EUROPEAN PARLIAMENT 2014-2019

Committee on Civil Liberties, Justice and Home Affairs

6 January 2015

WORKING DOCUMENT

on the Entry/Exit System (EES) to register entry and exit data of third-country nationals crossing the EU Member States' external borders

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Agustín Díaz de Mera García Consuegra

1.- Introduction

The report on the creation of an Entry/Exit System (EES) is linked to the proposal which forms part of the 'Smart Borders Package'. This working document, which includes the modifications and personal opinions of the current rapporteur, builds on the work of the previous rapporteur and identifies the key issues raised by the technical studies and by the Commission's estimated cost analysis. It will hopefully also serve as a basis for reflection and discussion in Parliament.

2.- Technical study: proposals

The technical study analysed a number of key aspects of the EES in detail, such as its purpose, the data collected (including identifying what data would be required, how long they should be retained, what level of protection would be required in relation to processing, etc.), border control procedures and the system architecture (including, importantly, whether the system would be compatible with pre-existing national systems). On many of these issues, the conclusions reached differed to such an extent from those in the current legislative proposal that the Commission has promised to present a revised proposal as soon as the testing phase is complete and the results have been analysed.

2.1.- Purpose

The rapporteur supports the comprehensive, European-led management of border controls, through which the current systems are strengthened and the freedoms of the Schengen Area are secured. The technical study worked on the basic assumption that 'the objectives and scope of legislative proposals comprising the Smart Borders Package will not be changed' (p. 30 of the study). However, as a result of the various debates held on the topic, the possibility of granting security forces access to the EES is now being proposed as a secondary aim. (It might be recalled that the original proposal already included a possible evaluation two years after the start of operations.)

The rapporteur believes that granting access to security forces would make the EES more useful and effective, which would, in turn, help to improve the management of the Schengen Area. Let us not forget that, in most cases, border control is the responsibility of Member States' security forces. Security forces can already access the Visa Information System (VIS) and Eurodac in specific cases and with appropriate safeguards. In order to uphold the principles of need, proportionality and respect for individuals' human rights, a study should be undertaken of the possible repercussions that such access would have on the EES, with regard to data requirements (whether or not fingerprints should be included), aspects of the system's technical architecture, the data retention period, data protection and the impact on border control procedures.

2.2.- Border control procedures

The need for better and swifter management of border controls is justified by day-to-day practices at the various kinds of border control points (land, air and sea) and by the predicted number of future traveller movements (76 million people are predicted to travel across a total of 302 border crossings in 2025).

One of the priority objectives of the EES is to improve the management of border crossings; any future measures that are adopted should therefore have the lowest possible impact on waiting times at border crossings.

Chapter 3 of the study analyses this point in detail. It highlights that waiting times are dependent on whether or not third-party nationals possess a visa. Special focus is placed on the need to maximise use, in the EES, of data that can be automatically accessed from the machine-readable zone of travel documents and from the photograph stored in the chip of biometric passports. Equally, a study should be undertaken of the comparative effectiveness of Active Authentication and Passive Authentication in verifying the integrity of travel documents, and of the synergies and divergence that would result if such a decision was taken to use the VIS as well.

Chapter 3.6.5 of the study details the principal recommendations for the implementation of both these systems.

2.3.- Accelerators

The study introduces the concept of 'process accelerators', which are intended to reduce waiting times at border crossings by making border procedures faster. Chapter 3.5 discusses a number of possible accelerators, such as the provision of advanced passenger information (API) by airlines, the installation of kiosks at which travellers can pre-register certain personal details, the extension of the retention period for personal data (as this would reduce the number of new registrations in the EES), the improved organisation of border checkpoints (particularly those crossed by rail), the use of data from biometric passports, the extension of the use of automatic border control gates to third-country nationals, and the use of fingerprint or iris sensors as an alternative biometric control.

2.4.- Data

Chapter 5 of the study focuses on determining what data will need to be stored in the EES. As a result of the debates held on the issue, and in order to uphold the principles of proportionality, need and maximising automatic data collection, the study concluded that the 36 pieces of data originally proposed for inclusion in the EES could be reduced to 26 (Table 5.2.3).

