COUNCIL OF
THE EUROPEAN UNION

Brussels, 24 June 2003 (02.07)
(OR. it)

10857/03

LIMITE

VISA 109
COMIX 407

NOTE

from :	Presidency
to:	Visa Working Party
Subject :	Presidency initiative on visa security and controls

1. Introduction

a. Need to increase security and controls

The need to tighten controls on foreign nationals entering and residing in the Schengen area led the Laeken European Council to call for the creation of a common information system on visas as an appropriate means of contributing effectively to the fight against terrorism, organised crime and illegal immigration.

The Seville European Council subsequently confirmed that undertaking by including it in an action plan.

b. Study of the VIS project requested by the Visa Working Party

In accordance with instructions, the Visa Working Party drew up a number of guidelines for the establishment of a Visa Information System (VIS), which were adopted on 13 June 2002.

On the basis of those guidelines the Commission launched a feasibility study, the final results of which were published on 10 May 2003 and presented to delegations at the meetings on 15 and 27 May 2003.

Amongst other things, the study indicates the amount of time required to implement the whole project. Current estimates are that the system will not be fully operational until 2009 at the earliest.

c. Decisions taken by the JHA Council (5 June 2003)

The Council approved the results of the VIS project and invited the Commission to continue its preparatory work on the VIS, opting for a common platform with SIS II and a centralised architecture. The Council undertook to give the necessary political guidance by December 2003 at the latest, so that VIS and SIS II could be covered by a single call for tender.

d. Thessaloniki European Council on 19 and 20 June 2003

In point 11 of its conclusions, the European Council deemed it necessary that "following the feasibility study by the Commission on the VIS, orientations should be determined as soon as possible, in order to satisfy the preferred options, with regard to the planning for the development of the system, the appropriate legal basis which will permit its establishment and the engagement of the necessary financial means, while respecting the financial perspectives." It then invited the Commission to prepare the appropriate proposals, starting with visas, while fully respecting the envisaged timetable for the introduction of SIS II.

2. Aim of the proposal

a. What to do pending a fully-operational VIS

It would appear desirable, pending a fully-fledged VIS, to implement the European Council recommendations swiftly and to consider the possibility of Member States adopting uniform control systems which, using state-of-the-art technology capable of guaranteeing security in the off-line mode as well, could at least partially - yet substantially - meet the desired aim. At the same time, from the point of view of setting up the VIS, the introduction of such control systems would be a first important step, both because the personal and biometric data available in off-line mode would be certified by the consulates in the countries issuing the visas and because they would be stored at those consulates and made available on the VIS when it was set up. Apart from being easy to integrate, such a system would have the advantage of making the introduction of the VIS more flexible and of swiftly achieving a significant increase in the overall level of security by virtue of having a sure match between a person's identity and the biometric data stored off line.

b. Development of the points in paragraph 10.11 of the VIS report

Paragraph 10.11 of the VIS report refers to the possible use of electronic devices such as contactless smart cards on which to enter the visa applicant's biodata. This type of data storage on an easily portable medium is an off-line system capable of meeting practically all the aims of the VIS. It is stated that "*contactless chips in the visa sticker will facilitate the off-line visa and traveller verification, without connectivity to the VIS. This lowers telecommunication costs and has a small impact on the processing power requirements for the VIS infrastructure*". On this basis, consideration was given to the benefits which the use of such devices could bring to the control system as a whole, pending full development of the VIS and also once it is in place.

c. ICAO recommendations with reference to contactless integrated circuits

The ICAO recommendation to be published shortly indicates that all Member States are very interested in improving controls and security by obtaining biometric physical data on passengers arriving on international flights. The identification techniques referred to in that document also rely on the use of contactless chips on which a person's individual data may be stored, given how easily such devices may be carried and read thanks to so-called "smart" technology. Attention is drawn in particular to the need to meet the following specific requirements:

