Diana Ombelli
and Fons Knopjes

DOCUMENTS: THE DEVELOPER’S TOOLKIT

IOM International Organization for Migration

via Occidentalis

Title: **Documents: The Developer's Toolkit**
Editor's: **Diana Ombelli** and **Fons Knopjes**

Publishers: **IOM** and **Via Occidentalis Editora Lda.**
Cover design: **Jaap Drupsteen**

Printing: **EU**
Firts edition: **April 2008**

ISBN [IOM]: **978-92-9068-407-7**
ISBN [VO]: **978-972-8966-44-7**

Via Occidentalis Editora Lda.
http://toolkit.blogs.sapo.pt - occidentalis@netcabo.pt

IOM - International Organisation for Migration
www.iom.int - publications@iom.int

CONTENTS

CONTRIBUTORS

CURRICULUM VITAE

■ Ångström, Nils

Nils Ångström (1942), BSc, is a forensic document examiner. He has worked for the Swedish National Laboratory of Forensic Science in Linköping, Sweden, since 1972.
Contact: nils.ångström@skl.polisen.se

■ Baggeroer, Chuck

Chuck Baggeroer (1944), has over 20 years experience in the field of financial and identity document personalisation. Prior his retirement he worked as a Director of Security Technologies and Industry Liaison for the Datacard Group. Furthermore Mr Baggeroer serves on a number of industrial committees, including ISO/IEC JTC1/SC17/WG3; International Travel Documents, ISO/IEC JTC1/SC17/WG10; International Driver Permits; and the International Association of Financial Crimes Investigators.
He also serves as an advisor to the New Technologies Working Group of the International Civil Aviation Organisation (ICAO). He has provided document examination training to investigative and forensic divisions of numerous national police agencies.
Mr. Baggeroer has BS and MS degrees in Mechanical Engineering from Purdue University and an MS in Business Administration from the University of Minnesota.
Contact: cbaggeroer@comcast.net

■ Baltazar, Isabel

Isabel Baltazar (1967) has been head of the Fraud Unit and Identification Department of the Portuguese Immigration Service in Lisboa, Portugal, since 1993. She is responsible for providing training on document fraud and security documents to police and service forces, consular services and similar entities world-wide. She has participated in the development of new travel documents, particularly the residence permit for foreigners and the portuguese passports, and has been advisor in the use of technical equipment for the detection of fraudulent documents. Not only does she represent Portugal at EU meetings regarding the development of travel documents and fraud prevention, but she is also a member of the Portuguese delegation of ICAO’s Technical Advisory Group. She studied at the “Instituto Superior de Ciências Sociais e Políticas” of the “Universidade Técnica de Lisboa”, taking a degree in International Relations in 1989.
Contact: isabelb@sef.pt

■ van Blankestein, Jan Heim

Jan Heim van Blankenstein (1963) M.Sc. is a senior consultant ICT architecture and information security with Montelbaan Internet & ICT BV in the Netherlands. He graduated in biophysics at the Utrecht University in 1988 concentrating on computer modeling and information theory. After graduation he has been a research fellow at the center for cardiology at the Erasmus University Rotterdam. In 1995 he moved into the ICT business as a consultant for secure messaging and directory technology and in 2000 started Montelbaan Internet & ICT BV. He now focuses on technical and organisational aspects of information security in general and biometrics and PKI in particular. As ICT project manager he was involved in the successful development and introduction of the new Dutch Travel Document in 2001.
Contact: jan.heim.van.blankenstein@montelbaan.nl

■ Broekhaar, Sjef

Sjef Broekhaar (1955) is now a Training Officer and Technical Specialist for the International Organization for Migration, in short IOM (2008), in his previous position he was Research & Development Manager at the Personal Records Database and Travel Documents Agency of the Ministry of the Interior and Kingdom Relations (2002). He is an expert in the field of document research. Previously, he was Programme Manager of the Documents & Payment Crime Programme of the National Criminal Intelligence Division of the National Police Agency (1998). He is the originator and co-developer of the electronic database for the application of international travel documents: Edison TD (1991). He is also a guest lecturer for national and international courses in the field of document research (1983). He is the author of several publications.
Contact: sbroekhaar@iom.int

■ Buursma, Cor

Before his retirement, Cor Buursma (1940) filled a number of positions at Joh. Enschede and Sdu Identification (formerly Enschede/Sdu). He has over 40 years experience in the development of secure documents, including production and personalisation. He was the manager of several departments, such as the prepress and printing department, composing room, identity card personalisation department, and project and product development department.
He set up several production facilities, including a card factory for the production of bank cards and a department for the personalisation of bank and identity cards. At Sdu Identification, he was responsible for the new generation of Dutch travel documents, which included the design and production of the new range and the setting up of a new personalisation process for these documents.
Contact: cor.buursma@wanadoo.nl

■ Cardell, Birgit

Birgit Cardell (1953) works as a forensic document examiner at the Swedish National Laboratory of Forensic Science in Linköping, Sweden. She started in 1986 and is now head of the document group.
Contact: birgit.cardell@skl.polisen.se

■ Chatwin, Charles

Charles Chatwin (1939) is a consultant in security printing and identification. He holds two degrees in chemistry from Oxford University. After a short period in the chemical industry, where he worked on additives for PVC, he spent 38 years in the printing industry in fields ranging from national newspapers to posters. He devoted 27 years of his career to secure documents, first with McCorquodale, then Bradbury Wilkinson and lastly De La Rue, where he was Technical Manager of the Security Printing Division and later Card Systems Division. He was responsible for the development of the De La Rue Fortas card. He was a founder member of ISO WG3, leads its Task Force 2 and also serves on WG10.
Contact: charles.chatwin@btinternet.com

■ Dell, Mike

Mike Dell (1969), MSc, is a senior consultant for information security at Montelbaan Internet & IT BV in the Netherlands. He studied at the Faculty of Mathematics and Computer Science at Utrecht University from which he graduated on a thesis on Key-Escrow cryptosystems in 1995. He started his career in IT as a technical specialist at BSO/Origin. BSO/Origin later became part of Atos Origin where he joined the Adaptive Infrastructure Solutions group as a security consultant and became chairman of security service development. He has been employed at Montelbaan Internet & IT BV since November 2001. He has worked on several large projects in the field of technical infrastructure, systems integration, expert systems, telecommunications, e-commerce and, most importantly, information security and PKI. As an IT consultant, he was involved in the successful development and introduction of the new state-of-the-art Dutch Travel Document in 2001.
Contact: mike.dell@montelbaan.nl

■ Felix, Idius

Idius Felix (1964), MSc, is a management consultant at the Consulting and Project Management Division of Atos Origin, the Netherlands. He graduated in Public Administration from the University of Twente in Enschedé the Netherlands, majoring in organisational issues and change. He is an expert in solving organisational problems and the challenges posed by the developments in and new possibilities of IT and their impact on organisations. He has also participated in several major IT-oriented projects initiated by the central government in the Netherlands, such as the development and implementation of the Municipal Personal Records Database (GBA), the introduction and handling of information security within government organisations and the successful development and implementation of the new state-of-the-art Dutch travel document in 2001. As a management consultant, he supports organisations in organisational structuring and change, information management, IT and information security.
Contact: idius.felix@atosorigin.com

■ Graber, Daniele

Daniele Graber (1966) works as a legal counsellor at the Swiss Society of Engineers and Architects (SIA) in Zürich. He is also currently writing his doctoral thesis at

Fribourg University: “Public procurement of services – Swiss, community and international law”.
After an apprenticeship as a machine draughtsman (1982-1986), he studied at the Hochschule für Technik NTB in Buchs, Switzerland, obtaining the title of engineer in micromechanics (1986-1989). After that, he specialised in Applied Optics and Statistics (1989-1991), working for two years at the IMAC Institute of the Swiss Federal Institute of Technology in Lausanne. From 1994 to 1999 he studied Law at Fribourg University, graduating in 1999.
Contact: graber@sia.ch

■ Knopjes, Fons

Fons Knopjes (1953) is Managing Director of IDManagement Centre an independent, international organisation with knowledge and expertise in the field of identity chains and training. Fons was Research & Development Manager of travel documents at the Ministry of the Interior and Kingdom Relations and worked as project leader for the development, production and customisation of the Dutch travel documents . He also advised in the development of a large number of (electronic) identity and other valuable documents introduced in 2001. He gained much of his experience at the National CID Information Desk of the Dutch National Police Agency, and represented the Netherlands for over ten years in the false documents working group of the European Union. He was also a member of the NTWG (New Technology Working Group) and EPWG (Educational and Promotional Working Group) of ICAO (International Civil Aviation Organisation) and is now member of the ISO WG3/TF3. He is a member of the core group of experts on Identity- related crime of the United Nations. He is also board member of the Dutch Biometric Forum and has both developed and taught various national and international training courses in the field of document investigation. He has numerous publications in the field of identity documents, falsifications, etc.
Contact: fons.knopjes@idmanagement-centre.com

■ Lakeman, Piet

Piet Lakeman (1958) is a Senior Manager for Visa Europe’s Fraud Management Department, London, United Kingdom. Previously, he was project leader for the Universal Classification System for Counterfeit Payment Cards project, which is a public/private cooperation between Interpol General Secretariat, Lyon, France, and the credit card industry. Before that, he was employed with the National CID Information Desk of the Dutch Police Agency. He was also a consultant for the “Fraud Prevention” project group of the European Commission and a consultant for the G8 “Payment Card Fraud” project group. As a consultant, he has been involved in national and international document development. He is the author of numerous publications in the field of card fraud.
Contact:lakemanp@visa.com

■ Meuwly, Didier

Didier Meuwly (1968) graduated from the School of Forensic Science (IPS) of the University of Lausanne in 1993 and obtained his PhD from the same institution in 2000.

From 2004 he works by the Netherlands Forensic Institute (NFI), that is part of the Dutch Ministry of Justice. He is currently principal scientist, in charge of a national research project on forensic individualization based on fingerprint statistics and contributing to the research and education programme of the NFI. Between 2002 and 2004 he was a senior forensic scientist within the Forensic Science Service (FSS), an executive agency of the British Home Office. From 1999 to 2002 he was responsible of the biometric research group of the IPS.

He is also a founding member of 2 working groups of the European Network of Forensic Science Institutes (ENFSI): the Forensic Speech and Audio Analysis Working Group (FSAAWG) in 1997 and the European Fingerprint Working Group (EFPWG) in 2000.

Contact: dmeuwly@mac.com

■ Nordberg, Tommi

Tommi Nordberg (1963) is Executive Vice-President of the Identity Product line of Gemalto. He is also the CEO of Setec Oy in Finland, a wholly-owned subsidiary of Gemplus. He joined Setec Oy in 1998 and has held several key management positions in the company, including responsibility for two business lines, Security Printing and Government & Corporate. He holds a MSc degree from Helsinki University of Technology and a degree in International Marketing from the Helsinki School of Economics. He joined Setec Oy, after having held several positions as project manager and in marketing development at UPM-Kymmene plc.

Contact: tommi.nordberg@setec.fi

■ Ombelli, Diana

Diana Ombelli (1970) works as a project manager at Sdu Identification, a security printer, in Haarlem, the Netherlands. Previously, she was head of the laboratory of this security printer. She worked for three years as a forensic scientist at the Police Forensic Laboratory in Bern, Switzerland, analysing microtraces and specialising in the field of the fingerprint evidence. Later, she was employed by the Swiss Federal Aliens Office where she assisted the project leader of EVA (Electronic Issue of Visa) to award the public procurement of the supply of visa stickers and related hardware.

She was a member of the New Technology Working Group tasked by the Technical Advisory Group of ICAO to study and make recommendations on new technology to be used in machine-readable travel documents. She studied at the "Institut de Police Scientifique et Criminologie", Faculty of Law at Lausanne University in Switzerland, graduating in Forensic Science in 1993.

E-mail: diana.ombelli@tiscali.nl

■ Ponsioen, Paul

Prior to his retirement in 1993, Paul Ponsioen (1942) worked as a project manager for Sdu Identification in Haarlem, the Netherlands. After a technical education he specialised in printing techniques. He filled various positions in the printing industry, one of which was trainer at a Design Training Centre in a developing country. During his career at the Dutch State Printer (Staatsdrukkerij), he specialised in quality assurance

and the development of secure documents, such as cheques, lottery tickets and passports.
Contact: paul.ponsioen@planet.nl

■ Ruiter, Ineke

Ineke Ruiter (1951) is director of the Management Centrum, a centre for strategic implementation management for the public sector, which was founded by the Dutch government in 1990. Ineke Ruiter has carried out several large commissions for the Dutch government. She was deputy project leader for the Municipal Personal Records Database (GBA) project and project leader for the New Generation Travel Documents project in which capacity she was responsible for the development and implementation of the new travel document as of October 2001. As a programme manager she is now responsible for the development and implementation of a new system of unique identity numbers for all citizens in the Netherlands.
Contact: ineke.ruiter@idmanagement-centrum.com

■ Wayman, Jim

Jim Wayman (1951) received his PhD degree in engineering from the University of California, Santa Barbara, in 1980 and joined the Mathematics Department of the U.S. Naval Postgraduate School in 1981. He holds four patents for his early work in speech processing and speaker recognition. In 1986, he became a contractor to the U.S. Department of Defense for biometric and technical security system development and analysis. In 1995, he started the Biometric Test Center at the College of Engineering at San Jose State University. The effort was designated as the U.S. National Biometric Test Center by the Biometric Consortium in 1997 and served in that capacity until 2000. He has over two dozen peer-reviewed publications in biometrics and biometric system testing, is a Principal U.K. Expert to the ISO/IEC SC 37 committee on international biometric standards and is a "core member" of the U.K. Biometrics Working Group, a member of the National Academy of Sciences/National Research Council committee on "Whither Biometrics", a member of the previous NAS/NRC committee on "Authentication Technologies and their Implication for Privacy" and a Fellow of the IEE. He is co-editor of J. Wayman, A. Jain, D. Maltoni and D. Maio, <Biometric Systems: Technology, Design and Performance Evaluation> (Springer, London, 2005) He lives in Monterey, California, with his wife, Kristina, and 3 daughters.
E-mail: biomet@email.sjsu.edu

FOREWORD

Migration management is becoming an increasingly complex area of governance, inextricably linked to issues of economic and social development, human rights, security, stability and regional cooperation.

The ability to address migration issues comprehensively and cooperatively is today a fundamental requirement for responsible national governance, effective international relations and full participation in international or regional institutions.

The challenges facing governments are complex and include: reducing irregular migration, promoting the rights of migrants, protecting the most vulnerable, reducing economic pressures that influence outward migration, and directing regular migration towards strategic national goals.

A major challenge facing governments today is how to improve the reliability and quality of identity and travel documents.

The International Organization for Migration (IOM) subscribes to the view that more secure travel documents make it easier to manage migration processes.

As part of its broader work in helping government partners to strengthen their migration management capabilities, IOM also seeks to improve the quality of travel documents and associated issuance and inspection systems.

This work includes helping countries to critically assess their existing documents and systems; developing new specifications and processes, supporting the development of tender documentation, and managing the implementation of related projects.

In this context IOM identified a need for improved reference materials to assist partners embarking on the process of developing a new travel or identity document.

As a learning tool, this Developer's Toolkit meets this need, providing an overview of the key issues that should be considered in every new secure document development process.

It highlights the importance of the 'security chain,' in which the weakest link determines the overall security the document and addresses issues from the security concept through the logistics infrastructure.

The information and guidance contained in the Toolkit aims to expand the knowledge and facilitate the work of both individuals and agencies involved in developing improved travel and identity documents.

Technical Cooperation on Migration Division

PREFACE

The management and use of secure identity and travel documents, including documents incorporating biometric technology, is an increasingly important and complex issue for States. The management of identity and travel documents has implications for mobility, access to services, security and governance. Managing the issuance and verification of secure documents is now a daily routine world-wide. In particular, verification processes requires that secure documents are highly reliable and easy to check. These requirements can greatly influence the options available in developing secure documents and the associated selection of issuers and producers of security documents.

The development of documents is often viewed as a highly technical process. However, it is important for a range of stakeholders – both government and private – to possess a sound understanding of the basic concepts and processes that underpin the issuance of a secure document. For example, too often reference is made to the identity function of a document without really knowing what an identity is. Similarly, there are often moves to modernize identity and travel documents through the incorporation of biometrics without fully understanding the benefits and limitations of biometric technology in supporting more secure identity management.

Very little reference material is publicly available on the fundamental processes involved in developing a secure document. This gap in reference material challenged two documents specialists, Diana Ombelli and Fons Knopjes, to compile and edit a book about how secure documents are developed. Working closely with a number of respected international experts to document and record their knowledge and experience, this Developer's Toolkit seeks to provide a detailed overview of all topics related to the development and implementation of a new security document as well as to offer some inspiration in setting up a document development project.

The Toolkit is not a do-it-yourself manual indicating step-by-step the way to follow, but represents a reference source, where the manager or developer of a secure document can find tools and ideas to fine-tune their project and the product. Given the great variety in the types and form of secure documents, the editors have concentrated their attention on travel and identity documents. The Toolkit is intended to present an overview of the key issues that should be addressed in every new secure document development process. It covers issues including the security concept through to logistics infrastructure. The Toolkit also highlights the importance of the "security chain" in which the weakest link determines the overall security the secure document.

In summary, this manual is designed to provide up to date technical and managerial guidance on the process of developing new identity and travel documents (including passports) to all interested stakeholders. The Developer's Toolkit is available in English, French, Spanish, Russian and Arabic.

Acknowledgements from the editors

Knowing that a document developer has to cope with a large number of factors when creating a new secure document, the expertise of various specialists was sought. The combination of their expertise, their practical knowledge and acquired experience in the field of secure documents makes this book unique. The editors, Fons Knopjes and Diana Ombelli, would like to especially thank Birgit Cardell, Charles Chatwin, Chuck Baggeroer, Cor Buursma, Daniele Graber, Didier Meuwly, Idius Felix, Ineke Ruiter, Isabel Baltazar, Jan Heim van Blankenstein, Jim Wayman, Sjef Broekhaar, Mike Dell, Nils Ångström, Paul Ponsioen, Piet Lakeman and Tommy Nordberg for their valuable contributions. They are introduced individually in the section "Curriculum Vitae of the contributors" of this book.

The editors are also extremely grateful to Jaap Drupsteen for designing the cover of the Toolkit, John Mercer and Ana Bela Nobre for their review work and comments and Fred Zwarts for his support during the start of this book (2001).

Finally, the editors would like to thank the International Organization for Migration for its support in the translation of this manual into French, Spanish, Russian and Arabic and its publication.

CHAPTER 1

GENERAL INTRODUCTION

1.1 Definition of a secure document

A secure document is any kind of document that has special value to the holder and contains certain data and information, but has the property of allowing, at any given time, the confirmation of its veracity, validity and authenticity as a genuine document issued by a competent authority or organization for that purpose.

The fact that a secure document's authenticity can be corroborated at any given time gives it legal or commercial value to its user and/or registered holder. As such, it is also a legal document because it grants the authorized holder certain rights, such as access or currency value. When used for identification or travel purposes, it is immediate proof of one's legal status, in particular one's identity and nationality.

Two characteristics are essential in the development of secure documents: function and value. These are described in the succeeding sections.

1.2 Function

The specific function of a document must be determined before it is produced. For instance, is the document going to serve as a means of identification or of payment or both? Defining its function is also important because it will determine the standards that a contracting party is required to specify on its requirements list (see Chapter 2, Getting Started).

In the past, secure documents normally had only one function, e.g. that of a banknote. In contrast, today's documents have become increasingly multifunctional. Take the passport for example. It is traditionally a travel document. But now, it also functions as an instrument for identification. In North America, the driving license serves as an identity document in addition to being a proof of driving ability. Attributing various functions to a document would naturally enhance its value. But at the same time, the more functions it has, the more vulnerable it is to misuse.

The shift to multifunctional documents has been made possible by developments in technology, and specifically the graphics industry. A modern printing house is far more advanced than that of 50 years ago. Offset plates have replaced leaden types, polymers have substituted paper, and the layout department is now using "computer-to-plate" techniques. These technological advances are extremely fascinating and have raised the security levels of documents. However, they have also made the development process more complex, requiring more disciplines to be involved.

Although it is possible to define a general method for the development of all types of secure documents, the functional characteristics of each type call for more specific approaches. The approach to be used, among others, is also related to the intrinsic value of the document.

■ 1.3 Value

Secure documents can be categorized based on their value, whether it is monetary and legal (van Assem et al, 1994). Such value, which a document user is often unaware of, requires a fitting level of security. The risks and consequences of fraud associated threats to any document will determine which security level to assign.

Figure 1-1 groups the known types of documents into categories. Category 1 documents are manufactured with customized materials in a secure environment and their issuance is registered. Category 2 documents could contain some basic security features. Category 3 documents have (private) value for the owner and are seldom protected by features which could confirm its veracity.

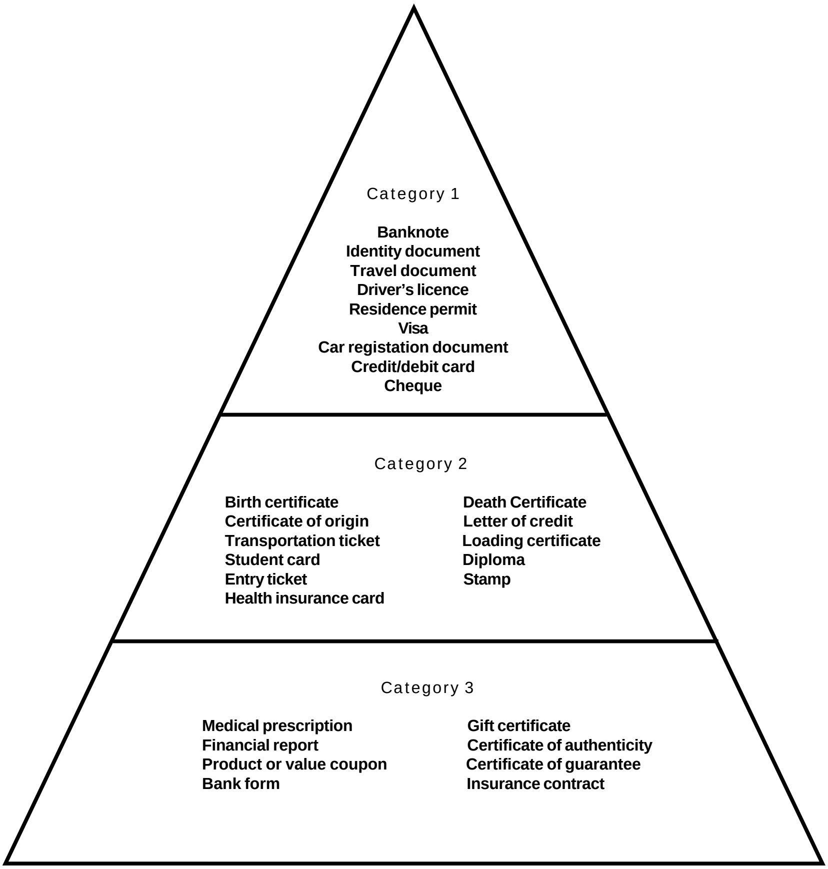


Figure 1-1: Document categories

■ 1.4 Means of securing a document

There is no single definitive method to protect documents against fraud. Fraud protection is a process that needs constant updating and can only be achieved by combining different security features, the effect of which may only temporary.

Choosing which security features and the combination of security features to use depends on the security level assigned to the document. Apart from fraud risk, the security level is also closely related to the document's authentication process. The persons involved in this process and their level of knowledge for verification often determine the combination of security features to be used (see also Chapter 2, Target group). A banknote, for example, needs control points for:

- ordinary citizens
- shop assistants
- bank and postal personnel (including central bank processing)
- forensic examiners
- the producer.

Similarly, a travel document can be examined by:

- airlines and travel agents
- personnel of hotels and shops
- police
- border control authorities
- forensic laboratories
- the producer.

In each case, document verifiers must be sufficiently informed of security features. Anyone who inspects a document, regardless of the level, needs to know how the genuine document looks like and what to look for when examining the document.

The extent of knowledge of the examiner, however, normally corresponds to the pertinent security level.

There are at least three security levels to which document experts often refer to:

- Security Level 1 involves ordinary citizens. The document can be examined by the naked eye. Obvious security features include watermarks, security threads, diffractive optically variable devices (DOVIDs), and the characteristics of the paper used (its feel and sound).

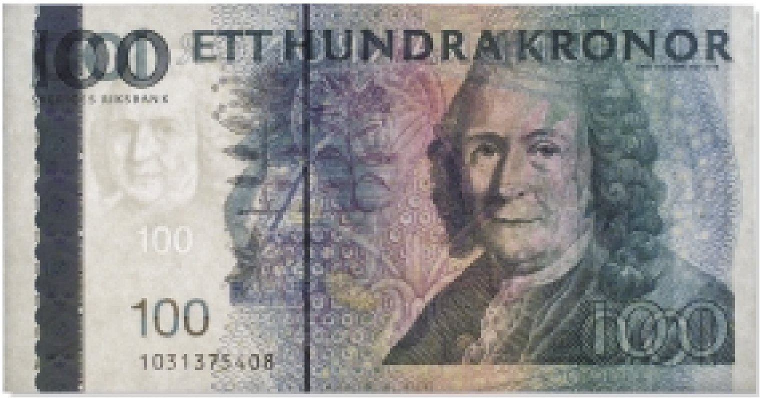


Figure 1-2:
Example of a watermark on the 100 Swedish crowns banknote

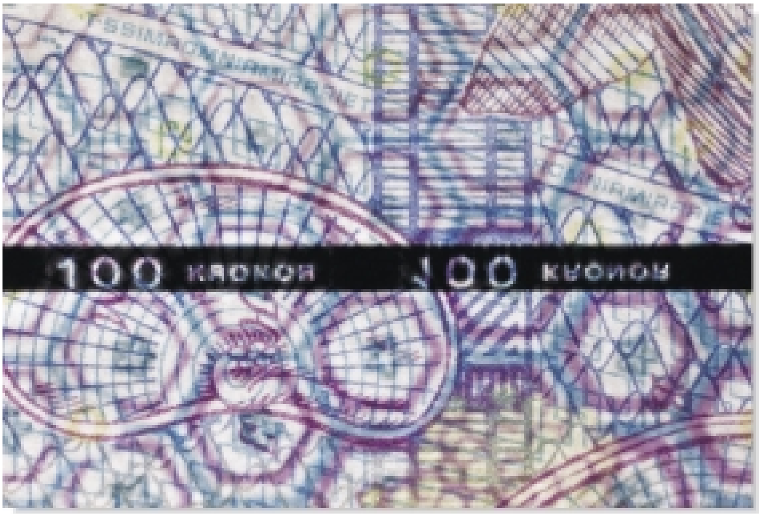


Figure 1-3:
Example of a security thread on the same banknote as in Figure 1-2

- Security Level 2 requires basic equipment, such as a magnifying glass or an ultraviolet lamp (black light). Features at this level include extra small printing (microprinting) and inks or particles (e.g. fibres) that react to ultraviolet light.

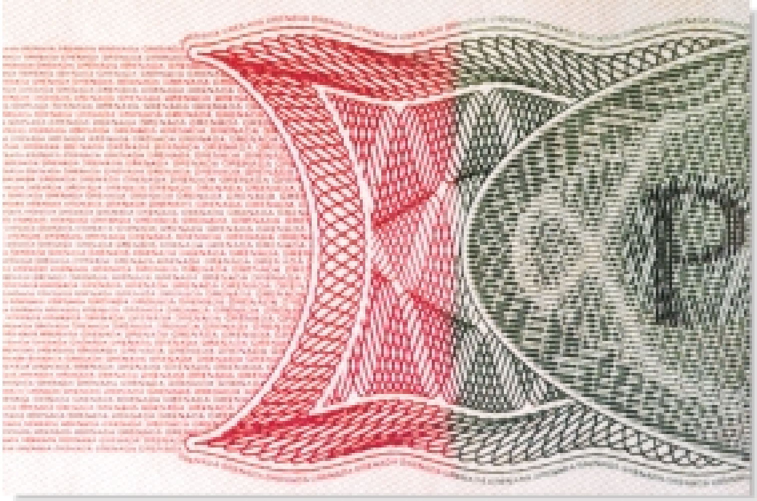
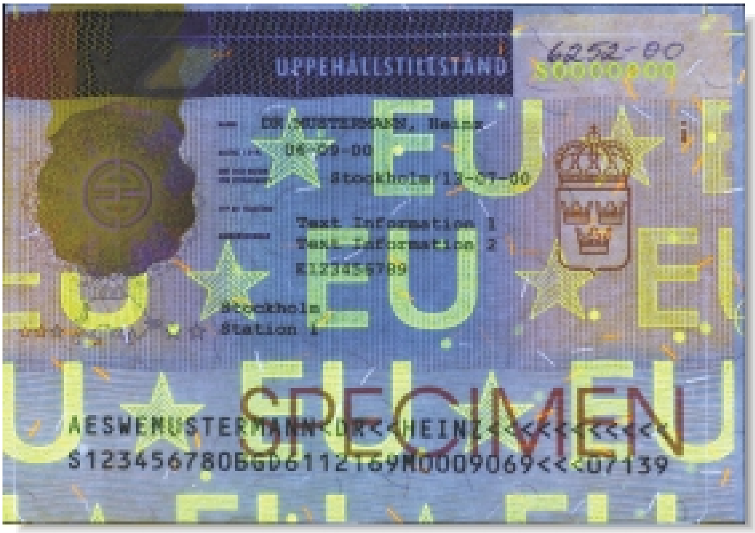


Figure 1-4:
Example of microprint



UPPEHÅLLSTILLSTÅND

6252-00
S0000000

DR.MUSTERMANN, Heinz
06-09-00
Stockholm/13-07-00
Text Information 1
Text Information 2
E123456789
Stockholm
Station 1

SPECIMEN

AESWEMUSTERMANN<DR<<HEINZ<<<<<<<<<<<
S12345678OBGD6112169M0009069<<<07139

Figure 1-5:
View of the UV fluorescent print on a European residence permit

- Security Level 3 features are confidential and require access to more sophisticated equipment, such as microscopes, infrared sensitive light equipment or a laboratory for verification. At this level the producer could add features that could confirm if a particular product was manufactured at its own premises.

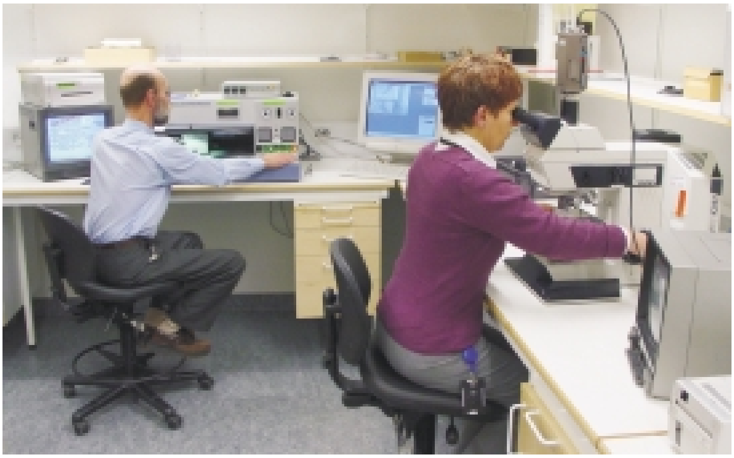


Figure 1-6:
Using a microscope and infrared sensitive equipment
(Courtesy of the Swedish National Laboratory of Science in Linköping)

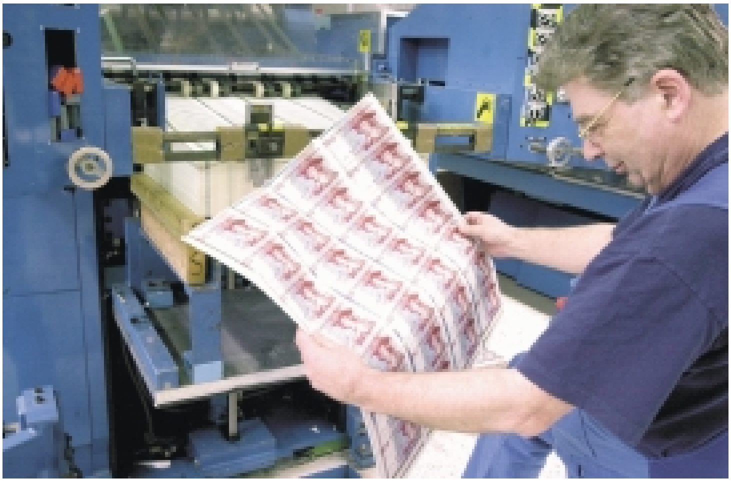


Figure 1-7:
Product control at the press (Courtesy of Setec Oy of Finland)

First-level security features are extremely important because the wide public can quickly examine them without using any tool. In reality, however, too many Level 2 security features, which require the use of tools to determine their authenticity, are currently being developed. Although a wide range of tools, such as lenses, lamps and filters, are available on the market, document inspectors must have access to them to effectively examine a document. And even with access to the appropriate tools, a document that contains a myriad of complex security features is difficult to authenticate. An examiner generally has little time to inspect documents and might restrict himself to the security features that are the easiest to verify. Hence, producers should consider these restrictions before adding too many security features.

This is a good argument for the development of limited but high-quality authentication features. The dissemination of information on such features, however, must be balanced and guarded. Cloaking these features in secrecy is not conducive to alert the interested public but providing information must not also facilitate counterfeiting. As for professional users (e.g. financial institutions), knowledge can be enhanced by in-house training, which could also deal with the verification of Level 2 security features.

■ 1.5 The secure document chain: the high-level description

The development and use of a secure document are integral parts of a larger chain. Since a chain is only as strong as its weakest link, a secure document normally goes through the following phases:

- application
- production
- issuance
- use
- withdrawal.

1.5.1 Application

There are different ways to apply for a secure document. One may apply in person, at a counter or by post. With identity-related documents it is crucial that an applicant's identity is verified by using an original document or its copies (see Chapter 4 for more details).

As the photo beneath shows it's not always technology. Trusted authority and the verification of someone's identity in person by a trusted authority are the basics for securing the integrity of a document.

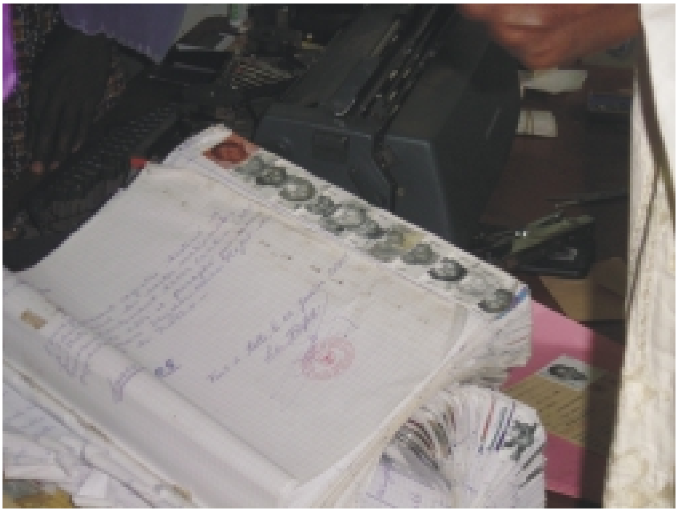


Figure 1-8:
Example of an administration on Identity cards (anno 2006)
(Courtesy of IDManagement Centre, the Netherlands)

1.5.2 Production

Highly secure documents need to be developed and produced in a secure environment using materials specifically developed for their manufacture. Quality and quantities must also be checked during the entire production process.

1.5.3 Issuance

Some secure documents are personalized after production. This means that variable information is added to the generic document: e.g. personal data, issue date, place, authority, etc. Quite often, documents are issued at a different location than from the production site.

Furthermore, other issues also need to be looked at. In some cases the recipient of the document is also the user of the document (e.g. passport).

Moreover, the issuing authorities must be considered. Who are they and how do the application and issuance processes take place? Is the document immediately issued after personalization or are there intermediate phases?

1.5.4 Use

During this phase the document is in the hands of the users, which may complain to the issuer and the producer. This information should be collected and analysed before a new generation of this document is developed. Also, it must be noted that a document developer often loses contact with the developed product itself, unless he acquired a personal experience with it.

1.5.5 Withdrawal

Secure documents can be withdrawn from circulation for a variety of reasons such as wear (e.g. banknotes). They can also be replaced by a new edition.

■ 1.6 Defining the process

In order to avoid ambiguity, the term “gestation process” refers to the creation and implementation of a new secure document. The term

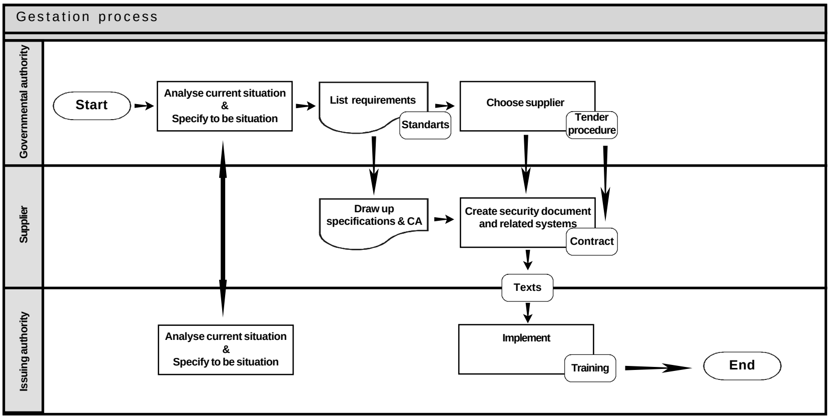

Gestation process
Governmental authority
Supplier
Issuing authority
Start
Analyse current situation & Specify to be situation
List requirements
Standarts
Choose supplier
Tender procedure
Draw up specifications & CA
Create security document and related systems
Contract
Texts
Analyse current situation & Specify to be situation
Implement
Training
End

Figure 1-9:
Gestation process

"development process" describes only a part of the gestation process. Figure 1-9 illustrates a typical situation where three parties are involved in the gestation process of a government issued document: the government authority (usually one or more ministries), the supplier (producer or system integrator from the industry) and the issuing authority (executive government entity, e.g. police or passport office).

■ 1.7 Ensuring quality

1.7.1 Quality qualification of companies

There are two main indicators of quality management in business environments: ISO 9001 and certification programs.

A. ISO 9001
The ISO 9001 is a fee-based universal standards program for quality certification. Following a threshold model, programs for excellence aim at improvements to meet these thresholds or target levels. They are based on periodical measurements (self-evaluation), and involve all stakeholders (customers, employees, management, suppliers, etc.).

The purpose of the ISO 9001 standard is to help organizations implement and administer their in-house quality management systems. Management, within an ISO 9001 certified company, is required to ensure standards and conformance at all stages of the production process. These stages include conceptualization, development, production, installation, and after-sales services and should be described and documented in the quality handbook, i.e. the company's manual for the quality management. Policies, targets and the quality system, which includes organizational charts, procedures[1] as well as operational procedures and instructions or work procedures (Maniak et al, 1997) should also be described in this handbook. A company with ISO certification will have its quality system audited on a regular basis by external auditors.

[1] Procedures can be defined as a specific way to accomplish an activity (ISO 8402).

B. Certification programs

The Brussels-based International Confederation for Printing and Allied Industries (INTERGRAF) has developed two certification schemes for security printers and suppliers.

The CWA 14641:2003 (CEN Workshop Agreement) Certification for Security Printers provides them with well established criteria to execute efficient and secure management systems with precise auditing processes to certify their compliance.

The CWA on Security Management System for Secure Printing, on the other hand, aims at certifying printers based on specifications agreed upon by partners in the industry: printers, customers, suppliers and public authorities (see CWA 14641:2003). Intuitively, the words security, reliability and quality belong together. The fact is that they are tightly linked in the document chain. Particularly in the governmental inspection environment, security and the reliability of a secured document is based on the quality of the product: poor quality could raise the suspicion of fraud.

1.7.2 What does quality mean?

Quality can be understood by taking cues from industry and business. In an industrial setting, the concept of quality is used in order to characterize a product and manufacture it consistently. From the consumer point of view, quality is often a subjective characteristic. Many quality experts tried to rationalize this subjectivity. Harvard Business School Professor David Garvin, for example, separates quality into eight dimensions: performance, features, reliability, conformance, durability, serviceability, aesthetics, and perceived quality. Customers very seldom talk about all eight dimensions. Usually they focus on one or two that are the most salient to them (Flower, 1990).

Of these, the dimensions applicable to security documents are the following: conformance, features, reliability, durability, perceived quality and aesthetics.

Conformance is the extent to which the security document obeys the rules set by international norms.

Features are, of course, the security features which protect the document from fraud.

Reliability can be described as the degree that people accept it for the purpose it has been produced.

Durability refers to the document's capacity to withstand the standard conditions of usage during an agreed period of time.

Quality in a security document can be determined by various elements such as the sharp details of the printing or of the watermark, the steadiness of the paper and/or the neatness of the binding of a passport booklet.

Last but not least, *aesthetics*, because as the saying goes, "there is no accounting for tastes".

A variety of experts, including Garvin, have refuted the myth that quality costs money. If processes are analysed and redundant steps eliminated or made more effective, costs will be reduced. Higher quality, therefore, can mean lower costs (Flower, 1990).

After having defined what quality is, it is essential to know how to measure it. A combination of process management and product-related control instruments can be used to measure quality. Tools considered for process management include the reviews, walkthrough or the Plan-Do-Check-Act (PDCA) cycle. Originally developed by Walter A. Shewhart and popularized by W. Edwards Deming in the 1950s, the PDCA cycle is an instrument that helps identify variable sources that can cause products to deviate from what customers want and expect. It recommends that business processes be placed in a continuous feedback loop so that managers can identify and change the parts of the process that need improvements. Product-related control will be detailed in Chapter 5 (see 5.3 Materials and 5.4 Personalization: Process and techniques).

■ 1.8 Overview of the next chapters

In the following chapters, steps and important issues in the development process of a secure document will be thoroughly explained. Chapter 2 describes the preparatory activities, such as (fraud) analysis, drafting list of requirements and project organization. The standards related to secure documents will also be presented. Chapter 3 is devoted to the choice of supplier: from the tender procedure right up to the contract. Chapter 4 describes the elements forming the document chain.

In Chapter 5, all aspects related to the development of the physical security documents are described: materials and design, personalization process and techniques, testing and production. Chapter 6 will offer more in-depth knowledge about identification. Chapter 7 provides an overview of the link between documents and people through the use of biometrics. Chapter 8 explains the process of digital identification. Finally, Chapter 9 includes a wide range of sources of information and describes cooperation schemes as well as training elements.

References

2006 European Foundation for Quality Management, http://www.efqm.org, Brussels.

Flower, J.,
1990 "Managing Quality", *Healthcare Forum Journal*, Vol. 33 (5);64-68, Sep-Oct.

Maniak, R. et al.,
1997 *Marketing industriel*, Nathan, Paris.

van Assem, B., Brongers, D. *et al.*,
1994 *Sterke papieren, Praktische gids in de wereld van beveiligd drukwerk,* Sdu Publishing, Koninginnegracht, The Hague.

CHAPTER 2

GETTING STARTED

■ 2.1 General assessment

Strengths, weaknesses and potential risks can be detected in a structured way by conducting assessments. Detailed analysis during the development phase of a document will gain timely recognition of these risks during the development process and provide information on the type of risks. This methodical analytical approach also enables the detection and anticipation of possible bottlenecks and threats.

The sources of information to be collected depend on the type and functionality, of the product to be developed. They could be close to the source, such as the producer's work floor, the relevant governmental authority, or the issuing authority. "Closed sources" are equally important because they can provide information that is often confidential and inaccessible to the general public. Closed sources include the police, customs and immigration services.

Sources of information can also provide specific detail on sub-products. The Hologram Image Register, for example, protects Optical Variable Devices producers, who are associated to the International Hologram Manufacturers' Association (IHMA), against forgery, and awards copyrights to their OVDs (see Chapter 9).

In general, any assessment should supply insights into the following aspects:

- Function
- How and how often will the document be used?
- How will the document be stored or carried?
- In which environment will the document be used?

- What is the climatologically environment - cold and dry or hot and humid?
- Desired lifespan
- Extension of validity or substitution
- Target group
- Methods of authentication
- Application process
- Issuance
- Inspection circumstances

2.1.1 Function

How a document is developed depends on its function. This raises a number of questions. For instance, will the document function as a means of identification, a means of payment or as ticket to an event such as a pop concert? If the document is to be used as a means of payment, bank standards will have to be met. If the document only functions as visual evidence, as in the case of a pop concert ticket, recognition is very important. Moreover, a distinction will have to be made between the recognisability of a document and the readability of the document holder's data.

Documents can have different functions:

- carry monetary value
- determine identity
- grant authority
- prove ownership
- grant access.

Documents with monetary value include banknotes, cheques, debit cards, stamps, gift vouchers, bank guarantees, and credit cards. Meanwhile, documents that determine identity are used to verify the identity of the holder. These include national identity cards, passports, alien residence permits, and, in some cases, driving licenses.

If the document is the type that grants authority, it can serve as evidence that the holder possesses certain qualifications granting them the capacity to perform certain tasks. Such documents include diplomas, permits, driving licenses, pilot licenses, taxi licenses etc. Certain documents can also prove ownership which make them even more valuable. Examples of these are land registry documents, title deeds, vehicle registration documents, and legal deeds.

The last category, which grants access, is often important in the private sector. These types of documents can grant access for example to premises, computer files or social services.

Function of a document

Passport
The passport is an internationally recognized travel document that guarantees the identity of the holder. It enables the holder to apply for a visa for those countries that require it upon entry. It also allows the authority to annotate the passport, and record entry and exit dates. In some cases, the passport serves third parties as a means of identifying the holder either inside or outside the third parties' territory.

Banknote
The banknote is a legal means of payment officially issued by a central bank, and serves as a means of exchange in the transfer of property or acquisition of services. Vital to its use is the trust the public puts in the integrity of this medium. This trust is based on the central bank's sound issuance policy and on the authenticity of the notes in circulation.

2.1.2 How and how often will the document be used?

A document is prone to wear and tear each time it is used. For instance, the document can be abraded and flexed when it is inserted into a reading device. The more the issuer can advise potential suppliers about probable use, the better they can respond with cost-effective solutions.

2.1.3 How will the document be stored or carried?

The combination of continual flexing and abrasion will be demanding on the makeup of any document. Small format documents (e.g. ID1, see section 2.6 Standards), subjected to conditions or frequent use, might need a protective sleeve.

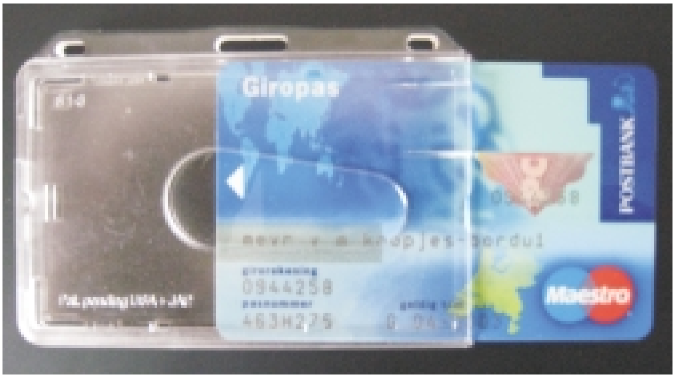


Figure 2-1
Example of a sleeve to protect a bank card.
(Courtesy of Fons Knopjes, the Netherlands.)

This question will also gain in relevance as documents increasingly use machine-readable technologies.

2.1.4 In which environment will the document be used?

Environments can be distinguished as follows:

- closed environment: document is used in one organization only;
- hybrid environment: document of one organization may be used in other organizations;
- national environment: document applies at the national level;
- international environment: document applies worldwide.

Where the document is used?

Passport

At the border control, the passport is handled by a select group of document inspectors with wide knowledge of current travel documents. If an inspector has doubts about the authenticity of a particular document or about the identity of the holder, specialist tools and expertise should be available in the back office. In other situations, the passport may be used by third parties to determine a person's identity. This is a group of users with presumably less experience in assessing the authenticity of the document and the data it contains. As such, the document should effectively facilitate the use of either group.

Banknotes

Banknotes are documents that serve the general public. This group of users is therefore large, diverse, and has little knowledge of the documents. Moreover, there is often little time to carefully examine the banknotes, and only simple tools are available to dispel doubts about their authenticity. Banknotes are impersonal and can be stored in various conditions because they often change hands. Great demands are made on the first-level features which must be durable and understandable. The issuing authority must therefore make a special effort to inform the general public of these features.

2.1.5 What is the physical environment – cold and dry or hot and humid?

Current documents must be able to withstand all kinds of extreme climatic conditions. Extreme heat and humidity attack card structures differently than low temperatures. It is important that all the environments the documents can be subjected to are accounted for, analysed and included in the list of requirements.

For instance, a document that at one moment is taken to Alaska, where temperatures of minus 40 degrees Celsius are common should also be able to be taken to a tropical jungle, where temperatures can reach 40 degrees Celsius and where there is high humidity. Fully defining the various environments where a document needs to be used will better inform choices, in terms of material, design and security of the document, to the customer.

