

► A BUNDESDRUCKEREI
POCKET GUIDE TO
ePASSPORT SYSTEMS

Revised and updated – August 2007

Published by

*Bundesdruckerei GmbH
Oranienstrasse 91,
10969 Berlin, Germany
www.bundesdruckerei.de*

Project Management

*Krowne Communications GmbH
Schlüterstrasse 37, 10629 Berlin, Germany
www.krowne.de*

Copyright

*© 2007 Bundesdruckerei GmbH
No reprinting of this document is allowed.*

CONTENTS

About Bundesdruckerei	10
-----------------------------	----

PART I

1.0	More security for a modern lifestyle.....	13
1.1	About ICAO	14
1.2	Changes to the passport personalisation Et issuance process	16

PART 2: IMPLEMENTATION OF A COMPREHENSIVE IDENTIFICATION SYSTEM

2.0	ID systems: so much more than just an ePassport.....	19
2.1	Objectives of a comprehensive ID system.....	20
2.2	Identification system	23
2.3	Supporting government	23
2.4	Ongoing commitment	24

PART 3: DOCUMENT SECURITY

3.0	History of the passport.....	25
3.1	Many uses for a passport.....	26

PART 4: HIGH TECH FEATURES

4.0	System security begins with the document	29
4.1	Sophisticated processes and materials.....	29
4.1.1	Properties of the passport book.....	30
4.2	An international standard	30
4.3	Introduction to security	31
4.3.1	Paper security	31
4.3.2	Security printing techniques and use of security inks... ..	31
4.3.3	Security design and further security features	32
4.4	Book binding, numbering and personalisation.....	33
4.4.1	First ePassport types: paper data pages	33
4.4.2	Passport document description	34
4.4.3	Cover materials / security features	34
4.4.3.i	Cover	34
4.4.3.ii	Endpapers (inside front and back cover)	34

4.4.3.iii	Inside pages (visa).....	35
4.4.3.iv	Binding thread	36
4.4.3.v	Biographical data page with data protection foil	36
4.4.3.vi	Security inks	37
4.4.4	Printing techniques.....	38
4.4.4.i	Security printing	38
4.4.4.ii	Cover	38
4.4.4.iii	Inside pages (visa and biographical data page)	39
4.4.5	Passport numbering	39
4.4.6	Design aspects	40
4.4.6.i	Security features integrated in the design.....	40
4.4.7	Additional technological security features.....	42
4.4.7.i	Transparent holographic overlay.....	42
4.4.7.ii	Transparent kinogram overlay	42
4.4.8	Second ePassport type: polycarbonate data page	43

PART 5: PERSONALISATION, ENROLMENT AND ISSUANCE

5.0	Continuing security into personalisation	45
5.1	Enrolment and issuance.....	45
5.2	Personalisation trends	46
5.2.1	Centralised personalisation	46
5.2.2	Decentralised personalisation	47
5.3	Personalisation solutions	48
5.3.1	Laser engraving.....	48
5.3.2	Inkjet personalisation.....	48
5.3.3	Electronic personalisation	50

PART 6: WORLDWIDE SECURITY STANDARDS

6.0	Security assured – worldwide	51
6.1	ICAO Doc 9303	51
6.2	Visual uniformity	53

PART 7: TECHNOLOGY ASPECTS OF EPASSPORTS

7.0	High tech passport	55
7.1	The storage device	55
7.2	Chip technology	56
7.3	Choosing the chip.....	57
7.4	Biometric technology.....	59
7.4.1	Why face?	60
7.4.2	Image requirements	60
7.4.3	Quality control	61
7.5	Data stored on the chip	62
7.6	Accessing the information on the chip.....	62
7.7	Authentication methods	63

PART 8: LEVELS OF AUTHENTICATION

8.0	Levels of authentication.....	65
8.1	Level one manual authentication	65
8.2	Level two authentication with technical equipment....	66
8.3	Verification and identification.....	67

PART 9: INTEGRATION

9.0	Choosing an integrator.....	69
9.1	Responsibilities.....	69
9.2	Defining the passport system	69
9.3	Supply and installation of the system.....	70
9.4	System components	70
9.5	Project implementation	71
9.6	Fitting the project together.....	71
9.7	Establish realistic plans	72
9.8	Training and support.....	73
	Glossary	74

Initially the government printer of the Federal Republic of Germany, Bundesdruckerei became a private business in 2000. The company has a long history in secure printing as well as border management and biometrics, and is ISO 9001 certified for the manufacture of blank passport booklets and the personalisation of passports. This means it is responsible for ensuring all the physical characteristics of the passport comply with all relevant ISO specifications.

Bundesdruckerei has produced identity cards, passports and driving licences for major governments worldwide for many years. Since 1987, the company has produced more than 64 million passports for Germany alone, and since 1994, it has been producing passports or providing passport consultancy services for countries including Germany, UK, Romania, Bosnia Herzegovina, Portugal, Albania, Latvia, Venezuela Luxembourg, Lithuania and the Czech Republic. It also has extensive experience in the installation of ID systems, even in extremely critical infrastructural conditions such as Palestine, Bosnia and East Timor. Furthermore, the company is a permanent consultant to the German Ministry of the Interior for its part in international working groups such as Interpol and the Schengen-Visa activities of the EU.

For more than 15 years, Bundesdruckerei has produced the German passport and ID card centrally. Its involvement extends to more than 6500 decentralised application offices and more than 220 million documents produced in Europe alone.

In 2005, Bundesdruckerei began producing Germany's new ePassports. As the major player in the rollout of these documents, the company produces the passports (estimated to be around 2 million each year) on its premises and is also responsible for establishing the infrastructure such as visualisation equipment and fingerprint scanners at passport offices throughout Germany.

Bundesdruckerei's history as a security printer has taught it to work closely with the Federal Criminal Police Office on aspects of secure document design. As the only security printer to be represented in the ICAO working groups, Bundesdruckerei stays one step ahead of all developments, and has a role in directly influencing the latest standards for identification documents. As a result, the company guarantees it can fulfil all ICAO and EU requirements.

1.0 MORE SECURITY FOR A MODERN LIFESTYLE

It goes without saying that the world we live in today is vastly different to the one we inhabited 20 years ago. A new world order has emerged, bringing with it new threats, new opportunities and new ideologies.

While the international political arena has been categorised by the formation of new alliances, the weakening of older partnerships, the opening of borders and the establishment of new trading relations, the technology and identity sectors have been undergoing their own revolutions. New technology – and the ‘always on’ mentality – have brought a greater sense of urgency to how citizens conduct their day-to-day life. And identification technology has taken off, with many people becoming familiar with the idea of verifying themselves with a biometric, smart card, secure token or Public Key Infrastructure (PKI).

While these changes have been taking place, governments and businesses have had to address the global challenges of growing levels of financial fraud, illegal immigration, identity theft and international terrorism. Whether such activities involve small-scale low-key operations or organised gangs of international criminals, they all usually take advantage of one common flaw: weaknesses in managing identity.

International organisations have been working together to combat the forgery and counterfeiting of identities for some time, and have made particular progress in the area of passports. Consequently, a large number of passports now deployed contain the holder’s information in a format that may be read by both the naked eye and a machine, enabling border controls to increase the throughput of people while providing higher levels of security.

1.1 ABOUT ICAO

The International Civil Aviation Organization (ICAO) – a specialised agency of the UN representing over 190 nations – sets standards and regulations necessary for aviation safety, security efficiency and regularity as well as aviation environmental protection. Its standards include the Machine Readable Passport (MRP) format and characteristics, which officially became a worldwide standard in the 1990s. Meanwhile, its standards for electronic components and biometrics were formally adopted in July 2005. The ICAO's work in the area of biometrically enhanced Machine Readable Travel Documents (MRTDs) dates back to 1997. By the first half of 2002, the ICAO announced that facial recognition was the favoured biometric for inclusion in ePassports.

The ICAO estimates that 110 states are currently issuing ICAO standard MRPs, with all remaining 80 states agreeing to begin issuing these documents no later than 1 April 2010.

Today's MRPs comprise the holder's identification details, including a photograph or digital image, and a two-line Machine Readable Zone (MRZ) at the bottom of the data page (the page containing mandatory information on the passport holder). This strip provides security and efficiency advantages because it enables passports to be read quickly at border control, enabling details to be cross-referenced with immigration computers.

Taking security a step further, passports are now evolving to become electronic passports (ePassports), which are defined as MRTDs with an embedded contactless chip. Using the latest chip technology – which has been proven for applications in other sectors such as banking, telecommunications, travel and healthcare – passports are becoming smarter. Unlike the MRZ, which provides a more restricted machine readable amount of data, smart card chips allow much greater amounts of data – including electronic visas, biometrics, photo images and text data – to be stored securely.

These developments come at a time when governments and citizens have become more positive about the use of biometric data as part of the fight against 21st century threats of organised crime, terrorism and identity theft. In particular,

requirements from the US for smarter passports have helped push ePassports onto the agenda faster. This came in the form of the US Enhanced Border Security and Visa Reform Act of 2002, which was one of the measures passed in response to the tragic events of 9/11. Initially, that Act had required all 27 visa waiver countries (countries whose citizens can travel to the US for short trips without a visa) to begin issuing ePassports from 26 October 2004 onwards. When it became obvious that this deadline was not going to be achieved, the date was extended for another year and then until 2006.

However, this is not a deadline that is going to be extended year after year: Following consultation with Congress and the US Department of State, the US Department of Homeland Security (DHS) has introduced additional security requirements for visa waiver countries. The central requirement was that visa waiver countries had to start to produce passports with digital photographs from 26 October 2005 on. At this point, the Visa Waiver Program countries had also have to present an acceptable plan to begin issuing chip-based passports by that deadline.

In addition to the ICAO's specifications, passports issued in Europe must conform to council regulation (EC) no 2252/2004, which was passed on 13 December 2004. This was established to harmonise security features used in the production of EU passports and travel documents, and defines standards and technical specifications for material and printing techniques, biographical data, as well as protection measures to prevent copying and counterfeiting. The specifications include the use of personal data as well as a photograph of the passport holder, which will be stored on a chip. The regulation also introduced a requirement for two fingerprints of the passport holder to be included in EU passports from June 2009. Following the adoption of this regulation, EU member states (except the UK and Ireland) had 18 months from December 2004 to implement facial images and three years to implement fingerprint images in all new passports issued. Although this regulation standardises European passports, each member state will continue to be responsible for producing its own passports and travel documents.

