Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

Contents

1. Australia, Department of Foreign Affairs and Trade, “Request for Proposals for Biometrics Research and Development Assistance”, Request for Proposals No. 02/010138
2. New Zealand, Department of Internal Affairs, “Registration of Interest (ROI) for Supply of New Zealand Travel Document Books and Personalisation Technology”, ROI Document Ref: (DIA/2006-014)

12. Project Management and Implementation

Planning, scoping, governance, change management, stakeholder management, risk management, resource management, quality management, status reporting, evaluation and project closure.

Contributors and Acknowledgements

Project overseer - Australia
APEC BMG Co-sponsors
APEC Economies’ experts on Biometrics
APEC BMG Members
Identity Branch, Department of Immigration and Citizenship, Australia
Jim Wayman; Director of the Biometric Identification Research Program of San Jose State University
APEC Section, Department of Immigration and Citizenship, Australia
Biometric Consulting Group

List of Abbreviations

AEC	Advanced Encryption Committee
ANSI	American National Standards Institute
APEC	Asia Pacific Economic Cooperation
API	Advanced Passenger Information
APO	Australian Passport Office
ATM	Automated Teller Machine
BAC	Basic Access Control
BMG	Business Mobility Group (APEC)
CA	Certificate Authority
CBEFF	Common Biometric Exchange File Format
CCTV	Closed Circuit Television
CIs	Configuration Items
CTTF	Counterterrorism Task Force
DFAT	Department of Foreign Affairs and Trade (Australia)
DoS	Department of State (USA)
DSC	Document Signing Certificate
DVS	Document Verification Service
EAC	Extended Access Control
FR	Facial Recognition
FRVT	Facial Recognition Vendor Testing
G8	Group of Eight (International forum of eight major powers)
HKSAR	Hong Kong Special Administrative Region
HSM	High Security Module
IATA	International Air Transport Association
IBM	International Business Machines
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit [Chip] Card
ID	Identity
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
IT	Information Technology
JTC	Joint Technical Committee
LAN	Local Area Network
LDS	Logical Data Structure
MAPI	Manual of Australian Passport Issue
MoU	Memorandum of Understanding
MRTD	Machine Readable Travel Document
MRP	Machine Readable Passport
MRV	Machine Readable Visa
MRZ	Machine Readable Zone
NEDA	National Economic Development Authority
NIST	National Institute of Standards and Technology (USA)
NPA	Note Printing Australia
OCR	Optical Character Recognition
OID	Object Identifier
PAM	Passport Agency Manual
PIB	Project Initiation Brief
PICS	Passport Information and Control System
PKD	Public Key Directory
PKI	Public Key Infrastructure
PMBOK	Project Management Body of Knowledge
POI	Proof of Identity
PP	Project Proposal
PRC	People's Republic of China

QA	Quality Assurance
RAM	Random Access Memory
RF	Radio Frequency
RFI	Radio Frequency Interface
RFI	Request for Information
RFID	Radio Frequency Identification
ROK	Republic of Korea
SAM	Secure Access Module
SC	Steering Committee
SDLC	Software Development Life Cycle
SFP	Systems for People
SOD	Document Security Object
TAG	Technical Advisory Group
TD	Travel Document
UK	The United Kingdom of Great Britain
USA	The United States of America
USB	Universal Serial Bus
UV	Ultraviolet

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 1 Introduction

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

1. Introduction

In the last 25 years, passports have evolved as the number of people travelling internationally has grown. Machine-readable passports, first introduced in 1981, have become the familiar standard and are now issued by approximately 140 countries. However, as the 21st century progresses, governments are facing challenges posed by unprecedented migration flows as well as increases in identity theft, cross-border crime and terrorism, and are responding by introducing new technology in passports as one of various measures to counter these challenges. At the end of 2006, some 50 countries had implemented an ePassport program that was compliant with new international standards.[1]

Although many economies are still using conventional machine-readable passports, and may wish to do so for some time to come, since ePassports are now being issued by a number of States, governments may find they need to introduce ePassports in order to prevent their citizens facing increasing difficulties with immigration and travel.

This document, "A Guide to Biometric Technology in Machine Readable Travel Documents" (hereafter referred to as "the Guide"), is intended as a reference document to assist APEC economies that are considering the introduction of ePassports. It is the outcome of a project established by the APEC Business Mobility Group (BMG) aimed at continuing to build the capacity of APEC economies "to accelerate, on a best endeavours basis, work towards adopting international standards on biometrically enhanced passports and supporting infrastructure as a means of enhancing border security, thereby facilitating the safe and secure movement of business people across the APEC region".

The mandate was to produce a readily accessible, web-based reference tool document covering technical and non-technical issues; and best practice options for financing, cost recovery and procurement; and other issues associated with adopting biometric Machine Readable Travel Documents (MRTDs) and related border systems. The Guide seeks to inform economies of the various ePassport options and best practice already available, with information drawn from a wide range of sources, including responses by APEC economies to project questionnaires as well as presentations given during BMG workshops in 2006, in order to enable economies to arrive at a solution that best fits their specific business requirements and circumstances. (For further information about the APEC BMG see Appendix 1.)

What is a Machine Readable Travel Document (MRTD)?
A Machine Readable Travel Document (MRTD) is an international travel document containing visual and machine-readable data. MRTDs currently in existence include Machine Readable Passports (MRPs), Machine Readable Visas (MRVs) and Machine Readable Official Travel Documents.
http://mrtd.icao.int/content/view/18/199/

What is an ePassport?
A biometric passport, or ePassport, is a MRTD passport that has a contactless integrated circuit (IC) chip embedded in it, in accordance with International Civil Aviation Organization (ICAO) standards.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf

What is a biometric?
A biometric is a biological and behavioural characteristic of an individual (eg, fingerprint, iris) that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals.
http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/JTC_1_SC_37_Agreed_Harmonized_Core_Biometric_Terms_and_Definitions.pdf?nodeid=5675848&vernum=0

[1] Paul Wilson, "Preparing for ePassports", *ICAO MRTD Report*, Vol. 1, No. 2, pp. 37–42.

APEC BMG Mandate for MRTD Development

Excerpt from Joint Statement of 16th APEC Ministerial Meeting
Santiago, Chile—17–18 November 2004

"Ministers noted the progress made by the Counter-terrorism Task Force (CTTF) in implementing the 2003 APEC Leaders' Human Security commitments, especially those aimed at facilitating secure and efficient trade within the region. Endorsing the agreements reached within the CTTF, Ministers:

- called for cooperation to ensure that all APEC economies will begin issuing Machine Readable Travel Documents (MRTDs), if possible with biometrics, by 2008, and, on a best endeavours basis, to accelerate replacement of Non-MRTDs by MRTDs as well as implement ICAO travel document security standards."

http://www.apec.org/apec/ministerial_statements/annual_ministerial/2004_16th_apec_ministerial.html

The Guide offers a systematic reference for the steps that need to be taken when specifying, developing and implementing an ePassport program in accordance with international guidelines. The intention is to present all the issues that need to be considered and to describe possible options so that economies will be able to decide what suits them best.

This document does not prescribe one particular path for economies to follow. Each economy is very different, so it is important that each economy investigates for itself the whole range of possible options when considering the introduction of ePassports.

The Role of the International Civil Aviation Organization (ICAO)

The International Civil Aviation Organization (ICAO) has played a major role in establishing the specifications, international standards, and best practices for the issuance of passports and other travel documents. ICAO has published **Document 9303** (see box below) that includes complete specifications for travel document production and issuance.

To assist economies, ICAO has also developed a list of questions and lessons learned that should be considered as part of a passport upgrade. The entire list is included as an appendix to this chapter (see Appendix 2), and individual questions and lessons learned will be included in subsequent chapters according to the topic to which they relate.

ICAO: For information about ICAO and MRTDs, please refer to the following websites:
http://www.icao.int/
http://icao.int/mrtd/guidance/IssSupport.cfm

The information provided in the Guide should be read in conjunction with related ICAO documents such as Document 9303, relevant International Organization for Standardization (ISO) publications, open and closed source information, and specific legal and procedural

documents as they relate to individual economies and jurisdictions.[2] The information in the Guide is not intended to replace or supersede any material previously printed about ePassports and is not intended to provide detailed specifications for ePassports.

ICAO: Document 9303
ICAO requirements for Machine Readable Travel Documents (MRTDs) and ePassports are set out in ***Document 9303: Machine Readable Travel Documents***. First published in 1980 as "A Passport with Machine Readable Capability", Document 9303 is now published in three separate parts:

- Part 1, Volume 1: Machine Readable Passports, Volume 1: Passports with Machine Readable Data Stored in Optical Character Recognition Format, Sixth Edition, 2006
- Part 1, Volume 2: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capabilities, Sixth Edition, 2006
- Part 2: Machine Readable Visas, Third Edition, 2005
- Part 3: Size 1 and Size 2 Machine Readable Official Travel Documents, Second Edition, 2002

Document 9303 is available for purchase from ICAO.

http://mrtd.icao.int/content/view/33/202/
Sales information: http://mrtd.icao.int/content/blogcategory/21/210/

Disclaimer
The material in "A Guide to Biometric Technology in Machine Readable Travel Documents" is provided for the information of APEC economies, and, *except in respect of ICAO technical and other relevant international standards*, does not prescribe or endorse the use of any particular option, solution or method for ePassport development.

Unless otherwise stated, all case studies in the Guide are drawn from presentations made at BMG workshops held in 2006 or from responses by APEC economies to questionnaires sent to them as part of this project.

References

1. ICAO-New Technologies Working Group (IEC JTC1 SC17 WG3/TF1), "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation", Draft 1.4, 7 March 2007, TAG-MRTD/17-WP/16.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf
2. Paul Wilson, "Preparing for ePassports", *ICAO MRTD Report*, Vol. 1, No. 2, pp. 37–42.

Appendices

Appendix 1: APEC Business Mobility Group and ePassports
Appendix 2: ICAO: "How to Proceed: Deciding to Issue MRPs and Making Improvements to MRP Systems"

[2] See also ICAO-New Technologies Working Group (IEC JTC1 SC17 WG3/TF1), "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation", Draft 1.4, 7 March 2007, TAG-MRTD/17-WP/16, http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf

Appendix 1

APEC Business Mobility Group and ePassports

APEC, through its Business Mobility Group (BMG), has been looking at the development and use of ePassports with the aim of assisting APEC economies that are considering whether to introduce ePassports for their citizens.

The BMG is one of the sub-fora working groups of the APEC Committee on Trade and Investment, and is comprised of representatives from the immigration and consular affairs agencies of each APEC member economy. The role of the BMG is to enhance the mobility of business people to facilitate trade and investment activity in the APEC region. It achieves its aim by building the capacity of members to implement transparent, streamlined short-stay and temporary residence arrangements, and immigration and related border systems to ensure the safe and secure movement of people. As a result of this role, the BMG has been given responsibility for developing APEC initiatives relating to ePassports. This mandate came from the 16th APEC Ministerial Meeting held in Santiago, Chile, in November 2004.

To begin fulfilling this mandate, the BMG conducted a successful seminar (in Ho Chi Minh City) and a workshop (in Hong Kong, China) in 2006 to raise economies' awareness of the standards and benefits of biometrics to ensure the greater safety and security of travellers across the region.

The seminar in Ho Chi Minh City was attended by 52 delegates from 19 (of 21) APEC economies. It raised economies' awareness of the ICAO international standards for biometrically enhanced MRTDs (ePassports), as well as of existing, agreed BMG document security standards for the management of databases and documents, manufacture, storage and identity verification processes. It also provided an opportunity for economies to learn of developments in biometric technology and their application to MRTDs at the border.

The Hong Kong, China, workshop was attended by over 45 delegates from 18 APEC economies, represented through expert speakers and/or nominated participants. Independent experts from the International Civil Aviation Organization and the International Organization for Standardization also participated.

The workshop sought to build on the outcomes of the seminar, and examined both the technical and non-technical issues that are associated with introducing and maintaining ePassports. Presentations by a number of economies provided case studies that described their experiences and the solutions they had found for addressing financial and other resource issues. Other issues covered included the benefits of biometric passports; financial and cost recovery issues; stakeholder and consultation processes; technology and systems integration issues; and privacy, societal and legal issues related to the introduction of ePassports.

Feedback from APEC Ministers and Economic Leaders on BMG's ePassport work program has been positive, and BMG has been asked to continue this work through capacity building and other methods to meet APEC objectives.

Appendix 2

ICAO: How to Proceed—Deciding to Issue MRPs and Making Improvements to MRP Systems

http://icao.int/mrtd/guidance/IssExplanation.cfm

A Notional Explanation of Factors

As you, the passport issuing authority, prepares to upgrade your State's passport, you must have a firm understanding of what you are doing now, what you want to improve, and whether you are willing to change your processes. The answers to these questions will have a bearing on the equipment you choose, its costs, the method of procurement, the level of security in the passport document itself, and how you engineer your issuance process. Here are some of the questions you must be able to answer before sharing your requirements with potential contractors:

- What level of threat to the integrity of your passport are you dealing with? External fraud? Misuse? Alteration? Counterfeiting? Malfeasance?
- Do you want to use a biometric in your passport? Have you verified that what you want to do in this realm is consistent with your country's laws?
- Do you have one-person-per-passport as recommended by ICAO? Are you converting to that system?
- Does the citizen have to appear in person to apply for a passport?
- Do you want a centralised or decentralised issuance system? If the latter, how many issuance locations do you want?
- How many types of passports (Regular, Official, Diplomatic, Overseas-issued) are there? How many do you produce of each?
- How many pages are in the present passport? Do you want a change?
- Are there types of security features (intaglio printing, watermark paper, paper with an embedded thread, special stitching, ultraviolet printing, other special inks) that you want in the passport? How will they be verified?
- Do you want to change personalisation from the end leaf page to the interior of the passport, or vice versa?
- Have you verified that the security features can coexist in the same document and that your document construction can support them?
- Who in your government makes the decisions about the standards for quality and security content of your document? Should the decision process be changed?
- Have you resolved transliteration issues so that entries in your passport's machine readable zone (MRZ) will be in compliance with the transliteration standards of Doc. 9303?
- What is your passport's validity period? Do you want to change it?
- How do you want to reproduce the passport bearer's image in the passport?
- Do you mail out most of your issued passports, or must the applicants come in to pick up their passport?
- Do you issue passports from your embassies in other countries? If so, are they the same as domestic issue passports? Do you want them to be?
- What percentage of your applications are urgent? Require one day service?
- Have you a national passport data base? Do you want to alter it, or create one?
- What is your interrelationship with other identity and citizenship document producers in your country? Do you wish to establish such relationships where they don't now exist?
- How do you want to include amendments and observations?

Once you have decided to upgrade, and can answer the above questions, here are others that you must answer as you consider timing, cost, and acquisition method. Remember that the finished product will require everything from the making of paper, to the printing of passport books, methods of accepting applications, determinations of what acceptable evidence will be to establish eligibility, the personalisation process, the presence of internal controls and anti-fraud systems, and filing and retrieval systems for the applications. Each aspect impacts the others in some way; and some - as in method of personalisation - must be decided upon before other aspects can be determined.

- Especially if your previously issued passports can be easily altered or counterfeited, do you want to replace them before they would normally expire? If so, how do you verify that the holders of those passports did not obtain them by fraud?
- How much money do you have allocated to the project? Can you identify secondary funding sources should the cost of what you want exceed your estimates?
- How rapidly do you need to begin issuing the new passport?
- Do you wish to do it all at once, or on a phased basis (both as to changing over your facilities and in terms of adopting the new passport format before actually printing an MRZ)?
- What type of procurement do you contemplate for the new passport? Sole-source? Competitive? Multiple contractors? A single prime contractor with subcontractors? Direct purchase of needed materials with government staff performing the integration process? (Make certain that your contractor can deliver an ICAO-compliant document.)
- Have you thought out how you will verify that you are getting the level of quality that you need from your contractor(s)? Utilising the services of other government offices? Utilising the services of others in the private sector?
- How will your new system impact your customers and your workforce?

Planning for Implementation
http://icao.int/mrtd/guidance/IssPlanning.cfm

Some lessons that have been learned by governments installing machine readable systems are presented here as a means of helping prevent common implementation mistakes.

- Do a formal project plan early in the process, and share it widely among the organisation's management team. Identify critical milestones and don't proceed beyond them until they have been satisfactorily achieved.
- Remember: It will almost always take more time to implement a new system than expected. Be certain that you have contingency plans for unexpected situations and delays.
- Involve the users early in the design and testing of the hardware and software. Be certain that the resulting requirements documents are clear and specific.
- Make sure there is adequate government expertise available to monitor the contractor's performance under the contract.
- Make sure the contractor has adequate on-staff expertise to execute the contract within agreed upon dates even if human resources on which they depend suddenly exit.
- Have staff participate in the design of a training program for users, and make certain that there is adequate contractor support for the training process.
- Include in your requirements the need for a Headquarters test facility for testing contractor software improvements.
- Build in redundancy wherever in the system a breakdown of delicate or difficult to replace equipment can bring your production process to a halt.
- Identify and correct problems in the new system before leaving the old system. Don't rely on temporary "work-arounds"; fix the underlying problems.
- Make sure that the contractor documents the system so that the government has a complete record of the software.
- Be certain that you have well documented standard operating policies, processes and procedures at all issuing points so that there is consistency in your issued documents.

Costs and Funding
http://icao.int/mrtd/guidance/IssCosts.cfm

Funding technology improvements is a major concern, but one which can allow for some creativity. Major ways to approach this include:

- Direct funding of the entire effort by the government;
- Advance funding of start-up by the government, but recipients of the documents assessed an apportioned fee that covers costs of issuance plus the improvements;

- Advance funding of start-up by a contractor, with receipts from passport recipients used to repay the contractor's costs plus a reasonable profit;
- Advance funding of start-up and operations by the contractor; with the fees set (and an agreed upon percentage given to the contractor) for their initial and continuing services; One note of concern: Utilising contractors to produce your documents has many positives, but Governments should be careful to retain in the hands of direct hire government officials the judgements about who is entitled to receive a passport.

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 2 Why ePassports?

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

2. Why ePassports?

As the APEC Business Mobility Group (BMG) has agreed to introduce Machine Readable Travel Documents (MRTDs) with inclusion of biometrics (if possible) by 2008, and to accelerate the replacement of non-MRTDs with International Civil Aviation Organization (ICAO)-compliant MRTDs, it is important for economies to understand the features and benefits of MRTDs, and how they relate to ePassports.

The importance of passports for identification and travel, and the ease with which they can be used to facilitate criminal activity, has meant that there is a long history of fraud relating to passports, including:

- production of completely counterfeit passports;
- issuance of genuine passports on the basis of fraud (eg, fraudulent breeder documents, imposters with genuine breeder documents) or corruption of passport-issuing officials;
- issuance of genuine passports to the same person using multiple names and biodata;
- tampering with genuine documents (eg, biodata page or photo substitutions);
- imposters posing as the rightful holder of a passport;
- lost or stolen genuine passports (blank or interception of personalised passports, for example in the mail) can be used to perpetuate other types of fraud.

ICAO: Issues to consider when deciding to make improvements to passport systems

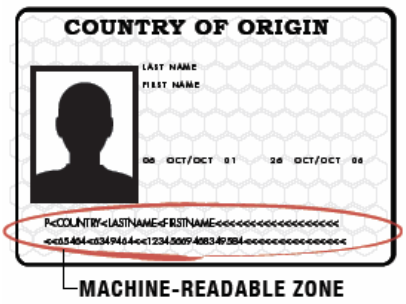
- What level of threat to the integrity of your passport is your economy dealing with? External fraud? Misuse? Alteration? Counterfeiting? Wrongdoing (especially by a public official)?

http://icao.int/mrtd/guidance/IssExplanation.cfm

Given such issues and their ability to impact negatively on travel facilitation and security, ICAO has responsibility for standardising travel documents, particularly MRTDs, and providing guidance for implementation of their specifications.

What are the features of Machine Readable Travel Documents (MRTDs)?

Each type of MRTD (ie, Machine Readable Passports, Machine Readable Visas and Machine Readable Official Travel Documents) contains, in a standard format, the holder's identification details, including a photo or digital image, with mandatory identity elements reflected in a two-line machine readable zone (MRZ) printed in Optical Character Recognition-B (OCR-B) style.



A machine-readable passport has two lines of text as letters, numbers and chevrons (<<<) at the bottom of the personal information page, along with your picture.

http://mrtd.icao.int/content/view/18/199/
http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm

Benefits of MRTDs[1]

http://mrtd.icao.int/content/view/28/203/

Governments benefit from the implementation of MRTDs, because MRTDs can:

- improve capacity for visual authentication of travel documents and holders at borders given their uniform and standard layout;
- be read by readers at border crossings to better detect false or fraudulent travel documents;
- facilitate the rapid and precise identification of those people who would misuse travel documents;
- permit the use of Advance Passenger Information (API) systems;
- improve ability to identify "problem cases" rapidly and precisely, which allows governments to spend their always-limited border control and law enforcement resources on those who should be given a more detailed inspection;
- through use of automated issuance processes, allow issuing authorities to electronically monitor and control each stage of travel document application and issuance, thereby reducing workload and increasing efficiency of the passport issuing agency;
- create a source of reliable, standardised data from which governments can build databases to improve border control processes;
- enhance ability to share data with other governments and the private sector with a view to improving the detection of stolen and fraudulently-obtained travel documents.

The rollout of MRTDs is actually also a cost-effective option for governments, as it is relatively inexpensive to improve a passport and its issuance systems in comparison with the cost of fraud as well as case-related investigations and prosecutions that are conducted by law enforcement authorities after the travel document system has been compromised.

For travellers, the primary benefit of MRTDs is faster processing at borders, because machine verification allows honest travellers to go through border screening quickly so that border staff can focus their time and resources on problem cases.

Airports and other port authorities benefit from MRTDs as the rapid and efficient processing of passengers through port facilities leads to more efficient use of port space and a reduction in the need to build or improve those facilities.

Airlines and other travel companies also benefit from MRTDs through:

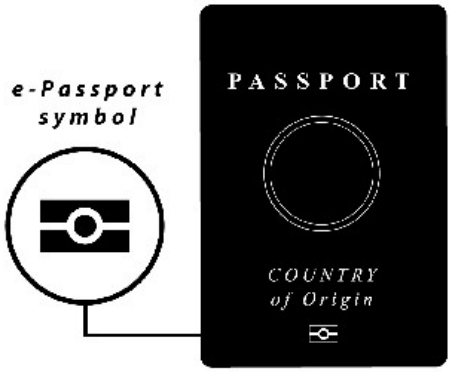
- improved verification of document authenticity and other efficiencies as a result of linkage of automated passport readers at the check-in counter to various databases;
- reduced time required to handle each passenger;
- better avoidance of fines or other penalties for carrying undocumented or improperly documented aliens into a country.

All of these benefits will expand significantly as more countries issue MRTDs, and as the technology needed to produce and read them becomes less expensive. The benefits will be expanded even further as document security features continue to improve, and as biometric identity verification technology is more widely used (eg, through the introduction and use of ePassports).

[1] For ICAO document on Benefits of MRTDs, see:
http://mrtd.icao.int/content/view/28/203/
http://mrtd.icao.int/content/view/29/204/
http://mrtd.icao.int/content/view/30/205/
http://mrtd.icao.int/content/view/31/206/
http://mrtd.icao.int/content/view/32/207/

How Do ePassports Differ from Machine Readable Passports (MRPs)?

An ePassport is a type of Machine Readable Passport (MRP) with an embedded microchip that contains data printed on the data page of the passport, including biographic and biometric information of the holder, and passport data. The chip also contains security features for preventing passport fraud and forgery and misuse of data stored on the chip. ePassports are easily recognised by the international ePassport symbol on the front cover.[2]



Benefits of ePassports over Other MRPs

ePassports have a number of advantages over other MRPs, although they will not be the answer to all passport fraud on their own. However, the rollout of ePassports in combination with other initiatives such as improved identity enrolment processes when issuing ePassports (see Chapter 5) and enhancement of border processes and systems (see below) will be effective in reducing passport fraud in both the home economy and other economies where passport holders may travel. A list of benefits is given below:

- Biometrics can be used to improve the quality of the background checking performed as part of the passport application process (eg, improves ability for watchlist checks and checks against other biometric databases such as those for identity cards) and to increase the level of confidence of the binding between the travel document and the person who holds it;
- Storing biodata and biometrics on the ePassport chip as well as the ePassport biodata page offers greater protection against fraudulent misuse and tampering;
- Capacity for biometric matching (as opposed to visual checks only) reduces the risk of identity fraud at passport issue and border crossing through improved detection of imposters;
- Security and efficiency at borders can be enhanced with the improved ability to verify ePassports and the identity of incoming ePassport holders, particularly if more automated processes are used;
- Authenticity of the data on the ePassport's chip can now be validated at the border using PKI certificates downloaded from the ICAO Public Key Directory (see Chapter 6).

These benefits do not preclude, however, the need for traditional passport security features (eg, watermarks, micro-printing, etc) and processes (eg, security of blank passports), or the need for the presence of border officials at border checkpoints to make informed judgments when necessary.

Implications for Border Processes

When developing an ePassport, economies will need to give consideration to how their ePassport will fit in with existing and potential border processes.

---

[2] http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm

The use of ePassports for border processing can bring a number of benefits, including:

- Enhanced border security, through better identification of travellers, particularly high-risk travellers;
- Deterrence of identity fraud and the use of forged or stolen travel documents;
- Ability to process increasing numbers of passengers with increased automation of border control processes for low-risk travellers and consequently more efficient use of resources.

Economies should consider these benefits in terms of both the use of ePassports (national and foreign) at their own borders, and the use of their own ePassport at other economies' borders.

To aid inspection at its own borders, each economy will need to put robust infrastructure and procedures in place to:

- Verify the identity of citizens and visitors, perhaps using new, automated systems;
- Handle exceptions and process secondary inspection;
- Ensure officials can inspect an ePassport and its bearer by means of machine-assisted as well as visual inspection.

To aid inspection of its citizens at foreign borders, each economy will need to:

- Ensure its ePassport complies with ICAO's interoperability standards so that it can be validated and authenticated by the receiving state;
- Authenticate the data on the ePassport's chip by downloading validated Public Key Infrastructure (PKI) certificates from the ICAO Public Key Directory (see Chapter 6);
- Ensure that the ePassport and its bearer can be inspected by means of machine-assisted and visual inspection.

Given these issues, the implications of ePassports for border processes can be separated into several areas that will be discussed: namely, identification, automation, integration of upstream processes, and 'the big picture'.

ICAO: Aims for ePassports and automated border processing

1.5 Today the international movement of passengers is still growing and (air)port operators, control authorities and carriers are seeking for new ways to process passengers with minimum intrusion into individual privacy but, at the same time ensuring that security of border controls and the threat of international crime and terrorism is totally maintained.

1.6 It is acknowledged that the vast majority of passengers are low risk, often frequent travellers who pose no risk to the integrity of States' immigration controls. It is these passengers that automated border clearance facilities should target and facilitate, since they represent an important percentage of the users of airport facilities.

1.7 With the introduction of the ICAO standards for e-passports, many States are implementing or considering to implement the necessary infrastructure, to issue e-passports in the near future.

1.8 It is recognised that the e-passport could be the means to facilitate Automated Border Control, since at least one of the by ICAO selected biometric features, the face, is stored on an electronic medium.

1.9 One of the aims of ICAO with the introduction of biometric identifiers in travel documents was to facilitate at the same time Automated Border Control schemes.

(ICAO, New Technologies Working Group, "Proposal for a Technical Report on Automated Border Control Systems", Working Paper 11, 13/09/2005, presented to 16th meeting of the Technical Advisory Group on Machine Readable Travel Documents, 26-28 September 2005, paragraphs 1.5–1.9.)
http://www.icao.int/icao/en/atb/fal/mrtd/tagmrtd16/TagMrtd16_011_en.pdf)

Identification

With the significant growth in the international movement of travellers over recent years, one of the most important improvements that ePassports offer for border processing is that they allow rapid and precise identification of travellers. The information on the embedded chip will enable border officials to verify that the traveller presenting the passport is the rightful holder of the passport he or she is presenting. Furthermore, since the digital data on the chip is difficult to forge, border control officers can have a greater degree of confidence that the passport has not been tampered with.

The ePassport gives border control officers another tool in addition to the usual document examination procedures for detecting passport and visa fraud. First, the ePassport's combination of biometric and security features will make it harder to substitute one identity for another. Second, the machine readable zone provides a basis for the ePassport to be readily verified against reference databases.

Automation

ePassports offer the possibility that border clearance processes can be automated, in part or in full, as suits the needs of each economy. Three stages in progression towards the ICAO goal of full automation can be delineated:

- **Manual processing:** Visual checks only, as with standard passports. Even where automation is not being considered at present, it is perfectly feasible that such manual checks could be augmented with an additional check of the photo and other data on the passport chip. This would require the use of passport readers, but would not involve the implementation of a wholly automated biometric-enabled system;
- **Semi-automated processing:** Further checks would involve biometric matching and immigration clearance conducted by border officials;
- **Fully automated processing:** Biometric matching and immigration clearance would be conducted without the involvement of border staff so those staff can concentrate their efforts on high-risk passengers.

	Authentication	**Verification**	**Identification**
Current procedures at primary inspection points	MRZ reading—[sometimes detects] forgery	Visual	Matching MRZ data with database
Future procedures (2-5 years)	**Data page** • Automated forgery detection • [Checking against] different document databases **Chip data** • Validation of signatures • Integrity of data **Data page matching chip** • Facial image match • Biographical data match **Additional documents** • Visa • Registered Traveller cards	**ePassport vs live data** • Chip image vs live image • Chip finger vs live finger • Chip iris vs live iris **ePassport vs database** • Chip image vs database image • Chip finger vs database finger **Visa vs live characteristics** • Database finger vs live finger	Matching of MRZ data with database Biometric identification at secondary control

Table taken from: Gregor Költzsch, "Next Generation Border Crossing: ePassports and their impact on border control", Bundesdruckerei GmbH, Berlin.
http://www.3dface.org/files/slides/070322/3Dface-Koeltzsch-BorderControl-070322.pdf

Automated processing may speed up clearance processes, but will also involve:

- Rollout of new technology, including hardware and software, and this will have to be integrated with existing systems;
- Adjustment to new systems by staff, and changes in what work they perform;
- Appropriate environmental conditions for hardware.

Integration of Upstream Processes

The collection of biometrics at visa application can allow economies to verify the identity of visa applicant/holders *before* they arrive at an economy's borders. It also means that economies can verify at the border the identity they have already established for that traveller at visa application.

This offers the potential to speed up border clearing processes, and to close up and secure the chain between visa issuance and border control.

The Big Picture

It is important that economies consider ePassports in the context of their wider border processes and systems in order to ensure that the benefits from their ePassport investment are maximised. Processes and systems to consider include those introduced above (ie, identification processes, automation of processing, data sharing and integration of upstream processes before the border), but can also include initiatives such as Advance Passenger Information, watchlist checks, registered traveller programs, etc.

These concepts for maximising the benefit of ePassports, biometrics and other complementary technologies and systems at economies' borders will be the subject of further work proposed for the APEC BMG's 2008 work schedule.

References

1. ICAO, New Technologies Working Group, "Proposal for a Technical Report on Automated Border Control Systems", Working Paper 11, 13/09/2005, presented to 16th meeting of the Technical Advisory Group on Machine Readable Travel Documents, 26-28 September 2005, paragraphs 1.5–1.9.
http://www.icao.int/icao/en/atb/fal/mrtd/tagmrtd16/TagMrtd16_011_en.pdf
2. ICAO, Technical Advisory Group on Machine Readable Travel Documents, "Report", 17th meeting, 20–22 March 2007.
http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,startdown/id,20/
3. Gregor Költzsch, "Next Generation Border Crossing: ePassports and their impact on border control", Bundesdruckerei GmbH, Berlin.
http://www.3dface.org/files/slides/070322/3Dface-Koeltzsch-BorderControl-070322.pdf
4. Richard Norton, "e-Passports: Uses, Limitations, and Impact on Simplifying Passenger Travel Initiatives", June 2005.
http://nationalbiometric.org/publications/e-Passport%20Oct05.pdf
5. Paul Wilson, "Preparing for ePassports", *MRTD Report*, Vol. 1, No. 2 (2006), p. 41.
http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,startdown/id,6/

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 3 Legal Framework

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

3. Legal Framework

Adopting ePassports is a complex process, and if the program is to be implemented successfully, one of the first matters that needs to be addressed is reviewing the legal framework that underpins the production of passports. The “legal framework” could include the various laws, legislative acts, regulations or legal instruments of whatever kind through which a state prescribes how passports may be produced and issued.

Making changes to the legal framework, if that is necessary, can be a lengthy process. A number of APEC economies have introduced ePassports without needing to make any changes, or without needing major changes, in their legal framework (eg, Brunei, Canada, Hong Kong China, New Zealand, the USA). In some cases, all that was required was a change to regulations that set the fee for passports (eg, Japan, New Zealand).

Other countries found they required substantial changes in existing legislation to cover the introduction of ePassports and the collection of biometrics from passport applicants (Australia, Korea). In some instances, this process was complex and took several years.

ICAO: Issues to consider when deciding to make improvements to passport systems
Do you want to use a biometric in your passport? Have you verified that what you want to do in this realm is consistent with your country's laws?
http://icao.int/mrtd/guidance/IssExplanation.cfm

Issues that economies should take into consideration when reviewing their legal frameworks for ePassports are discussed below.

Does the legal framework cover the collection of biometric information?

It may be necessary to introduce specific legal provisions to allow for the collection of biometric identifiers from passport applicants. These provisions may specify how such collection is to be performed, which persons or class of persons are authorised to collect biometric identifiers, and how the data is to be conveyed to the body or bodies that will store the data and issue the passport.

Does the legal framework cover access to, and disclosure of, biometric information?

It may be necessary to introduce specific legal provisions to define which persons or class of persons will have access to collected biometric information, and for what purposes. Similarly, it may be necessary to define the circumstances under which biometric information may be disclosed, to whom it can be disclosed, and for what purposes.

ICAO: Issues to consider when deciding to make improvements to passport systems
- What is your interrelationship with other identity and citizenship document producers in your country? Do you wish to establish such relationships where they don't now exist (eg, for exchange of biometric data or breeder document data)?
- Have you verified that what you want to do in this realm is consistent with your country's laws?

http://icao.int/mrtd/guidance/IssExplanation.cfm

Does the legal framework cover the storage and disposal of biometric data?

It may also be necessary to introduce specific legal provisions for the storage and disposal of biometric data. This may involve reference to legal provisions relating to governmental archives and how government records are required to be stored or to the disposal of government records.

Does the legal framework allow for subsequent addition of other biometrics in the future, should that become necessary?

At present the only biometric that is required for passports by the International Civil Aviation Organization (ICAO) is a facial biometric, but some nations either have included another biometric (eg, fingerprints) as well, or have made provision for future inclusion of one or more biometrics.

How will the biometric data be used? Will it be used only for matters directly related to the issuance of the ePassport, or for other purposes, such as law enforcement?