2.1.6 What is the desired lifespan?

Different materials and construction techniques offer varying levels of durability, which can also impact on costs. In general, a card with a long service life is more expensive than one with a shorter lifespan. It is therefore important to determine whether the document will have a long or short lifespan. An identification document valid for a one-day or one-week event may need to be secure, but not necessarily durable. On the other hand, investing in more resistant materials may counter the costs associated with the replacement of failed or worn out documents.

The minimum requirement for secure documents is that they last as long as the event for which they are intended. Documents that are designed to identify the holder often have a longer lifespan. A lifespan of five years is quite common for an ID card. Some countries assign their identity documents for more than five years, some even for a lifetime. Long life spans can hamper the effective control of the personal data of the document holder in determining if the person on the document is identical to the user. A holder's appearance can considerably change over five years, and even more so over a period of ten. The commissioning authority, therefore, must weigh the choice of materials and techniques against the risks attached to long-life documents and the expense that comes from reissuance at shorter interval.

The use of biometric features is a special case. Some encoded biometric features, e.g. facial features, are liable to change. But if they are contained in static storage devices, then the document can only be valid for as long as the biometric feature applies. If the biometry needs to be updated, then a new document must be reissued.

Additional issues that have an impact on the lifespan of a document include the technical design of a document, the techniques applied as well as how the document is treated. From an economic perspective, a commissioning authority may find longer lifespans more advantageous, whereas a producer may wish to limit them.

In sum, there are a variety of factors to be considered apart from cost. For this reason, deciding on a document's lifespan can be complex.

2.1.7 Extension of validity or substitution

One important question is the possibility for a document to be extended after it has been issued. Another issue is whether a document should be replaced after certain period. The answers depend on the purpose and the desired validity of a document. After several years, a document is often technically obsolete. Moreover, the usage frequency of a document is also an important issue. In some cases, it is less expensive for both the issuing party and the user to extend a document than to replace it. This, however, does not hold true for machine-readable travel documents because the validity of information (date of expiration) is included in the Machine Readable Zone (MRZ) and can't be updated reliably in the document.

2.1.8 Target group

Target groups of secure documents vary. In principle, any citizen of a state may avail of a government document while specific groups can obtain certain documents issued in the private sector. Identifying the target group is important because only then can an organization effectively assess the numbers, security level, trends, and risks involved. For instance, certain documents may invoke different attitudes from different users. Some may find them a nuisance, others a source of pride. To illustrate, the users of a police pass are often proud of their IDs and subsequently take good care of them.

Target group

Passport

A passport is made out to the name of the holder. While the holder enjoys the conveniences of the travel document, he is not the only user. The main stakeholders are the internal and external border officials. However, a travel document may also be used by a third party to determine the identity of the holder. For example, a passport can serve to establish the identity of a customer with whom a third party is about to enter into an important financial or legal transaction.

Banknote

The user of a banknote is usually the owner until the moment the banknote changes hands. Similarly, the receiver of a banknote is also a user. These documents are used as a general means of exchange, which requires an important level of reliability. They are issued by a central bank, which ensures their reliability and proper circulation so their use in society is guaranteed in terms of quality and quantity. The central bank also holds the copyright for banknotes.

2.1.9 Methods of authentication

Security features incorporated into a document should reflect the authentication environment. Will online authentication be available? If so, data authentication can reduce the need for some physical security features.

2.1.10 Application process

There are numerous ways to apply for a document. Each method has corresponding restrictions depending on the type of document. Certain applications may be submitted by natural or legal persons. They may be done in person, but also on behalf of a person, and either in writing or via the Internet or telephone (see Chapter 4, section 4.3).

2.1.11 Issuance

The issuance procedure, which may range from local or regional to centralized, can affect an applicant's choice of a certain security document. (Chapter 4 discusses the application and issuance procedures in more detail.) These processes largely determine the product requirements, which in turn influence the choice of a particular producer.

2.1.12 Inspection circumstances

It is necessary to gain an overview of the circumstances in which control takes place. There is a huge difference between verification of an identity card in a post office, which has better conditions (in lighting, references, and front and back office support) than in a bar which is usually poorly lit and where the personnel is often distracted. Such control conditions influence the choices that are made for determining the characteristics of a document.

■ 2.2 Fraud risk analysis

2.2.1 The enemy

The availability of computers, printers, scanners and other sophisticated equipment has facilitated illegal attempts to imitate, alter, complete or transform documents so they appear authentic. The credibility of a false document depends largely on the degree of its resemblance to the original. Well known paintings and their copies are a case in point. As far as documents are concerned, resemblance is based on shape, colour, the materials used and the control circumstances. It is like comparing euro coins from two different countries, which are identical on one side and customized for each country on the other side. The forger that produces an average false document tends to imitate the more evident characteristics and avoids the more complex ones.

In order to keep abuse or infringement of documents at bay, it is important to analyse the criminal factor, especially with respect to documents that are politically sensitive or could severely damage the reputation of an enterprise. An analysis of these threats will enable producers to take appropriate measures to reduce risk. In order to isolate them, documents must be regarded in a much broader context. For instance, criminals could exploit threats involved in transport, issuance or sale of the documents. In such cases, measures should not only be made to prevent alteration of the document itself. Rather precautions must be taken in the transport or pre-issuance stage. Procedures can also be tightened.

Document abuse may also be influenced by political developments. The liberalization of the labour market among the member states of the European Union is an illustration. Legislation dictates that all EU citizens have the right to work in any other member state. However, before a citizen may be admitted to the labour market, a potential employer must first establish whether the citizen concerned is indeed a European subject. This requires a passport or an identity card that specifies both identity and nationality. It goes without saying that the liberalization of the labour market has increased the value of European passports and has prompted criminals to traffic in these European documents.

A document's application or purpose in everyday life also affects the ways in which it can be abused. Some documents are abused more often, more quickly and more easily than others. Insight into the forms of abuse may be gained from analysing counterfeit or forged documents. Conditions under which documents are counterfeited or forged are also worth investigating.

2.2.2 Analysing the chain

Threats may be detected early by conducting a fraud threat analysis before embarking on the development of a document. Document developers and contracting parties need to know which threats may affect a particular document, and if it is vulnerable to certain forms of fraud.

An analysis should therefore be conducted on the various links of the document chain. For example:

Where are documents stored?

Are the stored documents checked?

Is there a division of tasks between the employees that handle the documents?

If application fees are due, who oversees this?

Are the procedures involved required by law or do they merely serve as administrative guidelines?

Are all the rules relevant and applicable to the development of the new document?

The various aspects of the production process and materials to be used also determine the risks involved. Ideally, the production process should be divided into separate stages. Production rooms must be separate and secure, and verification stages must be built into the production process. Through compartmentalization, producers reduce the risks of abuse of the production machinery. A document produced in a poorly secured and ineffectively controlled production environment rapidly increases the risk of theft of materials and end products.

Production personnel should also have an appropriate attitude and be aware of the value of the documents being produced. In some cases, the commissioning authorities make special demands on personnel, e.g. requiring that their references are checked before involving them.

If production occurs at more than one location, and materials and parts have to be transported, the level of risk increases. Transport in itself involves risk, and the control at the issuing location involves more. This is especially the case with documents that have monetary value (e.g. lottery tickets) or ones to be used as identity documents. As long as these documents are blank and still free from personal data, they remain very attractive to criminals. For this reason, it is necessary to store and supervise these documents on the basis of the "four eyes" principle, also known as "two-person rule".

People using fraudulent documents

The use and abuse of fraudulent documents are not a means in itself. They are usually means to perpetrate more serious crimes. They are used first, to achieve a final target which lies beyond gaining access to a certain area or region, and second, to succeed in defrauding the security patterns put in place by governments as part of their mission to protect national sovereignty.

These documents are manipulated to hide a certain identity in order to obtain a genuine document, or to adapt given data on a document to make it consistent with the story behind the new identity. This transformation can be done directly, by means of mechanical erasure, chemical baths, digital software or unofficial reproduction processes. It can also be done indirectly, such as by resorting to bribes, manipulating the weaknesses of each system and exploiting ethnic and physiognomic similarities among individuals. In short, the threat resides in the document's vulnerability to manipulation; granting a right that would normally be denied.

2.2.3 Ways to forge or falsify documents

A document can be copied or manipulated in many different ways. As a result, every document has to be protected against various kinds of misuse.

The following are the main types of fraud:

- *Counterfeits*: The reproduction of a relatively new document from similar or completely different material and potentially simulates the genuine security features.
- *Forgeries*: Changes made to the content of a genuine document. This could involve photograph substitution, changes to personal and/or value data or page manipulation, e.g. page swapping.
- *Unauthorized issuing procedures*: The unauthorized personalisation of a genuine non issued blank document.
- *Misleading the issuer*: The obtention of a genuine document based on false pretenses.

- Look-alike: an individual who assumes the name or identity of another individual (living, dead or fictitious) in order to fraudulently obtain a legitimate identity or travel document.
- Alternative documents: Documents that are produced, issued and delivered by non-existing or unrecognized organizations, or in the name of countries that no longer exist.

Counterfeit documents come in different types, from a simple copy without attempts at simulating security features to excellent ones with good imitations of paper, print and security features. This is where the importance of good quality in the genuine document becomes apparent. If the genuine document is of poor quality, it could be difficult to distinguish it from the false one.

With forgeries, there has been a steady shift to more sophisticated manipulations of genuine documents in recent years. Simple and easily detectable photo substitutions have become rare and have been replaced by more skilful and advanced techniques. There are different ways to change information on a document such as using mechanical erasure techniques to remove the original information; using chemicals or a combination of the two techniques. An elegant alternative is to incorporate parts of another genuine document (e.g. a page or laminate) into a document, which makes it more difficult to detect the manipulation.

It is very difficult, on the other hand, to detect improperly issued documents because their material is genuine. Therefore, it is recommended to add an extra attribute during the issuing process or use a personalization technique which offers uniqueness.

If a person obtains a secure document under false pretences by presenting false identity documents, it could be difficult to trace this at a later date. Every country should, therefore, aim to introduce a security level in identity documents as they do in passports. These identity documents include birth certificates, identity cards and other personal identification papers.

A look-alike document is a genuine document without manipulations, but is carried by the wrong person; an imposter. The only way to expose this is by applying relevant screening procedures and/or biometric checks.

The look-alike strategy has probably gained in popularity in recent times because identity and travel documents are more difficult to counterfeit or alter. However, it is difficult to ascertain just how serious is the problem. It may be assumed that the actual figure is much higher because of the difficulty to detect look-alikes without digital biometric border control equipment.

Alternative documents may either be fantasy or camouflage documents. These documents resemble a secure document, particularly passports, but come from an incompetent or unrecognized organizations. Although they are not an acceptable proof of either nationality or identity, they emerge often enough to be listed as a threat. Only updated information and training can help detect and effectively combat this type of fraud.

2.2.4 Countermeasures

In a steady effort to improve the document's response to the continuing technological developments in this field, the high figures for forgeries and counterfeits have been countered by the incorporation of a variable but balanced number of security features. In parallel, routine-breaking procedures aimed at thwarting forgers have proven to be more efficient. Examples are the successive introduction and circulation of different generations of documents. But this sword cuts both ways. While new better documents are better, change upon change can cause confusion and fatigue among document inspectors.

Additional measures are pre-boarding checks, which enable the pre-screening of documents and people, or the deployment of liaison officers at risky points of embarkation. The dissemination of concise, precise and timely information by a competent entity is also an effective weapon in the fight against document fraud.

While the risks of alteration and counterfeiting are declining, because production methods are easier to analyse and therefore more effective, the abuse of genuine documents has risen. This fraudulent tactic either involves the use of someone else's documents or the acquisition of genuine documents by means of fake supporting documents or corrupted procedures. Examples of this are the use of a birth certificate of a deceased infant, or the modern crime of identity theft, i.e. the theft of electronic personal data belonging to another individual. These impostors use lower-value false documents to obtain legitimate high-value ones.

Counterfeiting cannot simply be resolved by introducing additional security measures. Excess information on a document makes it difficult to pick out the essential security feature and can therefore lead to the false authentication of a document. For example, if during a quick check everything points towards the existence of a given security mark – watermark, intaglio, etc. – the tendency is to validate a document on that mark, without conducting a detailed check on the document nor the data it includes.

Validation of a document as a physical object is not a sufficient guarantee of ownership because anyone can be the holder of a document, but only one person has a real and inseparable connection to it. Therefore, it is necessary to analyse the profile of the document holder. It is very important that an individual's behaviour and psychological make-up is observed and interpreted, thus avoiding an analysis merely based on the observation of the document. The document exists in a context and that context should be included in the assessment of a document's authenticity.

All of the cases referenced are difficult to detect and investigate because when collecting the evidence other factors come into play, namely:

- the vulnerable issuing processes of identity documents;
- the inadequate rules on the storage of secure documents;
- the decentralized means of delivery of the documents to the applicants (dispatch by post);
- the present rules on airport facilitation, which demand faster controls to respond to the ever growing movement and displacement of people around the globe.

A consequence of the globalization of the world economy is the increased number of passengers crossing borders, which calls for a speedier, but effective control of document security features and their validation against relevant databases, especially those containing law enforcement alerts. This process is bound to affect the individual and/or the documents.

Biometrics, therefore, takes on special importance when it comes to look-alikes. It implies the use of mechanisms that are capable of storing bio-physiognomic parameters, which remain unaltered during the shelf time of the document and which establish a constant, updated and strict relationship between the rightful bearer and his secure document (see Chapter 7). As a result, this inextricable information link between the identity on the document and the rightful bearer not only eases document inspection, but also ensures proven effectiveness which, together with the techniques for recognition of impostors, is both a guarantee for well meaning persons, and facilitates the detection down of fraud and crime.

Nevertheless, the use of machine-readable documents and their link with biometric parameters also raises a few problems, namely regarding their readability and the training required of document inspectors. Hence, it is important to note the factors that influence the legibility of machine-readable documents. A document's wear due to permanent use, careless handling, accidents, or atmospheric and environmental conditions can lead to unforeseen alterations that can invalidate the acceptance of the document by a machine. When faced with this, it is important that inspectors know which alternative control mechanisms to activate.

It is important to remember that a document's machine reading is not the automatic authentication of the entire document. When documents are machine-read, only part of the variable data is captured and possibly validated. In the case of passport booklets for example, the picture of the holder, visas, entry and exit stamps, page numbering, and pagination should also thoroughly be checked manually.

This is an important caveat because criminals rapidly exploit the weaknesses of any system. Consider the theft of blank documents. This is a type of crime that is often organized on a transnational scale. Effective countermeasures must be implemented and should be coordinated both nationally and internationally. Besides regulation of the storage of blank documents and strict procedures for their transport, especially where non-centralized issuing systems exist, there are additional security measures which include:

- Defining secure means for the authentication of documents (electronic seals, e.g., digital signatures or embedded images, dry embossing, wet stamps, etc.) and the distribution of relevant information among the entities involved.
- The possibility to access the original application forms at ports of entry, especially photo and supporting documents.
- The use of biometric standards.
- International cooperation to establish rapid and adequate channels for the exchange of information, namely, through access to online databases containing information about stolen blank documents, suspicious travellers and fraudulent documentation.

If a physical document is genuine, it is far more difficult to detect fraud. With genuine physical documents, the only points to check are the manner in which the personal data has been entered and the authentication instruments for which hardly any reference information exists. Irrespective of security features, the exchange of information about personalization and authentication techniques between partner entities is crucial.

It must also be emphasized that the most effective method of countering the illegal issue of stolen blank documents is to centralize production and personalization, a fact that has been pointed out in several publications discussed worldwide. In this context, special attention should also be paid to 1) the physical security of all premises, from production, including storage, to shipment; 2) the records on all materials – used, unused, defective or spoiled, and 3) the tracing and control numbers of all principal document components (laminates, optical variable devices (OVDs), etc.).

In addition, one should not forget falsified stolen blank documents in the shape of adhesive vignettes and labels. Through the manipulation of a serial or assembly number – by concealing or adding characters – fraudsters aim at reducing the risk of detection by consulting the relevant databases on stolen blank documents. In these cases the rapid dissemination of information among the relevant entities is the best way to tackle the problem.

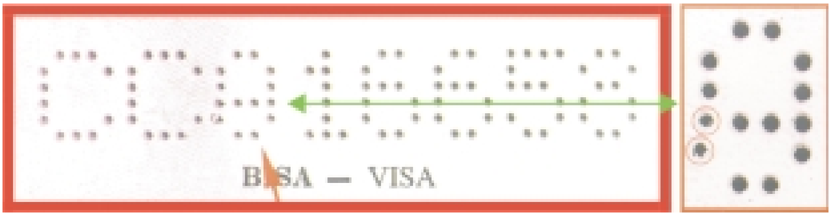


Figure 2-2
Example of manipulation of a number. By adding two holes to a 9 they changed it into a 8. (Courtesy of Serviço de Estrangeiros e Fronteiras, Lisbon, Portugal.)

■ 2.3 List of requirements

Drafting a list of requirements necessitates that all above-mentioned aspects are addressed. The more exhaustive the information, the more useful the list. Insufficient information can lead to misunderstandings and weaknesses, i.e. risks. A checklist approach has been suggested by van Renesse (Renesse Rudolf L. 2006). The conclusions drawn from the inventory phase, together with other requirements that the proposed document must meet, should be recorded in a product specification format. This forms part of the list of requirements that have either been drafted by or for the commissioning authority.

Such list of requirements could be exhaustive, meaning that no additional demands or changes may be made during the development process. However, the complexity of the chain could draw attention to new angles during the development requiring some changes or additions. A list of requirements specifies when the product is to meet a particular requirement and how this is to be measured.

This list makes considerable demands on the contracting authority, but its importance cannot be emphasized enough. It forces the contracting party to take a structural approach, which requires that the usefulness and necessity of each demand is discussed in such a way that the information from the inventory phase is integrated into the final project. It also ensures that the formulation of each demand is unequivocal. In addition, the list of requirements offers a firm starting point for the contracting party to compare the different solutions that the individual producers have to offer.

It is clear that drafting a comprehensive list of requirements takes time. Often, the tasks of taking inventory and drafting the list of requirements can take as long as meeting the requirements, i.e. going through the process of developing the definitive product, including the manufacture of specific materials, components, and additional security elements.

In the final phase of drafting the list of requirements, the contracting authority could decide to have a design drawn up to supplement the list, which could facilitate the internal decision-making process and valuation of tenders. A designer is chosen based on the list of requirements. But the design would only function as an indicator: it will offer leeway for further additions and details, partially depending on technical possibilities and the results of the selected supplier's product development.

2.3.1 Scope and format of the list

The list of requirements serves several purposes. For instance, the commissioning party may use the list in its call for tenders, whereas a producer may consult the list to decide whether he wants the contract, and to glean the necessary information from it in order to make a bid for the contract. It also enables a producer to carry out precise calculations and make a competitive offer based on these. Moreover, the commissioning party may also use it in conjunction with the description of requirements in order to verify whether a product does match the description.

The list of requirements resembles a comprehensive book, which clearly specifies the kind of product to be produced and the specific requirements to be met. It enables a commissioning party to draw up a very structured and detailed description of the desired product and services. Primary and secondary demands are distinguished and specified. Examples of "must-haves" for a secure document could be a multitone watermark and a certain type of security thread, and "should-haves" could be fibres or planchettes. Although some of the requirements are optional, they may be favoured by the issuing authority. It is up to the producer to discover ways to creatively comply with these wishes. The failure to do so, however, does not give grounds for rejecting a commission.

The list of requirements indicates which international standards apply to the document to be developed. Generally, a new travel document must fulfil the general International Standards Organization (ISO) and International Civil Aviation Organization (ICAO) standards on dimensions, machine readability, etc. The list should also indicate which testing methods will be used during development and which will apply to those demands that are not covered in the above standards. In particular, the assessment of the fraud-resistance (forgery and alteration) and user qualities of the document should not fall short of international document specifications and industry standards. The contracting party may indicate which authorities will be approached for this assessment, which assessment approach will be taken, and at what point the document qualifies for acceptance.

Alongside the physical specifications and user constraints on the document, the list of requirements also gives insight into requirements regarding quantity, timeframes for development and production, as well as requirements for materials, components, production equipment and relevant logistic processes. Guarantees desired by the contracting party regarding insurance and continuity of the production process during the term of the contract should also be addressed. Depending on the nature of the assignment, this could lead to a demand for buffer stocks of materials and components, duplication, guarded storage of the electronic records and films used for document production, and in a centralized and customized situation, possibly a demand for a back-up provision and/or a demand for production at several locations, either with or without reserve capacity.

2.3.2 Product definition

Before the order is given for production, it is necessary to draw up an exhaustive description of what is expected of the product. The specification of requirements should be formulated in such a way that it allows for alternatives, so that the product can capitalize on the latest developments regarding materials and production techniques. If the specification is too rigid, there is a risk that the final product will be unsuitable for further adaptation to counter new threats posed by forgers.

Once the kind of document to be developed has been decided, it is essential that all the technical requirements that the document must meet are incorporated into the list. This should not only concern the material composition of the physical document, but also its personalization.

Considerable thought must also be given to a document's potential for development at a later stage. In some cases, the issuing authority may have plans to migrate their product later on. Therefore, it is essential that solid agreements are made with the producer before the production process is started. If the development potential of a document is insufficiently specified before production commences, this could lead to serious problems later (e.g. legal issues in relation to tender clauses). The producer might deliver the initial product, but might be unable to implement further development as envisioned by the commissioning party. It could well be just as good as ordering the wrong product. Sometimes products are ordered on the assumption that certain equipment will be used in the inspection process. If this equipment is not purchased for the inspection phase, then again the product is faulty.

Another thing to consider is the kind of issuing process to be applied. Centralized personalization procedures offer many advantages, as all resources can be concentrated in a single or limited number of locations. Centralized issuing processes have more sophisticated and expensive equipment at their disposal than decentralized issuing processes, the production is largely standardized and homogenous, and the risk of stolen blank documents is minimized.

If a centralized issuing process is chosen, for example for a national passport, it is vital that a decision be made regarding the security requirements for a temporary passport. Otherwise the problem of forgery will be displaced to another document.

2.3.3 Support in editing the list of requirements

Commissioning parties develop a new product only periodically. This means that they cannot be expected to have the expertise to carry out a commission, and thus, they may call in the help of advisers. However, it is essential that the commissioning party is confident that the adviser is experienced and knowledgeable. If the national forensic laboratory or some other similar body checks and oversees every proposal and suggests the best option from a forensic point of view, the parties involved from the inspection point of view should also be consulted.

■ 2.4 Project management

The execution of large commissions also involves risks for producers. Before a producer receives the order to start producing a document, often the commissioning party and producer have already discussed the project frequently and extensively. The following aspects need to be dealt with:

- cooperation and coordination
- product and cost
- planning and amendments.

These are all risks that must be considered before the go-ahead is given for production. Once production is started, the document will undergo the development process as specified in the tender and list of requirements. Interfering in the process at a later stage involves risks and should be avoided as much as possible.

2.4.1 Document development team

Once the commissioning party has chosen a supplier and a creative designer, there remains the question of how to achieve the best possible integration of the list of requirements on the one hand, and product concept and creative design on the other. The ultimate aim is to develop the document in an effective and structured way. This can be achieved by setting up a small and professional document development team, which ideally consists of a representative of the commissioning party, the creative designer and the supplier’s product developer. To be effective, the development team must be characterized by a respectful and open attitude to the other team members’ qualities and by a shared objective to achieve the best possible results for the commissioning party. The team must also possess creativity and have the ability to work together in order to solve the problems that may come their way.

The commissioning party acts as chairman and should have the power to prepare decisions in order to ensure quick and effective development. To do this responsibly, the representative for the commissioning party should have expert knowledge in the areas of document use and production. Likewise, the creative designer should be capable of translating the selected product concept into the desired design, thereby effectively integrating the requirements with respect to document security and ergonomic document use. On the other hand, the product developer is expected to have the necessary technical and organizational expertise in order to arrive at the end product, besides possessing detailed knowledge of the product concept and list of requirements.

The project team plans, manages and oversees the development process. The team is guided by the supplier's project plan, which specifies the time available for the various steps of the document's development. It plans with the producer the frequency of meetings, the way in which progress is reported, and arrangements for the necessary bilateral contacts between designer and technical expert.

At this stage, a great deal of openness and exchange of information is vital so that all members of the team may proceed from a shared level of knowledge. The commissioning party provides the necessary information, explains the list of requirements and highlights the aspects it deems important. The creative designer presents his vision of the document and its use, and clarifies the concept behind his design. Ideally, his draft design will serves to guide the further development of the product concept, and allow for further fleshing out of the design depending on the technology selected by the commissioning party. The product developer should give him detailed information on the product concept, which initially served as the basis of the commission. These include the choice of materials and techniques, security possibilities, and the product developer's vision regarding the integration potential of different elements into the product.

The moke-up developed by the producer is a first visual rendering of these possibilities, which, in this phase, is helpful to visualize the final product. In addition, the designer is given the opportunity to gather detailed knowledge of the techniques and methods available in the company, e.g. by paying a visit to the supplier's production and staff departments. Emphasis should be put on knowing the production parameters during mass production, the test results during product concept development, and especially the possibilities of conversion of the draft design into secure products. The suppliers of the materials should be involved in the early stages of the development of the graphic design.

2.4.2 Product and costs

The producer must be clear on the specifications that the product must meet and the people and means that will be employed to achieve this. Before the development of the product is started, the commissioning party must be very clear on what kind of product it wants and how much it will cost. The parties may then agree on a suitable price and plans which reflect the customer requirements. Subsequent changes will invariably affect price and delivery times.

2.4.3 Planning and change management

Producers may often find themselves in an awkward situation: on the one hand, they are eager to satisfy their client, but, on the other hand, they need to protect their business interests. Furthermore, carrying out sizable orders that involve the production of important and complex products is often time-consuming. The commissioning party, which has less experience with large orders, often has the feeling that there is still plenty of time to propose changes. Changes are possible, but their effects should always be analysed. It would unfortunate for either party to discover that an amendment resulted in failure. Subsequent changes on price and technical aspects as well as their effect on planning also have to be scrutinized. Apparently, easy alterations often have considerable impact on planning. If changes are accepted, their effects on planning must be clear and acceptable to the commissioning party.

■ 2.5 Critical issues

Commissioning parties, which are composed mostly of issuing document authorities, should be aware of the issues involved in the development of new documents. The following aspects are critical:

- public acceptance of the document;
- verifiability of the document;

- political risk if the product is discredited.

These "soft issues" must be borne in mind in awarding the contract. Once the contract is awarded, a producer will proceed to produce the document on the basis of his own proposal and quotation.

2.5.1 Public acceptance

Ordering a product that is not accepted by the public is a risk often underestimated. Issuing authorities and clients should not disregard the views of its future users. Certain issuing bodies often wrongly assume that they know what the users think about their products. As a result, users may simply ignore the product in question. This risk might be less relevant to products that have a short lifespan, but should not be ignored.

For instance, a product put into circulation that is not accepted by the public can be disastrous. In the late 1990s, several financial institutions in the Netherlands circulated various bank cards, which resulted in the products "Chipper" and "Chipknip". These bank cards contained a chip, which enabled the user to use a chip aside from the traditional magnetic stripe. However, for one reason or another, the owners of such cards refused to use the chip. This led to the replacement of both the "Chipper" and the "Chipknip" by a bank card that was accepted by the public. Such an operation can have huge financial implications as a result of the damaged reputation of the issuing organizations and the waste of money.

In the case of governments, which often have a monopoly on the issuance of certain documents that users have no recourse to a competitor for an alternative product, they would do well to consider the views of the public when developing their documents. If a government develops a product that fulfils what the public desires, the public is more likely to take pride in it and regard it in a more favourable light.

2.5.2 Controllability

Designing and producing a secure document is extremely important and should not be taken lightly. It is a process governed by internationally accepted standards and procedures that cover the entire process. These standards ensure the best possible control of IDs, travel documents or residence permits, regardless of nationality, type or model, or the location where the control or verification is carried out.

The current state of technology often enables producers to fit out products with the latest high-tech devices. Such applications are intended to enhance the security of the document. Although very appealing, their ultimate value must be assessed in relation to the document chain. It is, therefore, important to determine beforehand what a particular application has to offer, and what its added value is security-wise.

The effectiveness or performance of a secure document also depends on the ultimate target group. We can distinguish two target groups: entities which need to verify personal information for granting a service and the ordinary citizen. A survey conducted by the Bank of the Netherlands (de Heij, 2000) showed that the public, which thus also include the document inspector, is only capable of remembering a few of a document's features. Document developers would be well advised to consider the restrictions of both target groups:

A. Authorities

The authorities that first come to mind are the police, immigration services, transport companies / carriers, local and regional administrative services, banking and financial institutions, etc. Factors that also need to be considered here are:

- the reference materials and equipment available in order to verify a document's authenticity;
- the logistic / physical working conditions in which control is carried out;
- the previously-mentioned fraud risks.

Additionally, one must bear in mind that, for each of the above-mentioned targeted groups, there are different training methods, information networks, and distinct practices and procedures for addressing problems. For each group, however, it is vital that the documents are not only secure and reliable, and that, where there is doubt, forensic examination is possible.

B. Public

While training is the central issue as far as the above-mentioned authorities are concerned, ordinary citizens benefit most from receiving accurate information. No matter how the information is provided, it should always be precise, concise, well-timed, up to date and on a "need to know" basis. Although this last principle applies to both target groups, it is particularly relevant to the public in view of the huge number of persons concerned.

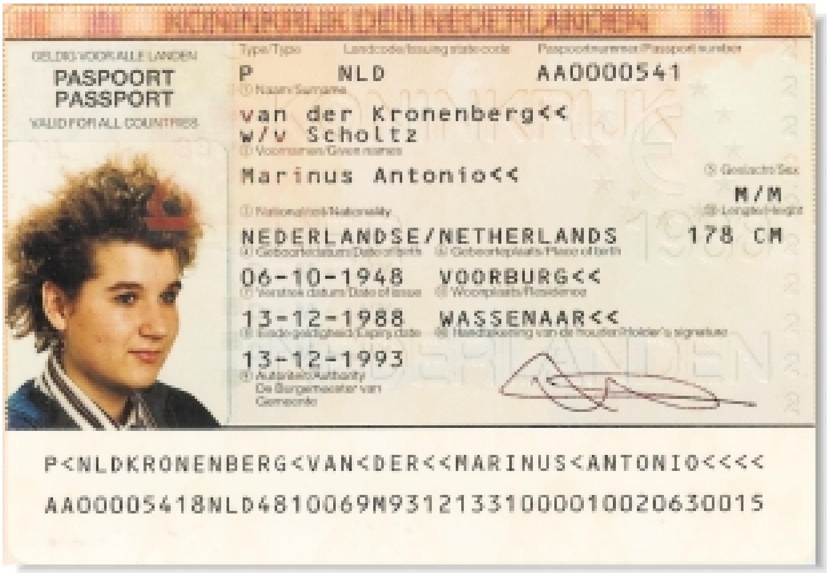
Above all, the provision of information should enhance the public's trust in the system and prompt it to contribute to the common welfare and security in society. The information provided should be restricted to the most elementary security features (first-level security), and to the basic facts about the legal value of the document.

The ultimate aim is that, where there is suspicion, the relevant party or parties will know where to go, how to act, whom to talk to, etc., provided that the official support infrastructure is in place. In the end the proper information channels and structures will help optimize the system.

2.5.3 Political risk

Governments are solely responsible for putting certain products into circulation. From an economic point of view, it may be interesting to hold the monopoly on this, but such a position often involves huge risks. Products such as banknotes and identity documents receive considerable political attention, so if something goes wrong with them, political tension would ensue. The Dutch "Paspoortaffaire"[1] is an example of this. In 1984, the Dutch government was developing a new fraud-resistant European passport. The contract was granted to a joint venture of three companies: Kodak, Elba (a printing company) and Philips. They formed the KEP joint venture. Four years later, it was found that KEP was not able to fulfil its duties. The resulting parliamentary investigation looked for the reasons for the failure and discovered that the passport decision making process on was flawed and did not work. This resulted in the resignation of two ministers (Parlementair Documentatie Centrum, 2006).

[1] The Parliamentary Passport case



KONINKRIJK DER NEDERLANDEN

GELDIG VOOR ALLE LANDEN
PASPOORT
PASSPORT
VALID FOR ALL COUNTRIES

Type/Type P
Landcode/Issuing state code NLD
Paspoortnummer/Passport number AA0000541

Naam/Surname
van der Kronenberg<<
w/v Scholtz

Voornamen/Given names
Marinus Antonio<<

Geslacht/Sex
M/M

Nationaliteit/Nationality
NEDERLANDSE/NETHERLANDS

Lengte/Height
178 CM

Geboortedatum/Date of birth
06-10-1948

Geboorteplaats/Place of birth
VOORBURG<<

Verstrek datum/Date of issue
13-12-1988

Woonplaats/Residence
WASSENAAR<<

Einde geldigheid/Expiry date
13-12-1993

Handtekening van de houder/Holder's signature

Autoriteit/Authority
De Burgemeester van
Gemeente

P<NLDKRONENBERG<VAN<DER<<MARINUS<ANTONIO<<<<
AA00005418NLD4810069M9312133100001002063001 5

Figure 2-3:
Image of a prototype of the fraud-resistant Dutch KEP passport.
(Courtesy of Fons Knopjes, the Netherlands.)

The commissioning authority should be aware of the political risks involved in certain choices. It is, therefore, essential that the commissioning party strike the right balance between the choices it makes and the creation of a sufficient support base for these. Sometimes this can lead to a conflict of interests between the commissioning party and the producer. For instance, a choice that initially appeared logical for technical reasons could be assessed very differently if the proposal encounters resistance. In such cases, the contracting party would be well-advised to increase support for the proposal, or else consider an alternative solution.

If certain techniques and materials are proposed for which there is insufficient support, this can lead to political risks, no matter how justified the proposed applications are from a production or security-technical point of view.

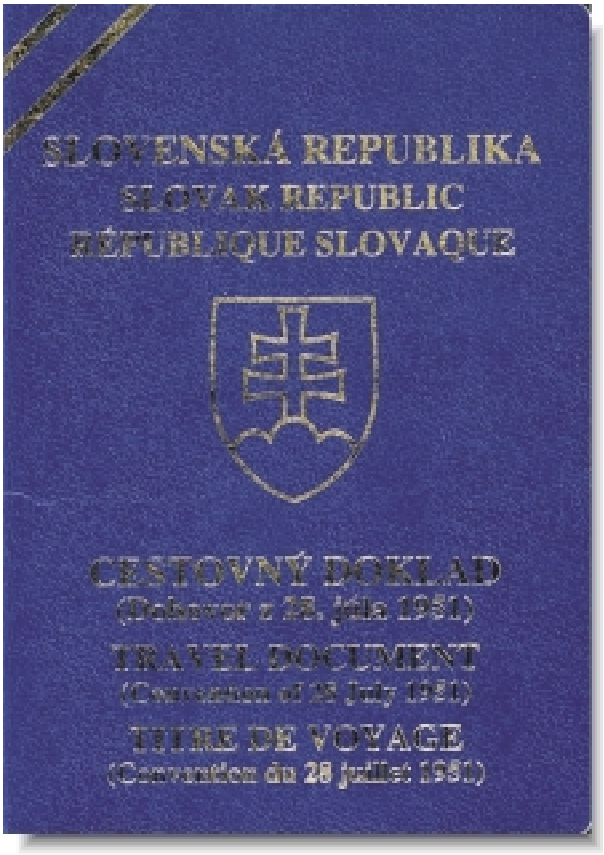
■ 2.6 Standards

In the history of secure documents, there has been no apparent need for international standardization of identity and travel documents issued by governments until recently. However, the increase in international travel by air, sea and road necessitated faster processing of people crossing international borders. A need for traffic police that could effectively inspect a driving licence issued by another country and possibly in a different language has also been felt. These needs were originally identified by the relevant bodies of the United Nations.

2.6.1 Introduction of international standards for government issued documents

The first attempt to agree on a uniform style of passport goes back to the beginning of the twentieth century. The Provisions Committee on Communications and Transit of the League of Nations in Geneva called together an International Conference on Passports, Custom Formalities and Through Tickets in 1920. A resolution drawn up by this Committee and passed in October 1920 fixed the date for introduction of a new standardized passport at July 1921. The document, a 15.5 cm by 10.5 cm booklet, was supposed to contain 32 numbered pages and be in at least two languages (the national language and French) (Lloyd, 2003).

In the case of travel documents, the United Nations drew up two conventions after World War II to establish the rights of refugees and stateless people. The UN Convention relating to the Status of Refugees, adopted on 28 July 1951, states that "Contracting States shall issue identity papers to any refugee in their territory who does not possess a valid travel document."(Art. 27) and "[…] shall issue to refugees lawfully staying in their territory travel documents for the purpose of travel outside their territory […] (Art. 28). Annex A to the Convention describes the features of the new travel document for refugees. Its cover bears two stripes appearing in the upper right corner of the front cover.



SLOVENSKÁ REPUBLIKA
SLOVAK REPUBLIC
RÉPUBLIQUE SLOVAQUE

CESTOVNÝ DOKLAD
(Dohovor z 28. júla 1951)
TRAVEL DOCUMENT
(Convention of 28 July 1951)
TITRE DE VOYAGE
(Convention du 28 juillet 1951)

Figure 2-4:
Example of a Refuge document of the Republic Slovakia.
(Courtesy of National Criminal Intelligence Service, the Netherlands.)

This travel document for refugees is in some way a successor of the Nansen passport of the 1920s, introduced by Fridtjof Nansen, a Norwegian diplomat and former High Commissioner for Refugees within the League of Nations, who was awarded the Nobel Peace Prize in 1922 for his humanitarian work. In 1954 the United Nations adopted the Convention Relating to the Status of Stateless Persons, which covers the issuance of identity and travel documents to stateless persons to the same extent as the 1951 Convention. The cover of this type of travel document bears the words “travel document” in English and French (and often in the language of the issuing state) along with the date of the convention.

The driving licence also received partial international standardization after World War II. The United Nations held a meeting on transport in 1949 and again in 1968. These meetings covered an array of transport issues, including driving licences and resulted in two conventions. Both conventions envisaged the licence as a booklet. The booklet would give details of the driver, the types of vehicle(s) the driver was permitted to drive, and any special requirements, such as the wearing of glasses. The problem of language was overcome by presenting the details of the driver in a standard sequence and vehicle types and requirements by means of standardized symbols. The 1949 Convention specified that the licence should be pink. States issuing new licence designs were encouraged to submit them for endorsement to a UN maintenance agency based in Geneva.

2.6.2 International Civil Aviation Organization and travel documents

The Convention on International Civil Aviation signed in Chicago in 1944 by 52 states set up the International Civil Aviation Organization (ICAO), based in Montreal, as a means to secure international cooperation to the highest possible degree on the uniformity of regulations and standards, procedures and organization regarding civil aviation matters (ICAO, 2006). As air travel became increasingly popular in the 1970s, ICAO grew concerned about the delays incurred at airports as a result of the time inspectors needed to examine a wide variety of passports of different sizes and with different forms of data presentation regarding the holder, their nationality and their right to enter the country of destination. As a result, ICAO established a Technical Advisory Group on travel documents (TAG-MRTD) when it foresaw the need to streamline the immigration processing of travellers.

In 1980, ICAO established a standard for machine-readable passports, known as ICAO Document 9303 (later ICAO Doc 9303 part 1). This document envisaged a card-type passport, as the one already suggested by ICAO twenty years earlier at the United Nations Conference on Passports and Frontier Formalities. The card format was never adopted primarily because governments insisted on reserving a space on the document to affix visas.

During the ongoing efforts towards developing this initial standard, a major obstacle was the fact that several states had privacy laws that prevented these states from demanding that their citizens carry documents containing information about themselves that they could not see. This, coupled with the technologies available at the time, led to the selection of optical character recognition for the machine-readable data. Provided the format of the data is explained, a citizen can easily check the information contained in the two lines of the typeface OCR-B in the Machine Readable Zone of a passport book.

Subsequently, ICAO extended its standards to include machine-readable visas in two sizes (ICAO Doc 9303 part 2), and what have become known as Official Documents of Identity used for travel, which are cards in two sizes that may be used for inter-governmentally agreed cross-border travel (ICAO Doc 9303 part 3). Although no country has, as yet, issued a passport in the form of an isolated card, it is clear that this could become the passport of the future. The use of OCR-B as data medium was retained so that all documents could be read by a single type of reader. The data is presented in two lines, with differences in the number of characters as a result of the different sizes of the documents, with the exception of the smaller size Official Document of Identity, where the OCR-B data is contained in three lines.

This smaller card, known as Size 1, is similar to ID-1 but has larger dimensional tolerances in its basic form. This is to allow for variations when, for example, the card is assembled in an office environment without the highly accurate punching equipment normally used for making ID-1-size cards. However, if the card contains an additional data storage technology that requires the card to be inserted into a reader, the tighter ID-1 dimensional specification applies.

The standards for machine-readable travel documents are published as ICAO Document 9303 and consists of three parts:

- Part 1 Machine Readable Passport Books Volume 1 and 2
- Part 2 Machine Readable Visas

- Part 3 Machine Readable Official Travel Documents that may be used for cross-border travel.

The sixth edition of part 1 (Volume 1 Passports with Machine Readable data Stored in Optical Character Recognition Format and Volume 2 Specifications for Electronically Enabled Passport with Biometric Identification Capabilities) was published in 2006, part 2 published in 2005, a second edition of part 3 in 2002. The standard for crew member certificates has been included as a special annex to the new second edition of part 3, published in the spring of 2002.

During a meeting held in New Orleans in March 2003, ICAO's New Technologies Working Group (NTWG) drew up a resolution supporting the facial image as a primary identifier (even as a digitally stored facial image) and opened the possibility to ICAO member states to use standardized digitally stored fingerprints and/or iris image as additional globally interoperable biometrics in support of machine-assisted verification and/or identification. Moreover, the NTWG encouraged adopting contactless IC media for the storage of digital information. This resolution was endorsed by the TAG-MRTD Meeting 14 (2003).

During the following meeting (TAG-MRTD 15, 2004) a symbol for the e-passport was chosen.

Due to several decisions made by the TAG-MRTD in the last two years, the sixth edition of part 1 of Doc 9303 has been completely restructured. The document is divided into two parts: the first part provides the specifications for the basic Machine Readable Passport (MRP) while the second will provide the specifications necessary to turn the basic MRP into an e-passport (deployment of biometrics, logical data structure, Public Key Infrastructure (PKI)).

Only if there is widespread acceptance can the advantages of global interoperability facilitate and secure immigration processing. ICAO's role is to assist and advise the member countries in the implementation of the developed standards.

In March 2007, it was decided that the TAG-MRTD should form two working groups to undertake the detailed work tasked by the TAG-

MRTD. The two groups are the New Technologies Working Group (NTWG) and Universal Implementation of Machine Readable Travel Documents Working Group (UIMRTDWG).

The UIMRTDWG is responsible for assisting the Secretariat in the implementation of project in States, including training, technical and sources of financial assistance under the Universal Implementation of MRTD (UIMRTDWG) to meet the 2010 deadline to carry out capacity building outreach activities and in conjunction with States, other international organizations and the private sector.

The NTWG is responsible for examining all aspects of new technologies that may be relevant to travel documents. It assesses the technologies and recommends those it considers suitable for inclusion in future editions or amendments to ICAO Doc 9303. In recent years, its work has included the tightening of the standard for the holder's portrait, and has introduced, recommended minimum security standards. Its current work includes the development of a standard means of biometric identification of the travel document holder, the methods by which the biometric data can be stored on the document, and methods by which the travel document may be machine-verified as genuine. These involve the handling and storage of significant amounts of data. A logical data structure (LDS) has been developed to enable states to record the data in a standard form so that other states can easily access it.

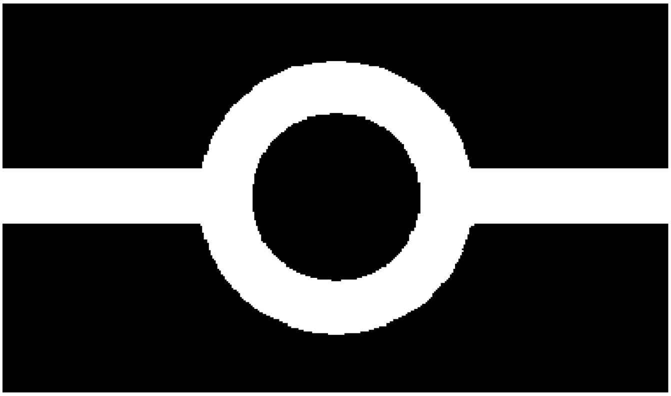


Figure 2-5: The ICAO symbol on electronic Travel Documents.
(Courtesy of Sdu Identification, Haarlem, the Netherlands.)

2.6.3 International Standards Organization

The International Standards Organization (ISO), based in Geneva, Switzerland, develops standards relating to almost every field of human endeavour. Most countries have a national standards body, which is associated with ISO. Most ISO standards are established by working groups drawn from a particular industry. The expert members of these working groups are usually employees of industrial companies involved in the production and use of the products whose standardization is being

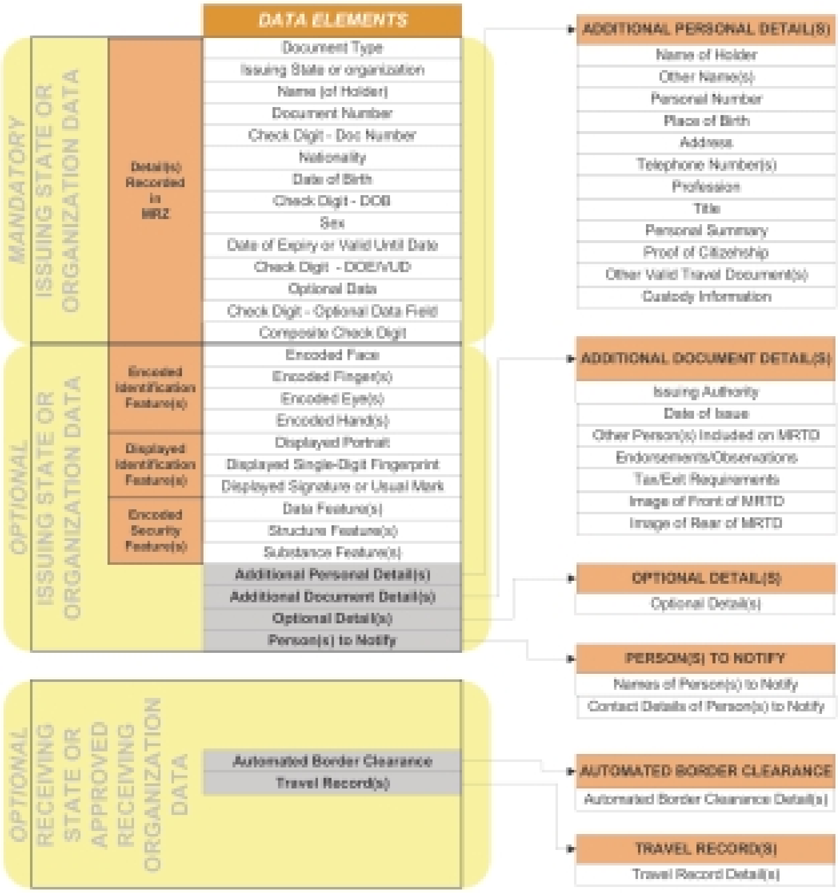

DATA ELEMENTS
MANDATORY
ISSUING STATE OR ORGANIZATION DATA
Detail(s) Recorded in MRZ
Document Type
Issuing State or organization
Name (of Holder)
Document Number
Check Digit - Doc Number
Nationality
Date of Birth
Check Digit - DOB
Sex
Date of Expiry or Valid Until Date
Check Digit - DOE/VUD
Optional Data
Check Digit - Optional Data Field
Composite Check Digit
OPTIONAL
ISSUING STATE OR ORGANIZATION DATA
Encoded Identification Feature(s)
Encoded Face
Encoded Finger(s)
Encoded Eye(s)
Encoded Hand(s)
Displayed Identification Feature(s)
Displayed Portrait
Displayed Single-Digit Fingerprint
Displayed Signature or Usual Mark
Encoded Security Feature(s)
Data Feature(s)
Structure Feature(s)
Substance Feature(s)
Additional Personal Detail(s)
Additional Document Detail(s)
Optional Detail(s)
Person(s) to Notify
OPTIONAL
RECEIVING STATE OR APPROVED RECEIVING ORGANIZATION DATA
Automated Border Clearance
Travel Record(s)
ADDITIONAL PERSONAL DETAIL(S)
Name of Holder
Other Name(s)
Personal Number
Place of Birth
Address
Telephone Number(s)
Profession
Title
Personal Summary
Proof of Citizenship
Other Valid Travel Document(s)
Custody Information
ADDITIONAL DOCUMENT DETAIL(S)
Issuing Authority
Date of Issue
Other Person(s) Included on MRTD
Endorsements/Observations
Tax/Exit Requirements
Image of Front of MRTD
Image of Rear of MRTD
OPTIONAL DETAIL(S)
Optional Detail(s)
PERSON(S) TO NOTIFY
Names of Person(s) to Notify
Contact Details of Person(s) to Notify
AUTOMATED BORDER CLEARANCE
Automated Border Clearance Detail(s)
TRAVEL RECORD(S)
Travel Record Detail(s)

Figure 2-6:
Overview of the structure of ICAO's Logical Data Structure. (Courtesy of the International Civil Aviation Organization, in Montreal Canada.)

established. Usually, the need for standardization of a particular class of product is identified by a relevant ISO sub-committee, and a working group is established to propose a suitable standard that satisfies the requirements of both the producers and the users of the product. The working group can, however, only prepare a draft of a standard and propose its adoption. To become an international standard, the draft is subjected to an international ballot in which all eligible national standards bodies vote to support, reject or amend the proposal. Usually, a period of discussion follows to deal with any objections or reservations.

