WORLD MARITIME UNIVERSITY

Malmö, Sweden

SMART CARDS
AS PROOF OF SEAFARERS' IDENTITY AND CERTIFICATE

By

HAMID REZA AKRAMI

Iran (Islamic Republic of)

A dissertation submitted to the World Maritime University in partial fulfilment of the requirements for the award of the degree of

MASTER OF SCIENCE

In

MARITIME AFFAIRS

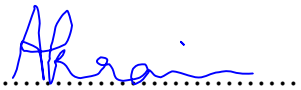
(MARITIME ADMINISTRATION)

2004

Declaration

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature): 

(Date): 30 August 2004

Supervised by: Professor Malek Pourzanjani
Professor at World Maritime University

Assessor: Professor Takashi Nakazawa
Lecturer at World Maritime University

Co-assessor: Captain Andy Winbow
International Maritime Organization

In the name of GOD

Acknowledgement

I would like to dedicate this dissertation to my wife, who has always supported me and given me courage and inspiration to keep going. While suffering a lot due to my busy student life, she gave birth to my lovely daughter on August 26 this year, which was one of the greatest happenings in our lifetime. I love both of them.

I would also like to express my gratitude to the Ports and Shipping Organization of Iran (PSO), which provided me with the opportunity to study at the World Maritime University, which is a great pleasure.

I would like to convey my sincere gratitude to my course professor and heartfelt thanks to the supervisor of my dissertation Professor Malek Pourzanjani, for his valuable guidance and kind assistance during the study and preparation of this paper.

I am really grateful to Mrs. Susan Wangeci Eklöw and all other members of WMU Library for their valuable assistance in providing me with the rare materials on the subject, without which completing this dissertation would have been extremely difficult. I also wish to express my sincere thanks to Mr. Clive Cole for his advice and guidance in preparing the dissertation.

Last but not least, my special thanks is dedicated to all WMU students of the class of 2004, who gave me the best moral support and were friends throughout the study.

Abstract

Title of dissertation: **SMART CARDS AS PROOF OF SEAFARERS' IDENTITY AND CERTIFICATE**

Degree: **MSc**

The dissertation is a study of the seafarers' identity (SID) and Certificates of Competency (CoC) documents, with a view to combine the two into one.

A brief look is taken at the history of identification and certification of seafarers and the importance of identity and certificate documents is described. Relevant rules and regulations in this respect are described and the changes that have been made to the documents and the methods and the reasons behind the changes are also examined.

Current methods used by different States are explained and the relevant problems and implications are introduced, including the issue of shore leave and fraudulent practices in the certification of seafarers.

Recent changes in the identification and certification of seafarers are analysed in more detail and the status of the new ILO convention number 185 (C185) about seafarers' certificates is investigated. The role of technology in this area is described by first reviewing the two major elements, i.e. biometrics and smart card technology. Different biometric identifiers are also described and compared, and various card types are introduced. The combination of the two is also covered, followed by a scientific analysis of which combination best suits document for identity and certificates of seafarers.

The chosen combination of biometrics/card in the ILO proposed solution is then examined based on the findings of the previous discussions.

Then the idea of Seafarers' Identity and Certificates document (SIC) is introduced, which is a combination of the SID and CoC. The idea is further developed by examining different aspects, such as the requirements, conditions, pros and cons and obstacles. Finally, several measures are introduced to tackle the problems, which is necessary for a successful implementation of the new document.

Keywords: Identification, Certification, SID, CoC, SIC, biometrics, smart card, shore leave, fraudulent practices

Table of contents and appendices

List of Tables, Figures and Abbreviations

List of Tables

List of Figures

List of Abbreviations

ILO	International Labour Organization
IMO	International Maritime Organization
SID	Seafarers' Identification document
CoC	Certificate of Competency
SIRC	Seafarers' International Research Centre
STCW	Standards of Training, Certification and Watchkeeping for Seafarers
FAL	Facilitation of International Maritime Traffic (convention)
FAR	False Accept Rate
FRR	False Reject Rate

Chapter 1

Introduction

1.1. Introduction

Shipping is a demanding business; while the world economy depends on it and around 90% of the world cargo (in volume) is transported by sea (Doumbia-Henry, 2003, p. 130), several obstacles threaten this global industry. Seafaring is, in itself, a difficult job and the number of seafarers is declining. (BIMCO, ISF, & U. Warwick 2000) However, there are certain problems in this business that are forced from outside. For example, one of the major difficulties that seafarers experience today is the refusal to be allowed shore leave, which is one of the fundamental rights of the seafarers. This is a direct result of the security concerns imposed from outside the shipping sector. Another serious problem of the shipping world is "fraudulent practices" in the certification of seafarers, which is rooted mostly in financial problems, and imperils the safety of shipping, as well as the marine environment.

Seafarers need to have their basic rights to satisfactorily perform their duties. However, the immigration authorities in most countries need credible proof of identity, as well as any other evidence, to ensure that the person going ashore is a genuine seafarer. Furthermore, the industry needs seafarers to have the required qualifications. This is mostly to promote the safety of shipping and protection of the

marine environment, by lowering the probability of having accidents, which are believed to be 80% due to human error. (Schröder, 2004)

Documents have been used for a long time to satisfy both needs, but the problem is that they are not tamper proof. For this reason, along with the other drivers of change, ILO proposed a new document for the identification of seafarers in its C185 convention, which was adopted on 19 June 2003. However, the new document has not succeeded, and the problem persists. Moreover, the ILO solution only considered the issue of identity as an urgent matter and without enough time and effort to consider all the relevant aspects of the problem. Yet, part of this problem, i.e. the certificates was not addressed.

The above circumstances are causing major difficulties for seafarers, who are not allowed to go ashore after long working periods onboard. Furthermore, they suffer from long inspections of their certification documents by Port State Control officers and Flag State inspectors, due to the highlighted problem of fraudulent certificates. Shipowners and Flag States also suffer from this situation, as the inspections and detentions result in delays, which lead to financial losses, as well as the resulting dissatisfaction among the crews. The boom in security has a role to play in making the conditions even more complicated. Nevertheless, the position of the USA is an important factor, which can change the state of affairs at any time. The fact that the USA does not accept the ILO proposed solution is a significant deterrent for the international community to ratify the ILO C185 convention.

However, there should be a solution to this problem. Even if the ILO document does not work, other solutions could be sought to rectify the hindrances and find a way out. Although the current focus of IMO and many other maritime entities is on security, identification and certification of seafarers should be placed on the agenda by considering all the relevant discussions. This approach can lead to a rational, internationally accepted, and working solution.

1.2. Preceding studies conducted on relevant subjects

Although biometrics and smart cards have a short history, due to the growing application of them for different purpose, they are being increasingly respected. For this reason, there are many sources of information and numerous researches done on each. Combination of biometrics and smart cards is also well considered by researchers and the industry. However, application of smart cards for seafarers is quite a new subject. It was only after the Liberian Register started to test a new document for its seafarers and the ILO initiated the new identity document that the idea was developed. The history of using biometrics and cards for seafarers does not exceed three years, and therefore, it is not easy to find preceding research in this area.

ILO must have performed some studies before adoption of the new convention (International Labour Organization, 2003), as well as the Liberian Register, before starting its trial application of the new seafarers' ID cards. During this research, it has been tried to get as much information as possible using different available sources, but access to such researches was not facilitated, since, for example, companies rarely unleash technical information which can threaten their position in the market.

1.3. The objectives

This study tries to review the identification and certification of seafarers over time, and to identify current practice and relevant issues and debates in this concern, including the initiatives for change and the results. It also focuses on the technological side to provide an analysis of the most suitable methodologies and equipment. However, the main objective is to examine the idea of a combined identity and certificate document, and the different solutions for this purpose. To

achieve this, different biometric identifiers and cards are examined to find out which best suit the requirements of the identification and certification of seafarers.

In doing so, the research does not try to find a definite solution. Rather, it tries to highlight some aspects, and show certain ideas in dealing with the issue, which can be considered as an outline for the actual practical solutions.

1.4. Methodology

This study tries to review current state of seafarers' identification and certification, analyse the situation to achieve better understanding of the important factors and drivers of change, the changes that have happened so far, and then, by considering all relevant factors and circumstances, tries to come up with the idea of a solution to solve the problems. The study is intended to have a practical view. To this end, contacts have been made with experts, manufacturers and service providers in this area and the results are reflected in the work.

1.5. Limitations of the study

This study was undertaken and done under a limited time of less than 8 weeks. On the other hand, as the subject is new, there were not enough resources and references at hand.

Chapter 2

Background

2.1. Introduction

Identification has always been a matter of concern for human beings. People in small communities recognize others by looking at and listening to them, but for bigger societies with large populations, more sophisticated methods of authentication seem to be necessary. In fact, in a big community with hundreds of thousands of people, it is neither accurate nor possible to authenticate people by looking at their faces or listening to them. So, they started to use symbols as proof of identity (what you have). By personalizing symbols, like writing a name or any other individual mark on it, identity documents came into existence. In this way, everybody had their own identity document and had to carry and present it whenever needed. Identity documents have long been used for authentication.

Documents as proof of identity

Later on, application of documents as proof of identity for access control became common practice. This kind of control was applied in the entries to certain public or private locations like buildings and airplanes, or to control access to a resource such as getting money from a bank. However, the checking and authentication process

was still being done manually (by human beings.) Then came the development of Information Technology (or "IT") and the movement towards automation also affected authentication methods. The idea was to replace people, who performed the checking and recognitions, with machines. To use machines for this purpose, the documents had to change to machine-readable formats. Even then, authentication was based on "what a person had" in hand, i.e. the document. Then, as the use of codes and passwords became more common, another factor of "knowledge" came to help the authentication process. In this way, only the person who knew a secret code or password would be successfully authenticated. Yet, it was possible for a person who could, somehow, access the document and knowledge to impersonate another one and falsely enter a location or use a service. The next step was to use something for authentication that is permanently bound to the individuals and cannot be stolen or imitated, such as biometrics. Biometrics was already a known subject in terms of criminal law enforcement procedures when it entered the domain of personal authentication. So, authentication has gradually become stronger by the use of "What one has", "What one knows", and "What one is."

2.2. Seafarers' identity

In the shipping world, which is a global industry, identification plays an important role. A vessel's crew members, who are not necessarily nationals of the Flag State, need to identify themselves at different stages of their job; so, they need an identity document. To solve the problem, States have established their systems to issue appropriate "Seafarers' Identity Document" or SID. However, these systems were designed to satisfy the requirements of individual States. In other words, each State could not recognize the identity documents issued by other States, as there was little harmonization in the issuance system. Regional cooperation among several States to accept each other's SIDs could be a good solution to this end, but not enough to entirely solve the problem for this global industry.

2.2.1. Discussions at ILO

The International Labour Organization (ILO), founded in 1919, is the first specialized agency of the United Nations. This organization tries to bring governments, employers and workers' unions together for united action to achieve social justice and better living conditions for workers all over the world. (Doumbia-Henry, 2000, p. 1) This objective is achieved through a special tripartite structure, i.e. the there kinds of delegates to ILO; *Government delegates*, *Workers' delegates* and *Employers' delegates*. Relying on this tripartite construction, ILO tries to make a balance among all the stakeholders, which is a good policy to guarantee success for its conventions.

ILO also involves seafarers, as a specific class of workers with special circumstances and requirements. Feeling the need for special privileges to be granted to seafarers regarding their movements all over the world, the ILO started preparatory work in London in 1956 to come up with a measure to facilitate international recognition of seafarers' identity documents so that seafarers can easily enter the territories of other countries for the purpose of shore leave, transit movement, or any reason independent on their own will. (International Labour Organization, 1959)

Two years later, the drafting committee presented its proposed convention to the 41st session of the International Labour Conference. A review on the discussions at the conference, as well as those in the seafarers' identity card committee, can show some of the concerns in this respect at that time. One interesting point is that prior to the adoption, the name of the proposed convention and the committee has the words "identity card" in it, which implies the original intention of the drafters to design a card-like document.

The record of proceedings of the 41st session of the International Labour Conference shows that Seafarers' unions were in favour of an internationally acceptable document for seafarers throughout the discussions. The Employers' delegates,

though quite active in the drafting committee, did not take part in the discussions and seem to have had no opposition against the convention. However, Government delegates had a challenging debate.

The first important point in discussions is the opinion of the USA Government delegate. This delegate was against articles 5 and 6 (giving shore leave) and this is quoted as a clear "No" on behalf of the US government. Another point is the debate between the Government delegates of India and Pakistan about the special situations of their seafarers and the two-sided problems they have in this respect. Yet it is an important issue, as it shows how bilateral circumstance can discourage global agreements. So far, neither of the two has ratified the C108 convention.

On the other hand, the Government delegate of India believed that western and European seafarers needed shore leave, but the major concern was that some seafarers would abuse this opportunity. This delegate claimed that if European seafarers were granted shore leave easily, they would settle in Indian ports and take jobs that belonged to their nationals in Indian ports. Some delegates were also concerned about complications arising from issuing cards for non-nationals.

