

Project acronym: **ASSET**
Project full title: Aeronautic Study on Seamless Transport
Grant agreement no.: **FP7 - 211625**
SEVENTH FRAMEWORK PROGRAM
Transport
Aeronautics and Air Transport

WP: WP1
Deliverable No.: D1.2
Originator: ID PARTNERS

Report on privacy constraints and the work carried on by standardization bodies



Due date of deliverable: 6/2009

Actual submission date: 1/2010

Start date of project: 01/06/2008

Duration: 36 months

Project coordinator: DLR

Revision: V2.0

Change Records

Version	Date	Changes	Author
V1.0	28.01.2010		ID PARTNERS
V2.0	08.02.2010	Minor Changes	ILR/VIA/DLR

1	Executive summary	4
2	Regulatory context	5
2.1	EU regulation categories	5
2.2	EU critical infrastructures	6
3	ID control regulatory framework	14
3.1	Airlines mandate to control traveller IDs	14
3.2	EC regulatory documents on ID control	16
4	Collaboration of members states in the field of judicial matters	20
5	Infrastructures Security regulatory framework	27
5.1	Generic Infrastructures:	27
5.2	Information Technology Infrastructures:	48
5.3	Aviation sector infrastructures protection	52
6	Privacy protection Regulatory framework	65
6.1	Main Directives and regulatory documents	65
6.2	Privacy enhancing technologies (PET)	80
6.3	Standardisation activities addressing privacy issues	82
7	Asset recommendations	93
7.1	Recommendations to the ASSET consortium	93
7.2	How shall ASSET comply with industry standards and international bodies ?	93
8	Use case: scenario of three travellers using IT systems compliant with EU privacy framework	95
8.1	Scenario background	95
8.2	The technology response to the growing demand for airport passenger automation.	97
8.3	Facilitation scenario compliant with EC privacy directives	99
8.4	Abbreviations	104

1 EXECUTIVE SUMMARY

As Travelers' Privacy is key to the implementation of advanced IT systems for facilitating airport's processes, the ASSET consortium has investigated the various issues that constitute the legal framework prior recommendations be given to the various stakeholders :

As the ASSET consortium aims at speeding up A/C TRT and automating travelers' various controls, specific attention will be paid that recommended systems and equipment do not to store data but rather streamline procedures until the ultimate barding phase.

The present document is based on an in depth assessment of both aviation security regulations and the privacy framework following fruitful discussions with the French DPC, Data Protection Commissioners (CNIL¹) and various technology providers. Aviation security regulation shall be considered as a subset of the EC EPCIP initiative, European Program for Critical Infrastructures Protection launched in 2005.

Having in mind the various technologies that allow speeding up both passengers and baggage controls, we describe an ideal airport scenario involving advance facilitation systems without infringing passengers' privacy.

Based on the various assessments carried on during this study, it is recommended that airports and airlines do not manage proprietary systems for speeding up the passengers' processes but rather rely on ePassports and governments' cards and avoid storing passengers' data.

¹ Commission Nationale Informatique et Liberté, Paris

2 REGULATORY CONTEXT

2.1 EU regulation categories

The legal basis for the enactment of regulations is article 249 of the Treaty establishing the European Community and, as such, regulations only apply within the European Community pillar of the European Union.

Article 249

In order to carry out their task and in accordance with the provisions of this Treaty, the European Parliament acting jointly with the Council, the Council and the Commission shall make regulations and issue directives, take decisions, make recommendations or deliver opinions.

- A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.
- A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.
- A decision shall be binding in its entirety upon those to whom it is addressed.
- Recommendations and opinions shall have no binding force.

The Council can delegate legislative authority to the Commission and, depending on the area and the appropriate legislative procedure, both institutions can make laws. There are Council regulations and Commission regulations. Article 249 does not clearly distinguish between legislative acts and administrative acts, as is normally done in national legal systems.

Regulations are in some sense equivalent to "Acts of Parliament", in the sense that what they say is law, and do not need to be mediated into national law by means of implementing measures. As such, regulations constitute one of the most powerful forms of European Union law and a great deal of care is required in their drafting and formulation.

When a regulation comes into force it overrides all national laws dealing with the same subject matter and subsequent national legislation must be consistent with and made in the light of the regulation. While member states are prohibited from obscuring the direct effect of regulations, it is common practice to pass legislation dealing with consequential matters arising from the coming into force of a regulation

2.2 EU critical infrastructures

2.2.1 Definition

The European economy and the welfare of its citizens require that the European energy infrastructure functions properly. National authorities are responsible for policies regarding the security -protection against external threats- of energy facilities in their territories, involving measures oriented to prevent disruptions, mitigate damages and restore supply under the best conditions.

In the last few years, however, new international threats have emerged, necessitating increased capability in awareness raising, prevention and response. On top of this, the development of the energy networks in the context of European internal market results in more trans-European infrastructures, which integrity and functionality affects several member States. A European dimension is necessary to properly manage the arising risks.

Since 2004, the European Union has taken the initiative on this issue, by working towards a common European approach to the protection of energy infrastructure as defined in the European Program for Critical Infrastructure Protection. A number of sectors other than energy (i.e. Transport, ICT, Finance ...) are also addressed by this program.

Other initiatives, such as the Security thematic area within the Seventh Framework Program for research and technological development (FP7), contribute to this goal.

The initial effort concentrates on those energy infrastructures which, if disrupted, might have a significant impact in other Member States. Once identified, these would then be nominated as European Critical Infrastructure and consequently subject to a specific approach with a European dimension in regard of their protection. The Key tasks are:

- Establishing legal instruments for implementation of EPCIP, with a sectoral dimension.
- Identification of European Critical Infrastructures in the different energy sub-sectors: oil, gas, electricity.
- Recommendations and technical assistance to Member States
- Follow-up of national critical infrastructure programs
- Fostering networking among the EU, Member States, security technology companies and energy infrastructure owners and operators
- Coordination with relevant international organizations.

2.2.2 Transports²

Transport is one of the Community's foremost common policies. It is governed by Title V (Articles 70 to 80) of the Treaty establishing the European Community. Since the Rome Treaty's entry into force in 1958, this policy has been focused on eliminating borders between Member

² http://europa.eu/legislation_summaries/transport/index_en.htm

States and to therefore contribute to the free movement of individuals and of goods. Its principal aims are to complete the internal market, ensure sustainable development, extend transport networks throughout Europe, maximize use of space, enhance safety and promote international cooperation.

The Single Market signaled a veritable turning point in the common policy in the area of transport. Since the 2001 White Paper, which was revised in 2006, this policy area has been oriented towards harmoniously and simultaneously developing the different modes of transport, in particular with co-modality, which is a way of making use of each means of transport (ground, waterborne or aerial) to its best effect.

Transport is one of the typical infrastructures that relies on transnational assets (routes, stations, power, telecoms....). For this reason, we will explain what are the current rules in force for their protection.

2.2.3 Aviation

Following the terrorist attacks of 11 September 2001, the Commission has stepped up all aviation security standards. In particular, Regulations make the security measures laid down by the European Civil Aviation Conference (ECAC) compulsory within the European Union (EU)³.

These provisions establish a system of unannounced inspections, introduce more rigorous screening of passengers, luggage and staff, and require Member States to introduce national security programs and common standards for equipment.

Each Member State must adopt a national civil aviation security program in order to ensure that common standards are applied. They must also designate a competent authority to be responsible for coordinating and monitoring the implementation of its national quality control program. That authority may also adopt national security measures applicable to small airports.

The Regulation provides for the strict application of airport access controls (permanent access controls and background checks on authorized staff) and checks to be carried out on passengers, baggage (cabin and hold) and members of staff, including the crew and their baggage.

These are screened before being allowed into security-restricted areas (areas requiring an access badge). One year after the entry into force of the Regulation, these checks became compulsory in certain 'critical parts' of these areas, for example aircraft access areas. These 'critical parts' are to be gradually harmonized throughout the Community within five years of their being adopted by the Commission. The Annexes to the Regulation set out security measures concerning:

³ http://europa.eu/legislation_summaries/transport/air_transport/124253_en.htm

- Airport security;
- Aircraft security;
- Passengers and cabin baggage;
- Hold baggage;
- Cargo, courier and express parcels, mail and air carrier materials.

2.2.4 EU CIP History⁴

On 17-18 June 2004, the European Council asked the Commission to prepare an overall strategy to enhance the protection of critical infrastructures. In response, the Commission transmitted on 22 October 2004 a Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism" putting forward suggestions to enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures (CI).

The Commission's intention to propose a European Program for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN) was accepted by the 16-17 December 2004 European Council in the Council conclusions on prevention, preparedness and response to terrorist attacks and in the Solidarity Program, both adopted by the Council on 2 December 2004.

Throughout 2005, intensive work was done on the elaboration of EPCIP. Two European seminars on critical infrastructure protection and a number of informal meetings were held bringing together experts from all EU Member States. This work culminated in the adoption by the Commission on 17 November 2005 of the Green Paper on a European Program for Critical Infrastructure Protection (COM (2005) 576 final).

The Green Paper exercise was followed by a detailed impact assessment and the adoption on the 12th of December 2006 of a policy package on EPCIP composed of a communication and a Directive. The communication deals with general policy in connection with EPCIP (CIWIN, work-streams to develop EPCIP, sectoral interdependencies, annual work planning and the residual work on National Critical Infrastructure) whereas the Directive focuses on the designation of critical infrastructure of a European dimension (European Critical Infrastructure or "ECI").

2.2.5 CIP objective

Firstly, the Commission has been asked to develop work on protecting critical infrastructure by European Councils in March and June 2004. This has been backed by the Justice and Home Affairs Council in December 2005.

⁴ <http://www.euractiv.com/en/security/critical-infrastructure/article-140597>

Secondly, given its role in promoting the internal market, the Commission is interested in ensuring that it is not impeded by protection measures, nor is it damaged by their absence.

A growing number of Member States are preparing their own approaches to critical infrastructure protection and are waiting for the Commission to put forward a general European CIP program, so that they can take into account the common EU approach. Delaying the adoption of a common framework would increase the chance that various incompatible approaches to CIP would be developed by the Member States.

Weak links have to be eliminated especially where transboundary effects came into play. The risk of one Member State suffering because another has failed to adequately protect infrastructure on their territory needs to be minimised. Additional costs for companies operating in more than one Member State resulting from differing security measures need to be minimised. Some infrastructure are becoming increasingly European, which means that a purely national approach is insufficient e.g. the energy pipelines and transmission network.

Some of the work concerning the details of how to better protection critical infrastructure in Europe (especially on such issues as the identification of interdependencies) can reasonably be expected to take a long time. Such work should start as quickly as possible and needs to be based on a common approach.

Stakeholder consultations have been ongoing since 2004 and have included three EU CIP Seminars, the adoption of a Green Paper, the holding of two informal CIP contact points meetings and numerous bilateral meetings with government and private sector representatives. Criminal and terrorist threats are not diminishing and that there is an interest, and potentially synergies, in Member States and the Commission cooperating to protect against them.

2.2.6 *Subsidiarity principle*⁵

The subsidiary principle means that security threats cannot be met by any single Member State on its own. Although it is the responsibility of each Member State to protect the critical infrastructures present under its jurisdiction, it is crucial for the security of the European Union to make sure that the most important infrastructures having an impact on the entire Community or on two or more Member States are protected to a satisfying degree and that particular Member States are not made vulnerable because of the existence of lower security standards in other Member States. The identification and protection of infrastructures having an importance for the EU (ECI) cannot be done below EU level as an EU perspective is needed in order to assess interdependencies

⁵<http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihtmlang=en&lng1=en,fr&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=485618:cs&page=>

and develop common minimum protection measures. Such measures are needed in order to make sure that a minimum level of security exists in the EU and weak links cannot be exploited. In general:

It is clear that the protection of critical infrastructures is first and foremost a national responsibility. All stakeholders acknowledge that due to interdependencies and the general nature of today's economy, there exists in the EU a certain number of critical infrastructures which if disrupted or destroyed would have a serious impact on the entire Community or on a number of Member States. There is therefore a need to identify and designate in a coherent fashion (using the same sector-based criteria in the entire EU) the above mentioned critical infrastructures and assess whether they require additional protection measures.

2.2.7 Proportionality principle

The EU does not go beyond what is necessary in order to achieve the underlying objectives of improving the protection of critical infrastructures in Europe. No other approach would allow the EU to achieve the required objective within a reasonable period of time. At the same time, common rules in the CIP field will be of benefit to businesses, which are currently subjected to various regimes in the MS. The EPCIP proposal puts forward a minimal number of measures needed to improve the protection of critical infrastructures. The underlying objective cannot be sufficiently achieved through other measures, namely by adopting a guideline approach to EPCIP, as this would not guarantee similar levels of protection across the entire EU and weak links could be exploited.

2.2.8 Type of infrastructure addressed

The Commission's actions will focus on European Critical Infrastructure – that is critical infrastructure that, if disrupted or destroyed, would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State. With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States. The Commission will support the Member States in these efforts only where requested to do so. (EPCIP) will therefore also include the possibility for Member States to take action themselves on their national critical infrastructure.

2.2.9 *Member States collaboration*

Once an event involves two Member States there is a transboundary dimension. If one Member State decides to take insufficient action to protect this type of infrastructure then the other Member State can suffer.

Some stakeholders did feel that European Critical Infrastructure need only consider infrastructure where the impact will affect three or more Member States, arguing that existing bilateral arrangements were sufficient to cover infrastructure involving only two Member States. The Commission considered this carefully but concluded that, legally, three or more Member States was not in-line with the concept of transboundary that runs throughout the EU treaties. It also realized that while some bilateral agreements did exist for what might be termed European Critical Infrastructure, this was certainly not the case for all of it. Finally, the use of the three or more Member States approach to EPCIP would eliminate certain Member States from the scope of EPCIP (e.g. in several sectors Portugal could only be impacted by infrastructures located in Spain).

2.2.10 *All-hazards vs terrorism?*

When considering the seriousness of the impacts of an event, it is (from the disruption point of view) largely irrelevant what caused it. When considering whether something is or is not European Critical Infrastructure, there is no need to make a distinction here as it is the impact of the disruption that is of importance. Clearly when considering protection measures the nature of the threat and the vulnerability needs to be considered in more detail. Given the greater experience of dealing with natural hazards, component failure and criminal threats, the protection measures are likely to focus on terrorism.

2.2.11 *European Critical Infrastructures sectors*

The European Commission wants to co-ordinate efforts in member states and reassure the public that efficient alert and information systems are in place to protect the main elements of critical infrastructure. In its main policy document, 'Critical infrastructure protection in the fight against terrorism' from 2004, the Commission offers this broad description:

"Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services."

In the Green Paper on Critical Infrastructure, published on 24 November 2005, the Commission addressed key issues such as against what threats the EPCIP should protect, the definition of what is EU critical infrastructure and what is national critical infrastructure and the role of owners and operators of infrastructure.

The EPCIP identifies the following ECI sectors:

- Energy;
- nuclear industry;
- information, communication technologies, ICT;
- water;
- food;
- health;
- financial;
- transport;
- chemical industry;
- space, and;
- research facilities.

The issue at hand which requires action is the vulnerability of critical infrastructures in Europe and the ensuing vulnerability of the services they provide. This applies to all critical infrastructures in Europe regardless of whether they can be considered as having EU or national importance.

Taking into account the **principles of subsidiarity and proportionality**, EU level action should concentrate on those critical infrastructures having an EU importance. With this in mind, EPCIP will develop into a process leading over time to an assessment of vulnerabilities of particular CI sectors and the preparation of proposals on how to best address these vulnerabilities. These key activities and especially the development of specific protection measures will concentrate on European critical infrastructure, with the Member States however being encouraged to adopt similar approaches concerning their national critical infrastructure.

2.2.12 Protection of infrastructures and privacy

By the means of the European Program for Critical Infrastructures Protection (EPCIP), both EC and governments are taking advantage of a strong regulatory framework to control civil transport activities as a whole and aviation in particular.

This is the reason why it is important to assess what are the various regulations to protect the aviation infrastructures and authenticate the citizens, on one side; and then highlight what is the current framework to protect passengers' privacy.

