MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

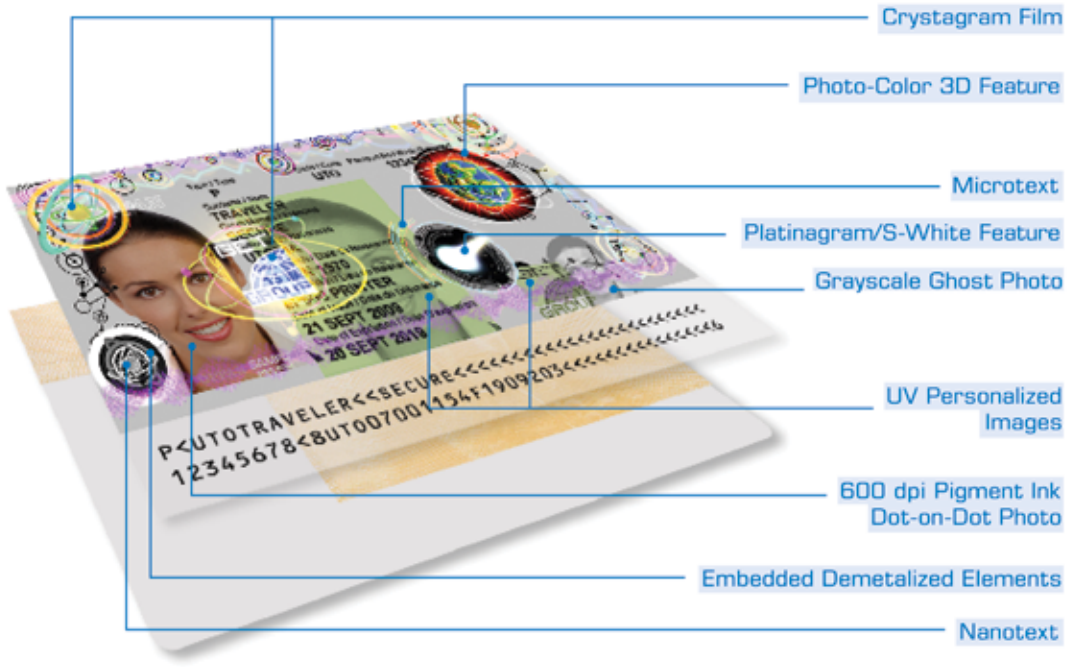
The New Mobility

How ongoing efforts on behalf of the ISO, States and other important stakeholders are helping address the challenges of an evolving facilitation and security framework

In this issue:
New Advances in UK Border Protection • ISO 9001 and the US GPO
Frontline Fraud Detection and Forensic Document Examination
Key Features of an ICAO-compliant Visa • ISO Biometrics Standards
ISO 3-letter Country Codes • Seventh MRTD Symposium Preview

Vol. 6, No. 2

Global Enterprise Technologies Corp.
230 Third Ave., Waltham, MA 02451 USA
T: +1 781 890 6700
F: +1 781 890 6320
www.getgroup.com



GET. Secure

The new eP600 ePassport printer from GET Group produces our most secure passports ever, employing unique EDE Crystagram security film which incorporates extraordinary features to protect the integrity of the data page.

With fully automatic book processing, high speed, and biometric interface, the eP600 continues the Toppan legend of state-of-the-art printers for both centralized and decentralized passport issuance.

GET. Into the future

ICAO MRTD REPORT
VOLUME 6, NUMBER 2, 2011

Editorial
MRTD Programme—Aviation Security
and Facilitation Policy Section
Editor-in-Chief: Mauricio Siciliano
Tel: +1 (514) 954-8219 ext. 7068
E-mail : msiciliano@icao.int

Content Development
Anthony Philbin Communications
Senior Editor: Anthony Philbin
Tel: +01 (514) 886-7746
E-mail: info@philbin.ca
Web Site: www.philbin.ca

Production and Design
Bang Marketing
Stéphanie Kennan
Tel: +01 (514) 849-2264
E-mail: info@bang-marketing.com
Web Site: www.bang-marketing.com

Advertising
Keith Miller, Advertising Representative
Tel: +01 (514) 954 8219, ext. 6293
Fax: +01 (514) 954 6769
E-mail: kmiller@icao.int

Submissions
The *MRTD Report* encourages submissions from interested individuals, organizations and States wishing to share updates, perspectives or analysis related to global civil aviation. For further information on submission deadlines and planned issue topics for future editions of the *MRTD Report*, please contact Mauricio Siciliano, managing editor at: msiciliano@icao.int

The publishers extend their thanks to the companies, organizations and photographers who graciously supplied photographs for this issue.

Published by
International Civil Aviation Organization (ICAO)
999 University Street
Montréal, Québec
Canada H3C 5H7

The objective of the ICAO *MRTD Report* is to provide a comprehensive account of new developments, trends, innovations and applications in the field of MRTDs to the ICAO Member States and the international aeronautical and security communities.

Printed by ICAO

Contents

www.icao.int

Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD)

Member	Nominated by	Member	Nominated by
Mr. R. Tysoe	Australia	Mr. J. Verschuren	Netherlands
Mr. G. K. McDonald	Canada	Ms. A. Offenberger	New Zealand
Ms. M. Cabello	Chile	Ms. I.O. Sosina	Nigeria
Mr. M. Vacek	Czech Republic	Mr. Y. Xuefeng	People's Republic of China
Ms. M. Pujau-Bosq	France	Mr. C. Ferreira Gonçalves	Portugal
Dr. E. Brauer	Germany	Mr. O. Demidov	Russian Federation
Mr. A. Manickam	India	Mr. S. Tilling	Sweden
Mr. J. Nugent	Ireland	Mr. R. Vanek	Switzerland
Mr. H. Shimizu	Japan	Mrs. K. Mitchinson	United Kingdom
		Mr. M. Holly	United States

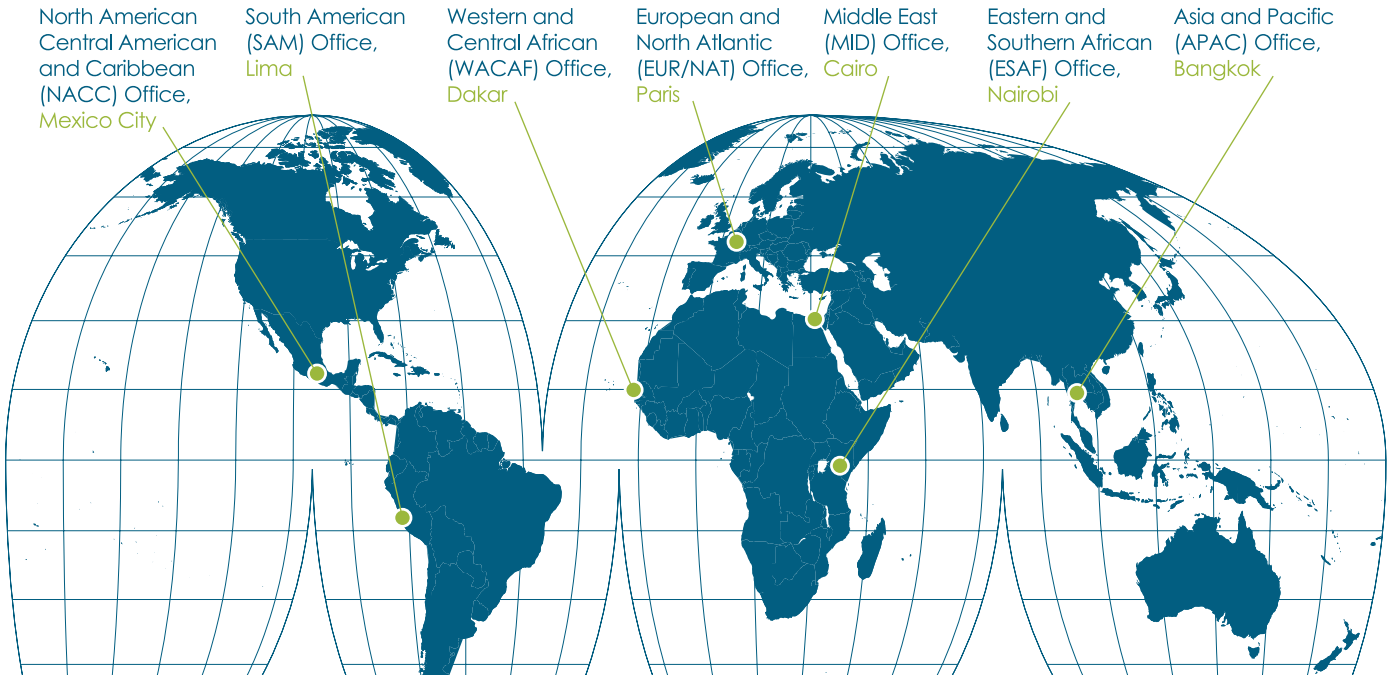
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

The TAG/MRTD develops specifications for machine readable passports, visas and official travel documents, electronic machine readable travel documents and guidance material to assist States in implementing these specifications and exploiting modern techniques in inspection systems

Observer organizations

Airports Council International (ACI)
European Union (EU)
International Air Transport Association (IATA)
International Criminal Police Organization (INTERPOL)
International Labour Organization (ILO)
International Organization for Standardization (ISO)
Organization for Security and Cooperation in Europe (OSCE)
International Organization for Migration (IOM)
United Nations (UN)
Organization of American States (OAS) - Inter-American Committee on Terrorism (CICTE)

ICAO's Global Presence



Responding to the Challenges of an Evolving Security Environment

ICAO is the only global agency with the mandate to establish and maintain standards governing the issuance and verification of Machine-readable Travel Documents (MRTDs) and related border control issues.

In recent decades, the ICAO MRTD Programme has developed universal specifications for robust identity management, travel document security and data sharing. These have been employed on a global basis to better prevent terrorist mobility and trans-border crime, and the effective implementation of MRTD specifications has been instrumental in increasing national and international security while simultaneously making it easier for the general public to enjoy international travel.

In particular, biometric travel documents (e-MRTDs or e-Passports) and ICAO's Public Key Directory (PKD) represent a particularly effective solution in preventing forms of identity fraud which could otherwise be exploited for terrorist and criminal purposes.

Global Security Challenges

The evolving aviation security debate has recently moved beyond passenger screening to take into account border security matters such as identity management, inter-agency cooperation, data sharing and combatting identity fraud. These new approaches were triggered in part by the failed Northwest Airlines bombing plot on 25 December 2010, which highlighted the need to be able to identify and stop perpetrators before they engage in attacks against aviation.

The ICAO Declaration on Aviation Security, unanimously adopted at the ICAO 37th Assembly, places particular emphasis on the collection, analysis and timely sharing of information, and urges States to share best practices in areas such as travel document security, fraud detection and effective border controls.

The 37th Assembly also guided the MRTD Programme to address additional travel document security concerns, including evidence of identity ('breeder documents'). The broadening scope of the MRTD Programme and emerging synergies with the Organization's aviation security priorities is today spearheading the development of a comprehensive, multi-layered security approach relevant to the present environment while anticipating future needs.

"The transborder crime and terrorism focus has consequently shifted to the pre-issuing and post-issuing phases in the travel document security chain."

The following are three of the more important trends that have been shaping the ICAO MRTD Programme.

