EUROPEAN
COMMISSION

Brussels, 28.2.2013
SWD(2013) 50 final

COMMISSION STAFF WORKING PAPER

IMPACT ASSESSMENT

Accompanying document to the

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

ESTABLISHING A REGISTERED TRAVELLER PROGRAMME

{COM(2013) 97}
{SWD(2013) 51}
{SWD(2013) 52}

COMMISSION STAFF WORKING PAPER

IMPACT ASSESSMENT

Accompanying document to the

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

ESTABLISHING A REGISTERED TRAVELLER PROGRAMME

TABLE OF CONTENTS

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Background

The present impact assessment report and the legislative proposal it accompanies[1] are to be seen in the context of the progressive establishment of a European model of integrated border 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 second challenge: a separate report[3] and legislative proposal address the first one. The two reports and proposals are not dependant on each other as regards their implementation but a solution needs to be found to calculate the time spent in the Schengen area if fully automated border crossings would be provided for third-country nationals. An Entry/Exit System (EES) which is reflected in the second report and proposal would be a solution for that.

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 a Registered Traveller Programme (RTP[5]) for frequent and pre-vetted third-country national travellers. Such a programme essentially entails that certain groups of third-country nationals would benefit from facilitated border checks when entering the Schengen area, checks which are at least partly automated through the use of Automated Border Control (ABC) technology. The Communication was accompanied by an impact assessment report[6].

The RTP was endorsed in the "Stockholm Programme"[7] agreed by the European Council in December 2009, which highlighted that the Union must continue to facilitate legal access to the territory of the Member States. The RTP was included in the overview among the initiatives announced in the Action Plan Implementing the Stockholm Programme[8].

---

1 COM(2013) 97 final (RTP).

2 COM(2011) 777 final, 15.11.2011. The work programme is published on the following website: http://ec.europa.eu/atwork/programmes/index_en.htm

3 COM(2013) 95 final (EES).

4 SEC(2008) 154, 13.2.2008.

5 A list of acronyms is provided in Annex 1.

6 SEC(2008) 153; http://eur-lex.europa.eu/SECMonth.do?year=2008&month=01, as well as the "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')" carried out by GHK and the "Entry/Exit Technical Feasibility study" carried out by Unisys. These studies are published on the following website: http://ec.europa.eu/home-affairs/doc_centre/borders/borders_schengen_en.htm#studies

7 OJ C 115/1, 4.5.2010. The Stockholm Programme is published on the following website: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_en.htm

8 COM(2010) 171 final, 20.4.2010. The action plan is published on the following website: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0036_en.htm

A Commission Communication in July 2010 on information management in the area of freedom, security and justice[9] 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. It set out the conditions the Commission will apply in future when assessing any new system in this area including the approach of "privacy by design"[10]. 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[11] could have in providing technical advice.

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 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 RTP would speed up the border crossings of 4-5 million travellers per year and lay the basis for enhanced investments in automated border control technologies at major border crossing points.

Against this background, the present impact assessment examines different implementation options in order to find the *best possible way to implement the RTP*. However, the impacts of the whole RTP 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 RTP.[13]

1.2. Consultation of interested parties

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

---

9 COM(2010) 385 final, 20.7.2010. The Communication is published on the following website: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF

10 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".

11 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.

12 COM(2011) 680 final, 25.10.2011. The Communication is published on the following website: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0680:FIN:EN:PDF

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 and positions received from different stakeholders on the 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.

The consultation was carried out in several ways:

- publishing the 2008 impact assessment and communication;
- presenting a comprehensive technical assessment of the system 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 them with the discussion papers;
- meeting stakeholders bilaterally;
- publishing the 2011 Communication;
- giving presentations on the RTP and automation of border control at different fora.

Stakeholders views

Member States

The RTP has been under discussion at meetings with Member States' experts since 2008. A majority of Member States support the establishment of the RTP. During the consultations on the Commission's communication adopted in 2011, five Member States had doubts about the benefits of the RTP. Based on them the administrative burden should not be higher compared to the normal border check process. Furthermore, the high costs, solid cost-benefit analysis and the low number of travellers crossing their part of the external border were mentioned.

Member States are in favour of collecting a fee from the applicants for participation in the RTP. A large majority of Member States prefer to store information on Registered Travellers in a centralised database and consider that the implementation of ABC should be voluntary for them. However, there are concerns especially regarding the costs, vetting criteria/vetting procedure and lodging and examining of applications. Slightly divergent views exist on whether a fully automated or semi-automated system should be used, where applicable. Many third countries are also taking forward similar initiatives in this field, as shown through several meetings at the level of ministers and with senior officials from countries such as the USA and Canada.

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 RTP but most of them did not indicate their practical or technical implementation preferences.

The summary of the conference prepared by the Presidency[15] concluded that the RTP would bring significant benefits for the border check procedure, providing a possible means for a more effective deployment of border management resources from 'low-risk' to 'high-risk' passengers. This could help enhance security and reduce illegal migration, while providing travellers and business with cost-effective border passage services. However, some technical and political questions need to be discussed such as the storage of the data and the possible use of a token, the abolition of the obligation to stamp the passports and the full respect of privacy of the traveller including data protection. The Presidency conclusions were presented at the JHA Council on 8 March 2012.

During the consultations Member States commented on the specific options of the RTP (for example data storage) only at a very general level asking the Commission to come forward with the legislative proposals.

European Parliament

In its resolution on the February 2008 Communication, the European Parliament (EP) supported in principle the concept of the RTP and advocated a harmonised approach. The Parliament expressed doubts about establishing a new centralised database and was also concerned about the costs of the proposed system(s), stressing that all investments should be economically justified on the basis of benefits, and should produce mission value.[16]

The EP did not submit its opinion on the 2011 communication.

At the conference on Innovation Border Management 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 actually under development should be in place and evaluated before the work on the RTP can be started.

European Data Protection Supervisor

On 7 July 2011 the European Data Protection Supervisor (EDPS), in his opinion[17] on the communication of the Commission on Migration[18], stressed the need to assess the use of existing systems before proposing any new ones. The EDPS was not fully convinced that the RTP is really necessary.

---

14 Member States replies are published on the following website: http://eu2012.dk/en/Meetings/Conferences/Feb/Konference-om-innovativ-graenseforvaltning. See also Council document 7166/12, presidency summary of findings.

15 Council document 7166/12, Presidency summary of findings.

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.

17 C(2011)-0445. The EDPS opinion is published on the following website: http://www.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC/OC2011

18 COM(2011) 248 final, 4.5.2011. The Communication is published on the following website: http://ec.europa.eu/home-affairs/news/intro/docs/1_EN_ACT_part1_v11.pdf

The EDPS was also consulted informally on the 2011 Communication on smart borders before its adoption. In his informal comments, the EDPS highlighted that the RTP proposal has to be supported by clear proof of its necessity and effective evaluation of current measures. He stressed: a) the principle of "privacy by design" e.g. designing the system in a way that limits its data protection impact, b) that only a one to one verification of biometrics should be possible, c) that no record on border crossings should be stored in the RTP, d) that data protection rights have to be ensured and e) that measures are taken to prevent "positive discrimination" from turning into "negative discrimination" of persons who are for example infrequent or first-time travellers. Furthermore, he asked to clarify which sources of data will be used for vetting.[19]

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 inter alia that the transparency and legal certainty should be ensured, retention period should be limited in certain cases and Member States should not be allowed to store the data in national files.

Article 29 Data Protection Working Party

The Working Party addressed a letter to Commissioner Malmström on 12 June 2012 reacting to the 2011 Communication. It stressed that convincing evidence should be provided that the RTP would significantly facilitate access to the EU for registered travellers without placing an extra control burden on non-registered travellers. The Working Party also asked to consider all possible options for limiting the storage of personal data to the smallest amount possible. Furthermore, the Working Party highlighted that the vetting criteria should be clear and transparent, and that the final decision to grant/refuse access to the RTP would have to be made by a human being.

Civil society and the private sector

Civil society (academia, think tanks and NGOs), the private sector and FRONTEX[20] participated actively in the debate and organised several relevant conferences. Civil society provided input in various conferences and academic papers published on the subject. Civil society and the private sector support the establishment of the RTP[21]. The industry dealing with biometrics and manufacturing border control equipment asked for a harmonised approach to the RTP and minimum technical standards for equipment.

---

19 C2011-0860, 4.10.2011.

20 Frontex is a European Agency for the management of operational cooperation at the external borders of the Member States of the European Union. More information on Frontex can be found: http://www.frontex.europa.eu/

21 See for example ACI EUROPE Position on the use of automated means for border control in the airports, June 2009. http://kpi.aci-europe.org/upload/ACI%20EUROPE%20-%20position%20paper%20on%20USE%20OF%20AUTOMATED%20MEANS%20FOR%20BORDER%20CONTROL%20AT%20EUROPEAN%20%20AIRPORTS%20[06%202009].pdf, Roma/Lyon Migration Experts Sub-Working Group: G8 Best Practices of Biometric Usage in Travel Continuum and the position statement of the American Chamber of Commerce to the European Union on the Smart Borders, 23 of March 2012.

At the conference in Copenhagen a representative of IATA expressed support for an RTP. However, he stressed that the RTP should not 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 these consultations have been integrated in the choice of options and in the assessment of impacts. By organising series of meetings and presenting one impact assesment and 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. Minimum standards for consultation were met.

1.3. Data gathering

Data-gathering and consultations with relevant authorities in the Member States and other stakeholders were undertaken by the Commission. The 2008 impact assesment showed the lack of data especially as regards exact travel flows and the time needed to cross the external border.

Therefore, 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/sea/land) and groups of travellers (EU citizens and visa exempt/required third-country nationals);

- Time currently needed for border checks.

Data used was collected through questionnaires[22] 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. 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.

With the help of FRONTEX the existing national ABCs based on Electronic Machine Readable Travel Documents in the EU as well as in third countries were analysed[23].

---

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

23 See draft reports "ABC solutions based on Electronic Machine Readable Travel Documents (eMRTD) in EU Member States" and "ABC solutions based on Electronic Machine Readable Travel Documents (eMRTD) in third countries" prepared by Frontex in September 2011.

1.4 Inter-service steering group

An inter-service steering group (ISG) 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, on 2 December 2010, on 16 February 2011 and on 31 January 2012. The last ISG meeting was also attended by the 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 opinion on 14 March 2012. The recommendations for improvement were accommodated in the final version of the report. In particular, the following changes were made: baseline scenario was sharpened and clarified; problem definition was widened including lessons learnt from the development of other large scale IT-systems and lessons learnt from Automated Border Control systems and national RTPs implemented in Member States and non-EU states; links to the Annexes and to the 2008 impact assessment were improved; stakeholders views were reported as widely as possible taking into account that views expressed by the stakeholders were quite general; the explanation of method used for calculating the costs was expanded and the expected costs and benefits for different stakeholders were more rigorously reported; re-affectation of border guards taking into account the expected increase in travel flows was clarified; and finally a clear overview on the European Data Protection Supervisor's views was added.

2. PROBLEM DEFINITION

2.1. Why the creation of an RTP is being examined?

The 2008 impact assessment identified and examined the main problems for a better management of migration flows. That impact assessment concluded that an RTP for third-country nationals should be established in the future, but did not discuss comprehensively all the relevant and important issues for the implementation of the EU wide RTP such as implementation options, costs and fundamental right aspects. As explained in the 2011 communication:

> *A RTP would significantly facilitate border crossings for frequent, pre-vetted and pre-screened third-country travellers at the Schengen external border. It would reduce the time spent at the border crossing points and facilitate travel and cross-border contacts. As far as possible, it would make use of new technologies such as Automated Border Control systems (used also for EU travellers) moving towards EU smart borders.*

It is now time to assess the exact design of the system based on the specific implementation options identified during the consultations. Before discussing how best to design such a system, it is useful to recall the main aspects of the problems it will address because the nature and scope of these problems have direct implications for design choices. In the continued absence of an EU RTP for third-country nationals the basic problem remains the same as in 2008. Therefore the current problem definition is built on the previous impact

assessment. However, the data gaps identified in 2008 were solved by organising data collection exercises at the external border and collecting information from Member States via questionnaires. The baseline scenario (status quo in 2008 impact assessment) is almost the same in the 2008 and 2011 impact assessments. The main differences between the two are that the VIS started operations and more ABC systems are implemented for EU citizens at the external border crossing points.

The following issues are not included in the selection and definition of implementation problems to be assessed, taking into account policy choices already made, input during the stakeholder consultation, and in view of the need to focus on the main implementation problems.

The scope of the RTP (only visa-exempt or all third-country nationals) and the use of different types of biometrics are not discussed in this impact assessment as they were discussed in the previous impact assessment and in the February 2008 Communication. First, current border checks do not distinguish between persons holding a visa and those that do not. A programme that aims at facilitating border checks for third-country nationals should therefore also not distinguish between these groups. Secondly, the same biometric identifier – fingerprints - should be used in the RTP as already decided at EU level with regard to the VIS, e-passports and residence permits.

Based on the evaluation carried out by Frontex, there has not been any major changes in technology or functioning of ABC systems since the 2008 impact assessment was carried out[24]. The forms of national RTPs have also followed the same approach as in 2008. They are developed for EU citizens and require enrolment of biometric data. The continued use and possible small increase of national RTP is not relevant in the selection and definition of implementation problems to be assessed, as the basic scope is different: a national RTP is for EU citizens, while a EU RTP will be for third-country nationals.

2.1.1. Legislative and technical aspects

EU law requires that systematic checks are carried out at the Schengen external borders on all travellers (both on entry and exit). The Schengen area without internal border controls currently includes all Member States except Romania, Bulgaria, Cyprus, UK and Ireland and four other European countries (Norway, Iceland, Switzerland and Liechtenstein). Schengen states are committed to maintaining common EU borders and common standards for border controls.

Thorough checks are normally carried out on third-country nationals, and minimum checks on EU citizens and persons enjoying the right of free movement[25]. As illustrated in Annex 2, current rules for third-country nationals could be described as "one-size-fits-all" as the same checks apply regardless of any differences in risk between different travellers or their frequency of travel. This is because current legislation does not allow for exceptions to the principle of thorough border checks except for those categories of third-country nationals that

---

[24] See draft reports "ABC solutions based on Electronic Machine Readable Travel Documents (eMRTD) in EU Member States" and "ABC solutions based on Electronic Machine Readable Travel Documents (eMRTD) in third countries" prepared by Frontex in September 2011.

[25] OJ L 105, 13.4.2006, OJ L 158, 30.4.2004.

are specifically mentioned in the Schengen Border Code[26] or in the Local Border Traffic Regulation[27] such as Heads of States and border residents.

Only a very small minority of persons crossing the external border are able to benefit from the above-mentioned exceptions: approximately two million equivalent to 0,2 % of total passenger flows. This number can be expected to remain largely constant, with a marginal increase due to an increased take up of local border traffic regimes. By the end of 2010, 110 000 local border traffic permits were issued by Member States.

While the Visa Code allows frequent travellers to be issued with a multiple-entry visa, thereby avoiding the situation where those travellers would need to apply for a visa for each journey into the Schengen area during a five year period, multiple-entry visa holders do not benefit from any facilitation at the actual border crossing.

Border checks on EU citizens can be automated, based on the current legislation, if they hold an e-passport (also called biometric passport) which stores biometric data of its holder (facial image and, as of 2009, fingerprints). Several Member States have already implemented such ABC systems at their airports. Only Portugal has implemented ABC systems at all international airports and the UK several airports as can be seen from Annex 3. Other Member States have implemented them only at their biggest airports. The ABC process is described in Annex 2, chapter 2 but in principle it is the same as in the manual border check booth but, in this case, is carried out by a machine.

Although ABC systems are widely used by Member States and non-EU Member States alike as illustrated in Annexes 3 and 4[28], they still follow the same principles as they did in 2008. The main lessons learnt and the main rationale behind the ABC systems are to improve the accuracy and efficiency of border checks by enabling the accurate verification of travel documents and identification of travellers with biometric data. Automated border controls have a positive effect on deterring forged or stolen passports and improving identity verification. Furthermore, they increase throughput capacity at border crossing points and border efficiency by allowing border guards to focus on higher risk travellers or serve other travellers not using ABC. A majority of ABC systems rely on an e-passport.

Some Member States have implemented a form of national RTP for EU citizens[29]. The main feature of national RTPs is that they do not rely on the e-passport. Therefore the traveller needs to be pre-enrolled before being granted access to the RTP i.e. biometric data must be captured and stored in a database or in a token.

Many non-EU countries such as the US, Canada, Australia and Singapore have also automated their border check procedures based on the same type of technology. The access granted for these programmes are limited. They are established only for their own citizens or their own citizens and neighbouring country citizens. However, as the figures in Annex 4 demonstrate some of the programmes have numerous participants; Singapore eIACS system

---

26 OJ L 105, 13.4.2006.

27 OJ L 405, 30.12.2006.

28 Based on the International Air Transport Association the ABC systems are used at 83 airports in 31 states.

29 For example, the Netherlands (Privium), France (PARAFES), the United Kingdom (Iris) and Germany (ABG) have this kind of programme.

has three million users and the US systems have one million users. The average processing time at the gate is 12 seconds for all the systems described in Annex 4.

