EUROPEAN
COMMISSION

Brussels, 6.4.2016
SWD(2016) 115 final

PART 2/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Annexes to the Impact Assessment report on the introduction of an Entry Exit System

Accompanying the document

Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

and

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/xxx as regards the use of the Entry/Exit System (EES)

{COM(2016) 194 final}
{COM(2016) 196 final}
{SWD(2016) 116 final}

Table of Contents

1. ANNEX 1: PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Identification

Lead DG is Directorate General of Home Affairs and Immigration (DG HOME).

The agenda planning reference is 2016/HOME/001

1.2. Organisation and Timing

The Impact Assessment Steering Group was composed of: Secretariat General (SG unit E1), DG HOME (B3, A2), DG JUST (C3 and C1), Legal Service (SJ); DIGIT (B6); GROW (I4), DG BUDG (A3), JRC, and TAXUD (A1).

Chronology of events prior to the Impact Assessment

This chronology does not show all intermediate steps in working groups. Its purpose is only to help the reader of the Impact Assessment understand that the current document builds on a previous proposal and preparation work leading to a new proposal.

February 2013	Commission adopts Smart Borders package (called "2013 Proposal") consisting of: (1) a Regulation for an Entry/Exit System (EES) (2) a Regulation for a Registered Traveller Programme (RTP) (3) a Regulation amending the Schengen Borders Code in order to take into account the existence of the EES and RTP.
March 2013 till February 2014	First reading in working groups of Council and Parliament.
February 2014	Commission initiates with the support of both co-legislators a so-called 'proof of concept' exercise consisting of two stages: (1) A Commission-led Technical Study on Smart Borders (hereinafter 'the Technical Study') and, (2) A testing phase led by eu-LISA on a limited set of technical options.
February till October 2014	Execution of the Technical Study (published in October 2014).[1]
3 December 2014	Commission announces that modified proposals will be submitted early 2016.
19 December 2014	Terms of Reference of Pilot Project defined by Commission.

[1] Technical Study on Smart Borders, European Commission, DG HOME, 2014.

23-24 February 2015	Interparliamentary Committee meeting on Smart Borders organised by the European Parliament with national parliaments and participation by Commission including Commissioner D. Avromopoulos.
30 June 2015	Publication of the Inception Impact Assessment. No comments were received on this document.
29 July till 29 October 2015	Public consultation on Smart Borders
January till November 2015	Execution of testing phase by eu-LISA (report published in November 2015, hereinafter 'The Pilot')[2] including site visits.
January till December 2015	Further discussion on a set of issues identified in the first reading of the "2013 Proposal" in the Council working group (Frontier's Working Party) and the LIBE Committee (committee of European Parliament dealing with Smart Borders).
September till October 2015	Meeting with technical experts from Member States on 24 September and 26 October 2015.
January till December 2015	As part of the preparation of a new legislative proposal, Commission conducts a set of informal meetings: (1) Meeting with Civil Society on 5 May 2015, (2) Meeting with Carriers on 28 May 2015, (3) Meeting with Law Enforcement Services from Member States on 13 July 2015, (4) Meeting with Fundamental Rights Agency on 22 June and 23 July 2015, (5) Workshops with European Data Protection Supervisor (EDPS) on 20 March and 21 September 2015.

Chronology of the Impact Assessment (IA):

This chronology only includes the steps related to formalising and completing the IA

Public consultation	12 weeks from 29 July until 29 October 2015, then extended till 31 October

[2] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_report_on_the_technical_conclusions_en.pdf.

First meeting of Impact Assessment Steering Group (discussion and comments on a first draft Impact Assessment)	4 November 2015
Written consultation of the Impact Assessment Steering Group on the draft Impact Assessment	14 December 2015
Meeting of the Impact Assessment Regulatory Scrutiny Board	20 January 2016

On 22 January 2016, the Impact Assessment Regulatory Scrutiny Board gave an overall positive opinion on the Impact Assessment and recommended the following points to be clarified under section B of its document:

Points to be clarified	**How comments were implemented**
1) How does this initiative relate (or not) to the refugee crisis and to the terrorists threat? What are the technical and practical problems identified in relation to the 2013 proposal which are being addressed by this initiative? What border management systems exist in third countries and what lessons can be learnt?	Sections 1.3. Changed context, 1.4.Revised proposal, 2.2. Implementation problems addressed by this impact assessment, 2.3. The drivers of the problems 2.5. Experiences with EES and RTP in third countries were added or redrafted.
2) How do the policy objectives address the outstanding technical/practical problems related to the entry/exit system? Why is access for law enforcement considered as a "secondary" objective	Section 4.1. General policy objectives reworded.
3) How would the entry/exit system work in practice and how would it fit into the context of other border management and security systems (e.g. VIS, Eurodac, etc.) and would these systems together cover all border crossings by third country nationals?	Introduction and chapter 1 redrafted Annexes 3 (Practical implications of the initiative for the affected parties) and 8 (New Smart Border processes at border crossing points) are better referenced.

The positive opinion included under section (C) the main recommendations for improvement and under section (D) the improvements on presentation.

Recommendations for improvement	**Way it was addressed**
(1) Clarify the policy context and the problems addressed	Introduction and chapter 1 redrafted
(2) Clarify/update the policy objectives	Sections 4.1 and 4.2 amended.

(3) Clarify the policy options.	Introduction and chapter 1 redrafted.
Procedure and presentation The option description should be clearly separated from the impact analysis, and the report should be simplified by removing duplications. Furthermore, the report should be clarified by avoiding acronyms as far as possible and explaining used acronyms at their first appearance	Abbreviations explained, List of Abbreviations and Glossary added, option description shortened and comparisons of options moved to chapter 7.

In addition specific questions sent were addressed by editing the document. The list above is not exhaustive for all the changes made.

1.3. Consultation and expertise

Use of external expertise

External expertise was used during the Technical Study:

- The consulting firm PwC was used for its expertise on analysing the technical issues (data and architecture), collecting statistical data and developing a new cost model for estimating the cost of the EES/RTP system. There was no expertise available as such on the contents and the way to perform the border control process as this would anyhow remain unchanged and compliant with the Schengen Border Code.
- During this study, the expertise from the Research and Development Unit of Frontex was used for the development and running of a simulation model assessing the impact of additional checks implied by Smart Borders on traveller's waiting time at border crossing points (expressed as "service level" and "dwelling time") and on the workload for border guards.
- Eu-LISA was associated to the study in order to understand the technical options that would be part of the Pilot phase they would have to conduct, and to collect relevant information on current systems operated by the Agency (resources required, best technical options, cost elements).

The Pilot was conducted by eu-LISA.

No external expertise was used during the Impact Assessment itself.

2. ANNEX 2: STAKEHOLDER CONSULTATION

2.1. Consultation Strategy

In line with the Commission's minimum standards regarding participation and openness to stakeholders' views presented in the Better Regulation Guidelines[3], a consultation strategy has been developed to ensure a wide participation throughout the policy cycle of this initiative.

The strategy consisted in making sure all parties affected by the implementation of the Entry-Exit System would be consulted at least by the Public Consultation and the most affected parties (citizens, border guards) by another specific feed-back mechanism. Finally, a specific consultation was aimed for Law Enforcement authorities. The table below shows how the consultations were organised or the benefit taken from the one organised by the European Parliament.

<table>
<tr><th></th><th colspan="5">Type of Consultation</th></tr>
<tr><th></th><th>Public Consultation</th><th>Meeting of EP with national Parliaments</th><th>Specific Stakeholder consultation</th><th>Pilot test case feed-back</th><th>Survey from FRA[4]</th></tr>
<tr><td>EU citizens</td><td rowspan="2">Specific questionnaire for individuals + Questionnaire for associations</td><td rowspan="2">European Parliament (EP) + National Parliaments representing EU citizens.</td><td rowspan="2">Specific consultation</td><td>-</td><td>-</td></tr>
<tr><td>Third-country nationals</td><td>Specific feed-back requested</td><td>Survey targeted this group</td></tr>
<tr><td>Border guards</td><td rowspan="3">Specific questionnaire for Authorities</td><td>Specific session in the meeting</td><td>-</td><td>Specific feed-back requested</td><td>-</td></tr>
<tr><td>Law enforcement authorities</td><td>Specific session during the meeting</td><td>Specific consultation</td><td>-</td><td>-</td></tr>
<tr><td>Authorities (in the generic sense)</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Carriers and operators of infrastructure (airports, ports)</td><td>Specific questionnaire</td><td>-</td><td>Specific consultation</td><td>-</td><td>-</td></tr>
<tr><td>Industry</td><td>Questionnaire for associations includes industry</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
</table>

[3] SWD(2015) 111

[4] FRA stands here for Fundamental Rights Agency

	associations				

By these extensive consultations on top of the regular meetings with the working parties of the co-legislators[5], the Commission has sought a wide and balanced range of views on issues covered by the Regulation by giving the opportunity to all relevant parties to express their opinions.

Results are reported as follows:

– The report of the public consultation is published on the Commission website and is summarised in section 2.2 and included in section 2.6.

– The outcome of the meeting of EP with national Parliaments is in section 2.3.

– The result of the specific stakeholder consultations is summarised in section 2.4 and takes also the feed-back from the Pilot into account.

– The executive summary of the survey from FRA is included as annex to the report of the Smart Borders pilot but some facts and figures are included in section 2.5.

2.2. Public consultation

The public consultation was launched on 29 July on a dedicated Commission website and was available during 12 weeks until 29 October 2015. The objectives of the public consultation were:

- to collect views and opinions on the policy options, their likely impact and hence testing existing ideas and options with all stakeholders and the general public;
- to gather new ideas and general relevant knowledge and
- to test existing ideas and analysis.

A total of 101 participants have provided answers to the questionnaire, in the following categories:

- 62 individuals, out of which 9 were non EU citizens
- 14 organizations (NGOs as well as industry representatives)
- 14 public authorities, all from EU countries
- 11 'carriers' (airlines, ferries, buses as well as airports or seaports operators)

The questionnaire was divided in chapters corresponding to sets of options identified in the road map and analysed in the impact assessment.

[5] Smart Borders was a regular agenda item of the Frontier's Working Party (Council) and the LIBE Committee (European Parliament).

Biometrics

Participants have been requested to indicate their preferred option as biometric identifier: fingerprints (FP), facial image (FI), the combination of fingerprints and facial image or no biometric identifier

- 42 % of individuals have indicated that there should be no biometric identifier. 58 % of individuals have indicated that a biometric identifier should be used with a preference for the combination of FI and FP.

- 8 out of 14 organizations have indicated that there should be no biometric identifier. 6 out of 14 preferred the combination of FP and FI.

- Public authorities have favoured the combined use of FI and FP.

- 7 out of 11 carriers supported the use of biometric data, with a clear preference for the use of FI alone or in combination with FP. The need to use a biometric identifier was rejected by 4 out of 11.

Facilitation

The need for a process to accelerate border crossings was first addressed. In a second step, the participants had to answer questions on the different options for facilitation as well as their respective consequences.

There is a clear majority of respondents in favour of general facilitation of border crossings, as compared to more selective RTP type programmes. The use of alternative process accelerators such as self-service kiosks is largely supported.

Data retention

The participants had the choice between a 180 day retention period and a longer retention period (no duration specified in the questionnaire).

- Nearly half of the individuals are in favour of a data retention period of maximum 180 days while one third considers that the data retention period should be longer.

- Organisations are equally distributed.

- Public authorities are in favour of a longer data retention period.

- The majority of carriers are in favour of a longer data retention period.

Law Enforcement Access

The participants had the choice between authorising and refusing the access to EES data for law enforcement purpose.

The Public Authorities are in favour of the access to EES data for law enforcement purposes, while for the three other categories replies are equally distributed on the two possibilities.

2.3. Meeting of the European Parliament with national Parliaments

What was done. The European Parliament consulted the EU national Parliaments on the basis of the "2013 Smart Borders proposal" and LIBE held an interparliamentary committee meeting with representatives of national Parliaments on the Smart Borders from 23 till 26 February 2015. At that moment in time, the Technical Study was available and the Pilot was defined but no test cases were yet on-going.

The opinions expressed by the national Parliaments. Only seven national Parliaments (BE, CZ, ES, PT, RO, SL, RO, UK) replied with an opinion on the "2013 proposal". The national Parliaments are supportive to the idea of the introduction of an EES system, there are some doubts on the need of the RTP (CZ) and both the use of biometrics from the start and the access to EES by Law Enforcement Authorities is considered necessary from the beginning. The remaining most often cited concern is about the cost of the system (BE).

The opinions expressed during the meeting at the European Parliament (23 to 26 February 2015). During the debate Members of national Parliaments and the EP stressed the need to be clear on the purpose of the new systems (borders management and fight against irregular migration/secondary security purposes), maximise the use of existing instruments and a strictly respected budget. A large majority expressed their support for the proposal and the inclusion of the law enforcement element. In its conclusions, the EP Rapporteur for the EES called for a clearer definition of the EES's objective, with the improvement of passenger traffic as primary objective and security/access to law enforcement authorities as secondary objective. He pointed to the need to take into account the experience gained with VIS, to guarantee a robust data protection system in the respect of existing case-law and to ensure the interoperability with existing systems. The EP Rapporteur for the RTP, explained that the biggest concerns were on proportionality and costs, and reminded that the original objective is travel facilitation and increased attractiveness for the EU.

Whether/how comments were taken into account: The comments from the EP and national Parliaments have been addressed with the new proposal: primary and secondary objectives for EES are defined, the architecture of the EES/RTP has been simplified first by building both parts as one single system and later on by removing the need for a specific RTP component, costs have been reviewed and are substantially lower than in the 2013 proposal, benefits have been estimated in the Impact Assessment and show that the investment is justified, the Pilot results have validated operational solutions and in particular the use of four fingerprints and the facial image as biometric identifiers rather than ten fingerprints. The impact assessment contains a thorough impact assessment on fundamental rights of which the right to privacy is part of. Finally access by law enforcement authorities is granted from the beginning but under a set of conditions.

2.4. Stakeholder Consultations

2.4.1. EU-citizens and Third Country Nationals

What was done. The informal meeting on 5 May 2015 was attended by nine non-governmental organisations. The public consultation was responded by 62 citizens (nine of them being third country nationals) plus 14 non-governmental organisations. The feed-back during the pilot was done by travellers actually passing a border control implementing the features of a border control as he/she would experience them. The pilot

received the feed-back of about 50% of the 58.000 travellers who participated. The FRA survey interviewed 1.234 randomly selected third country nationals (see section 2.5).

The opinions expressed. At the informal meeting, organisations essentially asked questions for understanding the proposal contents and also expressed their concerns that refugees and asylum seekers could be flagged as overstayers.

The public consultation shows a 50/50 split between those in favour or not of using biometric identifiers, of 5 years (or more) data retention periods and Law Enforcement Access (LEA). There is essentially an expectation of more justification and guarantees on independent control of the use of data and the right of redress.

The feed-back of travellers participating in the pilot was for a large majority very positive on the way border crossings would be done. The border crossing situations involving an enrolment/verification of biometrics achieved very high satisfaction rates (more than 80%). Where the satisfaction was lower it was related to equipment/technology problems resulting in a slow-down of the border crossing.

Whether/how comments were taken into account. The scope of the 2013 proposal remains unchanged: no residence permit holders are included, neither refugees nor asylum seekers.

The new proposal builds on the positive experience of the use of biometrics in VIS in particular and giving LEA in specific conditions. The justification is part of this Impact Assessment. The new proposal maintains all the positive measures contained in the 2013 proposal on the control of the use of data and on the right of redress.

2.4.2. Border guards

What was done. The opinion of border guards was collected during the pilot and at the occasion of a debriefing session at the end of the test case. In total the feed-back was collected from approximately 200 border guards split over the 12 test locations.

Opinion expressed. Feed-back of border guards is to a large extent unfavourable in the test cases where 8 or 10 fingerprints have to be collected. Feed-back was otherwise positive in the other test cases. The use of biometrics is viewed favourably provided the tools were user-friendly and reliable. Border guards had further suggestions for improving the traveller's flow or the ergonomics of the way the border post was set up as the time-scale for the pilot did not allow to introduce significant changes to existing premises.

Whether/how comments were taken into account: The proposal uses biometric identifiers that minimise the personal data and biometrics to be captured to comply with the principle of data protection by design. This principle at the same time concurs with the expectation from border guards to avoid capturing 8 or 10 fingerprints. The current proposal further assumes that user-friendly and reliable equipment is purchased and the cost/benefit computation includes significant amounts for equipment purchases.

2.4.3. Law Enforcement authorities

The informal meeting on 13 July 2015 was attended by delegates from 25 Schengen countries. None of these authorities answered the public consultation.

Opinion expressed. Law enforcement services (LES) are essentially in favour of having 10 fingerprints as biometric identifiers, having border guards recording additional information in EES than the data from the travel document, and having a data retention that "would be sufficiently long" given the duration between the moment a crime occurs and investigations are conducted on its circumstances. This duration would however not be longer than five years. LES themselves acknowledge the fact that access to personal data had to be justified on a case by case basis.

Whether/how comments were taken into account: As LEA is a secondary objective in the new proposal it cannot justify additional requirements on EES. Anyhow the pilot project showed that taking ten fingerprints at the border for all third country nationals is not feasible. For border control purposes there is no need and no time for collecting additional data than the ones on the passport. The data retention period to facilitate border control is however long enough (5 years) to meet the expectation from LES.

2.4.4. Authorities (in the generic sense)

MS authorities are consulted as part of the usual decision making process on legal proposals. However some authorities, essentially local ones, used the widely advertised public consultation to express their opinion.

Opinions expressed. On biometrics, the majority of authorities were in favour of using two biometric identifiers, as doing so reduces risk. Authorities also favour the existence of provisions that facilitate border crossing. Some of the opinions were expressed by authorities from regions where part of the economy rests on trade with neighbouring non-Schengen countries. Therefore, there is an expectation for having strong controls (security) but without creating a burden on travellers. The need to have a longer data retention period is understood. However it is unclear whether this longer duration is proposed in order to meet expectations of law enforcement authorities or to facilitate the process.

Whether/how comments were taken into account: The preferred solution meets the opinions expressed by local authorities although a longer data retention period is justified for other reasons than those expressed in the respondents' answers.

2.4.5. Carriers and operators of transport infrastructures

The informal meeting on 28 May 2015 was attended by seven organisations. Public consultation responded by 11 carriers and operators of transport infrastructures.

Opinion expressed. At the informal meeting carriers also essentially asked questions to understand the proposal. The public consultations showed a strong support for the use of biometrics and measures aimed at facilitating border control. Carriers and transport operators were the only group of stakeholders that made the link between a longer data retention period and facilitation of the process for a larger group of travellers. The majority of carriers consider that it is unfair that they are responsible for taking back travellers refused at the border.

Whether/how comments were taken into account: Most of the comments made correspond to what the new proposal contains. It also includes the use of a web-service where carriers will receive the answer that meets their current obligation ("Is this traveller eligible for transportation till destination?"). However there is no change to carrier's current obligations as this is outside the remit of border control.

Comments of airport and seaport operators are taken into account by using biometric identifiers that put a low burden on border crossing time and protects existing investments. Further the new legal package enables explicitly the use of self-service kiosks.

2.5. Survey from the Fundamental Rights Agency

In the framework of the eu-LISA Pilot, FRA has investigated the views of travellers on a number of fundamental rights (dignity, respect for private life and family life, right to protection of personal data, non-discrimination) related to the use of biometrics in the context of border control. FRA interviewed 1.234 randomly selected third-country nationals at BCPs.

The results show that the majority of persons are comfortable with providing biometrics when crossing the border and don't perceive the provision of biometrics in the context of border control as compromising their right to privacy and to dignity. Trust in the reliability of biometric technologies is also high. The majority of respondents believe that only adults (i.e. 18 years of age onwards) should be allowed to go through biometric checks.

The travellers, however, expressed concerns with regards to the proper functioning of the system (i.e. more than half of the respondents believe that they will not be able to or do not know if they will be able to cross the border if the system malfunctions). Similar concerns emerged in relation to the right to rectify the data, where half of the respondents believed that if there was a mistake in the data, it would be difficult to correct.

The results of the survey show that third-country national travellers take data protection seriously and more than 80% consider it important to be informed on the purpose of collecting and processing their personal data.

There is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – as compared to checks carried out in person by border guards. This might be based on the assumption that machines entail a lower risk of discriminatory profiling compared to checks by border guards.

Key findings

Acceptability of technology: Approximately 1 in 10 travellers feel very uncomfortable with providing fingerprints or facial image, while 38.7 and 39.6 percent respectively feel 'comfortable' and 'very comfortable'. The percentage of travellers feeling very uncomfortable is considerably higher for iris-scan: 21.3 percent chose this answer. This tendency is visible across all BCPs, across all regions of citizenship of travellers, gender and age groups.

Private life: 46.9% and 42.9% believe that providing fingerprints and facial image respectively is not intrusive to their privacy. Attitudes towards iris-scan are different, with a higher percentage (38.6%) believing that letting their iris be scanned is intrusive or very intrusive to their privacy.

Dignity: Almost one third (32.3%) believe that letting their iris be scanned might be humiliating, one in four (26.8%) finds that that providing facial image might be humiliating and slightly more than a fifth (22.8%) that providing fingerprints might be

humiliating. However, these results have to be put in relation with the fact that 15.9% of respondents are considering that any kind of border check is humiliating.

Accuracy of the data: Close to half of the respondents trust that biometric technologies will always properly identify who they are but there is a great amount of uncertainty about how well biometric systems work to properly identify people (20% have chosen the middle value).

Data protection: 83.9% of the respondents strongly agree, or agree, that it is important to be informed on why their biometric identifies are collected and used. Half of the respondents (50.8%) believe that their data could not be easily corrected in case of error. Only 17.2% believe that the data could be easily corrected. The majority (75%) of travellers trust that only legally authorised people can access biometric data. 55% of travellers agree or strongly agree with data access for law enforcement purpose.

Automated border control systems: Respondents were asked if they were to choose, whether they would go to a machine or a border guard. Approximately one third of the respondents reported they would go to a machine and another third reported they would go to a border guard. For one in every four respondents, it makes no difference. A large proportion of respondents (61%) consider that automated systems cause less discrimination than border guards because of the absence of human judgement selecting passengers for further checks.

Whether/how comments were taken into account: The results of the FRA are taken into account in the new proposal by including provisions for correction and redress of data to the data subjects. Otherwise the study results confirm the acceptability of biometrics and a wider support for fingerprints and facial image as opposed to the iris scan.

2.6. Results of the public consultation on Smart Borders[6]

2.6.1. Introduction

The objectives of the public consultation were:

- to collect views and opinions on the policy options, their likely impact and hence testing existing ideas and options with all stakeholders and the general public;
- to gather new ideas and general relevant knowledge and
- to test existing ideas and analysis.

For this purpose, the public consultation was published online on 29 July 2015 on a dedicated Commission website[7] during 12 weeks (i.e. until 29 October 2015).

Seeking the highest number of participants possible, representatives of the civil society, carriers, and operators/organisations of the transport, tourism and transport infrastructure sectors were directly informed of the publication of the consultation by the services of the Commission. The information was also posted on Twitter and advertised on the Commission's general website and on the websites of EU Delegations abroad. Information on the consultation was furthermore disseminated by the the Fundamental Rights Agency (hereinafter ***FRA***), which informed civil society actors, and eu-LISA, which shared information with the Members and Observers of the Management Board.

The public consultation consisted of four different questionnaires targeting respectively:

1. individuals;
2. organisations (non-governmental, civil society organisation, academia, research, social partner, interest group, consultancy, think-tank…);
3. public authorities;
4. carriers, transport and tourism operators/organisations and transport infrastructure operators/organisations.

The four questionnaires targeting the four different groups followed the same logic and presented the same structure:

1. General information;
2. The use of biometric identifiers;
3. The processes for accelerating the border crossings of non-EU citizens;
4. The data retention period;
5. The law enforcement access to the data (hereinafter ***LEA***);
6. The consequences of the abolition of stamping of passports of non-EU citizens crossing the Schengen borders.

In total 101 responses were received. 62 replies came from individuals, 14 from organizations, 14 from public authorities and 11 from carriers, transport and tourism operators/organisations and transport infrastructure operators/organisations.