- **Consider legal provisions to allow exchange of data either generally or specifically with other government agencies, and with other governments and/or international agencies.**

As increasing amounts of biometric data of passport applicants are collected and stored, authorities other than the passport issuing body, such as law enforcement agencies, may wish to use the data for checking against watchlists, such as lists of missing persons. If that kind of information sharing is anticipated, it may be necessary to introduce legal provisions to allow the passport data to be shared with other agencies or governments, domestic or international.

Do the legal provisions fit with privacy laws, if applicable? For example, do you need to add a provision to ensure that when a passport applicant is asked to provide biometric data, the applicant is simultaneously informed about how that data might be used (eg, for checking against watchlists, for law enforcement purposes)?

In some economies, the protection of personal information is regarded as being of considerable importance to citizens, and may be enshrined in law. In such circumstances, any new legal provisions that are introduced to allow for the production of ePassports, or for collection, storage or disclosure of biometric information, will have to consider privacy law. You may also wish to consider including in passport legislation specific provisions for the protection of data.

Case study: Australia

- The Department of Foreign Affairs and Trade commissioned its program to develop ePassports in 2001.
- Australia required new laws to implement biometric technology in passports.
- The biometric program was subject to **parliamentary scrutiny and extensive public consultation** throughout each stage of development.
- **New passports legislation** (Australian Passports Act) came into effect in July 2005. This legislation updated the passports law overall, including authorising the use of new biometric technology.

Did economies that have already introduced ePassports encounter any major obstacles relating to legal frameworks? Is it a long process for economies?

Each economy will have to assess what legal changes will need to be made in the light of its own existing legal framework. As all economies already issue passports within their own legal framework, in most cases there will be no major problems of *principle* involved in switching to ePassports.

The introduction of ePassports has taken several years for most economies that have already started to produce ePassports. Notably, the requirement of the USA that nationals of visa-waiver countries must have biometric passports was initially set for October 2005 but had to

be deferred to October 2006 after it became clear that the deadline could not be met by most countries. However, as more nations have now gone through the experience of changing to ePassports, others can benefit from that experience and avoid some pitfalls.

Links to useful information

1. Australian Passports Act (2005)
http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/all/search/3982C24F6D146070CA2572BA0082D806
2. Singapore Passports Act
http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_getdata.pl?actno=1971-REVED-220&doctitle=PASSPORTS%20ACT%0A&date=latest&method=whole&sl=1
3. Office of Technology Assessment at the German Parliament (TAB), "Biometrics and identity documents: Performance, political context, legal considerations", TAB Working Report No. 93, December 2003.
http://www.tab.fzk.de/en/projekt/zusammenfassung/ab93.htm
4. EU Consortium on Security and Technology, East-West Institute, "Information Security and Identity Management", December 2005.
http://www.enisa.europa.eu/doc/pdf/studies/EWIReport_Information_Security_and_Identity_Management.pdf
5. EU: Note from Presidency to Visa Working Party, Brussels, 24 June 2003 (02.07), 10857/03; LIMITE; VISA 109; COMIX 407
http://www.statewatch.org/news/2004/dec/visas-presidency-paper-03.pdf
6. Council of Europe, "Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005)"
http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/O-Biometrics(2005)_en.asp
7. Malcolm Crompton (Australian Federal Privacy Commissioner), "Biometrics and Privacy: The End of the World as We Know It OR The White Knight of Privacy?", 20 March 2002.
http://www.privacy.gov.au/news/speeches/sp80notes.doc

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 4 Financing Options

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

4. Financing Options

The introduction of an ePassport is a big undertaking for any economy, so one of the first things that will have to be considered is how the project will be financed. Although some existing passport production processes may be retained as the basis for ePassport production, the distinctive technological features of an ePassport mean that extra costs are inevitable.

Areas that are likely to entail additional costs include:

- Software and hardware costs;
- Installation of new machinery;
- Booklet and printing supplies;
- Chip units to be integrated into the passport;
- Implementation of new security measures;
- Changes in production processes and additional quality assurance processes;
- Training of staff;
- Allowance of a reserve facility to produce blank passports in case of emergency or disaster;
- Public information campaigns.

These areas and what is involved in each are discussed in subsequent chapters.

ICAO: Issues to consider when deciding to make improvements to passport systems
How much money do you have allocated to the project? Can you identify secondary funding sources should the cost of what you want exceed your estimates?
http://icao.int/mrtd/guidance/IssExplanation.cfm

Different Options for Funding

Several possibilities for funding an ePassport program are available, and economies may wish to consider which method suits their circumstances best. Four options that have been suggested are:

- Government funding—finance is provided by the government concerned;
- Privatisation—finance is provided by the private sector;
- Public-Private sector partnership—government and private sector companies share financing the project;
- Bilateral assistance from another government.

Government Funding

The government of an economy may choose to fund the introduction of an ePassport entirely from its own resources. This method has the advantage of giving the economy's government good control of the quality of all processes and of the final product, since the government can monitor progress closely at each stage. It would also permit a greater level of protection for the privacy of the biographical and biometric data that is collected. There may be advantages for the government in terms of how the economy's citizens perceive the government's level of social responsibility and how the government facilitates travel by its citizens to other economies.

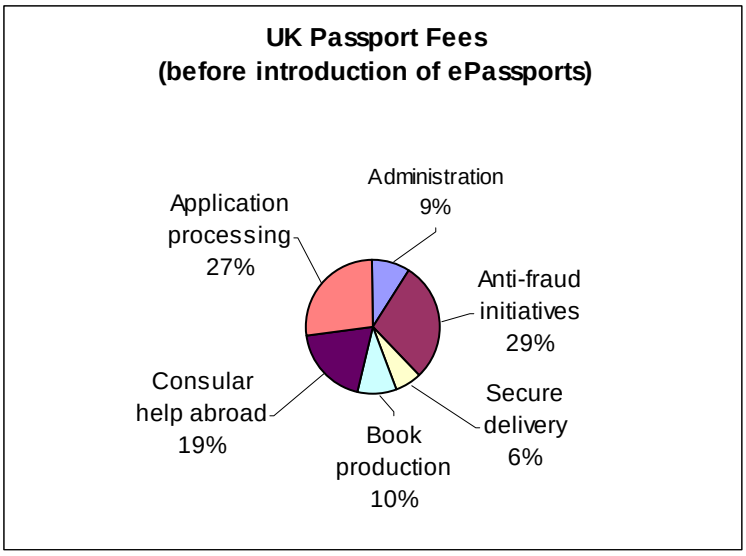
The big disadvantage of funding such a project from government resources is that it requires a large capital investment.

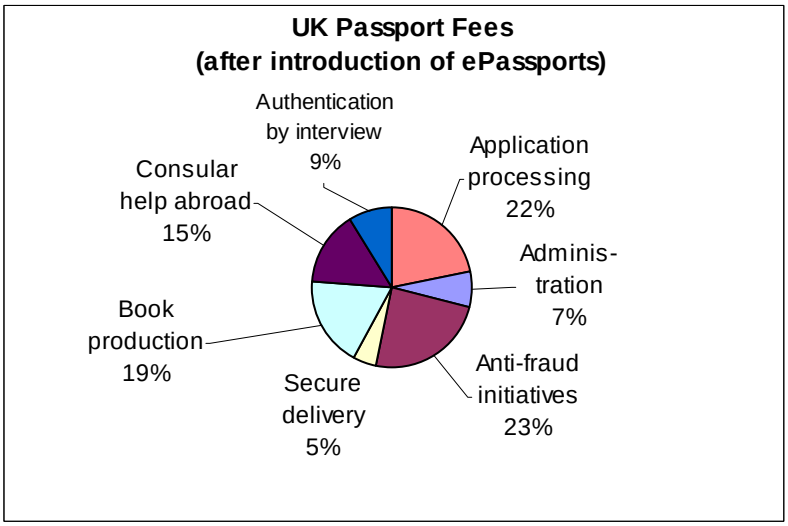
In the event that the government of an economy chooses to fund the ePassport project itself, it will need to decide the basis for setting the price of the ePassport. Options include:

- Full cost recovery (that is, the price of the ePassport is set at a level that will in time allow the government to recoup its costs);
- Subsidisation (that is, the price of the ePassport is set at a lower level than full cost recovery in order that citizens can more easily afford to obtain an ePassport).

Passport fees often represent the recovery of costs in many areas, not just the direct production of the passport booklet. Fees may also NOT recover costs, but be set at a particular level for political reasons.

Passport Fees: Example from the UK[1]





[1] Based on figures given in: National Audit Office (UK), "Identity and Passport Service: Introduction of ePassports", Report by the Comptroller and Auditor General, HC 152 Session 2006-2007, 7 February 2007, p. 11. http://www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf

ICAO: Issues to consider when deciding to make improvements to passport systems

Funding technology improvements is a major concern, but one which can allow for some creativity. Major ways to approach this include:

- Direct funding of the entire effort by the government;
- Advance funding of start-up by the government, but recipients of the documents assessed an apportioned fee that covers costs of issuance plus the improvements;
- Advance funding of start-up by a contractor, with receipts from passport recipients used to repay the contractor's costs plus a reasonable profit;
- Advance funding of start-up and operations by the contractor; with the fees set (and an agreed upon percentage given to the contractor) for their initial and continuing services. One note of concern: utilising contractors to produce your documents has many positives, but Governments should be careful to retain in the hands of direct hire government officials the judgments about who is entitled to receive a passport.

http://icao.int/mrtd/guidance/IssCosts.cfm

Case studies

Australia

Australia's biometric passport program was funded on a **full cost-recovery** basis—the passport fee was increased by A$19 to cover the additional costs of the ePassport (current cost of a standard 10-year ePassport is A$193 (US$143 approx)).

Japan

In Japan, the national budget covered the costs of developing ePassports and of issuing them once developed, while the various prefectures (regional governments) cover the costs of regional passport offices and staff to man them. The price of the ePassport was increased to cover costs.

New Zealand

The development of the New Zealand ePassport was funded through an increase in fees. All costs associated with the issuance of passports, including new developments in technology, are recovered through application fees. This is a legal requirement under the *Public Finance Act* and there is no crown funding. Fees were increased in November 2005 to cover the cost of a number of security related passport initiatives including the e-Passport.

Singapore

Singapore's ePassport project is funded on a cost-recovery basis. The ePassport fee was increased to cover costs.

Chinese Taipei

The ePassport will be self-financed on a cost-recovery basis, so passport fees will be raised to offset the higher costs of ePassports.

Privatisation

In some cases, the government of an economy may decide that the introduction of an ePassport will be funded wholly by the private sector. It is important to be aware that the basis of such an undertaking is that the service providers will make profits from ePassport production. For this reason, the economy will need to negotiate carefully with the service providers to ensure that prices are fixed for a certain initial period, that frequent changes to the fee charged to passport applicants are avoided, and that the actual cost of the ePassport is smoothed over time.

The privatisation route has certain advantages for economies. First, the financial implications for the government of an economy will be much lower than where the government funds the project itself. Second, the risks are shared between the private sector service provider and the government, and can be managed through carefully-written contracts.

There are some negative aspects of privatisation that economies will need to consider before deciding whether to follow this path or not. These include concerns about data privacy (will the personal data of citizens be satisfactorily protected?) and intellectual property issues. Further matters for consideration are that the management of a fully privatised project may be quite complex for the government concerned, requiring correspondingly complex legal provisions. There may be other social costs: for example, the cost of the ePassport may be higher than it might otherwise have been; if the service provider is a foreign company, there may be minimal flow-on of new technology and technical skills to citizens of the economy; and the profits may be sent abroad rather than being kept within the economy.

Public-Private Partnership

A partnership between government and the private sector is a third possible option for funding of an ePassport project. This option combines commercial participation with government authority, and can also involve cost-sharing with government departments other than just the passport-issuing authority. Areas of cooperation could include database set-up and maintenance, back-end systems (the server side of a client/server system, as distinguished to the front end or client side), front-end system (the client side of a server system), and the security system.

Case study: Thailand

The Thai passport authority decided to outsource the project. The vendor was responsible for the total investments for book printing, hardware and software equipment for routine work and the back-up system, software application development, employment of staff for the enrolment process and production services, as well as for the overall training program.

The main reasons for outsourcing the project were:

- sound finance on the part of the government as the project would involve a large sum of finance;
- the Ministry could optimise the best technology expertise from the best vendor in developing and implementing the project;
- the shortage of biometric technology expertise on the part of the Ministry.

The vendor is a consortium composed of a Thai and a foreign company—Chan Wanich Company Limited, that is a famous for security printing in Thailand, and NEC Solutions Asia Pacific Pte. which has lots of experience with biometric technology.

The advantages of this kind of public-private partnership are that the private sector finances the project, so the government does not have to provide large investments of capital funds, and that the synergy effect of a good and effective public-private relationship can influence uptake of the technology and increase acceptance.

The disadvantages are that risks may be unclear, because responsibilities are shared; that the financial status of contractors has the potential to threaten the project; and that there may be management problems that the government will have to manage skillfully. Nevertheless, this may be a good option for some economies.

Bilateral Assistance from Another Government
A fourth option for economies may be that assistance for production of an ePassport is offered on a bilateral basis by another economy.

The Philippines to ask Japan for P1-B loan for ePassport project
A news report posted on the Internet says The Philippines government will ask Japan for assistance to develop an ePassport. Documents from the National Economic Development Authority (NEDA) indicate that the ePassport project seeks to develop ePassport issuance and biometrics-based screening systems to prevent counterfeiting and forgery and the multiple issuance of passports. The project is still under review by the NEDA.
http://www.gmanews.tv/story/46254/RP-to-ask-Japan-for-P1-B-loan-for-e-passport-project

Which Option to Choose?
The ultimate decision depends on many factors—the business needs of the economy, its financial situation, the expectations of its citizens, the maturity of the economy's infrastructure and technical expertise—and there is no one correct option. **Each economy must choose what is best for itself.** The International Civil Aviation Organization (ICAO) offers information to assist with making such decisions, and other APEC economies that have already introduced ePassports are also willing to provide information on the basis of their experience.

Risks and Risk Management

Despite the best intentions and thorough planning, unforeseen events can occur which may disrupt a project such as rolling out an ePassport and cause costs to increase enormously. This kind of risk is impossible to predict, but some provision must be made to deal with eventualities such as the following should they occur:

- Sovereign risks, such as unanticipated instability in the government or in the economy;
- Devaluation of the local currency;
- Labour unrest or political unrest;
- Technical issues with implementing biometric technology;
- Other technical issues, such as those related to interoperability with existing systems.

Damage from such risks can be mitigated to a certain degree by developing strategies for managing them, and further information about risk management can be found in Chapters 11 and 12. Certainly a thorough assessment of investment and finance-related risks should be carried out before the project starts, to ensure that the short-term and long-term risks have been considered.[2]

Reference

1. International Forum for Travel Documents (IF4TD), Presentation. Contact: sjef.broekhaar@bprbzk.nl
http://www.icao.int/icao/en/atb/MRTDsymposium/MRTD_06/Presentations/Broekhaar.pdf

[2] For an interesting account of risk-management, see UK National Audit Office, "Identity and Passport Service: Introduction of ePassports", Report by the Comptroller and Auditor General, HC 152 Session 2006–2007, 7 February 2007.
Full Report: http://www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf
Executive Summary: http://www.nao.org.uk/publications/nao_reports/06-07/0607152es.pdf

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 5 Establishing Identity and Collecting Biometrics

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

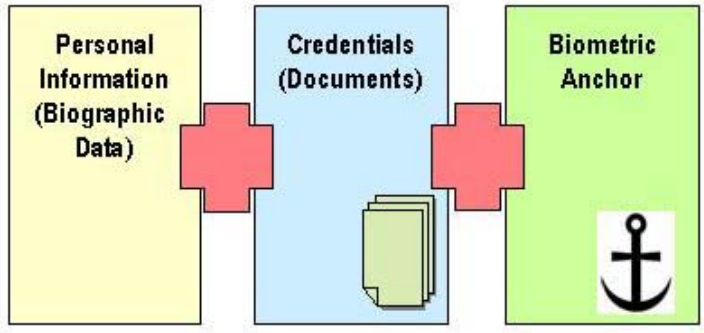
5. Establishing Identity and Collecting Biometrics

Establishing identity is a major purpose of travel documents, and international confidence in the identity of those who travel is essential. Secure travel documentation is at the heart of supporting that confidence and requires that the appropriate steps are taken to ensure that the identity of the holder is thoroughly established before any travel document is issued.[1]

The identity of a passport applicant is usually established by a combination of biographical attributes (such as name, address, date of birth, gender, nationality, sample signature and a description of a person's physical characteristics) and important documentary credentials (such as a driver's licence, birth certificate, or national identity card). These credentials are verified by the production of the relevant document or by successfully completing a data match with the relevant electronic record. (Please note that some economies no longer use documents for checking identity, but have moved fully to checking of relevant electronic records such as births, deaths and marriages databases.) How identity can be established will be discussed later in this chapter.

Because it is widely recognised that a person might change their biographical details and that documents can be tampered with or forged, the key aspect of the introduction of biometrics in ePassports is to "anchor" identity, so that the passport issuing agency can be sure that one person has only one passport in one identity. As a paper prepared for the 2005 G8 meeting puts it:

> Biometric technologies do not establish identity—they confirm the physical features of an identity claimed by the person whose biometric is used—whether the identity claimed is genuine or not. Once assigned, biometrics limit the individual to one specific identity and curtails ability to travel or obtain other travel documents of the issuing state using multiple identities. Authentication of identity is therefore particularly important before any biometrics information is attached to that identity. It is recommended that biometrics, reading equipment at the borders, and access to one-to-many as well as one-to-one matches, should be adopted at the first practical opportunity.[2]



Enrolment—defined as the process of collecting, vetting, and storing an applicant's personal information—is the foundation on which document integrity is based. If the enrolment process is undermined, the document is compromised, despite its advanced security features. The very belief or perception that an enrolment process can be undermined casts doubts on the integrity of the overall process (and on the documents it produces).

[1] G8 Lyon-Roma Group, Migration Experts Sub-Group, "Authenticating Identity Underlying the Issuance of Travel and Identity Documents", May 2005. We are indebted to this paper for a large part of the discussion in this chapter.
[2] Ibid.

Establishing Identity

All economies have processes for establishing the identity of applicants for their passports, but for the reasons alluded to above, the introduction of ePassports may offer opportunities for economies to enhance existing processes. This chapter sets out best practice for establishing identity.

Establishing Identity—The Applicant

Establish, as far as is practicable, the eligibility of the applicant for the ePassport, ie, is the applicant really a citizen of your economy and entitled to get a passport? This is usually done by checking relevant databases or documents such as birth certificate, citizenship or naturalisation certificate, or other identity-related documents that have been supplied by the applicant. It could also involve checking the applicant against available watchlists or databases in order to uncover past actions of the applicant that might disqualify the applicant from getting the document.

ICAO: Issues to consider when deciding to make improvements to passport systems

If you intend to replace your previously-issued passports before they are due to expire (which may be the case if your previously-issued passports can be easily altered or counterfeited, for example), how do you verify that the holders of those passports did not obtain them fraudulently?

http://icao.int/mrtd/guidance/IssExplanation.cfm

Acceptable Documentation—Authentication

Documents have two essential functions: those that establish an identity, and those that prove the applicant is the person entitled to that identity. Two questions must be answered affirmatively:

- Is the identity a real one?
- Is the person applying for the passport the genuine owner of that identity?

Normally, in cases when authentication is done through checking of documents rather than by checking of database information, original documents should be required. All applications and supporting documents provided by the applicant should be physically examined. Staff will need to be trained to be familiar with any safety features such as watermarks, typeface, materials used, and general appearance of supporting documents. If necessary, confirm details on documents against the original entry on a register. Check any discrepancy, either by cross-reference with other reliable sources of documentation and/or direct questioning of the person.

ICAO: Issues to consider when deciding to make improvements to passport systems

Do you have one-person-per-passport as recommended by ICAO? Do you intend to convert to that system?

http://icao.int/mrtd/guidance/IssExplanation.cfm

All new passport applications, and applications for passport renewal, should be checked against existing databases, to verify the identity of the applicant (by checking biographical information and/or for social footprint—see below), and to ensure that the holder does not already have a passport in another identity (by checking the biometric identifier, if a database that holds biometric identifiers is available).

Case study: Australia

Facial Recognition (FR) is a photo-matching system that will identify an individual according to the measurements of his/her face. It can be a key to fraud detection. FR software compares a range of facial dimensions and displays likely matches in priority order. FR is not discriminatory (ie, it is not based on race, colour, age or sex) but is purely mathematical.

(*cont. over*)

The FR matching process can perform several functions:

- It checks the image on a new application against all images recorded (**1:Many**);
- It matches the image on renewal application with previous image (**1:1**);
- It can also check an image against watch-lists for fraud, or against a database of lost or stolen passports (**1:Few**).

A FR matching process, integrated into the Australian passport issuing process, was introduced concurrently with the ePassport. Prior to passport issue every applicant's image is matched against the image database (currently 6.5 million) to combat identity fraud.

Primary and secondary documents

"Primary" documents bear identity details and are issued by a trusted government or other official source, and have already been subject to a high level of verification by trusted personnel before being issued. In some economies, birth or marriage certificates may be classed as "primary"; in other economies they will not. Classification of this type will be for each economy to decide.

Examples of primary documents include:

- existing passport or identity card records and databases;
- official records for births, marriages, or deaths;
- records of naturalisation and immigration.

TIP: It is a common form of impersonation for a birth certificate to be obtained and used in relation to a person who has died. It is therefore important that it is established that no recorded death certificate exists.

"Secondary" documents are generally not acceptable as evidence of identity when presented in isolation. This type of document can, however, contribute to the overall evidence of identity when presented along with other forms of documentation.

Examples of secondary documents include:

- evidence of enrolment on register of electors;
- census records, land registry or real estate ownership and residence records;
- medical records, hospital registration, or medical insurance records;
- social security, national insurance, welfare benefit records, or tax records;
- employment records;
- driving licence or motor vehicle ownership records;
- reference to local authority records, or local or national police records.

Most economies provide a list of documents that are mandatory, plus a list of other documents that will be accepted as secondary documents to verify an identity.

Most economies will not accept a passport application without full documentation. In some cases, the applicant will be asked to present secondary documents that may verify his or her identity, and a decision whether to issue the passport or not is made on a case-by-case basis.

Social footprint

A "social footprint" is the impression each individual leaves within the community by their personal involvement in the events or interactions within society at large. Such information, usually built over a long period of time and through a combination of varied sources, is difficult to falsify successfully. Sources of this type of information include:

- school attended—where, when and how long?
- qualifications achieved—certificates, awards (official records);
- academic qualifications gained—what, where, when?
- employment history;

- bank reference, credit card statements—could show an address, and possibly corroborate employee or employer information if salary is paid into account;
- utility bills (gas, water, electricity) or rent payment records should confirm address and show usage of utilities;
- checking against commercial databases can confirm credit card and other financial checks.

Case study: The UK's 'Personal Identity Project'
As a way of improving their system of identity authentication, the UK Passport Service checks the "biographical footprint" of applicants—that is, the basic facts of an applicant's life, such as name, date of birth and address—against information held in other databases such as National Insurance or driving licence records. Applicants are asked to attend in person for an interview that makes use of information verified in the first stage of application. This process makes it more difficult for someone to pretend to be another person when applying for a passport. When it has been confirmed that the identity has not been stolen, the biometric in the passport links to the document to the individual and will prevent any future attempt by any other person to obtain a passport in that identity.

Review of Breeder Documents
Breeder documents are those that are widely trusted and frequently used as the basis for issuing secondary documents. Birth certificates are an example. Because the establishment of identity is so crucial for the issuance of ePassports, it may become necessary for economies to consider reviewing how breeder documents, particularly those classified as primary documents, are issued and recorded.

- Are breeder documents secure and securely issued? If not, they may be used easily to support fraudulent passport applications.
- Are sufficient checks made to confirm legitimacy of breeder documents submitted with passport applications?
- Is old data available in a format that is easily used for checking? If not, the economy may need to consider re-formatting it, eg, digitalisation for electronic storage (converting paper documents to electronic format).

Case study: Australia
Australia is establishing a national **Document Verification Service (DVS)** as part of efforts to enhance procedures for verifying the integrity of key identity documents. The DVS will be a secure, electronic, national, real time, on-line system accessible to all accredited Australian Government, state and territory agencies, and potentially by the private sector. It is intended that the DVS allow participating agencies to verify that:

- a document was in fact issued by the document issuing agency claimed on its face;
- the details recorded on the document correspond to those held in the document issuing agency's register;
- the document is still valid (ie, has not been cancelled or superseded);
- the document has not been lost or stolen.

It is intended that the verification process consist of the following steps:
- A person presents their proof of identity (POI) documents to an agency in support of their application for a benefit or service;
- The individual authorises the agency to undertake checks to verify the document;
- Details on the identifying document such as name, date of birth, official registration number of the document, or other identifying features are entered into a computer system linked to the DVS;
- The information is sent via a secure communications pathway to the document-issuing agency where an automated check of the agency's register will verify whether the information provided is identical to the information on the document;

(*cont. over*)

- If the information provided matches the information held by the issuing agency, a YES response is transmitted to the inquiring agency informing them that the document has been verified. Otherwise, a NO response is returned indicating that the document details were not verified.

ICAO: Issues to consider when deciding to make improvements to passport systems
What is your interrelationship with other identity and citizenship document producers in your country? Do you wish to establish such relationships where they don't now exist?
http://icao.int/mrtd/guidance/IssExplanation.cfm

Authentication of Identity Process
Evaluation and acceptance of evidence presented should take place only after the evidence has been checked and it is established that it meets the required level of confidence in that identity. Both the quality and quantity of evidence presented will contribute to the overall weight of evidence and the final decision that an identity should be accepted and authenticated.

ICAO: Issues to consider when deciding to make improvements to passport systems
Do your citizens have to appear in person to apply for a passport?
http://icao.int/mrtd/guidance/IssExplanation.cfm

Face-to-face interviews or not?
First-time applicants. Individual economies will need to consider whether to require applicants to appear in person as part of the authentication of identity process. There may be some advantage to requiring an interview, especially for those applying for the first time, or where a previous document has been lost. It provides an opportunity to question the applicant on the detail of their application, and enables biometric identifiers to be taken and confirmed by the issuing authority.

Renewals. With renewal of a passport, economies should consider whether the same level of checks should be applied as to a first-time application. Facial recognition technology can be incorporated as part of the passport renewal process to assist with detecting imposter or multiple identity frauds. Checks against the database of facial biometrics should be done first at **1:1**, to ensure that the applicant is the same as the originally verified holder of the document, then **1:Many**, to prevent the person from using more than one identity.

Application options
- All applicants must apply in person and have an interview, to allow capture of biometrics
- First-time applicants must apply in person, but renewals can be done by mail
- Proxy or agent may submit application

If face-to-face interviews are not feasible
If face-to-face interviews are not feasible, economies should consider what sort of guarantees will be needed to ensure integrity of the biometric data and the identity of the applicant.

One possibility would be verification of the identity by a trusted person who knows the applicant. Trusted persons might include government officials of long standing, doctors, lawyers, justices of the peace, teachers, police, etc.

Outsourcing of interviews
It may be possible for the interview process to be outsourced to a third party. Some economies have contracts with outsourced providers to perform interviews and/or take the biometric identifier. For example:

- at post offices (Australia, Canada, the USA);

- at local government or district offices (Japan, Korea).

Attachment of Authenticated Identity to the Applicant: Biometric Data Collection
With the introduction of ePassports, when a biometric identifier will be included in the passport, it is vital that there should be a secure process for attaching that biometric to the identity of the applicant. Once the identity of the applicant has been satisfactorily established, the next crucial stage is to ensure that this "authenticated identity" is appropriately attached to the rightful owner of the identity. Great care is needed to ensure that others do not assume authenticated identities through a breach in the security of the authentication process.

The **enrolment process** involves the capture of a raw biometric sample from each applicant and the recording of the applicant's biodata. The **capture process** is the acquisition of the biometric via a capture device such as a fingerprint scanner, photograph scanner, live-capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process—for example, standard pose facing the camera head-on for a facial recognition capture; whether fingerprints are captured flat or rolled for fingerprint capture; eyes fully open for iris capture. The **storage** of "optimally-compressed images" is mandatory. Storing optimally-compressed images ensures maximum flexibility and vendor independence for both current and future biometric matching requirements.[3]

For some economies it is not feasible to require that biometric identifiers must be given in person (ie, directly to the passport issuing authority or other officially outsourced provider). The important matter is to ensure that whatever method an economy uses to collect the biometric identifier(s), the data collected must meet relevant standards for use in an ePassport.

For some economies, collection of the biometric will rely on the facial image from a photograph submitted through the postal system with the application. In those circumstances, a passport official or an agent acting for the passport issuing authority may not have seen the applicant. In such cases, **it is vital that the photograph or facial image of the application should be verified** (that is, certified as relating to the identity claimed, by means of certification by a known, trusted and reliable third party that can be contacted and has also had their identity verified independently). It is therefore even more critical that the steps taken to establish the applicant's identity are comprehensive.

Integrity of the passport enrolment process
The integrity of the enrolment process is primarily compromised by fraud and processing errors (involving applicant information). Enrolment fraud is committed when, for example, an applicant obtains one or more illicit identity documents by claiming an identity other than his or her own. Process errors are attributable to administrative mishandling and include wrongly-entered demographic data and poorly acquired biometric images, which impair the ability to authenticate the holder's identity when the document is inspected.

Basing the enrolment process on the International Civil Aviation Organization (ICAO) recommendations and "best practices" for ePassport handling and issuance not only allows fraud and process errors to be mitigated, it also maximises the end-to-end integrity of the eID (electronic identity) enrolment process. In practice, this necessitates the introduction of measures at each phase of the enrolment process, which covers data collection, vetting and storage. This way, the security and integrity of the overall process can be safeguarded. Maintaining the integrity of the data collection phase calls for measures that guarantee the accuracy, quality and authenticity of applicants' identification and demographic information.
(*cont. over*)

[3] "Technology landscape: Eyes on the chain", *Keesing Journal of Documents & Identity, Annual Report e-passports 2005–2006*, pp. 4–7.

Necessary factors

Trustworthiness of officials

- Officials must be capable and trustworthy
- Skills and trustworthiness must be assessed on an ongoing basis
- Must recruit carefully
- Keep audit trail of network transactions performed by officials
- Ongoing training is critical
- Provide automated support tools that automatically capture and format biometric data to ICAO standards (to minimise number of low-quality images and scans)

Secure storage is important

- Collected and vetted identity information must be stored in secure yet accessible environment
- ICAO guidelines for ePassport data storage emphasise use of encryption techniques and electronic security locks (PKI) to protect stored data
- Ensure software avoids compression-related data degradation (balance between size and image quality)

Hugh Gilenson, "E-passport security: Implications for eIDs: Maintaining the integrity of the enrolment process", *Keesing Journal of Documents and Identity*, Issue 15, 2005, pp. 31–33.

Biometrics: ICAO Guidelines

ICAO Recommendations

Facial recognition is the biometric mandated by ICAO for inclusion in ePassports, for reasons of global interoperability. **This means facial recognition must be addressed as the priority.** Finger and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing State.[4]

Economies may consider whether to deploy a second biometric, for their own economy's use or for bilateral use. This may be particularly relevant if the economy has an existing fingerprint or iris database from another government program (such as for an identity card) against which biometrics submitted with passport applications can be verified.

Which ICAO-compliant biometric identifiers have other economies used?

- Facial image only (Australia, Hong Kong China, Japan, New Zealand, the USA)
- Facial image and thumbprint (Brunei, Malaysia)
- Facial image and fingerprints (Singapore, Thailand, Korea)

ICAO Photograph Guidelines

In order to maximise effectiveness of facial recognition and interoperability, photographic guidelines have been developed by ICAO for use in ePassports. These guidelines are available online at: http://mrtd.icao.int/downloads/publications/Technical_Reports/Annex_A-Photograph_Guidelines.pdf.

Although photographs are a common component for recent passports, economies that intend to issue ePassports should **review their existing photo capture requirements** to ensure that all new facial images captured are compliant with the ICAO photographic guidelines and compatible with facial recognition technology once it is implemented. This will maximise the number of ICAO-compliant images that will be available, which will in turn increase effectiveness of facial recognition once it is in place.

[4] ICAO Recommendation: http://icao.int/mrtd/biometrics/recommendation.cfm

It may also be helpful to **review existing image databases** in order to decide whether to normalise quality; that is, whether to digitalise existing images so they will be compatible with facial recognition technology and can be used to check an application as described above.

Many economies allow passport applicants to submit paper photographs with their applications. These photographs may be taken in several ways: by professional photographers, by individual applicants, or at photo booths. As a result, **it is important that economies publicise the ICAO guidelines** (for example, as part of passport application forms) and **work with the photographic industry** to ensure that the ICAO guidelines are understood and complied with.

Biometric Image Quality and Format
The ePassport specifications in ICAO Document 9303 incorporate standards developed by the International Organization for Standardization (ISO) for each type of eligible biometric (ie, a face plus fingerprint and/or iris, if desired). These standards establish criteria and procedures for biometric capture processes to help ensure that biometric samples are acquired with adequate fidelity and format to meet ICAO's requirements.

ISO/IEC biometric standards included in ePassport specifications
- Facial Image Format for Interoperable Data Interchange (ISO/IEC 19794-5)
- Iris Image Format for Interoperable Data Interchange (ISO/IEC 19794-6)
- Fingerprint Image Format for Interoperable Data Interchange (ISO/IEC 19794-4)
- Fingerprint Minutiae Format for Interoperable Data Interchange (ISO/IEC 19794-2)
- Fingerprint Pattern Format for Interoperable Data Interchange (ISO/IEC 19794-3)

Biometric image quality and format are discussed further in Chapter 9.

Storage of Biometrics on ePassports—Integrated Circuit Chips
The second part of the ICAO recommendation concerns the storage of biometrics on high-capacity contactless integrated-circuit (IC) chips. Further information on selection of chips (eg, size), what should be stored on them and how are discussed further in Chapters 6, 8 and 9.

Lodgment of Passport Applications

How ePassport applications are lodged and how finished ePassports are distributed to their holders can have a very important impact on the integrity of the identity established for an ePassport and the linkage of a biometric to that identity.

ICAO: Issues to consider when deciding to make improvements to passport systems
- Do you want a centralised or decentralised issuance system? If the latter, how many issuance locations do you want?
- Do you issue passports from your embassies in other countries? If so, are they the same as domestic issue passports? Do you want them to be?
- Do you mail out most of your issued passports, or must the applicants come in to pick up their passport?

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Methods for Lodging ePassport Applications
Passport application lodgment methods should be reviewed when an economy implements an ePassport, particularly if applicants must present in person for a subsequent face-to-face interview when establishing their identity or collecting their biometric.

In general terms, passport applications can be lodged in a number of ways:

- in person;
- on-line;
- by mail;

- at a passport office;
- at a district/regional office.

Most economies offer more than one method for lodging passport applications.