Addressing New Challenges

The need to expand the current MRTD Programme scope was recognized by the recent Technical Advisory Group on MRTDs (TAG/MRTD). Historically, the MRTD Programme focused on developing harmonized specifications for manufacturing and personalizing MRTDs to ensure their global interoperability. Due to the fact that this objective has now been achieved, the transborder crime and terrorism focus has consequently shifted to the pre-issuing and post-issuing phases in the travel document security chain.

The weak links here include documents and administrative mechanisms establishing evidence of identity ('breeder documents'), as well as civil registries and gaps in the internal integrity of issuance processes. Border controls, travel document fraud, forensic examination and detection, and cross-border intelligence sharing have also emerged as areas in need of more collaborative and effective solutions. Those new areas of security concern and focus need to be addressed with considerable political will and resources and will assist in consolidating the core MRTD Programme with respect to its security mandates.

Need for Increased MRTD Capacity-building

The current MRTD specifications are state-of-the-art and up to the

“The ICAO Declaration on Aviation Security provided further guidance on the future of the MRTD Programme, especially with respect to the need for a more comprehensive security architecture able to respond to current terrorism challenges.”

standards of the most developed States. Given the complexity of the specifications, however, there have been demonstrated constraints in less-developed States due to a lack of technical expertise or funding or both. In addition, even developed States have been facing significant challenges in ensuring full ICAO compliance of their e-Passports. Such capacity gaps have been compromising universal MRTD implementation and suggest an urgent requirement for a closer technical dialogue with States in need, intensified liaison with donor agencies and expanded capacity-building programmes. ICAO is currently exploring ways to better help States more effectively develop their MRTD implementation capacity.

MRTD/AVSEC Synergies

The ICAO Declaration on Aviation Security provided further guidance on the future of the MRTD Programme, especially with respect to the need for a more comprehensive security architecture able to respond to current terrorism challenges.

In addition to traditional aviation security measures such as the employment of new technologies for passenger and cargo screening, aviation security experts have highlighted the importance of travel document security, identity management and improved data sharing as key elements of a more enhanced and comprehensive 21st century aviation security regime. In particular, the Declaration called for intensified and expanded use of the ICAO Public Key Directory (PKD) and INTERPOL’s Stolen and Lost Travel Document (SLTD) database, two key global instruments in preventing and combatting identity fraud. The Declaration placed particular emphasis on information collection, analysis and timely sharing, urging States to define and share new best practices relating to travel document security and fraud detection.

Re-affirming the Importance of the TAG/MRTD Working Groups

The MRTD Programme continues to receive invaluable support from the TAG/MRTD and its working groups. The New Technologies Working Group (NTWG) continues developing MRTD specifications and incorporating newly-emerging technologies. The Implementation and Capacity-building Working Group (ICBWG), established two years ago, has been gaining momentum and expanding its activities in project development and implementation, capacity-building and developing training programmes. The ICBWG has become an international framework that increasingly links the needs of States, available technical expertise and donor funding. In addition, the Chairs of the TAG/MRTD and its working groups have been actively involved in defining the emerging mid-term MRTD strategy.

Ongoing contributions by the NTWG and ICBWG remain essential to the continuing success of the MRTD Programme. ■

Leveraging the Advantages of New UK e-Borders

The United Kingdom (UK) has one of the toughest borders in the world and the UK Border Agency (UKBA) is determined to ensure it stays that way.

In transforming its border, the UK has integrated the work of immigration and customs services into a newly consolidated Border Force. The UKBA is taking advantage of improvements in technology to increase the level of data and intelligence support to frontline operations, as well as to effectively manage increasing passenger numbers through automated systems that complement, rather than compromise, the UK's strong border controls.

As Ian Neill, Deputy Director of the UK e-Borders Programme describes, by using new technology the UKBA is transforming the manner by which its national border is protected, tackling smuggling, illegal immigration, and associated organized crime activities while helping identify other threats to the UK and facilitate legitimate travel and trade.

Ian Neill has a wealth of experience in the UK Border Agency, having commanded two terminals at Heathrow as well as holding a variety of posts in the enforcement arena and heading up the worldwide Airline Liaison Officer network.

Neill's current role is as Deputy Director for the United Kingdom's e-Borders Programme. During his time with e-Borders, Ian has had particular responsibility for operational projects, including the highly successful project Semaphore—the de-risking pilot for the eventual e-Borders solution and IRIS (Iris Recognition Immigration System) providing pre-registered travellers with expedited clearance through the UK border via biometric technology.

The UKBA is among the world's leaders in using state-of-the-art technology to support its mission and mandate.

The Agency's new Border Force will collect information, store it securely and employ this data on a realtime basis to support its frontline personnel. This new strategy will increase the proportion of interventions based on intelligence and targeting and focussing on risk and harm.

More advance information on the people and goods arriving at UK border checkpoints will now be available through these technological advancements, putting the UKBA's trained personnel in a better position to identify suspect people and goods and to intervene where appropriate.

Border Force technologies will both 'export' the border—flagging risks before they arrive in the UK—as well as establish an automated clearance option for certain categories of passengers in order to expedite and facilitate their passage through border controls.

It is precisely for this purpose that the UKBA has introduced new ePassport gates, which are currently being trialled at 10 terminals across the UK—including Heathrow Terminals 1, 4 and 5. These gates use facial recognition technology and can be used by European Economic Area (EEA) nationals aged 18 years and over who are in possession of a biometrically-enabled ePassport.

These developments and efficiencies entail no compromise to security. To avoid any missteps the UKBA is using risk assessments and advance data to pre-screen passengers so that its officers can focus instead on the highest-risk traffic.

Implementing e-Borders

To better protect the public, the UKBA has begun targeting terrorist suspects, known criminals and would-be illegal immigrants before they travel. This is accomplished by increasingly checking cross border travel using the electronic border control system known as 'e-Borders'.

e-Borders revolutionizes the way in which the UKBA operates its primary border checkpoints. Passengers arriving in and departing from the UK are now pre-checked before departure, with alerts being made available earlier to allow Border Force and police officers the opportunity to identify known and suspected criminals.

The e-Borders system is currently analyzing over 120 million passenger movements per year in and out of the UK, cross-referencing its data against UK Border Agency and police watch lists.

Since 2005, this new integration of database and border control technology has led to over 6,700 arrests for crimes including murder, rape and assault. It has helped target individuals connected to counter-terrorist investigations, as well as leading to forged British passports being impounded, the confiscation of drugs and tobacco, and immigration offenders being refused entry.

e-Borders also enables the UKBA to profile known trends, traits and interlinked passenger movements in order to target particular travel patterns which reflect higher risk levels of immigration and smuggling crimes.

The UKBA will be enhancing its future intelligence and data efforts so that Border Force officers can prioritize

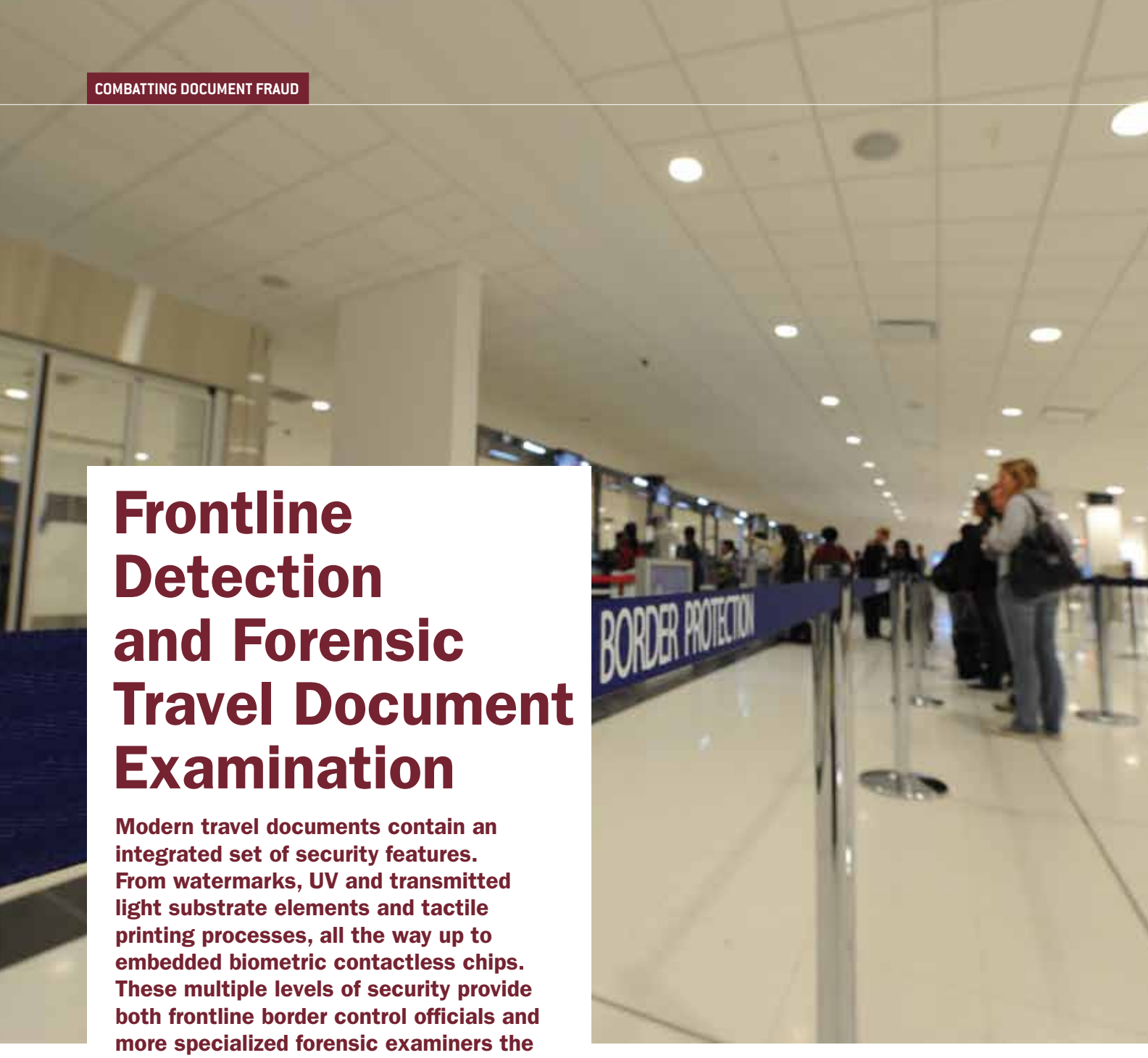
"Since 2005, this new integration of database and border control technology has led to over 6,700 arrests for crimes including murder, rape and assault. It has helped target individuals connected to counter-terrorist investigations, as well as leading to forged British passports being impounded, the confiscation of drugs and tobacco, and immigration offenders being refused entry."

against higher risk targets. The UKBA will also continue to develop its relationships with police and other law enforcement partners to improve and increase the inter-relationships between these national and international stakeholders and Border Force.

The special multi-agency National Border Targeting Centre (NBTC) and other regional hubs provide the bulk of intelligence and profile briefings for Border Force operations. The new purpose-built NTBC in Manchester enables the UKBA to work alongside our partners in the police and security services to analyze, verify and act upon the vast stream of passenger information that flows through the e-Borders system 24 hours a day, seven days a week.