The rationale behind the national RTPs and the main implementation choices made have not changed since 2008 impact assessment. The essential elements of the implemented RTPs are:

- Ensuring that registered travellers do not present a risk in terms of irregular immigration or internal security. This is generally done by:

  – Undertaking a risk assessment prior to the registration. For instance people are checked against watch lists and other police databases. Biometrics may also be collected for undertaking security searches in police databases (i.e. biometrics are collected, stored and used to run security checks in the US, Canada, the Netherlands, Germany and France).

  – Restricting the eligibility of participants. For instance, in France and the Netherlands only EU, EEA and Swiss nationals can participate; in the APEC countries the scheme is open only to business people that are frequent travellers and national of countries participating into the scheme.

  – Eligibility might be extended to non-nationals providing that certain security conditions are met. For example, participants to the APEC business Card are checked against watch lists of all participant countries and the US/NL citizens can join the FLUX programme after vetting is done by both parties and green/red light exchanged.

- Ensuring faster border checks. This is done by creating ABC systems or self-service kiosks and creating separated lanes.

- Ensuring the integrity of border checks by undertaking random checks.

- Verification of travellers' identities with biometric checks. All the schemes use biometrics.

However, under current EU law, this kind of automated process cannot be used for third-country nationals. The thorough border check requires border guards to interview a traveller and manually stamp his/her travel document and to calculate the time spent in the Schengen area, processes which cannot be automated, and, as described above, the legislation limits the exceptions that can be made to this rule.

At the moment, several systems such as the SIS, the VIS, EURODAC and API (Advanced Passenger Information) are used at the external borders. These systems, their legal basis, objectives and some statistics are described in Annex 5. Some of the existing systems such as the VIS and the SIS would have a strong managerial, technical and border check procedural link with the RTP as explained in Annex 6. As a summary, the same technical solutions and equipment already used for the VIS and the SIS at consulates and at external border crossing points could also be used for the RTP purposes.

In summary, the current legal and technical context present the following problems:

– only a very minor share of third-country nationals can benefit from any kind of facilitated or simplified border check, and Member states border guard authorities have no

possibilities to distinguish between travellers presenting a lower level of risk or an unknown level of risk,

– existing technical means, in the form of automated border control and registered traveller programmes, can only be used for EU citizens and at national level, not for third-country nationals or for the Schengen area as a whole.

2.1.2. Operational and practical aspects

Current travel flows at the EU external border and potential target group for the RTP

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. The overwhelming majority of passengers are travellers who comply with all the existing rules. At the busiest and largest border crossing points Member States have problems managing existing passenger flows and therefore they have started using ABC systems for EU citizens.

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 from 31 August to 6 September 2009[30]. Based on the data collected during this exercise, 73,5 % of travellers crossing the border are EU citizens or persons enjoying the 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).

It would, however, be wrong to assume that all third-country nationals are a potential target group for an RTP, as several factors must be taken into account. Not all third-country nationals are frequent travellers and thus not willing or eligible to join the RTP. An important element to highlight is that, based on some Member States' estimates, 10 % of travellers can make up 70-80 % of overall border crossings at certain border crossing points. In other words, the share of the total travel flows made up of frequent travellers is more interesting and relevant than the share of persons crossing the border. Fluidity of border crossings and throughput capacity of border crossing points can be greatly improved even if only a small percentage of third-country nationals were to join the RTP. Moreover, the number of third-country nationals crossing the border differs significantly among Member States and also among border crossing points. As an illustration: during the one week period of the 2009 data collection exercise, over three million travellers crossed the borders of Spain whereas the figure was 8 000 to Luxembourg. Most third-country nationals, including visa-holding third-country nationals, cross the border via land borders, the next largest number by air borders and the smallest via sea borders.

Nevertheless, it is reasonable to assume that many third-country nationals cross the borders several times a year. For example, business travellers, workers on short-term contracts, researchers, students, third-country nationals with close family connections to EU citizens and third-country nationals living in regions bordering the EU are all likely to make multiple border crossings in a given year. These third-country nationals are the main target group for

[30] Final results of the data collection exercise are in Annex 7.

the RTP. Approximately 11 million Schengen visas are issued every year[31]. On average around 20 %[32] of visa applications are for multiple-entry visas, which could entail around 2.2 million third-country nationals among visa holders crossing the external borders several times per year. Considering the needs of business and economic cooperation including constant international travel, the demand should, at least, be similar among non visa holders. Based on the above reasoning, it is estimated that maximum of 5 million new applications for the RTP would be submitted by third-country nationals every year. As statistics on third-country nationals' border crossings per nationality and/or statistics on the reasons for applying a multiple-entry visa do not exist at the EU level, more detailed evidence on the expected breakdown of potential candidates by region or professional status cannot be provided.

During the above-mentioned one week period 6,5 million travellers crossed the border via air borders. 2,6 million of them (40%) crossed the air border via the 10 busiest airports of the EU and 3,7 million (57%) via the 20 busiest airports[33].

It is important to know the existing border check time, as even small change in it per traveller could remarkable affect the overall time needed to cross the border. According to the Member States' replies to the questionnaire prepared by the Czech Presidency together with the Commission, average time for a border check for visa holders on entry at air borders is 1 minute 44 seconds, for visa-exempt third-country 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. Average border check for third-country nationals last at land borders 10-30 seconds longer than at air borders. Average border check times at land borders are reported in Annex 2. At sea borders the average times are quite similar than at land borders.

In summary, the operational and practical context presents the following problems:

– an already massive travel flow at the EU external border can be expected to further increase,

– border checking times is significantly longer for third-country nationals compared to EU citizens, and can be expected to further increase due to the implementation of the VIS.

2.1.3 Fundamental right issues

Data protection is a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union and has to be protected accordingly.

Initiatives in the area of freedom, security and justice for the purpose of border management or law enforcement which include the collection, storage and use of personal information pose significant challenges in terms of achieving the right balance between the legitimate aim of maintaining internal security or managing migration and the individuals' right to privacy and data protection. Interference with the right to privacy should be considered necessary if it answers a social need and if it is proportionate and justified with regard to the aim pursued.

---

31 http://ec.europa.eu/home-affairs/policies/borders/borders_visa_en.htm

32 The per cent varies remarkable from one year to another.

33 Excluding the UK airports as it did not participate in the data collection exercise.

With the RTP the Data Protection Directive 95/46 applies and mechanisms shall be established for the effective protection of the fundamental rights of third-country travellers who are willing or who have been accepted to the programme.

In addition, the basic instruments need to be complemented by laying down specific rules on certain aspects of the protection of personal data i.e. specify the purposes for collecting and accessing the relevant personal data, the competent authorities which have access to these data, to the extent of the access, the retention of the data, the rights of the data subjects, which personal data shall be processed in the system and the competence of the supervisory bodies for monitoring the processing of data, both as regards the Member States and Community institutions and bodies; for the supervision of the latter the European Data Protection Supervisor is the competent authority.

2.2. Problem: how to design an RTP?

2.2.1. The core features of an RTP

The common features of an RTP which would be necessary in order to develop it in the first place need to be defined without prejudice to any choice on how it should be implemented. These core features, which formed part of the preferred option of the impact assessment carried out in 2008, can be defined as follows: a programme which allows certain third-country nationals to benefit from a facilitated border check (as opposed to the current rules on a thorough border check for all third-country nationals), during a given period of validity, and which involves using new technology to either semi-automate or fully automate the border check process. Participation in the programme would be subject to a pre-screening which would involve the vetting against certain criteria and the enrolment of personal data, including biometrics. The RTP would not change the requirement of obtaining a visa, if applicable. Finally, the RTP and all processes involved (data on application, pre-screening etc.) would be designed so that they adhere to data protection rules and do not decrease the level of border check security compared to the baseline situation.

Taking into account that border checks are currently fully harmonised at EU level, an EU RTP must be implemented in a harmonised way in the whole Schengen area with regard to the above criteria. The third-country nationals participating in the RTP would benefit from the same facilitated border checks at all parts of the external borders of the EU (of all Schengen Member States) and can use ABC systems wherever available.

2.2.2. Could these features be provided through existing systems?

The existing systems, the SIS, the VIS or EURODAC, cannot be used for the RTP purposes as they are developed for distinct and different purposes, namely, to enhance security of the Schengen area, to manage visa applications and to manage asylum applications whereas the RTP would facilitate travel. To expand the functionalities of the VIS and/or the SIS and/or the EURODAC would require a complete change of the legal basis and current capacity limitations could only be overcome by significant further investments. 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. The workflow of the VIS is optimised to deal with 10 million visa applications per year. Adding 5 million RTP applications to top of that would require significant investments especially with hardware, software, data storage and communication infrastrucure. Furthermore, working processes should be changed as the VIS would cover both visa holders and visa exempted. Moreover,

there would be significant data protection implications if the system were to include both visa holders and visa-exempt persons.

Border guards' work at the external border crossing points would be more difficult and time-consuming if the security and facilitation tools (for example the SIS/VIS/EURODAC and the RTP) were to be mixed. The different types of alerts and information would be delivered by one system and border guards would every time need to verify very carefully whether the information received concerns security or facilitation aspects. At the moment, border guards know immediately that there is an important issue with the traveller and a more thorough check is required, if an alert is distributed by the SIS.

Moreover, the principle of purpose limitation needs be adhered to and the risk of "function creep" has to be prevented as highlighted by the EDPS in his opinion on the Commission Communication on migration[34]. With regard to Advanced Passenger Information (API) and Passenger Name Record (PNR) the situation is even more difficult as the API directive is implemented differently in Member States, no central component exists, data submitted by carriers is limited and the quality of data, even though reliable, does not meet the requirements of the RTP. The same applies to the PNR. Therefore the possibility of including the RTP functionality in the VIS/SIS/EURODAC/API/PNR itself/themselves can be discarded. Nevertheless, intelligent use could be made of possible synergies with technical equipment already in place as described in Annex 6.

In addition, there would be major technical and functional links between the VIS and the RTP. The technical development of an RTP should exploit technical synergies, organisational simplification and economies of scale to the maximum by using the same technical platform as the VIS. Biometric matching functionality could be performed by the existing Biometric Matching System, which already provides such a functionality for the VIS. However, the biometric data stored in the VIS could not be legally exploited by the RTP as the VIS is systematically checked only on entry wheras the ccess granted to the RTP (and biometrics) should be checked both on entry and exit.Although some Member States have implemented a national form of the RTP, those RTPs cannot be expanded or used as a platform for the EU wide RTP. National RTPs are developed mainly for EU citizens based on the national needs and technical specifications and they are not interoperable. Furthermore, already existing national RTPs neither store the data of entries or exits nor do they calculate the duration of stay within the Schengen area. Therefore, the Smart Borders Package (i.e. RTP and EES) specifically complements the required elements to attain the objectives.

Finally, building a new system upon existing national systems would contradict essentially the lessons learnt from the development of other large-scale IT systems, which were already presented in the 2010 Communication:

(a) it might lead to unpredictable technical problems and delays, especially for the adaptation of national systems and the migration of data;

(b) the development of the RTP shall not be started before the legal basis is in place, in order to avoid developing premature functional specifications;

---

34 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_EN.pdf

(c) the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice shall be entrusted to develop and operationally manage the centralised part of the system including uniform interfaces in Member States;

(d) the processes established with the new IT system shall follow the same principles as for VIS to make the process as easy as possible for border guards and consular authorities.

2.3. Design issues

There are a number of key choices that need to be made when designing an RTP. These choices must strike the right balance between maximising the overall usefulness and efficiency of the system in addressing the overall problem as described in section 2.1 and minimising its impact on fundamental rights. This involves choices both with regard to the overall architecture of the system and additional features in relation to the "core" system as described in section 2.2.1.

By maximising only usefulness and/or efficiency of the system there is a risk for ignoring other important aspects such as fundamental rights and vice versa. For example, the RTP could be designed so that it would be easy to use for border and consular authorities, 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 huge data protection implications and would not be proportionate against the objectives of the RTP. The best possible balance must be found taking into account usefulness, efficiency, security and fundamental rights.

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.

2.3.1. Lodging an application for an RTP

The actual application process will need to be designed i.e. determining where should applications be submitted in practice. The overall take-up for participation in the programme will determine how many travellers will in practice be able to benefit from a facilitated check at the border and consequently directly impact on queuing times. The interest in the RTP among third-country nationals will greatly depend on how difficult or easy it will be to join the RTP. From the traveller's point of view one key issue is how convenient it will be for him/her to reach the office where (s)he will be able to lodge an application for the RTP. Generally, travellers are not willing to journey hundreds of kilometres to sign up to a voluntary system. This decision will also have an effect on the authorities obliged to receive and process the applications.

There would be three sub-options for lodging an application: a) at any external border crossing point, b) at any Member State consulate[35] and c) at both places.

Sub-options 1a and 1b would have a negative effect on the number of the RTP applications and thus would limit the advantages of the RTP. Sub-option 1a would require visa holders to

[35] Consulates include also Common Application Centres.

submit two set of applications including supporting documents; first at the consulate for a visa and then at the external border for an RTP. This would require extra time and work from visa holders and one could estimate that 1/3 of potential registered travellers among visa holders equivalent to 800 000 third-country nationals per year would not be willing to do it i.e. would not apply for access to the RTP.

On the other hand, sub-option 1b would include extra costs and loss of time for visa-exempt nationals since this category of travellers would have to travel to the consulate to lodge their application for the RTP and have their biometric data captured. One could estimate that at least half of potential RTs among visa-exempt third-country nationals equivalent to 1,3 million third-country nationals per year would not apply for the RTP in the consulate.

Implementation costs for EU and Member States would only be between 1 to 5 million EUR more in case of the sub-option 1c – allowing the lodging of applications at the border crossing points as well as at the consulates – than either sub-option 1a or 1b. Comparing the costs and the effects of the sub-options against the number of the RTP applications sub-option 1c would clearly be the most cost-effective sub-option to meet the objectives "to facilitate the crossing of EU external borders and to promote access to the RTP". Furthermore, it would be coherent with the existing border and visa policy. Therefore, the chosen sub-option is 1c without further analysis. At Member States level all the implementation costs would fall on visa and border authorities. Allowing the traveller to choose the best place for him/her to lodge an application would guarantee a larger number of participants in the programme, thus helping Member States to manage their passenger flows at the external border crossing points.

It can be predicted that the applications would be directed to the most appropriate authorities: travellers requiring a visa would most probably lodge their applications at the consulates and visa-exempt travellers would do so at the border crossing points.

2.3.2. Data storage

The pre-screening will involve the enrolment of the applicants' personal data, including biometrics (fingerprints). The design of this part of the process is important for the overall security of the system, the potential impact on the fundamental rights of RTs, and the actual functioning of a facilitated check at the border. Persons without fingerprints or with unreadable fingerprints would need to be excluded from the RTP[36]. Alphanumeric data from the application file as well as biometrics specified in Annex 8 need to be stored somewhere, so border guards can verify at the border, whether the person is a registered traveller. The question therefore arises how and where that data should be stored and for how long, taking into account that it must be available to the border guard of any Member State where the person is physically crossing the border. Whenever new information systems and different ways of storing information are at stake, the respect of the Charter of Fundamental Rights of the EU, particularly the right to respect for private life and right to the protection of personal data, and the cost of the systems require a careful assessment before any final decisions are made.

The need for real-time information exchange between Member States will need to be considered, taking into account that one Member State's decision to grant/revoke/extend access to the RTP will determine whether a person will benefit from facilitated border checks

[36] However, this does not mean that the person cannot travel to the EU. He/she could use the manual border check booth as nowadays.

at the external border of another Member State. Integration with existing processes at the external border and/or at the consulates should be ensured. Furthermore, security aspects of data storage need to be highlighted.

Whatever the system used to store the data, the effective implementation and enforcement of data protection rules must be ensured. Personal data should be protected against any unauthorised use. The right to access and verify the data, purpose limitation, etc. must be monitored.

2.3.3. Vetting criteria

The RTP requires that all participants are pre-vetted and pre-screened. The criteria for that process must therefore be defined, to ensure that the same criteria are applied by all Member States and that they meet the requirements in terms of preventing irregular immigration and ensuring security.

Vetting criteria should be proportionate in relation to both the internal security of the EU and the objectives of the RTP, as their definition will influence the take-up of the programme. Also, the time needed for examining and processing the applications as well as related costs should be taken into consideration.

2.3.4. Automation of border control for registered travellers

A key question involves defining how facilitated border checks should be implemented in practice at the border crossing points. In other words, as concerns RTs, how the current thorough border checks should be adapted for this specific group of travellers. Directly linked to the definition of "facilitation" is the question of automating border checks. To fully automate third-country nationals' border checks, a solution has to be found for calculating the period of authorised stay in the Schengen area at entry and exit or this requirement needs to be abolished as regards RTs. At the moment, the calculation is based on the stamps affixed on the third-country nationals' travel document.