In some countries, travel documents and driving licences are also used as identity documents. However, ISO initially intended identity documents as plastic cards for financial and related transactions. The need for international standards for financial cards arose as the international use of credit cards increased. It became necessary to develop standards for the dimensions and other physical properties of the cards, test methods to verify these properties and the location and structure of encoded data stored on the card. The encoded data was initially embossed onto the plastic. Subsequently, magnetic stripes were introduced. As each card has a unique number, a system for managing the issuing of the numbers had to be established. And as data storage progressed from magnetic stripe to contact microchip-some card types already use contactless microchip and optical memory-appropriate standards had to be agreed on and implemented.

The involvement of ISO in government-issued identity documents came relatively late and some years after the first passport and driving licence standards were established. Though the first UN standard for driving licences dates from 1949, it was not until 1997 that ISO became involved. ISO's interest in travel documents dates from the late 80s, some years after ICAO published its first standard. Initially, the ISO's purpose was limited to examining the ICAO document to see if it was suitable to be endorsed as an ISO standard.

As already stated, both standards were produced under the auspices of the United Nations. One of the rules under which UN agencies operate is that only government employees are allowed to serve on their committees. When the original standards were drawn up, the governments concerned had employees who were involved both in the issue and use of the documents and, through their state printing agencies, in the document's production. The situation has changed significantly in recent years. Many governments have privatized their state printing agencies, and because of this, their employees can no longer sit on the UN committees. Many more states have become involved, often contracting out the production of their ID documents to recognized security printers. The technologies now being considered are much more complex so that there is a real need for expertise, which is only available in the commercial sector. This expertise can also be found within the structure of ISO. So while ISO's initial involvement in travel documents was to examine the standards set up by the UN specialized agencies to determine whether the standards could be endorsed by ISO, the relationship between the organizations now works to the benefit of all.

A. Travel documents

To ensure the availability of relevant expertise, ISO operates in a committee, sub-committee, and working group structure covering specific classes of standards. In the case of identity documents, the parent committee is known as Joint Technical Committee 1 (JTC1) and the relevant Sub-Committee is known as SC17. Although ISO is currently involved in identity documents, its experience in financial cards is reflected in the fact that the Secretariat of SC17 is provided by the Association of Payment and Clearing Services (APACS), based in London. SC17 has its own web site, www.SC17.com.

There are nine working groups under SC17, of which WG3, concerned with machine-readable travel documents, and WG10, involved in motor vehicle driving licences, are relevant to government-issued ID documents. However, other working groups which provide input relevant to travel documents and driving licences are:

- WG1: Physical characteristics and test methods for identification cards;
- WG4: Contact Integrated Circuit cards (contact ICs);
- WG8: Contactless Integrated Circuit cards (contactless ICs);
- WG9: Optical Memory Cards and devices;
- WG11: Application of Biometrics to cards and Personal Identification.

Although Working Groups 1, 4, 8 and 9 have developed standards for financial cards and the data encoded on such cards are different from that needed for travel documents or driving licences, the aim is to make the utmost use of the existing standards for government ID documents with these advanced technologies. Travel documents and driving licences typically have validity periods that are much longer than those of financial cards. This means that test methods for financial cards can only provide an indication of their eventual performance.

Because the use of bar codes is used in many fields besides identity, one and two-dimensional bar codes come under a different sub-committee, SC31.

Everyone involved in the development of international standards does this part time, diverting them from their work for their employer (government or company). The work of WG3, which started as a modest effort, has grown to include the ongoing development of the range of travel documents, the updating of standards to incorporate these new developments, and providing assistance to governments wishing to introduce machine-readable travel documents. To deal with the increased workload, several years ago, WG3 set up Task Forces (TF). TF1 monitors and assesses new technological developments. TF2 was originally established to ensure harmonization between the various parts of ICAO Doc 9303, but now oversees the update of the standards and ensures that they conform to ISO guidelines. TF3 provides advice to governments and deals with the problems of converting national characters into the limited character set permitted in the travel document's Machine Readable Zone. TF4's objectives are the development of an RF protocol and application test standard for e-passports and a durability test protocol. The two protocols aim to improve interoperability of e-passports and readers and verify the functional conformance to ISO standards and ICAO recommendations (see section 5.5.3 Compatibility to standards). TF5 working area is the Public Key Infrastructure.

Whereas WG3 meetings used to deal with the minutiae of every aspect of the standards, these are now dealt with by the task forces. WG3 meetings now consist of receiving and approving reports on the work of the task forces, and planning strategies to meet the challenge of what is becoming a rapidly changing environment.

B. Driving licences

Being a newer group than WG3, WG10 was able to draw heavily on the experience of WG3's activities. Many members serve on both groups. WG10 has established some ten task forces covering a range of topics. Like WG3 it makes extensive use of the expertise available within ISO Working Groups 1, 4, 8 and 9.

ISO SC17 established its Working Group 10 at a meeting in 1998. Like WG3, WG10 meetings are attended by government and industry personnel. Japan, South Africa and several European and North American countries are strongly represented. The American Association of Motor Vehicle Administrators (AAMVA) plays a major role, including currently providing the convenor of WG10. AAMVA represents driving licence issuing authorities in the USA, Canada and Mexico.

With 640 different driving licences in Europe alone, the worldwide number is huge. WG10 has spent considerable time trying to take stock of the practices of countries around the world to determine a starting point for the development of a standard.

There is one document that is technically outside the brief of WG10: the International Driving Permit (IDP). This document, recognized by the UN Convention, is issued to a driving licence holder to prove that the said holder is licensed to drive. This is established in a standard which is recognized by officials in other countries. In its present form it is a paper document to which a portrait of the holder is affixed. There is no security against counterfeit or fraudulent alteration. In many countries the issue of the IDP is subcontracted to unofficial bodies such as motoring organizations.

The IDP is therefore unsatisfactory in many respects. It is, however, the only internationally recognized driving permit. WG10 had therefore decided to develop a proposed standard for a new International Driving Licence.

The new ISO standard 18013-1 establishes the design format and data content of an ISO-compliant driving licence (IDL) with regard to the human-readable (visual) features and the placement of ISO machine-readable technologies on the card. The intent of the ID-1 sized IDL is to allow one document to serve the purpose of both what is currently known amongst driver licensing authorities as a domestic driving permit and an international driving permit (IDP). Thus the IDL replaces the need for two separate documents. Alternatively, those countries that choose to maintain their individual domestic design can issue a second card (with or without ISO machine-readable technologies), a domestic driving licence (DDL), whilst the IDL serves to replace the current IDP paper document only (ISO, 2006).

2.6.4 The partnership between ICAO and ISO

ICAO issues and controls the standards for machine-readable travel documents. ISO's role in relation to the standards is to endorse them as satisfying the tight requirements laid down by ISO for an international standard. The original and primary role of WG3 is to ensure that ISO's requirements are observed, and to recommend to ISO that each new edition of each part be endorsed. Each of the standards bodies of the ISO member countries vote to approve endorsement. If any body votes against endorsement, reasons must be given, which must subsequently be addressed even if the overall ballot result is positive.

ISO endorsement takes the form of an ISO Standard ISO/IEC 7501 parts 1, 2 and 3. This is a very simple document, which records the endorsement of specific editions of ICAO Doc 9303 parts 1, 2 and 3.

2.6.5 Standardization activities of the European Union

A. Passports, visa and residence permits

The European Union has, in recent years, established some standards of its own. In the beginning these standards were set up with the intent to give to passports EU member states passports corporate identity. Later the European directives related to passports, visa and residence permits interacted to the above mentioned ICAO and ISO standards for the integration of new technologies and for the sake of global interoperability.

In the 1980s, Europe introduced a common design for a machine-readable passport, which largely conformed to the ICAO standard. However, there was one deviation, which is currently being corrected by an amendment to the ICAO standard, whereby the ICAO standard called for the name of the issuing state and the word ‘passport’ to appear at the top of the passport data page in a relevant language. The European passport did not conform because a previous page in the book contained the name of the issuing state and ‘passport’ in all EU languages. ICAO, in consultation with EU representatives, agreed to change the ICAO standard to specify that, where the name of the state and the word ‘passport’ appeared on a page prior to the data page, it was not necessary for this to be repeated on the data page. Some European states have chosen to conform to both standards by giving the information on both pages.

In the 1990s, Europe introduced a common machine-readable visa known as the Schengen visa. This also generally conforms to the ICAO standard except that the name of the document holder only appears in the Machine Readable Zone (MRZ) and not in the visual zone. Moreover the original European visa had no place for a picture, which subsequently has been changed. Often, the missing name in the visual zone does not pose a problem. However, where a name is truncated to make it fit the MRZ or where transliteration has occurred to deal with national characters that are not permitted in the MRZ, nowhere on the visa does the holder’s name appear in its correct form. It can be argued that the name is given correctly on the data page of the passport containing the visa.

During the TAG meeting in 2000, Germany initiated standardization of the security level against counterfeiting and alteration of travel documents. There were discussions between European governments that led to the establishment of this standard in 2001, also adopted by ICAO. At one point, there was a need for more detailed security standards in ICAO Doc 9303, because the document merely warned issuing states of the need to secure documents, leaving it up to the individual states to incorporate the security features they deemed necessary. The ICAO TAG-MRTD requested the NTWG and DCFWG (document Content and Format Working Group, dissolved) work together to develop an ICAO security standard based on the EU standards. This resulted in the annex to section III Doc 9303 part 1, fifth edition.

One of the problems was to ensure that the standard encouraged and did not stand in the way of future development. An example of this was when the data page was put on the cover of a passport book. This construction led to the most serious type of passport fraud, namely photo substitution, which was solved by the addition of a digital photo in the chip of the passport.

In the early 1990s, Interpol issued a recommendation that the data page should be an inside page and not the cover. This recommendation became mandatory in the EU security standards. Placing the data page on the inside has some advantages in that attempts to substitute the bromide print photograph and other data are much more difficult, and additional security can be achieved by means of a visible watermark in the paper. However, there are also disadvantages: the data page is less sturdy and susceptible to damage when presented for reading, particularly if the reader is a swipe reader. Once the page becomes crumpled, there is a chance that the Machine Readable Zone becomes illegible. To deal with this, the page is often made more robust, which potentially makes it more vulnerable to photo substitution. Some governments solve the problem by adopting systems in which an ID3 plastic card is bound into the book to become the data page. The ICAO security standard therefore grants issuing states the freedom to take advantage of new solutions, while ensuring that, if they choose to use the traditional cover construction, they also take the appropriate precautions.

More recently, the EU took advantage of research carried out by the ICAO NTWG on machine-assisted identity confirmation, and subsequently adopted a Council regulation for the implementation of biometrics in EU passports and travel documents in December 2004. On 28 June 2006 the second part of the technical specifications where established. Member states received deadlines for the application of the new regulations: 18 months for facial image (28 August 2006 introduction on documents) and 36 months for fingerprints (28 June 2009 introduction on documents the latest) (European Union, 2006).

The EU also approved a regulation laying down a uniform format for residence permits for third-country nationals. The uniform format may be used as a sticker or a stand-alone document. The annex of this regulation describes design, layout, content and materials to be used for the manufacture of the permits. Additional secret technical specifications define the security features and issuance details.

B. Driving licences

The EU has worked closely with the UN in promoting the development of a common driving licence for Europe. This is necessary because, at present, there are 640 different licences in use within Europe, 84 of which are currently being issued. The EU has had to issue a manual showing the 640 permutations.

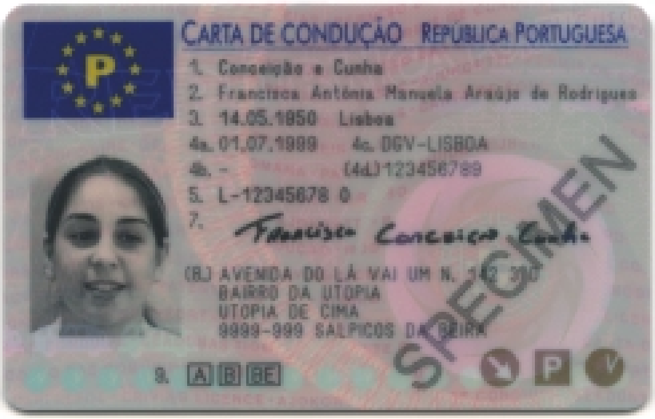
In the early 1990s, the EU recommended, in Council Directive 91/439/EEC, the issue of a standard paper driving licence. However, the rapid growth of plastic cards led to the introduction of a card version in Council Directive 96/47/EC. This directive also mentions the possible initiation of a common data storage technology, e.g. the microchip. To ensure that such an introduction, when it is made, provides for interoperability between states, the unilateral launch of such a technology by an individual state is prohibited. Bar codes may be used, but only to duplicate information already visually readable on the card or to facilitate issuing procedures.

The directive specifies what information is required regarding the issuing state and driver, including a portrait. It also stipulates that the types of vehicles the holder may drive must be indicated by means of the UN symbols. Specifications with respect to the background colour and text as well as the colours of the EU symbol are also set out in the directive.

The specified background colour is pink, in accordance with the 1949 UN Convention. The continued use of this colour is regrettable, as 'pink' is very close to the magenta primary colour used in colour copiers and colour printers. There is already ample evidence of the exploitation of this weakness and the simplicity of the design in the production of counterfeits. Much could have been done to achieve a combination of design and colours that would have resulted in a licence that was both distinctive in appearance and difficult to counterfeit or alter. The directive allows states to add security features which offer some protection against fraud.

Another Council directive was issued in 1997 (97/26/EC) providing additional standardization of the conditions under which the licence holder may drive a motor vehicle. These include eyesight and hearing correction as well as any driver disability modifications to the vehicle.

A new directive on driving licences has been prepared in 2003 by the European Commission and has been approved by the European Parliament in 2007. It contains multiple fraud countermeasures. Firstly, the new model to be issued should be a plastic "credit" card type, already used in some EU countries, which allows greater protection against forgery. Secondly, to raise the protection against fraud still further, the licence could contain a microchip. The EU deems that the repetition of the information printed on the card in the microchip increases the anti-fraud protection and at the same time ensures protection of the data. Thirdly, a mandatory and regular administrative renewal of driving licences would ensure that all documents in circulation be updated using the most up to date security features. Besides, the renewal would have a positive effect on the likeliness of the holder to the displayed the photograph. Figure 2-7 illustrate the layout of the new European Driving licence.



CARTA DE CONDUÇÃO REPÚBLICA PORTUGUESA

1. Conceição e Cunha
2. Francisca Antónia Manuela Araújo de Rodrigues
3. 14.05.1950 Lisboa
4a. 01.07.1999 4c. DGV-LISBOA
4b. - (4d.)123456789
5. L-12345678 0
7. Francisca Conceição Cunha

(8.) AVENIDA DO LÁ VAI UM N. [illegible]
BAIRRO DA UTOPIA
UTOPIA DE CIMA
9999-999 SALPICOS DA BEIRA

9. A B BE

P
SPECIMEN
P

Figure 2-7:
The European Driving Licence from Portugal (front).
(Courtesy of Imprensa Nacional-Casa De Moeda S.A., Lisbon, Portugal.)

C. Vehicle registration documents

There is also an EU directive on the harmonization of form and content of the registration certificate for vehicles to facilitate comprehension and thus help toward the free movement. The first Council directive on the registration document for vehicles was issued by EU in 1999. More recently, the Council Directive 2003/127/EC amended the older one to provide EU member countries with specifications for the issue of vehicle registration documents in microprocessor smart card format instead of paper (Stauffer and Bonfanti, 2006).

2.6.6 Standardization activities in Africa and America's

The first East African passport was officially launched in April 1999 as the result of the initiative of the East African Community (EAC) (www.africa-union.org/root/AU/recs/eac.htm).
The Economic Community of West African States (ECOWAS) has established in May 2000 new standards for the common passports of its member states (Decision C/DEC.1/5/2000 signed in Abuja in May 2000 relating the Adoption of an ECOWAS Passport).

The member states of MERCOSUR (Argentina, Brazil, Paraguay and Uruguay) approved the features of the common passport in 1994 (Resolución No. 114/94).

The Caribbean Community (CARICOM) developed more recently the CARICOM Common passport. In 2005 Suriname became the first full member state to officially launch the new CARICOM Passport (Wikipedia, Caribbean Community).

2.6.7 International Labour Organization and the Seafarer Identity Card

The International Labour Organization (ILO), established in 1919, is a specialized agency of the UN. It is a tripartite organization, in which representatives of governments, employers and workers take part with equal status. As a consequence of international terrorism and to balance the interest of maritime workers, the ILO adopted in 2003 a revised Convention on Seafarers' Identity Documents (entered into force on 9 February 2005).

The Convention includes several aspects of the document chain such as, among other, the issuance of the Seafarers' Identity Documents, their content and form, quality control and facilitation. The Seafarers' Identity Document is a machine-readable document conforming to ICAO specification in Document 9303. ILO member states may, as they wish, include a biometric template in the document. ILO tested intensively different products and chose eventually the fingerprint template to be stored in a barcode as the global interoperable biometric for seafarers.

References

The following is a list of standards that are either directly related or relevant to government documents.

United Nations

UN Convention on International Civil Aviation – Annex 9 Facilitation (the Chicago Convention), 7 December 1944
UN Convention Relating to the Status of Refugees, 28 July 1951
UN Convention Relating to the Status of Stateless Persons, 28 September 1954
UN Convention on Road Traffic in Vienna, 8 November 1968 (includes specifications for paper driving licences)

International Civil Aviation Organization

ICAO Document 9303, Machine Readable Travel Documents, part 1, Machine Readable Passports
ICAO Document 9303, Machine Readable Travel Documents, part 2, Machine Readable Visas
ICAO Doc 9303, Machine Readable Travel Documents, part 3, Official Travel Documents, including passport cards and crew member certificates.
ICAO TAG MRTD/NTWG Technical report, PKI for Machine Readable Travel Documents offering ICC read-only access v 1.1 (latest available in January 2005)
ICAO TR Development of a Logical Data Structure v 1.7 (latest available in January 2005)
ICAO TAG MRTD/NTWG Technical Report, Biometrics Deployment of Machine Readable Travel Documents v 2.0 (latest available in January 2005)
ICAO Technical Report, Use of Contactless Integrated Circuits in Machine Readable Travel Documents v 4.0 (latest available in January 2005)
ICAO Technical Report, Digital signatures for MRTDs v 4 (latest available in January 2005)

ISO Standards

ISO 7501 parts 1 – 3, ISO endorsement of ICAO 9303 parts 1 – 3.
ISO 1073 part 2, Character sets for OCR-B – shapes and dimensions.
ISO 1831, Printing specifications for Optical Character Recognition.
ISO 3166 part 1, Country codes.
ISO/IEC 7810, Identification cards – physical characteristics.
ISO 7816, Several parts covering various aspects of contact smart cards.
ISO 8601, Interchange formats - representation of dates and times.
ISO 10373, Several parts covering test methods for various types of cards.
ISO/IEC 14443, Several parts covering proximity contactless integrated circuit cards (proximity implies reading at up to 10 cm).
ISO 18031-1 ISO-compliant driving licence — Part 1: Physical characteristics and basic data set

EU legislation on passports and travel documents
Council Regulation (EC) 2252/2004 is extended by the addition of the second part (introduction of biometric identifiers (fingerprints)).
Council Regulation of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by member states (2004/L 385/01)
Resolution of 17 October 2000 supplementing the resolutions of 23 June 1981, 30 June 1982, 14 July 1986 and 10 July 1995 regarding the security characteristics of passports and other travel documents (2000/C 310/01)
Resolution of 10 July 1995 supplementary to the resolutions of 23 June 1981, 30 June 1982, 14 July 1986 concerning the introduction of a passport of uniform pattern (1995/C 200/01)
Resolution of 14 July 1986 supplementary to the resolutions of 23 June 1981 and 30 June 1982 concerning the introduction of a passport of uniform pattern
Resolution of 30 June 1982 supplementary to the resolution of 23 June 1981 concerning the adoption of a passport of uniform pattern (1982/C 179/01)
Resolution of 23 June 1981 (1981/C 241/01) concerning the adoption of a passport of uniform pattern

EU legislation on visa
Council Regulation of 29 May 1995 laying down a uniform format for visas (1995/L 164/01)
Council Regulation of 18 February 2002 amending Regulation of 29 May 1995 laying down a uniform format for visas (2002/L 53/07)

EU legislation on resident permits
Council Directive 2002/1030 of 13 June 2002 on the introduction of a uniform model for residence permits for third-country nationals

EU legislation on driving licences
COM 2003 (621) Proposal for a Directive EC of the European Parliament and of the Council on driving licences
Council Directive 97/26/EC of 2 June 1997 amending Council Directive 91/439/ECC on driving licences
Council Directive 1996/47/EC of 23 July 1996 amending Council Directive 91/439/EEC on driving licences
Council Directive 1991/439/EEC of 29 July 1991 on driving licences

EU legislation on vehicle registration documents
Council Directive 2003/127/EC of 23 December 2003 amending Council Directive on the registration document for vehicles
Council Directive 1999/37/EC of 29 April 1999 on the registration document for vehicles

International Labour Organization
C185 Seafarers' Identity Documents Convention (Revised), 2003
C108 Seafarers' Identity Documents Convention, 1958
Report ILO SID-0002, Finger minutiae-based biometric profile for seafarers' identity documents

Bibliography

de Heij, H.A.M.
2000 “The design methodology of Dutch banknotes”, proceedings of SPIE, 3973, San José, USA

ICAO
2006 “The Foundation of the ICAO”, http://www.icao.int/icao/en/hist/history02.htm ICAO, Montreal.

ISO
2006 “ISO 18031-1 ISO-compliant driving licence — Part 1: Physical characteristics and basic data set”, abstract,http://www.iso.org/iso/en/CatalogueListPage.CatalogueList.
ISO, Geneva.

European Union
2006 Press release IP/06/872, New Secure Biometric passports in the EU, strengthen security and data protection and facilitates travelling

Lloyd, M.
2003 *The Passport: The History of Man's Most Travelled Document,* Sutton LTD, Stroud, UK

Mastenbroek, N. et al.
1995 “Identiteitsvervalsing”, *Studiereeks Recherche*, 4, Editors van Vliet, A., Knopjes, A., Broekhaar, J.M.J., Dutch National Police Agency, Zoetermeer, The Netherlands

Parlementair Documentatie Centrum
2006 “Parlementaire enquête paspoortproject (1984-1988)”, *Parlement & Politiek*, http://www.parlement.com/9291000/modules/g8pdhdiw, Parlementair Documentatie Centrum, The Hague.

Renesse, Rudolf L. van
1996 “Security design of valuable documents and products” Proceedings of the *Conference on Optical Security and Counterfeit Deterrence Techniques.* San José, California, USA, SPIE vol. 2659, pp. 10-27

Stauffer, E., Bonfanti, M.S.
2006 “Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles”, *Examination of Vehicle Registration Documents,* Academic Press, Burlington, USA.

Wikipedia,
2007 Caribbean Community, http://www.wikipedia.com

CHAPTER 3

PRODUCER

■ 3.1 Producer or system integrator?

Here we arrive at the stage where the issuing organization or authority seeks out a competent partner to help produce the desired end product.

As already mentioned in Chapter 1, the complexity of the document chain requires a certain expertise in order to ensure the proper working of the interfaces. That is why the term system integrator is frequently used. The system integrator overviews the entire chain and makes sure that all parts are compatible. Thus, he must be capable of working together with other parties. This cooperation is an important prerequisite to arrive at the product quality and the targeted security level. Likewise, it may be essential that agreements made on all relevant issues between the system integrator and other companies are laid down in a contract.

■ 3.2 Tender procedures

There are different ways to choose a producer. However, government and associated agencies in most countries have developed procurement policies in order to get maximum value for their money.

To enhance transparency, contracting authorities have decided to apply these policies, especially with respect to security documents whose production is to some extent considered a state secret (e.g. passports). Secure documents are often high-tech products which require expertise, but because only a small number of experts can provide this, contracting entities are increasingly setting their sights on foreign suppliers in order to find products that best suit their needs.

The economic value of public procurement, however, is directly affected by politics. Contractors could be under strong pressure to favour domestic suppliers over foreign competitors. The modern approach, which is largely based on the principle of free competition, calls to move away from such attitudes though.

Nevertheless, the political, social and economic dimension of public procurement orders awarded by public authorities is increasing. Therefore, it is vital that people involved in the development of a secure document know the relevant public procurement procedures, such as:

- which regulations and procedures apply;
- the point at which the contracting authority has to make a choice between tenders; and
- which issues must be addressed before the process can officially be started.

Answers to the above enable all parties concerned to effectively plan and pursue the tender process to a successful conclusion.

Legal sources mentioned hereafter
World Trade Organization (WTO):
Agreement on Government Procurement 1994 (AGP).

European Law:
Council Directive 93/36/EEC, coordinating procedures for the award of public supply contracts, which was adopted on 14 June 1993 and Council Directive 2001/78/EC on the use of standard forms in the publication of public contract notices.

■ 3.3 Agreement on Government Procurement

3.3.1 Source

The WTO Agreement on Government Procurement (AGP 1994) was signed in Marrakech on 15 April 1994 in the course of what is referred to as the Uruguay Round[1], and came into force on 1 January 1996. This

[1] The text of the AGP 1994 can be downloaded from the site www.wto.org/english/docs_e/legal_e/final_e.htm or viewed on www.wto.org/english/tratop_e/gproc_e/agrmnt_e.htm

agreement is found in Annex 4(b) of the Agreement Establishing the World Trade Organization. It is a **plurilateral** and not a multilateral agreement; not all WTO member countries but only the 39 parties[2] must adhere to it. By ratifying the AGP 1994, the signatory parties expressed their wish to harmonize their laws, regulations and administrative procedures with the dispositions held in the agreement before it came into force. That occurred at various levels. For instance, the European Union translated the agreement specifically into the Community Directive 93/36/EEC that became binding among EU member states.

3.3.2 Aim of the Agreement

The signatory countries basically wanted to create a new legal instrument in order to achieve greater liberalization and expansion of world trade and improve its international framework (Preamble AGP 1994).

3.3.3 Principles

Three basic principles underpin the AGP 1994: the principle of national treatment, the principle of non-discrimination, and the principle of transparency (Senti, 2000).

The principle of national treatment requires that "each Party shall provide immediately and unconditionally to the products, services and suppliers of other Parties (*read* countries) offering products or services to the Parties, treatment no less favourable than a) that accorded to domestic products, services and suppliers; and b) that accorded to products, services and suppliers of any other Party" (see Art. III (1) AGP 1994 and (2) Preamble AGP 1994).

The principle of non-discrimination requires that each Party ensures "that its entities shall not treat a locally-established supplier less favourably than another locally-established supplier on the basis of degree of foreign

[2] The signatory countries are: Canada, the European Union (27 member States), Hong Kong (China), Iceland, Israel, Japan, Korea, Liechtenstein, The Netherlands on behalf of Aruba, Norway, Singapore, Switzerland and United States of America. The complete schedule is published on the Internet site http://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm.

affiliation or ownership". Moreover, each Party must ensure "that its entities shall not discriminate against locally-established suppliers on the basis of the country of production of the goods or services being supplied, provided that the country of production is a Party to the Agreement" (see Art. III (2) AGP 1994 and Preamble (2) AGP 1994). Nevertheless, this principle is not absolute. It was the EU Commission's idea to adopt a flexible system which aims at encouraging other non-signatory countries (King et al., 1994) to become a Party to the AGP 1994.

The principle of transparency states that every Party should encourage entities to specify the formalities and conditions that apply to the acceptance and awarding of contracts. (Preamble (3) AGP 1994 and Art. XVII AGP 1994).

3.3.4 Application

The AGP 1994 is applicable to the entities that operate within the signatory states. Specifically, it applies to orders procured by the awarding entities specified in Appendix I, Annex 1 (containing central government entities which procure in accordance with the provisions of the agreement), Annex 2 (containing sub-central government entities) and Annex 3 (containing all other entities that procure in accordance with the provisions of the agreement)[3].

There are no AGP 1994 provisions that regulate the awarding of public procurement by international organizations. The Annex of Appendix I also make no reference[4]. Consequently, their awards are not subject to it. In any case, organizations such as the International Monetary Fund or the United Nations award their orders according to the basic principles of transparency, efficiency, and cost-effective use of public funds, in the same way as the signatory countries agreed to trade in the AGP 1994. The types of procedures are also similar to those in AGP 1994[5].

[3] For complete annexes of the signatory countries: http://www.wto.org/english/tratop_e/gproc_e/loose_e.htm

[4] Some International Organisations are observers; for more details visit: http://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm

[5] For the definition of SDR, see http://www.imf.org/external/np/exr/facts/sdr.htm

Additionally, AGP 1994 regulates the award procedure of public supply contracts, public construction work and services.

3.3.5 Thresholds

The agreement applies to contracts worth more than the specified threshold values. These thresholds, indicated in the Annex of Appendix I (Art. I (4) AGP 1994), are specific to each signatory state. For central government purchases of goods and services, the threshold is SDR (Special Drawing Right)130,000[6]. For purchases of goods and services by sub-central government entities, the threshold varies, but it is generally about SDR 200,000. For utilities, thresholds for goods and services are generally about SDR 400,000, and for construction contracts the threshold value is around SDR 5,000,000.

3.3.6 Types of procedure

The AGP 1994 provides for three types of procedure: open tender, selective tender, and limited tender.

In an open tender procedure, all suppliers are invited to tender (Art. VI (3) (a) AGP 1994). In the selective tender procedure, only suppliers invited by the awarding authority may tender (Art. VI (3) (b) AGP 1994). "To ensure optimum effective international competition under selective tender procedures, entities shall, for each intended procurement, invite tenders from the maximum number of domestic suppliers and suppliers of other Parties consistent with the efficient operation of the procurement system. They shall select the suppliers to participate in the procedures in a fair and non-discriminatory manner" (see Art. X (1) AGP 1994).

In the limited tender procedure, the awarding authority contacts suppliers individually. This procedure is applicable according to the provisions laid down in Art. XV AGP 1994: e.g. "for works of art or for reasons connected with protection of exclusive rights, such as patents or

[6] Method A has been rejected by the Swiss Cantonal tribunal of Fribourg. Method B is a guide on public procurement published by a Swiss canton. Method C was developed by two Swiss experts, Pictet and Bollinger.

copyrights, or in the absence of competition for technical reasons, the products or services can be supplied only by a particular supplier and no reasonable alternative or substitute exists" (see Art. XV (1) (b) AGP 1994).

■ 3.4 Aspects of the tender procedure

Below is a checklist of the procedure to be followed in the tender process:

- Select the appropriate tender procedure.
- If the procedure is selective, define the selection criteria.
- Prepare tender documents (define product/services), including the list of requirements.
- Define award criteria and calculation methods for awarding points.
- Choose time limits in accordance with legal sources.
- Prepare a notice or call for tenders.
- Set up an award commission.
- Draw up a report.
- Draw up an award notice.

In the sections below, AGP 1994 and European law will be referred to as examples.

3.4.1 Select the appropriate award procedure

In general, a contracting authority will prefer either an open or a restricted procedure. In Europe, the negotiated procedure (same as the limited in AGP) is restricted to situations specified in Art. 6 (2) and (3) of Directive 93/36/EEC.

The technological value of secure documents renders them unique. In order to prevent counterfeiting and alteration, they are produced from exclusive raw materials using sophisticated technological methods. Their production process is characterized by discretion and secrecy. This is the reason why in some cases, contracting authorities opt for the negotiated procedure.

However, contracting authorities often choose the selective tender procedure because it offers transparency of products and prices. This is also known as an open two-part procedure. In the first part or pre-qualification, potential suppliers apply for qualification to participate. In the second, only suppliers which qualify are invited to submit a tender after they received the list of requirements.

3.4.2 The selective procedure

In the selective procedure, only suitable suppliers are allowed to bid. The awarding commission selects the suppliers that meet the selection criteria specified in the notice or call for tenders. This selection can take place at any given time before or during the award phase. AGP 1994 recommends that "in the process of qualifying suppliers, entities should not discriminate among suppliers of other Parties or between domestic suppliers and suppliers of other Parties."

In selections prior to awarding, the awarding authority announces the pre-qualification in the notice. At the end of this phase, the selected suppliers are invited to tender.

For selections during the award phase, pre-qualification takes place just before valuation of the tenders. The awarding commission verifies whether the tender bidders fulfil the selection criteria. The basic procedure is as follows. A supplier submits two envelops: the first contains information regarding suitability and the second holds the technical data relevant to the tender. Tenders that do not meet the selection criteria are not opened.

The decision is based on "suitability" criteria (also called qualitative selection criteria), which are required to be published in the call for tenders. In the EU, Directive 93/36/EEC specifies the conditions under which suppliers may be excluded from participation in a contract (Art. 20).

The Directive also instructs contracting authorities to evaluate the suitability of candidates on the basis of criteria pertaining to economic, financial and technical capacity. In order to assess suitability, the awarding entities may request candidates to furnish a series of documents in conformity with Art. 22 and 23 of the Directive. These include the following: appropriate bank statements, balance sheet information, evidence of overall turnover and turnover with respect to the products to which the contract relates over the previous three financial years, a list of the principal product deliveries/services provided over the previous three years, a description of the supplier's technical facilities, its quality control measures, its study and research facilities, details on the technical bodies and personnel, samples, description and/or photographs of the products to be supplied, and certificates drawn up by official quality control institutions.

A security check might also be a selection criterion which would involve physical security of the plant, for example.

3.4.3 Documentation

The Art. XII and VI of AGP 1994 give information on technical specifications and documentation, which the contracting authority should include in the procedure. The following paragraphs are quoted from the agreement.

The list of requirements defines the "characteristics of the products or services to be procured, such as quality, performance, safety and dimensions, packaging, marking and labelling, or the processes and methods for their production and requirements relating to conformity assessment procedures prescribed by procuring entities" (Art. IV AGP). Technical specifications should not be drawn up "with a view to creating unnecessary obstacles to international trade," but "should be based on international standards, where such exist; otherwise, on national technical regulations or recognized national standards. There shall be no requirement or reference to a particular trademark or trade name, patent, design or type, specific origin, producer or supplier, unless there is no sufficiently precise or intelligible way of describing the procurement requirements and provided that words such as 'or equivalent' are included in the tender documentation."

"Tender documentation provided to suppliers shall contain all information necessary to permit them to submit responsive tenders, including information required to be published in the notice of intended procurement, and the following:

- the address of the entity to which tenders should be sent;
- the address where requests for supplementary information should be sent;
- the language(s) in which tenders and tendering documents must be submitted;
- the closing date and time for receipt of tenders and the length of time during which any tender should be open for acceptance;
- the persons authorized to be present at the opening of tenders and the date, time and place of this opening;
- any economic and technical requirement, financial guarantees and information or documents required from suppliers;
- a complete description of the products or services required or of any requirements, including technical specifications, conformity certification, necessary plans, drawings and instructional materials;
- the criteria for awarding the contract, including any factors other than price that are to be considered in the evaluation of tenders and the cost elements to be included in evaluating tender prices, such as transport, insurance and inspection costs, and in the case of products or services of other Parties, customs duties and other import charges, taxes and currency of payment;
- the terms of payment;
- any other terms or conditions."

The entities will forward the tender documentation to any supplier participating in the tender procedure by way of an open procedure, to any supplier requesting to participate in a selective procedure, and to suppliers invited to submit a bid in a limited or negotiated procedure.

All conditions included in the notice represent the *lex specialis* of the tender procedure and are binding for the tenderers as well as for the contracting authority.

3.4.4 Award criteria

The tenders are evaluated on the basis of the award criteria stated in the tender documents or in the notice. In accordance with the publicity principle, the contracting authority is not allowed to adopt criteria during the award procedure other than the ones advertised in the notice. The award criteria enable the award commission to critically evaluate the tenders.

A. Price

The best tender for a contract could be the cheapest one (Art. 26 (1) (a) Directive 93/36/EEC) or the most economically advantageous (Art. 26 (1) (b) Directive 93/36/EEC). However, cost as a criterion is more appropriate for standard products. Given the technological complexity of the production of secure documents, additional criteria besides the price should be used in the evaluation of tenders in this area. For instance, a ratio between cost and technology level could be set.

B. Multiple criteria

Where secure documents are concerned, evaluation should be based on multiple criteria. In the EU Art. 26 (1)(b) of Directive 93/36/EEC suggests e.g. price, delivery date, running costs, cost-effectiveness, quality, aesthetic and functional characteristics, technical merit, after-sales service and technical assistance. The European Commission recently published two interpretative communications on Community law that apply to public procurement and the possibilities for integrating environmental and social considerations into public procurement (Official Journal, 1993). The contracting authority is free to define alternative or supplementary specific award criteria, e.g. user-friendliness.

The following could be used as award criteria:

- Technological level of the producer: has the producer kept up with technological developments? For instance, if the contracting party decides it wants to radically update their document, does the producer have the proper equipment, know-how and technology to carry out the desired innovations?
- Project team: There have been examples in which contracting parties were confronted with completely different teams after the order had been awarded. Such situations could lead to delays or the production of a wrong product.

It would be unfortunate if national interests stood in the way of awarding a contract to a foreign producer. The state-of-the-art techniques that are available these days are not accessible to the general public. That means that the number of providers of sophisticated technology is limited, and that sometimes a technology that a producer would like to see applied in his document is unavailable in his own country. If the requirements that a producer must meet are not well formulated, national producers could be quickly excluded from bidding for a contract. Such exclusion often brings in political debate.

C. Awarding points

The method of grading or awarding points to the tenders is the part of the process that receives the most attention. How many points should a tender be awarded for a specific award criterion? The following examples illustrate just how difficult it is to hit upon the best method of giving points. Here are some calculation methods for the criterion of price.

Table 1: Calculation methods[7]

Method A

Tender	Price	Difference in % with respect of the best tender	Points
A	514,000	0.0	3
B	514,650	0.12	2.5
C	578,000	12.45	2

Method B

Tender	Price	Difference in % with respect of the best tender	Points
A	514,000	0.0	3
B	514,650	0.12	2.99
C	578,000	12.45	2.66

Calculation of the number of points: $\frac{\text{lowest price x max. points}}{\text{prices offered by tenderer}}$

[7] Method A has been rejected by the Swiss Cantonal tribunal of Fribourg. Method B is a guide on public procurement published by a Swiss canton. Method C was developed by two Swiss experts, Pictet and Bollinger [Council Directive, 1997].

Method C

Tender	Price	Difference in % with respect of the best tender	Points
A	514,000	0.0	3
B	514,650	0.12	2.96
C	578,000	12.45	0

Calculation of the number of points: $\frac{\text{(highest price - price of the gender) x max. points}}{\text{highest price - lowest price}}$

The number of points scored by the three methods varies considerably. The method of awarding points may remain secret and not be available to the tenderers. This allows the contracting authority considerable latitude in assessing the tenders. On the other hand, if the method is known to the tenderers, the offer would probably reflect the award criteria.

3.4.5 Time limits for tendering and delivery

In order to guarantee equality of treatment between tender bidders, it is important to establish non-discriminatory time limits. These are defined with a view to allowing each candidate to draw up a tender on an equal footing with other contenders.

Table 3.1: Time limits

Type of procedure	**EU Directive "Supply"**	**AGP Art. XI**
Open procedure	Minimum period between dispatch of notice to the Official Journal of the European Communities and closing date for the receipt of tenders: 52 calendar days.	Not less than 40 days from the date of publication.
Selective procedure	Request to participate, minimum period between dispatch of notice to the Official Journal of the European Communities and closing date: 37 calendar	Not less than 25 days for submitting an application to be invited to tender. Period for receipt of tenders not less than 40 days from date of

Type of procedure	EU Directive "Supply"	AGPArt. XI
	day; accelerated procedure 15 calendar days. Invitation to tender, minimum period between dispatch of invitation to tender and closing date: 40 calendar days; accelerated procedure 10 days.	than 40 days from date of issuance of the invitation to tender.
Limited or negotiated procedure	Invitation to tender, minimum period between dispatch of notice to the Official Journal of the European Communities and closing date: 37 calendar days.	Period for receipt of tenders not less than 40 days from date of issuance of the invitation to tender (whether or not this date coincides with the date of publication).

AGP also provides for circumstances that allow for reduction of the above periods (Art. XI (3)).

3.4.6 Notice (call for tenders)

The notice is an administrative instrument used by the contracting authority to invite potential bidders to submit a tender. It contains rules and conditions that apply to the award procedure.

The notice should not only contain formal information necessary to ensure a proper award procedure, but also all the technical information required by the bidders to draw up a customized tender.
EU member states are required to draw up notices in accordance with the provisions in Directive 93/36/EEC (Art. 9 (4)) and the new directive on the use of standard forms in the publication of public contract notices (2001/78/EC), amending annex IV of Directive 93/96/EEC.

3.4.7 Setting up an award procedure

During the award procedure, the awarding commission evaluates the tenders submitted by the suppliers by means of the evaluation criteria. This activity culminates in the award of the contract to the most suitable supplier.

The awarding authority is free to organize this activity in any way it chooses. It independently sets up an award commission made up of various experts, e.g. legal or financial advisers. In the case of secure documents it is not unusual for representatives of law enforcement agencies or the border control authority to be part of an award commission. These experts assess the security aspects, analysing whether the solutions offered fulfil the technical requirements with respect to security features or personalization, aspects which could be award criteria.

3.4.8 Report

The AGP requires that for each contract awarded, a written report that includes all information pertaining to the tender procedure is drawn up by the contracting authority. Basically, the contracting authority clarifies why it has selected a particular tender from among the other bidders, and, if known, indicates which part of the contract the winning bidder plans to subcontract to third parties.

3.4.9 Award notice

Art. XVIII AGP 1994 states that "entities should publish a notice in the appropriate publication listed in Appendix II no later than 72 days after the award of a contract under Articles XIII through XV. These notices shall contain:

- the nature and quantity of products or services in the contract award;
- the name and address of the entity awarding the contract;
- the date of award;
- the name and address of the winning tenderer;
- the value of the winning award or the highest and lowest offer taken into account in the award of the contract;
- where appropriate, means of identifying the notice issued under paragraph 1 of Art. IX or justification according to Art. XV for the use of such procedure; and
- the type of procedure used.

European rules stipulate that contracting authorities that have awarded a contract are required to make the results public by means of a notice. "However, entities may decide that certain information be withheld where the release of such information would impede law enforcement or otherwise be contrary to the public interest or would prejudice the legitimate commercial interests of particular enterprises, public or private, or might prejudice fair competition between suppliers. Contract award notices must be sent not later than 48 days after the contract in question has been awarded and has been published in full in the Official Journal of the European Communities." (Directive 93/36/EEC Art. 9 (3), Art. 9 (5), Art. 9 (6)).

3.4.10 Case of abnormally low prices

In the European Union, "if tenders appear to be abnormally low in relation to the goods to be supplied, the contracting authority shall, before it may reject those tenders, request in writing details of the constituent elements of the tender which it considers relevant and shall verify those constituent elements taking account of the explanations received" (see Art. 27 Directive 93/36/EEC).

This directive specifies the kinds of explanations the contracting authority may take into consideration: "explanations relating to the economics of the manufacturing process, or to the technical solutions chosen, or to the exceptionally favourable conditions available to the bidder for the supply of the goods, or to the originality of the suppliers proposed by the bidder."

The aim of this detailed procedure for verification of the tenders is twofold: on the one hand to protect tenders from arbitrary evaluations by the awarding authority; and on the other, to protect the awarding authority from bidders that may not be able to guarantee a long-term contract.

■ 3.5 The contract

3.5.1 Purpose and content of the contract

The contract between the contracting party and producer is an official, legal guarantee of that which both parties have agreed upon regarding the provision of the products and/or services.

In effect, such a contract is drawn up as a safeguard against the worst possible situation. The contract becomes crucial particularly if problems arise in the contractual relations, e.g. if the parties fail to meet their obligations. In such a situation it is very important that each of the parties can fall back on a contract that provides for clear and unequivocal provisions.

The contract, however, never leaves the filing cabinet, if the services are rendered as was agreed upon, as is most often the case. For the operational management of the provision of services, a Service Level Agreement (SLA) is a far more useful instrument.

A contract also stipulates conditions that are tailored to the specific nature of the services and relationship between the parties concerned. However, the main part of the contract contains a number of general provisions that usually also apply to the products and services being discussed in this book.

3.5.2 From draft contract to contract management

A. Draft contract as part of the tender

As seen in Section 3.2, the selection of a new producer usually occurs by means of a tender procedure. Irrespective of the exact procedure, the tender must be based on a list of requirements or a tender document. The draft contract must also be included in the list. This makes the situation clear to both parties. The contracting party receives information on which provisions may present problems, and the producer, or aspiring producer, learns what the contracting party's terms of delivery are. The producer also has the opportunity to indicate which conditions he either cannot or does not wish to meet, and which alternatives he proposes to do in their stead.

All parts of the draft agreement prior to the tender do not have to be worked out in detail. Some provisions can be fleshed out later once more is known about the producer's bid. It is often inevitable that the final contract is only negotiated after the contract has been awarded.

B. Negotiating and signing the contract

As already stated, after awarding, negotiations are conducted on the final details and any changes that the producer may have proposed during the tender procedure. Although considerable agreement may have been reached in the pre-negotiation stage, the negotiations themselves are often very time-consuming. Topics such as intellectual and industrial property rights, liability, penalties and damage receive the most attention.

After the contract has been awarded, there is huge pressure to immediately commence operations. In order to prevent delays due to the negotiations, the contracting party and producer may opt to sign a declaration of intent immediately following the award, which provides for an obligation to rapidly conclude the negotiations and sign the contract. A salient point here is that such a situation may weaken the negotiating position of the contracting party.

C. Contract and SLA management

As was already explained above, it is not uncommon for a contract to be stored away after signing only to be retrieved when the expiry date comes up.

More and more often, a Service Level Agreement (SLA) is drawn up to serve the operational control of the provision of services. It is part of the contract and applies to the operational stage. It can only be drawn up after all the particulars regarding the services are worked out and known. Usually this is shortly before the start of the operational stage.

The producer gives an account of the services he renders by means of interim reports. If there are deviations from the standards agreed upon, then certain procedures must be followed that should lead to improvement of the services so that the standards are met. Should the producer fail to perform as arranged, the contracting party may impose a fine.

3.5.3 Content of a contract

A. General provisions

The general provisions include definitions, the parties to the contract and the subject of contract. Moreover, the documents that are part of the contract, such as those used for the (European) call for tenders, must also be mentioned as well as their order of relevance.

B. The development phase

Although the contract focuses on the provision of services by the producer, as a rule the contract becomes effective as soon as it is awarded. Given the nature of the specific services being discussed here, the operational phase is preceded by a period of development, construction, testing, and acceptance of the products and services. Therefore, the contractual provisions for the development phase differ from those for the operational phase. It is therefore advisable that the contract distinguishes a development and operational phase.

As far as the development phase is concerned, certain agreements have to be made regarding the procedures for meetings and decision-making, and especially how these are to be committed to writing. The products and services developed and completed in this phase must also be specified. And in cases where more or less work is involved than initially estimated, again agreements will have to be made. Often, there is considerable debate on whether something does or does not fall within the contract's specifications. Agreements must also be laid down in the contract concerning the testing and official acceptance of the products and services by the contracting party.

It is also advisable to draw up a similar set of agreements for the operational phase. A situation can always arise in which the products and/or services must be altered during the operational phase, and that procedures similar to those that apply to the development phase may also have to be followed here.

C. Intellectual and industrial property rights

In cases where a producer or a third party manufacture ready-made products, the intellectual and industrial property rights are obvious. Matters become more complex when products and services are developed by a producer under contract to a contracting party. The question arises who the rightful owner is of the product, concept and/or system.

On the one hand, the contracting party might argue that the product, concept or system is developed on the basis of its list of requirements, and thus it has a claim to the property rights. It might want exclusive rights to the product, e.g. from a security perspective or, if the product is either partially or entirely reused, it could claim compensation for capital outlay.

The producer, on the other hand, might claim that its commercial prospects would be seriously restricted if it were prohibited from selling the marketed products and services to other parties. In the area of secure documents, this would often affect the core business of such producers.

One way to break this impasse is to distinguish between concepts and general solutions, on one hand, which would remain the domain of the producer, and, on the other, the specific, unique applications for the contracting party, which may not be sold to a third party without the permission of the contracting party. Experience shows that this subject often unleashes intensive negotiations and debate.

D. Products and services

The contract should include a detailed description of the products and services to be provided. It may be worthwhile here to distinguish between the development phase and the operational phase. For instance, the development phase could be accompanied by a description of *how* the service will be organized and provided, while the operational phase could indicate *what* the specifications of the service are.