The study also proposed a number of possible sources of these data, such as the VIS and the Registered Traveller Programme (RTP), biometric passport chips, machine-readable zones and visa stickers on travel documents.

2.5.- Biometrics

Chapter 4 of the study analyses the use of biometrics with regard to their security, their impact on border control and their ease of use. The study focuses in particular on fingerprinting and facial recognition, owing to their high level of technological development and reliability during both verification (1:1) and identification (1:n). Some arguments suggest that iris

scanning should also be studied during the test period.

Although the current legislative proposal recommends that 10 individual fingerprints be taken, the study assessed several different options involving the use of 1, 2, 4, 8 or 10 fingerprints (see Table 34 and pp. 150-153). It also studied the use of facial recognition in isolation and in combination with fingerprinting (Tables 36 and 37).

In summary, we could say that we are facing a choice between security and speed – the more fingerprints taken, the more reliable the results, but this in turn slows down border control procedures (Table 39).

The different characteristics and climate conditions of border controls across the EU must also be taken into consideration, with regard to issues such as temperature, the volume of traveller flows and the devices available.

2.6.- Data retention period (Chapter 5.3)

Given the rapporteur's insistence that personal data be handled carefully and securely at all times, the final regulation should uphold the principles of need and proportionality. The study shows that the retention period currently specified in the legislative proposal would hinder the correct management of traveller movements as it is too short; an individual who wishes to enter the EU would therefore have to repeatedly re-register with the EES over a short period of time, thereby slowing down the process. This period will also be insufficient if access is eventually given to security forces. The study also demonstrates how much of a difference is made by a five-year retention period, as stipulated in the RTP.

This issue is highly dependent on the structure of the system architecture, in particular with regard to whether or not it is linked up to the VIS.

The main recommendation made is that the retention period for both systems should be aligned, regardless of whether it is set at 5 years, 366 days or another period.

On pages 200 to 211, the study compares these options and provides statistics for each with regard to issues such the time taken to cross the border, the implementation complexity and the cost.

2.7.- Target operating model (TOM)

In order to transform the various options assessed in the study into real elements of analysis, target operating models (TOMs) have been drawn up that bring together all possible aspects of the system.

Three TOMs have been created for the EES (pp. 17-19), which are differentiated mainly by the number of fingerprints used. TOM A uses only facial recognition, whereas TOM B uses facial recognition and four fingerprints, and TOM C uses facial recognition and eight fingerprints.

Each of these options will have repercussions for 1:n identification.

2.8.- Architecture
The rapporteur would refer to the joint document as regards this aspect.

2.9.- Cost

The cost of the EES has dropped considerably, especially if consideration is given to the possibility of building a single system (EES/RTP) or of reusing parts of the VIS. Regardless of which option is finally chosen, it is important that we learn from the experiences of SIS II and that we do not allow the final procedure or the budget allocated to be modified or diverted.

The EES must be efficient and interoperable, as far as possible, with pre-existing national systems. It must also reduce the cost of any future maintenance.

The additional cost of granting security forces access to the system must also be studied, and the various possible data retention periods must be decided.

3.- Questions for parliamentary debate

The rapporteur's aim in this working document is to spark a debate in Parliament and encourage MEPs to reflect on the current proposal, in particular with regard to the promised revised version of the legislative proposal. Many aspects must be taken into account, of which the most important are the following:

- What are the primary and secondary aims of the EES? Particular consideration should be given to the possibility of granting security forces access to the system, in which case limits will have to be set and safeguards put in place in order to protect individuals' rights.
- What is the most viable and efficient architectural model for the system?
- Data protection must be guaranteed, both nationally and at EU level. The principles of proportionality and need must also be upheld. In this sense, the rapporteur would like to raise the following questions: What data would be necessary for the EES to achieve its objectives? For how long should data be retained? How should the EES interact with the VIS?
- The budget for building the EES must be used as effectively as possible, making it as interoperable as possible with pre-existing national systems, reducing current costs and facilitating the future maintenance of the system.