1.2 CHANGES TO THE PASSPORT PERSONALISATION & ISSUANCE PROCESS

Rolling out a national ePassport system is a major challenge that involves considerable changes to the regular passport personalisation and issuance process. First, passport enrolment and issuance systems must now be able to capture the passport holder's biographic details, fingerprints and photo image. Second, this information will have to be stored in the chip and retrieved using special readers. The chip will need to be embedded in the passport book and the integrity of the data stored on the chip – including text data, biometrics and photo image – must be protected through secure methods. Finally, the passport must continue to utilise the latest security printing techniques enabling overt and covert features in the paper, printing, stitch and laminate.

Many of the world's leading economies are committed to these changes and, according to ICAO figures, more than 40 states have been upgrading to biometrically-enabled ePassports since end of 2006.

Always one step ahead of counterfeiters – the new German ePassport

International co-operation in all aspects of security is a must as globalisation increases. Protecting ID documents against forgery and ensuring the unique identification of travellers are the prerequisites for protection against crime.

For many years, German ID documents, i.e. passports, ID cards and driving licences, have ranked among the most secure in the world. Germany – as one of the first countries worldwide – set a new milestone in terms of ID security with the introduction of the new electronic passport which complies with EU regulations and ICAO standards. Bundesdruckerei GmbH produces a good 2 million German ePassports a year and also equips the 5,700 passport issuing agencies in Germany with the required infrastructure. The outer appearance of the electronic passport differs insignificantly from the traditional document. The internationally standardised logo on the cover is the only indication that a chip is included in the passport cover.

Since November 2005, the optically visible data of the passport holder, i.e. photograph and personal information such as name, gender or place of birth, is additionally stored in the chip. From November 2007 two fingerprints of the passport holder will also be stored in all newly issued ePassports. Both the chip hardware and the software used on the chip have been tested and qualified by the German Federal Office for Information Security (BSI) on the basis of the internationally recognised "Common Criteria" process.

High security and protection of personal data

The digital data stored in the chip is protected by several security mechanisms. They bear an electronic signature which warrants the integrity and authenticity of the data. In order to prevent unnoticed reading of the data, the so-called Basic Access Control process is used which is mandatory for the biometric EU passport. During the second phase, the additional cryptographic EAC protocol (Extended Access Control) will be used to access this data.

All the communication steps are encrypted and cannot be started until the passport holder has given his document to the official and the latter has placed the open passport on the terminal device. The serial number of the RF chip changes automatically during each new reading process, so that tracking and tracing of data is prevented. These security measures ensure that unauthorised tapping of the contactless communication between passport and terminal is not possible.

As in the past, the personal data is destroyed after the passport has been produced and checked at Bundesdruckerei. All data protection requirements are adhered to, with regular audits being carried out by the Federal Data Protection Commissioner.

Issuing biometric ID documents is an important building block in the fight against organised crime and international terrorism. Existing high standards must be used as a basis, and document security must be enhanced as a whole.

This pocket guide is designed to outline the requirements for a national ePassport system, identifying the drivers, challenges and issues associated with successfully deploying an ePassport system.

2.0 ID SYSTEMS: SO MUCH MORE THAN JUST AN ePASSPORT

For some governments, ePassport systems are just the starting block for a much wider – and more ambitious – identification programme. They could, in fact, be one part of a broader national security document solution that could cover many of the day-to-day aspects of citizen life.

This approach, which comprises a comprehensive identification system that is fully integrated with a civil registry system, forms the basis of many future government ID systems. Using this approach, the central production of secure electronic identification and travel documents should be based on fundamental data obtained from the civil registry.

The base system is constructed from a modern and trustworthy civil registry system that uses basic personal data to issue a unique National Personal Identification Number (NPIN) to everyone at birth. This NPIN then acts as the pivot to link personal records across the different component systems. The system also includes an Automated Fingerprint Identification System (AFIS) component that guarantees the identity of the person matches a given NPIN.

Other ID system security improvements can include updating border control systems. A wide range of interfaces that interact with other components or systems is also provided, so facilitating the online exchange of data with components or systems such as a drivers' and/or vehicles' register as well as external applications.

This approach ensures a smooth transition to ID systems, enabling governments and citizens to move with a minimum of disruption to a more efficient way of working based on e-government principles. Governments taking this route should choose companies whose technology uses open standards to achieve independence from providers. This approach offers trouble-free operation because it is based on application components already proven in similar environments.

2.1 OBJECTIVES OF A COMPREHENSIVE ID SYSTEM

An ID system without a trustworthy corresponding civil registry to sustain it lacks credibility. In fact, the effectiveness of most national systems depends on the quality and accuracy of the personal records they contain. Issues such as these help us understand how important it is to set clear objectives for such a project.

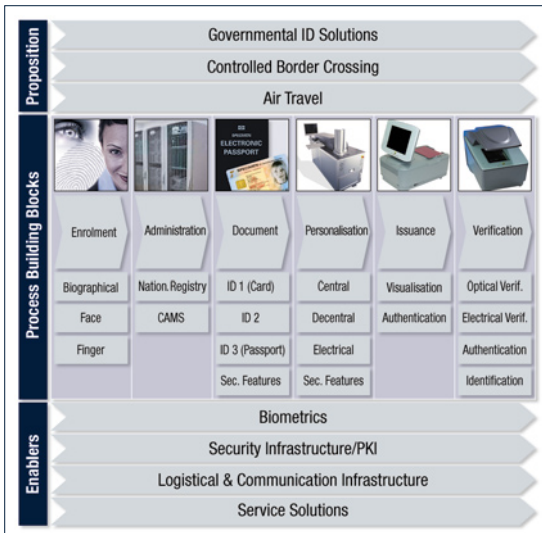
Objectives may include:

- ▶ **Modernisation.** Most countries' ID systems are operating well, but as new technologies become available, modernisation is required to ensure optimum performance. This factor is recognised by most authorities.
- ▶ **Security.** For obvious reasons, any attempt at modernisation must also ensure that all security issues remain of paramount importance.
- ▶ **International and national credibility of the issued documents.** The documents produced should be of the highest possible quality and the data used must be obtained from the most reliable sources. A trustworthy civil registry system and AFIS are also vital parts of the solution.
- ▶ **Universal coverage of the population.** The services and documents must be easily accessible to both residents and non-residents entitled to services, i.e. nationals living abroad.
- ▶ **Operational continuity.** New electronic ID systems often provide a continuation of existing services. Therefore, any new solution must include realistic and solid plans that guarantee operational continuity at all times.

Bundesdruckerei's offering:

- ▶ A comprehensive civil registry and identification system as a kernel, with fully integrated components including AFIS and border control systems.
- ▶ The highest security throughout the entire system, in particular in the production and issuing of documents.
- ▶ A system relying on open systems standards and protocols to ensure the independence of providers.
- ▶ Efficient access to services, based on the concept of e-government. To facilitate this, the system offers:
 - Swift service, particularly at front desk functions;
 - High availability of services;
 - Operational simplicity;
- ▶ Maintenance and support corresponding to the function and quality of the services given.

Bundesdruckerei's approach incorporates a civil registry system that can issue electronic ID cards and ePassports and ensure the integrity of the essential data associated with a person for identification purposes. The quality of the biometric data is guaranteed by one of the most advanced AFIS technologies and the documents issued will be produced with equipment, materials and procedures that meet the most stringent international standards.



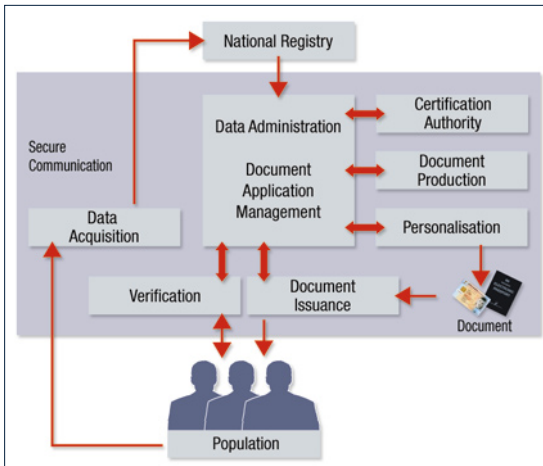


Figure 1 – Requirements ID Systems

Although the interaction with AFIS, border control and other external institutions is an integral part of the solution offered, the general public will see the most visible service units as interrelated:

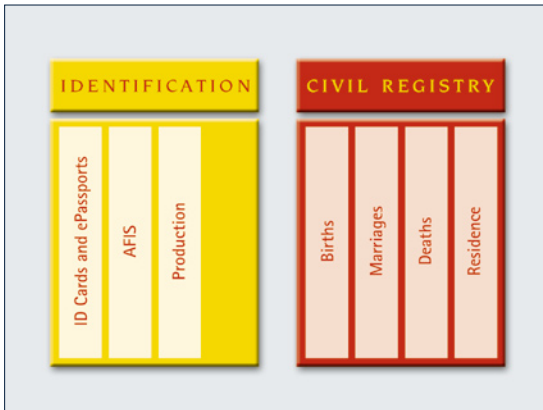


Figure 2 – Solution Parts

2.2 IDENTIFICATION SYSTEM

The identification system is a computer system consisting of several software modules and corresponding hardware. The interaction of the different modules between themselves and with other systems supports the request and issuance processes for identification documents, such as identity cards and ePassports.

This system can:

- ▶ Input a request for identification documents from applicants. For this function, it is necessary to capture and register textual data as well as digital images of the applicant's photographs, signatures and fingerprints;
- ▶ Verify the identity of the applicant via automatic AFIS or manually;
- ▶ Produce the requested documents;
- ▶ Dispatch the documents to the office indicated by the applicants;
- ▶ Deliver the documents to the applicant;
- ▶ Control every task associated with the process of issuing documents;
- ▶ Provide information to government organisations and to external entities;
- ▶ Administer the various versions of the documents (for example, marking as void a stolen document).

For all these tasks, the necessary tools and interfaces are provided to operate with specialised subsystems, such as the capture of images, the classification and verification of fingerprints, as well as the production of documents.