- use of biometric means of identification;
- use of contactless chips with a minimum capacity of 32Kbyte on paper documents such as visas and passports;
- use of an encryption technique;
- use of the public/private key pair provided for in the Public Key Infrastructure (PKI) for the authentification of data recorded via an electronic signature.

d. Implementation of part of the VIS project using contactless technology

Thought is now being given to the idea of using this kind of new technology to prepare the ground for certain parts of the VIS project, without affecting the final aim of the project. We should not overlook the considerable importance of setting up a database which could be used to store biographical, biometric and additional data on all visa applicants. The possibility of feeding such a database with data from all the consulates in the Schengen States would make the database an indispensable consultation device in view of the invaluable information it would provide. By bringing forward part of the project through the use of contactless technology and microchips, the intention is to provide any foreign national wishing to enter the common area with a computer-readable paper capable of identifying the person both at the border and within the Schengen area, a paper which, in order to optimise consultation times and speed of identification, would be both electronic and smart.

e. Proposed innovation

The proposal provides for the once-only registration by consulates of the visa applicant's details. Biometric information, starting with a photo and then fingerprints, would be gathered on the spot. It is already intended that the photo should be added to the visa sticker. At the same time as the data are recorded, a suitable security device would be added to the chip. Data from one or more fingers could be obtained simply by linking a fingerprint reader to a computer at the consulate. Once a fingerprint had been acquired and checked, it would not only be recorded on the microchip but also stored in the consulate's database, until such time as the VIS system was able to centralise all data in the C-VIS database.

Accordingly, as a complement to the VIS system, information would be recorded twice:

- at central level, in the VIS database;
- at a local level, using the same paper base as the visa applicant's passport.

The microchip, if provided with all the data and necessary safety features at the same time as the sticker is being produced, would then be "final". Given the flexible, self-adhesive nature of the material used, the chip would be applied to a page of the passport and protected, as well as concealed, by the visa sticker, which would be affixed on top of the self-adhesive film containing the microchip.

The completed document would thus consist of:

- a passport with an identification number, biodata and a photo;
- a sticker, produced in accordance with Schengen criteria, with its own identification number, the reference number of the passport, biodata and a photo;
- a microchip containing all the information recorded in both documents.

All of this would be combined in a single paper document which could be described as "smart" in that it would incorporate an electronic medium which could be consulted and to which further information could be added throughout its period of validity, which would be the same as that of the passport. Only one chip, valid until the expiry date of the passport, would be necessary. The recorded information would consist mainly of border crossing dates and the dates of any new visa stickers issued subsequently for the same traveller and the same passport.

Once the biometric data had been added, the document issued would become forgery-proof: a faithful copy of the details of the person arriving at the border would be recorded on it.

Any attempt to tamper with the microchip would cause it to self-destruct.

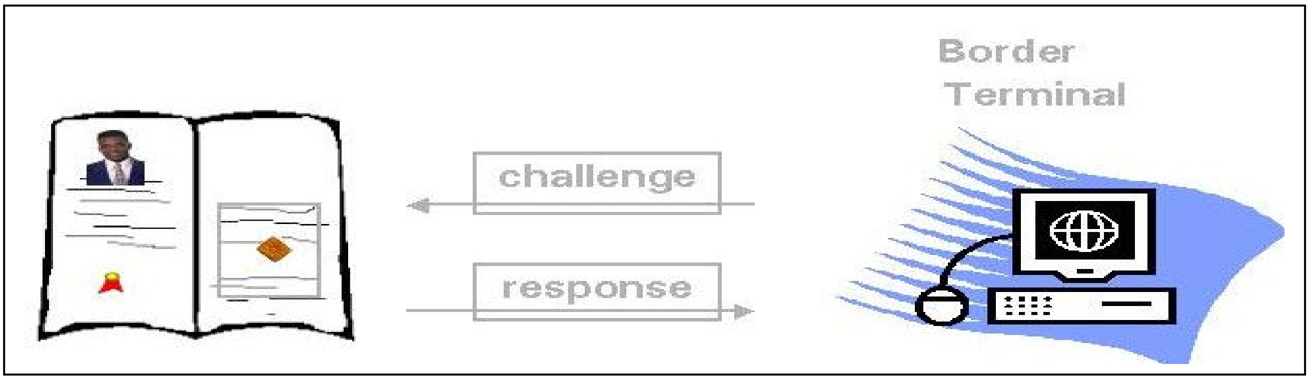
It would be impossible to construct a microchip similar to the one issued by the consulates without knowing the encryption procedure and the secret codes or the authentification methods based on asymmetrical signatures and the PKI's dual key system. Security would be noticeably improved, reducing the risk of forgery to virtually nil.