---

[6] http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/docs/consultation_030/results_of_the_public_consultation_on_smart_borders_en.pdf

[7] http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

2.6.2. General information

As regards individual persons, 9 replies were supplied by non-EU citizens. From these 9 non-EU citizens, three were holding a residence permit of a member state (hereinafter ***MS***) while the remaining five held a multiple-entry visa. Five of the third country nationals (hereinafter ***TCN***) who participated in the consultation could be considered as frequent travellers (i.e. they travel at least 3 to 5 times a year to the Schengen area).

As regards the organizations, the 14 replies represent organizations of different nature, such as international human rights associations, associations of commercial undertakings or churches.

As regards public authorities, 7 replies out of 14 came from Finland, the remaining replies were submitted by different national authorities (from the Netherlands, France, Estonia and Greece) and European organisations. The European organisations who replied to the consultation were the European Data Protection Supervisor (hereinafter ***EDPS***) and the European Union Border Assistance Mission to Moldova and Ukraine (***EUBAM***).

As regards carriers, transport and tourism operators/organisations and transport infrastructure operators/organisations, from the 11 replies, 8 contributors are carriers or transport operators and 3 are transport infrastructure operators.

2.6.3. Presentation of the results

<u>The use of biometric identifiers</u>

Summary results:

The necessity to use biometrics was confirmed by the majority of the respondents from all the groups except "Organisations".

"Individuals" and "Public authorities" showed their preference for the combination of the identifiers (FI and FP), whereas "Carriers" showed their preference for FI only.

Main advantages of biometrics that were mentioned: data reliability, certainty and speed of checks and security.

Main drawbacks mentioned: perceived intrusiveness of biometrics, issues related to proportionality of the measures, data security and a potential breach of fundamental rights

After a short introduction into the 2013 Smart Border proposals, the participants were invited to share their opinion on the preferred kind of biometric identifiers.

Individuals

A majority of the individuals (58%) were of the opinion that some kind of biometrics is necessary with a preference for the combination of fingerprints (hereinafter ***FP***) and facial image (hereinafter ***FI***).

Those who preferred the 'no biometrics' option were mainly concerned with the perceived intrusiveness of biometrics, the proportionality of the measures, the risks of a potential

data misuse or theft and questioned the need of biometrics on top of the information already included in the travel documents. The supporters of the combination of FP and FI mainly argued that this would bring a better data certainty and security. When explaining their choice for FP only or for FI only, the majority of the respondents highlighted their perception that the respective biometric identifier was less intrusive and also indicated the enhanced security and speed of checks.

It is worth mentioning that 7 out of the 9 participating TCN expressed their positive views on the use of one of the proposed solutions comprising the biometric identifiers. When asked if giving FP would discourage them from travelling to the Schengen area 4 out of 9 replied positively. Moreover, 3 positive replies were given to the similar question with reference to the FI.

When asked about the link between the biometric identifiers and reliability of border checks 43% of the individual respondents agreed with the improved reliability and 28% were of the opposite view. The majority of those in favour mentioned the security aspect in their justification whereas those with the opposite view highlighted the potential privacy infringements and the potential delays.

Organisations

As regards the organisations, 6 out of 14 respondents preferred the combination of FP and FI arguing that the use of two biometric identifiers was more reliable than the use of one. 8 participants replied negatively to the use of biometric identifiers, indicating in most cases a potential breach of fundamental rights and a potential threat to data security.

When asked about the link between the biometric identifiers and reliability of border checks 8 out of 14 participants agreed with the improved reliability stating that the checks using biometric identity verification are more reliable than the checks relying on "human-based" visual identification. The respondents considering that the use of biometric identifiers would jeopardize the reliability of border checks raised the issues of data security and "false-positive" incidents.

Public authorities

As regards the public authorities, a majority of the respondents (11 out of 14) favoured a combination of FI with a limited number of FP. The reasons indicated were a higher certainty of identification, an enhanced security and a lower error rate.

9 out of 14 public authorities supported the enhanced reliability of border checks if biometric identifiers were to be used. The only negative opinion came from the EDPS which stated that the need to use biometrics has still to be demonstrated and that an evaluation period is needed prior to the introduction of biometrics. They also expressed concerns stemming from the perceived intrusiveness of biometrics and its potential impact on the respect of the private life.

Carriers and transport infrastructure operators

As regards carriers and transport infrastructure operators, 7 respondents supported the necessity to use biometric data, with a clear preference for the use of FI alone or in combination with FP. The need to use a biometric identifier was rejected by 4 respondents. The use of the combination of FI and FP was considered as more secure, whereas FI is considered faster and easier by most of the respondents. Among those who

rejected biometric identifiers in several cases the arguments were of a practical/operational nature (e.g. buses are not duly equipped to perform such verifications). Other respondents who replied negatively mentioned their perceived limitation for air passengers or their preference for alphanumeric data as it would be more convenient for their passengers.

The majority of the respondents supported the enhanced reliability of border checks if biometric identifiers were to be used. They considered that the use of biometrics would lead to a better security and reliability of the border checks and would reduce the time spent for these checks. The necessity of reaching good quality for the biometric data was also highlighted.

Process to accelerate border crossing for non-EU Citizens

Summary results:

The necessity to accelerate border crossing for the TCN was supported by the majority of the respondents from all the groups. The majority of the respondents supported both the 2013 RTP proposal and the second simplified option without prior application (in both cases the support among the TCN was above the average).

Main advantages mentioned of the 2013 RTP proposal: time saving, mobility improvement, higher security due to pre-vetting, support to the EU economy.

Main drawbacks mentioned of the 2013 RTP proposal: segregation of TCN travellers, fees, security of the automated controls, excessive data collection and high costs.

Main advantages mentioned of a system without prior application: efficiency, celerity of the process and simpler procedure.

Main drawbacks mentioned of a system without prior application: fear that the automated controls would not be secure enough, fear of a breach of privacy, potential data hacking or potential errors in the biometric technology.

In this part of the survey, after having recalled the principle elements of the 2013 RTP proposal, the question was asked if there was a need for a process to accelerate the border crossings of non-EU citizens at the Schengen area's external borders. In the second part, the participants were asked to answer questions related to their preferences on the different options for facilitation as well as on their potential outcome.

Individuals

More than half of the participants (53%) replied that there was a need to accelerate the border crossing[8].

Concerning the enrolment and facilitation process as envisaged in the 2013 RTP proposal, when asked if the RTP option should be available to non-EU citizens, 61% of the respondents replied positively (including 8 out of 9 of the participating TCN). Among supporters, the main reasons for implementing such facilitation process would be time

[8] Including 6 out of the 9 non-EU citizens who participated in the consultation.

saving and mobility improvement[9]. 39% of respondents argued against an RTP. The main arguments against were that the process would segregate the travellers into classes, that it would be unfair to pay for the accelerated border crossings and the concerns surrounding the security of checks performed in the automated controls.

The personal interest in the scheme was confirmed by 7 out of 9 TCN participants. The replies highlighted the necessity for a reduction of time for border checks and the wish to use automated border gates. However, some concerns were raised concerning the security of the stored biometric data.

Concerning the use of self-service kiosks[10], 61% of all respondents agreed that the self-service kiosks should be available for both the travellers holding a short-stay visa and the visa-exempt travellers whose data has been registered during a previous journey (if the retention period has not expired yet). The main argumentation provided by the respondents indicated efficiency gains and an acceleration of the border crossing process. The remaining 39% were against. The negative replies brought up the fact manual checks are sufficient, the fear that the automated controls would not be secure enough, the fear of a breach of privacy, potential data hacking or potential errors in the biometric technology.

When asked about the participants' opinion on the use of self-service kiosks, 7 out of 9 TCN confirmed their personal interest in the scheme. The main reason was the reduction of the time spent for border checks and, to a lesser degree, the fact the procedure did not required prior application.

If nevertheless the application was required in order to be able to profit from the facilitation (RTP proposal) 5 TCN confirmed that they could apply both online or personally at a consulate or at the border crossing point. In 3 cases online application was indicated. If fees were to be charged for the RTP the opinions were equally shared among those who agreed, those who were against and those do not have an opinion or are not sure. Concerning the maximum fee that could be accepted to benefit from the procedure, out of 3 positive replies the average amount was 40 euros.

One of the facilitation solutions to accelerate border crossing would be the use of self-service kiosks at the border crossing. After having explained the operations that the TCN travellers will have to carry out when using these kiosks, the TCN where asked if they would be interested in using them. The replies showed the acceptance rate of two thirds, with 2 participants not having opinion.

Organisations

More than half of the participants (53%) agreed that there was a need for a process to accelerate border crossings by non-EU citizens at Schengen area's external borders. A large proportion (5 out of 14) did not position itself regarding this issue.

When asked if the RTP process should be available to the non-EU citizens, 11 respondents agreed and highlighted the speed and gain on efficiency of checks, whereas

[9] Other replies indicated also that it would constitute a better tool to tackle the growing passenger flow, to level the non-EU citizens' rights with those of the EU citizens and reported a good experience with the existing facilitation systems (Privium and Parafe).

[10] To be used by the TCN already registered in the VIS system or, if not subject to the Schengen visa, those TCN whose data was still available in the EES.

the opponents indicated the risk of violation of the fundamental rights and of unjustified data collection.

Concerning the use of self-service kiosks, 11 of the respondents replied positively. The supporters brought up mainly time saving whereas opponents mentioned the potential infringement of the privacy due to the collection of the biometric data.

Then, the participants were asked if they envisaged any difficulties for the travellers, should the self-service kiosks be implemented. 7 of them replied positively and evoked potential problems if the devices are not sufficiently user friendly or if no assistance is provided to the traveller, especially at the beginning.

Public authorities

10 out of 14 respondents affirmed that there is a need for a process to accelerate border crossings by non-EU citizens at the Schengen area's external borders. When asked if the RTP process should be available to the non-EU citizens, 11 out of 14 respondents replied positively, 9 of them agreed that offering facilitation to its beneficiaries will effectively contribute to the overall facilitation of border crossings. 4 indicated that they considered the process as secure since it included pre-vetting. Additional arguments included positive economic impact for business (particularly for frequent travellers) and the necessity to limit a potentially higher procedural burden on border guards.

Concerning the use of self-service kiosks,, 10 out of 14 respondents replied positively. Subsequently 7 of them agreed with the statement that facilitating border crossing for a wide range of users could contribute to the overall facilitation of border crossing. A single negative reply from the Estonian Ministry of Interior highlighted security concerns and the difficulty to introduce self-service kiosks at land borders. Some participants called for a balance of the security and the facilitation of the process to be maintained, for the use of web or mobile apps for the pre-checking and for the benefits of maintaining the RTP. While recognizing its increase in the process speed, it was highlighted that the use of self-service kiosks should be carried out under the supervision of the border guards. Lastly, the facilitation efforts for some travellers should not turn out to be detrimental for some other groups (e.g. for local traffic).

Carriers and transport infrastructure operators

10 out of 11 participants replied positively, in 8 cases indicating a strong support. When asked if the RTP process should be available to the non-EU citizens, 9 respondents agreed indicating as advantages: more expedite process, better security and positive impact on business. A bus operator wished that the accelerated procedure were available for all passengers as it was a condition for quicker border crossing of the entire bus. Among the 2 negative voices, the high costs of the system were pointed out. A cruise operator highlighted the need of a system that could tackle thousands of customers arriving in a short period of time.

Concerning the use of self-service kiosks, 10 respondents replied positively. The most frequent justification given by the supporters pointed out again to better speed for border crossing process (also due to the use of self-service kiosks) and a positive impact for the crew members who were already registered in VIS. The main requirement for the system that was highlighted was that it must be simple to use. The only negative reply pointed out towards scarcity of space for installing the kiosks.

Employing technology in the pre-check stage (self-service kiosks) would limit the waiting time. The procedures should be as light as possible both for the passengers and for the carrier's personnel. All types of borders should be taken into consideration (land, sea and air).

Data

Summary results:

The opinions concerning the length of the retention period were divided. For non-overstayers: the majority of "Individuals" and "Carriers" preferred 181 days or longer, the majority of "Organisations" were opposed to any type of data retention and the majority of "Public authorities" favoured a retention period longer than 181 days.

Reasons for 181 days retention period: sufficient to calculate the duration of the authorised stay, lesser impact on privacy.

Reasons for a shorter retention period (less than 181 days): risks of errors in the biometric identifiers (i.e. linked to a general reluctance to use biometric identifiers).

Reasons for an extended retention period (more than 181 days): faster border controls.

For overstayers: the majority of "Individuals" preferred shorter than 5 years or 5 years, the majority of "Organisations" less than 5 years. The majority of "Public authorities preferred 5 years period or longer. "Carriers" were not consulted on overstayers.

Reasons mentioned to maintain the 5 years retention period: coherence with the validity of biometric passports and VIS.

Reasons mentioned for a data retention period shorter than 5 years: data protection and data collection concerns, erroneous data correction, reasons for overstay to be taken into account.

Reasons mentioned for a data retention period above 5 years: security reasons, better control of overstayers, improved mobility, data retention time used in other countries.

The third area that was consulted concerned the length of the EES data retention period. First, the data retention rules as envisaged in the 2013 proposals were presented and explained, and then with a reference to the revised proposal, the participants were asked to express their opinion on the length of time that the data could be kept after its collection at the entry/exit of the Schengen area's external borders. The proposed reply options were equally explained.

Individuals

Concerning the data retention period for the Entry/Exit System for non-overstayers (see the chart 4 below), 45% of participants favoured the option with a maximum data retention period of 181 days starting from the exit date (it was explained that 181 days is sufficient to calculate the duration of authorised short stays in the Schengen area), 31%

agreed with a longer retention periods in exchange for faster border controls, and 24% did not agree with either of the proposed replies.

The respondents who answered "other", could further explain their preferences in an open question, 8 individuals explained that they would opt for a much shorter or no data retention period whereas 2 participants explained that they would opt for a longer/unlimited data retention period. One of respondents indicated maximum data retention of 181 days, increasing the share of those who chose this reply to 47%. Some of the participants appear to have misunderstood the link between the retention period and the rules for the short stay in the Schengen area.

For a similar question on data retention period but concerning overstayers, half of the participants (50%) voted for a data retention period shorter than 5 years. The reasons for favouring a shorter retention period were mainly related to data protection concerns, a general reluctance to data collection or a perceived difficulty to correct / update wrong or obsolete data. Some stated that the reason for overstay should be taken into account and that for a justified or very short overstay, a period of 5 years of data retention would be disproportionate. The majority of the supporters of a period of data retention longer than 5 years explained that such an option would lead to an improved security and to a better control of overstayers. For one of the respondents it would lead to better mobility. The example of longer data retention periods in other countries was also mentioned. One respondent wondered why the 5 years' period was proposed. Those respondents who agreed with the 5 years period did not present additional arguments in favour of their choice.

Organisations

Concerning the data retention period for the Entry/Exit System for non-overstayers, the majority of the participants replied "other", and provided their main argumentation for their opposition to the proposed data retention period: that the choice of a longer data retention period should be optional for facilitation reasons and that it might bring up risks of "false-positive" incidents. For the question on data retention period which concerned overstayers, the majority of the respondents preferred a data retention period shorter than 5 years, their choice justified by the risk of profiling and of misuse of data. The supporters of a longer data retention period justified their opinion mainly based on security concerns.

Public institutions

Concerning the data retention period for the Entry/Exit System for non-overstayers, 8 out of 14 participants agreed with a longer data retention period, with the aim of speeding up border controls by avoiding a re-enrolment into the EES, whereas 3 replies indicated that the retention period of 181 days is sufficient to calculate the duration of authorised short stay in the Schengen area and has a minor impact from a privacy protection perspective. For the question on the data retention period for overstayers, 7 out of 14 participants agreed with the proposed 5 year period following the last day of the authorised stay while 4 of the participants favoured a data retention period longer than 5 years. The detailed explanations that were submitted included a view that the 5 year data retention period would be equal to the 5 year validity of the biometric passports and that the data retention period should be in line with VIS. Those indicating data retention periods longer than 5 years had in mind LEA purposes. The EDPS in its contribution requested further justification for a 5 year retention period. Another issue mentioned was the need to correct the EES data once the stay was extended by the authorities.

Carriers and transport infrastructure operators

The replies received showed a strong support (8 out of 9 replies) for data retention periods longer than 181 days. Only 1 reply favoured a data retention period of maximum 181 days.

”Carriers” were not consulted on overstayers.

Law Enforcement Access (LEA) to the Entry/Exist System

Summary results:

The opinions on the law enforcement authorities' access to the future EES system were divided. Among “Individuals” and “Carriers” there were slightly more opponents than supporters, “Organisations” were equally divided and a majority of “Public authorities” supported LEA.

Reasons mentioned for granting access: security, detection, prevention and investigation of criminal and/or terrorist offences, international character of the threats.

Reasons mentioned against granting access: lack of proportionality, lack of trust, potential errors leading to the criminalisation of foreigners, insufficient data security, threat to the privacy.

The safeguards that were indicated concerned mainly the limitation of the searches, their scope and their access, as well as the necessity to authorise LEA access by courts or independent administrative bodies.

The subject of the access of law enforcement authorities to the data was already included in the 2013 proposals. The 2013 proposals suggested that the option of access of law enforcement authorities to the data contained in the system should be evaluated two years after the entering into operation of the system. With the increase of the security concerns and the experience obtained in other large scale IT systems, the Commission envisaged proposing such access from the start of the system while respecting the principles of necessity, appropriateness and proportionality.

Individuals

When asked, 40% of the respondents agreed on granting law enforcement authorities' access to the EES for the purpose of preventing, detecting or investigating terrorist and/or serious crime offences from the start. 44% of the respondents were against, 11% considered that the matter should be reconsidered 2 years after the implementation and the remaining 5% did not express an opinion. The respondents who agreed with granting the access from the start justified the need for such access from a security perspective.

The respondents who replied that no LEA should be granted to the EES mainly considered that such measure would not be proportionate. Some respondents highlighted the lack of trust, the potential errors that could lead to the stigmatisation of foreigners, or the insufficient level of data security.

The participants were then asked to choose from the list of conditions aimed at mitigating the impact on the fundamental rights, should LEA to the EES be granted. Having a

choice among numerous conditions and safeguards which were proposed, the 3 most popular replies were: (1) searches should only be possible in specific cases under clearly defined circumstances (excluding searches on a systematic basis) (35 replies), (2) a court or an independent administrative body should verify in each case if the required conditions for consulting the EES for law enforcement purposes are fulfilled (31 replies) and (3) access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences (27 replies).

Organisations

Out of 12 replies that were received in this area, there were 5 respondents supporting the access and 5 opposing it. The supporters highlighted a security need, whereas the opponents did not see a need for such access bringing up previously mentioned arguments: the threat to privacy and other fundamental rights and the criminalisation of non-EU citizens. The participants were then asked to choose from the list of conditions aimed at mitigating the impact on the fundamental rights, should LEA be granted to the EES. Having a choice among numerous conditions and safeguards which were proposed, the 3 most popular replies concerned: (1) a court or an independent administrative body should verify in each case if the required conditions for consulting the EES for law enforcement purposes are fulfilled (8 replies), followed by (2) access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences (7 replies) and (3) there should be reasonable grounds to consider that the specific envisaged consultation of the EES data will substantially contribute to the prevention, detection or investigation of any terrorist and/or serious criminal offences (7 replies). One contributor mentioned the need to avoid data transfer to third countries.

Public authorities

10 out of 14 participants supported granting LEA, as they considered it justified for security reasons. One respondent (the EDPS) preferred that LEA to the EES would be evaluated two years after the implementation of the EES and requested the Commission to carefully evaluate evidence presented by the MS. The reasons mentioned in support of LEA to EES data were that the access will substantially contribute to the detection, prevention and investigation of criminal and/or terrorist offences. Since the organised crime and terrorism have an international character, such access is necessary for the security of the EU citizens. An EU arrest warrant was evoked as a base for the definition of crimes for which investigation access to the EES should be granted.

The participants were then asked to choose from the list of conditions aimed at mitigating the impact on the fundamental rights, should LEA was to be granted access to the EES. Having a choice among various conditions and safeguards the most popular replies were: (1) access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences (7 replies) and (2) there should be reasonable grounds to consider that the specific envisaged consultation of the EES data will substantially contribute to the prevention, detection or investigation of any terrorist and/or serious criminal offences (7 replies). Additional comments pointed at the utility of the national EES systems, the necessity to respect fundamental rights, the necessity to establish the rules of data information sharing among the law enforcement authorities from the different MS, and maintaining the envisaged LEA as a secondary objective of the future Smart Borders package.

Carriers and transport infrastructure operators

The replies received were not conclusive, as 3 respondents supported the access, 4 either opposed or did not see the need and 3 did not have an opinion.

Stamping

Summary results:

The majority of non-EU citizens confirmed the need for having access to the information provided by the stamps, mainly to be able to respect the 90/180 days rule of stay. If stamps were discontinued some of them favoured the creation of an online website and others the delivery of a ticket when crossing the border. A majority of the replies received from "Organisations" agreed with such need. "Public authorities" indicated the need to grant access to several national services or service providers. As for "Carriers", the majority of those directly impacted by the abolition of stamping confirmed the need to access the information previously provided by the stamp via alternative solutions.

The paragraph began with the explanation of the main purpose of stamping passports (which is the location and date of entry/exit) and based on this information, the calculation of the authorised length of a short stay. The main disadvantages of that method are the cumbersome calculation of the length of stay and the potential forgery of stamps. It was reminded that the Commission already proposed to abolish stamping in their 2013 proposals.

Individuals

When asked about the consequences of the abolition of the stamping of passports of the non-EU citizens crossing the external borders of the Schengen area, 7 out of 9 of the TCN who participated in the consultation confirmed the need to access to the information that the stamps currently provide. The main justification concerned certainty of respecting the 90/180 days rule during a stay or future stay. Some also indicated a need to prove their absence from the country of residence.

If stamps on passports were to be discontinued, the preferred alternatives to access the information that stamps currently provide (i.e. data and location of entry/exit to/from the Schengen area) were: the creation of an online website giving access to the relevant information (mentioned in 3 replies) and the delivery of a printed receipt when crossing the external borders (mentioned in 3 replies).

Organisations

If stamps on passports were to be discontinued, 9 out of 14 participants expressed as their opinion that the TCN should have access to the data that is currently provided by the passport stamp. On this issue, 1 respondent considered that TCN should not be granted access to this information and 4 did not have an opinion.

Public authorities

If stamping of passports were to be discontinued, the majority of respondents (8) agreed that public authorities other than border management authorities should have access to

the information currently provided by stamps (i.e. data and location of entry/exit to/from the Schengen area). Three respondents had no opinion and one was against.

When asked which public authorities would need access to this information and for which purposes the participants indicated: the police (identification of TCN without documents), the social services (to identify the welfare applicants), immigration authorities (to identify asylum seekers), the labour inspection (to determine legality of stay), the consulates (to verify visa applicants), the carriers (to check if a TCN fulfils the conditions for entry) as well as the accommodation providers (to check the legality of stay).

Carriers and transport infrastructure operators

If a web service was made available to carriers to enable them to verify if a single entry visa has not been used, 6 out of 10 confirmed this solution as necessary and sufficient. Some participants who replied negatively explained that in their activities they were not concerned by checking the documents.

As an alternative to the above presented solution, a carrier proposed a SMS service which would confirm the validity of a visa based on a visa sticker number or an integration into the into the departure control system of airports. A cruise operator highlighted the importance of the information concerning the time their passengers can stay in the Schengen area.

Comments

All the respondents from "Organisations", "Public authorities" and "Carriers" had the opportunity to submit their additional comments and suggestions under section 7: "Comments/other questions" of their respective questionnaires. Their comments and suggestions are directly available in their respective contributions.

3. ANNEX 3: PRACTICAL IMPLICATIONS OF THE INITIATIVE FOR THE AFFECTED PARTIES

This annex describes the implications of the initiative for the affected parties and in particular the implications of the preferred solution.

The description of the practical implications of the initiative (column 2) refrains from explaining the operations that are not visible to the affected party. A more detailed description of the future process at the border at entry and at exit is described in annex 8 - New Smart Border processes.

