MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Beyond 2010

ICAO's new Vision 2020 puts State needs at the forefront of a harmonized global regime of integrated and secure identity management and border control

Barry Kefauver, Mauricio Siciliano: The Vision 2020 mission
Robert Mocny: The challenges and success of the US-VISIT programme
Rey Koslowski: The future of global mobility regimes
Mike Smith: Future ICAO/UN CTED counter-terrorism coordination

Also:
Reviewing ICAO's 2010 MRTD deadline requirements and e-Passport definition
Markus Hartmann: e-MRTD project management: Part I of III

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

Secure Document Issuing Solutions

GET. Changing the Face of Passports & IDs around the World

ICAO MRTD REPORT
VOLUME 4, NUMBER 3, 2009

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 Contracting States of ICAO and the international aeronautical and security communities.

Printed by ICAO

Contents

COVER STORY: ICAO'S NEW 2020

SPECIAL SECTION: Defining e-Passports and ICAO's 2010 MRTD deadline

ERRATUM
In the ICAO *MRTD Report*, Volume 2, Number 4, the article attributed to Dr. Uwe Seidel contained several transcription errors that may have misrepresented facts and points that Dr. Seidel had correctly established in his 2008 MRTD Symposium presentation, and on which this article text was based. Anthony Philbin Communications, as editorial supplier to the *MRTD Report*, regrets these errors and has made corrections to the online version available for download on the MRTD Community Web site. We encourage any readers interested in this topic to review the corrected text at **www2.icao.int/en/MRTD2/Pages/PastIssues.aspx** and we apologize to Dr. Seidel for this administrative and editorial oversight.

www.icao.int

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

Member	Nominated by	Member	Nominated by
Mr. R. M. Greenwood	Australia	Ms. A. Offenberger	New Zealand
Mr. G. K. McDonald	Canada	Ms. I.O. Sosina	Nigeria
Ms. Marisol Cabello	Chile	Mr. C. Ferreira Gonçalves	Portugal
Mr. M. Vacek	Czech Republic	Mr. O. Demidov	Russian Federation
Mr. Y. Dumareix	France	Mr. S. Tilling	Sweden
Dr. E. Brauer	Germany	Mr. R. Vanek	Switzerland
Mr. S. Ramachandran	India	Mr. R. Chalmers	United Kingdom
Mr. H. Fukuyaama	Japan	Mr. M. Holly	United States
Ms. E. Gosselink	Netherlands		

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 Commission (EC)
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)

ICAO's Global Presence

Leadership and Vision in Global Civil Aviation

www.icao.int

The International Civil Aviation Organization

Beyond 2010: New challenges for a new decade

The 2010 ICAO MRP implementation deadline represents a first but very essential step in bringing global State travel document systems and technologies more in line with 21st-century border control, facilitation and security objectives.

As ICAO, Contracting States and the industry now begin to look beyond 2010, a new vision has started to emerge of an even more advanced and harmonized border, travel and identity management environment, one that will take full advantage of the latest e-Passport and related technologies while continuing to balance citizen privacy and traveller convenience with broader State security and mobility objectives.

In this special Symposium issue, the *MRTD Report* speaks to experts on the cutting-edge of State biometric implementation, mobility policy and global counter-terrorism activities as ICAO and global stakeholders begin to crystallize this new "Vision 2020"—a programme that will be based on comprehensive consultative frameworks and ensure the primacy of State policy and needs as the basis for future solutions.

Some simply call it a new era in security and identity. To insiders, it has been a long, concerted effort involving dozens of stakeholder and expert groups and a great deal of time, consultation, research and f exibility from every quarter. No matter how one chooses to characterize the new global, secure and integral border control and travel document and identity management environment, however, one thing remains very clear: much still remains to be done.

ICAO's 2010 implementation deadline for Machine Readable Passports *(MRPs, see page 30 for more details)* continues to proceed on track as those remaining States complete the updating of their documents and infrastructures to align with contemporary global objectives.

Simultaneously with these compliance developments, innovative methods for employing newer-generation

▶GOT A TEENAGER? THEN YOU PROBABLY KNOW THIS EXPRESSION.

www.bundesdruckerei.de

SORRY, BUT FOR US IT'S PERFECT.

▶ Please do not smile. Seriously. No smiles please, because the passport with biometric data requires a neutral facial expression. That way the document is safe from forgeries and abuse. Sorry about that – but you probably wanted to look cool anyway. ◀

BUNDESDRUCKEREI
We are family

e-Passport capabilities for additional improvements to facilitation infrastructures, identity confirmation and management systems, as well as related State objectives, continue to emerge at a rapid pace. Many States are now exploiting their MRP upgrade process as an opportunity to leap-frog basic 2010 compliance requirements and implement instead the more technologically-advanced and biometrically-enabled e-Passport. This is being accomplished through a thorough review of identity management systems as a whole and by securing the process of ID issuance—including breeder documents.

It is precisely these nascent e-Passport capabilities, and more specifically the win/win potential they hold for the emergence of a more harmonized, secure, yet still passenger- and citizen-friendly border environment, that have allowed experts and stakeholders in the security and facilitation sectors to begin considering a new set of MRTD goals and objectives for the international aviation, border control and immigration communities. Over the past several months, ICAO and industry experts have begun to frame these new possibilities and the means of achieving them under an approach being termed "Vision 2020".

"The Vision 2020 concept has essentially emerged from an evolutionary process," began Mauricio Siciliano, ICAO MRTD Officer. "In recent meetings, stakeholders and experts have begun to ask questions about how we can further assist States to fulfill their needs after the arrival of next April's MRP deadline. A wide range of suggestions and ideas has begun to be exchanged about the new capabilities now coming on-line and how the MRTD expert and regulator community can help to ensure that these are optimized at every stage to benefit State policy and strategic objectives."

"Vision 2020 has emerged in response to questions that have begun to be posed by stakeholders and experts about how we can further assist States to fulfill their needs after the arrival of next April's MRP deadline. A wide range of suggestions and ideas has begun to be exchanged about the new capabilities now coming on line and how the MRTD expert and regulator community can help to ensure that these are optimized at every stage to benefit State policy and strategic objectives."

Siciliano noted that Vision 2020 would not be a deadline-driven process as has been the case with ICAO's 2010 MRP timetable. That incredible effort on behalf of regulators, standards organizations, vendors and States was a specific objective with clear, minimal requirements, whereas Vision 2020 is more about ongoing consultation and exploration as States plan and implement their future policies and strategies in various fields, such as security, aviation, the environment, the movement of people, economic development, migration and beyond. It will also address how new technologies open up new doors and new opportunities for increased efficiency and harmonization to ultimately fulfill individual and collective State needs.

One worry that has accompanied this f urry of recent technical advancements is that, in some respects, the tail has begun to wag the dog where certain solutions to State identity and border objectives are concerned. Vision 2020 will therefore be clearly focused on establishing the primacy of national policies and needs—ensuring that State concerns continue to guide all future technological developments and implementations.

"Under the premise of Vision 2020, the role of experts and standards setters will be to thoroughly analyze State input and then manage the means by which State needs are addressed by emerging technologies and capabilities," confirmed Barry Kefauver, INSERT CURRENT BARRY TITLE.
"ICAO in this sense remains uniquely positioned as an international governance structure and fulcrum around which these activities should proceed."

Over the past two decades, ICAO has emerged as the only global body capable of providing a comprehensive forum for the complex mix of research, debate and solutions that have informed the recent MRTD evolution and, more importantly, for establishing binding and State-focused international Standards to ensure an effective and harmonized global border security and facilitation environment.

"A number of organizations have come together to help develop the comprehensive MRTD guidelines and standards," added Kefauver, " and these are now helping to manage progress in this area. Although ICAO may be the only body capable of producing binding standards, partners

Regula
Forensic Science Systems

DOCUMENT AUTHENTICITY CONTROL ON OPERATIVE, AUTOMATED, ADVANCED LEVELS

Regula is an original developer of equipment for document examination, automatic reading and verification of travel IDs and special equipment for law enforcement

- compact magnifiers for operative document check up

- document readers for automatic processing and verification of travel documents

- full-page mobile document reader

- database of travel documents

INTEGRATED SOLUTIONS WITH HARDWARE, SOFTWARE AND DATABASE COMPONENTS

www.regulaforensics.com

“Vision 2020 is really about providing a framework whereby we can leverage the momentum that has been generated by the creation of Doc. 9303 and the 2010 deadline, continue to ascertain and highlight State needs, and finally to further leverage ICAO’s unique role on the international stage.”

such as the International Standards Organization (ISO), the International Organization for Migration (IOM), INTERPOL, the UN Counter-Terrorism Executive Directorate (see interview page 16), the Inter-American Committee Against Terrorism of the Organization of American States, the Organization of Security and Co-operation in Europe and several others have provided invaluable input and increasingly coordinated outreach assistance. The work of all these groups, however, requires a binding international document to contain and focus their activities and that document is ICAO’s Document 9303.”

Annex 9 (Facilitation) to the Chicago Convention and ICAO Document 9303—*Machine Readable Travel Documents*, provides the basic framework by which present and future developments can proceed and represents a profound accomplishment in this respect. As new technologies and applications of these technologies continues to proceed so rapidly, however, the process of updating Annex 9 to State needs and requirements, not to mention adapting Doc 9303 to preserve its relevance and effectiveness, will require maintaining the significant momentum and coordination that allowed 9303 to be created in the first place.

