular it is recommended to address the following fields:

Data protection and privacy, by conducting research to examine the issues in relation to IoT deployments and to further extend security and privacy solutions. In particular, research is needed to support: (i) proper trust management, (ii) end-to-end policy enforcement and efficient rights management in highly distributed systems, (iii) data disclosure, usage, and purpose control, (iv) effective cryptographic techniques for devices/sensors with limited resources and privacy-preserving identity management and (v) architecting privacy-preserving systems, applications and services, as well as retrofitting existing ones to enable privacy options. This will further support and enhance a security and privacy by design approach.

Usability, by investigating the issues related to usability of security and privacy technologies, and consequently research and development in the related technical fields including human-device interfaces and assisted privacy policy (consent) specification and management. This should also address discriminatory or exclusionary aspects of how information is presented to citizens (including IT-illiterate).

Proposing standards of light cryptography protocols

Recently, a lot of research has been undertaken on light cryptography in the context of RFID, and many new protocols have been proposed (see, e.g., http://www.avoine.net/rfid). In spite of the large number of available methods, there are very few which were examined enough to be considered safe. There are examples of situations, where new light cryptography algorithms were widely deployed, and after some time of usage, serious security gaps were found by researchers (e.g. well known cases of MiFare Crypto-1 and Digital Signature Transponder). In any case it has to be considered that the security of encryption cannot be based on secrecy of algorithms. Contrariwise, the algorithms should be public in order to allow all interested researchers to test them (cryptanalysis). A protocol can then be considered secure if no security gaps were found. We recommend developing light cryptography standards and giving some time to the scientific community to test them before wide implementation.

In addition, based on the combination of light-weight cryptography protocols (for light duty devices usage), as well as the regular cryptography framework (e.g. PKI - Public Key Infrastructure, for back-end infrastructures) should be analyzed and implementation technology and testbeds (e.g. elliptic-curve cryptography mutual authentication RFID) be explored. A very important consideration in this is key management: such a holistic framework, should identify the actors generating the encryption keys (private/public keys) , how these will be distributed and who (which agencies/companies/authorities) will eventually be given access to such keys when necessary (e.g., to find information/cross-link data about suspects etc).

Managing trust

It is obvious from the risks identified, that lack of trust is a detrimental roadblock to next generation IoT air transportation implementation. Trust should thus be a central consideration; an enterprise should identify and understand its own trust framework in order to be able to deal with the IoT challenges. The most salient characteristic of IoT-driven pervasive computing is the formation of transient trust within a highly mobile environment. These trust relationships dictate how the devices, sensors, readers and operators exchange data and operate together (e.g. how much a passenger's smart phone can interact with the airport concession kiosk). See also research recommendation on '**Proposing standards of light cryptography protocols'**.

It is also recommended to focus particularly on the appropriateness and the compliance aspects of trust policies into the IoT applications. The policies should be appropriately developed and implemented, so as to ensure trust and should be complete in their specification, e.g. considering many different aspects, such as ethical, legal and business implications. Once they are in place, due care should be exercised, so that these policies are complied with and are consistent across any system integration.

Multi-modal person authentication

Automatic authentication of people is key to efficient and secure operational procedures in the air transport system. Experiences show that current implementations of biometric systems still show some weaknesses, even if they in principle seem to be promising. Using multifactor authentication (e.g. password plus biometrics, biometrics plus token) has the potential to increase overall security. In the same way, multimodal biometrics (several biometrics used in parallel) will make the authentication process more robust to errors and circumvention. Another aspect is the option to increase system flexibility by providing alternative (spare) authentication factors, which can be used in those cases where the basic way of authentication is not available (e.g. iris scan could be used for persons not having fingerprints).

In conclusion, the recommendation is to further investigate and develop biometric procedures for person authentication. Research work should be extended to investigate and advance single technologies and, in parallel, to develop multi-modal solutions, which combine dissimilar technologies in order to overcome their individual weaknesses.

Legal recommendations

Based on the risks identified in the previous section, and in view of the serious challenges regarding data protection that are envisaged in this new environment, we recommend that:

- The entities that process personal data, including any governmental or commercial entity, such as electronic communications providers, road infrastructure providers, airline companies or any other entity in the air transport sector, shall value highly the security of the personal data of the data subjects and shall take all the necessary technical and organisational measures to ensure it. More specifically, we recommend that:
  - citizens be notified of breaches concerning their personal data;
  - national audit offices compile statistics regarding the sectors, the companies and the government departments that have sustained the most data breaches;
  - companies and government departments are required to include in their annual reports an estimate of the risks posed by compromise of databases containing personal data, as well as information regarding the steps they have taken to minimise such risks by securing such databases (e.g., encryption of the data, physical access control measures, remote back-up of databases);
  - the government departments and companies involved in the international air transport sector be required to conduct Privacy Impact Assessments (see also Recommendations for the European Commission) before any decisions are taken to deploy projects or programs affecting privacy.