The term "practical implications" is also understood as only dealing with the mainstream cases.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
EU citizens Number of persons concerned : 550 million	Entry and exit of the Schengen area is not modified at all. There are no practical implications of the initiative for EU citizens.	Same as in previous column.
TCN-VE Third-country nationals coming from countries that are exempted of the obligation to obtain a visa. Number of persons concerned: 39 million persons in 2020 (start of EES operations)	**At first entry** into the Schengen area or at an entry after the period of retention of his/her data in EES: • Border control will be done as today but his/her individual file will be created by having the data from the biographical page of the passport (or from the chip of an electronic passport) stored in the EES and biometrics taken. This additional step will take more time depending on the biometrics used and on the congestion (or not) and organisation of the border control post. **At return visits** into the Schengen area during the retention period of his/her data in EES: • Border control will be done as today and the date and place of entry into the Schengen area recorded in the EES. His/her correspondence with the identity stored in EES will be checked by means of a biometric verification. This additional step will take less than 15 seconds and can be done concurrently with other border control steps and	**At first entry** into the Schengen area or at an entry after the 5 years (= the retention time) since the last exit: • The biometric referred to will consist of 4 fingerprints and a facial image taken with a digital camera. • The time this would take is estimated at 30 seconds plus the waiting time dependent on congestion (or not) and organisation of the border control post. • The traveller will also be able to prepare border clearance him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by a face-to-face time with the border guard. **At return visits** into the Schengen area within the 5 years period since his/her last visit: • The biometrics referred to in the previous column will consist of 1, 2 or 4 fingerprints checked vs the biometrics stored in EES, or the picture taken with a digital camera compared with the picture stored in EES. • The traveller will also be able to prepare border clearance

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	hence should not slow down the border control process. • The remaining duration of stay in the Schengen area will be provided to him/her: display, printed form, orally. **At exit:** • Border control will be done as today and the date and place of exit from the Schengen area recorded in the EES. His/her correspondence with the identity stored in EES will be checked by means of a biometric verification. This additional step will take less than 15 seconds and can be done concurrently with other border control steps and hence should not slow down the border control process. **General:** the traveller's passport will not contain Schengen entry/exit stamps anymore.	him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by face-to-face time with the border guard. **At exit:** • The biometrics referred to in the previous column will consist of either 1, 2 or 4 fingerprints checked vs the biometrics stored in EES, or the picture taken with a digital camera compared with the picture stored in EES. • The traveller will also be able to use an e-gate in the border crossing points equipped with this (this is Member State dependent). **General**: If the traveller wants to know the remaining duration of authorised stay he/she needs to access a web service, enter passport number and issuing country, answer a question related to his/her last trip, enter the intended entry and exit data and he/she will receive a YES or NO answer. This is only necessary if the traveller stays frequently in the Schengen area as the rules on short stay (90 days in any period of 180 days) are not affected.
TCN-VH Third-country nationals	Border control will be done as today including the verification by means of a biometric check of 1, 2 or 4 fingers that the visa belongs to the traveller (this is part	**At first entry** into the Schengen area or at an entry after the 5 years (= the retention time) since the last exit:

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
coming from countries that are required to obtain a visa. Number of persons concerned: 24 million persons in 2020 (start of EES operations)	of the control on visas). **At first entry** into the Schengen area or at an entry after the period of data retention in EES: • In addition, a picture will be taken with a digital camera and the picture stored in the EES. This additional step will take less than 15 seconds and can happen concurrently with other steps. **At return visits** into the Schengen area during the retention period of his/her data in EES: • No additional steps are required in addition to the one required. **At exit:** • Border control will be done as today and the date and place of exit from the Schengen area recorded in the EES. His/her correspondence with the identity stored in EES will be checked by means of a biometric verification. This additional step will take less than 15 seconds and can be done concurrently with other border control steps and hence should not slow down the border control process.	• The traveller will also be able to prepare border clearance him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by face-to-face time with the border guard . At return visits into the Schengen area within 5 years since his/her last visit: • The traveller will also be able to prepare border clearance him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by face-to-face time with the border guard. **At exit:** • The biometrics referred to will consist of either 1, 2 or 4 fingerprints checked vs the biometrics stored in EES, **or** the picture taken with a digital camera compared with the picture stored in EES. • The traveller will also be able to use an e-gate in the border crossing points equipped with this (this is Member State dependent). **General**: If the traveller wants to know the remaining duration of authorised stay he/she needs to access a web service, enter passport number and issuing country, answer a question related

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	General: the traveller's passport will not contain Schengen entry/exit stamps. Also the single/double entry visas will no longer be stamped.	to his/her trip, enter the intended entry and exit data and he/she will receive a YES or NO answer. This is only necessary if the traveller stays frequently in the Schengen area as the rules on short stay (90 days in any period of 180 days) are not affected.
Air, land and sea carriers Number of carriers on travel routes to and from Schengen area estimated to a few thousands.	Carrier's obligations do not change. In practice, they will continue to check that each traveller carries with him the required documents to enter the Schengen area. Like now, carriers therefore will check whether each third country national has a passport and a valid visa. The items the carrier has to check are : • whether the passport is valid, • whether a multiple-entry visa is still valid by means of the date mentioned on the sticker in the passport, • whether a single or double entry visa has been used by accessing a web-service. Carriers will be granted credentials to access a webservice that will answer the question: "Is this traveller eligible for transportation till destination?" on the basis of the passport number and the issuing country. The web-service will only give a Yes/No answer when at least one day of stay is left when the date of entry is	Same as in previous column.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	given. The webservice will only access a report generated daily by EES. No transfer of data to carriers will occur.	
Airports and seaport operators Number of operators affected in the Schengen area are estimated between 100 and 150	Operators or airports and seaports will face a situation where border crossing in and out of the Schengen area follows a modified process and at the same time contains opportunities to happen in a more automated way. Border clearance at entry for visa-exempt travellers has a risk to be more time-consuming as an enrolment step is added at first entry (or re-entry after data retention expired). There is much less risk of added duration for verification during return visits within the data retention period. Duration of border clearance at entry for visa-required travellers is not going to be significantly impacted by EES. Duration of border clearance at exit can be shortened since the opportunity exists to have most of the steps automated. Airports where a large share of travellers is visa-exempt need to organise the new border clearance process as efficiently as possible. If this was not the	Compared to the general situation described in the previous column, the preferred solution has the following practical implications: • As the data retention period is proposed to be 5 years, the proportion of visa-exempt travellers who need to be enrolled will be low once the system is in operation. During the first one or two years of operations however there will be a significant proportion of visa-exempt travellers who will have to be enrolled. • The biometric identifiers chosen (4 fingerprints and a facial image) only require on average 30 seconds for being captured and are not sensitive to environmental conditions. • The possibility of automating part of the border clearance process (use of self-service kiosk) at entry creates the opportunity to avoid that travellers spend more time at the border and that therefore more space is required as compared to the current situation. • The possibilities for automating the major part of the border clearance process at exit for all third country nationals, is another opportunity to avoid that travellers spend more time

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	case, the increased border crossing duration would lead to require more space for the higher number of travellers waiting. The same would apply for seaports except that the proportion of visa-exempt travellers in seaports is on average low. In the same way as is the case now dedicated solutions need to be worked out for travellers and crew on cruise ships. The problem of the large group of persons (up to 4.500 persons) to be controlled is mitigated by the fact that all travellers are identified, that cruise ship operators have dedicated staff for security and immigration questions, and that all entries and exits on and off the ship are recorded.	at the border crossing point and that hence a bigger waiting area is required.
Border guards Total number of border guards in the first line is estimated at 25.000 persons	The practical implications for border guards are the mirror image of the implications for travellers. What does not change: border control of visa-exempt and visa-required travellers do the same checks as today. What changes is adding the recording of the entry and exit date and place. Border guards will read the passport by means of the passport reader which will trigger the same database checks as today plus check whether the traveller is	Compared to the general situation described in the previous column the preferred solution brings the following additional elements: • At enrolment the personal file is completely create by data from the passport and does not include data that the travellers would declare and the border guards would record manually. • The biometrics stored in VIS are re-used for visa-exempt

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	known in EES and/or VIS. **<u>At entry</u>** **Most frequent case once the system is in operation: the traveller is known in EES and/or VIS** • If he/she is known in EES and is **visa-exempt**, a biometric verification is done: facial image or 1, 2 or 4 fingerprints are matched with the one in the database. If it yields an OK, the EES provides the duration of authorised stay. Upon verification that the other conditions for entry are met), the border guard authorises entry and the EES records the entry date and place. • If he/she is known in EES and is **visa-required**, a biometric verification is done as today. Without the border guard necessarily being aware of it, 1, 2 or 4 fingerprints are matched with the ones in *VIS*. If it yields an OK the EES provides the duration of authorised stay. Upon verification that the other conditions for entry are met, the border guard authorises entry and the EES records the entry date and place. **In case the traveller is not recorded in EES**	travellers. • The biometric identifiers are composed of 4 fingerprints and a facial image. This is a choice justified because it is fast, efficient, reliable and secure. • When the traveller uses the self-service kiosks, the border guard is relieved from the actions of reading the passport and taking biometrics, but he/she gets the replies on his screen and the history of entries and exits of the traveller over the last 5 years. This allows him/her to adapt the questions according to his/her assessment of the risk of overstay. • At exit, travellers can use e-gates (when available as to install e-gates or not is a Member State's decision). Border guards carefully watch what is happening in and around the e-gates and intervene for any unusual situation.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	• If he/she is **not known in EES** and is **visa-exempt**, the border guard enrols the traveller, meaning that he/she creates a personal file: – The border guard takes 4 fingerprints and a facial image and requests the system to check whether these biometrics already exist in EES and VIS. The answer should be "no". A "yes" would indicate that the person already exists in EES or VIS but that he/she has more than one passport. Entries and exits should then be linked to that existing identity. – When the person does not yet exist in EES, the border guard creates the personal file in EES by copying (automatically) the passport data (name, date of birth etc.) to EES and does the usual checks as per the Schengen Border Code. – Upon authorisation to enter, the entry date and place are recorded for that person • If he/she is **not known in EES** and is **visa-required**, then he/she will still be known in VIS, and the border guard enrols the traveller in EES, meaning that he/she creates a personal file: – The border guard takes 4 fingerprints and a	

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	facial image and requests the system to check whether these biometrics already exist in EES. The answer should be "no". A "yes" would indicate that the person already exists but with another identity. Entries and exits should continue to be linked to that existing identity. – When the person does not yet exist in EES, the border guard creates the personal file in EES and adds the facial image to the personal file in EES and does the usual checks as per the Schengen Border Code. – Upon authorisation to enter, the entry date and place are recorded for that person. **At exit:** In this case all travellers exist in EES as there must be an entry record created. • Upon reading of the passport data, the EES retrieves the last entry record for that person. • The border guard does a biometric verification match of the traveller's identity with the one recorded in the EES: either the facial image or 1, 2 or 4 fingerprints are matched with the ones in the database. The EES calculates whether there is a situation of overstay or not. In the normal case this	

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	should be "no". Upon verification of the other exit conditions the EES records the exit date and place. **General:** the traveller's passport will not contain Schengen entry/exit stamps anymore and to assess the likelihood of overstay the border guards will see the history of entries and exits over the retention period of entries and exits. Border guards will no longer stamp passports and visas at entry and exit, nor compute durations of stay.	
Migration enforcement Total number of persons is estimated at about 25.000 persons	Migration enforcement refers to any service that has a responsibility for controlling and implementing migration legislation. Compared to the current way of working where no reliable or complete data is available on overstayers, the EES will contain the identification of overstayers and keep this data for five years. Further the EES will provide a tool for giving or checking the identity of apprehended overstayers and successfully send them back. There are mainly two practical implications: • Migration enforcement can analyse the population of overstayers and identify patterns to better	In the preferred solution, the data of overstayers is kept for five years counting from their last entry record. However beyond five years, data is not simply destroyed but the possibility is offered to Member States to create a SIS alert for overstayers so that people can still be apprehended at the border and/or found during inland controls.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	evaluate the risk of overstay and share it with border control authorities. • Migration enforcement can currently find more overstayers than those it can handle the return procedure because when they are apprehended there is a difficulty to identify them with certainty. As long as the person's identity and country that issued the travel document is not established there are few chances that the return procedure will be successful. With EES, the identity of the apprehended person can be established: – Either the person apprehended is cooperative and gives his/her real identity. This identity is confirmed by a simple verification of 1, 2 or 4 fingerprints or the facial image with the one in EES, and can be sent back to the country of origin. – Either the person apprehended is not cooperative and refuses to give his/her real identity. In that case four fingerprints are taken and the facial image. This biometrics is then sufficient to find the identity back in EES provided the data are kept long enough.	

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
Migration management Total number of persons is estimated at about 5.000	Persons who have to monitor the status on illegal migration and within this on overstayers, can only rely on ad-hoc surveys to know basic information such as: where do overstayers come from, what is their profile, via which borders did they come, the date of entry/exit, etc. The EES contains the data of individual persons who are flagged as overstayers. As a system, EES has the possibility to provide non-personal statistics on a regular or on an ad-hoc basis.	The preferred solution proposes the existence of a specific statistical reporting module that can generate both regular and ad-hoc reports. This would also meet unexpected reporting requirements to suit infrequent requests.
Law enforcement authorities (police security services, …) Size of personnel employed by law enforcement services is probably in the millions but the part of the investigation services that could use EES is limited to a fraction of it, estimated at say 60.000 persons.	Investigation services will practically use EES for two situations: • Identification purposes. In this case the investigation service has a partial fingerprint and/or images from a video or from pictures taken. Investigation services will have to demonstrate that other means of identification have been used and yielded no useful answer and that access to EES may be useful given the case considered. The identification of a person can then be run based on the biometric material available vs the biometrics stored in EES. • Criminal intelligence. When the conditions for access are respected (essentially making sure it is	The data retention is 5 years which is a useful duration for investigation purposes which usually starts after the events occurred (typically one or two years later). The preferred solution contains safe-guards against the abusive use of data. When accessed for criminal intelligence purposes EES will exclude the possibility to establish profiles, meaning finding links/correlations between characteristics of persons (as opposed to specific cases) and border crossings over a period of time.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	for a specific case and EES can potentially be of use) the investigators are authorised to query EES using a mix of criteria. EES has the unique feature of recording entries and exits of all third country nationals authorised for a short stay, at *all borders* while other means are restricted to air or sea borders. Investigators could check whether a person suspected was indeed present in the Schengen area during a given period of time, the border crossing points used at entry or exit, correlate arrivals/departures of different suspects, and any similar query on data related to a specific case.	
Consular officers Total number of persons is estimated at about 25.000 persons (spread over 2.000 consulates around the world)	Consular officers handle the visa requests of visa-required travellers. For a new visa request the consular officer checks the visa application history and can see how many visas were issued over the retention period of visas (5 years from their expiry). With EES, consular officers will also see whether the durations of stay were respected and whether the traveller entered the Schengen area via the country whose consulate lodged the request. Especially the control of the duration of stay enables the attribution of visas to those who respect the rules.	The proposal intends to make the control on the use of visas very straightforward by ensuring the interoperability between the VIS and the EES. The result would be that when the consular officer consults the visa history he/she also accesses the entry/exit records directly without having to obtain data from VIS and then query EES.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
eu-LISA and IT services for border control / migration on Member State side eu-LISA employs 200 persons. An estimated 500 persons will be directly involved in the project on Member State side	**eu-LISA** The Agency will have to deliver a large-scale IT system in addition to operating and maintaining the SIS, VIS and Eurodac. This will require the resources (staff and budget) to be strengthened for the duration of the project (estimated at three years). Once EES is in operation, eu-LISA will have to operate and maintain the additional system. This will require resources to be strengthened on an on-going basis. The Agency will have to manage the credentials of operators on an on-going basis and the operations of the webservice. **IT services for border control/migration on Member State side** In the same way as the Agency, each Member State IT service for border control/migration will have to: (1) Deliver the integration of national border management applications and EES; (2) Meet the availability requirements of EES; (3) Operate the system on an on-going basis.	The proposal provides a time-frame of three years for building and testing EES. eu-LISA is in charge of not only delivering the central system but also a National User Interface (NUI) which provides a common solution for connecting the national domain with the central system. The proposal covers financially a large share of Member State costs for the integration of the NUI with the national domain and its operations costs.

4. ANNEX 4: ANALYTICAL MODELS USED IN PREPARING THE IMPACT ASSESSMENT

Appropriate analytical models were used for both the Technical Study (2014) and the Pilot (2015). For the Technical Study a simulation model was developed to assess the impact of additional checks implied by Smart Borders on traveller's waiting time at border crossing points. For the Pilot a methodology was developed for the assessment of results.

4.1. Simulation model used for the Technical Study

The model was developed by the Research and Development unit of Frontex for the specific purpose of the study.

4.1.1. Method for simulation

Discrete event simulation was used to assess the impact of any changes introduced in the border control process. The models used for air borders were customised versions of models previously used for simulations of actual air borders. The model for land borders was specifically built for this study.

Both models use real data from border crossing points that the concerned Member State's authorities have provided. The focus of the simulations was the EES processes at entry and exit. RTP is seen as a sub-case of the simulations. In addition to the real data provided there were estimates inserted, including added time for registration, verification, etc.

Appropriateness of the model

The model was considered to be the appropriate tool for simulating the impact on the border crossing time. While the study could estimate the impact on so-called "atomic" steps (the individual step in a border crossing process like taking a picture or reading the passport chip) for different biometric identifiers, a simulation tool is required to show the impact on a border crossing point. The reason is that the border crossing time is influenced both by parameters related to the border crossing point (e.g. the number of lanes), the travellers (e.g. the volume, the arrival rate, the proportions of EU citizens, VE[11] and VH[12]) and the duration of controls. In other words simply extrapolating the duration of atomic steps with the number of travellers does not yield a useful answer.

As an example, a VE at first entry could require 30 seconds more to cross the border than a VE who is already enrolled. If ten VE who need to be enrolled arrive at the same moment, there could be an added duration of 300 seconds for the last one in the queue. However, a simulation shows that this case seldom occurs as the arrival of VE to be enrolled is mixed with the arrival of EU citizens and VH. The outcome of the simulation is that the impact on the average duration for crossing the border will be dampened by the low proportion of VE.

The model has been extremely useful in understanding the impact of the duration of the atomic steps on the situation in a busy border post. The large possibilities for assessing

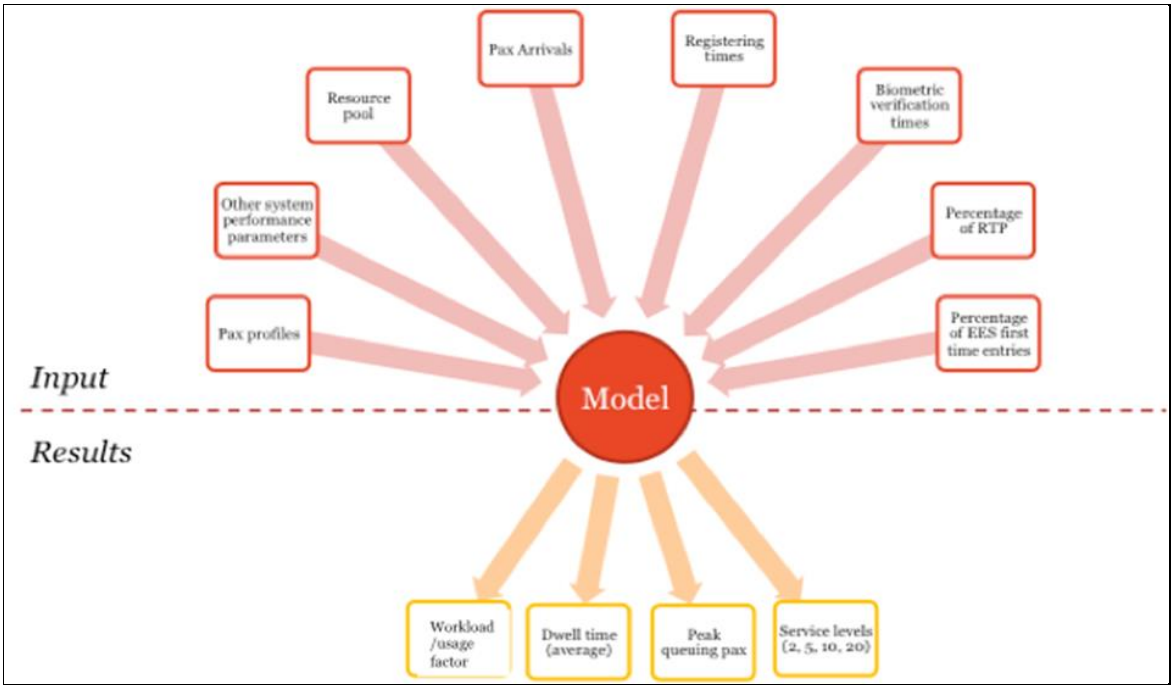
[11] Third-country nationals coming from countries that are exempted of the obligation to obtain a visa.

[12] Third-country nationals coming from countries that are required to obtain a visa.

the impact of changes to variables created awareness of which are the differentiating elements and which are the less differentiating. During the Pilot, the time values of atomic steps were assessed.

Model inputs and results

The picture below shows the type of parameters used for running the tool and the type of results that would come out of the simulation.



Input values

- The passenger profile, in this case the proportion of EU citizens, VE and VH.
- The "other performance parameters" refers to parameters like the proportion of travellers using ABC gates.
- The resources pool refers practically to the number of lanes and the number of border guards.
- The "pax arrival" refers to the pattern of arrival of travellers which is different per type of border. While the volume of travellers is a variable, the arrival rate is taken from real patterns.
- The registering time is the time for enrolling visa-exempt third country nationals at a first visit or after expiry of the retention period of data. This will be used as a variable meaning that the duration of this registration will be changed in successive computations.
- The biometric verification time is added as the so-called "overhead" for verification on top of the current border crossing time. This will be used as a variable as it is dependent of the type of biometric identifiers used.

- The percentage of RTP is the proportion of third-country nationals enrolled in the Registered Traveller's programme. RTP's border crossing time is equal to EU citizens'.

- The percentage of EES first time entries is the proportion of visa-exempt third country nationals at a first visit or after expiry of the retention period of data. This will be used as a variable meaning that the proportion of border crossings that require registration will be changed in successive calculations.

Service levels

The service level is in itself a time factor and the service level compliance is the percentage of travellers for whom each service level is fulfilled. What is calculated in the simulations is the service level compliance. The simulation shows how compliance changes for a range of added durations to the border checks. The graph also shows results for different volumes of travellers.

It should be noted that the service level time includes the total average dwelling time for the travellers, not only the time for the border check.

The service levels have different values for air and land borders.

Average dwelling time

The dwelling time represents the amount of time the traveller has to use to complete the border check clearance including the queuing time. It is computed from the moment the traveller arrives at the border check area, till the completion of the border check. The results are presented in relation to the same values of the service levels. It is the measurement that represents what the traveller experiences while "waiting for crossing the border".

