International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/16
WP/16
13/9/05
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS

Sixteenth Meeting

(Montreal, 26 to 28 September 2005)

Agenda Item 2: Implementation of e-passports
Agenda Item 2.1: Progress and issues

TECHNICAL REPORT ON E-VISAS

(Presented by the New Technologies Working Group)

1. INTRODUCTION

1.1 A work item to address the issue of electronic visas, including database, card and chip visa methods was approved as part of the NTWG workplan by TAG 15. It was acknowledged that States and member organisations needed to identify common MRTD compliance issues that may emerge as States begin to put in place electronic visas that may use MRTD biometric technology in common with the e-passport. It was agreed standardisation may be required in order to ensure interoperability with the emerging standards work on e-passports. Since TAG 15 a draft technical report has been undertaken.

1.2 The attached Technical Report provides a summary of the types of electronic visas under consideration and the issues as they are currently understood. Continued development of the policy issues is recommended as technical issues are further explored by member States.

1.3 The issue of collision between e-passport and visa chips was raised as a significant concern that may interfere with the successful operation of e-passports. A summary of the issue is provided in the attached technical report. This issue has been shown to be less of a technical concern with industry able to demonstrate that multiple chips can interoperate within a field without undermining the functioning of any single chip. ISO should be consulted to provide any required specification update. This will serve to validate this approach and report back to the NTWG.

(2 pages)

2. ACTION BY THE TAG/MRTD

2.1 The TAG/MRTD is invited to:

a) the TAG-MRTD is invited to approve continuation of the on-going development of an e-visas technical report being carried out by the NTWG.

— END —

Report on E-Visas

Version 3 – July 21, 2005

Drafted for ICAO/NTWG

V.1	19/10/2004	Lesley Soper (Canada)
V.1.1	20/10/2004	Comments from Germany: Uwe Seidel
V.1.2		Jean Salomon comments
V.1.3	15/11/2004	Baggeroer and Salomon comments merged
V.1.4	25/11/2004	J. Salomon revision
V.2	14/01/2005	Version 2 with recommended approach of NTWG
V.2.1	12/4/2005	Updated by Lesley Soper
	19/05/2005	Update proposed by Jean Salomon (one bullet in § 6.5.4)
		Second update proposed by Jean Salomon
V.3	21/7/2005	Updated with comments from NTWG Lyon

1 The case for e-visas

As part of the mandate of New Technologies Working Group (NTWG), ICAO has been developing an interoperable electronic storage media for documents with the goal of enabling machine assisted identity confirmation (biometric identity management) of persons for border control purposes. Significant work has been undertaken on this issue as it relates to the Passport standard as specified in ICAO DOC 9303 Part 1. In the meantime, member states have indicated their strong interest in preparing a technical report that synthesises the norms that were developed for an interoperable e-passport with the need for normative guidance on an e-visa.

Why an e-visa? E-visas present an opportunity for States to:
1. use electronic data collected for their entry programs
2. have a more speedy and ergonomic method to read data from an official travel document
3. facilitate the identity management of visa holders through machine assisted identity confirmation
4. facilitate travellers through check-in and border processes

Why should ICAO be involved? It is practical for States to harmonise their passport reading methodologies with those used for visas in order to ensure interoperability at border inspection, transit and airline check-in. As e-passports will conform to an interoperable standard, it is logical that guidance should be provided to ensure that the current ICAO DOC 9303 Part 2 is compatible with this vision as countries move toward electronic visas. Further, ICAO has a significant role in providing the basis for e-visa interoperability in order to ensure that e-visa techniques employed by individual states do not interfere with the successful global interoperation of e-passports and e-travel cards.

1.1 Goals

1.1.1 ICAO's MRTD compliance

This timely specification and updating of standards enables member States to continue to implement biometrics-related technologies as soon as possible, confident they are ICAO standards compliant.

