Brussels, 28.2.2013
SWD(2013) 47 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union

{COM(2013) 95}
{SWD(2013) 48}
{SWD(2013) 49}

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union

1. PROCEDURAL ISSUES AND CONSULTATIONS OF INTERESTED PARTIES

1.1. Background

The present impact assessment report and the legislative proposal it accompanies[1] should be seen in the context of the progressive establishment of a European model of integrated management of the external borders. The legislative proposal is part of the "next generation of border checks" package which is a strategic initiative in the Commission's work programme for 2012[2]. This package responds to two major and interconnected challenges: how to efficiently monitor travel flows and movements of third-country nationals across the external border for the Schengen area as a whole, and how to ensure that border crossings are fast and simple for the growing number of regular travellers that constitute the vast majority of border crossers, i.e. those fulfilling all entry conditions. This report addresses the first challenge: a separate report[3] and legislative proposal address the second one. The two reports and proposals are not dependent on each other as regards their implementation but the setting up of an entry/exit system is a condition for providing fully automated border crossings for certain groups of third-country nationals, as further analysed in the second report; hence the entry/exit system strongly influences to which extent a Registered Traveller Programme can meet its objectives of facilitating travel flows.

In its Communication of 13 February 2008 *preparing the next steps in border management in the European Union*[4] the Commission suggested the establishment of an entry/exit system (EES). Such a system would entail the registration of the personal data together with the dates of entry and exit of each third-country national admitted for a short stay when they cross the external borders. The 2008 Communication was accompanied by an impact assessment report[5].

The proposals were subsequently endorsed in the Stockholm Programme[6] agreed by the European Council in December 2009, which reaffirmed the potential for an entry/exit system allowing Member States to share data effectively while safeguarding data protection. The proposal to set up an EES was therefore also included in the Action Plan Implementing the Stockholm Programme[7].

A Commission Communication in July 2010 on information management in the area of freedom, security and justice presented an overview of the EU-level measures in place or planned that regulate the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migration management[8]. It set out the conditions the Commission will apply in future when assessing any new system in this area including the

---

1 Add ref when known

2 COM(2011) 777 final

3 [RTP Add ref when known]

4 COM (2008) 69 final.

5 SEC(2008) 153 and Preparatory study to inform an Impact Assessment in relation to the creation of an automated entry/exit system at the external borders of the EU and the introduction of a border crossing scheme for bona fide travellers ('Registered Traveller Programme') made by GHK and Entry/Exit Technical Feasibility study made by Unisys. Studies are published on the website: http://ec.europa.eu/home-affairs/doc_centre/borders/borders_schengen_en.htm

6 'An open and secure Europe serving and protecting the citizens', Official Journal of the European Union of 4.5.2010, C 115/1.

7 COM(2010)171 final.

8 COM(2010)385 final.

approach of 'privacy by design'.[9] It also drew the lessons of the development of other major systems in this area such as VIS and SIS II and concluded that 'as a possible safeguard against cost overruns and delays resulting from changing requirements, any new information system in the area of freedom, security and justice, particularly if it involves a large-scale IT system, will not be developed before the underlying legal instruments setting out its purpose, scope, functions and technical details have been definitively adopted.' It emphasised too that particular attention must be paid to the initial design of governance structures and pointed to the role that the new IT agency[10] could have in providing technical advice.

Strengthening security through border management is one of the five strategic objectives of the Internal Security Strategy[11] and includes the enhanced use of new technology for border checks, citing an entry-exit system.

The Visa Information System (VIS), which manages the exchange of short-stay visa data between the Schengen and Schengen Associated States, started operations on 11 of October 2011 at the consulates in North Africa, the Near East and the Gulf Region and 20 days after go-live of the VIS also at the border crossing points (verification of visas against the VIS).

The Conclusions of the European Council of 23 and 24 June 2011 called for work on "smart borders" to be moved forward rapidly. In response, the Commission adopted on 25 October 2011 a new Communication on the various options and the way ahead.[12] It concluded that the implementation of an EES would provide the Union with accurate data on travel flows in and out of the Schengen area at all parts of its external borders and on overstayers.

Against this background, the present impact assessment examines different implementation options in order to find the *best possible way to implement the entry/exit system*. However, the impacts of the whole EES are analysed based on the specific options.

The present report constitutes both the ex-ante evaluation required for programmes or activities occasioning expenditure from the EU Budget, and the impact assessment that will accompany the legislative proposal for the EES.[13]

1.2. Consultation of interested parties

The Commission considered that before proposing any new initiative, an in-depth technical assessment and debate with all relevant stakeholders on the future architecture of the EES was necessary.

---

9 Privacy by design means embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a proposed purpose and granting data access only to those entities that 'need to know.'

10 Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

11 COM (2010) 673 final

12 COM(2011) 680 final

13 Article 21 of Commission Regulation (EC, EURATOM) No 2342/2002 of 23.12.2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the EU, OJ L 357, 31.12.2002.

Based on the discussions with and positions received from different stakeholders on 2008 impact assessment and communication, the Commission identified the following interest groups as the most relevant stakeholders for consultation: Member States, the European Parliament, the European Data Protection Supervisor (EDPS), civil society and the private sector. Third-country nationals travelling to the EU are not as such represented in any given interest group in an organised way and it is therefore by definition difficult to obtain their views. The consultation was carried out in several ways:

- publishing the 2008 Impact Assessment and Communication;
- presenting a comprehensive technical assessment and compilation of Member States' responses (three meetings with the Committee on Immigration and Asylum and two meetings with two different working groups of the European Security and Research Innovation Forum (ESRIF));
- distributing questionnaires to Member States;
- organising seminars and meetings including specific expert meetings and stimulating debate with discussion papers;
- meeting stakeholders bilaterally;
- publishing the 2011 Communication;
- giving presentations on the EES at different fora.

Member States

The entry/exit system has been under discussion at meetings with Member States' experts since 2008. Discussions with Member States were held in the Council on the basis of two questionnaires prepared by the French and Czech Presidencies. According to the replies submitted by Member States there is a consensus on the added value of the system and on the purpose of storing the information, namely to detect overstayers and to calculate the length of stay.

Further consultations with Member States both at expert and ministerial level took place in 2011 and early 2012.

In preparation for the conference on Innovation Border Management organised by the Danish presidency and the Netherlands on 2 and 3 February 2012 in Copenhagen, Member States replied to the Presidency's questionnaire on the RTP and the EES[14]. According to these replies, a majority of Member States support the establishment of the EES but most of them did not indicate their implementation preferences.

The summary of the conference prepared by the Presidency[15] concluded that the EES would bring significant benefits for the border check procedure and the management of migration

[14] Member States replies are published on the following website: http://eu2012.dk/en/Meetings/Conferences/Feb/Konference-om-innovativ-graenseforvaltning

[15] Council document 7166/12, Presidency summary of findings

and migration policy as such. However, it was considered that answers still need to be found to some technical and political questions such as the storage of the data, the use of biometric data from the start, access for law enforcement authorities, the abolition of the obligation to stamp the passports and last but not least the full respect of privacy of the traveller including data protection. In particular, the summary points out that "the definition and purpose of the EES must be clear from the start as these set out the terms for data protection."

European Parliament

In its resolution on the February 2008 Communication, the European Parliament, while accepting that the proposed system might help to deter third country nationals from overstaying, underlined that the correct functioning of the entry/exit system will depend both materially and operationally on the success of the VIS and SIS II.

The European Parliament (EP) did not submit its opinion on the 2011 communication[16].

At the high level conference on Innovation Border on 2 and 3 February 2012 in Copenhagen, Members of the European Parliament expressed the view that the SIS II and the other IT tools currently under development should be in place and evaluated before work on the EES can start.

European Data Protection Supervisor

In his opinion of 7 July 2011 on the Communication of the Commission on Migration the European Data Protection Supervisor (EDPS) stressed the need to assess first the possible better use of existing systems and to prove the necessity and proportionality of an EES in particular. The EDPS was also consulted informally on the 2011 Communication on smart borders before its adoption. He stressed in particular the need to obtain evaluation results of existing systems – notably the VIS – and that the use of biometrics should be contingent on conclusive proof that the use of alphanumeric data only is not effective. He also questioned the evidence available for assessing the problem of irregular migration and overstays, that the main purpose of the system must be set out clearly and exhaustively, that the retention period must be the shortest possible and only what is necessary in relation to the main purpose, and to carefully assess whether and to what extent access should be granted for law enforcement authorities. The EDPS provided comments on a draft of this impact assessment as well on a draft of the legislative proposal by letter of 10 August 2012. While welcoming the attention paid to data protection he considered that access for law enforcement purposes should not be granted and that biometric data should not be collected. As to specific comments he highlighted among other things the need to clearly define the purpose and the benefits of an entry/exit system.

Article 29 Data Protection Working Party

[16] European Parliament resolution of 10 March 2009 on the next steps in border management in the European Union and similar experiences in third countries (2008/2181(INI)). Resolution is published on the following website: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2009-0085&language=EN

The Working Party addressed a letter to Commissioner Malmström on 12 June 2012 reacting to the 2011 Communication. It expressed doubts on the necessity of an EES and stressed that the reasoning needed to be appropriately explained, addressing comprehensively its impact on all fundamental rights. The Working Party considered that in any case the system should initially operate without biometric data, that the necessity of access for law enforcement purposes would need to be established separately, and that the retention period should be assessed against the main purpose of the system, ie detecting and preventing overstay.

Civil society and the private sector

Civil society (academia, think tanks and NGOs) and the private sector participated actively in the debate and organised several relevant conferences. Civil society provided input in various conferences and academic papers published on the subject. Most were critical of the setting up of an EES, considered that the added value was not proven and that it would not be proportionate to collect such amounts of personal data in relation to the aims pursued. At the conference in Copenhagen a representative of IATA expressed support for an EES provided the system does not have negative impacts on travel flows or lead to additional costs or burdens for airlines or airports.

The present report takes into account the questions and challenges raised by the stakeholders. Further details of the results of the consultations have been integrated in the description of the options and in the assessment of impacts. By presenting two communications opening for input for all stakeholders during a period of four years, the Commission has done its utmost in seeking the views of all stakeholders concerned.

1.3. Data gathering

Data-gathering and consultations with relevant authorities in the Member States and other stakeholders were undertaken by the Commission with the support of FRONTEX.

The following types of data were of principal interest:

- Information on current and future size of travel flows at the external border, distinguishing between types of borders (air/land/sea) and groups of travellers (EU citizens and visa exempt/required third country nationals);

- Time currently needed for border checks;

- Number of irregularly staying third-country nationals within the Schengen area, broken down by Member State, nationality, and causes for the irregular stay (irregular border crossing or overstay).

Data was collected through questionnaires[17] as well as case studies, pilot projects and literature reviews and was used in particular for describing the context, defining problems, specifying the most important implementation options and finally analysing the impacts. Comparable data were gathered on entries and exits and also on the time needed to carry out border checks on different categories of travellers at different types of external borders.

[17] Council document 7226/1/09 REV 1 FRONT 12 COMIX 200 and the Commission document JLS D(2009) 8729.

However, shortcomings in the availability and/or comparability of existing statistical data and the fact that many aspects (customs check, security check, infrastructure, etc.) affect the time needed for border crossings has made comparison and analysis difficult. With regard to numbers and forecasts of traffic of passengers it is important to note a wide disparity in the information available according to the different means of transport. If the information on air transport is reliable due to the particular challenges for this sector, it is much more reduced in relation to other modes of transport and it is obviously lacking in the case of people travelling by their own means of private transport. Most importantly the data collection showed that Member States were not able to provide data or any reliable estimates on the number of overstayers on their territory, and as a consequence neither on nationalities or reasons for irregular stays. Estimates of such data could only be found via one research project[18], aggregated for the Union as a whole.

1.4. Inter-service steering group

An inter-service steering group was set up on 29 September 2009 involving the Legal Service (SJ), the Secretariat-General (SG), DG Taxation and Customs Union (TAXUD), DG Enterprise and Industry (ENTR) and DG External Relations (RELEX). The group met on 2 October 2009 and, joined by DG Justice, Fundamental Rights and Citizenship (JUST), on 2 December 2010, on 16 February 2011 and on 31 January 2012. The last meeting was also attended by representatives of DG Mobility and Transport (MOVE) and of the Joint Research Centre (JRC). Communication between the members of the group was also conducted via e-mail and telephone.

1.5. Impact Assessment Board

The Impact Assessment Board (IAB) reviewed the draft impact assessment and delivered its opinions on 14 March 2012 and (on a revised version) on 8 June 2012. The recommendations for improvement were accommodated in the revised version of the report. In particular, the following changes were made: further information is provided on the consultation of interested parties; the overall intervention logic has been reviewed and streamlined; the problem definition has been further developed and made more detailed, both in relation to the overall problem of irregular migration and in relation to specific implementation problems; the baseline scenario has been extended to better describe how it would involve without further EU action; the options have been restructured and simplified; the assessment of the options have been refined and done in a more logical manner showing which options are linked and which are not; the explanation of the method used for calculating the costs was expanded; the analysis and description of the preferred option have been revised and linked more directly to data that will become available in the future.

2. PROBLEM DEFINITION

2.1. Why the creation of an EES is being examined

The 2008 impact assessment identified and examined irregular immigration, including the lack of data for identifying overstayers, and terrorism and serious crime as the main problems to be addressed through the creation of an EES. As explained in the 2011 communication:

[18] The *Clandestino* project; see further under section 2.1.1.3.

'An EES would allow the accurate and reliable calculation of authorised stay as well as the verification of the individual travel history for both visa holders and visa exempted travellers as an essential part of first line risk-assessment. It would do so by replacing the current system of stamping passports with an electronic registry of the dates and places of third country national admitted for short stays. While the main purpose of the system would be to monitor respect of the authorised stay of third country nationals, the system would also contribute to optimising border check procedures and enhance the security at the moment of the crossing of the external borders. '[19]

The 2008 impact assessment assessed a wide range of policy options and identified the setting up of an entry/exit system as the preferred option. This impact assessment looks again at the overall problem definition as relevant for that conclusion in the light of developments since 2008 with regard to border control aspects, irregular migration, and technological developments, at European as well as national level. In particular, the following sections address difficulties related to monitoring the authorised stay of third country nationals, delays in border checks, the lack of information on irregular immigration, and use of entry/exit systems at national level in the Member States as well as in third countries. Based on the overall problem definition it then looks in more detail at the more specific problems related to how such a system should be designed.

2.1.1. Border control aspects

2.1.1.1. The difficulties of monitoring the authorised stay of third country nationals at the external border

According to the Schengen Borders Code, EU citizens and other persons enjoying the Union right of free movement (e.g. family members of EU citizens) crossing the external border shall be subject to a minimum check, both at entry and exit, consisting of the verification of the travel document in order to establish the identity of the person. Third-country nationals, however, must be subject, at entry, to a thorough check which, in addition to a travel document check, implies a check of their purpose of stay, possession of sufficient means of subsistence, as well as a search in the Schengen Information System (SIS) and in national databases.

Third-country nationals who do not have a residence permit or long-stay visa issued by a Member State are admitted for a short stay of maximum three months per six month period. This applies both for those who are subject to the visa obligation and those that are not. There are no provisions however in the Schengen Borders Code on the recording of travellers' movements into and out of the Schengen area. Currently, stamping the travel document is the sole method to indicate the dates of entry and exit which can be used by border guards and immigration authorities to calculate the duration of the stay of a third-country national, thereby allowing authorities to verify that the third-country national is in compliance with the rules on short stays. Other measures and tools available at border crossing points (such as databases, whose consultation is compulsory at entry, but not at exit) are not intended for the purpose of recording border crossings and do not provide for this functionality. Therefore there are no centralised electronic means to check if a third-country national has entered the Schengen area in one Member State and left via another.

[19] COM(2011) 680 final

The calculation of the exact time spent in the Schengen area of third-country nationals coming for a short stay based solely on stamps in the travel documents is both time-consuming and difficult. Checking a traveller who has been making 10 visits to the Schengen area during the last months means verifying 20 stamps. Maintaining the quality and security of the stamps requires both resources and efforts, as they can be subject to counterfeiting and forgery. In addition, there is no stored record available indicating that a third-country national has entered the Schengen area or of the time he/she has spent within it.

For these reasons, there are currently no reliable means to determine if a third-country national has exceeded his/her lawful right to stay and there is no consistent record of entries and exits of travellers to and from the Schengen area. Furthermore in-depth verification of the authorised stay is time consuming and can lead to tensions between border guards and travellers who, for example, need to catch a flight.

Difficulties affecting the legibility of the stamps as well as the absence of entry stamps were highlighted by the Member States in their replies to the questionnaire carried out by the Commission prior to the report on the operation of the provisions on the stamping of travel documents of third-country nationals.[20] The report also highlighted further problems encountered by third-country nationals crossing the external border frequently, such as lorry drivers or cross-border commuters, due to the need to use separate sheets for affixing the entry or exit stamps when there are no free pages left in the passport.

The setting up an entry/exit system would leave the current legislation and border checks unchanged except for the stamping of passports of third-country nationals, which would be replaced with the obligation to electronically record entry and exit dates in the entry/exit system and an automatic calculation of the authorised stay.

2.1.1.2. Increased border crossings and delays in border checks

According to the most recent comprehensive data provided by the Member States, there were 669 million external border crossings in 2009, 675 million in 2010, and 700 million in 2011, including EU citizens and third-country nationals. The number of border crossings did not increase significantly during the past few years, presumably because of the economic downturn. However, based on discussions with Member States, it can be assumed that border crossings at the largest and busiest border crossing points have been generally increasing and will continue to do so in the future[21]. Further predictions by Member State cannot be made with any precision; main third country nationality vary greatly between Member States eg due to their geographical situation and historical ties, and the development of those flows will be greatly influenced by the economic development in each third country in question.

---

[20] COM(2009) 489 final. Report from the Commission to the European Parliament and the Council on the operation of the provisions on stamping of the travel document of third-country nationals in accordance with Article 10 and 11 of Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)

[21] See also the World Trade Organisation (WTO) forecast: Tourism 2020 vision, http://www.wto.org/english/tratop_e(ser_e/omt.ppt and the travel forecast of the Office of Travel and Tourism Industries (OTTI), http://tinet.ita.doc.gov/view/f-2000-99-001/index.html.

To gather comparable data on border crossings, the Czech and Swedish Presidencies together with the Commission organised a data collection exercise at all external border crossing points between 31 August to 6 September 2009.[22] Based on this data, it is estimated that 73.5 % of travellers crossing the border are EU citizens or persons enjoying the Union right of free movement (9,1 million/week), 15,2 % are third-country nationals without a visa (2,1 million/week) and 11,3 % are third-country nationals holding a visa (1,4 million/week). On a yearly basis this means around 109 million third-country nationals without a visa and around 73 million with a visa. Most third-country nationals cross the border via land, the next largest number by air and the smallest number via sea borders. The number of third-country nationals crossing the border varies significantly between Member States and also between border crossing points.

Taking into account the size of travel flows and the principle of a thorough border check on all third-country nationals, queuing time at the border is a problem for many Member States. This problem is influenced by the time needed under current rules for systematic stamping of passports and the need to verify a sometimes long travel history based on previous stamps to calculate the authorised stay at entry and exit as described in the previous section. The implementation of the Visa Information System and the resulting obligation to verify the identity of all visa holders using fingerprints may further slow down border crossing times. The options for facilitating and speeding up border crossings is further assessed in the parallel impact assessment on the setting up of a Registered Traveller Programme, but this problem must be kept in mind when assessing the design of an entry/exit system also.

Differences between Member States in this regard are obvious due to geographical location (with or without an external land border) or size (with major airports). Future developments are linked to economic developments but also to developments in visa policy, where a lifting of the visa obligation with a neighbouring third country would most likely lead to a major increase in the travel flows to, in particular, the Member State(s) directly bordering that country.