Workload (air borders)

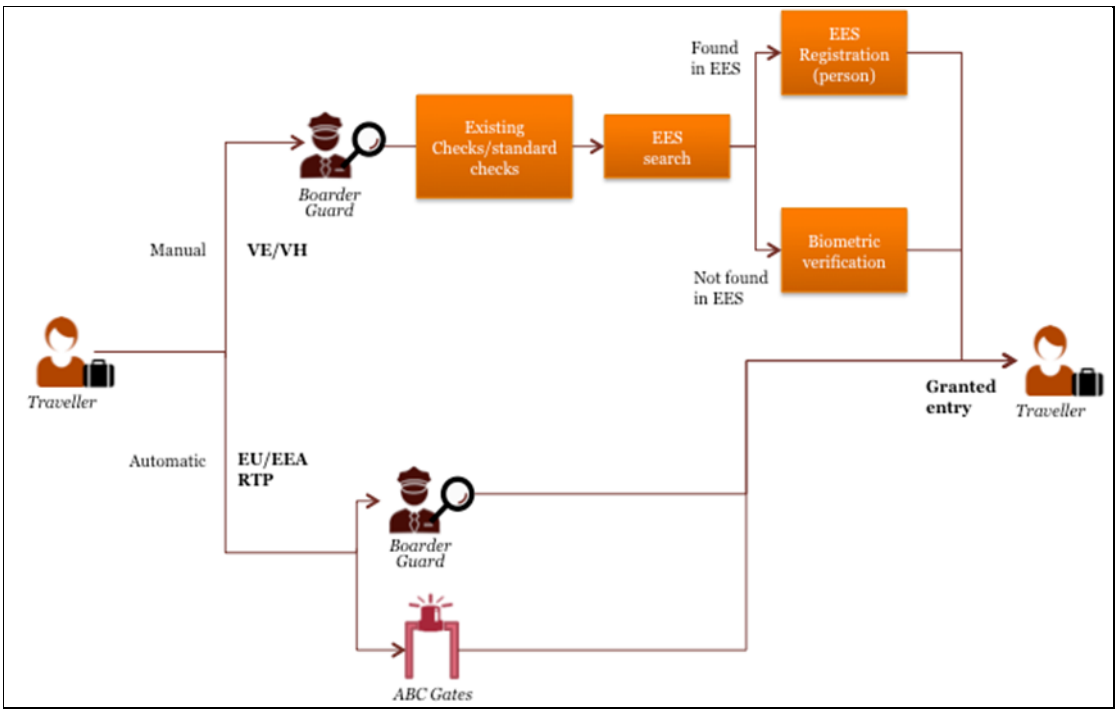
The workload included represents the total number of minutes of officer's time required to perform border checks at the manual booths in one natural day. The results were computed for workload related to the added time for the actual check.

Usage factor (land borders)

The measurement at land borders is not defined as workload but as something called a “usage factor” that shows the percentage of activity (i.e. when checks are being done) for the border guards. At land borders, the flow and peak patterns differ from air borders and there is a need for continuous manning of booths. The usage factors also indicate the need for resources to replace the person in the booth at certain intervals.

Model of the flow

The picture below shows the abstract model of the flow per category of traveller, including the EES and RTP. The picture shows the situation at entry. The only difference for the exit is that the step "registration in the EES" does not exist and only the step "biometric verification" takes place at exit. The "registration process" corresponds to what is called the "enrolment" of travellers.



The simulations were made for two types of borders: air borders and land borders. No simulation was run for sea borders due to practical constraints and the consideration that the majority of travellers pass via air (with a large proportion of VE) or land borders (with a large proportion of VH).

Model validation

In each case the model was applied to a real border crossing. In order to validate the simulation model the existing situation at the border was reproduced: current values for the parameters were introduced and the simulation produces current observed values of the outputs.

4.1.2. Simulation of air borders

Conditions

Real data from four filters[13], two for arrival and two for departure, at a large airport within the Schengen area were put into the simulation tool. This data comes from an average day within the busiest month of the year.

Two filters (in the text named “Arrival filter B” and “Departure filter D”) could be seen as very busy border crossing points comprising both manual booths and ABC gates; and the other filters (in the text named “Arrival filter A” and “Departure filter C”) as border crossing points with more moderate volumes.

The simulation is performed for "incoming flows" at arrival (travellers entering the Schengen area) and "outgoing flows" at departure (travellers leaving the Schengen area).

The data used in the simulation is the following:

[13] "Filters" is the word the model uses for border crossing points.

Volumes (traveller/day)		Simulations run
Arrival filter A No ABC gates, 5 manual booths	3 000	The volumes are estimated to increase up to 3500-4000 in the coming 5 years. This was taken into account in the simulation
Arrival filter B 6 ABC gates, 6 manual booths	10 000	The volumes are estimated to increase up to 11-12000 in the coming 5 years. This was taken into account in the simulation
Departure filter C No ABC gates, 6 manual booths	11 000	The volumes are estimated to increase up to 12-13000 in the coming 5 years. This was taken into account in the simulation
Departure filter D 6 ABC gates, 12 manual booths	21 600	The volumes are estimated to increase up to 24-25000 in the coming 5 years. This was taken into account in the simulation

The following split between categories of travellers was again taken from real data in that airport.

Categories (traveller)				
Arrival filter A	EU/EEA 69%	VE 15 %	VH 15 %	Premium 1%
Arrival filter B	EU/EEA 74%	VE 12.5 %	VH 12.5 %	Premium 1%
Departure filter C	EU/EEA 79%	VE 10 %	VH 10 %	Premium 1%
Departure filter D	EU/EEA 69%	VE 15 %	VH 15 %	Premium 1%

The term “Premium” (travellers) refers to fast-tracked travellers; they still go through the same checks however. Practically, it mainly refers to airline crews.

Variables explored

The variables to be explored in order to assess the impact of EES and RTP are presented in the table below.

Variables	Range of variation	Explanation
Percentage of border crossings of TCNs that require registration (called "enrolment step" in the process descriptions) of the individual file in EES	0-50 %	What is presented in the graph, in relation to this range are the values for 10% and 50 %.
Percentage of border crossings of TCNs who are already	0-10 %	The assumption is that RTP travellers have the

registered in the RTP		same border crossing time as EU/EEA travellers and that they use ABC gates when available
Time overhead for TCNs requiring registration of an individual file in the EES	Range of 0-180 sec	The values shown in the graphs are the average values of the potential additional time on top of the current border crossing time for performing the registration of the individual file in the EES.
Overhead for TCNs who need to be verified (not needing registration)	0-30 sec	This is the average value used for the potential added time to verify a TCN at entry/exit (the time for creating the entry/exit record is assumed to have a duration of 0 seconds)

The simulations were run for an extensive number of scenarios, exploring different values of the variants in the table above, to simulate what a day at an air border crossing point could look like after EES and RTP are implemented.

As an example, 1 400 simulations were run to obtain the data for airport filter A at arrival (entry). Up to 7 000 simulations were run, 5 times, in other cases, to capture the statistic variations.

Assumptions

Below are the values used for the time the border check takes today, not taking into account the implementation of EES and RTP:

EU/EEA = 15 sec (manual)

EU/EEA = 20 sec (ABC-gate)

VE = 30 sec

VH = 45 sec

These values are realistic values for the given airport. The simulation tool in addition attributes a duration to each border crossing that is stochastically distributed so that the mean value equals the values mentioned above for each category of traveller. This brings the simulation closer to the reality.

Results

The results were computed for the following areas:

- Service levels. For air borders the service levels used are the following:

  - SL 2 = 2 minutes. This is a very challenging service level that is only used for ABC gates.
  - SL 5 = 5 minutes. This is a very high requirement for manual lanes.
  - SL 10 = 10 minutes. This is the most frequently used service level: having 85 or 90% of travellers served within 10 minutes is considered as a very good achievement.

- Average dwelling time.

- Workload (air borders)

The results of the simulation are that an added duration of more than 60 seconds, at first entry, has the following impacts:

– A measurable impact on ”service level 2”, which has the objective of serving a traveller within 2 minutes. Once the additional tasks implied by EES equal 60 seconds, the decrease in service level becomes steeper;

– Service levels of 5 and 10 minutes are in principle not affected by the additional duration and very limited impact on the dwelling time;

– An impact of around 7% (at 60 seconds) on the workload necessary for the entry checks and around 11% (at 100 seconds).

The results further show:

– At first entry, an added duration of less than 60 seconds on average for the EES registration, using 30 seconds for verifications, shows a limited impact on the service levels defined for the case studied. The dwelling time increases by less than 16 seconds and workload increases by less than 9.4% (at 40 seconds the increase is around 4.5%);

– At subsequent entries and exits, an added duration of 30 seconds or less has in principle no impact on service levels, dwelling time or workload.

4.1.3. Simulation of land borders

The real data that was used represents one month of border traffic and comes from a 24h/24h operating land border crossing point with Russia. Only exit traffic was used in the simulation. Trucks and pedestrians are not included in the simulation for land borders. As regards trucks, the average checking time is around 30 minutes, mainly due to customs declarations and vehicle inspections, which makes it less relevant for the purposes of the simulation.

Three lanes with one booth per lane were used in the simulation and the vehicles were a combination of buses and private vehicles (motorbikes and private cars). Two lanes were used for private vehicles and one for combined buses and private vehicles. Checks take place while travellers stay in their vehicles (no need to step out). Most travellers are Russian citizens that are visa holders. It should be noted that neither the simulation nor the Study takes into account the potential change of this status. This is consistent with the assumption used throughout the Study that there are no (major) changes to the list of visa-exempt countries.

The land border concerned uses both a pre-reservation scheme (a border crossing timeslot is reserved in advance prior to arrival at the BCP) and a live queue (for those who show up at the BCP without a pre-reservation) for all vehicles.

Conditions

The set-up and conditions of the land border simulation are different from the air border simulation because a land border has different characteristics (a land border crossing point located on a road is used in this simulation).

The real data used in the simulation is the following:

Data used		Comment
Number of vehicles in month of observation	10 382	
Private vehicles	98%	The other vehicles (buses) have only a marginal occurrence, as at most land borders.
The chosen month's traffic in relation to the given year	9.1 % of yearly volume	The simulations were run for a month that is busier on average than the rest of the year, as the volume accounts for more than $1/12^{th}$ (8.3%) of the year.
Number of vehicles using the live queue	62%	
Number of vehicles using pre-reservation	38%	

The simulated border crossing is border checks at exit. Therefore, it is reasonable to use a potential added time of 30 seconds for the duration of the check against EES (biometric verification mainly) as a representative value. The time for added duration in the simulation is however per vehicle, which makes the comparison to the time it takes to verify 1 person more complicated. While preparing the simulation, it was seen that there was a certain degree of parallel activity and that the vehicles had an average occupancy of 1.5 to 2 persons. A value of 1 minute of added duration per vehicle could therefore be a representative value in this simulation. It should however be considered that if the occupants were to have to leave the car for such a verification, then the added time for the duration would presumably be longer.

Results

The simulation provides the results at exit as seen for the land border included in the simulation. This is a normal case because for the entry, the queue cannot be measured as it is occurring on the other side of the border in the neighbouring country. The results are related to service level fulfilment, dwelling time and workload and represent the results for the vehicles included in the simulation, passing through the specific border check.

The results were computed for the following areas:

- Service levels. In the case of land borders, the service levels are the following:
  - SL 10 = 10 minutes. This a very challenging service level for a land border of this type;
  - SL 30 = 30 minutes. This can be seen as the most representative service level for this type of land border.
  - For comparison, service levels of 60, 120 and 180 minutes were also simulated.
- Average dwelling time
- Usage factor (land borders)

The simulation is fully representative of the border crossing concerned, from where the real data and actual configuration of the border check were used.

The main result of the simulation is that for an added duration of 60 seconds per vehicle, at exit, has the following impacts would be measured:

– The impact on the situation at the border is dependent of whether the border crossing point already now is close to its nominal capacity or not;

– The impact is heavier when the border operates on 24h/24h basis as this eliminates situations of relief at the border post;

– The service level of 30 minutes decreases by around 2%, which represents around 35 seconds of added time for the total time of queuing and being checked (i.e. the so-called “dwelling time”);

– The dwelling time increases by around 3 %;

– The usage factor increases by 12 % points but this still leaves some margin to handle peak situations.

– A complicating factor, related to EES, would be if travellers needed to leave their cars for the biometric checks for instance.

4.1.4. Simulation of RTP

The simulation of the RTP could only be made at the air border. In this context RTP members are assumed to be able to use ABC-gates.

The summary takes into account the simulation conducted using arrival filter B and departure filter D (see section above on simulation of air border), with high volumes and equipped with ABC gates. The ABC-gate has a service level of 2 minutes and the manual service level is at 5 minutes, for comparison with the service level of the ABC-gate.

The simulated variable is the percentage of border crossings made by TCN travellers with RTP status. This value was changed from 0 to 25%.

Main results are:

– The use of ABC gates for RTP travellers makes it possible to keep a higher service level than at manual gates. The service level (2 min) used in the simulation includes dwelling time;

– The general trend is that the more crossings are made by RTP travellers, the more the service level compliance at manual gates improves, the shorter the dwelling time becomes and the lower the workload;

– The workload decrease when more than 12% of TCN border crossings is made by RTP subscribers can off-set part or the totality of the workload increase induced by the implementation of EES (additional first time enrolment and subsequent verification time).

4.2. Methodology used for Pilot Project

The Pilot (also referred to as Testing Phase or "the Project") took place under responsibility of eu-LISA, with the objective of verifying the feasibility of the options identified in the Technical Study and validating the selected concepts for both automated and manual border controls.

4.2.1. Objective

The main objective of the Testing Phase was to test the limited technical options identified within the Technical Study against specific measurable criteria, notably accuracy, effectiveness and impact on the border crossing duration in operational and other relevant environments. The Testing Phase was not aimed at testing full end-to-end EES and RTP systems.

4.2.2. Requirements set by Commission

The Testing Phase of the Proof of Concept was based on the Terms of Reference (ToR) issued by Commission, which determined which options should be tested and conditions to be met.

The following conditions were outlined:

- The Testing Phase needs to be conducted as a continuation of the Technical Study as they both belong to the same Proof of Concept exercise. Practically this means that in the documents produced within the framework of the Testing Phase changes to concepts and abbreviations will be avoided. It also means that similar project management roles are followed and that all results of the Technical Study can be re-used or referred to in the Testing Phase.

- The Testing Phase should be carried out in such a way that the impact of the change introduced by an option can be identified. Where applicable, the reference values will be measured (e.g. duration of a process or process steps, quality) before a change occurs and after the change is implemented.

- The selected BCPs (air, land and sea borders) should be representative of the variety of Schengen border conditions (e.g. border type, ABC gate types, land border with personal cars). Particular attention should be given to the special conditions found at land borders.

- The biometric devices to be used for the tests should already be on the market.

- Adequate data protection measures should be in place. The data collected for the test should be depersonalised and saved only locally and the retention of those data should be limited to the time necessary to produce the relevant statistics and analysis.

- The Testing Phase needs to be conducted in compliance with data protection provisions. Insofar as personal data are to be processed in the tests, eu-LISA will have to comply with Regulation (EC) 45/2001 and the Member States' authorities will have to comply with Regulation (EC) 45/2001, Directive 95/46/EC and the national implementations of this Directive 95/46/EC or other applicable data protection rules. In this regard, the European Data Protection Supervisor as well as, if necessary, national supervisory authorities should be involved.

- The tests will be conducted in compliance with fundamental rights, particularly the right to respect for private life, protection of personal data, dignity, non-discrimination (on grounds listed in Article 21 of the Charter, e.g. sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, disability or age). They will also have to ensure respect for vulnerable groups (such as children, unaccompanied children, disabled people, elderly people, pregnant women, single parents with minor children, victims of human trafficking, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture or other serious forms of violence).

- In order to have personal data processed, the data subject shall be informed of the type of data collected, the purpose of the processing and the controller's identity. The data subject shall explicitly and freely give his/her consent to participate in the test. The data subject shall also be informed of his/her right as a data subject in accordance with data protection law.

- The Testing Phase needs to be conducted in compliance with the existing legislation (e.g. the SIS II and VIS regulations, the Visa and Schengen Borders Code).

- Some Test Cases could be complemented with a stand-alone installation connected to a system simulating the relevant EES/RTP processes.

4.2.3. Test Cases

The Test Cases that were tested during the Testing Phase were based on the options outlined in the ToR, and presented in the table below.

Categories of options	Test Cases
• **Enrol biometrics for individual file in EES**	TC1 Enrol 4 fingerprints at first-line border check TC2 Enrol 8 fingerprints at first-line border check TC3 Enrol 10 fingerprints at first-line border check
	TC4 Enrol live facial image

	TC5 Enrol iris (including desk research regarding spoofing attempts and anti-spoofing measures for iris pattern enrolment)
• **Capturing FI from e-MRTD and verifying it against another source**	TC6 Capture Facial Image from e-MRTD TC7 Verify FI captured from e-MRTD against live facial image
• **Accelerators**	TC8 Search VIS by Travel Document Number TC9 Automated Exit Checks of TCNs TC10 Use of Self-Service kiosks TC11 Pre-border checks at Land Borders
• **Technical options**	TC12 Web-interfaces to the carriers and to the travellers TC13 Fall-back options

4.2.4. Testing approach

The testing approach took into account compliance with fundamental rights during the execution of tests:

1. At borders, persons must be checked in a manner which respects human dignity, regardless of the volume of traffic or the behaviour of travellers;
2. All border guards should receive refresher training on how to treat travellers respectfully and professionally as well as on the importance of remaining polite and formal in all situations;
3. Border guards should also pay attention to cultural and language differences when communicating with travellers. As a result, the tests will emphasise the languages that border guards are most likely to use, particularly English and the languages of the relevant neighbouring countries.

Three types of methodologies were employed, each achieving different purposes:

- Desk Research;
- Partial operational testing;
- Operational testing integrated in border control process.

For each methodology type, the following items were identified, recorded and guaranteed by a quality control process:

- Data source (e.g. traveller), data capture equipment (e.g. fingerprint scanner) and data capture method;
- Required data (e.g. fingerprint template) and data evaluation tool and process (e.g. NFIQ);
- Output (e.g. quality score) and expected or actual outcome (e.g. FAR/FRR);

- Time: the duration of the border crossing process and the atomic steps integrating the new TC step;
- Security and accuracy: the confidence in the identification decisions (e.g. passport authentication, biometric verification, bearer verification) made before, after and at the border;
- User acceptance: the perception of the travellers and the border guards.

During the Testing Phase other indicators were also recorded, such as exceptions and observations on complexity from a technical or organisational viewpoint. These indicators were consolidated and evaluated to propose measurable results based on the criteria outlined by the ToR.

Most of the Test Cases were addressed by several methodologies depending on the relevant question. In general, a combination of operational testing and desk research was performed.

Desk research

Desk research complemented the real life testing performed and it was applied in the following particular cases:

- For specific topics as specified by the ToR (e.g. anti-spoofing methods for the iris enrolment);
- When other projects / experiences have already provided meaningful findings;
- When it is impractical or non-feasible to perform real-life testing;
- When the timing and budget of the Proof of Concept does not make it possible to perform real-life testing.

In light of the above, a number of questions for each TC were addressed as desk research. These questions were categorised in the following domains:

- Cost of the solutions;
- Security (i.e. anti-spoofing and required supervision);
- Equipment (e.g. minimum requirements, environmental conditions influencing the performances, etc.);
- Process (e.g. for what type of border the kiosks are a suitable solution, what operations can be performed in a self-service kiosk by the traveller).

Additionally, the following Test Cases were addressed only through desk research:

- Searching VIS by Travel Document Number;
- Fall-back options;
- Web interfaces to carriers & travellers.

Partial operational testing

Partial operational testing was applied:

- When integration of equipment / system was not manageable or not practical (e.g. integration of kiosk in existing system, set-up of new ABC-gates);
- When a technical study was been requested by the ToR.

Concretely, this methodology made it possible to introduce the option to be tested with minimal changes to the actual border crossing process and made it possible to test the feasibility of the option in real life conditions.

Full operational testing at BCP (Border Crossing Point)

Full operational testing was applied:

- When the testing of the option was feasible in an operational environment;
- When Member States provided the necessary resources to perform the adequate adaptations and measurements (human resources, infrastructure, required time, border guards and operators).

The following methods were used for full operational testing at BCP:

- Measurement of the baseline indicators, coming from the existing process when applicable;
- Adaptation of the existing border crossing process to integrate with the existing process an option of the EES/RTP;
- Measurement of the change indicators, coming from the new process;
- Calculation of the difference between the existing process and the new process.

4.2.5. Time Measurement

One of the main objectives of the testing was to assess the impact of the proposed changes to the current border crossing process in terms of duration.

Durations to be measured

Baseline measurement: in order to gauge the impact in terms of duration, it was necessary to also measure the baseline for the "as-is" process. The baseline measurement was mostly relevant for the end-to-end duration of a process; however, in some cases it appeared necessary to measure it for certain atomic steps, in order to correct the end-to-end time measured (either by adding or subtracting average durations). According to the ASQ Performance (ASQP) programme of Airports Council International[14] (ACI)'s a minimum sample size of 100 is considered sufficient.

Duration of atomic steps: the duration of new or changed steps.

This includes:

- Biometric capture (FPs, FI, iris). The duration of the failed attempts will be also registered.
- Retrieval of the FI from the e-MRTD
- Verification of live FI against FI from e-MRTD

End-to-end duration: the duration of the entire border crossing process, from start to end, was measured where relevant (i.e. if the test is part of the real process and not

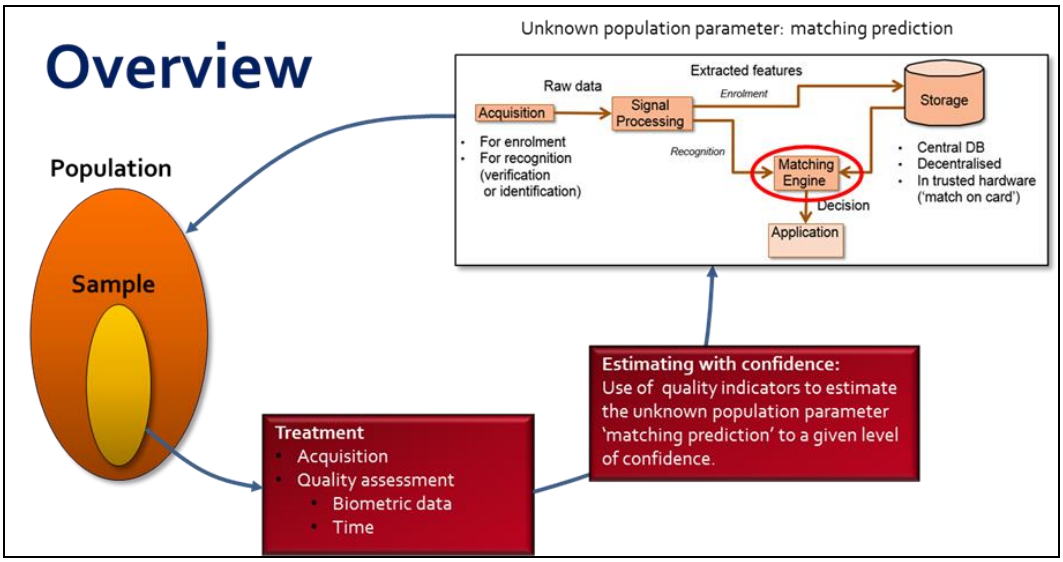
[14] ACI World Facilitation and Services Standing Committee recommended practice 300A12: manual measurement of passenger services process time and KPI's drafted by ACI World secretariat and DKMA.

performed in an isolated and stand-alone manner). The main focus was to determine the differences obtained at various BCPs between the "as-is" process and the proposed "to-be" process.

4.2.6. Biometric Quality Measurement

The approach to biometric performance assessment can be summarised as "estimating with confidence". Biometric data was acquired from a sample amount of travellers, which was sufficient to allow a reliable estimation of the performance of a biometric system. During the Pilot, as no actual matching was done (except for facial biometrics), estimation was based on the quality of the data captured. The approach was based on the following steps:

- The selection of quality indicators for the different biometric characteristics within the scope;
- The selection of confidence level and sample size;
- The preparation and execution of the data processing, i.e. the actual acquisition and quality assessment of biometric data;
- The estimation with confidence of the matching prediction for both verification and identification against galleries of different sizes.



Overview of the "estimating with confidence" approach for biometrics

When "estimating with confidence", a confidence interval was used to estimate an unknown population parameter. It is an interval that has the form "estimate +/- margin of error" and has a confidence level property. In such a setting:

- The "estimate" is the guess for the unknown population parameter. The estimate is based on the outcome of the biometric quality assessment, e.g. NFIQ for fingerprints.
- The margin of error *m* reflects how accurate we believe our guess is. The margin of error of a confidence interval for the mean of a normal population is easily

calculated for a given confidence level (e.g. 99%) by $m = z * \frac{\sigma}{\sqrt{n}}$. The terms used are defined below[15].

- If the population is not normal, a bootstrap can be used to understand the distribution. However, eu-LISA calculations indicated that, for the current BMS (Biometric Matching System) quality score data, the distribution is approximately normal. The assumption is therefore made that quality scores will generally be distributed normally irrespective of the algorithm used for quality assessment.