In implementing biometrics standards for MRTDs, key considerations are:

- Global Interoperability – the crucial need for specifying how the biometrics deployed are to be used in a universally interoperable manner
- Uniformity – the need to minimise via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States
- Technical Reliability – the need for provision of guidelines and parameters to ensure member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading data encoded by other States can be sure that the data supplied to them is of sufficient quality and integrity to enable accurate verification at their end
- Practicality – the need to ensure that recommended standards can be operationalized and implemented by States without them having to introduce a plethora of disparite systems and equipment to ensure they meet all possible variations and interpretations of the standards
- Durability – that the systems introduced will last the lifespan of a travel document, and that future updates remain backwards compatible.

1.1.2 Improved verification and facilitation at borders, transit points and other control points

Visas communicate data in a machine readable format to airline authorities and border officials in transit and receiving countries. The machine readable zone provides a systematic way to gather and compare personal data electronically particularly when the passport document is not already machine readable. With the advent of e-visas, the same data and additional biometric or other data can be stored and read. This offers the possibility of facilitated or self-service inspection and the capacity to verify biometric information that is stored on or linked to the visa. Moreover visa programs are linked to identity management of persons seeking asylum and allow countries to determine whether irregular migrants travel via official channels or underground ones. Guidance on electronic visas can serve to assist countries in better managing the irregular flow of people.

1.1.3 Derived - Practical experience on implementing multiple biometrics

The work recently undertaken on the e-passport and testing conducted on prototype documents have indicated that significant work still needs to be done to ensure that IC Chip/RF technology can handle multiple functions and that readers can handle multiple signals. Interoperability and anti-collision are two key concerns that will be addressed in this report.

2 e-Visa types – advantages and limitations

NTWG has authored a Technical Report related to biometric use in passports which specifies many interoperable standards which are relevant to e-visa. This document takes into consideration the passport technical report and adapts the concepts contained to the following three general methodologies that can encompasses a number of information storage techniques:

- Visa information written to an e-passport chip: This technique has the advantage of a single technology in a given book but will not address the ongoing need for states to issue visas where an e-passport is not available. Countries that are interested in implementing a system based on this notion will be limited by the lack of availability of e-passports and the need to set up an alternate non-electronically enabled visa system to deal with countries that do not issue e-MRTDs. For these reasons, this solution is a long-term strategy. Nonetheless, NTWG should work to establish a set of standards to achieve use of this visa option.
- Chip visa sticker: A sticker IC contactless chip has many advantages for visa issuers including the capacity to carry biometric data on a document without requiring a real-time database at all points of service to verify biographic and biometric data. This is particularly useful concept given that many travel documents are not machine readable. However, technical constraints such as a collision will be key to the proliferation of this method.
- Chip in a multi-use visa card: Multi-use documents have increased in use in binational and multi-lateral settings. As biometric and card technology matures, card visas will grow in popularity owing to their durability and ease of use.
- Central database: visa points to data stored in a database
- Central database: passport points to data stored in the database
- Hybrid: chip points to database

3 Visa Programs and the Need for Biometric Data

States will have varying requirements for what type of biometric and other data are required for the purpose of a visa. Minimum information is already specified in DOC 9303 Part 2 and it appears in the visual and machine readable zones.

Visa programs are linked to management of visitors and asylum within countries. There is a strong tendency for countries to consider a visa as the first opportunity to enrol a client as they move through a client identity management continuum. The biometric, if captured upfront in the process can be used for many downstream processes: e.g., facilitated entry, asylum identification, change of status management, benefits. For these reasons there is strong interest in a multimodal approach to biometrics in this program. From environment analysis of countries considering biometric visa programs, a multi-layered approach is emerging as a common requirement.

It is possible that, unlike the e-passport, not all states will require an electronic portrait to be registered for the visa. Instead States may consider other biometric data for registration such as fingerprints or iris. Given the limited amount of data storage that may be available on a visa or passport chip, ICAO should recommend a flexible standard that takes into consideration the storage constraints of each visa methodology.