2.1.1.3. Lack of reliable information on irregular immigration, in particular on overstayers, and problems of return

Reliable data on the number of irregular immigrants currently staying in the EU does not exist, a point emphasised by the EDPS in his preliminary comment on the draft 2011 Communication. Conservative estimates of the number of irregular immigrants within the EU vary between 1.9 and 3.8 million according to the results of *Clandestino*[23], an EU-sponsored project implemented by the International Centre for Migration Policy Development. Assessing how individual Member States are affected by this phenomena is therefore equally difficult and can only be a matter of estimates. It is generally assumed that the Member States most affected by irregular migration (including irregular border crossings as well as overstays) are those at the southern external border of the EU as well as the biggest economies of the EU. Future developments in this regard are hard to predict as they are influenced by the political situation in, especially, the wider European neighbourhood (cf

22 See annex 7 for further details.

23 Accumulated total at the time of the study, 2008 (EU 27) http://clandestino.eliamep.gr/

Arab spring) and the economic situation in that region as well as in the EU, both in absolute and relative terms.

It is generally agreed that a clear majority of irregular immigrants are 'overstayers', i.e. persons who have entered legally for a short stay, with a valid visa when required, and then remained in the EU beyond the limit of their authorised stay.

In terms of apprehensions of irregular immigrants[24] in the EU, the total for 2011 was 351 000 which shows, in comparison to the above estimate, that a very small share of overstayers are actually apprehended.

The lack of reliable data is confirmed by the replies of Member States to the questionnaires mentioned in section 1.2. Only 14 Member States were able to provide data on the estimated number of irregular immigrants within their territory and the number of overstayers detected at the border. An additional four Member States were able to provide data for one of the two categories. The total number for the two categories was 76,669 persons, although it should be noted that three Member States accounted for 51,543 persons in total.

As a consequence of this lack of reliable data, no breakdown can be provided concerning overstayers per third country or per category of traveller[25].

As a result of the absence of any electronic recording of travel movements it is not possible at any given time to know who, among the millions of third-country nationals admitted legally for a short stay every year, has actually complied with the obligation to leave the territory after a maximum of three months. This means also that there is no information on the nationalities of overstayers or whether they are from countries subject to the visa obligation or not. The risk of overstay should be assessed by Member States authorities when assessing whether to grant a visa and whether to allow entry at the border, but there is thus limited feedback on which nationalities present a higher risk than others in this respect, as well as to whether the visa obligation is imposed on the third countries with a high overstay rate.

There is reason to believe that not all overstayers who voluntarily leave the territory are detected at the exit border check due to the problem of stamping as described above. Such overstays can therefore not be sanctioned (i.e. with a fine) or taken into account for a subsequent decision on allowing a new entry.

In turn this contributes to the difficulty in detecting those that do overstay in each Member State. Member States carry out random checks within the territory for this purpose, for example, at major transport hubs or workplaces suspected of hiring irregular migrants.

The low number of detections of irregular migrants taken together with problems of identifying them (as many will have no identification document) and in ensuring cooperation of third countries explain the low number of returns carried out by Member States each year compared to the overall estimate of the total number of irregular migrants on EU territory.

---

[24] Frontex annual risk analysis 2012. Including both persons apprehended within the territory and when exiting the territory.

[25] E.g. holding a visa or not, by purpose of stay, by nationality, etc.

A major obstacle to effective return is uncertainty concerning the identity of the person and/or his or her lack of necessary travel documents, which may make it impossible to either issue a return decision or to enforce such a decision. Countries of origin often delay or deny the issuing of return travel documents because of missing information on nationality or identity. In order to avoid removal, irregular residents may therefore hide or destroy their travel documents and often claim a completely false identity and/or nationality. Figures provided for the follow up of the Return Directive show that over the last years, an average of only 200,000 out of 500,000 return decisions could be carried out, however, this data includes situations in which returnees could not be returned also due to other reasons, such as *non-refoulement* or because no third-country would accept them.

2.1.1.4. National EES systems and experiences with EES in third countries

There are several Member States and third countries implementing their own national entry/exit systems. 13 Member States[26] currently have such a system in place and the only data collected are alphanumeric. The main purpose of these systems is to give law enforcement authorities the opportunity to store travel records of certain third-country nationals in accordance with security-related national legislation. Therefore these Member States give access to their national systems not only to border authorities but also to law enforcement authorities for the purpose of investigating crime. As for non-Schengen countries, part of the UK's e-Borders programme aimed, among other things, to record entry and exit data based on the advance passenger information transmitted to government authorities by carriers transporting persons to the UK.

If a person lawfully exits the same Member State through which he or she entered, then any overstayer would be detected by the relevant national EES systems. Beyond that, there are no possibilities for using such systems to detect overstayers as entry and exit records cannot be matched when persons leave the Schengen area via a different Member State from the one through which they entered and in which their entry was recorded.

As regards third countries, the US-VISIT programme was implemented in the wake of 9/11 in the United States. The objectives of this system go considerably beyond those of an entry/exit system and are achieved by collecting, maintaining and sharing information on individuals who enter and exit the United States to detect fraudulent travel documents, verify traveller identity, and determine traveller admissibility through the use of biometrics[27]. The matching of entry and exit records for the purpose of identifying overstayers is currently done based on alphanumeric data, although pilot projects incorporating the use of biometrics have been carried out recently. While the number of overstayers remains significant, the creation of the exit part of an entry/exit system based on biometrics has been repeatedly postponed. The US-Congress has long pushed and is still pushing for a biometric exit system.The US Department of Homeland Security (DHS) stated that several more years are still needed to implement the technology because of the high costs, manpower and the scope of the issue due to the variety and number of ways to exit the United States, in particular through its land borders. The ultimate impediment to biometric exit is that highway lanes and other

[26] Finland, Estonia, Spain, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, Bulgaria, Cyprus, Portugal, Malta.

[27] Intrinsic physical or behavioral characteristics uniquely recognizing individual persons.

architecture have been designed for entry only[28]. This is the main reason why implementation problems are not transferable or applicable to the Schengen area, because there exists a full and complete developed architecture and sufficient human recources at all border crossing points in both directions.

Arrival and departure records of travellers to and from Australia are contained within the Movements Reconstruction database, set up in 1981. In Japan, a biometric border control programme for all non-Japanese citizens was introduced in 2007 as a measure for preventing terrorism and irregular immigration, while a system for recording biographical entry and exit data has been in place for several years.

At the high level conference on 2 and 3 February 2012 in Copenhagen (see footnote 15), representatives from the responsible authorities in the USA and Australia described the new systems as a success and as an effective tool for the authorities to detect irregular migrants and to fight serious cross border crime. However precise figures on the number of apprehended irregular migrants were not presented.

2.1.1.5. Summary of overall problems related to border control and irregular migration

The overall problems related to border crossings, stamping, irregular migration, overstays and returns have remained fairly constant since the impact assessment report of 2008 was carried out. There has not been any technological developments either that would influence the problems. These can be summarised as follows based on what was described in the preceding sections:

[28] Hearing of Homeland Security Secretary Janet Napolitano at the Senate Judiciary Committee on 25 April 2012

- Absence of any electronic means for recording travel movements of third-country nationals admitted for a short stay;
- The very limited value of national systems for such purposes in an area without internal border control between 26 countries;
- The absence of means for identifying persons detected within the territory without travel documents who cannot be identified using the VIS;
- The absence of any information of who is on EU territory and who complies with the maximum allowed short stay of three months per six months;
- The complexity and slowness of the current stamping obligation, which does not guarantee that the border guard can assess the authorised stay at the border check of the traveller;
- The absence of information on nationalities and groups (visa exempt/required) of travellers overstaying;
- The absence of information that can support random checks within the territory to detect irregularly staying persons.

2.1.2. Law enforcement aspects

Border controls play an important role in combating terrorism and serious crime. Europol's EU Organised Crime Threat Assessment 2011 (OCTA 2011) points out that most organised crime involves international travel, including trafficking in human beings or the trafficking of illicit drugs, weapons and other illicit goods into the EU. Information about the travel record of persons who are suspects of these serious crimes can be necessary for criminal investigations.

Controls of third-country nationals at external borders involve identity checks and searches against various databases of known persons or groups posing a threat to public security that should be either apprehended or denied entry to the territory. Currently, all verifications are carried out based only on the travel documents. Even though the alerts on these persons may have been recorded in the Schengen Information System (SIS), or other national and international databases, they can only be identified on the basis of the alphanumeric data that was introduced with the alert. This makes it difficult for the authorities to detect a person using different identities to cross the borders.

In general, identification is essential for law enforcement authorities in their mission to prevent and combat terrorism and other serious crime. However, in the event that a third country national destroys his/her official documentation once having entered the Schengen area, it can be very difficult for law enforcement authorities to identify that person in case he/she is suspected of a crime or is a victim of crime. While data on EU citizens exists in different databases in Member States that are in general accessible to law enforcement authorities, there is an information and verification gap concerning third country nationals that are not covered by the Visa Information System (VIS).

2.1.2.1. Summary of overall problems related to law enforcement aspects

The overall problems related to identifying and detecting terrorist and criminal suspects have also remained fairly constant since the impact assessment report of 2008 was carried out. There has not been any technological developments either that would influence the problems. These can be summarised as follows:

- Lack of information on the travel and cross-border movements of suspect persons;
- Difficulties in detecting persons subject to an alert who use different identities to cross the borders;
- Difficulties identifying a suspect having destroyed his or her travel documents.

2.1.3. Fundamental rights issues

An EES would, due to the personal data involved, in particular have an impact on the right to the protection of personal data, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. An EES would need to guarantee the right to an effective remedy before a tribunal (Article 47 of the Charter) for challenging a notification of an overstay, for example in cases of forced overstay, errors or when a migrant has a legal right to stay.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[29] and the Regulation (EC) 45/2001 would apply to the processing of personal data carried out for the purpose of an EES respectively by the Member States and by the EU institutions, bodies and agencies involved. Negative impacts of sharing personal data have to be minimised by appropriate technical safeguards against misuse, clear legal limitations for access, including purpose limitations and data retention periods which are as short as possible.

Council Framework Decision 2008/977/JAI[30] on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, the Europol Decision 2009/371/JHA and the Regulation (EC) 45/2001 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 would apply to the processing of personal data if access would be given for law enforcement purposes.

According to the Commission Communication of July 2010 on information management[31], data protection rules should be embedded in any new instruments relying on the use of information technology. This implies the inclusion of appropriate provisions limiting data processing to what is necessary for the specific purpose of that instrument and granting data

[29] OJ L 281, 23.11.1995, p.31
[30] JO L 350 of 30.12.08, p.60
[31] See footnote 8.

access only to those entities that 'need to know.' It also implies the choice of limited data retention periods depending solely on the objectives of the instrument and the adoption of mechanisms ensuring an accurate risk management and effective protection of data subjects' rights.

The system would have to comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data. All safeguards and mechanisms should be in place for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data. Third-country nationals must be made aware of these rights.

In accordance with data protection legislation, access should be given to the data stored in the entry/exit system only for specified, explicit and legitimate purposes. This means that the authorities who should have access to the entry/exit system have to be designated for a specific limited purpose. The EDPS raised this concern in his preliminary comment on the 2011 Communication as well as in his letter of 10 August 2012, stressing that the purposes and modalities of access to EES data have to be closely circumscribed. Therefore, access for consulting the data should be reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes of the entry/exit system and limited to the extent the data are required for the performance of the tasks in accordance with these purposes.

2.2. Problem: how to design an EES?

2.2.1. The core features of an EES

An EES would need to allow the accurate and reliable calculation of authorised stay as well as the verification of the individual travel history for both visa holders and visa exempted travellers as an essential part of border checks. It would do so by replacing the current system of stamping passports with an electronic registry of the dates and places of border crossings of third country nationals admitted for short stays. As part of the preferred option, the 2008 impact asessment identified a "core" entry/exit system, that is, the common minimum features which are needed to develop the system in the first place, without prejudicing any choices on how it should be implemented. These core features are still valid in the light of the overall problem definition as described in section 2.1. There have been no technological developments since 2008 influencing these core features. They can be defined as follows:

- a system which records and stores, as a minimum, the basic alphanumeric data (equivalent to the biographic data in the passport) of a third-country national admitted for a short stay, together with the date and place of entry and exit, upon each crossing of the external border of the Schengen area, with a defined retention period for the storage of the data;

- a system that would automatically calculate the authorised stay and issue an alert to the authorised competent national authorities when there is no exit record on the expiry of the authorised stay;

- access to the data in the system would be given to the national authorities responsible for immigration and border control, at the external border and within the Schengen territory.

A number of safeguards would be integral to the core system, in particular for complying with fundamental rights:

- If there were errors on the identity checks of passengers, facilities would need to be made available for carrying out manual checks and for amending the data on entry and exit at all border crossing points. Regarding such facilities, the Schengen Borders Code currently requires that thorough second line checks for third-country nationals shall be carried out in a private area where the facilities exist and if requested by the third-country national.

- Individuals should have the right to access information held on them and to challenge and correct it, if the processing of this data does not comply with the provisions of Directive 95/46 and Regulation 45/2001, in particular because of the incomplete or inaccurate nature of the data. In case the information is held by law enforcement authorities following access to the EES, such rights shall be granted under Framework Decision 2008/977**.**

- Individuals should have the right to lodge a complaint with a data protection authority regarding the processing of their personal data and they should also have the right to effective administrative and judicial remedies (Article 47 of the Charter).

- Guarantees ensuring an effective remedy (Article 47 of the Charter) for third-country nationals that would enable them to challenge a notification of an overstay by the entry/exit system must be in place, for example in situations when they were forced to overstay, particularly if it appears that they overstayed for a valid reason (e.g. hospitalization, change in travel arrangements), when errors were made in recording dates of entry or exit or to show that they have a legal right to stay (e.g. based on a new visa, marriage to an EU citizen, application for asylum, refugee status). Given the large numbers of new travellers affected and the new requirement for them to provide information, safeguards for data protection and mechanisms for ensuring an effective remedy would need to be visible and evident.

- In case the entry/exit system notifies an overstay, this indication should not lead automatically to detention, removal or a sanction for the third-country national. Third-country nationals should have access to effective remedies in such proceedings in order to protect the right to liberty and security (Art. 6 of the Charter), right to asylum (Art. 18 of the Charter), respect for family life (Art. 7 of the Charter) and the obligation of *non-refoulement* (Art. 19(2) of the Charter). A decision to detain, remove or sanction a third-country national shall not be based solely on a nofitication of overstay by the entry/exit system. In addition the safeguards of Directive 2008/115/EC have to be respected.

- The supervision of all data processing activities should be carried out by Member States data protection authorities and the European Data Protection Supervisor which should be conferred with all the necessary powers to intervene and enforce compliance with data protection rules.

- The measures protecting rights of travellers, including right to an effective remedy, must also take into account the privileged position of non-EU family members of EU citizens whose right to enter and to stay depend on the right of the respective EU citizen in accordance with Directive 2004/38/EC.

2.2.2. Could these features be provided through existing systems?

A number of Member States raised the issue of whether the Visa Information System (VIS) could be expanded to incorporate the features of an EES.

The main purpose of the VIS is to permit the verification of the visa application history and, at entry, to verify whether the person presenting the visa at the border is the same person to whom the visa has been issued. It concerns only those third-country nationals who are required to hold a visa.

The VIS was not developed to keep track of entries and exits of third-country nationals nor is it meant to allow checking whether a person, after entering the EU legally, has or has not complied with the authorised stay according to the visa. The VIS feasibility study, carried out in 2003 before the development of the VIS, suggested that it would not be beneficial to develop several large-scale IT systems as one, nor to use VIS to record entry and exit data. It would need substantial changes to the nature and capacity of the VIS if entry/exit data were also to be recorded in it. The workflow of the VIS is optimised to deal with 10 million visa applications per year. Adding around 200 million records of entries and exits would require significant investments especially in hardware, software, data storage and communication infrastructure.

Moreover, there would be significant data protection implications if the system were to include both visa holders and visa-exempt persons. The principle of purpose limitation needs to be adhered to and the risk of function creep has to be prevented as highlighted by the EDPS in his opinion on the Communication on Migration.

Therefore the possibility of including entry/exit functionality in the VIS itself and the storage related to non-visa holders in the VIS can be discarded. However, there would be major technical and functional links between the Visa Information System (VIS) and the entry/exit system. Besides the same technical features and common matching functionality, VIS is the repository of the biometric identifiers of visa holders who will be registered in the entry/exit system. It must be checked systematically upon entry of the visa holders.

The technical development of an EES should therefore exploit technical synergies, organisational simplification and economies of scale to the maximum by using the same technical platform as VIS. Biometric matching functionality could be performed by the existing Biometric Matching System, which already provides such a functionality in the VIS. Furthermore, the fingerprints of the visa holders would not be stored in the entry/exit system, as they already exist in the VIS. Duplication of data would be subsequently avoided. This would allow also for cost savings by building on the technical platform of the VIS. Therefore, storing fingerprints of visa holders in VIS only and not in the entry/exit system would create economies of scale and avoid storing the fingerprints of visa holders twice. Indeed, building the EES on the same technical platform as the VIS (but not on the VIS itself) would mean that the EES would take advantage of the biometric matching functionality already built for VIS and would optionally re-use the visa holder fingerprints already captured for the benefits of VIS, without duplicating the effort or the data.

Annex 4 summarizes the other main EU level systems (SIS, Eurodac and the Prüm Decisions) that are currently used at the external border or which are relevant for internal security and migration management, the future plans for the systems and their possible link to the entry/exit system. Annex 6 summarizes the current and future management of those systems.

None of these instruments are, however, a pre-condition for the setting up of an entry/exit system, nor is there any potential overlap with the functions that an entry/exit system would carry out. Other developments in the EU's policy on border management are not relevant here, such as changes to the legal framework of Frontex, the development of Eurosur, or other amendments to the Schengen Borders Code. Likewise, no other initiatives to combat irregular immigration[32] or to combat serious crime and terrorism are relevant either for reducing the number of overstayers or the possibilities of identifying or detecting them.

2.2.3. Implementation issues

There are a number of key choices that need to be made when designing an entry/exit system and that will influence to what extent it will solve the overall problems described in section 2.1. These choices must maximise the overall usefulness and efficiency of the system while respecting fundamental rights. By maximising only usefulness and/or efficiency of the system there is a risk of contravening fundamental rights. For example, an EES could be designed so that it would store the largest possible amounts of data, any search criteria used would give access to all information (alphanumeric and biometric data) and flexible access rights would be given for all relevant authorities, even third countries. However, all this would cause exorbitant data protection implications and would not be proportionate against the objectives of the EES.

This involves choices both with regard to the overall architecture of the system and to additional features, including possible adaptations of the basic purpose of the system, in relation to the "core" system as described in section 2.2.1.

In summary the choices involve deciding the data to be collected and processed; defining with precision the purpose of the system; deciding the retention period of the data taking into account the purpose; and finally deciding on how to technically implement the system in practice.

2.2.3.1. What type of personal data should be included in the entry/exit system?

As mentioned above a minimum amount of alphanumeric personal data[33] on third-country nationals admitted for a short stay is required to make the system functional. The question arises, however, as to whether biometric data should also be stored on these travellers (taking into account that such data is used for the VIS) in addition to alphanumeric data. While the use of biometric data helps in identifying people, it would present a negative impact on privacy and data protection. It would also require more resources for processing and storing additional data. This is a recurring issue that was widely discussed especially in the context of the VIS.

---

[32] Cf. "EU Action on Migratory Pressures – A Strategic Response" adopted by the Council on 26 April 2012 (8714/12) for an overview of on-going and planned EU measures in this field.

