

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 28/12/2004 - Document attached to the procedure

COMMISSION'S IMPACT ASSESSMENT

1. PROBLEM IDENTIFICATION:

At present there are 134 third countries whose citizens are required to have a visa issued by a Member State to enter the territory of Schengen States. Visas are issued by Member States separately, and the absence of a joint information processing centre has left the system open to abuse.

Other problems increase the need for a centralised visa information system:

- the existing arrangements for the exchange of visa data between Member States are slow, can be inaccurate and are not comprehensive;
- it is often difficult to check that a visa applicant is not using a false identity or stolen travel documents;
- an applicant who is refused a visa by one Schengen country can apply to others (visa shopping) and there is no formal information system for the authorities to check multiple applications;
- Member States dealing with asylum applications do not have efficient means to check whether the applicants have been issued with visas by other Member States; and
- inefficiencies in dealing with visa shopping and fraud make it more difficult to prevent and detect terrorists and members of organised crime groups.

For more information regarding the context of this paper, please refer to the summary of the Commission's initial proposal COM(2004)0835.

2. OBJECTIVE:

The establishment of the Visa Information System (VIS) represents one of the key initiatives within the EU policies aimed at supporting stability and security. Given the potential for a significant impact arising from action in this field, the Commission, in its Annual Policy Strategy for 2004, decided that an Extended Impact Assessment should be carried out. This paper focused on the estimation of the potential impacts of various options under consideration for the VIS. Economic/financial impacts were taken into account as well as social/political ones. Furthermore, proportionality aspects of the storage and the use of data as well as data protection issues have been considered.

This paper highlights the need for the VIS and its impacts in comparison to other policy options. It explains, in particular, why the storage and use of biometric data is essential to achieve the objectives of the VIS and identifies the appropriate safeguards for data protection and data security.

3. POLICY OPTIONS AND IMPACTS:

3.1 - Option 1: no VIS : this option would not create improvements in exchanges of visa application information between consular authorities of Member States. The absence of a visa information exchange system would not address some of the most pressing issues, such as visa shopping and visa fraud;

3.2 - Option 2: entry-exit system to obtain and check biometric and other data on visitors when they enter and leave the country: the main aims of an entry-exit system would be to enable people arriving and departing to be examined, and for appropriate information - which is relevant to their immigration and residence status - to be gathered. This information is also stored in the central database. People who overstay their visas would also be identified in this part of the system. In principle, an entry-exit system would be a computerised system for collecting personal details of all visa holders entering and exiting Schengen territory.

An EU entry-exit system, incorporating biometrics for visa applicants, would provide a continuum of measures to control the movements of third country nationals, from a visa application stage through arrival at an external border to leaving the territory of the Schengen states. Such a system would enable much more efficient and effective border controls to be operated. There would also be improvement to immigration control arrangements, overall, due to the existence of more comprehensive records. However, it would be extremely costly to implement.

Moreover, opportunity costs for visa applicants can be expected, as applicants would have to travel to consular posts to provide biometric data. Furthermore, time will be lost at entry and exit points by providing and checking biometric data. The study comes to the conclusion that opportunity costs in this option are higher than the opportunity costs in a VIS with biometrics (Option 4).

In addition, the impact of entry-exit system on human rights would be extensive, and there would be a substantial need to meet personal data protection and data security requirements in particular in view of the use of biometrics, since there would be a risk of misuse.

Considerable reductions in visa fraud (and some reduction in other document fraud) can be anticipated, as well as in visa shopping.

There would be substantial advantages for bona-fide travellers requiring visas as past visa history could be established in the same way as a VIS with biometrics. This would be especially beneficial for regular travellers, who make repeated applications for Schengen visas. The entry-exit system would provide a big stimulus for IT industries.

3.3 - Option 3: to set up VIS without biometric data: a Visa Information System without biometrics would be an electronic system containing information about the visa applicant taken from the visa application form and the decisions hereto, as well as the photograph of the applicant, introduced as a security feature in the uniform sticker for the Schengen visas. Access to enter and update visa data would be granted to persons authorised to be involved in the visa issuing process or in the process to annul, revoke and extend visas. These authorities would also have access for the purposes of consultation. Provided that visa data is required for the performance of their tasks, other authorities with responsibility for controlling border checkpoints as well as other competent authorities of each Member State would have access in accordance with the purposes of the VIS.

This system would ensure improvement of consular cooperation but would have little impact as a contribution towards internal security and fight against terrorism and on the fight against illegal immigration. Furthermore, bona fide travellers would benefit to a small extent from a VIS without biometrics as there would be just some improvements in the visa issuing process but no improvement in case of lost or stolen travel documents as they could not prove their identity quickly.

3.4 - Option 4: *to set up VIS with biometric data:* a Visa Information System with biometrics would contain all the information envisaged in a VIS without biometrics (and the same access and consultation procedures), but, crucially, it will also include biometric information of visa applicants, such as fingerprints. The choice of the biometric identifier should follow a coherent approach for documents and databases. Even if the biometric technology changes, fingerprint databases will still be used for a long time. Background checks to prevent threats to internal security can be done with fingerprints, contrary to, for example, iris technology. Further development at a later stage might enable the use of photographs for facial recognition.

The paper highlights that, in a large database, it is not possible to identify persons with alphanumeric data alone. Even for bona-fide travellers, the spelling of the same name can be different from one country to another, many instances of the same name exist and, in some countries, dates of births are not completely known. Identifying undocumented persons or persons is virtually impossible without biometrics.

Inclusion of biometric data in the VIS would not only significantly support the assessment of applicants in view of preventing 'visa shopping', fraud and threats to internal security, but would have positive consequences for bona-fide travellers. Matches against biometric data would help to verify their identity in case of a new application or at checks, but also in case of lost or stolen travel documents as bona-fide travellers could quickly prove their identity to get new travel documents and visas. Moreover, the inclusion of biometric data would also significantly support the identification of undocumented illegal immigrants and the return procedures, if these illegal immigrants have once applied for a visa.

It should, however, be noted that this option would entail very significant financial costs. Due to opportunity costs for visa applicants and the perceived invasion of privacy and human rights, some reductions in business travel and tourism might be anticipated.

CONCLUSION: The assessment highlights the need for the VIS and points out that, in spite of high costs and data protection issues, the storage and use of **biometric data is essential to achieve the objectives of the system. Therefore, Option 4 has been chosen as it closely meets the objectives and purposes outlined by the Council in February 2004.**

4. FOLLOW-UP: The effective monitoring of the VIS requires evaluation in regular intervals. For these purposes, it is necessary that systems are in place to monitor the functioning of the VIS against objectives, in terms of outputs, cost-effectiveness and quality of service. ***It is recommended that every 2 years a report on the technical functioning of the VIS should be submitted to the European Parliament and the Council.*** This report should include information on the performance of the VIS against quantitative indicators predefined by the Commission. ***Moreover, an overall evaluation of the VIS*** should be produced, including examining results achieved against objectives and assessing the continuing validity of the underlying rationale and any implications of future options.