International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/18-WP/8
22/4/08
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRTD)

EIGHTEENTH MEETING

Montréal, 5 to 8 May 2008

Agenda Item 1: Activities of the NTWG
Agenda Item 1.8: Guidance to Border Control Authorities on Handling ePassports that Fail to Read

GUIDANCE TO BORDER CONTROL AUTHORITIES ON HANDLING ePASSPORTS THAT FAIL TO READ

Presented by the New Technologies Working Group (NTWG)

1. INTRODUCTION

1.1 The increasing volume of ePassports that are now in circulation means that globally border authorities will encounter increasingly large numbers of these documents. It is recognised that much of the development of ePassports has been led by passport issuers and that amongst border inspection authorities there are varying degrees of understanding about the ePassport and its interface with the border inspection process

2. BACKGROUND

2.1 The provision of some form of guidance on ePassports and in particular guidance focused on the chip, is now essential for border control authorities given the rise in ePassports in circulation. The primary aim of such guidance is to provide guidelines on how to deal with ePassports that fail to read. The secondary aim is to avoid unnecessary delay for genuine travellers holding an ePassport that fails to read at border control.

2.2 At TAG17 in March 2007 a paper was presented on processing travellers presenting ePassports that fail to read (TAG-MRTD/17-WP4). The TAG approved the need to develop guidelines which are now attached.

(2 pages)

2.3 The guidelines aim to provide a relatively non-technical approach to the ePassport, some background information, how it works, how it provides added security value to the travel document and what problems a border inspector may encounter with such documents. The guidance includes practical steps that should be taken where a problem with the chip is encountered and explains why such problems can occur.

2.4 is acknowledged that there is a balance to be struck between facilitation of travellers and ensuring the security of the border inspection process. Inclusion of the chip allied to existing physical security features in the book together provides an increased degree of security to the overall book. Consequently the guidance emphasises that where there is a problem with the chip, the physical security features of the book continue to be of paramount importance in the border inspection process.

3. ACTION BY TAG/MRTD

3.1 The TAG/MRTD is invited to:

a) Approve the content of the attached Guidance paper
b) Approve its inclusion in the next Supplement
c) Approve its inclusion as an informative annex to Annex 9

— — — — — — — —

TAG-MRTD/18-IP/3
related to WP/8
22/4/08
English only

International Civil Aviation Organization

INFORMATION PAPER RELATED TO WP/8

GUIDANCE TO BORDER CONTROL AUTHORITIES ON HANDLING ePASSPORTS THAT FAIL TO READ

Presented by the New Technologies Working Group (NTWG)

(7 pages)

1. INTRODUCTION

1.1 An increasing number of countries are now producing ePassports and consequently border control authorities (and others) are increasingly being presented with such documents. ePassports constitute a significantly different document from previous passports as they contain a Contactless Integrated Circuit *commonly known as a contactless chip*. For the purpose of this guidance the terms 'contactless chip' or 'chip' should be taken as meaning contactless IC as per 6th Edition Document 9303 – Part 1 volume 2. The chip contains the biographical details and image of the holder as shown on the bio data page. Whilst the inclusion of a chip offers considerable benefits to the overall integrity of the document, it will inevitably introduce circumstances where the chip does not appear to be functioning properly.

1.2 Having developed an ePassport to make the document more secure and to enhance overall travel security through the use of biometrics, it would be perverse to penalise the genuine traveller as a result of a faulty/damaged chip about which they may have no knowledge. However care needs to be taken to balance this against the potential for fraudsters to disable the chip to prevent validation of the data taking place. Consequently it is important that some guidance is available to those that routinely inspect ePassports to assist them in determining whether difficulties in opening/reading/validating chips are potentially due to a fraud attempt or something much less sinister. It is also important that where documents cannot be read (e.g. due to damage) that they are withdrawn from circulation by the issuing authority.

1.3 At ICAO TAG 17 in March 2007, a paper was presented by the New Technologies Working Group on 'Processing Travellers presenting ePassports That Fail To Read' (TAG-MRTD/17-WP4). The TAG approved the need to develop guidelines for border inspection authorities and others, suggesting action that should be taken, and giving reasons why the chip in a passport might be unable to read. It was also agreed that these guidelines should also address staff training issues.

