International Civil Aviation Organization

TAG/MRTD/22-WP/12
16/04/14
English Only

WORKING PAPER

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

TWENTY-SECOND MEETING

Montréal, 21 to 23 May 2014

Agenda Item 2: Activities of the NTWG

PROPOSED TEXT FOR CHAPTERS 4 AND 6 OF PART OF RESTRUCTURED ICAO DOC 9303

(Presented by the New Technologies Working Group (NTWG))

1. INTRODUCTION

1.1 At the nineteenth meeting in December 2009, the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) was invited to support a project to "clean-up" and consider restructuring Doc 9303.

1.2 At the following meeting in September 2011 (TAG/MRTD/20), the International Organization for Standardization (ISO) invited the TAG/MRTD to approve expanding on these efforts and confirm its support for a restructuring of ICAO Doc 9303, continuing the clean-up of the supplement, and incorporating endorsed Technical Reports into the new edition of Doc 9303.

1.3 ISO/IEC JTC1 SC17/WG3/TF2 (ISO TF2) is currently leading this exercise on behalf of the International Civil Aviation Organization (ICAO), but has been regularly consulting the New Technologies Working Group (NTWG) throughout the course of the project.

2. BACKGROUND

2.1 In the course of restructuring Doc 9303, ISO TF2 recommended that the NTWG work to update the guidance material on Secure Production (Chapter 4) and Lost, Stolen and Revoked Travel Documents (Chapter 6) that will both be included in the new Part 2 of Doc 9303, which focuses on *Specifications for the security of the design, manufacture and issuance of Machine Readable Travel Documents*.

3. CURRENT STATUS

3.1 As the scope and depth of guidance on these subjects were quite limited, other resources and materials were used to expand these Chapters. Accordingly, the NTWG is recommending that the text included in Annex A (Chapter 4: Secure Production) and Annex B (Chapter 6: Guidance on Lost, Stolen and Revoked Travel Documents) replace the current text in Doc 9303:

> **Existing Text:** The State issuing the MRTD shall ensure that the premises in which the MRTD is printed, bound, personalized and issued are appropriately secure and that staff employed therein have an appropriate security clearance. Appropriate security shall also be provided for MRTDs in transit between facilities and from the facility to the MRTD's holder. Appendix C provides recommendations as to how these requirements can be met.
>
> **Proposed Text:** Annex A.
>
> **Existing Text:** States should provide specific information on lost or stolen MRTDs, such as the MRTD document number, to the central database operated by INTERPOL at the appropriate time and according to agreed procedures. This includes details of any unpersonalized MRTDs which may be stolen from a production or issuance facility or in transit.
>
> **Proposed Text:** Annex B.

4. ACTION BY THE TAG/MRTD

4.1 The TAG/MRTD is invited to:

a) endorse the texts in Annex A and B; and

b) agree to their inclusion in Chapters 4 and 6 of Part 2 in the reformatted Doc 9303.

— END —

Annex A: Guidance on secure production

The following factors should be considered in the establishment of production and issuance facilities:

1) Resilience
2) Physical security and access control
3) Production materials and MRTD accounting
4) Transport
5) Personnel
6) Cyber security
7) Application fraud

Resilience

States should take adequate steps to ensure that MRTD production can be maintained in the event of disaster situations such as flood, fire and equipment failure. Some considerations are:

- Use of distributed production and issuing facilities;
- Secondary production sites when production is centralised;
- Emergency issuing facilities;
- Rapid access to spare parts and support;
- Second sourcing of all MRTD components.

States are recommended to consider possible failure modes in the design of production and issuance facilities, with the objective of eliminating common failures and single-points of failure.

Physical security and access control

States should control access to production and issuance facilities. Control should be zoned and the requirements for access to each zone should be commensurate with value of the assets being protected.

Some examples of good practice for production facilities are:

- Wire cages or solid walls to segregate production areas;
- Strong rooms for storage of finished, un-personalised MRTDs and key security components for MRTD production;
- Token-based access control between zones;
- Video surveillance inside and outside the facility;
- Perimeter security;
- Full time security personnel.