In keeping with the spirit of the e-passport standard, when a biometric is registered and where there is intent to achieve global interoperability via use of biometrics, storage of the biometric image is mandatory, and storage of an associated template is optional at the discretion of the Issuing State.

As with the recommendations for the e-passport, secure enrolment is critical to the overall integrity of a biometric/electronic document program. Recommendations on secure registration from the Technical Report on e-Passports should be applicable also to visas.

4 Interoperability issues

4.1 Readability by other stakeholders such as airlines and transit countries

One of the benefits of an electronic visa program will be the potential to share information with airlines at check-in and with countries processing travellers in transit. If interoperability is to be complete, the e-visa should be readable and authenticable by all interested parties along the travel continuum. Like the MRZ, electronic visa information can help to facilitate known travellers and provide the additional capability of providing identity confirmation.

4.2 Increased capacity to authenticate

If electronic visas are compatible with e-passports, there will be greater incentive for airlines and border administrators to adopt a policy of verification using a single suite of document and biometric reader technology. Increased use of electronic verification tools would contribute to ICAO's overall security goals.

4.3 Technical constraints

There are significant technical constraints to proposing interoperable technology:

- Database only methods will not be capable of interoperability, unless the method is based on an open network structure that is accessible by multiple authorities (see ETA).
- Multiple biometrics on a IC chip in a visa sticker as well as on a separate card will pose problems in terms of storage. In the Logical Data Structure (LDS), the variable size data item that has the most impact on storage capacity are the images of the biometric features. In practice, a facial image can be compressed to an optimal range of 15K-20K. Similar studies on fingerprint have shown the optimal image size is approximately 10K of data per finger. Similar studies on iris have shown the optimal image size is approximately 30K of data per eye. Storing optimally-compressed images ensures maximum flexibility and vendor independence for both current and future biometric matching requirements. However, initial analysis of placing this type of data on a visa sticker indicates that it is likely to be both cumbersome and costly.

4.3.1 Relieving some technical constraints

- There may be a need to consider an alternate set of minimum data items for a visa LDS that would allow chip visas to be both interoperable, technically feasible and cost effective. A rationale for it would be that, most of the time, the State issuing the visa is also the most interested in further examining it. This would make e-visa interoperability less of an open problem, and could also lead to promoting the use of minutiae instead of full biometrics images (with reduced chip size, faster access times and reduced cost).
- As a consequence, most of the interoperability burden may shift back on the e-passport, above and beyond the present face image endorsement, should multiple biometrics become a *de facto* standard in future border crossing procedures. This cannot be practically resolved until the e-passport can be rewritten.
- At the same time, States will need to have a minimum data standard such as the digital portrait to ensure basic interoperability with all states as per the passport recommendations. Though, as suggested in Section 3, States may not have a requirement for the digital portrait making compliance difficult.
- There is still a significant issue of collision between multiple visa or card chips and e-passport chips when used simultaneously. This is dealt with in Section 6 below.

Comment [S1]: ?

5 Data Requirements

5.1 Draft Visa Data Requirements

The current ICAO standard for a visa contains the following data elements that would be the basis for inclusion on a passport chip visa:

- Doc type
- Issuing state
- Name of Holder
- Document Number (Passport or Visa number)
- Check digit.
- Nationality
- Date of Birth
- Check digit - Date of Birth
- Sex
- Date of Expiry
- Check digit - Date of Expiry
- Optional data

It is assumed that the same data requirements are needed for electronic visas, even though this data may be a replication of elements that may already exist in the LDS of a passport chip. In order to avoid duplication at the passport and visa level, a simplified set of visa specific data can be derived that could include:

- Doc type
- Issuing state
- Visa Number
- Check digit
- Date of Expiry
- Check digit - Date of Expiry
- Optional data

Within the optional data there may be scope for other data requirements, including:

- Visa type
- Conditions
- Updated biometric info or template
- Public key data

6 Visa information written to an E-passport chip

The current ICAO standards for the e-passport specifiy an IC contactless chip formatted according to the Logical Data Structure (LDS). Within the LDS, there are data groups reserved for the capacity for States to write information to the chip, such as visa information. At present, further work is required since the current LDS Technical Report does not provide a methodology for non-issuing states to write visa information to the passport chip. The LDS Technical Report, in effect, recommends locking the chip after personalisation until such a time as a smart function can effectively manage changeable data. This type of function would be a cost-effective method to manage visas, however, owing to lack of use of e-passports, this will not be a viable solution for most countries with visa regimes.