Therefore, we propose to break down this assessment of regulatory context based on the following structure:

- ID control regulatory framework
- Collaboration of Member States in the field of judicial matters
- Infrastructures protection framework
- Generic infrastructures
- IT Infrastructures
- Aviation infrastructures
- Privacy regulatory framework
- Standardization activities addressing privacy issues
- Typical Airport process compliant with EC privacy regulatory framework

3 ID CONTROL REGULATORY FRAMEWORK

3.1 Airlines mandate to control traveller IDs

3.1.1 *The Schengen Agreement context*

Air carrier's liability under international public and internal legislations is mainly known about the level of compensation and protection of passengers involved in air accidents⁶.

However, in addition to the air carrier liability in the event of accidents, some of the European Union's Member States signed a Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. As of today, founding Members were joined by Italy, Spain, Portugal, Greece, Austria, Denmark, Finland and Sweden.

Chapter 6 (Accompanying measures) of the Convention sets in its Article 26 a unique system of air carrier liability "obliged to take all the necessary measures to ensure that an alien carried by air or sea is in possession of the travel documents required for entry into the territories of the contracting parties":

- 1.The contracting parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967, to incorporate the following rules into their national law.
- (a) If aliens are refused entry into the territory of one of the contracting parties, the carrier, which brought them to the external border by air, sea or land, shall be obliged immediately to assume responsibility for them again. At the request of the border surveillance authorities, the carrier shall be obliged to return the aliens to the third State from which they were transported or to the third State which issued the travel document on which they travelled or to any other third State to which they are certain to be admitted.
- (b) The carrier shall be obliged to take all the necessary measures to ensure that an alien carried by air or sea is in possession of the travel documents required for entry into the territories of the contracting parties.
- 2.The contracting parties undertake, subject to the obligations resulting from their accession to the Geneva Convention relating to the Status of Refugees of 28 July 1951,as amended b the New York Protocol of 31 January 1967,and in accordance with their constitutional law, to impose penalties on carriers which transport aliens who do not possess the necessary travel documents by air or sea from a third State to their territories.

⁶ Convention for the Unification of Certain Rules Relating to International Carriage by Air signed at Warsaw, followed by the Convention of 28 May 1999 for the Unification of Certain Rules for International Carriage by Air (the Montreal Convention). See also : Wowern, (Johann Van Der) . "Recent developments and perspectives in European and international air transport law" by Dr J. L. van de Wouwer. - Brussels : Bruylant Homes International, 1998. - XIII-231-VII p. ; 24 cm. - Bibliogr. p. VI-VII. - ISBN 2-8027-1218-7 (br.)

- 3.Paragraphs 1(b)and 2 shall also apply to international carriers transporting groups overland by coach, with the exception of border traffic.

3.1.2 Airlines liability

Considering the above, operators have implemented strong verification procedures to check the travelers' ID. The average – and non official - liability for air Transport carriers amounts 100 M€ / year to carry back unauthorized travelers to their home countries. In the post 9/11 context, it is worth highlighting that ASSET sits at the crossroad of two main trends which combine:

- Automation of travel documents control
- Strengthening ID checks by implementing pax data processing and reinforced credentials by the means of ePassports and national ID cards.

We shall make a difference between external borders of the Schengen area and internal borders. In the first case, it is the responsibility of air carriers to ensure that travelers possess the right documents to enter the area; in the second case, since there is no border crossing, therefore it is the responsibility of “government authorities” under national laws rather to than airlines to check the travelers' ID.

3.1.3 ID control within the Schengen are

Further investigation shall be carried on with the EC so as to determine how legally an Airline shall become liable, should it transport an Alien without proper ID within the Schengen area. If this is confirmed; this issue will campaign for the wide introduction of biometrics verification, should Air Carriers automate ID control, starting at the check in stage.

But this is not yet the case, as airlines are not allowed to authenticate the biometrics sample stored in the chip of the passports, due to the EAC (Extended Access Control) policy currently put in place between governments which ensures that both chip and readers authenticate each others and the biometrics is not stolen.

Biometrics would indeed become the most powerful means to ensure that travelers carry their own IDs. Furthermore, the device should embed additional data such as visa expiry date to verify that the individual is still authorized to stay in the Schengen area⁷. Even though the ASSET consortium continues to assess the plans of the EC DG JLS, it shall be investigated how an Airline can confirm pax' IDs at least at boarding stage if check in is dematerialized in the near future..

⁷ This is the typical aim of the EU JLS « Entry / Exit » program. But it is not clear at this stage how the MS will identify travelers who will overstay their visa period.

3.1.4 *International Case*

As it is mentioned by the Convention for the implementation of the Schengen Agreement, Air carriers shall control travelers ID to allow the crossing of external borders. Since there is definitively an immigration control by national police authorities to proceed to the airside zone, it should be investigated further what will be the procedure for the carriers to control pax IDs: mere passport facial control or access to the MRZ ? . But as mentioned above, airlines are not yet allowed to access biometrics stored in the sample of the passport, even in the case of crossing external borders.

3.2 **EC regulatory documents on ID control**

We propose the following description grid so that to easily identify the relevance of the selected documents vis à vis the ASSET objectives.

Title:	Title of document
Type:	Type of document
Date:	Date of publication
Ref:	Reference of publication
Status:	Status (when available)
Link:	Link to document
OJ:	Official Journal reference for EU documents, when available
Summary:	Short summary of the regulation objectives
Scope:	Scope and perimeter of the regulation

Title: Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency.

Type: Regulation (EC)

Date: 10 March 2004

Ref: (EC) No [460/2004](#)

Status: Text with EEA relevance

Link: [http://eur-](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=460)

[lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=460](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=460)

OJ: L 077 , 13/03/2004 P. 0001 - 0011

Summary: Computing and networking * have become an essential part of the daily lives of European citizens. The exponential development of communication networks and information systems * inevitably raises the question of their security, which has become a subject of growing concern to society.

Individuals, public administrations and businesses have reacted by deploying security technologies and security management procedures. However, apart from certain administrative networks, there is no systematic cross-border cooperation on this issue between Member States.

Scope: ENISA's prime aim is to enhance the capability of the European Community, the Member States and the business community to prevent, address and respond to network and information security problems.

Title: Standards for security features and biometrics in passports and travel documents issued by Member State

Type: Council Regulation

Date: 13 December 2004

Ref: (EC) No 2252/2004

Status: N/A

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:NOT)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:NOT)

OJ: O L 385/1

Summary: a coherent approach is needed in the European Union on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems (VIS and SIS II).

The harmonisation of security features and the integration of biometric identifiers is an important step towards the use of new elements in the perspective of future developments at European level, which render the travel document more secure and establish a more reliable link between the holder and the passport and the travel document as an important contribution to ensuring that it is protected against fraudulent use. The specifications of the International Civil Aviation Organisation (ICAO), and in particular those set out in Document 9303 on machine readable travel documents, should be taken into account.

This Regulation is limited to the harmonisation of the security features including biometric identifiers for the passports and travel documents of the Member States. The designation of the authorities and bodies authorized to have access to the data contained in the storage medium of documents is a matter of national legislation, subject to any relevant provisions of Community law, European Union law or international agreements.

In order to ensure that the information referred to is not made available to more persons than necessary, it is also essential that each Member State should designate not more than one body having responsibility for producing passports and travel documents, with Member States remaining free to change the body, if need be. For security reasons, each Member State should communicate the name of the competent body to the Commission and the other Member States.

Objective: Passports and travel documents shall include a storage medium which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.

This Regulation applies to passports and travel documents issued by Member States. It does not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less.

4 COLLABORATION OF MEMBERS STATES IN THE FIELD OF JUDICIAL MATTERS

It is worth mentioning at this stage what are the regulatory documents that allow government to collaborate on judicial matters and exchange information for this purpose. In a second step we will highlight how the privacy framework can protect passengers and what is the limit of information exchanges between MS.

The EU Council voted an Act of 29 May 2000 “establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union”⁸. The purpose of this Convention is to encourage and modernise cooperation between judicial, police and customs authorities by supplementing the provisions and facilitating the application of the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters, and its 1978 Protocol, the 1990 Convention applying the Schengen Agreement and the Benelux Treaty of 1962. Such mutual assistance shall respect the basic principles of each Member State and the 1951 European Convention for the Protection of Human Rights. This Convention deals with Personal data protection. A Member State that has obtained personal data under the Convention may use them only:

- for judicial or administrative proceedings covered by Convention;
- for preventing an immediate and serious threat to public security;
- for any other purpose, with the prior consent of the communicating Member State or of the data subject.

The communicating Member State may ask the Member State to which the personal data have been transferred to give information on the use made of the data.

The main text regarding the collaboration between MS are the following

- Act “establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union”
- Europol Convention to prevent and combat organized and other forms of crime, terrorism, trafficking in persons, offences against children, illegal trafficking in drugs and arms, corruption and fraud.

⁸ Official Journal C 197, 12.07.2000. See also : Communication - Official Journal C 197, 12.07.2000
Communication by the Secretary-General of the Council of the European Union under Article 30(2) of the Convention, established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union. The Communication quotes the declaration made by Luxembourg, at the signing of the Convention, **on the protection of personal data**. See also Council Act of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [Official Journal C 326, 21.11.2001] . See also Explanatory Report - Official Journal C 379, 29.12.2000 . Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (Text approved by the Council on 30 November 2000).

- The Council Framework of 13 June 2002 on combating terrorism

Title: Act “establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union”

Type: Act

Date: 29 May 2000

Ref: N/A

Status: N/A

Link:

http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l33108_en.htm

OJ: OJ C 197 of 12.07.2005

Summary: Legal and judicial systems vary from one Member State to another and there is a strong need to establish cooperation in this respect. The Council accordingly adopted this Convention to facilitate mutual judicial assistance between the authorities of the Member States (police, customs and courts) in order to improve the speed and efficiency of judicial cooperation.

Objective: The purpose of this Convention is to encourage and modernise cooperation between judicial, police and customs authorities by supplementing the provisions and facilitating the application of the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters, and its 1978 Protocol, the 1990 Convention applying the Schengen Agreement and the Benelux Treaty of 1962. Such mutual assistance must respect the basic principles of each Member State and the 1951 European Convention for the Protection of Human Rights.

Relevance for ASSET:

Interception of data communication may be done at the request of a competent authority from another Member State - a judicial authority or an administrative authority designated for the purpose by the Member State concerned. Communications may either be intercepted and transmitted directly to the requesting Member State or recorded for subsequent transmission.

Member States are to consider such requests in accordance with their own national law and procedures. Interception may also take place on the territory of a Member State in which earth satellite equipment is located if the technical assistance of that Member State is not required by the service providers in the requesting Member State. Where interception takes place on the territory of a particular Member State because of the location of the subject but no technical assistance is

needed, the Member State carrying out the interception should inform the other Member State of its action.

Personal data protection

A Member State which has obtained personal data under the Convention may use them only:

- for judicial or administrative proceedings covered by Convention;
- for preventing an immediate and serious threat to public security;
- for any other purpose, with the prior consent of the communicating Member State or of the data subject.

The communicating Member State may ask the Member State to which the personal data have been transferred to give information on the use made of the data.

Title: Europol Convention

Type: Council Act

Date: 26 July 1995

Ref: N/A

Status: N/A

Link:

http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14005b_en.htm

OJ: OJ C 316 of 27.11.1995

Summary: The European Union was made responsible for police and customs co-operation by the 1992 Maastricht Treaty. The 1997 Amsterdam Treaty increased the EU's powers to act in this field, and a special meeting of the European Council in Tampere, Finland, in October 1999, made specific proposals with deadlines and mapped out future developments in the field of justice and home affairs for the European Commission and the Council of the EU.

This Council act establishes the European Police Office (Europol). The objective of Europol is to improve police cooperation between Member States in order to combat terrorism, unlawful drug trafficking and other serious forms of international organised crime. Member States are setting up national units to liaise between Europol and the national authorities responsible for fighting crime.

Objective: The objective of the Europol Convention is to increase all forms of co-operation between member states' law enforcement forces and agencies, including co-operation with and through Europol. Article 29 of the Amsterdam Treaty mentions that this co-operation is needed to prevent and combat organized and other forms of crime, terrorism, trafficking in persons, offences against children, illegal trafficking in drugs and arms, corruption and fraud.

The Commission is fully involved in all the work of the EU on police and customs co-operation. Decisions on actions and concrete measures are taken by unanimity by the Council of the EU. Both member states and the Commission may propose policies and activities.

The Commission participates on behalf of the European Union in meetings of Interpol. In addition it co-operates with member states in a number of Council working groups. The most important ones deal with police co-operation, Europol, terrorism, drug trafficking and the Schengen agreement (Schengen Information System, Sirene, SIS-Tech). The Commission also co-operates with member states to make Europol function, regularly attending the Europol Management Board.

According to the articles 4.6. and 6. of the Europol Convention, this organization is entitled for” **storage in the computerized system**” in compliance of the law. Article 8 (CONTENT OF THE INFORMATION SYSTEM), authorizes Bio-ID data collection and storage.

In particular, Article 14 (STANDARD OF DATA PROTECTION) provides that :

- 1. By the time of the entry into force of this Convention at the latest, each Member State shall, under its national legislation, take the necessary measures in relation to the processing of personal data in data files in the framework of this Convention to ensure a standard of data protection which at least corresponds to the standard resulting from the implementation of the principles of the Council of Europe Convention of 28 January 1981, and, in doing so, shall take account of Recommendation No R(87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987 concerning the use of personal data in the police sector.
- 2. The communication of personal data provided for in this Convention may not begin until the data protection rules laid down in paragraph 1 above have entered into force on the territory of each of the Member States involved in such communication.
- 3. In the collection, processing and utilization of personal data Europol shall take account of the principles of the Council of Europe Convention of 28 January 1981 and of Recommendation No R(87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987. Europol shall also observe these principles in respect of non-automated data held in the form of data files, i.e. any structured set of personal data accessible in accordance with specific criteria.”

One should also take note of the Council Decision of 17 October 2000 “establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention)”⁹. This Council Decision sets up a “Data-protection Secretary”.

⁹ Official Journal L 271 , 24/10/2000 p. 0001 – 0003

Title: Council Framework on combating terrorism

Type: Council Framework Decision

Date: 13 June 2002

Ref: 2002/475/JHA

Status: N/A

Link: [http://eur-](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002F0475&model=guichett)

[lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002F0475&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002F0475&model=guichett)

OJ: L 164/3. 22

Summary: At European Union level, on 3 December 1998 the Council adopted the Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice. The European Union has adopted numerous specific measures having an impact on terrorism and organized crime, such as the Council Joint Action 96/610/JHA of 15 October 1996 concerning the creation and maintenance of a Directory of specialized counter-terrorist competences, skills and expertise to facilitate counter-terrorism cooperation between the Member States of the European Union.

Article 3 (Offences linked to terrorist activities) provides that : “ Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts: (...) (c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).”

Objective: This Framework Decision respects fundamental rights as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they emerge from the constitutional traditions common to the Member States as principles of Community law. The Union observes the principles recognized by Article 6(2) of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union, notably Chapter VI thereof. Nothing in this Framework Decision may be interpreted as being intended to reduce or restrict fundamental rights or freedoms such as the right to strike, freedom of assembly, of association or of expression, including the right of everyone to form and to join trade unions with others for the protection of his or her interests and the related right to demonstrate.

Title: On the use of Passenger Name Record (PNR) for law enforcement purposes

Type: Proposal for a Council framework decision

Date: 06/11/2007

Ref: COM/2007/0654 final - CNS 2007/0237

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007PC0654:EN:NOT>

OJ:

Summary: Currently, arrangements for the transmission of PNR data in the context of the fight against terrorism and transnational organized crime have been concluded between the EU and the United States and Canada and are limited to travel by air. These require that air carriers, which were already capturing the PNR data of passengers for their own commercial purposes, are obliged to transmit these data to the competent authorities of the USA and Canada.