States should also consider the security that is in place at organisations providing MRTD components to the production facility because theft or sale of such components could make it easier to forge an MRTD.

Issuance facilities should separate back-office areas from public areas, with access control between the two. Staff should be afforded adequate protection, as determined by local circumstance.

Production material accounting

States should ensure that all material used in the production of MRTDs is accounted for and that MRTD production is reconciled with MRTD orders, so that it may be demonstrated that no MRTDs and no MRTD components are missing.

Defective materials, MRTDs, and MRTD components should be securely destroyed and accounted for.

Generally, reducing the number of issuance and production sites will make material accounting easier. However, this must be balanced against the need to provide resilience and acceptable customer service.

Transport

States are advised to use secure methods to transport MRTDs and MRTD components; cash-in-transit methods are normally adequate unless particularly high value assets are being transported (e.g. holographic masters).

States should seek to minimise the amount of material transported in any one batch to reduce the effect of theft. In particular states should not transport complete sets of printing plates in one operation.

Personnel

States should ensure that all personnel are subject to a security clearance process, which confirms their identity and suitability for employment in an environment where high-value assets are produced. Staff should be provided with credentials to enable them to identify themselves and to gain access to secure areas which they need to access in connection with their role.

Cyber security

Production and issuance facilities are vulnerable to a variety of cyber attacks:

1) Viruses and other malware, both in conventional computing facilities and in production machinery;
2) Denial of Service attacks through online MRTD application channels and web services exposed by production and issuance systems;
3) Compromise of issuing systems to enable attackers to issue passports or steal personal data or cryptographic assets (such as private keys for eMRTD production).

Countermeasures for these and related attacks are beyond the scope of this document. States should seek advice from their national technical authority.

Annex B: Guidance on Lost, Stolen and Revoked Travel Documents

The exchange of information on lost, stolen or revoked travel documents is a key strategy to strengthen border control and mitigate the impacts of identity theft and immigration fraud. Accordingly, States should consider implementing the following operational procedures to offset the threats that work to undermine border management and national public safety:

1. Communicating proactively with document holders
2. Maintaining National Lost, Stolen and Revoked Travel Document Databases
3. Sharing information about lost, stolen and revoked travel documents with INTERPOL and verifying documents against INTERPOL databases systematically at primary inspection.
4. Installing checks to determine whether a holder is presenting a lost, stolen or revoked document at border crossing

6.1 Communicating proactively with document holders

States should ensure that holders of travel documents are fully aware of their responsibilities regarding the use, safe-keeping and reporting procedures for lost or stolen travel documents. Guidelines for safe-keeping travel documents both at home and while travelling may assist in preventing the loss or theft of travel documents. At the time holders receive their documents, holders should be informed of the appropriate actions (including timely reporting) and channels for reporting lost or stolen documents. To assist in this process, States may consider providing travel document holders with multiple channels for securely reporting lost and stolen documents, including in person, telephone, physical mail and various ways of electronic communication including internet.

States must also take appropriate measures to ensure that holders of travel documents are educated about the potential disruptions, inconveniences and added expenses that can arise when lost, stolen or revoked documents are presented at border control for the purposes of travel. This advice should highlight that once a travel document has been reported lost/stolen it is cancelled and can no longer be used and may be seized by authorities if an attempt is made to use it.

National legislation, or any suitable framework, should be in place, to oblige holders of travel documents to report a lost or stolen travel document immediately. No new travel document should be issued, until this report has been filed.

6.2 Maintaining National Lost, Stolen and Revoked Databases

States that use national travel document databases to assist in the verification of the status of their nationally-issued travel documents should take measures to ensure that information is kept up-to-date. Reports about lost and stolen documents provided by the holders should be recorded into these systems in a timely fashion to ensure that risk assessments conducted using these systems are accurate. States may also wish to consider recording information about lost, stolen or revoked travel documents intercepts in these databases. In addition to updating these databases, States should ensure that border control and police authorities are able to easily access them.

6.3 Sharing information about lost, stolen and revoked travel documents with INTERPOL and verifying documents against INTERPOL databases systematically at primary inspection.