2.3 SUPPORTING GOVERNMENT

Because any passport or broader identification system may be eventually handed over to a state's government, it is necessary to work with organisations that have experience of commissioning and installing the various ePassport and identification components while also bringing government staff on board. Initially, this may simply be a case of working with staff to deliver a complex technical solution that functions in the real world. In the longer term, it involves sharing expertise and

knowledge with government employees so they can successfully operate all aspects of a border or identity management system, from biometric enrolment to document issuance, chip reading and biometric verification. After all, if a poor quality biometric image is initially enrolled into the system, it will be much harder for the biometric reader at a border control or government department to verify that the document holder is who he or she claims to be some time later. Alongside the training, which should be conducted in the native language of border control staff, documentation and course materials should provide easy-to-use back-up information on how the system operates.

2.4 ONGOING COMMITMENT

When the ePassport or identification system has finally been successfully rolled out, governments and suppliers enter a new phase in their relationship. From this point on, relationships between providers need to be sustained so that all support and maintenance services can be provided in a timely manner to ensure the smooth operation of the entire system. It is essential at this point that all commitments between providers and governments are met, because any failure in an ID or ePassport system could – at best – result in unacceptable delays for the public, and – at worst – result in terrorists slipping through the net.

3.0 HISTORY OF THE PASSPORT

The concept of a passport has existed for several centuries, with the term 'passport' possibly originating from the medieval documents that were required to pass through the gate (or 'porte') of city walls. These documents were generally issued by local authorities to any traveller and contained a list of the locations through which the holder was permitted to pass. However, it was not until the 20th century that the modern concept of a multi-journey, multi-destination passport issued by the holder's country of nationality emerged. In 1920, the League of Nations, and later the United Nations and the ICAO, issued guidelines on standardising passport features and layout. Less than 100 years after the first standards were devised, an estimated 600 million passports are believed to be in circulation worldwide. Although this represents only a fraction of the global population, the basic assumptions about a passport remain the same: this is an important document that is trusted internationally to establish the identity and nationality of the individual.

Clearly the main – and legal – reason most citizens apply for a passport is to facilitate easy travel from country to country. But the modern passport offers a lot more than access to other countries, continents and cultures.

Today, the average citizen in the developed world is just as likely to show his or her passport for administrative purposes as they are for boarding an aeroplane or entering a country.

During the limited life of the modern passport, the world has gone through major changes: the political landscape has altered beyond all recognition, international civil aviation has taken off, technology has leaped forward and economies have grown. But the bad news is that crime has taken on an increasingly international dimension. Driven by the prospect of significant economic or ideological rewards for successful criminal offences, modern criminals have become more savvy – with passport forgery providing an opportunity for a host of mega-buck crimes ranging from identity theft to people trafficking, terrorism, money laundering and the international drugs trade. In particular, many governments now claim that

identity theft is the fastest growing offence. In the US, for example, a Federal Trade Commission survey in 2003 showed that 27.3 million Americans had been the victims of some form of identity theft over the last five years. And in the UK, the Home Office estimated that a total of 461 fraudulent passports were detected in 2002, an increase of 28 per cent over the figure for 2001.

3.1 MANY USES FOR A PASSPORT

A raft of legislation and best practice policy has been set out in every major economy, aimed at preventing crimes such as the money laundering associated with bank-rolling international terrorism as well as the growing problem of identity theft. This has translated into a greater requirement for citizens to provide some form of identification when carrying out their business. In the absence of identity cards in countries such as the UK, many institutions now demand a photocopy of a passport as part of the identification process before allowing certain transactions to take place. For example, anyone setting up a limited company in the UK must send a photocopy of his or her passport to Companies House. Likewise, those sending money overseas are often required to provide a photocopy of their passport to the money transfer agency. And if you want to buy a property, open a bank account or set up a fixed telephone line, a photocopy of an ID card or passport is frequently demanded.

It is a tall order to create an ePassport that can successfully work for up to 10 years, especially when you are talking about a document that will have to operate in a variety of environments, from dusty border crossings to air conditioned airports. You've got to be sure that the passport is sufficiently robust to cope with these difficult – and changeable – conditions, yet sufficiently portable that it does not become a cumbersome item that is difficult to carry and frequently lost.

Whether we are talking about a traditional passport or an ePassport, the basic document requirements regarding durability are similar.

The German experience

In Germany, passport registration authorities can send the applicant's data to Bundesdruckerei electronically. Today, Germany's registration offices use Bundesdruckerei's digital 'Digant' application process to send the encrypted data to the company electronically. This has the advantage of providing a secure process that is faster and more convenient than traditional postal delivery.

Once the information has reached Bundesdruckerei, the electronic order forms and application data are processed directly. Thereafter, the data is processed on photographic security paper and developed by a photochemical special colour process.

Next, production involves integrating security features, laminating the personalised documents using special foil and trimming the passport to its final dimensions. The 'chip inlay' that consists of the chip, the chip module and the antenna is integrated into the cover of the passport booklet, whilst in other countries it may be integrated into one of the pages of the passport instead. Finally, the passport holder's personal data, digital facial image and fingerprint images are encrypted and stored on the chip.

At this point, the personal data that was sent to Bundesdruckerei is deleted in order to adhere to German data protection requirements.

4.0 SYSTEM SECURITY BEGINS WITH THE DOCUMENT

Passport issuers are keeping one step ahead of the organised criminals and have upped their game to ensure the passport continues to be a valued and trusted internationally recognised document. Over the decades since the League of Nations meeting, security levels have been improved. Today, multiple levels of security are incorporated into all passport books. And although 9/11 has provided a major impetus to improving the security of passports and other ID documents, stronger security features were incorporated into passports during the 1980s and 1990s following a series of international collaborations aimed at improving security and preventing falsification.

Considering that the average lifespan of a passport is 10 years, it is essential that any security feature included in the document is durable and future-proof. Such sophisticated security features (both optical and electrical) provide an enhanced level of security for both passport types (traditional passports and electronic passports), because they make counterfeiting of and alterations to the documents very difficult. On the other hand, the documents have to be checked accordingly, ideally with the aid of a machine. Because numerous security features of varying levels are often combined in the same document, it can become impossible to perform visual checks without such technical aids.

4.1 SOPHISTICATED PROCESSES AND MATERIALS

Complete duplication of passports is very rare, with the theft of blank books tending to be more common. To combat this problem, sophisticated processes should be adopted to incorporate the personal data and photograph in such a way that the passport becomes a unique document.

Today, pre-personalisation passport books must contain sufficient security features to prevent photo substitution and page splitting and to make counterfeiting, forgery and cracking almost impossible.

4.1.1 Properties of passport book

The cover of a passport is made of a non-PVC material. The endpapers of the passport (otherwise known as the front and last inner pages) act as a country's 'brand' or 'image'. Here, symbols of sovereignty, such as coats of arms and other traditional national themes, may be included. A number of different printing techniques can be used for these pages; however, most countries opt for intaglio printing. Some countries also incorporate additional anti-copying features in the design or as a functionality of special materials like invisible fluorescent fibres. The inner pages of the passport, meanwhile, are produced using designs that incorporate a range of security features, such as logo designs, two-colour guilloche printing, integration of page numbers into the background design, security printing, fluorescent printing, binding threads and laser-perforated inner pages.

4.2 INTERNATIONAL STANDARD

The passport should conform to all relevant ICAO and European Union standards and recommendations. This means the format of the passport should be ID-3 (the standard size of a passport: 125mm x 88mm) as set out in ISO and ICAO specifications.

Choosing a company to provide ePassports means finding an organisation with relevant expertise. Ideally, a company should be chosen that has experience in security printing as well as applying ePassport production techniques, cryptography and contactless technology. In combining this know-how, the company will be required to follow all relevant ICAO (Doc 9303 Machine Readable Travel Documents) and ISO standards, and in particular those relating to physical characteristics of the security design, security features, specific printing techniques, bookbinding and personalisation.

This means adhering to physical characteristics such as:

- ▶ Security features;
- ▶ Data page layout;
- ▶ Contactless chips that meet ICAO 9303 specifications (not less than 32KB) and EU specifications (not less than 64KB);
- ▶ Intelligent chip operating system and software (firmware);
- ▶ Quality control (physical and electronic testing);

4.3 INTRODUCTION TO SECURITY

4.3.1 Paper security

Paper for passports should be secure and hard to imitate with standard technologies. Paper designed for use in passports provides the first layer of security. This type of paper uses a mixture of cotton and cellulose without use of optical brighteners. Other chemical reagents are recommended by security organisations. These provide a chemical reaction on acids and bases, bleaching agents and solvents. A customer specific multitone watermark is integrated during paper production. Small holographic stripes could be completely embedded or partly shown as a window thread. Additional features integrated in the thread could be used (microlettering, partly demetallization, UV fluorescence). It is common to integrate random fibres visible under white light or invisible fibres visibly under UV light. It is also possible to add planchettes in different colours.

4.3.2 Security printing techniques and use of security inks

The next layer of security can be achieved using printing techniques. Taking into account the fact that relatively sophisticated reproduction technologies such as professional graphics software, scanners and printers for home PC use have become inexpensive and ubiquitous, passport printing uses highly sophisticated methods that can work in the variety of applications that a modern passport may be used for.

In other words, the security features are designed to be strong enough to prevent tampering and forgery, yet sufficiently user-friendly to ensure the document remains a useful form of identification for the growing number of administrative functions now demanded by citizens, governments and other organisations.

Additionally to the security level of the passport paper some dedicated functionalities of pigments are used. Passport printers know a lot about fluorescent inks, UV inks, IR-readable or non-readable inks, metameric inks, or customer specific marked inks. Especially Bundesdruckerei is able to integrate combinations of specific inks known to few people on both sides.

Steps can be taken to address the typical problems of counterfeiting and tampering throughout the passport. For example, the background of the passport can be printed with a design that is difficult to copy with conventional copiers and scanners through a process such as rainbow printing.

The front and/or back cover of the passport can include single or multi-colour intaglio printing. These printing techniques could be combined with the use of inks with different IR properties or optically variable ink (OVI). After printing, a ridged profile is detectable by fingertips and makes it possible to include additional security features such as a latent image.

4.3.3 Security design and further security features

Passport security design should combine the possibilities of special printing or production techniques, special inks or other materials and the "knowledge of counterfeiters". The designer has to integrate passport functionality with national and cultural interests of the issuing country under aspects of document security and document verification and last but not least the passport must follow international recommendations or standards. It's a real challenge to build up a sophisticated "document architecture". For the background design features like positive and negative micro-lettering, combined two-tone guilloches, security rasterization and anti-copying structures are used. Especially the data page has to be secured against tampering and counterfeiting, so that an optically variable device (OVD) must cover individual information (facial image and biographical data). Some

hidden information could be integrated during the personalisation process. Normally the additional information is only machine readable. It shouldn't be possible to prepare a new data page from visa pages. Therefore, a slight difference in design has to be taken into consideration between visa pages and the data page, thereby making it obvious when people remove visa pages from their passport. To secure the order of the pages, the page number is printed with UV ink and additionally a conical perforation is used.