6.1 Background

According to the E-Passport Technical Report, ICAO has maintained the capacity to add data to a passport chip though has not enabled this capacity in the first version of the standard. The report states:

> *LDS Data Update by Other States: To minimise security and data protection complexity, the NTWG has decided at this time [ref The Hague - February 2004] to not endorse updates of chips in ePassports subsequent to their personalisation at the time of passport issue to the holder ie ePassports will be "write-once".*
>
> *In the future however, the LDS will need to support "write-many" applications. Some such practical applications for the "write-many" version of the LDS specification include:*
> - *Issuing State writing a second biometric into the LDS created by the Issuing State – eg: updating a facial biometric as a result of plastic surgery, adding a different type of biometric at a later date eg: future addition of an iris image*
> - *Receiving State writing a second biometric into the LDS created by the Issuing State – eg: adding verified live image of the passport holder as captured at the airport*
> - *updating visa data*
> - *updating frequent traveler data*
> - *storing travel records*
> - *storing automated border clearance records.*

It is anticipated that within the next ten years, as States adopt e-passports, there will be pressure on ICAO to expand the potential use of the e-passport chip to include other data. In order to address potential concerns and to build a future capacity for the addition of visa data to the e-passport, a minimum set of requirements are needed. To facilitate the expanded use Data Group 18 (DG18) has already been designated in the Logical Data Structure to accommodate visa information.

6.2 Data Security Requirements

The e-passport is subject to a PKI digital signature to ensure the authenticity. Likewise, DG 18 would be subject to the same level of certification, put in place by the visa issuing state when writing visa information to a passport. The specification for this function will be similar to the current ICAO DOC 9303 PKI process for the e-passport.

6.3 Storage Contraints

6.3.1 Size allotted for visa use

It is recognised that adding visa data to an e-passport chip will add to the overall data carried on that chip. As such, passport issuers would be responsible for making a reasonable amount of storage space available as a courtesy to other countries that may use this space. Consideration needs to be given to how much space would be reasonable and the maximum number of visas that may be permissible in a book. To mitigate storage constraints, consideration could be given to delete visas that are no longer required by the holder or expired.

6.3.2 Option of a standalone visa sticker

It is recognised that adding visa data to an e-passport chip may place too much burden on the passport issuing state to have a larger memory capacity on their RF chip. As options, ICAO NTWG should consider a standalone visa chip that could be part of passport manufacture or which is added by the visa issuing state that is the first to add a chip visa to a book.

- Passport issued standalone chip: The advantage would be to have the infrastructure for e-visas in place in a collision managed environment. The disadvantage would be the cost burden for passport issuing states, however the capacity may be sold as a benefit to holders that travel frequently and require visas.
- Visa issued standalone chip: The advantage of a single standalone visa chip added by the first issuer is a collision managed e-passport independent system for electronic visas. To its disadvantage, two types would need to emerge: a low memory capacity supplement chip to an e-passport and a high memory chip to hold data elements that are not available in a passport without a chip, such as biometric data. The cost burden would be on the first visa issuer which may hinder the uptake of e-visas.

6.3.3 Durability of chip

Particular policy concerns may arise if a visa is written to a faulty chip. Clearly, States would need to assure themselves that the passport chip is sufficient to meet their visa needs. It would be that chips will invariably fail either through tampering or for technical/physical reasons. In cases of failure to read, a backup option may be necessary, such as an electronic travel authority via database or a sticker.