A confidence level expresses how frequently the observed interval contains the parameter. This value is represented by a percentage, so the statement, "we are 99% confident that the true value of the parameter is in our confidence interval" expresses that 99% of the observed confidence intervals (samples) holds the true value of the parameter.

4.2.7. Target sample size

The overall principle for the choice of sample size is finding the right balance between the available resources for the test, passengers' throughput per BCP and the desired accuracy[16] to make conclusions about the population from the sample.

During the execution of the Testing Phase, the amount of passengers per each Test Case at each BCP was monitored and compared against the target sample size. This allowed the testing team to make any necessary adjustments during the execution (e.g. add extra staff, improve information activities).

The table below indicates a target sample size for each TC per each BCP in order to reach representativeness, as requested in the ToR.

		4FP + FI	8FP + FI	10FP + FI	Live FI	Iris	FI e-mrtd	of FI against other	ABC exit	Kiosk	Kiosks (waiting areas)
Country	**BCP**	**TC1**	**TC2**	**TC3**	**TC4**	**TC5**	**TC6**	**TC7**	**TC9**	**TC10**	**TC11**
Sea											
EL	Port of Piraeus	600	1000	1550	1550		1550	1600			
FI	Helsinki port	600	1000		1550		1550	1600	1000	1000	
FR	Cherbourg	600			1550	1550					
IT	Genova	600			1550		1550	1600			
Air											
DE	Frankfurt	600	1000	1550					1000		
ES	Madrid	600			1550		1550	1600		1000	
FR	Charles de Gaulle		1000		1550		1550	1600	1000		

[15] σ = standard deviation, n = sample size and z* = the value on the standard normal curve with the area corresponding to the confidence level between –z* and + z*.

[16] The desired accuracy of the population parameter is expressed as the width of the confidence interval or, equivalently, as the margin of error (half the width).

NL	Schiphol	600	1000	1550					1000		
PT	Lisbon airport					1550			1000	1000	
SE	Arlanda				1550		1550	1600			
Land: train											
FR	Gare du nord		1000		1550		1550	1600	1000		
RO	Vicșani		1000		1550		1550	1600	1000		
Land: road											
EE	Narva								1000		1000
EL	Kipoi Evrou	600	1000	1550		1550					
FI	Vaalimaa	600	1000	1550	1550		1550	1600			
HU	Udvar	600	1000	1550							
RO	Sculeni				1550	1550	1550	1600			

Target sample size for each TC per each BCP

5. ANNEX 5: SUMMARY OF PROCESSES AT ENTRY/EXIT ACCORDING TO CURRENT SCHENGEN BORDER CODE

EU citizens and persons enjoying the Union right of free movement

EU citizens and other persons enjoying the Union right of free movement (e.g. family members of EU citizens holding a visa or a residence card) crossing the external border are subject to a minimum check, both at entry and exit, consisting of the verification of the travel document in order to establish the identity of the person. Such a minimum check comprises the verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting.

In addition, on a non-systematic basis, national and European databases may be consulted in order to ensure that such persons do not represent a genuine, present and sufficiently serious threat to the internal security, public policy, international relations of the Member States or a threat to the public health.

The travel document of this category of persons is not stamped at entry and exit, with the following two exceptions which are subject to stamping:

- nationals of third countries who are members of the family of a Union citizen to whom Directive 2004/38/EC applies, who are admitted for a stay but who do not present the residence card provided for in that Directive

- nationals of third countries who are members of the family of nationals of third countries enjoying the right of free movement under Union law, who are admitted for a stay but who do not present the residence card provided for in Directive 2004/38/EC

Third Country Nationals (TCN) who do not exercise their right of free movement and who are admitted for a short-stay

Third Country Nationals (TCN) who do not have a residence permit or a long-stay visa issued by a Member State are admitted for a short stay of maximum 90 days within any period of 180 days (hereinafter referred as the "90/180 day" rule). This applies both for those who are subject to the visa obligation and those that are not. TCN admitted for short stays represent the majority of border crossings.

As described in the table below; these third-country nationals are subject, at entry, to a thorough check which, in addition to a bearer verification and more thorough travel document check, convey the following additional checks: that at their entry they still respect the "90/180 rule", their point of departure and destination and the purpose of their stay, the possession of sufficient means of subsistence, as well as a search in the Schengen Information System (SIS) and in relevant national databases.

– Verifying at entry (and also at exit) that the "90/180 rule" is met, currently the verification can only be based on the entry and exit stamps in the passport. In practice this is a very impractical exercise as stamps of Schengen countries may be mixed with stamps of other countries. Stamps may be difficult to read and anyhow different periods of stay might be combined.

– In addition, TCN with the citizenship of a country on the list of visa-required countries (TCN-VH)[17] need to have a valid visa delivered by a Schengen Member State in accordance with the provisions of the Visa Code[18]. Accordingly, for these travellers, border guards perform an additional check as they verify the validity of the visa as well as the identity of the holder of the visa and the authenticity of the visa, by consulting the VIS, using fingerprints and the visa sticker number.
Indeed, since 11 October 2014, border guards ascertain that each visa holder is the owner of the visa-sticker affixed in his/her passport by verifying whether one, two or four fingerprints of the traveller match with the fingerprint set enrolled in the Visa Information System (VIS). The fingerprints were enrolled at the moment of applying for the visa in the consular post of a Schengen Member State.
By the end of 2015, the so-called VIS "roll-out" will be completed and all consular posts will register both the visa information and the required biometric information in the VIS.

– For all third country nationals, once the border guard authorises the border crossing, the passport is stamped marking the date and place of entry. In case entry is refused, the border guard affixes an entry stamp on the passport, cancelled by a cross in indelible black ink, and writes a code letter corresponding to the reason for refusing entry.

– At exit, the checks on TCN do not include the verification of their point of departure and destination and the purpose of their stay; nor the possession of sufficient means of subsistence. In addition, some checks are optional (the verification that the person is in possession of a valid visa; the verification that the person did not exceed the maximum duration of authorised stay in the territory of the Member States; and the consultation of alerts on persons and objects included in the SIS and reports in national data files). The verification that the third-country national is not considered to be a threat to public policy, internal security or the international relations of any of the Member States shall be carried out whenever possible;

Of relevance here is that the travel document is stamped at exit. It is by comparing the date of exit with the stamp at entry that overstayers are identified.

	Entry/ Exit	TCNVEs TCNVHs	Description
Bearer verification (Article 7(2) SBC)	Entry Exit	✓	Checks made to secure that the bearer of the travel document is the lawful owner of the document, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents.
Travel document check (Articles 7(3)(a)(i),	Entry Exit	✓	• Verification that the TCN is in possession of a valid travel document entitling the holder to cross the border satisfying the following criteria:

[17] Council Regulation (EC) No 539/2001* of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and t those whose nationals are exempt from that requirement (OJ L 81, 21.3.2001, p. 1).

[18] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1)

7(3)(a)(ii), 7(3)(b)(i), 7(3)(b)(ii) and 5(1)(a) of the SBC)			○ its validity shall extend at least three months after the intended date of departure from the territory of the Member States. In a justified case of emergency, this obligation may be waived; ○ it shall have been issued within the previous 10 years. • Verification that the travel document has not expired, • Thorough scrutiny of the travel document for signs of falsification or counterfeiting.
Visa check (if applicable) (Articles 7(3)(a)(i), 7(3)(aa), 5(1)(b), 7(3)(c)(i) and of the SBC)	Entry Exit - *optional*	*Only TCNVHs*	• Verification that the travel document is accompanied, where applicable, by the requisite visa • Verification of the validity of the visa • Verification of the identity of the holder of the visa and of the authenticity of the visa, by consulting the VIS, using fingerprints and the visa sticker number.[19]
Stamp check (Articles 7(3)(a)(iii) and 7(3)(c)(ii) of the SBC)	Entry Exit (optional)	✓	Verification that the person has not already exceeded the maximum duration of authorised stay. For that purpose, entry and exit stamps are checked and the duration of previous stay is calculated manually

Questions
(Articles 7(3)(a)(iv) and (v) of the SBC)
	Entry	✓	• Questions are asked as regards:
			  • the point of departure and the destination;
			  • the purpose of the stay;
			  • sufficient means of subsistence for the duration of the stay and the return to the country of origin.
			• If necessary, the concerned supporting documents are checked (e.g. tickets, hotel reservations or invitations to meetings).

Verification on the person, means of transport and objects transported **(including SIS II consultation on alerts)** (Articles 7(3)(a)(vi), 5(1)(d), 5(1)(e) 7(3)(b)(iii) and 7(3)(c)(iii) of the SBC)	Entry Exit - *optional*	✓	Verification that the person, his/ her means of transport and the objects she/he is transporting are not likely to jeopardise the public policy, internal security, public health, or international relations of any of the Member States or that not allowed in the Schengen area Verification that there is no alert on SIS II on the person for the purpose of refusing entry. This verification includes a consultation of SIS II and other relevant systems
Stamping (Articles 10(1) and 13 and Annex V, part A, paragraph	Entry Exit	✓	The passport is stamped on entry and exit. Where entry is refused, the border guard affixes an entry stamp on the passport, cancelled by a cross in indelible black ink, and write opposite it

[19] Fingerprints are mandatory as of October 2014.

1(b)			on the right-hand side, also in indelible ink, the letter(s) corresponding to the reason(s) for refusing entry.
Second line checks and actions (Article 7(5) of the SBC)	Entry Exit	✓	Depending on the results of the checks, further verifications may be carried out in a special location away from the location at which all persons are checked (first line).

– The average border crossing time at entry for visa-exempt TCN is estimated at 63 seconds at entry (so about four times more than for an EU citizen) and for a visa-required TCN at 104 seconds at entry (so about seven times more than for an EU citizen). The average border crossing time at exit for visa-exempt TCN is 53 seconds (3,5 times more than for an EU citizen) and 71 seconds for a visa-required TCN (so five more than for an EU citizen). As a consequence although 34% of border crossings are due to TCN, they account for more than 60% of the workload for border guards.

TCN with a long-stay visa

TCN with a long-stay visa issued by a Member State are also submitted to a thorough check. Long-stay visas are not submitted to the "90/180 days rule" of the short-stay visas as this duration of stay is precisely the differentiating factor. Long-stay visas are also not recorded in VIS, hence up to now the correspondence between the person who applied for the visa and the bearer is done on the basis of the photo. Long-stay visas are stamped at entry and exit. Like for all TCN, systematic checks are performed vs SIS II and national databases at the moment of border crossing.

TCN with a residence permit

TCN who travel with a residence permit are also submitted to a thorough check.

Residence permit holders are not submitted to the "90/180 days rule" of the short-stay. The permits are not recorded in VIS.

In addition, residence permit holders are as a general rule neither subject to the question on sufficient means of subsistence for the duration of the stay and the return to the country of origin, nor on the questions on the purpose of the stay.

Like for all TCN, systematic checks are performed vs SIS II and national databases at the moment of border crossing.

6. ANNEX 6: COST MODEL FOR SMART BORDERS SYSTEM

6.1. Cost Model

In 2014 as part of Technical Study a revised cost analysis was developed in order to provide up-to-date, reliable cost estimates of the EES and RTP systems to be borne at the European Commission (central) and Member State (national) level covered by a central envelope (ISF/Smart Borders line). The figure below details the split between the costs to be covered by the central envelope and those to be covered by Member States' budgets (National budgets or ISF/National programs).

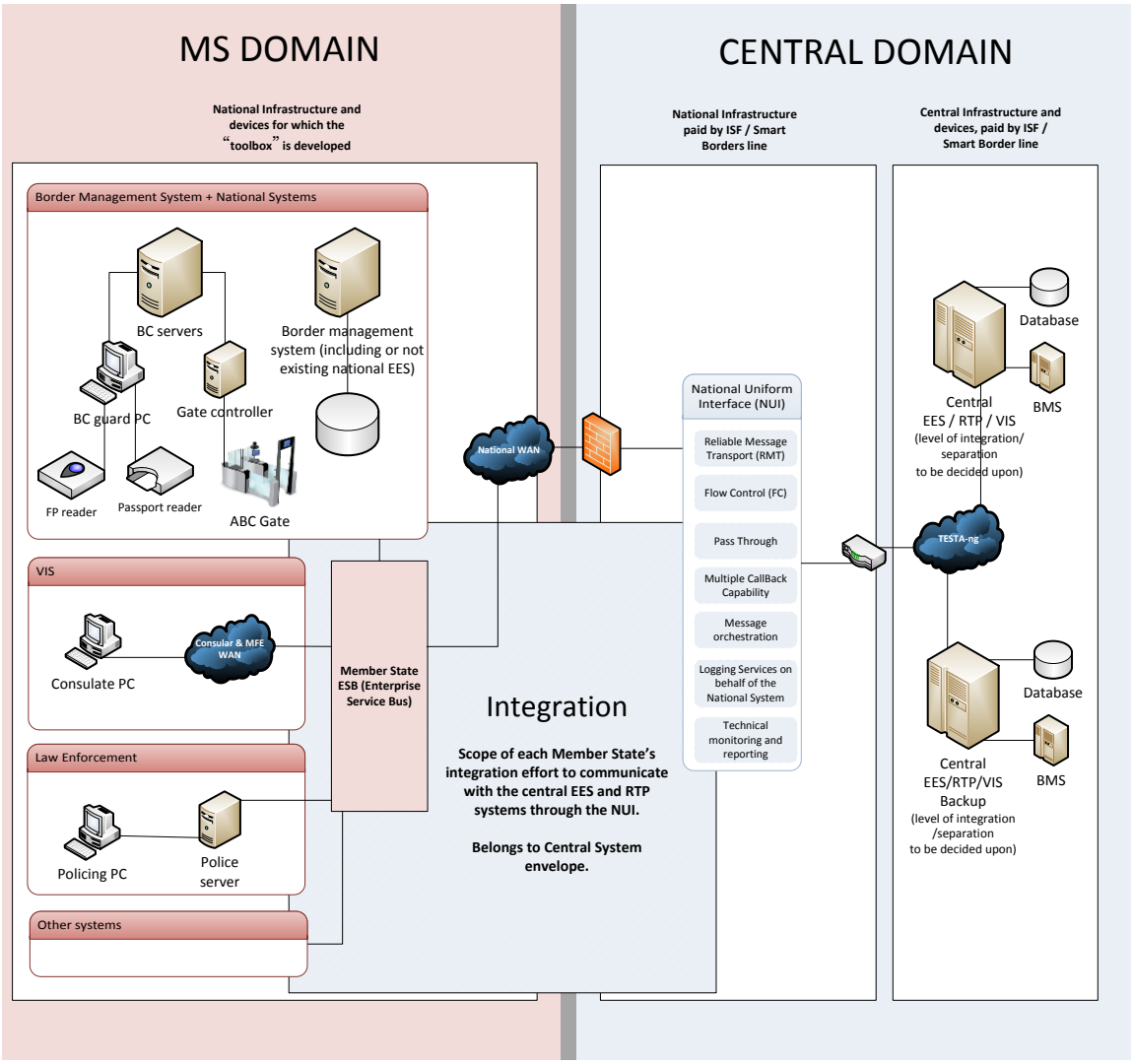


Figure: Split between the Central Envelope and Member States' budgets for the infrastructure of the EES and RTP systems. Blue sections (Central Domain and Integration) would be covered by the Central Envelope; pink sections would be covered by the Member State's own budgets or the National Programmes of the ISF borders/Smart Border Line.

The cost model developed and described in the Cost Report that is part of the 2014 Technical Study, contains a set of main assumptions and options.

Overall a cautious approach has been used throughout the report regarding cost estimation. This approach is aimed at avoiding underestimation of the final costs.

As this cost model is developed at a moment when only a concept of the Smart Borders system exists figures cannot be better estimated than with a 15 to 20% margin despite being accurate.

The following general assumptions were used for developing the model:

- Financial timeline: EES and RTP development period is expected to last three years, assumed to start in 2017 and ending in 2019. Both systems are expected to become operational in 2020.

- Benchmark with existing systems: The VIS and the SIS II provide benchmark data when relevant, as they operate in a comparable environment to that of the future EES and RTP. Experience values for contractor development cost were also taken from large-scale IT systems in other areas than Home affairs.

- National Uniform Interface (NUI): The assumption is that a NUI will be developed to provide the interface between the Member States (MS) and the Central System. The NUI enables Member States to connect to the Central System without having to develop and deploy their own infrastructure, reducing the complexity and the costs of the project. An envelope of €4 m is provisioned for each MS to cover the integration effort from their existing infrastructure to the central system. This option reduces the costs to be borne on Member States' side as the development costs of the NUI are shifted to the central side.

- SOA (Service Oriented Architecture)-based BMS (Biometric Matching System): the assumption is that a new SOA-based BMS serving the needs of VIS, EES and RTP will be developed.

- Number of Member States: 30 countries. This is the same assumption as in the 2013 proposal.

- Central Unit / Backup Central Unit (CU/BCU) configuration: the setup between two nodes is considered to be active/passive. This is also the current way the back-up sites of SIS II and VIS are designed. It means that only CU handles the transactions (active node) and that the BCU is only permanently updated so to remain in "hot" stand-by. In case the CU would be destroyed (or unavailable for a long time), the BCU takes over all operations. For cost purposes the investments in hardware and software are doubled compared to the situation where there is one single central unit and the cost for a redundant high-speed and high-capacity link between both sites is added to.

6.1.1. Cost comparison between different biometric options

The same study further identified three different TOMs (Target Operating Models) for EES and two TOMs for RTP. The three TOM's for EES correspond with the different biometric choices. The two TOMs for RTP correspond to the option (a) and (b) for doing the RT application.

EES:

- TOM A – Facial image from e-MRTD (Machine Readable Travel Document) as biometric identifier and relying on MRZ (Machine Readable Zone) (plus visa number for Visa Holders (VH)) as data for EES. Absence of systematic 1:N identification at first entry for TCNVE.

- TOM B – Facial image from e-MRTD and 4 fingerprints as biometric identifiers and relying on MRZ (plus visa number for VH) as data for EES. Systematic 1:N identification at first entry for TCNVE.

- TOM C – Facial image from e-MRTD and 8 fingerprints as biometric identifiers and relying on MRZ (plus visa number for VH) as data for EES. Systematic 1:N identification at first entry for TCNVE.

RTP:

- TOM M – Fingerprints (live)-only for VE- and photo (from e-MRTD) as biometric identifier for RTP. For VH, the FP used in the VIS will be used as the basis for verification and identification. In this TOM the enrolment of an RTP follows the process from the current legal proposal, which is very close to a visa application process: RT status is requested by the applicant (and this can be done via internet), interview with applicant takes place where his/her biometrics are captured (the number is equal to what the TOM A, B, C requires) and this cannot be done via internet, MS instructs the request and grants/refuses RT (this can also happen over internet).

- TOM N – No biometrics taken at enrolment (i.e. no physical visit necessary), existing biometrics (EES and VIS) used for verification purposes. In this TOM the enrolment of an RTP is only possible when the TCN has already travelled to EU Schengen area and is therefore recorded in the EES. The RT status is requested by the applicant via internet, no face to face meeting is necessary anymore as the applicant can provide all evidences via internet and the biometrics are in the EES personal file. Finally MS instructs the request and grants/refuses RT (this can also happen over internet).

TOM C and M are taken as the baseline for the calculation of the costs of the EES and RTP projects, as they are the most cautious in terms of costs as well as the closest to the existing legal proposals. In this section, the study evaluates the cost impact of the other TOMs on the overall project.

The general impact of TOMs is split between the cost components of the project. The study looked into each impacted cost component to provide an estimate of the cost impact of each TOM. The results will be presented as a fixed figure where possible, or as a percentage of the cost component.

The results are presented in the table below (comparison of costs over 4 years: 3 years development and one year operations):

	TOM A		TOM B		TOM C (baseline)	
	TOM M	TOM N	TOM M	TOM N	TOM M (baseline)	TOM N
EES	€214.3 m	€214.3 m	€225.2 m	€225.2 m	€226. m	€226. m
	95%	95%	100%	100%		100%
RTP	€194.6 m	€194.1 m	€204.4 m	€203.8 m	€204.4 m	€203.8 m
	95%	95%	100%	100%		100%
EES and RTP	€359.3 m	€358.8 m	€379.6 m	€378.3 m	€381. m	€379.1 m
	94%	94%	100%	99%		99%

This table supports the conclusion that the cost difference of the choice of the biometric identifier for EES and RTP enrolment solution is only significant when the facial image without fingerprints would be selected. The difference is however not more than 6% for the 4-year accumulated cost but which represents €22,2 million.

6.2. Marginal Cost of RTP

The cost model was developed in order to compute the cost for EES and RTP are each built as a system on its own and when EES and RTP are built as one system. In this last case, two major cost items being the BMS costs and the integration cost of the National Uniform Interface (NUI) are shared 50%-50% over both systems. The cost model does not provide the straightforward answer on how much RTP would cost if it was considered as "added" to the EES. In this case the major differences are that BMS and NUI development and integration costs are allocated 100% to EES, and that RTP network costs do not include the network set-up costs.

In order to compute the marginal cost of RTP, the difference needs to be made for the cost of EES and RTP built as one system and the cost for building EES alone. The cost model was first used to compute the cost of EES and RTP built as one system using 4 fingerprints and facial image as biometric identifiers and a data retention period of 5 years. Then the cost model was used for computing the cost of EES alone with the same assumptions of 4 fingerprints and facial image as biometric identifiers, a data retention period of 5 years, and costs for BMS (Biometric Matching System) and NUI (National Uniform Interface) allocated completely to this system. The results of both computations were then subtracted which gives:

Marginal of Cost of RTP (in million €)	Total (4 years)	Operational costs 2021 (2nd year)	Operational costs 2022 (3rd year)	Operational costs 2023 (4th year)	Total (7 years)
Total Central System	14,78 €	1,80 €	2,29 €	2,05 €	20,92 €
Total National Systems	59,31 €	19,71 €	19,71 €	19,71 €	118,44 €
Total envelope	74,09 €	21,51 €	22,00 €	21,76 €	139,36 €

Summary of the marginal costs of RTP obtained as the difference between the cost for EES and RTP as one system and the cost of EES alone

The result of this computation is that the **marginal cost of RTP** is estimated as € 74,09 million over four year (sum of € 52,58 million development cost and € 21,51 million operations costs for the first year - the details of this computation are not shown above). The cost of yearly operations is strongly impacted by the assumption that per Member State a small team of operators needs to be dedicated to RTP operations on a 365/24/7 basis (meaning to ensure a permanent service throughout the year).

The calculation of the marginal cost of the RTP system was done under the assumption of using TOM N (this is the operational model assuming the traveller has already been recorded in EES and therefore biometrics can be re-used). For the cost of the RTP system there is however only a marginal (like 1%) difference with the situation where TOM M would be used (this is the operational model where the traveller applies for Registered Traveller's status even before travelling, his/her biometrics are taken separately).[20]

[20] See "Technical Study on Smart Borders – Cost Analysis" section 3.4 and accompanying tables: "TOM N does not have an important impact on the cost on the central envelope. The main purpose of TOM N being to rely on the EES for biometric matching of RTP members, and making online RTP enrolment compulsory, the impact is going to be felt on the national side as opposed to the central side, as RTP applications would be received directly online, reducing the need for administrative officers to deal with requests at the consular or administration post".

6.3. Cost of Preferred Solution

For computing the cost of the preferred solution, the following **specific assumptions** were applied to the cost model:

- Architecture: only one system is built (the Entry Exit System) and the development of a specific RTP is discarded. For the cost model this means that the EES has to bear the full BMS and NUI-related costs which were otherwise shared with RTP as these are two common architecture components.

- Architecture scope. The cost model has been amended to include the cost for having a fall-back solution whereby transactions are buffered at the level of the location(s) or Member State(s) from where the central EES was unavailable and released once the central EES can be accessed again. The cost model also includes the development and operations of a web-service for information to travellers and carriers.

- Architecture: the cost model has been adapted in order to take into account technical options for ensuring interoperability and system availability.