States should participate in the global interchange of timely and accurate information concerning the status of travel documents to support in-country policing and border management, as well as efforts to

mitigate the impacts of identity theft. Sharing information about lost, stolen and revoked travel documents serves to:

a. Improve the integrity of border management;
b. Assist in detecting identity theft or immigration fraud at the border, or in other situations where the document is presented as a form of identification;
c. Improve the chances of identifying terrorist operatives travelling on false documents;
d. Improve the chances of identifying criminal activity, including people smuggling;
e. Aid in the recovery of national documents; and
f. Limit the value and use of lost, stolen or revoked documents for illegal purposes.

INTERPOL's Automated Search Facility (ASF)/Stolen and Lost Travel Document Database (SLTD) provides States with a means to effectively and efficiently share information about lost, stolen and revoked travel documents in a timely fashion. States should share information about lost and stolen documents that have been issued, as well as blank documents that have been stolen from a production or issuance facility or in transit. Annex One outlines the factors that must be considered prior to participating in the ASF/SLTD.

States should verify documents against INTERPOL databases systematically at primary inspection to ensure that only travellers holding valid travel documents are crossing border control checkpoints. Verifying the status of travel documents against these databases offers many of the same benefits afforded by sharing information about lost, stolen and revoked documents.

6.4 Installing checks to determine whether a holder is presenting a lost, stolen or revoked document at border crossing

States must work within existing national laws and respect international agreements relating to the use of travel documents and border control when processing travellers at their borders. All travellers with reported travel documents (lost, stolen, revoked) shall be treated as if no illegal intention existed, until otherwise proven.

6.4.1 When a travel document gets a "hit" on INTERPOL's Lost, Stolen or Revoked Database.

A traveller should not be refused entry or prevented exit solely based on the document appearing on the lost, stolen or revoked travel document database. There are many steps that States must take to support these actions. If a traveller is in possession of a travel document that has been recorded as lost, stolen, or revoked on the ASF/SLTD, States should, where possible, liaise with the issuing and reporting country to confirm that the document has been rightfully recorded as a lost, stolen or revoked travel document. States should also conduct an interview with the traveller to ascertain his/her true identity or nationality, and determine if they are the rightful bearer of the travel document.

If the document contains a chip, States should conduct biometric verifications to support their efforts to determine the true identity of the traveller. States should also make efforts to determine whether the data has been altered and whether the document is authentic.

6.4.2 Processing the rightful owner of the travel document through border control

In dealing with the rightful owners of travel documents, States should be cognizant that those identified as the rightful bearers of a travel document declared lost, stolen or revoked are not necessarily attempting to commit a criminal offense. Rather than focusing on penalizing these individuals, States should focus on identifying ways of removing these documents from circulation, while minimizing disruption to travel.

Where permitted under national law, States may consider alternate methods of dealing with these travellers that differ from ways of dealing with those that are intentionally attempting to illegally enter the country by committing identity fraud.

Travellers entering a foreign country on a document declared lost, stolen or revoked as a result of a data error	Border control in the receiving State should contact the issuing authority to confirm the data error. Once confirmed, States may process the document as a valid travel document, but should advise the traveller to contact the issuing authority upon return to their country. Travel document issuing authorities in the issuing State should take all the necessary steps to have this document removed from the lost, stolen and revoked database. States should also consider replacing the affected document at no cost to the client.
Nationals attempting to leave their country on a document declared lost or stolen	Where exit controls exist, border control should advise these travellers that their documents are not valid for travel, and that they must to obtain a valid travel document before embarking on their journey, as lost, stolen and revoked travel documents are considered to be invalid.
Nationals attempting to leave their country on a revoked document	Where exit controls exist, border control should consult with national law enforcement to determine what measures/laws may be invoked to prevent the traveller from leaving the country. If permitted, border management/police authorities should prevent travellers from leaving the State.
Nationals attempting to leave a country and return to their country on a document declared lost, stolen or revoked	Where exit controls are in place and the identity and nationality of the holder has been confirmed, border control may allow the traveller to proceed, but should advise them that the document presented is not valid and that they may be refused boarding by the carrier. When re-entering their country of origin on a document declared lost, stolen or revoked, border control may, where permitted by national law and/or international agreement, seize or impound the document to return it to the issuer. If their documents have been seized or impounded, travellers should be advised to obtain new valid travel document.
Nationals attempting to leave a foreign country and continue to a third country on a document declared lost, stolen or revoked	Where exit controls are in place, border control should advise the traveller that their travel documents are invalid, that they may be refused boarding by the carrier, and that they may face difficulties upon arrival in their next destination.
Travellers entering a foreign country on a	Travellers that have been permitted to board should be