Automation will significantly impact many issues, for example, the throughput capacity of border crossing points and hence the impact on border crossing times. It will also have an impact on the required space and human resources needed at the border crossing point, and naturally, it will significantly impact the traveller's border crossing experience. The overall benefits that will be derived from how facilitated border checks will be defined can subsequently be assessed against the costs for setting up the system (cf section 2.3.2. on data storage).

2.3.5. Application fee

Whether an application fee should be paid by the applicant would need to be decided. An application fee, if any could follow the same logic as the visa fee according to current EU legislation (60 EUR) i.e. the fee would be calculated so that it covers Member States' administrative costs for examining applications.

2.4. Baseline scenario - how will the situation evolve if no new action is taken at EU level?

Doing nothing at the EU level would mean that third-country nationals' border crossings could not be facilitated except those specifically mentioned in the SBC and the Local Border

Traffic Regulation meaning that thorough checks would be applicable for third-country nationals and no access to ABC could be given for them. Taking into account that border crossings at the largest and busiest border grossing points have been increasing and will continue to do so in the future[37], Member States with problems managing queues already today would have no other tool than hiring more staff and rebuilding infrastructure if at all feasible; any future increase in travel flows would lead to more problems of this kind. Furthermore, the full roll-out of the VIS will worsen the situation at the external border crossing points and thefore longer queues are expected. All third-country nationals holding a visa will be verified against the VIS on entry by using the visa sticker number in combination with verification of fingerprints. The fingerprint verification against the VIS will start in 2014 and it will inevitably slow down the border check procedure by some tens of seconds per visa holder. To cope with the forecasted 80% increase of travel flows at the air borders and the verification of visa holders' fingerprints at entry, Member States would need to hire approximately 17 500 border guards more equivalent to costs of 542,5 million Euro per year across the EU. Any increase in travel flows at sea and land borders would require a proportionate increase of staff level. All the costs would fall on border guard administrations.

This impact assessment is prepared in parallel with the impact assessment on the creation of an EES. An EES would replace the current system of stamping passports with the electronic registration of the dates and place of entry and exit of third-country nationals admitted for short stays to the Schengen area to allow for accurate and reliable calculation of authorised stays. In order to fully meet its purpose, such a system should record visa holders' and non-visa holders' movements alike and be applied consistently at all border crossing points. An EES would be integrated into the ABC and would allow for fully automated border crossings for third-country nationals replacing current manual calculation of authorised stay based on the stamps in the passport. Without the EES fully automated systems could not be implemented for third-country nationals.

However, the RTP could be implemented without an EU-wide EES, but Member States would then have to implement a semi-automated border control for RTs meaning that after successfully passing through the automated part of the border control procedure (i.e. ABC gate), the RT would be guided to the border guard who would stamp the travel document and calculate the length of stay in the Schengen area. This would remarkable diminish the added value and attractiveness of the RTP.

The EES does not as such form part of the baseline for this impact assessment - the two systems (EES and RTP) are not dependent on each other as regards their implementation – but the potential development of an EES has to be taken into account in relation to automation of border control for third-country nationals.

In terms of national developments, a continued further introduction of ABC for EU citizens by Member States at major airports is likely, as is the further development of national RTPs. However, these developments are not relevant, as they only concern EU citizens, except with regard to the automated gates installed at border crossing points. Those same gates installed

---

[37] See Eurocontrol's "long-term forecast for the next 20 years" published on 17 of December 2010, http://www.eurocontrol.int/statfor/gallery/content/public/forecast. Eurocontrol expects an increase from 400 million in 2009 to 720 million border crossings at the air borders in 2030. 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 Office of Travel and Tourism Industries (OTTI), http://tinet.ita.doc.gov/view/f-2000-99-001/index.html.

for EU citizens could largely be also used by third-country nationals if the EU RTP is implemented.

Currently, only one Schengen country has a project running at the air border crossing point with a third country based on semi-automated border controls both in the Member State and the third country[38]. Some other Member States may develop an RTP for third-country nationals based on this model. The overall impact of such systems with regard to facilitating travel flows of third-country nationals to the EU can however be assumed to be limited: they only involve a minimum facilitation of the border check (a semi-automated system). Moreover, such programmes can only operate on a bilateral basis based on an agreement between one Member State and one specific third country. The target group for this type of RTP is therefore also effectively limited to third-country nationals who cross the external border of the two countries at the same location each time. A widespread take up of such programmes will also be hampered by the exponentially increasing number of bilateral agreements needed should they involve several Member States and several third countries, with travellers obliged to carry out multiple registrations with each programme individually.

While the continued use and possible small increase of national RTPs described in section 2.1.1 forms part of the baseline for this impact assessment, it is not relevant for the problem definition or the assessment of the options, as the basic scope is different: a national RTP is for EU citizens, while a EU RTP will be for third-country nationals. Member States can thus continue to use their "national RTPs" also in the future[39], and these national RTPs would not affect the implementation of the EU-wide RTP discussed in this impact assessment. The EU RTP needs to be developed based on the common technical standards and it should be interoperable with the existing and future processes and workflows at the consulates and at the external border. Furthermore, synergies with the existing EU-wide systems should be exploited.

In general, no significant change is expected in the current situation with regard to third-country nationals' border checks. Therefore, the baseline for this impact assessment consists of the existing SIS[40], the successful roll-out of the VIS as well as the establishment of an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (the Agency)[41]. 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.

In summary, the baseline scenario can be described as the following:

– the current one-size-fits all approach to border checks of third-country nationals will continue with no possibility to distinguish between different travellers based on risk and no possibilities to provide a facilitated border check for low-risk, frequent travellers,

---

38 The Netherlands and the US have this kind of scheme called FLUX. See Annex 3 and also http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Flux.htm.

39 Including the FLUX scheme.

40 The switch from SIS to SISII is not relevant as the implementation of the SISII will not bring any new elements to the border check procedure when implemented.

41 OJ L 286, 1.11.2011.

– assuming limited expansion of personnel numbers in the Member States, border crossing times will increase due to the higher passenger flows, use of larger passenger aircrafts and ferries/cruise ships, and the implementation of the VIS,

– border crossing times for EU citizens will decrease due to a continued take-up of ABC systems.

2.5. Subsidiarity

Under Articles 74, 77(2)(b) and 77(2)(d) of the Treaty on the Functioning of the European Union, the Union has the power to adopt measures relating to checks on persons and the efficient monitoring of the crossing of external borders.

The need for intervention at European level is clear. No Member State alone is able to build up an RTP providing facilitated border checks across the Schengen Member States. One individual Member State's decision to grant access to an EU-wide RTP would have an impact on all Schengen countries and must therefore be regulated at EU level. Any measures related to border control would have to apply to the Schengen area without internal border controls which currently includes all the Member States except Romania, Bulgaria, Cyprus, UK and Ireland and four other European countries (Norway, Iceland, Switzerland and Liechtenstein). Schengen states are committed to maintaining common EU borders and common standards for border controls. Checks are carried out only at the external border, after which the traveller can travel freely within the Schengen area.

It is vital for the internal security of the Schengen area that all the binding rules linked to border control are decided at EU level.

Therefore, the objectives cannot be sufficiently achieved by the Member States acting alone but can be better achieved at EU level.

3. OBJECTIVES OF THE RTP

The general objectives of the RTP are:

- To facilitate the crossing of EU external borders by third-country nationals;
- To maintain the current level of security.

The specific objectives are:

- To promote access to the RTP for certain categories of frequent, pre-vetted third-country nationals;
- To ensure protection of registered traveller's fundamental rights, in particular their personal data;
- To avoid discrimination between different groups of travellers.

The operational objectives are:

- To decrease the time and costs of border crossings for frequent travellers and to increase the throughput capacity of border crossing points. Border checks of registered travellers should not take more than 20-40 seconds on average.

- To free up border control resources by 25% from checking cross border movements of frequent and pre-vetted travellers and to enable better focus on checking higher risk travellers[42] and/or serve other travellers.

4. POLICY OPTIONS

In addition to the baseline, five policy options linked to the implementation of the RTP were identified during the consultation with stakeholders. Because stakeholders had diverging views on their implementation and in order to allow for a cost-benefit analysis, for each of these five policy options real practical implementation options have been defined.

The five policy options and their sub-options are independent implementation options for the RTP in the sense that the choice of one sub-option does not influence the choice of sub-options in relation to the other policy options. In total, there are 13 sub-options which could be combined into a large number of equally feasible combinations or "packages" which would have been impractical to analyse. For this reason, each sub-option has been analysed individually. It should be noted, however, that the *impacts* of policy options 3 and 4 and their sub-options are linked. Furthermore, as the best choice for the **Policy option** 1 "lodging an application for an RTP" is clearly the lodging of applications at both border crossing points and consulates (cf 2.3.1.), it is not discussed again in this section.

4.1. Policy option 2: Data storage

4.1.1. An RTP based on data stored in a separate token[43] (sub-option 2a)

Under this sub-option, the personal data (alphanumeric and biometric data)[44] enrolled from each successful RTP applicant would be stored on a chip on a plastic card ("token"), to be issued by the Member State having approved the application. The alphanumeric data (but not biometric) would be stored by the Member State in question in a national database. No European database would be set up nor any information exchanged at European level.

When crossing the border, using automated gates, the document reader incorporated into the gate would read the traveller's passport, the visa sticker if applicable, and the token. The traveller's fingerprints would be read by the fingerprint reader incorporated into the gate. Checks against databases (such as SIS and national databases) would be run using the data from the passport. The validity of the visa, if applicable, would be checked against the VIS. The traveller's identity and the access granted to the RTP would be verified against the data stored on the token (alphanumeric data and biometrics).

---

42 Travellers who have decided not to join the RTP are not and shall not be considered, due to their non-participation in the RTP, as higher risk travellers.

43 In the context of an RTP, a token can be described as a physical device given to the authorised user to prove his/her identity electronically. The token acts like an electronic key to access something, in this case to the ABC system.

44 See annex 8 for the data to be stored.

This sub-option would involve defining common technical standards for the token including security and layout aspects to guarantee interoperability and security across the Member States and visibility across the Schengen area. On the basis of the prior definition of business requirements for the token to be adopted by the Commission in a comitology procedure, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011 of 25 October 2011 (the Agency) would be responsible for the definition of the technical specifications for the token. The technical specifications would be agreed with Member States by the Commission in a Comitology procedure. It can be noted in this regard that the option of using an e-passport held by the third-country national as a token can be discarded from the start; not all third-country nationals are issued with e-passports, most if not all third countries issue e-passports with only the facial image as biometric identifier, and full access to the third-country national's data on the chip for all Member States' border guard authorities is not feasible within the short- to medium-term.

During the consultations on the Commission's communication adopted in 2011, one Member State was clearly in favour of a token-based system. The majority of Member Sates preferred a centralised system.

4.1.2. An RTP based on data stored in a centralised database (sub-option 2b)

Under this sub-option, a centralised database would be developed, in the form of a Registered Traveller System (RTS). Biometrics (fingerprints) and alphanumeric data from the application file on all registered travellers would be stored in the RTS[45].

When crossing the border, using automated gates, the document reader incorporated into the gate would read the traveller's passport and the visa sticker, if applicable. The traveller's fingerprints would be read by the fingerprint reader incorporated into the gate. Checks against databases (such as SIS and national databases) would be run using the data from the passport. The validity of the visa, if applicable, would be checked against the VIS. The traveller's identity and the access granted to the RTP would be verified against the data stored in the RTS (alphanumeric and biometric data).

It is assumed (based on the technical studies and the consultations) that the centralised system could be based on a similar technical platform as the VIS. Functionalities and responsibilities for the RTS would be established. On the basis of implementing measures adopted by the Commission in a comitology procedure, the Agency would develop and operationally manage the RTS[46].

During the consultations on the Commission's communication adopted in 2008 and 2011, Member States expressed a clear preference for a centralised system. The European Parliament expressed doubts about the setting up of a new centralised database and was of the opinion that no new instruments and systems should be launched until the existing tools are fully operational, safe and realiable.

---

45 See annex 8 for the data to be stored.

46 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.

4.1.3. An RTP based on data stored in a separate token combined with a central repository (sub-option 2c)

Under this sub-option, only the unique identifier (application number) would be stored on the token, while biometric data together with the unique identifier and data from the application would be stored in a central repository. A link (unique identifier e.g. application number) between the repository and the token is needed to verify the validity of the access granted to the RTP. The token is needed in order to carry out a verification (1:1) against the repository[47] at the border check. A verification takes only seconds.

The main difference between a central database and a central repository is that in a central database, the alphanumeric and the biometric data are stored together and accessed together. In the repository, the alphanumeric data and the biometric data are, from a technical perspective, stored in separate sections. In this case, the biometric verification at the border check can only be performed by physically producing the token (unique identifier). This verification produces only a hit/no hit result. However, the visa and border authorities should use the central repository for examining applications, for the examination whether to revoke or extend access granted to the RTP, in case of lost or stolen token and if any problems occur with facilitating registered travellers' border crossing. Since for these purposes all information stored in the central repository may be relevant, the competent authority should have access either to the complete application file including biometric data of the applicant or only to the separate section of central repository containing alphanumeric data. Access shall be given to the competent authorities only if the specific search criteria are met.

The same principles as in the two sub-options above would apply, with regard to the issues related to the token as well as the issues related to the centralised database. The Agency would be responsible for the development and management of the central repository and for the definition of the technical specifications for the token whereas Member States would be responsible for management of tokens. The technical specifications would be agreed with the Member States by the Commission in a Comitology procedure.

When crossing the border, using automated gates, the document reader incorporated into the gate would read the traveller's passport, the visa sticker if applicable, and the token of the traveller. The traveller's fingerprints would be read by the fingerprint reader incorporated into the gate. Checks against databases (such as SIS and national databases) would be run using the data from the passport. The validity of the visa, if applicable, would be checked against the VIS. The travellers' identity and the access granted to the RTP would be verified against the data (alphanumeric and biometric data) stored in the central repository. However, any verification would not be possible without physically producing the token at the border. The link between the token and the repository would be the unique identifier stored on the token.

During the consultations on the Commission's communication adopted in 2011, two Member States were in favour of a token/central repository system. However, these Member States did not provide concrete reasoning why they prefer this option.

---

[47] Verification means the process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.

4.2. Policy option 3: Vetting criteria

4.2.1. Same as for multiple-entry visa holders (based on current EU law) (sub-option 3a)

Under this sub-option, vetting criteria would be aligned with the criteria for multiple-entry visa holders[48]. As can be seen from Annex 9 vetting would be performed to verify that the entry conditions are met. Vetting would be done using the same data sets as used when examining multiple-entry visa applications (application form, supporting documents, EU-wide databases such as the SIS and VIS, if applicable and national databases).

The EDPS in his informal comments on the draft 2011 communication highlighted that the sources of data used for the vetting of applicants must be clarified.

4.2.2. More thorough vetting procedure (sub-option 3b)

A few Member States have raised the issue of having as thorough a vetting procedure as possible. For them, the vetting done for visas is insufficient to give access to the RTP and especially to move to a full automation of border control. Fully automated border control would therefore, in their opinion, require stricter vetting procedures.

This sub-option involves therefore adding the following procedural steps:

- a consultation between Member States would always be compulsory before a decision on an RTP application is made,

- a third-country national should choose the Member States at whose external borders he/she would like to benefit from a facilitated border check. Each of the Member States chosen would check the third-country national's data from their own databases (border guard, police, etc.) and verify watch lists before the third-country national's access to the RTP would be granted/refused.

4.2.3. Discarded sub-option: Involvement of third countries in the vetting (sub-option 3c)

Some Member States considered that the country of origin of a traveller should also be involved in the pre-screening by carrying out a check of their databases (border guard, police, etc.) and watch lists and deliver a "green light/red light" message, or grant a certificate on the traveller's good behaviour in the country of origin. This possibility is discarded from the start, for several reasons. A vetting by a third country would effectively give a third country a decisive influence on whether (or not) a third-country national should benefit from facilitated checks to enter the EU. Some third countries may not be willing to do any kind of vetting on their own citizens for several reasons; one being that it would cause additional burden for them without bringing any concrete benefits. Certain third countries, especially those with a poor human rights record, could delay the vetting procedure or postpone the delivery of a certificate, particularly with regard to specific individuals (journalists, rights defenders etc.). In the worst situation access to the RTP could be given only to persons having a "privileged status" in their country. For its practical implementation it would also require the exchange of personal data using technical means between each Member State and each third country. This kind of vetting would neither be proportionate in light of the objectives of the RTP nor feasible within the short- to medium-term, and this sub-option is therefore not further

[48] As resulted by the Visa Code; OJ L 243, 15.9.2009.

assessed. This option also raises serious data protection concerns as it requires the exchange of personal data with third countries which may not provide adequate safeguards and protections for processing personal data. Furthermore, this sub-option would not be coherent with the EU's policy on information exchange with third countries.