On the basis of an exchange of information with these third countries, the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes. The EU has further been able to learn from the experiences of such third countries in the use of PNR data, as well as from the experience of the UK from its pilot project. More specifically, the UK was able to report numerous arrests, identification of human trafficking networks and gaining of valuable intelligence in relation to terrorism in the two years of the operation of its pilot project.

The European Council of 25-26 March 2004 invited the Commission to bring forward a proposal for a common EU approach to the use of passengers' data for law enforcement purposes. This invitation has been reiterated twice, namely on 4-5 November 2004 in The Hague Program and at the extraordinary Council meeting of 13 July 2005. A European policy in this area had also been announced already in the Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" of 16 December 2003.

Passenger Information Units is subject to a standard of protection of personal data under their national law which at least corresponds to the standards of the Council Framework Decision of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters (2008/977/JHA) and to the level of data protection resulting from the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R(87)15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the use of Personal Data in the Police Sector.

5 INFRASTRUCTURES SECURITY REGULATORY FRAMEWORK

The Commission has published various documents on the protection of critical infrastructures. It is worth mentioning them as aviation security shall be considered as a subset of these.

5.1 Generic Infrastructures:

- Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency.
- Prevention, preparedness and response to terrorist attacks
- The prevention of and the fight against terrorist financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions
- Preparedness and consequence management in the fight against terrorism
- EU Plan of Action on Combating Terrorism – Updater
- European Program for Critical Infrastructure Protection
- Decision C/2005/3179 on the financing of a pilot project containing a set of preparatory actions with a view to strengthening the fight against terrorism
- European Program for Critical Infrastructure Protection
- Identification and designation of European critical infrastructure and a common approach to assess the need to improve their protection
- Council Directive of on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience

Title: Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency.

Type: Regulation (EC)

Date: 10 March 2004

Ref: (EC) No [460/2004](#)

Status: Text with EEA relevance

Link: [http://eur-](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=460)

[lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=460](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Regulation&an_doc=2004&nu_doc=460)

OJ: L 077 , 13/03/2004 P. 0001 - 0011

Summary: Computing and networking have become an essential part of the daily lives of European citizens. The exponential development of communication networks and information systems inevitably raises the question of their security, which has become a subject of growing concern to society.

Individuals, public administrations and businesses have reacted by deploying security technologies and security management procedures. However, apart from certain administrative networks, there is no systematic cross-border cooperation on this issue between Member States.

Objective: ENISA's prime aim is to enhance the capability of the European Community, the Member States and the business community to prevent, address and respond to network and information security problems. It also provides assistance and delivers advice to the Commission and the Member States. In addition, it facilitates and enhances cooperation between different actors operating in the public and private sectors in order to achieve a sufficiently high level of security in the Member States. The Agency may also be called upon to assist the Commission in the technical preparatory work for updating and developing Community legislation.

Tasks: To achieve the objectives set out above, the Agency:

- Collects appropriate information to analyse current and emerging risks and provides the results of the analysis to the Member States and the Commission;
- Provides advice and, if appropriate, assistance within its objectives to the European Parliament, the Commission and the competent European and national bodies;
- Enhances cooperation between the different players in the sector (e.g. consultations, networking);
- Facilitates cooperation between the Commission and the Member States in the development of common methodologies to prevent security problems;
- Contributes to awareness raising and the availability of rapid, objective and comprehensive information on network and information security issues for all users.

This can be achieved by promoting exchanges of best current practice, including methods of alerting users, and by seeking synergy between the public and private sectors;

- Assists the Commission and the Member States in their dialogue with industry to address security-related problems in hardware and software products;
- Tracks the development of standards for security products and services and promotes risk assessment and management activities;
- Contributes to Community efforts to cooperate with third countries and international organisations to promote a global common approach to security issues;
- Gives its own conclusions, guidelines and advice.

Organisation: The Agency comprises:

- A Management Board composed of representatives of the Member States and of the Commission, as well as business representatives, academics and consumers with no voting entitlement;
- An Executive Director appointed by the Management Board on the basis of a list of candidates proposed by the Commission;
- A Permanent Stakeholders' Group established by the Executive Director. The Group will be composed of representatives of information and communication technology businesses, consumers and academic experts. The Group will give the Agency access to the most recent information available in order to be able to respond to network security challenges.

Requests to the Agency

Requests for advice and assistance from the Agency should be addressed to the Executive Director and accompanied by background information explaining the issue to be addressed. Requests may be made by the European Parliament, the Commission or any competent body appointed by a Member State (such as a national regulatory authority).

Independence

For the Agency's advice and opinions to be accepted by individuals, public administrations and businesses, its independence will need to be guaranteed and recognised. Accordingly, the members of the Management Board, the Executive Director and the external experts participating in ad hoc working groups will be obliged to declare the absence of any interest which might place their independence in question.

Transparency

The Agency must ensure that the public and any interested parties are given objective, reliable and easily accessible information, in particular with regard to the results of its work. Access to ENISA documents is in line with the general conditions of [Regulation \(EC\) No 1049/2001](#).

Review clause

Within three years from the Agency's creation, the Commission will carry out an assessment to determine whether the period of time for the Agency's running should be extended, assess the Agency's working practices and impact, and examine the current objectives and mechanisms in place, envisaging, if necessary, the adoption of appropriate changes, in the light of institutional and legal developments in the EU and with specific regard to broader security issues.

Seat

Heraklion, Greece.

Title: Prevention, preparedness and response to terrorist attacks

Type: Communication from the Commission to the Council and the European Parliament

Date: 20 October 2004

Ref: [COM\(2004\)698 final](#)

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0698:EN:HTML>

OJ: Not published in the Official Journal

Summary: Following the attacks in Madrid in March 2004, the European Union (EU) is proposing to intensify and enhance its action to combat terrorism. To this end, the European Commission has decided to increase the involvement of civil society in measures designed to improve its protection. It is also proposing to take preventive action in order to avoid terrorist attacks as well as to ensure that it is fully prepared to respond effectively. As part of this strategy, it would like to make fighting terrorism an integral part of general EU policy.

Context: This Commission communication is a response to the terrorist attacks in Madrid on 11 March 2004. It is one of four communications, all proposing solutions to the priority problems addressed by the European Council in Brussels on 18 June 2004 in the Revised EU action plan on combating terrorism:

- prevention of terrorist attacks and consequence management,
- protection of critical infrastructures,
- financing of terrorism

Protecting and mobilising civil society

The Commission is proposing to involve civil society in the fight against terrorism. This will mean national parliaments, economic agents, civil society organisations and all European citizens participating in the development of effective tools to combat terrorism. The Commission is also convinced there is a need for action in the following areas:

Defending fundamental rights against violent radicalisation. The Commission is aiming to protect fundamental rights and avoid violent social radicalisation. To this end, it plans to work with the Council drawing on existing EU policies and instruments.

Involving the private and public sectors. The Commission intends to encourage the private and public sectors to enter into dialogue, to exchange information and to coordinate methodology in face of the need to step up EU security.

Supporting the victims of terrorism. The Commission plans to develop projects to assist the victims of terrorism. It would also like to raise public awareness of terrorist threat, notably through commemorative action. And so, 11 March 2005 will be the first European Day of the Victims of Terrorism, and the Commission and the Council will mark the occasion by producing a memorial report dedicated to the victims.

Security research

Reinforcing scientific and technical research in the area of security is another of the Commission's key objectives. To this end, it is advocating the funding of a European security research program that would focus on:

- fighting terrorist financing,
- protecting critical infrastructures,
- developing consequence management,
- cyber security.

Title: The prevention of and the fight against terrorist financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions

Type

Date: 20 October 2004

Ref: [COM\(2004\) 700](#)

Status: Communication from the Commission to the Council and the European Parliament

Link:

[http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_700_fr.p
df](http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_700_fr.pdf)

OJ: C 14 of 20 January 2005

Summary: The European Council of June 2004 asked the Commission and the High Representative to prepare an overall strategy to protect critical infrastructure.

The present Communication gives an overview of the actions that the Commission is currently taking on protection of critical infrastructure and proposes additional measures to strengthen existing instruments and to meet the mandates given by the European Council.

Title: Preparedness and consequence management in the fight against terrorism

Type: Communication from the Commission to the Council and the European Parliament

Date: 20 October 2004

Ref: [COM\(2004\)701 final-](#)

Status: N/A

Link:

http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l332_20_en.htm

OJ: Not published in the Official Journal

Summary: This communication deals with preparedness and consequence management in the fight against terrorism, detailing Commission action in two areas: civil protection and health protection. The purpose is to introduce mechanisms and training facilities with a view to protecting and giving maximum assistance to civilians in the event of an attack, in particular bioterrorist attacks. The communication also describes the various existing rapid alert systems.

Scope: The Commission expressed its intention to further strengthen the Community civil protection mechanism along the lines set out below:

- stronger coordination and communication;
- the inter-operability of technical equipment, including civilian-military inter-operability;
- common insignia for the intervention teams to enhance the visibility of European solidarity;
- finding the means to finance transportation of equipment and teams in the event of a disaster.
-

Title: Critical Infrastructure Protection in the fight against Terrorism

Type: Communication from the Commission to the Council and the European Parliament

Date: 20 October 2004

Ref: [COM\(2004\)702](#) final

Status: N/A

Link: http://eur-lex.europa.eu/LexUriServ/site/en/com/2004/com2004_0702en01.pdf

OJ:

Summary: In order to counteract these potential vulnerabilities the European Council requested in 2004 the development of a European Program for Critical Infrastructure Protection (ECIP). Since then, a comprehensive preparatory work has been undertaken, which has included the organisation of relevant seminars, the publication of a Green Paper and discussions with both public and private stakeholders.

Scope: Establishment of an horizontal framework concerning the protection of critical infrastructures in Europe.

- Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan,
- Set up of a Critical Infrastructure Warning Information Network (CIWIN),
- Set up of a Critical Infrastructure Protection (CIP) expert groups at EU level,
- Rules on CIP information sharing processes
- Identification and analysis of interdependencies
- Support for Member States concerning National Critical Infrastructures (NCI) which could optionally be used by the Member States
- Contingency planning
- Set up of accompanying financial measures and in particular the proposed EU program on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP related measures having a potential for EU transferability.

Type of infrastructures adressed :

- energy installations and networks;
- communications and information technology;
- finance (banking, securities and investment);
- health care;
- food;
- water (dams, storage, treatment and networks);

- transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems);
- production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials);
- government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

Damages : cascade effect because of the synergistic effect of infrastructure industries on each other.

Stakeholder: Critical infrastructure can be owned or operated by both the public and the private sector but, in any case, the public sector has a fundamental role to play in making it secure.

Definition for identifying critical infrastructure : Critical infrastructures are those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States.

Criteria for identifying potential critical infrastructure:

- the extent of the geographical area which could be affected,
- magnitude
- effects with respect to time.

Title: EU Plan of Action on Combating Terrorism - Updater

Type: Note from Presidency to Council

Date: 29 November 2004

Ref: N/A

Status: N/A

Link: <http://www.consilium.europa.eu/uedocs/cmsUpload/EUplan16090.pdf>.

OJ:

Summary: The European Council welcomed in its meeting on 17 and 18 June the Action Plan on Terrorism and urged the institutions and Member States to fulfil outstanding commitments within the deadlines established. It stated that it would review the Action Plan twice a year, beginning at its December 2004 meeting.

This document presents this first review, drafted by the Presidency in close cooperation with the Counter Terrorism Coordinator and the Commission. It consists of three parts: this Cover note, an updated matrix, containing all the actions of the Action Plan and an annex showing an overview of the implementation by Member States of EU-legislation in the fight against terrorism as well as ratification of the relevant UN-Conventions.

Objective: Advances on the following seven strategic objectives for the EU's Action Plan against terrorism:

1. To deepen the international consensus and enhance international efforts to combat terrorism;
2. To reduce the access of terrorists to financial and economic resources;
3. To maximize the capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and to prevent terrorist attacks;
4. To protect the security of international transport and ensure effective systems of border control;
5. To enhance the capability of the European Union and of member States to deal with the consequences of a terrorist attack;
6. To address the factors which contribute to support for, and recruitment into, terrorism;
7. To target actions under EU external relations towards priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.

About 150 actions were attached to these strategic objectives. Many of them were accompanied by specified deadlines. Other actions are of an on-going nature or specified in more general terms ('as soon as possible' or 'without delay'). Action should be undertaken by different EU-bodies (Council, Commission) or by Member States. The Matrix, attached to this review of the Action Plan, shows the progress for every specified action.* This Cover note reports in more general terms on the work carries out during the Netherlands Presidency of the Council.

Title: European Program for Critical Infrastructure Protection

Type: Green Paper

Date: 17 november 2005

Ref: [\[COM\(2005\)576 final\]](#).

Status: N/A

Link: [http://eur-](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2005&nu_doc=576)

[lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2005&nu_doc=576](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2005&nu_doc=576)

OJ: N/A

Summary: The main objective of the green paper is to receive feedback concerning possible EPCIP policy options by involving a broad number of stakeholders. The effective protection of critical infrastructure requires communication, coordination, and cooperation nationally and at EU level among all interested parties - the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public.

The Green Paper provides options on how the Commission may respond to the Council's request to establish EPCIP and CIWIN and constitutes the second phase of a consultation process concerning the establishment of a European Program for Critical Infrastructure Protection. The Commission expect that by presenting this green paper, it will receive concrete feedback concerning the policy options outlined in this document. Depending on the outcome of the consultation process, an EPCIP policy package could be put forward during 2006.

Title: Decision C/2005/3179 on the financing of a pilot project containing a set of preparatory actions with a view to strengthening the fight against terrorism

Type: Decision

Date: 15 September 2005

Ref: [COM \(2005\) 3179](#), [C \(2006\) 110](#)

Status: N/A

Link: [http://ec.europa.eu/justice_home/fsj/terrorism/docs/C\(2005\)3179.3.pdf](http://ec.europa.eu/justice_home/fsj/terrorism/docs/C(2005)3179.3.pdf)

OJ: N/A

Summary: Financing of a Pilot Project containing a set of preparatory actions with a view to strengthening the Fight Against terrorism.

Scope: The general objective of the Pilot Project, as defined in the description of Article 18 05 06 of the 2005 general budget of the European Union, is to tap into the full potential of the fight against terrorism and to speed up the Community's activities to further improve the security of citizens and to combat terrorism, in particular by filling the gaps between the various existing Community activities.

The Decision concerns a set of preparatory actions that cover both the award of subventions and calls for tenders.

One of the key elements of the Project is the Pilot Program for Critical Infrastructure which supports activities associated amongst others with the specific objective of enhancing protection of critical infrastructure.

Purpose of the CIP Pilot Project

The general focus of the Pilot Project with regard to the protection of critical infrastructure is to support the forthcoming European Program for Critical Infrastructure Protection.

Future of the CIP Pilot Project

The Commission is committed to a longer-term approach to the protection of critical infrastructures in Europe. Consequently, a number of funding opportunities will become available in the coming months and years.

Title: European Program for Critical Infrastructure Protection

Type: Communication of the Commission

Date: 12 December 2006

Ref: COM(2006)786 final].

Status: Text with EEA relevance

Link: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

OJ:

Summary: Proceed with the implementation of ECIP adopted by the Council in December 2004;

Key principles of EPCIP:

. **Subsidiarity** – The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States concerning National Critical Infrastructures.

• **Complementarity** - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.

• **Confidentiality** - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis. Information sharing regarding CI will take place in an environment of trust and security.

• **Stakeholder Cooperation** – All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.

• **Proportionality** – measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.

• **Sector-by-sector approach** – Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors

The EPCIP framework

The framework will consist of:

- A procedure for the identification and designation of European Critical Infrastructures (ECI),.
- Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN),
- Support for Member States concerning National Critical Infrastructures (NCI) which may optionally be used by a particular Member State.
- Contingency planning.
- An external dimension.
- Accompanying financial measures and in particular the proposed EU program on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013,

Expert groups

The Commission may setup CIP expert groups at EU level to address clearly defined issues and to facilitate public-private dialogue concerning critical infrastructure protection. Expert groups will support EPCIP by facilitating exchanges of views on related CIP issues on an advisory basis. These expert groups constitute a voluntary mechanism in which public and private resources are blended to achieve a goal or set of goals judged to be of mutual benefit both to citizens and the private sector.