Considering all the above discussions, the convention was formally adopted with 105 votes for, 6 against and 15 abstentions on May 13 1958. At the time of the adoption, there were 24 Government members, 8 Employers members and 8 Workers members. To achieve equality of voting, each Government member had one vote and each Employers' member and each Workers' member had three votes; the reason why the number of votes is larger than the number of delegates.

2.2.2. ILO C108 convention

The ILO C108 convention, which was the first convention about identification of seafarers, was an effort to harmonize seafarers' ID documents, aiming at the recognition by each State of SIDs issued by other States, for the purpose of

facilitating shore leave and professional movement. In other words, they had to recognize seafarers' SIDs to let them go ashore or move to/from their vessels instead of using passports and visas.

The convention entered into force in 1961 and gradually got a wide acceptance rate. With 105 positive votes at the International Labour Conference at the time of the adoption, 62 States have ratified the C108 convention so far (30 August 2004.) According to this convention, States are obliged to issue a SID for their nationals upon request. Nevertheless, they are not prohibited from issuing SIDs for non-national crew onboard their ships.

The convention considers simplicity of design and use of durable materials for the document as necessary and then defines the necessary information to be included in the document. However, the precise form and contents of the document are left to be decided by individual States.

Shore leave

In article 6 of the C108 convention, the important issue of shore leave is raised. This article obliges ratifying States to give permission to seafarers to go ashore while their ship is in a port of that State, without holding a visa. It also requires each ratifying State to let seafarers from other States enter their territory without a visa for the purpose of professional movement, which is defined as three different instances: to join their ship, to pass in transit to join their ship in another territory, or for any other purpose approved by State authorities. These are explained by using the words "Shall permit", which shows the intention to put a strong obligation on States in this respect.

Entry into force of the C108 convention is explained as being 12 months after two ratifications registered with the ILO Director-General, which was 19/2/1961.

2.2.3. IMO FAL convention

To emphasize the right of seafarers to use shore leave, IMO also addressed the issue in its Convention on Facilitation of International Maritime Traffic (FAL) 1965, which entered into force on 5 March 1967. The main objectives of the FAL convention are to prevent unnecessary delays in maritime traffic and improve cooperation among States. Nevertheless, in section G, standard 3.44 clearly obliges the public authorities of member States to allow foreign crew members ashore while the ship is in port, provided that they have no reason to refuse permission due to reasons of public order, health or safety. To further emphasize the issue, the next standard 3.45 States: "Crew members shall not be required to hold a visa for the purpose of shore leave."

Actually, IMO has tried to underline the importance of shore leave for seafarers In this widely accepted convention (98 ratifications so far.)

2.3. Seafarers' qualifications

On the other hand, seafarers should receive enough training and experience for each position they occupy onboard. So, besides the identity document, each seafarer should have valid documents called Certificates of Competence (CoC) to prove the qualifications they have obtained. Today, CoC is an integral element of professional jobs onboard ships, and it is by having a valid CoC that a seafarer can be qualified as a crewmember.

IMO addressed the issue of minimum standards of competence for seafarers in its International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) in 1978, as amended in 1995 (hereinafter called the STCW convention.) The STCW convention has certain procedures to be followed by the member States to ensure the training and competence of seafarers. The fact that

training and certification of seafarers is one of the main pillars of the IMO can reveal the level of importance of the issue for the whole industry.

While some non-maritime entities may be responsible for the SID, maritime administrations are the ultimate body in charge of the CoC. The argument about SIDs is that immigration authorities of the seafarers' State of nationality are the most competent entity to issue them.

2.4. Current practice

Although the C108 convention is in place to set a standard for SIDs, the format of the SID still depends a lot on the issuing State. This is also true of CoCs, which are issued by the maritime administrations in Flag States. Thus, States issue documents for their seafarers in a way that best suits their requirements, while those who have ratified the conventions also try to comply with the rules set by the relevant conventions.

Currently, seafarers carry the SIDs issued by Nation States. Regarding shore leave, different States have various practices in place; some follow the regulations of the C108 convention, some give seafarers even more freedom by relying on crew lists and some require individual visas. For example, as the United Kingdom is a member of the ILO C108 convention, foreign seafarers calling at a UK port enjoy all the rights conferred by the convention, including the visa exemption for shore leave and professional movement. Thus, seafarers that have a valid identity document in hand (even if they are not a national of the issuing country) can go ashore in UK ports if their names are listed in the crew list. However, this is valid only for seafarers who obtain their identity documents from a ratifying State of the C108 convention. (The UK Immigration & Nationality Directorate website, 2004) In the Netherlands, foreign seafarers on the crew list are allowed to land for shore leave without any documentation. There is also no requirement to produce a passport or a seaman's book or to be in possession of a shore pass. Seafarers on shore leave are completely

free to move within the city limits where the port was located and in neighbouring cities. (International Labour Organization, 2003a, p. 14)

In the Philippines, crew list visas are used. A crew list visa is a seaman visa issued for all foreign members of the crew of a vessel approaching a country. In the Philippines, a crew list visa is valid for single entry only. (The Philippine Embassy in Stockholm website, 2004) Although the use of crew list visas has been the normal practice in the USA, the situation has changed now, meaning that all such seamen would have to apply for a normal visa to go ashore in US ports. ("US insists that crew list visas must end", 2004, p. 1)

On the other hand, CoCs are issued by the maritime administrations for the seafarers who join one of their vessels. The certificate can be issued based on a training course pursued by the seafarers or it can be an endorsement of a certificate already issued by another State. The rules and regulations governing these certificates are set in the IMO's STCW convention. As this is a widely ratified convention, with 147 ratifications so far, most of the countries follow its procedures and many States issue endorsements based on the certificates issued by other member States. However, there are certain problems in the system such as fraudulent practices, which shall be covered in the next section.

Meanwhile, there are also some trial plans to combine the two, such as what Liberia is doing now. This is a test project that tries to employ a single document for both identity and certificates. This, as will be seen, is considered to be the solution to many problems currently experienced in the identification and certification of seafarers.

2.5. Problems and implications

As the importance of documents and certificates increases, fraud and forgery also escalate. Fraud is a significant problem in the shipping world, especially where most

of the crews come from developing countries. Sometimes, it is really hard to prevent it from happening, as the people involved have rarely any other choice. For example, a person who has problems in earning a living for his family may do anything to get a job, and if he does not have enough qualifications, he may gladly pay for a forged document or certificate of competency.

2.5.1. Fraudulent practices

The problem of fraudulent certificates has been stressed and focused upon by IMO, after commissioning a study in this respect, done by the Seafarers' International Research Centre (SIRC) in 2001. The study shows that there has been evidence of fraud in the CoC or other documents in all visited countries. The research paper categorizes fraud in two major classes: fraud in the certification process and forgery of the certificate itself. The former results in an incompetent person obtaining a genuine certificate, while the latter result in a forged certificate being produced and used by a seafarer.

Obviously, to solve this problem, both sources of fraud should be combated. This means besides strengthening the documents against forgery, there should be a set of well-developed administrative measures in place to prevent unscrupulous employees from fraudulently issuing genuine certificates to incompetent persons. Nevertheless, relevant authorities can make forgery impossible or very hard to achieve by strengthening the documents.

This applies to any important document, including SID and CoC. By choosing secure and hard to forge documents, the issuers can assure immigration authorities in other States of the true identity of the seafarers, as well as the credibility of their documents, thus giving seafarers more chance to get their rights, including shore leave.

2.5.2. Security

As mentioned above, in large societies, one needs to prove one's identity by presenting valid documents. This becomes a vital necessity in circumstances where security is a major concern. Nowadays, it is quite common to doubt anything on a vessel if a seafarer does not present the necessary SID or CoC documents on request. While other modes of transport are already considered to be unsafe due to security threats, the shipping industry is also under close scrutiny by the security authorities.

So, the credibility of SIDs and CoCs is essential for all relevant authorities, such as Port State Control, Flag State inspectors, shipowners, etc., to prove that a vessel is being run by a competent crew who can safely and securely perform their tasks.

Chapter 3

The change

As described in the last chapter, the importance of identification and certification of seafarers in the shipping business is to be seen in conjunction with specific problems. So, it is expected that the responsible entities come up with solutions to the problems. To this end, IMO and ILO are the ultimate accountable entities, where IMO is more focused on the certification of seafarers and ILO interested in seafarers' identification. In fact, IMO has a major concern about fraudulent practices in the certification of seafarers. On the other hand, with its unique position in labour related issues, ILO has a special focus on seafarers' affairs. Although ILO had already adopted a convention for seafarers' identification in 1958 (the C108 convention), yet they decided needed to come up with an update, to solve the shore leave and other security related problems for seafarers. Thus, IMO and ILO initiated the change.

3.1. The driving forces of change

Problems in the identification and certification of seafarers are important driving forces of change. However, existence of problems is not the only factor that has necessitated the change in this field by IMO and ILO; in effect, several other causes have accelerated the change, which shall be covered here.

3.1.1. SIRC report

After receiving reports about the observed fraudulent practices in documents related to seafarers by its secretariat, IMO decided to have research done to identify the dimension of the problem. The outcome of the research, which was done by the Seafarers' International Research Centre (SIRC), caused a great impact and gave the States a good incentive to change the current system of issuing SIDs and CoCs.

The SIRC report clearly shows that fraud is a major problem in the shipping industry. It says: "Evidence of fraudulent practices was found in respect of all certificates issued in accordance with chapters I to VI of the STCW-95 convention" and "A survey of seafarers (n=1,105) from six of the largest labour supply countries … found nine per cent of respondents reporting direct or indirect experience of fraudulent certificates." The report also suggests that "The existing format and security measures of certificates of competency and other documents issued in accordance with STCW-95 Convention are inadequate." (Seafarers International Research Centre, 2001, pp. 2, 3, 4)

Therefore, something had to be done to solve these problems.

3.1.2. September 11

The incident of September 11 in the United States affected virtually everything in the world. The most important upshot for seafarers was a much more stringent policy regarding shore leave. After the incident, officials in the USA decided to demand visas for seafarers (of nationalities which need a visa to enter the US) to go ashore. This actually meant "no more shore leave in the US ports" because it was virtually impossible for seafarers to go to a consul and request a visa for each voyage to the USA, while they rarely have a fixed and predefined itinerary. This caused major problems for seafarers, as it is vital for them to go ashore after staying and working in the confined area of the ship for a long time.

9/11 caused a major change in the shipping world, regarding security. In harmony with many consequent security measures after September 2001, the new security instrument called the ISPS Code, which is one of the fastest instruments ever developed by IMO, entered into force to try to raise the security level onboard vessels and in port facilities. One of the issues addressed by the code, which is relevant to this dissertation, is a supplementary measure introduced in conference resolution 8 (dated 12 Dec. 2002), inviting ILO to continue the development of a SID instrument as a matter of urgency. (International Maritime Organization, 2003, pp. 134-135)

On the other hand, the US congress directed the US maritime administration to negotiate an international agreement "that provides for a uniform, comprehensive, international system of identification for seafarers" in a measure signed into law (PL 107-295) on November 25, 2002. This finally led to the adoption of the ILO C185 convention (International Labour Organization, 2004).

Moreover, after such an incident, everyone thought something should be done, even if the acquired measures were not pervasive and convincing. Thus, something was to be done to rectify security threats in all transport sectors, including shipping. As identity forgery is one of the most primitive issues relating to terrorism and many other unlawful acts, seafarers' identification was a good topic to focus upon.

3.1.3. Technology

Another powerful driver for change is the availability of new technology in IT and biometrics. Today, the use of computers and peripherals makes it possible to create more secure documents. Besides, while biometrics has long been used manually, the recent integration of IT and biometrics gives us the possibility to authenticate people by using machines.

"IT" is a very dynamic technology. It has been improving at a surprising rate, which is second to nothing in the whole world. Day after day, innovations introduce new ways of doing things and open new horizons in this technology. This trend causes the price of IT equipment to fall over very short periods. Talking about integrated IT/biometrics applications, factors such as advancements in IT, availability of information about it and continuous price reductions have made it feasible to think about a solution of this kind for the identification and certification of seafarers.

On the other hand, the application of biometrics and IT in other sectors such as aviation has encouraged the shipping industry to contemplate the use of these technologies. Aviation has already started to use biometrics to automatically authenticate its workers, and it seems to have been successful. Although the two sectors are not identical, they have many similarities and thus, the successful application of this technology in aviation has led to the perception that it could also be successful in the shipping business.

3.1.4. Political situations

Various political situations in the world have also contributed to necessitating the change. Even though it has rather a unilateral approach in dealing with certain issues, the USA plays a major role in world politics. As an example, one could refer to the consequences of the 9/11 in the world, where an incident inside US territory and in another sector, i.e. aviation, led to widespread changes in the transport industry, including the inclusion of biometrics in visas and passports and the adoption of a new security instrument by IMO (the ISPS Code) which has now entered into force.