4.4 BOOK BINDING, NUMBERING AND PERSONALISATION

4.4.1 First ePassport type: paper data pages

Inkjet personalisation

During inkjet personalisation, the citizen's biographical and biometric information is printed on the data page of the blank passport booklet. The ink is partly absorbed into the paper (as opposed to colour laser printing, where the toner only makes an impact on the surface of the paper). Any attempt to remove the ink will also destroy the surface of the page, making forgery difficult. It is also important to make sure that only machine readable ink (ink which reflects under infrared light) is used for printing personal data.

After printing additional security components a transparent optically variable foil is laminated on top of the data page. This foil contains diffractive optical structures which give the data page an appearance of having different patterns, colours, and designs depending on the amount of illumination and the viewing angle. The beauty of this approach is that the designs can be very complex, making them effective in deterring counterfeiters. Furthermore, because of the inherent thinness of the foil – and its binding to the biographical data page – paper forgery attempts (on the data) can be detected.

In order to achieve a high level of security, the production process of the blank passport booklet is designed to protect all documents in such a way that any attempts to counterfeit or falsify a genuine document become instantly recognisable. The security features are provided at three levels.

► **Level one**

Can be identified by any individual without any specialist training and without the use of technical equipment;

► **Level two**

Security features which are identifiable by trained experts employed by regulatory bodies and/or by laypersons using simple technical tools;

► **Level three**

Security features which can only be identified using laboratory procedures.

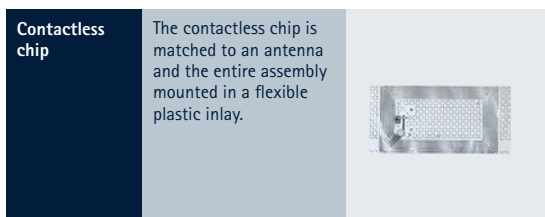
4.4.2 Passport document description

ePassport production requires specialist technologies. Over the following pages we will look at how passports in Europe are being designed to incorporate these techniques.

4.4.3 Cover materials / security features


4.4.3.i Cover

The inlay which is to contain the chip / antenna assembly is inserted in the front cover of the booklet.



4.4.3.ii Endpapers (inside front and back cover):

These are prepared from security paper made for example of 100% cotton, without a watermark. The paper should be free of optical brighteners (thus remaining dull after being exposed to an ultraviolet light), but should include chemical reagents.

<p>Reagents</p>	<p>Chemical reagents are mixed into the paper to prevent manipulation by:</p> <ul style="list-style-type: none"> ▶ Acids ▶ Alkalis ▶ Alcohol ▶ Petrol derivatives ▶ Ink killer ▶ Whitening elements 	
------------------------	---	---

The paper includes:

- ▶ Visible (micro) fibres (white under IR light and/or single-coloured);
- ▶ Invisible fibres (two colours after being exposed to UV light).

<p>Micro fibres</p>	<p>These fibres have a length of approximately 3mm and are about 25 dtx thick.</p>	
----------------------------	--	---


4.4.3.iii Inside pages (visa):

The paper of these pages should be free of optical brighteners (thus remaining dull after being exposed to a UV light), but should include chemical reagents. The paper includes:

- ▶ Visible (micro) fibres (white under IR light and/or single-coloured);
- ▶ Invisible fibres (two colours after being exposed to an ultraviolet light).

Watermark:

- ▶ Multi-tone cylinder mould-made watermark

Watermark	Multi-tone cylinder mould-made watermark that has been customised designed and can be placed in a fixed position.	
Security thread (optional)	A security thread is embedded in the paper and contains micro text (extra small printing) and colours that become visible after being exposed to a UV light source.	

4.4.3.iv Binding thread

The passport should be bound with stitching threads, comprising a fluorescent triple thread made of three different colours.

Stitching thread	A natural cotton fibre thread 'step' stitches the pages together with twisted stitching. The thread is coloured and is made of three separate and individual threads, all of which fluoresce after being exposed to a UV light source.	
-------------------------	--	--


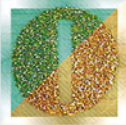
4.4.3.v Biographical data page with data protection foil

The data page is made from paper with a bending strength of 10,000 cycles (at the binding) for the passport, suitable for inkjet personalisation.

Paper	The paper should have been heavily tested to withstand heavy environmental conditions.	
--------------	--	--

4.4.3.vi Security inks

The inks used to print passports are not commercially available and their distribution is restricted.

Special inks	The ingredients of special inks are a closely guarded secret by all security printers and ink providers. Many inks are made to a special formula and may also contain chemical reagents to prevent forgeries and counterfeits. The inks may also react differently after being exposed to UV or IR light.	
Optically variable ink	Optically Variable Ink (OVI), also called colour shifting ink, is printed on the inside covers in the form of a customised emblem. The inks may also react differently after being exposed to UV or IR light.	

4.4.4 Printing techniques

4.4.4.i Security printing

A number of different printing techniques can be deployed to produce passports. All printers used for this process are specially designed. There are many restrictions on their availability on the open market, making it extremely difficult for a forger to purchase or gain access to such specialist equipment.



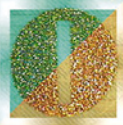
4.4.4.ii Cover

The passport cover is embossed with a customised design.

Inside cover


Dry offset and / or indirect letterpress	These printers are capable of great precision and can therefore create characteristics such as continuous line patterns, which are typically used for high security passports. Inks that react after being exposed to UV light allow the fine lines and/or motif to fluoresce when exposed to such a light source.	
Intaglio	The front and back inside covers contain a motif that includes wording and/or images which can be seen when tilted. The printed areas have a raised profile, making them identifiable by touch. Text could also be printed in intaglio on the inside front and back covers. OVI may be added on both inside covers. The ornaments on the inside covers also have multi-colour mixing.	

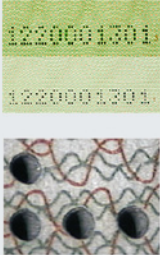

4.4.4.iii Inside pages (visa and biographical data page)

<p>Dry offset and/or indirect letterpress</p>	<p>Passport printers are capable of great precision and can therefore create characteristics such as continuous line patterns, which are typically used for high security passports.</p> <p>Inks that react after being exposed to UV light allow the fine lines and/or motif to fluoresce when exposed to such a light source.</p>	 
<p>Silk screen printing</p>	<p>In silk screen printing, the inks used, including those with large pigments such as OVI or silver paste, are pressed through various different screens, enabling the creation of unique features in the appearance due to the potentially high ink application and iridescent effects.</p>	

4.4.5 Passport numbering

Numbering appears on all inside pages of the passport. Different methods can be used to print the passport number. By combining these methods, governments can make it significantly harder for counterfeiters to reproduce the document in full or forgers to alter part of the document.


<p>Number on front end paper or reverse of data page</p>	<p>This may be printed by letterpress. The ink fluoresces after being exposed to UV light.</p>	
---	--	---





Number and barcode (optional)	In addition to the passport number, a barcode corresponding to the serial number is also printed. Barcode is an optional security feature.	
Paper pages	The passport numbers are perforated by laser through page 3 to the last visa page as well as through the endpaper in the cover. The holes burnt through the material ensure the pages cannot be easily replaced by those of another passport. The holes on page 3 are of a wider diameter than those on the last pages due to the 'cone' form of the laser beam.	
Biographical data page	The passport number must also be printed on the data page during the personalisation process.	

4.4.6 Design aspects

The passport contains a customised design that is featured on the cover, data page, inside pages and security backgrounds.

4.4.6.i Security features integrated in the design

Guilloches	Customised coloured guilloches are integrated into the design. These are continuous very fine interweaving lines without apparent end or beginning, which are very difficult to replicate.	
-------------------	--	---

<p>Micro text</p>	<p>Very small text (about 0.3 mm high) is integrated into the design. The size of this text makes it almost unrecognisable to the naked eye. This text can be printed continuously.</p>	
<p>Rainbow printing</p>	<p>One of the guilloches can be rainbow printed which means colours smoothly change and blend into each other. This effect is very difficult to copy.</p>	
<p>Integrated page numbers</p>	<p>The page number can be integrated into the design of each page (except page 2 – the data page). Page numbers are printed so they become visible after being exposed to UV light. They are also positioned differently on each page in a process known as floating page numbering.</p>	
<p>Special anti-copy patterns</p>	<p>Special anti-copy patterns are incorporated into the design to help make the pages difficult to reproduce using conventional methods such as scanners and colour copiers.</p> <p>The combination of colours is chosen to increase the difficulty of counterfeiting.</p>	

ICAO and EU conformity

The data page conforms to ICAO and EU standards. In other words, the layout of the data page has certain differences to other pages. This makes it impossible to substitute another page in the passport as the data page.

The layout is horizontal with the area for the photograph being located near the left hand side. The data page also features a machine readable zone including data that is coded and printed with special characters.



4.4.7 Additional technological security features

4.4.7.i Transparent holographic overlay

Holographic protection foil

For the highest level of hologram security a diffractive image device is integrated in a transparent overlay. This is one of the most secure types of optically variable device and is attached on the data page as a transparent overlay.



4.4.7.ii Transparent Kinegram Overlay

Kinegram foil

A Transparent Kinegram Overlay is applied. This is one of the most secure types of optically variable device and is attached on the data page as a transparent overlay.



4.4.8 Second ePassport type: polycarbonate data page

If an RFID chip is integrated into a polycarbonate data page instead of a paper data page, it becomes far more important to use a highly durable attachment (binding) in the passport booklet. Furthermore, both the chip and antenna must be capable of resisting physical and chemical attack.

A polymeric hinge material is integrated into the polycarbonate when the data page is sewed into the passport booklet. This process has gone through extensive durability testing to ensure the data page binding is capable of enduring more than 10,000 bends.

It is understandable that governments should be concerned about the quality, reliability and durability of the data page. As no specific standards for polycarbonate data pages exist, governments should ask their supplier what tests the page goes through. For example, Bundesdruckerei applies tests according to the upcoming ISO and ICAO recommendation.

Over the following pages, we look at the additional security features specific to a polycarbonate data page.

Laser engraved numbering of biographical data page

During production, the passport number is laser engraved on the reverse side of the data page. It is also engraved into the data page during the personalisation process.