National Critical Infrastructures (NCI)

With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States.

The Commission will support the Member States in these efforts where requested to do so. With a view to improving the protection of National Critical Infrastructures each Member State is encouraged to establish a National CIP Program. The objective of such programs would be to set out each Member State's approach to the protection of National Critical Infrastructures located within its territory. Such programs would at a minimum address the following issues:

The identification and designation by the Member State of National Critical Infrastructures according to predefined national criteria. These criteria would be developed by each Member State taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure:

Scope - The disruption or destruction of a particular critical infrastructure will be rated by the extent of the geographic area which could be affected by its loss or unavailability.

Severity - The consequences of the disruption or destruction of a particular infrastructure will be assessed on the basis of:

- Public effect (number of population affected);
- Economic effect (significance of economic loss and/or degradation of products or services);
- Environmental effect;
- Political effects;
- Psychological effects;
- Public health consequences.

Where such criteria do not exist, the Commission will assist a Member State, at its request, in their development by providing relevant methodologies.

- The establishment of a dialogue with CIP owners/operators.
- Identification of geographic and sectoral interdependencies.
- Drawing-up NCI related contingency plans where deemed relevant.
- Each Member State is encouraged to base its National CIP Program on the common list of CI sectors established for ECI.

The introduction of similar approaches to the protection of NCI in the Member States would contribute to ensuring that CI stakeholders throughout Europe benefit from not being subjected to varying frameworks resulting in additional costs and that the Internal Market is not distorted

Title: Identification and designation of European critical infrastructure and a common approach to assess the need to improve their protection

Type: Proposal for a directive fo the Council

Date: 12 December 2006

Ref: SEC(2006) 1648} {SEC(2006) 1654}, [COM\(2006\)787](#) final]. CNS 2006/0276

Status: N/A

Link: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2006&nu_doc=787 .

OJ: N/A

Summary: This proposal for a Directive presents the measures that the Commission is proposing on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection.

Scope: Set up an integrated EU-wide approach to complement and add value to the national programs for critical infrastructure protection already in place in the Member States.

Establishment of a common list of critical infrastructure sectors in order to facilitate the implementation of the sector-by-sector approach to critical infrastructure protection and to ensure:

- adequate levels of protection concerning ECI;
- all ECI stakeholders are subjected to similar rights and obligations;
- the stability of the Internal Market is maintained.

No horizontal provisions on critical infrastructure protection currently exist at EU level. This directive establishes a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures.

Title: Council Directive of on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Type: Council Directive 2008/114/EC

Date: 8 December 2008

Ref: Council Directive 2008/114/EC

Status: Text with EEA relevance

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML)

OJ: L 345 , 23/12/2008 P. 0075 - 0082

Summary: Identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Objectives: Proceed with EC initiatives for the protection of European Critical Infrastructures (ECI) (June 2004, overall strategy to protect critical infrastructures; 20 October 2004, Communication on critical infrastructure protection in the fight against terrorism; 17 November 2005, Green Paper on a European program for critical infrastructure protection (Critical Infrastructure Warning Information Network), December 2005, European program for critical infrastructure protection. In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ("ECIs") and the assessment of the need to improve their protection.

This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ("ICT") sector.

Designation of ECIs

Member State shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI.

The Member States shall inform ECI owner/operators of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be classified at an appropriate level.

Operator security plans (OSP)

An operator security plan ("OSP") procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection.

Security Liaison Officers

Each Member State shall assess whether each designated ECI located on its territory possesses a Security Liaison Officer or equivalent

The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority.

Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned.

Reporting

Member State shall conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.

Member State shall appoint a European critical infrastructure protection contact point ("ECIP contact point").

Title: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience

Type: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection

Date: Brussels, 30.3.2009

Ref: COM(2009) 149 final

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.

OJ:

Summary: Electronic Communication services and networks provide the backbone of the European economy and are vital to citizens, businesses and governments. They are often referred to as critical information infrastructure. Information infrastructures like telephone lines, fibre optic cables and computer networks rule our lives, and they have to be safe. Large parts of the EU economy are relying on this. Many services and processes have become increasingly dependent on the functioning of information and communication technology (ICT) networks. As these networks tend to be decentralised, highly interconnected and interdependent, failures of these infrastructures could cascade and spread beyond national borders. To address this, the European Commission is launching a policy initiative to protect these Critical Information Infrastructures.

Objectives: The Critical Information Infrastructure Protection (CIIP) policy proposed by the Commission focuses on **prevention, preparedness and awareness** and defines a plan for immediate actions to strengthen the security and resilience of CIIs.

To achieve an enhanced level of awareness and preparedness throughout the EU, the Commission proposes the following set of actions:

- Preparedness and prevention: to ensure preparedness by defining a baseline of capabilities and services of national/governmental Computer Emergency Response Teams, creating a European Public-Private Partnership for Resilience and a European Forum of Member States to share information and good policy and operational practices.
- Detection and response: to provide adequate early warning mechanisms, by supporting the development and deployment of a European Information Sharing and Alert System, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems.
- Mitigation and recovery: to reinforce EU defense mechanisms for CII, via the development by Member States of national contingency plans and the organization of

regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination, and by strengthening the cooperation between national/governmental Computer Emergency Response Teams.

- International and EU wide cooperation: to promote EU priorities internationally, by driving a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet, by working with Member States to define guidelines for the resilience and stability of the Internet and by working on a roadmap to promote principles and guidelines at the global level, possibly leveraging strategic cooperation with third countries.
- Criteria for the ICT sector: to support future implementation of EPCIP, by continuing to develop, in cooperation with Member States and all relevant stakeholders, the criteria to identify the European critical infrastructures in the ICT sector.

5.2 Information Technology Infrastructures:

The European Commission has issued various documents on aviation security, especially in the context of the post 09/11 events. But it is worth recalling what is the current regulatory context of the Information Technology sector as more and more passenger data (API, PNR, ETA..) are processed by operators and government agencies and therefore are governed by these.

- Universal Service Directive (2002/22/EC) which deals inter alia with the integrity of public electronic communications networks
- Authorisation Directive (2002/20/EC) which deals inter alia with the integrity of public electronic communications networks
- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems
- Regulation (EC) No 460/2004 of 10 March 2004 establishing the European Network and Information security Agency ENISA

Title: Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

Type: Directive of the European Parliament and of the Council

Date: 7 March 2002

Ref: (2002/22/EC

Status: N/A

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML)

OJ: L 108 , 24/04/2002 P. 0051 - 0077

Summary: This Directive establishes the rights of end-users and the corresponding obligations on undertakings providing publicly available electronic communications networks and services. With regard to ensuring provision of universal service within an environment of open and competitive markets, this Directive defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition. This Directive also sets out obligations with regard to the provision of certain mandatory services such as the retail provision of leased lines.

Objective: Within the framework of Directive 2002/21/EC (Framework Directive), this Directive concerns the provision of electronic communications networks and services to end-users. The aim is to ensure the availability throughout the Community of good quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market.

This Directive establishes the rights of end-users and the corresponding obligations on undertakings providing publicly available electronic communications networks and services. With regard to ensuring provision of universal service within an environment of open and competitive markets, this Directive defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition. This Directive also sets out obligations with regard to the provision of certain mandatory services such as the retail provision of leased lines.

Title: On the authorisation of electronic communications networks and services (Authorisation Directive)

Type: Directive of the European Parliament and of the Council

Date: 7 March 2002

Ref: 2002/20/EC

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:EN:PDF>.

OJ: L 108/21

Summary: The aim of this Directive is to implement an internal market in electronic communications networks and services through the harmonisation and simplification of authorization rules and conditions in order to facilitate their provision throughout the Community.

This Directive shall apply to authorisations for the provision of electronic communications networks and services.

Objective : Convergence between different electronic communications networks and services and their technologies requires the establishment of an authorisation system covering all comparable services in a similar way regardless of the technologies used.

The objective of this Directive is to create a legal framework to ensure the freedom to provide electronic communications networks and services, subject only to the conditions laid down in this Directive and to any restrictions in conformity with Article 46(1) of the Treaty, in particular measures regarding public policy, public security and public health.

This Directive covers authorisation of all electronic communications networks and services whether they are provided to the public or not. This is important to ensure that both categories of providers may benefit from objective, transparent, non-discriminatory and proportionate rights, conditions and procedures

Title: Council Framework Decision on attacks against information systems
Type: Council Framework Decision
Date: 24 February 2005
Ref: 2005/222/JHA
Status: N/A

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML)

OJ: L 069 , 16/03/2005 P. 0067 - 0071

Summary: The objective of this Framework Decision is to improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.

There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.

An effective response to those threats requires a comprehensive approach to network and information security, as underlined in the eEurope Action Plan, in the Communication by the Commission "Network and Information Security: Proposal for a European Policy Approach" and in the Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security [2].

5.3 Aviation sector infrastructures protection

- Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security
- Regulation (CE) No 622/2003 of the Commission of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security
- Commission Regulation (EC) No 1217/2003 of 4 July 2003 laying down common specifications for national civil aviation security quality control programs
- Commission Regulation (EC) No 1486/2003 of 22 August 2003 laying down procedures for conducting Commission inspections in the field of civil aviation security
- Commission Regulation (EC) No 68/2004 of 15 January 2004 amending Commission Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security
- Regulation (EC) No 849/2004 of the European Parliament and of the Council of 29 April 2004 amending Regulation (EC) No 2320/2002 establishing common rules in the field of civil aviation security
- Commission Regulation (EC) No 1138/2004 of 21 June 2004 establishing a common definition of critical parts of security restricted areas at airports
- Commission Regulation (EC) No 781/2005 of 24 May 2005 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security
- Commission Regulation (EC) No 857/2005 of 6 June 2005 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security
- Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security (April 2008)

Title: Regulation establishing common rules in the field of civil aviation security

Type: Regulation (EC) No [2320/2002](#) of the European Parliament and of the Council

Date: 16 december 2002

Ref: [COD/2001/0234](#)]

Status: Text with EEA relevance) – Inter institutional declaration

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R2320:EN:HTML>

Into force: 19/01/2003

OJ: OJ L 355, 30.12.2002,

Summary: The criminal acts committed in New York and Washington on 11 September 2001 show that terrorism is one of the greatest threats to the ideals of democracy and freedom and the values of peace, which are the very essence of the European Union.

The protection of the citizen within the European Community should at all times be ensured in civil aviation by preventing acts of unlawful interference.

Objectives:

1. The main objective of this Regulation is to establish and implement appropriate Community measures, in order to prevent acts of unlawful interference against civil aviation.
2. The additional objective is to provide a basis for a common interpretation of the related provisions of the Chicago Convention, in particular its Annex 17.
3. The means of achieving the objectives set out in paragraphs 1 and 2 shall be:
 - (a) the setting of common basic standards on aviation security measures;
 - (b) the setting up of appropriate compliance monitoring mechanisms.

Definition of Common Security standards

1. The common basic standards on aviation security measures are based on the current recommendations of European Civil Aviation Conference (ECAC) Document 30 and are laid down in the Annex.
2. The necessary measures for the implementation and the technical adaptation of these common basic standards shall be adopted in accordance with the procedure referred to in Article 9(2), due consideration being given to the various types of operation and to the sensitivity of the measures relating to:

- (a) performance criteria and acceptance tests for equipment;
- (b) detailed procedures containing sensitive information;
- (c) detailed criteria for exemption of security measures.

3. The appropriate authority of a Member State may, on the basis of a local risk assessment, and where the application of the security measures specified in the Annex to this Regulation may be disproportionate, or where they can not be implemented for objective practical reasons, adopt national security measures to provide an adequate level of protection, at airports:

- (a) with a yearly average of 2 commercial flights per day; or
- (b) with only general aviation flights; or

(c) with commercial activity limited to aircraft with less than 10 tonnes of Maximum Take Off Weight (MTOW) or less than 20 seats, taking into account the particularities of such small airports.

The Member State concerned shall inform the Commission of these measures.

4. The Commission shall examine whether the measures adopted by a Member State in accordance with paragraph 3 are justified for objective practical reasons and provide an adequate level of protection. If the measures do not comply with these criteria, the Commission shall take a decision in accordance with the procedure referred to in Article 9(3); in such case the Member State shall revoke or adapt them.

National civil aviation security program

1. Within 3 months following the entry into force of this Regulation, each Member State shall adopt a national civil aviation security program in order to ensure the application of the common standards referred to in Article 4(1) and the measures adopted in accordance with Article 4(2) by the date specified in these measures.

2. Notwithstanding that, within a Member State, one or more bodies or entities may be involved in aviation security, each Member State shall designate an appropriate authority responsible for the coordination and the monitoring of the implementation of its national civil aviation security program.

3. Within 6 months following the entry into force of this Regulation, each Member State shall require its appropriate authority to ensure the development and implementation of a national civil aviation security quality control program so as to ensure the effectiveness of its national civil aviation security program.

4. Each Member State shall ensure that their airports and air carriers providing service from that State establish, implement and maintain airport and air carrier security programs appropriate to meet the requirements of its the national civil aviation security program. These programs shall be submitted for approval to and monitored by the appropriate authority.

5. Each Member State shall require the appropriate authority to ensure the development and implementation of a national civil aviation security training program.

Title: Commission Regulation laying down measures for the implementation of the common basic standards on aviation security

Type: Commission Regulation

Date: 4 April 2003

Ref: (EC) No [622/2003](#)

Status: Text with EEA relevance

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0622:EN:HTML>

Into force: 19 April 2003.

OJ: 05/04/2003 P. 0009 - 0010

Summary: This Regulation contains detailed implementing measures for improving aviation security. In order to prevent unlawful acts, the Annex to the Regulation is classified, for security reasons, as an 'EU restricted' document, which is not for the public domain.

Scope: Recommendations for the implementation of common basic standards for aviation security throughout the European Union. A Regulation is the most suitable instrument for this purpose.

In accordance with Regulation (EC) No 2320/2002 and in order to prevent unlawful acts, the **measures laid down in annex to this Regulation should be secret and not be published.**

For this purpose it is necessary to permit a distinction between airports in the light of local risk assessment. Therefore, the Commission should be informed of airports that are considered to present a smaller risk.

This Regulation lays down the necessary measures for the implementation and technical adaptation of common basic standards regarding aviation security to be incorporated into national civil aviation security programs.

Those measures shall be secret and shall not be published. They shall be made available only to persons duly authorised by a Member State or the Commission.

Title: Common specifications for national civil aviation security quality control programs

Type: Commission Regulation

Date: 4 July 2003

Ref: EC N° 1217/2003

Status: Text with EEA relevance

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:169:0044:0048:EN:PDF>.

OJ: L 169/44

Summary: This Regulation lays down the common specifications for the national civil aviation security quality control program to be implemented by each Member State. This includes establishing common requirements for quality control programs, a common methodology for the audits to be undertaken and common requirements for auditors.

Scope: The development and implementation of a national civil aviation security quality control program by each Member State is essential to ensure the effectiveness of its national civil aviation security program in accordance with Article 5(3) of Regulation (EC) No 2320/2002.

Specifications for the national civil aviation security quality control program to be implemented by the Member States should ensure a harmonised approach in this respect. Therefore a Regulation is the most suitable instrument for this purpose.

The monitoring of national civil aviation security quality control programs at Community level requires a harmonised approach to the assessment of compliance at national level.

To be effective, audits to be undertaken under the responsibility of the appropriate authority should be carried out regularly. They should not be restricted as to the subject, stage or moment at which they are carried out. They should take the most suitable forms to ensure their effectiveness.

Title: Commission Regulation of laying down procedures for conducting Commission inspections in the field of civil aviation security

Type: Commission Regulation

Date: 22 August 2003

Ref: (EC) No [1486/2003](#)

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:213:0003:0006:EN:PDF>.

OJ: L 213 of 23 August 2003

Summary: The Member States and the competent authorities shall cooperate with the Commission so that inspectors can conduct their inspections in a transparent, effective, harmonised and consistent manner. The Regulation contains rules on the notification, preparation, performance and conclusion of inspections.

