

ICAO NTWG REQUEST FOR INFORMATION (2007/8) 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 Contracting States. The Summary Report will be divided into the following categories:

- Multi-application data chip environment
- Self-service facilitation
- Data mining technologies
- Travel document security concepts
- E-commerce and e-government
- Biometric database management
- Biometric verification on the move
- Portable enrolment and verification stations
- Transliteration software

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 familiarise ICAO Contracting 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 Contracting States. It should highlight - in summary form - **all** information that interested parties would like to convey to ICAO.

3 CATEGORIES AND REQUIREMENTS

CATEGORY 1: MULTI-APPLICATION DATA CHIP ENVIRONMENT

Requirements: *Effective methodology for creating a secure multi-application environment within the data chip, where the e-passport application co-exists securely with other applications (e.g. e-government applications).*

The ability to store a range of separate data, with each application within the chip environment retaining individual functionality, is sought for consideration. Secure methods of writing and retrieving non-passport data and functionality in an existing passport without compromising the security of the original data is paramount.

Vendors may link information in this category to e-government applications/technology submitted under Category 5 (e-commerce and e-government).

CATEGORY 2: SELF-SERVICE FACILITATION

Requirements: *Technologies and processes suitable for automated self-identification at international borders and/or entitlement facilities that will enable either unattended border crossing or program enrolment.*

Systems and technologies that enable border control agencies to reduce personnel costs for lower risk high volume transactions through the use of automated, secure, unassisted clearance processing at international ports of entry/or departure. These systems may be used for unassisted enrolment in travel document application or issuance processes. Key attributes of these systems are:

- Simplicity of use for applicants and travellers
- Rapid transaction processing
- Secure systems that authenticate the data on the e-passport chip (ICAO mandatory Passive Authentication scheme) and verify the certificate chain
- Secure systems that facilitate the link between the document and holder or application and applicant
- Secure systems that facilitate the link between the holder or applicant to existing database records.

Submissions should detail connectivity with existing infrastructure, explain methods by which enrolment can be accomplished with or without assistance, and explore costs and impact of system deployment in various live environments. Where available, performance data from previous or existing system test should be included for the purpose of detailed evaluation.

Vendors may link information in this category to e-government applications/technology submitted under Category 5 (e-commerce and e-government).

CATEGORY 3: DATA MINING TECHNOLOGIES

Requirements: *Pattern recognition for applicant and staff behaviours to assist in the identification of external and internal fraud.*

NTWG is interested in database technologies that identify patterns of behaviour or commonalities in application or system information. The technology will perform database searches to connect seemingly unrelated information, and identify consistencies that may not be immediately apparent. Ultimately, the technology should assist in the detection of inappropriate or fraudulent activity on the part of processing staff or applicants.

CATEGORY 4: TRAVEL DOCUMENT SECURITY CONCEPTS

Requirements: *Document security features, innovative data page materials, substrates, binding materials and adhesives, advanced anti-copying devices (e.g. holographic / cryptographic features or security inks), and security technologies that allow for globally interoperable machine assisted document authentication and verification.*

Currently passports are constructed almost exclusively from polycarbonate and/or paper. NTWG is looking for alternatives that may have a positive impact on security and durability while retaining the more traditional ability to receive ink-based stamps.

NTWG is also interested in the following areas:

- Document and visa security concepts that may be used to protect on-board data from alteration or simulation, either at the point of document personalisation, document manufacture, or at the point of adhesion (in the case of visas)
- Bonding substances with the ability to mould substrates (passport and visa) together
- Embedded security features that will verify the authenticity of the travel documents when presented by travellers at various points throughout an international journey. These security features should be visible to the naked eye. Ideally, security features will not only verify the authenticity of the actual travel document but also protect bio-data elements such as the holder's portrait, resulting in increased confidence that these key elements have not been altered after the document has been issued
- Advanced anti-copying features such as high resolution diffractive optically variable devices, preferably personalised to the passport holder to prevent re-usage of these optical elements
- Machine assisted document authentication and verification technologies; and globally deployable machine-readable security features (technologies must be interoperable with current reading software).

NOTE: Any associated reading systems/decoding software must be freely and easily available at no cost to enable immigration authorities to utilise the technology. NTWG will only consider technologies that meet this requirement.