“Vision 2020 is really about providing a framework whereby we can leverage the impetus that has been generated by the creation of Doc. 9303 and the 2010 deadline, continue to ascertain and highlight State needs, and finally to further affirm ICAO’s unique role on the international stage,” elaborated Kefauver.

Together these efforts represent one of the best examples yet of how the world’s various States and Regions can come together in this new century, through a unique mix of partnerships and cooperative frameworks, and produce harmonized, effective results to the benefit of governments and the citizens they serve.

“ICAO may need to adjust some its governance in this area, and possibly adapt its Working and Advisory Groups as the policy environment requires, but its fundamental responsibility as the custodian of State interests and generator of binding Standards is what will ultimately enable all of these efforts to achieve fruition,” Kefauver concluded. ■

secunet GRT platinum edition

GOLD GOES PLATINUM

New edition of Golden Reader Tool from October 1st 2009

Better than gold – secunet presents the new platinum version of the well-proven Golden Reader Tool. This new extended version is totally flexible, modular and innovative. The new approach allows the usage of biometrics as well as further electronic documents beside epassports. This makes it the best guarantee for protecting identities in times of globalisation where eID-documents are becoming increasingly important and widespread.

For more details see:

www.secunet.com/GRTplatinum

Key benefits of the new platinum edition:

- Commercially available
- Supports biometrics via BioAPI/biomiddle
- Supports all EAC versions
- Flexible in terms of features, design and use cases
- Internationally recognised as the reference implementation

Golden Reader Tool is a joint project of the German Federal Office for Information Security and secunet.

Benchmarking biometric success: The US-VISIT programme

The 2001 terrorist attacks on the United States of America were in many respects the 'prime movers' of recent advances in aviation and border security. Exit and entry concerns were high on the list of U.S. priorities immediately following 9/11 and, as described here by US-VISIT Director Robert Mocny, the programme that his country has implemented to address entry/exit security and identity challenges continues to provide global leadership in the implementation of advanced border control systems and technologies.

Robert A. Mocny leads the U.S. Department of Homeland Security's (DHS) US-VISIT travellers, serving first as its deputy director and then as acting director before his appointment to director in April 2007. Prior to his role with US-VISIT he served in senior positions related to U.S. immigration policy and operations at the former Immigration and Naturalization Service (INS), including as director of the Entry/Exit Project, acting assistant commissioner and assistant chief inspector.

ICAO *MRTD Report*: When was the decision made to use biometrics for the US-VISIT programme?

Robert Mocny: On April 29, 2003, during a speech at the National Press Club, then U.S. Department of Homeland Security Secretary Tom Ridge announced that US-VISIT would use biometrics to verify the identities of international travellers to comply with a congressional mandate for an automated entry exit system. The Secretary had brought two speeches to the event—one that announced a biometric future and one that didn't. When my colleagues and I heard the speech and the Secretary's promise that, not only would we implement a biometric solution, but that in so-doing we'd also beat the congressional deadline associated with the new mandate by a full year, we realized we had a lot of work ahead of us.

What were the main qualities being sought for the new system and what supplier was eventually selected?

When US-VISIT began, the technology (hardware and software) to efficiently collect 10 fingerprints in a port environment did not yet exist. We began by employing scanners that could collect a single fingerprint at a time and implemented a policy to collect two index fingerprints from international programme when they applied for visas and arrived in the United States. In the meantime, we worked with the private sector and other Federal agencies—including the Departments of State, Justice, Defense, and Commerce—to develop requirements for 10-fingerprint scanners that would meet all of our needs.

Those requirements called for scanners that were small, lightweight, f exible in different operating environments, compatible with existing hardware, and capable of collecting 10 fingerprints in either a f at or rolled fashion. More precisely, the scanners we were looking for had to be less than 5 pounds and no larger than 6 inches by 6 inches by 6 inches. They had to operate in temperatures ranging from 35–120°F, or 2–49°C. They also had to operate in direct sunlight and extreme humidity. In 2008, Crossmatch and Identix were chosen to supply these 10-fingerprint scanners for US-VISIT.

What type of database network provides the foundation for the US-VISIT programme?

US-VISIT is actually an over-arching programme that refers to a 'system of systems', if you would. The Arrival and Departure Information System (ADIS) houses all the primary biographic

information, including visa classifications, how long a person is permitted to stay, etc. ADIS also includes a Fingerprint Identification Number (FIN) field which links to US-VISIT's Automated Biometric Identification System, or IDENT.

ADIS additionally links to other domestic systems, including the main Citizenship and Immigration System (CLAIMS3), as well as the Student and Exchange Visitor Program (SEVIS). Obviously, the programme's data is also linked to a significant number of law enforcement and security agencies, both domestic and international, such as INTERPOL.

How has the deployment of the proposed biometric exit data collection system proceeded to this point?

US-VISIT has taken an incremental approach to deploying its biometric identification capabilities. We started by deploying biometric entry procedures to airports and seaports, then expanded these to land border ports of entry—all using existing infrastructure.

Unlike entry, there is no pre-existing exit infrastructure that we can leverage. So, while deploying biometrics for arriving travellers, we also tested different ways to apply biometrics to an automated exit system. Most recently, we tested biometric exit collection procedures for non-U.S. citizens departing the United States by air. From these tests, we have identified technology that works in the airport and seaport environments and we're now fine-tuning a process to collect biometrics from travellers departing the United States in these environments.

Biometrically recording non-U.S. citizen departures at U.S. land border ports of entry poses significantly greater challenges. A one-size-fits-all solution will not work due to variations in infrastructure, environment, and traffic volume from port to port. At this stage we have examined several options for the land border environment and recently provided a report to Secretary Napolitano outlining the opportunities and challenges of a land border exit solution.

"It was critical in the early going to address the establishment of public trust not only in the technology, but also in the programme itself in order to ensure public acceptance."

A DAY IN THE LIFE OF US-VISIT	
97,000	International visitors' identities enrolled or verified at ports of entry for **U.S. Customs and Border Protection and U.S. Border Patrol**
11,000	Benefit applicants' identities enrolled or verified for **U.S. Citizenship and Immigration Services**
3,500	Immigration violators' identities enrolled or verified for **U.S. Immigration and Customs Enforcement**
9	Illegal migrants' identities enrolled or verified for **U.S. Coast Guard** at sea
26,800	Visa applicants' identities enrolled or verified for **U.S. Department of State**
7,000	Fingerprints verified as part of investigation support **across agencies**, helping to solve crimes, identify John Does, and support terrorist investigations
500	Identities of criminals, immigration violators, and known or suspected terrorists enrolled or verified for **DOD and intelligence agencies**.

*Current capacity of 250,000 transactions a day

What were some of the main challenges for US-VISIT and how have these been addressed to this point?

When US-VISIT began in 2004, it was the first large-scale biometrics programme of its kind. There was definitely some early skepticism that the programme would be able to meet its fundamental goals of facilitating legitimate travel, protecting privacy, enhancing security, and ensuring the integrity of our immigration system.

Biometrics in those days was still a nascent technology outside of criminal applications. The public's unfamiliarity with the technology therefore held the potential for misperceptions and misplaced fear. It was critical in the early going to address the establishment of public trust not only in the technology, but also in the programme itself in order to ensure public acceptance.

To build that trust, US-VISIT ensured from the outset that the public knew what information we collected, why we were collecting it, and how we were using and protecting it. We launched a global public education and information effort to ensure that anyone touched by US-VISIT requirements understood how the programme worked and how it affected them. This international outreach effort essentially meant engaging a broad range of stakeholders in two-way dialogues. Working with foreign governments, the travel and tourism industry, public interest organizations, and taking advantage of public and online forums, we identified challenges and issues and in some cases even amended US-VISIT's planning in response to stakeholder input. To cite one example, US-VISIT waited to begin collecting biometrics from international travellers at airports and seaports until January 5, 2004, rather than December 31, 2003, primarily because international travel and tourism organizations expressed concern about starting a new biometric collection programme during the busy holiday season.

Our continued commitment to international public education and global outreach has resulted in continuing support and validation of the programme by travellers, foreign government partners, and international industry leaders.

What are some of the statistics associated with your programme's success up until now?

Since US-VISIT began in 2004, the programme has processed more than 100 million international travellers without affecting wait times at our ports of entry. This is impressive, especially when you look at the number of international travellers whose identities are verified on any given day through US-VISIT.

Using biometrics alone at U.S. ports of entry, DHS has stopped more than 8,800 criminals, immigration violators, and known or suspected terrorists from entering the country. Behind those statistics are significant security successes, such as when one particular individual applied to enter the United States at a U.S. port of entry using an alias and false identification. During the biometric check by U.S. Customs and Border Protection officers, the person's fingerprints matched those of someone on the US-VISIT watchlist. Through biometric matching we were able to see that this person trying to enter our country had multiple warrants against him, including a warrant for murder and obstruction of justice, and that he had been using 22 aliases and 9 different dates of birth to avoid detection by authorities.

Are other countries planning similar systems coming to the United States for advice and assistance in this regard?

In the last few years several countries—some of which even initially opposed US-VISIT—have begun developing their own biometric identity management systems. Today, many countries are approaching US-VISIT as an early adopter of biometric technology in order to discuss our lessons learned as they develop their own systems.