Scope: Definition of procedures for conducting Commission inspections in the field of civil aviation security

In order to monitor the application by Member States of Regulation (EC) No 2320/2002 the Commission should conduct inspections starting six months after the entry into force of that Regulation. The organisation of inspections under the supervision of the Commission is needed to verify the effectiveness of national civil aviation security quality-control programs.

The Commission should coordinate with the Member States the schedule and preparation of Commission inspections. Its inspection teams should include qualified national auditors made available by the Member States.

Commission inspections should be carried out according to a set procedure, including a standard methodology.

Sensitive information relating to inspections should be treated as classified information.

The Commission should take into account the activities of Member States and examine the activities, procedures, training programs and facilities of intergovernmental organisations to make the most efficient use of technical knowledge and resources, and to achieve a harmonised, cooperative approach in the field of civil aviation security, wherever possible.

The measures provided for in this Regulation are in accordance with the opinion of the Committee instituted by Article 9(1) of Regulation (EC) No 2320/2002,

Title: Commission Regulation of laying down procedures for conducting Commission inspections in the field of civil aviation security

Type: Commission Regulation

Date: 22 August 2003

Ref: (EC) No [1486/2003](#)

Status: Text with EEA relevance

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:213:0003:0006:EN:PDF>.

OJ: **L 213 of 23 August 2003**

Summary: The Member States and the competent authorities shall cooperate with the Commission so that inspectors can conduct their inspections in a transparent, effective, harmonised and consistent manner. The Regulation contains rules on the notification, preparation, performance and conclusion of inspections.

Scope: Definition of procedures for conducting Commission inspections in the field of civil aviation security

This Regulation lays down procedures for conducting Commission inspections to monitor the application by Member States of Regulation (EC) No 2320/2002 at the level of each Member State and each individual airport. The inspections shall be conducted in a transparent, effective, harmonised and consistent manner

Title: Measures for the implementation of the common basic standards on aviation security

Type: Commission Regulation

Date: 15 January 2004

Ref: No 68/2004

Status: N/A

Link: [http://eur-](http://eur-lex.europa.eu/Notice.do?mode=dbl&lng1=en,fr&lang=&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=490472:cs&page=&hwords=null)

[lex.europa.eu/Notice.do?mode=dbl&lng1=en,fr&lang=&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=490472:cs&page=&hwords=null](http://eur-lex.europa.eu/Notice.do?mode=dbl&lng1=en,fr&lang=&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=490472:cs&page=&hwords=null)

OJ: L 10/14

Summary: The annex to Regulation No 622/2003 laying down measures for the implementation of the common basic standards on aviation security, as amended by Regulation No 68/2004, which was not published in the Official Journal of the European Union , has no binding force in so far as it seeks to impose obligations on individuals. In particular, the measures adapting the list of articles prohibited in the security restricted areas and on board an aircraft attached as an annex to Regulation No 2320/2002 establishing common rules in the field of civil aviation security, in so far as they are set out in the annex to Regulation No 622/2003, cannot be enforced against individuals.

Title: Corrigendum to Regulation establishing common rules in the field of civil aviation security

Type: Proposal for a regulation of the European Parliament and of the Council

Date: 29 April 2004

Ref: COM/2003/0566 final, [COD/2003/0222](#)]

Status: N/A

Link: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=185573

Into force: 20/05/2004

OJ: 29/06/2004 P. 3 - 4

Summary: The Commission proposes to amend Regulation (EC) 2320/2002 with an amendment of a technical nature that seeks to rectify operational problems inadvertently caused by the Regulation, as follows:

In Article 4(3) the Regulation permits the application of equivalent levels of security than those explicitly prescribed in the legislation at airports used only by small aircraft, general aviation or airports used infrequently, on the grounds that investment in expensive security equipment would be inappropriate. Most commercial airports - even very large ones - have separate facilities that are used exclusively by small aircraft and general aviation. For all intents and purposes these are separate aerodromes. However, the Regulation does not permit them to be considered as such.

The Commission proposes, in a new paragraph 4(3a), permitting Member States to designate areas of large airports as autonomous small airports for the purposes of security. This is conditional on a notification procedure for flights departing from such demarcated areas of airports, so as to ensure that levels of security are not compromised at arriving airports. A new definition covering demarcated areas of airports is also added.

The proposed change will maintain the high levels of aviation security within the European Union that are mandated in Regulation 2320/2002, but will facilitate their efficient application at the areas of airports used by small aircraft.

Title: Commission Regulation establishing a common definition of critical parts of security-restricted areas at airports

Type: Regulation (EC) No 849/2004 of the European Parliament and of the Council

Date: 21 June 2004

Ref: (EC) No 1138/2004

Status: Binding in its entirety and directly applicable in all Member States

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R1138:EN:HTML)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R1138:EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R1138:EN:HTML)

Into force: 1 July 2004 .

OJ: [Official Journal L **221 of 22 June 2004**].

Summary: The critical parts of security-restricted areas are any part of an airport to which departing passengers or baggage have access. The definition applies for the duration of the period in which persons and baggage are present in such places

Scope: Common definition of the critical parts of security restricted areas, namely those parts of an airport to which departing passengers, after screening, have access and those parts through which departing hold baggage, after screening, may pass or in which it may be held.

All staff, including flight crews, and the items they carry, should be screened before being allowed access to the critical parts of security restricted areas.

An exemption should be allowed for parts of an airport through which departing hold baggage, after screening, may pass or in which it may be held, if the baggage, having been secured could be handled by unscreened staff without compromising the level of security. Measures should be taken to ensure that such secured baggage has not been tampered with before being loaded onto an aircraft.

At airports where very few staff have access to security restricted areas, a balance should be struck between the need to ensure security and the need to ensure operational effectiveness.

Unscreened staff should be allowed access into critical parts of security restricted areas of an airport only on condition that they are at all times escorted by screened and authorised staff.

Where other unscreened persons may have had access to critical parts of security restricted areas, a full security search should be carried out in order to ensure that critical parts of security restricted areas do not contain prohibited articles. Where critical parts are not continuously maintained as such, then immediately before being re-established as such they should be subjected to a full security search.

The measures provided for in this Regulation are in accordance with the opinion of the Committee instituted by Article 9(1) of Regulation (EC) No 2320/2002,

Title: Amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security

Type: Commission Regulation

Date: 24 May 2005

Ref: (EC) No 781/2005

Status: Text with EEA relevance

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:131:0024:0025:EN:PDF)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:131:0024:0025:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:131:0024:0025:EN:PDF)

OJ: L 131 24

Summary: The Commission is required, by virtue of Regulation (EC) No 2320/2002, to adopt measures for the implementation of common basic standards for aviation security throughout the European Community.

Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security ⁽²⁾ was the first act containing such measures. There is a need for measures giving precision to the common basic standards

In accordance with Regulation (EC) No 2320/2002 and in order to prevent unlawful acts, the measures laid down in the Annex to Regulation (EC) No 622/2003 should be secret and should not be published. The same rule necessarily applies to any amending act

6 PRIVACY PROTECTION REGULATORY FRAMEWORK

6.1 Main Directives and regulatory documents

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
- Regulation of the European Parliament and of the Council of 18th December 2000
- Data Protection Regulation (EC) 45/2001 relating to processing by Community institution and bodies
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

The Charter of Fundamental Rights of the European Union recognises in Article 8 the right to the protection of personal data. This fundamental right is set forth in a European legal framework on the protection of personal data consisting in particular of the Data Protection Directive 95/46/EC and the ePrivacy Directive 2002/58/EC as well as the Data Protection Regulation (EC) 45/2001 relating to processing by Community institution and bodies.

This legislation lays down several substantive provisions imposing obligations on data controllers and recognizing rights of data subjects. It also prescribes sanctions and appropriate remedies in cases of breach and establishes enforcement mechanisms to make them effective. However, this system may prove insufficient when personal data is disseminated worldwide through ICT networks and the processing of data crosses several jurisdictions, often outside the EU. In such situations the current rules may be considered to apply and to provide a clear legal response. Furthermore, a competent authority to enforce the rules may also be identified. However, considerable practical obstacles may exist as a result of difficulties with the technology used involving data processing by different actors in different locations and there may be hurdles intrinsic to the enforcement of national administrative and court rulings in another jurisdiction, especially in non-EU countries¹⁰.

¹⁰ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs)

Title:	Protection of Individuals with regard to Automatic Processing of Personal Data
Type:	Convention from the Council of Europe
Date:	28.I.1981
Ref:	N/A
Status:	N/A
Link:	http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
OJ:	N/A

Summary: The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Objectives: The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

- that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;
- that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;
- that it will also apply this convention to personal data files which are not processed automatically.

Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

Title: Protection of individuals with regard to the processing of personal data and on the free movement of such data

Type: Directive of the European Parliament and of the Council

Date: 24 October 1995

Ref: 95/46/EC

Status: N/A

Link: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

OJ: L 281/35

Summary: In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1

Scope: This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

This Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, by a natural person in the course of a purely personal or household activity

Objective The objective of Directive 95/46 is to harmonize national laws on processing personal data and protect the rights and freedoms of the persons concerned, in particular their right to privacy.

- This Directive applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
- It does not apply to the processing of personal data: by a natural person in the course of a purely personal or household activity; in the course of an activity, which falls

outside the scope of Community law, such as operations concerning public security, defense or State security¹¹.

- The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when this processing is lawful. The guidelines relate to: data quality; making data processing legitimate; special categories of processing; information to be given to the data subject; the data subject's right of access to data; the data subject's right to object to data processing; confidentiality and security of processing; notification of processing to a supervisory authority.
- The Member States are to determine more precisely, within the limits of the guidelines mentioned above, the conditions under which the processing of personal data is lawful.
- Provisions on judicial remedies and sanctions for any breach of a person's rights.
- Transfers of personal data from a Member State to a third country with an adequate level of protection are authorised. However, they may not be made to a third country which does not ensure this level of protection, except in the cases of the derogations listed.
- Each Member State is to provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Directive.
- A Working Party on the Protection of Individuals with regard to the Processing of Personal Data is set up, composed of representatives of the national supervisory authorities, representatives of the supervisory authorities of the Community institutions and bodies, and a representative of the Commission.

The deadline for the implementation of the legislation in the Member States was set on 24.10.1998 and the Date of entry into force 13.12.1995

Relevance of the Directive to the ASSET project

With reference to the Directive 95/46, aviation stakeholders shall declare to the DPC (Data Protection Commissioners) of their respective countries any storage or processing of personal data. This regulatory framework includes the various frequent travelers programs, whether they are generated by airlines, airports or governments as a means to provide expedited procedures to their favorite customers.

Currently , DPC are very cautious that facilitation systems respect the following rules:

¹¹ SECTION VI - EXEMPTIONS AND RESTRICTIONS - Article 13 - Exemptions and restrictions : 1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security; (b) defense; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others.

Proportionality :

- This means that technical system shall correspond to the risk incurred. As an example , access control procedures are justified to proceed to restricted areas.

Causality

- This means that equipment shall match the objectives they have been designed for. In other words a Frequent Traveller Program shall be used to facilitate the control procedure of passengers and not to detect suspects or unwanted travelers, unless this purpose has been specified in the design of the system.

It is important to precise that the Directive does not allow to transmit pax data to countries which do not provide the same level of protection as it is the case for the Member States. Even though this article opens the way to standardization and interoperability of Frequent Flyer in the MS, based on shared databases, it constitutes an obstacle to sharing these data with countries outside of EU. This explains the difficulty to implement the PNR program between EU and the US as many data provided to the carriers are protected by the EC Directive.

Title: Processing of personal data and the protection of privacy in the telecommunications sector

Type: Directive of the European Parliament and of the Council

Date: 15 december 1997

Ref: 97/66/EC

Status: No longer in force

Link: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML)

OJ: L 024 , 30/01/1998 P. 0001 - 0008

Summary: This Directive provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

The provisions of this Directive particularize and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons.

This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Relevance of the Directive to the ASSET program: The 97/46 Directive complements the objective of the 95/46 in the context of telecommunication networks. As mentioned above, it constitutes an obstacle to the transmission of passenger data to countries which do not provide the same level of protection of privacy.

As it is the case for Directive EC 95/46, privacy protection rules do not apply to the cases which fall outside of the scope of Community law, eg. Third Pillar (Titles V and Titles VI of the Treaty on European Union), where authorities are allowed to process data for the purpose of state security and defense.

Title: On the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Type: Regulation No 45/2001 OF THE European Parliament and of the Council

Date: 18 December 2000

Ref: (EC) No 45/2001

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF>.

OJ: 12.1.2001

Summary: A Regulation is necessary to provide the individual with legally enforceable rights, to specify the data processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies.

The aim is to ensure both effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms and the free flow of personal data between Member States and the Community institutions and bodies or between the Community institutions and bodies for purposes connected with the exercise of their respective competences.

To this end measures should be adopted which are binding on the Community institutions and bodies. These measures should apply to all processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

This Regulation does not affect the rights and obligations of Member States under Directives 95/46/EC and 97/66/EC. It is not intended to change existing procedures and practices lawfully implemented by the Member States in the field of national security, prevention of disorder or prevention, detection, investigation and prosecution of criminal offences in compliance with the Protocol on Privileges and Immunities of the European Communities and with international law.

Objective : The Regulation of the European Parliament and of the Council of 18 December 2000, "on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data ", provides in its article 3 (scope) that :

- 1.This Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.
- 2.This Regulation shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of

personal data which form part of a filing system or are intended to form part of a filing system.”

Title: Processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Type: Directive of the European Parliament and of the Council

Date: 12 July 2002

Ref: 2002/58/EC

Status:

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>

OJ: L 201 , 31/07/2002 P. 0037 - 0047

Summary: This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Relevance to the ASSET program : The objective of this directive is to amend and complement the legal framework on privacy defined by both EC Directives 95/46 and 97/66. It takes into account the recent developments on internet and mobile networks so that to make sure that fundamental rights are preserved, in particular:

- (2) This Directive seeks to respect the fundamental rights and observes the principles recognized in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.
- Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, **regardless of the technologies used.** That Directive should therefore be repealed and replaced by this Directive.

- (5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. **Access to digital mobile networks** has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.
- (6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.
- (7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, **in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.**
- (9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and **taking particular account of the objectives of minimizing the processing of personal data and of using anonymous or pseudonymous data** where possible.
- (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to **activities which are not governed by Community law.** Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the **ability of Member States to carry out lawful interception of electronic communications,** or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. **Such measures must be appropriate, strictly proportionate to the intended purpose** and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.
-
- (22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed..... this Directive should not prevent such information from being further

stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

- (23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction..... The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged
-
- (26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. **Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time.....** Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.
- (30)Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.
- (32)Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.
- (35)The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.
- (38)Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

- (39) Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.
- (46) It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected.
- This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Objective of the Directive: It is worth mentioning that this Directive is particularly adapted to the context of air transport as it mentions the various technologies that will be used to facilitate the airports procedures:

- Mobile networks (internet and mobile check in systems)
- Data storage
- Data processing
- Data Transmission

As this is the case for both preceding Directives, governments may restrict the obligations provided for to safeguard their national security (i.e. State security), defense, public security, and for the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC, in line with Article V and Article VI of the Union Treaty (Second and Third Pillars)¹². In this case, and for the purpose of State security, government might joint their forces by collaborating and process personal data

¹² The second pillar establishes common foreign and security policy (CFSP), enshrined in Title V of the Treaty on European Union. This replaces the provisions of the Single European Act and allows Member States to take joint action in the field of foreign policy. This pillar involves an intergovernmental decision-making process which largely relies on unanimity. The Commission and Parliament play a modest role and the Court of Justice has no say in this area. The third pillar concerns cooperation in the field of justice and home affairs (JHA), provided for in Title VI of the Treaty on European Union. The Union is expected to undertake joint action so as to offer European citizens a high level of protection in the area of freedom, security and justice. The decision-making process is also intergovernmental.