Case studies: Current practice for passport application lodgment

- Some economies allow an application to be made only at a passport office (Hong Kong China, Malaysia, Thailand). Within this requirement, several options may be available, such as lodging the application at the counter, or putting it in a deposit box, or applying through a kiosk machine at the passport office (live thumbprint needed).
- In some economies applicants may apply only in person (Japan, the Philippines, Thailand, the USA (first-time applicants)); in other economies, applications can be lodged either in person or by mail (Canada, Hong Kong China, New Zealand).
- In one economy, applicants can apply on-line, but the application must be printed in hard copy, signed and submitted (Canada).
- In one economy, the *entire* application process can be done on-line (ie, the applicant can apply, submit the application, and make payment on-line) (Singapore).
- In some economies an agency other than the passport office, such as post offices, courts, libraries, or designated municipal or regional government offices, may be authorised to accept passport applications, in order to increase the number of places where people can apply (Australia, Canada, the USA).
- In one economy, receiving applications, reviewing them, ID checking, printing of ePassports, and delivery are all entrusted to prefectural governments (Japan).

Economies may need to review their procedures for the issuance of travel documents to their overseas citizens. Consideration may need to be given to the repatriation of passport issuance or the development of an alternative Emergency Travel Document process.

Collection of Finished Passports

Similarly, finished passports may be delivered to the holder in various ways.

Case studies: Current practice for passport collection

- Collection through walk-in, live thumbprint needed (Malaysia).
- Finished passport is mailed or couriered to applicant (Australia, New Zealand (courier only), the USA).
- Applicant must collect passport in person from passport office.
- Applicant may authorise a proxy to collect the passport if the applicant has already attended the passport office during the application process (Singapore).

Economies should be aware that around the world problems with theft or loss of passports delivered by mail have been encountered. This can lead to the use of lost/stolen passports for fraudulent purposes, and may influence some economies to require applicants to collect their ePassports in person.

References

1. Michael A. Caloyannides, “Insider threats to document security”, *Keesing Journal of Documents & Identity*, Issue 18, 2006, pp. 25–27.
2. Francis Fungsang, “U.S. E-Passports: ETA August 2006: Recent Changes Provide Additional Protection for Biometric Information Contained in U.S. Electronic Passports”, *I/S: A Journal of Law and Policy*, Vol. 2, No. 3, pp. 521–46.
http://www.is-journal.org/V02I03/d-fungsang.pdf
3. Hugh Gilenson, “E-passport security: Implications for eIDs: Maintaining the integrity of the enrolment process”, *Keesing Journal of Documents & Identity*, Issue 15, 2005, pp. 31–33.
4. G8 Lyon-Roma Group, Migration Experts Sub-Group, “Authenticating Identity Underlying the Issuance of Travel and Identity Documents”, May 2005.

5. Frans van Kleef, “Biometrics in the Dutch passport: 2B or not 2B contributes valuable experience”, *Keesing Journal of Documents & Identity*, Issue 14, 2005, pp. 19–20.
6. Joel F. Shaw, “ICAO Standards in Practice: Technical Deployment of Biometric Systems”, Presentation to APEC Business Mobility Group Capacity Building Workshop on Biometric Technology in MRTDs, Hong Kong, China, 19 July 2006.
7. Kevin Sheehan, “UK strengthens identity authentication: Focus on biographical identity to improve e-passport security”, *Keesing Journal of Documents & Identity*, Issue 15, 2005, pp. 7–10.

Other ICAO reference documents, including technical reports as well as reports from various working groups, are available on the ICAO website:

ICAO Technical Reports
http://icao.int/mrtd/download/technical.cfm

ICAO Biometrics Deployment Technical Report, Annexes A – D.
http://www.icao.int/icao/en/atb/fal/mrtd/tagmrtd15/Docs/index.html

Use of Contactless Integrated Circuits in Machine Readable Travel Documents
http://icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf

Further information on ISO standards can be found on its website:

ISO/IEC JTC 1—Home page
http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/customview.html?func=ll&objId=327993sc37/default.asp

ISO/IEC JTC 1 SC 17: Cards and personal identification
http://www.sc17.com/index.cfm?pageTitle=About%20SC17&DepartmentID=1&HAT=7830234901180334832768-07470012-855896&ts=07470012-991702

ISO/IEC JTC 1 SC 37: Biometrics
http://isotc.iso.org/livelink/livelink?func=ll&objId=2262372&objAction=browse&sort=name

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 6 Operational Issues

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

6. Operational Issues

The introduction of an ePassport will require numerous changes in an existing passport production regime, necessitating a comprehensive review of existing operational infrastructure and processes in the early stages of the project. Such a review will identify which processes can be modified and where new processes will have to be introduced. It will be vital to manage carefully how the changes are implemented and how new processes are integrated into existing systems.

Although change on such a scale will inevitably be stressful and demanding, economies may find that integrating biometrics into existing passport production processes can provide a beneficial opportunity to evaluate and improve current infrastructure and processes.

TIP: "I hope you have supportive bosses. The inclusion of integrated circuits, antenna arrays and biometrics into passports is a revolutionary departure from our previous paper-based machine-readable travel documents. Revolutionary change generally isn't easy. Having supportive executives at the head of an agency or department is essential to the success of this effort. Not only do they have to buy into the program, they must understand that delays are likely, that budgets may need to grow and that new issues will arise that require action. It is an ideal situation if your senior management understands that introducing biometrics is 'hard' and that this process may not always go smoothly."

Frank E. Moss, "The development of the American e-passport", *Keesing Journal of Documents & Identity*, Issue 17, 2006, pp. 22–24.

Project managers should keep in mind that the chosen ePassport platform will need to be flexible enough to accommodate the addition of new features that might be required as work on standards for Machine Readable Travel Documents (MRTDs) progresses and as the International Civil Aviation Organization (ICAO) requirements change.

Operational matters that will need to be considered include:

- IT structure—software, hardware (including chips), IT security issues, integration with existing IT systems, interoperability with international systems (including Public Key Infrastructure (PKI), Public Key Directory (PKD));
- Staffing—recruitment, training, transfer of knowledge to or from outsource workers;
- Management of change—incorporation of new processes, changes to existing processes, workflow, documentation;
- Physical and process security—review of security chain to ensure integrity of all processes, audit and reporting.

ICAO: Issues to consider when deciding to make improvements to passport systems

- Do you want a centralised or decentralised issuance system? If the latter, how many issuance locations do you want?
- Do you issue passports from your embassies in other countries? If so, are they the same as domestic issue passports? Do you want them to be?

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

IT Structure

Software

The introduction of new software will be a major requirement for the manufacture of ePassports. When considering software requirements, it is most important to keep in mind that there are established international standards relating to the software aspects of ePassport production: for scanning biometric identifiers, for transfer of data (for example, from

the biometric scanner to where the data is stored), for storage of biometric data, and for exchange of data with other agencies, domestic or international (such as with law enforcement agencies). It is essential that ePassports conform with ICAO standards as a minimum requirement, so that other economies will be able to read the data that is stored on them.

In order to make a decision about what is needed, economies will need to be clear about how they will use the biometric information that they capture for the ePassport. As has been described in Chapter 5, the process of authenticating and verifying the identity of passport applicants may be (or become) part of a wider identity management strategy for the government of an economy, and the biometric and biographical information that is gathered may be valuable for other government activities, such as for law enforcement or for checking entitlement to social welfare. If such use is envisaged, involving the transfer or exchange of data, an economy will need to pay particular attention to ensuring that the appropriate standards are met so there will be no problems of interoperability down the track.

Economies can choose from numerous brands and types of software produced by many vendors: there is no single solution that will be appropriate for every economy. Each economy must decide what suits its circumstances best—but whatever is the final choice, the bottom line is that the ePassport that is produced must comply with ICAO standards.

The following list of software that might be required is a guide only, and is not intended to be definitive:

- Software for biometric capture—to create electronic digital templates that are encrypted and stored and can then be compared to encrypted templates derived from "live" images in order to confirm the identity of a person. The templates are generated from complex and proprietary algorithms and are then encrypted using strong cryptographic algorithms to secure and protect them from disclosure;
- Facial recognition software;
- Quality assurance software, to ensure that facial images match ICAO standards;
- Software tools for auditing the production process;
- Database software for storing the biometric templates and biographical information of passport applicants;
- Data warehouse software (a data warehouse is a database for storing data that has been copied from operational systems, then modified and combined to make it suitable for analysis and reporting on by business-orientated users).

If biometric identifiers are to be used for checking the identity of applicants, any existing databases may need to be upgraded or replaced, and old data may likewise need to be formatted to be useable with new systems.

ICAO: Issues to consider when deciding to make improvements to passport systems

- Include in your requirements the need for a headquarters test facility for testing contractor software improvements.

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

One further matter needing careful consideration relates to network bandwidth. It will be necessary to have adequate capacity for transferring data. Don't economise in this area.

Hardware

Hardware needs will include:

- Contactless integrated circuit chips (these will be discussed below);
- Computers, printers, scanners, etc;
- Photo sample capture and positioning devices;
- Passport readers for border control points (these will be discussed below);

- Sample passport readers for citizens to check the data on their passports (an ICAO requirement);
- Production line machinery, such as high-grade printers or machinery to provide special security features.

Chips

Typically, three major systems are involved in the ePassport-to-reader communication process: the chip, the reader, and the host computer associated with the reader.[1] The first, and most prominent, is the contactless integrated circuit (or chip) that is embedded within the passport. Interoperability tests have clearly shown that not all chips are created equal: while some are very generic in their physical design, others have hardware architecture that is optimised specifically for use in applications similar to ePassports. Since the architecture of the chip is a key contributor to performance, and the computing power and capabilities of the chip have a significant impact on the ePassport-to-reader performance, it would be wise for passport issuing authorities to select chips that offer an appropriate level of performance.

Two additional chip-related performance issues are the type and data rate of the chip. ICAO allows two types of chip, so it would be pointless to use readers that are not automatically capable of working with both Type A and Type B chips. Type B chips are typically more complex and may therefore exhibit different performance characteristics to Type A chips.[2]

The ICAO ePassport technical documents reference the ISO/IEC 14443 specifications, which in turn stipulate the data rates of the chip—either 106 kbps or 424 kbps. The data rate supported by the chip will have an impact on the performance of chip-to-reader communications. Faster chips are also available, but for the moment, there seems no clear advantage to using higher data rates.

The software that is running on the chip includes the operating system and the Logical Data Structure application, and both will affect performance. Optimal performance cannot be expected from a broad-featured or generic operating system, nor, in terms of the ePassport application, from a recycled retail Radio Frequency Identification (RFID) application. ISO/IEC 14443and ISO/IEC 15693 lay down the radio frequency to be used in the chip.

The Logical Data Structure is the format in which the personal data is stored on the chip. This data structure has been mandated by ICAO, but has been subject to ongoing revisions as well as misinterpretations. **Economies should ensure that they are working with the latest version of the ICAO technical directives, and are also advised to perform a broad suite of interoperability tests before releasing any ePassports.**

These key performance factors are under the control of the ePassport issuing authority, and must be thoroughly understood and managed prior to formal execution of the document issuing process.

When determining the size of the chip, passport-issuing authorities will also wish to consider factors such as how much data is to be stored now and what additional information may be stored in the future, and technical issues to do with compression of data on the chip. The more data is stored in the chip, the longer it takes to read out at border control points, which may become an issue for other economies. ICAO has recommended target retrieval times as a goal for inspection systems and ePassports to aim for.

See ICAO: “Use of Contactless Integrated Circuits In Machine Readable Travel Documents”. http://icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf

[1] For this discussion, we are indebted to Todd Kealy, “Developing ePassport solutions that work”, *Keesing Journal of Documents & Identity*, Issue 14, 2005, pp. 6–8.

[2] For information about Type A and Type B chips, see, OTI America, “ISO 14443: An introduction to the contactless standard for smart cards and its relevance to customers”. http://www.otiglobal.com/objects/ISO%2014443%20WP%204.11.pdf

Chip options used by APEC economies	
Australia	512kb
Brunei	72kb
Hong Kong, China	Chip Type: ISO 14443 Type B Memory: 64kb EEPROM Digital Signature Algorithm RSASSA-PSS
Japan	ISO/IEC 14443 Type-B NV Memory: 32kb and 512kb (tender requirement 32kb or more) 424 kbps acceptable
Malaysia	Chip Memory Capacity: 72kb
Singapore	72kb, Type A
Thailand	72kb, Type A

Readers

The key systems involved with readers are the reader, its software development kit (tools that govern the interface between the host system and the reader hardware), the host system, and the host application (for example, Issuance Quality Analysis application or Border Control application).[3]

The design of the reader and its software tools are very important elements. A reader unit can be designed to offer the greatest degree of interoperability, reliability, performance, and ease of use, and may be tailored to suit the particular working environment of its users.

A number of software tools may be offered with the reader. If they are well designed and optimised, overall performance will be improved. For the host system, it is essential to comply with (and better still to exceed) the reader's minimum required criteria for memory (RAM), hard disk space, and the operating system. The type of physical interface between the reader and the host system is important. An optimal design, based on a high speed USB 2.0 interface, will enjoy good performance levels and not be affected by data transfer bottlenecks.

The application—for example, an Issuance Quality Analysis application or a Border Control application—has a visible effect on performance. Real-time referencing of external databases for authentication purposes, or the execution of complex cryptography functions, for example, will degrade application response time, which users may misinterpret as chip-to-reader communication delays. A modular application design that manages interactions with the ePassport independently of other functions will offer greater performance and reliable core functionality when it is disconnected from a backbone Local Area Network (LAN).

In some economies, the choices determining ePassport and reader performance are not made by the same authorities. Whereas document issuers control the ePassport components, readers are primarily selected by border management authorities, usually in a different country. The only solution to questions of performance and interoperability is on-going dialogue, and repeated interoperability tests involving sample ePassports and readers.

Security of Information

Currently ICAO provides basic recommendations for security and provides an optional regime for higher security as part of ePassport implementation. These security options (Passive Authentication, Active Authentication, Basic Access Control and Extended Access Control) are discussed in Chapter 9.

Other changes in IT security, which may need to be considered or upgraded with the introduction of ePassports, include:

- Security printing;
- Security techniques against reproduction, particularly optically variable security features;
- Issuing techniques for data integration into the document material.

[3] Todd Kealy, "Developing ePassport solutions that work", p. 8.

Public Key Infrastructure (PKI)
ICAO standards provide for a PKI for ePassports. Such a scheme generates PKI certificates, which are used to digitally sign the data on the chip, and which validate this data, thereby assuring the border inspector that the data in the chip has not been altered since being put there, and that it has been placed there by an entity with authority to do so.

In ICAO's simplified PKI system, a hierarchy of certificates is used for security purposes, along with a proposed methodology for certificate circulation to all States.

The PKI scheme consists of two parts:

- **Secure In-Country Key Generation**. Each participating State will install its own secure facility designed to generate PKI keys (private and public). This facility will be well protected from any unauthorised access, and include hardware and software security features. Although these in-country systems are independent and autonomous, the PKI certificates generated for use in ICAO compliant ePassports must comply with ICAO's Document 9303 standards to ensure global interoperability;

- **ICAO Directory Services**. In order to efficiently share the corresponding public keys of all countries, ICAO provides a Public Key Directory (PKD) Service to all participating States. This is a simple service, which accepts information on public keys from all countries, stores them in a PKI directory, and makes this information accessible to all other States. Access for updating the PKD is restricted to member States".[4]

ICAO's role is to validate the source and data integrity of the public document signing certificates (DSC) received from participating States, by using that State's Country Signing CA Certificate, and once validated, to upload them to the PKD. (See next section on the PKD for further explanation.)

The responsibilities of each economy are to:

- Submit new certificates (including certificate revocation lists) to ICAO;
- Ensure that the data in each certificate is correct;
- Ensure that the designated keys will decrypt authentic ePassports.[5]

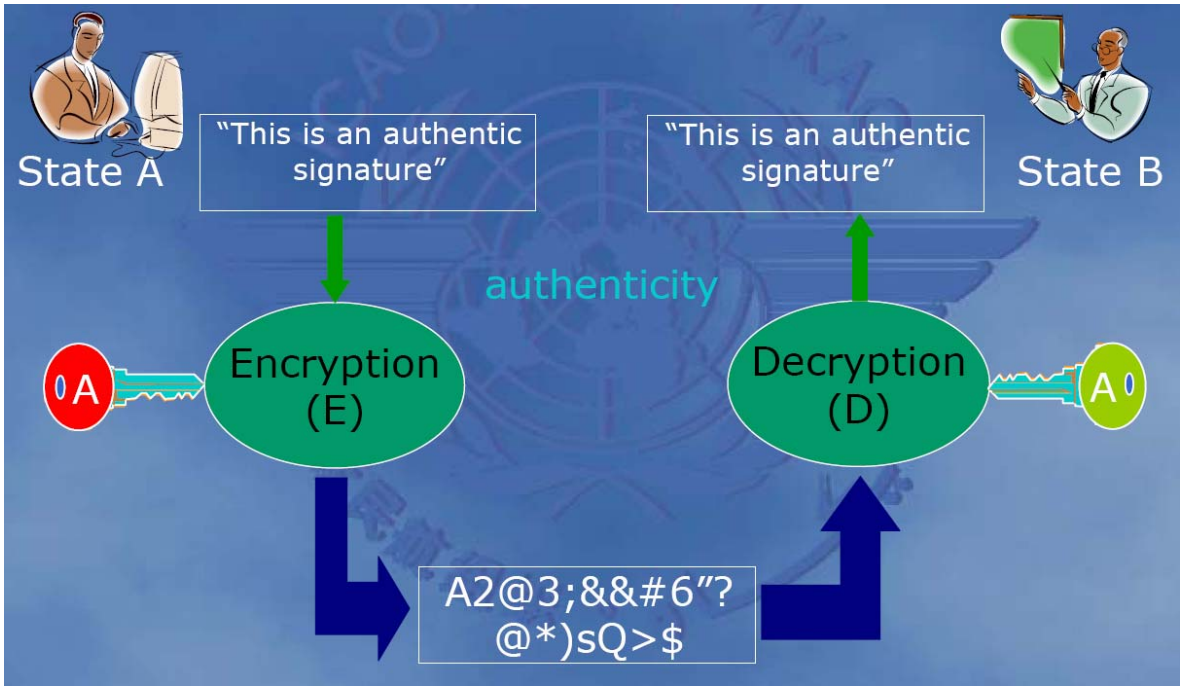
The need to adhere to ICAO requirements in regard to the PKI system gives rise to some issues that economies will have to consider. New components will be required, including the equipment to read the contactless chips and the PKI. Although ICAO has specified some aspects of the implementation of a PKI to support the production of standard, interoperable ePassports, some features are optional, and many processes and procedures are not detailed but left for subsequent determinations by implementing States.

Case study: New Zealand
- New Zealand contracted expertise in PKI
- Established own in-house certification authority/PKI infrastructure, requiring:
  – Highly secure environments
  – A number of staff with high level security clearance
  – Multiple storage locations
  – Disaster recovery considerations

[4] ICAO, *Document 9303, Part 1: Machine Readable Travel Documents, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability*, Section IV, Paragraphs 5.5.1 and 5.5.2.

[5] Paul Hooper, "ICAO Public Key Directory", Presentation given at APEC Business Mobility Group Capacity Building Workshop, Hong Kong, China, 18-20 July, 2006.

Simplified schematic of how PKI works



Paul Hooper, "ICAO Public Key Directory", Presentation given at APEC Business Mobility Group Capacity Building Workshop, Hong Kong, China, 18-20 July, 2006.

Public Key Directory (PKD)

As indicated in the section on PKI above, the ICAO PKD is an integral part of the international system for validating ePassports. As required by ICAO Document 9303, it is the primary global distribution point for public document signing certificates from all issuers of ePassports who have formally joined the ICAO PKD.

The ICAO PKD provides much greater levels of assurance for border authorities than are currently possible with traditional MRTDs. PKD Participants can access and download ICAO validated certificates, and actively use them in their border inspection systems to validate the data on the chip of ePassports presented for inspection.

Furthermore, outside the arena of international travel, ICAO validated certificates may be used to validate travel documents that are presented to financial institutions as proof of identity. Combating identity fraud in the financial services sector as well as managing illegal access to a State's services are both areas of focus for many States.

The ICAO PKD was officially opened, and commenced operations, on 20 March 2007. The ICAO PKD board was constituted, and the initial meeting held, on 19 March 2007. As at 1 May 2007, six States are participating in the ICAO PKD; with a seventh State afforded observer status. The first 15 States that join the ICAO PKD will be invited to join the PKD board.

The PKD currently holds Document Signer Certificates and Certificate Revocation Lists that have been validated against the respective Country Signing CA Certificates, and these are now available for secure download by the other participating States.

An ICAO document "ICAO PKD", gives the latest details about the PKD, and is attached at Appendix 2. Further information on how to become a Participant in the ICAO PKD can also found on the ICAO MRTD website.[6]

[6] See "ICAO PKD", http://mrtd.icao.int/content/view/47/251/

Interoperability Between Existing Systems and New Systems

Because a passport is primarily a document used for identifying travellers who are travelling from one economy to another, it is essential that the information it contains can be read easily and quickly by border control authorities of all economies. This is why ICAO has put such emphasis on standards and why it requires that all ePassports meet certain criteria. The new technologies used in ePassports enhance the security of the passport document, as well as giving border control authorities greater assurance about the identity of the ePassport holder, but it will be necessary for each economy's passport-issuing authority to ensure that the technical features chosen for its ePassport are indeed interoperable with passport reading equipment used worldwide.

In addition, economies will wish to ensure that their ePassport's features are interoperable with certain databases and systems within their own economy, depending on what is planned in terms of using the information on the ePassport.

The requirement for ePassports to meet certain standards has been emphasised in earlier chapters of this reference document, but it is worth noting again that in order to facilitate biometric data interoperability and data interchange, biometric standard profiles should be utilised.

Base standards to be considered in these biometric profiles include for example:

- Biometric Data Interchange Formats;
- Common Biometric Exchange File Format (CBEFF), NISTIR 6529-2001. (An augmented version of CBEFF is under development by the NIST/BC Biometric Working Group);
- ANSI/INCITS—Information Technology—BioAPI Specification;
- ANSI/NIST-ITL—Standard Data Format for the interchange of Fingerprint, Facial and Scar, Mark and Tattoo (SMT) Information;
- ANSI/X9 X9.84-2001—Biometric information management and security (presently under revision by ISO);
- Federal Information Processing Standard (FIPS)—FIPS 197 Advanced Encryption Standard (AES)—Nov 2001;
- ISO/IEC JTC 1/SC37 standards.

Testing of ePassports and passport readers is an important part of ensuring interoperability. Since 2004 a series of passport interoperability test events has taken place: in Canberra, then later in Morgantown, Sydney, Baltimore, Tsukuba and Singapore, with a large-scale test in Berlin in June 2006. The results of these tests have brought some changes in various features of the software and hardware used in ePassports. Each economy that introduces an ePassport should include provision for testing in its project plans.

Information about the various tests is available from the authorities that sponsored the tests as well as from the vendors whose equipment was tested.[7]

Staff

In manufacturing an ePassport it may be possible to use existing procedures and production lines with some modification, but it is likely that additional staff resources will be required. The project manager will need to consider what resources are available and whether it will be possible to recruit staff with necessary skills. Training of staff for the new tasks will be important, as will communicating to them a clear idea of what the goals of the ePassport project are.

[7] Berlin Interoperability Tests, June 2006
http://www.interoptest-berlin.de/reading_material.htm
http://www.essen-group.org/berlin/download.html

ICAO: Issues to consider when deciding to make improvements to passport systems

- How will your new system impact on your workforce?
- Involve the users early in the design and testing of the hardware and software.
- Have staff participate in the design of a training program for users, and make certain that there is adequate contractor support for the training process.

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

If the project involves outsource vendors wholly or in part, it may be necessary to ensure that knowledge of different aspects is transferred appropriately so that all areas have adequate knowledge to do their job. This transfer of knowledge may be from the passport issuing authority to the service provider (for example, knowledge of security requirements, bureaucratic procedures and reporting obligations), or in the reverse direction (for example, technical knowledge).

Management of Change

Since there will inevitably be considerable change involved in moving to production of ePassports, the project manager will need to consider how best to introduce changes and how to enlist the active cooperation of staff. A communications strategy may be helpful, aimed at informing all relevant stakeholders, parties and groups, including staff, that need to receive information throughout the project.

ICAO: Issues to consider when deciding to make improvements to passport systems

- Identify and correct problems in the new system before leaving the old system. Don't rely on temporary "work-arounds"; fix the underlying problems.
- Build in redundancy wherever in the system a breakdown of delicate or difficult to replace equipment can bring your production process to a halt.

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Preparing full documentation of all processes and procedures that are established will help with training and communications with staff and other stakeholders. Such documentation could include:

- Policy manuals;
- Procedure Manuals;
- Training material;
- Vendor contracts;
- Supporting agreements—internal and external (such as MOUs with law enforcement and other agencies);
- Passport application forms, public relations, media and guidance material, new photo guidelines;
- Open and closed source publications and marketing material.

ICAO: Issues to consider when deciding to make improvements to passport systems

- Be certain that you have well documented standard operating policies, processes and procedures at all issuing points so that there is consistency in your issued documents.
- Make sure that the contractor documents the system so that the government has a complete record of the software.

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Physical Process Security

One of the key drivers pushing economies to introduce ePassports is the promise that, by giving greater assurance about the identity of the holder, the ePassport enhances security for all of us. If border authorities are to be able to trust an economy's ePassport, they must be sure that the ePassport has been produced under totally secure conditions, so that there is minimal chance of fraud having been perpetrated during the manufacturing and issuance process.

This means that adequate security measures to protect the production process must be established and maintained. The top levels of the passport authority must be serious about preventing fraud, and must make this clear to all staff. They can demonstrate this commitment by emphasising passport integrity as much as the need to assure production, by providing adequate resources (in terms of staff, equipment and tools) for detecting possible fraud, and by prosecuting fraud when it is found. Fraud prevention, along with passport integrity and quality assurance, should be emphasised as being of equal importance to timeliness and customer service.

The security requirements mean that staff should be thoroughly investigated before being employed, and their trustworthiness should be regularly assessed. Ongoing training will be critical for avoiding administrative errors, such as faulty capture of data or mistakes in anchoring data to an identity. Software tools are available that automatically capture and format biometric data to ICAO standards, as are automated support tools that can help to avoid corruption of the data collection process.

Audit and Reporting

One method for achieving a secure production process is to audit the process at all stages. Proactive auditing can facilitate early detection of any subverted operators. Automated or semi-automated auditing methods can be employed, depending on the volume of data that needs to be checked. Biometric authentication software can provide the capability to maintain an audit trail of the network transactions performed by a given official.

An effective ePassport auditing system should:

- permit secure access to business resources for authorised employees;
- automate the creation, management and deletion of user access rights across systems;
- audit activities to ensure that systems are being administered and utilised as intended;
- have the capability to collect, record, analyse and respond to all reported events in every system across the enterprise network (for example, every key stroke on a computer can be recorded and analysed).

Business Mobility Group Security Standards for Travel Documents

Attached at Appendix 1

References

1. David Clark, "PKI and Public Key Directory: An ICAO programme for ePassport Security", *MRTD Report*, Vol. 1, No. 1, p. 35.
http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,select/id,2/
2. Hugh Gilenson, "E-passport security: Implications for e-ID's", *Keesing Journal of Documents & Identity*, Issue 15, 2005, pp. 31–33.
3. John Hotchner, "Guideline for Dealing With External Passport and Other Travel/Identity Document Fraud", Part One, *Keesing Journal of Documents & Identity*, Issue 16, 2006, pp. 20–22.
——, Part Two, *Keesing Journal of Documents & Identity*, Issue 17, 2006, pp. 6–10.
——, Part Three, *Keesing Journal of Documents & Identity*, Issue 18, 2006, pp. 9–11.
4. ICAO TAG NTWG, "A Proposed Methodology for an ICAO PKI Infrastructure for Implementation of Digital Signatures on MRTDs", Technical Report, 19 April 2003.

http://www.icao.int/mrtd/download/documents/PKI%20Digital%20Signatures.PDF
5. ICAO, “PKI for Machine Readable Travel Documents offering ICC Read-Only Access” http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf
6. Barry Kefauver, “The integrity of travel document systems: A gun waiting to smoke”, *Keesing Journal of Documents & Identity*, Issue 15, 2005, pp. 19–22.
7. Barry J. Kefauver, “ePassports: Are we there yet?”, *MRTD Report*, Vol. 1, No. 2 (2006), p. 10. http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,select/id,2/
8. Simon Lofthouse, “ePassports and the Implications of ICAO Standards”, *ICAO MRTD Report*, Vol. 1, No. 2, pp. 14–17.
http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,select/id,2/
9. Graham Swain, “Unlocking the ICAO PKI”, *Keesing Journal of Documents & Identity*, Issue 11, 2005, pp. 8–10.
10. UK Home Office, Office of Science and Innovation, Biometrics Assurance Group, “Annual Report 2006”, (May 2007).
http://www.identitycards.gov.uk/downloads/Biometric_Assurance_Group.pdf

Appendices

Appendix 1: APEC Business Mobility Group, “Standards for Travel Document Security”, 2004/SOMI/CTI/IEGBM/03
Appendix 2: ICAO, “ePassports and the ICAO PKD”.

Appendix 1

APEC Informal Experts Group on Business Mobility: Standards For Travel Document Security

http://www.apec.org/apec/documents_reports/informal_experts_group_business_mobility/2004.html

2004/SOMI/IEGBM/003rev1
Informal Experts Group on Business Mobility
Santiago, Chile, 27 February 2004

STANDARDS FOR TRAVEL DOCUMENT SECURITY

I. Introduction

1. The APEC Business Mobility Group has a goal of increased capacity to facilitate the movement of business people while at the same time ensuring border integrity. To achieve this goal, expert working groups within APEC have already prepared papers covering issues including:

- Common immigration standards in the areas of pre-arrival, entry, stay and departure; *APEC Business Mobility Standards: A Key to Capacity Building,* (May 2001)
- Effective examination of travel documents; *APEC Standards for the Examination of Travel Documents* (August 2001)
- The identification and articulation of fundamental core values to serve as the basis for an effective professional service; *Standards on Professional Conduct paper* (August 2002) and,
- The collection and transmission of Advanced Passenger Information (API) *Advanced Passenger Information Standards* (May 2003).

2. In each of these earlier papers, the philosophy has been to set a best practice benchmark for all of the APEC economies. To achieve this, many existing standards have been endorsed and in some instances expanded, particularly in areas where optional endorsements which provide for higher than minimum requirements. This paper continues the practice of setting best practice benchmarks by examining existing standards and endorsing those options that contribute to best practice. Each economy would seek to implement agreed standards on a 'best endeavours' basis, consistent with APEC principles.

3. In the area of Travel Document Security well-prepared standards and best practice guidelines already exist. These are either standards or blueprints that have been prepared by international bodies such as ICAO and G8 for ratification and adoption by ICAO. These are contained in:

ICAO 9303 Machine Readable Travel Documents (5th edition, 2003)

Annex A to Section III Security Standards for Machine Readable Travel Documents

Minimum Security Measures for the handling and issuance of machine readable (and other) passports (recommended standard practices for the World's Governments)
ICAO has this document under review for ratification at the next ICAO Technical Advisory Group Meeting in 2004. It outlines best practice principles and should be referred to by APEC economies as the guideline to adopt.

ICAO Biometrics Deployment blueprints consisting of:
**** *Biometrics Deployment Technical Report and its Annexes A-H*
**** *Contactless Integrated Circuit Chip Technical Report*
**** *Logical Data Structure Technical Report*
**** *PKI Encryption Technical Report*

All ICAO standards can be sourced from: http://www.icao.int/mrtd/download/technical.cfm

4. These existing standards were examined and this paper is a composite document regarding best practices in the areas of:

- Manufacture and Security of blank documents
- Verification of Identity, Breeder documents/information at application
- Issuing
- Recording of Issued Documents
- Distribution, and
- Immigration Control Aspects.

5. Most of the standards referred to in Paragraph 3 already represent best practice. Accordingly they have been referred to in this document without necessarily extracting full quotations. This paper should always be read in conjunction with those existing standards documents.

6. Throughout this paper and the source standards and guidelines there are a number of terms, which are explained as:

TRAVEL DOCUMENT	A Travel Document is an official document issued by a state or organisation, which is used by the holder for international travel (e.g. passport, document of identity) and which contains mandatory visual (eye readable) data and an image of the bearer.
ICAO	ICAO is the International Civil Aviation Organization. ICAO is a specialised agency of the United Nations, which sets international standards and regulations necessary for the safety, security, efficiency and regularity of air transport and serves as the medium for cooperation in all fields of civil aviation among its 188 Contracting States.
IATA	IATA is the International Air Transport Association
ISO	ISO is the International Standards Organization
CONTACTLESS IC	Contactless Integrated Circuit (IC) refers to an electronic chip attached to a radio frequency (RF) antenna. When inserted into a travel document this device can be read without any physical contact with the card reader.
INTEROPERABILITY	The crucial need for specifying how travel documents and the information contained therein, as deployed by one economy can be used by all other economies
BIOMETRIC	The automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits. The ICAO endorsed biometrics are face, fingerprint and iris, with the face being mandatory.

II. The Security Continuum

7. The assessment of Document Security Standards is not restricted to any one element within the production, use or examination of documents but is a much wider concept, requiring a very broad assessment principle. Throughout the paper on effective examination of travel documents; *APEC Standards for the Examination of Travel Documents* (August 2001), there were a number of references to this principle including:

- "Effective internal processes for producing, issuing and controlling travel documents.
- *Procedures for producing secure travel documents that are resistant to fraud and conform to International Civil Aviation Organization (ICAO) standards for travel documents (Document 9303);*
- *Internal controls to ensure that documents are issued only to those entitled to them and that blank stock is kept secure from theft or misuse;"*

8. Although these are comprehensively addressed in the ICAO documents, it is also important to include a number of other points for consideration such as:

- Global interoperability needs to be a guiding principle in the establishment of any protocol or application of new technology. However, Economies should be aware that some proprietary technologies may be subject to patent and intellectual property issues which could inhibit their global interoperability.
- Quality control and quality assurance protocols at all stages of the broad security continuum are essential in maintaining integrity of the entire process.
- Security recommendations may in some instances appear to contravene existing guidelines or legislation with respect to privacy issues and each economy should consider these recommendations in the context of their own legislation.
- To implement security across the broader spectrum it is essential that adequate and focused training be provided in all levels of the process.
- Lost & stolen documents are a major concern but are outside the scope of this paper. Developments by international bodies mentioned earlier have solutions to this particular problem well advanced and should be reviewed within APEC when such proposals are finalised.

III. Manufacture and Security of blank documents

9. Well defined standards on manufacture and security already exist and are comprehensively outlined in ICAO document 9303 'Machine Readable Travel Documents'. In addition points 3 to 5 and 7 of the ICAO Annex to Section III 'Security Standards for Machine Readable travel documents', and point 4 of ICAO proposed informative annex 'Minimum measures for the handling and issuance of Machine Readable travel documents' contain relevant best practice principles and should be referred to by APEC economies as the guidelines to adopt.