Changeable laser image (CLI) (optional)

In order to protect against photo replacement, a lenticular structure (window) is precisely positioned and integrated into the passport body during the lamination process. During personalisation two individual pieces of information are laser engraved into the lenticular structure. One of these could be the photo of the passport holder which is laser engraved a second time in the CLI window, thereby creating a thumbnail image.



Personalised data: combination of different laser settings to make data reproduction even harder.

Different parameters for laser beam set-up can be established. Depending on how these parameters are set, data can be applied to the substrate surface, which can be verified both visually and by touch. Other data may be printed underneath the top layer of the document.

5.0 CONTINUING SECURITY INTO PERSONALISATION

Turning a blank passport into a usable personal document involves a process of personalisation, which is a key part in the ePassport production process. At this stage, it is essential that issues such as security, quality and consistency are ensured and maintained so that all passports work successfully for their intended life.

5.1 ENROLMENT AND ISSUANCE

For security to be effective, the passport enrolment and issuance system must capture the passport holder's information – such as biographic details, biometrics and digital photo image – before encoding, compressing and storing it in the passport chip. This electronic storage and integration of personal data effectively provides an additional 'back up' of all the information stored on the passport.

However, this process involves a lot more than simple data capture. Successful personalisation requires governments to think about stock management (where should you store blank passports? How many should you have in reserve? What security procedures will you adopt in the locations where the passports are stored?) And it doesn't stop there: logistics issues need to be taken into account during issuance and enrolment. For example, should the passports be stored locally or centrally? How can they be issued to passport applicants? Where can citizens go to enrol their personal and biometric data?

With the advent of biometrics and chip technology, the arguments over centralised vs. decentralised approaches to passport enrolment and issuance become even more important.

5.2 PERSONALISATION TRENDS

Although it will always be possible for enrolment to take place in a decentralised location, personalisation and production of a passport can be either centralised or decentralised.

As the term suggests, the centralised approach involves the citizen sending his or her passport application to a central authority and waiting several days or weeks for the document to be processed. This document may then be sent by post (possibly using a recorded or registered delivery service), or may be available for collection from a local municipal office or police station.

Issues such as quality, consistency and security, are now driving a trend for more governments to adopt a centralised approach to passport personalisation.

5.2.1 Centralised personalisation

Centralised personalisation is a favoured option for many EU countries. Centralised personalisation of the documents means that personalisation is carried out at one site only, while the application and issue processes are decentralised. The countries have identified the following advantages:

- ▶ Improvement in the quality and consistency of the personalisation process;
- ▶ No logistics system needs to be established for the distribution of blank passports;
- ▶ No storage requirements in decentralised locations, meaning a reduced risk of theft;
- ▶ The introduction of new security features or passport designs is more economical;
- ▶ Greater economies of scale may be introduced, thereby making personalisation cheaper;
- ▶ Centralised systems can use stronger security measures, thereby protecting private data.

Countries that have opted for a centralised route include:

- ▶ Belgium
- ▶ Czech Republic
- ▶ Denmark
- ▶ Estonia
- ▶ Finland
- ▶ Germany

- ▶ Hungary
- ▶ Ireland
- ▶ Latvia
- ▶ Lithuania
- ▶ Luxembourg
- ▶ Netherlands
- ▶ Norway
- ▶ Poland
- ▶ Slovak Republic
- ▶ Sweden
- ▶ Switzerland
- ▶ United Kingdom
- ▶ Venezuela

5.2.2 Decentralised personalisation

Other countries, meanwhile, are opting for decentralised personalisation.

The decentralised approach has several advantages:

- ▶ The passport application process is quicker;
- ▶ It provides a chance to link the passport applicant to his or her history, which may be stored in a municipal, local, register.

However, the risks include:

- ▶ Inconsistency between offices in terms of quality of personalisation and identification checking;
- ▶ Security risks are considerably higher as security infrastructures tend to be less advanced than in centralised environments;
- ▶ An increased risk of theft of blank passport books from multiple locations;
- ▶ Higher costs of maintenance and support.

Countries that have opted for this route include:

- ▶ Bulgaria
- ▶ Greece
- ▶ Italy
- ▶ Portugal
- ▶ Spain

5.3 PERSONALISATION SOLUTIONS

With the introduction of the chip-based electronic passport there are now two kinds of personalisation that must take place. The first is the optical personalisation through laser engraving and inkjet personalisation. The second kind of personalisation is that of electronic personalisation as the data is recorded and stored onto the chip itself.

5.3.1 Laser engraving

Optical personalisation provides an opportunity to introduce the most high tech secure printing techniques to make it practically impossible to alter the data that is visible to the naked eye. Some passports have a specially coated data page, which enables the paper to be personalised in a process known as laser engraving. This involves the partial burning of the substrate in order to fix the information. It enables the passport holder's personal data to be raised from the surface of the paper, allowing border control staff to tell easily whether the passport is genuine or has been tampered with merely by feeling the profile of the paper.

5.3.2 Inkjet personalisation

Inkjet personalisation prints the biographical and biometric information on the data page of the blank passport booklet. The ink is partly absorbed into the paper (as opposed to colour laser printing, leaving the toner only on the surface of the paper). Any attempt to remove the ink will also destroy the surface of the page, making forgery very difficult. It is important that only machine readable ink (in other words, ink that reflects under IR light) is used for printing personal data. After printing is complete, an additional security component such as a transparent optically variable foil will be laminated on top of the data page. This foil contains diffractive optical structures which give the data page different patterns, colours and designs depending on the amount of illumination and viewing angle used. Because these designs are very complex, they are ideal for deterring counterfeiters. And because of the inherent thinness of the foil and its binding to the biographical data page, paper forgery attempts can also be detected.

In order to achieve high levels of security, the production process of the blank passport booklet is designed to protect all documents in such a way that any attempts to counterfeit or falsify a genuine document become instantly recognisable.

Solid ID solutions for laser engraving

Maurer Electronics GmbH based in Munich, Germany, specialises in manufacturing high-security systems for identification documents. Founded in 1975, the company initially developed, manufactured and sold avionics, audio equipment and security systems. Their focus changed in 1983 and shifted towards ID documents. Today, Maurer Electronics develops state-of-the-art ID document production technology and takes a leading edge in the supply of integrated systems for both national and international ID applications.

Their ME5000 Laser Engraving System is designed for personalisation of cards (ID1) and passports (ID3) for high production volumes. These documents can be personalised with visual as well as electronic data. Constant items (logos, grids etc.) and personal data (name, portrait etc.) can be processed.

The new system addresses the demands of high throughput laser engraving. It's now possible to have the advantages of large-scale personalisation without the disadvantages of large and difficult-to-maintain machines. The ME5000 also offers exceptional operational economy as it needs little operator attention, has a high uptime and no full system stop during maintenance. The solution uses the multi-laser concept, which combines redundancy and central operation in a simple but unique way. As a matter of course the system incorporates full smart card and ePassport capability.

5.3.3 Electronic personalisation

The new ePassport adds another dimension to the passport personalisation process. As the visual information recorded on the passport is stored in the contactless chip, it is also absolutely essential that all details held on the data page exactly match the information stored in the chip. Furthermore, the inclusion of biometric technology creates new logistical questions in terms of where and how citizens enrol their individual biometrics.

One approach to personalisation is to develop a generic solution to personalise chip data in central sites. This could include fast generation of personalisation scripts as well as digital signing and securing of both biometric and other sensitive data using algorithms such as RSA. The electronic personalisation process for ePassports basically consists of the following steps:

- ▶ Prepare the data to be stored in the contactless chip in the so called "Logical Data Structure" (LDS) which has been defined by ICAO
- ▶ Electronically signing the data using a public key infrastructure to protect the integrity of the contents and to prove authenticity during the verification process
- ▶ Write the prepared data in the EEPROM memory of the chip

The public key infrastructure needed for ICAO compliant ePassports has a Country Signing Certification Authority (CSCA) as the root certification authority of the infrastructure. The CSCA is typically run by a ministry and installed at their premises. The Document Signer (DS) forms the unit which signs the Logical Data Structure. The key material used by the DS is signed by the CSCA. Thereby the whole certificate chain can be checked for authenticity during the verification process.

6.0 SECURITY ASSURED – WORLDWIDE

If the integrity of a passport is to be trusted, the personalisation process must be designed to meet the overall security specifications of the project, which should be in line with the ICAO standards covering both the visual appearance and the technical operation of a passport.

All countries participating in the ICAO have agreed to these standards, which in turn means Machine Readable Passports (MRPs) are expected to be interoperable worldwide. Responsibility for the development of these standards falls to the ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD).

6.1 ICAO Doc 9303

The ICAO first laid out specifications for machine readable passports in 1988 as ICAO Doc 9303, for passports with machine readable capability. During the 1990s, Doc 9303 went through several revisions and was sub-divided into distinct parts to cover the range of machine readable travel documents used for international travel. Consequently, passports were covered by Part 1 of ICAO 9303, visas by Part 2 and other official travel documents – such as crew member certificates or documents in formats other than for passports – by Part 3.

The technical specifications of ICAO 9303 standards have been developed mostly in the subcommittee ISO/IEC JTC1/SC17 'Cards and Personal Identification' and its working groups. Subcommittees SC37 and SC27 of JTC1 have also provided substantial input related to biometrics and security techniques to 9303. Due to the close relationship between ICAO and ISO/IEC the 9303 parts are officially approved via an ISO/IEC balloting process and thus carry an ISO/IEC standard number – ISO/IEC 7501.

The most recent and up-to-date ICAO specification of relevance to ePassports is the sixth edition of ICAO 9303 Part 1, which has again been split into two pieces. Volume 1 contains the former Part 1 of 9303 up to its fifth edition and is titled 'Passports with Machine Readable Data Stored in Optical Character Recognition Format', whereas the Volume 2 of Part 1 contains all additions making a passport an 'ePassport'. Its title is 'Specifications for discretionary expansion of data storage capacity and globally interoperable biometric identification'. The sixth edition of Part 1 was approved by the ICAO TAG/MRTD on 28th September 2005.

The new Volume 2 of the ICAO 9303 Part 1 incorporates changes to include references and definitions relative to biometrics and chips. Also included are more substantial modifications. These reflect the role of the contactless chip as the standard for data storage and facial recognition from a stored image as the globally recognised biometric standard, with fingerprint and iris biometrics recognised as secondary technologies.

