EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

BACKGROUND INFORMATION ON SMART BORDERS INITIATIVE

Registered Traveller Programme (RTP)

The aim of the RTP would be to facilitate border crossings for frequent, pre-vetted and pre-screened third country travellers at the Schengen external border.

It would make use of new technologies such as Automated Border Control systems, thus giving Member States tools to manage their passenger flows efficiently and releasing human resources needed at the external border for checking riskier travellers or serve other travellers. Third country nationals having access to the RTP would be able to use Automated Border Control facilities whenever available at the Schengen border crossing point.

Functioning of a Registered Traveller Programme

Individuals would lodge their applications at either a Member State consulate or at an external border crossing point, whichever is more convenient for them. Visa applicants may apply to join the fee-based programme at the same time their visa application is submitted, while visa-exempt travellers may apply on arrival in the Schengen area. Visa applicants would only need to enrol their fingerprints once when applying for both a visa and for the RTP.

A Registered Traveller would be issued a token in the form of a machine-readable card containing only a unique number, which is swiped on arrival and departure at the border using an automated gate. The gate would also read the travel document (and visa, if applicable) and the fingerprints of the travellers, which would be compared to the relevant database(s). If all checks are successful, the traveller is able to pass through the automated gate. In case of any problem, the traveller would be assisted by a border guard.

The fingerprints to be stored in a repository would be anonymous data and the result that would be returned to border authorities would simply be a 'hit or no-hit,' confirming that the person is indeed the same who applied for the RTP (i.e. no personal data would be returned). A separate alphanumeric repository would contain the application data. This data would only be accessible to specified authorities when assessing the application or renewing/revoking access to the RTP. The RTP would therefore allow any pre-vetted (according to multiple-entry visa criteria) third-country national to use automated gates at any Schengen border crossing point where such gates are available.

Entry/exit system (EES)

The aim of the entry/exit system would be to permit the accurate and reliable calculation of authorised stays as well as identification and verification of travellers.

It would do so by replacing the current system of stamping passports by the electronic registry of the dates and place of entry and exit of third-country nationals admitted for short stays.

Functioning of an Entry/Exit System

The maximum period of authorised stay for third-country nationals is limited. The electronic recording of this information at central level would allow for the automatic calculation of the authorised length of stay of a person and provide Member State authorities with accurate information on where a person has entered the Schengen area and where he/she has exited. The system would flag a record in case the third-country national has remained in the area longer than authorised. Member State authorities would also have a valid travel history of an individual, allowing them to make more informed decisions when deciding on a future visa application, an RTP application or making an entry decision.

Biometrics would allow the identification of any undocumented third country national with accuracy, rather than relying on names, which can be easily altered. Nowadays visa-required and visa-exempted travellers can camouflage their travel history, including their undeclared work, by using different passports or applying for new travel documents, claiming that the previous document was lost. In some third countries, it is possible to legally change one's name (even slightly), effectively resulting in a 'no-hit' against any database storing only alphanumeric data. Without biometrics such persons (in the case of non-visa holders) would go undetected.

On the other hand, the use of biometrics could delay the border check process in particular at the land border and will increase the amount and degree of sensitivity of the personal data to be stored.

As a result, at first the system could operate only with alphanumeric data, and at a later stage, biometric functionalities could be activated, which will also allow time to assess the impact of the use of the VIS on border checks.

A biometric entry/exit system, as well as the Registered Traveller Programme, cannot become operational before **the full roll-out of the Visa Information System** (3 years after go live) as both systems would use the same technical infrastructure and equipment as for the VIS.

Estimated costs of the systems

A study for the Commission in 2010 assessed the costs of a number of options for the system. The table below sets out the one-time development costs, the yearly recurring costs for operations and the accumulated total costs for three years of development followed by five years of operations). It is based on the implementation of an RTP with alphanumeric data stored in a token and biometric data stored in a central repository plus the following two options of EES:

- implementing an EES as a centralised system with biometrics added later,
- implementing a decentralised EES with biometrics.

These estimates can only be indicative: first of all they were based on the assumption that the legislative proposals would be made in 2011 and adopted in early 2013 after which development work would start. Secondly, the decisions to be taken by the colegislators on the nature of the systems could increase or decrease the costs while those decisions themselves will be influenced by the discussions on the new Multiannual Financial Framework (which will cover seven years).

	One-time development cost at Central and National level (3 years of development 2013 – 2015) (in million Euro)	Yearly operational cost at Central and National level (5 years of operation 2016 – 2020) (in million Euro)	**Total costs at Central and National level between 2013-2020 (in million Euro)**
RTP: Option – Data (unique number) stored in a token and (biometrics and data from applications) in a repository	207 (MS 164 - Central 43)	101 (MS 81 - Central 20)	**712**
EES: Ooption – Centralised system with biometrics added later	183 (MS 146 - Central 38)	88 (MS 74 - Central 14)	**623**

The total costs would however be about 30% lower if the systems under these two options were to be built together (i.e. on the same technical platform).

Data protection aspects

The RTP and the EES must comply with the relevant legislation on the protection of personal data, in particular the data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data; and that safeguards and mechanisms are in place for the effective protection of the fundamental rights of the individual travellers and in particular the protection of their private life and their personal data. Visa and border authorities as well as third-country nationals must be made aware of these rights.

Data would be collected and handled only by the competent visa and border authorities at consular posts (for the RTP) and at border crossing points (for the RTP and EES) as far as is necessary for the performance of their tasks. Access to the data would be strictly defined and would be handled in accordance with current EU and national privacy and data protection legislation. Measures for redress, in case of any human error, would need to be put in place so that travellers would be able to rectify any data contained in their Registered Traveller application and/or their entry/exit record. Every effort would need to be made to ensure that the data is stored securely and is not subject to misuse. The data processing would be supervised by the European Data Protection Supervisor as far as EU institutions and bodies are involved, and by national data protection authorities, as far as Member States' authorities are involved.