Moreover, the Article 29 Data Protection Working Party has noted the lack of harmonisation in the collection of data by airport shops from passengers making purchases.[14] In addition to the above, the IoT/RFID expert group agrees with and supports the conclusions and recommendations of the Article 29 WP, in particular, that

- Shops and customs authorities should be aware that data collection should be restricted to what is strictly necessary, applying the principle of data minimisation. In most cases, shops should only need to collect the flight number/destination mentioned on the boarding pass.
- Data should not be used for law enforcement purposes unless they are necessary as evidence of abuse in specific cases (no bulk transfers to police).
- Data should not be used for other purposes incompatible with the original purpose (disclosing data to third parties without information or consent, for example, to carriers) unless they are used for statistical purposes.
- There shouldn't be any systematic compilation of customers' purchases to allow for analysis of their behaviour and buying habits.
- The retention period should be limited to the strictest necessary and should be harmonised across Europe.

We also note that one of the main results of the Art. 29 WP's investigation of duty free shop practices was that information provided to passengers is insufficient. We recommend that airport operators oblige vendors and service providers in airport to provide passengers adequate information about their collection of personal data, why it is collected and how it is to be used.

The Art. 29 WP also expressed concern that neither the provisions of the Excise Duty Directive nor data protection provisions are uniformly applied and respected across Europe by duty-free shops. Like the Art 29 WP, we recommend that there be further harmonisation of the current practice and efforts be made to raise awareness among travellers as to the collection and processing of data when purchasing duty-free items.

Some further legal recommendation are identified in the section below on recommendation for the European Commission.

[14] Article 29 Data Protection Working Party, Opinion 8/2009 on the protection of passenger data collected and processed by duty-free shops at airports and ports, 02318/09/EN, WP167, Adopted on 1 December 2009.

Recommendations specific for the European Commission

Given the importance of these technologies and the issues of IoT/RFID, and also given the current initiatives of the European Commission towards addressing the concerns already raised on RFID and Internet of Things [9], [10], [11], we have identified below some particular recommendations for the European Commission to act upon.

- We recommend that the European Commission prepare guidelines on the better enforcement and application of the European regulatory framework, especially in view of the challenges posed by technological developments. More specifically, we recommend that:
  - amendments of data protection legislation be introduced to give Data Protection Authorities (DPAs) stronger powers to audit companies or government departments with regard to their compliance with the relevant data protection legislation and that DPAs should be given the resources needed in order to achieve this task;
  - the European Commission negotiate amendments to the EU-US PNR agreement so that there is transparency what the US does with PNR data, whether such data is shared, and so that European citizens have access to their data in a timely, low or no-cost way.
  - the European Commission gives a priority to the regulation of profiling and behavioural marketing in order to ensure the protection of the data subject from their consequences.
- We further recommend that the European Commission:
  - adopt an 'end-to-end' approach for securing IoT/RFID applications: appropriately mitigating IoT/RFID risks lies beyond securing the RFID tags, it actually extends from smart devices to readers and back-end databases
  - in order to improve the usability of future research results, and align research with industrial and societal needs, promote the participation of industry, and in particular SMEs in research activities as FP7. More specifically, we recommend that the Commission reinforce pilot activities in the line of the present CIP ICT-PSP programme with more ambitious targets and measures for participation of SMEs, and also initiate support actions, to better disseminate the results of such research to them;
  - encourage more (and better) research at EU level on the ethical limits of private data capture and circulation, and on the societal implications of developments in this regard, e.g. under the Science and Society programme of FP7.
  - endorse and promote awareness raising and educational activities for the citizens, as well as other specialised audience (professionals, personnel etc.)

Security in flights may be subject to emotional decisions that are taken only to please public opinion. New technologies can and must be used to improve security; however, rushed decisions may have a

cosmetic effect (i.e., satisfying public opinion) but open more security questions than they can fix. Moreover, it is important to follow and promote the approach of *security* and *privacy by design*, so that security and privacy are considered in the early stages of development of applications and technologies, being thus features of the systems and not mere add-on functionalities.

It is thus recommended that any decision on the introduction of new technologies and new procedures should be taken only after a **privacy, security and technology impact assessment** and by a **joint panel with representatives comprising all stakeholders** (industry, civil society organisations, legislators, technology experts, health experts, data protection authorities, ENISA etc.), truly tested and adopted jointly by all Member States. The European Commission should appropriately endorse and steer such a process.