f. An example of how the automatic control procedure would work

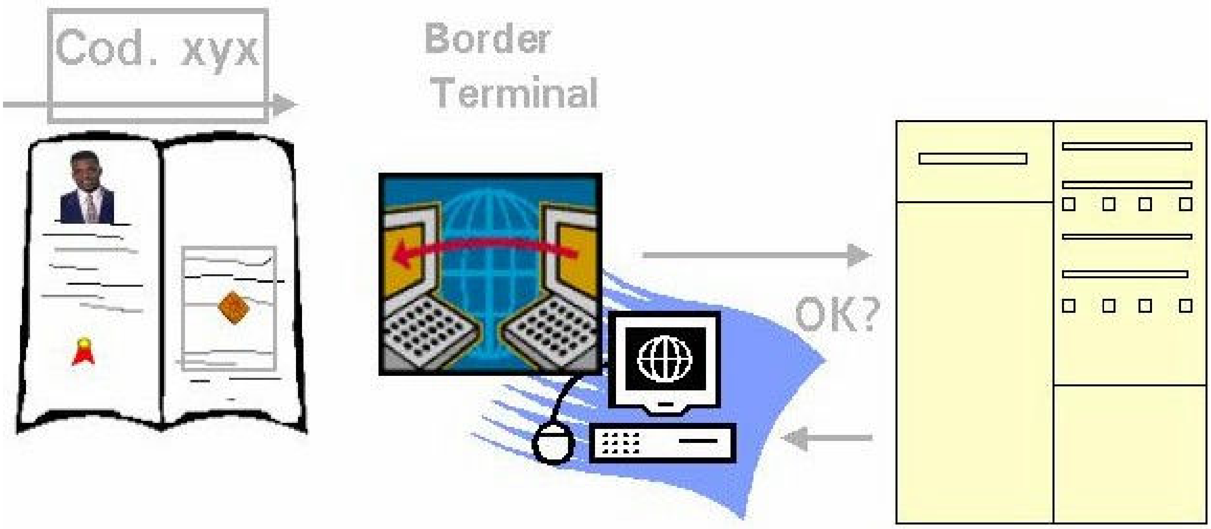
To make it easier to understand the immediate advantages and the simplicity of the proposed solution, here is a brief description of how an automatic border control would work:

(i) There would be a cross check between the border terminal and the visa microchip to ensure that:

- the microchip was authentic;
- the data contained were accurate;
- the data were properly recorded;
- the terminal's read/write access to the data was valid.



(ii) The identification code embedded in the chip would be rapidly checked to ensure that it was not one of those on the central database's Black List: if it were, the person would be immediately held for further checks.



(iii) The personal and biometric data stored in the microchip would then be compared with that printed in the passport and the visa sticker and with the person's fingerprints in order to ascertain the person's identity in a sure and unequivocal manner.