- Biometrics. The preferred solution assumes that the facial image and four fingerprints are taken as a biometric identifier. This corresponds to what is called the Target Operating Model B in the cost report. This model also assumes a systematic 1:n identification at first entry for visa-exempt third country nationals.

- Facilitation. The assumption is made that facilitation will use the "fast lane for all" concept. This concept does not impact the costs included in this model apart from giving the rationale for discarding a specific RTP.

- Retention time. A five-year data retention time for all travellers (visa-required and visa-exempted) is assumed. This has an important consequence on costs as the database accumulates data over 5 years and this impacts storage capacity and the cost of some specific software, like BMS, which evolves according to data volume.

- Law Enforcement access is granted from the beginning. This does not impact the cost model in an important way. The only significant cost impact stems from adding the capacity to BMS to also search on latencies.

The result of the cost model is provided on the following page. The **development cost** to be borne by the EU budget amounts to **€394,77 million, split as €222,10 million for the central system (including the National Uniform Interface) and €172,67 million for the (thirty) national systems (including the technical integration of national systems with the National Uniform Interface). This is the cost accumulated over the estimated three years required to build the system**. In addition, changes would be required to VIS (to establish interoperability between EES and VIS) and SIS (for the creation of an alert for overstayers not found at the end of the EES data retention period), which have been estimated as €40 million development cost and no additional operational costs.

The first year of operations the EU budget would bear a total operations cost of €45,47 million split as €25,76 million for the central system and €19,71 million for the (thirty) national systems.

When comparing with the MFF, the cost to borne by the EU budget amounts to €480,2 million over 4 years (3 years development and 1 year operations). This is the same amount as included in the financial annex to the legal proposal.

EES Development Cost

	2017	2018	2019	Total Develop-ment Cost	2020	Total over 4 years
Development Central System						
Contractor development	32.650.130	32.650.130	35.265.130	100.565.391	0	**100.565.391**
Software	8.051.249	0	46.559.996	54.611.245	3.555.000	**58.166.245**
Hardware	4.753.537	0	22.852.995	27.606.532	0	**27.606.532**
Administration	1.898.000	1.898.000	3.530.500	7.326.500	0	**7.326.500**
Set Up Data Center	219.336	0	0	219.336	0	**219.336**
Meetings/Training	816.000	816.000	1.740.936	3.372.936	327.370	**3.700.306**
	48.388.252	**35.364.130**	**109.949.557**	**193.701.940**	**3.882.370**	**197.584.310**
Maintenance Central System						
Contractor operations	0	0	1.734.254	1.734.254	1.748.254	**3.482.509**
Software	1.342.866	1.342.866	9.101.711	11.787.443	9.938.811	**21.726.254**
Hardware	568.525	568.525	2.925.348	4.062.397	3.585.748	**7.648.144**
Administration	0	0	0	0	4.208.000	**4.208.000**
Running costs Data Center	0	90.202	90.202	180.403	90.202	**270.605**
	1.911.391	**2.001.592**	**13.851.514**	**17.764.497**	**19.571.015**	**37.335.512**
Communication Infrastructure (Network)						
Network development	4.122.530	0	210.000	4.332.530	0	**4.332.530**
Network operations	1.995.303	1.995.303	2.310.303	6.300.908	2.310.303	**8.611.210**
	6.117.833	**1.995.303**	**2.520.303**	**10.633.438**	**2.310.303**	**12.943.740**
Total Central System	**56.417.475**	**39.361.025**	**126.321.374**	**222.099.874**	**25.763.687**	**247.863.562**

	2017	2018	2019	Total Develop-ment Cost	2020	Total
Integration in Member States						
Contractor development (integration of NUI)	40.000.000	40.000.000	40.000.000	120.000.000	0	**120.000.000**
Administration	16.236.000	16.236.000	20.196.000	52.668.000	0	**52.668.000**
Operations of National Systems						
Administration	0	0	0	0	19.710.000	**19.710.000**
Total National Systems	**56.236.000**	**56.236.000**	**60.196.000**	**172.668.000**	**19.710.000**	**192.378.000**

Total EES (including SIS/VIS adaptations)				**394.767.874**	**45.473.687**	**440.241.562**
SIS/VIS adaptations		20.000.000	20.000.000	40.000.000		**40.000.000**
Total EES (including SIS/VIS adaptations)						**480.241.562**

7. ANNEX 7: COMPARISON OF OPERATIONAL ASPECTS OF DIFFERENT BIOMETRICS

Option	Fingerprints (FP) only	Fingerprints (FP) and facial image (FI) combined	Facial image (FI) only	Iris and facial image (FI) combined
Stability	FP are stable from the age of six years onwards. Enrolled FP remain valid for many years.	See column on the left for FP and on the right for FI.	FIs are more stable as the person gets older. FI loses its relevance as a reference biometric over time: 10 years is seen as a maximum while 5 years is the preferred option for renewal.	Iris is a stable biometric from a few days after birth and throughout life. See previous column for FI.
Enrolment	The more FP (1,2,4,8 or 10) are enrolled the more time it takes. Taking 8 FP's takes about two times more time than 4 FP's. Taking 10 FP's takes about three times more time than 4 FP's. Environmental conditions (weather, type of border) can make practically impossible the enrolment of more than 4 FP even with high performance equipment. Taking 1, 2 or 4 FP's takes about	The enrolment time and complexity is the combination of both. FI and FP can be taken at the same place and can even be combined to some extend so that enrolment time does not cumulate.	A quality FI can be taken fairly quickly in all situations.	When iris is taken at a distance, the enrolment time is fast and FI is the biometric that is considered to be "obtained for free" as the software driving the camera needs to recognise a face first before zooming in on the eyes to capture the iris pattern. The camera for FI and iris pattern capturing is not the same but both are combined in the same device. When iris is not taken at a distance the enrolment times of

Option	Fingerprints (FP) only	Fingerprints (FP) and facial image (FI) combined	Facial image (FI) only	Iris and facial image (FI) combined
	the same time and is possible in all environmental circumstances.			taking the iris pattern and the facial image cumulate as they happen in front of different devices.
Verification	In practice, 1, 2 or 4 FP are sufficient for a reliable and fast verification. (Note: at least the same number of verified FP needs to have been enrolled)	Using both FP and FI does not improve verification. One of the two biometric identifiers is enough for that purpose.	FI is enough for a reliable and fast verification, because verification only matches the FI with the live picture of a particular person.	Using both iris and FI does not improve verification. One of the two biometric identifiers is enough for that purpose
Identification for inland controls	At least 4 FP are required for a reliable identification on a 100 million gallery size.	At least 2 FP and FI are required for a reliable identification on a 100 million gallery size	FI can only be used for identification on a 1 million gallery size.	The iris pattern taken at a distance and FI allow a reliable identification on a 100 million gallery size. However the reliability percentage is inferior to the obtained using 4FP's and a FI.
Identification at the border (when required processing capacity is available)	At least 8 FP are required for a fast and reliable identification on a 100 million gallery size	At least 4 FP and FI allow a fast and reliable identification on a 100 million gallery size	FI alone is not suited for that purpose. Increasing processing capacity does not solve the issue.	
Exceptions	Experience with VIS shows that about 2% of travellers have no FP mainly because these are worn out (result of heavy manual work).	See column on the left for FP's and on the right for FI. The FI acts as a "fall-back" in case no FP can be taken.	None: a facial image can be taken from all travellers ("everybody has a face")	Iris is difficult to take for a small portion of population. See column on the left for FI. The FI acts as a "fall-back" in case no iris can be taken.

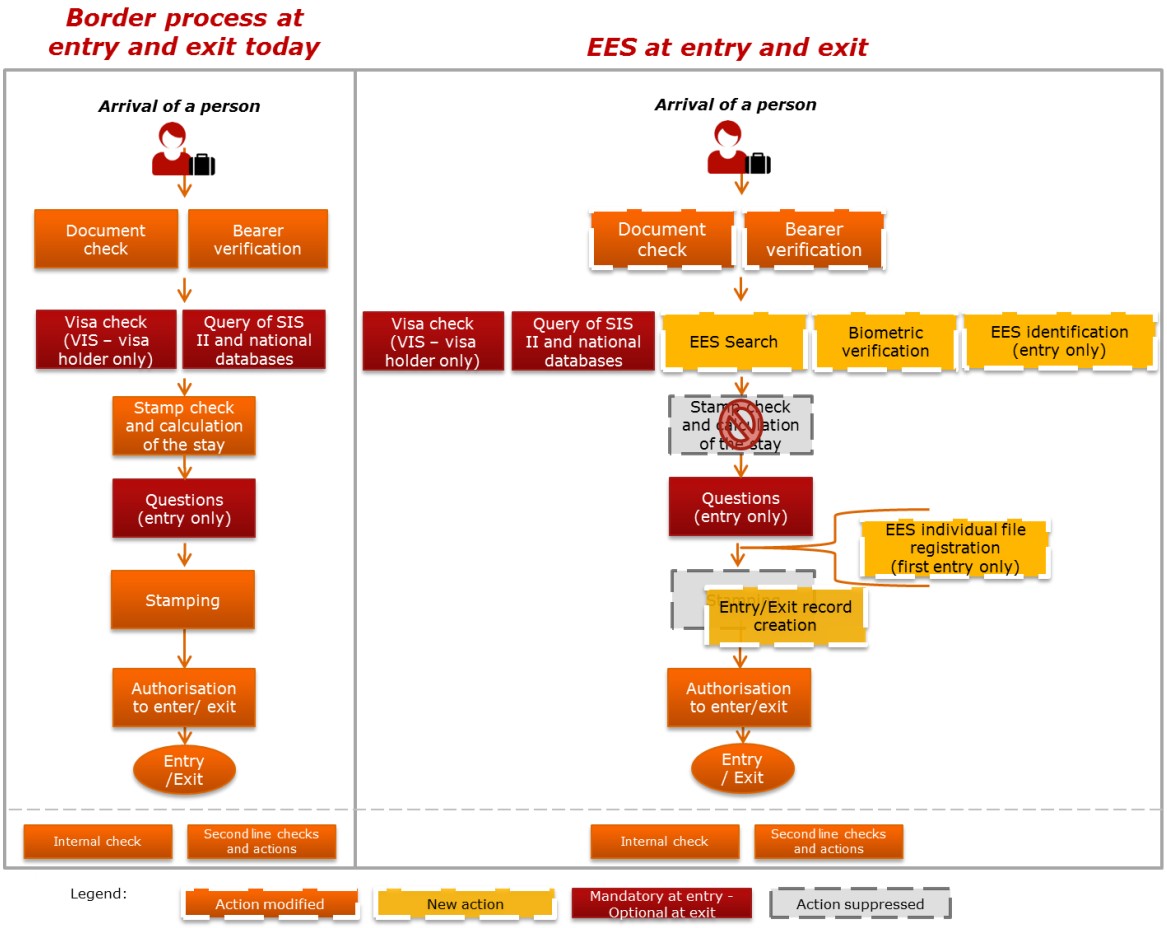
Option	Fingerprints (FP) only	Fingerprints (FP) and facial image (FI) combined	Facial image (FI) only	Iris and facial image (FI) combined
Risk of fraud	FP's can be spoofed and countermeasures are mandatory (liveness detection).	Multi-modal biometrics are less prone to be spoofed as two biometrics need to be counterfeited. Countermeasures remain mandatory.	FI can be spoofed and countermeasures are mandatory (liveness detection).	Multi-modal biometrics are less prone to be spoofed as two biometrics need to be counterfeited. Iris is not less nor more prone to be spoofed than other biometrics. Countermeasures remain mandatory.
Cost implications: cost for installing and operating the biometric capturing/reading devices at the border control points (this is what is borne by Member State budgets potentially co-financed by the Internal Security fund).	The devices implemented for the deployment of VIS checks at the border can be re-used as long as 4 or less FP are enrolled at the border, and therefore also used for verification. When 8 or 10 FP's are enrolled, all devices (mobile and fixed) must allow the enrolment of at least 2 FP's at once.	See column on the left for FP and on the right for FI. So there is an additional investment required for handling FIs.	Devices for taking and comparing FI will need to be installed at all borders. The cost per device is however low.	Iris at a distance requires an expensive device (a few thousand € a piece) and would require all border posts to be re-equipped.
Cost implications: cost for building and operating the central system and the national systems connected to it (this is what is paid for by the EU budget)	This cost is only marginally (a few percentages difference) affected by the choice of biometrics. The difference originates from the network costs for the message exchange between national and central systems: the more biometrics are used, the "heavier" the messages. However this effect is strongly counter-balanced by the fact that network costs are only one item among many. The biggest budget impact stems from the inclusion or not of a systematic identification at the border for all travellers			

8. ANNEX 8: NEW SMART BORDER PROCESSES

The contents of the pages in this annex are mainly taken from section 3.2.2 – Process description of the 2014 Technical Study report. A reference to that section would not have been sufficient as the description has now been adapted on the basis of the options selected for the preferred solution.

8.1.1. Overview

The following picture shows the major differences between the current and future processes at entry and exit.



The entry and exit processes for the EES would be integrated within the existing overall border control process, as regulated in the Schengen Borders Code. The main changes to the generic process would be the ones highlighted in yellow:

– **EES Search**. At every border crossing, as part of the verification, a search is run in the EES. The combination of issuing country and the document number, captured from the MRZ of the travel document are sufficient for doing this search.

– **EES FP's Identification.** A 1:N identification to the EES using 4 fingerprints and the facial image would help detect duplicates in the EES, to avoid that the same person would have more than 1 individual file registered.

– **Biometric verification.** When a person is found in the EES, further verification is made to secure the identity of the person, by electronic use of biometric data and/or by manual verification.

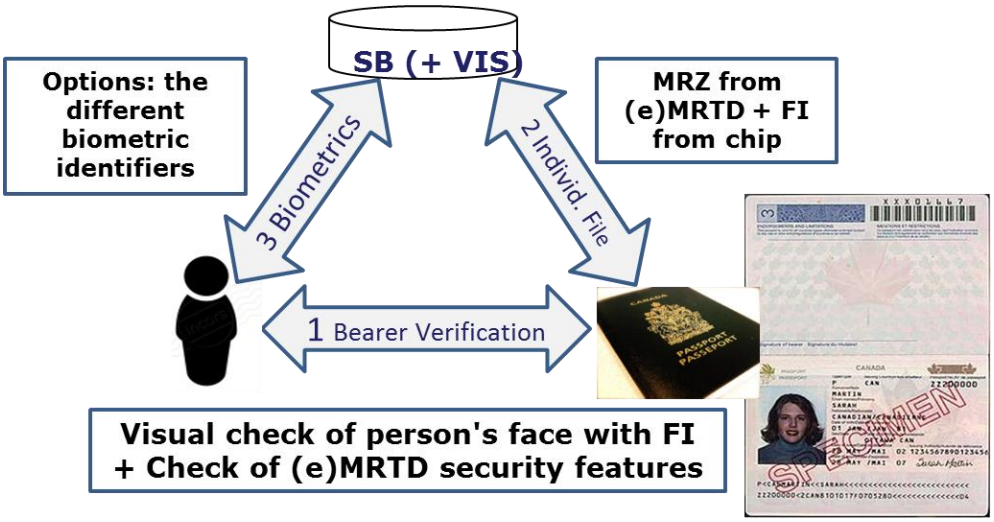
– **EES individual file registration**. In the case of a first entry, an individual file on the person will be registered in the EES. This would include an alphanumeric dataset and the addition of biometric data in the form of fingerprints and a photo.

– **Entry/exit record creation**. All entries/exits are recorded in the EES with data specific to the crossing (date, border crossing point, authority granting access).

Stamping and checking of stamps is abolished. The stakeholders concerned will be able to retrieve or receive information as regards the remaining number of days for the allowed stay.

The Identification Triangle

Whatever the way the process is described the key element is that the "identification triangle" remains. This "identification triangle" means that the consistency needs to be established at each border check between the person, the travel document (passport and visa) and the Smart Borders (SB) system, supplemented with VIS in case of visa-holders:



The first side of the triangle is the **"bearer" verification** which checks whether the traveller is the rightful owner of the passport (and visa). The most common way this is done is the border guard checking whether the passport is real (check of the optical security features of the passport and comparing the picture in the passport with the bearer). The introduction of e-Passports (e-MRTD's) allows this to be supported or even automated.

The second side of the triangle makes the **link between the travel document and the record in the Smart Borders (SB) system**. The most common way this is done is using part or all of the data in the MRZ (Machine Readable Zone) and querying the SB database. The result should be that either the system responds that the person does not exist in the system yet or that a person with that passport has already been recorded and that the MRZ data match with the ones in the individual file in the SB system. With e-Passports the data from the chip (which sometimes provides the advantage of not being truncated) can be used rather than the data from the MRZ.

The third side of the triangle is the **match between the person and the identity** that is recorded, the answer to the question *"is this person the one we know with that identity"*? This is done using biometric identifiers: a biometric reference sample needs to be taken at enrolment (the preferred choice is facial image and four fingerprints taken flat) and a new sample taken to verify whether it matches with that reference. While enrolment and verification of the facial image is the same operation (a digital picture is taken), there is a difference with fingerprints: enrolment needs to be done carefully for multiple fingerprints (four in this case) while verification can be done quickly with only one fingerprint.

8.1.2. Detailed Border processes at entry and exit

Table 1 *Border processes at entry and exit today*

	Entry/ Exit	**TCN-VEs TCN-VHs**	**Description**
Document check	Entry Exit	✓	Manual verifications of valid travel documents or other document authorising a traveller to cross the border and where applicable the requisite visa or residence permit. The documents are also checked to detect falsifications.
Bearer verification	Entry Exit	✓	Manual checks made to secure that the bearer of the travel document is the lawful owner of the document (side 1 of the identification triangle).
Visa check (VIS)	Entry Exit - *optional*	*Only TCN-VHs*	Schengen visas are issued at consular posts around the world. The VIS is checked, using fingerprints (1, 2 or 4) and the visa sticker number[21] (side 2 using the visa-sticker number vs. VIS and side 3 of the identification triangle for visa-holders).
Stamp check	Entry Exit (optional)	✓	Stamps are checked and the stay is calculated manually.
Questions	Entry	✓	Questions are asked as regards: • the purpose of the stay; • sufficient means of subsistence for the duration of the stay and the return to the

[21] Fingerprints are mandatory as of October 2014. By the end of 2015 all consular posts register the visa information in the VIS (the end of the so-called VIS roll-out).

			country of origin; • other supporting documents (e.g. tickets, hotel reservations or invitations to meetings).
SIS II check (and other databases)	Entry Exit - *optional*	✓	SIS II and other relevant systems are checked to verify that the person is not a threat to public policy, internal security, public health, or international relations of any of the Member States or not allowed in the Schengen area.
Stamping	Entry Exit	✓	The passport is stamped.
Authorisation to enter/exit	Entry Exit	✓	When the result of all checks can be approved, the passport is stamped and the person can be granted access to the Schengen area.
Internal checks		✓	After going through the border checks and gaining entry, a person can still be checked in the national territory (either as part of a police check or an identity check by authorities responsible for immigration).
Second line checks and actions	Entry Exit	✓	Depending on the results of all the checks and on the questions and observations included at the border crossing, there could be alternative actions taken related to law enforcement, migration and asylum or to verify certain requirements (e.g. checking that the document is valid or that it is not a forgery). Those actions are not described here but can be seen as part of the overall Border Control Processes.

The following table describes the border processes at entry and exit as would result from the preferred solution. This process description does not detail the required tools. There is no absolute sequence of activities prescribed whether in the pictures or in the text. Some activities do have a sequence, guided by mere logic or by the Schengen Borders Code, and others can be done in parallel, depending on the routines and equipment at the specific border crossing point.

As the legend on the chart above indicates the overall border crossing process is modified in different ways:

– The actions related to the verification of the visa are not changed,
– The actions involving stamping of travel documents at entry and exit are replaced by a new action: the recording of the entry or exit in EES,
– The other actions in the border crossing process remain but are modified due to EES.

***Table 2** Border processes with the use of EES*

	Entry Exit	TCN-VE TCN-VH	Description
Document check 	Entry Exit	✓	Action modified Manual verifications of valid travel documents or other document authorising a traveller to cross the border and where applicable the requisite visa or residence permit. The documents are also checked to detect falsifications. Modification *For travellers with Electronic MRTD:* Both for manual and ABC gates, the Study and the Pilot confirmed the need and feasibility to include Passive Authentication (PA), which is a mandatory check according to ICAO standard 9303. PA verifies the integrity of the contents of the various on-chip Data Groups (containing biographic information, facial image, fingerprints, etc.). Furthermore, where feasible, the discretionary Active Authentication (AA) or Chip Authentication (CA) may be added. AA/CA verifies the authenticity of the chip on which the Data groups reside. *For travellers with Non-electronic MRTD:* In this case, the documentation check for falsifications is limited to manually checking the traditional document security safeguards (e.g. ink and optically variable elements).
Bearer verification 	Entry Exit	✓	Action modified Manual checks to ensure that the bearer of the travel document is the lawful owner of the document (side 1 of the identification triangle). Modification *For travellers with Electronic MRTD*: Both for manual and ABC gates, the Study and the Pilot concluded on the feasibility of doing a biometric verification of the live captured photo against the photo stored on the chip. For manual gates, this recommendation would imply that investments have to be made in camera equipment, since this type of equipment does not normally exist at manual gates today. This action applies for checks at first entry and for TCN-VEs. TCN-VHs are considered to be verified as part of the visa application process. *For travellers with Non-electronic MRTD:* In this case, the authentication check is limited to manually checking the picture on the document against the document holder.
VIS check (VIS)	Entry Exit	*Only TCN-VHs*	Action modified The VIS is checked, using fingerprints (1, 2 or 4) and the visa sticker number (side 2 and 3 of the identification triangle for visa holders). At exit, the VIS check described above is not mandatory.

	Entry Exit	TCN-VE TCN-VH	Description
			Modification The document number and country code (from MRZ or from the e-Passport) is used to proceed with the check in the VIS.
SIS II check (and other databases)	Entry Exit	✓	Action not modified SIS II and other relevant systems (e.g. Interpol, national databases/watch lists) are searched (SIS II searches are optional at exit) to determine whether the person could be refused entry, is wanted and/or constitutes a threat to public security.
EES Search 	Entry/ exit	✓	New action A search is made in the EES using the issuing country and the document number, taken from the MRZ or from the data in the passport chip. The date of birth and the name can be used automatically for further searches, if needed (side 2 of the identification triangle).
Biometric verification 	Entry/ Exit	✓	New action If the person is found in the EES, a biometric verification is made by either using the facial image or the fingerprints stored in the traveller's individual file (side 3 of the identification triangle). At entry: For TCN-VHs - the biometric verification done via the VIS check is trusted. At exit: • For TCN-VHs, the check made against the VIS is trusted, if it is made (it is not mandatory at exit). If no VIS check is made, the verification related to EES is manual (ocular), using the photo of the travel document or a displayed stored photo from EES; • In ABC gates a) making an automated Document check (using at least Passive Authentication), b) making a Bearer verification using the e-MRTD and facial recognition and c) ensuring the EES and VIS data exist for the traveller would validate the chain of trust and so would be seen as sufficient, also without a biometric verification against the VIS.
EES fingerprint identification 	Entry	✓	New action If the person is not found in the EES on the basis of the travel document data, a biometric 1:N search for identification is launched using four fingerprints and the facial image taken live. The identification is for the purpose of finding duplicates in the EES database, meaning the same person appearing more than once, with different names and/or documents. This identification is done at entry and for TCN-VEs. TCN-VHs are identified as part of the visa application process and this should keep the risk of having duplicates to a minimum.