7 GLOSSARY AND ABBREVIATIONS

ACI	Airport Council International
BCBP	Bar Coded Boarding Pass
DCS	Departure Control System
DG	Directorate General
DPA	Data Protection Authorities
EC	European Commission
EDS	Explosive Detection System
EFR	Emerging and Future Risks
ETA	Electronic Travel Authorisation
GA	German Air
GNSS	Global Navigation Satellite System (or Service)
GPS	Global Positioning System
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IFE	In-Flight-Entertainment
IoT	Internet of Things
IPF	Ideal Process Flow
IS	Information System
IT	Information Technology
JLS	Justice Liberty and Security
LAGs	Liquids and Gels

LBS	Location Based Service
MMS	Multimedia Messaging Service
MRO	Maintenance, Repair and Overhaul
NFC	Near Field Communication
PCP	Physically Challenged Passenger
PDA	Personal Digital Assistant
PET	Privacy Enhancing Technology
PIN	Personal Identification Number
PIU	Passenger Information Unit
PKI	Public Key Infrastructure
PNR	Passenger Name Record
RT	Registered Traveller
RFID	Remote Frequency Identification
SIM card	Subscriber Identity Module card
SPT	Simplifying the Passenger Travel
SSD	Solid State Drive
StB	Simplifying the Business
SUICA	Super Urban Intelligent Card
TB	Tera Byte
VIS	Visa Information System
VPN	Virtual Private Network

8 REFERENCES

1. Adey, Peter, *Secured and Sorted Mobilities: Examples from the Airport*, Surveillance & Society, Vol. 1, No. 4, pp. 500-519. Available at: http://www.surveillance-and-society.org
2. Albrecht K., McIntyre L. (2005). Spychips. How major corporations and government plan to track your every move with RFID. Nelson Current 2005.
3. Bachelor, Lisa, *Ryanair scraps airport check-in*, The Guardian, 14 May 2009. Available at: http://www.guardian.co.uk/money/2009/may/14/ryanair-online-check-in
4. Bar-El, H. (2003). *Introduction to Side Channel Attacks*. Whitepaper, Discretix 2003. Available at: http://www.discretix.com/wp.shtml
5. Bono et al. (2005). *Security Analysis of a Cryptographically-Enabled RFID Device*. 14th USENIX Security Symposium, pages 1--16. USENIX, 2005. Available at: http://www.usenix.org/events/sec05/tech/bono/bono.pdf
6. Bowcott, Owen, *Face scans for air passengers to begin in UK this summer*, The Guardian, 25 Apr 2008. http://www.guardian.co.uk/business/2008/apr/25/theairlineindustry.transport
7. Courtois, N.T; Nohl K. & O'Neil S. (2008). *Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards*. Cryptology ePrint Archive: Report 2008/166. Available at: http://eprint.iacr.org/2008/166.pdf
8. Estrin, Deborah (ed.), *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*, Committee on Networked Systems of Embedded Computers, National Research Council, National Academy Press, Washington, D.C., 2001. Available at: http://www.nap.edu/openbook.php?isbn=0309075688
9. European Commission, Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *Internet of Things — An action plan for Europe*, COM(2009) 278, Brussels, 18.6.2009
10. European Commission, Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final, Brussels, 12.5.2009
11. European Commission, Commission Staff Working Document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification, SEC(2009) 586, Brussels, 12.5.2009

12. European Council, Regulation EC 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L385/1, 29.12.2004

13. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, Brussels, 22 July 2009.

14. European Economic and Social Committee, *Opinion on Aviation security for passengers* (2009/C 100/07), Brussels, 23 October 2008.

15. European Group on Ethics and Science in New Technologies (EGE), *Ethical Aspects of ICT Implants in the Human Body*, Opinion to the Commission, 16 March 2005. Available at: http://europa.eu/comm/european_group_ethics/docs/avis20en.pdf

16. European Network and Information Security Agency (ENISA), *Emerging and Future Risks Framework – An Introductory Manual*, March 2010. Available at: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/emerging-and-future-risks-framework-introductory-manual

17. European Parliament and the Council, Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L 97, 9.4.2008.

18. European Parliament, Resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, Brussels, 23 October 2008. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0521+0+DOC+XML+V0//EN

19. Finkenzeller, K., Flörkemeier, C., [et al.] (2004) *Security Aspects and Prospective Applications of RFID Systems*, Federal Office for Information Security (BSI). Available at: https://www.bsi.bund.de/cae/servlet/contentblob/475744/publicationFile/27966/RIKCHA_englisch_Layout_pdf.pdf;jsessionid=85804244C5ED7038E6EFEBC9723C4740

20. Fishkin, K.P. and Roy, S. (2003). *Enhancing RFID Privacy via Antenna Energy Analysis*. Tech. memo IRS-TR-03-012, Intel Research Seattle, 2003.