3. Technical aspects of the project

a. Need for portability of sensitive data

A process is underway whereby computer technologies are converging toward global systems of communication and mobility. This requirement has made it ever more necessary that, for communicating with the central information systems, there should be secure, privacy-respecting methods of transmitting sensitive and personal data. This information on the individual is needed in order to identify them so that they can be granted access to the information systems and thus make use of the online services, regardless of the point of access to the information. This is the context which has given rise to the success and the enormously wide distribution of electronic cards.

b. Contact and contactless microchip technology

– Among electronic cards, particular importance has been assumed by the technology of memory and microprocessor cards. Historically, these have taken the form of a plastic medium of the same size as an ordinary bank card. On the card, a module is placed in a precise, standardised position, providing electric contacts to the outside, while inside, it contains a memory or microprocessor chip. Cards fitted with microprocessors are also commonly known as smart cards, because of their ability to execute logical functions, process complex encryption algorithms and guarantee a level of security not otherwise attainable. A smart card's module is the active part of the card itself which contains the electronic circuitry and interfaces with the outside world via a system of flat, gold-plated contacts. The module is made up of a microprocessor, a plastic medium and a set of connectors between the electronic circuitry of the chip and the external contacts on the plastic medium.

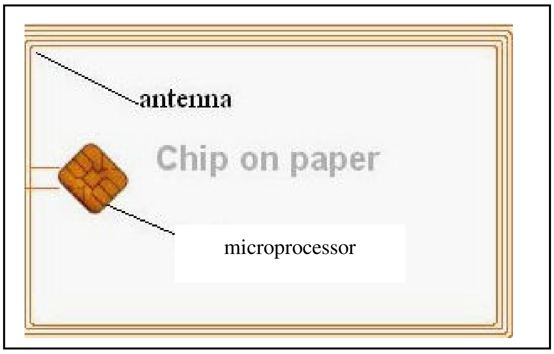
In a very general way, a smart card can be seen as a personal database plus an electronic key which both enables the user to be identified and provides secure access to and interaction with the centralised information systems, interconnecting a hardware structure with an expressly developed and personalised software application system.

– A natural and important development of the smart card is the contactless smart card, born essentially of two requirements: on the one hand that of allowing rapid, secure transit, and on the other permitting the card's read/write terminal to retain its efficiency over a large number of readings of the card without servicing. Basically, the contactless card is equipped with a module which can transfer data which has been made secure via traditional terminals which require well-defined and time-managed information channels, that is to say, ones which give a full guarantee of correct flow through control cycles. The card is then able to establish two-way communication with a terminal in radio frequency, i.e. without physical contact, thereby providing and guaranteeing the same features as traditional systems but also affording the possibility of communication from a local logic system which is in movement relative to a fixed terminal. It is estimated that at the present time more than 100 million contactless cards are in circulation, evidence of the reliability and durability of this technology.

c. Contactless smart card compared with chip on paper: advantages of chip on paper (single document as against two separate documents)

"Chip on paper" technology can be regarded as a further technological development of the contactless microprocessor card, the only, but fundamental, difference being that of having an extremely thin physical paper-type medium, and thus being particularly suited for use within identification documents which are also necessarily tied to a paper medium, e.g. a passport or a visa attached to a passport.

d. Physical appearance of a chip on paper (adhesive stamp, antenna, etc)



In brief, chip-on-paper technology consists in inserting in an appropriately treated paper support, two linked-elements:

- a microprocessor equipped with sufficient memory to be able to hold in secure form a set of fixed data and variable, that is to say, updatable data.
  These data are transferred to read/write device a few centimetres away, without the need for physical, let alone electrical contact;
- an antenna enabling the microprocessor to converse with the informatic environment without it being any longer necessary for the various contacts to be physically linked. The antenna in this case is made of a conductive material in the form of a spiral deposited on a thin film. The microprocessor is linked to it. The whole is "pasted" onto the paper using a self-adhesive support.

e. Accessibility of data using contactless technology

As already indicated, contactless technology is particularly indicated for accessing data contained in microprocessors rapidly, as well as securely, thanks to the use of radio frequency transmission. Not by chance, its major application at present is in the mass transit of passengers at access gates to metro and railway stations. Crowd situations notwithstanding, contactless technology guarantees ticket payment at the moment at which passengers pass through the payment gate. The technicalities of data transmission in radio frequency are governed by specific international standards.

f. Security of data using contactless technology

This technology permits a very high level of security both as regards methods of data entry, maintenance and modification within the microprocessor and as regards the methods of transferring data from the microprocessor to the telematic infrastructure of the system which leads to the device used to read/write the data in the microprocessor.