6.4 Reading Constraints

When reading a passport chip containing a visa, a significant amount of data is involved if all of the DGs are read in sequence. Readers may wish only to read from the visa DG 18 - the feasibility and the desirability of this is to be determined.

7 Chip in visa sticker

7.1 Background

In the same way that e-passports are enabled with a contactless chip, new chip and security technologies will allow visa stickers to carry the same type of IC chip. This technique requires that similar, interoperable and consistent addressing and storage methods are used in order to ensure that e-visas are compatible with e-passport

7.2 Data Security Requirements

The e-visa would need to be subject to a PKI digital signature to ensure the authenticity in the same manner as an e-passport. The specification for this function will be similar to the current ICAO DOC 9303 PKI process for the e-passport. States may be interested in a non-interoperable, fully encrypted visa. Guidance should be provided on how this type of e-visa could be achieved and the limitations this may place on enhanced interoperable uses detailed in 6.4 below.

7.3 Interoperability

E-visas are placed in a passport for primary use by the issuing state. However, it must also be recognised that third parties may wish to use the visa information such as airlines, transit authorities and other entities within the issuing country. To be of value as an interoperable data carrier, the e-visa must conform to a data standard and have universal reading capacity. Moreover, basic interoperable elements will need to be present such as the biographic data contents of DG1 and the primary biometric data of DG2 both of which are considered mandatory within the e-passport standard. The key barrier to the proliferation of e-visas and interoperability is collision. Section 6.5 below describes the issue of collision when several chips are placed within a single reading field.

7.4 Collision

The capability to distinguish between with various RF tags and communicate simultaneously with them while present in the same RF field (aka resolving anti-collision) has been demonstrated in many other ISO 14443 applications (eg: mass transportation).

However, only very few of those applications have as additional constraint the fact that one given tag (ie the e-passport) should never be made unreadable by others simultaneously present (ie one of the e-visa chips embedded in a sticker).

Thus, there is significant concern that chip visas that are used within or in tandem with an e-passport and potentially with multiple e-visas will cause RF signals to malfunction and not interoperate. A key goal of this Technical Report will be to review limits for such co-existent chips to be interoperable.

Comment [S2]: This is quite a goal. To achieve this, very deep technical considerations or, on the other hand, formal regulations (such as "it is forbidden to use multiple e-visas in stickers within the same passport book") are required. We have this discussion within the EU right now. See some text below from the Draft EU document which explains the problem.

7.4.1 Constraints

The integration of electronic RF-chips in visa stickers will lead to a number of technological and practical challenges to be overcome for a successful deployment of biometrics. When implementing contactless RF-chips into visa stickers glued into passports, it must be ensured that:

- the function of the e-visa is guaranteed, even if there are more than one electronic chip present in the field of the RF-reader (anti-collision detection)
- the introduction of e-visas will not disturb the functionality of an ICAO compliant RF-chip in the passport itself,
- the interoperability with the system infrastructure for the electronic passport remains guaranteed,
- the reader is able to chose to communicate with one particular chip, after establishing the "list" of all responding chips. Consequently, the reader will have to establish the communication with all chips in the field in the reader, then determine which is the "valid" visa, then read data (this may have some impact on the global reading time, should many tags be present in the e-passport),
- the presence of multiple tags in the RF field will not alter the ability of the reader to operate on specs, while successfully reading back information transmitted by each tag. This particular point will be further described in the two paragraphs below.