CATEGORY 5: E-COMMERCE AND E-GOVERNMENT

Requirement 1: *Electronic on-line systems that may be applied to secure Internet based passport and visa application processes.*

Vendors are invited to propose applications or solutions they have developed which would readily support the implementation of internet based e-commerce or e-government style travel document issuance channels. Issues relating to privacy and the ability to satisfy stringent identity authentication requirements are critical to the successful implementation of on line travel document application and issuance systems. Such solutions would be expected to include the following functionality:

- Secure online customer or citizen application for a variety of travel documents
- Secure receipt of required bio data, most typically but not exclusively photo.
- Secure business-to-business style ability to merge data from a variety of sources online application processing that can link more than one party (i.e. referees and photographers) to assist in validating applications including payment functionality
- Ability to support customer-centric reporting on processing status without agency intervention
- Ability of solution proposed to enable electronic sharing of validated data to facilitate travel movements
- Ability for people to enrol remotely, without the use of specialist equipment.

Vendors may link information in this category to technology submitted under Category 1 (multi-application data chip), and Category 2 (self-service facilitation).

Requirement 2: *Secure communications for multi-lateral data sharing*

Member states wish to share travel document data. Normally this would require an information broker to manage enquiries and responses. NTWG is seeking vendors who can demonstrate this capability. The three key issues to be considered are: timeliness, security and reliability.

CATEGORY 6: BIOMETRIC DATABASE MANAGEMENT

Requirements: *Integrated ID management tool that enables concurrent, multi-factor biometric searching and matching for profiling and alert management.*

Currently the majority of ID management systems and processes rely on a number of additional software tools to perform key identity management functions. Vendors are invited to present on integrated identity management systems or tools that allow for concurrent searching and matching of multiple biometrics.

Performance of algorithms and speed of search engines are key factors – for example, engines that can search 100 million biometric records in seconds rather than minutes.

CATEGORY 7: BIOMETRIC VERIFICATION ON THE MOVE

Requirements: *Biometric matching in a non-intrusive way with a high tolerance for distance and angles.*

NTWG seeks technology with the ability to identify/verify people moving through controlled areas (such as air-bridges) without presenting identification in a traditional manner.

Also, vendors are invited to submit intelligent, layered and fast approaches for staff-assisted biometric border control (using face and/or fingerprint) in conjunction with document authentication.

Technologies that perform well without compromising security or integrity are sought.

CATEGORY 8: PORTABLE ENROLMENT AND VERIFICATION STATIONS

Requirements: *Portable multi-modal enrolment enabling the capture and verification of multiple biometrics (particularly fingerprints).*

Vendors are invited to present highly portable devices/systems (e.g. networked PDA) for use in border control environments that are less traditional (for example, on trains or cruise ships). Ease of transportation and assembly, security, link to PKI schemes such as the PKD, and reliability are all key factors.

Vendors are also invited to present scanner and software developments for the capture of fingerprints at portable border enrolment and verification stations. Information relating to the effectiveness of the technology during live testing should be included.

CATEGORY 9: TRANSLITERATION SOFTWARE

Requirements: *Language software technologies to assist in transliterating non-Latin characters into Latin characters.*

Vendors are invited to present software technologies to aid in the transliteration of non-Latin characters (e.g. Cyrillic or Arabic) into Latin-based characters.

New technology is required to eliminate errors and minimise false matches when transliterating from name-based passenger lists. This technology is intended to both increase security through more accurate passenger identification, and enhance passenger facilitation.

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 PDF format. 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”. Submissions must be written in English.

5 ORAL PRESENTATIONS

Following 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, IATA and representatives of ICAO Contracting States. The oral presentations, each lasting no more than 45 minutes, are planned for the week of 28 April – 2 May 2008 in Montreal, Canada. The language of work is English.

All questions should be directed to:

David Philp, RFI Coordinator
ICAO New Technologies Working Group
c/o New Zealand Passport Office
Department of Internal Affairs
PO Box 10-526
Wellington
New Zealand

Phone: +64 4 382 3512
Fax: +64 4 382 3403
email: david.philp@dia.govt.nz

NEW TECHNOLOGIES WORKING GROUP
2007/8 Request for Information Summary Paper Format
Summary Paper may not exceed three pages
(If submission does not follow this format, submission will not be considered)

1. Name of Company or Entity:
2. Name of Technology
3. Trade Name:
4. Company Address: *(Please include country)*
5. Website Address:
6. Contact Representative
7. Telephone Number: *(Please include international country codes)*
8. Email Address:
9. Description of Technology
(In narrative form, please provide information on the product/technology. Please include performance data ensuring that the environment in which performance results were achieved is defined.)
10. Application of Technology:
(This section will be useful in assisting the reader to understand how you perceive the use of your technology in travel documents and visas, border control systems, or in the facilitation of passengers. Please comment on the technology's potential for global interoperability, and indicate how this technology will improve facilitation and/or security)
11. Current Use of Technology:
(Describe, if applicable, where and how the technology is currently being used.)
12. Relative Pricing Information:
(This information could provide a basis for measuring costs associated with use of the described technology.)

Please note that sections 9 to 12 may be as detailed as you choose; however, the total length of the summary paper may not exceed three pages.