In particular economies should ensure that:

- There is a stock control number on every sheet within the document, which can be either perforated or printed
- To maintain database integrity and minimise problems at border control points economies should avoid recycling of travel document or stock control numbers
- Regular and comprehensive stock audits are conducted
- Where proprietary features have been used to ensure document security that such features can be maintained over the life cycle of the document. Economies should also beware of contractual limitations in respect of proprietary features

IV. Verification of Identity, Breeder documents/information at application

10. Confirmation of the identity and entitlement of applicants is the key to travel document integrity.

11. The prime principle in the verification of breeder documents/information e.g. ID cards/birth certificates is that they should not be taken on face value but should, where possible, be verified electronically with issuing authorities. To ensure the effectiveness of this approach issuing authorities should strive to coordinate cooperation with other entities issuing breeder documents.

12. Once again, point 5 of ICAO proposed informative annex 'Minimum measures for the handling and issuance of Machine Readable travel documents' outlines best practice principles and should be referred to by APEC economies as the guideline to adopt.

V. Issuing

13. At border control points, corrections after issue can cause undue delay in processing, and if those corrections are not in the correct format, there could be an incorrect decision on the admissibility of the bearer. The recommended best practice is that where an error is detected after issue, the document is cancelled and a new document is issued with correct details.

14. Specifications for which biometrics to use, and biometrics deployment, have been prepared after extensive research by ICAO and other international bodies. Enrolment and deployment guidelines are clearly stated in the ICAO-endorsed document (Biometrics Deployment Technical Report) and although not yet formally published as standards, these and other ICAO biometric blueprints are endorsed by APEC as the guidelines to follow.

15. ICAO document 9303 'Machine Readable Travel Documents' contains many standards together with some options for document issuance. To follow best practice, economies should ensure that:

- Machine Readable Zone (MRZ) and data page layout is in accordance with ICAO standards
- It is strongly recommended that photographs be digitised (i.e. There should be no stick-in photographs)
- Up to a maximum of 5 year validity is encouraged as a way of avoiding technical obsolescence. For detailed discussion see the ICAO biometrics deployment technical report.
- A document should have one validity only (i.e. no extensions or renewal)
- The principle of one person per document (i.e. no collective or family passports) adds to the integrity of the identity process
- Where there is an expressed need for deliberate secondary or additional passports, the documents should only be issued with specific temporal or geographical limitations
- Biometric stored image should be derived from the same image as that on the document and the application

VI. Recording of Issued Documents

16. Recording and being able to retrieve information about the documents that have been issued by any economy is critical in maintaining faith in the integrity of the entire issuance process. Border control points need to be confident that they can rely not only on the integrity of the document but on the ability of the issuing economy to rapidly provide accurate information where an apparent anomaly exists. In addition to the standards within document 9303 and the proposed informative annex, economies are encouraged to consider the establishment of 24/7 contact centres to assist in the verification of details.

VII. Distribution

17. There are two elements to the topic of distribution.

1. Economies should ensure that their documents are distributed in a secure and accountable manner in accordance with the standards addressed in the ICAO documentation. If documents are not picked up by the applicant or an authorised third person, use of a registered delivery service is recommended

2. Economies should ensure that they have distributed adequate information or samples to other APEC economies. This point was addressed in an earlier APEC paper with

the following: “Samples of valid travel documents from all countries provide a means of comparing travellers’ documents to known legitimate ones. Since it is expensive and very time consuming to collect these documents in a book form for all points of entry. Economies may wish to consider an automated system that would house samples electronically. As the EDISON travel document system (which has samples of travel documents of almost all countries) is already used by HKSAR, China and some other economies, the automated system may be developed on the base of EDISON (preferably used in the computer network). (PRC)” *APEC Standards for the Examination of Travel Documents (August 2001)*. As at July 2003, other APEC economies using the EDISON system included Australia, Canada, Indonesia, Malaysia, New Zealand, Thailand, Singapore, the USA and Vietnam. Economies are encouraged to consider joining the EDISON program.

VIII. Immigration Control Aspects

18. Economies must use automated capture systems at the border to minimise errors in data collection and enable accurate data matching.

19. It is acknowledged that there may occasionally be quality control errors and other inconsistencies present in a document presented at a border. In such instances a full examination, which must be non-destructive, should be undertaken to determine whether the anomaly in the document could be a quality control or fraud issue.

20. As with any part of the security continuum, proper training is essential. Border inspection procedures should take into account the document, computer records and personal interview to determine whether eligibility requirements have been met.

21. There are already many protocols in existence, regarding the exchange of information on fraudulent travel documents. Whenever questionable or fraudulent travel documents have been detected, timely contact with the issuing authority should be considered. Where possible the document should be returned to the issuing authority.

IX. Conclusion

22. Based on the benchmark standards outlined in this document, each economy can now identify its needs through self-assessment and then develop an individual capacity building strategy tailored to meet those specific, individual needs. As more innovations are made in technology and methodology, each economy should also ensure that they have established a review process so that they may always maintain best practice.

Appendix 2

ICAO: Public Key Directory

Apart from preserving a high level of data security, the ICAO PKD provides validation that the travel document being examined was issued by the competent authority and that the details of the document have not subsequently been altered.

ePassports and the ICAO PKD
http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,select/id,3/
http://mrtd.icao.int/content/view/47/251/

The inclusion of a computer chip in ePassports is a major enhancement in ensuring the integrity of travel documents through:

- Providing machine assisted verification (and validation) of biometric and biographical information that allows objective confirmation of the identity of travelers.
- Identifying attempts to fraudulently alter ePassports through the need to match the electronic data contained in the chip to the printed information in the passport to the physical characteristics of the traveller.

The introduction of ePassports is therefore a very important step in improving aviation and border security, while at the same time offering benefits in enhanced facilitation of passenger processing.

With traditional MRTDs, detection of photo substitution or other tampering has been dependent on the border inspector's training and expertise. However, the ICAO PKD provides a validation that the travel document being examined was issued by the competent authority and that the details of the document have not subsequently been altered.

The Business Case for the ICAO PKD

The business case for validating ePassports is compelling.

Where validation using the ICAO PKD occurs during travel, whether at points of embarkation, transit and entry clearance, it provides much greater levels of assurance than are currently possible with traditional MRTDs. This provides the following benefits:

- control authorities will be better able to identify inadequately documented travelers;
- control authorities in all States can in effect assist the issuing authority in managing the integrity of all ePassports.

The ICAO PKD can also be used to improve the efficiency of airline operations through providing airlines with a higher level of assurance that travellers are properly documented - a commercial benefit where it means that fines currently levied for carriage of undocumented travellers can in future be avoided.

Outside the travel context the ICAO PKD can also be used to validate travel documents presented as proof of identity to financial institutions and to police and immigration control authorities. Combating identity fraud in financial services and managing illegal work and access to services are areas of focus for many States.

From the foregoing it is apparent that the benefits of the ICAO PKD increase exponentially as the number of States participating, and the number of ePassports in circulation, increase. It is also the case that participating States stand to benefit most, because their participation in the ICAO PKD maximises global coverage of validation of their own documents.

Operational Status

The ICAO PKD was officially opened, and commenced operations, on 20 March 2007. The PKD board was constituted, and the initial meeting held, on 19 March 2007.

As at 30 March 2007, six States are participating in the PKD (Australia, Canada, Japan, New Zealand, Singapore and the United Kingdom). The United States is in the process of completing the formalities to join the PKD.

The first 15 States that join the ICAO PKD will be invited to join the PKD Board.

The PKD currently holds Document Signer Certificates and Certificate Revocation Lists that have been validated against the respective Country Signing CA Certificates, and these are now available for secure download by the other participating States.

The security surrounding the PKD operation is significant. The Montreal infrastructure of the PKD is located in a purpose built vault within the ICAO offices. Access to the vault is limited to a small number of suitably cleared staff of ICAO and of the service provider who constructed the system, Netrust Pte Ltd.

The vault features layers of physical controls and monitoring. Once access is gained to the vault, system controls ensure that only authorised operators can access the system and that their work in the system is comprehensively logged both on the system and through CCTV.

Governance and Costs of Participating in the ICAO PKD

The ICAO PKD has been established on a cost recovery basis.

The current fee structure was put in place to recover the costs of establishing the ICAO PKD, the major component of which was the US$692,000 payable to Netrust Pte Ltd under the contract to develop and implement the system.

Details of the current fee structure are attached.

The PKD Board is responsible for consulting with the operator and ICAO to approve the operational budget and review the financial activities of the ICAO PKD. This includes a provision requiring the PKD Board to review audited financial statements of the ICAO PKD on an annual basis. The PKD Board can, in consultation with ICAO and the operator, vary the annual fees and recommend changes to the one-off initial registration fee.

ICAO will commence negotiations on an operational contract with Netrust Pte Ltd shortly. The PKD Board has requested that ICAO consult the Board on the terms of the contract prior to it being finalised - consistent with the Board's responsibilities for operational and financial oversight of the ICAO PKD. It will be the operational contract, and ICAO's operational costs, which are also subject to oversight by the PKD Board, that will determine the ongoing cost of operating the PKD.

Once the costs of developing the ICAO PKD are met, the marginal cost of providing services, and scaling the infrastructure as the number of participating States grow is expected to be relatively low.

As a result, variations to fees are already being considered:

- The PKD Board has asked ICAO to develop options for substituting affordability as the primary criteria for setting annual fees.
- The PKD Board intends to reduce annual fees for all participating States, matching income to costs, as the number of participating States grows.
- Once the costs of the development phase are fully recovered, subject to prudent management of the ongoing capital budget and other liabilities of the ICAO PKD, and as the number of contracting States increases, the PKD Board expects in future to

recommend changes to ICAO to reduce the registration fee for new Sates joining the ICAO PKD.

As additional States join the ICAO PKD they will be invited to join the PKD Board and thus participate in the financial and operational oversight of the ICAO PKD, including changes to those frameworks. Therefore, while the initial States joining the ICAO PKD are effectively paying a premium to establish a viable validation system, they receive in return a seat at the table responsible for determining the future of that system.

Technical Architecture

The ICAO PKD has been designed to preserve a high level of data security but also, importantly, to support validation within a flexible, open architecture.

A key feature is that the certificates loaded to the ICAO PKD are validated for adherence to standards. This ensures interoperability for all States when the certificates are downloaded, work that would otherwise be necessary to be undertaken by States whenever certificates are exchanged.

The ICAO PKD also maintains a register of country contact information to support the secure exchange and delivery of country signing certificates, as and if required, between participating States. However, Netrust Pte Ltd does not, at any stage, have access to Country Signing CA Certificates submitted by participating States.

This systems architecture means that participating States can determine how the validation service offered by the PKD can best be applied, and through their participation in the PKD Board, how in future the architecture itself might need to be adapted and enhanced.

Documentation

The current technical and business architecture of the ICAO PKD is outlined in the following documents:

- ICAO PKD Memorandum of Understanding
- ICAO PKD Regulations
- ICAO PKD Procedures
- ICAO PKD Interface Specifications

Rules of procedure for the operation of the PKD Board, the terms and conditions for the use of the PKD Read Directory, and arrangements for the handling of operational and other complaints and amending the Memorandum of Understanding are to be developed, agreed and documented by the PKD Board in due course.

Further Information

Representatives of States interested in joining the ICAO PKD or obtaining further information or copies of the documentation referred to above can contact:

Mauricio Siciliano
ICAO Secretariat
MSiciliano@icao.int

or

Ross Greenwood
Chairman
PKD Board
ross.greenwood@dfat.gov.au

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 7 Data Management

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

7. Data Management

Data Resource Management has been defined as "the development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of an enterprise".[1] **Data security** is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Data security helps to protect personal data and to ensure privacy.

Biometric data management involves the proper management of biometric identifiers for an enrolled population. In considering biometric data management projects, where the potential for function creep and unplanned data linkage is ever-present, it is critical that the scope of the identity management system is carefully designed and constrained. The system should be fit for purpose, and there should be structures in place to ensure that the scope of the system is retained into the future. Establishing these structures will require combined action in three areas—law, technology, and organisational accountability:

- Legislation and administrative regulations define the "rules of the game", determining who has access to the data and under which conditions;
- At the level of technology, the focus is on operational access control and user management;
- Organisational accountability centres on data management processes within public authorities, including those relevant committees who overview these processes.

The challenge of implementing and managing such a system is to ensure that it provides functionality to the enterprise across all stages including registration, storage, identity assurance, identity protection, identity issuance, identity life cycle management, and system management.

TIPS

- Compile a set of comprehensive standards, policy and rules to ensure integrity of the system
- Vendors and suppliers should be bound by a set of rules which allow for independent auditing of outsourced functions
- Intellectual property rights should be included in contractual agreements

Suzanne Lockhart, "Biometric Data Management Issues in Large Scale Organisations", Presentation to Biometrics Institute (Australia), Canberra, 20 July 2007. For information, contact: biometricconsulting.com.au

International standard **ISO/IEC 27001** and its related code of practice **ISO/IEC 27002** (formerly ISO/IEC 17799:2005) provide internationally-accepted, standardised criteria to implement an effective information security management system. Information security is defined within the standard in the context of the C-I-A triad:

- the preservation of **confidentiality** (ensuring that information is accessible only to those authorised to have access);
- **integrity** (safeguarding the accuracy and completeness of information and processing methods);
- **availability** (ensuring that authorised users have access to information and associated assets when required).

[1] Data Management Association, quoted in Wikipedia, at: http://en.wikipedia.org/wiki/Data_management

International standards for information security
ISO/IEC 27001:2005 (Information security management systems—requirements).
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&scopelist=ALL

ISO/IEC 27002 (Code of practice for information security management)
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&scopelist=ALL

A basic principle is that if the system faces higher security risks, it will need to have higher security quality in order to counter them. This is generally termed "security assurance".

Typical factors that increase risks associated with a biometric database include:

- the scale and complexity of the system;
- the number of users;
- the number of likely enrolments;
- the security sensitivity of the data;
- whether the system is connected to other databases;
- whether it is connected to the Internet;
- whether it will store information which might make it an attractive target.

Protecting Privacy

In many economies, the use of biometrics raises important issues in terms of data management, since biometric information is regarded as personal data and needs to be addressed with particular care. Questions about human rights and human dignity may be raised among the general public.

In the past, issues relating to privacy concerns about biometrics have been paramount primarily because of the technical limitations of the technology. However, biometric systems infrastructure is being improved at a rapid rate and large-scale applications are now more accurate than they were. Nevertheless, economies or passport authorities may wish to put in place appropriate measures (at a wider level and/or more specific level, respectively) for protecting the privacy of the data, both biographical and biometric, that is collected and stored.

For further discussion of privacy, see Chapter 10.

Privacy guidelines
- Use as little personal data as is necessary for the aim of authentication
- If using personal data, protect the data from disclosure (eg, use encryption)
- Delete personal data as soon as possible
- Anonymise personal data whenever possible
- Do not use central databases where not required
- Give users control over their personal data ("identity protector")
- Make use of evaluation and certification to create a guaranteed level of trust

UK Biometric Working Group, "Privacy Issues and Biometrics - MS06"
http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&subMenu=4&displayPage=406

Database Security

With any large-scale database, progressive and slow degradation of data is a common problem, and can be difficult to control. It can affect confidence in the accuracy of the data or the database in general. It is also almost inevitable that bilateral or multilateral data-sharing will occur. If it is intended that data will be shared with agencies other than the passport-issuing authority (eg, for law enforcement purposes), a written agreement or a Memorandum of Understanding (MOU) that clearly states the rules about what can be done with the data should be established between the organisations. This should take into account any future

exchange of biometric information and identity data, in order to formulate lawful procedures for ensuring that data is shared only when necessary and that information held by various agencies does not end up being pooled. A lack of constraints and sanctions relating to the use of derived data released to another organisation may have serious implications.

The passport-issuing authority should be aware that, far from inhibiting identity-based crime, the existence of passport databases could actually facilitate it. Any database is at risk of being hacked or the data being compromised, whatever technical, organisational or regulatory measures have been taken. In recent years, there have been numerous examples of security measures that were deemed to be adequate having been bypassed. Personnel allowed access to the database can abuse their position and compromise data in spite of any regulation or supervision.

Case study: Australia
All actions undertaken in the mainframe Passport Information and Control System (PICS) and the Delta workflow system, can be tracked and periodic random audits are undertaken. Access to PICS is strictly controlled with only the functions necessary to perform a particular job available to individual operators. Officers must complete an online training program before more complex passport functions can be undertaken.

Economies will also wish to ensure that any contribution to initiatives external to the economy comply with internal departmental privacy statements and relevant legislative requirements.

Liability issues
Biometric systems are not yet mature, so there may be liability issues relating to:
- Performance
- Reliability
- Accuracy
- Independent evaluations
- Lack of standards
- User acceptance and human factor issues

These issues may result in:
- Failure to enrol
- False non-match
- False acceptance
- Denial of service

Recommendations
- Provide adequate fall-back mechanisms without causing undue disadvantage, discrimination or humiliation
- Redirect issues or uncertainty to qualified staff
- Formulate policy, procedure and training that covers these issues

Suzanne Lockhart, “Biometric Data Management Issues in Large Scale Organisations”, Presentation to Biometrics Institute (Australia), Canberra, 20 July 2007. For information, contact: biometricconsulting.com.au

What if a Biometric Identifier is Compromised?

Biometric identification relies on the individual uniqueness of the identifier for confirmation of a person’s identity. For this reason, it is imperative that the security of the biometric data is maintained, otherwise there is potential for impersonation to occur. If an enrolled biometric template is compromised it cannot be reissued like a like a password—it is gone forever.

In such a situation, revocation of the biometric template may become necessary.

Revoking the biometric template
"Revocation in a biometric system could refer to invalidating the binding of a biometric with a specific user ID, key or other value (identifier). A stored biometric could be associated (bound) with that identifier. Once a live biometric is compared to a stored biometric and a match is determined, the identifier can be declared valid. If this binding is removed (revoked), then the identifier will not validate."

M1/06-0087: Contribution to AHGBEA on Revocation by Dale Hapeman, BFC and Walter Hamilton, IBIA
http://www.incits.org/tc_home/m1htm/2006docs/m1060087.pdf

In relation to revocation of a biometric template, economies may wish to consider the following:

- Formulation of relevant policy relating to destruction of redundant data;
- Revocation should be conducted only by the system administrator;
- A biometric revocation list should be maintained;
- Whenever a user tries to identify or verify, after a match is found, the identity of the individual should be checked against the biometric identifier revocation list. If the particular subject is on the revocation list, that individual would not be authorised by the system. The benefit of this is that an audit can be constructed against identification and verification attempts made using the biometric which has been revoked;
- The database record which corresponds to the revoked biometric should be flagged, which also provides advantages similar to those of a revocation list.

References

1. Biometrics Institute (Australia) Privacy Code, 19 July 2006
http://www.privacy.gov.au/business/codes/biometricscode.doc
2. Council of Europe, "Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data" (2005).
http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/O-Biometrics(2005)_en.asp
3. EastWest Institute, Global Security Program, Consortium on Security and Technology, "Information Security and Identity Management", Report of meeting held 1 December 2005.
http://eubiometricsforum.com/dmdocuments/ReportInformationSecurityandIdentityManagement.pdf
4. Insight Security, "Protecting Your Data".
http://www.insight-security.com/solfind-016.htm
5. Ari Juels, David Molnar, David Wagner, "Security and Privacy Issues in E-passports".
http://www.cs.berkeley.edu/~daw/papers/epassports-sc05.pdf
6. Suzanne Lockhart, "Biometric Data Management Issues in Large Scale Organisations", Presentation to Biometrics Institute (Australia), Canberra, 20 July 2007. For information, contact: biometricconsulting.com.au.
7. UK Biometric Working Group, "Privacy Issues and Biometrics - MS06"
http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&subMenu=4&displayPage=406

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 8 Booklet Manufacture

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

8. Booklet Manufacture

As discussed in Chapter 2, the primary difference between an ePassport and other passport booklets is that an ePassport contains an embedded integrated circuit (IC) chip that contains both biographical and biometric data about its holder. In other respects the ePassport does not visibly differ markedly from its predecessors. However, the presence of that chip may make a great difference for economies wanting to introduce ePassports when they look at designing a new ePassport booklet or modifying an existing booklet.

Some economies will wish to integrate contactless IC chip technology into current passport manufacturing processes with as little change as possible occurring in terms of book design and printing processes. Other economies will be ready to make substantial changes to existing passports as part of a large-scale upgrade.

International Civil Aviation Organization (ICAO) specifications for ePassport booklets have been published in ICAO Doc 9303 and endorsed by the International Organization for Standardization (ISO) as ISO/IEC 7501 (see Chapter 1).

Further information is provided in the ICAO working paper, "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation", which was prepared for the TAG/MRTD 17 meeting held in March 2007. The working paper provides an overview of the development of MRTDs and includes a discussion of operational considerations and implementation strategies to assist in clarifying some of the approaches in deploying travel document programs. Section 7 of the working paper covers the characteristics of the documents themselves.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf

ICAO: Issues to consider when deciding to make improvements to passport systems

- How many types of passports (Regular, Official, Diplomatic, Overseas-issued) are there? How many do you produce of each?
- Do you intend to replace your previously-issued passports before they are due to expire? This may be beneficial if your previously-issued passports can be easily altered or counterfeited, for example.
- What is your passport's validity period? Do you want to change it?
- How many pages are in the present passport? Do you want a change?
- How do you want to reproduce the passport bearer's image in the passport?
- Have you resolved transliteration issues so that entries in your passport's machine readable zone (MRZ) will be in compliance with the transliteration standards of Document 9303?
- Do you want to change personalisation from the end leaf page to the interior of the passport, or vice versa?

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Chip Location

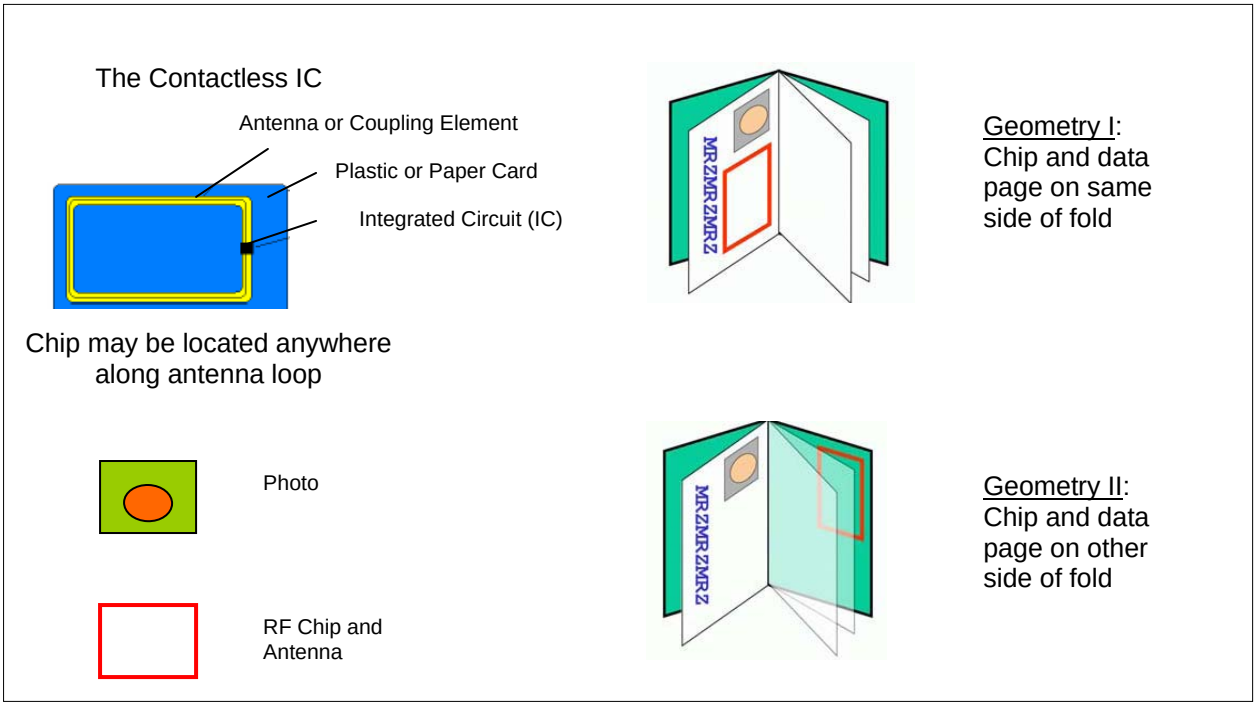
One main issue for economies to decide is where the chip and antenna assembly will be embedded within the ePassport. Allowing Issuing States some discretion over placement of the chip was a key factor in ICAO's decision to make the contactless form of chip the standard for ePassports.

Placement of the chip has proved to be less straightforward in practice than was expected. Available alternatives include:

- The biographical data page;
- Between the end paper and the cover (either at front or back);

- Between the centre pages of the document (where the binding is visible);
- Within a separate sewn-in page (in which case the page is not to be used as a visa page or travel stamp page).

Two basic configurations for chip placement



(From ICAO, New Technologies Working Group, "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation", p. 23.)

One factor that will influence location of the chip is how the ePassport will be used. Some ePassports are designed to be used closed, that is, the passport covers will be closed when it is inserted into a passport reader. This may dictate that the chip be embedded in either back or front cover. This is the case with Malaysian passports, where the chip is inserted in the back cover.

The chip can be encased in a flexible plastic sheet format, allowing it to be sandwiched between, or laminated into, the passport pages or cover. If this solution is chosen, it is essential to ensure that the chip and/or chip page cannot be easily removed and replaced.

Some economies have chosen to shield or encase the contactless chip in a metal jacket (such as aluminium foil) to prevent the chip from being read when the passport is closed. Care must be taken in reading documents that use such shielding.

Durability of the Chip

Durability of the chip is also a factor to consider, as chips and booklets may be required to last up to ten years. IC chips are in use across hundreds of applications round the world, and substantial testing of passport chips has been carried out by a number of countries. Economies should ensure that the selected chip unit will withstand up to ten years of normal passport use.

Economies will also need to ensure that the booklet manufacture process and the personalisation process do not introduce unexpected damage to the chip or to its antenna (for example, image-perforation security features puncturing the antenna, or heat lamination damaging the chip).

Other Security Features

The kinds of security features that have been used in traditional passports, such as high-quality printing with combinations of letterpress, offset and intaglio printing techniques, or UV features, or watermarks, will need to be continued, because they add another layer of measures to prevent passport forgery.

There have been reports in the media describing instances where technical experts have succeeded in reading and cloning ePassport chips. If forgers were to succeed in cloning a chip, they would also need to create a forged ePassport in which to insert that chip. The security features are intended to make the substitution of a chip into an existing ePassport virtually impossible. (If such a fake passport could be made, it could only potentially be used by someone who strongly resembles the genuine holder of the passport from which the chip data was taken. Immigration officials will still need to use existing skills to assess the bearer's claim to the identity associated with the passport.) (See also Chapter 6.)

ICAO: Issues to consider when deciding to make improvements to passport systems

- Are there additional types of security features (intaglio printing, watermark paper, paper with an embedded thread, special stitching, ultraviolet printing, other special inks) that you want in the passport? How will they be verified?
- Have you verified that the security features can coexist in the same document and that your document construction can support them?
- Who in your government makes the decisions about the standards for quality and security content of your document? Should the decision process be changed?

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Testing

The integrity of the passport is paramount, so functionality and usability testing will be required at various stages of manufacture. Allowance will need to be made for testing, and the time and resources needed must be made available.

The ICAO Test specification for Machine Readable Passports (MRPs) can be found at:
http://mrtd.icao.int/component/option,com_remository/Itemid,256/func,fileinfo/id,2/

It is essential that each economy should submit its ePassport for interoperability testing before launching into full production. As mentioned in an earlier chapter, ICAO has conducted several interoperability testing scenarios, and a number of problems were identified. These included:

- readers that did not properly receive data from passports due to the size and type of the chip, its location in the passport booklet, and the power of the reader's signal;
- problems associated with verifying digital signatures on the chip;
- problems with reading facial biometrics.

Allow Sufficient Time for Rollout

It can be a helpful strategy to have a gradual transition from issuing traditional passports to issuing ePassports through a progressive rollout, rather than switching to 100 percent ePassports on a fixed date.[1]

Passport agencies will also need to allow sufficient time to assess and choose the booklet manufacturer, and for any necessary upgrades of equipment and technology. Some economies will wish to continue to work with their existing passport manufacturer, so booklets may need modification for the chip to be included.

[1] National Audit Office (UK), *Identity and Passport Service: Introduction of ePassports*, Report by the Comptroller and Auditor General, HC 152 Session 2006-2007, 7 February 2007, p. 11.
http://www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf
http://www.nao.org.uk/pn/06-07/0607152.htm

Each passport agency should ensure that the services expected from the supplier are clearly documented, and that any contracts between supplier and purchasing agency are written in such a way as to mitigate transfer of blame from the vendor to the purchaser.

Stock Considerations

- Choose chip components and a supplier at an early stage to ensure that an adequate supply of chips is available when needed. Check that readers can handle both Type A and Type B chips.
- Some economies may need to use up their stocks of older-style booklets before new booklets are purchased.
- It may be worthwhile to take the opportunity to upgrade stock control, reconciliation, and audit systems.
- Take the opportunity to implement new stock control systems that cover the new components of the ePassport.

Case study: New Zealand—manufacture and storage of eMRTDs

Drivers

- To develop and integrate contactless IC chip technology into current passport with as little change as possible
- No major changes to book design or printing processes
- Integrity paramount

Development of ePassport

- Expectations clearly documented between supplier and New Zealand Passports
- Complex contract to maintain vendor's responsibility throughout personalisation
- Reduces potential for vendor to transfer blame

Stock control

- Stock control systems upgraded to improve blank stock management
- Reconciliation systems
- New stock control systems introduced for additional components
  - Transportation keys
  - Manifest management
  - Certificate management
- Careful separation of duties to ensure integrity

References

1. ICAO, New Technologies Working Group, "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation", Working Paper 16, prepared for Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD) 17th Meeting, held in Montreal, 20-22 March 2007
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf
2. A. J. Mansfield and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices", Version 2.01, August 2002.
http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf
3. National Audit Office (UK), "Identity and Passport Service: Introduction of ePassports", Report by the Comptroller and Auditor General, HC 152 Session 2006-2007, 7 February 2007, p. 11.
http://www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf
4. Safe ID solutions, "Think Personalization", October 2006.
http://www.safe-id.de/downloads/pdf/Think_Personalization.pdf
5. Stefan Rupp, "Facing the Challenges of Today's Passport ID Issuance", Safe ID solutions, February 2007.
http://www.safe-id.de/downloads/pdf/Facing%20ePassport%20Challenges.pdf

6. Michael Schlüter and Matthias Niesing, “E-passport interoperability: From crossover tests to standard conformity assessments”, *Keesing Journal of Documents & Identity*, Issue 23, 2007, pp. 3–5.

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 9 Quality Assurance

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

9. Quality Assurance

Every ePassport should be subject to rigorous quality assurance processes before being issued to its holder, to ensure that it is in full working order when received. If such quality assurance processes are not in place, and as a result other economies experience problems with a specific economy's ePassport, the perceived integrity and reliability of that ePassport as a travel document can become compromised. This situation would be very difficult to overcome, and could seriously jeopardise the returns from an ePassport investment.

In addition to the normal quality assurance processes that economies have in place for their regular passport production, passport issuing authorities will need to consider introducing supplementary quality assurance requirements for certain items specific to ePassports, such as:

- Data that is collected for storage on chips;
- Format for storage of data on chips;
- Relevant printed features on passport booklets;
- Insertion of fully-functioning chips into correct passport booklets.

This chapter discusses each of the items that require quality assurance and suggests how economies could carry out such quality assurance, including the application of relevant standards and specifications, as well as more general quality assurance measures.

ICAO: Issues to consider when deciding to make improvements to passport systems

- Who in your government makes the decisions about the standards for quality and security content of your document? Should the decision process be changed?

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Data Collected for Storage on Chips

An ePassport has biographical and biometric data stored on its chip. Because the inclusion of biometrics increases the connectivity between the passport and its holder, serious problems will be caused if the data stored on the chip is false or of poor quality. For example, poor quality biometric data can mean border officials are unable to verify the identity of the ePassport holder easily and quickly, which is likely to cause an additional workload for border staff and document examiners. It is, therefore, imperative that the biographic and biometric data stored on chips is accurate and of a useable quality and format.

As discussed in Chapter 5, the identity and eligibility of a passport applicant should be thoroughly established through presentation of various documents and other checks before a biometric is used to anchor that identity. The quality of the identity established can be greatly improved through, for example, verification of breeder documents, social footprint checks and face-to-face interviews.

Mechanisms for improving the quality of the biometric data collected for storage on a chip are also discussed in Chapter 5, where it is noted that if a biometric data sample is of poor quality, its utility is greatly diminished. These mechanisms include adhering to and promoting the guidelines for photographs that have been developed by the International Civil Aviation Organization (ICAO) and following other relevant international biometric standards.

The ePassport specifications in Document 9303 incorporate ISO/IEC standards for each type of eligible biometric and establish criteria and procedures for biometric capture processes, in order

to ensure that biometric samples are acquired with adequate fidelity and in an appropriate format to meet ICAO's requirements.

ISO/IEC biometric standards included in ePassport specifications

- Facial Image Format for Interoperable Data Interchange (ISO/IEC 19794-5)
- Iris Image Format for Interoperable Data Interchange (ISO/IEC 19794-6)
- Fingerprint Image Format for Interoperable Data Interchange (ISO/IEC 19794-4)
- Fingerprint Minutiae Format for Interoperable Data Interchange (ISO/IEC 19794-2)
- Fingerprint Pattern Format for Interoperable Data Interchange (ISO/IEC 19794-3)

The quality of biometric samples collected can also be improved through the design of biometric capture equipment sensors and the user interface for that equipment. Where quality-control cannot be achieved in this way, it will be necessary to have other ways for analysing the quality of a live sample (including to determine if it meets the relevant ISO/IEC standard). This may be done by visual examination, or by introducing software that can perform automated checks. Such measures can be useful for initiating a repeat acquisition of biometrics from a user when the original sample is found to be not suitable, but also for real-time selection of the best sample, and for selective use of different processing methods.

Storage of Data on Chips

For reasons of interoperability with passport inspection systems used by other economies, it is crucial that data be stored on the chip in the correct format. Not only must the biometric data be stored in the correct format, but other data stored on the chip (what it is and where it is stored) must also accord with the relevant international standards.

Biometric Data

The formats for biometrics stored on ePassport chips are prescribed in ISO/IEC standards included in the ePassport specifications (see box above). It is an important element of quality assurance that these standards are applied so that the biometric data stored on the chip can be read easily by those authorised to do so.