Title: Processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Type: Council Framework Decision

Date: 27 November 2008

Ref: 2008/977/JHA

Status: N/A

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML>

OJ: L 350 , 30/12/2008 P. 0060 - 0071

Summary: The exchange of personal data within the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Program, should be supported by clear rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in respect of such cooperation between the Member States while fully respecting fundamental rights of individuals. Existing instruments at the European level do not suffice; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3] does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, nor, in any case, to processing operations concerning public security, defence, state security or the activities of the State in areas of criminal law.

Objective: This Framework Decision **applies only to data gathered or processed by competent authorities for the purpose of the prevention, investigation,** detection or prosecution of criminal offences or the execution of criminal penalties. This Framework Decision should leave it to Member

States to determine more precisely at national level which other purposes are to be considered as incompatible with the purpose for which the personal data were originally collected. In general, further processing for historical, statistical or scientific purposes should not be considered as incompatible with the original purpose of the processing.

The scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States. No conclusions should be inferred from this limitation regarding the competence of the Union to adopt acts relating to the collection and processing of personal data at national level or the expediency for the Union to do so in the future.

In order to facilitate data exchanges within the Union, Member States intend to ensure that the standard of data protection achieved in national data processing matches that provided for in this Framework Decision. With regard to national data processing, this Framework Decision does not preclude Member States from providing safeguards for the protection of personal data higher than those established in this Framework Decision.

This Framework Decision should not apply to personal data which a Member State has obtained within the scope of this Framework Decision and which originated in that Member State.

6.2 Privacy enhancing technologies (PET)

Title: A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”

Type: Communication from the Commission to the Council, the European Parliament, the European Economic and social Committee and the Committee of the regions.

Date: 27 November 2008

Ref: COM(2006) 251

Status: N/A

Link: http://ec.europa.eu/information_society/doc/com2006251.pdf.

OJ: N/A

Summary: The purpose of the present Communication is to revitalise the European Commission strategy set out in 2001 in the Communication “Network and Information Security: proposal for a European Policy approach”². It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS).

National governments need to be able to identify and implement best practice in policymaking, as well as demonstrate commitment to these policy objectives by managing their own information systems in a secure manner. Public authorities, in Member States and at EU level, have a key role to play in properly informing users to enable them to contribute to their own security and safety. Raising awareness on NIS issues and providing appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices should be priorities. To this end, examining the feasibility of **creating a European multilingual information sharing and alert system**, which would build upon and link together existing or planned national public and private initiatives, could be a major goal for ENISA.

The global dimension of network and information security challenges the Commission, both at international level and in coordination with Member States, to increase its efforts to **promote global cooperation on NIS**, notably in implementing the agenda adopted at the World Summit on the Information Society (WSIS) in November 2005.

Title: Promoting Data Protection by Privacy Enhancing Technologies (PETs)

Type: Communication from the Commission to the European Parliament and the Council

Date: 2 May 2007

Ref: COM(2007) 228 final

Status: Text with EEA relevance

Link: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF>.

OJ: N/A

Summary: Article 17 of the Data Protection Directive lays down the data controller's obligation to implement appropriate technical and organisational measures and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive. A further step to pursue the aim of the legal framework, whose objective is to minimise the processing of personal data and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult.

The purpose of this Communication, which follows from the First Report on the implementation of the Data Protection Directives, is to consider the benefits of PETs, lay down the Commission's objectives in this field to promote these technologies, and set out clear actions to achieve this goal by supporting the development of PETs and their use by data controllers and consumers.

6.3 Standardisation activities addressing privacy issues

Title: Technical Management Board privacy task force . Draft final report 9

Type: Communication from the Commission to the European Parliament and the Council

Date: September 200

Ref: ISO/IEC JTC 1/SC 27 - IT SECURITY TECHNIQUES,

Status: Working Group 5: Identity management and privacy technologie

Link: http://www.iso.org/iso/iso_technical_committee.html?commid=45306

OJ: N/A

Summary: Covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.

6.3.1 Standards in development

Title: Information technology -- Security techniques -- Privacy reference architecture

Type: International standard

Date: 2008-09-19

Ref: [JTC 1/SC 27](#)

Status: N/A

Link: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45124

Title: Information technology -- Security techniques -- Privacy framework

Type: International standard

Date: 2010-11-27

Ref: ISO/IEC CD 29100

Status: N/A

Link: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45123

Summary: Under the umbrella of JTC 1/SC 27 Project 29100, the privacy framework standard will :

- Provide a framework for defining privacy requirements as they relate to personally identifiable (PI) information processed by any information and communication system in any jurisdiction;
- Set a common privacy terminology, define privacy principles when processing PI information, categorize privacy features and relate all described privacy aspects to existing security guidelines

Title: Information technology -- Security techniques -- Privacy reference architecture

Type: International standard

Date: 2009-04-06

Ref: ISO/IEC CD 29100

Status: N/A

Link: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45124

Summary: Under the umbrella of JTC 1/SC 27, Project 29101, the privacy reference architecture will

- **Describe best practices** for a consistent, technical implementation of privacy requirements as they relate to the processing of personally identifiable (PI) information in information and communication systems;
- **Cover the various stages in data life cycle management** and the required **privacy functionalities** for PI data in each data life cycle, as well as positioning the roles and responsibilities of all involved parties;
- **Present a target architecture** and provide guidance for planning and building system architectures that facilitate the proper handling of PI data across system platforms;
- **Set out the necessary prerequisites** to allow the categorization of data and control over specific sets of data within various data life cycles

Title:	Inventory of Data Protection Auditing Practices
Type:	CEN initiative
Date:	April 2006
Ref:	CWA 15499-01:2006
Status:	CWA, CEN Workshop Agreement
Link:	http://www.cen.eu/CENORM/Sectors/Sectors/ISSS/Activity/wsdpp.asp
OJ:	N/A

Summary: The aim of Workshop DPP is to help organizations to comply with the Data Protection Directive and relevant national legislation by facilitating harmonization of practice, developing the understanding and predictability of detailed or sector practices, contributing to resolving ICT technical compliance issues, and encouraging consistency of assessment and oversight. The Workshop has taken due regard of the provisions of the relevant EU legislation on data protection and privacy, including Directives 95/46/EC, and 2002/58/EC.

CEN ISSS WS DPP (Information Society Standardization System, Data Protection & Privacy)

The objective of the workshop is to develop and deliver three CEN Workshop Agreements (CWA) on the following topics:

- **1) European Best Practices** will provide with a complete and comprehensive management system helping firms processing and controlling data in a series of particular topics.
- **2) Audit tools for manager** will provide data managers with a set of tools helping them measuring their level of compliance and improving their processes.
- **3) Voluntary Technology Dialogue System** will set up a formal voluntary framework for dialogue and outline processes between industry and regulators, with the aim of ensuring new products, technologies and services comply with the data protection and privacy directive as transposed in the EU member states.

This CWA is subdivided in two parts:

- CWA 15499-01:2006; Part I: Baseline Framework - The protection of Personal Data in the EU
- CWA 15499-02:2006; Part II: Checklists, questionnaires and templates for users of the framework - The protection of Personal Data in the EU

Title:	Inventory of Data Protection Auditing Practices
Type:	CEN initiative
Date:	April 2005
Ref:	CWA 15262:2005
Status:	CWA, CEN Workshop Agreement
Link:	ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15262-00-2005-Apr.pdf .
OJ:	

Summary: Each organization processes personal data. Within the EU, processing personal data is subject to data protection legislation. Attention for the management of protecting personal data is important, not only because data protection is mandatory under the EU directive (95/46/EC) but also because data subjects expect their data is handled in accordance with their expectations and their privacy is respected. Therefore trust, privacy and data protection are inextricably linked.

A breach of privacy can destroy trust and consequently damage relationships between customers and their suppliers, employees and their employers, citizens and the government institutions etceteras. Since personal data is being processed using more and more complex and interrelated information and communication technologies, privacy (including security) and trust are essential conditions for doing (e-) business and running (e-) government processes. Because of the number of current and expected transactions and activities carried out online, privacy, data protection and trust become more and more important values.

Importance of a data protection audit

Trust can be realized by demonstrating compliance. Assurance whether personal data is handled in compliance with data protection principles can be provided by a data protection audit. An audit (especially when carried out on a regular basis) helps the organization:

- to identify non-compliance issues and/or to detect risks in it's own data protection management infrastructure;
- to maintain compliance with relevant privacy laws.

The data protection audit contributes to preventing privacy breaches (resulting in sanctions and/or negative reports). Also, for some organizations the data protection audit is an important tool in showing compliance with data protection requirements (e.g. via a privacy certificate); a positive outcome can be used by these organizations as a publicity advantage with regard to the competitors.

Title: Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization

Type: CEN initiative

Date: April 2005

Ref: CWA 15263:2005

Status: CWA, CEN Workshop Agreement

Link: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15263-00-2005-Apr.pdf>.

OJ: N/A

Summary: From a legal perspective, the rules with regard to protection of personal data are mainly laid down in Article F of the Treaty of the European Union, Article 7 of the European Charter of Fundamental Rights, Article 8 of the European Convention on Human Rights, the European Directive 95/46/EC⁴, hereinafter: DPD, and the European Directive 2002/58/EC⁵. The principles of these texts have been further refined and explained in numerous other documents, e.g. the Opinions and Recommendations adopted by the “Article 29 Working Party”⁶. Besides, self-regulatory initiatives have been developed, such as codes of conduct, industry guidelines and seal programs.

The DPD sets out a number of basic requirements for the lawful processing and acceptable use of personal data. There are nine privacy principles incorporated into the DPD⁷. The principles are collations of articles from the DPD that are frequently applied together⁸. These may be summarized as follows:

- 1. Intention and Notification - The processing of personal data must be reported in advance to the Data Protection Authority or a privacy officer (where applicable), unless the processing system in question has been exempted from notification.
- 2. Transparency - The person involved must be aware of who is processing his personal data and for what purpose.
- 3. Finality principle - Personal data may only be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- 4. Legitimate Ground for Processing - The processing of personal data must be based on a foundation referred to in national legislation, such as consent, contract, legal obligation, justified interest and such like. For special data, such as health, stricter limits prevail.
- 5. Quality - The personal data must be correct, accurate, sufficient, to the point and not excessive in relation to the purpose in question.
- 6. Data subject’s rights - The data subjects involved have the right to have access and to correct their data as well as the right to object.

- 7. Security - Providing appropriate security for personal data held within IT-systems is one of the cornerstones of the DPD. Measures of technical and organizational nature suitable and proportional to the sensitivity of the personal data and the nature of possible risks have to be taken to avoid potential harm should the PII be misused or disclosed in an unauthorized matter.
- 8. Processing by a processor - If processing is outsourced to a processor, it must be ensured that he will observe the instructions of the controller.
- 9. Transfer of personal data outside the EU - In principle, the transfer of personal data to a country outside the EU is permitted only if that country offers adequate protection

Title: Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)

Type: CEN initiative

Date: April 2005

Ref: CWA 15292:2005

Status: CWA, CEN Workshop Agreement

Link: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15292-00-2005-May.pdf>.

OJ: N/A

Summary: Contracts have to work within national law so European precedents or standard forms have to allow for national variations over matters such as legal formalities but they are still capable of achieving a high level of commonality. Contracts have long been considered as useful tools in achieving data protection compliance.

The achievement of a form of contract accepted by all sides of an industry, containing generic phraseology that can be adapted according to the individual circumstances, is a most valuable form of business standard for trade. A good example is the agreement on INCOTERMS standardization of business trading terms, which has practically eliminated contractual disputes over misunderstandings in traded goods. In the study produced by the Initiative for Privacy Standardization in Europe (IPSE) Project Team, it was recommended to take a broad view of the term “standardization”. In other words, it would be helpful to have a wide consensus agreement on the generic phraseology that can be used in contracts; this would be a very valuable and indeed essential area to be addressed.

A contract allows some or all of the obligations of a data controller to be transferred in an accountable way to the recipients of personal data, whether they are processors, agents, affiliates, business partners, or other organizations. Depending on applicable law, many different types of provisions may be relevant here. There is clearly no need to re-invent the wheel every time a contract is drafted, and indeed there are standard contracts for a variety of purposes. In view of this it was decided to undertake work within the CEN/ISSS Workshop on Data Protection and Privacy (WS/DPP), to define generic contract clauses and an implementation guide. The work was partly sponsored by the European Commission under its eEurope Support action program.

6.3.2 Update on recent standardization activities

Following the three most recent meetings of the International Organization for Standardization/ International Electrotechnical Committee Joint Technical Committee 1/ Subcommittee 27/ Working Group 5 (Identity Management and Privacy Technologies) (ISO/IEC JTC1/SC 27/WG 5, hereafter referred to as WG 5), held October 2007 in Lucerne, Switzerland, April 2008 in Kyoto, Japan and October 2008 in Limassol, Cyprus, we are able to provide a brief description of the projects currently underway in WG 5 and to show their current status.

WG 5 is currently working on seven (7) numbered projects and two (2) Standing Documents (SDs). WG 5 also agreed to initiate two new work items and to extend a study period. A brief description of each project and its current status follows:

1) **ISO 24760 – A Framework for Identity Management.** This standard defines and establishes a framework for Identity Management (an integrated concept of processes, policies and technologies that enable organizations and individual entities to facilitate and control the use of identity information in their respective relations). The Framework standard is intended to help designers, architects, evaluators, and users of IT systems building solutions related to identity controls, and to improve adherence to compliance regulations, internal security and privacy policies.

The current version of this document (5th Working Draft (WD)) was released 15 September 2008. An interim version (5th WD (Revised)), incorporating comments received prior to the October 2008 meeting, was released 14 November 2008. The next full version (6th WD) is due for release 1 February 2009.

2) **ISO 24761 – Authentication Context for Biometrics.** This standard defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion.

The current schedule calls for this document to be published as an International Standard (IS) in November 2008.

3) **ISO 24745 – Biometric Template Protection.** This standard is focused on the essential security mechanisms required for the protection of biometric templates.

Two major areas of concern have been identified with respect to this project, which have delayed progress. The first concerned the lack of technical maturity of some of the key technologies (cancelable biometrics and biometric encryption) being proposed for protection of biometric templates. The second concern was that of possible overlap between this standard and standards being developed in SC37 (Biometrics). Recent discussions have identified a way to address these concerns, so the document can continue to progress.

In addition, it has been recognized that there will be links to other WG 5 projects (e.g., to ISO 29100 (Privacy Framework), ISO 29101 (Privacy Reference Architecture) and ISO 29115 (Entity Authentication Assurance)) and harmonization with these projects will be required.

The current draft of this document (3rd WD) was released 20 June 2008. The next version (4th WD) is due for release 1 February 2009.

4) **ISO 29100 – A Privacy Framework.** This standard provides a framework for defining privacy safeguarding requirements as they relate to personally identifiable information (PII) processed by any information and communication system in any jurisdiction. The framework is applicable on an international scale and sets a common privacy terminology, defines privacy principles when processing PII, categorizes privacy features and relates all described privacy aspects to existing security guidelines.

The framework is intended to serve as a basis for desirable additional privacy standardization initiatives, for example a technical reference architecture, the use of specific privacy technologies, an overall privacy management, assurance of privacy compliance for outsourced data processes, privacy impact assessments and engineering specifications. In order to become widely accepted and to effectively form the basis for additional work, the framework needs to be general in nature and address system-specific issues on a high-level. The privacy framework needs to be closely linked to existing security standards that have been widely implemented into practice.

The current version of this document (1st Committee Draft (CD)) was released 12 December 2008.

5) **ISO 29101 – Privacy Reference Architecture.** This standard is intended to provide a privacy reference architecture model that will describe best practices for a consistent, technical implementation of privacy requirements as they relate to the processing of personally identifiable

information (PII) in information and communication systems. It will cover the various stages in data life cycle management and the required privacy functionalities for PI data in each data life cycle, as well as positioning the roles and responsibilities of all involved parties.

The privacy reference architecture will present a target architecture and will provide guidance for planning and building system architectures that facilitate the proper handling of PI data across system platforms. It will set out the necessary prerequisites to allow the categorization of data and control over specific sets of data within various data life cycles.