21. Ford, Richard, *Government bows to EU, undermining £1.2bn electronic borders scheme*, The Times, 18 Dec 2009. Available at: http://www.timesonline.co.uk/tol/news/uk/article6961141.ece

22. Hancke, G. & Kuhn, M. (2005). *An RFID distance bounding protocol*. IEEE SecureComm 2005, 5-9 September 2005, Athens, Greece
23. Hancke, G. (2005) A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005
24. Hicklin, A; Ulery, B; Watson, C, The Myth of Goats: How many people have fingerprints that are hard to match? NIST IR 7271, September 2005
25. International Standard ISO/ IEC 27005:2008 Information technology — Security techniques — Information Security Risk Management, 2008
26. Juels, A. (2005). *Attack on a Cryptographic RFID Device*. RFID Journal, 28 Feb. 2005. Available at: http://www.rfidjournal.com/article/articleview/1415/1/39/
27. Juels, A. ; Rivest, R. & Szydlo, M. (2003). *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. Conference on Computer and Communications Security - ACM CCS, October 2003
28. Kfir, Z. & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems. SecureComm, September 2005.
29. Kirschenbaum, I. & Wool, A. (2006). *How to Build a Low-Cost, Extended-Range RFID Skimmer*. IACR eprint, February 2006
30. Leppard, David, *Spy centre will track you on holiday*, The Sunday Times, 8 Feb 2009. Available at: http://www.timesonline.co.uk/tol/travel/news/article5683677.ece
31. Maghiros, I.; Rotter, P. & van Lieshout, M. (editors*): RFID Technologies: Emerging Issues, Challenges and Policy Options*. EUR Technical Report, EC DG-JRC, IPTS, 2007.
32. Michaels, Daniel, and Andy Pasztor, *Lufthansa to Upgrade to Better Wireless Connections*, The Wall St Journal, 12 Oct 2009. Available at: http://online.wsj.com/article/SB10001424052748703790404574467072334949300.html?mod=googlenews_wsj
33. Miller, Claire Cain, *It Knows Where You Are, and What You're Looking For*, The New York Times, 2 Nov 2009. Available at: http://www.nytimes.com/2009/11/03/technology/internet/03local.html?_r=1&ref=technology
34. Modinis Study on identity Management in eGovernment, Study prepared for the eGovernment Unit, DG Information Society and Media, November 2005
35. Page, Lewis, *Interpol proposes world face-recognition database*, The Register, 20 Oct 2008. http://www.theregister.co.uk/2008/10/20/interpol_face_scan_plan/

36. Rankl, W. & Effing, W. (2004). *Smart Card Handbook*. John Wiley & Sons Ltd, 2004.

37. Reid, J., et al. (2006). *Detecting Relay Attacks with Timing Based Protocols*. Proceedings of the 2nd ACM symposium on Information, computer and communications security, Singapore 2007, pp. 204-213

38. Rieback, M.; Crispo, B. & Tanenbaum, A. (2006*). Is Your Cat Infected with a Computer Virus?* Pervasive Computing and Communications - PerCom 2006, March 2006.

39. Rotter, P. (2008): *A Methodological Framework for the Assessment of Security and Privacy Risk for RFID Systems*. In: IEEE Pervasive Computing, Vol. 7, No. 2, April/June 2008, pp. 70-77.

40. Scott, Jennifer, *Heathrow rolling out facial recognition tech*, ITPro, 30 Nov 2009. http://www.itpro.co.uk/618298/heathrow-rolling-out-facial-recognition-tech

41. Stone, Brad, *As Phones Do More, They Become Targets of Hacking*, The New York Times, 20 Dec 2009. http://www.nytimes.com/2009/12/21/technology/21cell.html

42. Welt Online, *EU lawmakers criticize 'virtual strip search'*, 23 Oct 2008. http://www.welt.de/english-news/article2614271/EU-lawmakers-criticize-virtual-strip-search.html

43. Wortham, J. (2007). *How To: Disable Your Passport's RFID Chip*, Wired, vol. 15, no. 1, 2007. Available at: www.wired.com/wired/archive/15.01/start.html?pg=9

ANNEX I – VULNERABILITIES AND THREATS LIST

VULNERABILITIES

This section presents the vulnerabilities identified by the expert group. Vulnerabilities become risks only when they are exploited by a threat (see next section).

V1. INAPPROPRIATE DESIGN OF PROCEDURES

This vulnerability could be due to lack of accountability, high complexity of procedures, assigning extensive responsibilities to end-users (in critical parts of the procedures), etc.

V2. EXCESSIVE DEPENDENCY ON IT SYSTEMS, NETWORK AND EXTERNAL INFRASTRUCTURE

An excessive dependency arises when one relies on IT systems. It is a sort of "mug's game" in the sense that virtually every system will fail to a lesser or greater extent at some point or other.

V3. LACK OF BACK-UP / FAILOVER PROCEDURES

When things do go wrong, there is no adequate back-up system in place to take over. Availability/robustness has not been considered in the system design, , or appropriate failure modes have not been addressed.