In fact, there has been a strong influence by the USA over the international community during the past couple of years, to enhance security measures in different fields, including the shipping industry. One of the measures in this sector is to improve the identification and certification documents for seafarers.

On the other hand, despite their active role in the industry, many developing States have little say in the international fora. This leaves the international community unaware of their requirements and desires, and also opens the way for States such as the USA to influence the others and lead the whole community in a certain direction.

In these situations, the need for change felt by some States could easily be developed as an international necessity. This is also true of changes in seafarers' identification documents. In addition, the importance given to this issue by the G8 summit in Kananaskis and Evian supported the change even more. (Doumbia-Henry, 2003, p. 133)

3.2. The change

Having considered the needs for change, it is time to focus on the change itself, which was initiated by two major players; IMO and ILO. However, these two have acted in different ways.

IMO, being aware of, and very much concerned about the problem of fraudulent practices in the certification of seafarers, suddenly encountered the more important issue of security, which was given priority over all the other activities of IMO. As a result, it decided to transfer the job to ILO to find a solution for seafarers' documents.

On the other hand, ILO has had its own concerns regarding the refusal of shore leave and the professional movement of seafarers, which had deteriorated after 9/11. So, it decided to amend the C108 convention about seafarers' identification documents, but ILO did this in its own way; i.e., although IMO had favoured the inclusion of CoC, this never happened in the solution coming out of ILO, mainly because of the time factor.

3.2.1. IMO strategy

While IMO mostly has relied on the outcome of the ILO discussions, it has also tried some other measures to prevent or combat fraudulent practices in seafarers' certification. The STCW subcommittee at its 33rd session suggested parties follow the format of certificates in section A-1/2 and guidelines in section B-1/2 of the STCW code for the issuance of certificates. It also urged parties to design certificates so that they are expensive to forge.

The IMO website is also equipped with a certificate verification facility, which is a useful tool for the exchange of information about certificates among States. Besides, MSC has produced several guidelines on anti-fraud measures, such as MSC/Circ.1089 and MSC/Circ.1090 in June 2003, with the focus on prevention, as well as the detection of unlawful practices regarding certificates.

The measures suggested by IMO are mostly related to the detection of forged certificates, as well as some policies to be followed by administrations to avoid such practices as much as possible. However, it should be borne in mind that these are only suggestions, without any enforcement power. These measures include:

- Development of IMO website to provide links to maritime administrations for verification of certificates,
- Development of a national database of issued certificates and giving access to it for appropriate authorities such as PSC inspectors,
- Guidelines on how to strengthen documents by adding security features such as watermarks, use of special papers and inks, use of seals and laminates, etc.,
- Strengthening procedures of issuance of certificates through checks and audits, motivating employees, restriction of access to empty documents, etc.,
- and other measures pursuant to recommendations in the SIRC report.

3.2.2. ILO initiatives

In response to the request from IMO, the Governing Body of ILO, in its 283rd session (March 2002) placed on the agenda of the 91st session of International Labour Conference (held on June 2003) an urgent item to improve the security of seafarers' identification. The Governing Body did this with a view to amend the C108 convention by a single discussion process, which is the procedure normally followed by ILO to come up with a Protocol to a convention. However, the result of the work done by ILO turned into the adoption of a new convention at the 2003 conference.

It took only 15 months from the time the item was included in the agenda to the adoption of the new convention; C185. This is not a normal practice in ILO, as conventions and recommendations are usually adopted through a double discussion process.

Obviously, one of the reasons for this extraordinary procedure is the time pressure on ILO to come up with the new document. The other reason for changing the amendment to a new convention was to enable the automatic denunciation of the C108 convention for a member who has ratified it before the entry into force of the new instrument, as it needed to be freed from some of its obligations before ratifying the new convention.

On the other hand, ILO had long discussions, as well as a questionnaire, which is the normal procedure at the ILO, to come up with amendments or new instruments to achieve a common view of how to deal with the issue of seafarers' certificates. One of the items in that questionnaire was whether information about seafarers' qualifications should (or could) be included in the document or not. This question got 31 affirmative and 28 negative answers, but after all the discussions, ILO decided to avoid inclusion of the information about certificates in the new document.

The main reasons for this were: inclusion of CoC data in the document would cause a delay in the adoption of the instrument, would complicate the issue and would make

it hard to implement. (International Labour Organization, 2003b, pp. 79-84) This shows that under the time pressure and urgency of the issue, ILO has actually compromised inclusion of CoCs.

3.3. ILO solution

Therefore, the outcome was a set of guidelines and recommendations for seafarers' certificates from IMO, and a new convention for seafarers' identification documents (SID) from ILO. To understand this convention, a few important parts of it are highlighted in this section.

3.3.1. The C185 convention

The C185 convention tries to introduce an international identity document for seafarers, which would make SIDs more reliable, while maintaining seafarers' rights. Consistent with its tripartite structure, ILO undertook to make a balance between the interests of governments, workers (seafarers) and employers (shipowners, crewing agents, etc.) by enhancing security, facilitation of maritime commerce and movement of ships and seafarers (professional movement) and the facilitation of shore leave to avoid decent working and living conditions for seafarers.

3.3.1.1. Issuing State

The convention restricts ratifying States to issue SIDs only for seafarers who are their nationals or permanent residents (article 2).

3.3.1.2. Format

The contents and format of the SID are defined in article 3 by giving a model, which exclusively clarifies the particulars to be included. Some other general requirements about material of the card, simplicity, validity period of maximum 5 years,

biometrics to be used, and visibility of information on the SID are also described here.

3.3.1.3. Electronic Database

Similar to IMO's suggestions for CoCs, ILO has also obliged States in its new convention to maintain an electronic database to keep information of seafarers' identity documents. This requirement is mentioned under article 4. Security of the database, protection of seafarers' privacy rights, allowing seafarers to see their individual data fields in the electronic database, accessibility of the information for competent authorities, designation of a permanent focal point to respond to inquiries from the immigration authorities of all member States for verification of the identity documents, and exclusion of authorities from using the database for purposes other than verification of seafarers' identity are the measures considered by the convention in this respect.

3.3.1.4. Quality control

The new convention has a separate article, as well as an annex (Annex III) on the issue of quality control and evaluation of how the whole system works. Quality control requires States to have secure procedures for handling blank and complete identity documents, seafarers' applications and the electronic database.

Article 5 also obliges each State to carry out an independent evaluation of its issuance system, at least once every five years. The results of those evaluations should be made available to all members. This is a significant way of sharing knowledge and experience among States, because it lets all the States know how other States are dealing with the issue and teaches them how to get away from potential problems.

3.3.1.5. Facilitation of shore leave, transit and transfer

Article 6 covers the main objectives of the convention. Here, all ratifying States are obliged to give permission, in the shortest possible time, to seafarers who request to enter the State's territory in certain situations. These include: while a seafarer's ship is in port, if the seafarer wants to join a ship in that territory or transit the country to get to another country where he can join his ship, or any other purpose approved by the relevant authority of the member concerned. The last item leaves the issue open to cover other probable situations as well. Nevertheless, this article does not prevent States from refusing such permission when there are clear grounds for suspecting the authenticity of a seafarer's identity documents or on grounds of public order, health, safety or security.

3.3.2. The chosen card and biometrics

In an innovative style, compared to the C108 convention, ILO decided to use biometrics to bind the document to the seafarer. The application of biometrics is not groundbreaking in the transport section, as ICAO has already started to use facial recognition for its workers, but this is still a controversial issue. Notwithstanding all the opposition, which blames biometrics for invading the privacy rights of human beings, the C185 convention necessitates the use of fingerprints to identify seafarers.

Annex 1 of the C185 convention describes the model for seafarers' identity document. Regarding the document itself, it is stated, "the materials used, dimensions and placement of data shall conform to the ICAO specifications as contained in Document 9303 Part 3 (2nd edition, 2002)…." This document describes the specifications of different travel documents, such as Passports, Visas, and part 3, which covers Official Travel Documents (Cards.) This section contains the technical specifications common to all machine readable travel documents such as physical requirements pertaining to deformation, toxicity, resistance to chemicals, temperature

stability, humidity and light, and incorporates appropriate security safeguards to protect against fraudulent use and forgery.

Further in the annex, there are some necessary security measures such as watermarks, ultraviolet security, special inks, holograms, heat-sealed lamination, etc. and then the data to be included is described in detail. In this same part, the requirement for biometrics is mentioned as: "Biometric template based on a fingerprint printed as numbers in a bar code conforming to a standard to be developed." This shows that the chosen biometrics is fingerprint and the chosen method to store it on the document is barcode. As mentioned above, the standard was not yet developed when the convention was adopted. Therefore, the International Labour Conference, following the C185 convention, adopted a resolution in which the Governing Body was invited to request the Director-General to take urgent measures for the development by the appropriate institutions of a global interoperable standard for the biometric template adopted in the framework of the convention. (International Labour Office, 2003, p. 2)

The result was a choice between two biometrics standards, which were different only in the way the digital biometric information is extracted from the sample; one called pattern-based and the other minutiae-based. As explained in section 4.1.4.1, there are two methods to extract information from a fingerprint sample and make a machine-readable representation (called template) of it, viz. minutiae-based and pattern-based techniques. When talking about the pattern-based method, determination of the template by the geometrical patterns made by the ridges on the finger is meant, whereas in minutiae-based technique, the template is determined by the number and positions of the minutiae (breaks and points of bifurcation) that are found in those ridges. (International Labour Office, 2004, p. 2)

Obviously, one of the two had to be chosen and the Governing Body of ILO finally selected the latter (SID0002) as the standard to be used in its 289th session on 26th of March 2004. (The International Labour Organization website, 2004)

On the other hand, regarding the document itself, there was an examination of the two available options throughout the discussions in the conference; a document with an embedded processor (microchip) or Integrated Circuit (IC), i.e., a smart card, or a simpler document without a chip, i.e. a normal card? The decision was finally made to use the simpler document.

So, according to the standard chosen by ILO, two-finger minutiae-based biometric templates of the seafarer to whom the document has been issued, shall be printed on the document as numbers in a two dimensional bar code. The barcode has enough capacity to store additional information such as personal identification data, issuer, expiry date, and some other relevant information.

3.3.3. Ratification and entry into force

Like its ancestor, C108, the C185 convention requires two ratifying States for entry into force. As described in article 12 of the convention, C185 will enter into force "six months after the date on which the ratifications of two Members have been registered with the Director-General." This may seem a good way to have the convention in force as soon as possible, but the requirement for only two ratifications for entry into force of the convention is contentious. In effect, if the convention enters into force with only a few ratifications, it could be seen as a bilateral or multilateral agreement, rather than a widely accepted instrument. This suggests that entry into force is not the definitive factor for a convention.

When talking about international law, it should be taken into account that there is no international police, thus no one can enforce rules and regulations at the international level. The law of the land is the supreme power in each territory, which implies that only individual governments can enforce regulations inside their jurisdiction. Therefore, to have a successful international regulation, the only way is to have as many States accept and adopt the law in their national legislation as possible.

Considering the above-mentioned situations, a successful convention is one with the highest number of ratifications. However, some countries play a more important role than others in the shipping industry, depending on the specific issue concerned. For example, big Flag States have a crucial function in the registration of vessels, while some Port States have a significant position in the shipping business. To have a successful convention, the role of these States should also be considered. This suggests that both number of ratifying States and their positions in the business are significant.

Thus, the C185 convention could be a successful instrument if more States ratified it, but the success would be guaranteed if the ratifying countries include major States, such as the USA, which has a considerable position in the issue of identification of seafarers, as well as security in the shipping industry.

3.3.4. Evaluation

Even though the C185 convention is a good step forward, it does not seem to have been successful so far. Now, after 15 months from the consensus-based adoption of the convention, only three ratifications are registered; by France, Jordan and Nigeria. This signals a problem; otherwise, the States whose representatives agreed upon the convention would not fail to ratify it.

One of the major problems with the C185 convention seems to be the position acquired by the USA. The US State department has formally eliminated crew list visas since July 2004, reiterating "its objections to the ILO's seafarers' identity card as a potential substitute for the individual entry visas now required of mariners calling at US ports." (McLaughlin, 2004.) This means that seafarers who want to take leave ashore must request a visa and obtain one through the consular process before their travel to the USA. On the other hand, the banning of the ILO C185 convention by the US State department and clear indications that the US will not

ratify the convention, take away potential incentives of other States to ratify the convention.

The US State Department justifies its denial of the ILO proposed document by reasoning: “it is likely to take years for such a document to be developed and adopted widely” and insisting on the need to interview each visa applicant personally for security purposes. (“US insists,” 2004, p. 1) This makes a loop between two interrelated problems against the success of the convention; States do not ratify the convention or accept the new identity document as it is not globally accepted, and it is not globally accepted because States do not ratify the convention or accept the new document.

There are also certain aspects in the convention itself, which are potential obstacles. For example, the convention obliges States to issue identity documents only for their national seafarers. This would demand all States, even non-maritime ones to issue maritime documents, which might not happen.