This introduction of new technology, in addition to the vastly increased use of data and intelligence, will transform the amount of information frontline officers will have available to them when checking documents and assessing the legitimacy of people and goods—with the primary purpose of identifying people of interest more quickly.

The UKBA seeks to ensure that its law enforcement resources have the right tools to protect the public, but in doing so it recognizes the importance of striking the right balance between individual privacy and collective security. New technology will therefore assist in making the UK's border even more secure, realizing a 'win-win' scenario whereby the nation and its population are made safer through the more effective targeting of those who represent the most serious harm, while at the same time lower-risk passengers are provided with an automated clearance option that significantly expedites and facilitates their legitimate entry into the UK. ■



Frontline Detection and Forensic Travel Document Examination

Modern travel documents contain an integrated set of security features. From watermarks, UV and transmitted light substrate elements and tactile printing processes, all the way up to embedded biometric contactless chips. These multiple levels of security provide both frontline border control officials and more specialized forensic examiners the ability to detect and verify document fraud to levels never before possible.

As Charlie Stevens, former Head of the UK National Document Fraud Unit describes, covert second-level embedded security elements play a vital role in the establishing a more robust security framework for travel documents. It remains vitally important, however, that the largest number and range of security features continue to be accessible to frontline officials.

Charlie Stevens is the former Head of the UK National Document Fraud Unit. He worked for nearly 40 years for the UK Border Agency (UKBA), formerly the UK Immigration Service. Stevens' work encompassed many government projects, both in the UK and internationally, including representing the UK at the G8 Migration Experts Working Group, the EU False Documents Working Party and the EC Article 6 Committee. For 11 years he was the UK technical advisor to the ICAO New Technologies Working Group, assisting in the formulation of specifications for Document 9303 on MRTDs and e-MRTDs.

ICAO has always acknowledged in Doc 9303 that Machine Readable Travel Documents (MRTDs) need to contain a range of robust physical security features that can be checked by document examiners in addition to being machine readable.

It is important when dealing with security of MRTDs to remember the adage that 'a chain is only as strong as its weakest link'. With this in mind, it is first necessary to consider the problems and threats MRTDs face and the important role ICAO plays in combatting them.

Why does an MRTD need to be Secure?

This is not a frivolous question. To ensure that an MRTD cannot be counterfeited or unofficially altered (i.e. forged) it must contain a comprehensive range of document security safeguards.

The very first task required of a document examining officer is to confirm that the document being presented to them is of genuine issue and is in the possession of the rightful holder—before going on to accept the document as evidence of nationality and identity. This can only be achieved if the document is a high security document made of quality materials not readily available to the public and containing sophisticated security safeguards. The security safeguards must be many and varied to assure adequate levels of verification confidence at all levels of examination, including: front line border control inspections; back office reviews; expert forensics investigations; and security manufacturer confirmations.

Why do MRTD Manufacturing and Issuing Processes need to be Secure?

There is no point in having the most secure document that cannot be copied or altered if it is possible for anybody to obtain one fraudulently. Real documents can be obtained in a number of ways, three of the most common of which are outlined here:

1. *By stealing blank documents either from the manufacturer or from the issuing office.*

To combat this, MRTDs always need to be produced, transported and issued in conditions of the highest security. It is also vital that any losses or thefts are publicized globally as soon as they are detected so that control authorities have the intelligence information at hand to identify them. The Interpol database of lost and stolen travel and identity documents is a hugely important tool for detecting stolen blanks (as well as stolen issued documents) and should be a part of any frontline checking process.

2. *Documents obtained from issuing authorities by fraudulent application.*

This is where a person obtains a real MRTD by deceiving the issuing

authorities when making a bogus application for a document he is not entitled to. The application might reflect a real identity, a fake identity or the identity of a genuine citizen of the country concerned. The latter is what often happens in the growing area of fraud known as identity theft. To combat such fraud it is essential that rigorous and comprehensive procedures are in place in the issuing authority. These must involve the scrutinizing and verification of documents submitted in support of an application and, very often, interviewing the applicant in person to establish the truth of his identity and background. This is especially important in the case of first time applicants.

Another priority must be to check the document archives to compare the applicant against any previous applications for the same identity, as well as to carry out as many other checks of the issuing authorities' national databases as possible to confirm the application. These checks should include crime checks, proof of residency at an address, employment records and cross-referencing checks made with a range of databases such as birth, death, marriage and other civil registers. It is additionally of vital importance to have highly trained, efficient and well-motivated employees staffing document issuing centres so that issuance processes always reflect the highest possible standards of integrity, quality and accuracy.

3. *Through corruption.*

This is when bogus applicants obtain documents they are not entitled to by paying corrupt officials. This activity must be countered by strict legislation and law enforcement whereby the illegal applicants, the organized criminals helping them and the corrupt officials all face severe prison sentences when convicted. Key methods of reducing corruption involve careful and regular security vetting of document issuing staff and constant staff appraisals and reappraisals. It is also important that no single staff member has control of the complete end-to-end issuing process, for example those approving applications must not have access to the documents themselves or the physical issuing process.

Finally, it is always worth remembering that you only get what you pay for and that underpaid staff working in poor conditions will be less motivated and less reliable.

The Threat Posed by Organized Crime and Terrorism

It has often been questioned in our era of machine readability and standards for MRTDs, why it should still be necessary to have so many security features in travel and identity documents. The answer to that is that there is no such thing as a 100 percent fraud-proof document. MRTDs and new e-MRTDs have enhanced the reliability and automated

“Organized crime has brought extensive financial resources and the latest IT and printing technologies to the table with respect to the counterfeiting and forging of documents.”

verification aspects of documents but these developments have coincided with organized crime moving increasingly into travel and identity document fraud, which it sees as a relatively low-risk but high-return market place.

Organized crime has brought extensive financial resources and the latest IT and printing technologies to the table with respect to the counterfeiting and forging of documents. It is also quite willing to sell to a global market covering all areas of criminality from illegal immigration, to money laundering and smuggling, to documenting terrorists. The high level of resources available to fraudsters needs, therefore, to be combatted by constant revision and updating of the security features and safeguards deployed in travel documents.

The Role of ICAO in Combatting Document Fraud

ICAO’s aim in introducing global standards for MRTDs was based on the growing need to facilitate increasing numbers of international travellers in terms of passenger processing time, but at the same time to maintain and indeed enhance passenger, State and aviation security.

There are over 200 States in the world, each of which issues a range of travel and identity documents. Because of the vast range of different documents in circulation (virtually all MRTDs today thanks to ICAO’s excellent progress in this area) the job of control officials in examining documents is extremely difficult—mainly because it’s impossible for them to remember the specifics of format and content for all the countries’ various documents without there being an element of standardization.

Control officers operating on the front line therefore need high levels of training and technical support. This requirement, coupled with a standardized layout and format for documents meeting global standards of machine readability and a comprehensive range of document security safeguards covering identifiable generic types, can greatly assist in identification of document fraud. By generic rather than specific features I refer to those document security elements which permit the control agent to check for them without requiring that they also possess detailed knowledge of the specific mechanisms and components that make them up. Watermarks, ultraviolet (UV) printed safeguards or holographic devices all serve important roles in this regard. When necessary, more detailed checks of these generic features can be carried out at a more forensic level during a secondary examination.

Also essential for control officials is backward compatibility, i.e. the ability to check the oldest as well as the latest MRTDs using the same equipment and examination techniques. It is ICAO specifically, through its MRTD programme and the related standards and guidance as laid out in Document 9303 (covering both document security as well as machine readability), that has met this challenge for globally interoperable standards.

"The value of the format and content of the Machine Readable Zone is enormous, not simply for accurate machine reading but also in detecting alterations or counterfeiting through the MRZ check digits."

The Security Value of ICAO–compliant MRTDs

The globally harmonized size and format standards of Doc 9303-compliant MRTDs in and of themselves provide an immediate and valued guide to border control officials in the detection of fraud. Control officers used to handling often thousands of documents a day become accustomed to the size of an MRTD—be it a passport, visa or identity card. Officers also become accustomed to the layout of the data page and the machine readable zone and any deviations from the ICAO standards will be quickly apparent to the properly trained operative.

Furthermore, the value of the format and content of the Machine Readable Zone (MRZ) is enormous, not simply for accurate machine reading but also detecting alterations or counterfeiting through the MRZ check digits. Indeed, many skilled control officials are able to verify these check digits with a visual verification alone and without the need for a machine reader!

Why are many Security Features employed in each MRTD?

This is a case of not putting all your eggs in the one basket. By that I mean the more quality security features incorporated into an individual document the more difficult it becomes for forgers or counterfeiters to overcome them.

Quality security features are very expensive as they need to be difficult to replicate or alter and cannot be available for purchase on the open market. They must be produced by companies with a high level of security clearance in ultra-secure manufacturing environments and need to be transported and delivered under conditions of high security. They also invariably involve the use of expensive and hard to obtain materials. Manufacturers will also carefully vet customers and will report to enforcement authorities any prospective customers who do not have suitable accreditation or who have not demonstrated valid reasons for needing to procure the particular security features.

These requirements, in addition to the expense of the security features themselves, contribute significantly to the overall security of the document. The more difficult and expensive it is to obtain the security features the more criminal forgers or counterfeiters will struggle to produce credible fraudulent documents and, as a result, will often fail to reproduce many of the security features involved, thus making detection of the false documents easier.

It is important for document examiners, be they frontline or forensic back office examiners, to assess all or as many of the security features in a document as possible to ensure that each is properly in place and has not been altered or omitted. It is also important to remember that secure MRTDs are mass produced items and, accordingly, all documents of the same type or series should be identical and of the highest quality. Security document manufacturers work to the highest quality control standards and it follows that any MRTD that is different from others of the same type and series must be regarded as highly suspicious.

Why do we need Security Features in Biometric-enabled MRTDs?

ICAO has successfully taken on the responsibility for developing globally interoperable biometric standards for MRTDs and, as a result, has increased the security of the document against fraudulent use. In doing this, ICAO was also well aware that full global implementation of these standards would take many years to achieve. In addition, to be fully effective, biometric MRTDs will require all control points worldwide to be equipped with suitable readers to be able to conduct one to one verifications of stored biometrics against the persons presenting the documents.

On top of this there will remain a risk of chips (contactless integrated circuits or 'contactless ICs') failing for technical, accidental or deliberately malicious reasons. ICAO acknowledged that it is essential that all e-MRTDs be backward compatible; i.e. they can be examined and verified by skilled control officers even when the use of biometric document readers is not possible or the chip is not properly functioning.

Why is Frontline Examination so Important?

Frontline border control inspections are the start of the examination chain. If suspicions are not raised here then back office or forensic checks will not be conducted. Often it is the behaviour of the document holder that gives rise to suspicions, not simply the document itself. Frontline inspections are therefore the point where both impostors as well as document fraud are generally identified.

How is Document Fraud Detected at the Frontline Inspection Area?

The border control official must bear in mind the following:

- At the front line the passenger's bona fides are tested.
- Compliance of the MRZ is validated.
- Checks of passengers against watch lists are made.
- Checks of the document numbers against watch lists are made (such as the Interpol SLTD).
- Is the passenger the rightful holder? Biometrics verification is carried out, if possible.
- MRTD security features are checked.