4.3. Policy option 4: Automation of border control for registered travellers

4.3.1. Fully automated (sub-option 4a)

Under this sub-option the facilitated border check for registered travellers would essentially be identical to the minimum check currently applied to EU citizens, although for third-country nationals the consultation of databases (such as SIS) would have to be systematic and compulsory. Registered travellers' border checks could thus be fully automated and under normal circumstances no human intervention would be required, using largely the same automated gates as currently used for EU citizens. Verification of the identity of the traveller would be made against biometric data (stored according to one of the sub-options under policy option 2). However, human intervention should be provided immediately if a traveller is "refused" by the system or any malfunction occurs.

This sub-option would require that a solution is found to calculate the time spent in the Schengen area. The EES would be a solution for that.

The majority of Member States were in favour of fully automated border control system for registered travellers. However, some of them asked the Commission to launch a study on the usefulness of the ABC systems for third-country nationals and expressed doubts on demand for an RTP and ABC as they have only few entries/exits outside the Schengen area.

4.3.2. Semi-automated (sub-option 4b)

Under this sub-option, the facilitated check would be defined as a minimum check with certain additional elements. Registered travellers' border checks would include as a first step the same process as in sub-option 4a; passing through an automated gate for the verification of the identity, access granted to the RTP, and checks against databases (such as SIS). As a second step, human intervention would still be required; the automated process would be followed by an individual decision, by the border guard, to authorise or refuse entry or exit, and the passport could be manually stamped as today.

Only very few Member States supported a semi-automated border control for registered travellers considering that it would better guarantee security aspects.

4.4. Policy option 5: Application fee

4.4.1. Fee of 20 EUR (sub-option 5a)

Under this sub-option, a fee of 20 EUR would be introduced. The fee is calculated on the basis of the administrative cost to Member States for examining applications. It is estimated that 5 million third-country nationals would apply for access to the RTP each year. Half of them would be visa exempted and half third-country nationals requiring a visa. The

examination of one application would take 45 minutes, on average[49], including checking the supporting documents, capturing biometric data and conducting interviews, if applicable. If a multiple-entry visa application were examined at the same time as a RTP application and based on the same supporting documents, then the time needed for examining a RTP application would be reduced by half. In the abstract, the total time needed for examining and granting/refusing access to the RTP would be 2,81 million hours per year equivalent to 73,1 million EUR or 1 705 persons[50] across Member States. The fee could therefore be set at 20 EUR per each individual application. However, the fee could be reduced to 10 EUR if a visa and a RTP appliation were examined at the same time. The fee would not cover any additional costs for issuing a token and sending the token to the applicant by mail.[51] All the Member States which expressed their views during the consultations were in favour of collecting a fee from the registered travellers.

4.4.2. No fee (sub-option 5b)

This sub-option would involve imposing no fee whatsoever on applicants.

5. ANALYSIS OF IMPACTS

This section considers each of the sub-options described in section 4 against the assessment criteria. The sub-options have been rated on a nine-point scale with respect to their likely performance relative to the general 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 total one-time development cost of the system related to the expected duration of three years and the total yearly operational costs for the ensuing period of five years, divided into central (EU) and national (Member States) costs; the tables in annexes 10.1-10.3. contain more detailed information on cost categories and costs per item; a breakdown and more detailed description of the administrative costs is provided in annex 10.4.

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

Only the criteria relevant for each sub-option have been analysed, and otherwise omitted.

The impacts have graphically been indicated with symbols:

- √√√√	Highest negative impact/cost
- √√√	Significant negative impact/cost
- √√	Medium negative impact/cost
- √	Small negative impact/cost

[49] Based on replies of the three Member States that provided data the examination of a (multiple-entry) visa application lasts on average 45 minutes. This time includes capturing the biometric data. The procedures with a RTP application and a visa application are almost the same. A starting point for the calculation is that all multiple-entry visa holders submit an RTP application and a visa application at the same time.

[50] Assuming that one person works 7,5 hour/day and 220 days in a year.

[51] The cost for a token would vary between 1 and 5 euro and has been taken into account in relation to the costs for the relevant sub-options under policy option 2.

0	No impact
√	Small positive impact/savings
√√	Medium positive impact/savings
√√√	Very significant positive impact/savings
√√√√	Highest positive impact/savings

As explained at the start of section 4, all policy options and their sub-options are independent implementation options. However, the impacts of the sub-options with regard to policy options 3 and 4 (vetting criteria and automation of border control) are directly linked, in the sense that the impact of the sub-options with regard to vetting cannot be assessed without knowing which is the preferred option with regard to automation, and vice versa. Consequently the available four sub-options (3a, 3b, 4a, 4b) from the two policy options have been combined in the assessment into the four variations possible, and the impact of all four variations is assessed in an integrated way.

As the preferred sub-option of policy option 1 is clear (cf 2.3.1.) and the sub-options of policy options 2 (data storage) and 5 (application fee) are purely technical implementation options which are not linked to other policy options, they have not been presented and analysed in combination with the other policy options.

It must be noted that in the impact assessment it was very difficult to estimate the impact in practice of the RTP on the number of border guards needed at the external border and on travellers´ waiting time as these depend almost entirely on the individual border crossing point.

There are very big differences between the traveller profiles at different border crossing points at the external border as described in section 2.1.2. and Annex 2 (for example, the number of third-country nationals vs. EU citizens differs greatly). Also, the current capacity to manage passenger flows at a specific border crossing point (infrastructure, data transmission system, customs and security checks, etc.) has a significant effect on travellers´ waiting time and also on border guard resources needed. As a result of the above factors, precise estimates of the impact of each sub-option on border crossing times and the need for human resources would only be possible based on a detailed analysis of the current situation at each and every border crossing point (over 1800) of the Schengen area, which is not practically feasible.

5.1. Policy option 1: Lodging an application for an RTP

Sub-options are not analysed as the preferred option is clearly 1c; lodging an application for an RTP at the external border and at consulates (cf 2.3.1.).

5.2. Policy option 2: Data storage

As regards all the sub-options, the EDPS highlighted the privacy by design, only a one to one verification of biometrics should be possible, data protection rights should be ensured and no record should be stored in the RTP database/token.

5.2.1. Data stored in a token (sub-option 2a)

- To facilitate the crossing of EU external borders by third-country nationals √√√

A token-based system would significantly facilitate border crossings compared to the baseline situation. A token-based system would guarantee facilitated border crossings as any technical break down or failure of the system would not have effects on Member States' other systems.

However, a token-based system adds one step to the automated border control process, as a token needs to be physically placed on a document reader (integrated in the gate) and "opened", and the identity of the registered traveller should be verified against the data stored in a token. This additional verification step would increase somewhat (a few seconds) the time needed for a border check. From the travellers point of view the experience will therefore be a bit more complicated and cumbersome compared to a centralised system, as not only the passport and the visa sticker (if applicable) needs to be put on the reader but also the token.

A token as such would give more visibility to the EU RTP. However, a traveller who has forgotten to bring the token cannot make use of his/her access to the RTP. Furthermore, a renewal of access to the RTP could not be made centrally, as the person would need to appear in person to have a new token issued. This is likely to reduce the attractiveness of the RTP to persons who do not travel often but, as already indicated before, these do not constitute the main target group of the programme.

The EU could consider promoting the token-based system – based on existing and future EU technical standards – at a global level following its full implementation in the EU.

- To maintain the current level of security √√

The overall impact will increase security due to the verification of the identity of travellers using biometrics, as concerns non-visa holders.

However, a token-based system could be exploited for "Registered Traveller shopping", as no data is stored from any previous applications which can be accessed by the authority assessing the application. Nothing would prevent a person from repeatedly lodging applications at several locations to increase his/her chance of success, although a uniform application of the vetting criteria would minimise this risk.

Multiple tokens could be issued for the same registered traveller not subject to the visa requirement: it would be possible to lodge multiple applications and obtain several tokens linked to the same person travelling with different travel documents. This risk is not, however, relevant for visa holders as their identity can be biometrically verified in the VIS. For persons not holding a visa the risk of identity fraud could be reduced by requiring an applicant to hold a biometric passport.

Access to the RTP cannot be revoked centrally, in case a person no longer fulfils the conditions. As long as a token holder presents his token at the border within the validity period marked on the token, assuming ABC is used, he/she can use the RTP even if there would be reasons to cancel his/her "membership" (he/she could be flagged in the SIS but only for one of the legally possible categories of alerts). Access granted to the RTPcan only be revoked by physically cancelling (destroying) the token.

5.2.2 Data stored in a centralised database (sub-option 2b)

- To facilitate the crossing of EU external borders by third-country nationals √√√√

A centralised RTP would not require travellers to carry any additional document besides the passport. The traveller would however not receive any physical confirmation or "proof" that he or she is a registered traveller; this would be dependent on verification against the records in the RTS.

Border guards would always be able to check whether a person is a registered traveller by searching in the centralised database. During ABC, biometric verification against the RTS could be done simultaneously with other processes and can easily be integrated into the automated process.

Member States were in favour of centralised system whereas the European Parliament expressed doubts on establishing it.

- To maintain the current level of security √√√

Overall the impact on security is positive compared to the baseline due to the verification of the identity of travellers using biometrics, as concerns non-visa holders.

A centralised system would be more secure than a token-based system as there would be no token which could be falsified. Having a reliable, accessible record of the registered travellers would help to examine a subsequent application wherever the application is lodged. Problems related to Registered Traveller shopping, multiple identity fraud and central revocation/renewal of access granted to the RTP are effectively solved by a centralised database. However, a centralised system could be hacked, just as any other data storage which is connected to a network.

5.2.3 Data (unique identifier i.e. application number) stored in a token and (unique identifier, biometrics and data from applications) in a central repository (sub-option 2c)

- To facilitate the crossing of EU external borders by third-country nationals √√√

In terms of the border management process, this sub-option involves the introduction of two new factors compared to the baseline – travellers carrying tokens and a new central repository to which all border crossing points and consulates must be connected.

In this sub-option there is a need to read the token as well as to search the central repository, in order to verify the identity of the traveller and that he is the rightful holder of the token. The automated process may therefore be marginally slower (a few seconds) compared to the other sub-options. The traveller must carry the token to benefit from the RTP membership at the border, but appearance in person is not necessary for renewal or revocation.

The visibility of the programme is achieved, but the feasibility of promoting it at global level is reduced, as the functioning of the system depends on centralised storage of personal data.

- To maintain the current level of security √√√

Overall the impact on security is positive due to the verification of the identity of travellers using biometrics, as concerns non-visa holders.

This sub-option allows for preventing identity fraud and for revoking or renewing RTP membership centrally. "Registered traveller shopping" would be prevented if the fingerprints

of rejected applicants are also stored in the repository together with the date of previous application(s) and the reasons for rejection.

5.2.4 Costs (all sub-options)

The costs in the 2008 impact assessment were taken from the technical feasibility study performed earlier, where the minimum technically feasible option, a web-based application for both the EES and the RTP, was chosen as the option for cost calculation. 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 the EES and the RTP in 2008 impact assessment were 100.000 EUR per year, compared to 13 million EUR per year (based on the current market prices) for a secure network only for the one system now.

This was the main reason why it was decided to prepare a separate detailed cost study in 2010 with the help of an external contractor[52]. 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 10).

The table below sets out the total development costs, the yearly operational costs, and accumulated total costs for development and operation (one-time costs and 5 years of yearly operational costs) for each of the three sub-options. As there is no central technical development in the token-based sub-option there are no EU costs for that sub-option. The costs below do not include the costs for examining applications, which are described under policy option 5. The sub-option 2c is clearly the most expensive one. The development costs would be 164 million EUR for Member States (MS) and 43 million EUR for the EU. Yearly operational costs would be for 81 million EUR for Member States and 20 million EUR for the EU. During the consultations on the Commission's communication adopted in 2011, the majority of Member States were concerned about the high costs of the systems (RTP and EES) and asked for a cost-benefit analysis and the EU's financial support.

Table 1 – Costs, policy option 2

Suboptions	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 (8 years) (in EUR million)**	ANNEX
Data stored in a token	151 (Member States (MS) 151)	95 (MS 95)	**626** **(MS 626)**	Annex 10.1
Data stored in a centralised database	190 (MS 152, EU 38)	94 (MS 76, EU 18)	**660** **(MS 532, EU 128)**	Annex 10.2

52 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

Data (unique identifier number) stored in a token and (unique identifier, biometrics and data from application) in a central repository	207 (MS 164, EU 43)	101 (MS 81, EU 20)	**712** **(MS 569, EU 143)**	Annex 10.3

In Member States the costs would fall on the ministry responsible for managing the system. Every Member State would be free to choose the best possible one and it could be for example the Ministry of Interior as is the case in many Member States with the SIS or the Ministry of Foreign Affairs as is the case in many Member States with the VIS.

5.2.5 Protection of fundamental rights, particularly privacy and data protection

A centralised system would have significant impacts on fundamental rights, particularly data protection and protection of privacy. The data would be stored in a form that could be manipulated and there is a potential risk, as with any data of this type, that it could be used inappropriately. The RTP should follow the requirements set in existing EU law for the VIS as to privacy, data protection and fundamental rights of travellers, including establishing clear rules on access rights, purpose limitation, monitoring and supervision of data processing, data security, etc.

A token-based system excludes the need for establishing a new EU level IT-system and a new centralised database. A token-based system would therefore have less of an impact on fundamental rights, privacy and data protection than establishing a centralised system. Personal data on travellers is stored only on a token and no centralised register or database would exist. The authorities would have access only to one individual's data. A one-to-many search using biometrics becomes technically impossible. However, the same data protection rules as for the centralised system would be needed.

On the other hand, a missing, lost or stolen token is a de facto risk that will require high demands on preventing the misuse of tokens and ensuring their security. Furthermore, there would also be a risk of cloning the token (electronic chip) or of unauthorised access to the token, especially as regards the alphanumeric data which is not normally as well-secured as biometrics. To minimise the risks above the token would need to follow the same security requirements as residence permits or e-passports. The main risk with a purely token-based system would be "Registered traveller shopping" as no data is stored from any previous application which could be accessed by the visa or border authority assessing the application.

In a token-based system, data protection benefits would need to be safeguarded so that Member States could store the registered travellers' alphanumeric data but not biometric data in their national databases. This would mean that instead of having a single EU database for registered travellers, all Member States could establish their own database containing only alphanumeric data.

In the sub-option combining a token with a central repository, the drawbacks related to data protection of the two other sub-options are present but with clear limitations. A one-to-many search in the central repository to establish a person's identity is impossible at the border check, and the risk of cloning or accessing the data on the token is minimised. As regards biometrics, border guards would have only hit/no hit responses at the border check. Alphanumeric and biometric data from the application file stored in the repository would be accessible to duly authorised staff of border control and visa authorities when assessing

applications, renewing/revoking access to the RTP, in case of lost or stolen token or any problems occur with facilitating registered travellers' border crossings subject to the specific search criteria. The AMCHAM EU supports a token with a central repository approach as separating the storage of anonymised data may allow for the use of advanced and secure mechanism to protect the most sensitive data at a lower cost.

As regards all sub-options, the scope of access to RTP data should be limited exclusively to duly authorised staff of border control and visa authorities, as far as access to the data is necessary for the performance of their tasks namely assesing RTP applications and facilitating third country nationals' travel. No access to the information stored in the RTP should be given to any other authorities or third countries.

The RTP shall respect the fundamental rights of all travellers and comply with the principles laid down in the Charter of Fundamental Rights of the EU and in particular Articles 7 and 8 thereof. Furthermore, in addition to the intervention of national data protection authorities to require correction or deletion of erroneous data, a review procedure for challenging or correcting potential errors in accordance with the right to an effective remedy (Article 47(1) of the Charter of Fundamental Rights of the EU) would have to be laid down.

Table 2 - Assessment of policy option 2

Sub-options	To facilitate the crossing of EU external borders	To maintain the current level of security	Cost	Protection of fundamental rights
Data stored in a token	√√√	√√	-√√	-√
Data stored in a centralised database	√√√√	√√√	-√√	-√√√
Data (unique number) stored in a token and (biometrics and data from applications) in a repository	√√√	√√√	-√√√	-√

5.3 Policy options 3 and 4: Vetting criteria and automation of border control

As explained in the beginning of this section, the available four sub-options (3a, 3b, 4a, 4b) from the two policy options have been combined into the four variations possible, and the impact of all four variations is assessed in an integrated way. The variations are:

- Same vetting as for multiple-entry visa holders (3a), fully automated border crossing (4a)
- Same vetting as for multiple-entry visa holders (3a), semi-automated border crossing (4b)
- More thorough vetting procedure (3b), fully automated border crossing (4a)
- More thorough vetting procedure (3b), semi-automated border crossing (4b)

- To facilitate the crossing of EU external borders by third-country nationals

Vetting criteria and procedures should be proportionate to the objectives of the RTP. Multiple-entry visas have already been issued for years and the criteria for their issuance have been tested. Travellers subject to the visa requirement would not have to deliver several different supporting documents. This would enable simultaneous processing of a visa

application and an RTP application and hence minimise the increase of work at the consulates and maximise the number of RTP applications submitted by visa-required third-country nationals.