V4. LACK OF OR LOW USER AWARENESS AND/OR TRAINING IN PROCEDURES, USE OF DEVICES, SECURITY ASPECTS ETC

This includes unfriendly authentication mechanisms, too frequent requests for password change, too quick automatic log-offs, etc. This vulnerability may also arise because there has not been sufficient training given to staff in detecting and understanding security threats.

V5. LACK OF USABILITY / UNFRIENDLY USER INTERFACE(S) OF DEVICE(S)

This vulnerability is due to the difficulty of using device interfaces. The interfaces are not intuitive or user friendly. It may arise from excessive or unnecessary functionality options available to the users. A device may be too complicated for ease of use.

V6. LACK OF INTEROPERABILITY BETWEEN DEVICES AND/OR TECHNOLOGIES AND/OR SYSTEMS

A simple example of the lack of interoperability appears when the RFID reader at the airport cannot write data to the RFID tag on Akira's suitcase. This vulnerability is depending on the governance.

V7. Collected data is insufficient or incorrect [lack of adequate controls at data entry]

This vulnerability arises when systems do not collect enough or appropriate data or garble the data they do collect. For example, the data collected by passenger name records (PNR) may not be sufficient to identify a terrorist or an improper entry on no-fly lists, incorrect entries in relation to visa status, and mistaken identification of individuals by commercial entities. The problems of this were clearly highlighted by the failure of databases in respect of the attempted bombing of a flight from Schiphol bound for Detroit in December 2009[15].

V8. Dependency on power systems

If a natural disaster, for example, disrupts an airport's power system, everything comes to a halt.

V9. Lack of or inadequate logical access (identification, authentication and authorisation) and physical access controls

This vulnerability may refer to systems, devices, data access or network access. This also includes authentication of RFID and RFID readers, and since many RFIDs are writeable, this may increase the vulnerability.

V10. Flawed/insufficient design and/or capacity of devices and systems

Poorly designed devices or systems may create a vulnerability, whereby they are not sufficiently robust or resilient to withstand attacks by hackers (for example) or they may not do what is expected of them, especially at critical times.

V11. Lack of adequate controls in biometrics' enrolment stage

Biometrics are not 100 per cent reliable. Part of the reason why they are not may occur at the enrolment stage when an individual's iris or fingerprints or other feature are scanned.

V12. Lack of harmonisation and interoperability of procedures

Security or other procedures may vary from one airport to another, creating opportunities for evil-doers.

[15] http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/7037774/British-no-fly-list-as-intelligence-agencies-fear-second-Detroit-attack.html

V13. LACK OF OR INAPPROPRIATE PROTECTION OF RFID TAGS

V14. LACK OF SUFFICIENTLY SKILLED AND/OR TRAINED PERSONNEL [AIRPORT, AIRLINE]

It's often been said that the weakest link in any system is human. If personnel are inadequately trained, they become a vulnerability. They need to be trained adequately to detect and understand security threats and what to do in the event of a system malfunction.

V15. INSUFFICIENT EQUIPMENT

Airports with insufficient equipment may create a security vulnerability. The vulnerability might also pose problems to the efficient processing of passengers from check-in to boarding.

V16. INAPPROPRIATE EXPANSION OF THE TRUST PERIMETER

Too many people may have access to personal information. Often the biggest threat comes from insiders.

V17. LACK OF DEPENDABLE SENSORS, GPS

V18. LACK OF RESPECT TO THE DATA MINIMISATION AND PROPORTIONALITY PRINCIPLES

The data collected and processed shall be adequate, relevant and not excessive in relation to the purposes they are collected. An example of such lack of respect to the data minimisation and proportionality principles can be mentioned the case, when an LBS system collects not only the information absolutely needed for the provision of the service, but it also stores excessive information. The need-to-know principle is not enforced by any means.

V19. LACK OF RESPECT TO THE PURPOSE LIMITATION (FINALITY PRINCIPLE)

When the purpose limitation principle is not respected, more data are collected and processed than is strictly necessary the specified purpose. For instance, Christina's approximate physical location is revealed to both the cell communication provider as well as the navigation service that provides the map and traffic conditions applications.

V20. LACK OF RESPECT TO THE TRANSPARENCY PRINCIPLE

Lack of respect to the transparency principle means that the data subject is not able to determine the relevant data processing practices. In the IoT a lot of information is transmitted and processed via automated processes, most of which remain unnoticed by the data subject.

V21. INAPPROPRIATE / INADEQUATE IDENTITY MANAGEMENT

While the traffic and local map are being downloaded in real time, Christina's approximate physical location is revealed to both the cell communication provider as well as the navigation service that

provides the map and traffic conditions applications. Appropriate identity management would protect Christina's privacy in this case.