MRTD Security Features

As has already been mentioned, there are a number of back office and forensic levels of document examination available in addition to frontline inspections. At these higher levels document examiners will analyze documents using sophisticated equipment involving high levels of expertise and intelligence material. Because of this, covert document security features are often incorporated into secure MRTDs for examination at these secondary levels. It is, however, important that the largest number and range of security features are incorporated for frontline checking. As already mentioned, if fraud is not detected at the frontline inspection area then the MRTD will not be redirected for examination at the other higher levels and the control will have been breached.

It is vital that the vast number of security features can be identified at frontline areas with only the limited equipment available to the control officers; such as the MRZ and/or biometric chip reader, UV light, transmitted light and low-level magnification.

It follows that the majority of these frontline security features are either visually apparent (can be identified and checked with the naked eye) or tactile (identifiable and checkable by touch). Such security features range from quality watermarks to specialist security inks and printing processes, as well a range of holographic type devices.

Further information on the range and variety of suitable physical security features can be found in the Appendix[1] entitled *Security Standards for Machine Readable Travel Documents* in Parts 1–3 of ICAO Doc 9303. Equally important, however, it is essential both now and into the future that control officials are trained and equipped with all possible technical and professional skills. ■

[1] Informative Appendix 1 to Section III (Doc 9303, Part 1, Vol.1), Annex to Section III (Doc 9303, Part 2), and Informative Appendix 1 to Section III (Doc 9303, Part 3, Vol.1). Please note that the Supplement to Doc 9303, Release 9, also includes some updates on security features and should be read in conjunction with relevant chapters of Doc 9303. The current Supplement as well as all parts of Doc 9303 are available for download from the ICAO MRTD web site in all official UN languages.

Key Features of an ICAO-compliant Visa

The word 'visa' derives from the Latin *carta vīsa* or 'paper which has been examined'. With the rise of international mobility, a visa today is better understood as a limited authorization issued to a passport holder in the form of a stamp or label which entitles them to travel to and from a country or territory.

In order to facilitate border clearance processes and make visas globally interoperable, ICAO issues guidelines for the layout, security features and personalization of a machine-readable visa. Claudia Hager, CEO of OeSD International, examines these elements and highlights the importance of ICAO Doc 9303 as a key enabler of the improved levels of security and facilitation that passengers enjoy today when travelling between ICAO Member States.

Claudia Hager has been working in the document security sector for more than ten years and is currently the CEO of OeSD International, a subsidiary of the Austrian State Printing House. Hager advises different governments on how to correctly accommodate the proprietary needs regarding effective e-Passport and ID projects based on ICAO's recommendations and modern production technologies. She is currently the Austrian ISO representative for documents to ICAO and has contributed in various official roles to e-MRTD development.

ICAO provides visa specifications in Part 2, *Machine Readable Visas,* of the Third Edition of its Doc 9303 (2005). A Machine Readable Visa, or MRV, allows for improved compatibility and global interchange by being both eye-readable and machine-readable for easier processing during border or other State verification procedures.

A number of basic information elements have to be displayed on a Doc 9303-compliant MRV, namely:

- Territory covered.
- Validity period.
- Duration of stay.
- Number of entries.
- Fee paid.

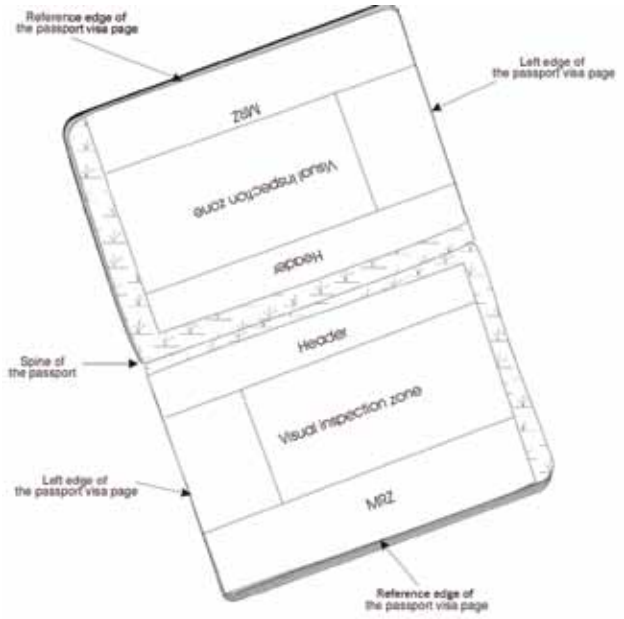
A typical visa for the Schengen States, illustrating the presence and location of the required MRV elements, is shown in Figure 1 *(above right).*

Figure 1: Required Elements of an ICAO-compliant Machine Readable Visa (MRV)

Some visa formats provide a field to include the fee that has been paid for the visa, while in other cases a separate receipt is issued and the visa itself serves as proof that the fee has been paid. Visas are typically attached to a page in a passport document. As such they can be issued in two sizes.

MRV-A is issued as a full format label (80mm x 120mm) which is only slightly smaller than the actual passport page it is affixed to (88mm x 125mm). It can be glued on either the left or right edge of the passport page but, due to its large size, can also cover the perforated passport number (where this is present) in both its top and bottom locations.

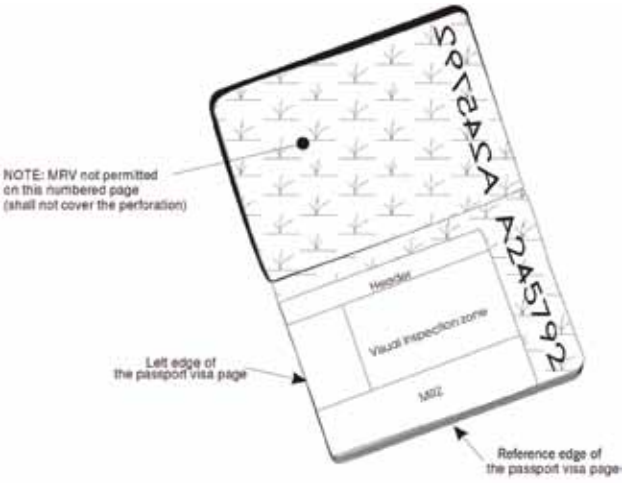
Figure 2: MRV-A Label Placement Providing for MRZ Left-edge Passport Page Positioning.



The MRV-A label has to be positioned in such a manner that the Machine Readable Zone (MRZ) is on the outer left edge of the landscape-proportioned passport page on which it appears, as shown in Figure 2 *(above).*

The smaller *MRV-B* visa label features nominal dimensions of 74mm x 105mm. It is small enough not to interfere with the laser perforated number appearing at the top or bottom of the passport page as it must be aligned with the opposite edge of the page.

Figure 3: MRV-B Label Placement when a Passport has its Perforated Number Positioned at the top of the Passport Page.



If the laser perforated number is located at the top of a passport's page, the MRV-B visa label can only be glued on the right-hand side of the passport's page 'spread' *(see Figure 3, below left).* If the perforated number is located at the bottom of the passport page, the MRV-B can only be attached to the left-hand page. The MRZ of the MRV-B visa label, as with the MRV-A format, always has to be positioned along the long outside edge of the passport page.

The tolerance of the nominal dimensions for both visa types is +/- 1mm. The thickness of the visa once its backing is removed and it is affixed to the page must not exceed 0.19mm. In the event that an additional protective laminate is used, said laminate's thickness must be no more than 0.15mm.

The layout of the MRV-A and MRV-B visa label sizes is very similar. Both contain six zones, each of which must present ICAO-specified information elements.

The top information area, *Zone I,* extends across the full width of the visa and contains the name of the issuing State and the document type (i.e. 'visa' or other document type, as appropriate).

Zone II contains personal details of the visa holder, such as their name, passport number, sex, nationality and date of birth. Readers may wish to pay special attention to the location of Zone II as it is actually below Zone III and not immediately below the Zone I header space as some might expect.

Zone III reflects information about the visa document itself. Here we will find the place of issue, the visa's validity period, its document number, the maximum number of entries it permits and its specific visa type. Zone III is located immediately below Zone I.

Zone IV is an optional field and can be used to display the signature or stamp of the issuing authority/officer.

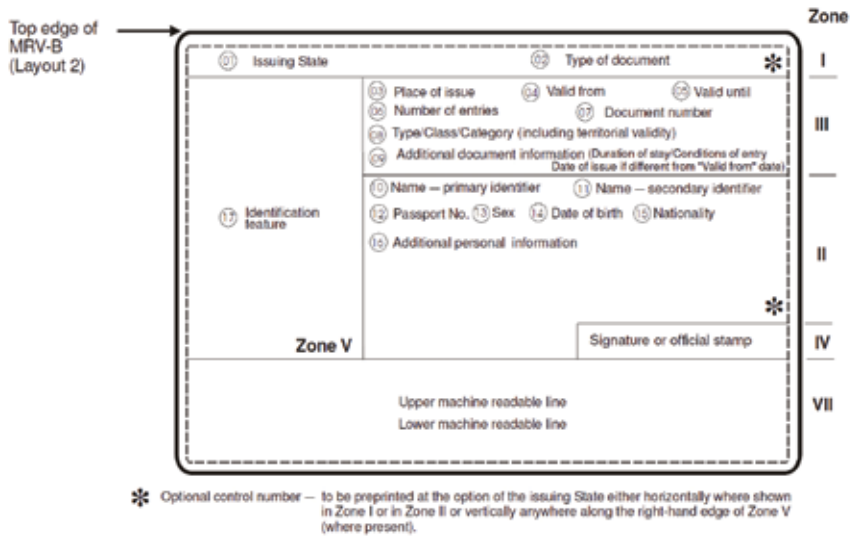
Zone V is located on the left side of the visa and is reserved for a photograph of the visa holder. The size of the photo shall be 36mm x 29mm and, in the event that no photo is printed on the visa, then this area shall contain other identification features which are standard for the issuing country (i.e. a national symbol or logo).

A visa does not contain a sixth zone (Zone VI), as this zone is reserved for specific features regarding reverse sides or adjacent pages and are therefore not applicable to visas.

Zone VII is reserved for the MRZ and consists of two lines.

Figure 4 *(p.17)* illustrates the positions of the zones described above as they appear on a typical visa.

Figure 4: A Typical Visa Layout reflecting its various Information Zones (I, II, III, IV, etc.) and the Data-types to be found in each Zone.