[33] The surname, first names, birth date, sex, nationality as well as the number and expiry date of the travel document

The impact on the time taken for the border check process would also need to be taken into account given that biometric data for third-country nationals not requiring a visa, who make up approximately 15% of all travellers, is currently neither collected nor stored in any other system.

The question of which type of biometrics to use is not addressed further in this impact assessment as existing EU law already stipulates the use of fingerprints as concerns the VIS, e-passport, and residence permits.[34] This legislation also stipulates that children under the age of twelve and persons physically unfit to give fingerprints should be exempted from that requirement, so for these categories alphanumeric data only will always be used. Using the same biometric data (fingerprints) under the same conditions in an EES would therefore be consistent with previous policy choices at EU level and also allow for the use of the same infrastructure and equipment as used for the VIS.

2.2.3.2. For which purpose(s) and by which authorities could entry/exit data be accessed?

One of the problems in enforcing returns of irregularly staying third-country nationals is linked to proving the identity and nationality of the person in order for the third country in question to accept to readmit him/her. For that reason Member States have the right under certain conditions to share data stored in the VIS with third countries. Data generated by the entry/exit system could be shared in a similar way for the same purpose. However, the sharing of personal data with third countries raises important questions related to data protection and under what conditions such data could be shared.

Moreover, the data generated by the entry/exit system could support law enforcement authorities in the fight against terrorism and serious crime both as an identity verification tool and as a criminal intelligence tool. The use of such data for identity verification would reduce the above mentioned identification and verification gap concerning third country nationals that are not covered by the Visa Information System (VIS). The use of biometric data, and more specifically fingerprints, would substantially increase the added value of the entry/exit data in establishing the identity of a person who is suspected of a crime or a crime victim such as victim of trafficking in human beings. Biometric information provides a reliable means to establish the identity of a person and the comparison of fingerprints is generally acknowledged as an important source of information for fighting crime. This is both in cases where the third-country national has destroyed his/her documents, but also where law enforcement authorities are investigating a crime through the use of fingerprints and wish to establish an identity.

The data generated by the entry/exit system could also be used as a criminal intelligence tool for investigations and prosecutions of terrorism and serious crime. The data could be used to construct evidence by tracking the travel routes of a person suspected of having committed a crime. However, as law enforcement authorities would need to go back sufficiently in time in their analysis of travel routes, an effective use of the data generated by the entry/exit system as a criminal intelligence tool requires a commensurate period of retention of that data.

---

[34] See also the Justice and Home Affairs Council Conclusions on 4-5.6.2010. The Council invited the Member States to move on a voluntary basis to a more extensive use of automated border control systems on the basis of the new passport i.e. passport which contains facial image and fingerprints stored in the chip.

2.2.3.3. For how long should entry/exit data be stored?

The conditions set for the retention of the collected personal data would have to be precisely defined on the basis of the system's objectives fully respecting data protection requirements. Whatever option is considered, the data retention period would have to be restricted to the minimum length required for the system to serve its purpose fully and effectively, while limiting the need for data from the same person to be enrolled several times over a short time-span. It should be ensured that the data in the record should be automatically erased after the retention period has expired. Conditions would also have to be defined for the possible advance deletion of data (e.g. in case the third-country national marries an EU citizen).

According to the information provided by Member States in 2009 concerning the existing national entry-exit systems, retention periods were ten years minimum in six Member States. For existing EU IT systems, the retention period is 2-10 years for Eurodac, 1-3 years for SIS, and 5 years for the VIS.[35] Member States did not provide concrete feedback on their preferred retention period for an EU EES.

This choice is directly dependent on the choices made with regard to the data to be stored and the precise purpose for storing the data. A table on the data retention period of the existing EU systems is in Annex 5.

2.2.3.4. Centralised vs decentralised storage of entry/exit data

This last implementation choice is essentially a technical one, independent of the previous choices, concerning how the system should be implemented technically to ensure reliable functioning as the system needs to be continuosly available at border crossing points, data security to prevent unauthorised access to the data stored in the system, and limit costs for developing and running the system. The system would eventually collect and store millions of records of third-country nationals personal data, which would need to be stored in a database to allow for matching of entry and exit records and the generation of alerts in case of overstay. A choice will therefore have to be made whether to set up a new centralised database at EU level, or whether the data could be stored at national level, with a connection for the exchange of data between the national databases. Lessons learnt from the development of other IT systems at EU level must be taken into account when making that choice.

2.3. Baseline scenario – how would things evolve without new EU intervention?

Currently there are some 700 million external border crossings every year. The tendency at least for the air borders is clearly leading upwards. For 2030 the figures of border crossings at the airports are expected to rise from 400 million in 2009 to some 720 million, an increase of 80%. As far as the expected development of irregular migration and overstay is concerned, it is difficult to estimate how figures for these phenomena will develop: Member States have not able to provide information on this issue. Both regular travel flows and irregular migration will be influenced by future economic development in the EU as well as in third countries.

The EU border management policy has to keep pace with this development. The optimisation of the existing instruments like the Schengen borders code and the role of the Frontex agency has continued but cannot address further this specific challenge. New instruments and possibilities to optimise the border management systems have to be found.

[35] See annex 5 for further details.

To cope with the increasing cross border travel and for the sake of speeding up and facilitation of border crossing procedures, IT technologies and new instruments are the most promising options.

It is reasonable to assume that the existing national entry/exit systems will continue to exist insofar they comply with EU law, in particular data protection rules. No other Member State has announced the development of a national system, awaiting the policy choices to be made at EU level concerning a European EES. In any case, national systems functioning in isolation will remain of little consequence as they cannot provide a response to the overall problems described in section 2.1.1.

In summary therefore the baseline scenario can be expected to develop as follows:

- Border checks will be carried in the same way as they are today, except that the biometrics of all visa holders will be verified at entry against the VIS as of 2014; this may contribute to preventing the legal entry of potential overstayers as this check will prevent identity fraud at the border; it may also increase the processing time of visa holding travellers at the border;

- The VIS will also give the possibility to identify overstayers within the territory who have entered legally with a valid short-stay visa and who are no longer in possession of their travel documents;

- The EU will continue its efforts towards further visa liberalisation with third countries based on the visa dialogues on-going for that purpose; however it can not be predicted when and for which third country the visa obligation will be lifted in the future; any such development will lead to an increase of the share of travellers who are not registered in the VIS when entering the EU;

- No tools exist or will be developed concerning visa exempt travellers with the exception of SIS/SIS II;

- In terms of overall irregular immigration, it is not possible to predict how the problem will evolve taking into account the influence of a number of economic and social factors as well as relations with and the situation in third countries; however, it can be assumed that the full roll-out and implementation of the VIS will have a positive impact in this respect;

- For the reasons outlined in section 2.1, different Member States may be affected differently by changes in travel flows and in irregular migration, but this cannot be predicted.

- The introduction of a Registered Travellers Programme could have a positive impact on reducing queuing time at the border, but this does not form part of the baseline as it is assessed in the parallel impact assessment report.

2.4. Subsidiarity

Under Articles 74 and 77(2) of the Treaty on the Functioning of the European Union (TFEU), the Union has the power to adopt measures relating to the crossing of the external borders of the Member States. Under Articles 82 (1)(d) and 87(2)(a) TFEU the Union also has the power to adopt measures to strengthen police and judicial cooperation by collecting, storing, processing, analysing and exchanging relevant information.

No Member State alone is able to cope with irregular immigration and with combating international terrorism and serious crime. A person may enter the Schengen area at a border crossing point in a Member State where a national register of entry/exit data is used, but exit through a border crossing point where no such system is used. The monitoring of compliance with EU rules on authorised stays can therefore not be done by Member States acting alone. Third-country nationals who enter the Schengen area are able to travel freely within it. In an area without internal borders, action against irregular immigration should in principle be undertaken on a common basis. Considering all this the EU is better placed than Member States to take the appropriate measures.

Although Member States may retain their national systems in accordance with security-related national legislation, an EU entry/exit system would allow Member State authorities to access data on third-country nationals who crossed the EU external border in one country and exited via another Schengen country.

Better information on cross border movements of third-country nationals at EU level would also facilitate the negotiation and conclusion of visa agreements between the EU and third countries and contribute to a common understanding of immigration issues with third countries of origin.

3. OBJECTIVES OF THE ENTRY/EXIT SYSTEM

The general policy objectives are, in order of priority:

- To counteract irregular immigration;
- To contribute to the fight against terrorism and serious crime and ensure a high level of internal security;

The specific objectives are:

- To enhance the efficiency of border checks through monitoring of the rights to authorised stay at entry and exit, and to improve the assessment of the risk of overstay;
- To monitor compliance with the authorised stay of persons within the territory;
- To generate reliable information to allow the EU and Member States to make informed policy choices concerning visa and migration;
- To identify and detect irregular immigrants, especially overstayers, also within the territory and to increase the possibilities for return;
- To identify and apprehend terrorist and criminal suspects crossing the external borders;
- To generate information that would reduce the identification and verification gap concerning third country nationals that are not covered by the Visa Information System (VIS) and that would contribute to the apprehension of terrorist and criminal suspects;

The operational objectives are:

- To create entry and exit records of third country nationals crossing the external borders;
- To automatically calculate the authorised stay and issue an alert when there is no exit record on the expiry of the third country national's authorised stay;
- To delete the EES data upon expiry of the retention period;
- To generate information on the size and trends of movements across the external borders, especially with regard to irregular immigration;
- To inform third country nationals of their rights and to implement effective appeal procedures.

4. POLICY OPTIONS

The problem definition and the consultation of stakeholders show that the key issues to decide are which data are to be processed in the system and for which precise purpose. The retention period needs to be chosen as a function of the choices made with regard to these two issues, that is, the shortest possible retention period needed to fulfill the purpose. The four policy options, in addition to the baseline (policy option 0), are therefore the following:

1) An entry/exit system with alphanumeric data for the purpose of border control and migration management; this option reflects essentially the "core features" of an entry/exit system as presented in section 2.2.1;
2) Same as policy option 1, with the addition of biometric data;
3) Same as policy option 1, with the purpose of the system extended to also include the fight against terrorism and serious crime;
4) Same as policy option 1, with the addition of biometric data and with the purpose of the system extended to also include the fight against terrorism and serious crime (so a combination of policy options 2 and 3).

Once the preferred policy option has been identified – in other words, what the system will do – a choice needs to be made how to implement the system technically.

4.1. Policy option 1: Core system

The alphanumeric data would include the surname, first names, birth date, sex, nationality as well as the number and expiry date of the travel document. Only an alphanumeric check would be made against the alphanumeric entry record upon exit.

In order to identify and return irregular immigrants, full access to the data stored in the entry/exit system should as a minimum be given to the competent border and immigration authorities carrying out checks at external border crossing points or within the territory of the Member States in order to determine whether the conditions for entry to or stay in the territory

of the Member States are fulfilled. Such access corresponds to the basic purpose of border control and migration management.

This option would as such have the support of a large majority of Member States as it involves the setting up of an entry/exit system per se, but many Member States would consider it insufficient in view of that only alphanumeric data would be stored and no access would be given for law enforcement purposes. The concerns expressed by members of the EP and the EDPS related to overall proportionality and added value of an entry/exit system are valid also for this policy option, but to a more limited extent taken into account that this option represents the most limited set of data and the most limited purpose that is possible.

4.2. Policy option 2: Core system + biometric data

An entry/exit system with biometrics would in addition contain fingerprints of third-country nationals. For visa-exempt third-country nationals, fingerprints would need to be enrolled on first entry at an EU external border crossing point. When the individual exits, his fingerprints would be verified against his/her entry record. For third-country nationals requiring a visa, the fingerprints enrolled at a consular post and stored in the VIS when applying for a Schengen visa would be verified on entry and exit at an EU external border crossing point. This option is in particular linked to the problem of identifying irregular migrants within the territory who are no longer in possession of their travel documents, and the specific objective of identifying and increasing the possibilities for return of those persons.

The results of discussions on the 2011 Communication showed that a large majority of Member States support the introduction of biometrics from the start of the system. In his preliminary comment on the Communication, the EDPS considered that the use of biometric data should only be considered if there is conclusive proof that the use of alphanumeric data only is not effective and that the impacts of the use of biometrics on privacy should be thoroughly examined.

4.3. Policy option 3: Core system + law enforcement purposes

In addition to the authorities mentioned under option 1 this sub-option would foresee access to the alphanumeric data, under specific conditions, to be given to national authorities and Europol for the purpose of fighting terrorism and serious crime, mirroring the solution for the VIS according to Council Decision 2008/633[36].

Member States' designated law enforcement authorities and Europol would consult the entry/exit data in a specific case, e.g. to establish the travel route of a person suspected of having committed a terrorist offence or another serious criminal offence, when there are reasonable grounds to consider that the consultation of the entry/exit data will substantially contribute to the detection or investigation of this offence.

Under this policy option, compared to the "core features" described in section 2.2.1, special data protection rules could be added to the extent necessary. For instance, the system could be developed in such a way that only specific data sets would be accessible and/or modifiable by specific authorities and data sets could be unlinked at the back-end. The database could also

[36] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences OJ L 218, 13.8.2008, p. 129–136

be designed to only provide a summary of events after a certain length of time or indeed to certain authorities. Such a 'privacy by design' approach limits the possibilities of abuse from the outset. The 2008 Framework Decision requires Member States in particular to lay down effective, proportionate and dissuasive sanctions to be imposed in case of infringement of data protection provisions, including criminal sanctions for particularly serious and intentionally committed infringements. Such safeguards would minimise the impact on fundamental rights and entry and exit data on travellers would automatically be deleted after the end of the retention period.

This is relevant for the problems described in relation to law enforcement aspects and the specific objectives of identifying and verifying terrorist and criminal suspects.

The results of discussions following the adoption of the Communication on smart borders showed that a large majority of Member States support the use of the information stored in the system not only for the purpose of border control but also by other immigration and law enforcement authorities.

4.4. Policy option 4: Core system + biometrics + law enforcment purposes

This is a combination of policy options 2 and 3: in addition to the core system biometric data would be stored as described under policy option 2, and access would be given to law enforcement purposes as described under policy option 3.

Member States' designated law enforcement authorities and Europol would consult the entry/exit data in a specific case for the purpose of establishing the identity of a person who is a crime victim or of a person who is suspected of having committed terrorist offences or other serious criminal offences if there are reasonable grounds to consider that this consultation will substantially contribute to this purpose.

This is likely to be the policy option most supported by the Member States, and the least supported by the EP and the EDPS.

4.5. Other issues linked to the four policy options

4.5.1. Transfer of data to third-country authorities

The transfer of data stored in the entry/exit system to border and immigration authorities of certain third countries could be authorised in compliance with fundamental rights and, subject to conditions, for the fight against irregular immigration. This would mirror the solution for the VIS where transfers of certain specified alphanumeric data are possible for the purpose of assisting the identification of a third-country national in relation to his/her return. This is linked to the specific objective of increasing the possibilities of returning irregularly staying third-country nationals. The validity of authorising such transfers is wholly dependent on the use of biometric data as the purpose of sharing data with a given third country would be to provide proof of the identity and nationality of a given individual to be returned to that country. This issue will therefore not be further assessed but taken as directly linked to the overall choice of the policy options, ie if policy options 2 or 4 would be chosen such transfers would be authorised for the purpose as described above.

Moreover, should access be given to law enforcement authorities of the Member States and Europol (cf policy options 3 and 4), transfers of data to the law enforcement authorities of

certain third countries for the purpose of fighting terrorism and serious crime could be envisaged. However, access for certain third countries for law enforcement purposes would have significant negative implications for data protection having regard to the potentially vast amounts of data that could be shared and the risk of "data mining". It would require the negotiation and conclusion of an extensive agreement with selected third countries to ensure, to the greatest possible extent, that the EU can regulate how and for what purpose such data would be used, and how long it would be stored. Certain third countries may also misuse access to data on their citizens (e.g. political dissidents) for exercising repercussions on the members of their families still present in that third country, which requires a serious analysis into which countries could potentially gain such access and under what strict conditions. Transfers of data for this specific purpose is therefore discarded regardless of which policy option is chosen.

4.5.2. The retention period of the personal data in relation to each policy option

For the determination of the retention period it has to be considered that for reasons of data protection as guaranteed by Article 8 of the EU Charter of Fundamental Rights and Article 8 of the European Convention on Human Rights, personal data should not be kept any longer than it is necessary for the purposes for which the data were collected. This principle was also stressed by the EDPS in his preliminary comments on the 2011 Smart Borders Communication. It should be ensured that the data in the record should be automatically erased after the retention period has expired. Conditions would also have to be defined for the possible advance deletion of data (e.g. in case the third-country national marries an EU citizen).

The shortest possible retention period would, as a minimum, be the time that the data is required for the calculation of the authorised stay, meaning a minimum of six months. Once the person has exited the Schengen area the need to store his or her personal data, and the entry/exit record, is significantly reduced. In other words, the data has served its purpose to monitor the respect of the authorised stay and should only be stored for a maximum of another 6 months to allow the correct calculation of the permitted stay of 90 days within a period of 180 days. However, the period cannot be set the same for all travellers, since for an overstayer who has not exited the territory it would be necessary to store the data for a longer period. This period can be set at 5 years, to ensure that data are available long enough to support the identification and return process, while remaining proportionate by setting an upper limit. It would also be coherent with the retention periods for the VIS and that envisaged for the RTP, and support applicants for a multiple-entry visa or to the Registered Traveller Programme, both in proving a travel history without overstays when applying for the first time as well as when applying for renewing their multiple-entry visa and/or access to the RTP. For a person who has exited within the authorised period of stay, and only visited the Schengen area once for a maximum of three months during a six month period, the data can be deleted after six months. To be effective and to benefit Member State authorities as regards future visa and entry decisions, statistical data in a fully anonymous form would have to be retained for a longer period on the history of cross border movements of third-country nationals, by nationality and visa required/exempt.

However, from a law enforcement point of view, and especially for the use of this data as a criminal intelligence tool, a travel record of a suspect of crime would need to cover a commensurate period of retention, possibly with several entries and exits, in order to have any added value as a source of information for law enforcement authorities. Hence should the

purpose of the system be extended to include the fight against terrorism and serious crime, a retention period of, as a general rule, six months would be too short to allow the system to meet its purpose. In order to construct evidence in criminal cases by analysing data on travel routes, law enforcement authorities have to be able to track the travel routes back for a period of several years.

Consequently the retention period in relation to the policy options would be the following:

- For an entry/exit system set up on the basis of either **policy options 1 or 2**, as a general rule 6 months, while for travellers who have not exited the territory within the authorised stay the period would be 5 years, and for participants in the RTP a period equivalent to the time they are granted access to the system;

- For an entry/exit system set up on the basis of either **policy options 3 or 4**, the retention period would be five years for all travellers.

4.5.3. Technical implementation

Two possibilities for the technical implementation can be identified. These will be further assessed in the light of the preferred policy option.

National databases running regular crosschecks

Member States would be responsible for the storage of data in a national system as well as for the acquisition and maintenance of those systems. At EU level, the setting up of a secure communication infrastructure for the exchange of data would be required, as the entry and exit data could be stored in different Member States for the same person (e.g. entering the Schengen area via one Member State and exiting through another).

This could involve obliging each Member State to set up a national EES. However, from a technical perspective, stand-alone national systems operating on a small scale as they currently exist in some Member States (cf section 2.1.3.) would not be of use or adapted to this solution. Despite their autonomy, such national systems should be built on the same technical platform and adopt interoperable technical specifications to communicate with the central infrastructure.