The most up-to-date information about ICAO 9303 can be found in the Document 'Supplement to Doc 9303', which ICAO issues on a quarterly basis. Six editions have been published, the sixth of which was posted onto the ICAO MRTD website on the 19th May 2007. The Supplement to Doc 9303 is designed to provide regular travel document guidance, advice, updates, clarifications and amplifications. As the ICAO says: "The Supplement shall serve as a 'bridge' between the formal drafting of standards and technical reports and the needs of the travel document community to have timely and official direction on which to rely... Much of the contents of the Supplement shall eventually be incorporated into a Technical Report or 9303 or both and, in that manner, can serve to shape and form such ICAO documents."

When having had organized international interoperability tests for ePassports within the years 2004 up to 2006, which had shown increasingly success and good results, but were quite costly and time-consuming. Therefore, in 2004 ICAO had decided to elaborate standardized test methods for ePassports and their readers which are intended to be used by issuers and manufacturers in order to maximise the probability for international interoperability, without the necessity to perform again and again big meetings for interoperability tests.

The extensive efforts over many years by ICAO and ISO have finally reaped success. Four Technical Reports on test methods were approved at the last ICAO TAG/MRTD Plenary at the end of March 2007 and have been available for download from the MRTD website since 20th May 2007:

- ▶ Durability of Machine Readable Passports (Version 3.2)
- ▶ RF Protocol and Application Test Standard for e-Passport – Part 2: Tests for air interface, initialisation, anticollision and transport protocol (Version 1.02)
- ▶ RF Protocol and Application Test Standard for e-Passport – Part 3: Tests for application protocol and logical data structure (Version 1.01)
- ▶ RF Protocol and Application Test Standard for e-Passport – Part 4: e-Passport reader tests for air interface, initialisation, anticollision and transport protocol (Version 1.01)

These four Technical Reports will be further maintained and developed by the ISO Subcommittee ISO/IEC JTC1/SC17 on behalf of ICAO TAG/MRTD, in order to gain fastest input and feedback from the involved industries. Parts 2 and 4 of the RF related Technical Reports have been already integrated into the revised text of ISO/IEC 10373-6, i.e. the test methods for contactless objects (like ePassports) being compliant to ISO/IEC 14443. A decision how to develop the other two test technical reports in ISO will be taken in early October 2007.

6.2 VISUAL UNIFORMITY

The visual appearance of a passport holder's information conforms to a uniform standard that is adopted worldwide. As passports have become more technically advanced, visual requirements have changed a lot.

This information, along with other visible data – classed as level one identity verification – is incorporated into the passport during personalisation for future visual inspection.

The following level one identity data is included in all passports:

- ▶ Unique passport number;
- ▶ Unique national identity number;
- ▶ Full name of passport holder;

- ▶ Country code;
- ▶ Colour photograph;
- ▶ Passport holder's signature;
- ▶ Passport holder's nationality;
- ▶ Date of issue of passport;
- ▶ Expiry date of passport;
- ▶ Passport holder's date of birth;
- ▶ Passport holder's place of birth;
- ▶ Passport holder's sex;
- ▶ Passport issuing authority;
- ▶ Machine Readable Zone containing
2 lines of Optical Character Recognition (OCR-B).

7.0 HIGH TECH PASSPORT

Although the visual layer of security in the passport – such as the passport number or colour photograph – has an important primary verification function, the added level of security in an ePassport is contained in the contactless chip, which is embedded in the document.

The process for harmonised worldwide integration of biometric identification in machine readable travel documents is contained in ICAO 9303, Part 1, Volume 2.

The specifications include:

- ▶ The face as the primary, mandatory biometric; the iris or fingerprint as secondary and optional;
- ▶ The contactless integrated circuit chip as the storage medium;
- ▶ A logical data structure for programming the chip;
- ▶ A modified public key infrastructure (PKI) scheme to secure the data against unauthorised alteration.

The Machine Readable Passport (MRP) in the format specified by ICAO 9303 became the worldwide standard in September 2005. The ICAO has devised a plan of action called the Universal Implementation of Machine Readable Documents to support states not yet issuing MRPs because of a lack of technical know-how or financial resources. The support includes technical assistance in applying the ICAO specifications and organising issuance systems, identification of resources from donor states and international financial institutions, project management through the ICAO's Technical Co-operation Bureau as well as quality control.

7.1 THE STORAGE DEVICE

When the ICAO examined the technology available for more secure passports, it initially looked at barcodes and optical cards to provide the extra memory capacity required. However, barcodes were considered unsuitable, because although they met cost criteria, they would not have been able to provide the necessary storage capacity in the space available.

Furthermore, they would prevent the possibility of reprogramming information if required. Optical cards, meanwhile, were considered too expensive and their use in a passport booklet was thought impractical. Smart card technology was therefore considered the most suitable to adopt.

Smart card technology has a well-won reputation in application environments as diverse as financial services, telecoms, healthcare, national ID and transport. These application sectors have all chosen the technology for its ability to meet the challenges of managing identity as well as its ability to be part of a secure, cost-effective solution.

7.2 CHIP TECHNOLOGY

However, unlike many of these applications which rely on the use of contact-based smart cards, ePassports use contactless technology, which operates using radio frequency (RF) technology and comprises a chip and an attached antenna. This technology has a good track record globally, particularly in applications such as the passenger transit market where speed, high throughput and harsh conditions are major daily challenges. It is also beginning to win praise in the payments sector, where security and fraud are areas of concern.

Contactless chips can store a large amount of data and transfer it between the passport and the reader without experiencing the maintenance problems connected with dirt, fatigue or moisture, which are sometimes experienced in contact-based systems. Also, as there are no mechanical parts in a contactless reader, the maintenance costs associated with wear and tear, misuse and harsh environmental conditions are substantially lower than those incurred during the life of a contact system.

The ICAO specifications for ePassports are for contactless chips that conform to the ISO/IEC 14443 proximity standard, which specify an operating frequency of 13.56 MHz and a read range of up to 10 cm. The standard data transfer rates are specified from 106 kbps (kilobits per second) to 848 kbps. Although the ISO/IEC 14443 standard provides a read range of up to 10 cm, it should be remembered that read ranges can be affected by the location of the RF reader. For example, if

the reader is hosted on or near metal, the metal could distort the excite field (the electromagnetic field that is transmitted from the contactless reader).

An equally important standard is ISO/IEC 10373-6 and its amendments which contain necessary test methods to verify ISO/IEC 14443 functionalities in both ePassports and their readers.

ISO/IEC 14443

ISO/IEC 14443 contains four parts:

- ▶ *Physical characteristics;*
- ▶ *Radio frequency power and signal interface;*
- ▶ *Initialisation and anti-collision;*
- ▶ *Transmission protocol.*

Several amendments to ISO/IEC 14443 have also become available, which are currently going to be integrated into revised versions of these four parts during the next few years.

ISO/IEC 14443 covers type A and type B cards. The ICAO specifies that the contactless chips can be operated either in type A or in type B. Typically the chip is embedded into the cover or inside pages of the passport.

In order to achieve worldwide interoperability, the contactless passport readers must be able to read both type A and type B chips.

In order to ensure that passports and passport readers can be operated according to the variety of ICAO specifications issued, ISO/IEC 10373-6 and its amendments provide the related test methods to be applied. The new RF related test methods for testing the ISO/IEC 14443 compliance of ePassports and readers, published on the ICAO MRTD website on 20th May 2007, are being processed as amendments to ISO/IEC 10373-6.

7.3 CHOOSING THE CHIP

Chip sizes are an important consideration because it is essential that they not only have sufficient memory to cope with the data stored on them, but also meet the cost criteria frequently demanded by taxpayers and government watch-

dogs. The ICAO recommends a minimum memory size of 32KB for a chip because this is sufficient for storing the information currently required. However, the EU requires that chips of no less than 64KB be used as two fingerprints will be stored from 2007. Furthermore, because some countries in other parts of the world are adding – or considering adding – other biometric identifiers such as fingerprints or iris, chips with a capacity of around 64KB are being chosen by some states. This approach has the advantage of enabling a government to future-proof its ePassports, but has the disadvantage of higher costs.

Germany has opted to equip its ePassports with contactless chips with a memory capacity of 72KB or 64KB. In this instance, Infineon Technologies and NXP provide the so-called inlays, which consist of the chip, the chip module and the antenna.

Chip durability – including its ability to retain data over a long period of time and the number of read/write cycles it can handle in its lifetime – is also a consideration, bearing in mind that the average passport life is ten years, and during that time the passport may have to operate in harsh environments. After all, the very nature of international travel implies a large amount of wear and tear. Take for example the case of a traveller boarding a plane in the middle of a freezing Nordic winter and disembarking in tropical or desert conditions less than six hours later. Or consider the case of the passenger who spills coffee on the passport, unwittingly drives a baggage trolley over it or sits on the document for the duration of a transatlantic flight. Up to ten years later, that passport holder is still going to expect his or her ePassport to work.

7.4 BIOMETRIC TECHNOLOGY

Biometric technology is becoming increasingly common in many parts of the world for applications such as access control, ID cards and even retail payments. This technology has the security advantage of not being able to be borrowed, lost or stolen, and can be used to authenticate an individual by measuring his or her distinct physical characteristics or behavioural traits.

Examples of physical characteristics measured by biometrics include:

- ▶ Face
- ▶ Fingerprint
- ▶ Hand geometry
- ▶ Iris
- ▶ Retina

Examples of behavioural biometrics include:

- ▶ Dynamic signature
- ▶ Gait recognition
- ▶ Keystroke recognition
- ▶ Speaker verification

Biometric systems can:

- ▶ Verify the claimed identity of an individual in what is referred to as 1:1 matching;
- ▶ Identify the individual's biometric against a database or watch-list of individuals in what is referred to as 1:n matching.

Many governments see biometric data as an essential tool in the international fight against organised crime, terrorism and fraud. The technology has major advantages in a border control environment: it enables authorities to establish whether an individual is attempting to enrol for a second document using false information; it can conclusively link an individual to a document; passport officials can be more certain that a person is who he or she claims to be; and its inclusion makes it much more difficult for criminals to duplicate passport documents successfully. In addition, using 1:n identification passport officials have a more robust way of checking whether an individual is on a pre-defined watch-list of terrorists or undesirables.