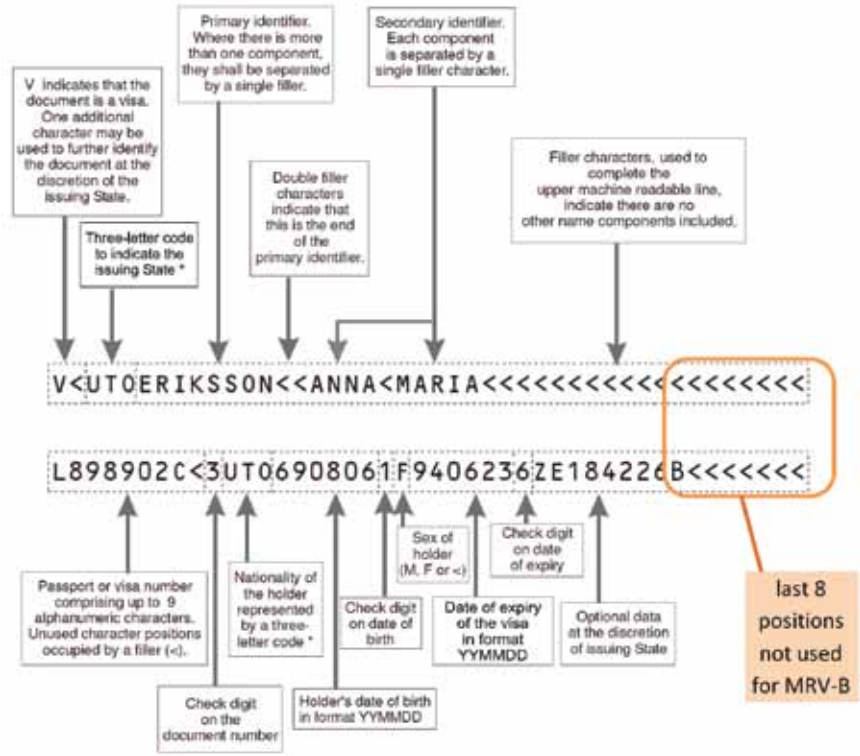
In order for a State to be able to issue a globally interoperable visa, the visa label must contain two lines of MRZ information and it is of the utmost importance to print the MRZ data in full compliance with ICAO's specifications.

Each alpha-numeric element within the MRZ is mandatory and reflects dedicated data content *(see Figure 5, p.18).*

The MRZ must only contain letters from the Latin alphabet and Arabic numerals. Any deviance from the established MRZ structure will necessarily result in detrimental results concerning its interoperability with the harmonized global system ICAO and its Member States have now established.

The number of alpha-numeric characters in the MRZ lines differs depending on the two visa sizes. MRV-A visas have two lines with 44 characters in each line. MRV-B visas also have two lines but can contain only 36 characters per line due to their smaller size. The mandatory data contained in the MRZs are identical for both visa sizes; the difference being that fewer characters for the bearer's name and fewer optional data elements can be added in the smaller MRV-B MRZ area.

Figure 5: Details of the MRZ's Alpha-numeric Composition.



For both visa types the two alpha-numeric MRZ lines must be printed in a special machine readable font, namely OCR-B size 1.

The MRZ represents the globally-harmonized format for encoding the individual data of the traveller. It is quickly and correctly readable with the OCR-B readers used by border authorities. If the composition guidelines for the MRZ are not properly followed, the readers cannot display the correct information for the correct fields. In cases where a wrong character set is employed and the MRZ is improperly positioned on the visa itself, a reader will be unable to read the MRZ at all.

Figures 6 and 7 *(right)* illustrate an example of the MRZ of a live visa and some consequent problems. The visa in question was issued to me by a State using Cyrillic characters. My name was displayed in the VIZ zone as per Figure 6, while the MRZ information was reflected as per Figure 7.

In the MRZ line one zone, the first character, 'V', is correctly printed, but the position for the optional second character is supposed to be indicated by the filler character '<' if no second character is used. This guideline has not been respected in this instance. My last name, 'HAGER', should only begin in the third character position but here it is beginning in the second position—where as noted the filler character should be used.

My first name, Claudia, is correctly printed in the VIZ in Figure 6, and correctly translated into Cyrillic in the VIZ such that the character 'C' has now been reflected as a 'K'. In the MRZ line one zone, however, the original Latin name 'CLAUDIA', with the 'C' spelling, should have been used, but unfortunately the Cyrillic translation was inserted here instead, leading to the incorrect spelling 'KLAUDIA'. The MRZ line one is not supposed to have a check digit, so the number '4' at the end of the line is also incorrect.

In line two of the MRZ zone, the first nine positions are reserved for the passport number and in the tenth position the check digit of the passport number must be displayed. The check digit for this passport number is '0', but it appears only in position 13. This has lead to the rest of the MRZ line two data appearing too far to the right in the character sequence. My nationality, 'AUT', is correctly printed (still three positions too far to the right, however), as are the following check digit and the 'F' indicating my gender. The positions after the gender character indicator are supposed to be reserved for the expiry date of the visa as per

Figure 6: Sample live visa, VIZ detail.

Figure 7: Sample live visa, MRZ detail.

"The MRZ represents the globally-harmonized format for encoding the individual data of the traveller. It is quickly and correctly readable with the OCR-B readers used by border authorities. If the composition guidelines for the MRZ are not properly followed, the readers cannot display the correct information for the correct fields."

a 'YYMMDD' format, but here totally different and unspecified information appears. The rest of the line contains optional information, which in this instance appears to be the place of issue and the application number for the visa.

The issuing authority in question needs to pay closer attention to the many sources for read errors based on how this visa's MRZ has been configured. Once the correct correlations between the identity and issuance data and the MRZ have been properly established and the checksums correctly calculated, the authority will at that point be better prepared to provide visas with MRZ data conforming to the fundamental ICAO-compliant guidelines that provide for global interoperability.

Detailed dimensions of visa zone locations and their tolerances, as well as the mandatory and optional content prescribed for each can be found in ICAO Doc 9303, *Part 2,* which is available from the ICAO web site at **www.icao.int/mrtd** in all of the UN's official languages.

Importantly, the *Release 10* version of the *Supplement* to Doc 9303 includes updated security standards for machine readable documents which are also applicable to visas. The provisions of the *Supplement* will be incorporated into the next edition of Doc 9303, but for the time being the *Supplement* remains a separate document which is also available via the MRTD web site. ■

ISO 9001 and the US GPO

by Garry Lambert

The Government Printing Office (GPO) of the United States has reached what it describes as *"a major milestone in the production of the US passport"*, arguably the world's most secure document. It has done this by achieving ISO 9001 Quality Management System (QMS) certification of the organization's secure production facility at the Stennis Space Center in Mississippi.

Since 2008, when the facility began implementing ISO 9001-conforming procedures and process improvements, the average amount of material waste dropped significantly. These improvements have included the installation of digital access to the QMS operating procedures on touch pad laptops to provide quick and easy access on the production floor.

***ISO Focus+* asked Steve LeBlanc, Managing Director of the GPO's Security & Intelligent Documents Unit, to expand on the organization's ISO 9001 implementation and certification experiences.**

The following article first appeared in the November 2010 issue of *ISO Focus+*, the magazine of the International Organization for Standardization. It is reproduced here with the permission of the ISO Central Secretariat (www.iso.org). Garry Lambert is a freelance journalist based in Geneva, Switzerland.

Steve LeBlanc

***ISO Focus+:* What were the key reasons for implementing ISO 9001 at the GPO, and what did you hope to achieve?**

Steve LeBlanc: We implemented and certified to ISO 9001 to create an environment of process improvement and high process standards, to assure customers that we are making products consistently, to raise the quality bar, and be able to show we meet the global standard of excellence. Since the GPO opened the Mississippi facility in 2008, employees there have made that facility a model of high standards and high quality manufacturing processes.

Was this a top management decision?

Yes, it was a top management initiative supported by GPO Public Printer, Bob Tapella, and myself. We established performance goals for the ISO 9001 implementation process and set time and resources aside for it.

GPO Passport Manager David Spiers (left) and Foreperson Dio Enterline inspect a passport print sheet produced in conformity with ISO 9001 quality procedures.

ABOUT THE GPO

The Government Printing Office (GPO) is the US Federal Government's primary centralized resource for gathering, cataloguing, producing, providing, authenticating and preserving published government information in all its forms.

The GPO is responsible for the production and distribution of information products and services. It makes government information available at no cost to the public through its Federal Digital System (www.fdsys.gov) and through partnerships with approximately 1,220 libraries nationwide which participate in the Federal Depository Library Program.

The GPO has been producing passports for the US Department of State since the 1920s at its secure facility in Washington, DC. In 2008, to meet the rising demand for passports, the GPO opened its second secure production facility in the US state of Mississippi.

In 2005, the GPO produced the first electronic passport (e-Passport) and switched to producing all e-Passports in 2007. GPO employees produced more than 23 million passports in the last two years, of which about seven million came from its Mississippi facility.

For more information, visit: **www.gpo.gov**

Average material waste dropped from 5.9 to 0.5 percent. ISO 9001 helped us simplify virtually every operating procedure.

Did you have to adapt the requirements of ISO 9001 to suit the organization, or was it a good fit?

We didn't change anything—we implemented ISO 9001 as written. GPO does a monthly review, i.e. following the 'planned intervals' as requested by the ISO standard, and it fit the business model without change.

Did GPO employees receive training in ISO 9001 requirements and procedures?

All employees were trained in-house. We developed our own training modules via steering committees and also trained our internal auditors. Employees were engaged in the training every step of the way, which was achieved with good will throughout.

In addition to installation of digital access, can you mention any other operating procedures that were adapted as a result of ISO 9001 implementation?

We chose to go paperless, and ISO 9001 implementation helped us simplify virtually every operating procedure.

You mention a reduction in material waste... How was that achieved?

We measured waste over a one-year period. *Step 1* was to track waste by getting operators to measure it from their own production processes, which made them aware. *Step 2* was to identify the big waste leaders, mainly the paper and electronic materials involved in the production of passports.

Have you extended ISO 9001 certification further in the organization?

The GPO's Security & Intelligent Documents division controls the production of millions of passports, border crossing cards, and associated documents each year through two facilities. In 2010, GPO's passport facilities in Washington, DC and Mississippi received ISO 9001 certification. This means that as of today 100 percent of US passports are produced in conformity with ISO 9001 standards. ■

The ISO Three-letter Country Code Regime

The three-letter codes employed by ICAO within Doc 9303, Part 1, are intimately linked with the alpha-3 signifiers used within ISO 3166-1 to denote countries and their subdivisions.

Gérard Lang, President of the ISO 3166 Maintenance Agency, provides here an overview of some of the similarities and differences at the heart of these two essential systems of international classification.

Gérard Lang is the convenor of ISO/TC 46/WG 2 (Coding of country names and related entities), liaison officer from ISO/TC 46 (Information and documentation) to ISO/TC 37 (Terminology and other language and content resources), chairman of ISO 3166/MA, and one of the ten members of the ISO 639/RA-JAC (Registration Authority/Joint Advisory Committee). He graduated from ENSAE (French national school for statistics and economic administration) in 1971 and has been working for INSEE (French National Institute for Statistics and Economic Studies) since then until his recent retirement. He was initially (and likes to think he still is) a logician and mathematician, interested with the limits of formal systems. Lang eventually became a lawyer (and historian) for the French national statistical system. He has been the French member of the European Committee for Statistical Confidentiality, and is currently Vice-president of the French National Toponymy Commission.

ISO 3166 (Codes for the representation of names of countries and their subdivision) is one of the most relied upon international standards. It is comprised of three parts, namely: *Part 1*—Country codes; *Part 2*—Country subdivision codes; and *Part 3*—Codes for formerly-used names of countries.

All three parts are available in English and French.

ISO 3166 is managed by Working Group 2 (WG2: Coding of country names and related entities), which falls under the oversight of ISO Technical Committee 46 (ISO TC 46: Information and documentation). The standard has a Maintenance Agency (ISO 3166/MA) whose secretariat is directly managed by the ISO's Central Secretariat.