document declared lost, stolen or revoked	advised by the receiving State to contact their consulate or embassy to obtain a valid travel document before attempting to continue on their journey. Travellers that have not been permitted to enter may be dealt with according to national law.

6.4.3 Processing a traveller after determining that they are not the rightful owner of a document declared lost, stolen or revoked

Once it is determined that a traveller is not the rightful bearer of a document, border/police authorities from the sending or receiving State should seek to determine how the traveller came into possession of the document, including whether there was collusion with the rightful owner, and should domestic law permit, working in cooperation with the issuing State, determine whether additional fraudulent documents have been issued in that identity. If it is determined that the traveller has presented a lost, stolen or revoked travel document, States should investigate the traveller, and where applicable apply criminal charges and/or removal from their State.

States should confiscate documents for the purposes of legal proceedings, including immigration and refugee processing, but should return these to the issuing State once they have served this purpose. Efforts should also be made to provide the issuer with as much information about the interception as possible, should domestic law permit.

States should also ensure that inadmissible persons are documented in accordance with the provisions of ICAO Annex 9 (Facilitation) to the Convention on International Civil Aviation.

Annex One

Table: ASF/SLTD Key Considerations	
Legislative requirements	Before States can begin uploading information to the INTERPOL ASF/SLTD, they must explore their legislation to determine whether they have the authority/mandate to provide international access to elements of citizen's travel document information. Should amendments to legislation be required, States should ensure that adequate coverage is provided for the: 1. Collection and storage of data; 2. Privacy provisions (including security); 3. Authorization for disseminating data to the international community; and 4. Data lifecycle and non-repudiation.
Data elements	A standard data set focusing on the document details rather than the holder of the document has been developed for the interchange of information pertaining to lost, stolen and revoked travel documents. States must meet the following required data fields when uploading to this database: 1. Document Number* 2. Issue Date 3. Type of Document 4. Nationality of Document *Where the travel document has been personalized this should be the number contained in the MRZ; if dealing with a blank book, this number should be the serial number, if the numbers are not the same.
Information gathering	States should ensure that tools used to collect information about lost and stolen travel documents (i.e. telephone interviews, online forms, etc...) are comprehensive and conducive to securely gathering all the information required to complete the ASF/SLTD report.
Timely and accurate data provision	The strength of INTERPOL's ASF/SLTD rests on timely and accurate information. Accordingly, States should ensure that they have the systems and processes in place to share information in the most timely fashion to intercept lost, stolen or revoked travel documents that may attempt to be used at border control. States should strive to share this information on a daily basis. Generally, once information is received that the travel document is no longer in the possession of the rightful holder or has been revoked, the issuing authority should officially record the information in their national database (if they run and maintain one) and/ in the ASF/SLTD. States should also make ongoing efforts to ensure that data is accurate and reliable. Care must be taken to avoid input errors and to provide all the

	required document data, as accurate reporting is the responsibility of the issuing authority. Errors in reporting can be disruptive to travel and costly to both the traveler and issuing State. States must therefore take the necessary steps to ensure for the accurate recording and reporting of lost, stolen and revoked travel documents. States should operate a 24/7 response facility to promptly action requests for further information from INTERPOL on behalf of inquiring States.
Leveraging National databases on lost, stolen and revoked travel documents	States maintaining national databases on lost, stolen and revoked travel documents should consider using automated ways to transmit this information to INTERPOL to leverage their efforts.