1.4 The following guidance is intended primarily for the use of border inspection authorities. Consequently it aims to provide a fairly non technical approach to the ePassport, how it works and what problems a border inspector may encounter with such documents. It also sets out some of the reasons why problems may occur and also gives some practical guidance on what action to take.

2. BACKGROUND

2.1 It has long been recognised that travel documents cannot provide a 100% guarantee that the holder of an identity document (MachineReadable Passport) assigned to that person by the Issuing State, is guaranteed to be the person purporting at a Receiving State to be the same person to whom that document was issued. Documents can be tampered with to change biographical data, the image can be substituted or a complete counterfeit document can be produced. The only method of relating the person irrevocably to their travel document is to have a physiological characteristic, i.e. a biometric, of that person associated with their travel document in a tamper-proof manner. After a five year investigation into the operational needs for a biometric identifier, which combined suitability for use in the MRP issuance procedure and in the various processes in cross-border travel, consistent with the privacy laws of various States, ICAO specified that facial recognition is the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

2.2 The introduction of ePassports provides a significant enhancement to the security of travel documents. The document holder's biographical and biometric data can be confirmed as being original to the document through the use of Public Key Infrastructure (PKI), which provides the means for machine assisted validation of this data. ePassports are, as a result, difficult to alter or counterfeit without detection **providing** Border control authorities carry out a proper document validation process in the course of the examination of the traveller.

2.3 The ICAO specifications require that digitally stored images are used, and these are "on-board" i.e. electronically stored in the travel document. A high capacity contactless Integrated Circuit chip is the electronic storage medium specified by ICAO as the capacity expansion technology for use with ePassports in the deployment of biometrics.

2.4 All ePassports that meet the minimum requirements set out in ICAO Document 9303 (Part 1 – volume 2) should carry the following symbol on the front cover of the passport, either near the top or bottom of the cover. The logo may also appear on the data page or on other pages of the passport and indicates that the passport contains a chip.

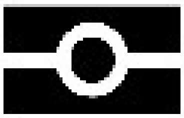


Figure 1 – ePassport Logo

2.5 Both issuing and any receiving States need to be satisfied that the data stored on the chip has not been altered since it was recorded at the time of issue of the document. Names and other personal details of the passport holder that are stored on the chip reflect the information that is presented in the MRZ on the data page. In addition, the privacy laws or practice of the issuing country may require that the data cannot be accessed except by an authorised person or organization. Accordingly ICAO has developed specifications regarding the application and usage of modern encryption techniques, particularly interoperable Public Key Infrastructure (PKI) schemes, to be used by States with their Machine Readable Travel Documents (MRTDs). The intent is primarily to augment international document security through machine assisted means of authentication of MRTDs and their legitimate holders.

2.6 It is not intended to go into detail on how PKI works in this guidance. It is sufficient to say that PKI provides a means by which border inspectors can authenticate through machine assisted means that the data that was placed on the chip when the passport was issued by the issuing authority has not been changed. The combination of the assurance given by PKI and the visual check of the document's physical security features will provide added security value.

However to do this, the inspection process needs to include not only a visual inspection of the data page, reading and opening the chip in the passport but also validating that information. This should be a normal part of the automated inspection process carried out by passport readers equipped to deal with ePassports.

2.7 It is critically important for both border inspectors and the holder of an ePassport that the technology works. The potential for a chip or its associated antenna (which is used in the chip/reader communication process) to be damaged during production of the passport is a concern. Issuing authorities are aware of the importance of the need for the contactless chip to be protected not just against physical tampering but also casual damage including flexing and bending. Extensive durability testing has taken place in the course of the development of ePassports to ensure that they are 'fit for purpose'. These checks included impact testing, bending and twisting the book, putting through a washing machine, and deep freezing, 2.8 Great care is taken with ePassports to avoid damage to the chip or the antenna in the production process. Checks are carried out at the end of the process to ensure that the chip is operating effectively. Additionally a number of countries provide facilities for holders of ePassports to check them after they have been issued. It is also common in some countries for the chip to be checked at the point of delivery to the document holder

2.9 Most countries advise recipients of ePassports that it is important that the document is treated properly. In some cases, there is a printed endorsement on the page that carries the chip requesting border authorities not to use it for entry/exit stamps. Although this may suggest that there is concern over the durability of the chip/antenna, this is not the case. It is simply there to alert the holder and border inspectors to the need to treat the document with appropriate care.