ISO 3166/MA comprises ten members, five of which represent a national standardization body (AFNOR [France]; ANSI [USA]; BSI (United Kingdom]; DIN [Germany]; SIS [Sweden]. The remaining five members represent international organizations (International Atomic Energy

Agency (IAEA); Internet Corporation for Assigned Names and Numbers (ICANN); International Telecommunications Union (ITU); United Nations Conference on Trade and Development (UNCTAD); and Universal Postal Union (UPU)).

Part one of the ISO 3166 standard (ISO 3166-1) now contains 248 entries. One hundred and ninety-three of these (the Vatican and the 192 United Nations Member States) are independent countries while the remaining 55 are considered to be territories of particular geopolitical interest.

ISO 3166-1 provides three different codes for the representation of each of its entries: alpha-2 and alpha-3 (two- and three-character codes respectively derived from the 26 letters of the latin alphabet) and numeric-3, a three-digit code which is provided by the United Nations Statistics Division (under the name 'Standard Country and Area Code for Statistical Use', also known as M.49).

As an example, the following list reflects five separate Dutch entries which were contained within ISO 3166-1:

- NETHERLANDS/PAYS-BAS (NL, NLD, 528)—an independent country, and the four following Dutch territories having particular geopolitical interest:
  - ARUBA/ARUBA (AW, ABW, 533);
  - BONAIRE, SAINT EUSTATIUS AND SABA/BONAIRE, SAINT-EUSTACHE ET SABA (BQ, BSE, 535);
  - CURAÇAO/CURAÇAO (CW, CUW, 531);
  - SINT MAARTEN (DUTCH PART)/ SAINT-MARTIN (PARTIE NÉERLANDAISE) (SX, SXM, 534).

Montenegro was initially contained in ISO 3166-1 as part of Yugoslavia (YU, YUG, 890/891). Later, Serbia and Montenegro (CS, SGG, 891) became the 192nd UN Member State, requiring two new entries: SERBIA (RS, SRB, 688); and MONTENEGRO (ME, MNE, 499).

KOSOVO, which is not a UN Member State, has neither a corresponding code element inside the UNSD M.49 code nor a corresponding entry within ISO 3166-1.

Clause 8.1.3. (User-assigned code elements) of the ISO 3166-1 normative text states that:

> *"If users need code elements to represent country names not included inside ISO 3166-1, the series of letters AA, QM to QZ, XA to XZ, and ZZ, and the series AAA to AAZ, QMA to QZZ, XAA to XZZ and ZZA to ZZZ respectively and the series of numbers 900 to 999 are available. These users should inform the ISO 3166/MA of such use."*

Moreover, clause 7.5.4. (Exceptional reserved code elements) states that:

> *"Code elements may be reserved, in exceptional cases, for country names which the ISO 3166/MA has decided*

OVERVIEW: ISO 3166 AND THE UN

The United Nations, some of its specialized agencies and other sub-organizations of the UN play several important roles with regard to ISO 3166-1.

- First, four members of the ISO 3166/MA are from the UN environment.
- Second, the UN organizations are major users of ISO 3166. For example the World Intellectual Property Organization (WIPO) or the UN Economic Commission for Europe (UN/ECE) use the alpha-2 code from ISO 3166-1 for their country coding systems. (See examples for implementations of ISO 3166-1)
- Third, the numeric-3 code for the country names in ISO 3166-1 is developed and maintained by the United Nations Statistics Division in New York. It is given in ISO 3166-1 just as the alpha-3 code is given in the UNSD-list for reference purposes.
- Fourth, the country names used in ISO 3166-1 are all from United Nations sources. Using these country names officially notified by the countries to the UN Secretary General helps in keeping ISO 3166-1 politically neutral and thus acceptable to as many users as possible.

This strong involvement of various UN experts in the maintenance of ISO 3166 was established in the development phase of the standard in the early 1970s. It is one of the contributing factors to ISO 3166 having gained the global acceptance it has today.

not to include in ISO 3166-1, but for which an interchange requirement exists. Before such code elements can be reserved, advice from the relevant authority must be sought."

In fact, ISO 3166-1 was notified that the alpha-2 user-reserved code element XK was used by the European Union to represent Kosovo. And moreover ISO 3166/MA agreed when ISO/IEC JTC 1 asked for an 'exceptional reserved' status for the alpha-3 code element UNK to represent KOSOVO. Therefore SO 3166/MA is essentially recommending the use of the reserved code elements 'XK' and 'UNK' to represent the country name 'Kosovo' when necessary.

Annex 7 of ICAO Doc 9303

The three-letter code used by ICAO inside its Doc 9303, Part 1, which is additionally adopted and referred to inside the international standard ISO 7501-1 (Identification Cards - Machine Readable Travel Documents - Part 1: Machine Readable Passports) and used by all international MRTD issuing entities, is intimately linked with the alpha-3 code employed within ISO 3166-1.

This ICAO code is provided within Appendix 7 to Section IV of Volume I, Part I of Doc 9303, with the title:

"THREE LETTER CODE (based on Alpha-3 codes for entities specified in ISO 3166-1, with extensions for certain States being identified by an asterisk)"

This ICAO code is definitely not a 'country' code per se (nor completely an alpha-3 code), but can be better described as a 'quasi' alpha-3 code for designation of nationality, place of birth or issuing State/authority. The ICAO code comprises four distinct parts, as follows.

Part A—Codes for designation of nationality, place of birth or issuing State/authority

This part exactly reproduces the complete list of entries and corresponding alpha-3 code elements given inside ISO 3166-1, with a number of exceptions.

ICAO's code element for Germany is not the alpha-3 code element 'GER', as reflected by ISO 3166-1, but rather the alpha-1 code element 'D' (meaning that ICAO's code is not strictly speaking an alpha-3 code, but rather a 'quasi' alpha-3 code as I previously noted. Germany is in fact the only State which is signified by a single alpha-1 code element inside ICAO's listing).

Concerning the United Kingdom (i.e. Great Britain and Northern Ireland), where ISO 3166-1 provides the alpha-3 code element 'GBR', ICAO's code system includes the following six additional alpha-3 code elements representing the indicated classifications:

- GBR (Citizen)
- GBD (Dependent territories citizen)
- GBN (National [Overseas])
- GBO (Overseas citizen)
- GBP (Protected person)
- GBS (Subject)

Apart from 'GBR', the remaining five alpha-3 codes in this list have also acquired 'exceptionally-reserved' status (by ISO/IEC JTC 1) within ISO 3166-1.

Part B—Codes for use in United Nations travel documents

This part contains the following three entries. They have no counterpart inside ISO 3166-1 and their alpha-3 codes have also acquired the 'exceptionally-reserved' status inside ISO 3166-1:

UNO: Designates the United Nations Organization or one of its officials.
UNA: Designates a Specialized Agency of the United Nations or one of its officials.
UNK: Designates a resident of Kosovo to whom a travel document has been issued by the United Nations Interim Administrative Mission in Kosovo (UNMIK).

Part C—Codes for issuing authorities

This part contains the following two entries which have no counterpart inside ISO 3166-1:

XCC: Designates the Caribbean Community (CARICOM)
XOM: Designates the Sovereign Military Order of Malta or one of its emissaries.
XPO: Designates the International Police Organization (INTERPOL).

These code elements may additionally be found within the list of user-reserved code elements in ISO 3166-1.

Part D—Codes for persons without a defined nationality

This part contains the following four entries. Once again these have no counterpart inside ISO 3166-1 but their alpha-3 indicators are included in the list of user-reserved code elements found in ISO 3166-1:

XXA: Stateless person, as defined in Article 1 of the 1954 Convention Relating to the Status of Stateless Persons.
XXB: Refugee, as defined in Article 1 of the 1951 Convention Relating to the Status of refugees as amended by the 1967 Protocol.
XXC: Refugee, other than as defined under the code XXB above.
XXX: Person of unspecified nationality, for whom the issuing State does not consider it necessary to specify any of the codes XXA, XXB or XXC above, whatever the person's status may be. This category may include a person who is neither Stateless nor a refugee, but who is of unknown nationality and legally residing in the State of issue.

Others Codes Linked with ISO 3166

Many additional and interesting codes are linked with ISO 3166, among them:

ISO 4217
(Codes for the representation [of names] of currencies and funds) provides for an alpha-3 code, based on the ISO-3166 alpha-2 code, for the representation of the names of currencies (e.g. 'USD' for United States dollars; 'CHF' for Swiss francs; or 'GBP' for British pounds).

ISO 639
(Codes for the representation of the names of languages) provides alpha-2 and alpha-3 codes for the representation of names of the principal languages of the world as reflected within ISO 3166.

ISO 15924
(Codes for the representation names of scripts) provides an alpha-4 code for particular scripts and completes ISO 639 with respect to written languages.

AFNOR XP2 44-002
(Code pour la representation des noms de pays historiques) is a French experimental standard providing an alpha-4 code for the representation of names of historical countries pertaining to the period from 1815 (Congress of Vienna) to 1974 (when ISO 3166-3 was launched).

AFNOR XPZ 44-020
(Code pour la representation des noms des océans et des mers) is a French experimental standard providing a code for the representation of names of oceans and seas. It is considered a natural complement to the codification of the land masses of the world via ISO 3166.

ISO 3166 is the most used ISO standard in the world and has many applications in international information systems. While ICAO-compliant MRTDs employ the ISO 3166-1 alpha-3 code, other applications like the 'country code Top level domain' (ccTld) of the internet Domain Name System (DNS) employ alpha-2 identifiers (e.g.: '.fr'; '.us'; '.nl'; etc.). Together with additional ISO standards such as ISO 639, ISO 15924 and ISO 4217, ISO 3166 therefore provides a comprehensive system of codes for the representation of fundamental elements in numerous information systems. ■

Who is who?

Biometrics Provide Solutions for the Public and Private Sector

by Fernando L. Podio

Fernando L. Podio is a member of the Computer Security Division of the Information Technology Laboratory at the US National Institute of Standards and Technology (NIST), and Chair of ISO/IEC JTC 1/SC 37, Biometrics. He has worked on different aspects of IT development, measurements and standards for over 30 years. For the past 12 years, Podio has been involved in biometrics testing, research and standardization. He is currently leading biometric standards activities and technology development efforts in support of biometric standards and associated conformity assessments, including the development of conformance test architectures and test suites for testing implementations of biometric standards.

One of the critical issues related to secured Information Technology (IT) systems and applications is the verification of the user's identity. The relationship between a biometric characteristic (e.g. something that you are), and the users of a system or application provides a strong binding.

This strong binding can also be achieved between a user and other technologies that are currently in use for personal authentication, such as passwords (e.g. something that you know) and tokens (e.g. something that you have).

Subcommittee SC 37, *Biometrics,* of the ISO/IEC Joint Technical Committee on Information Technology (JTC 1/SC 37), defines biometrics as: *"automated recognition of individuals based on their behavioural and biological characteristics."* Examples of biological characteristics are finger, face, hand, and iris. Behavioural characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. It is usual to find, in the literature, biometric characteristics identified as two different types: biological and behavioural.

According to JTC 1/SC 37 experts, behavioural and biological characteristics cannot be completely separated. For example, a fingerprint image results from the biological characteristics of the finger ridge patterns and the behavioural act of presenting the finger. Biometric recognition encompasses biometric verification and identification. Automated recognition implies that a machine-based system is used for either the full recognition process or is assisted by a human being.