Central database with national interfaces

This would mirror the solution for the VIS with central storage (at EU level) of the data, with the establishment and maintenance of a central database and a secure communication infrastructure between the central database and Member States, including the national interfaces. Member States would be responsible for establishing the national systems and transmitting data according to defined parameters and specifications. The development and operational management of the central database and the communication infrastructure would be handled by the Management Authority, which would be the Agency for the operational management of large-scale IT systems established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 (the Agency)[37] set up to manage existing systems (SIS II, VIS, Eurodac) as well as to develop and operationally manage any future large-scale IT-systems in the area of justice, freedom and security. This approach was

[37] OJ L 286 of 1.11.2011. Detailed information on the Agency can be found in Annex 6

clearly favoured by Member States during the consultations in terms of cost-benefits and synergies with other systems.

5. ANALYSIS OF IMPACTS

This section considers each of the four policy options described in section 4 against the assessment criteria. The options have been rated on a nine-point scale with respect to their likely performance relative to the general and specific objectives. The options are assessed against the baseline. All options are also assessed against other relevant criteria, in this case criteria belonging to the general economic and social criteria:

- The border management process, in particular ensuring a fast processing of travellers without compromising security.

- Protection of fundamental rights, particularly protection of personal data (Article 8 of the Charter), right to liberty and security (Article 6), respect for private and family life (Article 7), right to asylum (Article 18), protection in the event of removal, expulsion or extradition (Article 19) and right to an effective remedy (Article 47)..

- The total one-time development costs of the system related to the expected duration of three years and the total yearly operational costs for the ensuing period of five years, split into central (EU) and national (Member States) costs; the tables in annex 2 contain more detailed information on cost categories and costs per item; a breakdown and further description of administrative costs is provided in this annex also.

The impacts have been indicated graphically with symbols:

- √√√√	Highest negative impact/cost
- √√√	Significant negative impact/cost
- √√	Medium negative impact/cost
- √	Small negative impact/cost
0	No impact
√	Small positive impact/savings
√√	Medium positive impact/savings
√√√	Very significant positive impact/savings
√√√√	Highest positive impact/savings

5.1. Policy option 1: Core system

- To counteract irregular immigration √√

The efficiency of border checks will be enhanced compared to the baseline. Replacing the stamping obligation will speed up the border checks, as alphanumeric data can be entered into

the system in a matter of seconds by scanning the passport using already existing equipment at the border crossing points. Likewise the automatic calculator will immediately provide the border guard – and the traveller - with precise information of the authorised stay, which is of particular importance when, for example, a traveller is returning for multiple entries and exits during the 6 month period. This also means that the border guard will have immediate and precise information at exit whether the traveller has complied with the maximum authorised stay.

Compared to the baseline precise information will be available on the structure and composition of irregular migrants overstaying, meaning that visa and border authorities will have information on the nationalities and type of travellers (visa exempt or not) most at risk for not complying with the rules. This will support the application of the Visa Code, which in its Article 21 refers to the assessment of the risk of illegal immigration as part of assessing the visa application. This information can also help to better understand the overall phenomenon of irregular migration and influence visa policy, where a low rate of overstays would be an important factor in considering whether to lift the visa obligation for nationals of a given third country.

The core system would also provide the EU with a precise overall understanding of who is crossing the borders and who is on the territory, something which can be seen as a core responsibility of the state in managing access to its territory.

A positive impact can be assumed as the information can be used together with other data on the presumed place of stay of the person and other information indicating where the possibilities of apprehending irregularly staying migrants are the highest and hence help in deciding where to carry out spot checks. The information provided by the system on persons whose identity is known can contribute to enforcing a return decision. The system would thus have a positive impact in reducing the current gap between return decisions issued and decisions actually enforced.[38]

A further positive impact comes from the capacity to monitor voluntary returns. Information on persons subject to a return decision who subsequently decide to return voluntarily (for which preference should be given according to the return directive) are often not available to Member States' authorities today as no information is registered at exit when the person crosses the external border. The EES would ensure that such information is available to Member States' authorities, thus avoiding that persons are considered not to have complied with the return decision and in turn risks being imposed with an entry ban, although the person may have complied with the decision within the prescribed period of time.

In terms of actually detecting persons within the territory the impact compared to the baseline is more uncertain. Information that a given person has overstayed will by no means lead to an automatic apprehension as the person can at that time be in any of the 26 countries of the Schengen area.

- To fight against terrorism and serious crime 0

The impact of this policy option on this criterion can be regarded as close to zero taking into account that no access to the system is given for the purpose of investigating serious crime or

[38] Cf section 2.1.1.3.

terrorism under this option. A small indirect impact may occur due to more effective border checks on typical cross-border crimes such as trafficking in human beings or the trafficking of illicit goods.

- Border management process 0

The impact on the border management process of an entry/exit system based on alphanumeric data at entry would be positive, as the only process required is to swipe the machine-readable zone of the passport, which is already done today; adding this process at exit would add only 10 seconds (max) to the process, so the negative impact would be negligible. A positive impact will result from abolishing the manual stamping of the passport of travellers and need to manually calculate the authorised stay. Annex 3 provides further information on the impact of the entry/exit system in the border processing.

However, a certain number of false hits and mistaken identities could be expected due to the use of alphanumeric data only to match entry and exit records. For example, this could mean that a traveller registered as having entered on a given date is registered in another name on exit and as a result the system would signal the person as an "overstayer" although he or she has effectively left the Schengen area. This could occur, for example, for persons travelling with two equally valid passports. The effects will need to be mitigated by a careful scrutiny of the responses given by the system, especially at exit, where a missing entry record should be immediately checked and clarified before the traveller passes the border check.

- Protection of fundamental rights, particularly privacy and data protection -√

The recording of the border crossings would create a 'track record' of the cross-border movements of any individual and in order to guarantee the respect of fundamental rights the safeguards listed under section 2.2.1 and the purpose limitation must always be fully complied with. However, this recording can also have positive impacts as it could also be in the interest of the individual traveller e. g. in case he or she applies for the RTP or for a multiple entry visa, and by generating a reliable travel history and proof of compliance with the existing rules regarding the right to stay. While the storage of data is vast compared to the baseline, taking into account the limited retention period the overall impact on data protection can be regarded as limited under this option, and proportionate in relation to the objectives.

5.2. Policy option 2: Core system + biometric data

- To counteract irregular immigration √√√

This policy option would have a significant effect on reducing irregular immigration compared to the baseline. The biometric identifiers of third-country nationals holding a visa will be stored in the VIS (part of the baseline) and it will therefore be possible to identify them biometrically at border crossing points or within the Schengen area even without travel documents. Conversely, this would not be possible in the case of third-country nationals not holding a visa, if the entry/exit system were to be implemented without biometrics. Therefore, if biometrics are captured and stored also from third-country nationals not holding a visa, this policy option is likely to have a significant impact on reducing irregular immigration as it will allow for identifying any undocumented third-country national found within the territory.

It should nevertheless be recalled that compared to the baseline – which includes the VIS – the added value cannot be assessed with precision due to the absence of reliable data on the share of overstayers who entered legally with and without a visa respectively. The greater the share of overstayers who are visaholders, the lesser the impact of using biometric data in the EES. That share may change – in any direction – due to a possibly evolving baseline in the future, where the visa obligation is gradually lifted for further third countries.

A further positive impact on border control of this policy option would be the possibility to prevent identity fraud: as long as the data is stored, it would be impossible for an individual to cross a second time using another travel document with another identity, as his/her fingerprints can be compared with those stored at the first entry. It would also make it impossible for different individuals to use the same travel document.

- To fight against terrorism and serious crime 0

Same as for policy option 1.

- Border management process 0

As noted under the baseline, with the integration of the VIS into border check processes, border control procedures have become more complex. Visa holders will all be subject to a biometric verification against the VIS at the border, once the transition phase of three years (started on 31 October 2011) will have expired.

An entry/exit system with biometrics would introduce, in addition, the capturing of biometrics at the first entry and the subsequent biometric verification of the visa-exempt third-country nationals, who make up approximately 17% of all travellers. This will affect the time it takes to conduct a border check in comparison with a traditional check. Member States will need to ensure that their border crossing points take into account the possible increase in queuing time for third-country nationals, and adjust their procedures at border crossing checkpoints accordingly. This negative impact will concern all Member States with significant travel flows at the external borders, and in particular those with long land borders. However, this negative impact of biometrics should be nuanced by the fact that the process of recording biometrics of visa exempted third-country nationals will be done only at the first entry and will not need to be repeated as long as the data is still stored in the system.

Positive impacts on border control would occur due to the use of biometric data as the risk of mismatches would be minimised, as with biometric data entry and exit records can be matched using a unique identifier, ie fingerprints, of each traveller.

Transitional provisions as in the VIS for the compulsory use by Member States of biometrics could be considered for an entry/exit system also. However, also in that case it would be necessary to decide whether to use biometrics from the start taking into the overall impact of that choice. Moreover, there is a risk of uneven levels of security at the external borders, as persons not subject to the visa obligation could effectively chose whether their fingerprints will be recorded or not by choosing to enter the Schengen area via a Member State that is making use of such transitional provisions. Consequently any transitional period must provide for one common approach for all Member States, instead of allowing an individual Member State not to use biometrics.

The introduction of a Registered Traveller Programme would help to mitigate these effects, in particular at air borders, as further analysed in the respective impact assessment.

The exact impact on the border management process, including how that impact may differ between land, sea and air borders, can only be fully assessed after the full implementation and rollout of the VIS as of 2014, both with regard to adapting the processes and travel flows at the border crossing points as well as with regard to the use of mobile equipment for verifying fingerprints during the border check process (e.g. at land borders).

- Protection of fundamental rights, particularly privacy and data protection -√√

Fundamental rights are clearly negatively impacted by the use of biometric identifiers in combination with the systematic recording of border crossings of third-country nationals. Use of biometric identifiers would at the same time however reduce the instances of identity fraud and safeguard the identities of travellers. Otherwise the same considerations as raised under policy option 1 are relevant here also.

5.3. Policy option 3: Core system + law enforcement purposes

- To counteract irregular immigration √√

Given the longer retention period (5 years) for this policy option consulates and border guards would have better means for assessing the risk of future overstays on the basis of solid evidence in relaton to a given individual, i.e. a person who has travelled to the EU several times over the last five years and has never overstayed presents a practically non-existent risk of overstaying, and vice versa. Beyond this the impact is the same as for policy option 1.

- To fight against terrorism and serious crime √√

The entry/exit system would provide a record of travel histories of travellers including those who are suspects of crime. It would thus complement the information in the SIS.

The data generated by the entry/exit system could be used in specific cases as a criminal intelligence tool for investigations and prosecutions of terrorism and serious crime. The data could be used by law enforcement authorities to construct evidence by tracking the travel routes of a person suspected of having committed a terrorist offence or another serious crime. There would therefore be a positive impact on this objective.

Without biometric information, the data generated by the entry/exit system could not be used to establish the identity of person who is suspected of a crime or a crime victim in case that person no longer holds any official documentation. However, law enforcement authorities could still consult the system in order to check the documents presented by a suspect or found with a victim against the alphanumeric data in the system.

It should be noted that also without access for law enforcement purposes to an EU EES, Member States could continue to operate their national EES (where existing) and to provide for such access at national level.

- Border management process 0

Same as for policy option 1.

- Protection of fundamental rights, particularly privacy and data protection -√√

It can be seen as stigmatising to store the data of a traveller due to the simple fact that he/she has crossed the external border, and a risk of abuse certainly exists as that data would allow retracing the movements of an individual over a long period of time. The large amount of data that would be stored in the system should also be taken into account (cf size of travel flows in chapter 2) in relation both to the core purpose (border and migration management) and to the more extended purpose of law enforcement: the system would store hundreds of millions of records for 5 years although only a very small – and based on existing data, impossible to quantify - share of those records would be of interest in order for the system to meet its purposes. The resulting increase in the retention period would also lead to that the cumulative size of the database, at any given moment, would be 10 times bigger compared to options 1 and 2. The proportionality of this option compared to the baseline can therefore be put in question.

5.4. Policy option 4: Core system + biometrics + law enforcment purposes

- To counteract irregular immigration √√√

Identical to a cumulation of the impacts described in relation to policy options 1, 2 and 3.

- To fight against terrorism and serious crime √√√

The impact is the same as for policy option 3 but in addition, the inclusion of biometric data in the entry/exit system will also enable law enforcement authorities in specific cases to consult the system in the event a third country national who is suspected of a serious crime no longer holds his official documentation and where there are no other reliable means of establishing the identity of the individual.

The comparison of fingerprints is both a reliable and rapid means to check a suspect's identity. Timely availability of information on a suspect is particularly relevant to avert harm to persons or goods, or to prevent damage to critical infrastructures. Rapid access is also necessary to forestall destruction of evidence of a serious crime or attempt to commit a serious crime. Moreover, a fast check of the exact identity of a detained suspect is required if there are serious grounds to believe that the person is a member of a criminal organisation that is about to carry out a serious crime. Precise information about the identity of the detained suspect increases the chances to identify the other members of the organisation. Such information is also necessary to ensure that criminal investigation focuses on the right person.

- Border management process 0

The same as for policy option 2.

- Protection of fundamental rights, particularly privacy and data protection -√√√√

Same as for policy options 1, 2 and 3 combined, while taken together, even more serious questionmarks can be raised with regard to the proportionality of storing alphanumeric and biometric data for 5 years, when the share of that data that would justify the necessity for doing so both in relation to border and migration management and in relation to law enforcement cannot be quantified.

5.5. Assessment of costs

The costs in the IA 2008 were taken from the technical feasibility study performed earlier, where the minimum technically feasible option, a web-based application for both EES and RTP, was chosen as the option to for which costs would be estimated. The pure development costs for both systems together remained, therefore, relatively low and the cost estimation did not include other required costs, as for example a secure network. The costs for a web-based communication network for both EES and RTP in the 2008 IA were estimated at €100.000 per year, compared to € 13 Mio per year (based on the current market prices) for a secure network only for the EES.

This was the main reason why it was decided to prepare a separate detailed cost study of the different implementation options presented in this impact assessment in 2010 with the help of an external contractor. Costs were calculated for numerous different scenarios. However, only the most relevant cost scenarios are presented in this impact assessment. All the cost parameters were established so that the costs were calculated on the basis of 'maximum value' estimates within a reasonable range meaning that the cost were calculated so that they should not overrun the budget in any circumstances (details on the cost study are in Annex 2).

The table below sets out the total one-time development costs and the yearly recurring costs, and accumulated total costs for this period (one-time costs and 5 years of yearly recurring costs). Costs for the EU budget to develop the entry/exit system would range between 24 and 38 million euro depending on whether biometric data are included (cf policy options) and whether a centralised or decentralised approach is chosen (to be assessed under the preferred option).

The overall costs for the Member States to develop their national infrastructures would be approximately between 142 and 191 million euro. Annual costs for maintenance and operation would range between 70 and 80 million euro.

Adding biometrics plays a part in the variations of the costs described above. In the case of a centralised system, total development costs increase by approximately 8 million euro. This limited difference is explained by the possibility to leverage synergies with the VIS at central level and due to the fact that certain investments made in the Member States to prepare for the VIS can also be used for the entry/exit system, e.g. fingerprint scanners.

In the case of a decentralised system, total development costs would increase by approximately 33 million euro if biometrics are added. The very substantial difference is explained by the need for each Member State to develop a biometric matching capability, while with a centralised approach this needs to be done only once.

In general, for the centralised option, costs are higher at EU level and correspondingly lower for Member States, and vice versa – but significantly higher - for the decentralised option. Member States' development costs increase about 50 million euro for a decentralised system with biometrics, while EU development costs increase by 10 million euro for a centralised system with biometrics. On the other hand, the latter system increases Member States' yearly costs by approximately 7 million euro, while EU level costs increase with 6 million euro.

Table 1 – Comparative assessment of costs

	One time development cost at central and national level. (3 years of development) (in EUR million)	Yearly operational cost at central and national level (5 years of operation) (in EUR million)	Total costs at central and national level (in EUR million)	ANNEX 2
Centralised system with biometrics (options 2 and 4)	180 (MS 142 EU 38)	100 (MS 80 EU 20)	680 (MS 542 EU 138)	Table 1
Centralised system without biometrics (options 1 and 3)	172 (MS 146 EU 26)	88 (MS 74 EU 14)	612 (MS 516 EU 96)	Table 2
Decentralised system with biometrics (options 2 and 4)	219 (MS 191 EU 28)	87 (MS 73 EU 14)	654 (MS 556 EU 98)	Table 3
Decentralised system without biometrics (options 1 and 3)	186 (MS 162 EU 24)	84 (MS 70 EU 14)	606 (MS 512 EU 94)	Table 4

6. COMPARISON OF OPTIONS AND IDENTIFICATION OF THE PREFERRED POLICY OPTION

6.1. Comparison of options

Table 2 – Comparative assessment of the policy options

Objective/policy option	Baseline (Policy option 0)	Policy option 1	Policy option 2	Policy option 3	Policy option 4
Policy objective: To counteract irregular immigration	0	√√	√√√	√√	√√√
Policy objective: To fight against terrorism and serious crime	0	0	0	√√	√√√
Impact on fundamental rights	0	-√	-√√	-√√	-√√√√
Impact on border management	0	0	0	0	0

Table 2 summarises the assessment of impacts done in chapter 5. The following comparison and identification of the preferred option will also take into account the following criteria:

- Effectiveness – the extent to which options achieve the objectives of the proposal;
- Efficiency – the extent to which objectives can be achieved at least cost;
- Coherence – the extent to which options are coherent with overarching objectives of EU policy.

A difficulty revealed by the assessment of the impacts of each policy option is the lack of available data, which notably influences the possibility for comparing the effectiveness of policy options 1-4. The assumption that a system with biometrics will have a higher impact on counteracting irregular migration, and that as a consequence policy options 2 and 4 would be more effective, is influenced by the share of persons not subject to the visa obligation that overstay, and this exact number is not known. The negative impact on the border management process of verifying biometrics of this group of travellers can only be fully assessed when the VIS is fully implemented. Equally for assessing the impact of giving access for law enforcement purposes comprehensive data is yet missing, as the input provided by Member States' experts so far has mainly remained general and experiences of access for law enforcement purposes to the VIS are not yet available. It can be noted that entry/exit data can be necessary for the prevention, detection or investigation of terrorist offences or other serious offences in case they involve international travel. Furthermore, the positive impact on the objective of detecting and identifying terrorist and criminal suspects is higher for a system with biometrics.

Assessing the preferred option with regard to the inclusion of biometric data must start from the core purpose of the system, related to border control and migration management. On that basis option 2 has the highest positive impact on counteracting irregular migration. The potential negative impacts on the border management process could be managed through a transitional period, whereby the system would operate based on alphanumeric data for the first three years and subsequently on the basis of alphanumeric and biometric data.

On that basis, with regard to access for law enforcment purposes, the total negative impact on fundamental rights of option 4 could be seen as potentially disproportionate, also taking into account the need for a much longer retention period.

An evaluation after a period of 2 years, taking also into account the experiences of the implementation of the VIS with regard to access for law enforcment purposes and overall experiences with regard to operating the EES, would allow for returning to the question of law enforcement access on the basis of more complete data and information to assess the impacts in more detail.

The need to give access for law enforcement purposes to the system as well as the retention period could therefore be reconsidered when the entry/exit system is evaluated after a period of 2 years. This assessment will be able to take into account experiences with the VIS as regards the access of law enforcement authorities to that system both in terms of added value in fighting serious crime and with regard to fundamental rights.

On this basis, the system would in the short run not contribute to the objectives related to the fight against crime, nor parts of the specific objectives that relate to identifying undocumented persons within the territory, but is open for doing so in the future.