2.10 Given that the introduction of chips in passports is a new use of this technology, some concerns have been voiced as to how robust they are given that unlike chips used in credit cards etc, those used in passports need to be able to continue working over a much longer period (i.e. the maximum normal validity period for a travel document). Indications are that the level of faulty chips is extremely low and that detection of faults is happening prior to the book being sent out of the production facility. A number of issuing authorities have obtained warranties from malfunction from their chip manufacturer for the life of the passport (up to 10 years in some cases). <u>As a result, it is very unlikely that a newly issued ePassport will contain a defective chip</u>.

2.11 However it is not just the passport issuers and producers that need to be aware of the need to take care with the production of ePassports. It is also essential that those inspecting ePassports at the border are properly trained in the operation of passport readers to avoid operator error and a possible misconception that the chip is malfunctioning.

2.12 Apart from the inherent physical protection of the chip in the book, protection of the stored data from alteration and unauthorised access is achieved through two methods method specified by ICAO; Passive Authentication and Basic Access Control (BAC). Where the face is the only biometric stored on the document Issuing States primarily use the BAC mechanism in order to prevent unauthorised access to the chip data. This means that access to the chip data is not possible without the inspection system (i.e. the reader) ‘proving’ that it is authorised to access the chip. This is achieved from information taken by the reader from the passport MRZ. Where BAC is being used, information from the MRZ is critical to the successful reading of the chip. If the MRZ is damaged or of poor quality, the reader may be unable to access the chip. (This might be the case for example where the document has been folded or has been put through a washing machine impacting on the readability of the MRZ). However, the MRZ data can be entered manually by the border inspector in such cases and this should normally result in the chip contents being displayed for comparison with the document bio data page. Border Inspectors should be alert to the possibility that failure to open the chip could mean that the second line of the MRZ has been fraudulently altered. Extended Access Control (EAC) has been developed to provide additional protection to data in the chip (particularly in relation to fingerprint data) however the EAC protocols still require BAC to be successfully achieved before switching to the advanced access protocol.

2.13 An ePassport may be read at various points in a journey: on arrival at border control, exiting a country or in transit. At any one of those points the chip may fail to read. It is therefore important that guidance exists setting out suggested reasons for such failure, tell tale signs of attempted tampering and suggested guidance on the action to be taken. This should help achieve a degree of consistency in the treatment of such cases and ensure that genuine travellers holding ePassports are not unduly delayed should the chip malfunction (or appear to do so). Nevertheless, it is acknowledged that where the chip has failed to read, it would be expected that the document and its holder would be subject to greater scrutiny by border control officials.