In order to preserve vendor neutrality and backward compatibility, ICAO has made storage of the **image** mandatory **for each biometric type stored in the MRTD**, with the additional option of storing an **associated template** at the discretion of the Issuing State. When deciding whether to include a template, economies should consider that their ePassport can be valid for up to ten years and that templates may change during that time. This has implications not only for the storage of the data on the ePassport chip and the equipment used at borders to read the biometric information, but also for the vendor(s) the economy can use.

What is an image?

An image is the digital representation of a biometric as typically captured via a camera or scanning device.

What is a template?

A template is, usually, condensed and vendor-specific data that represents the biometric measurement of an enrolee and is used by a biometric system for comparison against subsequently submitted biometric samples.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf

General Storage of Data on the Chip

To ensure global interoperability for machine reading of stored details, ICAO has also developed a standardised organisation of data for the recording of details in an ePassport chip. This is the Logical Data Structure (LDS).

What is the Logical Data Structure (LDS)?
The Logical Data Structure (LDS) is the standardised data format common to optional capacity expansion technologies of MRTDs (ie, chips) to enable global interoperability for recorded details (travel document data) used during inspection of a person and their MRTD.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf

The LDS must meet a number of mandatory requirements: namely, it must ensure efficient and optimum facilitation of the rightful holder; protect details recorded in the optional capacity expansion technology; allow global interchange of the data; address the capacity expansion needs of Issuing States and organisations; support a variety of data protection options; allow updating of details; and utilise existing International Organization for Standardization (ISO) standards to the maximum extent possible.

To meet these requirements, the LDS identifies all mandatory and optional data elements and any prescriptive ordering and/or grouping of data elements that must be followed to achieve global interoperability for reading of details (data elements) recorded in a capacity expansion technology (chip). The details of the LDS structure are incorporated in Document 9303.

The ability to confirm that the LDS was created by the relevant Issuing State (ie, authentication) is maintained using **Public Key Infrastructure (PKI)**, which is discussed in Chapter 6.

Types of authentication of the data stored on a chip
Passive Authentication is a verification mechanism that does *not* require the processing capabilities of the chip in the MRTD. Passive authentication proves that the contents of the Document Security Object (SOD) and LDS are authentic and not changed. It does not prevent exact copying of the chip content or chip substitution. This type of authentication is mandatory.

Active Authentication is the explicit authentication of the chip. Active Authentication requires the processing capabilities of the MRTD's chip. The active authentication mechanism ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system (ie, reader) and the MRTD's chip. This type of authentication is optional.

A **Document Security Object (SOD)** is stored on the chip and contains a digital signature (Document Signer Certificate) of the passport holder's Issuing State. For Passive Authentication, the SOD also contains hashed representations of the LDS contents. For Active Authentication, a unique pair of public and private keys is also stored.

A **hash** is a number generated from a string of text using a formula to ensure that a message has not been tampered with.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf
http://lasecwww.epfl.ch/courses/sp07/MRTDreport.pdf

It is important that economies adhere to the specifications relevant to the LDS and PKI to ensure that their chips' data storage is of suitable format and quality to facilitate authorised reading of the data on the chip.

Relevant Printed Features in ePassport Booklet

It is not just the quality of the data on the chip or how it is stored that are important: the printed elements contained in the passport's machine readable zone (MRZ) must also be of high quality and conform to ICAO requirements in terms of containing mandatory elements in a standard sequence. The physical characteristics of the ePassport must be of sufficient quality to ensure that the document will last throughout the period of validity defined by each Issuing State, while

the visual information on the data page and the MRZ must remain readable under all sorts of conditions.

In addition, Basic Access Control (BAC), an optional mechanism specified as an ICAO best practice for preventing unauthorised access to the data stored on the chip, requires certain text to be included in the machine readable zone of an ePassport booklet, and this particularly must remain readable.

Types of access control
Basic Access Control (BAC) is a challenge-response protocol where a machine reader must create a symmetric key in order to read the contactless chip by hashing the data scanned from the MRZ. BAC prevents skimming and eavesdropping as access to chip data is only allowed if the reader can scan the MRZ printed inside the passport booklet (ie, this requires the passport to be physically opened and scanned).

Extended Access Control (EAC) is an advanced protection mechanism for additional biometrics included in the MRTD (ie, finger and/or iris), including the State's internal access specifications or the agreed bilateral access specifications between the States sharing the information. Unlike BAC, EAC does not derive a key from the MRZ, rather it is computed from a key agreement protocol.
http://www.icao.int/icao/en/atb/sgm/mrtd/TAG_MRTD17/TagMrtd17_WP016.pdf
http://www.trusted-logic.com/Flyers/jTOP_ePassport_11_06.pdf

Insertion of Fully-functioning Chips into Correct Passport Booklets

Adequate quality control needs to be applied to ensure that the correct data has been written to the correct chip in the correct passport booklet. Significant problems would be encountered if the information printed on the data page does not match the data on the chip.

Testing and Auditing

In order to ensure that the ePassports to be issued meet quality requirements, economies should consider introducing compulsory testing as part of their ePassport issuance process. This could include tests to determine that:

- Biometric data meets relevant image quality and format standards;
- Data stored on the chip meets ICAO's Logical Data Structure specifications;
- The correct SOD has been included on the chip;
- The PKI, and the authentication it supports (passive and active), are functioning properly;
- The MRZ is correctly printed;
- Any access control mechanisms (ie, BAC or EAC) are functioning properly;
- The right chip has been inserted into the right passport booklet;
- The chip is being read properly (if this has not already been established when testing PKI and/or access control mechanisms).

Regular audits could also be considered to ensure the entire ePassport issuance process is running efficiently and effectively, and to highlight any areas where any improvements could be made.

Redress Mechanisms

It is important that mechanisms are available to provide redress to passport holders in cases where the passport does not meet required quality standards, particularly because biometric identifiers are embedded in the ePassport.

Any redress mechanisms would have to be carefully constructed to ensure that ePassports are not amended or re-issued under fraudulent circumstances. For example, one scenario might be where an imposter presents an ePassport with a damaged chip in an attempt to get a replacement ePassport with the imposter's biometric data included on a new chip. Such redress mechanisms would need to take into account the issues discussed in Chapter 8.

References

1. Gemalto, "Moving to the second generation of ePassports", July 2007.
http://www.securitydocumentworld.com/client_files/secondgenrationepassportwp12.pdf
2. UK Home Office, Office of Science and Innovation, Biometrics Assurance Group, "Annual Report 2006", (May 2007).
http://www.identitycards.gov.uk/downloads/Biometric_Assurance_Group.pdf

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 10 Privacy, Human Factors and Public Awareness

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

10. Privacy, Human Factors and Public Awareness

When ePassports are first introduced, there will be a period during which countries and individuals will need to become accustomed to the new methods for inspecting travel documents and learn to handle the related issues that will accompany the implementation of biometric technology and information technology improvements. The technologies used in ePassports embody fundamental changes that affect operations, data integrity and privacy, and will have a resultant impact in the wider socio-economic realm.

Different perceptions on the part of the general public will need to be recognised and taken into consideration. Many individuals do not understand how biometrics work, what are the costs and risks, and—most importantly—what are the benefits. They will respond more positively if they understand the cost and benefits of introducing ePassports.

Citizens of every economy are influenced by specific localised social and cultural customs that will affect how they respond to the introduction of ePassports and biometrics. If such factors are not adequately taken into consideration, there is potential for resistance to ePassports to develop, which could have negative impacts, such as:

- Rejection or slow uptake of new passports;
- Poor systems performance;
- Poor enrolment and matching;
- Loss of faith in government processes;
- Reduced credibility for the economy and its processes within the international domain.

Economies are strongly urged to develop and employ means to communicate to their citizens why biometrics are being used, and to explain the processes and associated systems that will be involved. In time, as people learn more about biometrics and about ePassports, attitudes will change, and ePassports and the associated technology will become widely accepted.

Benefits for economies of understanding these issues

- Enhanced user acceptance of systems incorporating biometric technology
- Improved public perception and understanding of well-designed systems
- Smoother introduction and operation of these systems
- Potential long-term cost reduction (whole of life costs)
- Establishment of commonly-approved good privacy practice

Factors that Need to Be Considered

Privacy

Citizens of all economies have concerns about how passport authorities will protect the privacy of the personal information, including biometric identifiers, that they provide in order to be issued with an ePassport. In general, most citizens want to be sure that the information will be used only for the purpose for which it was given, that it will not be disclosed to other persons or agencies without the consent of the individual concerned, and that it will be kept securely by the passport agency.

There are two aspects to consider in relation to protecting the privacy of the information and biometric identifiers stored on ePassports. The first concerns the security of the various processes involved in production of an ePassport, from capture of data to delivery of a personalised ePassport, and afterwards with regard to long-term storage of the information. These processes are under the control of the passport-issuing authority, and every effort should be made to ensure that they are as secure as possible. Well-implemented systems will embody numerous mechanisms for enhancing security, such as supervision of personnel who submit the biometric data to validate information on the chip; regular auditing of computer use; audit control of data, data transfer and management; adherence to performance criteria; etc. Some of these issues have been mentioned in earlier chapters (see Chapters 5, 6, 7, 9).

The second concerns the vulnerability of the information that is stored on the chip in the passport to unauthorised reading. Protecting ePassport data against unauthorised access is a crucial part of the security of the entire system. Security and privacy threats to ePassports include clandestine scanning, clandestine tracking, "skimming" and cloning, eavesdropping, biometric data leakage, and cryptographic weakness. The International Civil Aviation Organization (ICAO) recommendations regarding the use of security measures such as Basic Access Control (BAC) and Public Key Infrastructure (PKI) address some of these threats, but some privacy concerns remain (see Chapters 6 and 7).

Case study: Australia
Privacy issues were a key concern addressed by a public relations campaign. Points emphasised included:

- The chip contains no information **other than already appears** in the printed data page of the passport (ie, name, sex, date of birth, citizenship, passport number and expiry date, and image of holder). Therefore there is no additional privacy risk;
- The Public Key Infrastructure (PKI) and Basic Access Control (BAC) technology protects privacy by providing **increased security and integrity** of data in the passport.

Economies can address the concerns of their citizens in relation to privacy by ensuring that all legislation and regulations relating to ePassports comply with privacy legislation. This may require close cooperation from the outset with national data protection authorities when drafting legislation. Some economies may find it helpful to enter into dialogue with privacy advocates to ensure that these groups have accurate information about what is being proposed. Such dialogue gives officials an opportunity to listen to the concerns and suggestions of advocacy groups and take them into account. Officials will need to maintain an awareness that the agendas of advocacy groups may differ in emphasis from the ePassport implementation agenda; it may be necessary to sell ideas to them and to test their opinions, as well as to listen to their advice.

In addition, information about how biometric identifiers and biographical information will be collected and stored, how they will be used, who will have access, and under what conditions that information can be disclosed to others, can be disseminated widely to allay citizens' concerns. Economies should not forget that it is an ICAO requirement that ePassport readers must be made available for citizens to check that the data on their ePassport is correct.

Case studies
Australia
There is strict access control of the passport processing system and the facility exists to examine what an individual system user has accessed. Audits are undertaken periodically internally. The Office of the Privacy Commissioner has undertaken several audits of the ePassport process.

Canada
The collection and sharing of personal information is governed by the Privacy Act. As part of a larger initiative to modernise IT infrastructure, additional measures will be introduced.

Hong Kong, China
The purpose of collection of personal information is explicitly stated in the application form.

Korea
Since ePassports use Radio Frequency Identification (RFID), Korea is concerned over the guarantee of technical security with the issuance of ePassports. It plans to devise a personnel and security system that would prevent unauthorised access to personal information.

Malaysia
All collection, sharing and access to personal information are for the Immigration Department only, through the personnel access system.
(*cont. next page*)

The Philippines
The data gathered from passport applicants will be accessible only by specific people in our Office of Consular Affairs. Once they receive the data gathered from different sources—posts abroad and local consular offices—they will match the data with the existing database and report back to the source of the data whether there is a match or not and if the application is approved for passport issuance. No other offices within the government's bureaucracy will have access to the personal information of an applicant. Any requests for personal information will be given on a needs basis only.

Singapore
Stringent procedures for all processes including the application, processing, production, quality assurance and issuance of ePassports have been put in place to closely monitor and track every stage. This will ensure only authorised officers are given the access to perform the specific tasks assigned. There are also systems in place to track all officers handling passport functions in order to minimise internal abuse. Policies guide officers on how the information is captured and stored in the system, and ensure that the collected information can only be shared for legitimate reasons and with proper approval. This ensures the protection of data privacy.

Thailand
All databases belong to the government's agencies. The vendor checks the ID, black list and passport holding history of the applicant, through the brokers set up by the Ministry.

The United States
The US Government abides by strict privacy laws but can share data with law enforcement. Data can sometimes be shared with other government agencies but to do so usually requires a written agreement.

Accessibility and Useability
It is important that the biometric equipment should be easy for people to use. This will mean that each economy has to consider how to manage physical and psychological factors that could influence how people interact with the equipment, particularly physical disabilities of users that may impede access. In any situation that involves taking biometric identifiers from large numbers of people, some portion is likely to be physiologically unable to use one or other biometric technique, therefore systems should be flexible enough to accommodate this variability. Factors to consider include:

- Physical access: Is it easy for all clients to use? Are the signs easy to understand? Is the approach to scanners, readers and kiosks easy to find and to negotiate?;
- Access for disabled people;
- Location of the system within the airport. Consider ergonomic aspects of the position of the system from the point of view of staff as well as of clients;
- Physical environment for biometric capture systems—factors such as lighting, humidity, dust-free atmosphere, etc;
- Ability of the system to handle throughput, particularly with the advent of larger-capacity aircraft;
- Developing fallback mechanisms for cases when enrolment fails;
- Developing processes for handling re-enrolment.

Health and Safety
Some concerns about health and hygiene issues in relation to use of biometric equipment have been raised, mostly with regard to potential transmission of infectious diseases. Perceptions that diseases transmission is possible may affect the success of a biometric program. Since most biometric enrolments are mandatory, people react to them more negatively than voluntary activities where infectious disease transfer is also possible (such as elevator buttons, ATM keypads, bathrooms, doorhandles).

Issues that cause concern include:

- Direct and indirect medical implications associated with using biometric technology (for example, will an iris scan cause eye problems later on?);
- Hygiene aspects (has the equipment been cleaned after use by a previous client?);
- Cross-contamination issues (can disease be transmitted by using equipment previously used by a person with an infectious disease?);
- Psychological disorders that might affect the user's ability to interact with the system;
- Effects on the client of temporary illness, or of drugs and alcohol, in terms of both capture of biometrics and later matching;
- Effects of degenerative illness or disfigurement, in terms of both capture of biometrics and for later matching.

Social and Cultural Considerations

Social and cultural issues have the potential to influence how readily the general public will accept biometrics and the idea of ePassports, and may, therefore, determine how effective ePassport implementation will be. Some of these issues are specific to particular economies, others are universal. One example is the requirement for members of certain religions to wear headdress; another is the perception in certain countries that the taking of fingerprints is associated with criminal behaviour. Issues that may need to be considered include:

- Cultural factors (for example, how does the biometric system cope with clothing, makeup, facial adornments, etc.);
- Religious factors (such as the requirement that a female may not be unveiled in the presence of non-family males, so photographs for an ePassport must be taken by a female photographer, in a private space);
- Personality factors—the emotional and psychological status of the user may influence their interaction with a biometric system;
- Previous experience of the user;
- Previous victimisation—how does the system cope with people who do not want to use a biometric system?;
- Demographic factors (such as age, gender);
- Politics;
- National security/identity fraud;
- Multinational environment.

Case studies

Korea

Koreans are reluctant to submit their fingerprints to any organisation or system, especially to government organisations. If there is strong resistance to submitting fingerprint images for ePassports and not enough technical support for the system, Korea will not push ahead with the policy, although there will be continued efforts to inform the public about ePassports through public hearings and workshops.

Malaysia

There have been no social-based issues in implementing the ePassport program, since the usage of thumbprint is a basic requirement for the National Registration program. There has been no religious clothing issue either.

Singapore

Religious headdress is allowed for the use of passport photographs. Singapore did not encounter any social-based issues in implementing its ePassport program with regard to the collection of fingerprints, as the collection of biometric data to apply for a personal identity document is not new. Since 1948, the fingerprints of Singapore citizens have been collected for registration purposes and they fully understand the rationale and need for them to give their fingerprints when they apply for an ePassport. Citizens regard the collection of fingerprints as helpful in preventing any one from impersonating someone else when applying for an ePassport.

(*cont. next page*)

Thailand
There has not been any social problem relating to fingerprint collection. Highest security for all databases, especially the fingerprint database, is maintained.

What Governments Can Do

The most effective way for economies to address these issues and encourage positive attitudes to biometrics and ePassports among the general public is to launch a thorough education and public awareness campaign. This campaign could cover matters such as:

- Explaining what “biometrics” means and what biometric technology involves;
- Explaining how biometrics can help to establish identity, and how this can benefit both individuals and the community in general;
- Describing the benefits of ePassports for ensuring the safety of passengers and for facilitating travel;
- Explaining how the privacy of data provided by ePassport holders will be protected;
- Explaining any increase in fees;
- Giving specific information about how to apply for an ePassport, how to use the system, and how to care for an ePassport.

Economies can use a number of methods for spreading information among the general population, such as press releases, public discussions, debates in parliament, use of brochures and posters, TV or internet campaigns.

Factors that may influence acceptance by the public

- Benefits associated with using the system
- Experience of the user
- The education level of the user
- Trust in government and government systems
- Visibility and transparency of the project to the public
- Convenience and reliability of the system
- Cost—Will the cost of the new system be absorbed by the implementer or the user?
- Level of invasiveness
- Risks
- Policies for coping with the media and activists

As is mentioned in Chapter 6 (Operational Issues) and Chapter 12 (Project Management), an essential part of any pro-active strategy for implementing ePassports will be consultation with stakeholders involved, to ensure that all aspects of the implementation are well understood and supported. Stakeholders include those such as vendors and their staff, staff of any ministries or other official agencies that have an involvement with any aspect of the implementation, politicians, privacy advocates, academics, various interest groups, as well as the general public.

With regard to the interface between government and vendors on expectations and requirements of both sides, some suggestions for managing these include:

- Encouraging companies to become members of associations or groups that represent large numbers of industry players (not just the biggest companies), so governments can approach them more easily;
- Sponsoring “industry days'” where needed, ensuring wide participation while keeping control;
- Setting up "Public-Private Partnerships", where this is the best option. These partnerships must be handled with care and caution.

Since the concept of biometrics and ePassports will be new to many administrative and operational personnel, and since in the majority of cases they will have little or no experience of biometrics themselves to apply to the functions necessary to manage users and support the application, it is particularly important that they be informed as thoroughly as possible.

As mentioned in Chapter 5, another group that should be the target of a special information campaign are professional photographers, because they will need to understand and comply with ICAO standards for photographs.

Case studies: Public awareness strategies

Australia

An active public relations campaign was undertaken in the lead-up to the introduction of the ePassport:

- to explain the new technology and benefits to the travelling public;
- to address concerns over privacy and other issues (including countering erroneous concerns or fears about privacy);
- to prepare the public for increased cost of passports.

The campaign emphasised the advantages of biometric passports:

- more secure and accurate proof of identity of the passport holder;
- more effective protection against identity fraud (estimated cost of A$1.2 billion in Australia each year), and against the use of false passports by terrorists or criminals;
- biometric technology will enable passport holders to access automated border controls planned for the future in many countries (this aspect was not over-emphasised as these benefits are not yet available).

Hong Kong, China

The ePassport program was publicised via mass media, poster, brochures and the Internet. The campaign was generally effective.

Japan

Japan had a public relations campaign on its ePassport program through the media, on the Foreign Ministry's website, and using posters and leaflets.

Korea

Korea has used, and will continue to use, the media and public hearings to promote ePassport programs to the general public. Scholars and people in the academic community have submitted their own editorials on the issue as well.

Malaysia

Information was disseminated through the media, brochures and website. The effective campaign and the security features of the passport raised public confidence. ePassport applications increase more than 20% every year. Lessons learned include the importance of actions such as (i) carrying out proper examination of supportive documents; (ii) relatively severe penalties for loss of passport due to negligence; and (iii) providing appropriate detection equipment or systems at all entry points, with officers trained to detect forged documents.

The Philippines

The program is quite well known to the public now, through lectures conducted by the Office of Consular Affairs, by word of mouth, and through media reports about the forthcoming implementation. Applicants need to know about the new procedures for issuance of passports and that they need to appear personally to apply for one. It is important for them to know that most countries require machine readable passports by now and [that] it is a condition for travel by April 2010.

Singapore

The campaign carried out before and during the implementation of ePassports in Singapore has been assessed to be effective. Citizens are very receptive towards the introduction of an ePassport for Singapore as they are fully aware of the reasons for introducing the ePassport program. Compliments that have been received from the general public in terms of design, functionality of ePassports and benefits derived from the use of the new travel documents, are a clear indication of acceptance of the ePassport program in Singapore.

(*cont. next page*)

Singapore (*cont.*)

The careful planning in the implementation phase of the ePassport program, international live tests with countries to ensure the interoperability of ePassports and readers, and good publicity to educate the general public on what they can expect in terms of passport fees and the timing for the public launch of the ePassport, are the key factors to ensuring the success of the ePassport program in Singapore.

Thailand
Thailand used newspapers and radio agencies. At all offices leaflets were distributed to the public and announcements made about the timeframe for launching the ePassport. At the beginning of the project, there were many complaints because each applicant now has to come in to enrol, whereas in the old system each applicant could apply at a provincial office. The Thai passport authority has set up a mock border crossing so citizens can become familiar with the system.

The United States
Through the media, brochures, websites, and public outreach appearances by Department of State representatives etc.

References

1. Julian Ashbourn, "The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management", Background paper for the Euroscience Open Forum ESOF 2006, Munich, July 2006.
http://www.statewatch.org/news/2006/jul/biometrics-and-identity-management.pdf
2. Malcolm Crompton (Australian Federal Privacy Commissioner), "Biometrics and Privacy: The End of the World as We Know It or The White Knight of Privacy?"
http://www.privacy.gov.au/news/speeches/sp80notes.htm
3. Ari Juels, David Molnar, and David Wagner, "Security and Privacy Issues in E-passports".
http://eprint.iacr.org/2005/095.pdf
4. A. J. Mansfield and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices", Version 2.01, August 2002.
http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 11 Procurement, Tendering and Contracting

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

11. Procurement, Tendering and Contracting

Once an economy has determined what is required for the development of its ePassport, processes need to be commenced to obtain it. This will require the economy to determine whether elements will be developed in-house (that is, by the passport-issuing authority or by another government agency), or whether some, or all, elements will be outsourced to external providers, either within that economy or from another economy.

ICAO: Issues to consider when deciding to make improvements to passport systems

- What type of procurement do you contemplate for the new passport? Sole-source? Competitive? Multiple contractors? A single prime contractor with subcontractors? Direct purchase of needed materials with government staff performing the integration process?
- Make certain that your contractor can deliver an ICAO-compliant document.

http://icao.int/mrtd/guidance/IssExplanation.cfm

Outsourcing as an Option

Most of the economies that have already introduced ePassports found it necessary to use outsource suppliers for at least part of the ePassport production process, particularly for supply of chips and software for the biometric requirements. For some, the whole process is outsourced; for others, part of the process of producing ePassports (for example, personalisation, certification) is done in-house.

Reasons for outsourcing

- **Expertise**: Outsourcing allows the passport agency to get the best available technological expertise from specialist vendors when the passport agency does not have appropriate expertise.
- **Time**: Outsourcing can cut down on the time needed to achieve implementation.
- **Funds**: Outsource provider may fund the project up front, which may assist an economy with financing the project.
- **Public Key Infrastructure (PKI) separation**: Prudent PKI certificate management suggests it is most desirable for the certificate generation and secure storage operation to be quite separate and distinct from the passport issuance process. In-house establishment of a certificate authority requires duplication of resources.

Some economies opted to have a prime contractor manage all aspects of the production process including design, supply, implementation, commissioning and maintenance of the hardware, software and related services. In such cases, the prime contractor will usually be responsible for calling for tenders for supply of components such as the chip and software (Australia, Hong Kong China, Thailand). Thailand chose a consortium composed of a Thai company and a foreign company; the Thai company had expertise in security printing, while the foreign company had expertise in biometric technology.

Case study: Hong Kong, China

The prime contractor offered a total solution on the design, supply, implementation, commissioning and maintenance of the hardware, software and related services for the implementation of the e-Passport System for the Immigration Department of the Hong Kong Special Administrative Region (HKSAR). The products may be sourced locally or overseas.

Other economies contracted with different suppliers for different elements and managed the overall process through their passport agency or related government agency (Japan, Malaysia, New Zealand, Singapore).

Some economies were obliged under the terms of existing contracts to continue with existing suppliers (for example, for supply of passport booklets), but used other companies to supply the new elements needed, such as biometric software and chips.

In some cases, commercial vendors supply all elements needed for the ePassport, while in others, government agencies perform part of the process. In Australia, for example, the passport booklet is printed by Note Printing Australia (NPA), a subsidiary of the Reserve Bank (Australia's central bank), but other elements (hardware, software, chips) come from private sector suppliers. In the United States, the Government Printing Office produces the US ePassport, but uses equipment, chips, and consumables from non-government vendors.

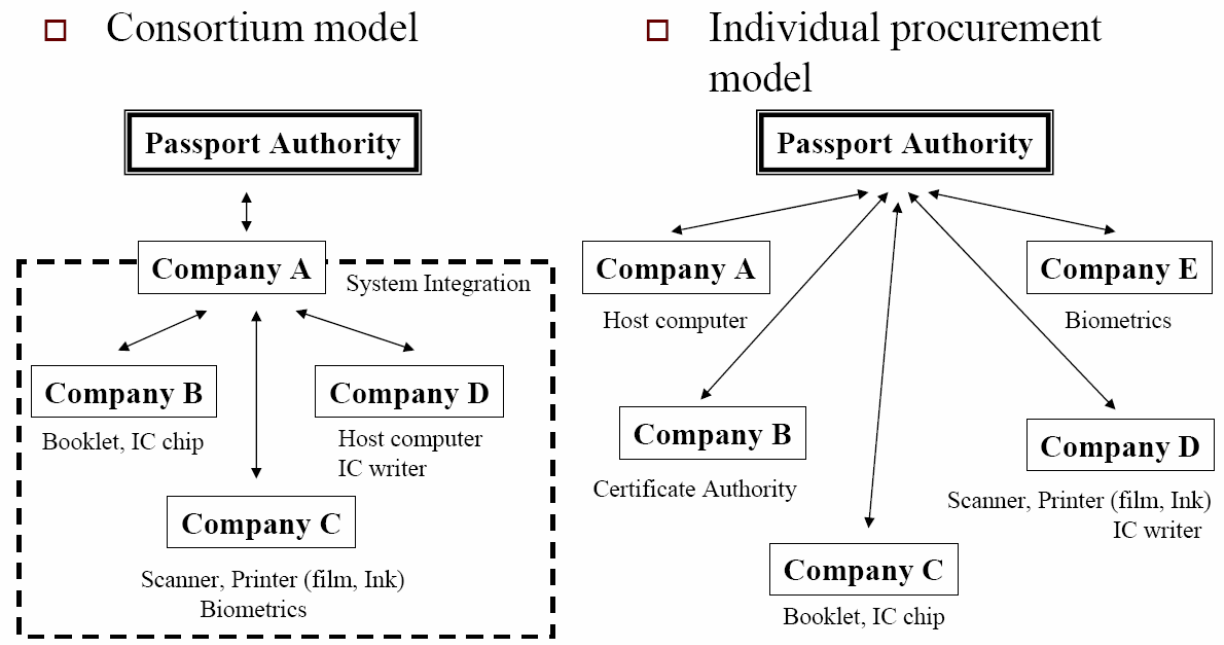
TIP: "Understand that procurement under conditions of 'full and open' competition will prove a challenge. I think we have seen it all—vendors who promised, but could not deliver; other vendors who could make small numbers of samples effectively, but were unable to scale up their operations or consistently meet technical specifications."

Frank E. Moss, "The development of the American e-passport", *Keesing Journal of Documents & Identity*, Issue 17, 2006, pp. 22–24.

There are a few economies that are able to source all the equipment, chips and other requirements in their own economy. For reasons of trust, security, smooth management and better control, Malaysia made the decision that all components of their ePassport and related systems would be procured and developed locally within Malaysia. Japan also has been able to source all components for ePassports from within its own economy. Other economies, however, get all or most of the components for ePassport production from overseas.

Japan has provided the following diagram that shows two options for procurement. One is called the "Consortium model", the other is called the "Individual procurement model". The Consortium model shows the option where a prime contractor has been chosen to manage all aspects of the production process. The "Individual procurement model" shows how the Passport Authority retains overall control of the project but outsources certain elements to various external suppliers.

Procurement Process Options



Procurement, Tenders and Contract Options

Once it has been decided how production of the ePassport is to be carried out, formalised processes involving tenders and contracts will have to be put in place for procuring the necessary services and equipment. All economies have their own established mechanisms and guidelines for government procurement. **The information on tenders and contracts given in the Appendices provide a general outline of standard tendering and contracting processes, including some checklists, and should be used as a guide only.**

ICAO: Issues to consider when deciding to make improvements to passport systems

- Have you thought out how you will verify that you are getting the level of quality that you need from your contractor(s)? Utilising the services of other government offices? Utilising the services of others in the private sector?
- Make sure there is adequate government expertise available to monitor the contractor's performance under the contract.
- Make sure the contractor has adequate on-staff expertise to execute the contract within agreed-upon dates even if human resources on which they depend suddenly exit.
- Involve the users early in the design and testing of the hardware and software. Be certain that the resulting requirements documents are clear and specific.
- Have staff participate in the design of a training program for users, and make certain that there is adequate contractor support for the training process.

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Economies that have introduced, or are considering the introduction of, ePassports either used tender processes for procurement of the various elements needed for ePassports or foreshadowed that they would do so. Some economies had open tenders for all elements, others had preferred providers for some elements and open tenders for others. Some economies invited only companies with demonstrated experience to tender. In the case of Malaysia, the government made a conscious decision to promote the development of "home-grown" (Malaysian) technology, so local vendors and suppliers were approached.

Case study: New Zealand—procurement and support

- Expectations between supplier and Passport Agency were clearly documented
- Complex contract used to manage vendors responsibility throughout personalisation
- Non-capital lease
- Penalty clauses incorporated in contract
- Currency risk incorporated in contract and carried by the vendor
- On-site vendor representation for development and on-going maintenance

"As New Zealand had an existing supply contract for the Passport, we were obliged to develop the ePassport under revised provisions of the contract. Re-tendering for the ePassport was therefore not a viable option as we had an obligation to purchase a certain volume of passport books over a number of years under the existing arrangements.

"A tender process was required to develop the systems incorporating e-passport functionality. As this contained areas of specific technical expertise, two international tenders were issued. Firstly for system design, and secondly for the development and implementation of the system.

"With both tenders for system design and development, tender responses were evaluated by a panel of internal staff with direct knowledge and understanding of the system requirements. The evaluations were scored against a preset criteria and a recommendation made to senior management for the selection of the chosen respondent. Contract negotiations were completed prior to each engagement commencing."

Sample Documents

1. Australia, Department of Foreign Affairs and Trade, “Request for Proposals for Biometrics Research and Development Assistance”, Request for Proposals No. 02/010138
2. New Zealand, Department of Internal Affairs, “Registration of Interest (ROI) for Supply of New Zealand Travel Document Books and Personalisation Technology”, ROI Document Ref: (DIA/2006-014)

Reference

1. UK Home Office, Office of Science and Innovation, Biometrics Assurance Group, “Annual Report 2006”, (May 2007).
http://www.identitycards.gov.uk/downloads/Biometric_Assurance_Group.pdf

Appendices

(The information in these four appendices has been provided by the Australian Department of Immigration and Citizenship (DIAC). However, the information is provided as an example only, and does not constitute legal advice or any recommendation on the part of DIAC. DIAC strongly encourages individuals to seek independent legal advice particular to their circumstances.)

Appendix 1: Stages of Tendering and Contracting
Appendix 2: Sample Procurement Plan
Appendix 3: Template for Statement of Requirement (SOR)
Appendix 4: Template for Evaluation Report and Recommendation

Appendix 1

Stages of Tendering and Contracting

Presented below is a general guide to the stages of a tender and contract process.

Phase 1: Preparing to purchase goods and services
All procurements require appropriate levels of planning. Once it has been decided to proceed with a project, a procurement plan should be developed. All economies will have government guidelines for how procurement of goods and services should be handled, so the plan needs to be prepared in accordance with these. The procurement plan should:

- Identify the outcomes to be achieved, including time and cost elements and risks to be managed;
- Detail the resources required and strategies recommended to manage the project;
- Allocate responsibilities;
- Set out the procedures for project administration and control;
- Detail timing of any necessary approvals;
- Set targets and performance measures to evaluate the planned procurement.

In the case of complex projects, standard planning tools such as critical path analysis, resource allocation and timeline sequencing can be used and software packages designed for project management can help organise and track all the elements.

See Appendix 2 for a sample procurement plan used in Australia.

Phase 2: Preparing and releasing tender documents
As part of the tender documents package, it is useful to draw up a template for responses, so that when tender proposals are received, the material from all vendors will be presented in the same format, making it easier to review numerous proposals and assess them.

In addition, before tender documents are released, you will need to determine what criteria you will use to evaluate tenders.

A Request for Tender (RFT) will usually include a Statement of Requirement (SOR), which lays out in detail what is the intended purpose of the RFT, and it should be written with the single focus of communicating the business requirements for your ePassport production program.

An example of a SOR is attached to this chapter, as a guide to the kinds of issues that will need to be specified in Request for Tender (RFT) documents (see Appendix 3).

Phase 3: Evaluating a tender
When tender responses have been received, they will need to be evaluated. Most economies will have existing government procurement practices that may include:

- satisfying mandatory business requirements;
- evaluating the quality of technical proposals;
- achieving best value for money.

The agency that issued the RFT should review tender responses against specific criteria that have been established for that tender, with particular attention to compliance with the tender requirements. Areas of non-compliance should be identified and addressed.

Financial vetting of vendor companies is an important aspect of this process, in part because the issuing of passports is a critical function, but also because some vendors may be required to provide goods or services over an extended period of time.

An example of an evaluation sheet used in Australia is provided as an attachment to this chapter (see Appendix 4).

Phase 4: Developing and negotiating a contract
Essential elements of a contract development process include the following:

1. Contract negotiations
   - Issues identified by supplier in the tender
   - Variations to the tender proposal required by your agency
2. Obtain any agreement to vary the contract in writing from the supplier
3. Establish the legal entity with which to contract
4. Reference your agency's requirement, or attach requirement
5. Reference the supplier's tender, or attach tender
6. Identify and state the contract deliverables and timeframes
7. Identify and state the nominated personnel
8. Identify and state Intellectual Property issues
9. Identify and state clear performance requirements or a service level agreement
10. Identify and state any need for auditing of performance data or collection by a third party
11. State the start and finish dates for the contract
12. Identify and state the payment milestones and fees payable
13. Consult your agency's legal staff if any change to the standard contract provisions is needed
14. Send two paper copies to supplier for signature
15. When signed copies returned from supplier, obtain signature of your agency's authorised representative
16. Send one signed copy to supplier and keep one copy for your agency.