US-VISIT currently shares its best practices and is working to develop common biometric standards, including privacy guidelines, which will improve security and facilitate travel worldwide. In fact, US-VISIT has seconded experts to provide technical support to the United Kingdom and Australia as those nations develop biometric identity management capabilities similar to those of the United States. US-VISIT has also provided direct technical assistance to several other countries engaged in planning or deploying biometric identity systems and has participated in several live tests of e-Passport documents. ■

Towards a more encompassing regime of global mobility

The number of international regimes has increased greatly over the past few decades in many areas, but international cooperation among States to regulate international migration has been limited to the extent that there is still no regime in this domain. As analysts and policy-makers now begin to think about international migration as a subset of all movements of people across international borders, Dr. Rey Koslowski, one of the world's foremost experts in the field and leader of the Global Mobility Regimes Project (www.globalmobility.info), notes that the possibilities for meaningful cooperation between States expands significantly.

In this special contribution to the *MRTD Report*'s Vision 2020 review, Koslowski describes why cooperation on international migration should be broadened to encompass the more inclusive phenomenon he calls *global mobility*, and on how the emerging and highly-under-appreciated international travel regime that ICAO continues to facilitate and enhance could serve as an important enabler in the establishment of more extensive cooperation in this area.

In contrast to the UN definition of migrants as those who live outside of their state of nationality or birth for more than one year, the term *global mobility* refers to movements of people across international borders for any length of time or purpose. In addition to the world's estimated 191 million migrants, there are billions of border crossings by tourists, business people and students who travel internationally for stays of less than a year.

To investigate this issue more comprehensively, Dr. Rey Koslowski, one of the world's foremost experts in migration- and mobility-related issues, established the Global Mobility Regimes Project in order to examine the existing set of interacting global mobility regimes: the established international refugee regime; an emerging international travel regime that ICAO's MRTD activities continue to nurture, and a non-existent but potential international labor migration regime.

"Although the issue areas of these three regimes overlap somewhat, leading occasionally to misunderstandings and policymaking at cross purposes," Koslowski noted, "potential issue linkages can also be leveraged for widening the scope of international cooperation, perhaps even far enough to allow for the development of an international labor migration regime."

The International Labour Organization (ILO) has long had conventions on the rights of migrant workers; however these are largely undersubscribed by UN member states, especially by migration destination states. The International Organization for Migration (IOM) has also expanded in recent decades beyond its historic role in the postwar repatriation of refugees and towards a more general mission of migration management, but although its membership has increased it remains outside of the UN system and has largely been relegated to service provision by Member States on a project-by-project basis.

"As policymakers have now begun to recognize that economic development in many source countries is facilitated by migrant remittances, and that destination countries are becoming increasingly dependent on immigrants to care for and financially support ageing populations, academics and policy analysts alike have recently begun to focus more of their attention on the development of a functional migration regime," Koslowski remarked. "Existing agreements in this area do not currently involve significant commitments on the part of a majority of the world's States to accept labour migration, nor do they add up to a regime that could

facilitate and govern the international movement of labour in a manner similar to how the General Agreement on Tariffs and Trade (GATT) currently provides for trade-related matters between States."

Given that contemporary migration often begins as tourism, study or temporary work abroad, global mobility is a more all inclusive category for understanding the dynamics of international migration and the potential for its regulation by States. Expanding the issue area of consideration from international migration to global mobility also widens the scope of regime analysis to include international cooperation on international travel in general and the activities of the international organizations such as ICAO that are concerned with it.

From a border security standpoint, the ever-increasing number of international passengers is a challenge to State officials who attempt to identify dangerous individuals within the f ows of legitimate travellers. This includes the 19 hijackers who attacked the World Trade Center and the Pentagon in 2001, 17 of whom entered on tourist visas, one on a business visa and one on a student visa. International cooperation on migration for the sake of economic considerations may have languished, but post 9/11 security concerns have re-invigorated international cooperation on mobility factors that encompass both migration- and travel-related issues.

"Existing agreements in this area do not currently involve significant commitments on the part of a majority of the world's States to accept labour migration, nor do they add up to a regime that could facilitate and govern the international movement of labour..."

Expanding the scope of international cooperation from international migration to global mobility should provide opportunities for linking cooperation on international travel to international labour migration. By increasing the share of international migration that is orderly, properly-documented with ICAO-compliant travel identity instruments, pre-screened and generated through ports of entry rather than around them, an international migration regime should help border authorities to more effectively focus their limited resources

on travellers and visitors that potentially pose the greatest security risks.

Since the legislatures and publics of many major migration destination countries are very interested in maintaining global mobility in support of ongoing business travel and tourism, while at the same time increasing security, cooperation on secure international travel may also serve as a stepping stone towards broader cooperation on international migration in general.

“The travel regime that is emerging at present, supported very strongly by the important work that ICAO has been achieving through its MRTD and e-Passport deadlines and outreach, is fundamental to much of this discussion,” Koslowski remarked. “I think it’s imperative at this stage, however, that these efforts now begin to expand beyond the document itself in order that we might begin to see a level of standardization for the breeder documents that are used to establish identity and legal status in the first place. In the United States alone we currently have more than 6,000 separate agencies that are authorized to issue birth certificates, while elsewhere UNICEF has now begun to call for birth certificates for all children. It estimates that 50 million of the world’s children under the age of five were not registered in any way at birth.”

Koslowski highlighted that ICAO would potentially be well-suited to leverage its existing work in travel documents and to assume a leadership role in highlighting the breeder document issue and engaging related international organizations to begin to address it.

“There is not only an obvious security component to this issue but a development and refugee factor as well,” Koslowski concluded. “Far fewer individuals are able to f y internationally using fraudulent travel documents today due to the work of ICAO and others in this area, but similarly, far fewer people who face violence and persecution by their governments are able to travel to countries where they could apply for asylum and receive protection as refugees.

More thought and more cooperation is needed to find appropriate solutions but I am confident that an improved consciousness of these issues is emerging and that ICAO and other international organizations will help us to achieve the more comprehensive mobility regime that the world now needs.” ■

Enhancing cooperation on security: ICAO and the UN CTED

Global security and related counter-terrorism activities are an important component of the ongoing progress being made in the implementation of MRTDs and newer-generation biometric identity documents. In this exclusive interview for the *MRTD Report*, Mike Smith, Executive Director of the UN counter-terrorism Executive Directorate, describes how ICAO's work to advance MRTD and e-MRTD implementation forms a crucial component of his group's broader global efforts to continue to minimize terrorist activity in the coming decades.

Mike Smith assumed the position of Executive Director of the UN Counter-Terrorism Executive Directorate on 19 November 2007. Prior to that he was Australia's Ambassador for Counter-Terrorism.

Smith served as Australian Permanent Representative to the UN at Geneva and Ambassador to the Conference on Disarmament between 2002 and May 2006. In 2004, he was, concurrently with his other responsibilities, Chairman of the UN Commission on Human Rights.

ICAO *MRTD Report*: Explain brief y the history of the UN Counter-Terrorism Executive Directorate (UN CTED) and it's primary mandate.

Mike Smith: The UN counter-terrorism Committee (UN CTC) was established in *UN Security Council* Resolution 1373 adopted approximately two weeks after 9/11. Thirteen-seventy-three remains one of the strongest resolutions that the Security Council has ever passed and it is mandatory for all Members of the United Nations. It requires, inter alia, all States to criminalize terrorism, bring terrorists to justice domestically and internationally, prevent terrorists from crossing borders, deny financial resources to terrorists and to submit reports regarding the status of their anti-terrorism activities.

Very quickly after its inception, the CTC began to receive State counter-terrorism status/implementation reports—so many in fact that they soon became overwhelmed by the amount of material they were receiving. It decided to establish a special political mission, or secretariat group, to provide needed support and that's how the Counter-Terrorism Executive Directorate I now head-up came into being, circa 2004/05.

What types of activities has the CTED been involved in since its inception?

Initially we analyzed the reports provided by States and then suggested questions that the CTC should ask those States based on any gaps in the information provided or other shortcomings that were identified. In this manner a type of dialogue was established early-on between the UN's 192 States and the CTC, with the CTED acting as an intermediary.

Since then, however, our modus operandi has changed significantly. Currently we prepare for every State a 'Preliminary Implementation Assessment' (PIA), basically an analysis of their implementation of Resolution 1373 in a standardized format based on information gathered in our early reports. Once a State's PIA is adopted by the CTC it is sent to the country for comment and updating. The process of managing the PIAs based on ongoing State updates, as well as maintaining a very large database of all the information related to this process, has become one important part of the CTED's work.

What about CTED's potential as a resource for States to more effectively share their counter-terrorism knowledge?

CTED produces what is called the Global Implementation Survey to provide a snapshot of how the international community is doing collectively on counter-terrorism. This divides the world into 15 regions and looks at what the particular CT challenges in each one are and makes recommendations on what issues need to be addressed most urgently.

Does the CTED also conduct outreach activities to compliment its PIA and Survey programmes?

Certainly. We often visit countries and conduct more localized and in-depth assessments of their implementation levels with respect to Resolution 1373. Originally, countries were chosen on the basis of a combination of the extent of the

threat that they faced and the CTC's sense that there could be gaps in their CT defences. Today we are less targeted regarding which countries we visit, mainly because it's become apparent over time that even high capacity States that look good on paper face challenges in implementing some areas of Resolution 1373. By visiting a broader range of countries we're also able to develop a much more nuanced understanding of how counter-terrorism strategies are evolving.

