COUNCIL OF THE EUROPEAN UNION

Brussels, 11 November 2004

14534/04

LIMITE

VISA 203
COMIX 684

NOTE

from:	The chairman of the Committee created by Article 6 of Regulation 1683/95 laying down a uniform format for visas
to:	Visa Working Party
Subject:	**Technical feasibility of the integration of biometric identifiers into the uniform format for visa and residence permits for third country nationals, passports and other travel documents issued by Member States**

Delegations will find attached the above mentioned document.

1. Introduction

On 24 September 2003 the Commission has presented two proposals as the first step in implementing the Thessaloniki conclusions, which aim to integrate biometric identifiers in the uniform format for visas and the uniform format for residence permits of third country nationals. The Commission's intention is to require Member States to integrate two biometric identifiers into the visa and the residence permit for third country nationals in a harmonised, interoperable way on a storage medium with sufficient capacity. The Commission proposals provide for the mandatory storage of the facial image as a primary biometric identifier for verification (one-to-one checks at the border) to be implemented within two years and the addition of an obligatory, second biometric identifier, which should be the fingerprint, to be implemented within three years, as it provides the currently best operational solution for so-called "background checks" (one-to-many searches) in databases.

A large consensus has been found on the approach proposed by the Commission and a political agreement–as requested by the European Council in Brussels on 16/17 October 2003- was reached at the Council (JAI) on 27 November 2003. Due to the fact that the EP had not yet given its opinion a final adoption of the proposals was not possible. The political agreement was confirmed in Council conclusions that also took up the issue of the necessity of a second proposal amending the Common Consular Instruction in order to create the obligation to enrol fingerprints during the visa application process and to specify the possible exceptions. Moreover these conclusions invited the Commission with the assistance of the Article 6 committee to start working on the technical specifications, necessary for the implementation of biometrics in the two documents in view of the confirmation of the technical feasibility of the solution adopted at political level.

On 23 February 2004 the Commission presented a proposal on common security standards and biometrics for passports and other travel documents issued by Member States as the second step. The proposal provides for the first biometric identifier, the facial image to be stored mandatory and leaves the second biometric identifier, the fingerprint, optional. At its meeting of 25/26 November, the Council (JHA) reached a political agreement on this proposal rendering also the second biometric identifier mandatory and providing longer time frames for its implementation (18 months for the facial image, 36 months for the fingerprints).

2. Procedure of the Article 6 Committee

In order to carry out the work within the time frame set out by the European Council of March 2004, which requests an adoption of the regulations and the necessary technical specifications for their implementation until the end of this year, the committee created 3 expert groups:

The first group, led by France, examined the question how the chip could be integrated into the visa and residence permit sticker; the second, led by Germany, what kind of chip would be necessary and how it would be rendered secure; and the third expert group, led by the Netherlands, had to find out about the necessary hardware for these operations. The work carried out would also be used for the establishment of the technical specifications for the passport.
The experts have met several times including joint meetings of the first and second group and the result of their work with several options was presented to the Article 6 Committee on 14 October 2004. The table in the annex summarises the outcome of the technical examination of the different options.

The chairman drew the following conclusions from the debate, which were endorsed by the Committee:

3. Conclusions

- Passports

The Article 6 Committee resumed from the work presented by the groups that the technical integration of a Radio Frequency chip in the passport and the storage of two biometric identifiers while assuring a high level of security of the data are technically possible in accordance with the provisions set out in the draft regulation and draft specifications.

- Visa and residence permits

The Article 6 Committee resumed from the work presented by the groups that there are more difficulties integrating a chip into a visa in accordance with the current draft regulation. The main problem consists in the so called "collision" problem, which leads to difficulties for the reader to read out the valid visa in case there are several contactless chips on different visa in the same passport. The reading of the valid chip in the visa would require difficult handling procedures. These difficulties lead to the conclusion that the solution envisaged by the draft regulation (option 1a) is technically not feasible.
These difficulties also apply to other similar solutions. Therefore, options 1b, 2, 3 and 3a are not technically possible at the current stage of technology (1a).