In summary, the preferred option is therefore policy option 2, with an evaluation to be foreseen after two years of operation, after which an assessment will be made whether to move to policy option 4. Any such change (i.e. to policy option 4) with regard to law enforcement purposes, and/or changing the retention period will require a new legislative proposal from the Commission.

6.2. Technical implementation

A decentralised approach with national databases running regular crosschecks would have several negative consequences on the capacity of the system to deliver on its purpose and objectives. There would be an increased risk of mismatches of entry and exit records as there would be one file for each Schengen country a person has entered and exited, with the ensuing higher probability that data is recorded and stored is a different way for the same person (eg. name spelled differently).

More specifically, even if all Member States develop national EES in order to interconnect them at European level, if they keep the entry/exit data at national level, three fundamental problems would arise: a) the interconnection would bring together more than 25 disparate legacy systems, built on diverse technical infrastructures trying to communicate with each other; such an exercise has proven extremely challenging in the case of SIS II; b) even if the interconnection took place, if the data are kept only in national databases, then for every exit from the border-crossing point of a Member State, the relevant national system would have to query more than 25 other national systems in order to match the exit record with the corresponding entry record and to calculate the duration of stay; and c) the communication infrastructure would thus become extremely critical and costly; failure of any segment of the network would mean that exit records might not be matched with corresponding entry records; in addition, every MS would have to be able to match not only its own exit records but provide processing and network capacity to match all the exit records in the Schengen area.

In order to avoid any disruption of the border control process when using the EES, border guards should have data from previous entries and exits immediately displayed on the screen, in such a way that they could directly take this information into consideration when assessing the traveller's right to entry.

Because the border guard would need to request relevant data for each traveller entering or exiting the Schengen area from all of the other Schengen countries, to be able to calculate the authorised period of stay (on entry) and to verify any overstay (on exit), the decentralised approach would be time-consuming and slow down the border process significantly.

Moreover, there would be for each traveller different files in the entry and exit Member States, with the ensuing higher probability that data is recorded and stored in a different way for the same person (eg. name spelled differently or a person holding and using different passports (national passports, service passports, diplomatic passports, which can not be linked to the same person, as would be possible with a centralised architecture).

Due to the risk of mismatching entry and exit records, the risk of false hits will also increase, i.e. that a person is indicated as having overstayed although he has in fact not done so and vice versa. On the other hand, the data protection implications of this sub-option are more limited as no single database containing the records of all travellers to and from the Schengen area would be stored. Further implications would need to be assessed based on access rules, i.e. how would other Member States be authorised to search and access the data stored in the national systems of other Member States.

Finally, a decentralised approach would not achieve all the objectives. On the one hand, the unavailability of a centralised and continously maintained status of third country nationals would not allow reliable reporting on overstayers, thus impeding policy decisions concerning visas and migration. On the other hand, a decentralised architecture would be detrimental for the efficiency of border checks, in that the calculation and assessment of the duration of stay would require querying all national systems in order to retrieve all possible individual entry and exit dates; conversely, with a centralised and continuously maintained status, the information could be displayed immediately to the border guard. Therefore, the decentralised option must be discarded.

A central database with national interfaces could use the same technical infrastructure as the VIS. It should be noted that border authorities will have access to the biometric data of visa holders stored in the VIS for the purpose of verifying their identity and this could be exploited for the entry/exit system; in case the biometric functionality would be activated at a later stage, there would thus be no need to enrol the biometrics of visa holders at the border for the purposes of the entry/exit system. It must be recalled that for legislative and data protection reasons (purpose limitation, etc.) VIS data shall not be accessed and used for any purposes other than laid down in the VIS Regulation.[39]

As the matching of entry/exit records can be done in relation to one file on each individual (instead of one file for each Schengen country the person has entered or exited) there would thus be a small risk of mismatch due to the technical architecture of the system itself.

The response times of a central system, i.e. the same as the VIS (5-15 seconds), would be such that no major negative impact on the border management process would occur.

The development of the national systems and the central database must take place at the same time for technical and financial reasons. To ensure the possible connection of the national systems to a central database, the first step must be to define the interface. If this is not the case, Member States might face serious difficulties with connecting their national systems to a central system later on. Furthermore, developing first the national systems and later connecting them with a central database, would increase the costs on the national side significantly: initially Member States would need to store the entry and exit records at national level, which would still remain incomplete due to the possibility of exiting via another Schengen State; later, when the central system would be available for interconnection, the entire national infrastructure for storing the data would become obsolete and a migration of the national data might become difficult due to the need to integrate different national interfaces.

The only approach to implementing an EES would be to first define the technical standard of the interface as an implementing measure and then start the development of the systems on both national and central levels at the same time. This guarantees a lean and cost effective development with clear comprehensive testing and full compliance of the separated and distributed tasks on both national and central levels.

In conclusion, the limited benefits of national storage of data from a data protection point of view cannot outweigh the benefits of a centralised system in meeting the objectives of the

[39] Regulation (EC) 767/2008.

system. Moreover, the cost savings from a decentralised system are negligible as shown in section 5.5; looking at total costs savings over the initial eight-year period they amount to 5 million euro per year with biometrics and less than 2 million euro per year without. Overall the centralised approach is therefore the most efficient and cost-effective solution. It is also coherent with the development and management of other IT systems in the field of migration, ie Eurodac, the VIS, and the SIS/SIS II.

6.3. Preferred option

According to the comparison of options made under 6.1, the preferred solution for an EES is to start with a system based on policy option 2 and assessing the need to change to policy option 4 after two years of operation:

- The EES would at first operate as a centralised database containing alpha numeric data only and without access by law enforcement authorities. The data retention period for ordinary cases would be 6 months and in case of overstay 5 years.
- After three years of operations, the EES would operate with alphanumeric and biometric data (the latter as concerns persons not subject to the visa obligation).
- After two years of operations, the EES would be evaluated. At this time the issue of the access for law enforcement purposes as well as the retention period would be considered.
- However, in order to grant law enforcement authorities access to the data generated by the entry/exit system, the necessity and proportionality of the use of this data must be clearly demonstrated with solid evidence and the access must be combined with appropriate safeguards and limitations.

The advantages of the preferred option can be summarised as follows:

- It will provide precise information on the number of persons crossing the external border of the EU each year, further broken down by nationality and place of border crossing. The same detailed information will be provided specifically on overstayers, which will provide a much stronger evidence base as to whether nationals of a given third country should be subject to the visa obligation or not.

- It will generate precise information on overstayers for all competent authorities in the Member States, which will help to apprehend and return irregular immigrants and thereby counteract irregular immigration in general. It is, however, impossible to quantify how many overstayers would be apprehended and returned each year. However, the combination of the data generated by the entry/exit system and other relevant information on irregular migration will assist Member States to target identity controls within the territory and support the return process of those found to be staying irregularly.

- The transitional period for the use of biometrics will allow Member States to adapt their border crossing points both in terms of processes and equipment, drawing on experiences of the VIS, to ensure that the use of biometrics will not cause longer waiting times for travellers.

- It will allow for identification of persons found within the territory without documentation and who cannot be identified using the VIS.

- For the retention period it would be sufficient and coherent with the main purpose of the system to keep the entry and exit records no longer than six months, which is the minimum period the system would require to fulfill its specific purposes. A longer retention period of five years should be set in case of overstayers. This will make it possible to facilitate the identification of the third countries whose nationals have records of overstay when defining the visa policy towards these third countries. The short retention period would not prevent producing aggregate, anonymised statistics on, for example, travels flows at different sections of the external borders or from each third country.

- A 5-year retention period for overstayers would also support the implementation of the Registered Traveller Programme, as applicants for this programme could clearly and easily demonstrate an absence of previous overstays, and be coherent with the launch of such a system.

- It will provide key data for the purposes of examining the applications of third-country nationals for the RTP (new and subsequent ones). In addition, it will give the competent authorities the information needed to ensure that third-country nationals benefitting from access to the RTP comply fully with all the necessary conditions, including the respect for the duration of the authorised stay. A reliable travel history would also be needed to renew access to the RTP.

- There will be a positive impact on the border management process, simplifying and speeding up each border check as the manual stamping of passports will be abolished.

- It minimises the potential impact on fundamental rights, notably privacy and data protection: Firstly authorities will not be entitled to execute searches in the database for third country nationals who are still within the limits of the authorised period of stay. Secondly the preferred option provides for a thorough review following two years of experience of running the system. Third, there will be a number of safeguards which are detailed in section 2.2.1. In addition, the system should be designed so that it takes into account the rights of third-country nationals who are members of the family of Union citizens.

- It is coherent with overall EU policy objectives on border management, irregular migration and fundamental rights, taking into account previous policy choices and the overall objectives laid down by the European Council.

The preferred option allows for launching a system which is not dependent on the implementation of the VIS. The experiences of the latter will be available in time for the switch to biometrics as well as for the evaluation, two years after operating the EES. This approach therefore partially takes into account the opinion of the EP and the EDPS in relation to evaluating existing systems before launching new ones, and it takes into account the opinion of the Article 29 Data Protection Working Party with regard to the choice of implementation options. It should in this context be recalled that a fully sequential launch of IT systems in practice – meaning that no proposals should even be presented to establish the EES until the VIS (and SIS II) are fully operational and implemented, including any

transitional periods – effectively would mean postponing the coming into operation of an EES with a further 2-3 years, which can be seen as too long taking into account the pressing problem of irregular migration. Such a postponement would also prevent the use of fully automated border control for the purposes of a Registered Traveller Programme in the same way.

While the total costs are substantial, economies of scale can be achieved as described above in order to reduce them as much as possible. It deserves also to be recalled that the system is designed for the whole Schengen area currently consisting of 26 countries. The average cost per Member State of the development of the whole system is around 7 million euro. Overall costs for the system must therefore be seen as proportionate.

Based on lessons learnt from the development of the VIS, the technical development of the system at EU and national levels would only commence once the legislative proposals have been adopted by the EP and the Council, to allow a stable specification of exact requirements. In practice, depending on the time needed to adopt the proposals, the start of the development of the system could be envisaged for 2015 at the earliest. The Commission would develop the technical specifications and adopt them with Member States as an implementing measure, handing them off to the Agency for development.[40]

6.4. Costs of the preferred option

Taking into account the relatively small cost differences between policy options 1-4 there is not a marked difference between them in terms of the efficiency of each option. Costs for developing an entry/exit system with a gradual implementation of biometrics would be slightly more costly for Member States than developing a system with or without biometrics. These costs would be approximately €37 million at central level in both cases, and €146 million at Member State level, as compared to €142 million for a central system that would use biometrics from the start; total one-time development costs would thus increase from 180 million to 183 million euro due to the phased approach. On the other hand, average yearly operational costs are lower, resulting in lower total costs for the whole period compared to including biometrics from the start**.** Taking into account the need to evaluate the necessity of biometrics and the impact on the border management process this approach is therefore the most efficient one.

Table 3 – Costs for the preferred option

	One time development cost at central and national level. (3 years of development) (in EUR million)	Yearly operational cost at central and national level (5 years of operation) (in EUR million)	Total costs at central and national level (in EUR million)	ANNEX 2
Centralised system biometrics added later	183 (MS 146 EU 37)	88 (MS 74 EU 14)	623	Table 5

The Commission's proposal for the next multi-annual financial framework (MFF) includes a proposal of 4,6 billion EUR for the Internal security Fund (ISF) for the period 2014-2020. In

[40] The implementing measures would follow the same general principles as with the VIS meaning that for example the design of the physical architecture of the system including its communication infrastructure and the specifications for the resolution and use of fingerprints for biometric verification in the RTP would be decided in a comitology procedure.

the proposal, 1,1 billion EUR is set aside as an indicative amount for the development of an EES and an RTP assuming development costs would start from 2015, and covering 4 years of operation. Moreover, outside the scope of the ISF, a separate amount of 822 million EUR is set aside for the management of existing large scale-IT systems (Schengen Information System II, Visa Information System and EURODAC).

The Commission envisages entrusting the implementation tasks for these systems to the Agency for the Operational Management of Large-Scale IT-Systems in the area of Freedom, Security and Justice established by Regulation (EU) N° 1077/2011 of the European Parliament and the Council.[41] Providing financial support for national development costs would ensure that difficult economic circumstances at national level do not jeopardise or delay the projects.

This is different from the approach under the current MFF where the EU has funded from its budget the central costs related to the development of VIS and SIS II, while the External Borders Fund has co-financed up to 75% of the costs incurred by Member States as part of their national programmes.

Once the new systems would be operational, future operational costs in the Member States could be supported by their national programmes. It is proposed that Member States may use 50% of the allocations under the national programmes to support operating costs of IT systems used for the management of migration flows across the external borders of the Union. These costs may include the cost for the management of VIS, SIS and new systems set up in the period, staff costs, service costs, rental of secure premises etc. Thus, the future instrument would ensure continuity of funding, where appropriate.

Member States are responsible for the development and the integration into their national IT-systems as well as into their national border control processes. It is therefore not possible to calculate or to assume the proportion of costs that is likely to be borne by the Member States, because the concrete implementation in each Member State will depend on the specific situation there. The main cost factors on the side of the Member States are the costs for human ressources in the border control and for the operation of the national systems. These costs are not included in the cost tables.

Cost savings would also be achieved if the entry/exit system is built together with the registered traveller programme, compared to the situation in which both systems would be built totally independently. The main cost savings come at the central level (EU) from reduced costs for hardware, software and infrastructure and at Member States' level from administrative and office space cost savings.

6.5. Risks

The most likely risk relates to possible technical failures or breakdowns of the EES, which would negatively impact the entry and exit process of third-country nationals. To reduce this risk and the negative impacts, contingency plans should be in place and these plans should be made clear to the travellers, airlines/carriers and all authorities working at the border crossing point. In case of any failure of the system(s), the easiest and clearest contingency plan would be to ensure the electronic registration of the data using alternative backup facilities at

[41] OJ L 286, 1.11.2011, p.1.

national or European level and subsequently enter the data into the central EES as soon as possible.

As with any large scale IT-system, there are always risks with implementation. Therefore, proper implementation of the EES can only be ensured if all relevant actors fulfil their obligations, completely respect the lessons learnt from previous large-scale IT systems and take advantage of the adopted legal basis and the technical possibilities for performing optimised border checks. Common technical processes, using the system in the same way all around the external borders and a consistent implementation combined with solid overall data quality would ensure the expected results are reached. Mitigating the implementation risks by entrusting the Agency to develop a common technical platform and a standard national client which is fully tested and fulfils all legal requirements for its use by Member States would ensure that all Member States could cope with the EES without having any major implementation problems.

Furthermore, a strong monitoring mechanism with clear milestones, benchmarks and advanced compliance testing are needed to ensure a coordinated development and implementation phase throughout all Member States.

6.6. European added value and proportionality

The preferred option would create an instrument providing to the European Union the basic information on how many third country nationals enter and leave the territory of the EU. This information is indispensibly needed for sustainable and reasonable policy making in the field of migration and visa.

Furthermore the preferred option would have significant added value in providing all Member States with clear and unambiguous data on overstayers and access to alerts on each individual, greatly contributing to the possibility of apprehending those persons and launching, where required, a return process. Compared to the baseline, with its reliance on the manual stamping of passports, and taking into account the size of the problem of overstayers at European level, the added value is apparent.

The preferred option will, compared to the national entry/exit systems currently in operation, bring benefits in terms of counteracting irregular immigration by providing border authorities with more reliable and modern tools for carrying out border checks. The investments made into hardware and software for their national systems might not be lost – some of the equipment and system software may be reused in the centralised solution. Member States will have the opportunity to discuss the specifications of the system in comitology procedures, and can argue to use a certain platform that they might have already proven useful. In any case, the national entry/exit systems may be maintained for national security purposes in accordance with Member States' own security-related legislation**.**

The preferred option is proportionate in terms of the right to protection of personal data in that it does not require the collection and storage of more data for a longer period than is absolutely necessary to allow the system to function and meet its objectives.

No further processes or harmonisation will be necessary at EU level to make the system work; thus the envisaged measure is proportionate in that it does not go beyond what is necessary in terms of action at EU level to meet the defined objectives.

The preferred option is also proportionate in terms of costs, taking into account the benefits the system will provide to all Member States in managing the common external border and progressing towards a common EU migration policy.

6.7. Legislative implications

An EU Regulation would be required to implement the entry/exit system, to provide a legal basis for the development and implementation of the technical system, rules on the storage of data and data protection safeguards, and monitoring and evaluation. The Schengen Borders Code would need to be amended regarding the use of the system as part of the border management process, and to eliminate the stamping obligation.

The Regulation establishing the Agency already foresees that the Agency may be made responsible for the preparation, development and operational management of new large-scale IT systems but this text will need to be amended to reflect the new tasks entrusted to it.

7. MONITORING AND EVALUATION

The Commission shall ensure that systems are in place to monitor the functioning of the entry/exit system and evaluate them against the main policy objectives. Two years after the system starts operations and every two years thereafter, the Management Authority should submit to the European Parliament, the Council and the Commission a report on the technical functioning of the system. Moreover, two years after the entry/exit system starts operations and every four years thereafter, the Commission should produce an overall evaluation of the system including on fundamental rights impacts and on examining results achieved against objectives and assessing the continuing validity of the underlying rationale and any implications for future options. The first evaluation should focus on whether access for law enforcement purposes should be granted and whether the retention period should be extended and would be accompanied by legislative proposals as appropriate. The Commission should submit the reports on the evaluation to the European Parliament and the Council.

Monitoring and evaluation indicators could be the ones listed below, in relation to each of the specific objectives and based on the preferred option. None of this data is available without an entry/exit system, which will allow not only to monitor and evaluate the system, including the possible phasing in of biometric data, but also to feed it into other relevant policy issues related to borders and visas.

Specific objective	Indicator
To enhance the efficiency of border checks through monitoring of the rights to authorised stay at entry and exit, and to improve the assessment of the risk of	Processing time at the border crossing points Numbers of overstayers identified at border crossing points

overstay;	System availability Error rates e.g. Failure to Enrol (FTE) rates, False Acceptance Rates (FAR), false hits, etc.
To monitor compliance with the authorised stay of persons within the territory;	Number of alerts on overstayers
To generate reliable information to allow the EU and Member States to make informed policy choices concerning visa and migration;	Number of alerts on overstayers by category visa-required/visa-exempt, by type of border land/sea/air, by Member State, by country of origin/nationality
To identify and detect irregular immigrants, especially overstayers, also within the territory and to increase the possibilities for return;	Numbers of alerts leading to the apprehension of overstayers
To safeguard the fundamental rights, especially protection of personal data and right to privacy, of third country nationals.	Number of incorrect alerts on overstayers Number of false matches of entry/exit records Number of complaints by individuals to national data protection authorities

ANNEXES

ANNEX 1

LIST OF ACRONYMS

EBF	External Borders Fund
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
ISF	Internal Security Fund
RTP	Registered Traveller Programme
SIS	Schengen Information System
TCN	Third-country national
VIS	Visa Information System
PNR	Passenger Name Record
API	Advanced Passenger Information
IATA	International Air Transport Association
Frontex	European Agency for the Management of Operational Cooperation at the External Borders
ESRIF	European Security and Research Innovation Forum
IAB	Impact Assessment Board
SBC	Schengen Borders Code
EU OCTA	European Organised Crime Threat Assessment
EURODAC	European Dactyloscopie (EU Fingerprint Database for Identifying Asylum Seekers

ANNEX 2 - COSTS

1. Introduction

This Annex provides the cost estimates for the different options that are described in the present impact assessment.

Due to the fact that the variables for each option are numerous and some of them are not relevant in terms of costs, this annex only presents the cost estimates for the following possible options:

- Centralised/decentralised architecture
- Biometrics/no biometrics/biometrics added later

An external contractor carried out the cost study in 2010[42], aimed at getting an objective cost estimation, comparing various options and sub-options in search of the most cost-effective ones, while evaluating the different business alternatives. The assessment of cost effectiveness was related both to the one-time costs for the development and to the yearly recurring costs, which can decrease or invert savings in development costs in a very short period of time.