How does cooperation with ICAO or other organizations assist you in this respect?

We cooperate closely with multilateral technical, regional and sub-regional organizations in as much as they act as force multipliers in our work of promoting good counter-terrorism practice. When we conduct an assessment mission we will always invite organizations such as Interpol, ICAO, the World Customs Organization, the International Maritime Organization (if the host State has a maritime border), the UN Office of Drugs and Crime, the World Bank on occasion, and very often a regional organization. When we go into these countries we operate as a team with the experts from these partners able to make assessments in their fields of expertise that we couldn't hope to make on our own with same degree of credibility.

Is this similarly helpful for the partnering organizations?

Absolutely. From their standpoint our missions provide them with an opportunity to move new or existing concerns forward by having them registered at a higher political level. Simply put, when you're part of a process that has the weight of the UN Security Council behind it the political attention in the country visited is elevated to the Ministerial or sometimes the Presidential level, which can mean action being initiated on an issue of particular interest to the international organization concerned that might not otherwise have happened.

Let's look at the partnership with ICAO more specifically for a moment. What does the CTED gain most from this relationship?

Notwithstanding the fact that ICAO's responsibilities only comprise one element in the spectrum of counter-terrorism fields that we're interested in, it's one of our closest relationships. What are probably most valuable for us are the Standards that ICAO has developed with respect to overall aviation and travel document security. The ICAO Standards are the result of processes and intellectual input that have taken place over decades and they are indispensable to us in assessing a country's performance in these fields. Secondly, we benefit from ICAO's expertise on our missions—either directly through the presence of an

EDAPS Consortium
is rising star of Secure Identification industry

EDAPS
CONSORTIUM

Water - flows, wind - blows, fire - burns, EDAPS delivers results

EDAPS Consortium - ID Solutions

EDAPS Consortium is successfully introducing its advanced technology in secure printing, informational, biometric and holographic technologies in Ukrainian & International markets.

OUR PRODUCTS:

- e-Passports
- Passports
- National Registry Systems
- National ID Cards
- Driving licences
- Vehicle registration certificates
- Tax stamps & control stamps

OUR SERVICES:

- System integration
- Turn-key Global infrastructure solutions
- Data enrollment & management
- Security design
- Document production & personalization
- Consultancy & project management
- Customer training

SECURITY ELEMENTS:

- Optical security features
- Security inks
- Microtext
- Laser engraving
- Laser perforating
- Holographic secure elements

EDAPS
CONSORTIUM

EDAPS Consortium, 64 Lenin Str.
Kyiv, Ukraine 02088

Tel. +38044 5612590
Fax. +38044 5612585

edaps@edaps.biz
www.edaps.biz

“CTED views ICAO’s April 2010 deadline as a very useful motivational device to encourage early action in this area. We’ve been working to raise the profile of this issue, both in the States we visit and with donors.”

expert, or indirectly when ICAO seeks a waiver from the relevant State that permits CTED to access recently-completed ICAO security audits. These audits are incredibly comprehensive and contain far more information than we could ever hope to assemble on our own.

What role has ICAO been playing more specifically on the MRTD front?

CTED is very aware of the important MRTD work that ICAO has been engaged in and of the April 2010 deadline for all countries to be issuing MRTDs. We view the latter as a very useful motivational device to encourage early action in this area and have therefore been working to raise the profile of this issue, both in the States we visit and with donors.

We’ve recently completed a couple of joint MRTD workshops with ICAO, including one held in Abuja this past April, to promote awareness of this issue within regions that may be lagging behind somewhat in their MRTD issuance efforts and to help the countries concerned address the problem.

Do you see this relationship with ICAO evolving over time?

I think this is going to be a continuing relationship of enormous importance. We will be looking at ICAO to lead the way in terms of fine-tuning technical standards to strengthen security levels affecting everything from travel documents to airports and aircraft. These are areas where CTED doesn’t have the expertise, the resources or the time to move those issues forward as effectively as ICAO can and we’ll therefore be relying on and encouraging it in whatever way we can to continue that important work. ■

UNITED NATIONS GLOBAL COUNTER-TERRORISM STRATEGY

- Improving the coherence and efficiency of counter-terrorism technical assistance delivery so that all States can play their part effectively.
- Voluntarily putting in place systems of assistance that would address the needs of victims of terrorism and their families.
- Addressing the threat of bioterrorism by establishing a single comprehensive database on biological incidents, focusing on improving States’ public health systems, and acknowledging the need to bring together major stakeholders to ensure that biotechnology’s advances are not used for terrorist or other criminal purposes but for the public good.
- Involving civil society, regional and sub-regional organizations in the fight against terrorism and developing partnerships with the private sector to prevent terrorist attacks on particularly vulnerable targets.
- Exploring innovative means to address the growing threat of terrorist use of the Internet.
- Modernizing border and customs controls systems, and improving the security of travel documents, to prevent terrorist travel and the movement of illicit materials.
- Enhancing cooperation to combat money laundering and the financing of terrorism.

The UN clearly affirms that terrorism cannot and should not be associated with any religion, nationality, civilization or ethnic group. It also reaffirms the responsibility of States to deny financial and operational safe havens to terrorists and to prevent terrorists from abusing the system of political asylum, bringing them to justice on the principle of extradite or prosecute.

For more information please visit:

www.un.org/terrorism/strategy

Implementing e-MRTD

Part I: Initiating and planning

Before evaluating vendor e-MRTD solutions, States need to concentrate on evaluating the specific national requirements with which any proposed technologies or processes will need to comply.

In this first of three exclusive articles covering the six steps required to successfully manage an e-MRTD project, Markus Hartmann, of HJP Consulting GmbH, highlights the planning and prioritization activities that State officials will need to engage in to fully benefit from their new e-MRTD systems.

A State Head of Immigration once asked me, very directly: "Why do we have the chip in our e-Passport?" It's the type of query I always hope to hear from an e-MRTD decision maker, primarily because it is the *central* question for issuing authorities when they're defining the requirements of a new e-MRTD issuance system.

What was noteworthy in this particular instance, however, was that the government official hadn't put the question to me during the planning stages of his new e-MRTD project—he raised it six months *after* his State's new system had already been launched. The story highlights how the efforts required to effectively plan and manage complex e-MRTD

projects, harmonizing them with actual State requirements, can often find themselves being ignored due to the 'dazzle' of more technology-driven considerations.

To help other States avoid getting similarly distracted from their priorities, the following article has been produced as the first in a series of three for the ICAO *MRTD Report* which together will provide government decision makers with a comprehensive overview of the key steps that should be adhered to in order to successfully manage an e-MRTD project. In addition to *Part I: Initiating and planning*, future articles will also focus on *Procuring and implementing* as well as *Approving and operating*.

Within each contribution to this series, the authors will not only point out where governments should focus their attention; they will also highlight related guidelines provided from bodies such as the ICAO Implementation and Capacity Building Working Group (ICBWG) which are intended to support governments in current and future developments of this kind.

Initiating your e-MRTD project: How to get started

At first glance, initiating an e-MRTD can appear to be rather simple. Very often, external factors will have pushed governments to begin improving their travel document infrastructures, such as a visa waiver status being reconsidered or an increasing incidence of fraud (with respect to an existing document) causing difficulties with visa issuing authorities from foreign States.

In cases involving a proposed major change in travel or identity document infrastructure, for instance if an upgrade to e-MRTD capability is being planned, the heterogeneous interests of multiple stakeholders have to be addressed and managed.

The project charter empowers the project owner

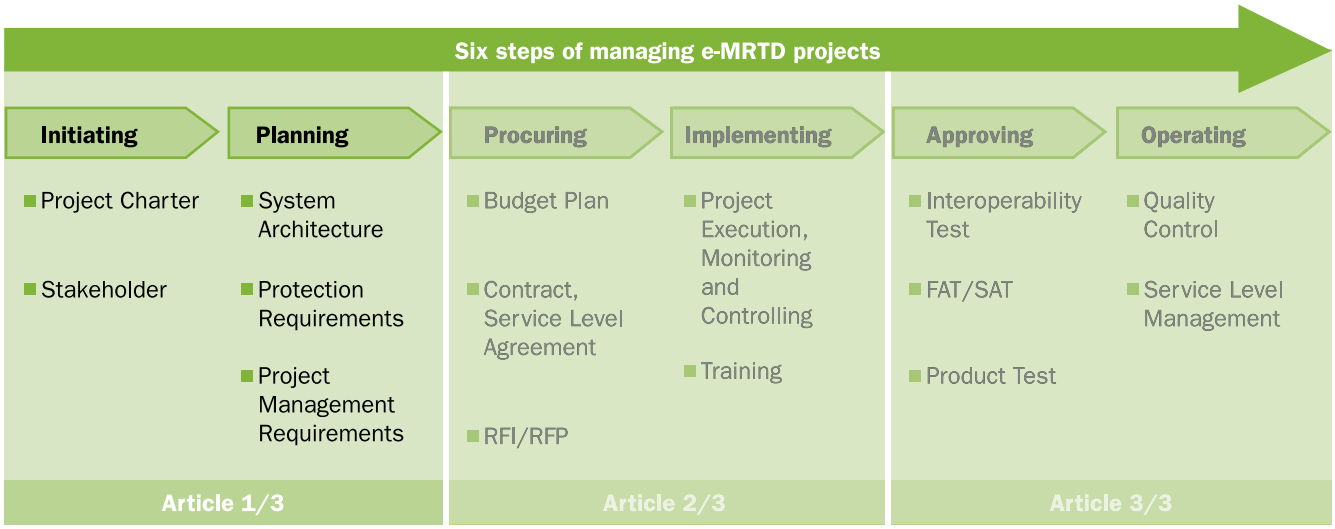
Key to any project's success is a situation whereby the assigned project manager is fully empowered by the project sponsor. The sponsor, meanwhile, who could be an individual, a steering committee, etc., should be minimally authorized to a level that allows them to control the funding for the project. In a project's charter, both the measurable project objectives and the means available to fulfil stakeholder expectations should be fully documented. A lack of authorization for the project manager often leads to a very slow decision making process.