Based on the Member States' analysis the border processing time using a fully automated ABC system is significantly shorter compared to the baseline (manual checks). For example, in Portugal's RAPID and Germany's EasyPass, e-passport based systems, automated border crossings based on facial recognition take 15-20 seconds, in Germany's iris-based ABG system using a conventional passport and template stored in a database, automated border crossings take 10-15 seconds and in France's fingerprint based PARAFE system, it takes 20 seconds. With the traditional border check procedure a border guard can perform an average of six EU citizens' border checks per minute whereas the same border guard can supervise 26 border checks by using the RAPID system. At Lisbon airport, one border guard monitors seven automated border check gates. In theory, RAPID increases the capacity of border checks during peak hours by around 430 % with the same number of border guards. Based on the presentation given by the Netherlands in the Innovation Border Management Conference held in Copenhagen on 2 and 3 of February 2012 36 e-gates, with 12 border guards supervising them, can process 5,7 million passengers per year. To process the same number of travellers with manual border control process 48 border guards would be needed. At Schipol airport, passengers' waiting time is reduced by 15 million minutes per year.

By comparison, according to the Member States' replies to the Czech Presidency and the Commission's questionnaire, currently (baseline) the average time for a (manual) border check is roughly between one and two minutes, depending on the type of border and whether the traveller is required to hold a visa or not. Based on these examples, the RTP with full automation would reduce significantly the border crossing time for third-country nationals at the busiest external border crossing points. As illustrated in section 2.1.2, 57% of border checks at air borders are performed at the 20 busiest air border crossing points in the EU.

In semi-automated border control, part of the process would be automated but border authorities would still carry out part of the border check manually (for example stamping of passport to calculate the time spent in the Schengen area). Time savings for border crossings for this sub-option would be limited compared to the baseline (manual checks). The interest for the traveller is also significantly reduced, as there will be a need to pass through two processes – the automated gate and appearing at the control booth – which can certainly be perceived as a step backwards compared to the baseline (manual check going directly to the control booth). The Netherlands conducted a survey from 9 May till 16 May 2011 in which a total of 242 of the US participants in the FLUX programme responded. The FLUX is a semi-automated programme. All respondents with an American passport indicated that their passports are stamped. 84% of the respondents were either outspoken negative (40%) about this requirement or regarded it as bureaucratic red tape (44%). Many comments which the respondents volunteered to give addressed this issue.

An automated system would allow for more efficient use of border control resources, the best use of available space at the border crossing points, and at the same time enable more efficient service for travellers[53], especially at busy border crossing points. As the experience of Member States' national ABC systems show, a substantial number of border guards can be

[53] The Privium program in Netherlands has processed millions of border crossings for its 46 000 members; Flux pilot programme report, February 2010.

freed up for other duties and thus facilitate also those travellers' border crossings who do not use the ABC system. Based on the final report on the cost analysis on Entry/Exit and RTP systems made by the external contractor[54], 7,68 border guards are needed per manual lane per million travellers to perform border checks whereas the rate using an ABC system is 2,73 persons. In a semi-automated system, these savings would largely be absent as each traveller would still need to be checked by a border guard.

Most travellers are already familiar with different types of e-services and are ready to use them. Approximately 90% of them are willing to use ABC systems as surveys conducted in the Netherlands, in the United Kingdom and in Australia show. The details of the surveys are reported in Annex 2.

During the consultations, several Member States recalled that the travel flows at the external borders are increasing constantly and all Member States are facing the same problem i.e. how to manage them efficiently and cost-effectively. The only answer for them is automation of border controls to the largest extent, also including for third-country nationals. Big investments would be needed in technology but "investing" only in human resources and old-fashioned border check procedures with stamping is the most expensive solution. In the long term, technical solutions will lead to savings. Some Member States saw an EES as a condition for the RTP and especially for full automation of border control. Common standards were pleaded as quickly as possible on the ABC and the RTP. Full automation of border control should be made available not only for business travellers but also, for example, for tourists travelling often to the EU.

Moreover, the American Chamber of Commerce to the European Union (AMCHAM EU) on its position statement on the Smart Borders of 23 of March 2012 highlights the use of ABC wherever possible to ensure more efficient border checks and a positive experience for the traveller.

By the end of 2010, over 200 automated border control gates have been installed at border crossing points. In addition to that, several Member States are planning to install them[55].

- To maintain the current level of security

With the use of fully automated border control, the same checks against databases (such as SIS) would be carried out as in the baseline situation (manual checks). Furthermore, the identity of the traveller would be verified using biometrics, which is not the case in the baseline situation as regards non-visa holders.

However, a few Member States proposed to have a more thorough vetting. For them, the vetting done for visas is insufficient to give access to the RTP and especially to move to a full automation of border control. The precise gains in security arising from stricter criteria are not easy to identify. If national databases of several Member States were to be checked, this would raise the level of security, but at the same time it would require additional time and

---

54 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

55 Several Member States have indicated in the External Borders Fund's Annual Programmes that they will start using the Automated Border Control systems at their external border crossing points. These Member States are reported in Annex 3 and in the Frontex's draft report on "ABC solutions based on eMRTD in EU Member States".

effort from Member States, thus reducing the positive impacts of the RTP. All data on the applicant would need to be sent to other Member States. Furthermore, awaiting replies from all Member States would be a time-consuming process. Notably, such a process would be inconsistent with the current process for the issuance of visas as well as the border checks, for which only the Member State carrying out the check consults its own national databases, the SIS and the VIS, if applicable. It would therefore be disproportionate to introduce such a requirement for registered travellers.

It is true that there could be some negative effects when using ABC for third-country nationals. Border guards are accustomed to observing even the faintest cues, for example, reading the unusual behaviour of a human being. This human factor is removed if the checks of the registered travellers are fully automated. It is possible to spoof fingerprints using modern techniques and materials; fingerprints can even be bought or stolen. However, the use of "liveness" detection built into fingerprint readers help mitigate this risk. Furthermore, border guards need to monitor ABC gates and could always check the traveller manually if any reason arises (e.g. random checks). Notably, these "weaknesses" of the ABC process cannot be addressed by introducing stricter vetting procedure, which shows that the impact on the level of security of stricter vetting procedure is in fact virtually non-existent.

5.3.1 Costs

Stricter vetting with a compulsory consultation mechanism between Member States would require the creation and maintenance of a communication network between Member States that would enable sending confidential information from one Member State to another, similar to the VIS Mail application, the consultation mechanism used in the VIS. The costs for the Agency to develop and create such a communication network would be approximately 1 million EUR at EU level and approximately 3 million EUR for Member States. In Member States the development costs for such consultation mechanism would fall on the ministry responsible for managing the system and operating costs would need to be paid by border and visa authorities.

Furthermore, stricter vetting procedure would significantly increase administrative costs for the Member States with an estimated 182 million EUR per year (see Annex 10.4). Half of the costs would fall on border authorities and half on visa authorities.

The costs for automation would vary between Member States depending on the number of ABC systems installed. All the costs for automation would fall on border authorities.

5.3.2 Protection of fundamental rights, particularly privacy and data protection

Although the RTP is voluntary for third-country nationals, stricter vetting procedure using a consultation mechanism between Member States would have a significant effect on the protection of fundamental rights, particularly privacy and data protection. Personal data would have to be sent through a network between Member States. This would require adeguate technical and security measures to ensure the protection of information processed and exchanged. The EDPS stressed in his informal comments on the 2011 communication that data protection rights have to be ensured irrespective of whether data subjects take part in a programme voluntarily or not.

The potential issue of discrimination through assuming that travellers who are not registered or accepted by a Member State are suspicious needs to be addressed. This issue was raised also by the EDPS in his informal comments on the 2011 communication. He highlighted that

measures should be taken to prevent positive discrimination from turning into a negative one of persons who do not have a strong track record of reliability, for example infrequent or first-time travellers. This issue arises especially if the vetting is too strict. This important topic should therefore be incorporated into the training programme on fundamental rights which Frontex organises for border guards. In order to raise awareness with the general public, this issue should also be covered during the information campaigns organised before the RTP starts operations. The leaflets and posters should clearly state that travellers are free to choose whether to apply for the RTP and use the ABC. Those not using the ABC are not considered as more risky travellers.

Detailed provisions would be required to provide third-country national applicants with the reasons why they have not been granted access to the programme. A system of review of the refusal and revocation of membership, and for challenging or correcting potential errors in accordance with the right to an effective remedy (Article 47(1) of the Charter of Fundamental Rights of the EU), would have to be put in place.

As technical failures or breakdowns can always happen, 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. If a registered traveller is unable, for example, for any reason, to use the ABC, and is redirected toward a manual border check, due attention should be paid to ensure that the ensuing procedures are in full compliance with fundamental rights, in particular with human dignity, and are conducted without stigmatisation.

As regards a centralised RTP in which the data is stored in a centralised database, supervision by the EDPS and cooperation between National Supervisory Authorities and the EDPS should be guaranteed and facilitated. As regards a token-based system without any centralised database or data exchange between Member States, National Supervisory Authorities would mainly be responsible for supervising and monitoring the access rights and purpose limitation. Data protection authorities should have the means necessary to access to the information processed and intervene and enforce compliance with data protection rules.

During the consultations, Member States highlighted the importance of data protection aspects in general.

Table 3 - Assessment of policy options 3 and 4

Sub-options and variations	To facilitate the crossing of EU external borders	To maintain the current level of security	Costs	Protection of fundamental rights
Same vetting as for multiple-entry visa holders, fully automated border crossing	√√√√	√	-√	0
Same vetting as for multiple-entry visa holders, semi-automated border crossing	√	√√	-√	0
More thorough vetting, fully automated border crossing	√√√	√√	-√√	--√√
More thorough vetting, semi-automated border crossing	√	√√√	-√√√	--√√

5.4 Policy option 5: Application fee

5.4.1 Fee of 20 EUR (sub-option 5a)

- To facilitate the crossing of EU external borders by third-country nationals √√

As described in section 4.4, this sub-option would allow to neutralise the costs incurred by the RTP as far as the examination of applications is concerned, which is approximately 73,1 million EUR. It would be consistent with the approach chosen for the treatment of visa applications, and also consistent with the fact that a registered traveller is effectively buying an additional service, on which he/she is not dependent in terms of his/her rights to cross the external border of the Schengen area, a service which will only be of interest to a certain category of travellers. From the travellers perspective, the additional cost of 20 EUR (independent application) or 10 EUR (a registered traveller application together with a multiple-entry visa application) is not likely to be considered discouraging in a context where the main target group are persons who travel to the EU several times per year. It is also relatively minor compared to the normal visa fee (60 EUR). There is broad consensus among stakeholders that a fee should be collected from the applicant for participation in the RTP.

5.4.2 No fee (sub-option 5b)

- To facilitate the crossing of EU external borders by third-country nationals √√√

This sub-option would undoubtedly have a bigger impact in attracting as many persons as possible to the programme, also in the sense of making the programme and its benefits known more quickly, as people who hesitate about the benefits would be more willing to "give it a try" if it were free. This impact is however limited, considering that any traveller will be able to observe the use of automated gates when crossing the external border and thus also observe the benefits in terms of shorter queues.

There is a risk that many ineligible applications would be submitted, thus increasing Member States authorities' workload and administrative costs.

5.4.3 Costs (both sub-options)

The cost of examining applications is fully taken into account when assessing the impact of these sub-options. This brings the net cost of sub-option 5a to zero taking into account the revenue from the fee, while the cost for sub-option 5b is equivalent to the full (estimated) cost for examining applications, that is, 73.1 million EUR. Half of the full cost for examining applications (i.e. 36,6 million EUR) would fall on visa authorities and half on border authorities.

Table 4 - Assessment of policy option 5

Sub-options	To facilitate the crossing of EU external borders	To maintain the current level of security	Costs for MSs	Protection of fundamental rights
Application fee 20/10 EUR	√√	-	0	-
No application fee	√√√	-	-√√	-

6. COMPARISON OF OPTIONS AND IDENTIFICATION OF PREFERRED POLICY OPTION

6.1. COMPARISON OF OPTIONS

Table 5 – comparison of policy options

Policy options and sub-options	To facilitate the crossing of EU external borders by third-country nationals	To maintain the current level of security	Costs	Protection of fundamental rights
Option 0 Baseline	0	0	0	0
Option 2 Data stored in a token (2a)	√√√	√√	-√√	-√
Data stored in a centralised database (2b)	√√√√	√√√	-√√	-√√√
Data (unique identifier number) stored in a token and (unique identifier, biometrics and data from application) in a central repository (2c)	√√√	√√√	-√√√	-√
Options 3 and 4*) Same vetting as for multiple-entry visa holders, fully automated border crossing	√√√√	√	-√	0
Same vetting as for multiple-entry visa holders, semi-automated border crossing	√	√√	-√	0
More thorough vetting, fully automated border crossing	√√√	√√	-√√	-√√
More thorough vetting, semi-automated border crossing	√	√√√	-√√√	-√√
Option 5 Application fee 20/10 euro (5a)	√√	-	0	-
No application fee (5b)	√√√	-	-√√√	-

*) the impacts of sub-options with regard to the policy options 3 and 4 (vetting criteria and automation of border control) are directly linked, in the sense that the impact of the sub-options with regard to vetting cannot be assessed without knowing which is the preferred option with regard to automation, and vice versa. Consequently the available four sub-options (3a, 3b, 4a, 4b) from the two policy options have been combined into the four possible variations, and the impact of all four variations is assessed in an integrated way.

Table 5 summarises the assessment of impacts done in chapter 5. The three sub-options of policy option 1 (lodging an application for an RTP) are not included in the table as the best choice is described already in chapter 2.3.1. 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 with the proportionate cost;
- Coherence – the extent to which options are coherent with overarching objectives of EU policy.

Data storage

All three sub-options contribute significantly to the objectives as defined and are notably fully coherent with EU border policy: security and prevention of irregular immigration is not diminished during the border crossing, while the EU's openness to the world and its capacity to facilitate cross-border people-to-people contacts, trade and cultural exchange is boosted. Furthermore, innovation and development of high-tech technology is accelerated. An RTP for all third-country nationals travelling frequently will show the EU's determined ambition to be open for legitimate travel. The programme would be the first in the world which is open to all third countries, and which is operable across several states, in this case across the whole Schengen area. In this context, Europe can be seen as a pacesetter for the rest of the world.

A drawback of all three sub-options is that the benefits are nowadays mainly related to air border crossing points. This is reflected in the data available from the benefits in terms of processing times which are all based on the experiences from airports. However, at land border crossing points that are organised in such a way that passengers are checked outside their vehicles, an ABC system can also be used[56]. Furthermore, at sea borders ABC systems could be easily implemented, especially in cruise and ferry terminals. Some Member States have already planned to do so[57].

The token-based sub-option allows for visibility and limits data protection concerns. The sub-option based on a centralised RTP is more secure and easier to implement in practice at the border crossing point. The latter is, however, counterbalanced by the need to develop a new centralised system in which all the data is available and subject to search.

The sub-option based on a token/central repository can be seen as a hybrid between the above two sub-options, combining their respective advantages. It minimises the use of personal data in an EU system and it avoids the main of the security drawbacks of the token-based system. It provides, however, for the most complicated integration into the border control process as it introduces both a verification of the token as well as a verification against a central repository.

Vetting criteria and automation of border control

The assessment showed that stricter vetting procedure does not have any real impact on the security of the border check itself, and also that the facilitation of border crossings of semi-automated border controls is too limited to bring added value. Furthermore, stricter vetting procedure would increase significantly Member States' administrative costs and would have a significant effect on the protection of fundamental rights. Therefore, stricter vetting criteria

---

[56] Finland has a pilot project running an ABC at the land border crossing point and Norway will launch a pilot.

[57] For example, Portugal has a plan to implement ABC systems at its sea borders.

and semi-automated border control would not be effective and/or efficient. Furthermore, stricter vetting criteria would not be coherent with the EU border policy.

Member States having implemented an ABC system reported that the system is the most cost-effective solution for them as it saves cost in terms of staff, increase throughput capacity of border crossing point and it enables border guards to focus more on the most risky travellers and/or serve other travellers.

Application fee

By introducing a fee of 20 EUR, Member States administrative costs for examining applications would be neutralised. It would also be consistent and coherent with the approach chosen for the treatment of visa applications. However, no fee sub-option would better guarantee large number of participants in the programme. Downside of this option would be that many ineligible applications would be submitted and the cost for visa and border authorities would be 73,1 million EUR.

Costs-benefit analysis

Data storage

The two sub-options on a token-based system and a centralised database are almost equal as concerns total costs, but this hides important differences between them: the token-based system puts effectively all costs on the Member States, as all technical implementation will be done by them.

An important difference between the token-based and the token/central repository sub-options is in the different costs for tokens: in the former case, biometric data needs to be stored on the token, in a secured chip, which brings the cost of one token to 5 EUR. In the latter case, no data other than the unique identifier (application number) needs to be stored on the token, in the form of a barcode, which limits the price to 1 EUR. The cost for tokens would fall on Member States i.e. border and visa authorities.