Based on the scenario-driven approach of the cost study and the cost models developed therein, it was possible to update the scenarios with modified options.

2. METHODOLOGY

The cost analysis study began by defining detailed scenarios and border-related specifications. MS were involved in the preparation of the definition of the parameters in the cost study[43].

The IT-related cost factors were taken from current market prices.

To calculate the costs accurately, the following techniques were used:

- Sizing
  - Hardware sizing based on simplified process models and forecasted numbers of RT travel events. Sizing in this context comes down to actually determine which of building blocks are required for which scenarios, thus calculating the actual "horsepower" needed to meet the required performance.
  - Software development sizing based on information in the Feasibility Study and completed with Function Point Analysis when necessary.
  - Network sizing based on predictions of the expected system load.
- Costing

[42] Final report on the cost analysis of entry/exit and RTP systems done by the external contractor on 19 of April 2010 (version 1.30) is published on the following website: http://ec.europa.eu/home-affairs/doc_centre/borders/borders_schengen_en.htm#studies

[43] E.g. through the exercise undertaken by the Swedish Presidency in the Frontiers Working Group at the end of August/beginning of September 2009 to count numbers of border crossings per category of traveller, etc.

- Parametric cost analysis techniques were used to estimate development efforts and maintenance costs to support the introduction of a new software product.

- Parametric cost estimation is based on the functional size of the solution, the level of re-usability of existing products and the proportion of "commercial of the shelf" (COTS) products that are used. Additional parameters are the hourly rates and skill levels of the development team as well as parameters associated with the development environment and project governance.

- Estimates of the costs of third party hardware, software and network products were based on list prices of popular and appropriate COTS products.

- For estimating operational costs a harmonised model was assumed, in which the average rates were used across the Member States. The same approach was chosen regarding the business hours throughout the European Union as well as the same number of holidays.

➢ Planning

- The initial planning was produced by the parametric costing tool "CostXpert". This includes in a first automated run specification, design, realisation, testing and implementation and the first phase of deployment, where any defects have been detected.

- Manual intervention and adjustment of the schedule became necessary, as "CostXpert" assumes unlimited resources to be available, which means that the planning needs to be adjusted to align it with the expected situation.

Based on these techniques for cost modelling, the different scenarios were established and calculated for the central side (Management Authority; EU budget) and the national side (Member States' authorities, national budget)

➢ Moreover, the gathered experiences and lessons learnt from the development of EURODAC, VIS and SIS II were also used to evaluate the cost calculations and the scenarios to improve the reliability of the cost calculation as mentioned on page 36.

3. FACTS AND FIGURES USED

General Parameters

For the cost calculation, a complete range of parameters (business parameters, technical parameters, cost parameters, data specifications, and parameters on the side of the MS[44]) were used:

➢ Development three years and five years of operation
➢ Both EES and RTP should, as far as possible, take advantage of the existing and fully rolled out VIS (e.g. fingerprints of visa holders are stored only in the VIS)
➢ Maintenance rate of hardware (8 %) and software (20 %)

[44] The parameters and the values used can be found in the final report of the available cost study.

- Hourly rates for contractors, management authority staff and EU (27) and Schengen associated country staff, working hours per year

Entry/Exit System

For the Entry/Exit System, the following core parameters were used for the sizing of the system:

EES Parameter		2013	2014	2015	2016	2017	2018	2019	2020
Border Crossings									
TCNVH Crossings IN	(million)	67	74	81	89	98	108	119	131
TCNVE Crossings IN	(million)	100	110	121	133	146	161	177	195
Total Crossings IN	(million)	**167**	**184**	**202**	**222**	**245**	**269**	**296**	**325**
TCNVH Crossings OUT	(million)	67	74	81	89	98	108	119	131
TCNVE Crossings OUT	(million)	100	110	121	133	146	161	177	195
Total Crossings OUT	(million)	**167**	**184**	**202**	**222**	**245**	**269**	**296**	**325**
Total Crossings	(million)	**334**	**367**	**404**	**445**	**489**	**538**	**592**	**651**

- For the network, the costs of the sTESTA network for the VIS were used + 50% to accommodate the higher volume of network traffic.

4. SENSITIVITY ANALYSIS

The cost study defines the underlying assumptions as well as the parameters to establish the cost model in a bottom – up approach.

The most sensitive parameters and assumptions were identified as

- the anticipated system load (number of expected entries and exits per traveller category);
- the number of fingerprint searches (identification mode) to be performed by the system;
- the footprint of the installed hardware especially in the case of a distributed scenario;
- the retention period;
- the time factor;

The assumption on the system load was based on the data collection exercise in September 2009 during the Swedish Presidency. Based on this empirical data gathered as an initial value, an annual increase of 10% was used in order to avoid any underestimation of the system load and to make the system capacity-proof at least for the first decade.

The number of fingerprint searches is the most time-consuming operation among the messages sent to the system. In relation to the policy options, the retention period is the relevant factor, because fingerprint searches are used on the one hand to identify individuals within the Schengen territory, who are no longer in possession of their travel documents; on

the other hand the fingerprint searches must be used during the enrolment of the first entry at an EU external border crossing point (4.1.2, pg 19). In case of a very short retention period, biometric data would need to be enrolled anew each time the person enters the Schengen area and the retention period is shorter since the last exit.

The footprint of the installed hardware is sensitive, especially in the case of a distributed scenario. In this case, instead of one set of central hardware at least in every Member State the installation of a partial hardware set is necessary. Improving the capacity of the installed hardware will be much more costly in case of a decentralised solution as in case of a centralised architecture.

The retention period is sensitive, especially if it is volatile. With a fixed retention period the required data storage and the related operations can be calculated based on the forecasted system load. The necessary capacity planning can also take place on the basis of the operational system monitoring. If the retention period is variable, this must be implemented in the underlying business logic. In addition, the possible variations with the retention period need to be respected in the capacity planning (the size of the data storage but also the capacity of the hardware to process all the necessary operations). As described above (under fingerprint searches) the length of the retention period affects the number of time consuming processes significantly.

In order to make the IA sensitive to time, discounting has been used, i.e. the discounted impact of a policy option was evaluated by calculating its present "value", be it benefit or cost. In practice, the real discount rate was used, in the sense of a long-run average of the real "value".

The costs calculated represent a 'maximum value' within a reasonable range not only assuming the best case scenarios regarding the sensitive parameters but also a wider range of possible scenarios.

5. COSTS OF A PHASED APPROACH

In order to calculate the cost differences for a phased approach, ie where after the operation of an EES after a period of three years there would be a switch to an EES processing biometric data and/or with a purpose extended to fighting terrorist offences and serious crime, two main aspects were relevant: the impact on the development costs and the impact on the maintenance costs.

For the development costs the possibility of the activation / deactivation of the use of biometrics and two different sets of messages (one with biometrics and one without biometrics) were considered. Some costs increased especially for the development. On the other hand, the costs for hardware and storage were reduced due to the smaller size of the initial configuration. The total costs for the central development decreased by 240.688 €.

On the MS side the development increased by 2.8 Mio €. The main reason is the higher effort for the development of the national systems (+ 2.1 Mio €) and to a smaller extent the administrative costs for additional testing. As the MS do not store biometric data and it is

assumed that the VIS fingerprint scanners will be re-used, no further decreasing cost effect was identified.

For the maintenance costs the phased approach has the following impact: Due to the smaller data storage and reduced personnel effort to maintain the system, the maintenance costs both on the central and the national side are reduced. Costs increase with the size of the system, however, with a delay due to the time of the deactivation of the biometrics. Due to the fact that the yearly costs for the maintenance of the system during the operational phase have been averaged, the differences are not directly obvious in the cost tables but they are respected.

1. Central EES with biometrics		Yearly operational costs	Total one time development costs	
	Required action		EU	MS
1	**Management Authority**			
2	MA Hardware	430.000	3.748.000	
3	MA Other (training, meetings)	503.687	503.687	
4	MA Infrastructure	12.062.948	13.872.390	
5	MA software	5.800.000	11.490.000	
6	MA Admin	924.685	2.504.941	
7	MA Office Space	9.000	27.000	
8	MA Contractor Development	536.027	5.360.274	
9	**Subtotal MA**	**20.266.347**	**37.506.292**	**0**
10	**Member States *)**			
11	MS Hardware	24.000		23.070.000
12	MS Other (training, meetings)	115.852		1.158.521
13	MS Infrastructure	0		0
14	MS software	836.000		41.159.100
15	MS Admin	64.135.354		37.567.248
16	MS Office Space	14.102.800		34.074.720
17	MS Contractor Development	575.859		5.758.592
18	**Subtotal MS**	**79.789.865**	**0**	**142.788.181**

*) Member States means the Schengen area as of 19.12.2011 plus Bulgaria and Romania and was calculated as one entity.

2. Central EES no biometrics		Yearly operational costs	Total one time development costs	
	Required action		EU	MS
1	**Management Authority**			
2	MA Hardware	28.000	2.764.000	
3	MA Other (training, meetings)	502.226	502.226	
4	MA Infrastructure	12.062.948	13.872.390	
5	MA software	970.000	3.168.000	
6	MA Admin	557.914	2.694.657	
7	MA Office Space	9.000	27.000	
8	MA Contractor Development	323.669	3.236.690	
9	**Subtotal MA**	**14.453.757**	**26.264.963**	**0**
10	**Member States**			
11	MS Hardware	24.000		23.070.000
12	MS Other (training, meetings)	157.075		1.570.747
13	MS Infrastructure	0		0
14	MS software	815.000		41.159.100
15	MS Admin	57.804.916		38.067.738
16	MS Office Space	14.002.800		34.074.720
17	MS Contractor Development	780.762		7.807.615
18	**Subtotal MS**	**73.584.553**	**0**	**145.749.920**

3. Distributed EES with biometrics		Yearly operational costs	Total one time development costs	
	Required action		EU	MS
1	**Management Authority**			
2	MA Hardware	161.200	873.200	
3	MA Other (training, meetings)	506.772	506.772	
4	MA Infrastructure	12.062.948	13.872.390	
5	MA software	116.000	1.164.000	
6	MA Admin	436.023	1.603.614	
7	MA Office Space	9.000	27.000	
8	MA Contractor Development	584.695	9.846.948	
9	**Subtotal MA**	**13.876.638**	**27.893.924**	**0**
10	**Member States**			
11	MS Hardware	54.000		35.748.000
12	MS Other (training, meetings)	1.176.912		11.769.115
13	MS Infrastructure	0		1.782.000
14	MS software	880.000		67.500.000
15	MS Admin	56.602.308		27.000.000
16	MS Office Space	14.002.800		36.499.680
17	MS Contractor Development	357.867		10.578.668
18	**Subtotal MS**	**73.073.887**	**0**	**190.877.463**

4. Distributed EES no biometrics		Yearly operational costs	Total one time development costs	
	Required action		EU	MS
1	**Management Authority**			
2	MA Hardware	67.600	816.400	
3	MA Other (training, meetings)	1.008.783	1.087.828	
4	MA Infrastructure	12.062.948	13.872.390	
5	MA software	440.000	1.164.000	
6	MA Admin	379.313	1.174.966	
7	MA Office Space	9.000	27.000	
8	MA Contractor Development	238.506	6.385.058	
9	**Subtotal MA**	**14.206.150**	**24.527.642**	**0**
10	**Member States**			
11	MS Hardware	40.500		30.213.000
12	MS Other (training, meetings)	1.548.535		15.485.352
13	MS Infrastructure	0		1.782.000
14	MS software	0		37.800.000
15	MS Admin	53.184.504		28.507.887
16	MS Office Space	14.002.800		34.074.720
17	MS Contractor Development	1.086.504		13.865.036
18	**Subtotal MS**	**69.862.843**	**0**	**161.727.995**

5. Central EES biometrics added later		Yearly operational costs	Total one time development costs	
	Required action		EU	MS
1	**Management Authority**			
2	MA Hardware	14.000	2.764.000	
3	MA Other (training, meetings)	503.874	503.874	
4	MA Infrastructure	12.062.948	13.872.390	
5	MA software	300.000	11.990.000	
6	MA Admin	757.854	2.475.776	
7	MA Office Space	9.000	27.000	
8	MA Contractor Development	563.256	5.632.564	
9	**Subtotal MA**	**14.210.932**	**37.265.604**	**0**
10	**Member States**			
11	MS Hardware	24.000		23.070.000
12	MS Other (training, meetings)	110.567		1.105.665
13	MS Infrastructure	0		0
14	MS software	815.000		41.159.100
15	MS Admin	58.244.916		38.367.738
16	MS Office Space	14.102.800		34.074.720
17	MS Contractor Development	549.586		7.807.615
18	**Subtotal MS**	**73.846.869**	**0**	**145.584.838**

ANNEX 3 – Border processing data

1. BORDER CHECKS

To find out the time needed to cross the external border the Czech Presidency together with the Commission launched a questionnaire. According to the Member States' replies to the questionnaire, currently the average time for a border check for visa holders on entry at the land border is 2 minutes 17 seconds, for visa-exempt nationals 1 minute 12 seconds and for EU citizens 20 seconds. The average time on exit at the land border is for visa holders 1 minute 34 seconds, for visa-exempt nationals 58 seconds and for EU citizens 18 seconds.

The average time at air borders on entry for visa holders is 1 minute 44 seconds, for visa-exempt nationals 1 minute 3 seconds and for EU citizens 15 seconds. The average time at air borders on exit is for visa holders 1 minute 11 seconds, for visa-exempt nationals 52 seconds and for EU citizens 15 seconds.

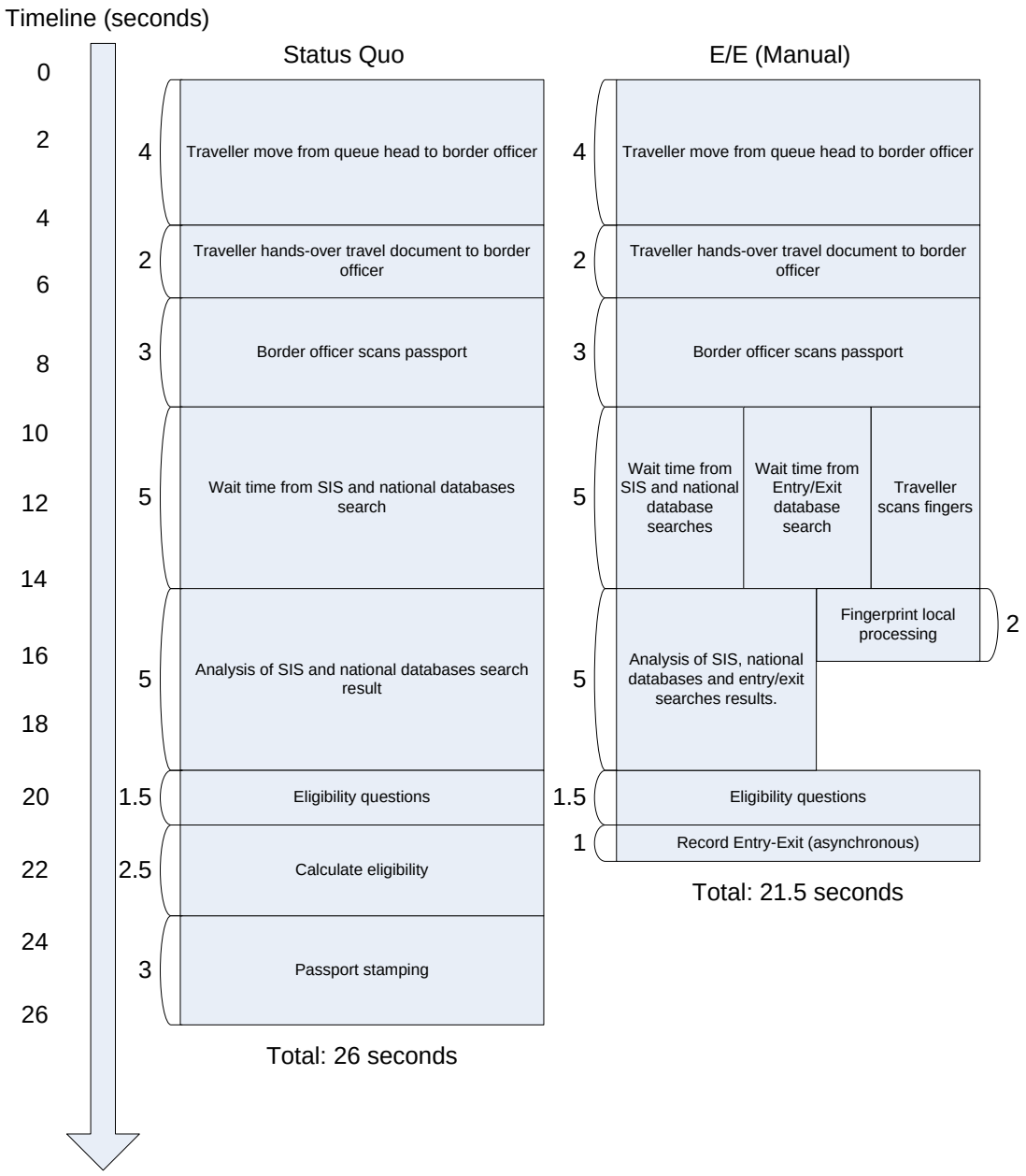
The time spent on a border check at the sea border is not reported because the results are quite similar to checks carried out at land borders. The aforementioned times do not include anything else but basic first-line border checks (verification of the identity of the person and checking of travel document(s) and necessary databases) in a situation where everything seems to be in order concerning the traveller.

As can be seen, the longest time is needed for border checks on entry at the land and sea borders for visa holders. However, visa holders represent only a small minority of travellers at sea borders.

Below an estimate is made of the additional time that would be needed to verify the identity of each person using biometrics under the assumption that the stamping obligation would be replaced with an entry/exit system, which would allow certain time savings. However, these estimates must be considered on the low side as well as mainly relevant for air border crossings.

2. VISA-EXEMPT TCN (TCNVE) - ENTRY

The following diagram highlights the timing of the different operations performed during a normal border crossing process for TCNVE travellers entering the Schengen area. The situation before and after the introduction of an EES are compared. The "Status Quo" or baseline scenario denotes the state of affairs after VIS is fully implemented and operational at all border crossing points.



The assumptions taken on the timeline above are:

- Eligibility questions (regarding the right to enter) are put to 10% of the travellers, on a random basis. An average of 15 seconds is presumably needed for the border officer and the traveller to interact. So, for the average population of travellers, we consider that the time necessary for eligibility questions is 10/100 * 15 = 1,5 seconds.

- The time necessary to manually calculate the maximum duration of the stay based on previous travels is estimated on the basis of taking around five (5) seconds per traveller who has previously travelled to the Schengen area. We estimate that in 50% of cases, it is the first journey of the TCNVE on this travel document. So, this is an average of 50/100 * 5 = 2,5 seconds per traveller.