V22. INADEQUACY OF RF TRAFFIC REGULATIONS

V23. OVER DEPENDENCY ON BIOMETRICS

Biometric identification has relatively high error rates (especially automatic face recognition). Also modern biometric sensors (especially fingerprint and iris sensors) are difficult to compromise ('liveness detection'), still is also possible to spoof them. Awareness of imperfection of biometric systems is an important factor of overall security [P. Rotter (ed.) Biometrics Deployment Study. Large-scale biometrics deployment in Europe. Identifying challenges and threats. JRC-IPTS report EUR 23564 EN 2008, ISBN 978-92-79-10657-6. Available at: http://ftp.jrc.es/EURdoc/JRC48622.pdf

V24. INHERENT FEATURES (SIZE, MATERIAL ETC.): EASY TO LOSE, TO BE STOLEN AND/OR COPIED (ESPECIALLY FOR RFID TAGS)

Inherent vulnerability of cards and devices (passports, RFID tags, etc.): they are small in size, and they are easy to lose, be stolen and/or copied.

V25. ACTUAL RFID RANGE LONGER THAN STANDARD

Malicious RFID readers may be able to operate from a distance several times longer than the intended range (Kirschenbaum & Wool 2006). Moreover, shielding of RFID is often not possible.

V26. RFID TAGS DO NOT HAVE A TURN-OFF OPTION

Unlike mobile phones or PDAs, most RFID tags cannot be turned off and are always ready to send data for a request received by radio waves. This feature is an inherent vulnerability.

V27. INSUFFICIENT PROTECTION AGAINST REVERSE ENGINEERING

In RFID and contactless smart cards, due to limited resources, the methods for protection against reverse engineering, such as dummy structures, scramble buses and memory cells, etc., are rarely applied. Active methods for detection of reverse engineering attack are impractical in these devices.

V28. INADEQUATE SECURITY MEASURES OF DATA STORAGE (E.G. INADEQUATE ENCRYPTION MEASURES)

In case RFID and contactless smart cards, due to limited resources, manufacturers often apply light cryptography and proprietary cryptographic methods.

V29. OVER-SENSITIVITY OF DEVICES (GENERATING MANY FALSE ALARMS)

Some devices are not 100 per cent reliable. They may produce inaccurate results or make false positives or negatives.

V30. SENSITIVITY TO MAGNETIC FIELDS

V31. DEVICES & EQUIPMENT USED IN UNPROTECTED ENVIRONMENTS

Devices used by a great number of people every day [health issues (e.g. infectious diseases spread by fingerprint scanners)]

V32. HIGH ERROR RATES OF BIOMETRIC IDENTIFICATION (ESP. FACE-BASED RECOGNITION)

Face-based identification has the highest social acceptance among all biometric identification methods. Unfortunately, it has also high error rates, which leads to many false alarms and/or false acceptances.

V33. COMMUNICATION OF DATA OVER UNPROTECTED OR PUBLICLY ACCESSIBLE CHANNELS

V34. DATA LINKABILITY

Different databases or data stored at different locations serving different purposes are / can be linked, thus enabling greater data matching, data mining, profiling, data aggregation or social sorting. Key question here is who is doing the linking and why – it could be for security reasons (catching terrorists before they fly), but it could also be for commercial exploitation by airlines, vendors, service providers operating in the airport as well as by evil-doers seeking to undermine air travel, airport systems or engaged in spoofing, phishing, spamming.

V35. LACK OF DATA CORRECTION MECHANISMS (AS NORMALLY DATA SUBJECTS DO NOT HAVE ACCESS TO THE DATABASES)

Many entities are collecting personal data, but rather fewer of them have procedures in place enabling individuals (data subjects) to see what data they have about them. Procedures for correcting incorrect data may not exist or may be cumbersome and bureaucratic.

V36. FAILURE OF BIOMETRICS SENSORS

V37. LACK OF COMMON OR HARMONISED LEGISLATION IN EU MEMBER STATES

Although Member States have transposed the EU Data Protection Directive, they have not done so in a fully harmonised way. In addition, there are lacunae in the legislation so that some matters are not addressed.

V38. INSUFFICIENT PROTECTION OF WIRELESS NETWORKS AND COMMUNICATION (WEAK OR NO ENCRYPTION ETC.)

Due to limited resources, RFID tags often use light, proprietary cryptography, which in some cases is not sufficient. Identifiers of tags which are sent in the beginning of communication are not encrypted at all (as a part of anti-collision protocol) and they may be used e.g. for tracking of people.

V39. LACK OF RESPECT TO THE LEGITIMACY OF DATA PROCESSING, E.G. CONSENT

The processing of personal data is supposed to be legitimate. However, some data controllers and data processors may not have obtained the informed consent of data subjects.

V40. LACK OF RESPECT TO THE DATA CONSERVATION PRINCIPLE

Personal data are supposed to be deleted when they are no longer necessary for the purposes for which they were collected or processed.