E. The provision of information, security and other requirements

Certain information of the producer relating to the service could be important to the contracting party. This information, for example, might be production data which is necessary for invoicing or management. It is important to safeguard this provision of information and to see to it that it is provided for in the contract.

Depending on the nature of the products and services, the contracting party may require that certain conditions regarding physical, organizational and data security are met. Responsibility for assessing whether the producer continues to meet requirements in terms of administrative organization and responsibility for physical, organizational and data security are best borne by an independent third party (auditor). The obligation to carry out these assessments, usually annually, should be included in the contract.

F. Penalty clause

As with intellectual property rights, provisions for penalties, liability and damage assessment can also be a cause for disagreement. The producer will try to keep the fines for failing to perform up to par as low as possible, and attempt to buy extra time to rectify his omissions. This would seem to be an effective instrument for a contracting party to force the producer to perform as contractually agreed upon. Experience shows that both the provision of services as well as the mutual relationship benefit from an effective penalty clause. After all, the ultimate objective is to achieve the quality of services as agreed on.

During the development phase, certain crucial milestones would be agreed upon, whereby penalties are linked to failures to meet the agreed performance agreed. The entire development phase is divided into such milestones, which served to help manage the phased completion of intermediate and end products for the contracting party.

Experiences with this method vary. On the one hand, this approach helps to get products completed on time, but there is also great pressure to meet obligations at all costs, which sometimes occur at the expense of the quality of the product or the working relationship between the producer and contracting party.

G. Termination and dissolution

Besides termination of the contract by operation of law, there may be reasons to terminate or dissolve the contract prematurely. In all cases of termination, whether premature or not, it is important to reach agreements on how the transition to a new product is to be arranged with a view to the continuity of services to the contracting party. In this way it can be determined which measures the producer needs to take to ensure a smooth transition.

H. Disputes and escalation

Disputes may arise between the producer and contracting party, which cannot be resolved by the parties. Although civil law provides for solutions (e.g. put the case before the competent court), it is advisable to agree on the course of action to be taken should a dispute arise before taking a matter to court. Such an escalation clause distinguishes several levels within the organizations of the producer and contracting party, and stipulates the procedures that must be adhered to. And if, in spite of this, the parties are unable to resolve their differences, they can decide to go to arbitration or submit the dispute to the court.

I. The Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a useful instrument for measuring the performance of the producer and balancing this against the service standards contractually agreed upon. It may include the following aspects:

- agreements on the management of the SLA, on the consequences of failing to meet the standards defined, and on the reports and meetings to discuss the reports;
- standards and criteria for the completion of products and services;
- standards and criteria for financial and other management information to be supplied;
- procedures for changes in management and version supervision.

■ 3.6 The role of the governmental entity in the quality chain

In order to monitor continuity during the term of the contract, it is important that the customer appoints a member of the staff to liaise with the producer's organization in order to monitor jointly the quality related issues agreed in the contract. The customer representative handles internal and external communication, and initiates the necessary action for the uninterrupted issuing of documents conforming to the conditions of the contract. This person is also responsible for keeping an eye on the level of components, the level of partial products, the end stock for the finished product, and the production planning, with the objective of guaranteeing the continuity during the issuing process.

The producer should also have a Quality Assurance Department, which is responsible of the management of the quality handbook and internal quality audits. It also supervises compliance and the correct handling of the agreed upon procedures, takes initiative for improvement and reports directly to management in an independent place within the organization of the producer for open communication. The totality of these measures should guarantee an uninterrupted and correct qualitative delivery of the products in the contract.

The producer will also have to make all arrangements to optimize and maintain the production processes during the term of the contract so that the quality agreed upon with the customer can be guaranteed. This control effort focuses on the production tools, the organization of the production, the auxiliary materials as well as on increasing and maintaining the knowledge level of the personnel, with the objective of maintaining or responsibly adjusting the process parameters found and recorded during the development phase.

Furthermore, during the term of the contract, it must be unambiguously recorded who is specifically responsible within the organization for the production components in relation to the quality norms agreed upon with the customer. In a modern company, this responsibility must be placed as deep as possible within the organization, preferably by the production employee who performs the component assignment. The production departments use the measurement and testing equipment necessary for their processes. Moreover, the producer must use a laboratory that is able to professionally perform other tests requiring special knowledge or specific research equipment.

Management must also see to the optimum organization of the work so the execution of the process is handled smoothly and efficiently.

References

Senti R.,
2000 System und Funktionsweise der *Welthandelsordnung*, Zurich, 2000, p. 671

King M., De Graaf G.,
1994 L'Accord sur les marchés publics dans le cadre de l' "*Uruguay Round*", RMUE 4/1994, p. 75-76

1993 Official Journal L 199, 09.08.1993, p. 1-53

1997 European Parliament and Council Directive 97/52/EC of 13 October 1997 amending Directives 92/50/EEC, 93/36/EEC and 93/37/EEC concerning the coordination of procedures for the award of public service contracts, public supply contracts and public works contracts respectively; Official Journal L 328, 28.11.1997, p. 1-59

CHAPTER 4

THE CHAIN FROM APPLICATION TO ISSUANCE

This chapter goes into a number of aspects relating to the application and issuance procedures of secure documents as well as the logistics involved. Although these processes do not form part of the technological development of a secure document, experience teaches us that the basis of fraud in the broadest sense of the word is often laid in the application and issuance stages.

Below is a brief description of a day in the life of a businessman named John, which gives you some idea of the kinds of documents we use daily. Based on those documents we will later proceed to identify the issuers.

> John has an appointment with a potential customer in another country. To get there, John buys an *airline ticket*. He leaves at 5:30 a.m. to arrive at the airport on time. Of course, John is carrying his *driving licence*, his *vehicle registration document* and his *insurance certificate*.

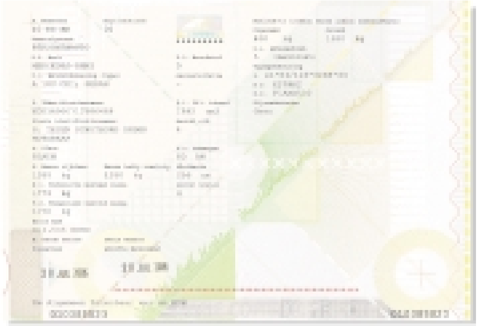


Figure 4-1: The vehicle registration document of the Netherlands.
(Courtesy of Fons Knopjes, the Netherlands).

When he arrives at the airport, John parks his car in a car park. To enter the car park he uses his *credit card*. In the departure hall he goes to the check-in desk, where he is asked to present his *travel document* and answer a few questions, after which a *boarding pass* is printed for him. As a regular traveller, John is naturally a member of a loyalty program and has his points stored on his *loyalty card*.

He then proceeds to immigration where he is asked to present his travel document and his boarding pass and state his destination. The immigration officer checks his travel document, runs it through the Machine Readable Zone (MRZ) reader and consult the watchlist. John then receives permission to cross the border and proceeds to the plane. Before boarding, John quickly buys a cup of coffee and a croissant, for which he pays with a *banknote* and returns the change to his wallet. His flight is announced and he boards the plane.

When he reaches his destination, John presents his travel document to the immigration officer, and he is permitted to enter the country. After a short taxi ride, he arrives at the agreed place. When he enters the company building, he is asked to show an *identity document*. John hands his ID card over to the receptionist, who enters his data into a system and gives him a *company badge*. John is then collected for his meeting.

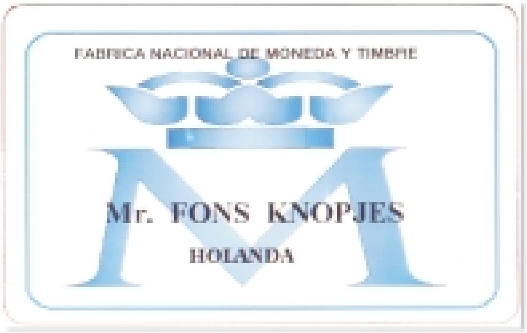
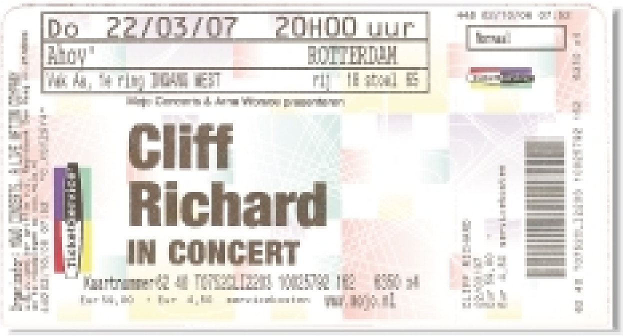


Figure 4-2: Example of a company visitors badge of the Fabrica Nacional de Moneda y Timbre.
(Courtesy of the Fabrica Nacional de Moneda y Timbre, Madrid, Spain).

The company badge appears to contain a contactless chip, which allows John to pass through the various zones in the company. The meeting proves productive and the participants take leave of each other after lunch.

John returns to the airport, where he goes through the whole process of checking in, crossing the border and boarding the plane again. After landing, John picks up his car, leaves the car park and uses his credit card to pay for the parking fee. On his way home, John pulls into a petrol station, where he refuels, paying with his *debit card*. The cost of the fuel is directly debited from his bank account and transferred to the petrol station owner's account. Upon his arrival home, his wife surprises him with *tickets* for a theatre performance.



Do 22/03/07 20H00 uur

Ahoy' ROTTERDAM

rij 18 stoel 65

Cliff Richard

IN CONCERT

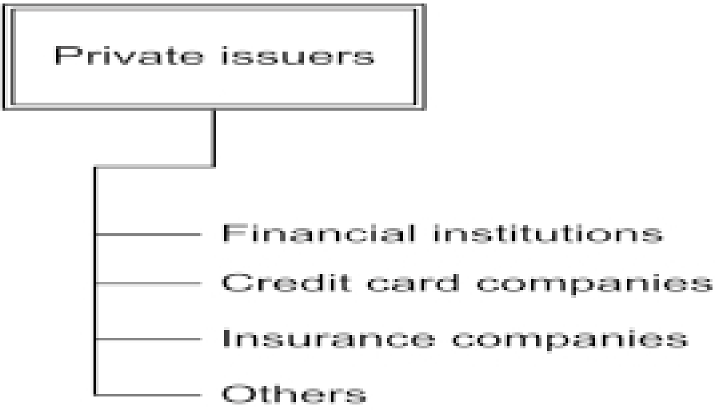
www.mojo.nl

Figure 4-3: The ticket for a concert of Cliff Richard.
(Courtesy of Fons Knopjes, the Netherlands)

They go to the theatre by public transport for which they use a special *contactless chip card* on which a sum is stored. The fee for each ride is debited from the card.

Many of us can identify with this brief impression of a day in the life of John, which clearly illustrates how frequently we use valuable documents.

Figure 4-1 shows the possible issuers of a secured document, taking in account the two most secured categories (see Chapter 1, Figure 1-1).



By private issuers add others.
Figure 4- 4: Issuers

■ 4.1 Governmental issuing authorities

There are many different issuing authorities of secure documents. An important distinction should be made between the issuance of documents by the government and the issuance of documents by the private sector. The government usually issues documents for the general benefit of society, whereas the private sector often provides documents that link the users to the issuer. However, only the government has the sole right to issue certain types of documents, giving it a monopoly. This is logical, given the important social value that these documents represent. Such documents include travel documents and identity documents, driving licenses, alien documents, and extracts from the population register.

The following is a brief overview of a number of government authorities that are tasked with the issuance of documents.

4.1.1 Passport Office

Anglo-Saxon countries often have passport offices assigned to provide citizens with a travel document. But not every town or city has a passport office. Usually there are only a few passport offices in a country. This geographical spread has logistic consequences for the application and provision of travel documents. The United Kingdom, for example, has 7 regional passport offices. In turn, these offices make use of around 2500 "street partners" (currently Post Office branches), which see to it that the citizen is provided with the necessary application forms. Citizens fill in these forms and send them to the regional offices. In order to determine whether or not an application for a travel document is legitimate, these offices may consult various government databases, such as the register of births, deaths and marriages, the tax register, etc. Searching these databases is necessary to verify the identity of the applicant. This method facilitates the detection of fraudulent applications.

4.1.2 Municipality

In many other countries, local governments, such as municipalities, play an important role in the issuance of documents. Such local entities are close to the citizens and thus close to the applicants documents. Municipalities often manage the personal data of the local population, which enables them to verify the identity of an applicant before proceeding to provide a document. The birth of a child, for instance, is registered with the municipality, which enters this in its population database. In many cases, birth data is a means to verify the identity of an applicant. The same holds true for citizens who move to a different municipality or die. All this data must be carefully and meticulously managed. The municipality may, often on government instruction, make use of the population database for the issuance of a travel or identity documents. In other cases the birth certificate is used as an identity proof for the issuance of a travel or identity document. Lack of management of the identity chain is a potential risk for identity fraud.

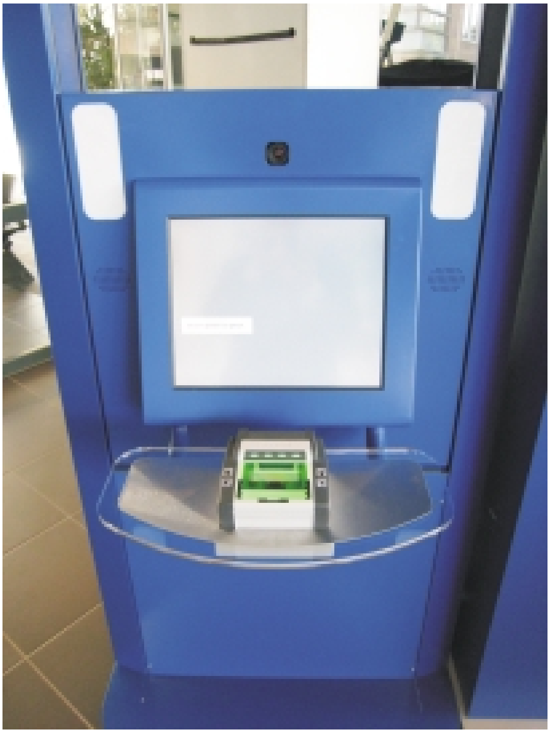


Figure 4-5: The life capture for photographs as a part of the application process of the Hong Kong ID card. (Courtesy of Fons Knopjes, the Netherlands)

4.1.3 Police

The police can also be tasked with the issuance of documents. In many countries, the citizens are required to apply for a driving license or passport at their local police station. Like the passport office, the police may also consult government databases in order to verify the identity of an applicant. Obviously, the police also have their own databases with information on criminal incidents and offences. Before a secure document is issued, these databases may be consulted. If it appears that an applicant has an outstanding fine, the police may demand its immediate settlement, or, in more serious cases, the police may detain the applicant. By assuming the role of issuing authority, the police are highly capable of preventing wanted persons from leaving the country undetected. The police have the same powers with respect to the provision of a driving license to applicants that display dubious driving behaviour.

4.1.4 Immigration Service

Many people think that the task of immigration services is restricted to checking travel documents at borders and airports. They have no idea that many immigration services worldwide also issue documents. Sometimes they only issue a limited number of documents, but in some countries important documents, such as passports, visas, residence permits and work permits are also issued by immigration services. If an immigration service is tasked with the issuance of all documents, the facilities for verification of the identity of an applicant are comparable to those of a police service. Often, immigration services are only authorized to issue travel documents in emergency situations in other cases they issue residence permits. In those cases, verification of an applicant's identity could be problematic, if the immigration services wouldn't have access to the information necessary to verify a person's identity. However, immigration service staffs have considerable expertise in the area of documents and identity control. Before a contingency document is issued, numerous questions are posed and where possible relevant documents requested so that the identity of the applicant can be verified.

In the last couple of years many countries have implemented so-called Trusted Traveller Programs where the identity of the traveller and his right to access the country are at once determined by the immigration services. This process is associated to the issuance of a card which in some cases contains biometric features for fast identity verification (see Chapter 7).

4.1.5 Driver Licensing Office

In many countries, the office for the provision of driving licenses is a separate organization. Often this office not only issues driving licenses, but also other documents related to motor vehicles, such as vehicle registration and car ownership documents. Similar to the above services, the driver licensing office can also consult various databases. The steps taken prior to the application for a driving license are also very important. Sufficient safeguards must be in place to ensure that an authentic driving license is issued to someone who has proven driving proficiency. This may sound evident, but the exchange of foreign driving licences has been happening for many years without any verification of the driving proficiency of the applicant, resulting in a potential risk for road safety.

Besides acting as a certificate of driving proficiency, the driving license often also functions as a national identity document. In countries where this is the case, a driving license is a very important and may be used to apply for other documents. Therefore, it is the task of these offices to ensure proper identity confirmation. In the United States, the Department of Motor Vehicles in some states (e.g. Oregon, California, Florida) is even tasked with the issuance of identity cards.

■ 4.2 Private sector as the issuer

A vast number of entities in the private sector may also issue documents. These include a number of large parties, such as financial institutions, insurance companies, credit card companies, employers, etc. In the sections below the main players will be briefly introduced.

4.2.1 Financial institutions

A large number of financial institutions, such as banks and credit institutions, issue their own documents. The criteria for the issuance of these documents vary widely, depending on the institution. These documents, usually bank cards, are an important link in the financial transactions between a bank and a bank card user. Although the verification of the user's identity is not the main task of the financial institution, nevertheless they want to be sure of their client's reliability. Moreover, the acceptor of a document demands guarantees that the financial institution that has issued the bank card vouches for all the transpiring financial transactions. It is therefore essential that these documents are reliable.

4.2.2 Credit card companies

Another type of institution that also issues financial documents is the credit card company. Similar to financial institutions, various credit card companies maintain their own rules for the issuance of documents. It is not uncommon for a credit card company to issue a document on the basis of a written application without ever having seen the applicant or having confirmed his identity. Often, a copy of an ID serves as the basis for verification. It is true, however, that credit card companies have their own methods to determine the reliability and financial position of an applicant.

4.2.3 Insurance companies

A completely different kind of organization that also issues valuable documents is the insurance company. Insurance companies operate in all sectors, one of which is health care. Health insurance companies issue documents to their members in the form of a client pass. Such a pass gives the holder access to health care.

4.2.4 Other private issuers

The list of other private issuers is very long and includes supermarkets, retail stores, hotels, airlines, newspapers, health clubs, etc. The issued documents are mostly showing limited personal data (a very small number of them has an integrated photograph of the holder) and has functional verification features (layout and colour). The security level of these cards is on the whole very low.

■ 4.3 Application procedure

The application procedure is the first link in the document chain. It determines whether or not an applicant is eligible for a particular document. The identity of an applicant plays an important role here, because it must be established whether an applicant may indeed be issued a particular document, or whether he is an impostor or a look-alike. Depending on the type and purpose of the document, the issuing authority must constantly be on the alert for misuse. Identity theft is on the rise, and the misuse of someone's identity often has far-reaching consequences for the rightful owner of that identity.

The application procedure, therefore, must also make a distinction between a first application and the extension of an existing document. In the first case, greater care will have to be given to the verification of the applicant's identity and whether an applicant has the right to a certain document. In the case of an extension, many issuers would be satisfied with a bare confirmation of the existing data. This may become a risk in a low-profile identity management environment.

A document may be applied for in the following different ways:

- by appearing in person at the issuing authority;
- by filling in and returning an application form;
- by making use of intermediary authorities;
- by applying online.

4.3.1 Appearing in person at the issuing authority

Depending on the type of document and the location of the issuer's offices, an applicant is required to appear in person, which in itself has many advantages. For instance, it can be confirmed on the spot that a person is still alive. The applicant can also answer questions directly relating to his application, making verification easier.

The issuing authority has access to several registers to carry out verification. If the issuer is a municipality, it has access to the population database, which is the registry of births, deaths and marriages. The police and immigration service have access to other sources. If the issuing authority is convinced of the identity of an applicant and has determined that he has a right to the document applied for, the authority may proceed to issue the said document.

4.3.2 Filling in and returning an application form

Another way to obtain possession of a document is to apply by application form. Often used in the private sector, it is also employed by the government. In countries that have passport offices, an application form is always part of the procedure.

An applicant may request that an application form be sent to his home or he may collect it from a designated distribution centre, such as a post office. After the form is filled in, it might also have to be signed by another independent person. This could be a lawyer, notary, cleric or other prominent resident of the applicant's municipality. This person issues an attestation, declaring that he knows the applicant in question. This is one way of verifying the identity of the applicant. The application form and any other accompanying documents, such as a birth certificate, extracts from the population register, or the expired documents may subsequently be sent to the issuing authority. This authority can then use the supplied information to check it against the databases at its disposal. If there are no objections, the authority may proceed to issue the document.

4.3.3 Making use of intermediary authorities

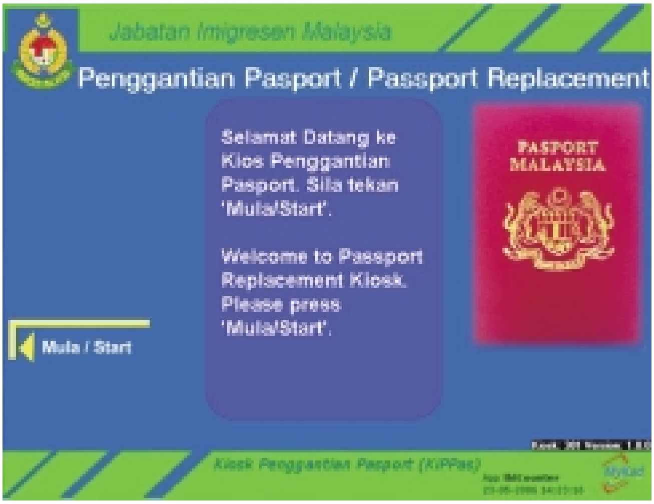
An issuing authority may also make use of an intermediary authority such as the post office. An applicant of a particular document goes to a post office, which has all the necessary application forms and expertise to assist an applicant.

The post office staff is trained to help citizens with the application procedure and have knowledge of control processes. However, they do not have access to references. Nevertheless, the fact that the applicant appears in person, submits the required documents, and signs the form in the presence of a civil servant, is a built-in control that guarantees verification and prevents fraudulent applications in the first instance. Often, the issuing authority has the possibility in the second instance to carry out further checks to guarantee the authenticity of an application.

4.3.4 Applying online

The last few years have seen the emergence of a modern way to apply for a document, i.e. via the Internet. The digital highway is a boon especially for large countries with scattered towns and villages, enabling governments to reach far-flung regions.

Through e-government, they try to offer as many services as possible through this medium, one of which is the digital application for a travel document. The form is filled in on the computer and supplemented with electronic documents, e.g. a scan of an applicant's expired passport. This package of documents is then safely forwarded to the issuing authority, which then proceeds to assess and verify the application. If the application meets all the requirements, the document is issued. However, this manner of application is still in its infancy, and at this stage, it is still is up to governments to first provide the proper tools, i.e. a safe means of communication using Public Key Infrastructure (PKI), along with smart cards and possibly biometrics.



Jabatan Imigresen Malaysia

Penggantian Pasport / Passport Replacement

Selamat Datang ke Kios Penggantian Pasport. Sila tekan 'Mula/Start'.

Welcome to Passport Replacement Kiosk. Please press 'Mula/Start'.

Kiosk Penggantian Pasport (KiPPas)

Figure 4-6: Screen of the Malasyan on line application kiosk where document applicants can manage their own reneweling application for passports. (Courtesy of IRIS, Kuala Lumpur, Malasya.)

■ 4.4 Processing the application

Besides building safeguards into the application procedure, it is also vital that measures are taken to protect the internal procedures of processing an application. They say opportunity makes the thief. In order to prevent the risk of internal fraud, the issuing authority must therefore ensure that the internal procedures are correctly followed. An important aspect of the procedures is the separation of tasks. Depending on the type of document, the issuing authority, and the value of the document in the user environment, there must be a distinct separation, e.g. between the employee who deals with the application and the employee who is responsible for the personalization of the document. One could even consider assigning a third employee the task of issuance. Another method to further ensure proper internal procedures is to keep a record of which employee does what and when.

In addition, sufficient thought must be given to the storage of blank documents. This strongly depends on the issuing system that has been chosen, and strict procedures must be developed for this. One golden rule is the principle of “four eyes”, where it is forbidden to give a single employee all the access to the blank documents storage. By ensuring that not one, but two employees remove the required daily supply from secured storage and return it after closing, the risk of irregularities is significantly reduced. The management of these documents should also be meticulously registered.

Once all checks have been carried out, the employee may proceed to produce the document. The manner in which this is done largely depends on the issuing system and the chosen personalization technique. See Chapter 5 for more information about the various issuing systems and for an overview of the techniques available.

■ 4.5 Personalization of the document

Personalization of a document means that variable data is added to it. This data relates to the person to whom the document is to be issued. This data may also relate to the document’s validity or, in the case of a financial document, include an account number. In the past, personalization data was often entered on the document manually. These days, there are many other ways to add personalization data. For the technical details on this, see the section *5.4 Personalization techniques*.

One important question, however, is who should personalize the documents. By answering this, it often becomes clear where the documents should be personalized. The technology currently available for personalization varies widely in quality from poor to excellent. But quality is not only determined by technology. The expertise necessary for the personalization process also has a great influence on the final quality. There are also a number of factors that play a role in the answer to the question of who should personalize the document. From a security point of view, centralized personalization is preferred over decentralized personalization. But from a service perspective, decentralized personalization is the favoured option. Centralized personalization entails that the applicant's data must be transported to the personalization location. Subsequently, after it has been personalized, the document must be returned to the applying authority. It is obvious that this delays delivery times. Also, there may be huge differences in the complexity of the operation of personalization equipment. Although many issuing authorities use relatively simple typewriters and printers, the application of high-quality dye sublimation techniques or laser techniques require considerably more expertise of the operator and an IT infrastructure.

■ 4.6 Issuance of the document

After the document has been personalized, it moves into quality control, which usually receives less attention in the entire application and processing procedure. After the document has been personalized, it is important to verify whether this process has been carried out properly, and whether the machine readable technologies contained in the document, which enable electronic reading of the data, function correctly. It could be a magnetic stripe, 2D barcode, contact or contactless chip, or a Machine Readable Zone in the OCR-B font. These technologies play an important role in the use of the document and therefore their proper operation needs to be guaranteed.

After the document is personalized, it is also important to check the data entered, such as the user's personal particulars, document number, validity and other data are correct, and to see if the quality of the data is consistent with the required technical specifications. This task must be carried out accurately so that the next link in the chain can rely and build on the document and the integrity of the added data. On the basis of this data, the following link in the chain enters into a relationship with the user of the document. If there are doubts about the authenticity of the document because the issuing authority was lax about quality, there would be unfavourable consequences for the user, some serious enough to lead to his detainment on the suspicion of possessing a false document.

Once all the quality controls are carried out, the document may be issued. The manner in which the document is issued depends in part on the method of application, the complexity of the personalization procedure, and the location of the issuing authority. If there is a representative of the issuing authority in each municipality, the user may collect his document in person. However, if the authority only has regional branches, then a different method of issuance is required. The same holds true with a single a single national office. Issuance may occur in the following ways:

- in person, while one waits;
- in person, with a waiting period of several days;
- by post;
- by post, with a user restriction.

The quickest service for the applicant is the "ready while you wait" service. In that case, the application is immediately dealt with. All verifications are carried out, after which the document is produced. Depending on how the process is organized, the applicant could be in possession of the desired document within fifteen minutes for instance.

A method of issuance that requires more time is that which involves a waiting time of several days. In this case, the user applies for the document in the required manner, and after the procedure is concluded, the user is requested to collect the document in person after several days. In some countries the applicant receives the document by post. In the meantime, verifications are carried out and the document is personalized. This method ensures a more secure and consistent procedure. The element of haste has been removed and the personalization may be done centrally.

Depending on the application and personalization procedure, it is also possible to send complete documents to the applicant by post. Many countries make use of the existing postal service, either with or without implementing extra guarantees.

The last option is similar to the above, but with a restriction on the use of the document. If the applicant wants to use the document, then he must perform an additional task in order to activate it. For instance, in the case of a credit card, the relevant company must first be informed of the receipt of the document, after which a number of specific questions are asked which can only be correctly answered by the prospective user. If all goes well, the credit card company proceeds to lift the restriction and the user is free to use the card.

4.6.1 Issuance systems

Each issuing authority issues documents within the scope of its responsibility. We have seen that there is a wide variety of documents, from passports through insurance passes and driving licenses to credit cards. All these documents share a common property in that, only after they are printed or otherwise fabricated, are they made out in the user's name at personalization. Depending on the type of document and the issuing authority, a particular system of personalization and issuance needs to be selected. The various possible choices are:

- decentralized personalization and issuance;
- decentralized personalization and central issuance;
- centralized personalization and decentralized issuance;
- centralized personalization and issuance.

Read for more detals and advice the ICAO Doc 9303, informative appendix 3, to section III, “The prevention of fraud associated with the issuance process”.

4.6.2 Decentralized personalization and issuance

An issuing authority is dependent on various factors when issuing a document: the geographical spacing of users, locally, regionally, nationally or internationally; the document producer(s); the database from which the data for the document must be extracted; and the frequency with which a document must be replaced or extended. These factors affect the issuing authority's method of personalization and issuance. Depending on the method and the necessary equipment, personalization may easily be achieved at one or more locations. However, if the issuing authority opts for that requires advanced and costly equipment, it becomes more difficult. If an issuing authority chooses the system of decentralized personalization and issuance, the authority must have more than one issuing centre or find an organization willing to facilitate this (e.g city hall or similar).

4.6.3 Decentralized personalization and central issuance

Another option is to personalize documents at more than one location. A reason for an issuing authority to do this would be because it wants to spread the risks to the vulnerable personalization process. If there is a defect at one location, it is possible to fall back on other locations that have the same expertise and equipment. After the documents are personalized, they are sent to a central location. With this system, the central location is often still required to ensure that the document is either additionally secured or prepared for dispatch.

4.6.4 Centralized personalization and decentralized issuance

Yet another issuance system is that in which personalization is performed centrally and issuance decentrally. This system enables the issuing authority to make use of very sophisticated equipment, which as a rule is also very costly. By organizing the personalization process at one location, it is easier to apply new security features if there is increased threat to a particular document. In addition, this system ensures greater quality and consistency of the personalization process for the simple reason that a document is checked at a single location and not at e.g. 550 across the country.

The Netherlands opted for this issuance system in October 2001, when it launched its new Dutch passport. The user applies for a new passport at the town hall in his residence. There, all data is registered and verified, after which the application is digitized and sent to the producer via a secure line. The producer of the Dutch passport deals with the application and returns the personalized passport to the town hall within the fixed term. The passport is then issued to the user, after the data has been checked a second time.

4.6.5 Centralized personalization and issuance

Centralized personalization and issuance entails one link less in the total process. Here, after the document has been personalized, it will be immediately issued or sent to the user. This system is frequently used by financial institutions. Bank cards are directly sent to the user, either with or without a user restriction.

Reference

ICAO
2006 Doc 9303, *Machine Readable Travel Documents*, Part 1, Machine Readeble Passports, sixth Edition.

CHAPTER 5

PRODUCT DEVELOPMENT

■ 5.1 Introduction

In product development, there is a lot of decision-making on aspects such as graphical and security design, materials, personalization techniques, product and production tests. It is a difficult process where the designer is called to know different facts and operational constraints. The following sections will give a detailed insight into these.

■ 5.2 Design

The choice of product materials to be used depends on a number of factors. It also determines the techniques to be applied. Important factors that often influence the choice of particular materials are the lifespan of the product and the environment in which it is used (See Chapter 2).

In case of an ID card, the selected material must ensure a long lifespan. Certain plastics offer a lifespan of 10 years. However, the use of plastic restricts the techniques that may be applied to production and personalization. Choosing paper for a product that needs to last 10 years involves obvious risks. Unfortunately, there are governments that still issue ID cards that completely disintegrate after some time. These faulty choices burden the document inspector, who is confronted with deficient documents and have to decide whether or not he should trust persons presenting them.

Comprehensive knowledge of the available technical solutions and of the limitations of the production process can reduce the risk of incompatibility of materials and techniques. Document producers are encouraged to explore potential combinations and try out new products which could prove suitable to the special requirements of documents. Currently, the chosen personalization techniques strongly influence the selection of a basic material. Inkjet printing technology, for instance, goes hand in hand with paper substrate, whereas laser engraving requires a laser sensitive polymer substrate (see sections 5.3 Materials and 5.4 Personalization techniques).

At the moment, polymers are increasingly superseding paper substrate because of the growing preference for durability. Moreover, polymers ask and allow the integration of new security features[1] and electronic storage means for the automated processing of documents. Document development acquires a whole new dimension when an engineered component is added to the traditional graphic design.

The graphic design involves the choice of structures, colours, printing techniques and inks, but at the same time depends on the combination of security elements and manufacturing process. The security designer is advised to liaise with the product development manager in order to arrive at the best solution.

Within the scope of its production development program, a professional company that specializes in the production of secure documents may independently explore new concepts for its product line. In order to know where to look, the producer needs to be able to fall back on the previously mentioned networks of users and their products, counter-fraud organizations and suppliers of materials. In addition, product development may also examine the techniques applied in adjoining fields and see whether these can be used for the enhancement of their own products.

A list of requirements and a project approach are the bases for the development. This makes it possible to control the project development in terms of quality, cost and time. The project covers a wide area and involves the selection of raw materials, the development of the various specific security elements, the production technologies to be applied,

[1] Watermarks, the paper specific security feature, is currently not available for polymers.

and in the case of travel or identity documents, the options for personalization. During this process, the ratio of price to performance is assessed, and different solutions are chosen, depending on the environment for which the document is intended.

Printing plays a less prominent role in the electronic ID card. Here, emphasis is on the development of a durable plastic carrier for integrated electronic components.

It is the product developer's task to define exactly which new materials, processes and equipment are required, and to consult various suppliers about these technologies. On the bases of the received proposals for solutions, a partner may be selected to assist in this part of the product development. Early in the process, how these technologies can be applied to the future mass production of documents needs to be explored.

The choice of security features in the document will depend on its susceptibility to fraud. It is ideal to choose features that cover more risks simultaneously and are harmoniously integrated into the graphic design of the document. This prevents reproduction as well as tampering. For example, an optical variable device can be used to prevent duplication. If it is intelligently placed on the document, the same device can also be a strong deterrent against the manipulation of variable data.

There are different trends in security design for documents. One extreme is to minimize the number of security features in order to avoid the Christmas tree effect, while the other is to include all the security features currently available. However, for a producer that heeds the document's risk analysis, his choice will be a practical one: one that eliminates duplication and leaves room for optional extras.

■ 5.3 Materials

This section describes some of the basic materials (or substrates) currently used in secure documents, the specified selection criteria, and the combination of different materials that are possible. And although the future will bring new solutions and materials, the materials presented here have performed well and are expected to continue to do so in the future. Many of them have been used by the industry for quite some time.

5.3.1 Paper

Paper, one of the most commonly available materials, has historically been the most preferred for secure documents. It is economical, flexible, easy to acquire, and expertise on its use is widespread. Paper documents, however, are vulnerable to attacks by counterfeiters and forgers (Fahrmeir, 2001). A producer must therefore first decide whether the paper solution provides the necessary security before choosing it.

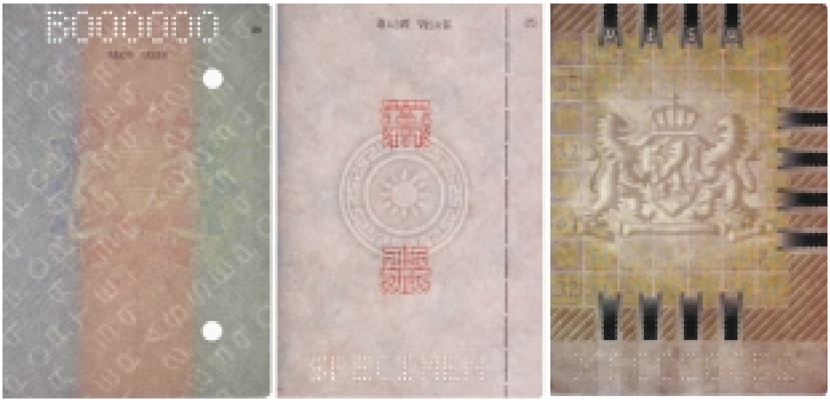
For secure banknotes and other means of payment, such as cheques and vouchers, paper is the most commonly used. The printing and manufacturing technologies for these banknotes are often also used in passport books, ID cards, driving licenses, and visa stickers.

The price range of paper substrates varies greatly. Raw materials, the types of watermark, additional security fibres or planchettes, and possible security threats may significantly increase the cost of this material.

Paper products typically provide an effective mass solution for what are referred to as "decentralized solutions", where the last part of the process, i.e. ID document personalization or entry of the value on a cheque or voucher, is done locally at e.g. a police station or bank (see section 4.6.2 Decentralized personalization and issuance). Assuming that the risk of stealing blank documents is under control, the focus should go to the features that guarantee the best protection against copying and counterfeiting. In secure paper documents, e.g. printed banknotes, which do not require any personalization processes, verification of genuinity is very important.

The following list of security features is an attempt to grade the different paper solutions according to the security they provide. In descending order, they are listed from the most to the least vulnerable to alteration, falsification or copying:

- Availability to parties other than security printers: banknote paper, for instance, is restricted to particular banknote printers only.
- Types of watermark: (e.g. line mark, single tone or multi-tone, which is the watermark of choice for security printing). The choice on the level of details in the design and the use of registered watermark depends on the functionality required, the level of security, and budgetary restraints.



Line watermark   Single tone watermark   Multi tone watermark

Figure 5-1: View of the different types of watermarks on authentic travel documents. (Courtesy of National Criminal Intelligence Service, the Netherlands.)

- Security threads and hologram stripes: these features offer a wide range of additional security: e.g. visual and/or machine-readable security. However, even with these security features, it is very difficult to upgrade non-secure paper to a highly secure level.
- Security fibres (UV-sensitive, IR-sensitive, dull or non-sensitive): these reliable security features are frequently applied, but are less known and used by the public. Forensic analysis (e.g. by means of secret markers) is often carried out by means of these features.
- Reaction to chemicals: attempts to alter or falsify the already applied information by using solvents or other chemicals leaves a stain or spot on the document. This feature's position at the bottom of the list is debatable.

In addition, there are several other solutions for identification and verification. These require a specific reader, or light wavelength. Such paper is useful in relatively simple applications, such as tickets or passes, but mostly in mass applications with a limited number of control points. A current, controversial issue is the effect of certain materials on the environment. In this respect, paper has a lot going for it. The debate whether to place more value on recycling and renewable natural resources over attractive energy and chemical-intensive processes is sensitive because for every argument in favour of paper, there are often several arguments against it.

Regardless of which security paper is chosen, it must be emphasized that paper, like most other substrates, is merely the basis of the secure document. The producer must remember that choosing paper with minimal or no security will influence subsequent processes, which are unlikely to compensate for the shortcomings of the original choice.

5.3.2 Plastic substrates: Polyvinyl chloride (PVC)

Whereas paper is the most commonly used material in security documents, polyvinyl chloride (PVC) plastic is probably the most commonly used plastic card material, especially in credit and debit cards, loyalty cards and ID cards.

The advantages of PVC are evident. It can be manufactured in a relatively simple mass production process, thus providing stable quality and keeping costs low. Furthermore, the surface is smooth and glossy, providing a good basis for printing and special effects.

Its main disadvantage is its reaction to temperature changes. Below freezing, it loses its flexibility and becomes brittle. At high temperatures deformation sets in relatively quickly. Even in ideal circumstances, a card is ready for renewal after three years. Major banks usually renew cards every other year to be on the safe side.

As is the case with many other materials, industrial PVC is practically always a mixture of polymers containing around 50 % PVC. The rest of the blend remains an industrial secret, but its main aim is to enhance durability and/or other properties of the plastic card.

Unfortunately, PVC's security advantages remain limited, and they are often based on personalization processes and add-on security features. Nevertheless, PVC has exceptionally good embossing properties, which is still an important factor in many credit card processes. If you personalize a card by embossing, it remains functional in mechanical credit card devices, and operates as a back-up system if electronic means fail. Embossing on PVC is stable and tolerates wear better than most other plastic substrates.

Moreover, PVC allows the industrial application of holograms, magnetic stripes, signature stripes, and smart card chips (see section 5.4.3 Machine-readable technologies). PVC is also adaptable to many state-of-the-art impact and non-impact printing methods, and even to laser engraving. For all its restrictions, its usage can be justified by its complementing properties in finishing processes, e.g. in personalization and control procedures.

PVC's flexibility in single card printing is also another reason why it is a commonly used material in e.g. ID and access cards. Since it is a stable material in office environments, printing procedures that are performed decentrally (or at points of sale) produce relatively good results. The variety of e.g. toners and colour ribbons, and personal preferences in pictures (colours and hues), however, may result in great differences in quality. The potential wastage may be unacceptable, but in principle, a plain PVC card is an inexpensive and insecure raw material.

Furthermore, PVC seems to be maintaining its position as a relatively safe material from an environmental point of view, although the word 'chlorine' in its name might suggest otherwise. PVC plastic cards remain relatively intact unless they are burned at low temperatures. If raw materials are ranked on the ecological scale, PVC loses a fair amount of its benefits. Also, the expected lifespan might be rather modest for more demanding circumstances such as in ID solutions. Even so, it is safe to say that even if PVC eventually loses its foothold on the industry, it will continue to be a very widely used material in secure payment cards, even if its security is based on factors other than itself.

5.3.3 Plastic substrates: Polyethylene Terephthalate (PET)

Another plastic laminate that is widely used is polyethylene terephthalate (PET or PET-G, where G stands for glycol - originally added to improve laminating properties). In many cases, PET is used instead of, or in combination with, PVC. It is mainly used in secure documents in banking and identification solutions. The printing properties of PET are not always as evident as in PVC, and therefore PET cards are generally laminated with PVC. PVC then provides the card with many of the printing properties for e.g. sublimation, ink jet or Dye Diffusion Thermal Transfer (D2T2) printing.

An advantage of PET over PVC is it longer lifespan, which is up to two to three years, and even longer under ideal conditions.

Its disadvantages are limitations in embossing, and possible sensitivity to delamination if adhesion between sheets remains uneven. Also, PET can be laser engraved; but whereas PVC produces grey images, PET typically gives brownish output.

The impact of PET cards on the environment is often seen as less detrimental than PVC. However, it is difficult to assess whether this is due to the fact that recyclable PET is largely used as soft drink packaging, or because of its longer lifespan.

5.3.4 Plastic substrates: Acrylonitrile Butadiene Styrene (ABS)

Acrylonitrile Butadiene Styrene (ABS) is not really a viable alternative for highly secure documents. However, it is used as a carrier for e.g. SIM cards for mobile phones. It provides teleoperators with a good medium for brand management for the short time it carries the phone chip. And as the chip is ultimately removed from the card, the ABS card can be disposed of with less concern about its future effects on the environment than PVC or PET.

An advantage of ABS is its price, and the fact that it is very easy to model mechanically.

A disadvantage of ABS is its finish. Printing can only be performed on the surface of the card. ABS cards are usually moulded, and very sensitive to high temperatures. Once exposed to heat these cards are unable to return to their original shape. All this indicates a modest lifespan, which is estimated at around one year, even in the most favourable conditions.

5.3.5 Plastic substrates: Polycarbonate

Polycarbonate is another industrial polymer, which has been used in ID documents the early 90s of the past century such as the Swiss ID card or German driver's license (Fahrmeir, 2001). It has many features that make it extremely attractive for secure documents, but at the same time processing polycarbonate requires expertise and devices to make it a viable alternative.

One advantage is that when it is combined with laser engraving, it provides a solution that it is hard to forge or counterfeit. In other words, the card cannot be delaminated, nor its data removed, if only polycarbonate has been used as a substrate. The laser engraving process decomposes polycarbonate material into carbon particles, which are surrounded by solid polycarbonate in the card (Billmeyer, 1984). In addition, polycarbonate can handle most security printing methods, image processing technologies and the application of e.g. light embossing. Furthermore, many additional security features (CLI (Changeable Laser Image™) and MLI (Multiple Laser Image™), Alphagram™, Kinegram™, Moviegram™, Pixelgram™)[2], and e.g. OVI (Optically Variable Ink) can be used. Also, a polycarbonate card is practically insensitive to climatic change, and tolerates most chemicals that are used to remove or alter surface printed images in PVC or PET. And because it has an average lifespan of at least 10 years, it offers long-term security. It is also a very durable platform for smart card chips and antennas.

But it also has drawbacks. Its lamination process is more complicated as compared with the above-mentioned plastics. In order to ensure that a polycarbonate card cannot be opened, the lamination process must be carried out under very strict conditions. Furthermore, there are limitations

[2] Trademarks of Giesecke & Devrient, Hologram Industries, OVD Kinegram

on design and the application of certain security features or chips. Additionally, the initial investment for personalization equipment may be several times higher than for the less secure PVC or other plastics. Moreover, polycarbonate can only capitalize on its advantages if personalization is done centrally. If the above technique is spread over three to five years, the unit cost might become very competitive, and the longer issuance time could be overcome by effective logistics services. In some cases, its main shortcoming is that it cannot produce a colour picture, unless future development makes it possible to engrave a colour picture on polycarbonate.

Nevertheless, as the requirements for travel documents increase, polycarbonate will eventually see healthy market growth. The expected long-term benefits and enhanced security justify the high initial investments. Centralized personalization reduces the need for several high-security premises, but may, on the other hand, increase customer waiting times.

5.3.6 Other plastics and combinations of materials

Polymer banknotes have regularly been considered as a replacement for banknote papers. Polymers are chosen because of their greater strength and longer lifespan. Experiences with the application of polymer have been both positive and negative (Wikipedia, 2006), and no doubt there will be further developments. Information on countries using polymer notes can be found on the internet (Polymernotes.org, 2006).

An interesting new area of secure documents is large-scale low-cost solutions, which have been developed by combining different materials. What are referred to as RFID (Radio Frequency Identification) laminates and stickers, which are based on e.g. paper or plastic foil carrier and electronics can nowadays be manufactured industrially. These solutions are currently used in price tags, transportation tickets and similar uses. They are more secure and have higher performance than most barcode solutions, yet they are far less costly than traditional memory or processor chips (contactless technology will be further discussed in the section 5.4.3 Machine-readable technologies, F. Contactless chips).

■ 5.4 Personalization techniques

Personalization is the final step in document production. The personalization process converts a generic “basic” document, printed and fabricated by a security printer, into a unique document.

It can also add anti-counterfeit and anti-tamper security features that are unique to a specific document and complement the security features included in the manufacturing process of the basic document.

Many view the personalization process as a separate, unrelated activity. Instead, it should be considered as one step in an integrated production process that spans design to issuance and re-issuance. Indeed, most decisions on personalization techniques require specific document materials and fabrication processes. These materials and processes often affect the security printing options.

An in-depth discussion of all the technologies identified in this section goes beyond the scope of this book. For a more thorough treatment please refer to one or more of the cited references. This section will attempt to provide the reader with an overview of the following:

- factors to consider when choosing a personalization technology;
- common types of human-readable personalization – graphics and imaging;
- common types of machine-readable personalization;
- the underlying technology, cost and usage of each method.

There are a number of personalization technologies available to the issuer. Each technology has its own advantages and disadvantages. The challenge to issuers is understanding how to match the available technologies with the requirements that have been set on a document. This would be a feat in itself if technology were static, but since technology evolves rapidly, issuers need to keep abreast of the latest developments.

5.4.1 Factors to consider

To determine the most suitable technology, the issuer needs to consider a number of factors, including usage, threats and costs. Over usage and threats please refer to sections 2.1 General analysis and 2.2 Fraud risk analysis. With regards to cost, one must remember that each personalization process incurs different costs. The following is a list of some of the factors that affect the total personalization and usage costs:

- Material costs: the base document supplied by the security printer, colorants used during personalization, wear-resistant and secure top-coats applied during personalization;
- Production costs: equipment amortization, labour, scrap rates;
- Readers: human and machine-readable security features, encoded data, e.g., magnetic stripe, integrated circuit;
- Security: physical protection and audits of scrap destruction – rejects, unused supplies and documents between various production processes (work in process); personalization personnel.

For the sake of brevity, only the more popular, currently available digital technologies will be discussed. With respect to human-readable technologies (text, logos, images) the following will be dealt with: thermal transfer, electrophotography, ink jet, laser engraving and laser perforation. The discussion of the machine-readable technologies will include the one considered by the International Civil Aviation Organization (ICAO) – contactless integrated circuits, which is recognized as globally interoperable- as well as others which could be used for regional or national applications. These are Optical Character Recognition (OCR), magnetic strip, 2-D barcodes, optical stripe and contact integrated circuits (ICs).

5.4.2 Human-readable technologies

All printing processes use a three-part system, which includes a colourant, a receptive material (receptor) and an applicator. The three parts must be compatible for the best results. For instance, a costly fountain pen (applicator) containing permanent ink (colourant), works well with a high-quality, partially porous substrate such as 100% rag bond paper, but yields unacceptable results when applied to low-quality, highly porous kraft paper or plastic.

