INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)
TAG/TRIP NEW TECHNOLOGIES WORKING GROUP

REQUEST FOR INFORMATION

INSTRUCTIONS FOR PREPARATION OF SUMMARY PAPER

1. OVERVIEW

Interested parties must present their technologies in the context of ICAO Document 9303, which prescribes international format and on-board data standards for machine-readable passports, visas, and other official machine-readable travel documents.

The requested summary paper must be submitted with all responses to the Request for Information (RFI). A separate summary paper should be submitted with each technology concept introduced. Summary papers will be included in a comprehensive Summary Report and will be presented to the ICAO Member States. The Summary Report will be divided into the following categories:

- Mobile / Virtual ID
- Image Manipulation Detection Systems
- Liveness Factor / Detection
- Smartphone and online application processes (ex. Security Tolls and photos)
- Creative ways to send certificates to the PKD
- Photo Quality Assessment Systems
- Physical Security Features
- Machine Readable Security Features / Machine Authentication
- Leveraging ePassports
- Storage media and contactless chips
- LDS2 and Mobile Technology
- Multimodal Biometrics (3rd Biometric) and Multi-Biometrics capture
- Facial Recognition Algorithms
- Remote verification of ePassports using devices and remote connections to PKD
- Biographic Search

2. PURPOSE

The summary paper is an information tool that may be used by the ICAO New Technologies Working Group (NTWG) when considering standards for new technologies, with possible application to machine-readable travel documents. The summary papers will also be used to familiarize ICAO Member States with the new technologies.

The summary paper should describe the technology being introduced in an accurate, succinct and complete manner. The summary paper will reflect how interested parties would like their technology presented to the NTWG and the ICAO Member States. It should highlight - in summary form - **all** information that interested parties want to convey to ICAO.

3. CATEGORIES AND REQUIREMENTS

CATEGORY 1: Mobile / Virtual ID

Requirements: *Mobile and virtual identity credentials are emerging new technologies with several iterations already available in the market. Examples are smartphone-based driver licenses and access control systems. These new technologies may also be adapted to traveler identification systems.*

Travel document technologies are centered on secure physical credentials. Passport booklets are ubiquitous however, options such as passport smart cards and biometric-enabled trusted traveler systems are already rolled out.

Smartphone-based and virtual identity systems are emerging in the market. Such systems provide opportunities to enable secure traveler identification without the need for a physical credential. They may also complement advances in automated border control systems to facilitate more effective, efficient and convenient border crossings for travelers.

The NTWG is interested to see examples of systems that enable such a capability. Options might include:

- A fully smartphone-based travel document that has strong security and authentication systems (similar to those in the current ePassport chip)
- Systems to enable the virtualization of traveller identification where the traveller's biometric becomes the sole credential
- Models that require a secondary enrolment beyond the standard passport enrolment are not requested
- The system may include models for virtualization of the LDS currently deployed in ICAO-compliant ePassports and means by which a traveler can deliver these credentials to border systems; or
- A combination of the two above i.e. a virtual passport activated by a smartphone application.

CATEGORY 2: Image Manipulation Detection Systems

Requirements: *Image manipulation detection systems that can be utilized to detect when an image (mainly photograph, but could be image of fingerprint or iris), submitted by travel document applicants has been altered, amended or tampered with in order to prevent attacks such as morphing or beautification.*

The system may detect any trace of manipulation that is difficult to be found with human eyes. Such systems should support travel document issuance authorities where quick and precise implementation of examination is needed. Special attention shall be put on the validation of electronically submitted photographs in on-line application systems.

CATEGORY 3: Liveness Factor / Detection

Requirements: *Passport enrolment processes remain vulnerable to photo manipulation fraud. This vulnerability is exacerbated in systems that allow for the remote provision by passport applicants of their biometric data (i.e. provision of a passport photo via and online or mobile-based application process).*

Several passport issuing authorities are already offering online channels for passport applicants. The number of such systems will expand in the future with more and more countries providing such a facility to their clients. Such systems provide an opportunity for criminals to provide digitally altered biometric data in order to circumvent critical biometric matching systems. Liveness detection systems provide a means to reduce this kind of passport fraud.

The NTWG is interested to see the latest developments in liveness detection systems and how they might be securely integrated in online and mobile passport application systems.