Most importantly however, the costs for the sub-option with a token/central repository are clearly the highest of all sub-options as can be seen from the table 1.

Automation of border control

The use of ABC is most efficient and cost-effective at those border crossing points where the number of travellers is the highest and where it is most challenging to manage passenger flows. However, there are border crossing points which would not gain any benefits on automation due to the small number of travellers.

An estimate would be that Member States in total would invest in 175 automated gates per year, to gradually expand their capacity for handling travel flows in this way as the number of travellers and also registered travellers increase.

The costs of automation would therefore greatly vary depending on the number of automated gates that would be implemented. Automation of border controls would introduce extra implementation costs for the Member States, but it would also guarantee more efficient management of passenger flows, release border check resources for checking on higher-risk

travellers and/or serve other travellers, and would generate cost savings in the long run due to a reduced need for personnel per million of traveller crossing the border.

As part of the baseline the required resources for border checks today in terms of border guards can be estimated at around 40 000 persons at a salary cost of 1 240 million EUR[58], equivalent to 1,65 EUR per passenger on each entry and exit.

At the moment, it is not possible to calculate the exact benefits of the automation and/or the RTP in quantitative and monetary terms as it would require at least the following information to be available in addition to the number of border crossings and the border crossing time per category of travellers (EU citizens, visa holders and non-visa holders): number of manual and automated lanes and number of registered travellers (visa holders and visa exempted) per border crossing point. However, some very general calculations can be done based on the Member States experiences. Together with automation, the RTP could reduce border control resources needed by around 40 % i.e. in theory 16,000 border guards (equivalent to 500 million EUR/year[59]) who can focus on/serve other travellers and cope with the expected increase of traveller flows. Even if more modest savings were to be the starting point for calculation (i.e. 250 million EUR/year), Member States would have net cost savings (+81 million EUR) already after the second year of operation of the RTP[60].

The release of around 40% of border guards includes the possibility to cope with an increase of 62% of travel flows, which means that 40.000 border guards would be able to check 1.125 million travellers instead of 675 million travellers[61]. With the introduction of the RTP, it would be possible to manage the largest part of the expected increase of 80% of travel flows at the air borders with the current number of personnel.

A further estimate was done in the external cost study where, compared to the costs incurred in the baseline, the need to invest in automated gates would increase Member States' one-time costs by 38 %, but would in the long run reduce their total costs by 64 %.[62]

Based on the general calculations above, the conclusion can be drawn that the personnel and the investment costs for establishing and maintaining the RTP system would be compensated within a reasonable timeframe in the form of a lower unit price per border check and

---

58 This estimate is based upon data from Member States. 18 Member States answered the question "how many border guards/police officers in total are performing border checks at the external border". There are an estimated 700-750 million passengers who enter or exit Member States per annum. In 2006, the average salary in EU-27 was 31 000 euro per year (Eurostat).

59 500 million would be applicable if all Member States would use ABC systems at all their border crossing points.

60 Savings 250 million euro/year – one time costs 207 million euro (the most expensive option; token with repository) – yearly recurring costs 101 million euro – costs of automation 5 million euro= -63 million euro after the first year of operation.
Second year: cost savings 250 million euro – first year -63 million – yearly recurring costs 101 million euro – cost of automation 5 million euro= + 81 million euro.

61 40.000 border guards check per year 675 million travellers (entry and exit). One border guard is therefore able to check 16.875 travellers per year. With the release of 40% only 24.000 border guards are needed to check the flow of 675 million travellers equivalent to 28.125 travellers per border guard per year. Based on this new performance value per border guard, the existing and trained border guards will be able to check yearly a new total of 1.125 million travellers, which is an increase by 62%.

62 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

personnel resources who are able to focus on other tasks and/or cope with the increasing travel flows. .

Risks

As technical failures or breakdowns can always occur with one or another system, 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 return to the existing process i.e. manual border check procedure. This would apply to any situation where the RTP is down with regard to all three sub-options. In this regard the token-based system can be regarded as less risky, in that it does not rely on the functioning of a central component to function.

As with any large scale IT-system, there are always risks with implementation. Therefore, proper implementation of the RTP can only be ensured if all relevant actors fulfil their obligations, respect the lessons learnt from establishing the previous large-scale IT systems and take advantage of the adopted legal basis and the technical possibilities for performing facilitated border checks on registered travellers. 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 RTP 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.

6.2. PREFERRED POLICY OPTION

Lodging an application for an RTP

For **policy option 1** it is clear that allowing the traveller to choose the best place for him/her to lodge an application would guarantee a larger number of participants in the programme, thus helping Member States to manage their passenger flows at the external border crossing points. Therefore, the preferred sub-option is lodging an application for an RTP at any border crossing point and at any Member States consulate. The cost-effectiveness of this sub-option is clearly the best and it is fully coherent with existing border and visa policy.

Data storage

To identify the preferred option with regard to **policy option 2** is more complex as demonstrated in chapter 6.1. The total scoring of each sub-option in relation to policy option 2 is almost equal, but each sub-option displays distinctly different weaknesses: the token-based sub-option displays significant security issues, the central database sub-option displays significant fundamental rights issues, and the token/central repository sub-option significant cost issues. However, the cost benefit analysis shows that even the higher one-time costs and yearly operational costs of the token/central repository sub-option will be fully compensated in the long run by the economic benefits of the RTP as a whole for the Member States. This is

therefore the preferred sub-option with regard to policy option 2. This sub-option provides for a proportionate balance between security, facilitation and data protection. The data stored in a central repository would be available for border guards only when assessing application, renewing/revoking access to the RTP, the token is lost or stolen or any problems occur with facilitating registered travellers' border crossings. While performing border checks a border guard would receive only hit/no hit information. With this option "privacy by design" is implemented.

Vetting criteria and automation of border control

For **policy options 3 and 4** it is clear that the total impact of combining the same vetting criteria as for multiple-entry visas with fully automated border control has the highest impact on facilitating registered travellers' border crossings. Furthermore, it offers a balanced approach to security and protection of fundamental rights. It is also the least expensive approach taking into account the costs associated with stricter vetting procedure and semi-automated border control. Full automation would be a cost-effective tool especially at the busiest border crossing points where capacity problem and queues exist already nowadays.

It should however be noted that the implementation of fully automated border control requires that an Entry/Exit System is developed and implemented in parallel, which would allow for replacing the stamping obligation with an electronic registering of entry and exit dates of all travellers including those having access to the RTP.

Application fee

For **policy option 5** it is reasonable to accompany the RTP with a fee of 20 EUR that would cover the administrative costs of examining applications, which would be set at a level that should not discourage potential applicants. The fee could be reduced to 10 EUR if a multiple-entry visa application and an RTP application are examined at the same time based on the same supporting documents.

Impacts on relations with third countries

There would be positive impacts on relations with third countries as all third-country nationals whether requiring a visa or not could apply for access to the RTP. The RTP would allow moving from a country-centric approach to a person-centric approach in which the country of origin does not play an important role. The main criteria to grant or refuse access to the RTP would be the security risk posed by an individual.

Impacts on other stakeholders such as operators, carriers and other authorities working at the external border

There would not be any direct impacts on other stakeholders. However, positive impacts could be achieved for operators and carriers as the throughput capacity of border crossing point would increase thus giving more flexibility for operators and carriers to plan their actions such as connection flights. This is especially of interest at airport hubs where connection times are often between 30 and 60 minutes as it would offer attractive connections from outside the EU into the Schengen area and vice versa.

Costs of the preferred option

Examining applications

The costs for examining the applications based on the preferred sub-option under the policy option 1 amount to 73.1 million EUR per year for the Member States.

The administrative fee would cover this part of the costs. The total maximum revenue of the administrative fee, which would cover the examination of applications, would be 75 million EUR/year.

Data storage

The estimated total one-time costs of the preferred option of the RTP for the Agency to develop a centralised part would be 43 million EUR, spread out over 3 years and annual average costs for maintenance/operations would be 20 million EUR/annum. The total one-time costs for Member States to develop and set-up their national infrastructures would be 164 million EUR, spread out over 3 years and annual average costs for maintenance/operations would be 81 million EUR/annum. The above-mentioned costs include also administrative costs except the costs for examining applications. These are however only the costs related to the development and running of the system itself. The following elements need to be added to this.

Automation of border control

ABC system costs will vary greatly from one Member State to another. For that reason, the cost cannot be calculated in advance. Member States can choose the border crossing points where they would implement the ABC system. Each Member State would inevitably have to make a precise assessment for each individual border crossing point, whether ABC would bring enough added-value to the throughput capacity of the border crossing point and thus decrease or limit travellers' border crossing time.

Information campaign

To raise awareness with the general public, the information campaign should be organised. The estimated costs for a campaign based on those for the VIS would be 80 000 EUR including video and printed materials such as posters and leaflet. These cost would be covered by the EU budget.

Cost for third countries and other stakeholders such as operators, carriers and other authorities working at the external border

For third countries and other stakeholders, no costs would be incurred due to the implementation of the RTP. After possible adoption of the RTP, third countries and other stakeholders will be informed accordingly of the facilitation mechanism and especially that third-country nationals could apply for access to the RTP.

Financial support

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 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.[63] 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.

Significant cost savings could also be achieved if the RTP is built together with the EES, 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.

Conclusion

In summary, the preferred option consists of

- The lodging of applications at consulates as well as border crossing points;
- The combination of a token and a centralised storage of anonymized biometric data of each applicant and the data from an application. The comprehensive list of data which would need to be stored is in Annex 8;

63 OJ L 286, 1.11.2011, p.1.

- Applying the same vetting criteria as currently defined in EU law for multiple-entry visas;

- Giving registered travellers access to a fully automated border control process;

- Charging a fee of 20 EUR per RT application. However, a reduced fee (10 EUR) would be introduced in cases where a visa application and an RTP application are examined at the same time based on the same supporting documents.

The preferred option should be designed so that it takes into account privileged position of non-EU family members of EU citizens who have a right to obtain a visa and move freely[64]. Furthermore, no entry and/or exit data should be stored in the central repository.

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

- It will significantly facilitate registered travellers' border crossings regardless of whether automation is used. Based on Member States but also other countries experiences, the RTP together with automation can reduce waiting times at the border crossing point by up 70 % - 85 %[65]. Even without automation, registered travellers' border crossing times will be reduced from two minutes to 20 – 40 seconds.

- Based on the very general calculation, it will considerably release border control resources to focus more on higher-risk travellers and/or serve other travellers. Together with automation the RTP could reduce border control resources needed by maximum of 40 % i.e. in theory 16 000 border guards, equivalent to 500 million EUR per year across Member States. The re-affectation of border guards would be very important noting the forecasted increase of travel flows especially at the air borders.

- It will give a tool for Member States to manage increasing passenger flows cost-efficiently using new technologies without decreasing the level of security.

- It will increase the efficiency and effectiveness of border checks and offer flexibility for operators and carriers to organise their tasks and actions.

- It will boost economy and cultural exchange especially at the local level.

- It will show the EU's determination to be open for legitimate travel.

- It will introduce a person-centric approach to border checks.

- It will minimise the potential impact on fundamental rights, notably privacy and data protection. Different sensitive data will be stored separately and any search against the repository at the first line control will not be possible without presenting a token. As regards biometrics, border guards will have only hit/no hit responses at the first line control. Furthermore, a one to many search using biometrics at first line control will be technically impossible.

---

64 OJ L 158/77, 30.4.2004.

65 Border crossing time by using the existing automated system is compared against the time needed for third-country national holding a visa to cross the external border via airport by using the manual booth. At the land borders waiting time can be reduced even more.

6.3. Assessment and considerations of EU added value, proportionality and legislative implications

6.3.1. European value-added and proportionality

The preferred option needs to be implemented at all EU external border crossing points and will have implications on the border guard resources of all Schengen countries. The preferred option ensures that the EU has a common approach to the RTP based on common legislation and thus it guarantees that rules continue to be the same at all Schengen borders. For third-country national travellers, this means that the RTP is available to them at all Schengen border crossing points without separate vetting. In other words, a person vetted by one Member State may benefit from facilitation when crossing the external borders of any other Member State. Without common rules this would not be possible.

In terms of proportionality, an RTP implemented based on the preferred option builds to a large extent on existing processes, investments and technical equipment, including: the same document readers and fingerprint scanners as used/installed today at all Member States' border crossing points, for the purposes of SIS and VIS; the same automated border control gates used/installed today for EU citizens could be used to a large extent also for third-country nationals; use of the same biometric identifiers as for the EU e-passport, for the VIS and for the residence permits (but only fingerprints); the same criteria for access to the RTP as for multiple-entry visa according to current EU legislation; a facilitated check practically identical to the current "minimum check" for EU citizens.

Based on the consultations, the preferred option was clearly supported only by two Member States. Majority of Member States were in favour of a centralised system without giving any statements of the reasons. Although the preferred option is not a preferred option for Member States, it provides for a balanced approach between security, facilitation and data protection as evidenced in this impact assessment. In this respect, the preferred option meets the requirement of proportionality.

A key issue to consider for proportionality is one of costs, as the development of the RTP entails significant costs for the Member States and/or the EU budget. This consideration should take into account that no other measure currently exists that could provide for facilitated border crossings for third-country nationals, that no such alternative exists that could be developed in the future, and that the RTP will allow significant savings for Member States in the medium- to long term. It should also take into account unquantifiable benefits in signalling to third-country nationals, from any third country, that the EU does not consider it necessary to impose a thorough border check for each individual, but is ready to facilitate the border crossings for, potentially, millions of persons; a measure of openness unequalled by any other country in the world.On this basis the preferred option therefore constitutes a proportionate mechanism to deliver on the objectives of facilitating third-country nationals' border crossings across the Schengen area and of countering the lack of tools to manage increasing passenger flows.

6.3.2. Legislative implications

New EU legislation would be required to implement the RTP. Furthermore, the Schengen Borders Code and the Agency regulation would need to be amended.

6.3.3. Measures to ensure data protection and protection of the rights of travellers

It is important that the preferred option fully complies with the relevant legislation on the protection of personal data, in particular the data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data; and that safeguards and mechanisms are in place for the effective protection of the fundamental rights of the individual travellers and in particular the protection of their private life and their personal data. Staff and third-country nationals must be made aware of these rights.

The data would be stored in a form that could be manipulated and there is a potential risk, as with any data of this type, that it could be used inappropriately. According to Article 6 of Directive 95/46/EC Member States shall provide, inter alia, that personal data must be processed fairly and lawfully, and that they are collected for specified, explicit and legitimate purposes. Furthermore, the processing of personal data must be adequate, relevant and not excessive in relation to purposes for which they are collected and processed.

The application of the same data protection provisions as for the VIS and the status quo including the retention of information for a maximum of five years would be necessary to ensure adequate data protection provisions for the preferred option. The personal data stored in the central repository (biometrics and alphanumeric data from applications) should be kept for no longer than is necessary for the purposes of the RTP. It is appropriate to keep the data for a maximum period of five years, in order to enable data on previous applications to be taken into account for the assessment of the subsequent RTP applications, renewal of the access to the RTP and also taking into account the re-use of fingerprints stored in the repository (59 months). Furthermore, a five year retention period would allow granting access to the RTP for five years without a new application. This would be in line with the issuance of a multiple-entry visa for trusted travellers (maximum period 5 years) whose data is kept in the VIS for 5 years. The data should be deleted automatically after the period of five years, unless there are grounds to delete it earlier. Data on refused applications should be kept five years whereas data from inadmissible applications should not be stored in the central repository at all. No personal data is stored in the token but only a unique identifier number (e.g. application number). A new application would need to be submitted to renew this access once the period of validity has expired. In addition, provisions would be necessary to ensure that:

- The data stored[66] is only accessible and used by duly authorised staff of responsible border and visa authorities, as far as necessary for the performance of their tasks. These authorities would also be responsible for correcting and/or deleting the data stored in a repository or in a token (biometrics and alphanumeric data).

- The registered traveller can opt out of the system at any time.

- Individuals are properly informed and have the right to access information held on them. A system for review of the refusal and revocation of membership in the RTP and a review procedure for challenging or correcting potential errors, by recourse to data protection authorities and by judicial review, in accordance with the right to an effective remedy (Article 47(1) of the Charter of Fundamental Rights of the EU) and Directive 95/46/EC

[66] All the data fields listed in Annex 8 would be needed as the vetting criteria would be the same as for multiple-entry visa holders. Furthermore, this would guarantee consistency between the VIS and the RTP and facilitate examination of a visa and a RTP application at the same time.

would have to be laid down. Reasons for refusal and revocation shall be given to the applicant.

- There is no potential issue of discrimination through assuming that travellers who are not registered or accepted by a Member State are suspicious.

- The data processing is to be supervised by the EDPS as far as EU institutions and bodies are involved, and by national data protection authorities, as far as Member States' authorities are involved. This supervision and cooperation between National Supervisory Authorities and the EDPS should be guaranteed and facilitated. Data protection authorities should have the intervention powers necessary to ensure the respect of compliance with data protection rules. The EDPS and the National Supervisory Authority shall ensure that an audit of the personal data processing activities is carried out in accordance with relevant international auditing standards. Access to information and all relevant documents and records shall be given to the EDPS by the Agency and by the Member State for the National Supervisory Authority.