As a matter of fact, refusal of including certificate information in the document is a major shortcoming of this convention. Without information regarding certificates of the seafarer, the SID is merely another identity document. This is actually one of the criticisms made by the US State department against the ILO C185 convention. Lack of any link between seafarers’ identity and their qualifications has the potential of making the SID non-credible; just consider a SID issued by a State for seafarers who have all their certificates obtained from another State. In this case, who is responsible to ensure the person is really a seafarer? Even if seafarers’ certificates were demanded by the issuing State, the next question would be: “Does the issuing State have enough competence to check validity of those documents?”

The suggested database in the C185 convention also has some vague points. A clear example is the requirement to avoid inclusion of seafarers’ date of birth in the database. This can cause problems with respect to seafarers with common names.

Chapter 4

Technology

To appreciate the situations regarding SIDs and CoCs and to evaluate the solution proposed by ILO convention C185, one needs to understand the technology involved. Talking about biometric identification solutions, one should deal with both biometrics and card technology. On the one hand, biometrics gives us the possibility to authenticate people using their biological or behavioural specifications. On the other hand, the information needed for this purpose should be stored on a medium that provides reliable access to the information. In fact, card and biometrics technologies complement each other and both need to be examined for the purpose of this dissertation.

4.1. Biometrics

To start the discussion about the biometrics, there should be a clear definition of it. Biometrics means the identification of an individual based of his or her distinguished physical or behavioural characteristics. (Bolle, Connell, Pankanti, Ratha, & Senior, 2004, p. 3)

4.1.1. Background

The basic task to perform is authentication, which has long been used by human beings, though in different ways. In this context, authentication means recognition of

a genuine person to access a right. Actually, authentication is needed whenever a person tries to use a service. The service can be a facility to attend, a resource to gain access to or any other privilege to attain. For a long time, authentication of people has been a requirement on certain occasions. For example, to pass a border or to board an airplane, everyone should produce a document as proof of identity.

Documents have been, and still are widely being used for authentication. However, application of the documents has had its problems. In a document-based authentication system, it seems to be easy to impersonate people by illegally acquiring a document. On the other hand, forgery could happen by modifying the information in the document. To prevent this, it was decided to add some other information in the document, such as a picture of the holder of the document. Security features such as watermarks and holograms were also added to documents to prevent fraud. Yet they were not strong enough and fraudulent practices by lawbreakers and criminals challenged the whole system through successful impersonations and forgeries.

Application of secret knowledge such as passwords and phrases for authentication was the next step, but this could not solve the problem either, since it was still possible for crooks to unlawfully acquire the information and use them as a successful disguise.

Then the industry decided to find a solution. The solution was an innovation, but its application for ordinary authentication was quite new. Biometrics had already been in place for *negative authentication*, i.e. to prevent known criminals from achieving their goals by preventing them from using a service they were not eligible to use. This is done by obtaining fingerprint samples from known criminals and keeping them in a database. Later on, when someone tries to access an important service, his or her biometric sample is compared with the database samples to see if there is any correspondence. It is also possible to trace criminals whenever a crime happens; by

comparing fingerprint samples obtained at the scene (called latent) with the database samples.

However, in the new solution, biometrics is used for *positive authentication*, which means to authenticate non-criminals to use the services they are eligible to use. Later on, as this coincided with the evolution of IT and microelectronics, the solution has turned out to be electronic biometrics.

4.1.2. Authentication methods

Authentication methods are based on three major modes: Possession, Knowledge and Biometrics. In possession-based authentication, identity is approved upon by holding a key or document or any other physical proof of identity, which is "*something you have*". This method is used in systems which control access to services using documents such as passports, ID cards, etc. The key can be shared, lost, stolen or even duplicated in this method, which all oppose the security requirements.

In knowledge-based authentication, a secret key or code or phrase, which is common to the person and the authenticating entity is the key for successful authentication. This is "*something you know*." User IDs/passwords used in computer systems are of this kind. The piece of knowledge used in this method can also be shared, or guessed by an intruder or even forgotten.

However, when authentication is based on biometrics, the system deals with "*something you are*"; i.e., a unique biological characteristic, which is permanently bound to the individual person, such as a fingerprint or iris. Contrary to the other methods, the biometric identifier cannot be shared, lost or stolen and is not easy to forge.

In the above sequence of authentication methods, the level of security steps up by moving from possession towards biometrics. To make authentication systems even

stronger, it is possible to employ a combination of two or more modes. For example, use of credit cards along with a PIN code, which is common in banking systems, is a combination of possession and knowledge.

4.1.3. How biometric authentication works

Biometric authentication is a multi stage process. It is based on the comparison of a live on-the-spot biometric sample of the person, with a previously obtained sample, which is already stored in a database. Therefore, the first step is biometric enrolment, in which the biometric sample of an individual is obtained and stored in a database. This is normally done by scanning a biometric sample and converting it to a digital format. Then the information representing the biometric sample, as well as the other personal information of its owner is stored in a database.

The next step is to get a biometric sample of the person at the time of authentication. The sample should then be digitized the same way as done at the enrolment stage, so that a machine-based comparison could be done. This comparison is the authentication stage, which gives us the result. The result of a machine-based authentication process might not be a direct yes or no; it usually gives us a probability of possible match between two (or more) biometric samples.

4.1.3.1. Identification vs. Verification

While authentication is the basic operation in both methods, *identification* and *verification* are two different concepts. Identification happens when a person presents his or her biometrics and the system should figure out identity by comparing this biometric sample with all the samples in the database. On the other hand, in a verification process, the person claims an identity and then presents a biometric sample to prove that claim. The system will then compare the presented biometric sample with a corresponding sample of that same person in the database and approve or reject the claimed identity. In fact, identification is a pure biometric measurement,

while in verification, a unique identifier is used to distinguish the person before dealing with biometrics.

The two methods also have some differences in their implementation, application and quality.

Biometric identification

Identification is a more complicated process, because for each authentication, the system should search the whole database to find a similar biometric sample. The result of an identification process could be a multiple match, rather than a single one.

On the other hand, identification needs a centralized database of all biometric samples, as the system needs to have access to all biometric samples to search and find similar sample(s). This means the authentication system should always communicate with a central database.

There are two different categories of identification: positive and negative. Positive identification means to find out if the person is enrolled in the system. This is usually done to authorize people to access a service. Negative identification, on the other hand, means to make sure the individual is not enrolled in the system. A sample application of this method is to detect wanted criminals and prevent them from accessing a service.

Biometric verification

This method simply involves the comparison of two biometric samples. The result of a verification process is a probability of the two samples belonging to the same person. In biometric verification, the need for a centralized database is not vital. This suggests that besides a centralized database, the database could be spread over individual documents. In other words, the enrolled biometric sample of each person can be stored on his/her document to be used by the system whenever the person is being authenticated. This is a good option for situations where accessing a

centralized database is not possible or economically feasible, e.g. onboard a vessel on the high seas.

4.1.3.2. System Errors (FAR, FRR)

While the system is performing authentication, two errors may occur; *false acceptance* of a person who is not enrolled in the system or *false rejection* of a person who is genuinely enrolled in the system. The number of these incidents compared to the total number of authentications is considered as a factor to measure the accuracy of the system. There are two such factors: False Accept Rate (FAR) and False Reject Rate (FRR.) In a system with the value of 1% for FAR, 1 person out of every 100 may be falsely authenticated. Similarly, a system with a value of 10% FRR may falsely reject 10 out of every 100 persons being authenticated.

These two can be adjusted by setting some parameters in the software by the system administrators. When higher levels of security are required, they usually set the authentication systems in a more stringent mode to lower the probability of false authentications. This can be interpreted as: the biometric matcher will compare the samples more precisely and will reject the presented sample upon finding any difference. Thus, such a system needs a lower FAR. However, as FAR and FRR are two interrelated factors, setting the FAR at a lower level will result in a larger FRR. This is because the extraordinary precision will cause genuine persons to be more frequently rejected upon minor variations in their biometric samples.

In high security applications, FAR is usually more important than FRR. This may be due to the different outcomes of each parameter; having a higher FAR means a higher probability of authenticating intruders, which challenges the security of the whole system. On the other hand, a higher FRR may need a repetition of the process or interference of an operator to decide, which decreases the efficiency due to the consequent delays. Therefore, in applications where big populations need to be authenticated in a short time, like an airport, FRR is also significantly important.

In effect, the FAR and FRR are chosen the result of a compromise between security and convenience. The higher the FAR, the more conveniently people are authenticated, while security is, to some extent, sacrificed. On the other hand, the higher the FRR, the more securely the system is working, for the price of a little more inconvenience.

4.1.3.3. Biometric authentication system components

A basic biometric authentication system is composed of three major parts: *Biometric Reader*, *Biometrics Database* and the *Biometric Matcher*.

The Biometric reader is the part that obtains a biometric sample of the person and prepares it for use by the Matcher, and usually has two components: *Biometric Scanner* and *Feature extractor*. ***The Biometric Scanner*** is the actual interface between the system and the person and scans biometric samples. Depending on the type of biometrics, various devices can be used as biometric scanners, such as optical scanners, photographic cameras, voice recorders, or video cameras.

To perform the comparison between biometric samples, the acquired samples need to be converted into a suitable format. The reason is the existence of extra information in a raw biometric sample, which will not be used in the authentication process, and should be omitted from the information given to the Biometric Matcher. This is done by the ***Feature extractor***. Therefore, only the features that are useful for the authentication process are extracted from the sample and stored in digital format.

The Biometrics Database is a place where biometric samples obtained from the individuals at the time of enrolment are stored. Depending on the chosen authentication method, this can be a centralized database or a decentralized one. For biometric identification, the database should be centralized, as the system needs to access all samples and find matching samples among them. For biometric verification, the database can be spread over all the issued documents. This is because the live sample should be compared only with the enrolled sample for each

person, which can be stored in his/her document. All these documents together will then form a decentralized database.

The Biometric Matcher is the core of the system, as it performs the most important part of the process, which is the comparison and all the calculations required to accept or reject an individual. Having access to the biometric database and the live biometric sample, this component can compare samples using its algorithms and come up with the result, either a few probable matching samples (for identification) or a single probability rate (in the case of verification.)

4.1.4. Biometric identifiers

There are several biometric features in the human body or behaviour that can be used to identify people. To be used for biometric authentication, biometrics should have certain specifications: (Bolle et al., 2004, pp. 5-6)

1. *Universality:* Everyone should have the biometric characteristic
2. *Uniqueness:* There should be no two persons with the same biometric characteristic
3. *Permanence:* It should not vary over time
4. *Collectability:* It should be possible to measure the biometric characteristic by obtaining a sample of it

Acceptability of employing the biometric identifier among people is also a significant factor, although this varies depending on the time and place.

Biometric characteristics are of two major types: Physiological and Behavioural. When dealing with physiological biometrics, the person does not need to do anything but present the biometrics to a sensing device, such as putting a finger or hand on a scanner or looking at a camera. In behavioural biometrics, the person should consciously do something, such as saying something or signing, etc. Among

different biometric identifiers, some are mature and used more widely than others, which will be shortly described.

4.1.4.1. Fingerprint recognition

After touching a surface, traces of the fingers or fingerprints may remain on the surface. This is because the skin in the inside surfaces of hands and feet contain minute ridges and furrows between them. Human fingerprints have a feature that makes it a good identifier for biometric authentication, which is uniqueness. There are no two persons in the world, even identical twins, with the same fingerprints. Therefore, it is possible to authenticate people based on their fingerprints.

The fingerprint has been used for a long time. There is proof that the Chinese were aware of the uniqueness of fingerprints 5,000 years ago. (Bolle et al., 2004, p. 31) Later, in the beginning of 20th century, law-enforcement bodies started to use fingerprints for negative authentication of criminals. This was a manual process until IT allowed electronic fingerprint authentication.

There are two approaches for matching fingerprint samples: image techniques and feature techniques. In image techniques, sample images are compared using different optical correlation methods, while feature techniques extract certain important features from the sample. The extracted features are then recorded in a way to accurately represent the sensed biometric sample. Important features in a fingerprint are ridge endings, bifurcations (where a ridge is divided in two), and individual ridges. These features are also called minutiae (see Figure 1.)

a: ridge ending
b: bifurcation
c: independent ridge
d: ambiguous ridge ending / bifurcation

Figure 1 – Fingerprint features

Source: Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). Guide to biometrics. New York: Springer-Verlag

Considering a fingerprint sample in a two-dimensional XY chart, each feature can be located using the X and Y-axes. The type and direction of the features can also be recorded by using numeric codes. This method can result in a digital representation of the sample. As an example, the position and angle of the features in each fingerprint sample can give a numeric representation that corresponds to the sample (see Table 1.)