V41. LACK OF RESPECT TO THE RIGHTS OF THE DATA SUBJECT (SUCH AS THE RIGHT FOR RECTIFICATION, BLOCKING OR DELETION OF DATA)

Data subjects are supposed to be given the opportunity to rectify incorrect data or to block its further use. For instance, Akira wishes to unsubscribe from "Hazukashi Not" service and to have his account deleted.

THREATS

T1. DENIAL OF SERVICE ATTACK / FLOOD / BUFFER OVERFLOW

A denial of service attack is sabotage, aimed at disrupting a service for fun or to achieve political or illegal goals. A DOS attack is sometimes known as a buffer overflow attack or flooding..

T2. SPOOFING OF CREDENTIALS / BYPASS AUTHENTICATION

This threat is a stepping stone to achieve next stage of sabotage or penetration.

T3. LARGE-SCALE AND/OR INAPPROPRIATE DATA MINING AND/OR SURVEILLANCE

The ease with which data can be collected, aggregated and mined coupled with the motivation of large financial paybacks make this a widespread threat. Roger Clarke coined the term dataveillance to describe the phenomenon of surveillance by means of data analysis. Both airports and governments may also have an interest in analysing data, to prevent terrorist related incidents, to develop more targeted advertising.

T4. TRAFFIC ANALYSIS / SCAN / PROBE

This threat is often found in conjunction with or preparation for another attack aimed at revealing protected sensitive operations. The threat gleans data implied in network communication patterns. Traffic analysis requires special skill and knowledge to be effective.

T5. Man-in-the-middle attack

This is one of the most common attack methods, especially for information collection. However, such attacks on RFID and smart cards do not occur very often. Such attacks are usually carried to appropriate others' identity rather than getting access to restricted areas or data, which is usually encrypted. Man-in-the-middle (or relay) attacks for contactless smart card has been theoretically analysed by Kfir and Wool (2005). For practical aspects, see Hancke (2005). Countermeasures such as distance bounding based on response time (Hancke & Kuhn 2005; Reid et al. 2006) or signal-to-noise rate (Fishkin & Roy 2003) are rarely applied.

T6. Social engineering attack

Social engineering attacks are widespread and too-often effective. They play upon gullibility or human psychological weakness. Phishing could be regarded as a form of social engineering.

T7. Theft [of cards, devices etc]

There will always be evil-doers engaged in theft of others' property, be it smart cards, smart phones or whatever. Theft is not, of course, the only crime. Extortion, fraud and many other crimes are common in cyberspace.

T8. Unauthorised access to / deletion / modification of devices / data etc.

This attacks refers to unauthorized access to data stored on RFID, smart cards (especially contactless) and personal devices. Also databases can be a subject of attack though the network, as well as data can be illegally accessed and modified by unauthorized personnel.

T9. Loss or misuse [of cards, devices etc]

Loss or misuse of a card or device is also a common threat.

T10. Use erroneous and/or unreliable data

Given the security implications of the non-identification of particular passengers (as in the recent Detroit example mentioned) unreliable data can have major implications for safety and security. Less dramatic risks could include for example allergy bracelets as described in the scenario incorrectly.

T11. Procedures / instructions not followed

This threat arises when, for example, a passenger doesn't follow instructions and makes a jam in the automated passport/immigration control or smart corridor.

T12. NON-COMPLIANCE WITH DATA PROTECTION LEGISLATION

This threat arises when governments and business do not comply with provisions of data protection legislation and the principles stated therein, for example, regarding data minimisation, purpose specification, proportionality, informed consent, access to data by the data subject, etc.

T13. FUNCTION CREEP (DATA USED FOR OTHER PURPOSES THAN THE ONES FOR WHICH THEY WERE ORIGINALLY COLLECTED)

Function creep occurs when data are used for other purposes than the ones for which they were originally collected for. For example, in the air traffic scenario, a car rental company doing some market analysis might approach an airport operator to gain access to its data on airport parking.

T14. UNAUTHORIZED CHECK-IN AND BOARDING / IDENTITY THEFT

For example, an attacker might use a fake fingerprint with a stolen passport to board the plane.

T15. CLONING OF CREDENTIALS AND TAGS (RFID RELATED)

An RFID clone can be either physically similar to the original tag or can be a notebook with a special antenna. Cloning is relatively easy for basic tags but even some advanced and apparently well protected tags with a challenge-response protocol have been cloned (Juels 2005; Bono et al. 2005; Courtois et al. 2008).

T16. UNAUTHORISED ACCESS TO OTHER RESTRICTED AREAS (APART FROM BOARDING E.G. CONTROL ROOM, PERSONNEL'S' OFFICES)

This threat can arise as a result of stealing or cloning authorisation tokens (like smart cards).