Phase 5: Managing a contract
A checklist for managing a contract could include:

1. Appoint contract manager
2. Handover from procurement team
3. Obtain copy of signed contract
4. Confirm purchase order was raised
5. Are there clear performance requirements or a service level agreement?
6. Is there a need for auditing of performance data, or collection by a third party?
7. Establish regular meeting with supplier
8. Establish regular reporting arrangements in accordance with the requirements of the contract
9. Is there provision to escalate issues for resolution before they become problems?
10. Contract variation requirements
11. Are payment milestones identified?
12. Are there arrangements for accepting the goods or services?
13. Is there a dispute resolution process in place?
14. Consult your agency's legal area if a dispute situation arises
15. Termination/ensure smooth transition to next Contractor.
16. Retrieving records at the end of the Contract.

Phase 6: Contingency planning
In case some unexpected contingency arises that results in key personnel being no longer available to work on the project, it is essential to have people trained and able to take over at short notice. This is relevant for both a contractor's specified personnel and to the passport agency's project officers.

Appendix 2

Sample procurement plan

PROCUREMENT PLAN FOR *<INSERT NATURE OF SERVICES>*

Purpose:
<This procurement plan seeks approval to proceed with the procurement as outlined. State objectives>

Background:
<Provide background to process>

1. Procurement Overview

1.1 Description:
<Describe nature of services.>

1.2 User Requirements:
<Identify
- who are the users of this proposed service;
- how the user requirements will be met by this procurement;
- how users been involved to ensure their needs are met (e.g. consultation; developing of the specification).>

1.3 Stakeholders:
<Who are the stakeholders, what impact this procurement is likely to make on stakeholders, and how have the concerns and interests of the stakeholders been addressed.>

1.4 Market Conditions:
<Assessment of the market conditions that influence the choice of procurement method and how that assessment was arrived at. This will often be directly linked with the selection criteria (eg, knowledge through constant monitoring of the registrations of quality assured companies that there are limited suppliers with the specialist expertise required).>

1.5 Method of Procurement:
<Type of procurement method proposed (eg, single stage, multi-staged, RFQ, RFT, EOI) and reasons for that method.

Include provision for industry briefing, if appropriate.

If not an open process, then how will the procurement be able to demonstrate value for money?>

1.6 Specifications:
<Statement on who will develop and sign off on the specifications, statement of requirement or tender brief>

1.7 Risk Assessment:
<Statement about the level of risk involved in the procurement and its acceptability or any specific action necessary to manage the risk

Canvas circumstances where the arrangements fail with the preferred supplier and how another supplier would be considered, through the tender evaluation process, to take up and continue with the arrangement with minimal disruption.

Comment on the availability and knowledge of in-house staff with the requirement to ensure a high level of support, management and direction to companies providing the service.

Attach a risk matrix and treatment plan where the value, complexity and sensitivity of the project warrant a detailed assessment of risk.>

1.8 Value of Procurement:
<Estimate of the whole-of-life value of the arrangement, estimated expenditure and identified savings related to the procurement.

Include items such as:
- contract development;
- financial assessment;
- value of services;
- legal advice;
- contract management.>

2. Procurement

2.1 Procurement Team:
<Who will be in the team and what are their roles?>

2.2 Probity Adviser:
<Does the value, complexity and sensitivity of the project warrant the appointment of a probity adviser, and development of a probity plan?>

<Does the project warrant the appointment of a probity auditor. What level of assurance will be sought from the auditor?>

2.3 Proposed Timetable:
<Timetable of key steps, for example:>

Task/Milestone	Responsibility	Due Date
Preparation of Tender Documents and Statement of Requirement		

Appendix 3

Sample Template for Statement of Requirement (SOR)

Statement of Requirement (SOR)

Purpose
Summarise the intended purpose of the Request for Tender (RFT).

Scope
Identify any pre-determined boundaries of the requirement.

1. Background
Provide some operational information that will help give suppliers a complete picture of the needs. Try to give bidders a detailed (and this can be technical) description of the operational environment. This might include operational constraints, equipment, systems or procedures that could impact on the requirement. If it is proposed to replace an existing product or service, provide a description of what that is and how it works now. Put this information into an annex if needed. Copies of reports or studies can provide important contextual information.

2. Requirement
The requirement should have the single focus of communicating the business requirements.

The specification is designed to help the bidders to understand what is required so they can work flow it and price it etc. Try to avoid technical requirements. Assume that the bidders are competent in their field and don't tell them how to do their business. Tell them what is wanted and use them to develop the best solution (in their view) for the needs.

The specifications will, therefore, usually be based on function or performance. They should state what is to be achieved (performance) or what needs to be done (functional) in non-technical terms.

Functional specifications outline the proposed function or role to be played by the product or service in helping the buyer achieve an objective. They define a task or desired result and may describe the general form of the goods or services. They focus on what is to be achieved rather than how it is to be done e.g. transport of goods, versus moving them by a particular means or type of vehicle; or an automated system to perform a nominated function, versus fully defined hardware and software.

Performance specifications detail the required performance characteristics, including acceptable variations, and methods for measuring performance. They are an extension of functional specifications. They set out the required performance by nominating details of the operating inputs and outputs required, but not the methods to be used to achieve them.

3. Skill/Knowledge Needed
Are any special skills or knowledge needed?

4. Timeframe
State the timetable for the whole tender process, and the timetable for the product supply or service delivery arrangement, and the critical dates for other events that it has to meet (if any).

Nominate the length of the contract proposed, and whether or not there will be an option to extend for a further period.

5. Deliverables
State the outputs, or deliverables, that the consultant is required to produce. For example:

"The deliverables for this project are:

a) A detailed evaluation model and methodology (to be developed by the successful consultant) documented for the approval of your agency;

b) Progress reports, the frequency and format of which will be agreed with the successful consultant;

c) A comprehensive final report (one bound paper copy and one copy in Microsoft Office 97 format on an IBM compatible diskette); and

d) An oral presentation of the final report to senior staff."

6. Price
What type of pricing is required? This needs to be stated fairly precisely so that the evaluation team can compare the prices of the various bids. Some common approaches are:

a) Total fixed price quote—usually all-inclusive. This type of price provides certainty on the cost front but requires that the SOR contains all the information needed for them to do a complete costing—it is not appropriate if there are significant uncertainties.

b) Time and materials—usually a daily or hourly rate for personnel plus expenses. Most appropriate if there is significant uncertainty or investigative or development work to be done. There is a risk of cost over-runs with this type of arrangement unless it is closely managed.

c) Price model—the point of a price model is to obtain the costs for typical scenarios of usage for the project in a consistent way from each supplier so that the costs between suppliers can be compared. This technique is most commonly used where the industry pricing is complex with many variables, and suppliers use varying approaches to quoting prices. A typical price model would specify all the details of the costs you want to capture and state all key assumptions. Cost models may be used alone, or in conjunction with other approaches to pricing.

Consider whether or not to publish a budget figure for the project.

Don't publish a figure if the market is well defined, the brief is very detailed and precise and the market is well known. In these circumstances expect price-competitive bids and price will be a major differentiating factor.

Do publish a budget figure if the above conditions don't apply.

Publishing the budget means that most bids will be priced at about that level which means that the focus can be on what you get (service, quality etc) for the money instead of the money itself. This approach also avoids the possibility that bids will be received that are priced well beyond the budget capability of the project (there is not much use getting bids for $200,000.00 if you have a budget of $50,000).

7. Selection
Prepare a format (eg, text and/or a table) for the bidders to provide their responses and to help summarise everything that they need to include in their bids so that the evaluation team can assess them. When the evaluation team comes to read and evaluate the bids it will be helpful to have all this information organised in the same way in each bid.

Sample statement: "Tenders are to be assessed on the basis of best Value For Money consistent with [your agency's] purchasing policies. For the purposes of evaluation, the following criteria will be used to assess Value for Money. Your tender should be arranged to address each of these as indicated in the column headed Response Requirement."

8. Alternate Approaches
Think of your requirement as defining your problem, need or deficiency so that suppliers can use their skills and creativity to design a solution for you—**don't** try to specify the solution.

Make it clear and easy to read. It should make immediate sense to managers, stakeholders and potential suppliers without the need for additional explanation.

Do not include any of the following in the SOR because they will be covered in the other elements of the tender package:

• bid evaluation details;
• contract terms and conditions;
• payment conditions or arrangements.

Generally, a company (or individual) involved in developing a specification should be specifically excluded from bidding for the work. This will help to preserve the appearance of fair treatment of all the potential bidders, and avoid the development of any conflict of interest.

Specifications are sometimes released in draft (if the project is complex, or the requirement is new or leading edge) to get feedback from potential suppliers. When a draft specification is released for comment it must be clear that you are not calling for expressions of interest, quotes, tenders etc. and that the draft specification in no way commits your agency either to that specification or to continuing with the purchase.

The requirement may be supplemented by a briefing, that could take the form of a site inspection, collective oral briefing, or individual briefings. It is sensible to have at least two officers present and to make a brief written note of the discussion.

Most matters can be discussed with a potential bidder related to the project provided that the same information is broadly accessible to all bidders. Do not provide privileged information to one bidder and withhold it from another. If a new bidder appears they should be afforded the same briefings and access opportunities extended to the other bidders.

Once the requirement is included with the RFT documents and released to the public, it cannot be changed without serious consequences to the whole tender process.

9. Conditions of Contract
Specify what kind of contract will apply.

10. Agency Contact
Specify who will be the contact for the RFT.

Appendix 4

Sample Template for Evaluation Report and Recommendation

To <Person in charge>
<Tender Title>
Tender Number < >

Purpose

Background
Tenders were invited to undertake <services>.
Tenders closed on ……. at 2.00pm. There were <specify number> tenders received at the Tender Box from the following organisations:
<names>

Summary of the Bids
Summation of the options received.

Selection Criteria
Responses were evaluated against the following criteria, and the response requirements specified to the tenderers are shown against them:

Criteria	***Response Required***
1.	
2.	
3. .	
4. .	
5.	
6. .	

Example of evaluation through a process of elimination

Stage	**Process**	**Criterion**
Stage 1	Preliminary Evaluation	Eliminate tenders that do not comply with preliminary evaluation criteria
Stage 2	Detailed Evaluation	Eliminate tenders that do not comply with detailed evaluation criteria
Stage 3	Cost Comparison	Compare total cost of all tender proposals, so as to derive the tender proposal that meets all requirements and provides the most cost effective and value-for-money services.

Approach to the Evaluation
The evaluation was undertaken by <specify persons>. The following procedure was followed:

<Example:
Review tenders for compliance
Identify and assess areas of non-compliance
Allocate score between 0-10 against each tenderer for each criterion (Each person made their evaluation separately)
Maximum 10
Minimum 0 (see table below for details)
Agree score against each criterion and complete spreadsheet (Attachment A-Evaluation Matrix)
Adjust scoring in accordance with agreed weightings (calculated automatically in the spreadsheet)
Recommendation>

All evaluators used the following scoring protocol:

Standard Rating Protocol © Enterprise Outsourcing (ACT) Pty Ltd	
Rating	**Description**
0	Does not meet the criteria at all. There may be a lack of supporting information or insufficient information to be able to rate it. Otherwise unacceptable.
2	Marginal or poor quality, mostly does not meet expectations. Important supporting information is missing or deficient. Difficult to assess.
4	Adequate or satisfactory, limited meeting of expectations. There may be shortcomings in scope or detail. Workable.
6	Good quality, mostly meets expectations. Selection criteria are satisfied in all respects and supporting information is convincing.
8	Very Good quality, meets all expectations. Supporting information is complete and comprehensive.
10	High quality that exceeds expectations. Referees confirm ability to consistently deliver superior performance. Outstanding.

Copies of the individual score sheets supporting the aggregated scores in Attachment A are available. A summary of tender responses is at Attachment B.

Individual Assessments

This chapter summarises each of the bids against the selection criteria. Could be an attachment.

Results

The scoring reflected the overall impressions of the evaluation team, and the final price index also reflected these impressions.

The scores for all the qualitative issues were as follows (highest is best): .....

Value for money is a combination of quality and price issues. A simple price index is a way of combining these factors to represent a value for money assessment. The price index is derived by dividing the qualitative score into the total price (tenderers were asked to provide a total, all inclusive, fixed price quote). This gave the following result (lowest score is best): .....

This chapter should include some cost analysis.

Other Issues

Each tenderer was asked to indicate the extent to which they were prepared to comply with the standard contract terms and conditions of the [economy's government]. The following responses were received:

Schedule B2 – Statement of Compliance with Draft Contract

Contract Clause/Annex/Attachment Number	**Tenderer's Response (complies/does not comply)**

COMMONWEALTH OF AUSTRALIA

Department of Foreign Affairs and Trade

REQUEST FOR PROPOSALS

FOR

BIOMETRICS RESEARCH AND DEVELOPMENT ASSISTANCE

REQUEST FOR PROPOSALS No. 02/010138

Table of Contents

1. OVERVIEW

1.1. Introduction

1.1.1 Passports Australia collectively refers to Passports Branch and the passport issuing offices within the Department of Foreign Affairs & Trade (DFAT).

1.1.2 Passports Australia's vision is to "provide a world-class passports service to Australians" and it is recognised world-wide as having achieved this. Passports Australia is a leading-edge implementer of enabling technologies including integrated imaging, handwriting recognition and workflow systems.

1.1.3 Passports Australia has undertaken significant research into the feasibility of using facial biometrics to reduce the incidence of identity fraud and to enhance border control.

1.1.4 Following successful trials conducted in 2001 and 2002, Passports Australia is now seeking specialist assistance from an Australian Government Endorsed Supplier to undertake further research, development and testing of facial biometric solutions.

1.1.5 It is anticipated that this program will commence in August 2002 and that much of it will be completed by 30 November 2002.

1.2. Background

1.2.1 The Department of Foreign Affairs and Trade is authorised to issue Australian Travel Documents (Passports and Documents of Identity) to citizens of Australia under the Passports Act 1938 as amended and Passport Regulations in force under that Act.

1.2.2 Passports Australia issues Australian Travel Documents from its 9 offices located in all States and Territories within Australia. Passports are also issued through Australian missions (Embassies, High Commissions and Consulates) overseas. Passport Applications are accepted at some 1600 Australia Post outlets around Australia and almost 100 Australian missions overseas.

1.2.3 Information about the services provided by Passports Australia is currently available through its website www.passports.gov.au. The information on this website is for background only and does not form part of this RFP document.

1.2.4 Australia issues some one million passports per year. Applicant photographs are supplied with the passport application form and scanned at passport issuing offices. Australia has been storing scanned photographs since late 1999 and has approximately 2.5 million 24 bit full colour 600dpi JPG photographs on file in an optical jukebox database.

1.2.5 Information about the process of applying for a passport, including the current specified requirements for applicant photographs, can be obtained from the Australian Adult Passport Application form, which is available from any Post Office.

1.2.6 There is an increasing level of identity fraud being detected in applications for Australian Passports, and an increasing number of fraudulently obtained passports being found in police raids.

1.2.7 In addition, the events of September 11 have resulted in the US Congress passing the Enhanced Border Security and Visa Entry Reform Act in April 2002. This Act requires countries that currently hold visa waiver status to introduce tamper proof passports, containing a biometric linking the passport to its holder, to maintain that status. Australia is such a country.

1.2.8 To further enhance the security and tamper-proofness of Australian Passports, and to meet various emerging international standards, Passports Australia is currently engaged in the design and development of a new Australian Passport, to be issued from mid 2003.

1.3. Timetable

1.3.1 An indicative timetable for the RFP process is set out in the following table:

Issue RFP	3 July 2002
Responses Close	25 July 2002 at 2.00 pm
Evaluation of Responses	25 July – 2 August 2002
Presentations	29 – 30 July 2002
Finalise Process	By 9 August 2002

1.4. Further Information

1.4.1 Further information in relation to this RFP can be obtained from the Commonwealth Representative:

1.4.2 All questions and correspondence in relation to this RFP must be furnished in writing to the Commonwealth Representative.

1.4.3 Answers to all queries will be circulated (via email) to all potential respondents to this RFP.

2. GENERAL CONDITIONS OF RESPONSE

2.1. Definitions

2.1.1 In this RFP, unless the context otherwise requires:

"**Annex**" means an annexure to this RFP;

"**Assignment**" means undertaking activities as per the Scope of Work in Section 4.3 of this RFP

"Closing Date" means the date specified in Item 1 of Annex A;

"Commonwealth" means the Commonwealth of Australia;

"Commonwealth's Representative" means the person specified in Item 2 of Annex A;

"Department" means the Department of Foreign Affairs and Trade representing the Commonwealth;

"GST" means Australian Goods and Services Tax;

"Respondent" means a person who has submitted a Response pursuant to this RFP;

"Response" means a written response pursuant to and in accordance with this RFP;

"Response Form" means the form at Annex B of this RFP;

"Services" means the services described in the Statement of Requirements;

"Small and Medium Enterprises" means companies employing fewer than 200 employees;

"Statement of Requirements" means the requirements specified in Section 4 of this RFP;

"Supporting Material" means material that:

a) the Respondent is not required to include in or submit with the Response Form; and

b) elaborates or clarifies the material included in or submitted with the Response Form, but which does not alter it in any material respect.

"Travel Document" means Australian Passports and Documents of Identity and includes the:

a) Ordinary Passport

b) Frequent Traveller Passport

c) Official Passport

d) Diplomatic Passport

e) Certificate of Identity

f) Document of Identity

g) Convention Travel Document (Titre de Voyage);

2.2. Interpretation

2.2.1 In this RFP, unless the context otherwise requires:

Plurals/Gender/Persons: the singular includes the plural and vice versa; words importing one gender include all genders; and a reference to a person includes a corporation, body corporate, statutory authority or other entity;

Legislation: a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

Successors: a reference to a party includes a reference to its successors, administrators, executors and assigns;

Headings: headings are for convenience only and do not affect the interpretation of this RFP;

Monetary Units: a reference to monetary units is a reference to Australian currency ($A);

Joint and Several: any covenant, term, condition or provision of this RFP to be performed or warranty, guarantee or indemnity given by two or more persons binds those persons jointly and each of them severally;

Time: a reference to time is a reference to Australian Eastern Standard Time (AEST);

Limitation: “including” and similar expressions are not words of limitation.

2.3. Acknowledgement and Disclaimer

2.3.1 All information (whether written, oral or in any other form) which has been and may subsequently be made available to Respondents to this RFP (“Respondents”) including any attachments to this RFP is provided on the following conditions:

(a) Respondents do not rely on:

(i) any representation (whether oral or in writing) other than as expressed in this RFP; or

(ii) other conduct of the Commonwealth, or any of its officers, employees, advisers or agents in deciding to lodge or not to lodge an expression of interest;

(b) the contents of the RFP are believed to be accurate as at the date of the document. The statements, opinions, projections, forecasts, or other information contained in the RFP may change. Where any such information relates to future matters, no steps have been taken to verify that the information is based upon reasonable grounds, and no representation or warranty, expressed or implied, is made by the Commonwealth, or any of its officers, employees, advisers or agents that the statements contained in the this RFP will be achieved;

(c) this document is designed to reflect and summarise information concerning the Services only and is not a comprehensive description of the Services;

(d) the Commonwealth will not be responsible for any costs or expenses incurred by any Respondent in preparing and lodging their Response;

(e) neither the delivery of the RFP nor any agreement made subsequent to this RFP shall imply that there has been no material change in the affairs of the Department or the Services since the date of this document or since the date as at which any information contained in this RFP is stated to be applicable;

(f) except as required by law and only to the extent so required, neither the Commonwealth, nor its respective management, agents and advisers shall in any way be liable to any person or body for any loss, damage, cost or expense of any nature arising in any way out of or in connection with statements, opinions, projections, forecasts, or other representations, actual or implied, contained in or omitted from this RFP or by reason of any reliance thereon by any person or body;

(g) Respondents should take their own professional advice as appropriate;

(h) Respondents are not to construe this RFP as investment, legal or tax advice; and

(i) It is not intended by the Commonwealth or a Respondent that the issue of this RFP or any Response to it commits, obligates or otherwise creates a legal relationship in respect of entering into a contract with that party or the process to be followed in handling proposals submitted by that party.

2.4. Governing Law

2.4.1 This RFP shall be subject to and construed in accordance with the law in force in the Australian Capital Territory.

2.5. Submission of Response

2.5.1 A Response may only be made by the submission of a completed Response Form (Annex B).

2.6. Language and Units of Measurement

2.6.1 All Responses, Supporting Material and any other supporting technical data, or other material must be:

(a) written in the English language; and

(b) refer only to Australian legal units of measurement.

2.7. Execution

2.7.1 The Response Form must be executed by the Respondent according to item 1.8 of the Response Form (Annex B).

2.7.2 If the Response Form is executed under a power of attorney, that power of attorney must be registered and a copy submitted with the Response Form.

2.8. Packaging and Identification of Responses

2.8.1 Responses must be lodged in a sealed envelope or wrapping which clearly identifies the RFP number, “PASSPORTS BRANCH” and the Closing Date. Responses are to be endorsed with the name and address of the Respondent and lodged in accordance with the lodgement directions in Annex A.

2.9. Submission of Copies

2.9.1 The Respondent must submit an original and three hard copies of:

(a) the Response Form, completed in accordance with this RFP;

(b) any documents/appendices required to be submitted with the Response Form; and

(c) any Supporting Material.

2.9.2 The Respondent must lodge one electronic version of the Response Form in MS WORD 97 (or later version) on CD ROM. The electronic document must include on the CD any non-standard Windows fonts used in preparation of the RFP and must be readable in an MS OFFICE XP environment.

2.9.3 The Response will become the property of the Commonwealth at the time of lodgement and the documents will be retained as commercial-in-confidence. The Commonwealth is not obliged to return any copies of the Response Documents.

2.10. Place for Lodgement of Responses

2.10.1 Responses may be lodged by hand delivery or courier service to the address specified in Item 3 of Annex A.

2.11. Closing Date

2.11.1 Responses may only be lodged before 2.00 pm AEST on the Closing Date specified in Item 1 of Annex A.

2.12. Late Responses

2.12.1 Any Response which is lodged after 2.00pm (AEST) on the Closing Date is late.

2.12.2 All late Responses will be the subject of a decision by the Commonwealth as to whether or not they are to be admitted for evaluation. Any such decision will be final.

2.12.3 In considering its decision, the Commonwealth will have regard to whether the Respondent has gained an unfair advantage.

2.13. Respondent to Inform Itself

2.13.1 A Respondent is deemed to have:

(a) examined this RFP and other information made available in writing by the Commonwealth to Respondents for the purposes of responding;

(b) examined all information relevant to the risks, contingencies, and other circumstances having an effect on the Response and which is obtainable by the making of reasonable enquiries;

(c) satisfied itself as to the correctness and sufficiency of the Response; and

(d) satisfied itself as to the nature and effect of any laws regulating the provision of the Services.

2.14. Respondent's Warranties

2.14.1 The Respondent warrants that in the preparation of the Response:

(a) neither itself nor any of its servants or agents has entered into, or will enter into, any contract, arrangement or understanding to pay any money or provide any other benefits to any trade association in respect of the Response or any Contract resulting therefrom;

(b) neither itself nor any of its servants or agents have, at the date of submission of its Response, knowledge of the terms and conditions of any Response submitted by any other Respondent;

(c) neither itself nor any of its servants or agents has disclosed, or will disclose, prior to the acceptance of a Response by the Commonwealth the terms of its Response to any other Respondent who submitted or proposes to submit a Response for the Services, or to any other person or organisation (excepting its legal and financial advisers);

(d) neither itself nor any of its servants or agents has provided, or will provide, information to any other Respondent or prepare a Response known as a "cover bid", whereby the Respondent is of the opinion or belief that another Respondent does not intend to genuinely compete for the Services; and

(e) neither itself nor any of its servants or agents, prior to the submission of its Response, entered into any contract, arrangement or understanding having the result that on being awarded the Contract, the Respondent would pay to any other Respondent who unsuccessfully responded for the Contract, any moneys or provide any other benefit in respect of or in relation to the Response or any Contract resulting there from.

2.15. Conflict of Interest

2.15.1 Respondents must state any circumstances or relationships which constitute or may constitute a conflict or potential conflict of interest in respect of this RFP or the Respondents obligations under any resulting contract if the Respondent is ultimately awarded a contract by the Commonwealth.

2.16. Supporting Material

2.16.1 Supporting Material may:

(a) only be provided to the Commonwealth by the Respondent, if the Respondent submits with the Response Form a written statement of its intention to provide Supporting Material;

(b) be requested by the Commonwealth;

(c) only be lodged with the Commonwealth before the Closing Date unless specifically requested by the Commonwealth after the Closing Date; or

(d) be disregarded by the Commonwealth, in its absolute discretion, if it is lodged after the Closing Date, unless specifically requested by the Commonwealth after the Closing Date.

2.16.2 Supporting Material must be lodged in a sealed envelope marked with the words "Supporting Material" and the RFP number.

2.16.3 Supporting Material which, in the opinion of the Commonwealth, effectively alters the Response Form will not be admitted to the evaluation.

2.17. Clarification and Amendment

2.17.1 Enquiries by prospective Respondents for further information or queries regarding the RFP must be directed to the Commonwealth's Representative at the address specified in Item 2 of Annex A. The Commonwealth's Representative requires that all enquiries be in writing.

2.17.2 No enquiry, request or notification pursuant to subclause 2.18.1 will entitle the Respondent to a variation of the Closing Date.

2.17.3 If a Respondent finds any discrepancy, error or omission in its Response the Respondent must notify the Commonwealth in writing of such discrepancy, error or omission on or before the Closing Date.

2.17.4 If any part of a Response is uncertain or unclear, the Commonwealth may, in its absolute discretion, seek clarification from the Respondent.

2.17.5 The Commonwealth reserves the right to amend the RFP at any time not less than five (5) business days prior to the Closing Date. Any amendment or clarification to any aspect of the RFP will be issued in the form of addenda and will be issued to all Respondents before the Closing Date. No explanation or interpretation of the RFP may be relied upon by the Respondent unless given in the form of addenda. Any such addenda will become part of the RFP.

2.18. Complying Response

2.18.1 A complying Response is a Response which:

(a) complies with every condition and requirement of this RFP;

(b) specifically responds to every Item in the Response Form; and

(c) is clear, precise and definite in response to every Item in the Response Form and, where appropriate, refers to the relevant page or paragraph numbers of this RFP and responds to them in numerical order.

2.19. Failure to Respond to an Item in the Response Form

2.19.1 If there is no response to an Item in the Response Form, the Response will be deemed not to comply with the stated requirement for evaluation purposes.

2.20. Non-Complying Response

2.20.1 The Respondent acknowledges that the degree of compliance with the Items in the Response Form and the conditions of this RFP will be an important consideration in the process of evaluating Responses.

2.20.2 The Commonwealth accepts no responsibility for the failure by a Respondent to comply with, or any misunderstanding by the Respondent of, this RFP including, without limitation, clause 2.20.

2.20.3 If a Response does not fully comply with this RFP, the Respondent must list by reference to the relevant page, clause or paragraph number every part of the RFP which has not been complied with.

2.20.4 Consistent with the Commonwealth's objective of achieving relevant best practice, a Respondent may submit a non-complying Response which the Respondent proposes as an alternative means of meeting the Commonwealth's requirements.

2.20.5 A Respondent may only lodge a non-complying Response if it clearly:

(a) specifies each instance of non-compliance; and

(b) states the reasons for each instance of non-compliance.

2.20.6 When a non-complying Response is received, the Commonwealth, at its discretion, may:

(a) exclude such non-complying Response from further consideration;

(b) enter into further negotiation with the Respondent on the basis of the non-complying Response; or

(c) accept such a Response.

2.21. Alterations and Amendments

2.21.1 Alterations will be permitted to be made to Response documents only:

(a) prior to the Closing Date; and

(b) if it can be shown to the satisfaction of the Commonwealth that a clerical/keyboard error has been made.

2.22. Illegible Responses

2.22.1 The Commonwealth may in its absolute discretion exclude from further consideration any Response that contains alterations or erasures and Responses which are illegible at the time of the lodgement.

2.23. Reservation of Rights

2.23.1 The Commonwealth reserves the right to:

cease to proceed with, suspend, vary the structure or alter the process (including the timetable) outlined in this RFP;

(a) in its absolute discretion, accept or reject any Response;

(b) issue a further specification or tender document to any Respondent;

(c) negotiate directly with any Respondent;

(d) enter into and conclude negotiations with any Respondent or any other person at any time on or after the Closing Date;

(e) in its absolute discretion, enter into any agreement for the provision of the Services on such terms as may be acceptable to the Commonwealth;

(f) add to, or remove any Respondent;

(g) require clarification of a Response or seek additional information from any Respondents;

(h) set priorities and weight assessment criteria or vary those priorities or weightings;

(i) accept a Response for a different requirement than is set out in this RFP; and

(j) cancel, add to or amend the information, requirements, terms, procedures or processes set out in this RFP; and

(k) the Respondent acknowledges that any such action of the Commonwealth will not lead to the Commonwealth incurring any liability or obligation to pay the Respondent or any other person any loss, damage, costs or expense incurred by that person.

2.24. Respondent's Personnel

2.24.1 The successful Respondent, and each person employed or engaged by the successful Respondent, or any subcontractor, to perform the Services in relation to any Contract, may be required to undergo security checks to the satisfaction of the Department.

2.25. National Competitiveness and Industry Development

2.25.1 National competitiveness and industry development is one of the fundamental principles of Commonwealth purchasing. The Government has announced that, where appropriate, industry development criteria must be included in projects valued in excess of $10 million.

2.25.2 Further information on this policy is available at www.dofa.gov.au.

2.26. Disclosure of Information by the Commonwealth

2.26.1 The Commonwealth is required by law to publish summary details of most of its contracts.

2.26.2 The Freedom of Information Act 1982 (the “FOI Act") gives members of the public rights of access to official documents of the Commonwealth Government and its agencies. The FOI Act extends as far as possible the right of the Australian community to access information (generally documents) in the possession of the Commonwealth Government limited only by exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by departments and public authorities.

2.26.3 Respondents are responsible for assessing the application of the FOI Act to any information and documentation contained in their Responses.

2.27. Confidential Information

2.27.1 DFAT operates within a Government and accountability framework which requires it:

- to ensure openness and transparency through a public reporting process;
- to allow for external scrutiny, for example by the Auditor-General and the Ombudsman; and

- on behalf of Ministers, to provide information to the Parliament of Australia, acting through its committees

2.27.2 In submitting a proposal the Respondent agrees to the disclosure of information in the proposal, for the purposes of this proposal process and any legal, policy or other Government accountability requirements, to:

(a) DFAT staff, employees and advisors for the purpose of this proposal process;

(b) the Minister;

(c) the House or a Committee of the Parliament of the Commonwealth of Australia;

(d) other Commonwealth departments, agencies, authorities and Ministers;

(e) the Auditor-General; and

(f) the Ombudsman.

2.27.3 If DFAT and a Respondent enter into contract negotiations, the confidentiality of contractual information and contractual provisions will be the subject of negotiation. Respondents are advised that a request for information to be protected as confidential must be supported by legally sustainable reasons.

2.27.4 Should DFAT agree to protect contractual information or provisions as confidential, the agreed position will be set out in any agreement that may be made between DFAT and the Respondent.

2.28. Respondents to list Confidential Information

Should DFAT enter into negotiations with the Respondent for the provision of services to the Commonwealth, the confidentiality of contractual information and contractual provisions will be the subject of negotiation. Respondents should list at item 1.7 of the Response Form (Annex B) any information provided in the response to this RFP that it wishes DFAT to protect as confidential and provide reasons.

2.29. Compliance with Law

2.29.1 The Respondent must comply with:

(a) all relevant legislation of the Commonwealth (particularly the Crimes Act 1914, Privacy Act 1988, Racial Discrimination Act 1975, Sex Discrimination Act 1984, and Disability Discrimination Act 1992) or of any State, Territory or local authority; and

(b) any obligations it has under the Equal Employment Opportunity for Women in the Workplace Act 1999.

2.30. Copyright Notice

2.30.1 This publication is copyright. Other than with the written permission of the Commonwealth, this RFP, or any part of it, may not be reproduced, stored in a retrieval system or transmitted in any form, by any method (including electronic), for any purpose, except as expressly permitted under relevant copyright legislation.

3. EVALUATION OF RESPONSES

3.1. Evaluation Criteria

3.1.1 Responses that do not, to the satisfaction of the Department, demonstrate relevant experience in the research, development and application of facial biometric solutions will not be evaluated.

3.1.2 The following evaluation criteria will be considered to determine the response which best meets Passports Australia's requirements and which represents best value for money:

(a) compliance with this RFP;

(b) status as an Australian Government Endorsed Supplier

(c) Proposed approach to the assignment, including flexibility and adaptability

(d) Relevant expertise and experience in the provision of independent research, development and implementation of biometrics, in particular facial biometrics and facial recognition solutions

(e) relevant expertise and experience in constructing scalable architectural designs customised to suit solution needs and the provision of viable, high performance information technology solutions to support mission critical applications

(f) relevant expertise and experience in the application of storage media solutions for cards and/or booklets

(g) relevant expertise and experience in the large scale conversion and matching of image files

(h) experience in the application of Privacy legislation and Information Privacy Principles

(i) capacity to prepare succinct, high quality strategic documents, including reports and business cases for Australian Government organisations

(j) quality, presentation and layout of the response to this RFP

(k) price; and

(l) risk.

3.1.3 Respondents should note that although the foregoing criteria are not necessarily in order of importance, nor exhaustive, they are representative generally of those factors which will be considered in the evaluation process.

3.1.4 In assessing Responses, the Department will use a weighted scoring methodology to assess the level to which the requirements have been met, and will undertake a risk assessment.

3.2. Evaluation Material

3.2.1 The detailed responses to the Items in the Response Form and this RFP and any further material provided or obtained from presentations, demonstrations, site visits or reference sites may be used to make assessments against the criteria set out in clause 3.1.

3.2.2 In assessing the financial viability of the Respondent, the Department may consider:

(a) status as an Australian Government Endorsed Supplier

(b) information obtained from annual reports, financial statements and other financial information provided by the Respondent;

(c) other publicly available information; and

(d) information obtained from credit reference or rating organisations.

3.2.3 The Commonwealth may, at its absolute discretion, consider other relevant material in making assessments against the criteria set out in clause 3.1.

4. STATEMENT OF REQUIREMENTS

4.1. Introduction

4.1.1 Passports Australia is seeking specialist assistance from an Australian Government Endorsed Supplier to undertake research, development and testing of facial biometric solutions.