Marketplace for Biometric-based Solutions

For decades, biometric technologies were used primarily in law enforcement applications. However, over the past several years, the marketplace for biometric solutions has significantly widened. Currently, they are increasingly being required in public and private sector applications worldwide to authenticate a person's identity, secure national borders, and restrict access to secure sites, including buildings and computer networks.

Biometrics are being used for the protection of buildings from unauthorized individuals, in employee IDs, in retail, banking and financial institutions (e.g. employee-based/customer-based applications), associated with the management of welfare programmes and in health care applications (e.g. service

"The deployment of standards-based, high-performance, interoperable biometric solutions is expected to increase levels of security for critical infrastructures to a level that has not been possible to date with other technologies."

provider security to protect patient privacy, patient delivery verification protecting patient and provider).

Other applications include verification of users' identity in mobile devices, colleges (e.g. online identity verification) and amusement parks. Consumer uses are also expected to significantly increase for personal security and convenience in home automation and security systems, retail, gaming and hospitality industries and even in childcare/school applications (e.g. lunch programmes, guardian verification for child release).

Need for International Biometric Standards

The success of biometric applications is particularly dependent on the interoperability of biometric systems. Deploying these systems requires a portfolio of technically sound international biometric standards that meet customer needs. As discussed above, the deployment of standards-based, high-performance, interoperable biometric solutions is expected to increase levels of security for critical infrastructures to a level that has not been possible to date with other technologies.

An important consideration and rationale for the development of a comprehensive portfolio of biometric standards is that they promote the availability of multiple sources for comparable products. These standards must provide support for a diverse range of systems and applications designed to provide reliable verification and identification of individuals. They should benefit the customers for whom these standards are developed, including end-users, system developers, the IT industry, as well as other standards developers working on related standards (e.g. security, token-based).

The following addresses published and ongoing work in JTC 1/SC 37. This subcommittee is responsible for the development of a large portfolio of biometric standards in support of interoperability and data interchange.

Secure IT Systems and Applications

Including published standards and ongoing projects, the JTC 1/SC 37 subcommittee is currently responsible for over 100 projects. Topics addressed by these standards include biometric data interchange formats for a number of biometric modalities, biometric technical interface standards, performance and conformance testing methodology standards, sample quality standards, and standards in support of cross-jurisdictional issues related to the utilization of biometric technologies in commercial applications.

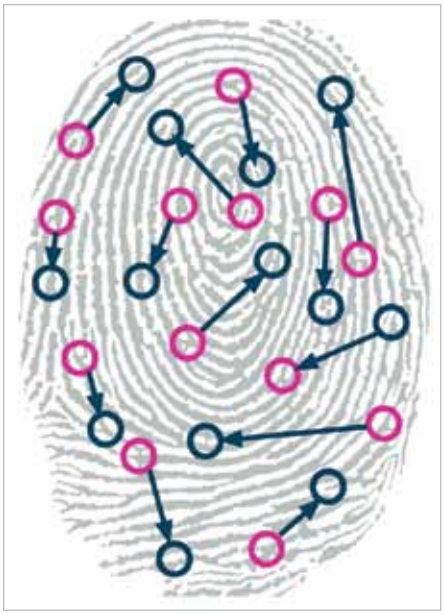
The subcommittee is also developing a harmonized biometric vocabulary to serve the standards community and other customers. To date, 44 international standards (including amendments) and six technical reports have been published. These standards are aimed at helping customers to achieve higher levels of security and interoperability in personal authentication and identification applications using biometric-based, open systems solutions. ISO/IEC JTC 1/SC 37 works in close collaboration with two other ISO/IEC JTC 1 subcommittees responsible for developing related standards: ISO/IEC JTC1/SC 27, *IT Security techniques;* and ISO/IEC JTC 1/SC 17, *Cards and personal identification.*

Impact and Benefits

A number of international and national organizations have adopted or are considering adopting many of the biometric standards developed by ISO/IEC JTC1/SC 37. ICAO, for example, selected facial recognition as the globally-interoperable biometric for machine-assisted identity confirmation for Machine Readable Travel Documents (MRTDs).

ICAO requires conformance to the face recognition standard developed by ISO/IEC JTC 1/SC 37. Other ISO/IEC JTC 1/SC 37 standards adopted by ICAO are the fingerprint data interchange formats, the iris recognition interchange format and an instantiation of the Common Biometric Exchange Formats Framework (CBEFF). The adoption of ISO/IEC JTC 1/SC 37 standards by this organization is expected to significantly impact the use of biometrics for MRTDs in the countries represented within ICAO.

The International Labour Organization (ILO) developed requirements for a Seafarers' ID Card which includes



the use of two fingerprint templates to be stored in a barcode. ILO requirements specify the use of some of the standards approved by ISO/IEC JTC 1/SC 37; specifically finger minutiae and finger image data interchange formats (published as International Standards in 2005). JTC1/SC 37, in collaboration with ILO, developed a biometric profile for Seafarers. The document, already published as an International Standard, includes normative requirements to several of the ISO/IEC JTC 1/SC 37 standards.

Several countries represented in ISO/IEC JTC 1/SC 37 are also adopting the ISO/IEC JTC 1/SC 37 standards. For example, Spain has two official documents that store biometric data using ISO/IEC JTC 1/SC 37 standard data interchange formats; the electronic national identity card (DNIe) and the Spanish e-Passport. The DNIe card includes the personal information of the citizen, details of electronic certificates and the biometric information. The Spanish e-Passport contains the face image conforming to a face image data interchange format developed by JTC1/SC 37.

In the United States, several organizations require selected biometric data interchange standards developed by ISO/IEC JTC 1/SC 37 and some of the ongoing biometric testing programmes use performance testing methodology standards developed by the subcommittee. The latest significant adoptions are the biometric standards that the Planning Commission of the Unique Identification Authority of India has recommended for its unique identity project.

After reviewing international standards and current national recommendations, the biometric committee established by the Indian Government concluded that the ISO/IEC series of biometrics standards for fingerprints, face and iris data interchange formats developed by ISO/IEC JTC 1/SC 37 were the most suitable for the project.

Roadmap

ISO/IEC JTC1/SC 37 is planning to continue the development of international standards, keeping in mind customer needs and the support for the mass market adoption of biometrics-based solutions. ISO/IEC JTC 1/SC 37 concluded the development of most of the 'first generation' of biometric standards.

Recent technological innovations and new customer needs are being addressed by the subcommittee through the development of the second generation of biometric standards. They include revision projects for biometric data interchange formats, the development of new biometric technical interface standards, performance (and conformance) testing methodology standards and biometric sample quality standards. The subcommittee is also responding to the needs of other standards organizations by initiating new projects in support of their requirements. ■

Ten Years After

In September of this year, ICAO's Seventh Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards will mark the tenth anniversary of 9/11.

Though ICAO's MRTD-related efforts date back significantly beyond the tragic events that unfolded on that day in 2001, it bears remembering that many of the remarkable advances forged by the MRTD Programme, particularly over the past decade, have been achieved in large part due to the tremendous political will demonstrated by ICAO's Member States in the wake of the 9/11 attacks to strengthen their border security systems.

Prior to 9/11, facilitation-based rationales had been the prime movers of the MRTD Programme. These priorities helped the Programme to move forward some excellent initiatives, lead the development of exciting new technologies and make great progress toward the global MRTD system which was achieved as of ICAO's April 2010 deadline. What changed on 11 September 2001, was that many States and air transport stakeholders also began to realize that the new technologies and standards that were being developed in the MRTD realm could also serve as components in a more robust and globally-integrated anti-terrorism regime.

The tenth anniversary of 9/11 provides those of us in the aviation facilitation and security fields with a profound reminder that terrorism remains a serious and ongoing threat to aviation and national security within all of ICAO's Member States. As a result, this year's Seventh Symposium will be focusing more than any previous MRTD event on the role of MRTDs and related border control advances in combatting and preventing terrorism and all forms of trans-border crime. The speakers and presentations will explore and clarify the emerging and more comprehensive links between recent MRTD-led facilitation advances and the broader aviation security regime.

In addition to traditional aviation security measures such as use of new technologies in passenger and cargo screening, this new and more globally-harmonized security framework is presently being redefined on the basis of more data-intensive cooperation between all levels of national and international law enforcement. These priorities are consistent with the unprecedented ICAO Declaration on Aviation Security, which was unanimously adopted at the 37th Assembly in late 2010.

The 37th Assembly also tasked the MRTD Programme to work on new work items to address new security concerns. One key area of persistent vulnerability in this regard lies in the methods and documents employed by all States to ascertain and confirm the identity of travel document holders. These 'breeder documents', as well as their secure administration within State bureaucracies, have served to make identity management issues one of the prime concerns for MRTD and security stakeholders moving forward and another important topic for this year's Symposium. No MRTD Programme advances will have proven worthwhile from a security standpoint until State systems supporting effective identity establishment and management have been addressed and remedied.

Those of us pursuing this improved aviation security framework would do well to remember the key finding from the *9/11 Commission Report,* which noted that: *"…for terrorists, travel documents are as important as weapons."* The issuance and integrity of travel documents, in addition to border security and identity management advances, today remain an important and integral part of global counter-terrorism capacity-building efforts in furthering the objectives of UN Security Council Resolution 1373.

As aviation security and other anti-terrorism and international law enforcement efforts begin to be harmonized as never before, due in no small part to the work and achievements by all of us who are active in the MRTD field, this year's Symposium promises to provide new ideas to address the challenges and define the solutions that will advance the continuing integration of passenger facilitation and border security for the 21st century. ■

Mark Your Calendar!

Seventh ICAO Symposium on

ICAO MRTDs, Biometrics and Security Standards

12–15 September 2011, ICAO HQ, Montreal, Canada

ICAO will hold its Seventh Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards from 12–15 September 2011. An Exhibition will complement the Symposium and highlight important products and services related to MRTDs, biometric identification and border inspection systems.

The 2011 Symposium follows last year's successful event, attended by approximately 600 participants from national governments, international organizations, companies and institutions. It will be of particular interest to officials of passport and official ID document issuing agencies, immigration, customs, and other border control and security authorities. Officials from airlines and airports involved in passenger service systems, handling of travel documents, facilitation and aviation security would also benefit by attending.

TAG-MRTD/20

7–9 September 2011, ICAO HQ, Montreal, Canada

ICAO's Technical Advisroy Group on Machine Readable Travel Documents (TAG-MRTD) is responsible for the development of specifications for travel documents with the goal of global interoperability. In addition, the TAG-MRTD seeks to advise ICAO on technology issues related to the issuance and use of machine-readable travel documents.

mrtd.icao.int

This glossary is included to assist the reader with terms that may appear within articles in the ICAO *MRTD Report*. This glossary is not intended to be authoritative or definitive.

Anti-scan pattern An image usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the image cannot be distinguished from the remainder of the background security print, but when the original is scanned or photocopied the embedded image becomes visible.

Biographical data (biodata) The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book, or on a travel card or visa.

Biometric A measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrollee.

Biometric data The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

Biometric sample Raw data captured as a discrete unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).

Biometric system An automated system capable of:

1. capturing a biometric sample from an end user for a MRP;
2. extracting biometric data from that biometric sample;
3. comparing that specific biometric data value(s) with that contained in one or more reference templates;
4. deciding how well the data match, i.e. executing a rule-based matching process specific to the requirements of the unambiguous identification and person authentication of the enrollee with respect to the transaction involved; and
5. indicating whether or not an identification or verification of identity has been achieved.