Table 1 – A minimal representation of fingerprint features

X	Y	Θ
x_1	y_1	θ_1
X_2	y_2	θ_2
⋮	⋮	⋮

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

There are different ways to scan fingerprint samples: Optical scan, Thermal scan, Ultrasound and CMOS. The fingerprint is a mature biometric identifier with a relatively low cost and good accuracy, but in practical terms, it suffers the negative image of being used by law-enforcement bodies to authenticate criminals.

4.1.4.2. Facial recognition

Facial recognition is a familiar concept for human beings. It is common practice in daily life to recognize people by looking at them and comparing their faces with the reference picture already in mind. For more official applications, pictures are used as

the reference for authentication, such as in passports and ID cards. There are different methods for scanning face images: single image (digitizing images), video sequence, 3D image, near infrared (for poor lighting conditions), etc.

To perform the matching, face recognition systems use two methods: appearance and face geometry. The first method reduces the amount of detail in the image and then performs a comparison between the two samples. Face geometry, on the other hand, extracts some features from the face image and then makes a numeric equivalent of it by calculating their respective positions.

Common to both methods is that after capturing an image, the system should detect the face in the image before it can proceed to other stages. Images can be captured with or without knowledge of the person being authenticated. Cameras can be placed at the check-in counters, or where people usually pay attention, such as a red flashing light above a clock at the top of an escalator or on top of a metal detector at the entrances. The best method is an image captured in tightly controlled conditions, where distance and lighting are flexible and can be adjusted, as they should be.

Facial recognition is considered as an unobtrusive biometric identifier with relatively low cost and moderate accuracy, but certain challenges stand facing it. Changes in physical appearance of face while doing different activities or due to make-up, wearing glasses or intentional disguise may cause problems. In addition, imaging conditions such as lighting, distance, obliqueness of the object, etc. can prevent the system from functioning correctly. Compressed images using compression techniques for faster data transmission may also lose some details that are vital for matching facial samples.

4.1.4.3. Voice recognition

The voice human beings use is dependent on physical characteristics such as vocal tract length, nasal tone, cadence and inflection. Nevertheless, voice is considered to

be a behavioural biometric identifier, as it also changes due to the different practices and situations of a person throughout life.

There are different methods for performing voice recognition: fixed text, where the person reads a defined word or phrase already recorded at the time of enrolment, text-dependent, in which a text phrase displayed by the system should be read, text-independent, where the system checks identity regardless of what is said, and conversational, in which the system asks some questions and demands correct answers from the right person. The last one seems to provide the highest level of security, as both voice and knowledge of the person are being matched.

Voice is not distinctive enough to be used for identification, thus making it more suitable for verification. Nevertheless, it is a very good option for telephony applications. Where remote authentication is needed, voice recognition can provide a cheap solution over legacy devices, such as the ordinary telephone network. As a sensing device for voice recognition, the microphone is the cheapest among all biometrics.

However, voice recognition has certain vulnerabilities to “replay attacks”, variations in the microphone and transmission channel, environment noise, and mismatch of microphones used for enrolment and verification. Sickness, aging, emotional states like stress and mistakes in reading the texts are also problems that may occur in the process.

4.1.4.4. Iris scans

Another unique feature of human beings is the coloured part of the eye surrounded by the sclera and pupil called iris. Iris scanning is an accurate, fast and stable biometric identifier. The iris does not change or distort from sample to sample, except the dilation of the pupil, which is also stable in similar illuminations.

Iris recognition requires the cooperation of the person being authenticated, as the iris should be at a predetermined distance from the camera. After capturing the image, the centre of the pupil is found and then the area of the iris is considered as a matrix of pixels. By giving a value to each pixel based on its phase, a code is generated for each iris, which is then stored in a small memory space (only 256 bytes.)

As the code is not big, it is possible to perform a search in a big database to find a similar code. Thus, iris scan recognition is suitable for identification. However, it is still not mature and cheap enough to be commercially used, except for high security applications.

4.1.4.5. Hand geometry

This method uses the geometric structure of hand and fingers such as length and width of fingers, width and thickness of palm and aspect ratio of palm or fingers. This is not a fully distinctive biometric identifier, and thus it has high values of FAR and FRR. Nevertheless, it is a common identifier, mostly due to its simplicity, very small sample size and the little computations required.

Hand geometry is mostly used for verification and rarely for identification purposes. Although capturing the biometric sample in hand geometry requires effort and the cooperation of the person being authenticated, it is a simple procedure; the palm should be flatly placed on a panel with the fingers outstretched. Then the scanner captures frontal and side images of the palm, which is then used to calculate the required parameters (see Figure 2.)

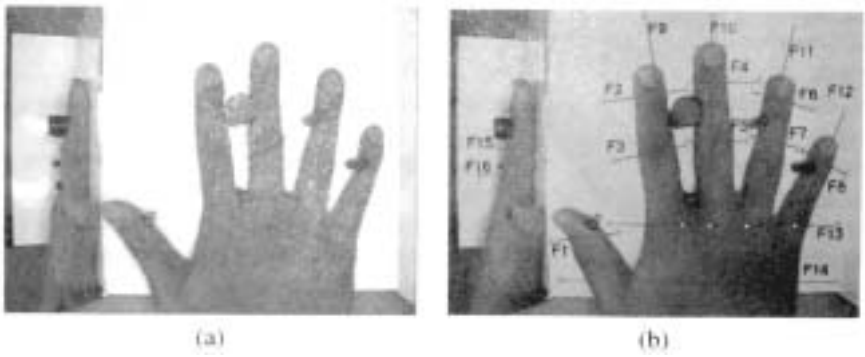


Figure 2– Hand geometry

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

Hand geometry is a good choice to combine with other biometrics such as fingerprints. This combination makes the whole system stronger and more secure.

4.1.4.6. Signature verification

Signatures have long been in place. However, "the way people sign" is something new to be used as a biometric identifier. Use of signature as a biometric identifier has a good chance of being accepted by people, governments, law courts and other legal entities, and commercial transactions. Yet, there are some disadvantages in it; firstly that signatures are easy to forge and secondly, one's signature might not remain permanent, as people can change their signature, as often as everyday! This is in contrast with one of the basic specifications of biometrics already mentioned, i.e., *Permanence*. Furthermore, frequent signatures of the same person are not identical. They may deteriorate due to aging, health conditions, and environmental factors.

The fact that people can choose their signatures also affects uniqueness of this biometric identifier, as selection of the same or very similar signatures by two persons is in opposition to uniqueness. Furthermore, the FAR and FRR parameters can be affected, depending on how simple or complicated the chosen signatures are.

To overcome these problems, On-line signatures can be used as opposed to the Off-line signatures described above. While off-line signatures are scanned from signatures originally on paper, on-line signatures are created using electronic pens. This is a device like a pen without ink, sensitive to movements and pressure on a surface, and connected to a computer. Each movement of the pen on a surface is accurately described by the information sent to the computer. So, if a person signs using this pen, all the information related to the signature is captured.

Using on-line signatures and special pens, it is possible to measure the speed of signing, delays in the process, pen force, number of vertical slope components, number of interior contours, and even angle of the pen, which all together form a good behavioural biometric identifier. Contrary to off-line signatures, on-line signatures seem to be hard to forge and also more stable, as they give priority to the signing procedure over the signature itself. All these can make the signature a better biometric identifier.

Nevertheless, sensing devices required for signature verification are special and expensive, which is a major problem against the practical application of it.

4.1.4.7. Other biometric identifiers

There are several other emerging biometric identifiers under development. While these identifiers still need time to be practically used, some of them can function very well in combination with certain other identifiers.

- ***DNA*** is a very accurate identifier. Every cell of the human body can be used to obtain a DNA sample. Then a code is generated from the sample, which can be used to identify the person. This method is now used in forensic applications mostly for the identification of criminals. One major disadvantage is that identical twins have the same DNA structure. DNA identification is also a slow and expensive process, and considered to invade privacy, as a DNA sample can

provide many other biological specifications of the person, which can be used for unforeseen purposes if revealed to inappropriate authorities.

- ***Retina scan*** uses the shape of blood vessels in the back of the eye (choroidal vasculature.) This is considered to be the most secure biometric identifier, as besides uniqueness, it is permanent and unaffected by anything, actually impossible to change or duplicate, and very accurate. To produce the biometric sample, the person needs to look into an eyepiece and focus on a specific light spot for a few seconds, which is not easy and comfortable for many people. On the other hand, the required contact with the eyepiece can be contrary to personal hygiene.

- ***Thermograms*** use the pattern of heat radiated by the human body. To make a biometric identifier using this technique, images of parts of the body are captured using infrared wavelengths. Some of the more common thermogram biometric identifiers are facial thermogram, hand thermogram, and hand vein thermogram. The advantage of thermograms over visual scans is their independence on illumination; an infrared image can be captured in complete darkness. On the other hand, in facial thermogram recognition, the results are not subject to changes of the face due to facial hair growth, make-up or other skin level changes. As the infrared wavelength captures the features under the skin, it is nearly impossible to forge or change thermogram identifiers. A disadvantage is the high expense of sensors, which make it impractical. Thermogram biometrics can also be used for covert recognition.

- ***Gait***, which is the way people walk, is a behavioural biometric identifier. Although gait is not distinctive, it is useful for low security systems where recognition of people at a distance on video is required. Gait recognition systems use video cameras to capture people while walking and make many computations to measure movements. It should be considered that gait might not stay invariant over time. Such a system is susceptible to the ground surface, viewpoint of the

camera, objects being carried by the person, shifts in body weight and health condition, and clothing of the person being tracked.

- ***Keystroke recognition*** has to do with each person's special typing capabilities. Calculating times between keystrokes and the hold time of each stroke will provide an identifier that could be used for identification, though it is not really individual. As the capture is done while the person is typing some text, keystroke recognition is considered as an unobtrusive method. The system can be text-dependent (fixed message or password) or text-independent (different text each time.) One of the practical concerns regarding this identifier is that some people do not use computers and do not know how to type, thus making the system ineffective for them.

- ***Ear recognition*** is based on the uniqueness of the shape of the ear and the structure of the cartilaginous tissue of the pinna, although it is not proved to be distinctive. The matching approach uses distances of salient points of the pinna from a landmark location on the ear. Ear recognition usually works well in combination with other biometric identifiers such as facial recognition, where both samples can be captured simultaneously.

- ***Lip motion*** is a behavioural biometric identifier. It is based on the motions of lips while the person is speaking. Thus the capture phase is done using a video camera. Obviously, the first task for the system is to find lips in the image. The drawback, thus, is the requirement for good illumination, as the system would be unable to recognize lips in the image in poor lighting. There are different methods for matching, which can be text-dependent or text-independent. Lip motion recognition is considered as the visual equivalent of voice recognition. To give the best results, lip motion can be combined with voice recognition or facial recognition techniques.

- ***Skin reflection*** is a new method. Using near-infrared light, it is possible to measure the reflection from skin. This can be used as a standalone biometric identifier, but an interesting application is to combine it with fingerprint sensors, to prevent forgery in fingerprint recognition.

- ***Body odour*** is different in different persons. Use of dogs to track people shows that it is possible to use odour as a biometric identifier. In practice, when a whiff of the air surrounding the person is sprayed over a spectrum of chemical sensors, each of which is sensitive to certain compounds, the chemical structure of the body odour is captured. Nevertheless, there are obstacles in practical application of this identifier, as body odour varies due to the use of deodorants, perfumes and soaps. Diets and health conditions also affect body odour.

While some of the above mentioned identifiers are good options for application in biometrics, most of them are not mature enough, and thus expensive and uncertain to be actually used. However, future improvements in the biometrics or advancements in other related technologies may make some of them good choices. Nonetheless, scientific research continues to devise new biometric identifiers suitable for identification.

4.1.5. Comparison

4.1.5.1. Biometric features

Biometric identifiers are different in terms of accuracy. As already mentioned, some of them may be more accurate in certain applications, while others might function less precisely. However, accuracy is only one of the many factors that should be considered for a proper comparison among biometric identifiers. These factors include cost, error rate, speed, acquirability, privacy and ease of use.

Table 2 shows a comparison between the six most common biometric identifiers.

Table 2 – Comparison of the attributes of the six popular biometric identifiers

	Finger	Face	Voice	Iris	Hand	Signature
Maturity	very high	medium	medium	medium	high	medium
Sensor type	contact	non obtrusive	non obtrusive	non obtrusive	contact	contact
Sensor size	small	small	very small	medium	large	Medium
Sensor cost	< $200	< $50	< $5	< $300	< $500	< $300
Template size (byte)	< 500	< 1,000	< 2,000	256	< 100	200
Scalability	high +	medium	low	very high	low	high -

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

Maturity plays an important role. A mature biometric identifier is based on a well-studied science and enough technological development. The application of a biometric identifier for a long time lets the industry recognize more aspects of it and find solutions for any potential problems that may occur as time goes by, including human behaviour in response to the biometrics. Thus, a more mature biometric identifier is preferable for practical application. The fingerprint has the highest level of maturity among all biometrics, due to its long history.