Looked at in more detail, the internal level of security in the microprocessor is guaranteed as follows: the data, both fixed and variable, are encrypted using appropriate cryptographic keys and stored in an Eeprom memory whose internal structure is such that, if an attempt is made to access it fraudulently via the hardware, it self-destructs; at the same time, if an attempt is made to access it in software form, access is immediately blocked by cryptographic security systems. The ROM code, which is determined by the processor's firmware, is also unattackable either via hardware or software.

As regards the level of security relating to the transfer of data, these are transferred using Des, 3Des or Des-x cryptography processes, both for the reading of fixed data and for the writing of variable data. In addition, it is also possible to encrypt the data contained in the microprocessor using asymmetrical cryptography keys, which however entail greater costs because of the greater complexity and size of the microprocessor itself, which must be supplemented internally by a math coprocessor. Authorised users are also defined clearly and securely, along with their level of authorisation: who can issue the certificate, who can update the data and who can merely read them.

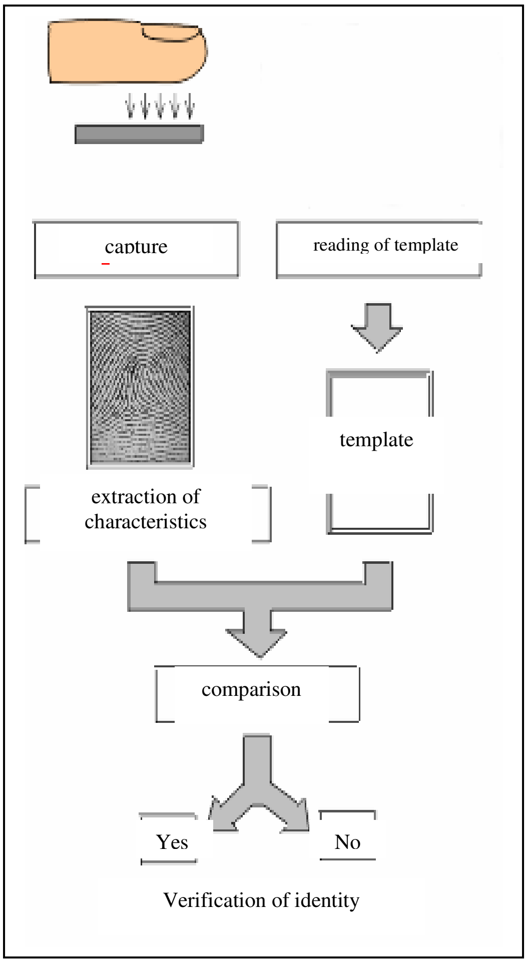
Any lack of correspondence between the content of the microprocessor and the data contained on the paper medium can be immediately identified by the person carrying out the check. And since the reading/writing of the microprocessor, as well as being immediate, can also be automated in the control phase, any name entered on a blacklist (e.g. the SIS) will be immediately signalled by the system.

g. Size of available microchips

The current state of the art of chip-on-paper technology and especially the recent advances achieved by silicon producers, who have succeeded in substantially reducing the construction geometries of microprocessors, make it possible to meet the requirements called for in the recently adopted ICAO recommendation regarding the storage in the microprocessor of biometric data such as photo and fingerprints in digital format, along with templates of the fingerprints themselves to facilitate comparison.

h. Link with biometric data processing systems

A *biometrics system* is an automated device for verifying identity or recognising an individual on the basis of physiological characteristics. Highly reliable, relatively inexpensive equipment is now available for capturing and checking digitised face prints and fingerprints. Such devices are readily available on the market and interface with any ordinary PC equipped with the software for entering and managing biometric data. The figure on the right depicts the off-line procedure for capturing, comparing and verifying the fingerprint of an alien entering a Schengen country. The identity check consists in capturing the fingerprint at the terminal, where it is immediately compared with the fingerprint template stored in the microchip. This process can be automated and takes only a few seconds.