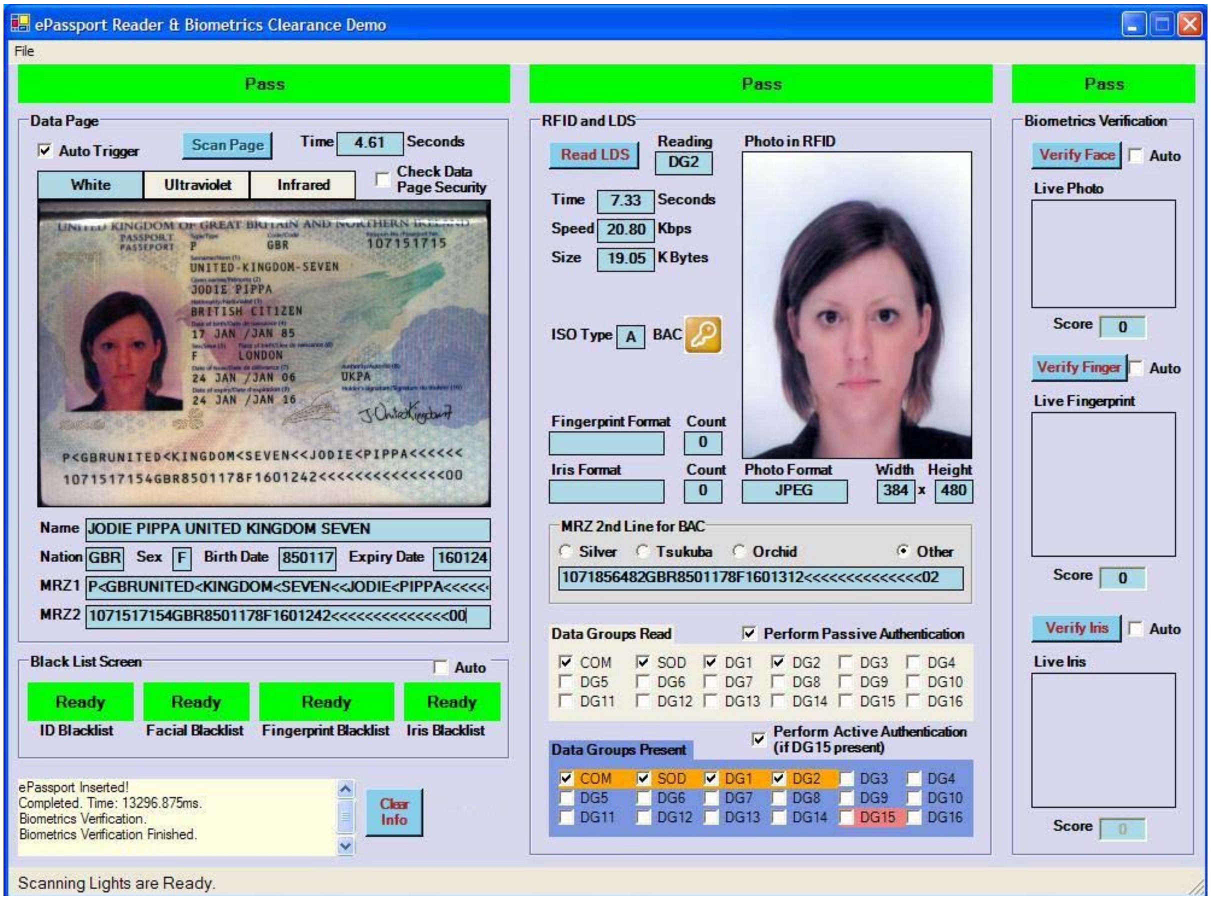
2.14 Finally, it is recommended that as States commence the issuance of ePassports, they ensure that specimens are provided to other states so that they may be tested against a range of passport readers. In this way, it should be possible to quickly identify any particular problems with documents/readers. It is also important that where chips are found to have a problem in the border inspection process, that this is raised by border control authorities with the relevant passport issuing authority in order to highlight the problem and so that remedial action can be taken if necessary.

3. INTERPRETING READER RESULTS

3.1 ePassports present significant obstacles to the fraudster if they are read and validated fully against the Public Key Directory or similar facility using the Passive Authentication mechanism as defined by ICAO. As the document contains a chip in which the data has been digitally signed by the issuing authority, any change to that data will be highlighted through the reading **and** validation process at border inspection. Consequently there may be attempts to disable the chip so that the inspection system is unable to read/validate the information contained in it or alter the second line of the MRZ so that the data on the chip cannot be accessed. In such circumstances a change to the bio data information in the book might go unnoticed as it would not be confirmed as genuine through reading/validation of the chip. Consequently, the physical security features contained in the book remain an essential and very important feature of the inspection process carried out at border control.