The biometric sensor is an important part of each biometric identification system, which can affect the whole process and should be considered carefully. Sensor type can be contact or non-contact. Contact sensors require the cooperation of people and thus are potentially obtrusive, while non-contact sensors are more suitable for populations that are more sensitive to privacy issues. These sensors are also used in covert identification and surveillance systems.

Sensor size is another varying factor among different identifiers. While some sensors like a microphone for voice recognition are very small, others are bigger, like the sensors used for hand geometry. Sensor cost is also a significant factor,

especially for non-mature biometric identifiers. However, importance of this factor changes as technology improvements cut the costs.

A biometric template is the digital representation of a biometric sample. In other words, it is the outcome of a feature extractor, which is stored in digital format. The size of a biometric template does not correspond to accuracy; a bigger template does not mean a more accurate biometric identifier. However, it is a significant factor in the implementation of biometrics, especially in systems that use distributed databases on cards. This is because cards have a limited capacity and can keep only certain amounts of information. As Table 2 shows, the template size of biometrics varies from very small for hand geometry to very big for voice recognition. Template size also affects the comparison methods and hence, speed of the system in checking samples with each other. For this reason, biometric identifiers with big templates are not suitable for identification, as it takes a long time to compare the sensed sample with all the samples in the database.

Scalability addresses the capability of the biometric identifier to be employed in larger populations, without getting high false acceptance rates. This depends on the distinctiveness of the biometric identifier, which helps the system authenticate people in large societies. Generally, as population grows, the number of errors in the system goes up. If this number becomes very big, the identifier is not scalable. Biometric identifiers with low scalability also cause problems in the enrolment process, due to the requirement for handling exceptions. Contrary to the pros of using highly scalable biometric identifiers is their weak acceptability due to privacy issues, because more distinctive identifiers are usually more obtrusive as well. Among the six identifiers described, the iris has the highest level of scalability.

4.1.5.2. Application properties

On the other hand, it is not possible to come up with a universal biometric solution for all applications; properties of the application for which the biometrics is to be

used should also be considered. A good biometric identifier for one application may be very bad for another application. This is due to the different requirements and conditions of each application compared to the others.

Selection of a suitable biometric identifier for a system depends on many factors including population, cultural issues, acceptability of the biometrics, necessity to use distributed databases, available data communications, time factors and costing conditions. All these factors affect the importance of features of the biometric identifier for the specific application.

Table 3 shows the weighting of some features and drawbacks of biometrics in three sample applications: physical access, credit cards, and airport access, which belong to the transport sector. On the left hand side, the potential drawbacks and features of using a biometric identifier are named and in the right hand columns, the weighting of those features for the three sample applications are given. For example, the drawback of requiring cooperation in airport access is higher than that of the others. The reason behind this is that in physical access, the person needs to be authenticated, while in airport access, people get a service for which they have paid and thus, looking at the authentication as an obligatory inconvenience for themselves. For this reason, it is not easy to ask people to cooperate with this system in airport access systems.

Population missing is another factor, which happens when people leave the system due to the inconvenience of employing biometrics. This is not a big problem for physical access, as the population is limited to a group of people who have enough incentive to use the system and must interact with it in the proper way. Quite the opposite, airport access or credit card systems are vulnerable to this problem, as people may easily avoid using the service and try other choices.

Among sampling properties, acquisition time is very important for airport access and physical access, as in these systems, due to the large number of users, any delay can

cause major problems. This is not the case for credit cards, as time usually is not as crucial in using them.

Table 3 – Important weightings for some applications

Importance weighting	Physical access	Credit card	Airport access
Intrinsic properties			
Required cooperation	low	low	high
Social stigma	medium	high	medium
Intrusiveness	medium	high	medium
Population missing	low	medium	medium
Sampling properties			
Inconvenience	medium	high	medium
Required proximity	low	medium	high
Acquisition time	high	medium	high
Failure to enroll	medium	High	medium
Failure to acquire	medium	High	high
1:1 matching properties			
# FA per 10K (when FRR = 10%)	medium	High	high
# FA per 10K (when FRR = 1%)	medium	medium	high
Template size (bytes)	low	High	medium
Technology properties			
Installation cost	medium	High	medium
Continual cost	medium	High	medium
Cost per match	low	medium	medium

Source: Derived from Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

Table 3 shows accuracy by using the number of False Accepts in two situations, depending on the value set for FRR in the system. This is only valid for verification systems, which are based on a 1 to 1 comparison of the sensed and the database samples. The first row addresses systems that are more focused on rejecting fake people, which is suitable for high security situations. In other words, the system is working more precisely or at a higher security level. The second row refers to systems set to accept genuine people, which is the case when the system is set to work in more secure environments. This is usually done when the system faces few security challenges.

The weighting considers the number of genuine people rejected in the above-mentioned situations. When the system is focused on rejecting fake people, the number of False Accepts is vital for high security applications such as airport access, as the risk factor is very big, but it has a moderate importance for credit cards and physical access systems, as the amount of damage is usually limited if a False Accept happens (a few hundred dollars in credit cards.) When the system is more willing to accept genuine people, the number of False Accepts is still important for airport access and credit card systems, as they use this setting for normal conditions, where large number of False Accepts would cause security problems.

As it can be seen, template size has a high significance for credit cards, as the template should be stored on a limited storage, i.e. the card memory. The last section of Table 3 shows that cost is not a matter of real concern for physical and airport access, compared to the high value of the assets in the application, or the levels of security that justify high costs.

4.1.5.3. Mismatch calculation

One of the methods used to evaluate biometric identifiers for different applications is mismatch calculation. This is done by calculating a number that shows how much the biometric features disagree with the application requirements; in other words, how much the drawbacks upset the application. Calculation of this number needs a comparative evaluation of drawbacks in different biometric technologies. Table 4 shows these values.

The values in Table 4 are mostly descriptive, which cannot be used in a numeric procedure, such as the calculation of a mismatch score. Thus, they need to be converted into numeric values. On the other hand, there should be a relationship between the importance of biometric features in an application (Table 3) and the drawbacks of a biometric identifier (Table 4.) For this purpose, the values of “1”, “3”, and “10” are assigned to “low”, “medium” and “high” respectively. For “1:1

matching properties", the numbers are calculated using the following formulae, considering v as the number in Table 4 and C as the resultant value:

#FA per 10K (FRR=10%): $C = \max(0, 10 * \log_{10} v + 10)$

#FA per 10K (FRR = 1%): $C = \max(0, 10 * \log_{10} v)$

Template size: $C = v / 100$

Table 4 – Approximate values for drawbacks of various biometrics in general (not application specific)

Drawbacks	Finger	Face	Voice	Iris	Hand	Signa-ture
Intrinsic properties						
Required cooperation	high	low	low	medium	high	high
Social stigma	high	low	low	medium	medium	low
Intrusiveness	medium	low	low	medium	medium	low
Population missing	low	low	medium	low	medium	medium
Sampling properties						
Inconvenience	low	low	low	medium	medium	medium
Required proximity	high	low	low	medium	high	high
Acquisition time	low	low	medium	medium	medium	medium
Failure to enroll	medium	low	medium	high	low	low
Failure to acquire	medium	medium	medium	medium	low	low
1:1 matching properties						
#FA per 10K (FRR=10%)	0.1	10	300	0.001	10	300
#FA per 10K (FRR = 1%)	10	1,000	1,000	0.1	100	1,000
Template size (bytes)	500	1,000	2,000	250	100	200
Technology properties						
Installation cost	low	low	low	medium	medium	medium
Continual cost	low	low	low	medium	low	low
Cost per match	medium	low	low	low	medium	Low

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

Then two columns are lined up for one application and one biometric identifier and the mismatch scores for each feature are calculated by multiplying the two values. As an example, Table 5 shows how this method works for "physical access" and "fingerprint".

Table 5 – Computing a mismatch score by assigning numeric values and summing. W = weight, P = penalty and X denoted product (W x P).

Importance weighting	Physical access		W	**X**	P		Finger
Intrinsic properties							
Required cooperation	Low	→	1	**10**	10	←	high
Social stigma	medium	→	3	**30**	10	←	high
Intrusiveness	medium	→	3	**9**	3	←	medium
Population missing	low	→	1	**1**	1	←	low
Sampling properties							
Inconvenience	medium	→	3	**3**	1	←	low
Required proximity	low	→	1	**10**	10	←	high
Acquisition time	high	→	10	**10**	1	←	low
Failure to enroll	medium	→	3	**9**	3	←	medium
Failure to acquire	medium	→	3	**9**	3	←	medium
1:1 matching properties							
# FA per 10K (FRR = 10%)	medium	→	3	**0**	0	←	0.1
# FA per 10K (FRR = 1%)	medium	→	3	**30**	10	←	10
Template size (bytes)	low	→	1	**5**	5	←	500
Technology properties							
Installation cost	medium	→	3	**3**	1	←	low
Continual cost	medium	→	3	**3**	1	←	low
Cost per match	low	→	1	**3**	3	←	medium
SUM				**135**			

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

As can be seen, the final result is a number that shows the amount of mismatch between the biometric identifier and the application. Obviously, the smaller this number, the better the biometric identifier is for the application.

4.1.5.4. Zephyr charts

One of the techniques used for comparative analysis of biometrics is the Zephyr^{TM} chart. This chart has four factors to consider for various biometric identifiers. Then by connecting the four points for different identifiers, each identifier would have an area covered. The decision on which identifier to choose is then made based on the size of the covered areas. Figure 3 shows an example of these charts for four biometric identifiers: Iris, Finger, Voice and Face, based on four criteria: effort, intrusiveness, cost and accuracy. The criterion to choose the identifier is to get the biggest possible area of A.

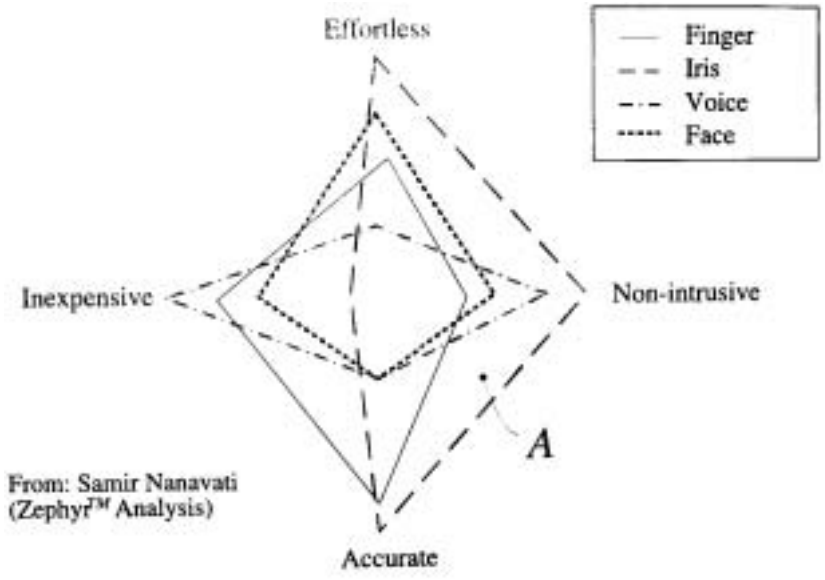


Figure 3 – An example of a Zephyr chart

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

However, it should be noted that this is not a general description of biometrics for all applications in every situation; it is a sample chart, which describes the features for a specific application in a particular population. In effect, each application in specific circumstances will have its own Zephyr chart with different values for the measured features.

4.1.6. Attacks to biometric systems

Like many other systems, biometric systems are vulnerable to attacks from forgers and criminals who try to illegally authenticate themselves in the system or prevent it from functioning. Although attacking biometric systems is not as easy as that of user/password systems, there are several types of attacks that can affect biometric systems in different ways. Nonetheless, they can be prevented, to a large extent, by following suitable measures.

Considering the structure of a biometrics authentication system, one can point out some points of attacks, where attackers may try to start their intrusion. Figure 4 shows the structure of a typical biometric authentication system, as well as the attack points, which are described here.

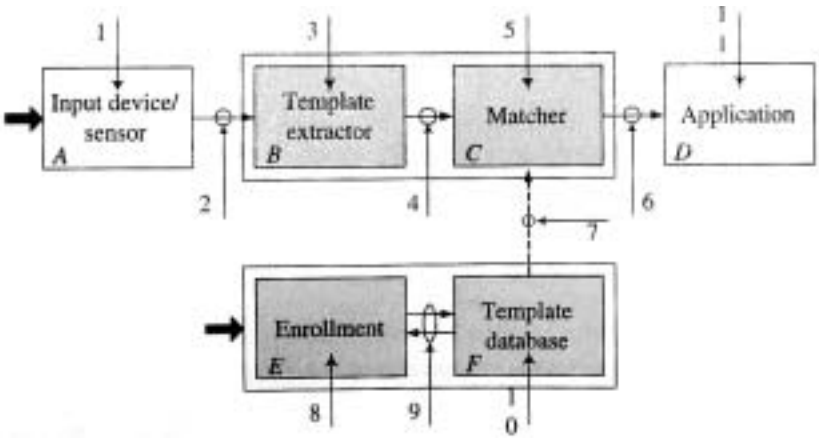


Figure 4 – Points of attack in a generic biometric authentication system

Source: Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

❶ This is the biometric scanner, where biometric samples are acquired from people to be matched against the samples in the database. Three attacks are probable to occur at this point; namely Denial of Service (DoS), coercion, impersonation or replay attacks.