All stakeholders must be identified

All stakeholders need to be considered when initiating an e-MRTD project. Said stakeholders are made up not only of the people or organizations that are directly involved, such as the issuing authorities, but include as well other government departments or ministries, the travelling and non-travelling public and even the press.

Very often, parties who fear any negative impact on their activities or status quo can become critical impediments as the project seeks to move forward. Several projects in

Figure 1: The six steps to successfully managing an e-MRTD project*



*This phase model has been adapted from the project management methodology of the *Project Management Body of Knowledge (PMBOK®) Guide*, developed by PMI®. The graphic above does not show the actual PMI phase model, but rather the phases and work packages of particular importance for e-MRTD projects—which this article series will focus on. Any other professional project management methodology may also be applicable.

Europe, for example, are currently facing significant public resistance related to data protection issues. In developing countries, meanwhile, the public seems more concerned about the possibilities of increasing passport prices and longer document delivery delays.

During the initial phases it is essential to identify as many stakeholders as possible, as well as strategies for establishing clear lines of communication with each throughout the project.

Planning: What will we need?

Many so-called 'requirements' are often expressed at a very early stage in a project's planning process, such as: *"We wish to use a 72 kilobyte RFID chip in our new e-Passport"* or *"We want to centralize our e-Passport personalization process."* At the same time, stakeholders can find it difficult to explain why these types of arbitrary conclusions may have been arrived at before any real analysis has been completed.

It is a State's sole responsibility to clearly define the requirements of their e-MRTD project. It is the vendors' responsibility to deliver a harmonized solution which meets these requirements as specified. These roles and responsibilities should be clearly understood and should not be subject to subtle or overt transformations as the project continues to its completion.

In every case it is essential that respective project managers assemble all stakeholder requirements and consolidate them into a single, comprehensive list. This activity represents an important step in the project process known as *scope management.*

Collect sound requirements

Even if all stakeholders believe that they understand exactly how their MRTD issuance system works, it is generally well worth the effort to perform a thorough re-assessment of the processes and technologies in place. In order to comprehensively analyze the baseline situation, all levels of staff hierarchy should be interviewed and processes should be documented by descriptions, photographs and video if possible. These documents will serve as a proof-of-evidence in the decision making processes that will ensue.

It is recommended that the project manager prepare a checklist of all subjects to be addressed during the preliminary assessment, including a set of questions covering all aspects of the system. The ICAO Implementation and Capacity Building Working Group (ICBWG) is currently in the process of

ASSESSMENT TOPICS AS RECOMMENDED BY ICAO'S GUIDE FOR ASSESSING SECURITY STANDARDS FOR HANDLING AND ISSUANCE OF TRAVEL DOCUMENTS

1. Travel Document Issuing Authority—Organizational Structure, Internal Security and General Security Practices.
2. Application Processes.
3. Entitlement Processes.
4. Treatment of Materials and Blank Books.
5. Personalization and Delivery.
6. Document Security.
7. Facility Security.
8. Information Technology Security.
9. Personnel and Internal Integrity Lost and Stolen Travel Documents.
10. Overseas Issuance.
11. National and International Stakeholders.

developing the Organization's *Guide for Assessing Security Standards for Handling and Issuance of Travel Documents*, which includes precisely this type of assessment, as shown above.

The ICAO Guide includes recommendations of best practices, such as references to the latest Standards issued by ICAO and other relevant organizations. This enables the project team to identify weaknesses in the current processes and technologies in place. It is also recommended to run the assessment with the help of external advisers who can share their experiences of other States' issuance systems. The adviser should not be biased to any third party and by no means should potential vendors be involved in the assessment.

In order to fully benefit from the assessment results within the planning process, it is essential to structure the report so that it conforms to the methodology used to design the future system. In general, three categories of requirements need to be distinguished:

- The requirements for the **system architecture** cover all aspects of how the system shall function.
- The **protection** requirements cover all risks that might compromise the system and define appropriate security objectives for the system.
- Finally the **project management plan** covers all expectations and constraints related to organizing and running the process.

The system architecture is the preview to the solution

Implementing an e-MRTD issuance system can be as complex as building an airport. There are multiple functions that the system has to fulfill and it needs to be upgradeable for future extensions. Many details need to be specified before the vendor can start building it and, in order to obtain an overview of the eventual system, it is recommended that a model of the system architecture be generated—very similar to architectural models prepared for building projects.

This system architecture model should become the underlying guideline for the requirements collection process. It should be comprehensive and able to generate easy-to-understand diagrams containing all system components and their respective interfaces. Figure 3 *(page 26)* shows an example of one such model.

There are many different methodologies available within the IT sector for facilitating the modelling of complex IT infrastructures, such as Zachman, The Open Group Architecture Framework (TOGAF) or Reference Model of Open Distributed Processing (RM-ODP). HJP has so far had very good experience with RM-ODP. It follows the ISO/IEC 10746 Standard and is therefore available to everybody virtually free of charge. The model distinguishes between five different viewpoints: the enterprise view; the computational view; the information view; the engineering view; and the technology view. All views cover different type of requirements, as shown in Figure 4 (*page 28).*

The number of single requirements collected for an e-MRTD issuance system can easily accumulate to a number in the

multiple thousands. Moreover, each of these requirements can inf uence the performance of others. The result is a complex matrix of requirements, dependencies, constraints and assumptions. It is recommended therefore that a professional requirements management software tool be employed to administer these requirements. Requirements management tools help the project manager to identify the impact to the different system components in case of any kind of change.

The modelling of the system architecture therefore provides the project team and all stakeholders with a virtual preview of their final solution. Once a comprehensive model has been completed, the future decision making process will be purely based on requirements and much less susceptible to inf uences from vendor-driven technology needs.

The protection requirements set the height of your fence

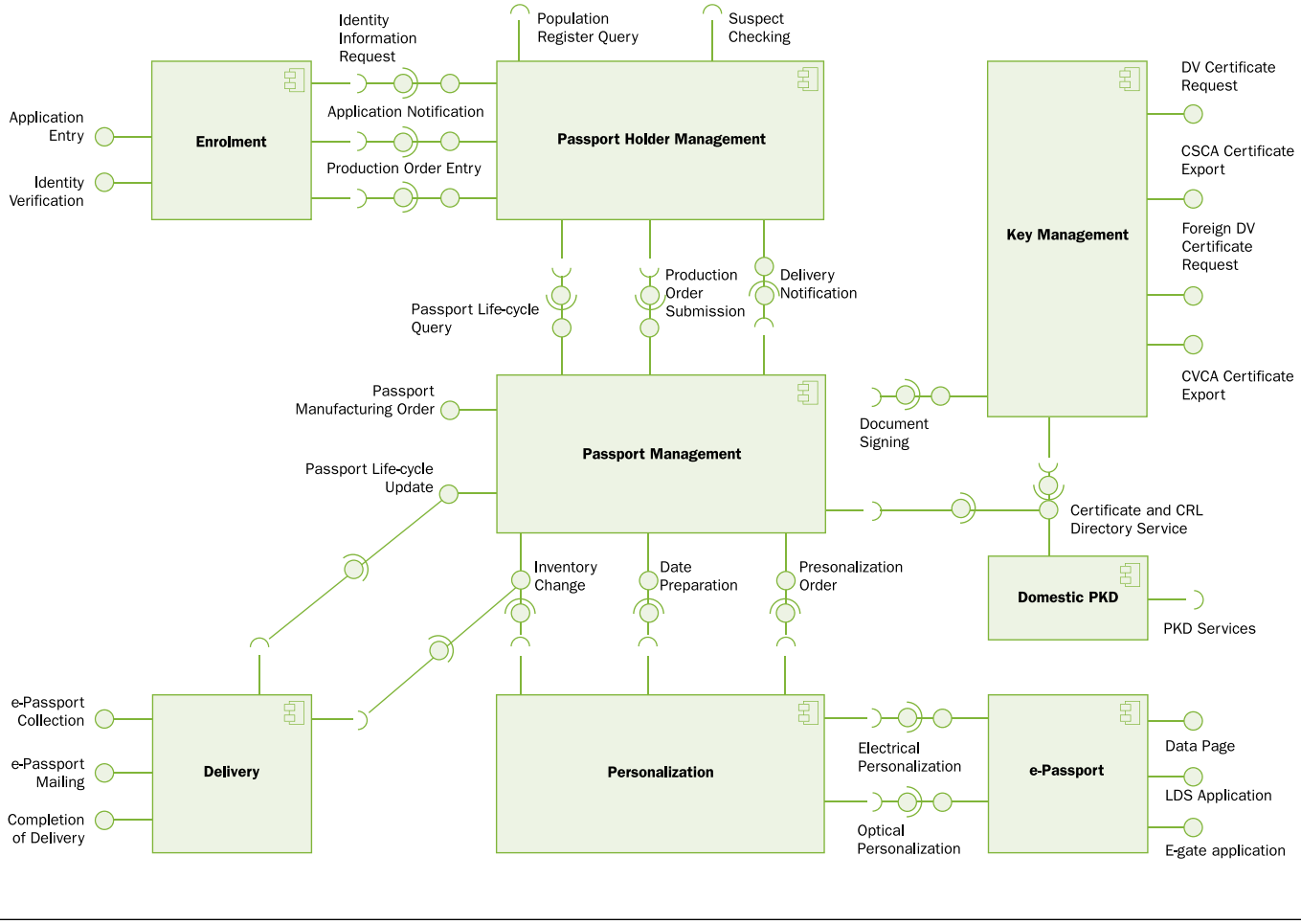
The developers of the protection requirements evaluate the system from all viewpoints and consider all the possible threats to your e-MRTD issuance system. These results often place strict limitations on the functional requirements defined in the system architecture.