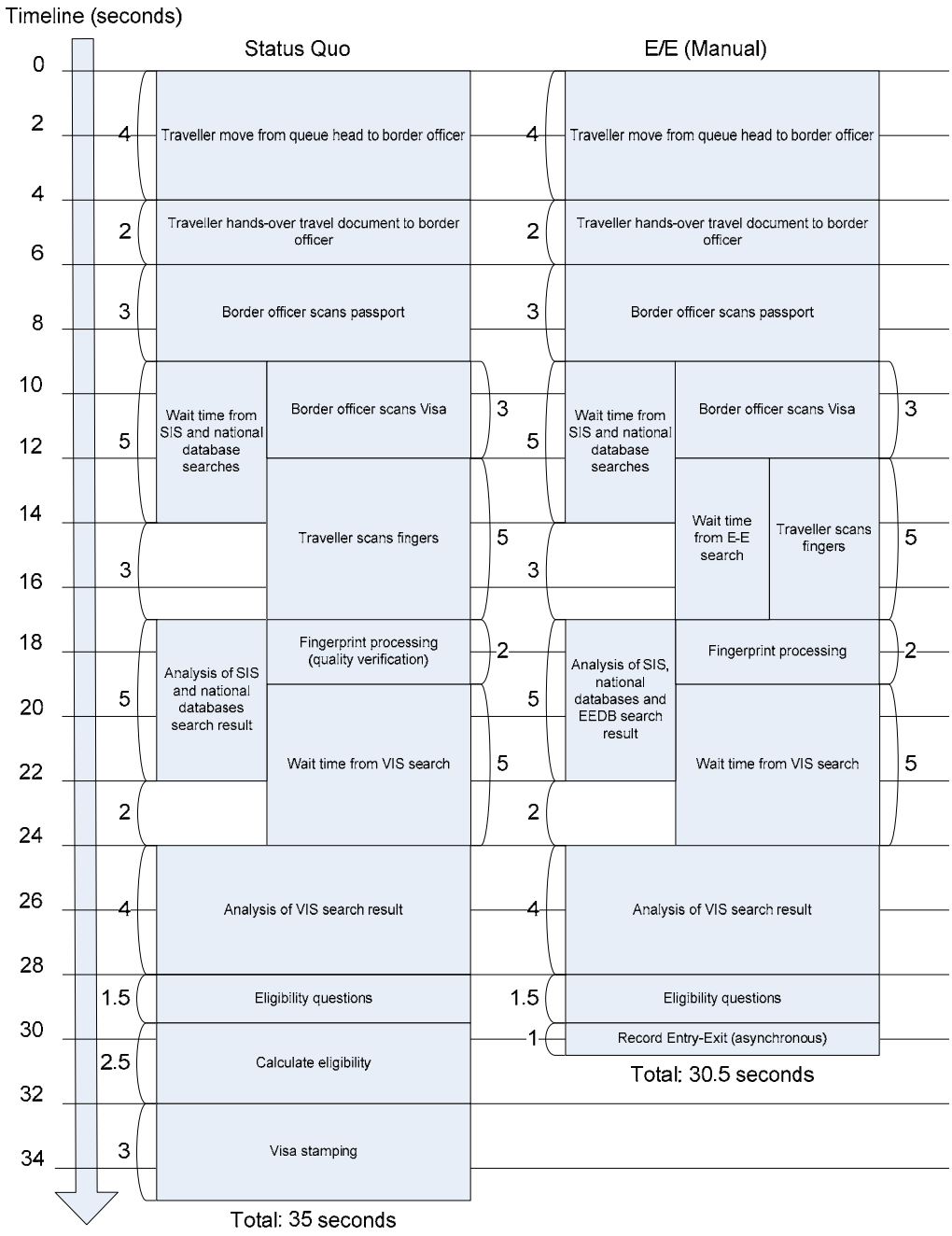
- Photo capture is not considered, as this is an optional component of the EES.

The assumptions above are also valid for the other timing cases below.

The introduction of an EES does not increase the time to process a TCNVE, as the fingerprint scan can be performed during the wait time required to get the results from the interrogation of the required databases. On the contrary, the processing time is slightly reduced due to the replacement of physical stamping by electronic entry recording, and also due to the automated calculation of the eligibility and maximum duration of stay.

3. THIRD-COUNTRY NATIONAL VISA HOLDERS (TCNVH) – ENTRY

The following diagram highlights the timing of the different operations performed during a normal border crossing process for TCNVH travellers entering the Schengen area. The situations before and after the introduction of an EES are compared.

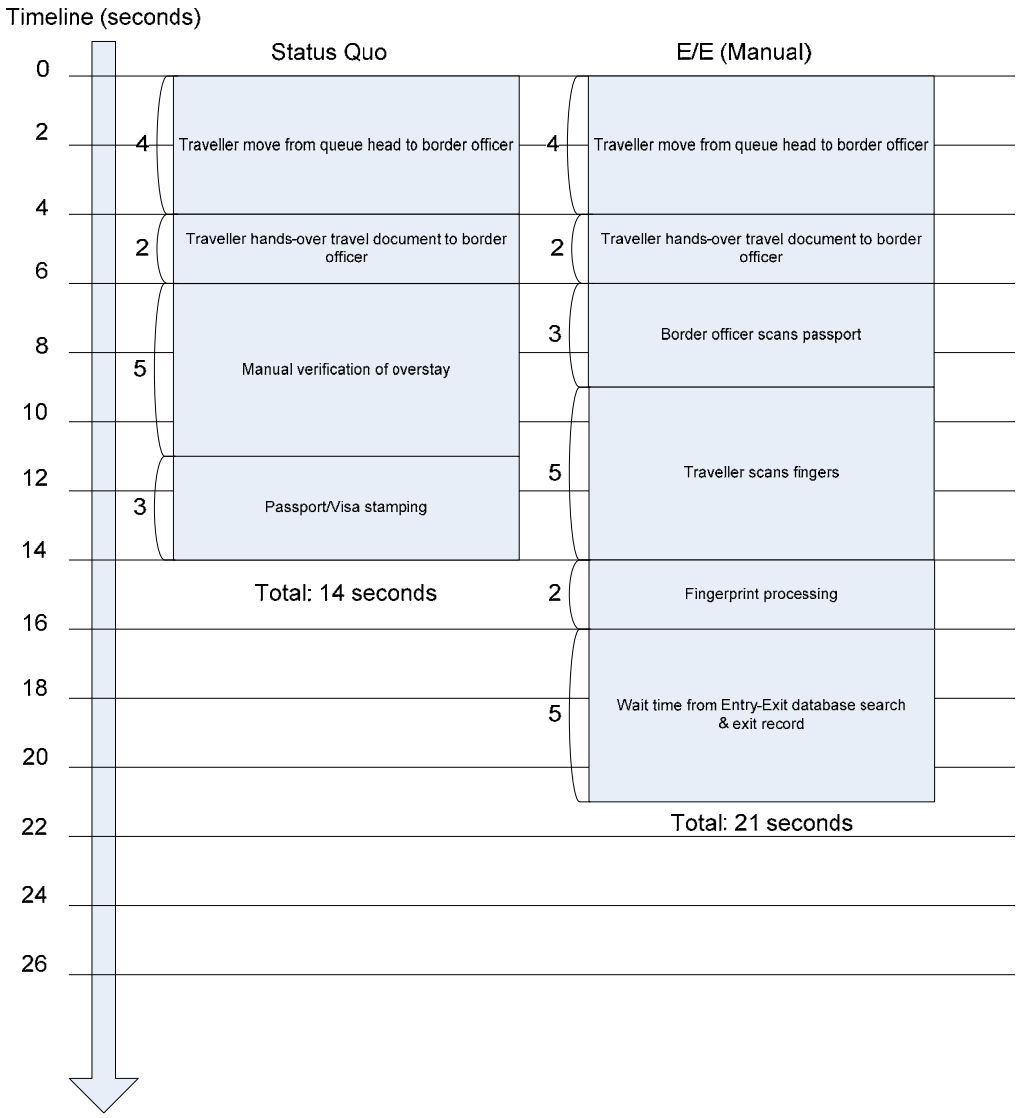


The introduction of an EES does not increase the time to process a traveller, as roughly the same operations are performed in both cases.

On the contrary, the processing time is slightly reduced due to the replacement of physical stamping by electronic entry recording, and also due to the automated calculation of the eligibility and maximum duration of stay.

4. TCNVH AND TCNVE EXIT

The following diagram highlights the timing of the different operations performed during a normal border crossing process for TCN travellers leaving the Schengen area. The situations before and after the introduction of an EES are compared. Both types of TCN travellers (TCNVE and TCNVH) are processed in the same way, and therefore, they are treated together in this section.



The time necessary to manually calculate whether a traveller has overstayed is estimated on the basis of five (5) seconds per traveller. This calculation needs to be made for all TCN.

As can be seen, the introduction of an EES considerably increases the time to process a TCNVE leaving Schengen. This is due to the introduction of fingerprint capture and remote database interrogation.

The process is identical for all TCN, as the travel document ID has been selected as the key for searches in the EES.

ANNEX 4 - DATABASES AND SYSTEMS AT EU LEVEL

Centralised databases containing alerts on persons and other categories of data for law enforcement and border check purposes (SIS), visa applicants (VIS) and asylum applicants in addition to other categories of persons (Eurodac) have been set up and/or are being developed at EU level. Furthermore, a police co-operation mechanism for exchanging information on DNA, fingerprints and vehicle registration data has been established through the Prüm Decisions.

None of these systems address the administrative requirements for managing the right to stay in the EU and the gaps that can be filled by an entry/exit system as regards identifying and preventing irregular immigration, especially as regards overstayers.

SIS

The Schengen Information System (SIS) is a centralised information system. The SIS, together with the cooperation of the SIRENE bureaux, set up pursuant to the provisions of Title IV of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (Schengen Convention) (15) constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union.

The main categories of data contained in the SIS are:
- Persons wanted for arrest for extradition purposes;
- Third-country nationals to be refused entry to the Schengen territory;
- Missing persons (minors and adults);
- Witnesses and persons required to appear before the judicial authorities in connection with criminal proceedings;
- Person or vehicles to be put under discreet surveillance or for specific checks;
- Certain categories of objects (e.g. stolen identity cards, vehicles, firearms, bank notes).

The Schengen Information System (SIS) provides access to alerts on persons and objects to the following authorities:
- authorities responsible for border checks;
- authorities carrying out and coordinating other police and customs checks within the country;
- national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation;
- authorities responsible for issuing visas, the central authorities responsible for examining visa applications, authorities responsible for issuing residence permits and for the administration of legislation on third-country nationals in the context of the application of the Union acquis relating to the movement of persons;
- authorities responsible for issuing vehicle registration certificates.

It is up to each Member State to decide which national authorities are competent and shall have access to some or all categories of SIS alerts depending on that competence.

Europol and Eurojust also have access to certain categories of alerts (16). Europol may access data entered for alerts for arrest, alerts for discreet surveillance or specific check and alerts on objects for seizure or use as evidence in criminal proceedings. Eurojust may access data entered for alerts for arrest and alerts for a judicial procedure.

The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system. The SIS enables the users to check persons and objects both at external borders and within the territory of the Schengen States. The SIS provides law enforcement authorities with information on why a certain individual is wanted, what action is to be taken and whether the person is presumed violent and armed.

However, as the information contained in the SIS is only sufficient for the authorities on the ground to take the correct initial actions it is necessary for the Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole.

Article 92(4) of the Schengen Convention provides that Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (SIRENE), all information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this System.

The Schengen States are the owners of the data they introduce into the SIS and bear the responsibility for their legality and accuracy.

Annual statistics on the number of alerts are collated and published by the Council, not only on the total number of alerts but also the different categories of alert.

- By the start of 2011 (01.01.11), the total of valid records in the SIS reached 35.69 million which means an increase by 12.9% compared to the start of 2010..
- Nearly 30 million records existed on that date on lost, stolen, misappropriated identity documents (passports, identity cards, driving licence);
- More than 1.2 million records existed on that date on wanted persons
- The vast majority of alerts on persons are about third-country nationals who shall be denied entry to the Schengen area;
- The SIS currently stores only alphanumeric data (letters and numbers), comprising data as regards individuals on[45]:
- names, including aliases;
- sex ;
- objective physical characteristics not subject to change";
- date and place of birth;
- nationality;
- whether the persons are armed or violent;
- the reason for the alert; and

[45] Article 94(3) of the Schengen Convention.

- the action to be taken.

In the context of EU enlargement, the technological platform needed to be upgraded and additional features were desired. For these reasons, the second-generation Schengen Information System (SIS II) is being developed.

SIS II has been designed to function in an enlarged Europe, but also to deal with new challenges and use biometrics to aid in the verification of a person's identity. SIS II will provide the following new functionalities:

- The addition of new categories of alerts (aircrafts, boats, boat engines, containers, industrial equipment, vehicle number plates, vehicle registration documents);
- The addition of new categories of data, including biometric data (biometric data such as fingerprints and digital facial images may be stored for the purposes of confirming identity;
- The interlinking of alerts.

On 20 December 2006 two Regulations and a Council Decision[46] were adopted on the establishment, operation and use of SIS II[47].

VIS

The Visa Information System (VIS) is a system for the exchange of short-stay visa data between the Schengen and the Schengen Associated States that was initially established in 2004[48]. All functionalities of the VIS are based on visa applications or visa decisions attached to applications. After a first registration, a visa application can be amended, until a decision is made whether or not a Schengen visa should be issued. After visa issuance, further decisions can be made, for example, an issued visa can be revoked or annulled, or a visa can be extended. The VIS supports the storage, maintenance and retrieval of this information.

The main objectives of the VIS are:

- to facilitate the visa application procedure;
- to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application ("visa shopping");
- to facilitate the fight against fraud;
- to facilitate checks at external border crossing points and within the territory of the Member States;
- to assist in the identification of any person who may not, or may no longer fulfil the conditions for entry to, stay or residence on the territory of the Member States;
- to facilitate the application of Regulation (EC) No 343/2003 ("Dublin II" Regulation);
- to contribute to the prevention of threats to the internal security of any of the Member States.

According to the text of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008, the VIS will store personal data from visa applicants:

- Data on the applicant (i.e. name, address, occupation);

46 Council Decision 2007/533/JHA.

47 Regulation (EC) No 1987/2006 and Regulation (EC) No 1986/2006.

48 Council Decision (EC) 512, 8.6.2004.

- Data on the visa application process (date and place of the application, visas requested, issued, refused, annulled, revoked or extended);
- Biometrics (photographs and fingerprints).

According to Council Decision 2008/633/JHA of 23 June 2008, law enforcement authorities from Member States and Europol will have a restricted and indirect access to the VIS data. Each Member State will have to designate an authority responsible for controlling law enforcement access to the database and the police will have to provide evidence that their query is necessary for criminal investigations.

Transfer of data to third countries or international organisations is in principle not allowed. By way of derogation, certain data may be transferred or made available if necessary in individual cases for proving the identity of a third-country national, including for the purpose of return, providing that specific conditions are met. Data obtained pursuant to Decision 2008/633/ JHA may only be transferred or made available in an exceptional case of urgency and only for the purpose of the prevention and detection of terrorists and serious crime offences and with the consent of the Member State that entered the data. Furthermore, a permanent Management Authority (the Agency) will be responsible for maintenance and operations of the VIS database and the visa application data will be stored for a maximum of five years.

The VIS started operations in the first region on 11 October 2011 on the basis of the Commission implementing decision of 21 September 2011 (2011/636/EU) and Commission Decision of 30 November 2009 (2009/49/EC). The operations started first at the consulates in North Africa and 20 days after go-live of the VIS also at the border crossing points (verification of visas against the VIS). On 10 May 2012, the VIS was successfully launched in the second region, the Near East (Israel, Jordan, Lebanon and Syria). Further, the VIS on 2 October 2012 started operations in a third region, the Gulf (Afghanistan, Bahrain, Iran, Iraq, Kuwait, Oman, Qatar, Saudi Arabia, United Arab Emirates and Yemen).

BMS

The Biometric Matching System (BMS) developed for the VIS is an information search engine that can match biometric data from visa applications, identity management systems and policing systems. The BMS is designed to enable justice and immigration authorities to deal with security and other issues related to terrorism, organized crime, irregular immigration, visa shopping, identity theft and fraud.

The BMS database will be able to store the fingerprints of up to 70 million people and process more than 100,000 verification and identification requests per day. The system will perform one-to-one comparisons for biometric verifications and one-to-many searches for biometric identifications.

The BMS is developed using a service-oriented architecture approach, has the capability to connect with a number of IT systems and manage functions related to visas, immigration, border control and police cooperation. In addition, the technical architecture will be flexible enough to accommodate new developments in EU policy as immigration and border control procedures evolve.

Eurodac

Eurodac is a fingerprint database that stores and compares the fingerprints of asylum applicants and irregular immigrants and allows Member States to determine the State responsible for examining an asylum application in accordance with the Dublin II Regulation[49]. The Eurodac central unit operates a central database comparing fingerprints, an automated fingerprint identification system (AFIS) and a secure communication system for data transmission from and towards the national units (National Access Points) in Member States.

Data collected for any asylum applicants over 14 years of age include:

- Fingerprint and control images;
- Date of the asylum application;
- The Member State where the asylum application was filed;
- The gender of the applicant.

Data are collected according to three categories:

Category 1: data of asylum applications. Fingerprints of asylum applicants are sent to the Central Unit for comparison against fingerprints of other asylum applicants who have previously lodged their application in another Member State. This data is retained for 10 years, but is deleted when an individual obtains the nationality of one of the Member States.

Category 2: data of aliens apprehended in connection with irregular crossing of an external border and where not repatriated. Fingerprint of these individuals are sent to the Central Unit for storage only, in order to be compared against the data of any asylum application submitted subsequently to the Central Unit. This data is retained for two years, but is deleted if the individual receives a residence permit, departs the territory of a Member State or obtains the nationality of one of the Member States.

Category 3: data of aliens found irregularly present in a Member State. This data is not stored but is searched against the data of asylum applicants stored in the central database. The transmission of this category is not mandatory but optional for Member States.

However, there is limited possibility to use Eurodac data for internal security purposes. In the revision of the Eurodac Regulation, the possibility to extend the scope of Eurodac with the view to use the data for law enforcement purpose and as a means to contribute to the fight against irregular migration will be explored.[50]

In 2010, EURODAC processed:

- 215,463 fingerprints of asylum seekers (Category 1), an 9% decrease compared to the previous year (236,936),
- 11,156 fingerprints of people crossing the borders irregularly (Category 2), a 64% decrease compared to the previous year (31,071), and
- 72,840 fingerprints of people apprehended while illegally residing on the territory of a Member State (Category 3). This figure has decreased by 14,86 % from the previous year

[49] Council Regulation (EC) No 343/2003 of 18 February 2003

[50] COM (2007) 299 final.

(85,554), demonstrating a growing interest from Member States to make use of this search possibility.

The increase in transactions may be due to the fact that most Member States have installed fingerprint scanning devices at their external borders.

EURODAC data also provide information on multiple asylum applications. In 2010, 24,16 % of aliens applying for asylum had already lodged one or more applications in the same Member State or in another Member State. Out of a total of 215,463 asylum applications, 52,064 were 'multiple applications". See Table 1 for a comparison with previous years.

Table 1 EURODAC information on multiple applications.

Year	Number of asylum applications recorded by EURODAC (Category 1)	At least one asylum application lodged previously (in the same or in another Member State)
2007	197,284	31,910 (16,17%)
2008	219,557	38,445 (17,5%)
2009	236,936	55,226 (23.3%)
2010	215,463	52,064 (24,16%)

Sources: EURODAC annual reports[51].

Prüm Decisions

The Prüm Convention was signed between Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria in May 2005 on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and irregular migration. In June 2007, important provisions of the Prüm Treaty dealing with police co-operation and information exchange on DNA-profiles, fingerprint reference data and vehicle registration data were incorporated into the legislative framework of the EU by the Prüm Council Decisions and were scheduled to be fully implemented in all Member States by August 2011. More than half of the Member States, however, were significantly lagging behind this deadline in 2011. Considerable implementation progress is now expected in the course of 2012.