CATEGORY 4: Smartphone and online application processes (ex Security tolls and photos)

Requirements: *Passport issuing authorities are increasingly providing online and mobile systems for passport applications. Such systems pose several new integrity risks for passport issuing agencies.*

Online and mobile passport application systems provide benefits for passport applicants (convenience and better access) and for passport issuing authorities (more efficient back office processes). They do, however present a number of new risks such as service denial blunt force attacks to circumvent fraud control measures.

NTWG is interested to see technologies that may mitigate new risks associated with moving to a predominantly online service channel:

- Strategies to prevent service denial attacks
- Measures to prevent blunt force attacks to overcome fraud controls built into the online system
- Measure that would provide assurances to the passport issuing authority as to the integrity and genuineness of individual online applications.

CATEGORY 5: Creative ways to send certificates to the PKD

Requirements*: Creative ways to send, upload / download ePassport certifying credentials to the Public Key Directory.*

CATEGORY 6: Photo Quality Assessment Systems

Requirements: *Assessment Systems that can be utilized to judge whether a facial photo submitted by travel document applicants is compliant with the photo specifications provided in Doc 9303 and appropriate ISO standard 19794-5.*

Verification/assessment of photos submitted digitally through channels such as online application or kiosk capture against international standards/specifications could increase photo acceptance rates. Doc 9303 and appropriate ISO standards, particularly ISO/IEC 19794-5, define acceptable photos and provide guidance on several aspects such as pose, prohibited items, lighting and color balance.

The NTWG is seeking information on technologies that allow for high true accept rate and low false accept rate for photo quality compliance. System needs to perform quick and automatic assessment, and when it rejects a photo, it should identify the appropriate reasons, so that the applicant may understand why their photo has been rejected.

CATEGORY 7: Physical Security Features

Requirements: *Physical security features that protect travel documents from counterfeiting, photo-substitution, alteration of text of the data page, and replacement of IC inlays.*

Features that can make it easy to recognize visually and/or be authenticated at automatic border control by automated inspection systems are welcome. Innovative features shall be suitable for various inspection levels, while the emphasis is on the first control level. Security features may also include novel technologies to secure a plastic data page into a passport booklet.

CATEGORY 8: Machine Readable Security Features / Machine Authentication

Requirements: *Systems and/or software that can optically and electronically read travel documents and be used for confirmation of their integrity and authenticity at passport application with kiosk systems or automatic border control.*

NTWG requests for the information of the following fields: Design rules and examples

- For documents suited for machine authentication;
- Reader systems;
- Authentication software and
- Reference databases.

CATEGORY 9: Leveraging ePassports

Requirements: *Use of the passport beyond purely as a travel document. Uses such as an identification document, whose validity can be verified through the use of the PKI process.*

CATEGORY 10: Storage Media and Contactless Chips

Requirements: *The NTWG is interested in new technology or improvements in storage media and contactless chips.*

CATEGORY 11: LDS2 and Mobile Technology

Requirements: *The NTWG is interested in applications to store and/or securely operate logical data structure 2 (LDS2) applications using mobile phone technology. The NTWG is seeking information on applications that allow mobile phones (i.e. smartphones) to securely communicate with integrated circuit chip inspection systems, send and receive information*

stored in LDS2 applications to inspection systems, and/or display data stored in LDS2 applications using a phone as a medium. Other areas of interest include employing mobile phones as inspection technology to view LDS2 data (terminal authentication may be necessary) and using near field communication technologies to interact with an LDS2-enabled ePassport.

LDS2 provides optional additional chip space that can be used by sending and receiving States to add other travel information not included in the current LDS (i.e. travel stamps, Visas, and additional biometrics), and is defined by the following international specifications:

- Logical Data Structure, specifying the optional applications, file structures, and data elements (WG3TF5_N0210 TR LDS2 9303 Part 10 V14.0);
- Protocols, specifying the mechanisms for secure and authenticated writing of data to the eMRTDs chip (WG3TF5_N0209 2015_11_02 LDS2-Protocols); and
- PKI, specifying the Public Key Infrastructure that supports the distribution of public key certificates, necessary for data, chip and inspection system authorization (WG3TF5_n0203 LDS2 PKI Draft 6.0 June 2015).