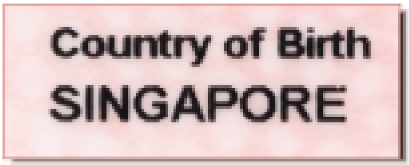
A. Thermal transfer

Thermal transfer, as the name implies, uses heat to transfer a colourant from a "donor" material, such as a ribbon, to a receiving material (substrate). The applicator or a "printhead" is typically a linear array of individually addressable dots (elements). The elements are heated by means of an electric current. The applicator can also be a heated roller with an engraved pattern. Transfer can be either direct or indirect; the latter making use of an intermediate medium. Transfer can be an 'all or nothing' process, commonly referred to as mass transfer. Alternatively, a controlled amount of colourant can also be transferred, based upon the amount of heat energy applied to each element. Below is a brief description of each process.

The density of thermal transfer print elements currently varies from 3 dots/mm (75 dots/inch) to 24 dots/mm (600 dots/in). For ID applications, 12 dots/mm (300 dots/in) is the most common. Each element can be addressed individually, similar to a "pin" of a dot-matrix printer. In addition, the amount of electric energy sent to each element can be controlled. Electric energy is converted into heat at the edge of the print head in closest proximity to the ribbon and substrate.

The colourant is a coated ribbon. The coating process and configuration vary depending on the specific printing process.

Single colour, or "solid colour" (single tonal level), text and graphic images can be created with a ribbon. A thin, usually 6-micron "donor" film is coated with material that is a combination of binder (wax, resin or wax-resin) and coloured pigments or dyes. Pigments have better light-fastness properties. The binder material serves as carrier for the pigment and as an adhesive to bond the pigment to the receptor surface. The chemical composition of the binder material may be optimized for the target receptor.



Country of Birth
SINGAPORE

Figure 5-2: View of the Single colour black text on an identity document. (Courtesy of Bundespolizeidirektion, Koblenz, Germany.)

Multi-colour, pigmented ribbons are also possible. A multi-colour ribbon is coated in "segments" or "panels". Each segment is coated with a different "colour". The length of the segment generally corresponds to the length of the document. The colours include the primary colours of a four-colour subtractive (reflected) printing process: Yellow (Y), Magenta (M), Cyan (C), and Black (K). The ribbon may also have segments for security materials and/or a protective coating.

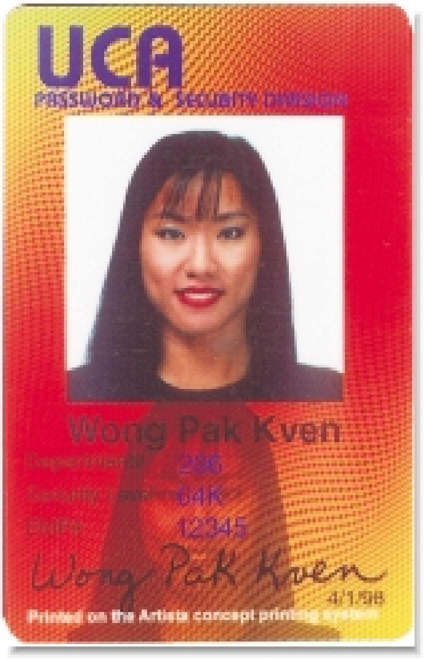

UCA
PASSWORD & SECURITY DIVISION
Wong Pak Kven
286
64K
12345
4/1/98
Printed on the Artista concept printing system

Figure 5-3: View of the Multi colour sample specimen card.
(Courtesy of Fons Knopjes, the Netherlands.)

Dye transfer-based ribbons, also known as "dye diffusion" ribbons, are more common. These ribbons are configured in the same way as multi-colour pigmented ribbons. The ribbon is segmented and includes at least YMC dyes. The "colour" black can be created using YM&C. Still, pigmented Black (K) is generally included to print barcodes and/or other symbology that must absorb infrared lighting. While not commonly used, monochromatic dye-based ribbons are also possible.

Pigments or dyes must be covered to minimize fading and secondary migration. Therefore, the ribbon may include one or more protective coatings, often referred to as “T panels” or “top-coat panels”. If a T panel is not included, a protective coating must be applied in a separate operation.

The specific sequences for dye and multi-colour pigmented ribbons can be quite complex, depending upon the capabilities of the target printer. For instance, a printer capable of printing the front and back of a document could use a ribbon with an YMCKSYMCK sequence (where S = Security, such as a holographic topcoat). In that case, pigmented colour images could be printed on the front and back and a security material could be applied on the front. Alternatively, the sequence could be YMCKTK, whereby dye colour printing is limited to the front of the document.

Thermal transfer requires a compatible substrate. An ID1 card is the most common application, where the receptive material is usually a pre-cut, plastic card. Dye transfer requires a polyvinyl surface or a surface coated with a receptive layer. Mass transfer materials can be applied to a wider variety of materials, including PVC, PET-G and ABS (see Sections 5.3.2, 5.3.3 and 5.3.4).

The receptor can also be a coated ribbon, which serves as an intermediate medium. The colourant is first transferred to the coated ribbon. Then, with the application of heat and pressure, it is transferred to the final target substrate. This process is used when the final substrate has an irregular surface or it is not receptive to the dyes or pigmented colourant on a thermal transfer ribbon. A paper data page of an ID3 size document (passport) can be personalized using this process. In that case, the paper on the data page is coated to promote adhesion with the receptor transferred from the intermediate medium.

Some indirect processes only transfer the colourant and receptive coating. It is also possible to adhere or laminate the colourant, coated media and carrier ribbon. The intermediate carrier ribbon would then serve as protective laminate.

The actual printing process is depicted in Figures 5-4 and 5-5.

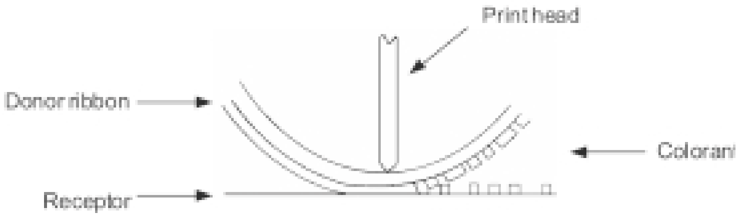


Figure 5- 4: Thermal transfer printing process: transfer of colourant

Figure 5-4 shows that when heat is applied, the colourant leaves the donor ribbon and is transferred to the surface of the receptor. Where heat is not applied the colourant remains on the donor ribbon.

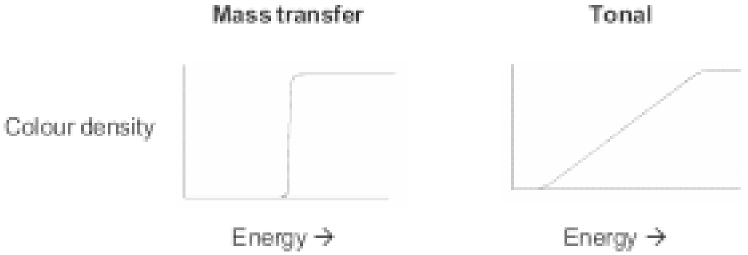


Figure 5-5:Thermal transfer printing process: difference between mass transfer and tonal level transfer

Figure 5-5 illustrates the difference between mass transfer and tonal level transfer. A mass transfer ribbon has a single temperature threshold. Energy is applied to the print head element. Heat energy is transferred through the donor ribbon. When the threshold temperature is reached, all of the colour opposite the print element is ‘released’ from the donor ribbon and adheres to the substrate.

A “dithering” process is used to create tonal level images with mass transfer ribbons. Groups of dots are combined to create a “pixel”. The individual dots are too small to be perceived separately. Instead, the human eye integrates the individual dots of a given pixel into one overall colour density level. Currently, the science and art of dithering has been the subject of considerable study. There are numerous considerations such as pixel dimension versus tonal level per pixel, the placement of dots within pixels to avoid interference effects and methods to reduce apparent colour gradations (Kodak, 2006).

Tonal level ribbons do not have a single temperature threshold. Instead, the amount of colourant transferred to the receptor varies with the amount of energy applied to a specific print element. Tonal level images are created by varying the colour density of each dot. Thus, in the case of tonal level ribbons, each dot is a pixel.

Recent technological developments have created a hybrid process. With the correct combination of print head, ribbon and receptor, it is possible to vary the size of a dot created with a pigmented ribbon. In this process, tonal levels are created by a combination of dithering and dot sizes.

Thermal printing can be a rapid, fully-automated process with high production rates (a few hundreds per hour) depending on the machine configuration. High-quality, full-colour images can be created for facial images. Distinctive colour graphics can be applied during personalization, thereby reducing the printing costs of the base document. Long-lasting documents can be created using cards with composite constructions, e.g. polyvinyl and polyester and wear-resistant topcoats. Depending on the document format, thermal printing can create and/or coexist with a large number of machine-readable data storage technologies.

The colourant supply costs in thermal printing may be higher than those in other technologies. If dyes are used as colourants, they must be sealed with a non-porous laminate or topcoat to prevent fading and dye migration. As thermal printing technology is readily available, appropriate anti-counterfeit and tamper-evident security features are needed and evaluated through a threat analysis.

B. Electrophotography

Electrophotography, also known as Xerography or "laser printing", shares a number of qualities with thermal printing. Like thermal printing, the technology is normally used to create colour images using Cyan, Yellow, Magenta (CYM) and Black (K) colourants. It is also possible to create solid and tonal monochromatic images. Printing can be done either directly or indirectly.

The electrophotographic process is more complicated than thermal printing. For a full description of this technique, please refer to one of the cited references (Canon, 2006). Below is a brief technical description of the process as it applies to identity documents.

In the three-component model, the "applicator" is a highly focused light source, such as a laser or linear array of photo diodes. The light source creates a series of dots, a latent image, on a photosensitive surface. The surface may be a hard-coated cylinder or a flexible belt. If a laser is used as the light source, an optics system sweeps the laser back and forth over the photosensitive surface as it passes the light beam. The beam is 'switched' on and off as it traverses the receptor, similar to a computer monitor. If a diode or other linear array is used, individual elements are turned on and off as the receptor passes, similar to a thermal print head.

Resolution can vary greatly. For identification applications 24 dots/mm (600 dpi) is common. However, colour printers are available with resolutions as high as 96 dots/mm (2400 dpi). Some of the newer printers can modulate the dot size to obtain tonal levels within a given dot.

Electrophotography typically uses toner particles as colourants. The toner particles can vary in size from sub-micron to several microns in diameter. High-resolution systems need smaller toner particles. Most systems use "dry toner", where the actual colourant is encapsulated within a binder that is attracted to the photosensitive surface and subsequently fuses with the surface of the target substrate. Binder chemistry can be tailored to different target substrates. Other systems use fine colourant particles suspended in a liquid.

Toner colours include Yellow, Magenta, Cyan and Black. Customized colours and security materials are also available.

Electrophotography is compatible with a wide range of receptive materials, plain and coated paper being the most common. In addition, Teslin® and a variety of polymer films can be used. Sometimes the polymer is subjected to a surface treatment to improve adhesion of the toner particles and binder material. Unlike thermal transfer, the dimensions of the receptive material are generally an A4 or larger size sheet, or continuous web, instead of a pre-cut card.

Many variations have been developed. The actual technology is quite complex. In general, however, all processes involve the following steps:

1. The optics system creates a latent image on the photosensitive surface.
2. Toner is attracted to the places exposed by the optics system.
3. The toner is transferred to the target substrate or an intermediate surface.
4. Steps 2 and 3 are repeated as often as needed for a multi-colour image.
5. The transferred toner is fused with the substrate using heat and pressure.
6. The receptive material is laminated and die-cut into individual cards.

Electrophotography can produce high-quality colour images. Like thermal printing, colour-coded backgrounds and graphics can be created to designate different privileges. Higher resolution printing systems can create limited micro-text with unique document specific content. On the whole, the colourant is less expensive than with thermal printing.

Since pigments are used as colourants, fading is not an issue; however, adhesion of the toner particles to the target substrate can be a problem. Prior printing processes, especially those involving intaglio, ink coverage, as well as the characteristics of materials all affect adhesion. In any case, the toner won't penetrate into the (paper) substrate, bearing the risk of intentional removal by mala fide users. For these reasons, use of a protective, tamper-evident laminate or topcoat is advisable in the case of security documents. However, the protective laminate should be carefully selected to ensure it strongly adheres to the printed document.

Lamination and die-cutting operations are required to create a finished document since electrophotographic printers typically use sheet or web format substrates. These processes could be integrated with the print system. Depending upon the target substrate, compatibility with optical stripes, contact and contactless integrated circuits integrated in plastic cards can pose problems. Like thermal printing, electro-photography technology is readily available to the consumer. Thus, anti-counterfeiting and tamper resist features are called for.

C. Inkjet

Driven by the popularity of personal computers, advances in inkjet technology during the last few years have been remarkable. Like the other printing technologies, only a brief overview is possible in this section. For a more detailed description, please refer to the Canon technology page or one of the excellent documents on this subject, such as the one written by S. Ponds (Ponds, 2002).

Until recently, the use of inkjet for identity documents was limited to paper applications, such passports. The inks currently available for office environments are not compatible with non-porous plastic substrates or highly porous substrates, such as Teslin®. As a result, the technology has not gained acceptance as a print system for ID-1-size documents. Considerable research has been focused on the development of inkjet compatible coatings that can be applied to polymer surfaces. Using this technology, direct and indirect inkjet printing onto ID-1-size documents is feasible.

Like other printing processes, inkjet uses a combination of Cyan, Yellow, Magenta, Black and possibly special security colourants. The colourants are dyes and/or pigments dissolved or suspended in a water-based (aqueous) solution. Non-aqueous-based inks are available but are generally reserved for industrial and non-paper applications. A variety of additives are combined, such as antioxidants, biocides, fixatives and UV-blockers. The resulting mixture is quite complex.

Both dyes and pigments have advantages. In general, pigmented inks have better light-fastness and water-fastness. Conversely, dye-based inks tend to have better penetration and abrasion-resistance. Pigments are used for IR-absorbing symbology, such as OCR-B. Pigment-based UV fluorescing inks tend to be more stable over time. Many printing mechanisms use a combination of dyes and pigments. The trade-offs are application dependent and not straightforward.

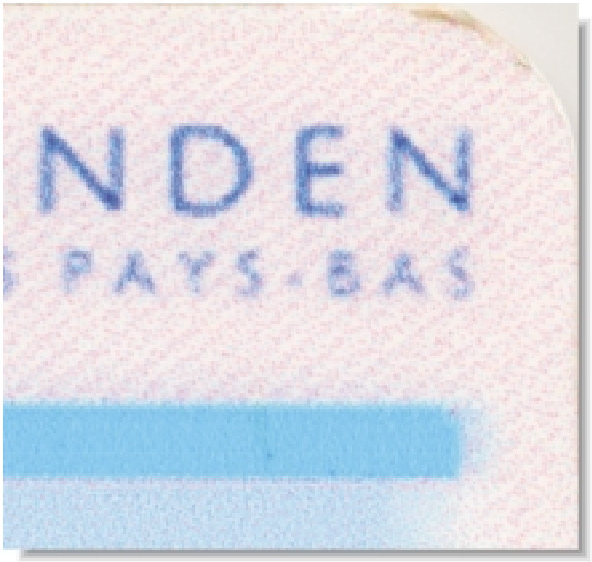


Figure 5-6: View of inkjet printing applied onto an Dutch counterfeit Identity card.
The characteristics of the coloured dots are clearly visible.
(Courtesy of Sdu Identification, Haarlem, the Netherlands.)

In inkjet systems, the applicator is a multi-orifice print head. For security documents a “drop-on-demand” process is used. Other technologies, such as continuous drop, are more applicable for high speed, web printing applications. The print head traverses over the target substrate in a manner similar to home or office inkjet printers. The ink is ejected from the print head using a variety of methods, hot melt and piezoelectric being the most common.

Resolutions are advancing rapidly. Ten to fifteen years ago, 300 x 300 dpi resolution was standard. Today, resolutions of 4800 x 1200dpi, 4800 x 2400 and 5760 x 1440 dpi are available. Such high resolutions both pose threats and offer opportunities to issuers of secure documents.

As previously-mentioned, the current rapid developments are being driven by office and home computer reprographic demands. However, our discussion here will focus on paper substrates. Security printing makes complex demands on receptors. To begin with, the target receptor has usually been printed using a lithographic or intaglio process. These printing processes alter the absorption characteristics of the paper. Security printing is also making demands with respect to light-fastness and water-fastness.

Absorption characteristics affect many secondary characteristics, such as drying time, lateral absorption, blooming and droplet scattering. These characteristics influence critical factors, such as colour fidelity, process speed as well as edge definition. Edge definition, in turn, is critical for machine-readable symbology and micro-printing.

Mechanical effects, such as curling and cockling are less problematic due to the thickness of most security paper. Still, they need to be considered.

Like other processes, text, graphics and images are created by means of a series of dots. Colours are created using combinations of Yellow, Magenta and Cyan dots. Particle-based systems create tonal images using dithering techniques. Dye-based systems offer the possibility of trading off dot spatial resolution for colour density levels. In either case, excellent colour images can be (re)produced. That is the reason why a security design is composed (also) of lines of colour.

Inkjet is an example of another technology that is also being driven by home and office reprographic demands. Systems designed for security printing enjoy the resulting technological advances. Once again, because the technology is readily available, anti-counterfeit and tamper-evident features are recommended.

Inkjet colourant costs are low, perhaps the lowest of all the cited technologies. Printing production rates are moderate; probably faster than laser engraving, but slower than electrophotographic or thermal transfer. Water-fastness, colour-fastness and UV-fluorescing stability may be a problem with dye-based systems. Appropriate UV-blocking laminates and anti-oxidants should remedy this. Conversely, abrasion resistance can be problematic with particle-based inks. Again, appropriate laminates should resolve this.

Of all the cited colour technologies, compatibility of the three-part system is crucial. Trade-offs will have to be made and the application requirements will propel these trade-offs.

D. Laser engraving

There have been a number of recent developments in laser technology. Laser engraving systems have benefited from these developments and there appears to be a growing interest in this method of personalization. Unlike other forms of personalization, laser engraving physically alters the document substrate.

The technical description below will give an insight of the laser engraving technology.

Current laser engraving uses Nd:YAG (Neodymium: Yttrium-Aluminum-Garnet) laser light directed by an optical system which acts as the applicator. The power of the lasers used range from 3.5 to 50 watts, which is considerably more powerful than those used in electrophotography.

Unlike other technologies, the "colourant"[3] is central to the receptor. For images and other high-resolution graphics, a layer sensitive to the YAG laser is laminated into the document structure.

The receptor is a laminated polycarbonate or composite "card" as depicted in Figure 5-7. Other materials can be used for laser engraving, including paper. However, specially formulated polycarbonate films react best with the YAG laser light for high contrast, detailed images. The format of the "card" can conform to ID-1, 2 or 3-size documents. For passport applications, the "card" is combined with the paper booklet by means of a variety of assembly methods.

In the case of secure documents, the appropriate decorative and security information (security design) would have been applied by the card manufacturer prior to lamination and die-cutting.

[3] However the resulting image is not coloured.

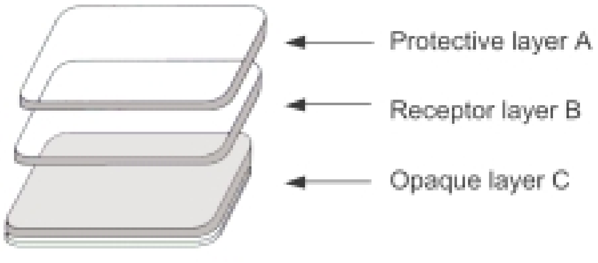
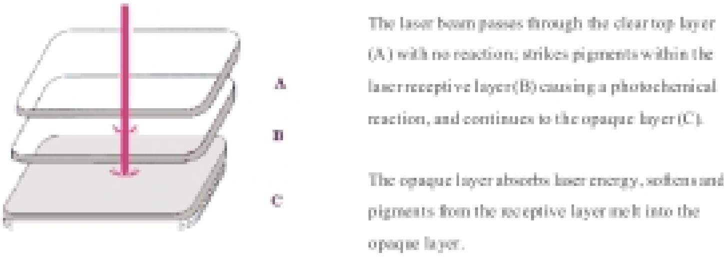


Figure 5- 7: Construction of the card

A variety of effects can be achieved by varying the laser power, beam focus, and depth at which the beam is focused. To create images under the protective layer a process similar to that described in Figure 5-8 is used.



The laser beam passes through the clear top layer (A) with no reaction; strikes pigments within the laser receptive layer(B) causing a photochemical reaction, and continues to the opaque layer (C).

The opaque layer absorbs laser energy, softens and pigments from the receptive layer melt into the opaque layer.

Figure 5- 8: The card during the laser engraving process

Tactile surface effects can be achieved using additional energy. Laser light energy is converted into heat energy that, in turn, causes the top layer (A) to rise sufficiently so that it can be detected by touch.

Laser can also be used to achieve a variety of security effects. Changeable Laser Images (CLI), developed by Mauer Electronics, and Multiple Laser Images (MLI), developed by Gieseke and Devrient, use a lenticular lens to create two or more images under the lens. By rotating the document around its vertical axis (for CLI) or horizontal axis (for MLI), the different images can be observed.

E. Laser perforation

More recently, Industrial Automation Integrators (IAI) has introduced ImagePerf™ (Hospel, 1998). ImagePerf™ uses a more powerful laser to create a matrix of fine holes through the substrate. Using a process similar to grey scale dithering, an additional image of the document holder, or other information, can be created. Under normal reflective lighting, the perforations are barely visible. Under transmitted light, the image created by the perforations is clearly visible.

The holes created by the ImagePerf™ process cannot be replicated by mechanical means as they are conically shaped.

IAI and Sdu Identification have developed the Tilted Laser Image® (TLI), which combines the effects of CLI/MLI and ImagePerf™ (van der Berg and Augustinus, 2000). Two images are created using the ImagePerf process. The images are achieved by creating holes at different angles. When the document is tilted over transmitted light, the different images can be observed.

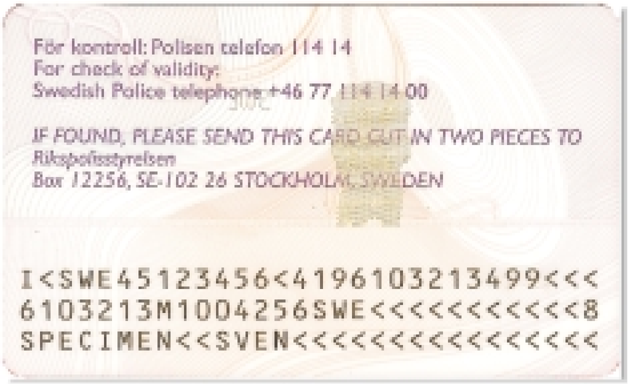
5.4.3 Machine-readable technologies

Machine-readable technologies provide a wide selection of data storage media. Those media are can be used for automated document or document holder authentication (see Chapter 7 The use of biometric with travel documents).

Depending on the technology used, one or more techniques can be encoded at the time of personalization. Such techniques include:

- optical character recognition (OCR)
- magnetic stripes
- two-dimensional barcodes
- optical stripes
- contact chips
- contactless chips.

Technically highly secured documents may combine different storage technologies. However, the International Civil Aviation Organization (ICAO), encourages Member States to adopt contactless IC media of sufficient capacity as the only globaly interoperable storage technology to facilitate the on-board storage of additional Machine Readable Travel Documents data and biometric identifiers (New Orleans resolution 21/03/2003). In closed systems issuers may wish to consider also alternatives. Before making choices, it is important to include also the price of readers in the overview of the costs. Here follows a brief overview of each of these technologies.



För kontroll: Polisen telefon 114 14
For check of validity:
Swedish Police telephone +46 77 114 14 00

IF FOUND, PLEASE SEND THIS CARD CUT IN TWO PIECES TO
Rikspolisstyrelsen
Box 12256, SE-102 26 STOCKHOLM, SWEDEN

```
I<SWE45123456<4196103213499<<<
6103213M1004256SWE<<<<<<<<<<<8
SPECIMEN<<SVEN<<<<<<<<<<<<<<<<
```

Figure 5-9: View of Machine Readable Zone applied on an ID-1 size Swedish identity document. (Courtesy of Swedish police, Stockholm, Sweden.)

A. Optical Character Recognition

The ICAO Panel on Passport Cards adopted Optical Character Recognition in 1978 as the first technology to be used for encoding machine readable information (ICAO, 2006). Ever since the OCR-B font type is being used for display machine-readable information in the Machine Readable Zone (MRZ) of travel documents. The MRZ is located in the lower part of the data page of the passport, on the visa and ID-2 size cards and on the backside of ID-1 cards. The MRZ contains a two or three lines sequence of letters representing information such as name, document number, date of birth, etc. This is the same information as the one displayed in the so-called Visual Zone (VIZ) of the travel document. For more information please consult ICAO Document 9303.

An information paper presented at the TAG/MRTD in 2004 by the Education and Promotion Working Group reported the status of the issuance of machine-readable travel documents. Based on data from surveys of the ICAO secretariat and from the Keesing Document Checker (online document database), the paper highlights that 100 ICAO contracting members worldwide and three other countries were issuing machine-readable passports.

B. Magnetic Stripes

The magnetic stripe is one of the oldest document machine-readable technology. Stripes have been added to financial cards as early as 1970s. They were added to ID-3-like savings passbooks at about the same time.

The magnetic stripe standard has remained virtually unchanged since it was first introduced in the 1960s, prior to floppy disks. In 2001 new magnetic stripe standards were published. The risk of forgers altering variable data contained in magnetic stripes was eliminated by the addition of a digital signature. However the risk of counterfeit/skimming is high. Skimming is a form of magnetic stripe counterfeiting in which criminals are able to copy magnetic stripe track information from a valid card (see Figure 5-10, skimming device).

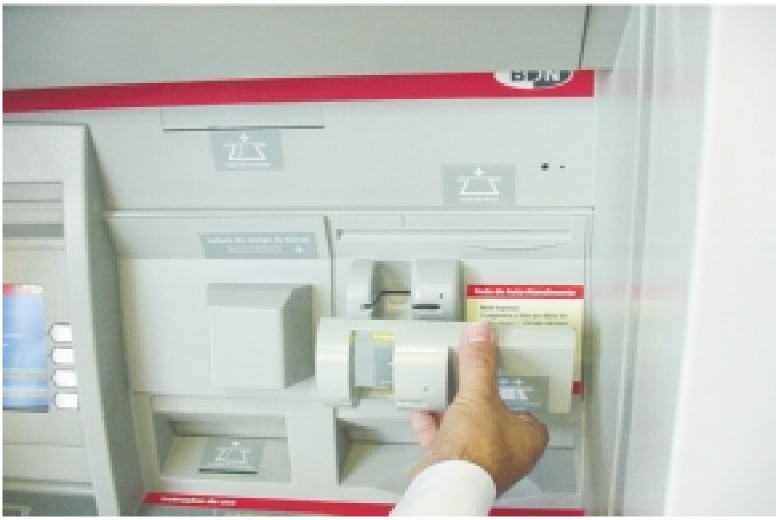


Figure 5-10: View of an skimming device placed up front an Automated Teller Machine (ATM). This skimming device is copying and storing the information of the magnetic stripe of a payment card.

(Courtesy of VISA international, London, United Kingdom.)

Information is then encoded on a counterfeit or stolen card and used fraudulently (APCA, 2006). Worldwide the security of ATM's has been upgraded to prevent that criminals would be able to alter the machine for catching the data of the card without the card holder's knowledge.

This way of storing digital information will probably be less used in security documents, as the contactless chip has become the choice for global interoperability (at least in travel documents). In the near future more and more credit cards issuers will switch over to chip technology.

C. Two-dimensional barcodes

High-capacity two-dimensional barcodes can store at least 10,000 bytes. The capacity of a given (proprietary) symbol varies depending on the available space, geometry of the space, print density, error correction level and mix of alphanumeric versus binary content.

Barcodes are very economical to print. If thermal printing is used for personalization, the barcode is printed at the same time as the other information, using the same ribbon segment. Thus, no additional time or supplies are needed. If electrophotograpic or inkjet technology is used, speed is unaffected and the additional colourant needed is negligible. Laser engraving does not require any additional material; however, personalization time could be affected.

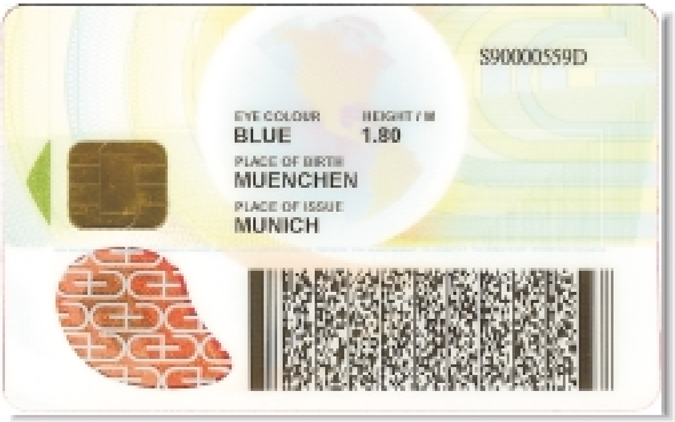


Figure 5-11: View of an Two Dimensional (2D) Barcode applied on a sample card. (Courtesy of Giesecke & Devrient, Munich, Germany.)

D. Optical stripes

Optical stripes offer the greatest storage capacity on ID-1 size cards. Stripes with a minimum area of 11.5 mm (0.45 in.) by 85.6 mm (3.37 in.) and a maximum area of 30.78 mm (1.21 in.) by 85.6 mm have storage capacities of 1.2 Mb and 2.8 Mb, respectively.

Optical stripes are similar to compact discs (CDs) in that they cannot be overwritten per se. Instead, new information is added and the previous information is identified as archived. Given the great capacities available, this approach should not pose problems and provides the built-in security of an audit trail. Like CDs, optical stripe data is stored on tracks. A small amount of data such a few thousand bytes may be best read all at once (serially). For larger amounts of data, it is better to read specific elements or groups of data (random).

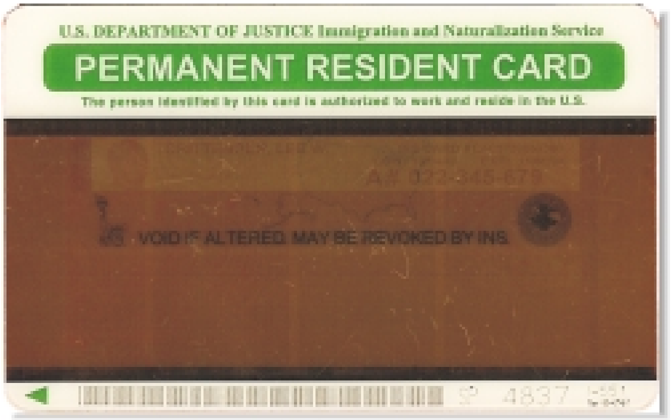

U.S. DEPARTMENT OF JUSTICE Immigration and Naturalization Service
PERMANENT RESIDENT CARD
The person identified by this card is authorized to work and reside in the U.S.
VOID IF ALTERED. MAY BE REVOKED BY INS.
4837

Figure 5-12: View of an Optical Memory Strip applied on the Permanent Resident Card (Green Card) of the United States. (Courtesy of Immigration Service, Washington D.C., United States of America.)

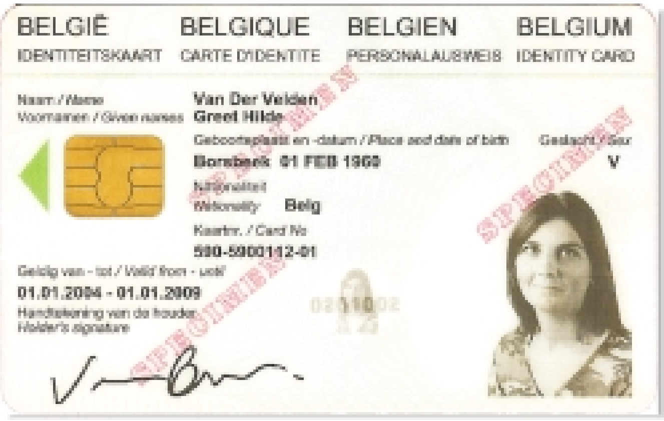
Like magnetic stripes and barcodes, the information recorded on an optical stripe is visible and therefore “skimmable”. However, specialized recording techniques can be used to render such visibility very poor without the proper reader. Given the amount of data recorded, manual interpretation would be tedious at best.

The cost of optical stripes is comparable to that of chip cards. However, reader costs should also be included in the equation, especially where applications call for a large number of readers. Surface abrasion can impair read reliability. However, an error correction feature is incorporated into a reader to maintain read reliability. Still, it could be worthwhile to supply a protective jacket for optical cards.

Personalization speeds can be a problem. Encoding times vary depending on the amount of data from up to one minute or longer.

E. Contact chip cards

Much like optical stripes, chip card technology is only available on ID-1 size cards.



BELGIË BELGIQUE BELGIEN BELGIUM
IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD

Naam / Name Van Der Velden
Voornamen / Given names Greet Hilde
Geboorteplaats en -datum / Place and date of birth Geslacht / Sex
Borsbeek 01 FEB 1969 V
Nationaliteit
Nationality Belg
Kaartnr. / Card No
590-5900112-01
Geldig van - tot / Valid from - until
01.01.2004 - 01.01.2009
Handtekening van de houder
Holder's signature

Figure 5-13: View of a electronic Identity card with a chip,
applied on an Belgium Identity card.
(Courtesy of the National Register of Ministry of the Interior, Brussels, Belgium.)

Chip technology is progressing rapidly, enjoying the benefits of integrated circuit developments in general. Capacities are being driven more by market demands than the challenge to break technological barriers. Currently, chips with 32 kb, 64 kb and higher of user data storage are available. Such capacities are quite sufficient for most ID applications. However, higher capacities could be needed for biometric applications.

Security, rather than capacity, is the primary advantage of chip cards. Chip cards can operate under a secure operating system. Write-access to specific data elements or groups of data can be cryptographically controlled, i.e., one seeking to modify or append data must correctly respond to a cryptographic challenge. Read-access can be similarly controlled. If necessary, data can be defined as secret, and if defined as so, may never be read from the card.

Like optical stripes, the data in a chip card can be read all at once (serially), or specific data elements or groups, if elements can be addressed and read individually (random).

Many chip cards are actually microprocessors. As such, they can be programed with other applications. When multiple applications are included, the chip operating system typically isolates the applications. Direct communication or data exchange between the applications is not possible.

Personalization speeds vary depending on the amount of data, chip input/ output speeds, how data is structured, and security protocols. Load times of 10 to 40 seconds are typical. For this reason, high-speed personalization systems generally load a number of chips in parallel, allowing a reasonable throughput of cards[4].

F. Contactless chips

Contactless chip technology has advanced rapidly. For most people, contactless technology is synonymous with simple radio frequency tags used for electronic article surveillance or proximity access control cards. Technological advances now permit chips comparable to contact cards - 32 bit CPUs, up to 1 Mb of total memory, asymmetrical encryption co-processors, Java interpreters and dual communication capabilities (contact and contactless). Costs are approaching those of contact-only devices.

[4] As each production system has peculiar characteristics in terms of machines, data, network and software it is here unfortunately not possible to predict any final process speed.

Currently there are two standards for non-contact cards: ISO 14443 for “proximity” devices, and ISO 15693 for “vicinity” devices. Proximity devices can communicate at ranges of up to 10 cm at speeds in excess of 100 kb/sec, approximately five times faster than most contact chips. The current base communication speed for ISO 14443 devices is 106 kb/sec (Finkenzeller, 2003). Vicinity devices can communicate at a range of up to 1 m at speeds of up to 26.48 kb/sec (in “fast mode”) (Finkenzeller, 2003). The range and communication speeds of vicinity devices vary depending on the mode of operation – read-only, authenticate or write. Higher communication speeds can significantly reduce the time required to load data onto the document.

In 2003 the New Technology Working Group Meeting in Glasgow eliminated ISO 15093 as an alternative standard for IC chips for Machine Readable Travel Documents. This choice means a reduced eavesdropping risk. Eavesdropping occurs when the communication to and from MRTD can be tapped. Skimming is a fraud method also applicable to contactless chips. As a countermeasure, an authentication procedure needs therefore to be implemented. ICAO recommends the Basic Access Control (BAC), which allows the access to the chip only after reading the MRZ of the travel document. However, according to experts, also this measure has a limited fraud prevention coverage (Fidis.net, 2006).

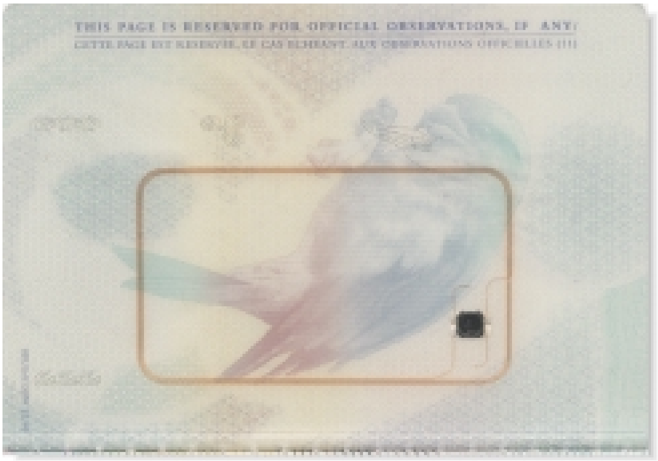

THIS PAGE IS RESERVED FOR OFFICIAL OBSERVATIONS, IF ANY:
CETTE PAGE EST RESERVEE, LE CAS ECHEANT, AUX OBSERVATIONS OFFICIELLES (11)

Figure 5-14: View of a proximity chip, applied in an British passport. (Courtesy of National Criminal Intelligence Service, the Netherlands.)

■ 5.5 Tests

Testing a product concept involves assessing compliance with the international standards, document functionality, effectiveness of the applied safeguards, and product durability. This is ascertained by subjecting the product concepts to an intensive test program in which each aspect must score a minimum number of points.

The producer is required to have access to independent experts and the means to conduct these tests in a responsible and effective way. For specific aspects outside the producer's expertise, the producer can call in the help of external laboratories and experts. For instance, a laboratory specialized in raw materials can conduct toxic tests, while a panel of user groups can assess the user functionality of the document during the development stage. In order to assess fraud resistance, the producer can rely on the help of anti-fraud organizations in addition to its own specialists.

The tests performed in laboratories with specific equipment can be divided into three categories:

- tests to ascertain compatibility of the materials;
- tests to verify resistance to fraudulent manipulations;
- tests to verify compatibility with international standards.

These tests are not performed in a fixed sequence, but are often conducted simultaneously and the results are evaluated as a whole.

5.5.1 Compatibility of materials

Tests related to substrates, inks and other elements to be integrated into the document (cover, OVDs, etc.) serve to verify the compatibility of the materials, to explore the choices of a supplier and to define the final specifications of the secure document to be produced. A classic example is the compatibility of substrate with the required personalization technique.

The compatibility test program may involve the following tests (this list is obviously not exhaustive):

- climatic tests

- resistance to light
- abrasion
- resistance to chemical agents
- wear and tear (e.g. simulating a person carrying the document in the back pocket of his trousers).

During the climatic tests, the document (or parts of it) is subjected to different conditions of light, temperature and humidity to simulate the ageing process. Special equipment and controlled conditions are used for this process. At the end of the ageing cycle, the laboratory staff notes all changes in appearance in terms of colour, shape, dimensions, etc.

One should bear in mind that a travel document accompanies its owner everywhere. Therefore, it is important that the materials used for the manufacture of this kind of document are resistant to climatic extremes. At the same time the appearance should, under normal conditions of use and storage, remain unchanged during its validity. For instance, consider what would happen to your driving license if you washed it with your clothes in the washing machine.

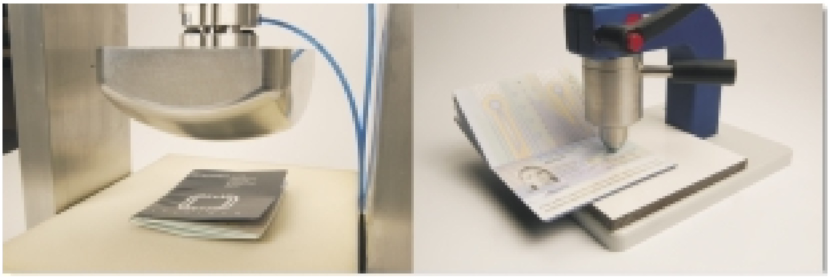
Another important test is the light resistance test. Travel documents can be used for several years. In some countries a passport can be valid up to 25 or 50 years! International standards recommend however a validity of 10 years[5]. During this period, the colour of some components should remain the same: the cover, personal data and printing inks. In the test, the material is exposed to an artificial source of light equivalent to sun rays at a constant relative humidity. A reference sample is subjected to the same treatment. Depending on the time of exposure, the colour of the reference sample changes according to the “Blue Wool Scale”. A material with value 3 on the Blue Wool Scale is less light resistant that one with value 5.

Resistance to (mechanical) abrasion is determined by means of a pin. The material is fixed to a carrier, and a pin, wrapped in new gauze, is put in contact with the surface undergoing testing. After a given number of cycles, the tested material is closely inspected to ascertain any damage. Generally, the cover and the data page are subjected to this test.

[5] This would probably allow to verify in the majority of the cases that the holder's face still bears a resemblance to the portrait displayed in the travel document.

To test resistance against chemical agents, the document is immersed in liquid chemical solutions for a given time, after which it is examined for damage.

Another test examines the interaction between the basic material and personalization technique. In some cases the documents undergo variations of pressure and/or temperature and possibly also mechanical stress (see Figure 5-14). The design of personalization machines needs to be fine-tuned with the documents to be personalized in order to avoid major problems during implementation of the concept. A typical example is the inkjet printer. The paper of the document has to be able to absorb the small ink droplets without spoiling the printed image, which would result in a blurred image.



Dynamic bending test

Stamp impact test

Figure 5-15: View of the dynamic bending (hip-pocket) test and the stamp impact test as described by Jan van den Berg in the (testing three types of e-passports) Keesing Journal Document & Identity.

(Courtesy of Sdu Identification, Haarlem, the Netherlands.)

5.5.2 Fraudulent manipulations

The materials chosen for the production of documents are also analysed for fraud risk. Where the composition of the document and its personalization is potentially at risk, a specialized laboratory may be called in to perform mechanical and chemical manipulations similar to the ones carried out by professional forgers. Since no standards explain which protocols have to be followed, the reliability and consistency of those test is proportional to the experience and skills of the examiner.

The role of the document expert is vital to the success of the entire test process. In the laboratory, he must examine and test the compatibility of the materials and the manner in which they interact, seeking the best solutions to increase and enhance the overall security of a document. The combination of security features, materials and techniques must be well thought of so as to ensure full compatibility and protection during the entire lifetime of a document. This is usually subordinate to the rest of the document's manufacturing process, but plays a decisive role in achieving an effective performance of the final product – the secure document. The test method involves an analysis of how documents react to several handling conditions. This includes how well they stand up to tests of durability, resistance, photosensitivity, as well as how they react to deliberate submissions to chemical solvents, bases, acids etc. with the ultimate aim at falsification.

5.5.3 Compatibility to standards

As mentioned in Chapter 2, international standards aim at interoperability. ISO standards describe tests applicable to ID-1 plastic cards (e.g. ISO/IEC 10373-1:2006).

As ICAO is more concerned with travel documents, a new series of durability tests, especially for e-passports, is supplemented to Document 9303 Technical Reports (RF Protocol and Application Test Standard for e-Passports).

Once the tests are concluded, the document developer receives the first draft of the document's specifications, which is important information for the ultimate mass production of the document.

■ 5.6 Preparing mass production

Even before the graphic design is finalized and approved, preparations are made for mass production. Depending on the nature of the project, some of the supplier's other in-house disciplines are involved in the project.

In the first phase, these preparations could involve drafting the final specifications for materials and equipment, concluding the contracts with the suppliers, ordering equipment and materials, making arrangements for the necessary production capacity, and drawing up control and quality objectives.

In the second phase, arrangements have to be made for housing the new equipment and techniques while plans for production, testing and acceptance are drawn up. In this phase, the progress and quality of the equipment being built must also be monitored, and the materials produced and supplied tested for conformity to specifications. Any necessary new production methods undergo testing, after which they can be approved and implemented.

This phase requires intensive interaction between the project developers, who are tasked with the development of the new document, and their production processes involving the necessary disciplines.

The third phase focuses on the selection and training of personnel as well as the implementation of new knowledge and skills in the supplier's organization. This phase typically involves intensive test programs for equipment, materials and procedures, concluded by an overall acceptance test by the contracting party, in which the operation and quality of all sub-processes are assessed.

Important in the preparation for mass production is that the contracting party and producer reach a clear agreement on product quality. As far as the printed matter is concerned, both the contracting party and graphic designer have to agree on the end result of each printed sheet produced under mass conditions. This process must be repeated for all relevant features of the final product. These are usually aesthetic features for which no international standards exist.

It is the producer's responsibility to present samples that are representative of the entire production, i.e. samples that have been manufactured under sound production technical conditions and can therefore be reproduced in future productions that may span several years. It is up to the producer to see to it that the above approvals are correctly documented for future printing.

■ 5.7 Quality Assurance

The binomial quality assurance is a well known one among most project managers. In which way would they give their personal interpretation to it in the field of security documents? The following paragraph describes a fictitious situation, which will nevertheless illustrate the need of quality assurance.

Imagine a highly secured building in some country. It is the weekend before the start of issuance of a new travel document. Because of very tight schedules, a big effort has been made in the last couple of days in the personalization facilities for fine-tuning the machines to achieve an acceptable quality standard. It is Friday late afternoon when suddenly the power supply fails everywhere in the building. The emergency generator starts immediately, but the working settings in the personalization machines are lost. The last operator on duty looks for the back-up files in order to restore the last settings. Unfortunately the support engineer responsible for making the back-up is sick since the beginning of the week and the storage media on her desk are labelled inconsistently. The supervisor has just stepped in the train and the production manager's mobile phone is out of range.

Instead of having a panic attack, the operator asks the security officer to meet in front of the safe room. Together they open the safe, where the proper back-up and the related documentation are stored. In the meantime, the machines have started up and the operator loads the last settings of that day. Luckily, the supervisor made the regular back-up just before leaving...

How can an organization assure that a certain event is handled according to agreements made with the customer? How can the customer verify that everything is in place for getting expected the product within the agreed quality frame?

Everything revolves around documentation and communication. Quality assurance requires people involved in a given process to know the answers to the “who-what-where-when-how-why” question if they are in an (extra)ordinary situation. This means that the product and the related production process are described in detail; that this information is available to people who need it; that the settings are recorded and that operational procedures are set up in the organization.

5.7.1 Product specifications

As seen in the previous chapters, a secure document is something in which various half-finished components make up the end product. The company that brings together the components for the manufacture of the end product adding own expertise, plays a central coordinating role in the development and supply of the components, with regard of the appearance, the specifications and the supplied services. Of course, the contracting party is directly involved in this.

The production of secure documents demands that quality and component specifications are documented. For each aspect describing the component, as well as the end product, nominal values and tolerances are defined: the product specifications. The producer draws up the product specification, as soon as the development phase has been passed. Next to that the producer makes agreements with the suppliers with respect to the specifications and quality standards of their products.

5.7.2 Inspection by attributes in a manufacturing environment

The concept of “Meten is weten”, a famous Dutch expression, translates to “what you can measure you can control”.

Besides the appropriate production process control, several checks are performed during the entire manufacturing process in order to inspect qualitatively and quantitatively the products characteristics and verify that they meet the specifications. Quality control is performed at three stages of the process:

1. When the raw materials are purchased in order to verify conformity to the specifications;
2. At the production stage: characteristics of semi-manufactured products are controlled in order to limit waste;
3. At the end of the manufacturing process: when final products are checked before shipping to the customer.

Agreements will have to be reached regarding the quality of each aspect of the separate components in order to ensure a consistent quality for each component. However, a security document customer is generally less interested in the features and specifications of a component than in the quality of the finished product, which is the result of the accumulated quality of the separate components. Quality control of the final product is integral to the producer's entire quality system, and setting down the properties of the materials and processes is an important part of this system.

The operator of the production equipment performs quality controls during the production process in order to adjust the process by the first appearance of deviations. For some semi-manufactured products an internal laboratory of testing person could check some characteristics, which require more expertise or special tools. If attributes requires visual checks, the producer can choose to make models which represent nominal values and models for the maximum and minimum tolerances.

ISO developed a series of different inspection methods. Security documents are not a simple consumer good because of their customized development. Therefore the most suitable inspection scheme is the sample plan called inspection by attributes.

This kind of plan is intended primarily for use in a continuing series of lots or batches. Inspection is the process of measuring, examining, testing, or otherwise comparing the sampled product with the requirements. A "lot acceptance sampling plan" is a sampling scheme and a set of rules for making decisions. The decision, based on counting the number of defectives in a sample, can be to accept the lot, reject the lot, or even, for multiple or sequential sampling schemes, to take another sample and then repeat the decision process. With inspection by attributes, either the unit of product is classified simply as conforming or nonconforming, or the number of nonconformities in the sample is counted, with respect to a given requirement or set of requirements.