4.2. Objectives of Research, Development and Testing Program

4.2.1 The objectives of the program for Passports Australia, are to build on the 12 months of research and development already undertaken to enable Passports Australia to:

- Develop a detailed project plan to achieve the objectives of the program
- Select (and/or confirm selection of) appropriate facial recognition software algorithms,
- Conduct detailed costings of technology implementation
- Acquire software licences and develop appropriate partnership agreements with vendors
- Specify, select, acquire and install hardware to support large scale testing and associated implementation
- Enrol several million facial images, including retrospective conversion from the existing Passports photograph image database, and ongoing enrolment for research purposes
- Conduct further analysis on matching results against this database, including further research and proof of concept tests and follow through of any fraud detected
- Analyse the effects of filtering matches to reduce the candidate set matched against, and hence the size of the potential exception set eg. streaming by age, sex, height etc.
- Analyse issues relating to security, technology, performance, enrolment and customisation
- Work with the Privacy Commissioner in responding to any privacy concerns in relation to the program and its resultant initiatives

- Obtain a better understanding of real life matching outcomes to enable the application of risk management principles to identity verification processes

- Design, develop, test and pilot integration of facial recognition extraction and matching into Passports Australia's existing enrolment and eligibility computer systems for identity verification purposes

- Faciliate the undertaking of appropriate customisation of selected facial recognition algorithms and software specific to the needs of Passports Australia, and as necessary the potential needs of Australian Customs and overseas Government border control environments

- Participate with Customs, as appropriate, in crew trials at airports, and subsequent trials to determine the viability of a facial biometric for Australian border control purposes

- Determine the optimal specifications for the capture and storage of images so as to maximise performance of facial recognition products in both identification and live verification modes

- Conduct research and development into the technology for insertion of biometric templates and/or images into the Australian passport via an appropriate interoperable storage medium

- Develop modifications to passport application forms to facilitate the collection of the biometric eg guidelines on how the photograph should be taken, additional questions with respect to twins, height etc.

- Continue to monitor overseas developments in biometric enrolment and border control

- Continue to actively participate in International forums and Standards groups regarding biometric technology and development of interoperability standards

- Prepare a detailed business case, with thorough cost and risk analysis, for implementation of facial biometrics for identity verification and fraud detection, and for the secure placement of a biometric in the new passport, which can be used for border control purposes

- Professionally document activities undertaken, outcomes achieved, and proposals for future activities

4.2.2 A key outcome of the program will be the preparation of a Business Case for consideration in the 2003/2004 budget context.

4.2.3 It is anticipated that the program will commence in August 2002 and that much of it will be completed by 30 November 2002.

4.2.4 The selected respondent is expected to provide specialist advice and assistance to support this program, as set out in the Scope of Work.

4.2.5 Passports Australia will manage and provide the direction for the program.

4.3. Scope of Work

4.3.1 The selected respondent will assist Passports Australia with tasks regarding research, development, testing and documentation with respect to facial biometrics technology, including:

(a) Develop and maintain a Project Plan for the program, and supporting plans as appropriate

(b) Review work Passports Australia has undertaken to date and provide comments with respect to the selection, or confirmation of selection, of facial recognition software vendor(s) to potentially participate in the program

(c) Specification and selection of hardware architecture required as a high performance platform for testing Passports Australia's chosen software solution(s)

(d) Conversion of Passports Australia's existing 2-3 million photograph database into a format to enable 1:many identification and 1:1 verification matching

(e) Integration of facial biometric database software and hardware to provide a large-scale test environment

(f) Development and undertaking of research tests and proof-of-concept tests, including but not limited to:

- facial recognition algorithms
- face finding algorithms

- eye finding algorithms
- database search techniques
- database match filtering techniques
- photograph image capture and cropping methods
- image enhancement aids
- hardware and software performance enhancement aids
- automation of processes to minimise as well as value-add necessary manual decision making
- automated border control (as required)

(g) Analysis of security, technology, performance, enrolment, scaleability and customisation issues

(h) Analysis of the performance of facial recognition software in relation to a range of variables, including but not limited to:

- ethnicity
- aging
- pose
- facial expression

(i) Provision of advice on developments overseas, in the biometrics arena, that the respondent becomes aware of

(j) Identification, discussion and input to the resolution of potential privacy issues

(k) Investigation, testing and piloting of how the technology would be integrated into Passports Australia's existing passport issuing systems (both in Australia and overseas) and, where appropriate, into Border Control systems

(l) Undertake risk assessment analysis and recommend thresholds and business practices for determining the optimal balance between automated vs manual facial matching acceptances in an identity confirmation situation

(m) Secure placement of a biometric in the new Australian passport, including

- Identification of storage media vendors
- Analysis of technology options given constraints and considerations of the passport booklet; length and type of data to be stored; robustness; security; speed of retrieval, international standards; business requirements of DFAT, Customs and DIMIA; business requirements of other Governments such as the USA
- Booklet production line insertion
- Writing, reading, updating and protection of data
- Compliance with ICAO data encoding standards
- Verification and reliability testing
- Interoperability development, encoding and piloting with Customs and DIMIA
- Interoperability development, encoding and piloting with overseas Governments

(n) Preparation of high-quality explanatory documentation as required to support the research and development program, which includes descriptions of the processes, procedures, findings and results

(o) Preparation of a detailed business case, with thorough cost and risk analysis, for implementation of

- facial biometrics into Passports Australia's systems, for identity verification and fraud detection
- the secure placement of a biometric in the new Australian passport which can be used for border control purposes

4.4. Project Management and Technical Direction

4.4.1 All work will be undertaken under the specific direction of Passports Australia staff.

4.4.2 The Project Director is Mr John Osborne, Director Passports Systems and Technology.

4.4.3 The Technical Director is Mr Terry Hartmann, Manager Passports IT.

4.5. Location

4.5.1 It is expected that project management and the majority of the integration, conversion and testing work will be undertaken in Canberra.

4.5.2 All testing involving Passports Australia's data will be performed in Australia, and preferably in Canberra

4.5.3 It is envisaged that some activities may require a resource presence in Europe and/or the United States of America.

4.6. Supply of Hardware and Software

4.6.1 This RFP specifically excludes the supply of hardware and software solutions.

4.6.2 Any hardware or software required to meet the requirements of this research, development and testing program will be acquired separately by the Department of Foreign Affairs and Trade.

4.7. Confidentiality

4.7.1 Respondents are reminded of the provisions of the Deed of Confidentiality they signed in order to obtain this RFP.

4.8. Contract Arrangements

4.8.1 A contract will be negotiated in accordance with the GITC 4 Head Agreement.

4.9. Presentations

4.9.1 The Department may choose to shortlist respondents and to invite those shortlisted respondents to make presentations of their solution to the RFP Evaluation Panel.

4.9.2 All presentations will be in held in Canberra at the respondent's or the Department's premises, as preferred by the respondent.

4.9.3 Presentations will be of up to 1 hour's duration with a subsequent 20 minute time allocation for questions.

THE DEPARTMENT OF INTERNAL AFFAIRS

Te Tari Taiwhenua

Registration of Interest (ROI)

For

Supply of New Zealand Travel Document Books and Personalisation Technology

Department of Internal Affairs

ROI Document
Ref: (DIA/2006-014)

Commercial in Confidence

The Department of Internal Affairs may, at its absolute discretion and without limitation, amend or withdraw this document at any time.

Table of Contents

1 ROI Information

1.1 ROI objective

The purpose of this Registration of Interest (ROI) is to establish a short list of interested vendors (Respondents) to participate in the Request for Proposal (RFP) process for the supply and support of travel documents and personalisation technologies for New Zealand's Department of Internal Affairs (DIA).

To this end, DIA is looking for a well-established, experienced passport manufacturer to lead a consortium providing travel document books and personalisation technology for the expected 5 year duration of the contract.

1.2 Registration closure date

Registrations must reach the Procurement Manager **no later than 12 noon (New Zealand time) Friday 15 September 2006**.

1.3 Registration delivery

The registration should be mailed to:

Department of Internal Affairs – National Procurement Group
PO Box 805
Wellington
New Zealand
Ref: DIA/2006-014
Attention: Craig Doherty, Procurement Manager

If required, hand delivered or couriered registrations can be delivered to:

Level 1 Reception
46 Waring Taylor Street
Wellington
New Zealand

1.4 Clarification process

All communications, including requests for clarification of requirements or additional information, pertaining to this ROI are to be submitted by email to craig.doherty@dia.govt.nz. Please note that Respondents, including organisations with existing relationships with DIA, may not question or canvass DIA staff on this ROI other than through Craig Doherty by e-mail. Any breach of this requirement will risk exclusion of the Respondent from the ROI and any future RFP processes.

Clarification requests should be submitted no later than 5pm, Monday 11 September 2006 (New Zealand time).

DIA will endeavour to provide a response to all clarifications within two (2) working days of receipt.

Clarification process, continued

DIA will release all clarifications to all Respondents who have registered to receive a copy of the ROI document. The exception to this is where a Respondent asks a question that involves proprietary ideas or matters of importance that are clearly stated to be "confidential due to commercial sensitivities or trade secrets". DIA will not release such information to other Respondents, without prior agreement of the questioning Respondent, unless compelled to do so by law.

1.5 Registration content

Every registration must:

a) be provided in a securely sealed envelope and labelled as follows:

ROI REF: DIA/2006-014

ROI NAME: Supply of New Zealand Travel Document Books and Personalisation Technology

COMMERCIAL IN CONFIDENCE

b) have an ROI Response Cover Sheet attached as a front cover (section 3);

c) be signed by a person or persons duly authorised to sign on behalf of the Respondent;

d) be formatted as shown in the ROI Response Sheet (section 4); and

e) include the following items:

i) two (2) printed copies of the registration and any supporting documentation (one bound and one unbound). Documents must be formatted to A4 size;

ii) one (1) electronic version of the registration and any supporting documentation on CD. The registration should be in Microsoft Word 2000 format (zipped is acceptable). Supporting documentation should be in the format most appropriate, but Microsoft Office 2000 formats are preferred. Registrations in PDF format will not be accepted. All CD's must be labelled "ROI DIA/2006-014" and state the full name of the Respondent. File names must be clear and recognisable in relation to their content;

iii) five (5) copies of each physical sample book (see section 4.3.2); and

iv) two (2) printed and signed copies of the Non-Disclosure Agreement (see Appendix A). Should the Respondent be selected to proceed to the RFP, one copy will signed by DIA and returned to the Respondent.

Registration content, continued

Please note:

a) DIA accepts no responsibility for lost or misdirected registrations.

b) DIA reserves the right to accept or decline late registrations at its sole discretion.

c) Registrations, any supporting documentation, CDs and sample books received by DIA will become the property of DIA.

1.6 Indicative procurement timeline

The key dates associated with this procurement process are expected to be as follows:

ROI	**Key Date**
Distribution of ROI	18 August 2006
ROI registration closing date	15 September 2006
ROI evaluations complete	13 October 2006
ROI evaluation report approved	24 October 2006
ROI Respondent notification	27 October 2006
RFP	**Key Date**
Distribution of RFP	3 November 2006
RFP response close date	26 January 2007
RFP evaluations complete	16 February 2007
RFP evaluation report complete	9 March 2007
RFP evaluation report approved	23 March 2007
RFP Respondent notification	26 March 2007
Proof of Concept (POC)	**Key Date**
Proof of Concept trial	April – June 2007
Proof of Concept sign-off	30 June 2007
Contract	**Key Date**
Begin negotiations with preferred vendor(s)	May 2007
Contract with preferred vendor(s) signed	August 2007

Please note this timetable may be subject to change at the sole discretion of DIA.

1.6.1 Proof of Concept

Following the completion of the RFP evaluation, the selected Respondent(s) will be required to complete a Proof of Concept (POC) trial for their solution.

The POC is expected to involve the production and personalisation of at least 10,000 travel documents (in final construction format, including examples of the intended security features). The physical location of this testing will depend on the proposed solution.

Although DIA expects the selected Respondent(s) to meet all vendor costs associated with the POC, DIA may consider sharing a portion of those costs in agreement with the selected Respondent(s).

1.7 Registration critical success factors

Registrations will be assessed on the following critical factors:

1.7.1 General

- provision of acceptable reference sites;
- an established in-house design capability;
- an established and proactive in-house research and development capability;
- has proactive and auditable quality management processes covering all aspects of passport design, development and manufacture;
- active participation in ICAO/ISO forums for travel document standards and development;
- company financial stability; and
- no adverse impact, in any manner, on New Zealand's national security interests.

1.7.2 Provision of travel document books

- significant passport design, development and manufacturing experience;
- ability to support the expected increases in travel document volumes;
- demonstrated experience in e-Passport development and integration;
- demonstrated experience in the development of advanced document security features; and
- ability to consistently produce high quality travel document books.

1.7.3 Provision of personalisation technology

- demonstrated experience in laser engraving technology with regards to travel documents;
- ability to consistently produce high quality personalisation output, with minimal spoilage;
- ability of Respondent's solution to scale to support the expected increases in issuance volumes;
- ability of Respondent's solution to operate in a distributed environment; and
- provision of on-site and on-call support and maintenance.

1.7.4 Consortium

A prime vendor who:

- will be a single point of contact for DIA; and
- will drive issue resolution between all parties within the consortium.

2 Project information

2.1 Project purpose

The purpose of the Personalisation Project is to put into operation a supply contract for newly designed travel documents and new personalisation technology, such that the implemented solution addresses the volume, operational and security requirements of DIA and New Zealand's travel documents over the term of the contract.

2.2 Project critical success factors

The following criteria must be met for the Project to be considered successful:

a. travel document security is enhanced;
b. the travel documents produced are such that New Zealand's reciprocal visa waiver entry status with key countries is maintained; and
c. the current high level of international regard for the New Zealand travel documents has been maintained, if not enhanced.

2.3 DIA Requirements

DIA is seeking a combination of travel document and personalisation technology that:

- will provide New Zealand with unique travel documents which include innovative security features;
- uses laser engraving personalisation technology;
- consistently produces high quality travel document construction, regardless of travel document type;
- consistently produces high quality personalised bio-data pages, incorporating the same security features, regardless of the personalisation site or travel document type;
- is scalable to meet forecast increases in issuance volumes (see section 2.4);
- will ideally make use of the same operator interfaces and software systems, regardless of the personalisation site;
- will ideally provide DIA with relationship management based within the Asia-Pacific region;
- will provide DIA with onsite support to DIA's Auckland and Wellington, New Zealand, personalisation sites during standard business hours; and
- will provide DIA with on-call support to DIA's Christchurch, Sydney and London personalisation sites.

2.4 Anticipated issuance volumes

The Department of Internal Affairs is facing a significant increase in passport demand volumes by October 2009 as a result of the recent legislated change from a ten year to a five year passport validity period.

Potential volumes, supplied as a guideline only, are as follows:

	06 - 07	07 - 08	08 - 09	09 - 10	10 - 11	11 - 12	12 - 13
Total Issuance volumes	424,000	441,000	468,000	525,000	653,000	706,000	736,000
Estimated New Zealand Issuance volumes	375,000	389,000	411,000	460,000	573,000	620,000	644,000
Estimated Sydney Issuance volumes	38,000	40,000	44,000	49,000	60,000	65,000	70,000
Estimated London Issuance volumes	11,000	12,000	13,000	16,000	20,000	21,000	22,000

It should be noted that seasonal fluctuations occur, i.e. the demand for travel documents fluctuates throughout the year.

2.5 Personalisation business model

Personalisation occurs, and ideally will continue to occur, from five (5) DIA sites:

- Wellington, New Zealand
- Auckland, New Zealand
- Christchurch, New Zealand
- Sydney, Australia; and
- London, United Kingdom.

Ideally the Wellington office will be the primary personalisation site, handling 75% of New Zealand issuance volumes on a normal daily basis (one 8 hour shift). The Auckland office is the secondary personalisation site, handling 25% of New Zealand issuance volumes on a normal daily basis. Christchurch handles very small volumes only as part of the provision of urgent and call-out services for the South Island.

Business continuance capability is required for both Wellington and Auckland such that either site has the capacity to complete 100% of the New Zealand issuance volumes in the event of fire, earthquake, volcanic eruption or other event affecting the operation of the office in either city. In a business continuance situation, DIA would expect to increase production to two 8 hour shifts if necessary to ensure the continuation of a near-normal issuance service.

2.6 Payment models

DIA expects payment to be made to the prime vendor on a per-book price basis. The per-book price is paid for each successfully personalised book, except where spoilage is due to DIA operator error, and includes the cost of the travel document, the personalisation technology, maintenance, support and software licences.

DIA may consider purchasing the personalisation machinery through the prime vendor, with an arrangement for the ongoing costs for maintenance, support and software licences.

2.7 Indicative project timetable

The key dates associated with the development and implementation of the Personalisation Project are as follows:

Initial Planning	**Key Dates**
Development and implementation plan, including site specific implementation plans	September 2007
Book Development	**Key Dates**
Book development	September 2007 – March 2008
Specimen book production and delivery	March – April 2008
First delivery of production books	July 2008
Technology and systems integration	**Key Dates**
Technology and system integration	September 2007 – March 2008
Site installation and transition	**Key Dates**
Site installations	March – September 2008
Site transition	August 2008 – September 2008

Please note this timetable may be subject to change at the sole discretion of DIA.

2.8 Additional project information

Appendix B provides additional project information, including DIA background information, DIA security strategies, the change drivers that led to the Project's initiation and the Project's scope.

3 ROI Registration Cover Sheet

Registration of Interest

Supply of New Zealand Travel Document Books and Personalisation Facilities

Department of Interest Affairs, September 05

Organisation name:	
Address for Correspondence:	
PO Box:	
Attn:	
Phone:	
Fax:	
Email:	
Signed by: **(Duly authorised person)**	
Registration Compliance and Completeness: Respondents must provide a statement confirming that the registration document complies with the requirements detailed in this ROI	
Respondents must confirm they have read, understood and accepted, the following sections: ▪ Section 1 (ROI Information) ▪ Section 2 (Project Information) ▪ Section 5 (Terms and Conditions)	

4 ROI Registration Requirements

4.1 Respondent company

The following company information must be provided for the prime Respondent's company.

4.1.1 Contact details

	Company contact details	Response
1.1.1	Company name	
1.1.2	Company address	
1.1.3	Company key contact person	
1.1.3.1	name	
1.1.3.2	office telephone number	
1.1.3.3	cell phone number	
1.1.3.4	fax number	
1.1.3.5	email address	
1.1.4	Company website address	
1.1.5	List those products and/or services for which this company will have production/delivery responsibility	
1.1.6	Outline how DIA can expect our account with your company to be managed, including the location of the intended ongoing account manager.	
1.1.7	**Non-Disclosure Agreement** Respondents must attach a signed copy of the Non-Disclosure Agreement to their ROI registration	

4.1.2 Company profile

	Company profile	Response
1.2.1	State the number of years the company has been in operation	
1.2.2	State the number of years the company has been offering travel document and personalisation technology	
1.2.3	List those countries within which the company has offices, branches or subsidiaries	
1.2.4	State the company's turnover for the last 5 years (please state the currency used)	2005 finance year (if available): 2004 finance year: 2003 finance year: 2002 finance year: 2001 finance year:
1.2.5	State the company's earnings before interest and tax as a ratio of debt for the last 5 years (debt/EBIT)	2005 finance year (if available): 2004 finance year: 2003 finance year: 2002 finance year: 2001 finance year:
1.2.6	State the company's debt to equity ratio for the last five years	2005 finance year (if available): 2004 finance year: 2003 finance year: 2002 finance year: 2001 finance year:

	Company profile	Response
1.2.7	List those ICAO/ISO forums for travel document standards and development within which the company participates. List company staff involved and their role in each forum	

4.2 Third party company(s)

Where elements of the proposed solution are to be sourced from one or more third parties, the following company information must be provided for each party. Where there are multiple third parties involved, add additional sections as required.

4.2.1 Contact details

	Company contact details	Response
2.1.1	Company name	
2.1.2	Company address	
2.1.3	Company key contact person	
2.1.3.1	name	
2.1.3.2	office telephone number	
2.1.3.3	cell phone number	
2.1.3.4	fax number	
2.1.3.5	email address	
2.1.4	Company website address	
2.1.5	List those products and/or services for which this third party will have production/delivery responsibility	

4.2.2 Company profile

	Company profile	Response
2.2.1	State the number of years the company has been in operation	
2.2.2	State the number of years the company has been offering travel document personalisation technology	
2.2.3	List those countries within which the company has offices, branches or subsidiaries	
2.2.4	State the company's turnover for the last 5 years (please state the currency used)	2005 finance year (if available): 2004 finance year: 2003 finance year: 2002 finance year: 2001 finance year:
2.2.5	State the company's earnings before interest and tax as a ratio of debt for the last 5 years (debt/EBIT)	2005 finance year (if available): 2004 finance year: 2003 finance year: 2002 finance year: 2001 finance year:
2.2.6	State the company's debt to equity ratio for the last five years	2005 finance year (if available): 2004 finance year: 2003 finance year: 2002 finance year: 2001 finance year:
2.2.7	List those ICAO/ISO forums for travel document standards and development within which the company participates. List company staff involved and their role in each forum	

4.3 Travel documents

The following information must be provided in relation to the company responsible for providing the proposed travel documents.

4.3.1 General requirements

	Company contact details	Response
3.1.1	Outline how the proposal will provide New Zealand with a unique travel document including innovative security features. Summarise how this solution meets DIA's solution requirements and critical success factors	
3.1.2	Outline how the proposal will consistently produce high quality travel documents	
3.1.3	Outline how travel document manufacturing facilities will be scaled to meet forecasted increases in issuance volumes over the term of the contract	

4.3.2 Current capability

	Respondent Information	Response
3.2.1	List those countries which issue travel documents produced and/or personalised by the company	
3.2.2	Summarise the company's current in-house design capability	
3.2.3	Summarise the company's in-house research and development capability	
3.2.4	Please include with your response five (5) physical sample books that demonstrate the advanced document security features your company has included in travel documents. List the security features included, noting their location within the sample books	

4.3.3 Past experience

	Respondent Information	Response
3.3.1	Summarise the company's experience in the design, development and manufacture of travel document books	
3.3.2	Summarise e-Passport development work completed within the last 12 months	

4.3.4 Commitment to quality

	Respondent Information	Response
3.4.1	Summarise the quality management processes applicable to the company's passport design, development and manufacturing methods	
3.4.2	List any international accreditations in relation to quality management processes given above	

4.4 Personalisation technology

The following information must be provided in relation to the company responsible for providing the proposed personalisation technology.

4.4.1 General requirements

	Respondent Information	Response
4.1.1	Outline your personalisation technology proposal. Summarise how this proposal meets DIA's solution requirements and critical success factors	
4.1.2	Summarise the management system(s) used to operate your personalisation technology, including infrastructure requirements, data flows and services offered	
4.1.3	Summarise the personalisation technology's maintenance schedule and requirements	
4.1.4	Outline how onsite support will be provided in Wellington and Auckland, during business hours	
4.1.5	Outline how on call support will be provided in Wellington and Auckland, outside of business hours	
4.1.6	Outline how on call support will be provided in Christchurch, London and Sydney, both during and outside of business hours	

4.4.2 Current capability

	Respondent Information	Response
4.2.1	List those countries in which the company's personalisation technology is currently operating (noting model and number of machines in operation)	
4.2.2	Summarise the company's in-house research and development capability	

4.4.3 Past experience

	Respondent Information	Response
4.3.1	Summarise the company's experience in the development of passport personalisation technology	
4.3.2	Summarise e-Passport personalisation development work completed within the last 12 months	

4.4.4 Commitment to quality

	Respondent Information	Response
4.4.1	List any international accreditations in relation to quality management processes	

4.5 References

Reference information will be treated with the utmost confidentiality. Proven performance is a significant evaluation criterion.

Any contact with the reference sites will be arranged by the Respondent and be made by DIA during the ROI evaluation.

Reference site A		
5.A.1	Country name	
5.A.2	Government department responsible for services provided	
5.A.3	Contact details for key contact person within Government Department	
5.A.4	Summarise the products and services provided	
5.A.5	Summarise the degree to which the Respondent is responsible for the production of these products and services	
5.A.6	Summarise the degree to which the third parties are responsible for the production of these products and services	

Reference site B		
5.B.1	Country name	
5.B.2	Government department responsible for services provided;	
5.B.3	Contact details for key contact person within Government Department	
5.B.4	Summarise the products and services provided	
5.B.5	Summarise the degree to which the Respondent is responsible for the production of these products and services	
5.B.6	Summarise the degree to which the third parties are responsible for the production of these products and services	

Reference site C		
5.C.1	Country name	
5.C.2	Government department responsible for services provided;	
5.C.3	Contact details for key contact person within Government Department	
5.C.4	Summarise the products and services provided	
5.C.5	Summarise the degree to which the Respondent is responsible for the production of these products and services	
5.C.6	Summarise the degree to which the third parties are responsible for the production of these products and services	

4.6 Additional information

Subject to Section 5.8 (Addenda to Registration), Respondents must provide any information that supports the registration or is reference material for the registration.

	Response

5 Terms and Conditions

This section sets out the terms and conditions of the receipt and submission of a registration in response to this ROI (ROI Conditions).

5.1 Validity of information

DIA has used reasonable efforts in compiling the ROI. However DIA will not be liable to Respondents or any third party for any inaccuracy or omission in the ROI or any additional information DIA may provide as part of the registration process. This section 5.1 is without prejudice to section 5.16 below.

5.2 Acceptance of conditions

Supply of a registration of interest by the Respondent to DIA will amount to acknowledgement and acceptance of these ROI Conditions by the Respondent. Where the Respondent intends to engage third parties to perform any part of the proposed solution, these third parties shall also be bound by these ROI Conditions (to the extent relevant).

Except as set out in this Section 5, there is no agreement between DIA and any Respondent as to the conduct of the ROI process.

5.3 Evaluation of registrations

Notwithstanding any stated registration evaluation method, DIA has complete discretion to consider, not consider, accept or reject any registration (including, without limit, any late or otherwise non-conforming registrations) and complete discretion as to registration evaluation methods. DIA will not enter into discussions with Respondents concerning its evaluation methods.

5.4 Validity period

Once submitted, each registration is irrevocable, and may not be withdrawn or changed, except with the written consent of DIA.

5.5 Authorised communications

Only those communications that are in writing from DIA from personnel who have been authorised for the purpose may be considered as a duly authorised expression on behalf of DIA.

5.6 Correspondence/clarification sought by Respondent

All correspondence is to be directed to the email addresses set out in Sections 1.4 and be received by DIA not later than two [2] Working Days before the closing date for registration. DIA will respond to any requests for clarification made via letter, facsimile or email and may respond to any other questions it receives.

If any enquiry and its response is deemed by DIA, at its discretion, to clarify or materially change the purpose and/or intent of this ROI, the question and answer will be communicated simultaneously to all Respondents and will, upon issue, be deemed to become part of the ROI.

If a Respondent is unable to obtain clarification on any matter relating to the requirements of this ROI, the Respondent should indicate where it believes the ROI to be ambiguous or unclear and should describe the interpretation it has adopted in preparing its registration.

5.7 Respondents to inform themselves

Each Respondent is deemed to have examined this ROI and any other information supplied by DIA to the Respondent and to have satisfied itself before submitting any of its registration as to the correctness and sufficiency of the registration.

DIA does not warrant the accuracy or correctness of this ROI or any other information supplied by DIA to any Respondent.

Each Respondent will undertake such further investigations as it may consider necessary before submitting any registration.

5.8 Addenda to registrations

Information not specifically required for the ROI but deemed by the Respondent to be of value to the evaluation should be included as an addendum to the registration. Addenda must not include advertising brochures or similar material. Where there is reference to published manuals, the relevant extracts from the manuals and those alone, must be placed in the addenda. References to websites and other online materials must be printed and included in the addenda.

5.9 Changes to ROI

Where, during the course of the ROI process, DIA modifies the essential requirements and evaluation criteria of the ROI, it shall publish such modifications on GETS[1] or transmit them in writing to all Respondents at the time the criteria are modified, in the same manner the original information was transmitted, and in adequate time to allow such Respondents to modify their registrations. If a registration has been submitted prior to the change, the Respondent will be permitted to produce an erratum to take account of the change, and submit this by the closing date for registrations.

[1] www.gets.govt.nz

5.10 Confidentiality

A Respondent may not copy the ROI in part or in whole except for the purpose of preparing its registration. This ROI and any other documents supplied by DIA remain DIA's property and must be returned to DIA upon request together with all copies.

DIA will use reasonable efforts to maintain the confidentiality of information supplied in the registration. However, DIA is subject to various disclosure requirements, for example the Official Information Act 1982, and shall not be liable for any disclosure it believes (acting responsibly) it is required to make. The Respondent should clearly indicate those parts of its registration that it regards as commercially sensitive and confidential. The entire registration may not be marked as such.

The above requirements are in addition to the requirements of the Non-Disclosure Agreement.

5.11 Registration preparation costs

The Respondent shall bear all its costs in preparing, submitting and presenting any registration and all other costs incurred by it throughout the evaluation process and any resulting RFP or contract negotiations, including without limitation, the cost of undertaking further investigations to finalise details of pricing, services or service levels.

Furthermore, no statement in this document shall be construed as placing DIA, its employees or agents under any contract or obligation whatsoever in respect to costs or losses incurred by the Respondents in the preparation of their registration.

5.12 Time

New Zealand time and dates apply at all times, except where explicitly stated to the contrary. For the avoidance of doubt, New Zealand time is GMT+12 hours during New Zealand standard time (NZST) and GMT+13 hours during daylight time. New Zealand daylight time (NZDT) will next commence at 2h00 NZST on Sunday 1 October 2006 and will cease at 2h00 NZST on 18 March 2007.

5.13 New Zealand law

New Zealand law governs this ROI process. The Respondent agrees to submit to the exclusive jurisdiction of the New Zealand courts in relation to any dispute or difference of any kind that may arise concerning this ROI process.

5.14 No Canvassing/Undisclosed Benefits

Respondents' communications with DIA must be in accordance with Section 1.4 (Clarification process). Respondents' representatives must not directly nor indirectly canvass, or provide any form of inducement or reward to, any representative of DIA in respect of this ROI. Any "unauthorized" contact or any attempt to canvass, induce or reward may invalidate the registration of the Respondent.

5.15 Notice of outcome

DIA will promptly notify each Respondent who submitted a complying registration of whether or not DIA intends to invite the Respondent to participate in the RFP process, following the Department making such decision.

DIA reserves the right not to notify or publish the name of any Respondent it chooses to invite to participate in the RFP process, or the terms of the Respondent's registration.

On request from an unsuccessful Respondent, DIA will promptly provide pertinent information concerning reasons for the rejection of its registration or the relative advantages of the registrations that were accepted.

5.16 DIA information

Except to the extent required by law, DIA may withhold any information from any Respondent for any reason and will not be responsible to any person for any information so withheld.

5.17 Information accuracy

DIA will rely on any information provided by or on behalf of a Respondent in respect of this ROI. The Respondent must ensure all information provided to DIA is complete and accurate.

5.18 Authorisation

Each Respondent authorises DIA to collect any information from the Respondent and relevant third parties (such as referees) and to use that information for the purposes of this ROI process. Where that information is incorrect or out of date, the Respondent may require DIA to update or correct that information.

5.19 Satisfactory solution

In order to procure a satisfactory solution, DIA reserves the right (and the Respondent must in no way impede DIA's ability) to:

a. Allow one or multiple Respondents to proceed to the RFP stage; or
b. Choose not to invite any Respondents to proceed to the RFP stage.

5.20 No liability of DIA

DIA shall not be liable in any way whatsoever and howsoever caused, including, without limitation, in contract, tort (including negligence), equity, or breach of statutory duty to any Respondent on the grounds that DIA has failed to consider a registration, has incorrectly evaluated registrations or has invited or has not invited any Respondent(s) to proceed to the RFP stage, or in respect of any other decision whatsoever concerning registrations submitted for consideration.

5.21 Rights reserved by DIA

DIA, in its sole discretion, may:

a. Change any date in this process (e.g. extend or shorten timeframes);
b. Apply, or change, any policy or criteria relating to participation in this process or evaluation of registrations;
c. Exclude any Respondent from this process for any reason;
d. Restrict or deny the supply of, or access to, any DIA site or other property or any of DIA's personnel, information or property to any Respondent or person;
e. Change its requirements;
f. Suspend or cancel this process by notice;
g. Change any condition, procedure or rule of this process by notice;
h. Consider (or not consider) any non-compliant registration;
i. Accept any registration at any time prior to the time for acceptance of registrations;
j. Contact any third party who has previously engaged the Respondent (or any person comprising or associated with the Respondent) to discuss the work performed for that third party;
k. Re-advertise for registrations;
l. Waive any irregularities or informalities in the process;
m. Provide further information in respect of, and modify the provisions of, this ROI at any time prior to the closing date for registrations by notice to all prospective Respondents;
n. Depart from any evaluation criteria or any other terms or conditions of any pre-contract documentation.

5.22 Public Statement

No Respondent, or any of its subcontractors (third parties), shall at any time make any public statement in relation to this ROI or the evaluation process without prior written consent from DIA.

In addition, no advertising or information relating to any part of this process shall be published in any newspaper, magazine, journal, broadcast of radio or television, on the internet or any other such medium without the prior written consent of DIA.

5.23 Indemnity

If a Respondent breaches these ROI Conditions and, as a result of that breach, DIA incurs costs or damages (including, without limit, the cost of any investigations, procedural impairment, repetition of all or part of the ROI process and enforcement of intellectual property rights or confidentiality obligations), then the Respondent indemnifies DIA against such costs or damages.

Appendix A: DIA Non-Disclosure Agreement

Dated: _____ / _____ / 2006

This agreement is entered into between **Her Majesty The Queen** in right of New Zealand acting through the General Manager, **Identity Services, Department of Internal Affairs** having its office at A.C. Nielsen House, 120 Victoria Street, P.O. Box 10-526 Wellington, New Zealand (hereafter the "DIA"), and **Respondent Limited**, **[insert details]** (hereafter "Respondent").

The parties are interested in discussing a possible business arrangement directed to the supply of products and services by the Respondent to DIA for the production and personalisation of New Zealand travel documents (hereinafter described as the "Discussion"). Each of the parties may need to disclose technical and business information to the other.

For each item of information, the party disclosing the item shall be called the "Disclosing Party", and the party receiving the item shall be called the "Receiving Party".

Certain portions of the technical and business information that may be disclosed may be of a confidential or proprietary character and include trade secrets of the Disclosing Party (hereinafter "Confidential Information"). It is necessary, therefore, to restrict the Receiving Party's use of the Confidential Information. In consideration of the disclosure of Confidential Information hereunder, the Parties to this Agreement agree that the use and disclosure of the Confidential Information shall be governed by the following terms and conditions:

1. This Agreement shall come into force on the date first written above. The limitations on the use of Confidential Information and the obligations of confidentiality imposed by this Agreement shall extend for a period of five (5) years from the date of disclosure, and shall survive any early cancellation or termination of this Agreement.