For example, while using a unique personal ID number as a document number could ease many processes within the planned issuance system, this type of single number approach may also engender high risks in terms of overall data protection and document security. As part of a sound risk assessment process, all processes and components of the current system should be checked against best practice security recommendations.

It is recommended in this regard that States take advantage of the existing guidelines described in ISO Doc 27001, entitled *Information Security Management—Specification with Guidance for Use*, which is the replacement for the original British standard, BS7799-2. Most of the vulnerable components of an e-MRTD issuance system, such as the e-Passport chip or the certification authority, should follow recommended protection profiles developed within the Common Criteria scheme or by the U.S. National Institute of Standards and Technology (NIST) scheme.

Any final solution should be protected by running and maintaining an information security management system. It is recommended that the issuing authority may be certified as compliant with ISO/IEC 27001 by any of the accredited registrars worldwide. This certification can only be completed after the e-MRTD issuance system is fully operational.

Figure 3: System architecture model for an e-Passport issuance system



The project management plan defines the framework for team work

It goes without saying that any issuing authority will look to the best technologies currently available when they are upgrading their e-MRTD infrastructure. What's often forgotten in this respect is the importance of utilizing the best people available for making it all happen.

Since all e-MRTD projects are highly customized towards end-client needs, the skill set of the key staff and their ability to adapt to the local culture is essential to executing the project successfully. The project management plan should address the authority's expectations regarding the qualification of key staff members and the methodologies which should be employed when executing the project.

It is very reasonable to require proof that the vendor's project manager has managed e-MRTD projects of a similar kind and scale before. The best proof is to provide the contact details of the project sponsor of the referenced project. Along the same lines, a vendor's system architect should be familiar with modelling complex IT system architectures by using modern methodologies such as Unified Modelling Language (UML) and RM-ODP.

It is important that your project management plan includes a master time schedule. It should be the vendors' task to plan the implementation of any solution being proposed within the plan's time frame. Last but not least, the project management plan should include a risk assessment of highly probable risks and any others which could cause a significant impact to the project's success.

Defining your scope statement

All the requirements developed during the system architecture, protection requirements and project management phases together form the basis of the project's scope statement. This statement describes in great detail what the issuing authority expects from the future e-MRTD issuing system. The scope statement is one of the most

critical documents for the project's success, since it will be used for getting a final approval from the project sponsor.

The scope statement will also be used as a baseline plan for all parties responsible for any deliverables associated with the project, though in the early stages it can often still be undecided how some of these deliverables will be split between your internal staff and the vendor or vendors. A sound scope statement should therefore include:

- All requirements
- Acceptance criteria.
- List of deliverables.
- Out of scope statements.
- Constraints and assumptions.

It is recommended that the project manager formulate all requirements according to internationally accepted standards, such as IEEE 830. This approach ensures that system requirements are correct, unambiguous, complete, consistent, ranked for importance and/or stability, verifiable, modifiable, and finally traceable.

In order to use the scope statement as the basis for your acceptance testing of the final solution, it is recommended that the State project manager include the relevant qualification plans for each deliverable in the scope statement. For testing e-Passports, the relevant ICAO test standards should be used. Tests of other components should be developed in reference to the respective requirements specifications.

Creating a Work Breakdown Structure (WBS)

Finally, the scope of work related to your project needs to be subdivided into smaller, more manageable work packages. The Work Breakdown Structure (WBS) is a deliverable-oriented hierarchical decomposition of the work to be executed by the project team. A deliverable is defined to be any unique and testable product, result or capability that must be produced to complete the project. Typical deliverables of an e-MRTD Issuance project are:

- e-Passport booklet.
- Enrolment system.
- Passport holder management system.
- Passport management system.
- Personalization system.
- Delivery system.
- Certificate authority.
- Quality control process.
- Information security management system.
- Project management charter.
- Project management report.
- Service level agreement.
- Service and maintenance agreement, etc.

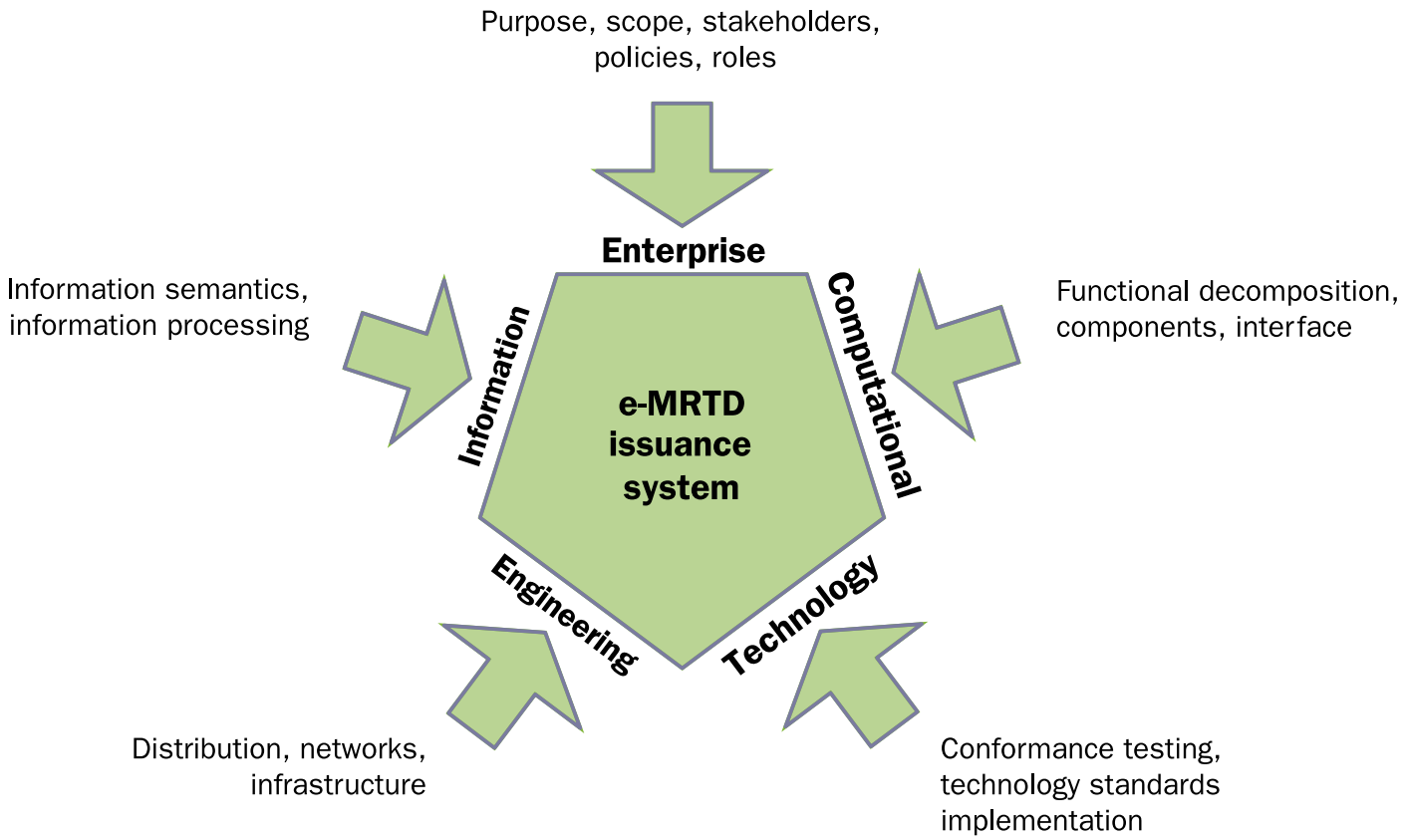
With the work breakdown structure, the issuing authority should also decide whether to make or to buy the system components. Whereas it is common practice that the potential vendors have to provide a formal proposal proving that their solution complies with all requirements, internal suppliers of system components should also be required to provide a similar proposal to the project owner.

All deliverables, regardless if provided by internal or external suppliers, must be tested against the same acceptance criteria, as stated in the scope statement.