7.4.2 Reader *vs.* Tag specifications

- ISO 14443 A and B specifications duly describe the reader characteristic RF field constraints, in particular in terms of radiating power which is emitted through the *reader antenna* ; on the *tag antenna* side, however, both for the e-passport and the e-visa, there is no precise specification which would require a particular design antenna *tuning* (eg: setting a *precise* resonance frequency and bandwidth during manufacturing).
- Hence, there may be room to further draft proper tag antenna specifications which would enhance the ability of the reader to operate according to its specifications even when multiple RF tags are present in its field.
- Such specifications could involve both the tuning frequency and size of the tag antennas to be used in e-visas. As an example only, here are two criteria which could be explored:
  - designing visa tags with antennas tuned toward higher frequencies resonance (eg: 22 MHz) would ease the dialog between the reader and each multiple tag, because the reader could still maintain the global RF field within its operational power range specifications, while meeting the requests to dialog with all tags present in the field.
  - since the above use of a tag antenna "detuned" towards higher frequencies would reduce the efficiency of the data communication between such tag and the reader, the use of a larger visa antenna (eg: ID3 vs. ID1) would tend to restore most of the lost sensitivity and facilitate each separate tag interaction with the reader.

7.4.3 Worsening cases *vs.* mitigating effects in the case of multiple tags

- From the practical point of view, each of the visa couples "chip-antenna" present in an e-passport with sticker visas will tend to modify the RF field for the other couples, thus necessitating, according to the passport reader design, an increased need to adjust the reader's emitted RF energy to break through to all other tags. This coupling effect between the various chips and antennas will be maximised when the visa sticker's antennas will be exactly overlaid in successive passport pages and will tend to affect negatively the global readability.
- A mitigating factor would be the increased thickness of each e-sticker (eg: because of its laminate anti-counterfeit). The sticker protection layer does increase the separation between adjacent antennas above the standard passport page thickness, which would decrease the importance of the above coupling.
- The additional mitigating effect of carefully designing the resonating frequency for the antennas of the tags above 13.56 MHz in the antenna-tag inlay manufacturing process has been discussed in Paragraph 6.5.2 above.

7.4.4 Interim Conclusion on Collision

- In view of the absence today of a well defined manufacturing standard imposed for the frequency tuning of the tag antennas, the approach to the issue of multiple tag handling in e-visas remains somewhat of a challenge.
- Effective worst-case practical scenarios need to be conducted to assess the maximum "reasonable" number of chips bearing visas retrievable at the same time. Such a pragmatic approach has been recently undertaken by a leading group of EU Control Authorities and their findings, if and when available, should been taken into consideration.
- To the extent that it is practically workable, we suggest to investigate within the industry the influence of varying the size and intrinsic resonance frequency of multiple chip-antenna couples (above 13.56 MHz by manufacturing) on the overall readability of multiple tags in the RF field. Since different types of e-visa chips, each powered via its antenna, might have specific power consumption data, such an investigation may have to be extended to multiple antenna-chips manufacturing sources as well.
- The matter was found important enough by some industry leaders, which are part of WG8, to recently propose a concerted research effort with the governments along some of the lines described in the above Paragraph 6.5.1 and 6.5.2. An initial technical description

of the underlying physics involved can be found in ISO WG8 Paper N1088 entitled "Electronic Passport and Electronic Visa, Air Interface". Additionally, ISO has compiled recent experimental results on the feasibility of collision avoidance in multiple e-visas.

- A practical goal of this type of investigation would be to produce a set of additional specifications which would permit compliance of the tag-antenna sets during the manufacturing process. Results, if and when available from the industry, could perhaps be part of an updated Technical Report to go beyond presently available experimental data. ~~reported in the concluding Paragraph 9 (Appendix II) of ??.~~

Comment [js3]: Suppress this double-stiked words !!