7.4.1 Why face?

The ICAO's New Technology Working Group (NTWG) first began investigating biometric methods in the 1990s. It eventually decided that facial recognition would be the globally interoperable biometric in passports with fingerprint or iris recognition specified as optional extras. Facial recognition was considered the most suitable because a biometric system can always acquire an image of a face (unlike fingerprint, iris or hand, which require some form of active participation by the individual). Facial recognition is acceptable worldwide because people are familiar with being recognised by their faces. It does not suffer from any of the hygiene issues that affect touch-based biometrics such as fingerprint and hand, and does not suffer from the criminal connotations sometimes associated with fingerprints. Citizens may also consider it less invasive than technologies such as iris or retina biometrics. In addition, face biometrics offer logistical advantages for ePassports: they can be captured from a suitably posed photograph, so do not require any special visits to dedicated enrolment stations or entail further costs for citizens and governments. Furthermore, many countries already hold legacy databases of facial images, and facial images are often the only biometrics on record for watch-lists of terrorists or other criminals.

There are a number of different facial recognition systems on the market, which has led the ICAO to recommend the use of facial images rather than templates to ensure passport interoperability between countries that may adopt different hardware and biometric matching devices to recognise passengers.

7.4.2 Image requirements

The mandatory introduction of face recognition in passports has changed the way citizens should provide their passport photographs. The ICAO has issued strict guidelines about how passport photographs should look. As a precondition to digitising the photograph and in order to enable the full electronic comparison with the holder at border controls, the photograph must show the bearer in a frontal pose (full face) rather than in portrait style (looking over one shoulder).

General recommendations for capturing facial images are that they should be compressed to between 15KB and 20KB, and should not be smaller than 12KB.

7.4.3 Quality control

Passport systems must rely on image quality at both the initial image capture stage and again at border crossings. If the image quality is not sufficiently high, it will lead to unnecessarily high False Rejection Rates (FRR), which in turn will slow down the throughput of travellers and undermine the confidence that citizens have in the system, especially if their ePassport has cost them significantly more than their previous document!

False Acceptance Rate (FAR)

False acceptance refers to the acceptance of an impostor into a system being protected by a biometric device. False Acceptance Rate (FAR) refers to the probability – expressed as a percentage – which a device will fail to reject an impostor.

False Rejection Rate (FRR)

A false rejection rate is the rejection of a legitimate user from the system being protected by a biometric device. False Rejection Rate (FRR) refers to the probability – expressed as a percentage – which a device will fail to accept a legitimate user.

Therefore it may help to give photographers guidelines for positioning the subject and setting up the photographic environment. Software can be used to find eye locations and to align, scale and crop an image as well as optimise the contrast.

Ideally, facial and fingerprint image quality should be assessed at the time of capture to ensure they work properly in a matching environment.

7.5 DATA STORED ON THE CHIP

In addition to biometrics, the chip will provide a back up of the passport holder's personal data.

Information backed up or encoded in the chip of an ePassport includes:

- ▶ Passport number;
- ▶ Unique national identity number;
- ▶ Passport holder's full name;
- ▶ Passport holder's mother's maiden name;
- ▶ Colour photograph;
- ▶ Sex;
- ▶ Signature;
- ▶ Nationality;
- ▶ Issue and expiry date of passport;
- ▶ Issuing authority;
- ▶ Date of birth;
- ▶ Minutiae of two fingerprints;
- ▶ Digital signature or hash algorithm.

7.6 ACCESSING THE INFORMATION ON THE CHIP

Retrieval of information stored on the chip of an ePassport involves contactless readers. Access to information is only possible by reading systems explicitly authorised by each state for this purpose. Unauthorised tapping of biometrics during communication between the chip and the reader system is prevented by encryption. For this purpose, a secure transmission channel is established when the connection between the reader system and chip is initiated.

All the communication steps undergo multiple encryptions and cannot be started until the optically readable data of the ePassport has been made available to the reader. In other words, the data exchange process starts when the passport holder gives his or her passport to the border control officer who then places the opened ePassport on the terminal unit. In order to prevent tracking and tracing of data, the access codes and all relevant keys in the ePassport – which are necessary for the communication between the integrated contactless chip and the reader – are different at every new reading process.

7.7 AUTHENTICATION METHODS

The ePassport can use a number of authentication methods, which are either mandatory or optional:

- ▶ Passive Authentication is mandatory. The cryptographic mechanism applied to this process is the digital signature. This provides proof that the Logical Data Structure (LDS) and Document Certificate are authenticated and not modified, but does not prevent 1:1 copying or chip exchange;
- ▶ Basic Access Control (BAC) is optional in many countries, but mandatory in the EU. BAC uses challenge/response mechanisms based on triple DES recommendations. It has the advantage of preventing skimming and eavesdropping via a secure communication, but does not prevent 1:1 copy or chip exchange;
- ▶ Extended Access Control is optional. This uses an additional symmetric key or asymmetric key pair to prevent unauthorised skimming and access to sensitive data and provides additional key management;
- ▶ Active Authentication is optional. This uses a challenge/response mechanism based on public key cryptography and digital signatures. It provides proof that the document is not copied and refers to the correct chip. It also proves the chip has not been exchanged;
- ▶ Data Encryption is optional. This uses a symmetric or asymmetric encryption method and is able to protect sensitive data, but it does not prevent against 1:1 copy or chip exchange;
- ▶ In the EU, fingerprint storage will be mandatory (except in UK and Ireland).

As with many governmental decisions, the optional methods of authentication need to be chosen by balancing the potential rewards (e.g. higher levels of security and integrity) with the potential costs (e.g. lower throughput of passengers and higher implementation costs).

In addition to the various digital security measures mentioned, systems are required which are capable of checking the optical and electronic security mechanisms implemented in the ID documents. The interoperability required is promoted, for instance, through regular interoperability tests by the ICAO during which adherence to ISO standards is checked. At the 6th interoperability test held in Berlin, the focus was, for example, on testing ePassports using commercial readers and verifying certificates in order to ensure the authenticity and integrity of the data stored on the chip. Interestingly enough, 96% of the ePassports were tested with BAC and 36% with active authentication although these are optional measures. Even though the majority of reading devices can read the ePassports used, it became clear that there is still only a limited number of commercial full-page reader solutions.

8.0 LEVELS OF AUTHENTICATION

However secure the passport production and personalisation process is, an ePassport is only as good as the people and the equipment verifying it. As we have seen, new ePassports incorporate several layers of personal data. However, it is not always necessary to use the most technically advanced level of data to verify an individual. Instead, it is about making judgements that balance the need for high levels of security with demand for the speedy processing of passport holders.

The key to verifying a passport holder successfully within a reasonable time frame is to use relevant data from that person's passport. For this to happen, it is important that those responsible for verifying an individual understand what the different levels of information are, how they work and which equipment is needed to identify an individual successfully.

The ePassport has three clearly defined levels of authentication, with level one providing the lowest and quickest level of verification, and level three providing the highest and – consequently – the slowest level of authentication.

8.1 LEVEL ONE MANUAL AUTHENTICATION

Level one authentication may be used in passenger travel as well as the numerous administrative activities for which passports are now demanded. No special equipment is required for this level of authentication. Instead, a visual inspection of the passport will be carried out by the person or organisation charged with verifying the identity of the passport holder (e.g. border control workers, government administrator or bank clerk). For a visual inspection to be completed satisfactorily, clear parameters need to be set so members of staff know what to look for. For example, because the members of staff only use their senses (touch and sight) to verify the passport, they should be instructed to examine aspects such as the colour photograph and the signature recorded in the passport together with some of the overt security features of that passport.

On occasions when security requirements are very low and throughput demands are very high, a decision may be made to conduct only the most basic of level one authentication techniques.

For example, a cursory glance at the photograph in the passport together with touching the profile of the passport cover may reveal enough about the authenticity of the document and its owner for authentication to take place. On other occasions, it may be more prudent to examine in detail the many security features incorporated in the passport.

8.2 LEVEL TWO AUTHENTICATION WITH TECHNICAL EQUIPMENT

While the visual inspection of ePassports marks the first line of defence against fraudsters, level two authentication ups the bar further.

At this point, passport reading equipment is brought into the equation so it can successfully check the optical and electronic part of the ID document. For this to work properly border control staff must not only visually examine the passport for obvious tampering or forgery, they must also use technical equipment and know how it works and how to use it. Accessing the MRZ information is a process that many border control workers are familiar with, and will require little more than the ability to place the page containing the MRZ on the machine reader. Checking further information (e.g. patterns, DAC) and accessing information stored in the contactless chip will require further training.

By using machine technologies to read information stored in the passport, border control officers can ensure the data stored electronically matches the information found on the passport's data page. In addition to basic personal data such as full name, and date and place of birth, the facial image stored on the chip may also be used as a cross check against the image on the passport. Furthermore, any attempted alterations to data stored electronically must result in errors when verifying the machine readable data.

As with all other stages in the rollout of ePassports, machine readers sourced from suppliers should be modular, scalable and upgradeable as well as state of the art and not obsolete.

8.3 VERIFICATION AND IDENTIFICATION

Is your document genuine or forged?	Are you in fact who you claim to be?	Who are you?
Authentication	Verification	Identification

What makes ePassports really special is their ability to authenticate something that cannot be lent, borrowed, stolen, lost or even forgotten: biometric data belonging to one single individual. This level of authentication should be conducted offline or stand-alone and may require specialist training. First, a machine must read encoded fingerprint data that is embedded in the passport. Then, it must compare this data with the live scanned fingerprint of the person claiming to be the passport holder. Although the process is relatively straightforward, border control staff may need training in aspects of verifying an individual's biometric such as:

- ▶ Where should the fingerprint be placed on the device?
- ▶ How should the fingerprint be placed on the device? For example, should the citizen press heavily or lightly? Does he or she need to roll the fingerprint across the device or does it simply need to be placed on the device once?
- ▶ How long should the fingerprint be on the device?
- ▶ How often should the device be cleaned?
- ▶ How should the device be cleaned?
- ▶ How many fingers need to be verified?
- ▶ Which fingers need to be verified?
- ▶ If the fingerprint reader fails to recognise the citizen, what steps should be taken? For example, should he or she be given a second or third chance to be verified? Should a more senior line manager be called in?

In the early stages of using biometric ePassports, it is quite likely that some of the travelling public will have questions about how the fingerprint system works as well as what happens to the data. It is therefore important that as part of a biometric

training process, border control staff are kept fully informed not just about how they should use the technology, but also about how it works.

In addition to border control scenarios, level three verification must also be available to authorised institutions that purchase offline stand-alone identity verification units. These units must include a stand-alone identity verification workstation or hand-held unit, a fingerprint scanner and a smart passport reader. As with border control staff, full training should be given on how to verify an individual's biometric, and procedures should be established to deal with anyone who fails to be recognised by the biometric reader.