Conclusion

The initiating and planning of an e-MRTD issuance system project is key to the successful completion of the project. In brief, the following guidelines should be addressed:

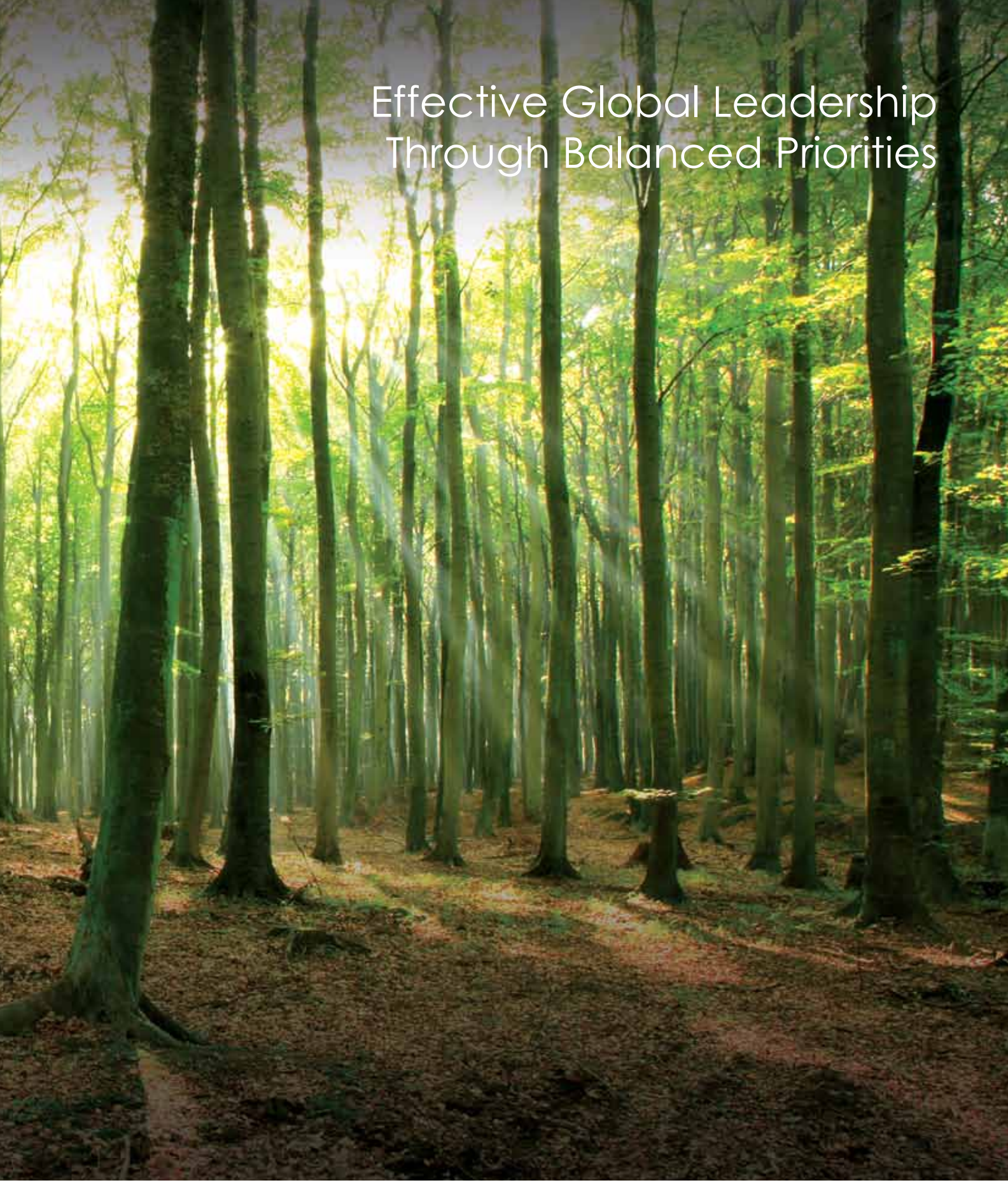
Figure 4: Reference Model for Open Distributed Processing



- Project managers need to be fully empowered to do their job.
- All stakeholders, including the public, need to be identified and managed properly.
- Issuing authorities shall define their requirements, not specify solutions.
- The system architecture should use a model approach to handle the project's complexity.
- Protection requirements should receive special attention.
- Scope statements need to be complete and follow a precise, formal language approach in order to be traceable up to the acceptance process at the end of the project.
- All suppliers must adhere to the requirements ref ected in the scope statement.

There are many more aspects to be considered in the initiating and planning phase, however the development of the scope statement is the most vital of all. The next article in this series will cover how to employ the scope statement during the procurement process and through the remaining implementation phase. All steps subsequent to the planning phase described in this issue will make use of the documents developed during this phase. Only a consistent set of documentation will enable the project manager to maintain control over the project's success. ■

Markus Hartmann is the founder and CEO of HJP Consulting GmbH, a consulting firm specializing in the planning, procurement and approval of e-Passport and e-ID card projects. Hartmann is an expert in e-MRTD solutions and project management and has advised governments and manufacturers implementing national e-Passport projects in Germany, the UK and the U.A.E. He also serves as ISO delegate in the ICAO Implementation and Capacity Building Working Group and, prior to forming HJP Consulting, was a member of the executive management board of the smart card manufacturer now known as Sagem-Orga.


Effective Global Leadership
Through Balanced Priorities

Is your State 2010 compliant?

Because the April 2010 MRTD implementation deadline and newer-generation e-Passport advances are now proceeding concurrently in the global border control and facilitation communities, some confusion has arisen over precisely what type of travel document is required to be implemented by those remaining non-MRTD States in order for them to achieve full 2010 compliance.

To help clarify and re-confirm these requirements, ICAO provides here a summary of the rationale and stipulations that inform the 2010 MRP deadline and the precise document attributes that need to be in place to satisfy its conditions.

In March 2005, the ICAO Council adopted Amendment 19 to Annex 9—*Facilitation*. This Amendment incorporates recommendations which had been made by the Twelfth Session of the Facilitation Division (FAL/12—Cairo, 2004), which included provisions for new Standards and Recommended Practices (SARPs) to control passport and other travel document fraud and enhance the overall security of global travel documents, ref ected in the twelfth edition of Annex 9 (July 2005).

These provisions included Standards that require ICAO Member States to issue only Machine Readable Passports (MRPs) by April 1, 2010 (Standard 3.10), according to specifications contained in Doc 9303, Part 1, Volume 1

What you WILL NEED for 2010

In order to comply with the ICAO deadline of the April 1, 2010, only Machine Readable Passports (MRPs) need to be issued.

MRPs are passports which conform to the specifications contained in Doc 9303, Part 1, Volume 1, and normally are constructed as an ID-3 size book containing pages with information on the holder and the issuing State or organization, as well as pages for visas and other endorsements. Machine readable information is contained in two lines of OCR-B text, each with 44 characters.

What is NOT REQUIRED for 2010

Electronic Machine Readable Passport (e-MRP or e-Passport, see page 32)

States are not required to issue e-Passports to comply with the 2010 ICAO deadline.

e-MRPs contain a contactless Integrated Circuit (IC) chip carrying data from the MRP data page, a biometric of the passport holder, and a security object to protect the data with PKI cryptographic technology. e-MRPs must conform to the specifications contained in both Doc 9303, Part 1, Volume 1 **AND** Doc 9303, Part 1, Volume 2.

(*"Machine Readable Passports, Passports with Machine Readable Data Stored in Optical Character Recognition Format"*). Another standard calls upon States to regularly update security features in new versions of their travel documents (3.7), and establishing further Standard establishes controls on the creation and issuance of travel documents (3.8).

The Council further adopted an additional Standard at that time which requires Member States to ensure that all non-MRPs expire and are removed from circulation by the November 24, 2015 (3.10.1).

A related Recommended Practice (3.9) also advises States to incorporate biometric data in their MRPs and other machine readable travel documents as specified in Doc 9303, Part 1, Volume 2 (*Machine Readable Passports, Specifications for Electronically Enabled Passports with Biometric Identification Capability*). This last recommendation has been confused by some States as forming part of the 2010 implementation Standard.

To clarify the differences between the types of passports that will become mandatory as of 2010 and those additional attributes which ICAO suggests be considered by States as they overhaul their passport document and issuance processes, a brief summary delineating the differences between MRTDs, MRPs and e-Passports would be useful at this juncture.

MRTDs, MRPs, e-Passports and 2010 ICAO Standard compliance

In order to fully understand the requirements of the 2010 MRP implementation deadline, States need to first be very clear on precisely what type of attributes are necessary for a travel document to qualify as an MRP.

A Machine Readable Travel Document (MRTD) is an official document conforming with the specifications contained in Doc 9303, issued by a State or organization, which is used by the holder for international travel (e.g. passport, visa, official document of identity), and which contains eye- and machine-readable data. Each type of MRTD contains, in a standard visual format, the holder's identification details (including a photograph or digital image) with mandatory identity elements ref ected in a two-line or three-line Machine Readable Zone (MRZ) printed in Optical Character Recognition-B (OCR-B) style.

Standardization of elements in these travel documents allows for automated interoperability between all participating countries. This global interoperability of MRTDs facilitates inspection of international travellers at borders and enhances travel document security.

MRTDs have been developed under the auspices of ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) with technical and engineering input from ISO Working Group 3 (JTC1/SC17/WG3). These specifications are published in ICAO Doc 9303 and endorsed by ISO as ISO/IEC 7501.

ICAO's mandate to develop MRTDs is provided by Articles 13, 22, 23 and 37 of the Chicago Convention which oblige Contracting States to develop and adopt international standards for customs, immigration and other procedures to facilitate the border-crossing processes involved in international air transport. These specifications apply to all 190 ICAO Contracting States. ■

Not all MRTDs are e-Passports

An e-Passport is simply one type of MRTD. While these terms may refer to different types of MRTDs that share many of the same fundamental benefits and characteristics, important distinctions do exist between each and it remains beholden upon all State, media and industry stakeholders to reference them correctly.