The Prüm Decisions do not establish a central database containing personal data, but allow law enforcement authorities direct access to databases in other Member States in the case of vehicle registration data and access on a 'hit'/'no hit' basis in the case of DNA and dactyloscopic data. Neither do they authorise the sharing of data on individuals who have been found irregularly staying in a Member State or who have remained beyond their authorised length of stay in the Schengen area.

Advanced Passenger Information and Passenger Name Record

Information collected on travellers via Advanced Passenger Information (API) and Passenger Name Record (PNR) applies to air travel only. It is therefore not directly relevant for the entry/exit system or the Registered Traveller Programme (RTP). In addition, due to the fact

[51] SEC(2009) 96, 26.1.2009, SEC(2009) 1246/6, 25.9.2009, SEC(2010) 954/10, 2.9.2010. .

that these data are normally collected from airlines, travel agencies or entered by the traveller himself, the quality of the data is often not sufficient to use this information for border check purposes.

According to Article 26 of the Schengen Convention, carriers are responsible for the checking of documents of the passengers they transport into the Member States and may be penalised when third country nationals are found at the borders without the necessary travel documents. Following the decision of the Executive Committee of Schengen in 1994 which considered the advanced transmission of passenger data as a valuable tool for enhancing border security, Member States gradually implemented API practices reflecting diversified national approaches. In order to harmonise these practices and introduce common standards on the information to be transmitted as well as on the data protection safeguarding clauses, Spain presented in 2003 an Initiative that led to the adoption of the Council Directive 2004/82/EC of 29 April 2004on the obligation of carriers to transmit passenger information (API Directive). The explicit purposes of this Directive are to improve border control and combat illegal immigration by the transmission of advance passenger data by air carriers to the competent national authorities.

Whilst the initial proposal aimed for the inclusion of all carriers, the version finally adopted limits its scope to air carriers given their key role in controlling immigration flows from distant places of origin and since they alone had the necessary registration system. In any case the Directive does not prevent Member States from imposing obligations on other carriers.
On the other hand the Directive does not introduce a general obligation for air carriers to transmit passenger information since data is only transmitted at the request of border authorities, depending on MS appreciation of the risks involved.

Moreover the information concerns only passengers who are carried from third countries into EU territory. The information shall be transmitted electronically (or in case of failure by any appropriate means), in advance of departure, to the authorities of the first authorised border crossing point.

Information shall comprise

- The number and type of travel document used;
- Nationality;
- Full names;
- The date of birth;
- The border crossing point of entry into the territory of the Member States;
- Mode of transport;
- Departure and arrival time of the transportation;
- Total number of passengers carried on that transport;
- The initial point of embarkation.

Article 4 of the Directive foresees an obligation on MS to impose dissuasive penalties on carriers, which, as a result of fault, have not transmitted the data required or have transmitted incomplete or false data (maximum amount not less than 5 000 €, minimum amount not less than 3 000 €)

The transmission, use and storage of such data are subject to strict compliance with Directive 95/46/EC on data protection by the authorities of the Member States and carriers. Data must be deleted by carriers within 24 hours after the arrival and also by the border authorities unless data is needed as evidence in proceedings aiming at the enforcement of legislation on entry and immigration.

The deadline to transpose the Directive was 5 September 2006. All Member States have adopted national measures to comply with the Directive since then.

However, according to the information available in most Member States no systematic use of the advanced passenger information is made yet.

PNR

PNR data is unverified information provided by passengers, and collected by and held in air carriers' reservation and departure control systems for their own commercial purposes. It contains several different types of information, such as travel dates, travel itinerary or ticket information. In February 2011, the Commission presented a proposal for a Directive on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)32 final).

ANNEX 5 - DATA RETENTION PERIODS IN EU IT SYSTEMS

Instrument	Purpose(s)	Personal data coverage	Data retention
Visa Information System (VIS)	To help implement a common visa policy and prevent threats to internal security.	Visa applications, fingerprints, photographs, related visa decisions and links between related applications.	5 years.
Schengen Information System (SIS)	To maintain public security, including national security, within the Schengen area and facilitate the movement of persons using information communicated via this system.	Names and aliases, physical characteristics, place and date of birth, nationality and whether a person is armed or violent. SIS alerts relate to several different groups of persons.	Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purpose for which they were supplied, and no longer than three years. Data on persons subject to exceptional monitoring on account of the threat they pose to public or national security must be deleted after one year.
Schengen Information System II (SIS II)	To ensure a high level of security in the area of freedom, security and justice and facilitate the movement of persons using information communicated via this system.	The data categories in SIS plus fingerprints and photographs, copies of European Arrest Warrant, misused identity alerts and links between alerts. SIS II alerts relate to several different groups of persons.	Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purpose for which they were supplied, and no longer than three years. Data on persons subject to exceptional monitoring on account of the threat they pose to public or national security must be deleted after one year.
EURODAC	To assist in determining which Member State should assess an asylum application.	Fingerprint data, sex, the place and date of the application for asylum, the reference number used by the Member State of origin and the date on which the fingerprints were taken, transmitted and entered in the system.	10 years for asylum-seekers' fingerprints; 2 years for those of third country nationals apprehended in connection with the irregular crossing of an external border.

ANNEX 6

EXISTING SYSTEMS LINKED TO THE EES AND MANAGEMENT OF EU IT SYSTEMS

When a third-country national enters the Schengen area it is obligatory for border authorities to consult the data and alerts on persons and, where necessary, objects included in the SIS. When a third-country national exits the Schengen area, the SIS may be consulted. This means that due to the current use of the SIS, the border crossing points are connected to the data network and equipped with travel document readers. The SIS check is carried out automatically when the machine readable zone of the travel document is read.

A second EU system, the VIS, forms an important part of the border check process. In order to facilitate border checks and fight against visa fraud, visas are checked at the external borders against the VIS by using the visa sticker number. Verification of fingerprints at the external border crossing points will also become mandatory after a three year transitional period from the start of operations ie in 2016.

The same document readers that are used for the SIS checks and the same fingerprint readers that are used for the VIS checks may also be used for the EES.

With the EES in mind, the above means that consulates and border crossing points should have already been connected to the data network (VIS and SIS) and fingerprint readers on entry will have been procured by 2013/2014 at the latest to fulfil the requirements for the obligatory use of the VIS.

Management

As regards large scale IT systems, only EURODAC and the VIS are operational and managed by DG HOME of the Commission with the support of DG DIGIT in the case of EURODAC[52]. The EURODAC system is located in Luxembourg and Brussels. SIS II is and VIS was developed by the Commission and, based on the legal instruments establishing and governing SIS II and VIS, the systems shall be located in Strasbourg (central unit) and near Salzburg (back-up unit). The VIS already started operations and the development of the SISII is ongoing.

Following an impact assessment carried out to study the different options for performing the task of "Management Authority" for SIS II, VIS and EURODAC in the long term, a new Regulatory Agency (the Agency for the operational management of large-scale information systems) was found to be the best solution as compared with entrusting Member States with operational tasks for part or all of the systems, FRONTEX with the three systems or EUROPOL with SIS II and the Commission with VIS and EURODAC.

The Agency Regulation was published in the Official Journal[53] and entered into force on 21 November 2011. The Agency will become fully operational on 1 December 2012.

---

[52] In the management context, the SIS 1+ is not discussed as migration form SIS 1+ to SIS II is ongoing.

[53] OJ L 286, 1.11.2011.

The Agency is funded from the general budget of the European Union. The budget of the Agency mainly covers investments in the site, security and operational management of the SIS II, the VIS and EURODAC and administrative expenses.

According to the Regulation of the European Parliament and the Council establishing an Agency for the operational management of large-scale systems in the area of freedom, security and justice, the Agency will be in charge of the operational management of the SIS II, the VIS, EURODAC and of developing and managing other large-scale information technology systems in the area of freedom, security and justice if so provided by relevant legislative instruments.

An EES would be developed and managed by the Agency. Member States would be responsible for the development and management of their national components and their adaptation to the central system. Existing equipment installed at the borders and at the consulates could be exploited. A legal basis for the EES needs to be adopted prior to any technical development and the agency's legal basis amended.

ANNEX 7

FINAL RESULTS OF THE DATA COLLECTION HELD FROM 31 AUGUST TO 6 SEPTEMBER 2009

The tables in this annex details the results of the data collection exercise carried out under the coordination of the Czech and Swedish Presidencies, where all entries and exits at the external border of the Schengen area were recorded by the Member States during one week for the purpose of estimating the total size of travel flows at the external border, in total and divided by type of border (air/sea/land) and by traveller (EU citizens, and visa exempt/required third-country nationals).

	AIR						Total
	Entry			Exit			
	EU	Non VISA	VISA	EU	Non VISA	VISA	Air
Austria	81.096	17.781	11.671	64.799	16.134	9.109	200.590
Belgium	78.372	14.295	15.432	68.132	10.028	8.955	195.214
Czech Republic	43.531	9.100	11.365	42.386	7.442	9.121	122.945
Denmark	40.764	9.924	4.894	52.139	8.454	3.354	119.529
Estonia	2.745	78	126	2.532	87	141	5.709
Finland	17.662	5.128	4.042	19.497	4.703	2.901	53.933
France	405.109	91.773	64.266	340.832	77.555	43.853	1.023.388
Germany	343.836	106.716	106.242	296.300	91.998	69.345	1.014.437
Greece	216.316	33.475	19.745	213.467	34.135	19.473	536.611
Hungary	20.347	4.002	3.294	18.706	3.313	2.588	52.250
Iceland	4.348	2.658	92	5.223	3.318	148	15.787
Italy	94.293	23.353	17.517	58.347	19.087	11.917	224.514
Latvia	12.946	1.850	911	12.096	1.660	1.118	30.581
Lithuania	3.899	44	300	4.352	250	267	9.112
Luxembourg	4.000	111	51	4.220	183	62	8.627
Malta	15.255	864	793	16.729	865	978	35.484
Netherlands	265.066	45.454	30.906	413.315	46.139	29.766	830.646
Norway	20.838	2.298	1.628	24.042	2.167	1.452	52.425
Poland	97.900	4.493	2.460	102.379	5.496	1.931	214.659
Portugal	50.208	11.436	5.558	44.584	11.269	3.840	126.895
Slovakia	14.316	405	108	11.946	262	54	27.091
Slovenia	7.522	1.219	2.597	6.253	955	1.908	20.454
Spain	661.325	29.184	36.080	661.387	24.609	31.290	1.443.875
Sweden	43.177	4.165	4.436	45.416	4.560	3.542	105.296
Switzerland	75.048	35.143	18.639	75.249	29.075	15.340	248.494
Total	2.538.823	437.168	351.482	2.539.529	387.610	263.344	**6.517.956**
Total entry AIR	**3.327.473**						
Total exit AIR	**3.190.483**						

	SEA						Total
	Entry			Exit			
	EU	Non VISA	VISA	EU	Non VISA	VISA	Sea
Austria	0	0	0	0	0	0	0
Belgium	5.036	94	321	6.128	96	363	12.038
Czech Republic	0	0	0	0	0	0	0
Denmark	937	12	11	1.881	20	26	2.887
Estonia	266	287	137	262	300	230	1.482
Finland	582	15	45	461	19	23	1.145
France	174.848	18.948	2.148	236.231	9.771	2.581	444.527
Germany	15.615	1.019	9.542	12.813	658	7.376	47.023
Greece	48.343	12.249	3.228	49.695	12.439	3.833	129.787
Hungary	0	0	0	0	0	0	0
Iceland	0	0	0	0	0	0	0
Italy	23.574	5.012	3.826	10.417	1.077	1.714	45.620
Latvia	449	464	322	424	544	307	2.510
Lithuania	218	496	0	495	504	0	1.713
Luxembourg	0	0	0	0	0	0	0
Malta	315	43	138	42	20	111	669
Netherlands	25.176	5.334	1.060	27.358	7.196	1.084	67.208
Norway	0	0	0	0	0	0	0
Poland	722	751	121	865	839	137	3.435
Portugal	5.756	623	1.567	4.418	504	1.477	14.345
Slovakia	0	0	0	0	0	0	0
Slovenia	564	439	70	1.083	902	95	3.153
Spain	135.830	63.919	7.459	67.934	24.199	10.226	309.567
Sweden	2.121	653	729	2.198	2.422	717	8.840
Switzerland	0	0	0	0	0	0	0
Total	440.352	110.358	30.724	422.705	61.510	30.300	**1.095.949**
Total entry SEA	**581.434**						
Total exit SEA	**514.515**						

	LAND						Total
	Entry			Exit			
	EU	Non VISA	VISA	EU	Non VISA	VISA	Land
Austria	0	0	0	0	0	0	0
Belgium	0	0	0	21.686	2.301	848	24.835
Czech Republic	0	0	0	0	0	0	0
Denmark	0	0	0	0	0	0	0
Estonia	39.640	755	4.515	38.051	841	5.030	88.832
Finland	21.050	528	46.441	21.733	514	45.606	135.872
France	150.853	15.678	3.170	186.855	13.087	3.855	373.498
Germany	0	0	0	0	0		0
Greece	126.563	25.854	42.206	129.486	16.612	34.702	375.423
Hungary	331.415	27.229	75.445	247.051	22.208	41.033	744.381
Iceland	0	0	0	0	0	0	0
Italy	0	0	0	0	0	0	0
Latvia	21.543	124	4.862	20.397	112	5.609	52.647
Lithuania	26.992	1.502	33.921	24.642	1.413	32.472	120.942
Luxembourg	0	0	0	0	0	0	0
Malta	0	0	0	0	0	0	0
Netherlands	0	0	0	0	0	0	0
Norway	255	154	637	257	199	672	2.174
Poland	87.310	1.266	118.474	83.852	1.264	112.190	404.356
Portugal	0	0	0	0	0	0	0
Slovakia	18.075	440	3.777	15.895	477	2.471	41.135
Slovenia	393.473	187.379	78.480	324.828	161.713	51.867	1.197.740
Spain	400.584	324.724	5.629	415.409	324.654	5.048	1.476.048
Sweden	0	0	0	0	0	0	0
Switzerland	0	0	0	0	0	0	0
Total	1.617.753	585.633	417.557	1.530.142	545.395	341.403	**5.037.883**
Total entry LAND	**2.620.943**						
Total exit LAND	**2.416.940**						

	Passenger category					
	EU		Non VISA		VISA	
	Entry EU	Exit EU	Entry Non VISA	Exit non VISA	Entry VISA	Exit VISA
Austria	81.096	64.799	17.781	16.134	11.671	9.109
Belgium	83.408	95.946	14.389	12.425	15.753	10.166
Czech Republic	43.531	42.386	9.100	7.442	11.365	9.121
Denmark	41.701	54.020	9.936	8.474	4.905	3.380
Estonia	42.651	40.845	1.120	1.228	4.778	5.401
Finland	39.294	41.691	5.671	5.236	50.528	48.530
France	730.810	763.918	126.399	100.413	69.584	50.289
Germany	359.451	309.113	107.735	92.656	115.784	76.721
Greece	391.222	392.648	71.578	63.186	65.179	58.008
Hungary	351.762	265.757	31.231	25.521	78.739	43.621
Iceland	4.348	5.223	2.658	3.318	92	148
Italy	117.867	68.764	28.365	20.164	21.343	13.631
Latvia	34.938	32.917	2.438	2.316	6.095	7.034
Lithuania	31.109	29.489	2.042	2.167	34.221	32.739
Luxembourg	4.000	4.220	111	183	51	62
Malta	15.570	16.771	907	885	931	1.089
Netherlands	290.242	440.673	50.788	53.335	31.966	30.850
Norway	21.093	24.299	2.452	2.366	2.265	2.124
Poland	185.932	187.096	6.510	7.599	121.055	114.258
Portugal	55.964	49.002	12.059	11.773	7.125	5.317
Slovakia	32.391	27.841	845	739	3.885	2.525
Slovenia	401.559	332.164	189.037	163.570	81.147	53.870
Spain	1.197.739	1.144.730	417.827	373.462	49.168	46.564
Sweden	45.298	47.614	4.818	6.982	5.165	4.259
Switzerland	75.048	75.249	35.143	29.075	18.639	15.340
Total	4.596.928	4.492.376	1.133.159	994.515	799.763	635.047

	Total			Total		
	Passenger category					
	EU	Non VISA	VISA	Entry	Exit	Total
Austria	145.895	33.915	20.780	110.548	90.042	200.590
Belgium	179.354	26.814	25.919	113.550	118.537	232.087
Czech Republic	85.917	16.542	20.486	63.996	58.949	122.945
Denmark	95.721	18.410	8.285	56.542	65.874	122.416
Estonia	83.496	2.348	10.179	48.549	47.474	96.023
Finland	80.985	10.907	99.058	95.493	95.457	190.950
France	1.494.728	226.812	119.873	926.793	914.620	1.841.413
Germany	668.564	200.391	192.505	582.970	478.490	1.061.460
Greece	783.870	134.764	123.187	527.979	513.842	1.041.821
Hungary	617.519	56.752	122.360	461.732	334.899	796.631
Iceland	9.571	5.976	240	7.098	8.689	15.787
Italy	186.631	48.529	34.974	167.575	102.559	270.134
Latvia	67.855	4.754	13.129	43.471	42.267	85.738
Lithuania	60.598	4.209	66.960	67.372	64.395	131.767
Luxembourg	8.220	294	113	4.162	4.465	8.627
Malta	32.341	1.792	2.020	17.408	18.745	36.153
Netherlands	730.915	104.123	62.816	372.996	524.858	897.854
Norway	45.392	4.818	4.389	25.810	28.789	54.599
Poland	373.028	14.109	235.313	313.497	308.953	622.450
Portugal	104.966	23.832	12.442	75.148	66.092	141.240
Slovakia	60.232	1.584	6.410	37.121	31.105	68.226
Slovenia	733.723	352.607	135.017	671.743	549.604	1.221.347
Spain	2.342.469	791.289	95.732	1.664.734	1.564.756	3.229.490
Sweden	92.912	11.800	9.424	55.281	58.855	114.136
Switzerland	150.297	64.218	33.979	128.830	119.664	248.494
Total	**9.089.304**	**2.127.674**	**1.434.810**	**6.529.850**	**6.121.938**	
						12.651.788

	AIR						Total
	Entry			Exit			
	EU	Non VISA	VISA	EU	Non VISA	VISA	Air
Bulgaria	79.034	5.448	11.407	96.899	5.943	16.206	214.937
Romania	78.238	6.037	1.146	79.597	5.790	1.071	171.879
Cyprus	109.944	1.532	18.863	108.887	1.313	9.402	249.941

	SEA						Total
	Entry			Exit			
	EU	Non VISA	VISA	EU	Non VISA	VISA	Sea
Bulgaria	1.351	106	2.284	1.329	2	2.532	7.604
Romania	570	782	8	632	661	2	2.655
Cyprus	2.558	39	315	2.484	51	281	5.728

	LAND						Total
	Entry			Exit			
	EU	Non VISA	VISA	EU	Non VISA	VISA	Land
Bulgaria	213.298	2.454	43.172	206.926	2.461	32.473	500.784
Romania	293.755	6.675	30.410	340.900	2.752	39.830	714.322
Cyprus	0	0	0	0	0	0	0

	Passenger category						Total		
	EU		Non VISA		VISA		Passenger category		
	Entry EU	Exit EU	Entry Non VISA	Exit non VISA	Entry VISA	Exit VISA	EU	Non VISA	VISA
Bulgaria	293.683	305.154	8.008	8.406	56.863	51.211	598.837	16.414	108.074
Romania	372.563	421.129	13.494	9.203	31.564	40.903	793.692	22.697	72.467
Cyprus	112.502	111.371	1.571	1.364	19.178	9.683	223.873	2.935	28.861

	Total		
	Entry	Exit	Total
Bulgaria	358.554	364.771	723.325
Romania	417.621	471.235	888.856
Cyprus	133.251	122.418	255.669