A DoS occurs when the intruder destroys the scanner in order to prevent the system from functioning. This can be done by breaking the scanner, blocking it or disconnecting it from the system. Coercion is when a genuine identifier is presented to the system, but in some unauthorized manner. For example, when someone is forced to put his or her finger on a fingerprint scanner to be authenticated, so that the intruder can access the person's bank account, a coercive attack is happening. Impersonation happens when someone tries to introduce to the system an identity that is different from his or her true identity. To this end, an impostor may use fake identifiers to be falsely identified as a genuine person (positive authentication.) In fact, "the most common method of launching a fake finger attack is to build an accurate three-dimensional model of a fingerprint from a latent fingerprint of a legitimate user." (Maltoni, Maio, Jain, & Prabhakar, 2003, p. 286) Fake identifiers also happen in other biometric methods, such as changing one's voice or altering one's face through simple disguises or plastic surgery.

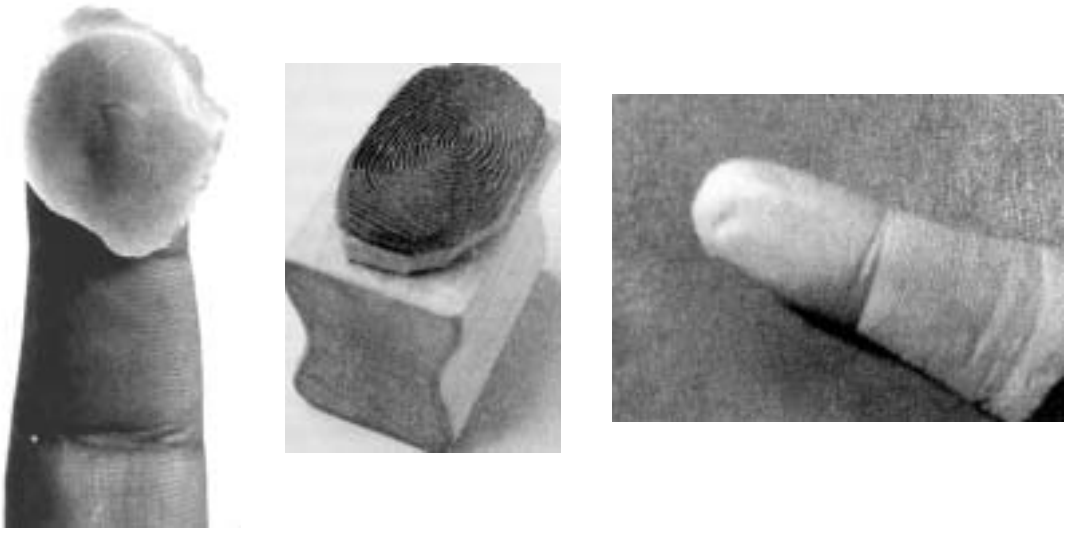


Figure 5 – Fake fingers and fibre used by imposters

Source: ***Left and Middle:*** Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). Handbook of fingerprint recognition. New York: Springer-Verlag, ***Right:*** Bolle, R. M., et al. (2004). Guide to biometrics. New York: Springer-Verlag

Another kind of impersonation involves changing the appearance of a person's biometric identifier, to avoid being identified in a screening system (negative authentication.) Replay attacks, which could also be considered as a kind of impersonation, happen when a previously recorded genuine sample is re-presented to the scanner, instead of using the real biometric identifier to produce a new sample. This is common practice in voice recognition systems where a fixed text should be read to the system for authentication.

However, employing suitable measures can prevent the above attacks. For example, replay attacks in a voice recognition system can be avoided by using variable texts instead of fixed phrases. Fake identifiers can also be recognized by the use of more accurate scanners or a combination of two or more identifiers. For example, regarding the impersonation attacks by using fake fingers, it is possible to use scanners that can detect "liveness", e.g. by making use of thermograms. Another solution for these attacks can be to combine biometrics with "secret knowledge", e.g. by asking a question after the fingerprint is produced to the system, to check if the person is really who he or she claims to be. It is also possible to lower the chance of DoS attacks by making physically stronger scanners. Guarding the scanners can also hinder such attacks, as well as coercive attacks. To detect coercion situations, some measures such as detection of "panic" could also be followed. In the case of fingerprint recognition, there are special scanning techniques that facilitate this. It is also possible to acquire a surveillance video of the transaction, to be further used by law enforcement authorities.

❷ This is the communication channel between the scanner and the feature extractor. Attacks at this point may be replay attacks, by electronically injecting information into the channel, e.g. to the "output" of a microphone.

The solution to this kind of attack can be the application of strong encryption algorithms for data communications, as well as the time-stamp method, in which the two communicating parts check synchronization of their clocks, which is not easy to

achieve for intrusion techniques. On the other hand, such attacks usually send exactly the same data to the feature extractor, which is impossible in practice. As biometric samples vary in different scans, the system would be able to detect perfect matches against previous samples.

❸ This is an attack on the feature extractor itself, by using a mechanism referred to as "Trojan horse." In software systems, a Trojan horse is a program that is able to fool the system by playing the role of another entity. Here, the Trojan horse is disguised as the feature extractor, and can send whatever the intruder wants to the biometrics matcher (C.) As it does not know the information is coming from another entity, and not the feature extractor, the matcher accepts the output of the Trojan horse as a valid input, based on which the rest of the authentication is done.

❹ ❼ These are two other communication channels that connect the feature extractor and the template database to the matcher. Attacks to these channels are aimed at sending unreal data to the matcher, so that it produces the desired result. Where the output data of the feature extractor should be sent to an external matcher, as can happen in the smart cards, this can be a real problem. The application of strong encryption algorithms can also be a solution here.

❺ Attacks to this point are also a kind of Trojan horse. As the matcher decides on the person's authenticity, the attacker can control the matching mechanism by replacing the matcher with a Trojan horse, so that, for example, a positive match result is always produced for a particular person.

❻ This is the point where the result of the authentication process is passed to the application, to grant or deny access to the user. Obviously, by attacking this channel, an intruder can get the desired result; i.e. access the application. However, the problem here can also be rooted in the system design. As in most of the systems, there are certain users with extraordinary rights, which can override the matcher's decision. Such a user is usually required to handle special cases, such as the people

who do not have fingers, in the case of fingerprint recognition, or to overcome a lasting False Reject, by the controlling officer. Obviously, such a special access right is a potential source of misuse by intruders, one way of which is collusion.

❽ ❾ ❿ These points are related to the enrolment process. Each of the three can be attacked to introduce a false template to the system, based on which the matcher checks the validity of the scanned sample. By attacking the database itself, fake templates can be included in the database, so that the fake persons can present their genuine identifier to the system, and be falsely authenticated as genuine users. As this part of the system is not in the forefront, attacks on it are called back-end attacks. In any trial to strengthen the system against attacks, it should be considered that the enrolment part, i.e. the back-end, is as important as the front-end.

⓫ The last point is the application itself, which is the ultimate target of the intruders in their attacks.

There are also other kinds of attacks that aim at several points. For example, a "Hill climbing attack" aims at attack points ❹ and ❻. The hacker starts with sending a biometric sample data to the matcher, and checks the resultant score. Then by repeatedly sending data with slight modifications each time, looks for improved scores until the positive match is achieved.

Attacks to biometrics can always happen. In effect, where cost is not a matter of concern, all identifiers can be threatened by impersonation attacks. However, the technology is continuously improving. As time goes by, commercial biometric companies use better fake identifier recognition techniques and try to rectify the problems. Yet, the hackers may find new ways to attack the system. This seems to be an ongoing challenge, which also exists in non-biometric systems.

In effect, no foolproof biometric authentication system exists at present and probably will never exist. However, this does not mean that biometrics should be avoided.

Like many other technologies, biometric authentication can be both safe and risky, depending on the way it is being used.

4.1.7. Privacy rights concerns

One of the difficulties in the application of biometric systems is the problem of privacy rights. Privacy is "the ability to lead one's life free from intrusions, to remain anonymous, and to control access to one's own private information." (Maltoni et al., 2003, p. 45) Another definition by Anton Alterman, claims privacy to be "a set of personal rights centred on the body as an integral part of the self, including rights to freedom of movement, self-respect, bodily integrity, and privacy, which create a personal *zone* protecting physical and emotional aspects of the self against harm." Privacy is also the right to maintain control over how people represent themselves to others, either in physical appearance or in iconic or indexical representations. (Alterman, 2003, p. 144) Here, indexical representation of a person means representation using the information related to them.

Biometric identification raises the issue of data privacy like other forms of identification. The reasons are: biometric identification is very accurate, especially in the case of the identifiers like iris and fingerprint, the related data is usually stored in interconnected databases, and even the strongest encryption methods are likely to be hacked. Thus, the data collected for biometric identification is potentially vulnerable to abuse. There are three types of privacy-related concerns with respect to biometrics; namely privacy of information, use of information for unanticipated applications (proscription) and unauthorized access to the information.

Regarding the first one, the individuals need to have their personal information protected, as they have interests in it. For example, people with criminal record are not necessarily criminals and thus, such records should not be used to discriminate among people in a positive identification system. Proscription is a major problem in the application of biometric systems, as, for example, it is always possible to make

links between the biometric database and the databases used by law enforcement authorities such as criminal databases. Application of information collected for specific purposes in other applications is a major problem, especially when the system is already in place and the law enforcement bodies insist on it.

The problem of illegal access to information is also a valid argument here, though it is not exclusive to biometrics. As the biometric identification data is stored in computer systems that are usually connected to a corporate network or even to the Internet, it is not impossible for professional hackers to encroach upon the system and access the information. Unscrupulous employees of the controlling firm may also sell the data to lawbreakers or any other entity. Although proper policy setting and choosing strong technical considerations such as the encryption methods can help, they can never entirely solve this problem.

However, there is another aspect of privacy, which is special to the use of biometrics. As human beings are interested in protecting their rights of physical representation such as the way they dress, their presence in public, and their private space at home, they are also concerned about the way they are "indexically" represented, such as the use of parts of their bodies for authentication. The application of biometrics for authentication suggests that people should loose this privacy right, by presenting their body for authentication whenever the system asks them to do so. Added to the above is the issue of religious beliefs, which may make it embarrassing or even impossible to obtain a biometric sample. There are even some allegations that the use of biometric recognition is "the mark of beast" by the so-called "dubious biblical references." (Maltoni et al., 2003, p. 46)

Using biometric samples for identification of people can also invade privacy by releasing extra information that is not needed for authentication. For example, retinal vasculature can disclose diabetes or hypertension (Bolle et al., 2004, p. 223) and HIV-positive cases. (Alterman, 2003, p. 146) Yet, new identifiers such as DNA, if practically used, can reveal much more physiological characteristics.

On the contrary, there is a different viewpoint in favour of biometrics, claiming that use of biometric identifiers can provide higher levels of privacy rights, by enhancing the integrity of the systems holding personal information.

Considering all the above discussion, whether biometrics invades privacy or not depends on how the systems are implemented. In effect, application of biometrics is like a two-edged sword; it can invade privacy, and it can provide privacy. If all the relevant security measures are considered, including the technical aspects and the human element, it can be a good tool to ensure a higher level of security and protection of personal data. Nevertheless, a system with several weak points, such as an unprotected database, open communications with other systems, unsafe encryption methods and unclear policies on who may access the data, can result in serious privacy concerns.

4.2. Cards

As the combination of biometrics and cards can be the ultimate solution for biometric identification with high security and ease of use, and especially for the identification and certification of seafarers, the cards and card technology concepts should also be well thought-out.

4.2.1. Background

The application of plastic cards started in the USA in around the 1950s. (Rankl & Effing, 2003, p. 2) This became possible due to the use of PVC as the body material for cards, which could produce durable and stable cards, compared to paper cards. In those days, cards were mostly used as a status symbol, which enabled the cardholders to pay their bills through their “good name” rather than by cash. Soon, cards started to be used as electronic cash for payments, with VISA and MasterCard leading the way. The first generation was a simple card containing some information such as holder’s name, card number, etc., protected by certain security features to prevent

forgery. Operation of these cards was entirely manual and all transactions needed to be dealt with manually, requiring lots of paperwork. Gradually, the increasing popularity of these cards demanded the industry to make them machine-readable. By doing this, handling costs decreased and sellers and customers could save more time. This also improved the security of the cards and thus diminished fraudulent practices, which were inflicting big losses on the card issuers.