The Acceptable Quality Level (AQL) is the percentage of defects forming the baseline requirement for the quality of the producer's product. The producer would like to design a sampling plan such that there is a high probability of accepting a lot that has a defect level less than or equal to the AQL.

The ISO standard 2859 sets the frame for the procedures for inspection by attributes.

5.7.3 Quality of software

Like the physical document, which is described by the customer, designed by the producer, reviewed and tested by both, software development calls for similar stages. The most difficult part to explain within the scope of this book is certainly the testing, which is a main metrics of software quality, according to ISO 9126.

Software testing primarily verifies that the code does what it is supposed to do, according to the specifications and without failures. Preparing a test protocol demands a good understanding of the test object. This means that the test designer oversees the functions of the software which would allow him to define a significant number of test cases. The tester's task is to perform a number of predefined actions for each test case, record the result and match it with the expected outcome. By unexpected findings, the tester would probably confer with the software engineer for the correct interpretation. The testing effort could be driven by acceptance or exit criteria which allow the tester to come to an end when they are met.

5.7.4 Quality of the personalization

Based on the reliability principle, the quality of the personalization should be constantly monitored, whether it is performed by a government entity or by a supplier.

The most critical elements in personalized identity and travel documents are the person-related features: signature, portrait and other biometric information (e.g. fingerprints, iris). Those features are used in practice for the verification of the identity of the holder of the document. Therefore they need to be recognizable enough to be used to this purpose. Beside this, it is crucial that those features satisfy international standards and agreements.

Independent of the data acquisition process, the variable information needs to be checked on at least three aspects at the input and output stages: correctness, completeness and formal specifications (e.g. position of the variable information).

Also in the personalization environment operational procedures are set up. The personalization staff is trained in quality assessments and has access to defined quality standards and supporting tools.

References

ACPA
2006 Australian Payment Clearing Association, Payment Fraud Statistics, Methodology paper, Sydney.

Billmeyer F. W.
1984 *Textbook of Polymer Science*, 3rd Edition, John Wiley & Sons Inc., New York.

Canon
2006 http://www.canon.com/technology/electrophotography/index.html

Fahrmeir A.
2001 "Government and Forgers: Passports in Nineteenth-Century Europe", *Documenting Individual Identity*, Caplan J. and Torpey J. eds., Princeton University Press, Princeton.

Fidis
2006 Budapest Declaration on Machine Readable Documents, http://www.fidis.net/press-events/press-releases/budapest-declaration/, Brussels.

Hospel W. G. J. M.
1998 *Application of laser technology to introduce security features on security documents in order to reduce counterfeiting*, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques II, SPIE vol. 3314:254-259, San Jose.

ICAO
2004 Technical Report V 2.0 "Biometrics Deployment of Machine Readable Travel Documents TAG 15 endorsed 21/5/2004.
ICMA
2006 http://www.icma.com/info/Polycarbonate5605.htm, International Card Manufacturers Association, Princeton Junction.

Kodak
2006 http://www.kodak.com/country/US/en/digital/dlc/book3/chapter1/digFundOutput6.shtml

Ponds S. F.
2002 *Inkjet Technology and Product Development Strategies*, Torrey Pines Research, Carlsbad.

Straus S.
2006 http://www.polymernotes.org, Kranj, Slovenia.

van den Berg J. and Augustinus A.
2000 “New optical security features in plastic documents”, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques III, San José, *SPIE* vol. 3973:167-175, San Jose.

Van den Berg J.
2004 testing Three types of e-passports. *Keesing Journal of Documents & Identity, a magazine about developments in the security industry*. Issue 8, 2004.

Wikipedia
2006 http://en.wikipedia.org/wiki/Polymer_banknote

CHAPTER 6

IDENTITY AND ITS VALUE

“I would here observe that very much of what is rejected as evidence by a court is the best of evidence for the intellect”
Edgar Allan Poe, The mystery of Marie Roget (1842)

■ 6.1 Introduction

The study of fingerprints as a means of positive identification by outstanding scientists like Sir William Herschel, Dr. Henry Faulds, Sir Francis Galton, Sir Edward Richard Henry and Dr. Edmond Locard was the starting point of the science of individualization, termed by some criminalistics, by others forensic science (Kirk, 1963).

The first part of this chapter is dedicated to the concept of identity and to its application in forensic science. The content of this theoretical basis is a brief summary of the unique and remarkable research effort on this particular topic, the brilliant but underrated PhD dissertation of Dr. Quon Yin Kwan entitled “Inference of identity of source” (Kwan, 1977). The second part illustrates the confusion associated with the notion of identity in forensic science. The third part is devoted to the description of the forensic individualization process based on the hypothetical-deductive method, while the last part proposes a framework to design a computer-based system for forensic biometric individualization.

Note of the Editors: this Chapter has been published by Didier Meuwly in *Science and Justice* in 2006 (Volume 46 nr 4)

■ 6.2 Identity

6.2.1 Definition

"In forensic science and law, identity is the set of characteristics in terms of which a human being defines its own personality and distinguishes itself from all others. In this context establishing the identity of an individual is the forensic task called identification. A human being may be similar to several others or to one other person to the extent that it causes errors; but it can only be identical to one person, himself. The challenge of identification lies in the careful discrimination of elements of similarity from elements of true identity.[1] (Locard, 1909)

6.2.2 Ambiguity

The term "identity" has a dual character and this duality gives rise to ambiguity. When the concept of source is used with reference to an object of interest to signify a class of individual entities from which this object could originate, it refers to qualitative identity. This is due to the fact that a class is defined by an identity of the properties of its members. The task in which a class is determined to be the source is termed "classification" or "identification" in science. When the concept of source is used to signify one particular individual entity from which an object originates, it refers to numerical identity. The operation in which a particular individual entity is determined to be the source of an object is termed "individualization" in science, but is often wrongly named "identification" in forensic science.

Confusion surrounds the terms "identity", "identify" and "identification" in forensic science. This is clearly demonstrated in popular practice, when

[1] Freely translated from the original French citation:
"En police scientifique et en droit, l'identité est l'ensemble des caractères par lesquels un homme définit sa personnalité propre et se distingue de tout autre. Dans ce dernier ordre d'idées, établir l'identité d'un individu est l'opération policière ou médico-légale appelée identification. Un homme peut être semblable à plusieurs autres, ou à un autre, au point d'amener des erreurs ; il n'est jamais identique qu'à un seul, à lui-même. C'est à discriminer avec soin les éléments de ressemblance des éléments d'identité que consiste le problème de l'identification".

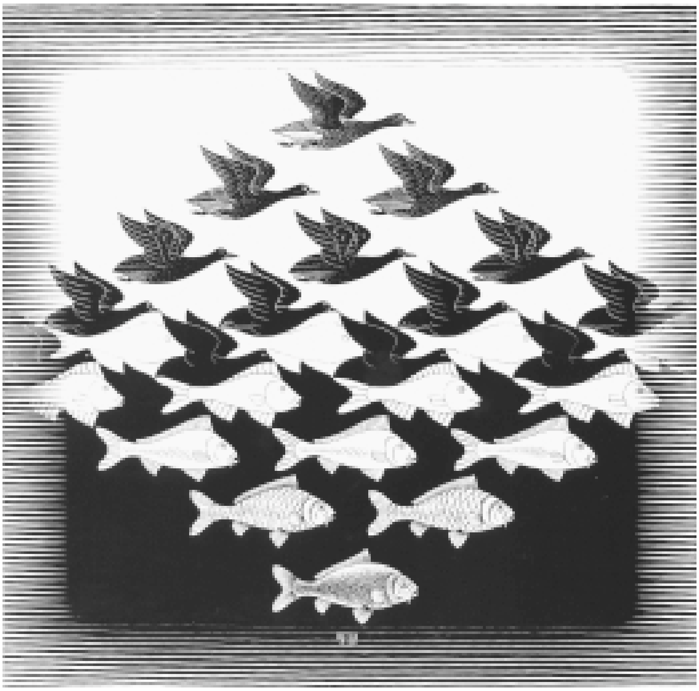


Figure 6-1 M. C. Escher, Sky and Water I, 1938.
The term "identity" has a dual character and its duality induces ambiguity.

the perpetrator of an infringement is said to be "identified from her/his fingerprints". The perpetrator is not identified but individualized. What is proved by the fingerprints is individuality (Tuthill, 1994; Doddington, 1985). Kirk (1963) emphasizes this confusion as well, but concludes:

"The real aim of all forensic science is to establish individuality or to approach it as closely as the present state of science allows. Criminalistics is the science of individualization. The criminalist is not ultimately interested in the similarity of two objects but in their source".

Therefore, to individualize a human being on the basis of biometric data in forensic science ultimately consists in determining if an individual is the source of the biometric feature analysed.

6.2.3 Identity in forensic science

According to Kwan, “what is meant by identity of source is relative to what source signifies. When source refers to class, identity is akin to qualitative identity and when source refers to an individual, identity of source is akin to numerical identity. This distinction made between the two kinds of identity is consistent with the classical forms of identity distinguished by philosophers over the ages. The reason for the approach from a philosophical perspective is that the central problem of identity of source comes to be known” (Kwan, 1977).

6.2.4 Distinguishing numerical from qualitative identity

Qualitative identity is established when a set of properties agrees in two objects. Numerical identity is demonstrated by establishing continuity in time. A well-known example of numerical identity in forensic science is the chain of evidence, or chain of custody. To be maintained, the chain of evidence requires proof that the item is the same individual entity, from the time of collection on the crime scene to the time of presentation in court. Because qualitative identity is not determined by this criterion of continuity, it is relative. The relativity of qualitative identity falls on the observer, especially with respect to his choice of properties to characterize objects (Kwan, 1977).

The principal distinguishing characteristic between numerical and qualitative identity is time. Time makes identity of objects absurd since no two objects can be one object simultaneously. Identity of source is a relationship that involves time because of the need to establish the continuity of objects from one source in time. Qualitative identity, on the other hand, is independent of time. Time implies that numerical identity is compatible with change whereas qualitative identity is not.

“A thing can be identical only with itself, never with any other object, since objects in the universe are unique. If this were not true, there could be no identification in the sense used by the criminalist” (Kirk, 1963). To convince yourself that numerical identity is compatible with change, take your ten-year-old identity document, compare your face with the passport photo of this identity document and observe the changes. This shows that two objects with different qualities, existing at different times, can be numerically identical. This finding illustrates that numerical identity does not entail qualitative identity and, vice versa, qualitative identity does not entail numerical identity. It demonstrates the absence of a logical relationship between numerical and qualitative identity.

■ 6.3 Confusion between numerical and qualitative identity in forensic science

The discussion on the relationship between qualitative and numerical identity provides different perspectives on identity. In his work Leibniz never explicitly stated a law relating qualitative and numerical identity, but two different interpretations of his position on identity have created considerable confusion. Leibniz's position on identity is expressed in two formal maxims: the Law of Identicals and the Law of Identity of Indistinguishables. The former says that what is featured in one thing is featured in another when the two are numerically identical simultaneously.

There is no problem with this interpretation although, according to Wittgenstein, it is just the same thing twice but in different words (Kwan, 1977). The latter simply equates qualitative identity with numerical identity, which is not a valid relationship, as explained above. In spite of the questionable validity of this second interpretation has become a general principle for forensic science.

6.3.1 General principle of uniqueness

A. DOGMA…

The idea that identity of source can be deduced on the basis of qualitative identity and on the assumption of uniqueness of the source is still widely supported by the forensic community (Tuthill, 1994). In forensic science the individualization process is most often perceived as a process of rigorous deductive reasoning (Taroni, 1997): as a syllogism composed of a major premise, a minor premise and a conclusion[2].

[2] Following the first rule of syllogism according to Aristotle "*Terminus esto triplex: medius, majorque, minorque*", a syllogism should be composed, to be valid, of a general principle, named major premise, a particular observation, called minor premise and the deduction, called medium term or conclusion.

The major premise is the principle of uniqueness applied to the properties of a source and to the properties of the object generated by this source, the minor premise is the observation of the correspondence of the observed properties between the source and the trace, while the conclusion is that the source and the trace have a common origin because of the correspondence of the observed properties.

B. …BUT SHORTCOMINGS

However, the general principle of uniqueness assumed in forensic science must be qualified as a dogma because "this principle of forensic identification" is based on inductive reasoning. It is founded on a line of reasoning that proceeds from particular statements (based on observation or experience) to universal laws or theories. Both Locard (1924) and Eco (1983) are conscious of this misuse of inductive reasoning in forensic science, when they invoke the eighth rule of syllogism according to Aristotle: no deduction can follow two minor premises.

This logical statement was first developed by Sextus Empiricus (AD 150-230) and Hume adapted this criticism of the application of induction to the notion of causality. Therefore induction cannot be considered as rigorous reasoning for individualization in forensic science because what is true in particular is not necessarily true in general. The misuse of induction provides the illusion that science substantiates categorical conclusions of identification or exclusion (Evett, 1996).

C. THE CRITERION OF EMPIRICAL FALSIFIABILITY

Popper uses Hume's position but argues that complete verification of any scientific statement is impossible; therefore, the complete verification of the general principle of uniqueness applied to forensic science is not possible. Popper refutes the criterion of scientific verifiability but proposes instead the criterion of empirical falsifiability as a demarcation criterion.

Popper's reasoning process is based on a fundamental logical consideration: to prove the hypothesis of a general principle from particular or singular statements is impossible, but it is possible to falsify it. Falsifying a hypothesis amounts to proving that the hypothesis of a general principle is false because one or more cases contradict it: what is false in particular is false in general. To fail in the attempt to falsify the hypothesis of uniqueness will never prove that the principle is true but, in standing the tests, the hypothesis can reach a sufficient degree of corroboration to be used as a basis for practical application, described as a degree of "verisimilitude" by Popper.

6.3.2 Principle of uniqueness applied to biometric individualization

A. DOGMA…

The uniqueness of the characteristics used for biometric individualization is in general assumed without debate, both in forensic and commercial applications of biometrics (Doddington, 1985). Moreover in forensic science, the principle of uniqueness assumed for the properties of the source is often extended to the properties of the trace without question. For example, the uniqueness is assumed for the fingerprint (source) and the fingermark (trace), for the face (source) and the still or the live picture of the face (trace) as well as for the voice (source) and the speech audio recording (trace).

B. … BUT SHORTCOMINGS

The demarcation criterion of empirical falsifiability developed by Popper in most cases conflicts with the hypothesis of uniqueness of the characteristics used for biometric individualization. The different extent to which various biometric characteristics are able to meet the demarcation criterion of falsifiability is experienced in everyday life as well as in forensic practice, as shown in the following examples.

C. ASSUMPTION OF UNIQUENESS FOR COMPLETE ROLLED INKED FINGERPRINT

Automatic fingerprint identification systems (AFIS) have been used for 30 years, collected in databases of convicted people and of asylum seekers in order to detect repeat offenders and prevent multiple asylum applications. In these two situations, a ten-print sheet from a suspected person or from an asylum seeker is made, and two fingers, generally the right index and the middle finger, are searched against the fingerprint collection. The eight other fingers are generally not used for the automatic research, but when the candidate is proposed by the system, they can be used by the fingerprint examiner to falsify the hypothesis of identity based on the automatic comparison of the two first fingers.

As far as we know, this procedure of individualization based on ten inked fingerprints (considered as secondary sources, the primary sources being the real papillary ridges) is extremely difficult to falsify. Of course this consideration only takes into account the output of the automatic process and not the output of the entire process including human interaction with the AFIS, because human errors due to clerical mistakes or others are intrinsic to any human activity.

From our point of view, the assumption of uniqueness of the fingerprint first formulated by Herschel and Galton (Bolt, 1970) reaches a sufficient "degree of verisimilitude" and therefore renders very valid the assumption that the complete rolled inked fingerprint is a reliable enough representation of the real finger for human individualization. This assessment is of capital importance for the choice of relevant biometric characteristics to be selected for the development of identity documents.

D. Assumption of uniqueness of the fingermark

In contrast, forensic practice is punctuated with several cases of false individualization of defendants on the basis of the comparison of fingermarks (traces) with inked fingerprints by fingerprint examiners. Apart from the "erroneous fingerprint individualization in the Madrid Train bombing case" in which Brandon Mayfield, a Moslem attorney-at-law from Oregon, was wrongly associated to fingermarks found on the crime scene (Stacey, 2004), one can quote the Scottish case of H. M. Advocate v. Shirley McKie.

In the second case, and for the first time since the adoption of the 16-point standard, a full identification of a latent mark has been challenged in a court of law in the UK, and that challenge was upheld by a unanimous verdict (Grieve, 2000). Therefore, from our point of view, the assumption of uniqueness of the fingermark does not reach a sufficient "degree of verisimilitude".

E. Assumption of uniqueness of the human face and voice

The uniqueness of properties of the human face is also questionable, as no idiosyncratic property is known or can be assumed for this biometric modality. As for voice, the hypothesis that no two humans speak exactly alike is plausible, but to date no large-scale demonstration of the extent of

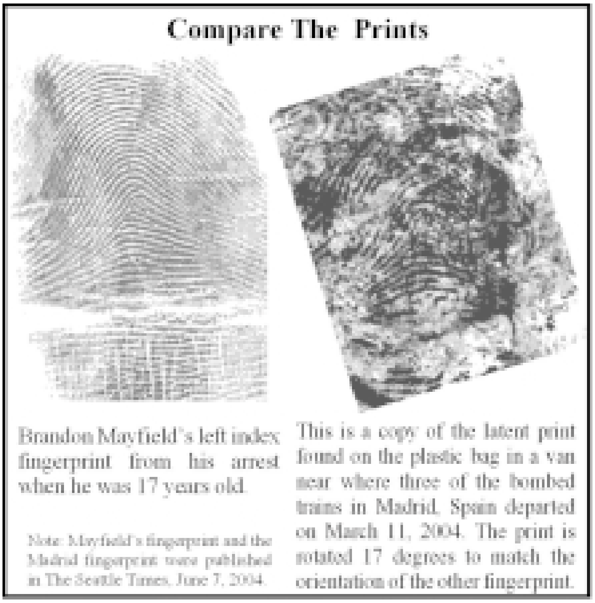

Compare The Prints
Brandon Mayfield's left index fingerprint from his arrest when he was 17 years old.
Note: Mayfield's fingerprint and the Madrid fingerprint were published in The Seattle Times, June 7, 2004.
This is a copy of the latent print found on the plastic bag in a van near where three of the bombed trains in Madrid, Spain departed on March 11, 2004. The print is rotated 17 degrees to match the orientation of the other fingerprint.

Figure 6-2: View of the fingerprints of the Brandon Mayfield case. The left fingerprint is of Brandon Mayfield while the right fingerprint was found at the crime chine of the Madrid train bombing.

idiosyncrasy in a homogeneous community of speakers has been adduced in support of this hypothesis (Nolan, 1991). Therefore, the assumption of uniqueness does not reach a sufficient "degree of verisimilitude" for the human face and voice.

F. Assumption of uniqueness of the properties of human face and voice traces

The consideration mentioned above is also true for the properties of the face and voice traces. Experiences of everyday life as well as the findings of applied psychology and artificial perception confirm the limitations of human beings and machines in their capacity for biometric individualization based on face recognition, voice recognition or on those two combined (Clifford, 1980; Boves, 1998). This situation is particularly relevant in forensic science, where the trace is normally of limited quality for voice and face, for instance a telephone quality audio recording, a CCTV video recording or a passport photo.

This assessment does not mean that fingermarks, face traces and voice traces cannot be used or unsuitable for biometric individualization in forensic science. It just clearly lays down limits on the certainty that can be expected, depending on the quality of the trace and on the efficiency of the biometric individualization process. The lack of constancy in the face and the voice, as well as in the fingermark, highlights the existence of within-source variability besides the between-source variability, which should also be considered in the forensic individualization process.

Since the forensic individualization process cannot be seen as a deductive process based on qualitative identity and on the general principle of uniqueness, another approach must be considered to infer the identity of source.

6.3.3 Binary decision schemes applied to biometric individualization

The binary decision schemes of discrimination and classification are considered as relevant for forensic biometric individualization because of the consensus of the forensic community about the applicability of the principles of qualitative identity and uniqueness. These decision schemes correspond to the verification process (discrimination) and the identification process (classification) used in the commercial applications of biometrics, for which a binary but relative decision on the identity of source is expected (Doddington, 1985).

A. DISCRIMINATION

The discrimination task used as decision scheme for forensic individualization is the process of accepting or rejecting a source as having generated the trace. The decision of discrimination between the trace and the source depends on a threshold. Discrimination is interpreted as rejection and non-discrimination as acceptation. This concept of identity does not correspond to the definition of the forensic individualization; if the random match probability is not nil (corollary of the threshold), the conclusion "the source is identified" is inadequate and misleading (Champod and Meuwly, 2000).

B. Classification

The classification task used as a decision scheme for forensic individualization is the process of determining which is the trace's source in a closed set of sources. Classification cannot take place in a closed set of sources, because the assessment of the credibility of the exhaustiveness of the sources in the set is outside the duties of the forensic scientist. In addition, it seems unfair to disclose only the identity of the best candidate, without providing the evidence obtained for the others, which may not exclusively come from the closed set of sources tested. To overcome this shortcoming, the classification should take place in an open set of sources, but such a framework still implies a final discrimination decision based on a threshold and suffers from the same conceptual drawbacks as the discrimination task (Champod and Meuwly, 2000).

C. Paradox in the use of binary decision schemes for forensic purpose

No discrimination or classification method is perfect. A decision of discrimination can suffer from two types of error: the false rejection (type I error), when the true source of the trace is rejected, and the false acceptance (type II error), when a false source is accepted as the source of the trace. A decision of classification can only suffer from false acceptance or type II error.

In the field of commercial applications of biometry, the evaluation of discrimination or classification methods is based on costs calculated for one or both types of error, depending on the task. In forensic science, on the other hand, there is a paradox in the belief that decisions could and should be simultaneously binary and error-free (absolute).

The inadequacy of the binary decision schemes for inferring identity and the paradox related to their use are good arguments for another approach to the inference of identity of source in forensic science. When the concept of source refers to a class of entities from which an object could originate, the question how the source is identified is merely an epistemological question of how qualitative identity comes to be known, i.e., through a set of characteristics, as explained above. When the concept of source signifies a particular individual entity from which an object originates, the question how the source is identified is a much more complex problem.

The general rule to demonstrate numerical identity is by establishing continuity. But this answer is impracticable for the forensic scientist, who almost never knows a priori the actual source nor has seen the source. Since there is no one to ensure unbroken continuity between the source and the object of interest since the creation of this object, there is no way of knowing the numerical identity of source (Kwan, 1997). In essence, the identity of source remains inferred in forensic science.

6.3.4 The hypothetical-deductive method

A. Principles

Proof is not subordinate to the concept of deduction. The hypothetical-deductive method is a much more practicable approach for inferring identity of source than the one consisting of the comparison of qualitative identity followed by a discrimination or a classification. It can be described as a process of hypothesizing and testing; a set of hypotheses is formulated which is tested and modified in a cyclic fashion until a modified hypothesis is arrived at which is not rejected.

"In using the hypothetical-deductive method, one commences by posing several hypotheses that could explain a phenomenon which has just been observed. Hypotheses are generally posed after taking into account what is generally known about the properties of the class of phenomena of interest – prior knowledge. One then proceeds to determine which one hypothesis from the set of all plausible hypotheses best explains the phenomenon.

Deductions are made from the posed hypotheses, and these serve as bases for proposing experiments. That is, if one can make predictions from these hypotheses, one can devise experiments to test them. This is the most valuable congruent of the hypothetical-deductive method. If a hypothesis either does not agree with the body of prior knowledge or if its predictions are falsified by experimentation, it is rejected. This is done successively until a single hypothesis remains that explains the phenomenon which no alternative hypothesis does" (Kwan, 1977).

The hypothetical-deductive method was already considered a relevant reasoning process by US writer Edgar Allan Poe, when he described the adventures of the detective Dupin, in his *Tales Stories*. As pointed out by

Locard (1924), Poe required the ideal detective to combine the imagination of the poet (to define the hypotheses) with the method of the mathematician (to test these hypotheses). Even Sherlock Holmes repeats "that when all other contingencies fail, whatever remains, however improbable, must be the truth" (Conan Doyle, 1953).

Although the analytical process described above is first of all an exercise of logic which is not directly related to reality, the hypothetical-deductive method requires an empirical validation of the resulting hypotheses (Truzzi, 1983).

Generating hypotheses is a necessary but insufficient condition for the reasoning coming from them. Since a hypothesis is intrinsically indemonstrable, it is necessary to distinguish the plausible alternative hypotheses from the fanciful ones. It is now acknowledged that it is impossible to derive criteria to define *ex nihilo* the notion of plausible hypothesis, because these criteria depend dramatically on the problem analysed (Marquis, 1999).

For the questions related to the inference of identity of source of a trace, it is possible to define two mutually exclusive alternative hypotheses: the prosecution hypothesis (H_p) and the defence hypothesis (H_d). A hypothesis can be considered as plausible when it is accepted as a possible explanation by the fact-finder.

B. Methods of statistical inference

Methods of statistical inference supplement the hypothetical-deductive method by assigning weight to predictions of hypotheses facilitating the selection of the hypothesis that best explains the source of the trace. But statistics will not lead to an objective process of absolute identification (Meuwly, 2001).

One important assumption to remember is that every quantitative method chosen for the inference of identity of source is based upon the premise of qualitative identity. It means that the features used to characterize an object must be selected on the criteria of distinguishability, ratio between the within-source and the between-source variability, stability in time, standardization and independence (Kwan, 1977).

Among the methods of statistical inference, the likelihood ratio approach premised on the Bayes Theorem is currently considered as the most logical framework for the inference of identity of source in forensic science. It has been used as early as the beginning of the twentieth century in the Dreyfus case (Taroni, Champod and Margot, 1998). Publications of the past fifteen years illustrate this trend for the interpretation of many kinds of forensic evidence (e.g. fingermark, DNA, speaker recognition or earmark) (Champod and Meuwly, 2000; Evett, 1998; Champod and Margot, 1995; Meuwly, 2001; Champod and Evett, 2001).

6.3.5 The likelihood ratio approach premised on Bayes Theorem

A. Definition of the hypotheses

The background information (I) on the case and the preliminary observation of the trace are the necessary information to define the set of all the plausible sources of the trace, named the potential population. The background information also determines which particular source of the potential population can be focused on and selected as the putative source of the trace.

The prosecution hypothesis H_p is the one according to which the putative source is truly the source of the trace. The defence hypothesis H_d is the one according to which an alternative plausible source is truly the source of the trace. A logical constraint necessitates that the two hypotheses are mutually exclusive, but not necessarily exhaustive.

B. Test of the hypotheses

The likelihood ratio approach shows how an a priori probability ratio of the two competitive hypotheses H_p and H_d can evolve to an a posteriori probability ratio, considering the background information and the result of comparison of the putative source with the trace, named the evidence (E). The likelihood of the evidence is evaluated when the hypothesis H_p is true on the one hand, and when the hypothesis H_d is true on the other hand. The ratio between these two likelihood values, the likelihood ratio (LR), is defined as the numerical value that allows for revision of the a priori probability ratio (prior odds), based on the new information E, to give the a posteriori probability ratio (posterior odds) of the two hypotheses H_p and H_d:

$$\frac{p(H_p|E,I)}{p(H_d|E,I)} = \frac{p(E|H_p,I)}{p(E|H_d,I)} \quad x \quad \frac{p(H_p,I)}{p(H_d,I)}$$

a posteriori				*a priori*
probability ratio	=	likelihood ratio	x	probability ratio
posterior odds				prior odds

■ 6.4 Toolkit for biometric individualization in forensic science

This section presents a concrete toolkit based on the hypothetical-deductive method for forensic individualization from biometric data. Summarized in the scheme presented in Table 6-1, it includes the definition of the alternative hypotheses, the selection of the sources and databases, the analysis and comparison of the biometric properties, and the interpretation of the evidence using the likelihood ratio approach.

6.4.1 Definition of the hypotheses and selection of the sources

The trace (X) considered for forensic biometric individualization can be a fingermark, a photo or a video recording of a face or a speech audio recording. The set of all the plausible sources of the trace is designed on the basis of the background information (I) and on the preliminary observation of this trace. The background information also determines which of the plausible sources can be focused on and selected as the putative source (Y).

The prosecution hypothesis is the hypothesis according to which the putative source (Y) is the source of the trace (X). For the clarity of the scheme, the subset of all the other plausible sources is considered as one generic alternative source. The defence hypothesis H_d is the hypothesis according to which an alternative source is the source of the trace (X). In reality however, background information on other plausible sources can vary, and if so, a distinct defence hypothesis should be considered for each plausible source.

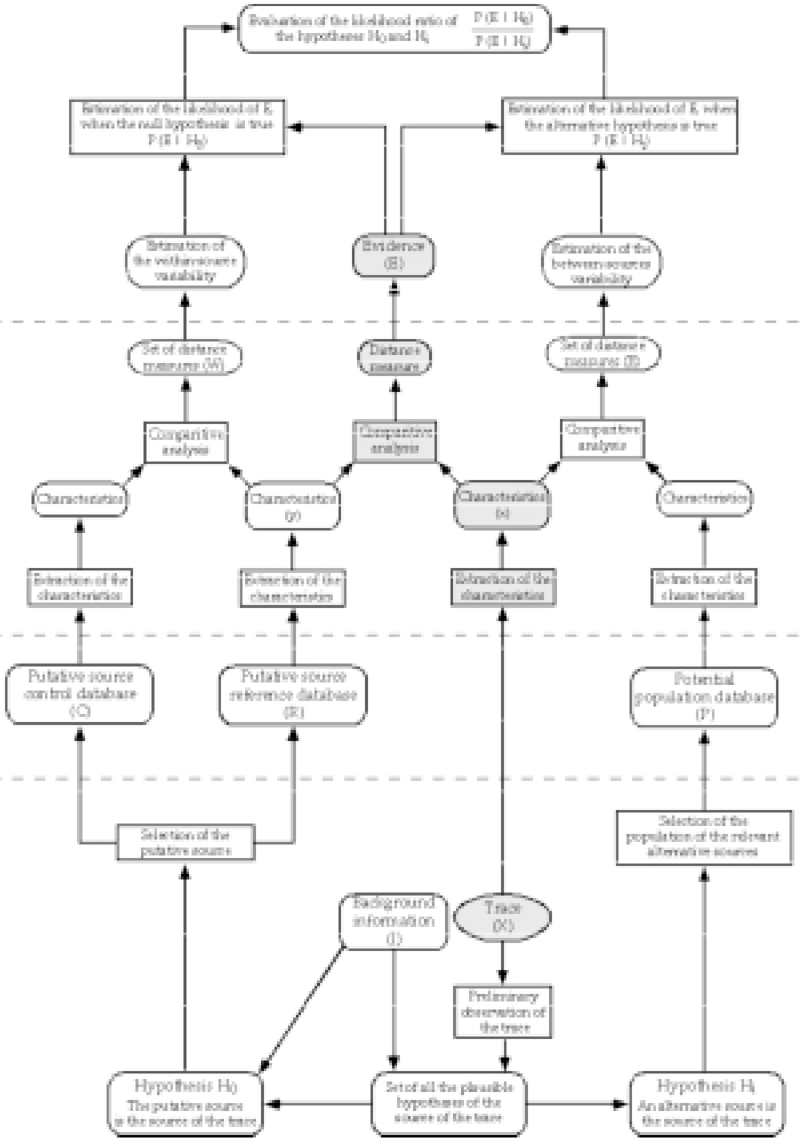

Evaluation of the likelihood ratio of the hypotheses H_0 and H_1 $\frac{P(E \mid H_0)}{P(E \mid H_1)}$
Estimation of the likelihood of E when the null hypothesis is true P (E | H_0)
Estimation of the likelihood of E when the alternative hypothesis is true P (E | H_1)
Estimation of the within-source variability
Evidence (E)
Estimation of the between-sources variability
Set of distance measures (W)
Distance measure
Set of distance measures (B)
Comparitive analysis
Comparative analysis
Comparative analysis
Characteristics
Characteristics (y)
Characteristics (x)
Characteristics
Extraction of the characteristics
Extraction of the characteristics
Extraction of the characteristics
Extraction of the characteristics
Putative source control database (C)
Putative source reference database (R)
Potential population database (P)
Selection of the putative source
Selection of the population of the relevant alternative sources
Background information (I)
Trace (X)
Preliminary observation of the trace
Hypothesis H_0 The putative source is the source of the trace
Set of all the plausible hypotheses of the source of the trace
Hypothesis H_1 An alternative source is the source of the trace

Table 6-1 Scheme of the computer-based system proposed for biometric individualization

6.4.2 Selection of the databases

When applied to forensic individualization from biometric data, the likelihood ratio approach needs biometric data to estimate the within-source variability of the putative source and the between-source variability of the trace. The data has been structured in three databases: the potential population database (P), the putative source reference database (R) and the putative source control database (C). The content and use of each of these databases is detailed below.

6.4.3 Analysis and comparison

A. Extraction of the characteristics

The importance of selecting characteristics judiciously cannot be overemphasized. If the characteristics are poorly chosen, no amount of mathematics can salvage an individualization scheme (Bremermann, 1971). For the fingerprint, the information is known and structured in three levels of characteristics: the first level is the pattern type of the fingerprint (arch, loop and whorl), the minutiae, or Galton points (ridge ending, bifurcation and dot) form the second level and the pores and ridge edges constitute the third one. The current AFIS systems use mainly the position and angle of the minutiae as well as the skeleton for the analysis, but the use of other characteristics such as the probability for minutiae configuration on the surface of the finger would contribute to developing a probabilistic assessment of fingermarks based on statistics (Champod and Margot, 1995).

For face and voice, the knowledge of the existence of idiosyncratic characteristics is hampered by the difficulty to provide a symbolic description for this information. In such cases, the individualization process is supported by the recognition of the information containing source-dependent characteristics, the information itself remaining impossible to define (Thévenaz, 1993).

B. Estimation of the value of the evidence

The evidence is the result of the comparative analysis of the characteristics (x) extracted from the trace X, with the characteristics (y) extracted from the putative source Y. In a computer-based approach of individualization from biometric data, the result of the comparison of x and y leads to a one-dimensional or multi-dimensional numerical value which estimates the "distance" or the "proximity index" between them; this information represents the evidence E.

6.4.4 Interpretation of the evidence using the likelihood ratio approach

A. Estimation of the between-sources variability and calculation of the denominator of the LR

The potential population database (P) is a large-scale database used to estimate the variability of the sources from the potential population. Ideally, P is made up of information that contains the exhaustive characteristics of interest of the alternative sources from the potential population. For individualization from biometric data, this database can be made up of rolled inked fingerprint pictures, 2D or 3D pictures of the face or spontaneous speech audio recordings of the alternative sources from the potential population.

The characteristics concerning the relevant alternative sources are extracted and compared to the characteristics of the trace. The result of this comparative analysis is a set of distance measures (B) used to estimate the between-source variability given the trace. This amounts to estimating the distribution of the distance measures that can be obtained when the trace is compared to the alternative sources of the potential population database. The between-source variability matches the relative frequency of the evidence in the potential population, in the limit of the P database in which it is observed approaching that of the full population. The calculated between-source variability is then used to estimate the denominator of the likelihood ratio $P (E \mid H_d)$.

B. Estimation of the within-source variability and calculation of the numerator of the LR

The putative source reference database (R) is made up of information that ideally contains the exhaustive characteristics of interest of the putative source. For individualization from biometric data, this database can be made up of rolled inked fingerprints pictures, 2D or 3D pictures of the face or spontaneous speech audio recordings. The characteristics (y) extracted from the putative source Y serves to calculate the evidence (E) when they are compared to the characteristics of the trace (x).

The putative source control database (C) is made up of information that is ideally of the same quality as the trace, but originated from the putative source. For individualization from biometric data, it can be fingermarks of the putative source detected on the same surface as the trace, pictures of the face of the putative source taken in similar conditions as the trace or speech audio utterances of the putative source recorded in similar conditions as the trace. These pseudo-marks are used to evaluate the within-source variability of the putative source when the characteristics of the samples of the C database are compared to the characteristics of the putative source.

The result of this comparative analysis is a set of distance measures (W) used to estimate the within-source variability of the putative source. It involves estimating the distribution of the distance measures that can be obtained when the putative source and a pseudo-trace of the same origin are compared. This distribution matches the within-source variability of the putative source, in the limit of the C and R databases in which it is observed, approaching the real variability of the putative source. This calculated within-source variability is then used to estimate the numerator of the likelihood ratio $P (E | H_p)$.

C. Evaluation of the strength of the evidence

The evaluation of the likelihood ratio of the two hypotheses results from the calculation of $P (E | H_p) / P (E | H_d)$. The strength of evidence can be expressed by numerical values, but it can also be expressed by linguistic qualifiers, which report the amount of support of the evidence E for the hypothesis H_p against the hypothesis H_d, following a qualitative scale of verbal equivalents corresponding to values of likelihood ratios (Evett, 1998).

■ 6.5 Conclusion

This chapter shows that the concept of identity in forensic science is related to the concept of identity of source. Establishing the identity of source refers to an individualization process, which consists of determining if a particular individual entity is the source of a trace. As the continuity of existence of a source and a trace cannot be proved in forensic science, the identity of source is relative and can only be inferred.

The assumption of uniqueness, which is often considered as a fundamental principle in forensic science, is not satisfied in the traces, and some of the sources considered for forensic biometric individualization. This assessment does not mean that fingermarks, face traces and voice traces are not suitable or usable for forensic biometric individualization, but it clearly lays down limits.

The logical consequence is that the individualization process used for the forensic biometric individualization cannot be seen simply as a comparative analysis of the characteristics of a source and a trace followed by a decision of discrimination or classification. The process should instead be arranged in accordance with the hypothetical-deductive method, whose main features the account it takes of prior knowledge, its requirement to consider all possible hypotheses to explain the source of a trace and its power to test them. The scheme proposed to design a computer-based system for forensic biometric individualization gives a possible framework to apply the hypothetical-deductive method.

This chapter also emphasizes that the extensive use of automatic fingerprint identification systems (AFIS) has shown that so far the inked fingerprint has stood the test of empirical falsifiability. In this field, the principle of uniqueness has reached a sufficient degree of corroboration (verisimilitude) to consider the inked fingerprint as a relevant biometric characteristic that could appear on new identity documents.

References

Bolt, R.H., et al.
1970 "Speaker identification by speech spectrograms: A scientists' view of its reliability for legal purposes", *Journal of the Acoustical Society of America,* 47(2):597-612.

Boves, L.
1998 "Commercial applications of speaker verification: overview and critical successfuctors", in RLA2C Workshop: Speaker Recognition and its Commercial and Forensic Applications, Avignon.

Bremermann, H.J.
1971 "What Mathematics Can and Cannot Do for Pattern Recognition", in Pattern Recognition in Biological and Technical Systems, O'Grusser, Ed., Springer-Verlag, New York.

Champod, C. and I. Evett
2001 "Earmarks as Evidence: A Critical Review", *Journal of Forensic Sciences,* 46(6):1275-1284.

Champod, C. and P.A. Margot
1995 "Computer Assisted Analysis of Minutiae Occurences on Fingerprints", in *International Symposium on Fingerprint Detection and Identification*, J. Almog and E. Springer, Editors, Israel National Police, Ne'urim, Israel, 305-318.

Champod, C. and D. Meuwly
2000 "The inference of identity in forensic speaker recognition", *Speech Communication*, 31(2-3):193-203.

Clifford, B.R.
1980 "Voice identification by human listeners: on earwitness reliability", *Law and human behaviour*, 4(4):373 - 394.

Conan Doyle, A.
1953 "The Sign of Four", in *The Complete Sherlock Holmes*, Doubleday & Company, New York.

Doddington, G.R.
1985 "Speaker recognition - Identify people by their voices", Proc. IEEE, 73(11):1651.

Eco, U.
1983 *The name of the rose*. 1st ed. 1983, Harcourt Brace Jovanovich, San Diego.

Evett, I.,
1996 "Expert Evidence and Forensic Misconceptions of the Nature of Exact Science", *Science and Justice*, 36(2):118-122.
1998 "Toward a uniform framework for reporting opinions in forensic science casework", *Science & Justice*, 38(3):198-202.

Grieve, D.,
2000 "Built By Many Hands", *Fingerprint World*, 26(100):51-60.

Grieve, M.C. and J. Dunlop
1992 "A Practical aspect of the Bayesian Interpretation of Fibre Evidence", *Journal of Forensic Sciences,* 32:169-175.

Kirk, P.L.
1963 "The Ontogeny of Criminalistics", *The Journal of Criminal Law, Criminology and Police Science,* 54:235-238.

Kwan, Q.Y.
1977 *Inference of Identity of Source,* in Department of Forensic Science, University of California, Berkeley.

Locard, E.
1909 *L'identification des récidivistes*, A. Maloine, Paris.
1924 *Policiers de roman et policiers de laboratoire*, Payot, Paris.

Marquis, P.
1999 "Sur les Preuves non Déductives en Intelligence Artificielle", in :(Ed.), in *Le Concept de Preuve à la Lumière de l'Intelligence Artificielle*, S. J and J. Szczeciniarz, Eds., Presses Universitaires de France, Paris.

Meuwly, D.
2001 "Reconnaissance de Locuteurs en Sciences Forensiques: l'Apport d'une Approche Automatique", in Institut de Police Scientifique et Criminologie, Université de Lausanne, Lausanne.

Nolan, F.
1991 "Forensic Phonetics", *Journal of Linguistics,* 27: 483-493.

Stacey, R.
2004 "A report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case," *Journal of Forensic Identification*, 54(6):706–718.

Stoney, D.A.
1991 "What Made Us ever Think We Could Individualize Using Statistics", *Journal of The Forensic Science Society,* 31(2):197-199.

Taroni, F.,
1997 "La recherche et la gestion des liens dans l'investigation criminelle: une étape vers l'exploitation systématique des données de police", in Institut de Police Scientifique et de Criminologie, Université de Lausanne, Lausanne.

Taroni, F., C. Champod, and P. Margot
1998 "Forerunners of Bayesianism in early forensic science", *Jurimetrics Journal*, 38:183-200.

Thévenaz, P.
1993 "Résidu de prédiction linéaire et reconnaissance de locuteurs indépendante du texte", University of Neuchâtel, Switzerland.

Thornton, J.I.
1997 "The DNA Statistical Paradigm vs. Everything Else", *Journal of Forensic Sciences*, 42(4): 758-759.

Truzzi, M.,
1983 "Sherlock Holmes", in *The sign of three*, U. Eco and T.A. Sebeok, Eds., Indiana University Press, Bloomington.

Tuthill, H.,
1994 *Individualization: Principles and Procedures in Criminalistics*, Lightning Powder Co, Salem.

CHAPTER 7

THE USE OF BIOMETRIC WITH TRAVEL DOCUMENTS

7.1 Introduction

The term “biometrics” refers to the automatic identification, or identity verification, of living individuals using physiological and behavioural characteristics (Wayman, 2001; Miller, 1995). Biometric authentication is the “automatic”, “real-time”, “non-forensic” subset of the broader field of human identification. Technological examples include iris, face, fingerprint, voice and hand geometry recognition. Sensor images from fingerprint, face, hand and iris systems are shown in figure 7-1.

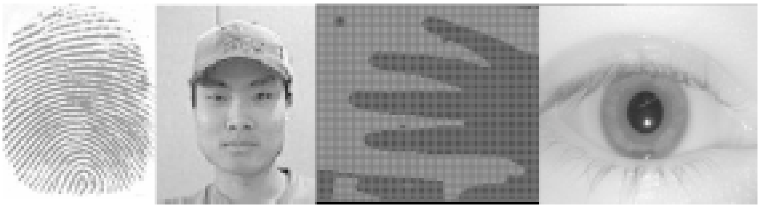


Figure 7-1: Fingerprint, face, hand and iris system sensor images.
(Courtesy of Jim Wayman, San José, United States of America)

Although facial photographs and fingerprints have been used in travel documents for nearly a century, the primary intent has been to allow traveller recognition by human inspection. The concept of using biometrics in “point of service” applications for identity verification dates to the early 1960s (Trauring, 1961). During the last decade, the government documents community has begun to apply this concept to the automatic, machine recognition of travellers. Following the 11 September 2001 terrorist attacks in the US, additional legislative and media attention has focused on the potential for applying biometrics in immigration and airport applications (US Public Law, 2002).

One of the first applications of biometrics in immigration documents was the 1992 experiment with the fingerprint-based "Schiphol Travel Pass" system at the Amsterdam airport. Although the original Schiphol system is no longer in operation, it later served as the model for the hand geometry-based US Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS), which has been operational between 1993 and 2002. Likewise it also served as a model, this time for the "Ben Gurion Express Entry" project in Israel (Troy, 2001). The hand geometry technology used in INSPASS has been shown to be technically highly effective (Wayman, 2000) in facilitating immigration procedures at US airports, but administrative reviews of the efficacy of the entire system have been mixed and government funding for the system has been undependable. Front and back faces of an INSPASS card are shown in Figure 7-2.

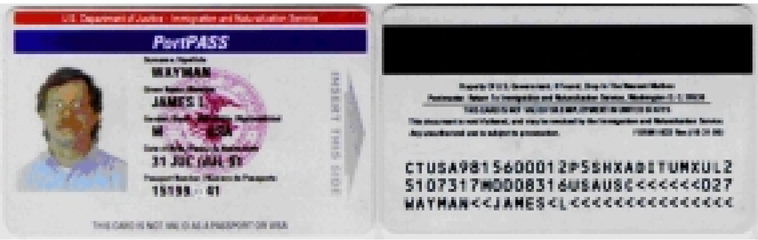

U.S. Department of Justice · Immigration and Naturalization Service
PortPASS
WAYMAN
JAMES L
M
31 JUL
15199 01
INSERT THIS SIDE
THIS CARD IS NOT VALID AS A PASSPORT OR VISA
CTUSA981560001 2PSSHXADITUMXUL2
5107317M0000831 6USAUS<<<<<<<<027
WAYMAN<<JAMES<L<<<<<<<<<<<<<<<<<

Figure 7-2: INSPASS Card.
(Courtesy of Jim Wayman, San José, United States of America)

The performance of all biometrics technologies, as measured in throughput rates and accuracy, depends heavily upon the human interactions with the devices. Although frequently demonstrating excellent performance in the laboratory, the behaviour of these technologies is much less predictable and more complicated in busy and hard-to-control environments, such as airports and border crossings. In addition to the Schiphol and INSPASS projects, pilots and tests of biometric immigration systems have also been conducted in the UK, Canada, Hong Kong and Malaysia, but data on performance of these systems has never been published in the biometrics literature. Consequently, the use of biometrics for automatic passenger processing is still a poorly understood.

This chapter intends to discuss the general properties of biometric systems as they are applied in travel documents, to explain how general biometrics systems work and how they are tested, to give recent test results, and to supply some details on the operation of the INSPASS system.

■ 7.2 The Functions of biometric identification devices

Biometric devices have two distinct functions:

1) to prove you are who you say you are, and
2) to prove you are not who you say you are not.

In the context of travel documents, the first function, called "positive identification", verifies if the presenter is the correct holder of the document and to prevent multiple users of the same document. The second function or "negative identification" verifies if an applicant is not already a document holder, and prevents the issuance of multiple documents to the same individual. Depending upon the system design, biometric systems can perform either or both of these functions.

7.2.1 Positive identification

In the first function, we use a biometric "sample" (say a fingerprint) to link the subject with a "template" pattern previously stored (or "enroled") in the system. The user of the biometric system makes a "positive" claim of identity, e.g. "I am James, as enroled in the system", which is verified by the automatic comparison of the submitted sample to the template for "James" already in the system. The template can be stored on the identity document or in a centralized location that is electronically accessible from the point of use of the document. If the sample and template biometric patterns resemble each other "closely enough", we can assume that the presenter is the same person who created the enrolment template.

The purpose of a positive identification system is to prevent the use of a single identity by multiple persons. If a positive identification system fails to find a match between an enrolment template and a submitted sample, a "rejection" results. A rejection also results if the biometric system cannot obtain a sample – a situation known as "failure to acquire". A match between sample and template results in an "acceptance". An impostor seeking to fool the system by inducing a "false acceptance" would be required to duplicate the biometric sample of an enroled user.

There are multiple alternatives to biometrics for positive identification. Throughout history, human inspectors have been successful in verifying identities against identification documents.

7.2.2 Negative identification

The second possible function of a biometric system, called "negative identification", establishes that a person is not someone or not among a group of people already known to the system. In this case, the user makes the claim (perhaps implicitly) that he is not already enroled in the system. His submitted biometric sample is compared to all enroled samples, which must consequently be stored in a centralized database. Usually the purpose of a negative identification system is to prevent the issuance of multiple identity documents to a single person. Proposed use of biometric systems to spot persons on "watch lists" also constitutes a "negative identification" application – all "users" making an implicit (and perhaps unknowing) claim not to be enroled on the "watch list".

Negative identification to prevent multiple enrolments of a single user constitutes the largest current use of biometrics and is used in driver's licensing, social benefit, and social security systems (particularly in the United States). If a negative identification system fails to find a match between the submitted sample and all the enroled templates, it results in an "acceptance". Generally, an acceptance would also occur if the system failed to acquire a readable measure. A subject who wishes to deceive the system by inducing a "false acceptance" would be required to cause the system to fail to find a match with a previously enroled template or "fail to acquire" a readable measure. A match between the sample and one of the templates consequently results in a "rejection".