7.5 Policy Considerations

In addition to the key issue of collision, the NTWG should seek clarity and direction for a number of policy considerations that apply specifically to the use of standalone visa chips

- <u>Notification to the country of passport issuance of the insertion of chip visas:</u> NTWG could consider recommended guidelines to ensure that appropriate protocols are used by visa issuers to notify of chip use in a visa.
- <u>Visible indication of chip use in visa:</u> It needs to be determined whether a physical notification is required on the visa to indicate that an IC chip is present. This is recommended practise for e-passports in order to notify holders and authorities who are users of the chip. An indicator would have the benefit of alerting other parties to the availability of the data in an interoperable electronic format.
- <u>Capacity to cancel a chip visa:</u> Methodologies exist to physically cancel a chip visa. Acceptable methods to indicate cancellation without prejudice may be required in order to disable a chip visa that may persist in use for a significant period of time after use. Passports typically have a ten-year validity while visas are typically issued for one time use up to 5 years. Likewise, visa issuing states may have need to erase or void content due to error without the capacity to mechanically void the contents of a chip.
- <u>Privacy safeguards:</u> NTWG should consider levels of privacy safeguards that should be in place to protect the holder of an electronic visa. Skimming and eavesdropping by non-authorized parties continue to be a concern. While trying to maintain the interoperable capacity of a chip visa, guidance on levels of encryption and/or basic access control guidance may be required.

8 Chip in multi-use visa card

8.1 Background

Multiuse visas are sometimes issued in the form of an ID format travel card and conform with the LDS that was developed for ICAO DOC 9303 Part 3. This standard needs to be updated to reflect the new LDS and the incorporation of biometrics as well as address concerns of collision with e-visas and e-passports.

To a large extent, a chip layered in a separate (detachable) visa card would not cause significant collision detection problem if and when read separately in the RF field. The analysis of the cost-effectiveness, security, the impact on standard border procedures as well as on exception handling cases for such e-visas might closely follow the results readily available in Singapore's recent Technical Report on the Hybrid e-passports.

8.2 Data Security Requirements

The visa card would need to be subject to a PKI digital signature to ensure the authenticity in the same manner as an e-passport. The specification for this function will be similar to the current ICAO DOC 9303 PKI process for the e-passport. States may be interested in a non-interoperable, fully encrypted card visa. Guidance should be provided on how this type of card visa could be achieved and the limitations this may place on enhanced interoperable uses detailed in 7.4 below.

8.3 Interoperability

Card visas have potential for use on a bi-national and multi-national level. It is also recognised that third parties may wish to use the visa information such as airlines, transit authorities and other entities within the issuing country. To be of value as an interoperable data carrier, the card visa must conform to a data standard and have universal reading capacity. Unlike e-visa stickers, collision is not seen as an issue as a card will be read as independent from a passport booklet.

8.4 Policy Considerations

There are a number of policy considerations that support the use of card format visas, primarily:

- Reduction of collision with co-existent passport technologies if the card is used independent of the e-passport
- Increased privacy for the bearer: The holder has the capacity to present or not present a standalone card as desired without a prejudicial mark in the passport

Nonetheless, NTWG will need to prescribe document security measures similar to the e-passport to ensure authenticity of the document and data carried within.

9 Central database

9.1 Electronic visa in data base only (pointer)

Owing to the sovereign nature of visa data, many States view database storage of this information as the only viable electronic option. This methodology ensures that information is not improperly accessed or misused. Such a system can interoperate with a traditional ICAO DOC 9303 Part 2 Visa. The visa document could be used for inspection but may contain a machine-readable pointer to allow the receiving state to access the electronic record of the holder, which may contain biometric or other information.

This model does not allow interoperability with stakeholders as discussed in Section 5 below. As such, any description of this methodology is for informational purposes not normative, as States will choose methodologies in accordance with their individual need.

9.2 Electronic visa authority

NTWG is interested in drafting a separate working paper on the concept of the Electronic Travel Authority.

10 Hybrid

There are many types of hybrid options that result from visa, card, passport and database storage methods. These include using the passport, visa or card to point to databased information instead of storing the data directly on the chip. This is a feasible option particularly for passport chips where States would want to ensure that their IC chip is not written to excessively by other States. This hybrid solution would ensure that only a minimum of data is stored, thereby minimising chip costs and visa issuing States would have better capacity to protect the data collected from being improperly accessed or misused. Further exploration is required to determine whether hybrid options can serve the goal of interoperability.