The expert groups also examined the technical feasibility of two other options, which were not in line with the current draft regulation, but would enable the integration of biometric identifiers.

According to option 4 the visa sticker would be accompanied by a separate smart card, which should then be defined as part of the visa. There would be one card issued with every visa.
In this case the collision of several chips would be excluded, as the card can be separated from the passport and read individually. The durability issue would also be fully taken into account.
Measures would have to be established on how to proceed if a traveller has lost or forgotten his/her smart card containing the biometric elements.
Some delegations wished to have the name of the holder on the card which would entail additional costs as they would have to acquire card printers. The solution proposed was to attach the control coupon of the visa sticker on the card. The link to the visa would be ensured via basic access control (the Machine Readable Zone of the visa would open the chip integrated in the smart card).

Some delegations were in favour of this solution that is technically feasible, either as a definitive solution or as a transitional one while awaiting the VIS. Some of these delegations asked whether it would not be possible to conceive a completely new "visa-card". However, it was stated that in the short time frame it would not be possible to establish a new uniform format for visa in form of a smart card containing all required security features. Furthermore, for security reasons the issuing process for cards should be laser engraving, which because of the high costs must be done by central issuing authorities. The whole process of visa issuing would have to be reviewed.

The Article 6 Committee asked the delegations to give some indications on the possible costs in relation to option 4 taking into account the equipment at the consular posts and the border control points which is necessary to implement this solution.

Two delegations were in favour of option 5: the visa sticker without chip but biometric elements would be stored on a 2-D-bar code.
In this case the collision problem would not occur. However, the 2-D-bar code has only capacity to store two fingerprint templates which is not in line with the current draft regulation and ICAO standards. Furthermore the design of the uniform format for visas would have to be completely changed, a complex and time consuming exercise.

Some delegations stated that they would rather prefer to wait for the VIS getting operational and integrating biometrics of visa applicants in the VIS rather than adopting costly solutions which would not bring a biometric solution that much quicker. However, a similar solution would presently not exist for residence permit applications. It was reiterated by two delegations that only if the VIS is operational with biometrics in 2007/2008 it could be an alternative but otherwise the biometrics in the visa is needed. It became clear that this solution depends on the timing for the VIS. COM assured that the central part of the VIS will be ready in time; of course, the full implementation of the VIS also depends on Member States as regards the connection to the national contact points. Therefore Member States have to judge, when they will be ready to connect their national systems to the central unit.

11.3 Options available

Option #	1a	1b	2	3/3a	4	5
Option description	**Each visa has a biometric chip**	**Each visa has a biometric chip on attachment**	**One biometric chip in visa every 3 years, conventional visa in between ("4+1")**	**One updateable/not updateable biometric chip in first visa**	**Visa sticker and separate Biometric Visa SmartCard**	**Visa sticker without chip, biometrics in 2D barcode**
Properties						
Application of visa	Conventionally glued in	Conventionally glued in visa sticker with fold out perforated attachment on visa page	Conventionally glued in	Conventionally glued in	Conventionally glued in visa sticker, separate biometric visa SmartCard	Conventionally glued in
Number n of eVisa chips in passport during 10 yr. lifetime (+ ePassport chip)[5]	n (+1) n unpredictable[1]	n (+1) n unpredictable, even with the possible removal of invalid visa chips[1]	3-4 (+1) $n \leq 4$[1]	1 (+1) $n = 1$[1]	0 (+1)	0 (+1)
Relation Chip : number of MRZ(s)[6] to be read for personal data of valid visa and BAC[7] of chip visa	1:1 (valid visa always with chip)	1:1 (valid visa always with chip)	1:1 (if valid visa with chip) 1:2 (if valid visa without chip)	1:1 (if chip was updated with latest MRZ or is included in valid visa) 1:2 (if chip in first visa is not updateable)	1:1	-

[5] This consideration neglects the possibility that third countries outside the EU could apply visa containing RF chips. If the passport does not contain a chip, the potential collision problem only occurs between eVisa chips. In that case, (+1) becomes (+0).