- Data security needs to be ensured to avoid unauthorised access or destruction or alteration of data and security breaches. Moreover, mechanisms to ensure effective monitoring of data processing need to be in place, such as logs of processing operations and access to the system.

Given the large numbers of new travellers affected and the need to process their biometric data the travellers would need to be well informed on the data protection aspects and complaints/appeals mechanisms in line with the right to an effective remedy, with indication of data protection authorities competent to deal with their complaints and requests.

7. MONITORING AND EVALUATION

The Management Authority (the Agency) would ensure that systems are in place to monitor the functioning of the RTP against the main policy objectives. Two years after the RTP is brought into operation and every two years thereafter, the Agency would submit to the European Parliament, the Council and the Commission, a report on the technical functioning of the RTP including the security thereof.

Three years after the RTP is brought into operation and every four years thereafter, the Commission would produce an overall evaluation of the RTP including examining results achieved against objectives, assessing the continuing validity of the underlying rationale, the application of the legal basis for the RTP, the implementation and the collection and use of biometric data, compliance with data protection rules and other fundamental rights, and the organisation of the procedures related to applications. The Commission would submit the reports on the evaluation to the European Parliament and the Council accompanied, where necessary, by appropriate proposals to amend the Regulation establishing the RTP.

Member States should provide the Agency and the Commission with the information necessary to draft the reports referred above. The information should be provided according to the quantitative parametres predefined by the Agency and the Commission respectively. The cost for reporting, monitoring, evaluating and organising periodical data gatherings are included in the Management authority/Member States admininistrative costs in Annexes 10.1 – 10.3.

Examples of monitoring and evaluation indicators:

General objective	**Indicator**
To facilitate the crossing of EU external borders by third-country nationals.	Number of persons in the programme. Time needed for registered travellers to cross an external border. System availability. Number of persons crossing the border using ABC systems.
To maintain the current level of security.	Number of persons whose access to the RTP is revoked or refused. Error rates e.g. false hits, Failure to Enrol Rate (FTE) and False Acceptance Rate (FAR).
Specific and operational objectives	**Indicator**
To promote access to the RTP for certain categories of frequent, pre-vetted third-country nationals.	Number of persons in the programme by category (visa required/visa exempt) and by grounds of access requested (business persons/students/workers etc). Average time of enrolment at the border crossing point and at the consulate.
To ensure protection of registered travellers' fundamental rights, in particular their personal data.	Number of complaints by individuals to the national Supervisory Authority (data protection authority). Error rates e.g. false hits, Failure to Enrol Rate (FTE) and False Acceptance Rate (FAR).
To avoid discrimination between different groups of travellers.	Number of complaints lodged against the authorities on wrong decisions and/or discrimination.
To decrease the time and costs of border crossings for frequent travellers and to increase the throughput capacity of border crossing points. Border checks of registered travellers should not take more than 20-40 seconds on average.	Time needed for registered travellers to cross an external border by using ABC systems/manual lanes. The throughput capacity of border crossing point increased by XX per cent.

To free up border control resources by 25% from checking cross border movements of frequent and pre-vetted travellers and to enable better focus on checking higher risk travellers and/or serve other travellers.	Average time of enrolment at the border crossing point and at the consulate. Border guard resources replaced/made available by the RTP to focus on checking higher risk travellers and/or carrying out other relevant tasks.

Most of this information would be generated automatically (repository and ABC). However, Member States would need to organise information gathering excercises on the time needed for registered travellers to cross an external border, average time of enrolment and border guard resources replaced/made available by the RTP. Furthermore, Member States should keep records on the complaints lodged against them. These information could be gathered from Member States' yearly reports and/or based on samples taken periodically. Periodical samples on the time needed to cross the border and on the enrolment time would need to be taken once per year.

ANNEXES

ANNEX 1

LIST OF ACRONYMS

ABC	Automated Border Control
Agency	Agency for operational management of large-scale IT systems in the area of freedom, security and justice
API	Advanced Passenger Information
BMS	Biometric Matching System
EBF	External Borders Fund
EDPS	European Data Protection Supervisor
ESRIF	European Security and Research Innovation Forum
EES	Entry/Exit System
EURODAC	European Dactyloscopie (EU Fingerprint Database for Identifying Asylum Seekers
Frontex	European Agency for the management of operational cooperation at the external borders of the Member States of the European Union
IAB	Impact Assessment Board
IATA	International Air Transport Association
ISF	Internal Security Fund
MRZ	Machine Readable Zone (of the travel document)
PNR	Passenger Name Record
RTP	Registered Traveller Programme
RTS	Registered Traveller System
SBC	Schengen Borders Code
SIS	Schengen Information System
VIS	Visa Information System

ANNEX 2

COMPLEMENTARY INFORMATION ON PROBLEM DEFINITION

1. Legislative aspects

While EU citizens' and third-country nationals' border crossing lanes are separated and respective border checks differ i.e. thorough checks are normally carried out on third-country nationals and minimum checks on EU citizens and persons enjoying the right of free movement, current rules could be described as "one-size-fits-all" regardless of any differences in risk between different travellers or their frequency of travel. The main reason behind the current approach has been to ensure a consistent and high level of security with regard to all travellers, taking into account that from the perspective of the border guard carrying out the actual checks, virtually all travellers are anonymous, with few if any tools available for the border guard to distinguish between the travellers posing no risk whatsoever (the vast majority) and those that do pose such a risk.

Consequently, all third-country nationals need to go through a manual border check procedure carried out by border authorities which requires time and human resources. In accordance with the Schengen Border Code, at entry, a thorough border check for third-country nationals, in addition to a travel document check, implies a check to determine their purpose of stay, whether they possess sufficient means of subsistence etc, as well as a search in the Schengen Information System (SIS) and in national databases to verify that they are not a threat to public policy, internal security, public health and the international relations of the Schengen States. Furthermore, a search in the Visa Information System (VIS) is obligatory at entry.

Current legislation allows only minor exceptions to the principle of thorough border checks. The Schengen Borders Code regulates the facilitated border checks for Heads of State; aircraft pilots and other crew members; seamen; holders of diplomatic, official or service passports and members of international delegations; and cross-border workers. The Local Border Traffic Regulation concerns facilitated border checks for border residents who provide proof of legitimate reasons to frequently cross an external land border under the local border traffic regime.

As a result, beyond these limited exceptions, the current legal framework does not allow for differentiating between, for example, a traveller coming to Europe for the first time and a traveller arriving for 50th time, having travelled regularly every month for the past years.

2. Technical aspects

The ABC process starts with passport scanning. The traveller inserts the data page of the passport into the passport reader. The reader technically checks the physical security features of the passport, reads the Machine Readable Zone (MRZ) and communicates with the chip in the passport to verify the authenticity of the document. A live facial image (or fingerprints) of the traveller is then compared to the one stored in the chip to verify the identity of the traveller. Random checks are carried out against the SIS and national databases. This process is in principle the same as in the manual border booth but, in this case, is done by a machine. If the match is successful and the travel document is found to be genuine, the automated gate

opens and the traveller can enter the territory of the Member States; if not, the traveller is referred to a manual check. Border authorities monitor the whole process including the matching of the facial image, but they can monitor several gates at once.

Some Member States have implemented a form of RTP for EU citizens. The main difference between this type of RTP and ABC is that a traveller needs to be pre-enrolled before being granted access to the RTP i.e. biometric data should be captured. The automated process at the border is the same with both programmes. However, in a RTP, a traveller's information is often stored in and retrieved from a database or in a token instead of the e-passport.

One Schengen country has a project running at the air border crossing point with a third country giving access to ABC both in the Member State and the third country. For third-country nationals, this programme involves a semi-automated border check to ensure that border guards can comply with the requirements in the Schengen Borders Code including stamping the travel document of the third-country national.

Based on Member States' experiences (but also on those of other countries such as the US), the use of an ABC system can drastically decrease waiting times, increase the throughput capacity of border crossing points and provide an effective tool with which to manage passenger flows. The US conducted a statistical analysis on the effectiveness of the Global Entry pilot programme based on data for 1 575 flights from November 19, 2008 to January 9, 2009. That analysis indicates that "participation in Global Entry may reduce a passenger's waiting time by up to 70 %. It also reduces the variability of waiting time[67]". Equally the Portuguese RAPID system has decreased both the border crossing time and human resources needed for managing passenger flows. RAPID was used between May 2007 and October 2009 by 612 066 travellers which is 18 % of the total amount of border crossings made in Portugal's external air borders by EU citizens and persons enjoying the right of free movement. The biggest group of users were men and travellers aged 26-35 years.

3. Operational and practical aspects

Current travel flows at the EU external border

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 from 31 August to 6 September 2009. Based on the data collected during the above mentioned exercise, 73,5 % of travellers crossing the border are EU citizens or persons enjoying the 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

---

67 The US Federal Register Vol. 74 No. 222, November 19, 2009. US citizens, US nationals, and US permanent residents who are at least 14 years of age are eligible for participation in the Global Entry pilot. On April 23, 2009 citizens of the Netherlands who participate in Privium (Dutch programme) were also accepted in the programme. See also http://www.thetransnational.travel/news.php?cid=international-trusted-traveler-program-permanent.Nov-09.24. "The US Department of Homeland Security estimates that the average customs processing wait time for participants upon their arrival on international flights is seven minutes, a 70 percent reduction compared with non-members-though it varies by airport, airline, time of day and flight origin. Less than 1 percent of Global Entry passengers are waiting longer than 20 minutes compared with approximately 10 percent of all U.S. citizens and lawful permanent residents waiting longer than 20 minutes." The US has several other Trusted Traveller Programmes, for example SENTRI at the land borders and NEXUS together with Canada. The US Customs and Border Protection (CBP) receives about 800 applications a day equivalent to 300 000 per year for its Trusted Traveller Programmes.

million/week).[68] Based on this exercise, in theory 26,5 % would qualify as a potential target group for a RTP.

The number of third-country nationals crossing the border differs significantly among Member States and also among border crossing points. Most of the third-country nationals and also third-country nationals holding visas cross the border via land borders, the next largest number by air borders and the smallest via sea borders. For example, in Finland 58 % of travellers are third-country nationals (52 % of them visa holders), whereas in Slovakia the number is 12 % (9 % of them visa holders). In Lithuania, 55 % of travellers crossing the land borders are visa holders whereas the proportion at some countries' air borders is quite small; 1 % in Luxembourg, 7 % in Portugal and 11 % in France.

Also, the total amount of travellers differs a lot between Member States. During the one week period, over three million travellers crossed the borders in Spain[69] and almost two million in France whereas the figures were only 8 000 in Luxembourg and 36 000 in Malta. Based on the figures above, one cannot estimate for the Schengen area as a whole how many third-country nationals would join a RTP and use it at a certain border crossing point.

Border processing times

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 borders check at first-line (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.

From a practical point of view it should also be noted that at air borders and sea borders the sizes of airplanes[70] and ships are growing and airplane/ship timetables are very tight. On the other hand, at land borders, border checks take longer than at air borders, and they are more complex to manage in instances when individuals arrive in groups at a land border crossing

---

68 Data were collected from all Schengen Member States, Romania, Bulgaria and Cyprus. Final results of the data collection exercise are in Annex 7.

69 Border crossings in Ceuta and Melilla are included.

70 For example, new aircraft types like BOEING Dreamliner and AIRBUS A 380 increase the pressure to manage passenger flows more efficiently at the airports.

point in cars, busses or trains[71]. It should also be noted that at the land border, border guards do not have any advance information on passengers before they arrive at the external border which means that it is not possible to perform any pre-arrival checks on the travellers. Normally this is not the case with other border types[72].

At the largest border crossing points there are often long queues; it can take hours to cross the external border. All passengers, including those who travel frequently and have always complied with all the rules, are negatively affected by the queues. EU citizens' and third-country nationals' border crossing lanes are separated, but this has not and will not solve the problem of queuing.

Given the very large number of border crossings, even small changes in the border crossing time are potentially very significant. However, also many other factors contribute to overall time spent at borders , including: check in times; customs checks; time spent waiting for luggage; air traffic delays and security checks.

Other factors influencing border processing times

Taking the current legislative framework as given and setting aside the use of new technology, possibilities to influence border processing times are very limited. Increasing the number of border guards working at the external border or adding new, traditional lanes and manual border control booths is not a workable solution for both practical and financial reasons as discussed already in the previous impact assessment. At many border crossing points additional traditional lanes and/or manual control booths cannot be added without undertaking extensive construction works; therefore some Member States are already using ABC/semi-automated systems at their external border crossing points.

From an EU perspective it should also be recalled that it is not possible to harmonize all factors influencing border crossing times at the border crossing points (infrastructure, exact border check procedure, number of border guards, use of ABC etc.) through legislation. Border crossing points and their passenger flows can differ significantly. This is also reflected in Article 14 of the Schengen Border Code: *"Member States shall deploy appropriate staff and resources in sufficient numbers to carry out border control at the external borders, in accordance with Articles 6 to 13, in such a way as to ensure an efficient, high and uniform level of control at their external borders"*.[73]

Some survey results

Many people crossing the border are already familiar with e-services and are capable of dealing with different matters without outside assistance. Among the e-services most commonly used are, for example, e-invoices, e-banking, flight check-in via internet or automated kiosk and internet shopping. Also, government services are increasingly provided to citizens online. The general trend is to gradually move towards online and automated

---

71 Cars onboard ferries undergo similar checks as at the land border.

72 For example, Advanced Passenger Information (API) is available at the airports.

73 See also EU Schengen Catalogue on External borders control, Return and Readmission updated version of 19 March 2009. On page 24, the Catalogue refers to the infrastructure at border crossing points (lanes and booths) and number of personnel needed. "Adequate number of officers and border check equipment should be deployed to control passenger flows and respond to actual risk assessment. Adequate number depends inter alia: on constant control of passenger flow, night time, border situation and threat level, available equipment, environment".

services. Taking into account the experiences of Member States having introduced ABC for EU citizens, the interest and readiness of travellers in using new technology can therefore be assumed to be high. Most travellers are willing to use ABC systems as a survey conducted in the UK shows. Based on the survey, around 90 % of UK air travellers support the use of biometric scanning and ABC systems[74]. The Netherlands conducted a survey from 9 May 2011 till 16 May in which a total of 242 of the US participants in the FLUX programme responded. 95 % of respondents considered the programme excellent or good. 82 % will renew their membership and 17 % are considering it. Some of the respondents (20 persons) asked for an expansion of the programme to other European countries. The main reason for joining the programme was a fast border crossing (98 %); not priority parking or availability of a lounge (17 %).

Australian Customs and Border Protection Service launched an independent survey involving face-to-face interviews at several airports during the last ten days of each month from October 2009 to January 2011. By almost all the respondents were generally satisfied with the service provided. More than two thirds of the respondents highlighted that SmartGate was an efficient, prompt and quick option. Over 80 % did not mention any negative aspects when questioned about SmartGate[75].

[74] Survey was conducted in 2006. Misense pilot started in October 2006 at Heathrow airport. UK survey is used as any other Member State has not carried out such a study for their citizens.

[75] See draft report "ABC solutions based on Electronic Machine Readable Travel Documents (eMRTD) in third countries" prepared by Frontex.

ANNEX 3

CURRENT AND PLANNED AUTOMATED BORDER CONTROL SYSTEMS IN THE MEMBER STATES

Country	**Locations**	**Biometrics**
Austria	Vienna airport	Face
Belgium	Brussels airport	Face
Czech Republic	Prague airport	Face
Estonia	Tallinn airport	Face and fingerprints
Finland	Helsinki-Vantaa Airport Vaalimaa land border crossing point	Face
France	Orly airport Paris-Charles-de-Gaulle airport	Fingerprints
Germany	Frankfurt Airport	Face
Netherlands	Schipol airport	Face/iris
Norway	Oslo airport. Plans to expand to the land border crossing points	Face
Portugal	International airports. Plans to expand to the seaports	Face
Spain	Madrid and Barcelona airports	Facie and fingerprints
United Kingdom	Several airports	Face/iris

Furthermore, at least Denmark, Bulgaria, Latvia, Romania and Hungary have preliminary plans to start using ABCs.

FLUX PILOT PROGRAMME

FLUX (Fast Low Risk Universal Crossing) is the official name for the pilot programme between the US and the NL which started on 23 April 2009. FLUX aim is to facilitate and speed up border checks for pre-approved, trusted travellers by providing them with automated processes at the border.

A single, web-based application is submitted simultaneously to both governments by the applicant. All applicants are subject to comprehensive Government background checks, collection of biometric data (Iris in NL and fingerprints in US) and interviews by both countries' officers. Each country conducts its own vetting and only for its own programme. Based on the agreed vetting criteria, several database checks are made but only "green light/red light" information is exchanged. In addition to that, travellers are checked every time when crossing the border against national databases (and the SIS in EU).