	Entry Exit	TCN-VE TCN-VH	Description
Questions	Entry	✓	Action not modified Questions are asked as regards: • The purpose of the stay; • Sufficient means of subsistence for the duration of the stay and for the return to the country of origin; • Other supporting documents (e.g. tickets or invitations to meetings); • The level of detail of questions and answers is adapted according to the travel history as shown in the EES.
EES individual file creation 	First entry	✓	New action If the person is not found in the EES (by means of the search and the identification actions), a first-time registration of an individual file is made. This includes data from the MRZ (captured from e-MRTD or MRTD), and biometrics. This is creating the link between the travel document and the SB database. For TCN-VE, four fingerprints and a photo from the e-MRTD, or a live photo are stored in the individual file. This is creating he link between the traveller and the SB database. For TCN-VEs, using an MRTD, a live photo is stored. Only in a last resort would the printed photo from the MRTD be stored as this can only be used for manual verification (ocular, using a display of the stored photo) at subsequent entries/exits, since the quality is not good enough for current automated matching algorithms. For TCN-VHs, the fingerprints are already stored in the VIS and no enrolment is needed for these in the EES. A photo, preferably from the e-MRTD or a facial image taken live, is stored in the EES individual file. **The use of photo in the EES** The main reasons for the use of photo as a complementary biometric identifier in the EES process are the following: • By using the photo of the e-MRTD (chip) it is possible to make a bearer verification against a live photo, which would highly improve the security of the border process in general; • Storing a photo from the e-MRTD or a live photo of sufficient quality in EES, means that there would be a biometric identifier that can be used in subsequent electronic and automatic (e.g. ABC-gates) verifications, in the border control process. The stored photo could also be used for manual (ocular) verifications, by displaying the photo and compare this to the traveller being checked; • Scanning and storing a printed photo in EES is of limited or no use for electronic or automated verifications, but can be useful in manual (ocular) verifications, where the photo can be displayed;

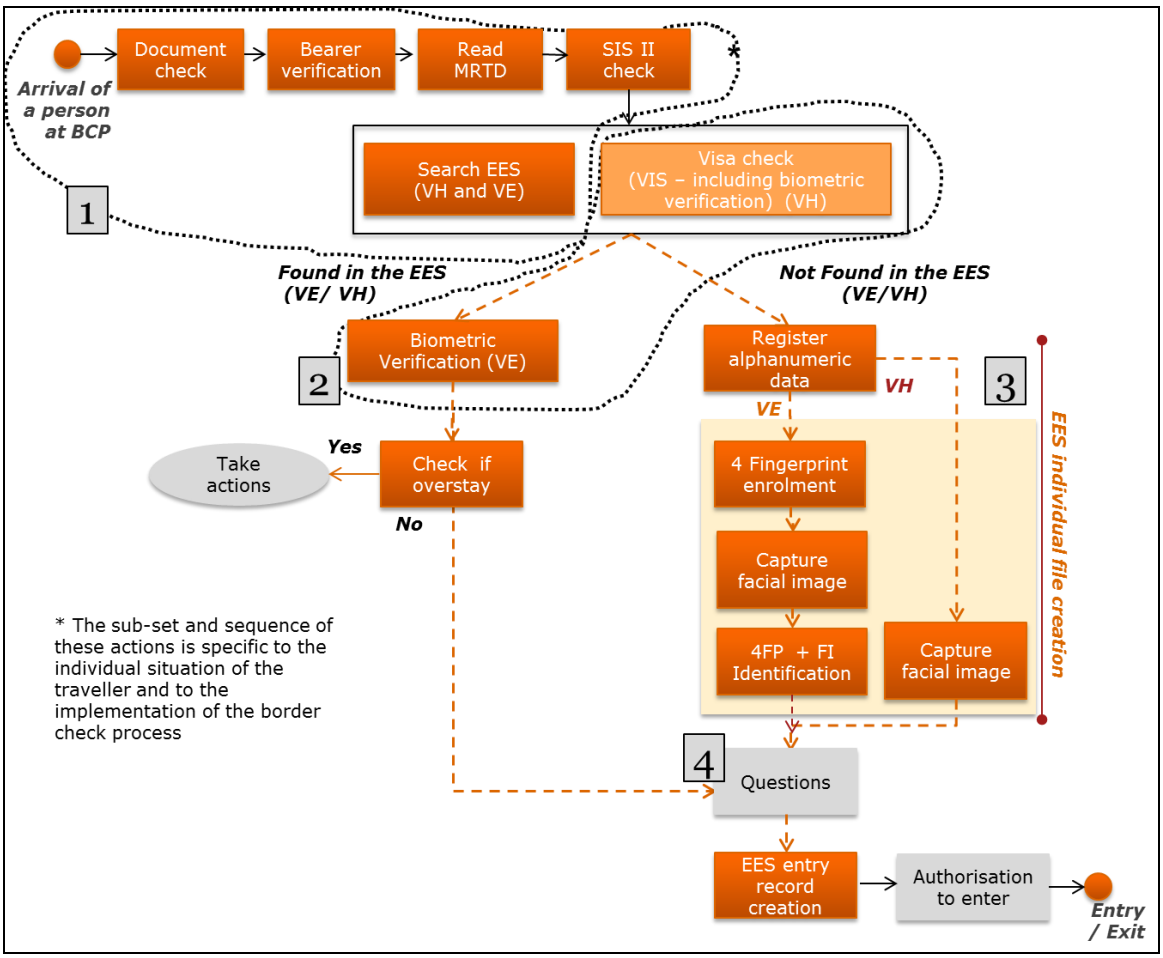
	Entry Exit	TCN-VE TCN-VH	Description
			• A stored photo in EES, from any of the sources mentioned, can always be used for identifying travellers believed to be overstayers.
EES entry/exit record creation 	Entry/ exit	✓	New action Entry/Exit data is entered in the entry/exit record in EES. Data are either copied from the chip in the e-MRTD or from the Machine Readable Zone of the MRTD.
Authorisation to enter/exit	Entry Exit	✓	Action modified Once all checks have been made and approved, and once the EES record creation is complete, the person can be granted access to the Schengen Area. Modification If the person is not granted access the refusal of entry is recorded in the EES.
Second line checks and actions	Entry Exit	✓	Action not modified Depending on the results of all the checks and on the questions and observations included at the border crossing, alternative actions could be taken in relation to LEA, migration and asylum. These are not described here but can be seen as part of the overall border process.
Internal checks	Entry	✓	Action not modified After going through the border checks and gaining entry, a person can still be checked in the national territory, either as part of a police check or security check.

8.1.3. Implementation of Processes at Entry

The description provided under the previous heading, can be split between the standard process at entry and at exit.

The mainstream process at entry can be represented in a flow diagram on the following chart. By "mainstream" is meant that the diagram does not show the actions when a step identifies a discrepancy between data.

The actions that are grouped by a dotted black line and numbered 1 to 4 are the group as actions that are distinguished by the traveller.



Mainstream Smart Border Process Flow at Entry
– (Group of) Actions 1 to 4 identifiable by the traveller
VE= visa-exempt third country nationals; VH= visa-holder third country nationals

The necessary sequence of actions is that:

- The process needs obviously to start with the document check and the bearer verification (refers always to the first check in the identification triangle).

- Once the travel document can be trusted, the traveller's personal data (taken from the MRZ or from the chip (passport or e-passport) can be used (action "Read MRTD") for querying different databases (SIS II, EES and VIS in the case of TCN-VH, but also Interpol and national databases). It can be noted that these queries can be launched simultaneously and have response times measured in at most a few seconds.
  The queries in EES (it is already the case with VIS) use an advanced search engine that retrieves identities despite spelling variations and thus can address the situation where the *same* person has a new or a different legally issued[22] passport.

- The process differentiates the cases where VE and TCN-VH are found in EES and the cases where VE and TCN-VH travellers are not found in EES (but where the visa-application exists in VIS).

[22] The cases referred here are the ones where a person has multiple passports issued by the same authority, multiple passports issued by different authorities because he/she has different nationalities, but where the biographical information is the same (same name, date of birth, etc.).

- The TCN-VH is authenticated by means of at least one fingerprint vs the fingerprints stored in the VIS application (side 3 of the identification triangle is confirmed) as part of the mandatory border crossing process for VH. This process assumes the VIS retrieves the visa application using the travel document number (and issuing country) read during the action "Read MRTD".

In the case the traveller is already recorded in EES (= side 2 of the identification triangle is established as an individual file matches the data from the travel document read) – part left on the slide:

- The process considers that the match between the biometrics (1, 2 or 4 fingerprints) of the VH and the reference sample (10 fingerprints) recorded in VIS is sufficient. In the case of a TCN-VE the facial image either taken live or taken from the passport chip or at least one fingerprint (according to the BCP set-up) is matched vs the biometric samples (4 fingerprints and a facial image) stored in EES. The biometric verification of the TCN-VE closes side 3 of the identification triangle and ensures the entry record is made for the same person as the one who was enrolled.
- The EES response provides also the status on the remaining number of days of authorised stay (action "Check overstay").

In the case the traveller is not recorded in EES – part right on the slide:

- The alphanumeric data from the travel document automatically populate a new EES record (action "Register alphanumeric data").
- In the case of a TCN-VH, only the facial image, either taken live or from the passport chip (action "Capture facial image"), is added to the newly created EES record.
- In the case of a TCN-VE, 4 fingerprints (of the right hand in the mainstream case) are enrolled (action "4 Fingerprints enrolment") as well as the facial image, again either taken live or from the passport chip (action "Capture facial image").
- For TCN-VE, both biometric identifiers are used to launch a process of identification (action "4FP and FI identification") where the reference samples are compared with all the samples in the database to find whether the same person has already been recorded under a different identity. This is not done for TCN-VH because it was part of the visa issuance process.

The next steps are again common for all TCN:

- The border guard asks the questions (action "Questions") in compliance with the "thorough investigation" required by the Schengen Border Code. The EES does not modify these questions.
- When the questions are satisfactorily answered, the border guard authorises the entry which creates the entry record in EES (steps "EES record creation" and "Authorisation to enter"). In the negative case (not shown on the chart), the refusal of entry is also recorded in EES together with the reason of the refusal.

From the description above it can be observed that all the steps performed except the questioning part (therefore mentioned in grey), are either triggered by reading the passport data or by providing biometrics. Therefore the proposal is made to use self-service kiosks for letting the traveller do this data and biometrics collection work himself.

From the traveller point of view as well as in order to estimate the duration for border clearance there are three steps to go through in case of a return visit and four steps at a first visit as can be seen on the chart above (the groups of actions surrounded by a black dotted line and with a number in a square).

In case of a return visit to the Schengen are (within the data retention period), there are three steps experienced by the traveller, where only step (2) is due to Smart Borders:

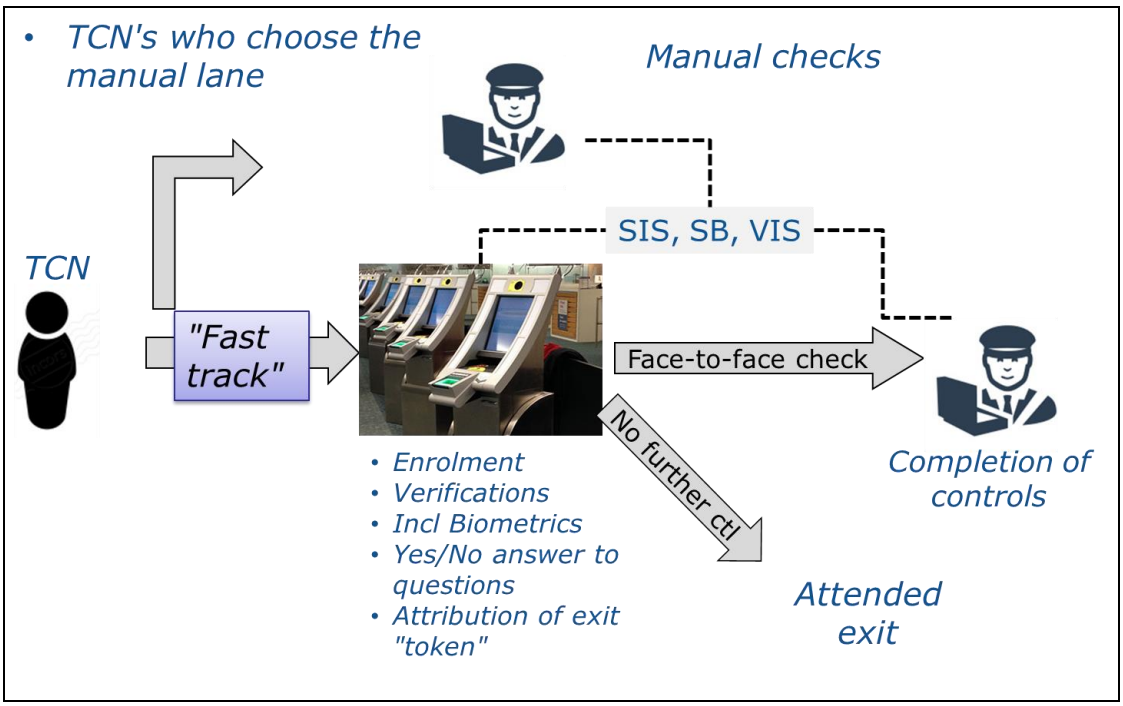
(1) Hand over his/her passport which triggers the passport authentication, bearer verification and the query of the databases.
(2) The biometric verification step.
For TCN-VH: put 1, 2 or 4 fingers for biometric verification (vs VIS).
For TCN-VE: put 1, 2 or 4 fingers for biometric verification or have a picture taken live or copied from the passport chip (vs EES).
(3) Answer questions.

In case of a first visit to the Schengen area there are four steps experienced by the traveller, where only step 3 is due to Smart Borders:

(1) Hand over his/her passport which triggers its authentication and the query of the databases.
(2) The biometric verification for TCN-VH.
For TCN-VH: put 1, 2 or 4 fingers for biometric verification (vs VIS).
(3) The biometric enrolment for TCN-VE and completion of enrolment for TCN-VH:
    - For TCN-VH: have a picture taken live or copied from the passport chip to be added to newly created EES record.
    - For TCN-VE: put 4 fingerprints of the right hand on the fingerprint scanner plate and have a picture taken live or copied from the passport chip to be added to the newly created EES record.
(4) Answer questions.

8.1.4. Accelerated processes at Entry

The process at entry is more time-consuming than the exit process as there are more steps to be executed. The "Fast-track" or "Fast-Lane" process is built by proposing that the traveller performs routine border control tasks on a self-service kiosk (at its own pace) and that the border guard completes the border control, as defined in the current SBC (Schengen Border Code), using the information introduced by the traveller and the results of the queried databases. This general idea is now detailed further.



In what follows it should be understood that the travellers never sees the results of operations but only the confirmation that the operation was done. This is the same for a manual control: the travellers does not see the border guard screen and mainly follows oral instructions.

The manual process is described as the "mainstream process". The following description only addresses the situation of the "fast track" process. The steps are not referred to on the picture.

Step 1: Reading the Travel Document

The traveller is requested to scan his/her passport by putting it on the kiosk passport reader.

In the case of an e-Passport, the passport reader accesses the chip, performs a passive authentication and reads the picture from the chip. On the basis of the data read from the chip, a query is launched simultaneously to the EES, the SIS, the Interpol database and the national databases and, in case of a TCN-VH, to the VIS.

In the case of a non-electronic passport, the passport reader scans the biographical page of the passport. The same query is triggered to the EES, the SIS, the Interpol database and the national databases and, in case of a TCN-VH, to the VIS.

In the case of an e-Passport, the check of the electronic security features of the passport confirms that the passport chip data is genuine. In the case of a non-electronic passport, the next steps are done assuming that the passport is authentic. This assumption will have to be confirmed by a border guard.

Step 2A - First entry: Enrolment

In the case of a first entry or a return visit beyond the data retention period, the EES has found no individual file and prompts immediately for an enrolment.

The kiosk camera takes a live picture from the traveller, scans the picture from the biographical page and stores both in EES. In the case of an electronic passport, the live picture is compared by means of facial matching software with the picture taken from the passport chip and provides a matching score. In the case of a non-electronic passport no comparison can be performed.

In the case of a TCN-VE, the traveller is requested to place four fingerprints on the kiosk fingerprint scanner. These fingerprints are recorded in EES and will be used as the reference sample for biometric verifications at return visits.

In the case of a TCN-VH, the traveller is requested to place one to maximum four fingers on the kiosk fingerprint scanner and these fingerprint scans are compared by the BMS (Biometric Matching System – the biometric system supporting VIS) with the fingerprints recorded in VIS at visa application. This operation confirms that the traveller is the TCN having been granted the visa.

After completion of the biometric enrolment, the traveller is invited to answer a series of questions on the points of departure and destination, purpose of the intended stay, means of subsistence and means of return.

The EES has created the individual file with the enrolled biometrics.

At the end of the process an "exit" token is created. The exit token allows identifying the traveller having completed the self-service process. This token can be material (printed piece of paper) or virtual (the traveller’s picture or a fingerprint used as a token) and can therefore be decided on in each BCP.

In any case, the traveller is directed to a manual booth for completion of the control and enrolment process.

Step 2B - Return visit: Identity verification and check of entry conditions

In the case of a return visit within the period the data are kept, the EES has found the individual file and prompts immediately for the verification.

An identity verification (matching the traveller vs. the document and vs. the EES or VIS contents) is performed and the traveller is requested to answer a series of questions concerning the purpose of intended stay and the means of subsistence.

The kiosk camera takes a live picture from the traveller and compares it by means of facial matching software with the picture from the passport chip and with the picture retrieved from the EES. In the case of a non-electronic passport the live picture is compared only with the picture retrieved from the EES. Facial matching software compares the live picture with the picture in the EES record and provides a matching score.

In the case of a TCN-VH, the traveller is requested to place one to maximum four fingers on the kiosk fingerprint scanner and these fingerprint scans are compared by the BMS (Biometric Matching System – the biometric system supporting VIS) with the fingerprints recorded in VIS at visa application. This operation confirms that the traveller is the TCN having been granted the visa.

After completion of the biometric verification, the traveller is invited to answer a series of questions on the points of departure and destination, purpose of the intended stay, means of subsistence and means of return.

The EES computes the remaining number of days of authorised stay and displays it to the traveller.

At the end of the process an "exit" token is created. The exit token allows identifying the traveller having completed the self-service process. This token can be material (printed piece of paper) or virtual (the traveller's picture or a fingerprint used as a token) and can therefore be decided on in each BCP.

Depending of the results of the self-service process, the traveller is directed to an (automatic) gate or to a manual booth for completion of the control process.

Step 3A – Special case: Exit without further checks

On border guard decision, the traveller at the kiosk receives what has been called the "exit" token that indicates that s/he can leave without a face-to-face interview with the border guard. This token allows passing directly to the "attended exit" as mentioned on the slide. As mentioned in the title this is not expected to be the mainstream case for most border crossing points.

This exit needs to be attended to avoid that travellers having to go to a manual booth would use it and also to allow a border guard to perform random checks. The "attended exit" can be implemented by installing an automatic gate using facial recognition. The EES entry record is created at the moment of crossing the gate.

The minimum criteria to be met in order for the border guard to dismiss travellers from further controls are:

- The traveller is "known" in EES or VIS, so in all cases newly enrolled travellers do have to pass via a border guard.
- The traveller has an electronic passport whose electronic security features were checked with a positive result in the kiosk.
- All the queried databases render a favourable result: no hit in SIS, Interpol or national databases.
- The biometric matching scores (of the biometry used in EES and the one in VIS for TCN-VH) yield values that leave no doubt on the complete correspondence of the traveller's identity and the identity in the reference databases.
- The EES travel history does not show any overstay at the occasion of previous travels to the Schengen area.
- The TCN-VH does have a valid multiple-entry visa. This facilitation must not be given to visa-required travellers with single or double entry visas.
- The answers to all questions demonstrate full compliance with the conditions on thorough checks under SBC Art 7.3.(a) in particular points (iv), (v) and (vi).

The conditions mentioned above could then be dynamically updated by considerations on age of the traveller, travel route, place of departure, travel history in EES, etc. or simply left to the appreciation of the border guard.

Step 3B – Main case: Completion of controls by a Border guard

The mainstream case will be that either the traveller did not complete all the steps or that the border guard considers that some further checks are necessary. The traveller goes to a manual booth for the "face to face" check and is identified by his/her token.

When the traveller was enrolled for the first time the border guard:

– verifies that the fingerprints enrolled correspond with the one of the TCN-VE by checking at least one fingerprint with the sample in EES,

– verifies that the live facial image corresponds with the ones in the passport chip and/or on the biographical page,

– completes the thorough examination on the basis of the questions answered.

In the case of a return visit, the border guard sees on his display:

– the results of the passport authentication in case of an electronic passport (or the absence of it for a non-electronic passport),

– the results of the different database queries (SIS, Interpol, national databases) triggered,

– the EES history of previous entries/exits,

– the answers to the questions asked at the kiosk.

On the basis of this information and his risk assessment, the border guard can decide on which controls remain to be done. Similarly to the current situation, the extent of these controls is completely dependent on the border guard appreciation.

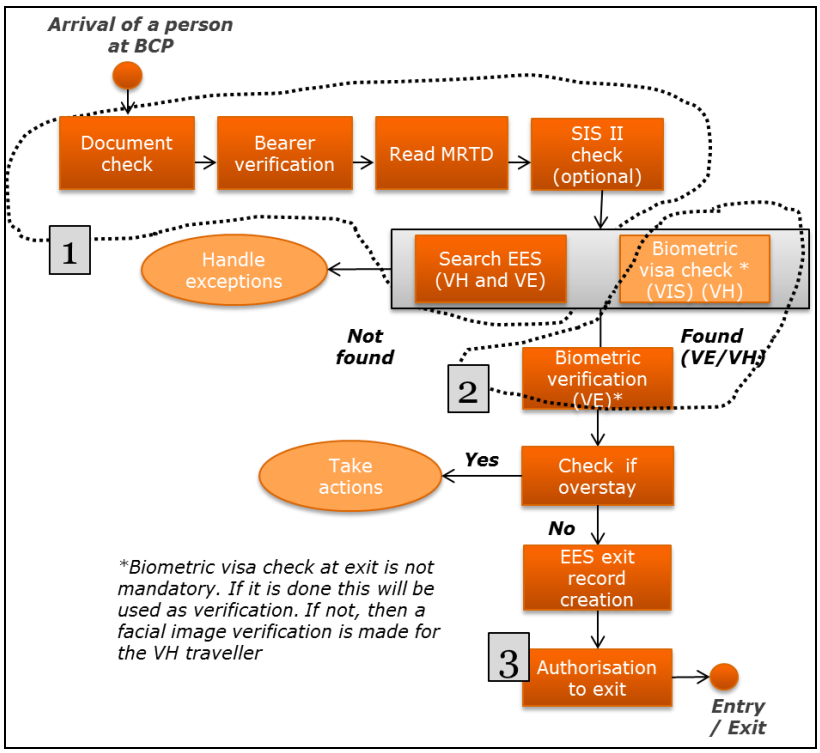
In the case of a non-electronic passport, the border guard needs to confirm that the passport is authentic and belongs to the holder by comparing the picture in the passport and the passport holder.

At the moment the traveller is authorised entering the Schengen area, the border guard clicks "OK for entry" on the display and the EES entry record is created.

*8.1.5. Implementation of Processes at **Exit***

The mainstream process at **exit** can be represented in a flow diagram on the following chart. By "mainstream" is meant that the diagram does not show the actions when a step identifies a discrepancy between data.

The actions that are grouped by a dotted black line and numbered 1 to 3 are the group of actions that are distinguished by the traveller.



Mainstream Smart Border Process Flow at Exit
– (Group of) Actions 1 to 3 identifiable by the traveller
VE= visa-exempt third country nationals; VH= visa-holder third country nationals

The necessary sequence of actions is that;

(1) The process needs obviously to start with the document check and the bearer verification (refers always to the first check in the identification triangle).

(2) Once the travel document can be trusted, the traveller's personal data (taken from the MRZ or from the chip (passport or e-passport)) can be used (action "Read MRTD") for querying different databases (EES and VIS in the case of TCN-VH, but also Interpol and national databases). Querying the SIS II database at exit is optional although recommended. It can be noted that these queries can be launched simultaneously and have response times measured in at most a few seconds.

At exit, in all normal cases the traveller is present in EES (= side 2 of the identification triangle is established: the database always contains an individual file that matches the data from the travel document as the database was necessarily updated at entry):

(3) At exit, it is an optional step to authenticate the TCN-VH (action "Biometric visa check") by means of at least one fingerprint vs the fingerprints stored in the VIS application (side 3 of the identification triangle is confirmed). It could happen more easily as VIS would retrieve the visa application using the travel document number (and the issuing country) read during the action "Read MRTD".