CATEGORY 12: Multimodal Biometrics (3rd biometric – what is available and the status) / Multi-Biometrics capture (i.e. face and iris at the same time)

Requirements: *Latest developments in biometric capture systems, specifically cost effective systems that would allow for the capture of high quality facial and iris biometrics in a single pass. Multi modal biometric controls provide for greater identity security. A barrier to greater uptake is cumbersome and intrusive enrolment processes. This is true for face and iris capture as well.*

Identity security can be greatly enhanced by the capture and use of multiple biometric measurements. Face is the primary biometric specified by ICAO for ePassports.

CATEGORY 13: Facial Recognition Algorithms

Requirements: *Algorithms that can be used to verify facial images at travel document application or border control.*

NTWG seeks new algorithms that can improve the accuracy of the following facial matching systems.

- Comparing an image submitted by applicant with registered images in large image data bases; or
- Comparing a live captured image with registered images in databases;
- Comparing an image read out from an e-passport with the bearer of the document.

For more accurate matching, NTWG is interested in algorithms that account for the following factors:

- Aging;
- different poses, such as tilt;
- hair style, beard or expressions: and /or
- glasses, head covering or any other non-facial artifacts.

Algorithms that work for children's photos are also welcome.

CATEGORY 14: Remote verification of ePassports using devices and remote connections to PKD.

Requirements: *Already NFC enabled smartphones are being used to read data on passport chips. This has potential to enable remote verification of passports. This could be strengthened by enabling such devices to also undertake PKI authentication of passport chips.*

While not all passport RFID chips can be read by NFC-enabled smartphone many can. Such mobile devices are already being trialed in law enforcement and border management scenarios. There are also potential commercial applications for banking and other sectors to enable fully online processes.

The integrity of this practice would be enhanced with ability to enable such devices to also undertake remote PKI authentication of ePassports. NTWG would be interested in seeing possible solutions.

CATEGORY 15: Biographic Search

Requirements: *As a consequence of the introduction of highly secure MRTDs with chips and biometrics, attempts at fraud tend to shift from the document itself to the pre-issuance (registration) stage. It is therefore of increasing importance to ensure that in this registration process the valid identity of individuals is captured in an objective, consistent and rigorous manner.*

In this RFI the NTWG seeks for information on the latest developments in database lookup algorithms that support this need for the pre-issuance stage of MRTDs. These "biographic search" techniques may involve;

- Name-matching. To ensure that the names originating from various sources are matched objectively, such as matching names as appearing in a civil register, birth certificate, marriage/name change certificate and passport application. Name-matching techniques could involve semantic analysis, phonetic analysis, typographical error analysis, international naming conventions, consistent separation of names' components, regional language and ethnic variations, removal of extraneous data from names, among others.
- Address equivalence. This could be a more complex instance of biographic matching where the same location is specified using different description in countries where address nomenclature is loosely defined.
- Any other text fields / descriptors may be evaluation through further study to be considered for coverage.
- Distance. Various metrics are being evolved to measure "distance" between texts, which seems to be the emerging trend inter alia for name-matching.

Lastly, the context of registration could be used for evaluating the need of a "social footprint" of the applicant. While this is an exciting new area and could be deployed using techniques such as block-chain and public ledger, privacy and legal issues may be far from resolved at this point of time.

4. METHOD OF SUBMISSION

The summary paper for each technology should be submitted in electronic form. Electronic copies should be submitted in Microsoft Word or compatible versions. PDF format is acceptable. Interested parties should use Times New Roman or compatible print font (12 point) in order to make all summary papers easy to read and similar in appearance for compilation into the Summary Report. Additional information, e.g. brochures, must also be submitted in electronic form to ensure easy transmission to an international review panel of government representatives.

Each summary paper should be limited to no more than three (3) pages.

Summary papers must follow the format prescribed in the attachment following this instruction, identified as "Summary Paper Format".

5. ORAL PRESENTATIONS

Following the receipt of summary papers and descriptive literature and information, a panel of government representatives from the NTWG will review all submissions. The panel will select those submissions that meet the requirements of the RFI and invite those interested parties to make oral presentations to government members of the NTWG and representatives of ICAO Member States. The oral presentations, each lasting no more than 45 minutes, are planned for 18-21 April 2017 in Amsterdam, the Netherlands.