Black-line/white-line design A design made up of fine lines often in the form of a guilloche pattern and sometimes used as a border to a security document. The pattern migrates from a positive to a negative image as it progresses across the page.

Capture The method of taking a biometric sample from the end user.

Certificating authority A body that issues a biometric document and certifies that the data stored on the document are genuine in a way which will enable detection of fraudulent alteration.

Chemical sensitizers Security reagents to guard against attempts at tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.

Comparison The process of comparing a biometric sample with a previously stored reference template or templates. See also "One-to-many" and "One-to-one."

Contactless integrated circuit An electronic microchip coupled to an aerial (antenna) which allows data to be communicated between the chip and an encoding/reading device without the need for a direct electrical connection.

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means.

Database Any storage of biometric templates and related end user information.

Data storage (Storage) A means of storing data on a document such as a MRP. Doc. 9303, Part 1, Volume 2 specifies that the data storage on an ePassport will be on a contactless integrated circuit.

Digital signature A method of securing and validating information by electronic means.

Document blanks A document blank is a travel document that does not contain the biographical data and personalized details of a document holder. Typically, document blanks are the base stock from which personalized travel documents are created.

Duplex design A design made up of an interlocking pattern of small irregular shapes, printed in two or more colours and requiring very close register printing in order to preserve the integrity of the image.

Embedded image An image or information encoded or concealed within a primary visual image.

End user A person who interacts with a biometric system to enroll or have their identity checked.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrollee A human being, i.e. natural person, assigned an MRTD by an issuing State or organization.

ePassport A Machine Readable Passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology, and which conforms to the specifications of Doc. 9303, Part 1.

Extraction The process of converting a cap-tured biometric sample into biometric data so that it can be compared to a reference template.

Failure to acquire The failure of a biometric system to obtain the necessary biometric to enroll a person.

Failure to enroll The failure of a biometric system to enroll a person.

False acceptance When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

False Acceptance Rate (FAR)
The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as FAR = NFA / NIIA or FAR = NFA / NIVA where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts.

False match rate Alternative to "false acceptance rate;" used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection."

False non-match rate Alternative to "false rejection rate;" used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection."

False rejection When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False Rejection Rate (FRR)
The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The false rejection rate may be estimated as follows: FRR = NFR / NEIA or FRR = NFR / NEVA where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrollee identification attempts and NEVA is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of enrollees. The false rejection rate normally excludes "failure to acquire" errors.

Fibres Small, thread-like particles embedded in a substrate during manufacture.

Fluorescent ink Ink containing material that glows when exposed to light at a specific wavelength (usually UV) and that, unlike phosphorescent material, ceases to glow immediately after the illuminating light source has been extinguished.

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.

Front-to-back (see-through) register
A design printed on both sides of the document or an inner page of the document which, when the page is viewed by transmitted light, forms an interlocking image.

Full frontal (facial) image A portrait of the holder of the MRP produced in accordance with the specifications established in Doc. 9303, Part 1, Volume 1, Section IV, 7.

Gallery The database of biometric templates of persons previously enrolled, which may be searched to find a probe.

Global interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all ePassports.

Guilloche design A pattern of continuous fine lines, usually computer generated, and forming a unique image that can only be accurately re-originated by access to the equipment, software and parameters used in creating the original design.

Heat-sealed laminate A laminate designed to be bonded to the biographical data page of a passport book, or to a travel card or visa, by the application of heat and pressure.

Holder A person possessing an ePassport, submitting a biometric sample for verification or identification while claiming a legitimate or false identity. A person who interacts with a biometric system to enroll or have their identity checked.

Identification/Identify The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the ePassport holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with "Verification."

Identifier A unique data string used as a key in the biometric system to name a person's identity and its associated attributes. An example of an identifier would be a passport number.

Identity The collective set of distinct personal and physical features, data and qualities that enable a person to be definitively identified from others. In a biometric system, identity is typically

established when the person is registered in the system through the use of so-called "breeder documents" such as birth certificate and citizenship certificate.

Image A representation of a biometric as typically captured via a video, camera or scanning device. For biometric purposes this is stored in digital form.

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his physical appearance to represent himself as another person for the purpose of using that person's document.

Infrared drop-out ink An ink which forms a visible image when illuminated with light in the visible part of the spectrum and which cannot be detected in the infrared region.

Inspection The act of a State examining an ePassport presented to it by a traveler (the ePassport holder) and verifying its authenticity.

Intaglio A printing process used in the production of security documents in which high printing pressure and special inks are used to create a relief image with tactile feel on the surface of the document.

Issuing State The country writing the biometric to enable a receiving State (which could also be itself) to verify it.

JPEG and JPEG 2000 Standards for the data compression of images, used particularly in the storage of facial images.

Laminate A clear material, which may have security features such as optically variable properties, designed to be securely bonded to the biographical data or other page of the document.

Laser engraving A process whereby images (usually personalized images) are created by "burning" them into the substrate with a laser. The images may consist of both text, portraits and other security features and are of machine readable quality.

Laser-perforation A process whereby images (usually personalized images) are created by perforating the substrate with a laser. The images may consist of both text and portrait images and appear as positive images when viewed in reflected light and as negative images when viewed in transmitted light.

Latent image A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles, most commonly achieved by intaglio printing.

LDS The Logical Data Structure describing how biometric data is to be written to and formatted in ePassports.

Live capture The process of capturing a biometric sample by an interaction between an ePassport holder and a biometric system.

Machine-verifiable biometric feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine.

Match/Matching The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. A decision to accept or reject is then based upon whether this score exceeds the given threshold.

Metallic ink Ink exhibiting a metallic-like appearance.

Metameric inks A pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a mismatch at other wavelengths.

Microprinted text Very small text printed in positive and or negative form, which can only be read with the aid of a magnifying glass.

MRTD Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes.

Multiple biometric The use of more than one biometric.

One-to-a-few A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a "watch list" of persons who warrant detailed identity investigation or are known criminals, terrorists, etc.

One-to-many Synonym for "Identification."

One-to-one Synonym for "Verification."

Operating system A programme which manages the various application programmes used by a computer.

Optically Variable Feature (OVF) An image or feature whose appearance in colour and/or design changes dependent upon the angle of viewing or illumination. Examples are: features including diffraction structures with high resolution (Diffractive Optically Variable Image Device (DOVID), holograms, colour-shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.

Optional data capacity expansion technologies Data storage devices (e.g. integrated circuit chips) that may be added to a travel document to increase the amount of machine readable data stored in the document. See Doc. 9303, Part 1, Volume 2, for guidance on the use of these technologies.

Overlay An ultra-thin film or protective coating that may be applied to the surface of a biographical data or other page of a document in place of a laminate.

Penetrating numbering ink Ink containing a component that penetrates deep into a substrate.

Personalization The process by which the portrait, signature and biographical data are applied to the document.

Phosphorescent ink Ink containing a pigment that glows when exposed to light of a specific wavelength, the reactive glow remaining visible and then decaying after the light source is removed.

Photochromic ink An ink that undergoes a reversible colour change when exposed to UV light.

Photo substitution A type of forgery in which the portrait in a document is substituted for a different one after the document has been issued.

Physical security The range of security measures applied within the production environment to prevent theft and unauthorized access to the process.

PKI The Public Key Infrastructure methodology of enabling detection as to whether data in an ePassport has been tampered with.

Planchettes Small visible (fluorescent) or invisible fluorescent platelets incorporated into a document material at the time of its manufacture.

Probe The biometric template of the enrollee whose identity is sought to be established.

Rainbow (split-duct) printing A technique whereby two or more colours of ink are printed simultaneously by the same unit on a press to create a controlled merging of the colours similar to the effect seen in a rainbow.

Random access A means of storing data whereby specific items of data can be retrieved without the need to sequence through all the stored data.

Reactive inks Inks that contain security reagents to guard against attempts at tampering by chemical erasure (deletion), such that a detectable reaction occurs when bleach and solvents come into contact with the document.

Read range The maximum practical distance between the contactless IC with its antenna and the reading device.

Receiving State The country reading the biometric and wanting to verify it.

Registration The process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Relief (3-D) design (Medallion) A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.

Score A number on a scale from low to high, measuring the success that a biometric probe record (the person being searched for) matches a particular gallery record (a person previously enrolled).

Secondary image A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.

Security thread A thin strip of plastic or other material embedded or partially embedded in the substrate during the paper manufacturing process. The strip may be metallized or partially de-metallized.

Tactile feature A surface feature giving a distinctive "feel" to the document.

Tagged ink Inks containing compounds that are not naturally occurring substances and which can be detected using special equipment.

Template/Reference template Data which represent the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Template size The amount of computer memory taken up by the biometric data.

Thermochromic ink An ink which under-goes a reversible colour change when the printed image is exposed to heat (e.g. body heat).

Threshold A "benchmark" score above which the match between the stored biometric and the person is considered acceptable or below which it is considered unacceptable.

Token image A portrait of the holder of the MRP, typically a full frontal image, which has been adjusted in size to ensure a fixed distance between the eyes. It may also have been slightly rotated to ensure that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the portrait rectangle if this has not been achieved when the original portrait was taken or captured (see Section 2, 13 in this volume of Doc. 9303, Part 1).

UV Ultraviolet light.

UV dull substrate A substrate that exhibits no visibly detectable fluorescence when illuminated with UV light.

Validation The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Variable laser image A feature generated by laser engraving or laser perforation displaying changing information or images dependent upon the viewing angle.

Verification/Verify The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with "Identification."

Watermark A custom design, typically containing tonal gradation, formed in the paper or other substrate during its manufacture, created by the displacement of materials therein, and traditionally viewable by transmitted light.

Wavelet Scalar Quantization A means of compressing data used particularly in relation to the storage of fingerprint images. ■

Enhance your visibility

The world's most trusted MRTD Web site

The **MRTD Partnership Community** is the only globally recognized Web site that can help you reach all of ICAO's Contracting States. Major industry experts in the MRTD, Border Control, Security and Facilitation field use our Web site to deliver their corporate message to key players in the MRTD community worldwide.

For more information on our comprehensive media package and marketing tools, visit us at:

www.icao.int/mrtdc

The best high-tech device for verifying government documents.

Thanks to the KINEGRAM®, the authenticity of government documents can be checked by the naked eye.

OVD Kinegram AG | Zählerweg 12 | CH-6301 Zug | Switzerland
Tel. +41 41 724 47 00 | Fax +41 41 724 49 11 | mail@kinegram.com | www.kinegram.com

KINEGRAM

Always one step ahead – identification systems from G&D

Creating Confidence. G&D is a leading company in smart chip-based solutions for secure ID documents and passports, and boasts in-depth experience in the field of high-security documents. We supply entire nations with passport and border control systems, ID card solutions and have become a trusted adviser and supplier to governments. We also provide customized document features, card operating systems and technology for integrating state-of-the-art security features into ID documents. G&D will find the best solution for your individual needs. We define requirements together with you and offer tailor-made, effectively protected products that meet international standards. ID system implementation by G&D – individual, international and secure. **www.gi-de.com**

Giesecke & Devrient

Creating Confidence.