4. Immediate advantages of a chip-on-paper solution

(a) Storage of the passport number: passport and chip are inseparable

A key item of biodata stored on the chip would be the number of the alien's passport to which the visa is to be affixed.

This means that the two media – the passport and the microchip applied to it – are inseparably linked, thus guaranteeing that no changes have been made since the bearer first crossed the border. Chip-on-paper technology in effect converts any passport into an electronic passport.

(b) Storage of the visa sticker data on the chip on paper

In addition, all the data appearing on the visa sticker would be stored on the microchip. In this case, too, the authenticity of the passport visa sticker is ensured by the data set.

(c) Storage of the other biodata on the chip

The applicant's biodata would be stored on the chip, thus making his passport fully electronic.

As a result, as soon as the alien had crossed the border once, his passport data would also be electronically recorded and readily available thereafter whenever the need arose.

This information would therefore be recorded only once and the process would not be repeated until the passport was changed (e.g. replaced). Here, too, there is a guarantee that the document has not been tampered with since the chip was first read and its contents recorded.

(d) Storage of the photo and biometric data on the chip

A considerable advantage of storing digitised photographic and, where applicable, biometric data on the chip would be to enable virtually error-free verification that the person presenting the visa was the same person who applied for it.

(e) The data can be fully encrypted

A further significant advantage of the chip-on-paper solution is that the data can be stored in encrypted form. Encryption is a barrier to reading by unauthorised persons and above all makes it difficult for potential forgers to tamper with the data in any way.

(f) The visa applicant's particulars are written indelibly

The digitised photo data (and any biometric data) would be entered and checked for accuracy, after which they would be indelibly stored on the chip on paper (i.e. could not be written over). This additional feature would ensure that the microchip, and by extension the passport, was completely forgery-proof. It should also be remembered that the application of contactless technology for reading/writing the data would enable them – in the interests of security – to be transmitted from terminal to microchip and vice versa in encrypted form in accordance with current international standards.

g. Record of border crossing movements

If chip-on-paper technology were applied to passports in this way, it could establish the entire history of an alien's movements across the border during the visa's period of validity. At present, it is difficult to compile such a record.
Subsequently, when receiving requests for visas, it would be extremely simple to check whether, under previous visas, the time limits for staying on Schengen territory had been complied with. At present, gathering such information when checking multiple-entry visas is a particularly onerous task.

One further advantage is that any alien crossing a border could be immediately checked by consulting the SIS to see whether his name had not been added in the meantime to the list of inadmissible persons. This could all be done automatically and without having to type in the person's biodata, since all these checks are performed when the border is crossed.

5. Advantages of integrating this solution into the VIS project

(a) Security of current documents enhanced

The paper documents that the visa applicant is required to carry are passport and visa sticker. Passports are issued according to current document security standards. Stickers, incorporating a kinegram, are printed in black ink using a dot matrix printer, techniques which ensure that the sticker is forgery-proof especially because of the difficulty of reproducing the kinegram. The VIS project adds a further security test, namely the comparison of the sticker with its image stored in the VIS database. If biometric data were used in addition, while the routine alphanumeric identity check was being carried out, the biometric data could be checked against the data stored in the VIS database.

The method of control, however, would continue to be by sample or spot checking. Document and identity checks at the border would be conducted on only a small proportion of aliens. If an alien had no travel documents at all, the investigation would obviously take longer and be more difficult and be entirely based on biometrics.

The use of the new chip-on-paper technology offers the possibility of incorporating the microchip sticker under the current visa sticker. In this way paper passport and chip-stored data are indissolubly linked.
Unlike the visa sticker, which can be removed, wiped clean of its original printed data (albeit with sophisticated technology) and filled in with the particulars of a quite different passport, the microchip incorporates an indelible reference to one specific passport and incorporates the biometric data of that passport's specific holder. Any attempt at forgery will damage the microchip, which is irreproducible because of its cryptographic protection

(b) Only one medium to be checked

The second important advantage of the chip-on-paper solution is that passport, sticker and microchip are inseparable parts of a single document. The microchip's transmission/reception properties in effect transform the passport into an electronic file, which, for border control purposes, merely requires there to be a data-reading device nearby.