FLUX participants become a member of both Global Entry in the US and Privium in the NL. Membership is fee-based and the fee depends on the chosen option i.e. the traveller can choose a higher fee and then use preferential parking, ClubLounge etc.

ANNEX 4

NUMBER OF PARTICIPANTS PARTICIPATING IN SOME PROGRAMMES AND PROCESSING TIMES

Country	**Participants**	**Processing time**	**Note**
Australia and New Zealand- SmartGate	All e-passport holders – 2 million processed/year	38 seconds (17 seconds at the automated gate)	AUS and NZ citizens
Germany - ABG	24 000	10-15 seconds	EU/EEA/CH citizens
Hong Kong – eChannel (all BCPs) and Vehicular eChannel (land)	All Smart Identity Card holders	12 seconds	Hong Kong and Macao citizens/residents + certain frequent visitors
Netherlands - PRIVIUM	46 000	12 seconds	EU/EEA/CH citizens. US citizens via FLUX
Singapore - eIACS	3 million users (70 000 transactions per day)	8-12 seconds	Singapore and Malaysian citizens
Malaysia – Autogate (at air and land border)	300 000	9-12 seconds	Malaysian citizens
United Kingdom - IRIS	250 000	15 seconds	EU/EEA/CH + third-country nationals under certain conditions
United States – Global Entry, NEXUS, SENTRI, and FAST	over 1 million in Global Entry	Depends on the programme	US citizens, US nationals, US lawful permanent residents. For example, Dutch citizens via FLUX.

ANNEX 5

DATABASES AND SYSTEMS AT EU LEVEL

Centralised databases containing alerts on persons and other categories of data for law enforcement and border control purposes 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 Treaty/Prüm Decisions.

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 (Schengen Convention) on the gradual abolition of checks at common borders 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 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. 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 (01.01.2011), 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 and 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[76]:

- names, including aliases;

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

- 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
- 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; and
- The interlinking of alerts.

On 20 December 2006 two Regulations[77] and a Council Decision[78] were adopted on the establishment, operation and use of SIS II.

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[79]. 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. VIS supports the storage, maintenance and retrieval of this information.

The main objectives of the VIS are:

- to facilitate the visa application procedure;

---

77 Regulation (EC) No 1987/2006 and Regulation (EC) No 1986/2006.
78 Council Decision 2007/533/JHA.
79 Council Decision (EC) No 512/2004, 8.6.2004.

- 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);

- 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 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 supply 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, 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 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[80] 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[81]. 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. Fingerprint of these individuals are s deleted when an individual obtains the nationality of one of the Member States.

[80] Council Regulation (EC) No 2725/2000, 11.12.2000 and (EC) 407/2002, 28.2.2002.
[81] Council Regulation (EC) No 343/2003, 18.2.2003.

- Category 2: data of aliens apprehended in connection with irregular crossing of an external border and where not repatriated. Fingerprints of these individuals are sent to the EURODAC 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 illegally 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.

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 (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[82].

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

Prüm Treaty

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 sigificantly lagging behind this deadline in 2011. Considerable implementation progress is now expected in the course of 2012.

In addition to the above, the Treaty contains provisions for the deployment of armed air marshals on intra-Schengen flights, joint police patrols, and entry of armed police forces into another state.

The Prüm Decisions does 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 to databases in the case of DNA and dactyloscopic data. Neither do they authorise the sharing of data on individuals who have been found illegally staying in a Member State or who have remained beyond their authorised length of stay in the Schengen area.

API

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 2004 on 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 Member States 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,
- code 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 Member States 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[83].

[83] SEC(2011) 132 final and SEC(2011) 133 final, 2.2.2011.

ANNEX 6

EXISTING SYSTEMS LINK TO THE RTP AND MANAGEMENT OF THE 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 MRZ 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.

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 RTP. Furthermore, ABC systems already implemented at the border may be used in the future for automation of third-country nationals´ border crossings through the integration of fingerprint readers. In some ABC systems fingerprint readers already exist.

With the RTP 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 Directorate HOME of the Commission with the support of DG DIGIT in the case of EURODAC[84]. 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.

---

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

The Agency Regulation was published in the Official Journal[85] and entered into force on 21 November 2011. The Agency will become fully operational on 1 December 2012. The selection procedure of its staff has started.

The Agency is funded from the general budget of the European Union. The budget foreseen for start-up activities of the Agency between 2011 and 2013 is 94,5 million EUR. 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. This amount is covered by the financial framework 2007-2013.

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.

A RTP, whether fully centralised or based on a token/central repository, 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. For a token based system, the same standards could be used as for residence permits to guarantee that the information stored in a token could be used across Schengen States, and existing equipment installed at the borders and at the consulates could be exploited. A token based system would be developed by the Member States based on the standards mentioned above. A legal basis for the RTP needs to be adopted prior to any technical development.

[85] OJ L 286, 1.11.2011.

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

ANNEX 8

DATA TO BE STORED

The following alphanumeric data and biometrics would be stored either in a token or in a centralised database or in a Member States' national database to guarantee that border and visa authorities can always verify whether the person really is a registered traveller and whether (s)he still fulfils the requirements of the programme. For example, if the registered traveller does not have sufficient means of subsistence, the data in a token/central database/national database/central repository confirms that there is a person liable to pay applicant's subsistence costs during the stay.

1. the unique application number (unique identifier);

2. status information, indicating that access to the RTP has been requested;

3. the authority with which the application has been lodged, including its location;

4. the following data to be taken from the application form:

   (a) surname(s); first name(s); date of birth, place of birth, nationality(ies); country of birth and gender;

   (b) type, number (and in case of a fully centralised system three letter code of the issuing country) of the travel document(s), the authority which issued it and the date of issue and of expiry;

   (c) place and date of the application;

   (d) if applicable, details of the person liable to pay the applicant's subsistence costs during the stay, being:

      (i) in the case of a natural person, the surname and first name, address of the person and telephone number;

      (ii) in the case of a company or other organisation, the name and address of the company/other organisation, surname and first name of the contact person in that company/organisation and telephone number;

   (e) main purposes of the journeys;

   (f) the applicant's home address,

   (g) the applicant's telephone number and e-mail address, if available;

   (h) if applicable, the visa sticker number;

   (i) if applicable, the residence permit number (and in the case of a fully centralised system the three letter code of the issuing country) ;

(j) in the case of minors, surname(s) and first name(s) of the applicant's parental authority or legal guardian,

5. fingerprints.

ANNEX 9

VETTING CRITERIA[86]

In the examination of an application, visa or border authorities should verify that the following entry conditions are fulfilled:

(a) the applicant does not present a risk of illegal immigration or a risk to the security of the Member States and the applicant intends to leave the territory of the Member States in due time;

(b) the applicant's travel document, visa or residence permit presented, if applicable, are valid and not false, counterfeited or forged;

(c) the applicant proves the need for or justifies the intention to travel frequently and/or regularly;

(d) the applicant has not previously exceeded the maximum duration of authorised stay in the territory of the Member States and he/she proves his/her reliability, in particular a genuine intention to leave the territory in due time;

(e) the applicant's justification of the purpose and conditions of the intended stays,

(f) the applicant proves his/her financial situation in the country of origin or residence and possesses sufficient means of subsistence both for the duration of the intended stay(s) and for the return to his/her country of origin or residence, or he/she is in a position to acquire such means lawfully;

(g) the applicant is not a person for whom an alert has been issued in the Schengen Information System (SIS);

(h) the applicant is not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States, in particular where no alert has been issued in Member States' national databases on the same grounds.

[86] Vetting for family members of citizens of the Union shall be done by using the same criteria as used when examining their visa applications (OJ L 158, 30.4.2004 and OJ L 243, 15.9.2009).

ANNEX 10

TOTAL COSTS

1. Cost Assessments

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

An external contractor carried out the cost study in 2010[87], which 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 to the one-time costs for the development and to the yearly operational 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 in line with ongoing discussions internally and with Member States.

2. Methodology

The cost analysis study began by defining detailed scenarios and border-related specifications. Member States were involved in the preparation of the definition of the parameters in the cost study[88]. 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 registered travellers' 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

---

87 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

88 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.

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 Member States[89]) were used:

- Development of three years and five years of operation.

- Both the EES and the RTP should, as far as possible, take advantage of the existing and fully rolled out the VIS and the SIS.

[89] The parameters and the values used can be found in the final report of the cost analysis prepared by the external contractor..

- Maintenance rate of hardware (8 %) and software (20 %).
- Hourly rates for contractors, management authority staff and EU (27) and Schengen associated country staff, working hours per year.
- Costs for the token 1 EUR (without biometrics).
- For the network costs, the costs of the sTESTA network for the VIS were used.

Registered Traveller Programme

For the RTP, the following core parameters were used for the sizing of the system:

RTS Parameter		2013	2014	2015	2016	2017	2018	2019	2020
Yearly Registrations	(million)	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
Registered traveller IN	(million)	30	60	90	120	150	150	150	150
Registered traveller OUT	(million)	30	60	90	120	150	150	150	150
Applications Consular Posts	(million)	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8
Applications at external BCP	(million)	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3
BCP Enrolments	(%)	45%	45%	45%	45%	45%	45%	45%	45%
Percentage of revocations/extensions	(%)	5%	5%	5%	5%	5%	5%	5%	5%
Average number or Rregistered travellers travels per yr	(n)	6	6	6	6	6	6	6	6

The cost per hour is based on a weighted average of the cost in EU27 administrations and the cost in Associated countries and has been rounded.[90]

The amount of human resources released by the RTP at the external borders is not taken into account due to the fact that it cannot be exactly calculated nor estimated. It varies a lot between Member States and indeed between individual border crossing points. In the longer term, Member States will have net cost savings especially if Automated Border Control Systems are used at the busiest border crossing points. Immediately after the start of operations of the RTP, the real administrative burden for border authorities will be positive. In the consulates the administrative cost will be real, as acceptance of applications will not release any human resources there. On the other hand, an application for a multiple-entry visa

[90] Average employment costs in the associated countries public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (32 EUR in 2005). The 2005 figure has been increased by 5 % (= 34 EUR). Average employment costs in the EU-27 public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (20,35 EUR in 2005). The 2005 figure has been increased by 5 % (= 22 EUR) based on Eurostat statistics "Unit labour Cost – Annual data". http://epp.Eurostat.ec.Europa.eu/portal/page/portal/national_accounts/data/database.
Average employment costs in the European Commission is 122 000 EUR per year equivalent to 74 EUR per hour (220 working days, 7,5 hour/day).

and an application for RTP can be processed at the same time which will diminish the amount of extra work.

ANNEX 10.1

EU Cost Model: **Token-Based RTP**		Yearly operational costs	Total one time development costs	
No			European Union (EU)	Member States (MS)
1	**Management Authority**			
2	Management Authority Hardware			
3	Management Authority Other (training, meetings)			
4	Management Authority Infrastructure			
5	Management Authority software			
6	Management Authority Admin			
7	Management Authority Office Space			
8	Management Authority Contractor Development			
9	**Subtotal MA**			
10				
11	**Member States *)**			
12	Member States Hardware	32.000		23.094.000
13	Member States Other (training, meetings)	273.916		2.739.162
14	Member States Infrastructure	-		-
15	Member States software	978.200		41.874.100
16	Member States Admin	53.450.881		40.205.855
17	Member States Office Space	14.541.600		35.385.840
18	Member States Contractor Development	811.725		8.117.246
19	Costs of tokens	25.000.000		
20	**Subtotal MS**	**95.088.322**		**151.416.203**

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

ANNEX 10.2

EU Cost Model: **Centralised RTP**		Yearly operational costs	Total one time development costs	
No			European Union (EU)	Member States (MS)
1	**Management Authority**			
2	Management Authority Hardware	1.032.000	4.152.000	
3	Management Authority Other (training, meetings)	502.145	502.145	
4	Management Authority Infrastructure	8.041.965	9.248.260	
5	Management Authority software	4.748.000	19.250.000	
6	Management Authority Admin	2.960.641	1.311.734	
7	Management Authority Office Space	9.000	27.000	
8	Management Authority Contractor Development	311.811	3.118.105	
9	**Subtotal MA**	**17.605.562**	**37.609.244**	
10				
11	**Member States**			
12	Member States Hardware	24.000		23.094.000
13	Member States Other (training, meetings)	285.756		2.857.555
14	Member States Infrastructure	-		-
15	Member States software	1.878.200		41.874.100
16	Member States Admin	58.906.097		40.375.430
17	Member States Office Space	14.541.600		35.385.840
18	Member States Contractor Development	845.876		8.458.763
19	**Subtotal MS**	**76.481.529**		**152.045.688**

ANNEX 10.3

EU Cost Model:				
Token together with central repository		Yearly operational costs	Total one time development costs	
No			European Union (EU)	Member States (MS)
1	**Management Authority**			
2	Management Authority Hardware	1.032.000	7.474.000	
3	Management Authority Other (training, meetings)	502.145	502.145	
4	Management Authority Infrastructure	8.041.965	9.248.260	
5	Management Authority software	8.398.000	19.250.000	
6	Management Authority Admin	1.960.641	2.658.448	
7	Management Authority Office Space	9.000	27.000	
8	Management Authority Contractor Development	372.801	3.728.008	
9	**Subtotal MA**	**20.316.552**	**42.887.861**	
10				
11	**Member States**			
12	Member States Hardware	24.000		23.094.000
13	Member States Other (training, meetings)	285.756		2.857.555
14	Member States Infrastructure	-		-
15	Member States software	1.878.200		41.874.100
16	Member States Admin	58.106.097		53.830.027
17	Member States Office Space	14.541.600		35.385.840
18	Member States Contractor Development	845.876		7.417.173
19	Costs of tokens	5.000.000		
20	**Subtotal MS**	**80.681.529**		**164.458.695**

ANNEX 10.4 – Administrative costs

The Agency's administrative costs correspond to the categories 3 and 6 of the total one time development cost (EU) in Annexes 10.1-10.3. and to the same categories of total yearly operational costs (EU).

Member States' administrative costs correspond to the categories 13 and 16 of the total one time development cost (MS) in Annexes 10.1-10.3. and to the same categories of the total yearly operational costs (MS).

Policy option 1

- Administrative costs for Member States

The administrative costs related to the **examination of applications** which are not included in the Annexes 10.1. – 10.3. will be tangible. It is estimated that 5 million third-country nationals would apply for access to the RTP each year. Examination of one application would last 45 minutes, on average[91], including checking the supporting documents, capturing biometric data and conducting interviews, if applicable. In the abstract, the total time needed for examining and granting/refusing access to the RTP would be 2,81 million hours equivalent to 73,1 million EUR or 1 705 persons[92] across Member States. This cost is equal for both sub-options 1a (applications lodged at the border) and 1b (applications lodged at the consulates), and would therefore be borne entirely by either the border crossing points or the consulates. However, these costs would be covered by the fee (20 or 10 EUR).

In sub-option 1c - allowing the lodging of applications at the border crossing points as well as at the consulates – these costs, and the need for extra staff, would have to be borne roughly equally by the consulates and the border crossing points.

Policy option 2

- Administrative cost for the Agency:

Administrative costs for the Agency caused by a **centralised system** would be approximately 1,8[93] million EUR for establishing the system and 3,5 million EUR for the annual maintenance/operating the system.

Administrative costs for the Agency caused by a **token/repository system** would be around 3,2 million EUR for establishing the system and 2,7 million for the annual maintenance/operating the system.

- Administrative cost for Member States:

---

91 Based on the three Member States answers the examination of a (multiple-entry) visa application lasts on average 45 minutes. This time includes capturing the biometric data. The procedures with a RTP application and a visa application are almost the same.

92 Assuming that one person works 7,5 hour/day and 220 days in a year.

93 See Annex 10.2. The 1,8 million corresponds to the summary of Management Authority total one time costs in categories 3 and 6. The same calculation rule is applicable for all the options and for yearly recurring costs.

Administrative costs for Member States created by a **token-based system** would be approximately 43[94] million EUR for establishing the system and 54 million EUR[95] for the annual maintenance/operating the system.

Administrative costs for Member States arising from the development of a **centralised system** would be approximately 43 million EUR for establishing the system and 59 million EUR for the annual maintenance/operating of the system[96].

Administrative costs for Member States arising from the development of a **token/repository system** would be approximately 57 million EUR for establishing the system and 58 million EUR for the annual maintenance/operating of the system.

Policy options 3 and 4

- Administrative cost for the Member States:

With stricter **vetting procedure** all Member States would face a noticeable extra workload with these checks. One could estimate that a compulsory consultation would require 1 million background checks per each Member States per year. To check one person would take approximately 15 minutes (database checks, supporting documents etc) equivalent to 250 000 hours per Member States and 7 million hours around the EU per year. This would be equivalent to 182 million EUR.

94 See Annex 10.1. The 43 million corresponds to the summary of MS total one time costs in categories 13 and 16. The same calculation rule is applicable for all the options and for yearly recurring costs.

95 See Annex 10.1. The 54 million corresponds to the summary of MS total yearly recurring costs in categories 13 and 16. The same calculation rule is applicable for all the options.

96 See Annex 10.2.