The current version of the document (2nd WD) was released 20 June 2008. The next version (3rd WD) is due for release 1 February 2009.

6) **ISO 29115 – Entity Authentication Assurance.** This standard provides objective and vendor neutral guidelines for identity assurance. It also describes the guidelines or principles that must be considered in identity assurance and the rationale for why they are important to an authentication decision. The standard provides a framework for assessing "how close" an identity (individual) is to the correct one and provides guidelines for how the strength of the authentication can be measured. It also provides the basis for a set of identity assurance measures that are general and applicable to a wide range of authentication mechanisms.

This project is a joint effort between ISO (WG 5) and ITU-T (Study Group 17, Question 6) and will result in the publication of a common-text Recommendation (ITU-T) and Standard (ISO). Current efforts are aimed at developing a new Recommendation/Standard based on the harmonization of the Liberty Alliance Identity Assurance Framework (IAF) Specification and 29115.

The current version of this document (3rd WD) was released 20 June 2008. The next version (4th WD) is due for release 1 December 2008.

7) **ISO 29146 – Framework for Access Management.** As a result of discussion at the 3rd WG 5 meeting (Lucerne, October 2007), a proposal was put forward for a new work item on an access management framework. Following balloting, the proposal was deemed to have met the required acceptance criteria and was added as a new project (ISO 29146).

This standard aims to provide a framework for the definition of Access Management and the secure management of the process to access information. This framework would be applicable to any kind of user, individuals as well as organizations of all types and sizes, and should be useful to organizations at any location and regardless of the nature of the activities they are involved in.

It was noted during the Kyoto meeting that there was already an Access Control Framework standard (ISO 10181-3). It was also noted that there must be a careful distinction made between identity management (who you are, what credentials you hold) and access management (what you are allowed to do).

Belgium and Spain are providing co-editors – the same persons as are working on ISO 24760 - Identity Management Framework as the two documents will need to be properly coordinated. The project editors will be tasked to review the existing document to determine what effect it will have on 29146.

The 1st WD of this document (1st WD) is due for release 1 February 2009.

8) **SD 1 – WG 5 Roadmap.** A new version of the WG 5 Roadmap is developed at each international meeting. The Roadmap provides a visual representation of the possible standards projects that might be undertaken by WG 5, as well as providing some sense of the dependencies between the potential projects.

The software application in use has limited ability to clarify interdependencies and interconnections. The current tree structure suggests a hierarchical relationship of the items, when in fact there is a matrix interdependency in many cases (an attempt has been made to show some of these interdependencies via the cross connections in the diagram).

Future versions of this roadmap will look at other options for displaying the information in the diagram, including structuring the activities into a three tier model, dividing them into “strategic”, “tactical”, and “operational” items, or possibly a two tier model using the categories of “What to do” (a management view) and “How to do” (an engineering view).

9) **SD 2 – Official Privacy Documents List.** This document contains a description and analysis of privacy-related laws, regulations and documents from many countries and legal areas that were identified by ISO members.

The main purposes of this document are to provide comprehensive guidance and explanations to assist individuals, entities and enterprises to address the privacy implications of laws and regulations applied in various countries and to improve the understanding of legal issues, specifications and exemptions related to data privacy and protection applied in these countries.

The current version of SD2 was released 22 July 2008. The next version is due for release 1 February 2009, for updating at the May 2009 WG meeting.

7 ASSET RECOMMENDATIONS

7.1 Recommendations to the ASSET consortium

As Titles V and VI of the EU Treaty do not fall within the scope of Community Law, the project will exclude from its recommendation the storage of information/Databases. Falling under this scope could lead the recommendation as being in breach of Community Law, with important liabilities and potential litigations. Rather than trying to recommend the airport stakeholders products and services close to being in breach with data protection legislations, the consortium must concentrate its efforts by cooperating with DPC to define facilitation systems that may develop further internationally for the recurrent profit of the Air Transport Industry as a whole.

The potential offered by EU DGs Home and Justice (Council and Commission) programs, Europol and Member States are vast enough to closely work with them for the building and adaptation of standards designed by ICAO and implemented by the said Member States through the EU's Institutions.

7.2 How shall ASSET comply with industry standards and international bodies ?

ASSET aims to ensure a wide acceptance of its recommendations by the Air Transport Industry by proposing the various stakeholders with facilitation solutions that can be implemented at each POA, Point Of Activity of the airport controls procedure. We propose to precise how each IT system can be implemented so that not to infringe the privacy framework .

Internet check in

As an example, Internet Check in does not infringe EC Directive 95/46 as it constitutes a facilitation program offered by the carriers to their customers. However, customer database shall be declared to each country DPC as they contains information relevant to the passengers' privacy. The carriers are not allowed to transmit these information to third parties (countries) ,which are not subject to privacy rules similar to the EU MS

Passenger Information Unit

Passenger data processing (EU PNR, PIU, Passenger Information Unit) ; as this initiative is still under consideration at EU DG JLS, it is too early to analyze its impact vis à vis the ASSET program.

In any case, it is not a decision taken by the aviation's stakeholders but rather a mandatory procedure to be applied by airlines which does not belong to the scope of the ASSET program.

However, it shall be investigated further – once the final version of the decision framework is available (Q1 2010) how internet methods can be used (pre-registration, what kind of information shall be delivered, etc... ?) to speed up the process.

Border control

As many airports are planning automated border control procedures, it shall be recommended to avoid the storage of biometrics and personal data to avoid infringing the rule of Directive 95/46. In this context, it is strongly recommended to use government's ID (Passports, national ID cards) to avoid airports and airlines to take the responsibility of enrollment procedures. At this stage, it is not clear how EC DG JLS will proceed with their Global Entry / Exit program which includes a Registered Traveler Program with Third Countries like US, Canada, Australia....

Security Control

As there is a debate on prohibited items authentication systems (body scanners, smart corridors, LAGs identification), DPC are currently assessing the various equipment to make sure that recommended equipment do not infringe pax' privacy. In any case, the ASSET consortium shall not make any recommendations that would not meet the current trends on security smart processing.

Boarding

Many devices for smart boarding are currently investigated by airlines to expedite their frequent travelers. Once again, it shall be pointed out that any solution that will be based on the storage /processing of personal data shall be prohibited. Otherwise carriers will have to negotiate with DPC to allow such a system. Concerning the usage of biometrics authentication, it shall be reminded that carriers are not yet allowed to access these data which are still restricted to governments based on the EAC protocol recommended by the EU.

Registered travelers procedure

As recommended by IATA IPF, (Ideal Process Flow), government's ID cards (Passports and National ID) can be used to speed up the border control procedure. Should a prior enrolment be necessary, it shall be performed on a **voluntary basis**. Furthermore, it is important to point out that the biometrics and the traveler's data shall be stored on the smart card only to avoid the storage of biodata on a central server.

8 USE CASE: SCENARIO OF THREE TRAVELLERS USING IT SYSTEMS COMPLIANT WITH EU PRIVACY FRAMEWORK

8.1 Scenario background

The majority of EU countries are now facing the contradictory challenge to automate border crossings due to the increasing number of travelers entering the Schengen Zone and a growing demand to reinforce the control of passports due to the security context of the 09/11. Airlines are also eager to decrease their costs by facilitating check in and boarding activities. In this context, the whole airport process shall be considered as a complex chain involving different stakeholders where advance IT systems will play an increasing role.

As these programs will take many years to be implemented, the present scenario proposes a feasibility approach for the early adoption of internet check in devices, biometrics, digital certificates, eID credentials and Location Base Services (LBS) as part of a global system shared by air transport and government stakeholders to automate the process of passengers across airports until their final boarding phase. To achieve this objective, the scenario will investigate the issues - regulatory, technical and financial - that need to be addressed prior to the implementation of such a system.

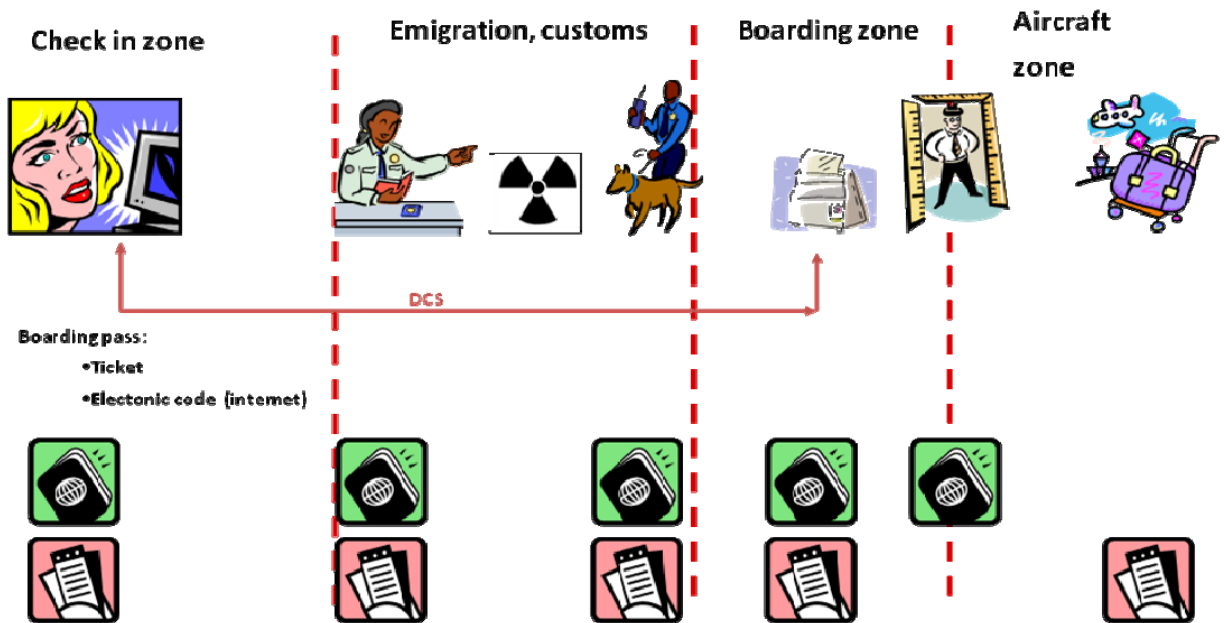
As the EU and US have different views on privacy issues, specific attention will be paid to Directives EC 95/46, EC 97/66 and 2002/52 which provide strong guidelines to avoid the unnecessary storage and processing of personal data and to the transmission of these data to countries which do not respect EU rules for the protection of privacy. This scenario fully takes into consideration geopolitical realities and the particular constraints of Europe (EU countries, Schengen area) rather than focusing on mere technical issues as this is often the case.

The liberalization of communications and the globalization of the world economy has increased the circulation of goods, services, people and trade which has in turn increased the need to travel. This has required governments, and specifically the European Union, to better monitor their flow of visitors. The dreadful events of 11th September 2001 has increased the threat of terrorism and hostile actions against the air transport, often considered as a most visible symbols of the modern economy. On the other hand, advance IT devices are yet considered as a means for both facilitating and enhancing the airport control process.

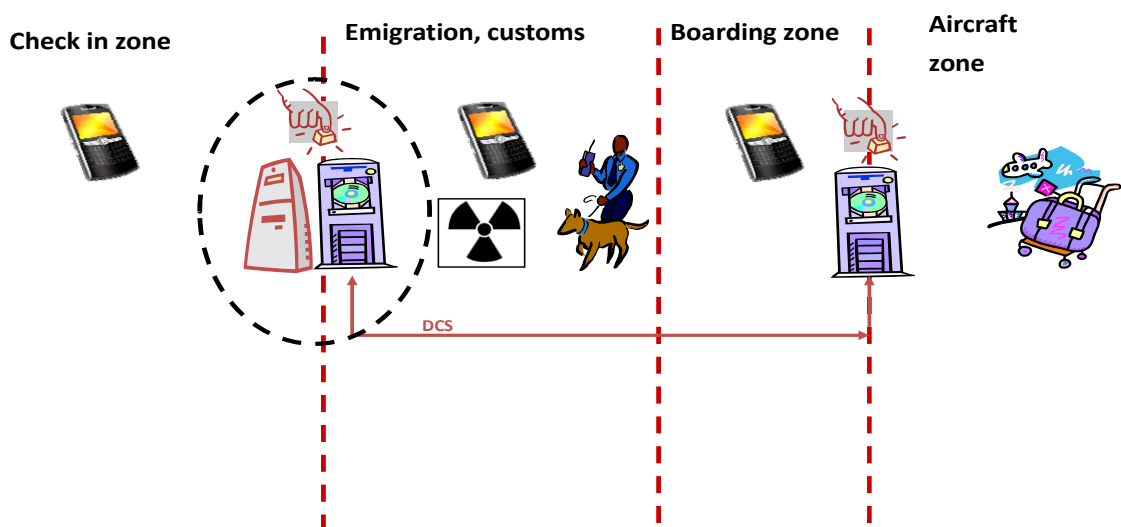
Many endeavors have yet been launched to facilitate airport processes based on modern technology. But it is clear that both governments and air transport stakeholders need to collaborate at international level to ensure that internet check in systems, eID control infrastructures, boarding pass control devices and Location Base Systems are interoperable and thus affordable equipment can be acquired by any airports sharing the same concerns to automate the process of passengers.

This scenario aims to reflect the works carried on by ACI – the Airport Council International – and IATA SPT, an international Interest Group made up of governments, security agencies, professional organizations, technology vendors, airports and airlines....driven by the international syndicate of airlines.

Current process

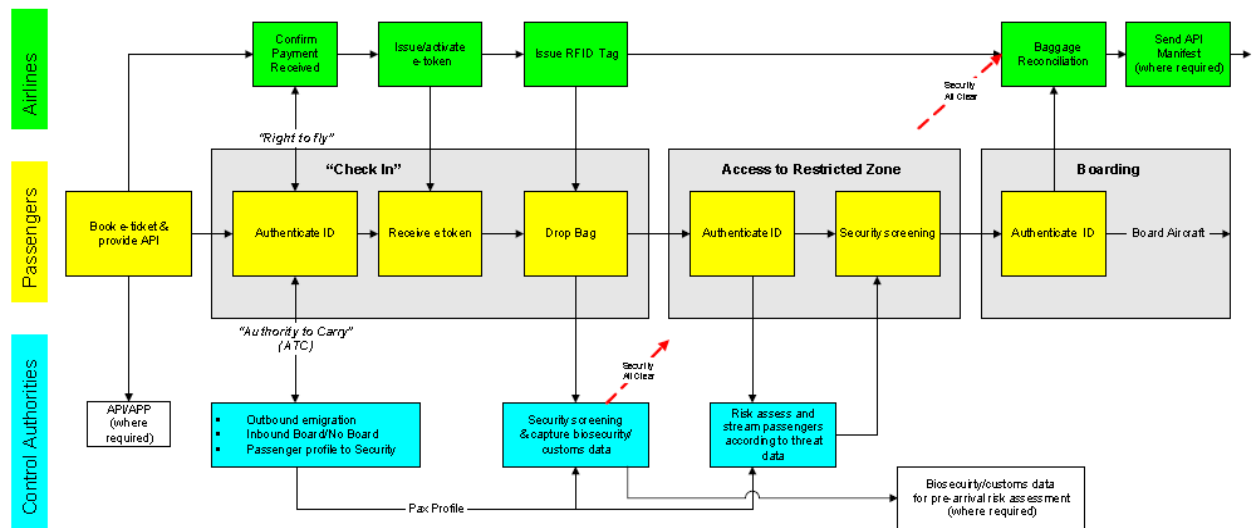


Smart boarding



We propose to base our scenario on the IATA-SPT (Simplifying the Passenger Travel) IPF, Ideal Process Flow and show how new devices like smart phones, RFID and LBS can contribute to enhance even more the facilitation process

Simplifying Passenger Travel : Departures Process - Overview



8.2 The technology response to the growing demand for airport passenger automation.

8.2.1 Step 1: Check in process

Thanks to the pioneering campaign of IATA’s StB (Simplifying the Business) program <http://www.iata.org/stb/index.htm>, most of the carriers (99%) have yet adopted eTicketing measures to replace costly paper boarding passes. But this still requires passengers to check in at airport counters or kiosks based on EKTG codes instead of directly accessing the air side zone. Even though carriers and airports are planning to implement more self service kiosks, there is still a long road for the implementation of fully dematerialized process based on IT devices like smart phones.