9.0 CHOOSING AN INTEGRATOR

Many companies operating in the global market provide systems integration services, and it is not always easy to differentiate between their offerings. Although individual governments have their own set procurement methods that may impact on the choice of systems integrator, it is worth remembering that a company should be selected on criteria such as track record, experience and the ability to work with a variety of different partners from both the public and the private sectors. Considering the unique requirements of a government, it also makes sense to select an integrator with well-documented experience of large-scale rollouts in the public sector.

9.1 RESPONSIBILITIES

The systems integrator should be able to support the government at every stage: from the initial idea through to product delivery and integration. It must be able to meet a clear brief, for example, to provide an automated process that will quickly and securely verify the identity of travellers. In addition, it should be able to adapt its solution to work with existing suppliers while providing cost savings to the government and bringing the ePassport system to market quickly. To achieve this, the systems integrator should be flexible enough to take on a variety of roles that may range from defining and designing platforms and systems to providing ongoing support and training.

9.2 DEFINING THE PASSPORT SYSTEM

It may seem an obvious statement, but rolling out an ePassport system is not going to happen overnight. Think of all the issues involved in deploying traditional passports. Then think of all the challenges associated with adding new technology and new partners. Add to this the numerous other components involved in border management – from passport readers to biometric systems, not to mention complicated back end systems –

and you're close to grasping the technical complexity involved. But it doesn't stop there: you've also got to factor in traditional taxpayer scepticism about whether or not more expensive, high tech documents are actually worth having.

Take all these factors into account and you get an idea of the challenges any government is up against when it attempts to successfully roll out an ePassport system.

It is therefore essential to consider the scope of work required for implementing an ePassport system and to understand the roles and the responsibilities that may be involved for the various parties enlisted to deploy the system.

9.3 SUPPLY AND INSTALLATION OF THE SYSTEM

Whether police stations, municipal offices, passport offices or central government ministries issue passports, a central host system will need to be supplied and implemented. In addition, passport issuing centres and remote centres may need to be established with both the technology and the staff in place to deal with the greater demands of a biometric passport.

The passport enrolment and issuance system can be thought of as two entities. As the use of biometrics in passports moves to incorporate fingerprint technology, so the system will need to comprise system software, a PC workstation, portrait camera, fingerprint scanner, passport printer and someone to input the data.

9.4 SYSTEM COMPONENTS

Of course, the passport may need to be examined by machine at any time, so a passport retrieval system including a PC workstation, verification system software and passport reader are also required.

Blank passport booklets incorporating chip technology will also have to be procured and securely stored.

9.5 PROJECT IMPLEMENTATION

ePassport systems are rapidly becoming a reality. Many government watchdogs and taxpayers are rightly concerned that public money shouldn't be wasted on schemes that do little to beef up a country's border security or improve passenger throughput at airports. With many critics standing on the sidelines, waiting for the rollout of a new passport system to flounder, it is essential that precautions be taken to guard against such an occurrence. The chances of achieving this may be greatly enhanced by rolling out the system in a number of phases, possibly involving the implementation of an initial pilot project before moving forward to a full nationwide rollout.

As most countries have relatively little experience of biometric technology, many are opting to phase biometrics in gradually, and are therefore implementing only face technology in passports in the short term, with many others committing to include the optional fingerprint biometrics at a later date. For example, the new German passport was launched in November 2005. Fingerprints will not be stored in them from November 2007.

Meanwhile, the US Department of Homeland Security (DHS) and the US Department of State were involved in 'live testing' ePassports in Australia and New Zealand throughout the middle of 2005. Drawing on volunteers from airline crew and officials employed by Qantas Airlines, Air New Zealand and United Airlines, the tests – rolled out at Los Angeles International Airport in the US and Sydney Airport in Australia – were established to enable the DHS to test the relevant operations, equipment and software needed for successful verification of the data stored in the ePassport.

9.6 FITTING THE PROJECT TOGETHER

The role of the systems integrator is considered key to the ultimate success or failure of an ePassport project. After all, this is where the nuts and bolts of the project will be put together. So an integrator with real commitment, leadership and experience of secure, large-scale government projects should be selected. The introduction of chip technology is bringing

new players to the table, so it is essential the integrator can establish and maintain relationships between all suppliers, while ensuring that implementation remains on track and on budget – a pretty hard task to achieve!

The systems integrator is directly responsible for defining the overall ePassport system architecture. This is a complex task that requires configuration skills as well as an ability to understand and address the various technical requirements by implementing the most suitable technologies. In the early stages, the integrator may submit a number of prototype ePassports for testing in government systems. The results of these tests should enable government decision makers to form an opinion on which type of ePassport technology to rollout to the general public. The integrator should also be able to define appropriate platforms and interconnectivity mechanisms.

By communicating with its clients, the integrator should be able to define levels of centralisation and appropriate workflow. Here, the integrator should take into account issues such as how a government's bureaucracy works as well as any national data protection requirements.

Depending on the nature of the national civil registry, the integrator needs to consult on how to modernise the existing registry to comply with future requirements such as the introduction of new technologies and online databases. This is a complex task that requires conformity with national laws. Here, security mechanisms such as passwords, smart cards or biometrics may be applied to ensure only those authorised to access the system can do so. Furthermore, parameters will need to be set so different members of staff can access only the parts of the database that are relevant to their particular job.

9.7 ESTABLISH REALISTIC PLANS

Having defined and designed the total system, the integrator should provide an overall project plan and schedule. This is of primary importance for managing the expectations of all stakeholders – from taxpayers to government watchdogs and government workers as well as all other organisations involved in rolling out the ePassport. Many projects fail at this point because integrators provide overly ambitious time frames

that do not take into account the length of the decision-making process within individual governments. It is therefore essential that realistic plans are made and achievable targets are set.

9.8 TRAINING AND SUPPORT

After the system has been installed successfully, the integrator must ensure that government employees are fully trained in all applications of the system. This may include basic data entry as well as more skilled training such as biometric enrolment and system maintenance.

Finally, once the ePassport system has been completely rolled out, the systems integrator should provide ongoing first-line support.

μs – microsecond

One millionth of a second

Active Authentication

Uses a challenge/response mechanism based on public key cryptography and digital signatures. It provides proof that the document is not copied and refers to the correct IC.

AFIS – Automated Fingerprint Identification System

This system is used by law enforcement agencies to compare fingerprints. Instead of performing a one-to-one match, it checks a fingerprint against a whole database of stored prints and gives a list of the most likely owners of that print.

API

Application Program Interface

Authentication

The process whereby an individual, a card or a terminal is checked to ensure that he/she or it is an authorised person or device.

Basic Access Control

Uses challenge/response mechanisms based on triple DES recommendations. It has the advantage of preventing skimming and eavesdropping via a secure communication.

Baud

The number of signalling elements that occur each second. Baud indicates the number of bits per second that are transmitted.

Biometric

Measurable, distinct physical characteristic or personal trait that can be used to recognise the identity or verify the claimed identity of an enrolled person.

Chip inlay

Comprises the chip, the chip module and the antenna and is integrated into the cover or one of the pages of the passport booklet.

CLI

Changeable Laser Image

Contactless card

A card that can be read from a distance instead of being swiped through or inserted into a card reader.

Cryptography

The process of turning readable text into cipher text and back again.

Data encryption

This uses a symmetric or asymmetric encryption method and is able to protect sensitive data.

DBMS

Database Management System

DES

Data Encryption Standard

DIGANT process

This digital application process, developed by Bundesdruckerei, is used to send encrypted data electronically. This has the advantage of providing a secure process that is faster and more convenient than traditional postal delivery.

dtx

Also known as decitex, dezitex or dtex. This is the measuring unit for thread and is the weight in grams of a 10,000m fibre. For example, with a value of 50 dtx, 10,000m of thread weighs 50g.

ePassport

An electronic passport with a contactless chip and an antenna embedded in it.

Endpaper

The front and back inside cover of passport.

Extended Access Control

Uses an additional symmetric key or asymmetric key pair to prevent unauthorised skimming and access to sensitive data and provides additional key management.

FAR – False Acceptance Rate

The acceptance of an impostor into a system being protected by a biometric device. False Acceptance Rate refers to the probability – expressed as a percentage – that a device will fail to reject an impostor.

FRR – False Rejection Rate

The rejection of a legitimate user from the system being protected by a biometric device. False Rejection Rate refers to the probability – expressed as a percentage – that a device will fail to accept a legitimate user.

ICAO

International Civil Aviation Organization

ICAO Doc 9303

The ICAO document that was first published in 1980 containing specifications for machine readable passports.

Intaglio printing

Form of printing that produces a ridged profile detectable by fingertips.

ISO

International Standards Organization

KB

Kilobyte

LDS

Logical Data Structure

Lenticular

When looking at a lenticular image, it is possible to see one image followed by another as the angle or view changes.

MRP – Machine Readable Passport

Key components of the MRP are the holder's identification details, including a photograph or digital image and a two-line Machine Readable Zone (MRZ).

MRTD

Machine Readable Travel Document

MRZ

Machine Readable Zone

OCR – Optical Character Recognition

The two-line Machine Readable Zone in a passport is made up from OCR-B characters.

OS – Operating System

The computer programme that manages all other programmes on the machine.

Passive Authentication

The cryptographic mechanism applied to this process is the digital signature. This provides proof that the Logical Data Structure (LDS) and Document Certificate are authenticated and not modified but does not prevent 1:1 copying or chip exchange.

PIN

Personal Identification Number

PKI – Public Key Infrastructure

A method for authenticating a message sender or encrypting a message.

RFID – Radio Frequency Identification

A method of identification using radio frequency technology, which does not require any direct contact.

RSA

A computing algorithm for encrypting data, named after its inventors Ronald L Rivest, Adi Shamir and Leonard Adleman to provide extremely high security.

SAM

Secure Access Module

Systems integrator

An individual or company that combines various components and programmes into a system and customises them for individual customer needs.

TAG/MRTD

Technical Advisory Group on Machine Readable Travel Documents. A subcommittee of ICAO responsible for the development of Machine Readable Passport standards.

Triple DES

A method of increasing the security of DES by encrypting three times with different keys.

Visa waiver program

Enables nationals of certain countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa.

Watermark

When light shines through the paper of the ePassport's data page, a multi-tonal watermark can be detected.