In this special Symposium Issue of the *MRTD Report*, ICAO takes a moment to reconfirm for the global border security and facilitation communities those required elements that must be incorporated into an MRTD travel document in order for it to be accurately described as an "e-Passport".

In as much as both Machine Readable Travel Documents (MRTDs) and e-Passports have been the result of ICAO-driven improvements to the specifications relating to State travel and identity documents, both of these instruments can be seen to have shared the same evolutionary path.

It is also true, however, that an e-Passport represents a generational advance in basic MRTD functionality and security. This makes it beholden upon border control and facilitation stakeholders, as they discuss and communicate their programme characteristics, not to confuse these identity tools—especially as regards the specific requirements of the Organization's 2010 global MRTD implementation deadline.

Historical and cooperative context

The far-reaching and highly cooperative process associated with travel document evolution has seen important input over the years, from multilateral organizations as well as innumerable industry and State experts. The process has essentially been ongoing since ICAO first undertook the

WHEN IS YOUR MRP AN ICAO-COMPLIANT e-PASSPORT?

Any passport which first satisfies all the requirements of an ICAO-compliant Machine Readable Passport, as specified in ICAO Doc 9303, Part 1, Volume 1, and must additionally include in the IC chip, the information contained in the two lines of OCR-B printed on the Machine Readable Zone of the datapage of the MRP, and the following characteristics contained in Doc 9303, Part 1, Vol. 2 in order to conform to ICAO's globally-interoperable requirements and qualify as a true "e-Passport".

e-Passport requirements as per ICAO Doc 9303, Volume 1, Part 2:

A facial recognition biometric in the form of a high resolution portrait.

Employment of the Logical Data Structure (LDS).

Data storage and communication permitted via a contactless, integrated chip (IC), conforming to ISO/IEC Standard 14443—type A or B.

Chip-based version of the information contained in the physical document's Machine Readable Zone (MRZ).

Incorporation of a Public/Private Key Infrastructure (PKI), as managed under the ICAO Public Key Directory (PKD). The PKI defines the system and procedures to be used for securing data on an IC and ensuring that access to it is appropriately controlled.

challenge to develop *"recommendations for a standardized passport book or card that would be machine readable"*, as far back as 1968.

In 1980, the specifications and guidance material that arose from those early efforts were published as the first edition of ICAO Doc 9303—then entitled *"A Passport with Machine Readable Capability"*—and established a basis for the initial issuance of machine readable passports. In 1984, ICAO formed the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), a body comprised of government officials with related specializations in order to update and enhance these specifications on a regular basis.

The TAG/MRTD has worked diligently since it was established to refine MRTD specifications. It had already begun to research the practical application of more advanced electronic security features when the events of September 11, 2001, moved the need for these new tools even more quickly into the spotlight.

Defining the e-Passport

First and foremost, an e-Passport must incorporate all the basic specifications related to MRTDs that are contained in the sixth edition of ICAO Doc 9303—*Machine Readable Travel Documents*, Part 1, Volume 1. This volume contains all the specifications necessary for a State to develop and issue a machine-readable passport (MRP).

Secondly and more specifically, an e-Passport must additionally fully conform to Doc 9303, Part 1, Volume 2, which contains the specifications for a contactless Integrated Circuit (IC) chip within which is stored certain specified MRTD data, a biometric measure of the passport holder, and a security object to protect the data with Public Key Infrastructure cryptographic technology.

These additional specifications and recommendations were developed by ICAO's New Technologies Working Group (NTWG). As per the NTWG's formal recommendations to the ICAO TAG/MRTD—made at meetings in 2003 and 2004—an MRP must employ the following in order to conform to ICAO's globally-interoperable requirements and qualify as a true "e-Passport":

- High resolution digitized displayed portrait with the digital data of the image stored in the chip. The facial image is the only globally interoperable biometric.
- Data storage and communication permitted via a contactless, integrated chip (IC), conforming to ISO/IEC Standard 14443—type A or B.
- Employment of the Doc 9303-mandated Logical Data Structure (LDS).
- Incorporation of a security object to protect the data with Public Key Infrastructure cryptographic technology. It is recommended that States join the ICAO Public Key Directory (PKD), the main global distribution point for public signing key certificates from all issuers of e-Passports who are required to validate and authenticate such documents.

These four characteristics must be considered to proscribe the basic definition of an ICAO-compliant e-Passport. Readers may wish to note that fingerprint and iris capture have also been supported as secondary biometrics, where applicable and/or mandated.

The e-Passport specifications contained in Doc 9303 require a high level of technical expertise on the part of States and contractors who may be involved in the work of creating electronically-enabled MRTDs and the systems required for capturing, encoding and reading the stored data and in its use in biometric identification. ■

it's live!

A new global hub for MRTD suppliers and information!

Whether you're an MRTD professional looking for the latest guidance, technology and assistance with your upcoming implementation project, or a supplier wanting to leverage the unmatched advertising potential of the web's most targeted location for MRTD decison-makers, **ICAO's new MRTD Community Web Site** is your one-stop shop for success.

For more information regarding listing your company on our site, or to enquire about new advertising opportunities, please contact:

Michelle Villemaire
mvillemaire@icao.int
+1.514.954.8219 ext.7090

www2.icao.int/en/MRTD2

2009-2010 ICAO CALENDAR OF EVENTS

2009 Meetings		
ICAO-World Bank — Routes Development Forum Maximizing Civil Aviation's Contribution to Global Development Aviation Development: Focus on Asia/Pacific	Beijing, China	14 – 15 September 2009
Fifth Symposium on ICAO MRTDs, Biometrics and Security Standards	ICAO Headquarters, Montreal	21 – 23 September 2009
Global ATM (Air Traffic Management) Forum on Civil/Military Cooperation	ICAO Headquarters, Montreal	19 – 21 October 2009
ICAO Alternative Fuels Conference	Rio de Janeiro	16 – 18 November 2009
Airports Economics Panel - Air Navigation Services Economics Panel	ICAO Headquarters, Montreal	30 Nov – 4 Dec 2009
Technical Advisory Group - Machine Readable Travel Documents (TAG-MRTD/19)	ICAO Headquarters, Montreal	7 – 9 December 2009
2010 Meetings		
Next Generation of Aviation Professionals Symposium	ICAO Headquarters, Montreal	1 – 4 March 2010
Air Transport Bureau Outlook Symposium	ICAO Headquarters, Montreal	13 – 15 April 2010
ICAO Environment Symposium	ICAO Headquarters, Montreal	10 – 14 May 2010
Diplomatic Conference	ICAO Headquarters, Montreal	21 Jun – 9 Jul 2010

Complete Security Begins with 3M

A trusted partner when you need a solution

For more than 30 years, 3M Security Systems has been providing security materials, secure printing, and hardware and software solutions for secure document issuance and border management. When you partner with us, you leverage that expertise—we help bring the critical elements of security together.

3M Issuance Systems ⊢ 3M Security Materials ⊢ 3M Authentication Systems

3M.com/security

3M

Gemalto: the fastest* ePassport

Gemalto's new Common Criteria certified Sealys eTravel operating system:

> **Speeds up border control** with a reading time of less than 3 seconds* in Extended Access Control (EAC) mode
> **Increases ePassport personalization** throughput by leveraging record writing performance

Available on multiple interchangeable microprocessor platforms, the new Sealys eTravel operating system secures your supply chain management.

Gemalto's Sealys eTravel operating systems are used in more than 21 national ePassport programs worldwide including Côte d'Ivoire, Estonia, Denmark, France, India (diplomatic), Norway, Poland, Portugal, Qatar, Singapore, Slovenia, Sweden and the United States of America.

Now you know who's behind.

* 2,6 seconds for a full EAC transaction with 48 KB of data, RSA 1024 and extended length (EAC tests in September 2008)

www.gemalto.com

gemalto
security to be free

Identity Management for a Safer and More Secure Aviation Industry

Federal agencies and international governments depend on L-1 Identity Solutions to provide complete secure ID issuance and authentication, and to help them protect citizens against crime perpetrated by fraudulent identities. Ensuring that travelers are who they claim to be – and assuring the legitimacy of IDs presented at ticket counters, airport delivery gates, and border crossings as proof of identity – is a matter of global security affecting the entire aviation industry.

L-1 Identity Solutions produces millions of secure government-issued IDs each year, including ID solutions for more than 20 countries. Our solutions and services for the aviation industry include:

- ICAO Compliant ID and Passport Book Production
- Document Authentication for Airport Employment and Passenger Screening
- Enrollment Services
- Knowledge Testing
- Multi-Biometric Identification
- Verification Applications

L-1 solutions are modular and can be used alone or together to form a complete identity management system. Visit us online to find out more: **www.L1id.com.**

Visit us at the 2009 ICAO Symposium!

Protecting and Securing Personal Identities and Assets

BIOMETRICS · SECURE CREDENTIALING · ENTERPRISE ACCESS SOLUTIONS
ENROLLMENT SERVICES · GOVERNMENT CONSULTING SERVICES

L-1 IDENTITY SOLUTIONS™
SECURE CREDENTIALING DIVISION

978-215-2400 / SCDinfo@L1ID.com