(c) Fast border controls

As a result, border checks would be speeded up considerably. To carry out a check electronically, it would no longer be necessary to type the names of the passengers into the computer. Border control staff would merely have to "swipe" passports in front of an electronic reader to display the entire contents of the microchip, i.e. biodata, photo, biometric data and any additional information. This would represent a valuable step forward as compared with the current situation; but even with a fully operational VIS, the speed with which border checks were carried out would be significantly increased.

d. Desirability of extending border controls to all travellers

Checking procedures will be so much faster and easier that serious consideration can be given to the idea of extending spot checks to a full, blanket check on all visa-holding foreign nationals crossing the border. Even for the further, more detailed checks applicable to only a tiny fraction of travellers, there will no longer be any need to key in data in order to check the VIS database. It will only be necessary to activate a button on the application mask at the border; this will make it possible, via a biometric data item, firstly to check the microchip data on the spot and secondly to check the VIS database. Those who fail to pass these checks and those with unreadable microchips in their passports, as well as those not in possession of a passport, will undergo separate identification by specialist personnel.

e. Storage of data obtained at the border

When it is up and running the VIS will contain a great deal of information on visa applicants and on the documents attaching to the visa. The inclusion of further information, obtainable at the border, such as the date of any border crossing, the type of crossing (entry/exit) and the identification code of the border crossing point, would considerably enhance the value of the VIS database from the point of view of future consultations. The database would contain a complete record of the person's movements within the Schengen area, for the purpose of checks at the border or within individual States. Chip-on-paper technology can confer this advantage at practically zero cost in terms of time and resources. By adding an extra "button" to the application mask, the information in question can be obtained automatically with minimal effort.

f. Utility of the chip-on-paper system pending a fully-fledged VIS

The chip-on-paper system is intrinsically useful, not only in the run-up to the full VIS. The VIS system will provide central validation via its database and store all data on travellers, which justifies the cost of setting it up.

However, the chip-on-paper system alone would make it possible to extend controls to all travellers, by virtue of the personal and biometric data on the microchip. A terminal at the border capable of reading the chip would be all that was necessary: travellers would simply have to place a finger on the fingerprint reader for the system to be able to check their identity and the match with the data on the "chip on paper".

6. Launching of a European prototype

a. Aim of the research

If a project of this kind is to be carried out, it would seem highly important for the operational stage to be preceded by the development of a prototype.

This should allow for the following:

- more extensive assessment of the logistical, organisational and technological implications;
- closer consideration of the details;
- further refinement of the technologies used;
- full testing of the entire architecture.

Establishment of a prototype would make it possible to assess directly the benefits obtainable from use of the proposed arrangement and might also enable adjustments to be made to organisational and application procedures at the selected sites.

b. Stages of the prototype

The prototype could be established in two separate stages:

- the first stage should involve local simulation of either a consular post or a border post interacting with the SIS database;
- the second stage would comprise actual testing in a particular area.

The first stage would last for a limited time and would allow for direct, swifter action for any architectural changes or modifications to be made.
It would be possible to assess the system's response to peak workloads and to stress affecting the entire architecture.
Once satisfactory results had been achieved for the first stage, the second stage could involve identification of suitable consular and border posts for prototype trials.

The criteria for selecting the posts which are to carry out the trials could be as follows::

- direct air links between the selected consular posts and the chosen borders; i.e. it should be possible for foreign nationals to reach the border in question without having to make a stopover in another Schengen country that does not have the prototype equipment;
- visa applicants of the type that can be expected to make multiple visits to the consular post or to the border itself;
- as the basic aim is a joint experiment, the selected posts should encourage the possible experimental inclusion of partners who may wish to participate at a later stage, thus permitting immediate integration of those with shared interests in the network of selected posts.