3.2 It is important that those who are required to examine passengers holding e-Passports fully understand the technology of the inspection systems that are deployed by their governments at ports of entry. Border control authorities are likely to replace existing passport readers for new inspection systems designed specifically for ePassports. It is important that staff receive training in the use of those systems which may require a different approach to reading the passport, for example by moving from a 'swipe' to a 'flatbed/full page' reader. Border Inspectors used to 'swiping' passports may initially be unfamiliar with 'flatbed' readers and this can lead to difficulties reading e-Passports and possibly lead to the reader being unable to detect the chip. Border Inspection authorities should ensure that staff are sufficiently trained to ensure that where an ePassport fails to read, it is unlikely to be due to 'operator error'. Errors can also occur where the chip takes longer to open than might be allowed by the border inspector or where the book has not been placed properly on the reader.

3.3 On reading a chip enabled document, the reader should normally display the image from the chip next to the scanned image from the bio data page. These images should be similar. If the image is missing, a second attempt should be made to re-scan the bio data page preferably on a different reader to eliminate a problem caused by a malfunctioning reader. See Figure 2.



☑ Auto Trigger

Time 4.61 Seconds

□ Check Data Page Security

Name JODIE PIPPA UNITED KINGDOM SEVEN

Nation GBR Sex F Birth Date 850117 Expiry Date 160124

MRZ1 P<GBRUNITED<KINGDOM<SEVEN<<JODIE<PIPPA<<<<<

MRZ2 1071517154GBR8501178F1601242<<<<<<<<<<<<<<00

□ Auto

Ready ID Blacklist · Ready Facial Blacklist · Ready Fingerprint Blacklist · Ready Iris Blacklist

```
ePassport Inserted!
Completed. Time: 13296.875ms.
Biometrics Verification.
Biometrics Verification Finished.
```

Reading DG2

Time 7.33 Seconds

Speed 20.80 Kbps

Size 19.05 K Bytes

ISO Type A BAC

Fingerprint Format Count 0

Iris Format Count 0

Photo Format JPEG Width 384 x Height 480

MRZ 2nd Line for BAC

○ Silver ○ Tsukuba ○ Orchid ● Other

1071856482GBR8501178F1601312<<<<<<<<<<<<<<02

Data Groups Read ☑ Perform Passive Authentication

☑ COM ☑ SOD ☑ DG1 ☑ DG2 □ DG3 □ DG4
□ DG5 □ DG6 □ DG7 □ DG8 □ DG9 □ DG10
□ DG11 □ DG12 □ DG13 □ DG14 □ DG15 □ DG16

☑ Perform Active Authentication (if DG15 present)

Data Groups Present

☑ COM ☑ SOD ☑ DG1 ☑ DG2 □ DG3 □ DG4
□ DG5 □ DG6 □ DG7 □ DG8 □ DG9 □ DG10
□ DG11 □ DG12 □ DG13 □ DG14 □ DG15 □ DG16

□ Auto Score 0

□ Auto Score 0

□ Auto Score 0

Scanning Lights are Ready.

Figure 2 – ePassport reader

3.4 There will be cases encountered where the ePassport reader detects that a chip is present but cannot display the chip image.

3.5 There are a number of reasons why the chip data may not be displayed. Some of the reasons may be quite innocent – for example an error in the issuing process, or a problem with the inspection reader software. However as mentioned in the introduction to this guidance, issuing states take great care to ensure that when the passport book leaves the production facility that the chip is in working order. Over a period of time of course the chance of some damage occurring to the chip may increase. Where there is a problem reading/validating the chip data, border inspectors should examine the document and the passenger presenting it carefully. A table is attached at Annexe A setting out a number of reasons that may lead to difficulties reading the chip. Recommended actions are also provided for each scenario. This table has been designed specifically to provide a simple and non-technical explanation of possible reasons for difficulties encountered reading an ePassport. Consequently it is a high level view of the common reasons for problems reading the chip and may not be comprehensive.

3.6 Where a problem has been identified with the chip, it will be up to national authorities to determine the appropriate action to be taken. This will depend on whether the problem is encountered either on departure from or entry to the issuing state or a foreign state. In some situations it may be appropriate to withdraw the document at the point of entry, especially if the holder is returning home from an overseas journey and does not require another document immediately.

3.7 However at the very least if the holder of the document has been allowed to enter or depart, it is recommended that he/she be advised to contact the passport issuing authority about the problem before their next overseas journey.