[6] MRZ: machine readable zone

Option #	1a	1b	2	3/3a	4	5
Option description	**Each visa has a biometric chip**	**Each visa has a biometric chip on attachment**	**One biometric chip in visa every 3 years, conventional visa in between ("4+1")**	**One updateable/not updateable biometric chip in first visa**	**Visa sticker and separate Biometric Visa SmartCard**	**Visa sticker without chip, biometrics in 2D barcode**
Proposed Handling						
Handling pages, including BAC (using MRZ data to access chip) optimum conditions assumed	1. Read MRZ of valid visa 2. access the chip 3. verify data: end	1. Folding out the attachment of the visa 2. Read MRZ of valid visa 3. Place chip attachment on reader 4. access the chip 5. verify data: end (chips of visa no longer valid are removed)	1. Read MRZ of valid visa 2. If visa has chip → continue with 3. If visa has no chip → continue with 5. 3. access the chip 4. verify data: end 5. select visa with chip 6. read its MRZ 7. access the chip 8. verify data: end	1. Read MRZ of valid visa 2. valid visa is first visa → continue with 3. valid visa without chip/*updateable chip* → continue with 5. valid visa without chip/ *not updateable chip* → continue with 8. 3. access the chip 4. verify data: end 5. select first visa 6. access the chip (chip was updated with latest MRZ) 7. verify data: end 8. select first visa 9. read its MRZ 10. access the chip 11. verify data: end	1. Read MRZ of valid visa 2. Place card on reader 3. access the chip (chip card contains MRZ of corresponding visa) 4. verify data: end	1. Read MRZ of valid visa 2. Read 2D barcode 3. Verify data: end

Option #	1a	1b	2	3/3a	4	5
Option description	**Each visa has a biometric chip**	**Each visa has a biometric chip on attachment**	**One biometric chip in visa every 3 years, conventional visa in between ("4+1")**	**One updateable/not updateable biometric chip in first visa**	**Visa sticker and separate Biometric Visa SmartCard**	**Visa sticker without chip, biometrics in 2D barcode**
Problems						
Anti-Collision[8]	Not possible, even when using tighter but proprietary standards (mifare ®), since n > 4	possible (but not proven), possibly using tighter but proprietary standards (mifare ®), n ≤ 4	possible (but not proven), possibly using tighter but proprietary standards (mifare ®), n ≤ 4	might be possible (but unproven) , n = 1	no problem	no problem
Standards compliance	• ICAO LDS[9] 1.7 • ICAO PKI[10] 1.0 • not possible even with tighter ISO 14443	• ICAO LDS 1.7 • ICAO PKI 1.0 • might require tighter ISO 14443	• ICAO LDS 1.7 • ICAO PKI 1.0 • might require tighter ISO 14443	• Not ICAO LDS 1.7 (for updateable chip) • ICAO PKI 1.0 • Possibly no changes to ISO 14443	• ICAO LDS 1.7 • ICAO PKI 1.0 • No changes to ISO 14443	• not ICAO compliant • does not correspond to EU proposal • proprietary templates necessary
Risk of failure due to interference between eVisa chips	Will "kill" eVisa chip functionality	high, since: • functionality not guaranteed • no standards • RF field might detect more than one chip	high, since: • functionality not guaranteed • no standards • RF field might detect more than one chip	n/a if no third party eVisa involved	n/a if biometric visa SmartCard removed from passport	n/a
Risk of failure due to interference between ePassport and eVisa	Will "kill" ePassport chip functionality	high, since: • no standards • RF field might detect more than one chip	high, since: • no standards • RF field might detect more than one chip	medium, since: • no standards • RF field might detect both chips (ePassport + eVisa)	n/a if biometric visa SmartCard removed from passport	n/a

[8] Collision: Describes the interference between various chips and the reading device, e.g. due to de-tuning of the resonance frequency, resulting in malfunction

[9] LDS: Logical Data Structure

[10] PKI: Public Key Infrastructure