A negative claim to identity can only be practically verified through biometrics. In any system exceeding a few hundred enroled persons, human inspectors wouldn't be capable of detecting multiple enrolments by the same individual or determining whether an individual is on a "watch list". Consequently, there are no alternatives and participation in the biometric system cannot remain on a voluntary basis.

Positive identification systems require submitted samples to be compared to the stored templates of only the person of claimed identity. Negative identification systems require some level of comparison of the submitted sample to the stored templates of every enroled person to prove non-membership in the database. Because the likelihood of a false match increases with the number of comparisons that must be made, only highly distinctive biometric patterns can be used for negative identification. Fingerprints and eye (iris and retinal) features are the only biometric patterns that have shown capabilities of negative identification against large databases.

7.2.3 Dual use systems

INSPASS is a system that only uses a positive identification. There is no provision made to prevent the issuance of multiple documents to a single traveller. The California driver's license system, on the other hand, was designed to use fingerprinting for negative identification only. The fingerprint template is not on the document, cannot be readily accessed from the database, and cannot be used to verify the authenticity of the license holder. Meanwhile, the social service identification card in the US state of Connecticut contains both "positive" and "negative" biometric components — negative identification performed at the time of enrolment to prevent the issuance of multiple identities to a single person, and positive identification at "point of service" applications to connect the presenter to the document.

Application of biometrics to travel documents could include both negative and positive identification, depending upon the goals of the system. Table 1 summarizes and contrasts the characteristics of positive and negative identification systems.

POSITIVE	NEGATIVE
To prove I am someone known to the system	To prove I am not someone known to the system
To prevent multiple users of a single identity document.	To prevent issuance of multiple identity documents to a single user.
Comparison of submitted sample to single claimed template	Comparison of submitted sample to all enroled templates
A "false match:" leads to "false acceptance"	A "false match" or a "failure to acquire" leads to a "false rejection".
A "false non-match" or a "failure to acquire" leads to a "false rejection".	A "false non-match" leads to a "false acceptance".
Alternative identification methods exist	No alternative methods exist
Can be voluntary	Must be mandatory for all
Can be fooled by submitting someone else's biometric measures.	Can be fooled by submitting no or altered measures.

Table 7-1: Identification: "Positive" and "Negative"

■ 7.3 The limitations of biometrics

We must be careful here, however, to understand the limitations of what we have just discussed:

1) "True" identity is not revealed in any biometric measure, but must be established through external documentation, which may or may not be reliable.
2) Not everyone can present a biometric pattern suitable for enrolment.
3) Some environments (and people) are not conducive to repeatable biometric measures.
4) Because only stable measures can be recognized, children and young people (those still growing) are not good candidates for reliable biometric identification using most technologies.
5) Matching errors do occur, either rejecting valid individuals or accepting impostors.
6) Biometric patterns are not secret, but are publicly observable.
7) Matching a biometric measure to a template on a document does not validate the document as authentic.
8) Biometric systems, like all computer-based technologies, require a significant investment in planning, installation, maintenance and operation, yet have a short vendor-support life span.

No biometric measure in itself contains the legal identity of the presenter. Establishing such an identity at the time of enrolment must be done with documentation outside of any biometric system. Such documentation might include birth or baptismal certificates, government identification documents, letters of introduction, employee identification cards, health insurance cards, and driver's licenses. In countries lacking national birth and death registration systems (such as the US), such documents may not be reliable. It follows that no biometric measure can determine the citizenship, age, or immigration status of a user. At enrolment, the system management can only be as confident in the presenter's true identity, age, citizenship and immigration status as there is faith in the external documentation. Biometric systems cannot establish the validity of external documentation. Rather, this is the role of enrolment personnel who must have been given special training in fraudulent document detection.

Not everyone can present good quality biometric measures. Every technology has a "failure to enrol" rate that is dependent upon the user population and the physical enrolment environment. Figure 7-3 (left) shows a fingerprint from a person of about 70 years of age, demonstrating a lack of contrast in the image, which is rather typical for this user population. On the right is the fingerprint of a child, not only small, but overly moist in places. These images can be compared to the fingerprint of a college student shown in Figure 7-1. Because of the variability of individuals, all biometric systems must have alternative procedures for accommodating those that cannot enrol.

But even when people have perfectly clear biometrics, a harsh imaging environment may prevent repeatable collection. For instance, collecting voice signals in noisy environments or face images against cluttered

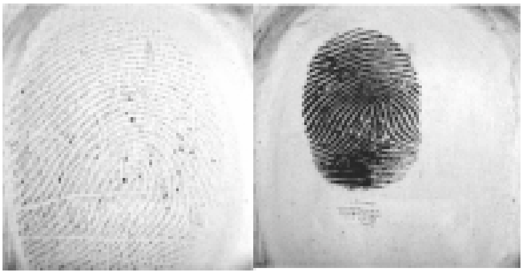


Figure 7-3: Fingerprint of senior citizen and child
(Courtesy of Jim Wayman, San José, United States of America)

backgrounds is a difficult challenge. Every technology has a "failure to acquire" rate that varies according to the population and application environment. Figure 7-4 shows a facial image acquired against a cluttered background, but such performance is not guaranteed under general conditions. Hence, all biometric systems require "exception handling" to allow alternative means for identity verification in the event that a dependable measure cannot be taken. The non-biometric "exception handling" mechanism, however, can become a target for security breeches.

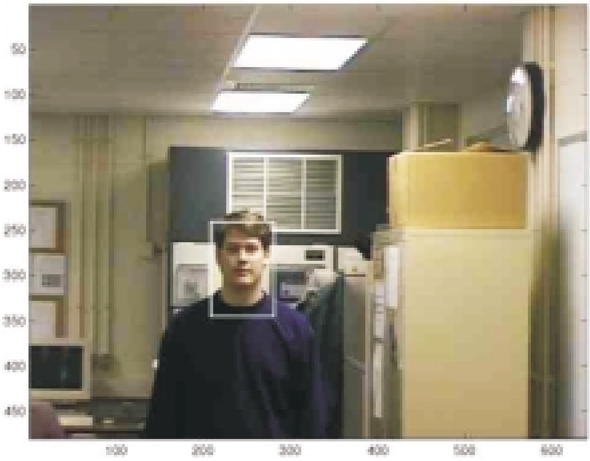


Figure 7-4: Face found among background clutter
(Courtesy of Jim Wayman, San José, United States of America)

Matching errors do occur with these systems. Matching samples to templates only establishes that the patterns are "close enough" to be assumed to be from the same person. Errors occur if the true document holder's biometric image has changed significantly since the time of enrolment or if an impostor has a biometric approximately similar to the enrolment template. Consequently, "false matches" and "false non-matches" are competing error rates which are controlled by some threshold set by system management to determine "what is close enough". When these error rates are combined with the failure-to-enrol and failure-to-acquire rates under some system policy, perhaps allowing multiple attempts at acquisition and matching, "false acceptance" and "false rejection" rates may be estimated for the system. These latter rates depend ultimately upon the system's decision policy and the strength of the technology within the chosen application environment with the specific user population.

Biometric patterns may be publicly observable, but stealing them normally requires more effort than mere observation. Methods for creating substitute fingerprints and facial images are well known (van der Putte, 2000; Blackburn et al., 2000; Matsumoto et al., 2002). Techniques for entering a stolen biometric pattern into a physically secure fingerprint system, however, would require some sort of prosthesis or physical model and are generally beyond the ability of the common traveller. Use of stolen measures can be prevented by adequate supervision of the biometric sensor (both at enrolment and at verification).

Even a correct match of a biometric sample to an enrolment template on a document does not validate the document. The document itself may be a forged one, holding the true biometric measure of the presenter. There are at least two ways of overcoming this problem to verify the authenticity of the information on the document: encryption and/or centralized storage.

Applying "public key cryptography", the template on the document can be encrypted using the "private key" of the issuing agency. Meanwhile, the only way to decrypt the template is with the "public key" assigned to that agency. If the presenter's biometric sample matches the template decrypted with the public key of the claimed issuing agency, the genuineness of the information can be verified. Consequently, the document can be tied convincingly to both the presenter and the issuer (see chapter 8 for more details on PKI).

A second approach, which is already used in the INSPASS system, is to centralize the template storage. The passport number, as read off the document, is transmitted with the collected sample to the central storage location. The sample is compared to the template identified by the passport number. Because the central database is secure, templates can only be entered through a trusted process. Consequently, a match between the sample and the template verifies both the identity of the presenter and the validity of the information on the document (in this case the document number).

Biometric systems require care in specification, purchase, and installation. Operator training and hardware/software maintenance are required throughout the system life cycle. User training and customized user interfaces may be required if user throughput rates are deemed important. If the systems link to a centralized database (as all negative identification systems must), network connectivity must be established and maintained. These requirements are time-consuming, expensive. Biometric systems are not "install and forget" technologies, and vendor support for installed products may be unavailable after just a few years. As such, the failure to adequately appreciate the difficulties inherent in these systems has lead to the discontinuance of many pilot projects.

■ 7.4 The technologies

There seems to be virtually no limit to the body parts, personal characteristics and imaging methods that have been suggested and used for biometric identification: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odours. Which characteristic is best? They depend on primary concerns which are at least five: the robustness, distinctiveness, accessibility, acceptability, and availability of the biometric pattern. Robustness means repeatable and not subject to large changes. Distinctiveness means the existence of wide differences in the pattern among the population. Accessibility means being easily presented to an imaging sensor. Acceptable means the perception as non-intrusive by the user. Availability is meant that some number of independent measures can be presented by each user.

Table 7-2 presents the technologies that have been demonstrated in publicly accessible negative and/or positive identification systems.

POSITIVE IDENTIFICATION	NEGATIVE IDENTIFICATION
Hand geometry	Fingerprinting
Finger geometry	Retinal scanning
Voice recognition	Iris recognition
Retinal scanning	
Facial imaging	
Fingerprinting	
Hand vein	
Dynamic signature patterns	
Computer keyboard usage	

Table 7-2: Technologies successfully tested for target application

■ 7.5 How the general biometric system works

Although these devices rely on widely different technologies, much can be said about them in general. Figure 7-5 shows a generic biometric authentication system, divided into five sub-systems: data collection, transmission, signal processing, decision and data storage. We will consider these subsystems one at a time.

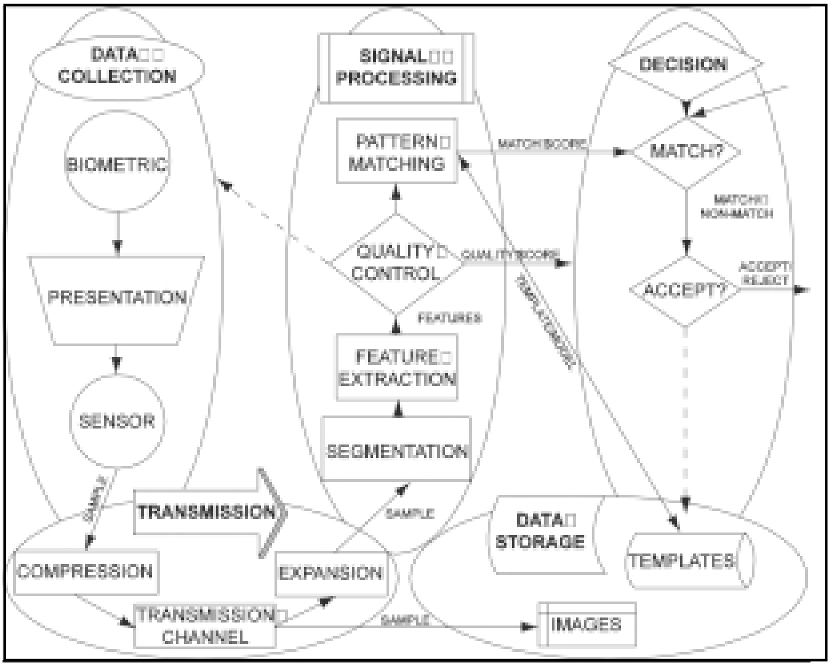


Figure 7-5: Generic biometric system diagram

7.5.1 Data collection

Biometric systems begin with the measurement of a behavioural/physiological characteristic. Key to all systems is the underlying assumption that the measured biometric characteristic is both distinctive between individuals and repeatable over time for the same individual. The problems in measuring and controlling these variations begin in the data collection subsystem.

The user's characteristic must be presented to a sensor. The presentation of the characteristic to the sensor introduces a behavioural component to every biometric method. The output of the sensor, which is the input data upon which the system is built, is the convolution of: 1) the biometric measure; 2) the way the measure is presented; and 3) the technical characteristics of the sensor. Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these factors. If biometric data is to be shared among systems (including future systems for the same application), the presentation and sensor characteristics must be standardized to ensure that biometric patterns collected with one system will match those collected on the same individual by another system. "De-facto" international standards exist for speech, fingerprint, and facial image data collection (ITU, 1996; CJIS, 2006; NIST, 2006, as well ISO standarts). In negative identification systems, the deceptive user must not be able to wilfully change the biometric or its presentation sufficiently to avoid being matched to previous records.

7.5.2 Transmission

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission. If a great amount of data is involved, compression may be required before transmission or storage to conserve bandwidth and storage space. Depending upon system architecture, the transmission subsystem might be placed between data storage and signal processing. In such cases, the transmitted or stored compressed data must be expanded before further use. The process of compression and expansion generally causes quality loss in the restored signal, with loss increasing with increasing compression ratio. The compression technique used will depend upon the biometric signal. "De-facto" international compression standards exist for voice, fingerprint, and facial data (Cox, 1997; CJIS, 1993; CCITT, 1993). Data format standards for fingerprint and facial information as well as data format specifications for general biometric data are given in the NIST website and are specified in the above ISO standarts.

7.5.3 Signal Processing

Having acquired and possibly transmitted a biometric characteristic, we must prepare it for matching with other like measures. The signal processing subsystem can be divided into three tasks: feature extraction, quality control, and pattern matching.

Feature extraction is fascinating. First, the biometric pattern must be found in the larger signal. For instance, in iris recognition, the iris region must be outlined and extracted from the image of the entire eye obtained from the sensor. Next, we must extract from the pattern those characteristics which are distinctive and repeatable, and discard those which are not or are redundant. Meanwhile, in a text-independent speaker recognition system, for instance, we may want to find the features, such as the frequency relationships in vowels, that depend only upon the speaker and not upon the words being spoken. And, we will want to focus on those features that remain unchanged even if the speaker has a cold or is not speaking directly into the microphone. Approaches to these difficult yet fascinating problems are always proprietary.

In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features. In some systems, transmission occurs after feature extraction to reduce the requirement for bandwidth.

After feature extraction, or maybe even before or during, we will want to check to see if the signal received from the data collection subsystem is of good quality. If the features "don't make sense" or are insufficient in some way, we can conclude quickly that the received signal was defective and must request a new sample from the data collection subsystem while the user is still at the sensor.

The development of this "quality control" process has greatly improved the performance of biometric systems in the last few short years. On the other hand, some people never seem to be able to present an acceptable signal to the system. If a negative decision by the quality control module cannot be overridden, then it results in a "failure to enrol" error. Increasing the quality level required for enrolment, and thus increasing the "failure-to-enrol" rate, can be an effective strategy to prevent the enrolment of users with poor biometric measures. Eliminating these users can lower operational error rates.

This feature "sample", now much reduced in size from the original signal, will be sent to the pattern matching process for comparison to one or more previously identified and stored templates. The purpose of the pattern matching process is to compare a presented feature sample to a stored template, and to send to the decision subsystem a quantitative measure of the comparison.

For simplification, we will assume closely matching patterns to have small "distances" between them. Distances will rarely, if ever, be zero as there will always be some biometric, presentation, sensor or transmission related difference between the sample and template from even the same person.

7.5.4 Decision

The decision subsystem implements system policy by directing the database search, determines "matches" or "non-matches" based on the distance measures received from the pattern matcher, and ultimately makes an "accept/reject" decision based on the system policy. Such a policy could be to declare a match for any distance lower than a fixed threshold and "accept" a user on the basis of this single match. It could also be to declare a match for any distance lower than a user-dependent, time-variant, or environmentally-linked threshold and require matches from multiple measures for an "accept" decision. It could be to give all users three tries to return a low distance measure and be "accepted" as matching a claimed template. In the absence of a claimed template, the system policy could also be to direct the search of all, or only a portion, of the database and return a single match or multiple "candidate" matches.

Management decides on the decision policy employed and it is specific to the operational and security requirements of the system. In general, lowering the number of false non-matches can be against raising the number of false matches while lowering the false rejection rate can be traded against raising the false rejection rate. The optimal system policy in this regard depends upon the statistical characteristics of the comparison distances coming from the pattern matcher and the relative penalties for false acceptances and false rejections within the system[1].

7.5.5 Storage

The remaining subsystem that must be considered is storage. One or more forms of storage could be used, depending upon the biometric system. The vendor-proprietary feature templates[2] are stored in a database for comparison by the pattern matcher to incoming feature samples. For positive identification systems, which require matching of a submitted sample only to those templates from the claimed individual, the database may be distributed on tokens carried by each enroled user (see Chapter 5, section 5.4.3 for more details about means of storage). Typical template sizes are shown in Table 7-3. Depending upon system policy, no central database need to exist, although in this application a centralized database can be used to detect counterfeit cards or to reissue lost cards without collecting again the biometric pattern.

Fingerprint	200 – 1000 bytes
Hand geometry	9 bytes
Finger geometry	14 bytes
Face	100 – 3,500 bytes
Voice	6,000 bytes
Iris	500 bytes

Table 7-3: Typical Template Sizes

Negative identification systems will require a centralized database for exhaustive search. As the number of enrolment templates in a negative identification system gets very large, system speed requirements dictate that the database be partitioned into smaller subsets such that any feature

[1] Also, an *a priori* estimate (best guess based on experience) of the probability that a user is a fraudster is required for setting the optimal thresholds. Consequently, setting the optimal threshold is always partially subjective.

[2] Because of the need for interoperability of "point of service" fingerprint systems used for card holder verification, the American Association of Motor Vehicle Administrators has created a fingerprint minutiae extraction standard, AAMVA DL/ID2000, Note C, available online at www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf

sample need only to match the templates stored in one partition. This strategy has the effect of increasing system speed and decreasing false matches but at the expense of increasing the false non-match rate owing to partitioning errors. This means that system error rates do not remain constant with increasing database size and identification systems do not linearly scale. Consequently, database-partitioning strategies represent a complex policy decision. Wayman gives methods for estimating error rates for large-scale negative identification systems (1999).

It is sometimes necessary for humans to examine the raw biometric images of system users, like in forensic applications or in adjudicating false matches for instance. Furthermore, if changes to the system or system vendor are to be made, re-extraction of vendor-specific templates from raw images may be required. Biometric images cannot be reconstructed from the stored templates, so some systems store centrally the raw, unprocessed data, although possibly in a compressed format.

■ 7.6 Testing and test results

Government-funded biometric testing has a history of at least two decades. During this period, many different and conflicting approaches to testing have been used. In an effort to establish a "nominal" approach, the UK Biometrics Working Group has established a "Best Practices for Testing and Reporting Biometric Device Performance" (UK Biometric Working Group, 2006). This is the de facto international standard.

The "Best Practices" document recognized three forms of testing: technology, scenario, and operational (Philips, et al., 2000). Technology testing focuses on the capability of signal processing subsystem to locate, extract, and match biometric images using a pre-collected database. Although a technology test can indicate software processing times, it cannot measure the throughput rate of humans through the system and, depending upon exact test design, may not be able to estimate failure to enrol/acquire rates.

Scenario testing takes a more extensive look at the biometrics system by using human subjects in a test environment created to mimic the target application. Scenario tests can measure throughput as well as error rates.

An operational test seeks to evaluate performance from data collected in the actual target environment. Because data collection conditions are hard to control, this form of testing is perhaps the most difficult. Reference documents the attempts to evaluate operational data from the INSPASS program (Wayman, 2000).

Most tests done on biometric devices are not publicly released. Many biometric devices are used as components of operational security systems, so system operators are reluctant to reveal performance data from operational tests. Furthermore, both technology and scenario testing are extremely expensive, owing to the need to track and manage a crew of human volunteers over repeated data collection visits. Government agencies paying for these tests generally will not reveal results to non-sponsoring agencies. Often non-disclosure agreements, required of test agencies by participating vendors, specifically prohibit dissemination of test results. One exception is the report of the biometric pilot performed by the Ministry of Interior and Kingdom Relations of the Netherlands in 2005 (also known as “2b or not 2b”). Unfortunately the report is available in Dutch only (Ministry of Interior and Kingdom Relations, 2005). Any way, there are very few biometric products that have undergone rigorous, developer/vendor-independent testing to establish robustness, distinctiveness, accessibility, acceptability and availability in “real-world” (non-laboratory) applications.

7.6.1 Application dependency of test results

All test results must be interpreted in the context of the test application and cannot be translated directly to other applications. Applications vary in several ways:

- the degree of supervision given to enrolment and use;
- the training and habituation of the users;
- the nature of the relationship between the system manager and the user (impacting user motivation and cooperation);
- the physical environment in which use takes place.

Most testing has been done in highly supervised applications with trained, habituated volunteers, under laboratory or office environment conditions. This is the application most suited to decision policies yielding low error rates and high user acceptability. Clearly, people who work daily with an attended system in an indoor environment with no data transmission requirements are the best able to give clear, repeatable biometric measures. Habituated volunteers, often "incentivized" employees (or students) of the testing agency, may be the most apt to see biometric systems as acceptable and non-intrusive. A recent survey about the public perception of biometrics demonstrated overwhelming support for biometric applications involving law enforcement, obtaining passports or identity documents and border crossing, while other applications ranked lowest on the list (Elliot et al., 2007).

However, performance of physical access device at an outdoor border crossing with occasional and distracted users, for instance, cannot be expected to be the same as in the laboratory. Performance in this application can only be predicted from measures on the same device in the same application. Therefore, it is impossible to predict performance of any biometric device in an immigration control setting by using laboratory data alone.

7.6.2 Fundamental test measures

"Best Practices of Testing and Reporting Biometric Device Performance" recognizes several fundamental test measures: failure to enrol and failure to acquire rates; false match and false non-match rates; and system throughput. For large-scale systems, particularly those using fingerprints, error and efficiency rates associated with database partitioning techniques are also measured and reported.

As already noted, the ultimate "false acceptance" and "false rejection" rates of the system will depend upon these fundamental measures and the system decision policies, such as operational thresholds and allowed number of attempts. Like the "false match" and "false non-match" rates, these error measures are also competitive. The system management might ultimately be interested in the absolute numbers of false rejections and false acceptances occurring in some period of time, say an hour or a day. Estimation of the number of such occurrences will depend not only upon their rates, but also on the number of genuine and impostor users presenting themselves during that time period and the number of comparisons engendered by each user presentation. Wayman suggests a rudimentary mathematical approach to estimating the number of errors from the basic test measures (1999, 2000).

7.6.3 Decision Error Trade-off Curves

The most useful method for displaying both the false match/false non-match and false acceptance/false rejection rates is by using the “Decision Error Trade-off” (DET) curve. These curves show graphically how the error rates stand against each other based on thresholds and decision

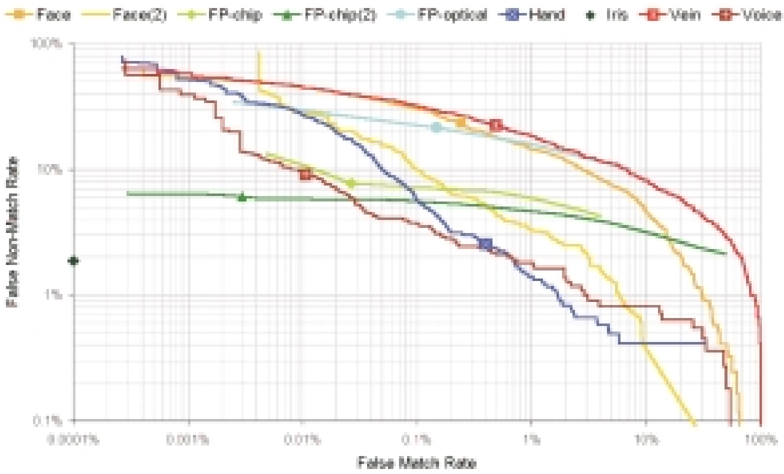


Figure 7-6: False Match/Non-Match DET Curves

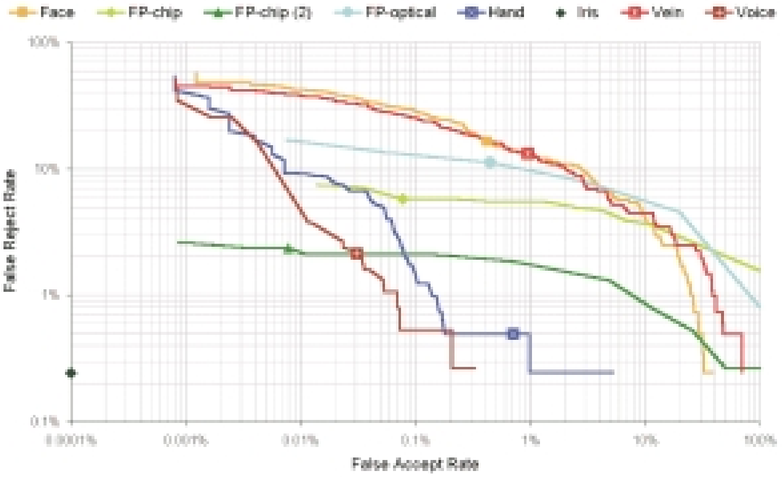


Figure 7-7: False Acceptance/ False Rejection DET Curves for “Three Tries” Policy

policies. A DET showing false match/false non-match trade-off for seven technologies tested in a carefully controlled office-type environment is given in Figure 7-6 (Mansfield, et al., 2001). The DET showing positive identification false acceptance/ false rejection rates for the same technologies, under a policy allowing three tries and considering failure to enrol/acquire rates, is given in Figure 7-7[3].

These results, although representative access control performance of these systems using volunteers in an office environment, would not be indicative of performance in most border crossing applications. We would predict that a more challenging environment would lead to higher error rates for all technologies.

■ 7.7 An example system: INSPASS

7.7.1 Background

US Federal law requires that US Citizenship and Immigration Services (USCIS) inspect every person entering the country. One of the programs developed by the former Immigration and Naturalization Services (INS) to automate the inspection process is the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS), which issued a hand-geometry-linked pass to “known travellers”. At “ports of entry” located in nine airports, travellers can present this pass to a fully automated kiosk instead of showing their passport to an immigration officer. The pass is linked to the presenter through a hand geometry measurement. US citizens and citizens from any of 26 countries participating in the “visa waver program” were eligible to participate.

INSPASS furthered the US government goal of improving customer service by decreasing the time that pre-enroled, low-risk travellers spend undergoing inspections. By removing these low-risk travellers from normal inspection lanes, available resources can be allocated to processing other travellers. Development of INSPASS costed INS over US$18 million (US DOJ, 2000).

[3] Figure 7 shows eight technologies because data collected with the solid-state fingerprint scanner was submitted “off-line” to an additional system.

7.7.2 Enrolment

Frequent travellers could enrol at INSPASS offices at six of the participating airports by presenting a valid passport and attesting in the application process that they have no criminal history. Fingerprints were taken electronically to facilitate a background check. The name and passport number were then sent to the Interagency Border Inspection System (IBIS) to ascertain that the traveller is not on a "lookout" list. The applicant was taught to use the hand geometry system and then submits three hand samples from which an average template is created. A photo identification card containing name, gender, nationality, date of birth and passport number, as shown in Figure 7-2, was created and given to the traveller at the time of enrolment. The entire enrolment process takes about 30 minutes. In 2000, there were approximately 60,000 users enroled in the system. The card was valid for one year, requiring repetition of the entire enrolment process for renewal. There is currently no charge for enroling or using INSPASS.

7.7.3 Use of the card

Once enroled, the traveller used the card upon their next arrival into the US. The following shows the number of travellers who were processed through INSPASS kiosks for the time period December 1999 to November 2000:

- New York (JFK) — 45,000 (seven kiosks)
- Los Angeles — 22,000 (five kiosks)
- Miami — 41,600 (three kiosks)
- Newark — 72,000 (two kiosks)
- Toronto — 48,600 (three kiosks)
- Vancouver — 32,000 (two kiosks)
- San Francisco — 14,000 (two kiosks)
- Dulles — 4,800 (four kiosks)
- Detroit — 1,300 (one kiosk)

All kiosks were within site of immigration inspectors, thereby deterring attempts to tamper with or spoof the system. No spoof attempts have ever been detected by INS inspectors. The system processed a valid traveler within an average of 30 seconds, as measured from the time the card is inserted into the card reader until the receipt has finished printing. Within this 30-second period, the system reads the card, received flight information (if required), validated the user's biometric sample against the enrolment template, updated the centrally stored template, and prints a receipt INSPASS transmitted a person crossing confirmation to IBIS at the completion of each successful validation. The traveller was able to exit through the gate within three seconds of accepting the receipt.

INSPASS holders were required to carry a passport while using the system, so in the event of a "rejection" by the system, INSPASS holders were instructed to go to the head of the nearest inspection line where they were subject to the same immigration procedures used for non-INSPASS holders. Additionally, random checks of INSPASS users against passports were performed by inspectors periodically.

7.7.4 Hardware

Figure 7-8 shows the INSPASS kiosk, which contains the following hardware:

- touch-screen monitor
- hand geometry unit with alternating current (AC) power adapter
- signal converter for hand geometry unit
- card reader
- gate with gate interface (site-specific)
- signal converter with AC power adapter
- receipt printer
- alert printer
- JetDirect print server
- workstation PC with keyboard and mouse
- uninterruptible power supply (UPS)
- adapter cards
- LAN Network Interface Card
- Ethernet four-port hub
- interface cables between all devices and components
- kiosk shell

The hardware for a typical airport set up, with four kiosks and an enrolment station, is estimated to cost about US$250,000 (Hornaday, 2001).

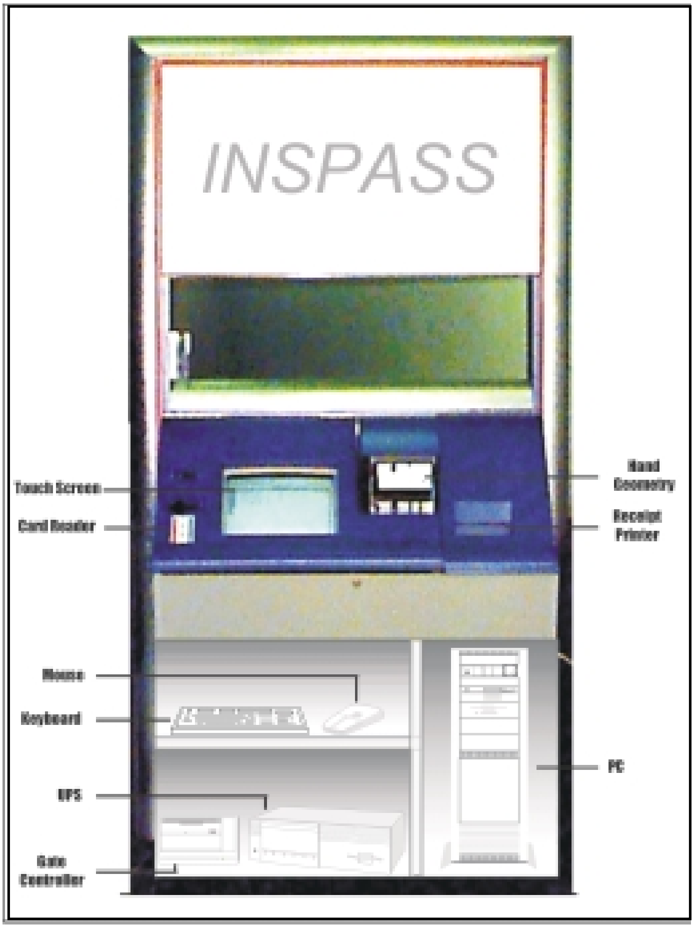


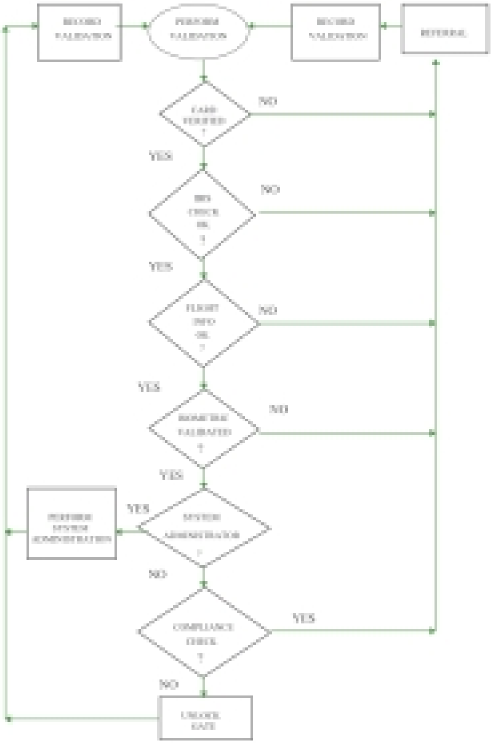
Figure 7-8: INSPASS Kiosk Hardware Overview
(Courtesy of Jim Wayman, San José, United States of America)

7.7.5 Software

The following software was used for INSPASS:

- MS Windows for Workgroups 3.11
- MS Access 2.0
- Novell NetWare Client 32 for Windows Version 1.22
- MicroTouch TouchWare Version 3.4
- Dynacom/Elite Version 3.52 DigiBoard Intelligent Board Driver for MS Windows 3.11 Version 1.4.3
- Imaging Automation EyeRead Version 1.93
- McAfee VShield (latest version)
- MS Open Database Drivers 2.0 (16-bit)

Figure 7-9 shows a software diagram of INSPASS.



A single INSPASS kiosk was capable of processing 15,000 users per month, retaining all data in a local database for an indefinite period of time. This allowed the production of historical reports. The following data were stored for all enroled users of the system: user identification (ID), last name, first name, date of birth, password, last date and time of update, and hand geometry templates. The system stored the following data for completed validation transactions: user ID, visa class, Country of Citizenship code, validation component identifier, card read attempts, card read failures, hand geometry reading attempts, hand geometry reading failures, hand geometry reading scores, pass/fail, fail reason, flight information source, start transaction time, end transaction time, IBIS time query, IBIS time response, IBIS time query history, IBIS time response history, and message number.

Because INSPASS was an automated data processing system that processes and stores sensitive-but-unclassified information about individuals, access to its database was regulated in the US by the Privacy Act of 1974 (US DOJ, 2006) and had to be safeguarded against disclosure and tampering. Administrative access to the kiosk databases was controlled through the card and hand geometry system on the kiosk, with system administrators issued a special card for this purpose.

References

Blackburn D., M. Bone, and P. J. Phillips
2001 "Facial Recognition Vendor Test 2000 Evaluation Report", www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.html, February 2001.

CCITT
1993 "Information Technology – Digital Compression and Coding of Continuous-tone still images: Requirements and guidelines", CCITT Recommendation T.81, ISO/IEC – 10918; www.w3.org/Graphics/JPEG/itu-t81.pdf

Criminal Justice Information Services
2006 CJIS-RS-0010 (V4), Appendix G Interim Iafis Image Quality Specifications For Scanners, www.engr.sjsu.edu/biometrics.

Cox, R.
1997 "Three New Speech Coders from the ITU Cover a Range of Applications," *IEEE Communications Magazine: Special issue on Standardization and Characterization of G.729*, 35(9): 40-47, September.

Elliot S. J., Massie S. A., Sutton M. J.
2007 "The perception of Biometric Technology: A Survey", *Proceedings of IEEE Workshop on Automatic Identification Advances Technologies,* Alghero.

Federal Bureau of Investigation
1993 "Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification", Criminal Justice Information Services, Federal Bureau of Investigation, IAFIS-IC-0110v2, 16 February.

Hornaday, B.W.
2001 "Automated ID devices are taking off at airports", Dallas-Fort Worth Star-Telegram, Northeast Edition, 20 June.

International Telecommunications Union
1988 Recommendations ITU-T G.711, "Pulse code modulation (PCM) of voice frequencies".
1996 G.712 "Transmission performance characteristics of pulse code modulation channels".

ISO
2005 ISO/IEC 19794-4:2005 Information technology — Biometric data interchange formats — Part 4: Finger image data.
ISO/IEC 19794-5:2005 Information technology — Biometric data interchange formats — Part 5: Face image data.

ISO/IEC 19794-5:2005/Amd 1:2007 Conditions for taking photographs for face image data.

ISO/IEC 19794-6:2005 Information technology — Biometric data interchange formats — Part 6: Iris image data.

ISO/IEC 19794-2:2005 Information technology — Biometric data interchange formats — Part 2: Finger minutiae data.

2006 ISO/IEC 19784-1:2006 Information technology — Biometric application programming interface — Part 1: BioAPI specification.

ISO/IEC 19794-1:2006 Information technology — Biometric data interchange formats — Part 1: Framework.

ISO/IEC 19794-3:2006 Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data.

ISO/IEC 19794-8:2006 Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data.

2007 ISO/IEC 19794-7:2007 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data.

ISO/IEC 19794-9:2007 Information technology — Biometric data interchange formats — Part 9: Vascular image data.

ISO/IEC 19794-10:2007 Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data.

Lucini, D.E.
2000 "Minutes of the May 10, 2000 INS User Fee Advisory Committee Meeting", Airports Council International – North America, http://216.205.117.217/new_website/depts/tech_envir_affairs/fi_services/MAY00_Meeting_Report_del.pdf, 26 May.

Mansfield, A., G. Kelly, D. Chandler, and J. Kane.
2001 "Biometric Product Testing Final Report", National Physical Laboratory, London, 19 March 2001, www.cesg.gov.uk/technology/biometrics

Matsumoto T., Matsumoto H, Yamada K., Hoshino S.,
2002 Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE Vol. 4677.

Miller, B.
1995 "Introduction to Identification Technologies", *PIN Industry Sourcebook*, Miller and Warfel.

Ministry of Interior and Kingdom Relations
2005 "Evaluatierapport Biometrieproef 2b or not 2b", The Hague, http://www.minbzk.nl/ onderwerpen/persoonsgegevens-en/ reisdocumenten/publicaties/54771/evaluatierapport.

National Institute of Standards and Technology (NIST)

2006 "Data Format for the Interchange of Fingerprint, Facial, Scar, Mark and Tattoo (SMT) Information," ANSI/NIST-ITL-1-2000, NIST Special Publication 500-245, www.itl.nist.gov/iad/894.03/fing/fing.html

2006 "CBEFF: Common Biometric Exchange File Format", NIST Technical Report 6529, www.itl.nist.gov/div895/isis/cbeff/CBEFF010301web.PDF, 3 January.

2006 "Best Practice Recommendations for Capturing Mugshots and Facial Images", Version 2, www.itl.nist.gov/iad/894.03/face/bpr_mug3.html

Philips, P. J., A. Martin, C. L. Wilson, and M. Przybocki

2000 "An Introduction to Evaluating Biometric Systems. *IEEE Computer*, 33(2):56-63, February 2000, www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.html

Trauring, M.

1961 "On the automatic comparison of finger ridge patterns for personal-identity verification", Hughes Research Laboratory Report #190, March 1961, reprints available from the Biometric Test Center, San Jose State University.

Troy, D.

2001 "Lessons Learned from Biometric Immigration Projects", *Biometrics 2001 Delegate Manual* from the Elsevier Advanced Technology Conference, London, 28-30 November.

United Kingdom Biometric Working Group

2006 "Best Practices in Testing and Reporting Biometric Device Performance", version 2.01, www.cesg.gov.uk/technology/biometrics

US Department of Justice

2001 "Management Challenges in the Department Of Justice ", US Department of Justice – Office of the Investigator General, http://www.usdoj.gov/oig/, 1 December. See also OIG Reports #00-07 (March, 2000) and #95-08 (March, 1995)

2006 5 U.S.C. § 552A, www.usdoj.gov/04foia/privstat.htm

US Public Law - Law Library of Congree

2002 "Enhanced Border Security and Visa Entry Reform Act of 2002" (United States Public Law.107-173), http://www.loc.gov/law/guide/uscode.html

Warren, J.

2001 "Entering a twilight zone at the INS", Chicago Tribune, 26 August.

Wayman, J.L.

1999 "Error Rate Equations for the General Biometric System", *IEEE Robotics and Automation*, 6(1):35-48, March. www.engr.sjsu.edu/biometrics/nbtccw.pdf

2000 "Evaluation INSPASS Hand Geometry Data", in *National Biometric Test Center Collected Works: 1997-2000*, San Jose State University, available on-line at www.engr.sjsu.edu/biometrics/nbtccw.pdf

2000 "Technical Testing and Evaluation of Biometric Identification Devices", *Biometrics: Personal Security in Networked Society*, A. Jain, et al (eds.), Kluwer Academic Press, London.

2001 "Fundamentals of biometric authentication technologies", *Int. Journal of Imaging and Graphics*, 1(1).

Van der Putte, T., and J. Keuning

2000 "Biometrical Fingerprint Recognition: Don't let your fingers get burned", proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers, 289-303, London.

CHAPTER 8

THE PROCESS OF DIGITAL IDENTIFICATION

■ 8.1 Introduction to digital identification

This chapter deals with the principles of digital identification. It first discusses identification in general, how it works, the aspects that relate to application and issuance, and the contracting procedure involved in digital identification documents. Over here, not only is technology important here, but also organizational and procedural measures such as security maintenance and the conducting of risk analysis. These applications and the creation of digital identities must always be weighed against the objectives and risks involved. One must always ask oneself two important questions: is it necessary and is it enough?

Digital identification is very important in environments where people work with or communicate by means of digital equipment for the simple reason that the digital devices need to know whom they are interacting with. A good example is the computer. When a computer is restricted to a single user, it must be able to know that the current user is authorized. Only if the registered user has a digital identity and is the sole user of this identity, can the computer confirm who is pressing the keys.

Digital identification is also required to authorize access to digitally stored data. The same goes for communication by digital means between humans, such as by internet or email, where the confirmation of a person’s identity is necessary. Do people really know who is on the other end of the communication link? Can one trust that the sender of an e-mail is also the author?

Persons, however, are not the only ones that need to be identified. The identification of systems is also important. This is because many tasks that are carried out by humans can also be done by systems automatically. Hence, a clear distinction must be made between persons and systems in the processes involved in the implementation of digital identification.

Digital identification also plays a vital role in secure digital processes such as applying for high-quality secure identity documents. These days, such documents are personalized by means of high-tech systems that are fed by digital personalization data. If these machines are unable to verify whether the data has been supplied by a legitimate person, the physical document would have no value whatsoever.

In order to understand how digital identification works in the above-mentioned cases, a number of principles and uses of physical documents need to be discussed first since they also apply to digital identity. Physical documents illustrate an identity document's reliability depends on the combination of document security, issuing policies, procedures and administration, security of the personalization process, and the logging and auditing of the entire process. The same principles also apply to digital identification.

8.1.1 Physical identification

A person can prove his identity in many different ways. How he does it depends on what is agreed on by the various parties. One way is by producing a physical identity document. This enables the verifying party to determine the identity of the holder and confirm whether or not he is the registered owner. This usually established by means of a photo. A document often has a limited validity which also appears on the document along with the name of the issuing authority. The verifying party must then ascertain whether the document is genuine or counterfeit. This is where security features play a significant role.

Identity documents are often used for a quick and reliable verification of someone's identity. However this only works if the parties involved have made an agreement on the level of reliability of the document and on matters relating to its issuance. This can be achieved by means of a bilateral or multilateral agreement, as in the case of travel documents. This agreement is usually based on the standard accepted by all parties. Without such an agreement, identity documents would have no value, regardless of their quality.

The parties using the documents rely on the aspects listed in Table 8-1, which are related to the issuance of identity documents. It provides a framework for the trust the verifying parties can place in a document. If one or more of these aspects is missing or incomplete, the document becomes unreliable.

Confidentiality aspects	**Description**
Issuing policies	Set of rules that determine document confidentiality, scope and features
Application procedures	Implements the issuing policies for application and guarantees the reliability of the applicant's identity
Security of personalization of the document	Guarantees reliability of the personalization data on the document
Archiving system for the status of the document	Enables verification of the validity of the document and whether or not the document has been revoked
Logging of application and personalization processes and of security issues surrounding documents	Enables audits, screening and investigation into the processes so that fraud may be eliminated
Security of the document	Guarantees authenticity and integrity of the document
Audits of the above	Confirms that the issuing policies have been properly carried out and consolidates the level of confidentiality. This results in feedback and recommendations for improvement.

Table 8-1: Confidentiality aspects in relation to digital identification

8.1.2 Digital identification

The need for a person to prove his identity often happens when the verifying parties do not know his true identity self. Only in situations where a person is recognized by her/his appearance or voice, is it unnecessary to identity verification by means of a document. However, the digital world lacks such an easily discernable method of identification. For instance, if one receives an ordinary e-mail, there is no way of telling who actually wrote and/or sent it. It could have been anyone.

In the digital world, the identification of persons and devices is usually achieved through a combination of identity data and a secret key. A person or device applies a secret key to prove that the identity data belongs to him. For instance, a user name could serve as identity data and a password as secret key. The principle behind this is that only the registered owner knows the secret key and only he can use it to validate his identity data. This digital verification process is referred to as authentication. As with physical documents, the context in which the key is used must be sufficiently secure so that there is no doubt the user is the registered key holder.

A distinction must be made between weak and strong authentications. In weak authentication, the user either supplies identity data manually or, when using a device, from a file. The most common form of this is the use of user names and passwords. In strong authentication, a secret key is stored on a secure token, e.g. a tamper-proof smart card. This secret key can only be used if the user enters a secret code. Strong identification is based on the principle that the user both owns (a token) and knows something (a password). It is also possible to make use of physical features (biometrics) producing the following combination: the user *has* something (token), *is* something (biometrics), possibly supplemented with *knowledge of* something (password).

This chapter only focuses on strong authentication, which presumes the use of a secure token for persons. The same technique can be used without a secure token, but this reduces the level of security.

In order to illustrate the difference between digital identification by means of strong authentication and physical identification, we will examine how money is withdrawn from an ATM and the safeguards involved. Although a bank card is not usually a smart card, the same process can be applied to a smart card. This process is illustrated in Figure 8-1.

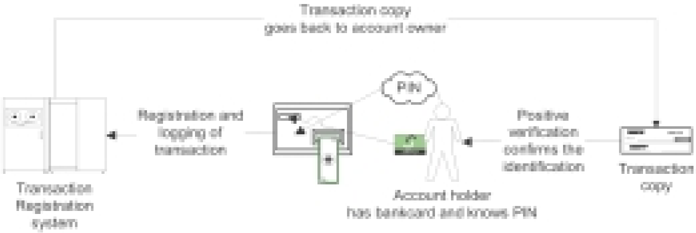


Figure 8-1: The account holder has a bank card and knows his PIN, enabling him to withdraw cash from a cash dispenser. The transaction is logged and a bank statement is sent to the account holder. If the account holder accepts the transaction, positive verification is confirmed.

The cash dispenser reads all identifying data from the bank card so that cash can be withdrawn from the corresponding bank account. However, at this point the cash dispenser does not know whether the registered owner has inserted the card or someone else. To determine this, the cash machine requests information which only the account holder knows, i.e. her/his Personal Identification Number (PIN). This PIN is the secret key that confirms the identity of the account holder. Once the correct PIN number has been entered, a positive verification is effected and the requested amount is ejected.

If the account holder keeps his PIN secret, it remains as a strong authentication mechanism. However, if the PIN is compromised, poorly stored or communicated to a third party, anyone with access to the card and PIN can bring to about a positive verification. That is why an extra verification must be built in. The cash dispenser administers the transaction and a bank statement is sent to the account holder. If the account holder discovers on his bank statement that another person has illegally withdrawn money from his account, the account holder can reclaim the amount, the card and PIN rendered invalid, and order a new card and corresponding PIN.

For the system to work, use of the bank card and PIN should be restricted to the account holder only. When someone applies for a bank card, the bank must establish that the applicant and account holder are indeed one and the same person. Also, the bank card and PIN should be sent to the account holder separately in order to ensure that they cannot be intercepted simultaneously. The PIN is secured in a sealed envelope so that it remains a secret and its integrity is verifiable, i.e. the envelope must not be opened upon receipt.

This brief description of how money is withdrawn from a cash dispenser using a bank card shows that digital identification has similarities in the use of physical identity documents. The transaction is not only about technical procedures, but the set of rules listed in Table 8-1 are also applicable here.

■ 8.2 How digital identification works

So far, we have looked at the context in which digital identification is applied, but nothing has been said about how digital identification actually works. The following section will give a brief overview of how digital identification works in general and the Public Key Infrastructure (PKI) in particular.

8.2.1 Digital identification in general

Digital identity is usually based on cryptographic technology. Someone has a secret code or secret key which is used to convert plain data into encrypted data. This is done in such a way that no one else can reproduce the original plain data from the encrypted data without the secret key. The encrypted text can only be generated by the owner of this secret key. Identity can be verified by checking if his data has been encrypted with the secret key that is linked to someone's identity.