(4) In the case of a TCN-VH, if not done as part of the previous step, the biometric verification can be done matching the facial image either taken live or taken from the passport vs the facial image stored in EES.
In the case of a TCN-VE the facial image either taken live or taken from the passport chip or at least one fingerprint (according to the BCP set-up) is matched vs the biometric samples (4 fingerprints and a facial image) stored in EES (action

"Biometric verification (VE)").
The biometric verification closes side 3 of the identification triangle and ensures the entry record is made for the same person as the one who was enrolled.

(5) The previous steps allow creating the exit record for the right person. The EES checks whether the traveller overstayed (action "Check if overstay") and provides the remaining number of days of authorised stay.

From the description above it can be observed that all the steps performed are either triggered by reading the passport data or by providing biometrics. Therefore the proposal to use self-service kiosks or e-gates for letting the traveller do this data and biometrics collection work himself.

From the traveller point of view there are three steps to go through at exit (the groups of actions surrounded by a black dotted line and with a number in a square), where only step (2) is due to Smart Borders (similarly to when estimating the duration for border clearance):

(1) Hand over his/her passport which triggers the passport authentication, bearer verification and the query of the databases.

(2) The biometric verification step.
For TCN-VH: put 1, 2 or 4 fingers for biometric verification (vs VIS) or have a picture taken live or copied from the passport chip (vs EES).
For TCN-VE: put 1, 2 or 4 fingers for biometric verification or have a picture taken live or copied from the passport chip (vs EES).

(3) Receive border clearance.

*8.1.6. Accelerated processes at **Exit***

The accelerated process at exit is very straightforward.

In case the TCN has an electronic passport an e-gate can be used:

– The e-MRTD data are read from the chip and the passport is authenticated by means of its electronic security features. This corresponds to document authentication.

– The passport data triggers the queries of the different databases including the EES. This corresponds to matching the document with the database (side 2 of the identification triangle),

– The biometric verification is done either by matching the facial image extracted from the chip with the picture taken live in the e-gate and the picture stored in EES (VE and VH), and/or a fingerprint taken live is compared with the fingerprints stored in EES (for VE) or VIS (for VH). This corresponds to the bearer verification and a biometric verification (sides 1 and 3 of the identification triangle).

It should be noted that in case of e-gates the exit is still attended. According to local set-ups, three to seven exit lanes are usually supervised by one border guard.

In case the TCN has a passport without a chip, a kiosk-based solution can be used because all the steps mentioned above can be performed, with the exception that the passport needs to be authenticated by its optical means, in which case the bearer

verification needs to be done by the border guard comparing the passport photo with the traveller.

9. ANNEX 9: INTEROPERABILITY

The purpose of this annex is to explain how the interoperability is conceived.

9.1. Introduction

In this annex, interoperability the interoperability between IT systems will be defined as the capacity of information technology services to allow for information exchange. The interoperability between IT systems is sometimes further refined as syntactic interoperability (data is exchanged in the same or in compatible formats) and semantic interoperability (the content of the information exchange requests are unambiguously defined: what is sent is the same as what is understood).

The question of interoperability is addressed as part of this Impact Assessment assuming that EES and RTP are built as one system, or that only one system is built (the EES as suggested in the preferred solution). The option of having EES and RTP as two different systems is no longer considered as an option for the purpose of this annex.

However, the single EES/RTP (further only EES will be considered as the preferred solution does not contains specific RTP functionalities) will be used by the same authorities (i.e. consular posts, border control, immigration and law enforcement authorities) that are already using VIS. If VIS and EES work next to each other, the same authorities will often have to duplicate tasks and data. The following example illustrates this: assume a visa-holder arrives at a Schengen border post with his valid passport and visa. This is one of the standard situations that occur a few million times per year taking all Schengen borders together.

In case the **VIS and EES are kept as separated systems**, the border crossing process (leaving out generic document controls) will be:

– Border guard scans the visa sticker. With this operation the VIS is queried on the existence of the visa sticker.

– If a visa exists in VIS, the traveller is asked to put 1, 2 or 4 fingers (depending on how the border crossing point is equipped) on the fingerprint scanner. These fingerprints are matched vs the fingerprints stored in VIS for the traveller to whom that visa was delivered in the consulate. This verification has the purpose of confirming that the traveller is the same person who obtained the visa.

– Assuming that the visa-holder is not yet recorded in EES, the border guard will request the traveller to enrol 4 fingerprints again (although 10 fingerprints are already stored in VIS) and a facial image. The passport biometric data is captured again and stored in EES (the same data is partially already recorded in VIS). Finally, the date and place of entry plus the authority authorising the entry are recorded for that traveller in EES.

At each and every new entry, having EES and VIS as separate systems will require each time to confirm the traveller's identity once vs VIS and once vs EES and add an entry record in EES.

The "obvious" answer would then appear to **combine EES and VIS and have one single system**. This option was examined in the Technical Study but has essentially three drawbacks:

– Adding EES data and volume of transactions requires VIS to handle a much higher capacity both in terms of data and transaction volume. *De facto* it means that an "upgraded" VIS would require a new IT infrastructure. This task is not impossible but building the EES "on top" of the VIS would anyhow require significant hardware and technology changes.

– The experience gained in operating VIS, since it went live on 11 October 2011, shows that some technical solutions implemented for VIS would have to be changed given the higher volumes that EES would add. So building EES "on top of" VIS would not happen on a VIS that is kept unchanged. Changes would essentially be required on message handling and on reducing the amount of work (and costs) it takes for Member States for combining the data exchanged with VIS in their national applications;

– The project of delivering EES built on the existing VIS appeared more risky than building EES next to VIS, albeit when re-using same technical components.

From the above it appears that building **EES separated from VIS duplicates work**, but building EES "on top" of VIS is not a "quick-win" solution and is maybe not even desirable because of project risks. The "third" and preferred way is therefore building EES next to VIS but in a way that both systems "speak" to each other, which is the intuitive way to ensure interoperability between the systems.

9.2. Levels at which interoperability matters

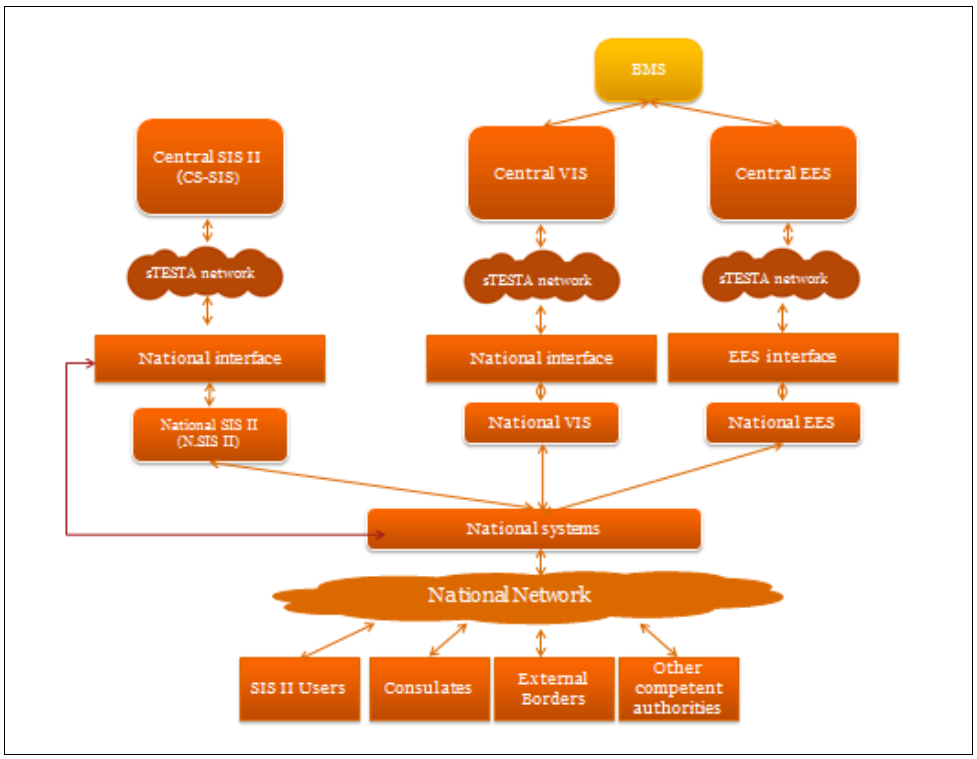
From the example mentioned above there are two levels where "interoperability" matters.

The first level concerns the **biometrics**. As the following example illustrates, biometrics (fingerprints) enrolled in a consular post of Member State A (and stored in VIS) on an equipment of a specific manufacturer need to be matched with biometrics taken at the border post of Member State A but using a different equipment (probably from another manufacturer), but also of a border post in Member State B. Biometrics (this time fingerprints and facial image) taken at the border of Member State A will certainly be used often for matching at exit at the border of Member State C, again each time using different equipment. The interoperability of the biometric identifiers means in this context that the samples taken at any place (consulate, border post, etc.) can be used at any other place (border post of the same or of a different Member State). This interoperability is no longer an issue provided that the biometric samples meet minimum quality requirements which will be specified during the EES development phase which in essence will repeat what has already proven to work well for VIS: VIS has already handled millions of operations with fingerprints and the biometrics are indeed interoperable.

The second level is about avoiding data to be duplicated in different central IT systems (SIS, VIS, EES), reducing the complexity for Member States to have their national systems "speaking" to these central IT systems and combining the use of data received from these systems.

9.3. Starting point: no interoperability between central IT systems

The situation is described as regards SIS, VIS and EES. This scenario is the one implied by the "2013 proposal" but where RTP is left out. In this situation, the interoperability of EES with existing systems is simply not addressed: EES is put next to VIS and SIS as another distinct system. EES simply benefits from re-using the solution developed for VIS.



Future situation when EES is added to the current SIS and VIS

The figure above shows how each IT system is conceived:

– In the case of SIS[23], the central system is connected over a European-wide value-added network to a National Interface in each Member State. This National Interface is identical for all Member States and is connected with a SIS national system whose main tasks are to handle the message flow between the central system and the specific national system that provides services to the end-user. In the case of SIS, there is the particular situation that 23 out of 28 Member States maintain a partial or complete copy (called national copy) of the data of the central system. The SIS national systems are different in each Member State because they need to "speak" with national systems that are different for each of them, despite the fact that the services rendered are the same.

– In the case of VIS, the same logic is applied as for SIS but in this case there is no national copy part of the national VIS.

– In the case of EES, the same logic as for VIS is applied.

For data protection reasons and because the legal basis is each time different, the communication networks for SIS, VIS and EES are separated. The services are procured

[23] The reference to SIS II has become redundant as SIS I+ was decommissioned on 8 May 2012.

to the same network services provider under the s-TESTA (secure Trans European Services for Telematics between Administrations) contract which allows having "bulk tariffs". Nevertheless, from a cost point of view, having three networks is a very detrimental solution as for many connections the sum of the individual maximum load is still inferior to the minimum capacity that can be procures. At the end, each of the three networks has an important over-capacity for most of its network connections. Combining the load of at least two networks would be possible without increasing the capacity of most network connections (i.e. one network could take up the required load of two networks without extending the capacity of most of its connections). This would not create data-protection issues as it is not because messages use the "same lines" that they are mixed.

While the National Interface provides the same services for SIS, VIS and EES, a specific interface is configured for connecting respectively the SIS, VIS and EES to the national system.

When EES comes in the picture, the complex and expensive item for Member States is (1) that the national systems must be adapted so that the data exchanged with the national EES are handled in a way that is meaningful for the end-user, (2) its use is combined with data from SIS and VIS. This so-called "integration of EES data" in the national systems is Member State-specific.

As an example, a consular officer receives a visa-request of a third-country national. When EES will be available, there are three checks that the officer will perform:

(1) use the biographical data of the visa-applicant's passport to send a request to SIS to know whether there is an alert recorded for that person,

(2) use the biographical data and ten fingerprints enrolled from the applicant to check in VIS whether the visa-applicant has already initiated a request in for example another Schengen consulate,

(3) use the biographical data of the visa-applicant's passport and its biometrics to check in EES whether the duration of authorised stay was respected during previous visits.

To ease the work of consular officers it is likely that these three actions will be hidden behind a single functionality called something like "check new visa-request". The answers from SIS (the expected case is a "no hit"), from VIS (the expected answer is "no other application pending") and from EES (the expected answer is either no history of entries/exits or a history of entries and exits without overstay) need also to be combined in a meaningful and practical way for the consular officer. Nevertheless, technically one message is sent to three different central systems and one answer from each of them is sent back via three different channels to be combined at the level of the national systems: total six messages triggered for one operation as seen by the consular officer.

It can be noted that at least three straightforward simplifications would have reduced this integration effort at Member State level:

(1) biographical data and biometrics could be sent to VIS to check whether another pending application exists,

(2) VIS would query the SIS central system for the existence of an alert using biographical data,

(3) VIS could retrieve the traveller's EES history by accessing the EES central system.

(4) one message is sent back to the Member State with a combined answer from SIS, VIS and EES.

The advantage is that it is much simpler to adapt national systems for handling the data contained in this message as data are already combined in a meaningful way. Technically, it also has the advantage that one operation triggers two messages (one question and one answer).

However, this simplification is not possible for the following reasons:

– When SIS and VIS were conceived a direct link between central systems has been discouraged for data protection reasons.

– Although it becomes simpler in this case to adapt national systems, it moves the complexity of combining data from different systems towards the central systems. Complexity does not disappear but is rather moved to the central level. Cost-efficiency would probably be improved by addressing complexity once rather than 28 times, but to reduce project risk the direct link between VIS and EES was also pushed back.

9.4. Reducing the impact of EES at national level

The Technical Study addressed the issue of reducing the impact on national systems of exchanging data with the central EES system. The idea is that while in VIS there is a standard National Interface doing nothing more than providing an encrypted access to the s-Testa network and a Member State specific national VIS system, in EES a centrally built standard system would take care of all message handling services that are necessary for all national systems. This is what is called the National Uniform Interface (NUI) and is therefore represented in another colour in the picture below. It is also this NUI concept that is included in the new legal proposal.

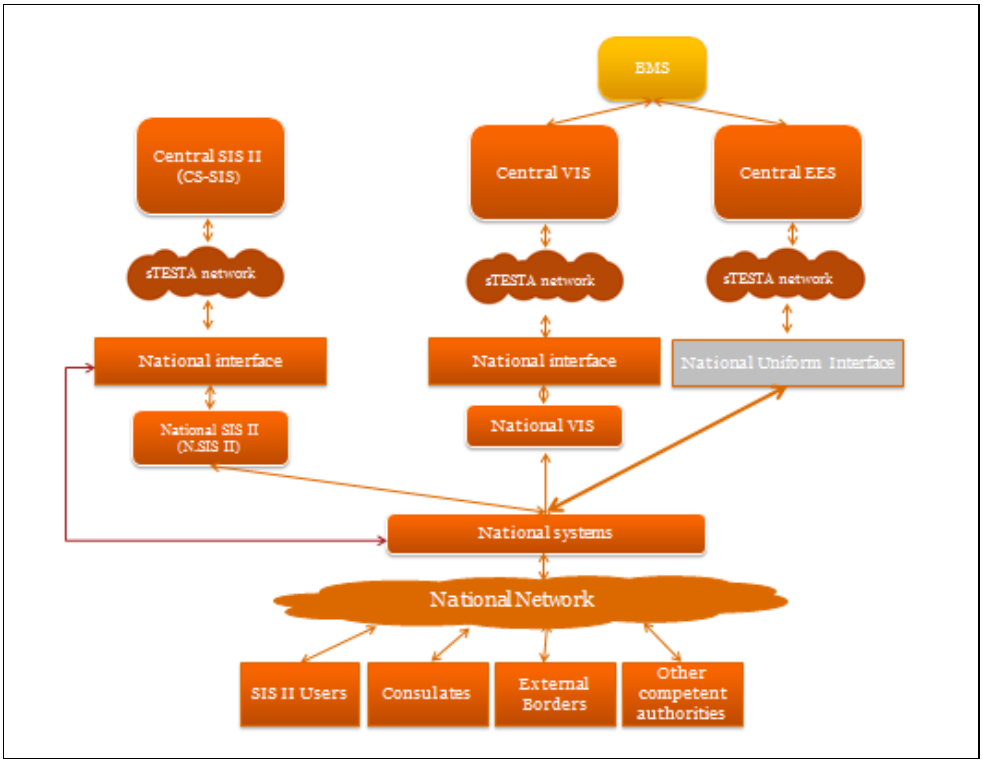


Illustration of the position of the NUI in the architecture

The message handling services of the NUI, refers to a set of services that do not deliver functionalities to the end-user but control the exchange of messages with the central system. To illustrate this concept, one of the most crucial services is called "Reliable Message Transport". This service ensures that a message sent by the national system is delivered to the central system: it records the identifier of each message and as long as it does not receive an acknowledgement of the central system the original message is re-sent according to a specific re-send strategy (e.g. in case the message is not delivered because of network congestion a re-send attempt is tried out every ten seconds). If these services were not provided by the NUI, each national system would have to include them in its modification of the national system in order to handle the exchange of data with the central EES.

The NUI concept does not address the interoperability between SIS, VIS and EES. It only addresses what is called the connectivity, but it nevertheless simplifies the effort (and cost) at national level of including the exchange of data with EES in the national applications. It also addresses the cost and connectivity concerns. The national systems can be considered to "call" the NUI services for handling the messages exchanged with the central EES. However, the national systems will still have to combine the data exchanged with VIS and EES. The example given of the consular officer initiating a new visa request would still imply the same message exchange.

As can be seen in the picture above, the SIS and VIS implementations remain unchanged. This is essentially seen as a benefit, as the EES project will therefore not impact current SIS and VIS operations.

9.5. Including the interoperability between VIS and EES

Building further on the solution described in the previous section that only addresses the connectivity between VIS and EES, the possibility that the central EES accesses VIS and that reciprocally VIS accesses EES is added.

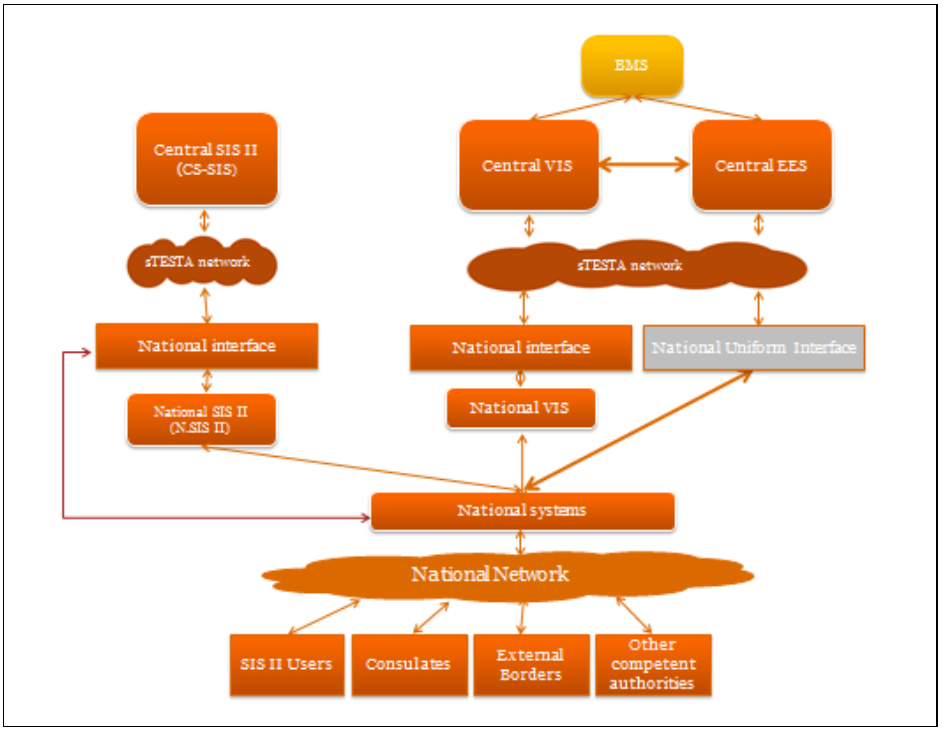


Figure with the proposed interoperability between VIS and EES

The interoperability of VIS and EES is based on the following assumptions:

– Interoperability of VIS and EES with SIS is not addressed. The reasons are mainly practical: it would require the amendment of the SIS legal proposal and, in the context of a legal proposal for EES, the data exchanges of this future system with SIS are not systematic. It is the interoperability of SIS and VIS that could provide further benefits but this could be handled independently.

– Although this was assumed from the beginning, in this case the Biometric Matching System (BMS) has to be the same for VIS and EES, while till now it was only a best option.

– The access to VIS and EES is bi-directional. As an example, VIS updates EES on the changes of visa status (annulment, revocation, extension of visa validity) of visa-holders and EES answers requests from VIS on the history of entries/exits.

– Identity verifications in VIS and EES are mutually trusted. This means that when the identity of a visa-holder is verified vs EES by means of his/her biographical data and facial image, the confirmed identity is also taken for granted by VIS. Otherwise a second identity verification would have to take place where this time at least one fingerprint would be matched with the biometrics stored in VIS. It would reduce the interest of interoperability.

– Since EES accesses VIS centrally and reciprocally, there is no justification of having a separate virtual network and the same network connections will convey EES and VIS messages. This will save network costs without any loss of data security.

As regards the systems on the Member State side, no additional changes compared to section 9.3 are assumed: messages to and from central VIS continue to be handled through the VIS national system and the National Interface, while messages to and from EES are handled through the NUI. There might be opportunities for simplifying the

architecture at the national level (like using the NUI also for handling the messages to and from VIS) but delivering EES is not dependent on changes to be first made to the VIS national implementation.

Referring to the example taken in section 9.3 of a consular officer receiving a visa-request of a third-country national, this is the way the described checks would be done:

– use the biographical data of the visa-applicant's passport to send a request to SIS to know whether there is an alert recorded for that person,

– use the biographical data and ten fingerprints enrolled from the applicant to check in VIS whether the visa-applicant has already initiated a request in another Schengen consulate. VIS sends a request to EES with the same biographical data and four fingerprints (taken from the set of ten) to check whether that person is known in EES. EES sends the travel history of that person back to VIS or the message of the absence of a travel history.

The answer from SIS will be sent to the national system used by the consular officer as one message and from VIS as a second message which also includes the EES data. Both answers will again need to be combined in a meaningful way to the end-user, however combining data coming from SIS and VIS is already taking place now. For sure more data is contained in the VIS message (in this case the travel history or the absence of travel history) but this is far easier to change than having to combine data from EES on top of the data from the other two systems. In this case, one message is sent to two different central systems (SIS and VIS) and one answer from each of them is sent back via two different channels to be combined at the level of the national systems: in total four messages triggered for one operation as seen by the consular officer. The consultation of EES by VIS represents two other messages which do not go over the s-Testa network. An access of one central system by another one is both faster and avoids network costs. The benefit may appear small but there are currently 17 million visa applications per year which will require the message exchange of this example to happen. Nevertheless the main benefit is essentially that it reduces the complexity at the national level.

The access of one central system is often viewed as an operation that has the inconvenience that it is more difficult to manage from the point of view of control on access rights and logs. However, this presumed disadvantage can be avoided by having EES access VIS by the same (existing) central interface that logs the messages and controls the access rights for consultations originating from Member States: EES messages would follow the same path as messages originating from Member State systems.

As an example, a border guard from Member State A sends the message to EES containing the passport data of a visa-holder to verify whether the traveller is already recorded in EES and whether there is a valid visa issued. The message hits EES which accesses VIS in order to find the valid visa (in this case on the basis of the travel document number). If it is designed like for VIS, the EES message will carry with it the information of the requesting authority and the access rights of this authority are checked by the VIS central interface. The access is also logged and is not recorded as "an EES request" but something like "border guard MS A identity check request" and therefore the control on access to data can remain as tight as it is currently.

In the reciprocal case of VIS accessing EES, the current message design is that the type of request plus the authority at the origin of the request remain identified and the corresponding access rights controlled. EES will have to implement a logically equivalent central interface as the one currently used for VIS.