In the context of the present scenario, we propose that the check in process be based on two technologies, which are yet considered as standards and widely implemented in the new generations of smart phones like blackberries and PDAs :

- 2DBarcodes
- NFC

The airlines stores the passenger data as usual; they are not shared with airports or government agencies, as required by EC Directives.

8.2.2 Step 2 : Passport control

Many fast track projects to automate passport controls have been carried on so far but without to rely on standard technology (eID, ePassport) as they are mainly based on proprietary enrolment systems due to the originating airport.

In the context of the current scenario, we propose that the border control be based on authenticating passengers by the means of biometrics encrypted in travel documents (eg. Fingerprints or face, on digital photographs in passports). As airlines cannot access the biometrics data stored in passports, pax' ID will be controlled at this stage.

Many endeavors have been launched to automate the border control; government ID document represent the most convenient way as they will facilitate the interoperability of the systems between the MS. In reference to EU Directives on privacy, there is no sharing of personal data with external parties or communication of these to countries outside of the Schengen area.

It is too early at this stage to examine how the future registered travelers programs of the EC with Third countries (US, Canada, Australia, New Zealand...) will be implemented and how they will comply with Privacy Directives since the procedure (enrollment, reciprocity, storage ?) is not yet defined.

Furthermore, as the EU PNR program will be implemented as of 2010, we anticipate that our travelers will fill in ETA (Electronic Travel Authorization) form 48 hours before departure from their home computers. As required by the PIU programs, PNR are sent to the carriers to be further processed by an agency. These PNR are not stored by the airlines. The Passenger Information Unit does not store either these data once processed, but they are communicated to the Ministry of Interior of the Departing country for international flights.

8.2.3 Step 3 : Security check

Considering the ban on LAGs (Liquid And Gels), we anticipate that passengers will no longer undergo physical searches and bottles confiscations. In the context of the next coming years, it is assumed that automated IT devices will be used for both authenticating LAGs and identify prohibited items. The following technology will be recommended

- Body scanners
- Smart corridors
- LAGs authentication systems

DPC are very cautious to control that pax' privacy is not threatened by these new devices. Great attention is currently paid to body scanners for two main reasons: medical issues (micro

waves impact on health) and passengers' intimacy. Various solutions are currently considered such as partially blurring intimate parts of the bodies.

8.2.4 Step 4 : Boarding

Currently, the boarding process is still based on paper control even though a great effort has been done on internet check in and electronic ticketing. In the context of the current scenario, we recommend a seamless process that will allow both controlling passengers based on the same system that is used at check in stage and authenticating them by their biometrics to avoid boarding pass exchanges. But this requires that the airlines can access the biometrics in the chip; which it not yet allowed. This issue shall be discussed with national DPC

8.3 Facilitation scenario compliant with EC privacy directives

As an example, we describe a seamless airport process for the following passengers leaving from Frankfurt. Various IT systems will be put in place, but we have taken care that there is no data storage nor communication of information between the stakeholders or to other countries.

Richard is a 50 year old US citizen working in Germany and flying back to Atlanta (outside of the Schengen Zone) for his vacations

Alex is a 35 year old engineer flying for business purposes to Madrid (Schengen Zone)

Cherry is a 20 years old female Indian student leaving Germany for Delhi after a 6 months scholarship in an University.

As the time frame of the scenario is 3-5 years in the future, the EU DG JLS (Justice liberty Security) has implemented its Global Entry program meaning that :

- A Registered Traveller scheme has been implemented between EU and US based on a prior enrolment of frequent travellers (eg. Richard)
- Non-EU citizen (eg. Cherry) are registered at their entry of the Schengen Zone to make sure that they do not overstay the agreed visa period (6 months)

We assume that our three individuals are IT familiar and will take advantage of any facilities offered by airlines and government to speed up their airport process. Both Richard and Alex have recently bought a new Blackberry device, namely the version including an NFC chip allowing to securely communicate with terminals.

As **Richard** is a non-EU citizen resident in Germany, he has enrolled to the Registered Traveler program at the Bundes Ministry of Interior offices from Frankfurt. The system is connected to black list databases of both Germany and the TSA, Transportation Security Administration in Washington. The enrolment procedure might include the capture of a digital image of his face (as it is stored in his passport delivered by the DOT) and an electronic certificate which confirms that the US passport is referenced by the ICAO PKD (Public Key Directory).

We assume that the Registered Traveler Program has been agreed by the following countries: EU MS, US, Canada, New Zealand, Japan and South Korea, allowing government agencies to automate border control requirements at both departure and arrival. Citizens can enroll indifferently in their home countries or location of residence.

Cherry arrived in Frankfurt exactly six months ago and was registered based on the new Entry / Exit system managed by EU DG JLS. The Entry / Exit procedure has confirmed that the Schengen visa holder is the right individual by matching her fingerprints against the templates stored in the chip of her visa and her passport. The system recorded her name, the date and location of her entry.

The Frankfurt airport is equipped with the last technology of the Fast Track Program shared with participating airlines, Lufthansa, Iberia and Indian Airlines, meaning that it is equipped with an automated passport control interfaced with the DCS (Departure Control System) of the airlines.

Pre-flight procedures

As our travellers are familiar with airport facilitation systems, we assume that they have performed the following tasks:

Richard's processes

- Richard benefits of the Lufthansa "Speed Flyers" program which allows frequent travelers to receive their boarding passes as MMS 2D BarCodes. The IATA standard uses existing codes such as Aztec and Datamatrix which are used extensively in Europe and North America. Both are proven technologies and can be read by a single scanner type that is cost effective and readily available globally.
- Richard has confirmed his flight 24 hours in advance directly from his Blackberry, by selecting a menu via his Frequent Flyer number and a PIN code. This check in menu can be activated both from a computer or a PDA; in response, he has received an MMS 2D BarCode confirming his flight booking.

- Richard has filled in 24 hours in advance the EU PNR form downloaded from the LH website, mentioning selected fields defined by EC DG JLS such as name, date of birth, nationality, passport issuance data, etc.... These data have been processed by the German PIU, Passenger Information Unit, a Department of the Ministry of Interior based in Berlin.
- As an US citizen, Richard does not need to fill in the US ESTA, the Electronic System for Travel Authorization (ESTA), which is yet mandatory for citizen of Visa Waiver Countries before boarding a flight to the US.

Alex' processes

- Alex is a member of Iberia "Gran Viajero" program. But he has selected the NFC option to communicate his flight references to the DCS, rather than the MMS 2D BarCode.
- As he doesn't leave the Schengen Zone, Alex is not subject to fill in a PNR form in advance.

Cherry's process

- As an Indian national, Cherry does not benefit of the Registered Traveller program agreed between EC and several Third Countries.
- But she is affiliated to the Indian Airlines "Speed Flyers" program which same as for Richard allows downloading the her boarding pass via an MMS 2D BarCode.
- She has filled 24 hours in advance her EU PNR form which has been reconciled with her Entry/Exit registration data by the Bundes Ministry of Interior in Berlin.
- As Cherry is very keen on perfumes, she has bought from the airport internet website several samples of Hermes for her family. But she needs to pick up the bottles at the airport.

Airport procedures

Richard's processes

- As Richard has already checked in in advance, he only needs to drop his luggage at a specific automated baggage system shared by participating airlines. The procedure is the following:
 - Display of his MMS boarding pass to a 2D Barcode reader
 - The MMS image calls the DCS, Departure Control System, of LH, which confirms that he has checked in and is registered on the next flight to Atlanta
 - Biometrics authentication by matching the digital image stored in his passport against his proper face.
 - Upon confirmation of his ID and flight booking, a device automatically inserts an RFID tag on his luggage.
 - The RFID tag has the following advantage,
 - It is automatically dispatched by the conveyor to the Atlanta containers
 - It can be retrieved from the A/C belly, should Richard decide not to leave for personal or medical reasons.

- To access the airside zone, Richard shall yet undergo the automated passport control. Thus, he proceeds to a border control booth and holds his passport to activate the contactless EAC (Enhanced Access Control) procedure as follows:
- The passport authenticates the digital certificate of the police reader and allows an access to its chip.
- The police reader authenticates the US digital certificate as registered in the ICAO PKD, Public Key Directory and reads the digital template of his face.
- The reader authenticates the personal certificate of his passport as a member of the EU/US registered traveler program.
- A camera compares his face against the template stored in his passport.
- Once the biometric system has confirmed that he is really Richard, he is asked to display his MMS 2D Barcode boarding pass on a reader which performs the following tasks :
- Access to the DCS to confirm that he is really booked on the LH flight to Atlanta
- Access to the PIU (Passenger Information Unit) of the Ministry of Interior which delivers an ETA, Electronic Travel Authorization, based on clearing his PNR data.
- The system then performs an unicity check to confirm that only Richard stays in the booth and is not accompanied by another traveler or carrying a child with him. Once these tasks have been carried on, a door opens to give access to security control zone.
- Richard then proceeds to a smart corridor equipped with metal, EDS and LAG detectors to authenticate prohibited items like arms and explosives. There is no staff present at this stage unless a suspicious goods is detected for more advanced investigation
- Richard can then enjoy the various facilities of the airport like connecting to the wi-fi network by validating his frequent flyer access code. When he buys goods from duty free shops, he confirms his flight booking from his Blackberry 2D Barcode.
- As Richard spends too much time in the duty free zone, he receives a message from LH on his Blackberry to recall him the boarding limit.
- At the boarding stage, Richard will perform the following tasks:
- Display his MMS 2D Barcode, which access the DCS and confirms his registration on the Atlanta flight
- Authenticate against a biometrics camera by matching his face against the digital template stored in his passport, to avoid boarding pass exchanges as it is the case for certain destinations.
- It shall be pointed out that Richard has not been controlled in the airport by any staff (airlines, government, security) and that the facilitation process allows to streamline an integrated process from ticketing until ultimate boarding based on the airline DCS and government controlled credentials.

Alex' processes

- As Madrid is located within the Schengen Zone and because Axel only carries an hand luggage, the departing procedure is much simpler than Richard's. He only needs to access the airside zone based on the following procedure
- Activate the NFC menu of his Blackberry in front of a reader that connects to the DCS (Departure Control System) of the airlines (As Alex prefers the NFC option to the MMS 2D BarCode chosen by Richard).

- The DCS confirms that he is booked on the Iberia flight to Madrid and opens a turnstile giving access to the security control zone.
- Axel then proceeds to a smart corridor equipped with metal, EDS and LAG detectors to authenticate prohibited items like weapons and explosives. There is no staff present at this stage unless a suspicious goods is detected for more advanced investigation.
- Axel can then enjoy the various facilities of the airport like connecting to the wi-fi network by validating his frequent flyer access code. When he buys goods from duty free shops, he confirms his flight booking from his Blackberry NFC menu.
- At the boarding stage, Axel will perform the following tasks:
- Activate the NFC menu of his Blackberry against a reader to confirm his registration on the Madrid flight
- Authenticate against a biometrics camera which ,by matching his finger against the digital template stored in his national ID card (he doesn't need a passport to travel within the Schengen zone), to avoid boarding pass exchanges as it is the case for certain destinations.
- It shall be pointed out that Axel has not been controlled by any staff (airlines, airport, government, security) and that the facilitation process allows to streamline an integrated process from ticketing until ultimate boarding based on the airline DCS and a government controlled credential (national ID card).

Cherry's processes

- As Cherry has already checked in by internet or her cell phone, she only needs to drop her luggage from the automated baggage system shared by participating airlines. The procedure is the following:
- Display of her MMS boarding pass to a 2D Barcode reader
- The MMS image calls the DCS, Departure Control System, of Indian Airlines, which confirms that she has checked in and is registered on the flight to Delhi.
- Biometrics authentication of Cherry based on the digital image stored in her ePassport against her proper face.
- Upon confirmation of her ID and flight booking, a device automatically inserts an RFID tag on her luggage which is absorbed by the conveyor and dispatched to the Delhi containers
- To access the airside zone, Cherry cannot undergo the automated passport control as India has not yet agreed on a Registered Traveler scheme with EU. Thus, she proceeds to the police booth which is equipped with a face biometrics authentication system. Her passport activates the contactless EAC (Enhanced Access Control) procedure as follows:
- The passport authenticates the digital certificate of the police reader and allows an access to its chip.
- The reader authenticates the Indian digital certificate as registered to the ICAO PKD, Public Key Directory, and reads the digital template of Cherry's face.
- A camera compares her face against the stored template
- Once the biometric system has confirmed that she is really Cherry, she is asked to display her Schengen Visa. The system checks first that she is its right holder by comparing the biometrics template to the sample stored in her passport, then verifies

that she has not overstayed the visa period based on the Entry / Exit procedure of the VIS (Visa Information System). (If this is the case, she may undergo a complementary check and not yet being allowed to leave).

- If these checks are positive, she is then asked by the police officer to display her MMS 2D Barcode boarding pass on a reader to perform the following tasks:
- Confirm that she is really booked on the Indian Airlines flight to Delhi.
- Access to the PIU (Passenger Information Unit) of the Ministry of Interior which delivers an ETA, Electronic Travel Authorization, based on the processing of her PNR, unless she has overstays her visa period.
- Once these tasks have been carried on, a door opens to give access to security control zone.
- Cherry then proceeds to a smart corridor equipped with metal, EDS and LAG detectors to authenticate prohibited items like arms and explosives. There is no staff present at this stage unless a suspicious goods is detected for more advanced investigation
- Cherry can then enjoy the various facilities of the airport like picking up the perfumes she has ordered from the duty free website. If a complementary check is needed, she displays her 2D Barcode boarding pass from her cell phone.
- At the boarding stage, Cherry will perform the following tasks:
- Display her MMS 2D Barcode boarding pass, which access the DCS and confirm her registration on the Delhi flight
- Authenticate against a biometrics camera which will match her face against the digital template stored in her passport, to avoid boarding pass exchanges as it is the case for certain destinations.
- It shall be pointed out that Cherry has only been controlled by police staff as India is not yet a member of a Registered Traveller alliance with the EU. As she holds an ICAO compliant ePassport, she could undergo an automated passport control, but the enrolment rules for Registered Indian citizens has not yet been defined by the EU.
- But the facilitation process currently put in place allows to streamline an integrated process from ticketing until her ultimate boarding based on the airline DCS and government controlled credentials.

8.4 Abbreviations

1	AAS	2	Integrated Airport Apron Safety Fleet Management
3	ACI	4	Airport Council International
5	AEA	6	Association of European Airlines
7	AIRNET	8	Airport network for mobiles surveillance and alerting
9	ATC	10	Air Traffic Control
11	ATM	12	Air Traffic Management

13	AVITRACK	14	Aircraft surroundings, categorized Vehicles & Individuals Tracking
15	CAA	16	Civil Aviation Administration
17	DCS	18	Departure Control System
19	DLR	20	Deutsches Zentrum für Luft und Raumfahrt e.V. / German Aerospace Center (German Aerospace Research Institut)
21	EC	22	European Commission
23	ETDS	24	Explosive trace detection systems
25	FAA	26	Federal Aviation Authority
27	FAR	28	Federal Aviation Regulation
29	H&S	30	Hub and Spoke
31	IATA	32	International Air Transport Association
33	ICAO	34	International Civil Aviation Organization
35	IFR	36	Instrument Flight Rules
37	ILS	38	Instrument Landing System
39	IPF	40	Ideal Process Flow
41	JIT	42	Just In Time
43	LCC	44	Low Coast Carrier
45	N/A	46	Not Available
47	PAX	48	Passenger
49	RFID	50	Radio Frequency Identification
51	SPT	52	Simplifying Passenger Travel
53	TAM	54	Total Airport Management
55	TAPE	56	Total Airport Performance and Evaluation

57	ULD	58	Unit Load Device
59	USC	60	United States Code
61	WP	62	Work Package
63	WLU	64	Work Load Unit