8.2.2 Symmetric encryption

Symmetric encryption is when encryption and decryption are carried out by a single key, as can be seen in Figure 8-2.

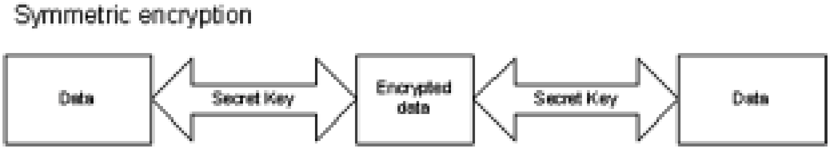


Figure 8-2: In symmetric encryption, a single, shared secret key is used for encrypting and decrypting data. Both the encrypting and decrypting parties can use the same key and perform the same actions.

Each party involved must have its own secret key and must only use this secret key for encrypting data for authentication. In order to apply symmetric encryption, each party must have a copy of the other parties' secret key. That means that with authentication, no one really knows whether the sender is actually the holder of the secret key (Rivest et al., 1978). Moreover, key management is quite complicated. The secret keys must be securely distributed to all the parties, and each party must closely guard their keys in order to safeguard the integrity of the system. All of the above makes symmetric encryption unsuitable for digital identification. Usually, this technique is only used for keeping data secret.

8.2.3 Asymmetric encryption

It is also possible to use two different, complementary keys: one for encryption and one for decryption. It is not possible to decrypt data with the same key that is used for encryption, which requires the complementary key. This technique is called asymmetric encryption (Rivest et al., 1978; Schneier, 1995).

One of the keys referred to is the public key. This key does not have to be kept secret, and may be made publicly available. The other key, however, is the secret key, which should only be disclosed to and used by the holder of the key. To keep information confidential, a person uses it to encrypt plain data by means of the crypto function P (see Figure 8-3.) Subsequently, the encrypted data can only be decrypted by means of the complementary crypto function S and the secret key. The owner of the secret key therefore is the only one who can decode the data. Because the public key is publicly available, anyone with access to the public key can use it to send secure data to the owner of the secret key.

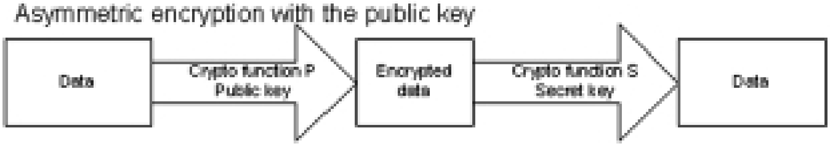


Figure 8-3: With asymmetric encryption, data that has been encrypted with the public key can only be decrypted with the secret key, which is only known to the holder of the secret key.

Asymmetric encryption has another quality that is interesting for identification. From a technical point of view, it is also possible to use the crypto function S together with the secret key to encrypt plain data. (See Figure 8-4.) The holder of the secret key is the only person who can perform this. In this way, anyone with access to the public key can decipher encrypted data back to the original, plain data by applying the accompanying public key using the cryptographic function P. Thus anyone who has access to the public key can decrypt data that has been encrypted with the secret key.

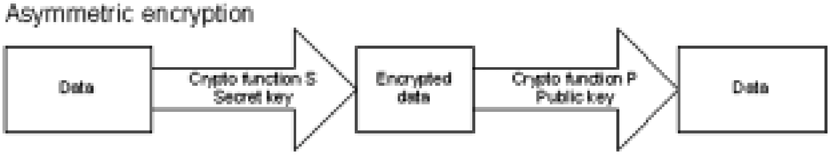


Figure 8-4: With asymmetric encryption, data that has been encrypted with the secret key (only known to the holder) can only be decrypted with the public key.

Now authentication is easy. Anyone wanting to authenticate himself is requested to encrypt with her/his secret key a piece of data known to the verifying party. The identity claimed can then be verified by decoding the encrypted data the public key that belongs to the identity of the person seeking authentication. If this is successful, the person is positively authenticated.

It is also possible to create a unique code of the message to be sent, which is an exact representation of this message. Also called the message digest, it is created in such a way that it is impossible to draft a meaningful message with the same digest other than the original message. If the data of the message is somehow altered, the message digest is completely changed. It is encrypted with a secret key so that the recipient can decrypt it and go through the digest of the received message for comparison. If they are the same, the recipient knows for certain who the sender is (for only he has access to the secret key) and that the message is intact. This technique is described in Figure 8-3, and is used to digitally sign documents to ensure document integrity (Schneier, 1995; ISO, 2001).

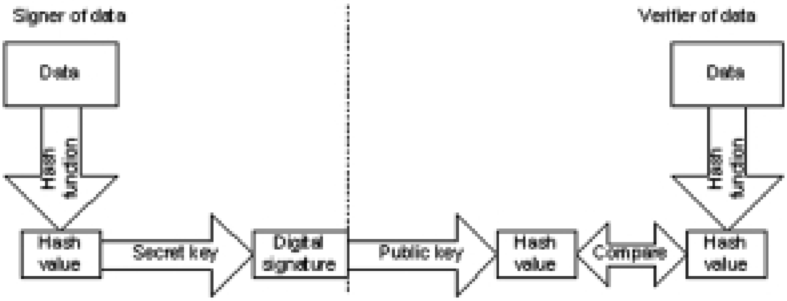


Figure 8-5: Process of generation of a digital signature.

As illustrated in Figure 8-5, a digital signature can be achieved in two steps. First, the data is ran through a hash function in order to generate a unique code for the data, whereby even the slightest change to the data – one bit is enough – may result in a totally different code. The hash function is decoded by means of the signing party's secret key. The signature is verified by decrypting the digital signature with the signing party's public key. This ensures that the signing party is the person he claims to be. The data is rehashed, and if this data is identical to the signed data, it gives the same result as the decrypted data.

If a sender encrypts a message or data with the recipient's public key, only the recipient, i.e. the holder of the secret key that corresponds with this key, can open the message. This technique is used to ensure confidentiality.

If the holder of a secret key has generated this key without outside assistance, this key is only known to the holder. If the holder of such a key digitally signs a document, message or transaction, it is virtually impossible for the holder to deny having done this. This gives a system that ensures complete and independent non-repudiation.

Various mathematical functions can also be applied to asymmetric encryption. The size of the key can also vary, whereby the general rule is that the longer the key the better the security, but also the longer the processing time. Hence, a longer key entails a longer wait. When selecting a mathematical function and accompanying key size, it is best to consult an expert. Mathematical functions might fall out of use due to the development of enhanced functions or if the technology is superseded. As far as key size is concerned, it should be long enough as not to be guessed or predicted. Usually, the strength of a key diminishes in time because the latest hardware facilitates the cracking of a key.

8.2.4 Public Key Infrastructure

There are still two questions that remain to be addressed: how can public keys be recognized as authentic and how do we know who is the holder of the private key?

The answer to both is a certificate or a digital identity document. This contains information about the holder, such as her/his name, date of birth or identity number. In addition, the holder's public key also contains information about validity, the level of confidentiality of the certificate and the name of the issuing organization. There are various formats for certificates; however, the most common standard for PKI is the X.509 certificate standard (ISO, 2001; Housely et al.; 2002).

These certificates form the core of the infrastructure that provides services on the basis of asymmetric encryption, also known as Public Key Infrastructure (PKI). The certificate is signed digitally by the issuing Certificate Authority (CA). PKI users know and trust the CA and the CA certificate. Other certificates issued by the CA can also be authenticated by means of the CA certificate.

According to European Union Passport Specification, “Each Member State must set up only a single *Country Signing CA* acting as the national trust point for all receiving states and at least one *Document Signer* issuing passports”. This document refers for details about the PKI infrastructure to an ICAO/NTWG technical report (ICAO, 2004), which as been recently integrated in ICAO Document 9303 (ICAO, 2006).

PKI architecture is based on asymmetric encryption technology, which does not single-handedly ensure blanket security. As in physical documents, the process for obtaining a document and the related management procedures also play a very important role security-wise. For instance, if the technology provides adequate security, but the procedure tolerates the use of a false identity, then obviously the system is not suitable for identity verification. The same holds true for the CA. If the CA is unable to guarantee that an individual is the sole holder of the secret CA key for signing certificates, then there is uncertainty as to whether a certificate was actually issued by the CA, seeing that someone else could have used a copy of the CA key.

In PKI, a Registration Authority (RA) handles the application and verification of the identity of an applicant, which is identical to the process for obtaining a physical identity document. The quality and management of the procedures determine the confidence we can place in the value of identification by means of a digital certificate. Because certificates can be revoked, the CA also has to keep and publish a list of all revoked certificates. This list may be consulted in one of the three following ways: by means of a Certificate Revocation List (CRL), an online protocol (OCSP) or an online protocol for the Internet standard XML (XKMS).

The issuing organization, the CA of a PKI, publishes a document which sets out the directives and measures regarding security. This document establishes the joint confidentiality value of the certificates within the PKI. This can be compared to the aspects listed in Table 8-1 regarding identity documents in the physical world. This document usually consists of two parts:

i. the Certificate Policy (CP), which is a “defined collection of directives that determine the applicability of a certificate within a certain community and/or class of applications with shared security requirements" (ISO, 2001), and

ii. the Certificate Practice Statement (CPS), which is an ' explanation of the measures and procedures that a certifying authority uses when issuing certificates' (American Bar Association, 1997).

These two parts are usually referred to as the CP and CPS of the CA. Internet RFC 2527 provides a framework for writers of CP and CPS documents. The CP and CPS are complementary and ensure an effective level of certificate security.

The total framework for a PKI can be seen in Figure 8-6, which shows which elements are important in a PKI. To set one up, it is best to begin with the CP/CPS. In order to do this, the general security policy must be available to ensure that the PKI provides an adequate level of security in relation to the environment in which it will be applied. For instance, in the application process for travel documents, the PKI has to guarantee that the personalization data is just as secure as the rest of the personalization process.

As demonstrated in the model, the CP/CPS imposes rules, obligations and procedures on the users. PKI auditors play an important role in the periodic checks of the PKI. They ensure that what happens in actual practice conforms with the CP/CPS, and draw up proposals for improvement.

The user's software must be suitable for a PKI. However, this does not automatically mean that the software is secure. If the process logic of the software is not secure, the PKI is unable to resolve this. The design and implementation of the PKI in the application must be subjected to close scrutiny and extensive testing.

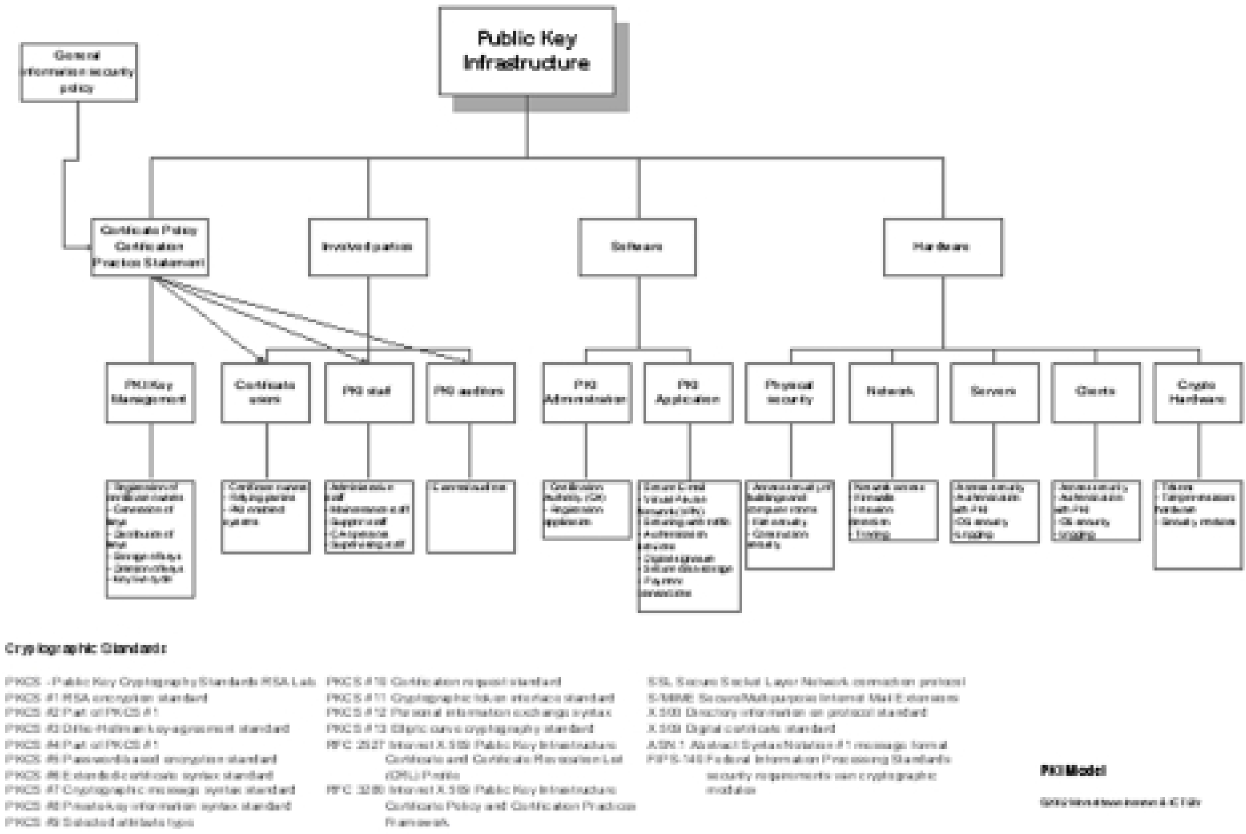

Public Key Infrastructure
General information security policy
Certificate Policy Certification Practice Statement
Involved parties
Software
Hardware
PKI Key Management
Certificate users
PKI staff
PKI auditors
PKI Administration
PKI Application
Physical security
Network
Servers
Clients
Crypto Hardware
- Registration of certificate owners - Generation of keys - Distribution of keys - Storage of keys - Deletion of keys - Key live cycle
- Certificate owners - Relying parties - All involved systems
Administrative staff - Maintenance staff - Support staff - CA operators - Registration staff
- Commissioner
- Certification Authority (CA) - Registration application
- Secure E-mail - Virtual Private Networks (VPN) - Extranet with traffic - Authentication in networks - Digital signature - Software distribution - Payment transactions
- Access security of building and computer rooms - Exit security - Observation security
Network access - Firewalls - Intrusion detection - Routing
- Access security - Authentication with PKI - OS security - Hardening
- Access security - Authentication with PKI - OS security - Hardening
- Tokens - Tamperproof hardware - Security modules
Cryptographic Standards:
PKCS - Public Key Cryptography Standards RSA Lab
PKCS #1 RSA encryption standard
PKCS #2 Part of PKCS #1
PKCS #3 Diffie-Hellman key-agreement standard
PKCS #4 Part of PKCS #1
PKCS #5 Password-based encryption standard
PKCS #6 Extended-certificate syntax standard
PKCS #7 Cryptographic message syntax standard
PKCS #8 Private-key information syntax standard
PKCS #9 Selected attribute types
PKCS #10 Certification request standard
PKCS #11 Cryptographic token interface standard
PKCS #12 Personal information exchange syntax
PKCS #13 Elliptic curve cryptography standard
RFC 2527 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
SSL Secure Socket Layer Network connection protocol
S/MIME Secure/Multipurpose Internet Mail Extensions
X.500 Directory information on protocol standard
X.509 Digital certificate standard
ASN.1 Abstract Syntax Notation #1 message format
FIPS 140 Federal Information Processing Standards security requirements can cryptographic modules
PKI Model

Figure 8-6: Framework of a PKI.

Figure 8-6 shows the framework of a PKI. There are four primary components: the CP/CPS, the users involved, the software and the hardware. The CP/CPS must be in accordance with the general security policy. It imposes rules, obligations and procedures on the users. The software enables the use of the PKI. The hardware is also important because it is directly exposed to threats to PKI.

8.2.5 Authenticity of certificates

The digital signature of the CA ensures the authenticity of certificates. The only secret element in this is the secret key of the CA, as opposed to the hash and other cryptographic functions that are publicly available. The secret key must be long enough to preclude it from being guessed. This means that PKI technology is public knowledge. The fact that all PKI mathematical functions are common knowledge makes the PKI secure. No security can be breached, except by the secret key. If the secret key is broken, only a single certificate is compromised and the system itself remains secure. There is no security based on secrecy or "security by obscurity" for digital certificates. This means that the secret mathematical algorithms do not ensure security.

8.2.6 The use of a PKI for digital identification

There are many ways to use PKI certificates as documents for digital identification, e.g. for secure access to a building, a computer, digital pockets diaries, mobile phones, a network, databases, etc. This is a fundamental difference from the physical world in that sometimes persons identify themselves digitally on a digital device instead of identifying themselves to other persons. This section will discuss several aspects that are characteristic of the application of digital identification.

Basically, PKI certificates are intended for identification of the holder. After authentication, an authorization process gives the certificate holder access to a system. Certificates can be applied in different ways in the authentication and authorization process.

One possibility is that the certificate only contains identity data of the owner. In that case, the certificate is used for authentication on a system and an authorization process on the system grants the user access to that for which he is authorized. The user can also use the same certificate to authenticate himself on different systems with the same certificate, whereby the rights to the system are linked to the identity in the authorization process. This application enables the registration of all actions of the user by means of his identity.

A second option is that in which the certificate contains data on the function of a user, which enables the certificate to link authorization and authentication. A separate authorization process is not required on the system. The user is not recognized by means of his personal identity, but as someone who performs a certain function, which is directly linked to authorization. An advantage of this is that different persons with the same function can use the certificates. Another is that new users to the system can reuse the certificates of other users. However, this application is not suitable where users are held responsible for their actions on the system. Another point to keep in mind is that the certificate cannot be easily used by other systems.

A third possibility is that the certificate contains identifying data in addition to data on the function of the holder. In that case, the certificates can be used for both the above-mentioned mechanisms. This could be useful if functions on systems are reserved for specific, authorized persons, while authorization is granted outside the system. For instance, if an organization that has no access to a system authorizes personnel to perform certain actions, then verification of authorization is possible in this manner. The application for authorization goes to the organization that grants the authorization. This authorization goes to the CA, and the CA issues the special certificate. In this way, the organization that grants the authorization has control over the system from a distance.

8.2.7 Authorization, digital signature and data encryption

Another important point is that a certificate may be utilized not only for authentication, but also for digital signatures and exclusive data encryption. Technically, all these three actions can be performed by using a single certificate. However, the requirements for these three actions can vary widely. It is important to decide whether to issue a single certificate for all three actions or different digital certificates for the separate actions. If a certificate is suitable for exclusive data encryption, it is likely that the secret key for encryption requires an escrow mechanism. This can be used to decrypt encoded data if the secret key is lost. However, this is not required for certificates that are used for authentication or digital signatures because in these cases only the public key is needed for decryption. An escrow mechanism is even undesirable for authentication and digital signatures because this means that a secret key could be known to a third party or be accessed unnoticed. This type of secret key must be generated by a smart card for high-quality applications, and it must be ruled out that the secret key can be read from the smart card. This ensures that the secret key can only be used by the microprocessor on the smart card. This means that the encryption functions for authentication and digital signatures must also be carried out by the smart card.

Authentication and digital signatures can also make different demands on the procedures used. For instance, the EU directives for digital *signature* certificates require that the issuing party accepts limited liability (EU, 1999).

Something that must be considered is whether a digital signature certificate is necessary when an authentication certificate is issued. An example of a protocol that uses a single certificate for authentication and data encryption is Secure Socket Layer (SSL) (Freier et al., 1996). This protocol uses an authentication certificate for data encryption, which gives no problems for retrieval because the data is only encrypted during sending and no storage is required. Because the encryption is only used for data transmission, a key-escrow is unnecessary. This ensures that the data sent is not eavesdropped on and that no other party has access to the secret key.

8.2.8 PKI in a request for tender

A number of important issues arise when a PKI system or service regardless if it is put out to tender independently or as part of a larger system.

The call for tenders must include of a clear list of requirements specifying the level of security that is to be implemented. This enables the contracting party to effectively assess the tenders. Also, changes during implementation can be easily tested against the list.

For PKI, the tender must include the items listed in Table 8-2.

Security Policy	Determines the required level of security
Risk Analysis	Identifies the risks to security and the level of countermeasures required
Certificate Policy	Defines the level of confidentiality of the PKI
General architecture and operating procedures	Gives the functional requirements of the system
Technical specifications	Gives the technical requirements that the system must meet
Criteria for acceptance	Defines the criteria that the system must meet to be accepted

Table 8-2: The issues that need to be addressed when putting a PKI out to tender

The above is based on the assumption that the users of the system and computer use PKI for strong authentication and digital signatures, possibly in combination with secrecy. Even if an IT system makes no use of a PKI, the items in Table 8-2 still apply to calls for tenders, with the exception of the Certificate Policy.

■ 8.3 Security policy

A general security policy must be drawn up that applies to all parts of the system or service being put out to tender. This must be included in the call for tenders in order to establish a baseline for overall security and IT security in particular. A manual for this is the *Code of practice for information security management* (ISO, 2005).

8.3.1 Risk analysis

As was previously explained, not only the digital certificate or the PKI service needs to be secure, but the entire process chain. It is all about striking the right balance between the IT, the procedures, the people, the organization and the other systems.

In order to arrive at the required security level, a risk analysis must be carried out. This analysis must describe the interdependence of the security of the procedures, organization, people, systems and reviews and audits. This must be combined with an analysis of the vulnerability of the said components in relation to each other. The basic principle is that the security of the system is a chain, and that the links in this chain must be equally strong. The risk analysis is used to describe security relations between the links and to define the measures necessary to arrive at the desired security level (BSI, 2004; ISO 2005).

Inclusion of a risk analysis gives the suppliers insight into the measures that must be taken in order to manage the risks.

8.3.2 Certificate policy

This document describes the policy for issuing digital certificates. A useful guideline for this document is the Internet RFC 2527 (Chokhani and Ford, 1999). The certificate policy sets out the requirements that the PKI must meet, which in reality are equivalent to those which the tenderer must offer. Even if a PKI is part of a larger system it is still important to include this document in the call for tenders.

8.3.3 Architecture and operating procedures

The architecture of the system must also be included in the call for tenders. It is also advisable to include data models for interfaces and messages in the same bid for tenders. This is particularly important when data is exchanged between various databases.

The operating procedures must be included so that the tenderer knows which functionality to supply.

8.3.4 Technical specifications

The technical specifications must also be included to clarify what the specific security requirements are. These must be state-of-the-art so as to keep up with the rapidly changing security conditions in the digital world. It is also necessary that a mechanism is defined and implemented that enables alterations, improvements and updates of the security components. The aspects mentioned in Table 8-2 must be included in this.

8.3.5 The criteria for acceptance

The criteria for acceptance must include the security requirements described in the security policy, the risk analysis and the technical specifications. If the acceptance criteria only contain the technical specifications, there is a risk that the final results will deviate from the requirements laid down in the security policy and risk analysis.

References

American Bar Association
1997 *Digital Signature Guidelines*

Bundesamt für Sicherheit in der Informationstechnik
2004 *IT-Grundschutz Manual: Catalogues of safeguards*, Bonn, Germany

Chokhani S. and W. Ford
1999 RFC 2527; Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

European Union
1999 *Community framework for electronic signatures*, Directive 1999/93/EC of the European Parliament and of the Council 13 December 1999

2006 Biometric deployment of EU passports: EU passport specification, Working document

Freier A.O., P. Karlton and P.C. Kocher
1996 *The SSL Protocol* Version 3.0, Transport Layer Security Working Group 18 November 1996, Internet-Draft, http://wp.netscape.com/eng/ssl3/ssl-toc.html

Housley R., W. Polk, W. Ford, and D. Solo
2002 *RFC 3280; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

ICAO NTWG
2004 *PKI for Machine Readable Travel Documents Offering ICC, Read-Only Access,* Technical Report, Version 1.1
2006 Document 9303 – Part 1 Machine readable passport, Volume 2 Specifications for electronically enabled passports with biometric identification capabilities, Montreal, Canada

ISO
2001 *ISO/IEC 9594-8:2001; Information technology – Open systems Interconnection – The directory: Public-key and attribute certificate frameworks,* Geneva.
2005 *ISO/IEC 17799: 2005, Information technology – Code of practice for information security management*, Geneva.

Rivest R.L., A. Shamir and L.M. Adleman
1978 "Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM,* 21(2): 120-126.

Schneier B.
1995 *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* 2nd Edition, John Wiley & Sons, New York.

CHAPTER 9

INFORMATION, COOPERATION AND TRAINING

■ 9.1 Information sources

This chapter provides several sources of information on the development of secure documents, including a selection of entities, companies and websites that are specific to highly secure documents. Geographical location, market segment, and financial means have a strong influence on the choice of suppliers so the following information should merely be used as a reference for further study.

9.1.1 Information on documents from international institutions and governmental entities

The International Civil Aviation Organization has a comprehensive website on machine-readable documents. It sheds light on ICAO Document 9303 and several technical documents that support the development of travel documents (see Section 2.6.2 for detailed information).

The website of the European Union contains information on European legislation regarding identity and travel documents (see section 2.6.5 for detailed information).

The European Central Bank (ECB) has a website that provides information on the new Euro banknotes from design to distribution.

The Hologram Image Register of the IHMA is maintained by the Counterfeit Intelligence Bureau (CIB). Established in 1985 by the International Chamber of Commerce, this organization represents and functions as a focal point for industry against the growing problem of counterfeiting. For more details see http://www.iccwbo.org/index_ccs.asp.

Furthermore, several countries have online technical information about travel/identity documents issued by relevant authorities: e.g. Estonia, Lithuania, The Netherlands, Pakistan, Canada and Switzerland. Other countries offer legal information (mostly in the language of the country): e.g. Italy, Spain and India.

Additionally, Italy has a public Internet site for running number checks in the "blank stolen documents" database, as well as number plates and VINs of stolen vehicles. The Czech Republic has a website in which invalid identity documents can be searched.

Table 9-1 is an overview of the websites of international institutions and governments entities.

Canada	www.ppt.gc.ca/passports/book_e.asp
Czech Republic	www.mvcr.cz/english.html
European Central Bank	www.euro.ecb.int
European Union	http://europa.eu.int./index_en.htm
Estonia	www.mig.ee/eng
ICAO	www.icao.int/mrtd/home/index.cfm
India	www.passport.nic.in
Italy	http://coordinamento.mininterno.it/servpub/ver2/principale.htmwww.poliziadistato.it/
Lithuania	www.dokumentai.lt
The Netherlands	www.identitydocuments.nl
Pakistan	www.nadra.gov.pk
Spain	www.mir.es
Switzerland	www.fedpol.ch/e/themen/index.htm

Table 9-1: International institutions and governmental entities.

9.1.2 Commercial information on documents

A lot of information about producers and products is available on the internet. Our "virtual" tour through the Internet sites (see Table 9-2 below) begins with companies that manufacture secure documents or the system integrators. Remember that the choice of the producer depends on the secure document to be developed, as well as the already mentioned technical requirements, financial means, etc.

The table also lists companies that supply components for secure documents, such as inks, paper, DOVIDs, protective foils, etc.

Information about the security features of documents can also be bought. Keesing Reference Systems, a company specialized in reference documentation, offers a database with images and accompanying descriptions of genuine ID documents and banknotes as well as forged banknotes.

Lastly, there is a list of companies specializing in personalization equipment.

Manufacturers	www.abncompany.com www.allaminyomda.com www.bundesdruckerei.de www.cbnco.com www.delarue.com www.fnmt.es www.gi-de.com (Gieseke+Devrient) www.goznak.ru www.imprimerienationale.fr www.incm.pt www.mirage-hs.si~ www.oberthur.com www.ofs.ch www.sdu-identification.nl www.setec.fi (Gemalto) www.staatsdruckerei.at www.trueb.com
Suppliers	www.3m.com www.fasver.com www.gsi-gmbh.com www.hologram-industries.com www.infineon.com www.kinegram.com www.kurz.de www.landqart.com www.louisenthal.de www.luminescence.co.uk www.museodellacarta.com/ing/home_page.html www.nxp.com www.opsecsecurity.com www.security.arjowiggins.com www.sicpa.comwww.tumbabruk.se (Crane AB)

Reference Systems	www.documentchecker.com (Keesing)
Personalization equipment	www.datacard.com www.diletta.com www.iai.nl www.maurer-electronics.de www.muhlbauer.com www.secure.ps.de www.toppan.co.jp/english/index.html

Table 9-2: Commercial links.

9.1.3 Specific information on biometrics

Biometrics in travel documents has been a hot topic in the past few years. Beside manufacturers and system integrators, there are governmental websites on this topic. Once more, the selection below is just a fraction of what the World Wide Web has to offer.

Governments	www.cesg.gov.uk/ www.engr.sjsu.edu/biometrics/index.htm www.itl.nist.gov/div895/biometrics/index.html
Other	ww.biometrics.orgwww.eubiometricforum.com

Table 9-3: Biometrics-related information.

9.1.4 Conferences and exhibitions

The fastest way to find information about products, companies and services is to visit an exhibition or participate in a conference. Events are organized worldwide and encourage dialogue between governmental and non-governmental entities in the search for the best solutions. The interaction between governments and the security industry should be primarily regarded as an alliance, in which the parties meet on a regular basis and arrive at decisions that further developments in the area of secure products.

Event	**Topic**	**Frequency**	**Website**
Biometrics (London)	Biometrics	Annual	ww.biometrics. elsevier.com
CardTechSecureTech (CTST)	Smart cards, identification, biometrics, PKI	Annual	www.ctst.com
Cartes (Paris)	Smart cards, identification, PKI, etc.	Annual	www.cartes.com
Cebit	IT, cards	Annual	www.cebit.com
Drupa	Printing systems	4-5 years	www.drupa.com
ICAO	Machine-readable documents	Annual	mrtd.icao.org
Intergraf	High security printing	Biennial	www.intergraf.org
Interpol *Note: attendance to the conference sessions for government representatives only.* *For more information, contact the Interpol Central Bureau of your country.*	Banknotes and fraudulent travel documents	The worldwide conference is held once every four years, the European one is biennial.	www.interpol.org
PISEC	Brand protection, security features	Biennial	www.pisec.com
Security Printing & Alternative Solutions in Central/Eastern Europe and Russia/CIS	Security printing	Annual	www.security-printing.com
SPIE Conference on Optical Security and Counterfeit Deterrence	Security features	Biennial	http://spie.org

Table 9-4: Conferences and exhibitions.

■ 9.2 International cooperation

Governments are working together intensively to achieve standardization and global interoperability. Since organized crime and terrorism have been identified as the major threats to public order, countermeasures on a broader geographical scale have been discussed at length and accepted, namely those concerning:

- the minimum security standards for identity and travel documents;
- the minimum training required of immigration officers and civil servants responsible for issuing documents;
- the exchange of training calendars;
- the procedures regarding prevention and support of the investigation of stolen blank documents;
- the minimum equipment required at all ports of entry and document issuing points;
- the exchange of immigration officers;
- the adoption of uniform and harmonized regulations where the personalization of documents is concerned, etc.

International cooperation plays an important role in the establishment of rules, procedures and recommendations on issues relating to secure documents.

Actually, many forums have been established for the very purpose of discussing international cooperation. Some forums focus on the technical aspects of document production, others on the detection of fraud and networks for the exchange of information (see sections 2.6.2, 2.6.3, 2.6.4).

Within the framework of the European Union there is the False Documents working group called the Visa Committee and Europol's Falsified Documents working group. This working group meet several times a year. As far as the international community is concerned, there is the Immigration Fraud Conference (IFC), which includes the countries of Western Europe and North America; the Pacific Immigration Intelligence Officers Conference (PacRim), which covers the Asian and Pacific countries; the International Conference for the Western Mediterranean (ICWM), comprising the EU southern countries, together with some Mediterranean Africa states, and the Budapest Conference, whose members include the EU states and the Eastern European countries.

Finally, there is the European Network of Forensic Science Institutes (ENFSI), which explores the harmonization of procedures within the international community. It also aims to achieve the certification of expertise.

Nevertheless, there is still room for worldwide organizations to operate. Interpol, for instance, uses an information system built from specific analysis work files, and made the exchange of information its priority using a network involving all its members.

International cooperation can also play an important role in helping governments enhance the security and integrity of travel and breeder or source identification documents consistent with international standards.

The International Organization for Migration (IOM) is an intergovernmental organisation that also helps governments to improve the legislation, policies, administrative structures, operational systems and human resources needed to tackle a range of migration-related issues.

Within the field of travel documents and border systems, IOM, as an impartial service provider, provides support to countries in assessing existing documents and systems, planning specifications, drafting tenders for such systems, and – at times – managing the implementation of projects aimed at improving and/or upgrading both the system and the document.

The IOM subscribes to the view that more secure travel documents make it easier to control cross-border flows (whether legal or otherwise). Through the Technical Cooperation on Migration (TCM) service, the IOM participates in relevant meetings, including ICAO meetings. The IOM not only supports ICAO's drive to promote interoperable standards for machine readable documents, it also participates in private-sector solutions in this area.

■ 9.3 Training and quality of training

The effectiveness of documents can be seen at the inspection level, and this is where document inspectors come in. Organizations need to ensure that these officers are sufficiently informed of new developments and receive suitable training to enhance their performance.

Figure 9-1: View of the “class room” of the European Seminar on Polymer Substrates under the flag of the European Argo program, where - organized by the Serviço de Estrangeiros e Fronteiras from Portugal - teachers shared their knowledge with European students from immigration and police services.

In view of the final objective, which is security, the effectiveness of a service or entity is measured by the efficiency level of each individual involved, whose proper performance depends, in the end, on appropriate means and levels of training and information.

According to the International Labour Organization (ILO), “professional training is an organized process of education, thanks to which people can expand their knowledge, develop their abilities and improve their attitudes and behaviour, thus increasing their technical or professional qualifications, as well as their participation in the socio-economic and cultural development of society, in a continuous process to achieve fulfilment and happiness”.

Represented in a schematic diagram (Figure 9-1):

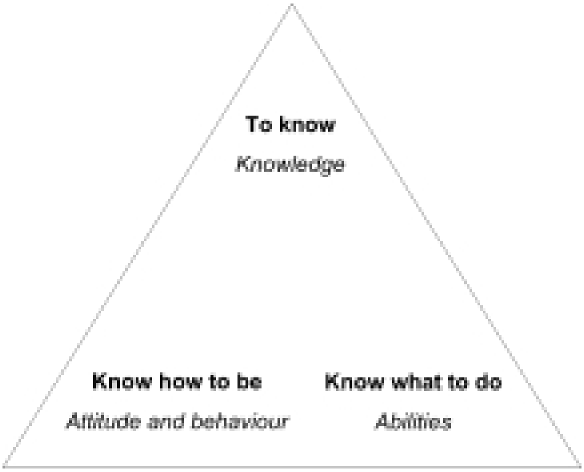


Figure 9-2: Schematic definition of training according to ILO.

Therefore, the training of document inspectors should be seen as a continuous process, ensuring that they not only have the necessary expertise at their disposal, but also know how to apply it in order to enhance the quality of the service they provide and ensure security.

Seen from this angle, training is without doubt more an investment than a cost. Not only is training more productive, but it has short, medium and long-term effects on the entire system. In order to gain a better understanding of this issue, it is important to be aware of the mission and objectives of the security services and police forces which are responsible for document inspection. It is up to them, in the final analysis, to control security and, in particular, to regulate the legal and illegal migratory flows, where documents assume a special significance.

The material and human resources are obviously interdependent as far as efficiency is concerned. Without human resources, the material ones are useless: they cannot operate or become more efficient on their own. Similarly, human resources, without the material ones, are powerless to carry out the tasks that are constantly demanded of them in this age of grand technological solutions.

Strategy, planning, structure, power and technology are not enough in the security services. Security officers also need to be dynamic, observant and prepared. For instance they need to know how to transpose those presuppositions for achieving the final goal of the service, having in due consideration all external circumstances.

As times change, needs, raw materials and objectives also change. Therefore, solutions need to adapt to new needs and not stay focused on old ones. In the context of global, international and contingency change, there is a constant demand for organizations to become more flexible and rapidly adapt their tasks and competencies to meet the new needs.

The new strategic management policy in the services urges for better security strategies. To renew and modernize is a challenge that needs to be faced by all parties in the services. Therefore, it is important to invest in the training of security officers in light of the new social values, methods and successful techniques of intervention. It is also necessary to minimize risks resulting from the lack of motivation and unacknowledged performance.

However, no matter where the emphasis lies in training, it is also important to first focus on correct recruitment procedures for officers. A rule of thumb is that it is not only easier, but far more efficient, to train good people than to motivate bad staff. The recruitment of human resources should be based on a thorough study and assessment of the service's needs and the officer's specific tasks. Identifying the right profile for the job is as important as keeping existent personnel knowledgeable by means of training.

The existence of a new model and new order is a reality, fortified by knowledge and information, which are the principal instruments to be handled with the greatest skill. Whoever knows how to use them best has the greatest competitive advantage. This idea of "competitive advantage" in relation to markets and companies has been reinvented by Porter, based on studies by Igor Ansoff on the "value" that each organization is able to develop and add to its "business", thus producing a chain of values.

As far as organizational reengineering is concerned, the control authorities and immigration services in particular need to know how to choose and make serious decisions about their "added value" in the context of their specific knowledge and organizational culture so as to build and shape their own "chain of values". This process is dynamic in its search of the best "competitive advantage" and exposes potential failures marked by lack of professionalism.

The citizen is at the receiving end of this complex process, along with the privileged security service entity. It should, therefore, be the citizen who determines the quality of the service. In other words, the product must satisfy the security needs of the citizen. The product endowed with this quality represents the value of the services.

In this respect, public acceptance plays a decisive role in the ultimate success of the entire process. National authorities should regard the provision of information and education to the general public as the key to achieving the best possible performance. Information about secure documents should be widely distributed. Security aspects and the legal relevance of identity and travel documents should be given due attention along with the possible consequences of their misuse.

The easiest way to do this is to organize a national campaign that publicizes a document's most relevant information. Such a campaign should concentrate on first-line security features. The information should be accurate, be rendered in simple and clear language and strictly avoid technical jargon. Where possible, the text should be supported by illustrations and diagrams to increase clarity and understanding. National authorities also have a responsibility to see to the constant updating of the information. The bottom line is that being misinformed is far worse than not being informed at all!

In short, only concise, precise and timely information promotes good communication, which, in turn is conducive to better interaction between law enforcement authorities and the general public.

Ultimately, a public conscience and shared sense of belonging will develop, enabling a spontaneous and genuine contribution to security.

This edifying attitude leads the general public to be more self-assured and more confident about the system. The citizen will feel encouraged to contribute in a more positive and active way to the success of the entire process, which, in time, will include the combating of crime. Informed citizens will, therefore, actively assist in the detection of fraud. They may even anticipate and deter crime by alerting the competent authorities. This attitude will encourage the citizen to actively intervene in the security process as a whole. This will result in a call for more and better security, and at the end of the day, that is what everyone's ultimate goal is.

The citizen is the first to evaluate the effectiveness of a document conceived for his security. It should, first of all, be practical, both to the citizen who uses it and to the inspecting officer who assesses its authenticity. Herein lies the merit of the service for both parties. However, the increasing technological demands on both the process of verification of a document's authenticity and the process of a document's conception should not be underestimated. Immigration services and control authorities need to stay on their toes so as not to be overtaken by the professionalism of forgers and frauds.

To this end, the following measures can be put in place to act as deterrents or countermeasures in the fight against document fraud:

- the exchange of information on the means and techniques used by fraudsters;
- careful monitoring of the secure document industry;
- ensuring regular contact with the manufacturers and security suppliers responsible for the production of the documents;
- providing adequate equipment to the services in charge of document inspection.

In short, sustained dialogue between governmental and non-governmental entities will potentially benefit both parties.

Depending on the control levels (first, second or third level controls) and the more or less sophisticated technical equipment available, the services should also have access to reference manuals for consultation. Obviously, both the equipment and references should be up to date so as to ensure the best possible results.

The same applies to the general public. For the best results, the ordinary citizen should have access to clear and easily accessible information, e.g. in the form of brochures, pamphlets, websites, national helpdesks and telephone numbers for public enquiries. Marketing experts know how to make the most of the possibilities available. The more accurately and effectively the information is communicated, the greater the system's credibility and the better the citizens' input into security.

The citizen attaches great importance to the trustworthiness and credibility offered by the system. He will observe its requirements willingly, even if it involves his being questioned or "bothered" about his ID, if he believes that his personal security is being served. This is one of the most important factors for any inspector doing his duty. Therefore, it is essential that an inspecting officer has the right profile and possesses the knowledge and competency required for the job. The best approach is to carefully recruit and prepare officers, a task that should be carried out by those who are responsible at the intermediate level, as much as by the first-line trainees. Their mission is to do this well and with the appropriate means at their disposal.

Therefore, investing in continuous, specialized training is more than a necessity, it is a challenge. Immigration officers are the representatives and national conscience of the immigration services. They are responsible for transparency and the guarantee that quality service is being provided effectively and efficiently.

9.3.1 Definition of quality in training

If we wish to apply this idea to the control authorities, particularly to the immigration services, then we can assume that quality means "being in conformity with the security requirements, which in turn conforms to the requirements of the citizens". Thus, the idea of "quality" will have to be regarded as an integrated and comprehensive process in which all the regional services, despite their geographical spread, will have to implement and observe the same quality standards. In this respect, the immigration officer will not only have to be competent and knowledgeable, but he will also have to be aware of relevant social aspects of the community he works for.

9.3.2 How to improve training

Increasing the skills of the immigration officers must be a constant concern of the system, and although it is true that the institutions have dynamic systems, change is inevitable and nothing stays right, stable and uniform forever.

Therefore, on the one hand, training and professional improvement should stimulate an officer to continue to train himself, while at the same time it remains the institution's duty to provide training to officers. Based on their newly acquired professional and personal competencies, officers should display a new mental and behavioural attitude resulting from professional training based on the philosophy of *know, know how to do,* and *know how to be.*

Only then will an officer have gained the proper insight and training necessary to serve and carry out his task. The acquired theoretical and practical knowledge and the ability to understand and support the cause, coupled with a sense of responsibility, will enable an officer to motivate himself when working under stress or difficult conditions.

If the officers of the immigration service interested in renewal *know how to be*, then this implies that they will undoubtedly be keen to apply the latest technological developments. This in turn will create working conditions that enable officers to automate the processes, thereby improving productivity and response rates.

Inspection authorities, including immigration services, have made considerable efforts, but there is still a lot of investment required, to promote the quality and to achieve a higher degree of development and motivation of the immigration officers. This is a main strategic factor in the success of the Immigration and Security Services. Innovation of human resource management is the key. Proper management and service provision call for a new mentality, alignment and coordination of human resources. To begin with, this means assigning the right person to the right place, or as the saying goes, "every jack to his trade", taking into account an employee's level of knowledge, his preferences and personal satisfaction gained from a willingness to serve with discipline, loyalty and adaptability.

Training departments, which play an important role in all stages of the quality process, are working together in search of the best solutions. Together with the responsible parties, they are tasked with carrying out the various types and levels of training, tailored to the specific needs of both the officers and the security services. The various training needs can be addressed in e.g. a classroom, via distance learning or even self-study.

It is important that the different management levels recognize and endorse the professional training of inspectors as a pre-condition, enabling the services to operate effectively. In other words, training should be considered mandatory.

To inform is just as important as training when it comes to the search for the best solutions. The recipients must be carefully selected, and the message conveyed in an appropriate way, i.e. objectively, precisely and briefly and at the right time. The message should clearly outline the main points and should be spread through the right channels. Equally important is the exchange of information between entities, the designation of specific contact points for the screening of suspicious cases/files, and the follow up of said cases in the context of international cooperation.

The general public's acceptance of and attitude to a given secure document, as to any issue in general, depends on how well informed the ordinary citizen is. A knowledgeable public can provide positive input to improve the overall performance of the system, ultimately contributing to security. Public opinion varies from state to state, and is related to a variety of factors. Culture, technological development and the history of a given population leads to different attitudes. Generally, a certain attitude lasts as long as a generation and its impact may only be perceptible for a medium to long term. As far as acceptance of a secure document is concerned, the public's tolerance of new technologies is quite important. Actually, states need to focus their attention on and be cautious about the demand for biometric data as a means of identification. If, on the one hand, biometrics is the best answer to the latest security-related events, on the other, biometrics implies a new concept of security and, in extension, a new public conscience.

In fact, promoting a relationship of trust between a state and its citizens undoubtedly contributes to the acceptance of any measure in this field.

Finally, we must not fail to appreciate the importance of human resources in the overall security process. It is none other than the officers who, guided by an overall strategic and operational plan, put into effect and give dynamism to the security process. They are the ones who are responsible for the success or failure of the institution. To quote H. Mintzberg: “strategy is not planned, it is constructed”. And humans are the only species that possess such building skills!

From all that has been said, one can conclude that the following potential benefits may be derived from training, either by the individual or the institution:

For the individual:

- greater motivation
- specific knowledge
- better technical abilities and communication skills
- openness to change
- capacity to make decisions
- self-confidence
- personal fulfilment
- sense of belonging in regards to the institution
- sense of progress in the learning process
- control over tension and conflict
- ability to overcome frustration.

For the institution:

- improve performance at all levels
- increase identification with the institution’s objectives
- increase productivity
- improve the organization’s climate
- improve motivation and participation levels
- facilitate communication and conflict control
- contribute to improvement of the institution’s image.

Quoting *Formar* (1997) on the professional training of workers: "*The dominant competitive weapon of the 21st century will basically be education and the skills of the workforce*" (Lester Thurow).

References

IEFP
1997 *Formar*, Training magazine of the Employment and Professional Training Centre, 29:4.

Morna Gomes, M.
1995 "Estratégia e Planeamento na Gestão e Administração Pública", ISCSP

ABBREVIATIONS

Abbreviation	Meaning
AAMVA	American Association of Motor Vehicle Administrators
ABS	Acrylonitrile Butadiene Styrene
AFIS	Automatic Fingerprint Identification System
AGP	Agreement on Government Procurement
APP	Allocation of Priorities Principle
AQL	Acceptable Quality Level
ATM	Automated Teller Machine
CA	Certificate Authority
CAD	Computer-aided design
CARICOM	Caribbean Community
CBEFF	Common Biometric Exchange File Format
CCTV	Closed-circuit television
CD	Compact Disk
CID	National Criminal Intelligence Division
CIB	Counterfeiting Intelligence Bureau
CJIS	Criminal Justice Information Services
CLI	Changeable Laser Image
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CTST	CardTechSecureTech
D2T2	Dye Diffusion Thermal Transfer
DCFWG	Document Content Format Working Group
DET	Decision Error Trade-off

DNA	Desoxyribo Nucleic Acid
DOVID	Diffractive Optically Variable Device
EAC	East African Community
EC	European Community
ECB	European Central Bank
ECOWAS	Economic Community of West African States
EFPWG	European Finger Print Working Group
ENFSI	European Network of Forensic Science Institutes
EU	European Union
EVA	Electronic Issue of Visa
FAR	False Acceptance Rate
FRR	False Rejection Rate
FSAAWG	Forensic Speech and Audio Analysing Working Group
FSS	Forensic Science Service
GBA	Municipal Personal Record Database (Gemeentelijke Basis Administratie)
IBIS	Interagency Border Inspection System
ICAO	International Civil Aviation Organisation
IC	Integrated Circuits
ICT	Information and Communication Technology
ICWM	International Conference for the Western Mediterranean
ID	Identity
IDP	International Driving Permit
IEE	Institution of Engineering and Technology
IFC	Immigration Fraud Conference
IHMA	International Hologram Manufacturers Association
ILO	International Labour Organisation
INSPASS	Immigration and Naturalization Service Passenger Accelerated Service System
IPS	School for Forensic Science
IOM	International Organization for Migration
IR	Infra Red
ISO	International Organization for Standardization

IT	Information Technology
JTC	Joint Technical Comity
LR	Likelihood Ratio
MERCOSUR	Mercado Común del Sur
MLI	Multiple Laser Image
MRTD	Machine Readable Travel Documents
MRZ	Machine Readable Zone
MRV	Machine Readable Visa
Nd:YAG	Neodymium- doped Yttrium Aluminium Garnet (crystal)
NFI	Netherlands Forensic Institute
NTWG	New Technology Working Group
OCR	Optical Character Recognition
OVD	Optical Variable Devices
OVI	Optically Variable Ink
PCM	Pulse-Code Modulation
PDCA	Plan Do Check Act
PET(G)	Polyethylene Terephthalate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PVC	Polyvinylchloride
RFC	Request for Comments
RFID	Radio Frequency Identification
SC	Sub Committee
SDR	Special Drawing Rights
SIA	Swiss Society of Engineers and Architects
SLA	Service Level Agreement
SSL	Secure Socket Layer
TAG	Technical Advisory Group
TLI	Tilted Laser Image
TF	Task Force
UIMRTDWG	Universal Implementation of Machine Readable Travel Documents Working Group

UN	United Nations
UPS	Uninterruptible Power Supply
UV	Ultraviolet
VAT	Value Added Tax
VIN	Vehicle Identification Number
WG	Working Group
WSQ	Wavelet Scalar Quantization
WTO	World Trade Organization

INDEX