The prototype could be jointly developed by a number of partners participating in the agreement. However, the first stage would be easier to carry out if located in a single country, for obvious logistical and time reasons.

c. Seeing how the microchip works under real conditions

The proposed experiment should make it possible to test the various elements of the project in the field.

This could involve a series of steps, to maximise the anticipated benefits and to assess the suitability of the technology (size of the paper medium, size of the microchip).

The best type of microchip could be identified and tested on the basis of actual requirements.

7. Limitations imposed by privacy rules

a. Current legal limitations

When it comes to the protection of natural persons with regard to the treatment of personal data and the free movement of such data, account needs to be taken of the fact that databases containing such information are not currently regulated in a uniform manner in the Member States; consequently, the first thing to be done would be to check compatibility between Member States.

b. Problems with present legislation

One particular problem is that the digital processing of biometric data (photos and fingerprints) is not covered by the present Community Directives (Directive 95/46/EC of 24 October 1995 and Directive 96/9/EC of 11 March 1996). The same is true of legislation in the various Member States. There does not appear to be any explicit reference to the management of such data in the legislation in force in the Schengen States on legal protection for either persons or databases.

c. How similar problems were overcome in the past

A similar problem arose in the past when the Schengen Convention was put into effect. In that case, all the Member States had to ensure that they had rules in line with the provisions of the Council of Europe's Convention No 108 and Recommendation R (87) 15.

d. Use of the VIS project and the European agreement to overcome the limitations

The VIS project already involves a central database containing personal and biometric data and a computer network on which such data will circulate. Since the present Community rules, transposed into national legislation, do not meet the fundamental security requirements of the ongoing VIS project, those rules will have to be amended and adapted to meet the project objectives, which are also set out in the current proposal. The legal framework for those objectives has already been described in the first section of this document.

e. Reference criteria

Implementation of the principles contained in this proposal requires the following considerations to be taken into account:

- the personal data kept in the databases must be relevant to the aims pursued;
- any transfer of such data must meet the same requirement;
- personal and biometric data collected or transferred may not be used for any other purpose than that for which they were collected.

8. Conclusions

a. Member States' contributions

Assuming a prototype using contactless technology and in exploring the attendant problems, it is thought that all contributions drawing on partner countries' previous experience could be of inestimable value. The exchange of relevant information is to be welcomed, especially information on contactless technology, biometrics and data compression methods. Compression is particularly useful for entering biometric data (which usually take up a lot of memory) on contactless media (which do not generally have a large memory because of their small size).

b. Definition of new standards for contactless chips

In addition to the international standards already referred to in the literature on such technology, new standards are to be set specifically for the use of data relating to visas and the biometric aspect of visas. It will be necessary to decide on sizes and set working ranges, as well as the average values to be complied with so that the sizes chosen will be practicable. Introducing jointly approved parameters and identifying the limits on such parameters will facilitate the study and selection of visa data, including the computer aspects. This should be the particular basis for defining how data are to be recorded on computer media and how the recorded data are to be consulted. A universally valid compression technique will be agreed on, a method of encryption/decryption will be chosen, and a PKI typology will be determined. Given the complexity of the task ahead, it is clear that the success of the prototype experiment will depend on the involvement of the Member States and their spirit of cooperation.

c. Cost-effectiveness of chip-on-paper technology

The costs for a fully operational project can be identified, merely by way of illustration, as follows:

- hardware costs for microchip read/write terminals and for any equipment for recording and checking fingerprints, estimated at about EUR 200 per workstation;
- consumable hardware costs for the chip on paper, estimated at about EUR 4 per item;
- software development costs for the interface between terminals and the chip on paper, estimated at EUR 100 000;
- software development costs for the interface between read/write terminals and the visa-issuing systems currently used by each individual Member State. The cost will vary according to the sophistication of the particular systems in use.

In conclusion, consideration of the proposal as a whole shows it to be especially cost-effective, bringing considerable benefits for a particularly low cost.