2. Confidential Information shall include any technical and business information disclosed by the Disclosing Party, except information which:

   (a) is presently in the Receiving Party's possession, provided that such information has not been obtained from the Disclosing Party;

   (b) is, or becomes, generally available to the public, through, for example, such sources as patents or other generally circulated publications, and such availability to the public does not result from any fault of the Receiving Party;

   (c) is received by the Receiving Party from a third party having no obligation to the Disclosing Party to keep it confidential;

   (d) is independently developed by the Receiving Party;

   (e) is released for disclosure by the Disclosing Party with its written consent; or

   (f) is inherently disclosed in, or capable of being determined, by the use, lease, sale, distribution, design, or operation of any product or service of the Disclosing Party or any documentation provided to facilitate the use or maintenance of the product or service.

Specific technical and business information shall not be within the exceptions of the preceding sentence merely because it is embraced by more general technical or business information within those exceptions, nor shall a combination of features be within those exceptions merely because the individual features are within those exceptions. The exclusion in item 2(f) does not extend to Confidential Information that is obtained by reverse engineering, deconstruction or scientific analysis of any product or service.

3. Disclosure of Confidential Information of either party hereto shall not be precluded if that disclosure is:

   (a) in response to a valid order of a court or other governmental body provided, however, that the party making the disclosure pursuant to the order shall first have given notice to the other party and made a reasonable effort to obtain a protective order requiring that information and/or documents so disclosed be used only for the purposes for which the order was issued;

(b) otherwise required by law; or

(c) necessary to establish rights under this Agreement.

4. The Disclosing Party represents and warrants that it has the unrestricted right to disclose any information that it submits, free of all claims of third parties and that such disclosure will not breach any obligations the Disclosing Party may have to any third party.

5. Where practical, Confidential Information shall be disclosed in documentary or tangible form and marked "Confidential".

6. The Receiving Party agrees that the sole purpose for the Disclosing Party disclosing its Confidential Information to the Receiving Party is to enable the Receiving Party to evaluate the Confidential Information for purposes of the Discussion. The Receiving Party will hold in strictest confidence all Confidential Information of the Disclosing Party and use that Confidential Information solely for this purpose. Any unauthorised use by the Receiving Party of that Confidential Information of the Disclosing Party for any other purpose shall be considered a breach of this Agreement.

7. The Receiving Party will disclose Confidential Information only to its employees who are bound in writing to keep it confidential and only to the extent necessary for the Discussion to be conducted. However, DIA may disclose Confidential Information to third party consultants and agents who need to know such information **provided that** such parties have entered into a non disclosure agreement with DIA upon terms that are substantially similar to the terms of this Agreement. DIA agrees that it shall not unreasonably withhold or delay its agreement to enter into such a non disclosure agreement with any such person.

8. The Receiving Party will treat any samples or other materials (hereinafter "Samples") received from the Disclosing Party as Confidential Information and further agrees that it will not, without the express written consent of the Disclosing Party, engage in or permit any analysis for composition, disassembly, decompilation or reverse engineering of the Samples and to maintain in strict confidence any information it learns from its inspection of any such Samples and the results of its evaluation of the Samples upon the terms of this Agreement.

9. The Receiving Party must implement and maintain adequate security procedures to prevent unauthorised disclosure, loss or destruction of Samples or documents or materials containing Confidential Information. The Receiving Party will promptly notify the Disclosing Party in writing of any loss or destruction of the originals of any writing or other tangible items, or any copies thereof, which contain the Confidential Information of the Disclosing Party. The Receiving Party will make all reasonable efforts to locate and return any such lost originals or copies.

10. Upon request, the Receiving Party will:

(a) destroy or return to the Disclosing Party any Samples, documents or other tangible materials disclosed by the Disclosing Party, or generated by the Receiving Party pertaining to the Confidential Information of the Disclosing Party or the Discussion;

(b) delete the Confidential Information from any and all retrieval systems and databases in which it has been placed or recorded; and

(c) cause an officer of the Receiving Party to certify in writing that the Receiving Party has complied with this paragraph.

11. Without the prior consent of the other party, neither party hereto shall disclose to any person (except those with a need to know as provided above) either the fact that Discussions are taking place, their status or any of the terms, conditions or other facts with respect to those Discussions **except that DIA** shall be entitled to disclose such information to Ministers of the Crown, government agencies, Parliamentary Committees, the Office of the Auditor-General and as required by law.

12. Neither this Agreement nor the disclosure of any information by the Disclosing Party shall constitute by implication or otherwise, a vesting of any title or interest or a grant of any license, immunity or other right to the Receiving Party with regard to the Confidential Information.

13. Nothing in this Agreement shall constitute a joint venture or partnership, or any other business, financial, or other relationship between the parties.

14. This Agreement shall be governed by and construed in accordance with the laws of New Zealand and the courts of New Zealand shall have non-exclusive jurisdiction to hear any dispute that may arise in relation to this Agreement.

15. This Agreement may only be amended, superseded or cancelled by a further written agreement signed by the parties. Any waiver of a term of this Agreement is only effective if given in writing and signed by the party waiving the particular term.

16. This Agreement sets forth the entire agreement and understanding between the parties as to the subject matter and supersedes all prior discussions, commitments, agreements, arrangements, and understandings of any nature between the parties relating to the subject matter.

17. No representation, promise, inducement or statement of intention with respect to the subject matter of this Agreement has been made by either party which is not embodied in this Agreement, and neither of the parties shall be bound by or be liable for any alleged representation, promise, inducement or statement of intention not so set forth.

18. The Receiving Party acknowledges and agrees that any breach of the covenants in this Agreement will cause the Disclosing Party immediate and irreparable harm and that damages and other remedies at law for any breach are inadequate. Accordingly, the Disclosing Party shall be entitled to seek injunctive relief for any breach of this Agreement by the Receiving Party. Nothing contained in this Agreement shall limit the Disclosing Party's right to any other remedies at law, including the recovery of damages for breach of this Agreement.

19. Neither party may assign its rights or obligations under this Agreement without the written consent of the other party. The terms and conditions of this Agreement shall be binding upon and endure to the benefit of any successor or permitted assign.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be signed by their duly authorized representatives on the date set forth below.

Her Majesty The Queen in right of New Zealand acting by and through the General Manager, Identity Services, Department of Internal Affairs	**Respondent Limited**
---	---
Name:	Name:
Title:	Title:
Date:	Date:

Appendix B: Additional project information

This section provides background information on DIA, DIA security strategies, the change drivers that led to the Project's initiation and the Project's scope.

B.1 Identity Services

Identity Services is a business unit of DIA, with approximately 400 staff spread across five locations in Wellington, Auckland, Christchurch, Sydney and London.

The Identity Services Group is New Zealand's primary source of information on personal identity and key life events. It registers birth, death, marriage and civil union details, manages these registers, issues passports and other travel documents and manages applications for New Zealand citizenship.

In the 2005/2006 financial year approximately 345,000 passports were issued. Identity Services began issuing e-passports at all sites in November 2005.

Additional information about DIA can be found on our website at www.dia.govt.nz

B.2 Security strategies

Identity Services is responsible for the achievement of the DIA outcome statement: "New Zealand and international communities trust the integrity of New Zealand's records of identity". This strategic context requires the maintenance of nationally and internationally trusted New Zealand travel documents. To achieve this, New Zealand travel documents must make the best use of modern technologies and sophisticated fraud prevention capabilities.

To maintain this level of integrity, four key security strategies for New Zealand travel documents have been developed, namely:

B.2.1 New Zealand travel documents shall adhere to International Civil Aviation Organisation (ICAO) standards and recommended practises as a minimum:

ICAO has developed internationally accepted standards and recommended practises for Machine Readable Travel Documents (MRTD): ICAO Doc 9303. New Zealand is a member of the ICAO MRTD programme and is active in working groups. New Zealand currently chairs the MRTD Technical Advisory Group (MRTD TAG).

B.2.2 New Zealand travel documents shall maintain their current visa-waver status:

Visa-waiver status is dependant on a number of factors, one of which is the travel document requirements. While the other factors, such as the stability of the government or changes to reciprocity between visa-waver countries are out of DIA's control, DIA can maintain the value of the travel document by ensuring that it continues to meet the travel document requirements to provide the same level of visa waver entry that New Zealanders currently enjoy.

B.2.3 New Zealand travel documents shall use sophisticated risk-mitigation technologies and techniques:

New Zealand travel documents shall be produced using sophisticated risk-mitigation technologies and techniques to maintain security within the constraints of practicality and economy of scale. DIA's current production of approximately 350,000 travel documents per annum is expected to grow to approximately 730,000 by 2012/2013.

B.2.4 Changes to New Zealand travel documents shall be subjected to various forms of testing:

Any changes to New Zealand travel documents shall be thoroughly tested to ensure the travel documents meet the following requirements:

- physical, as discussed above;
- technological – the e-Passport chip and the personalisation technology operates as specified; and
- security – the security features are in the correct position and operate as specified.

B.3 Personalisation Project initiation

There are three change drivers that led to the initiation of the Project, namely:

B.3.1 Anticipated passport demand volumes

The Department of Internal Affairs is expecting a significant increase in passport demand volumes by October 2009 as a result of the recent legislated change from a ten year to a five year passport validity period.

The expected volumes are outlined in section 2.4.

B.3.2 Renewal of book supply and print contract

The current contract, for travel document supply and printing capability, is due to expire during the third quarter of 2008. This provides an opportunity to enhance the security and effectiveness of the travel document personalisation system, through implementation of a new book design and change to the personalisation technology used.

B.3.3 Increased focus on security

Threats to international security over recent years have increased the focus on the security and integrity of identity-related records worldwide, particularly passports. The use of false or fraudulent travel documents by organised crime, including terrorists, has resulted in an increasing imperative to develop more sophisticated fraud prevention and detection capability within the passport processing system.

B.4 Project scope inclusions

The scope of the Project **includes** the following:

- design and development of a new suite of travel documents, including the incorporation of new artwork into the security printing. The suite of travel documents are:
  - Standard passport;
  - Diplomatic passport;
  - Official passport;
  - Certificate of Identity;
  - Refugee Travel Document; and
  - Emergency Travel Document (ETD)[2];
- design and development of endorsement labels;
- implementation of a new supply contract with the selected vendor, where the supply contract is to produce the physical travel documents, provide the personalisation machinery, maintenance, support and if applicable, consumables;
- installation of new personalisation technology at 5 issuing locations with the majority of throughput being processed at two sites. The technology will personalise and QA the bio-data page and e-Passport chip; and
- integration of the new personalisation technology with DIA's passport systems.

B.5 Project scope exclusions

The scope of the Project **does not include** the following:

- development of the artwork to be included within the travel documents, although this Project will determine the security parameters to which the artwork must adhere;
- validation, entitlement and proof of identity required to process a travel document application;
- verification, issuance and dispatch (mail out) of travel documents from DIA sites; and
- the personalisation, issuance and dispatch of ETDs from DIA and non-DIA sites.

[2] Not an e-Passport

Asia-Pacific
Economic Cooperation

A Guide to Biometric Technology in Machine Readable Travel Documents

Chapter 12 Project Management and Implementation

APEC Business Mobility Group
APEC Committee on Trade and Investment

August 2007

Prepared By
Business Mobility Group
Project overseer, Australia
Department of Immigration and Citizenship
PO Box 25, Belconnen
ACT 2616, Australia
www.businessmobility.org

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC#207-CT-03.3

12. Project Management and Implementation

The execution of a project as large and wide-ranging as the introduction of an ePassport will go more smoothly if it is planned and managed carefully, using all the tools of project management that are available.

While economies will have their own project management preferences, this chapter outlines the basic principles of project management in order to give economies some guidelines for how to manage an ePassport project and tips about what to look out for.

Project management is a formalised and structured method of managing change in a rigorous manner. It focuses on developing specifically defined outputs that are to be delivered by a certain time, to a defined quality, and with a given level of resources, so that planned outcomes/benefits are achieved. Effective project management is essential for the success of a project. The application of any general project management methodology requires an appropriate consideration of the corporate and business culture that forms a particular project's environment.

It should be realised, however, that adherence to a project management methodology does not of itself guarantee project success, since managing projects is about managing people to deliver specified outputs.

TIP: "Be aware that if it can go wrong, it probably will … It doesn't mean that the project plan is flawed or that there has been poor project management. This is simply the reality of any type of complex project. All that we as managers can do, I think, is to help identify—at an early stage—the aspects of a project that do not meet expectations. In addition, we should implement procedures to remediate those problems."

Frank E. Moss, "The development of the American e-passport", *Keesing Journal of Documents & Identity*, Issue 17, 2006, pp. 22–24.

Key elements of managing a large project include the following:

- Planning and Scoping;
- Governance;
- Organisation Change Management/Outcome/Benefit Realisation;
- Stakeholder Management;
- Risk Management;
- Issues Management;
- Resource Management (see also Chapters 6 and 8);
- Quality Management;
- Status Reporting;
- Evaluation;
- Closure.

Further detail on some of these key elements is set out below.

Planning and Scoping
At the outset of the project, it is crucial to establish a clear definition and statement of the areas of impact and the boundaries of the project. The **scope** of the project will include the outcomes, customers, outputs, work involved, and resources (both human and financial).

A **project plan** should be drawn up, to guide how the project will be implemented. It should, as far as possible, cover all aspects of the whole project, including such matters as risk management, issues management, quality management, stakeholder management, resource management, reporting, and evaluation. (This list is not intended to be definitive.) Any project

planning activities must take into consideration the amount of organisational change that will be required to deliver the project outputs and realise the project outcomes or benefits.

TIP: "Recognize that a project plan is useful, but that it is a tool, not an end in itself … Having a great project plan doesn't guarantee success, just as having a rudimentary plan does not ensure failure. A project plan helps to identify potential conflicts and logic gaps in terms of implementation, and breaks down a complex task into hundreds or even thousands of individual steps. But, as in other endeavors, success ultimately depends on identifying talented managers and technical experts, and harness those skills through effective strategic management."

Frank E. Moss, "The development of the American e-passport".

One of the first requirements for any project is to identify the **Project Manager**. This person is critical to the success of the project. The Project Manager runs the project on a day-to-day basis and works within the set parameters for scope, budget, schedule and quality. It is the Project Manager's responsibility to ensure that the project produces the required outputs to the level of quality specified, on time, and within budget. It is also the Project Manager's responsibility to have a detailed plan for the project drawn up, and to make sure the plan is followed.

ICAO: Issues to consider when deciding to make improvements to passport systems

- How rapidly do you need to begin issuing the new passport?
- Do you wish to do it all at once, or on a phased basis (in terms of both changing over facilities and adopting the new passport format)?
- Do a formal project plan early in the process and share it widely among the organisation's management team. Identify critical milestones and don't proceed beyond them until they have been satisfactorily achieved.
- Remember: It will almost always take more time to implement a new system than expected. Be certain that you have contingency plans for unexpected situations and delays.

http://icao.int/mrtd/guidance/IssExplanation.cfm
http://icao.int/mrtd/guidance/IssPlanning.cfm

Governance

It is important at an early stage to establish the management structure that will provide governance for the project, identifying the specific players, their roles and responsibilities, and the interaction between them for the life of the project.

Stakeholder Management

Stakeholders are the people or organisations that have an interest in the project processes, outputs or outcomes/benefits, and it will be necessary to plan for how their involvement will be managed on an ongoing basis.

Case study: Australia—managing stakeholders

- The ePassport program was administered by the Department of Foreign Affairs and Trade as a **whole-of-government** border security initiative. Close coordination with other government agencies was essential, in particular with the Department of Immigration and Citizenship and with the Australian Customs Service.
- Extensive consultation and liaison internationally with other countries and the International Civil Aviation Organization (ICAO) in regard to international standards, to ensure **interoperability** were also crucial to success of the program.

Risk Management
Processes to manage the risks associated with the project—identification and analysis of possible risks, evaluation of them, and development of strategies for handling them—will be an essential part of the Project Plan. Throughout the life of the project, issues or concerns will arise, and will need to be monitored and addressed so that they do not undermine the project.

TIPS
- Be prepared for surprises.
- Know that schedules will slip and the final product will almost always cost more than was originally planned.

Frank E. Moss, "The development of the American e-passport".

Quality Management
The Project Manager will also need to plan for quality management procedures to ensure that the outputs of the project are delivered fit-for-purpose. If outputs are not fit-for-purpose, it is likely the planned outcomes and benefits will not be realised, or will be realised to a reduced extent. It will be necessary to develop criteria for the quality of outputs, and to ensure that all project management processes are conducted in a quality manner.

TIPS
- Enlist the services of technical experts who understand the challenges associated with the e-passport program and who can translate their technical knowledge into layman's terms.
- Be flexible … A good attitude, a quality management team and the flexibility to make decisions and change direction will make a significant contribution to the success of the overall result.

Frank E. Moss, "The development of the American e-passport".

Status Reporting
Formalised reporting to the business owner(s) or project sponsor (or appropriate authority) on the status of the project with regard to performance, milestones, budget, issues and risks, is an important requirement for large and/or complex projects, and may be an integral part of the quality management of the project.

Evaluation
Evaluation of the progress of the project against well-defined criteria is another essential, to help determine whether the project is under control, whether plans are being adhered to, what methodologies and standards are being used, and whether outcomes and benefits are being achieved.

Case studies: Issues considered by APEC economies that have introduced ePassports

New Zealand: Planning and procurement considerations

Drivers for the ePassport project were:
- To develop and integrate contactless IC chip technology into the current passport with as little change as possible;
- No major changes to book design or printing processes;
- To keep integrity of the ePassport as the paramount consideration.

Planning for the ePassport project had the following features:
- Expectations between supplier and New Zealand Passports were clearly documented;
- Complex contracts to maintain vendors' responsibility throughout personalisation were drawn up;
- These contracts reduced the potential for the vendor to transfer blame for any failings.

(*cont. next page*)

Australia: Planning of the ePassport project

- The biometric passport development program was commissioned by the Australian passport issuing authority, the Department of Foreign Affairs and Trade, in consultation with the Department of Customs, in 2001.
- Extensive research and testing on the biometric passport was commenced and taken to the proof-of-concept stage.
- Evaluation of available products was undertaken in partnership with the private sector (at that time there were only a few providers with expertise in facial recognition (FR) technology).
- Each progressive stage of the program was submitted to government for approval and funding, with progress reports providing the case for further investment.
- Initial issue of biometric passports for a test program to prove interoperability between Australian and the United States border control systems commenced in late 2004. Qantas cabin crew were the first Australians to use the ePassport. The tests were successful.

Hong Kong, China: Risk management and quality management

- The fundamental first step for system integrity is to conduct a comprehensive risk analysis and THEN construct a risk management profile. This is particularly critical for assessment of the biometric data collected and its uses.
- Ensure that all aspects of the biometric system(s) are thoroughly understood by all involved, especially the staff on the line and those affected by its administration.
- Make extensive use of the tools of technology, eg, rules-based adjudication software.
- Standards define requirements that must be addressed as minimum specifications both for technical soundness as well as adherence to quality control.
- Institute fraud prevention programs: detection, deterrence, follow-up, information sharing.
- Monitor and audit border crossings as well as document issuance and entitlement authorisations.
- Database linkages and data sharing are multiplicative in impact and become especially powerful tools when conjoined with biometric data.

Australia: Planning and scoping—security issues

Key security features of the system used in the ePassport needed to be factored into the costing. These included:

- **Secure Access Module** (SAM) to prevent unauthorised writing to passport chip;
- **Write once-only** to chip;
- **Public Key Infrastructure (PKI)** digital signature guarantees information integrity;
- **Basic Access Control** (**BAC**) coding in the machine readable zone (MRZ) to prevent unauthorised remote access to chip data (ie, 'skimming');
- **Central chip-signing system**: ePassports are issued in three locations, but all chip signing is done centrally from headquarters in Canberra;
- **Enhanced quality assurance (QA) stages** introduced in passport book manufacture and personalisation processes (additional costs involved);
- Australia is currently the only country with **Facial Recognition (FR) matching integrated** into its passport issue system at applicant registration stage. This checks whether the applicant has previously registered in another identity.

Planning and scoping: Testing
(based in information provided by a number of economies)

The project plan for developing an ePassport needs to include adequate provision for testing of concepts, software, hardware, and other equipment at various stages.

- Durability and Integrated Circuit (Chip) Card (ICC) functioning evaluated as part of tender process evaluation
- Vendor testing (Facial Recognition Vendor Testing, etc)
- Laboratory testing
- Load tests

(cont. next page)

Planning and scoping: Testing

- Functional test/performance demonstration
- Testing of application software
- Testing of production processes (machinery/hardware, procedures for enrolment, domestic system testing)
- Systems integration test
- Reliability testing
- Anti-skimming tests
- Useability—trials with ePassports were conducted
- Interoperability testing: live tests with other economies; ICAO testing, etc
- Privacy Impact Assessment

Links to more information about project management

Project Management Body of Knowledge (PMBOK)
The Project Management Body of Knowledge (PMBOK) is a collection of processes and knowledge areas generally accepted as best practice within the project management discipline. As an internationally recognised standard (IEEE Std 1490-2003) it provides the fundamentals of project management, irrespective of the type of project.

***A Guide to The Project Management Body of Knowledge*—Third Edition** provides a basic reference for anyone interested in the profession of project management. It is published by The Project Management Institute, Inc.
http://www.pmi.org/info/pp_pmbok2000welcome.asp

Further information can be found at:
http://www.projectsmart.co.uk/pmbok.htm

Tasmanian Government (Australia) website on Project Management:
1. http://www.egovernment.tas.gov.au/themes/project_management
2.http://www.egovernment.tas.gov.au/themes/project_management/project_management/resources/public/tasmanian_government_project_management_guidelines

---

References

1. ICAO, Technical Advisory Group On Machine Readable Travel Documents (TAG-MRTD), "Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation", Release 1, Draft 1.4, 7 March 2007, pp. 4-5.
http://mrtd.icao.int/images/stories/Doc/publications/TAG17WP/WP.16.History-Interop.and-Impl.complete.pdf
2. Frank E. Moss, "The development of the American e-passport", *Keesing Journal of Documents & Identity*, Issue 17, 2006, pp. 22–24.

Appendices

Appendix 1: Project Controls—Example
Appendix 2: Sample ePassport Project Plan

Appendix 1

Project Controls—Example

(This information has been provided by the Australian Department of Immigration and Citizenship (DIAC). However, the information is provided as an example only, and does not constitute legal advice or any recommendation on the part of DIAC. DIAC strongly encourages individuals to seek independent legal advice particular to their circumstances.)

In any project the purpose of control is to ensure that the project:

- is producing the required deliverables (outputs) in accordance with the acceptance criteria that have been defined by the users of those deliverables;
- is being carried out to schedule and in accordance with its approved resource and cost plans; and
- remains viable against the Project Proposal.

Controls are designed to help those who are accountable for the project to:

- monitor project progress and review this against the project plan;
- detect problems and initiate corrective action;
- approve revisions to the project plan; and
- approve further work on the project.

Not all controls described in this framework will be applicable to all projects. The controls available in this methodology are:

- Project Initiation Brief (PIB);
- Project Proposal (PP);
- Plans;
- Stage Gates;
- Software Development Life Cycle (SDLC);
- Quality Management;
- Quality Assurance
- Change Management;
- Issues Management;
- Risk Management;
- Project Status Report;
- Project Closure Report.

The Project Initiation Brief (PIB)

The PIB is used to provide an initial demonstration that an idea for a project is viable, practical, affordable and sensible in terms of cost versus benefit. Approval of PIB allows work to be undertaken to produce the Project Proposal (PP). The project receives a budget to prepare the PP that is then to be reported on, once approved.

The Project Proposal (PP)

The PP is one of the most important project controls. The project cannot start without the existence of an approved PP, which, among other things, describes the project objectives, scope, constraints, benefits and costs. Throughout the project the validity of the PP is continually monitored and, if the PP loses its validity, the project should be stopped by the Project Governance Authorities. Monitoring of the PP is an ongoing process but it becomes a formal process at each Stage Gate when it is formally reviewed by the Project Governance Authorities.

Plans

Plans are the backbone of project management and are essential for project success. Although there is an overhead associated with the creation of plans that seemingly tends to delay the production of the project deliverables, the adage “failure to plan is planning to fail” is

very true of project management. One of the most common causes for projects failing to deliver the intended outcomes is failure to plan.

All plans address the issues of what has to be achieved, how it will be achieved, when it will be achieved and by whom. Apart from the Project Management Plan many other types of plans may be required (eg, Communications Plan, Risk Management Plan, Change Management Plan). Once approved, plans provide the mechanism for controlling the project.

Stage Gates
Stage Gates are used to control a project by ensuring that passage through each gate does not occur until the status of the project has been formally assessed. During this assessment, the Project Governance Authorities review the PP, confirm whether it is viable to continue with the project and, if so, approve continuation of the project. Work is authorised by the Project Governance Authorities only up to the next Stage Gate.

Software Development Life Cycle
The [proprietary] method has been adopted by [the Programme] as the preferred methodology for Software Development. In addition to the method, [the Programme] has also acquired a range of software tools to support this methodology. Within this programme, the SDLC Project is responsible for customising and implementing [the proprietary method] as well as coordinating the provision of training for both method and tools. The primary target for the SDLC project is the roll out of the method and tools to [the Programme 1] and [the Programme 2]'s project teams delivering between [date] and [date]. To ensure the effective on-going use of the method and tools, the SDLC team is required to build and hand-over to a skilled SDLC Support Team that will provide [business-as-usual] services through to completion of [the Programme].

Quality Assurance
For each project, specific points in the project will be identified during the initiation phase (and during subsequent planning activities) when checks will be made to verify that the quality control activities and project procedures have been effectively implemented. These review points are to be documented in the project quality plan, and a formal report to management will be provided as a result of each checkpoint. As a general principle for larger projects, these checkpoints will be conducted at the end of the project initiation phase, and then every 3 months. Each checkpoint will determine when the next checkpoint is appropriate.

Quality Management
Every project needs procedures and techniques to manage the quality of the deliverables being produced. These procedures and techniques are both project and deliverable specific but one technique that is particularly applicable to documents is a Quality Review. Quality Reviews may be conducted on critical project documents, such as Test Plans, Implementation Plans and System Design Documents. The technique involves the examination of the document for errors in a planned, controlled and independent manner by a group of people expert in the type of document. The results of the examination are recorded, the errors corrected and the corrections themselves quality checked.

Configuration Management
Within the context of project management, the purpose of configuration management is to identify, track and protect the project deliverables and project control documents. All items subject to configuration management are referred to as Configuration Items (CIs). As a rule-of-thumb, if more than one version of an item will be created, then configuration management needs to be performed.

Change Management
Every project will receive requests for change and every project must have a procedure for managing those requests. This procedure is called change management and without change management there is no project control. The procedure includes an impact assessment of the request, prioritisation, decision-making and action. Guidance on managing change is provided with the Project Change Request template in the Project Reference Suite.

Issues Management
A Project Issue is any potential or actual situation that might impact the project in terms of schedule, budget or quality. These issues take the form of project-related questions, concerns, problems and suggestions. Project issues are to be recorded and reviewed at least weekly. Guidance on managing and escalating issues is provided with the Project Issues template in the Project Reference Suite.

Risk Management
A project risk can be defined as an event that may impact on the ability of the project to produce its deliverables within budget, within schedule or to the appropriate quality. Risks are present in all projects and it is important to manage the project risks throughout the project. Risks to the project are recorded and are to be reviewed weekly, and revised and updated whenever a plan is produced or project progress is assessed. Guidance on the management of risks is provided in the Project Risk Management Plan template in the Project Reference suite.

Project Status Report
A Project Status Report is an example of a time-driven project control. It is generated by the Project Manager in Clarity at weekly intervals during the project and is circulated out-of-session to the Project Governance Authorities and Project Sponsor. The Project Status Report highlights:

- Current/Future work status
- Significant risks and issues
- Project dependencies
- Project costs
- Principle documents' status
- Project milestone dates.

Project Closure Report
The Project Closure Report covers the entire project, comparing actual achievements against the Project Management Plan. It summarises the changes that occurred throughout the project and it looks at the major issues and the risk history of the project. The Project Manager prepares the Project Closure Report at the end of the Delivery Phase. The project is not to be closed until the report is approved by the relevant Systems Board.

Appendix 2

Sample ePassport Project Plan

(provided by Australian Passport Office (APO), Department of Foreign Affairs and Trade, Canberra, Australia)

Management Program
Terms of Reference

Project Plan
Draft Project Plan distributed for comment
Project Plan final version
Project Communications Strategy
Identify resources
Develop Training Plan
Risk Management Plan
First ePassport manufactured
Cutover strategy approved and sent to passport offices
Go / No-Go decision made
First ePassport personalised / issued

Business Rules
Broad policy framework approved
Draft new policies and procedures
Chip failure policy as part of Business Rules
New policies signed off by Directors
New policies signed off by Steering Committee (SC)
New policies signed off by Minister
New Issuing Procedures developed
Issuing Procedures signed off

Legislation
Drafting Instructions issued
Determinations/policies approved by Minister
Determination tabled in Parliament

Fees and Charges
Fee structure developed for 1 July 2005
Fee structure endorsement
Fee structure developed for October 2005
Fee structure endorsement
New Fee Schedule developed
Schedule 4 Fees approved by Minister
Fees Schedule Amendment registered
Amend electronic funds transfer systems
Fees promulgated to all systems
ICAO Public Key Directory—Contribution towards infrastructure costs

Training

Planning for Training
Preliminary Project Plan meeting
Fine-tune Project Plan—(Workshop) includes an outside project manager consultant
Delivery of Training Plan
Finalise resource allocation

Develop Training Materials
Develop training activities
Develop “Easy Guide to Issuing ePassports”
Clear photo instructions—“Photo Guide: Instructions to Agent, States and Photo Outlets”

Regional Meetings for Posts
Program for show and tell
Actual training in test environment

Manuals
Manuals Updating
Amendments to Manual of Australian Passport Issue (MAPI) as required
Amendments to Passport Agency Manual (PAM) as required
Completion and sign-off—MAPI
Completion and sign-off—PAM
Quote for printing—PAM, MAPI
Printing MAPI, PAM (if required)
Distribution of new PAM, MAPI
Passport agencies to receive MAPI amendments
Passport agencies to receive PAM amendments

Website
Timeline prepared
Layout
Revise and update static content
New fees published on line

Public Awareness/Information Program
Develop Information Strategy and contractual arrangements
Engage contractor
Finalise information strategy

Ministerial Launch of ePassport
Prepare media release
Launch

Advertising Program
Production of video
Video script approval
Pre-production
Video shoot
Video edit
Post design
Video audio
Project complete
Production of ePassport pamphlet
Production of amended passport flyer slips reflecting ePassports
Distribution of video to passport offices
Liaise with agent/others on flyer inserts/posters/brochures
Examine need to amend flyers, brochures that contain fees
Graphic design of any revised flyers/brochures
Printing of revised flyers/brochures
Distribute brochures

Quality Assurance (QA) Process
Draft QA specifications input

Specs and Testing of ePassport Hardware
Write draft specifications QA readers inclusive of BAC ICAO functionality
Sign-off specifications QA readers inclusive of BAC ICAO functionality
Provide Request for Information (RFI) details to suppliers for QA readers
Receive quotes and equipment specifications from QA reader suppliers
Identify QA, Optical Character Recognition (OCR) readers as a result of RFI
Reader suppliers to provide sample readers for testing
Test reader

Sign-off on selected readers
OCR keyboard—Order test unit
OCR keyboard—Receipt of test unit
OCR keyboard tested
Write draft specifications for QA workstations
Sign-off specifications for QA workstations

ePassport Hardware
Order ePassport hardware
Order QA readers
Deliver QA readers
Part delivery of 32 readers
Order 40 OCR keyboard readers
Deliver OCR keyboard readers
Order PKI server
Delivery PKI server
Order workstations for encoding staff
Deliver workstations for encoding staff
Despatch equipment to passport offices

Public Key Infrastructure (PKI)
PKI server
PKI server planning and specifications
Design of PKI servers
Decision by Steering Committee (SC) on design of PKI servers
Location of PKI servers put to the SC
Decision by Steering Committee on location of PKI servers
Order Certificate Authority (CA)
Build production CA servers
Generation of Country Signing Keys
Generation of 3 months of Document Signer keys
Installation of PKI rack
Order PKI signing server software
Development of signing server
PKI application signing software installation
Order 5 Hardware Security Modules (HSM)
Hardware installation—5 HSM Servers
PKI logistics administration procedures
Monthly Document Signer Certificate (Public Key)
Options to Steering Committee on Signer Key sender options
Decision Signer Key Sender to ICAO
Country Signing Certificate Authority (CA) (Private Key)
Options to Steering Committee on Signer Key validity/despatch options
Decision on validity (3, 5, or 12 year)
Decision on despatch methodology of ICAO CA's to ICAO PKD countries
Strategy for delivery of CA keys
Delivery of Document Signing Certificates (DSCs)
PKI Changes
ICAO to create Australia’s Object Identifier (OID)

Bandwidth
Bandwidth increase to state offices support FR matching
Backup communications links to all ePassport encoding offices

Staff—Employment and Training—Encoding chips
Staff Strategy approved by EO and passport offices advised
Recruitment of 12 new ePassport staff to commence immediately
Approval for 10% increase in short-term contract staff provided
Staff training
Duty statements to be approved by Director

Staff employment—Start date—Overseas locations

Work Station Numbers and Space Design Issues
Chip requirements
Chips
Order 2-up inlays
Revised chip order
Order supply of Security Access Modules (SAM)
Transfer of PIN numbers for SAM
Transfer of SAMs
Pallet sizes
Box figuration for chip delivery

Design of ePassport Books
Book requirements
Order book
Specimen books
- Ordinary 2,000
- Diplomatic 2,000
- Official 2,000
- Frequent Traveller 2,000

Design and sign-off of brochure
Delivery of brochure
Order display folders
Delivery of folders
Real books
- Ordinary 48,000
- Ordinary 280,000
- Diplomatic 1,200
- Official 16,000
- Frequent Traveller 27,000

Delivery of Books
Secure transport
Develop delivery schedule
Plan of action
Transportation requirements
Delivery and unpacking at office stores
Specimen books
- Ordinary (2k)
- Diplomatic (2k)
- Official (2k)
- Frequent Travellers (2k)

Personalisation of specimens
Sample books (2k)
Real books
- Ordinary (48k)
- Ordinary (150k)
- Ordinary (130k)
- Frequent Traveller (27k)
- Official (16k)
- Diplomatic (1.2k)
- Ordinary (120k)
- Ordinary (120k) Estimate
- Ordinary (120k) Estimate
- Ordinary (120k) Estimate

Despatch of sample books + SAMS to offices ready for roll out
Despatch of real books to offices (6 months' stock)

Notification and Specimens to Host Governments
Provide examples of biometric travel documents to host governments
Notification and specimens to other authorities
Arrange destruction of superseded passport book

Software changes
Develop specifications and change documentation
Final sign-off on system change specifications
Steering Committee sign-off
Program changes
Develop Test Plan
Systems testing/documentation
Acceptance of changes
Roll-out

Testing of books
Test of live books
Sign-off

Project Audit and Review
Develop project review plan
Conduct project review
Report to Steering Committee