4. DETECTING ATTACK ON CHIPS

4.1 ICAO does not specify the location of the contactless chip in ePassports. Consequently they can be found contained in end covers, in the middle of the book, or within the data page. In most cases the chip and its antenna are not visible as they are ‘sandwiched’ between substrates. Nevertheless as mentioned earlier, many states indicate where the chip is located by a printed endorsement on the relevant area of the book.

4.2 In order to disable the chip, a range of attacks may be used. All of these are designed to prevent the inspection system from communicating successfully with the chip. It is inappropriate to provide examples of attacks on ePassports in this guidance. However it is recommended that border inspection authorities provide guidance to staff on a controlled basis that illustrates the type of attacks that might be made against the chip. It is recognised that given the relative newness of ePassports, there are very limited examples of documents where the chip has been attacked. Nevertheless examples of guidance do exist and may be used as a basis for individual countries to develop their own. Further help may also be available from other sources where contactless chips are used.

4.3 Whilst the failure of the inspection system to read the chip **may** indicate that there has been an attack on the chip or the antenna, border inspection authorities should not make a decision on the traveller’s eligibility for entry based solely on this factor. The inclusion of the chip in ePassports is an additional security feature of these new documents and failure in this one area by itself should not be a reason to refuse entry. It is acknowledged that it may lead to the traveller and the document being subject of a more rigorous examination. However a sensible balance needs to be struck based on the border inspector’s overall consideration of the document and holder’s reasons for travel.

5. CONCLUSION

5.1 The introduction of ePassports is a major step forward in providing a much higher degree of assurance on the genuineness of travel documents to border control authorities. Whilst it is still a relatively new use of this type of technology for travel documents, it is already clear that a number of governments have seen the opportunities that exist to harness the technology in ways that can assist the processing of travellers through border controls.

5.2 The contribution that inclusion of chips in documents can make to the security involved in border control is augmented by the contribution it can make to easier passenger processing. Consequently there are a number of benefits to be gained from the ePassport. It is important that ePassports are seen as a positive and helpful step forward in document security and passenger processing by Border Inspection authorities. This will be aided by those who handle ePassports on a daily basis at the border having an appropriate level of understanding about the documents and their technology. It is hoped that this guidance will go some way to providing that level of understanding.

— — — — — — — —

APPENDIX

Issue	Possible Reason	Recommended Action
No response	Reader communication fault Antenna damaged Chip damaged	➢ Inspect passport carefully, especially MRZ and physical security features ➢ Care: could be fraudulently altered MRZ preventing chip read ➢ Check reader/try different reader, ➢ If everything else appears valid allow entry subject to normal immigration examination ➢ Advise holder to contact issuer on return to home country
No chip data found	Error by issuer Passport placed in Microwave to remove data (this might be verified under examination) Passport issued as an emergency document	➢ Inspect passport carefully using physical security features ➢ If everything else appears valid allow entry subject to normal immigration examination ➢ Advise holder to contact issuer on return to home country
Chip data verifies but does not validate	**Care**: could be fraudulent passport	➢ Inspect passport carefully using physical security features and compare data on data page with chip data, ➢ Check with issuer that passport record exists and that passport data is correct. ➢ If correct allow entry, if not, conduct further investigation and potentially refuse entry.

Holder’s image does not match printed image, yet all other details appear correct	**Care**: could be substituted chip or any of the following: – Photo sub on booklet – Wrong photo stored – Digital photo in chip changed/substituted	➢ Inspect passport carefully using physical security features and compare data on data page with chip data, ➢ In secondary check with issuer that passport record exists and that passport data is correct. ➢ If correct allow entry, subject to normal immigration examination ➢ Advise holder to contact issuer on return to home country ➢ If not, conduct further investigation and potentially refuse entry.
Digital Signatures do not compute correctly	**Care:** could be a forgery Incorrect Document Signer Certificate attached to passport record	➢ Inspect passport carefully using physical security features and compare data on the data page with chip data, ➢ In secondary check with issuer that passport record exists and that passport data is correct ➢ If correct allow entry, subject to normal immigration examination and advise holder to contact issuer on return to home country ➢ If not, conduct further investigation and potentially refuse entry .

— END —