T17. SIDE CHANNEL ATTACK

Smart cards or RFID tags may be subject to side channel attacks based on information gained from physical implementation of a cryptosystem, like variations of power consumption, time of computations or electromagnetic field (Bar-El 2003). It is often combined with other cryptanalysis methods.

T18. BLOCKING

RFID or a GSM network can be blocked by exploiting vulnerabilities of information exchange protocols. Blocking can be also useful as a way to protect consumers' privacy (Juels, Rivest, Szydlo 2003).

T19. JAMMING

Jamming is malicious interference of a radio transmission. It can result in denial of service and forcing a system to use fallback procedures. Large-scale jamming requires extensive equipment setup and

exposure of the transmission source. It is not commonly practised unless with a clear and critical agenda.

T20. FAKE / ROGUE RFID READERS / SCANNING OF RFID READER AND /OR TAG

RFID Tags can be read by any RFID reader. Therefore, rogue RFID readers can scan for RFID and be used for unauthorized reading of information from a tag. As RFIDs often have light cryptography schemes (if any), powerful back-end systems can break the code in minutes, making the security protection ineffective. The range of a reader may be extended several times beyond the standard communication distance, for example ISO 14443 cards with standard range 10 cm can be scanned from 25-35 cm, which is enough to read a card in someone's pocket. Main countermeasures are: encryption, authentication of the reader, using short-range tags, shielding tags with an anti-skimming material (e.g. aluminium foil) and moving sensitive information to a protected database in the system's backend.

T21. PHYSICAL RFID TAG DESTRUCTION

The easiest way to disrupt RFID systems is to physically destroy the tags. Destruction becomes a serious issue when RFID tags are used as anti-theft protection. RFID tags in e-passports can be destroyed by owners who have concerns about possible abuse of their privacy – especially as an e-passport with a non-working RFID tag is still valid (Wortham 2007).

T22. MALFUNCTIONING/BREAKDOWN OF SYSTEMS /DEVICES / EQUIPMENT

This threat occurs when systems or devices malfunction due to hardware/software/implementation errors.

T23. E-VISA NOT ACCEPTED AT CHECK IN

T24. WORMS, VIRUSES & MALICIOUS CODE

Worms, viruses and malicious code are a part of our daily cyber life. They are a prevalent and effective way of disrupting systems. Even very simple RFID tags, such as those used for tagging goods, can carry a malicious code (Rieback at al. 2006).

T25. MALICIOUS ATTACK ON POWER SYSTEMS

This threat might be aimed at forcing a system to use fallback procedures, e.g., in order to get unauthorised access to restricted areas.

T26. STATE SURVEILLANCE ON CITIZENS

Unjustified political agendas often lead to excessive surveillance on citizens. Every described case (true or invented) dramatically decreases trust and acceptance of technology (especially biometrics, RFID).

T27. TRADE UNION/LABOUR STRIKES

T28. ADVERSE WEATHER CONDITION OR OTHER DISASTER

This threat is of low probability but potentially high consequence. The destruction wrought by natural disasters is difficult to predict. It could affect airport and telecommunication (network) operations.

T29. AD HOC NETWORK ROUTING ATTACK

Personal mobile devices may create ad hoc networks in order to exchange data and information between users. These networks can be used by attacker to break into personal devices and compromise the communication and information exchange between parties. For example, DOS attacks can flood ad-hoc networks; rogue participants can de-route or compromise legitimate messages and information exchanges.

T30. LOW ACCEPTANCE OF DEVICES / EQUIPMENT / PROCEDURES

RFID is perceived by many people as a privacy threat. They have been called "spychips" (Albrecht, McIntyre 2005). Most of the concerns presented during an EU public consultation on RFID were related to privacy (Maghiros, Rotter, van Lieshout 2007). Also some biometrics have low social acceptance, especially fingerprints which are commonly regarded as linked to criminal investigations.

T31. DATA LINKABILITY

The abundance of data collected and processed in the IoT and their storage in databases (commercial and state) facilitate their linkability.

T32. PROFILING

The abundance of data collected and processed in the IoT can lead to the creation of user profiles (relating to consumer preferences, travelling habits, etc.).

T33. EXCLUSION OF THE DATA SUBJECT FROM THE DATA PROCESSING PROCESS

The automatisation of the processes in the IoT threatens to exclude the data subject from the data processing process.

T34. TRIVIALISATION OF UNIQUE IDENTIFIERS

The use of unique identifiers, such as the human fingerprint, is increasingly being used for trivial transactions, such as in the case when Elena registers her fingerprint in order to "secure" her boarding pass.

ANNEX II – SCENARIO BUILDING AND ANALYSIS TEMPLATE

Please refer to accompanying document.

ANNEX III – RISK ASSESSMENT SPREADSHEET

Please refer to accompanying document.