The first generation of such cards employed magnetic data storage technology using a magnetic stripe on the back of the card. It was then possible to store the required information on the magnetic stripe to be read and used whenever needed. Earlier, it was quite common to use a signature for identification, but the introduction of these cards coincided with the use of PIN codes (or numbers) instead of signatures. In a PIN code system, the cardholder should present a secret code to the reader machine, which compares it with a reference number for authentication. As magnetic-stripe cards store the reference number on the card, it is possible to authenticate the cardholder anywhere. However, the PIN code on a magnetic-stripe is accessible to anyone, which can compromise security.

Developments in computer technology and communications made it possible to solve this problem by online comparison of the presented code against the reference code in the issuer's database. This combination is still one of the most common methods used for card-based authentication.

Nevertheless, magnetic-stripe cards have a major weakness; their information can easily be accessed and read by everyone who can access a reader device. Progress in microelectronics in the 1970s enabled card technology to replace magnetic stripes with microchips in new cards, and make them *smart* cards. The first real patent of a smart card was registered in France by Roland Moreno in 1974, yet it took some time until the patent turned into an applicable real card. The field trial of smart telephone cards in France and a pilot project conducted in Germany in 1984 and 1985 showed that smart cards would be successful. By 1990, 60 million smart telephone cards

were being used all over the world, rising to several hundred million in 1997. (Rankl & Effing, 2003, p. 4)

The application of smart cards in mobile phones (GSM) after 1988 also proved to be successful, with over 600 million subscribers in more than 170 countries until now. Banking and payment, though more slowly, have become major fields of application for smart cards as well. The reason behind the delayed use of smart cards in the banking system is the need for more security. The information in a payment card had to be coded using suitable methods, to prevent intruders from accessing the information and making illegal modifications to it. For this purpose, strong cryptography techniques were needed, which came into existence a little bit later on. The French banks were the first to introduce smart bank cards in 1984. Some other countries also started to employ the system, after the specifications for Eurocheque cards incorporating chips was issued in 1996. In the same year, Austria was the first country to have a nationwide electronic purse system. As a joint effort of the three major card issuers (Europay, MasterCard and Visa), the EMV specifications was also an important factor, which contributed to the worldwide application of smart cards for payment (credit cards.)

4.2.2. Card types

Cards are generally divided into three kinds; namely embossed cards, magnetic-stripe cards, and smart cards. To achieve harmony in making and using cards, specific standards have been developed by the International Standard Organization (ISO) for different types of cards. The ISO 7810 standards describe the physical characteristics of the identification cards, which are in three different types: ID-1, ID-2 and ID-3. Smart cards are in the first category, i.e. ID1, which is the most common format for ID cards used worldwide.

4.2.2.1. Embossed cards

This is the oldest method of adding machine-readable contents to cards. By making embossed characters on the card, it is possible to transfer the contents into paper using simple methods (by pulling a carbon copy paper over the card.) However, this simplicity allows the card to be employed worldwide, without the need for any reader device or communication methods. On the other hand, as already mentioned, the huge amount of paperwork is the major disadvantage of this kind of card. Nowadays, embossing is used in conjunction with other card techniques. In these cards, the embossed feature is used only when reader devices and online communications are not available.

4.2.2.2. Magnetic-stripe cards

The next in line is the magnetic-stripe cards. By including a magnetic stripe on the card body, this card is capable of keeping certain amounts of information. The information can then be accessed by pulling the magnetic stripe, manually or automatically, against a scanning head in the reader/writer device. Each card may contain 2 or 3 tracks on which data can be stored and retrieved. This is done by changing the magnetic status of the cells in each track of the magnetic stripe. Tracks 1 and 2 are usually read-only, while track number 3 can be used in the read/write mode. As can be seen in Figure 6, exact sizes and distances are also described in the ISO standard 7811.

The major problem with magnetic stripe cards is that the data can be read by anyone who has a reader device. There are certain measures that can reduce this problem, such as the one used by German Eurocheque cards, which is to store an unchangeable code in the body of the card, to be checked when reading or changing the information. (Rankl & Effing, 2003, p. 17) However, such solutions require special reader devices, which contradicts the standards and may prevent the card from being used globally.

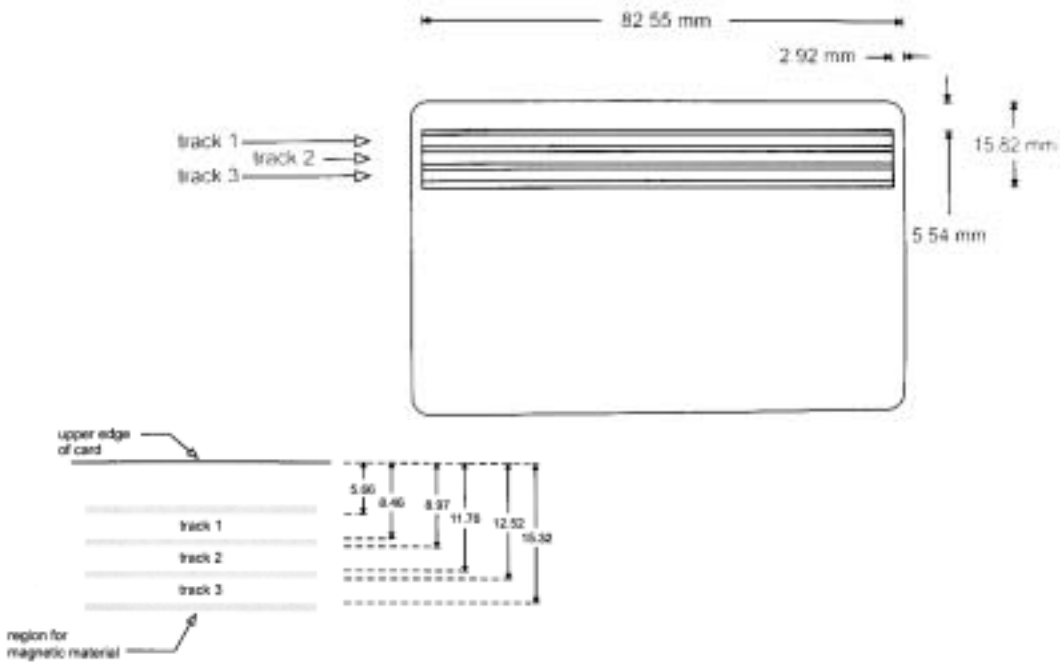


Figure 6 – Composition of the data tracks in a magnetic-stripe card

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

Standard magnetic-stripe cards have a capacity of 1,000 bits or around 125 bytes. This is apart from the read/write section, which takes up to 107 characters. Table 6 shows certain features of the tracks on a magnetic-stripe card.

Table 6 – Standard features of the three tracks on a magnetic-stripe card

Feature	Track 1	Track 1	Track 1
Amount of data	79 characters max	40 characters max	107 characters max
Data coding	6-bit alphanumeric	4-bit BCD	4-bit BCD
Data density	210 bpi (8.3 bit/mm)	75 bpi (3 bit/mm)	210 bpi (8.3 bit/mm)
Writing	Not allowed	Not allowed	Allowed

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

4.2.2.3. Smart cards

Smart cards are the next generation, which have significant advantages over the magnetic-stripe cards. A smart card is made up of an Integrated Circuit (IC) embedded in a card body. The information is stored in the IC, which communicates with the reader/writer devices through its contacts. Smart cards may have physical contacts, or be contact-less, using an antenna to communicate.

Two major improvements are higher capacity and superior measures for security. While capacities continuously increase by the advancements in microelectronics, most smart cards have more than 256 KB (256,000 bytes) memory today, which is much more than magnetic-stripe cards (less than 200 bytes.) The ISO 7816 describes the characteristics of smart cards. Furthermore, because the storage medium is an IC, it is possible to have certain security mechanisms, both on the software and hardware sides, to protect the information and prevent unauthorized access to it. This is in contrast with the magnetic-stripe cards, which store data on a medium that is open to impostors.

Memory cards

Memory cards are a simplified version of smart cards, with more focus on the storage of data. The IC in these cards comprises a memory section and a piece of software that provides addressing and security logic. The security logic is rather simple, mostly to protect parts of the memory from being modified. However, some more advanced methods can be used in this part to encrypt the memory data. Figure 7 shows the typical architecture of a contact-type memory card. As can be seen, the interface with the outside, i.e. the reader/writer device, is through the I/O contact. Control mechanisms are connected to the IC using the ‘ctrl’ contact. The ‘Vcc’ is used to give electric power to the IC. This is because smart cards depend on outside sources for power. In fact, the IC in a smart card is not working all the time; it only works when a transaction should be performed, either a read function to read information or a write function, to add or remove or change the data on the card.

Therefore, no permanent power is needed, and the power is given to the IC through the 'Vcc' contact, while the card is in the reader device.

'Clock' provides clock synchronization between the card and the device, and 'GND' is used for ground connection. 'ROM' is the read-only memory that stores permanent data related to the card issuer, the application, etc. and the 'EEPROM' is the read/write memory used to store the actual information. Both ROM and EEPROM are kinds of memory that can keep data in them, regardless of the presence of power in the IC.

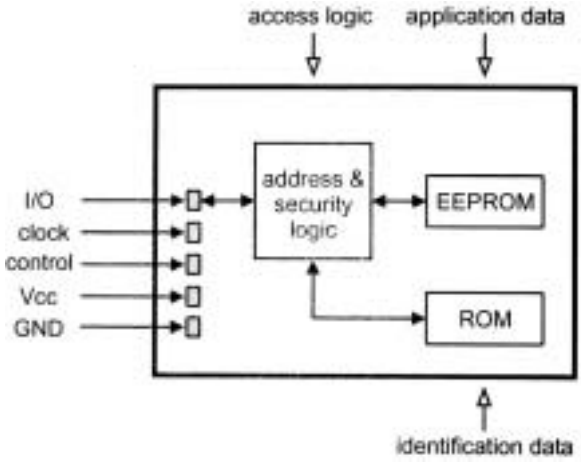


Figure 7 – Typical architecture of a contact-type memory card

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

Memory cards are mostly designed for a single application, with predefined update methodology, such as decreasing a counter value. This makes the cards very cheap, and suitable for applications such as telephone cards and health insurance cards, where the value of the counter is decreased depending on the service received.

Microprocessor cards

As the name suggests, these cards have a complete microprocessor in them. The major advantage of microprocessor cards over memory cards is that due to the existence of a Central Processing Unit (CPU), stronger measures can be established

to protect the data on the card. In effect, the card behaves like a small computer, with its own CPU, Operating System (OS), Memory, Input/Output, etc. Figure 8 shows the typical architecture of a contact-type microprocessor card.

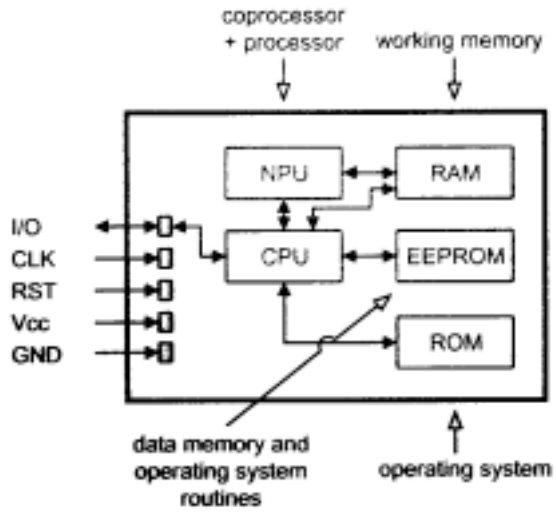


Figure 8 – Typical architecture of a contact-type microprocessor card with coprocessor

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

The CPU is the system's brain, which performs all operations and calculations. If additional data encryption methods are needed, another special purpose CPU may be added, which is called Coprocessor or Numerical Processing Unit (NPU.) The OS in a computer system is the most important software, which controls other programs, and relates them to the computer hardware, by assigning system resources such as the CPU time, memory and I/O channels to them. The OS in a card has a similar role; i.e. the major routines and programs needed for the card to work logically. The card OS is loaded into the ROM when the card is being produced. The EEPROM and the contacts are almost the same as that of the memory card. However, RAM is new; RAM is another kind of read/write memory, which is significantly fast, but depends on power. In other words, the data remains in a RAM unit as long as the power is connected, and thus, it can be used only as a temporary memory. In the microprocessor smart cards, the CPU uses RAM to store operational data.

Unlike memory cards, microprocessor cards can be used for more than one application. Although the main part of the OS is stored in the ROM, it is possible to have the specific information needed to operate applications in the EEPROM and have them all function at the same time. As EEPROM is a read/write memory, new methods allow the adding and removal of new applications, even after the card is issued to an individual. Microprocessor cards are used in many applications, such as credit cards.

Contact-less smart cards

Contact-less cards are not a new type, but they present a different communication channel for the IC or microprocessor. Both memory cards and microprocessor cards can be of contact or contact-less types. In effect, the card remains intact; only a new interface is added to it to manage the contact-less communication with the reader/writer devices. Figure 9 shows the typical architecture of a microprocessor card and a contact-less interface.

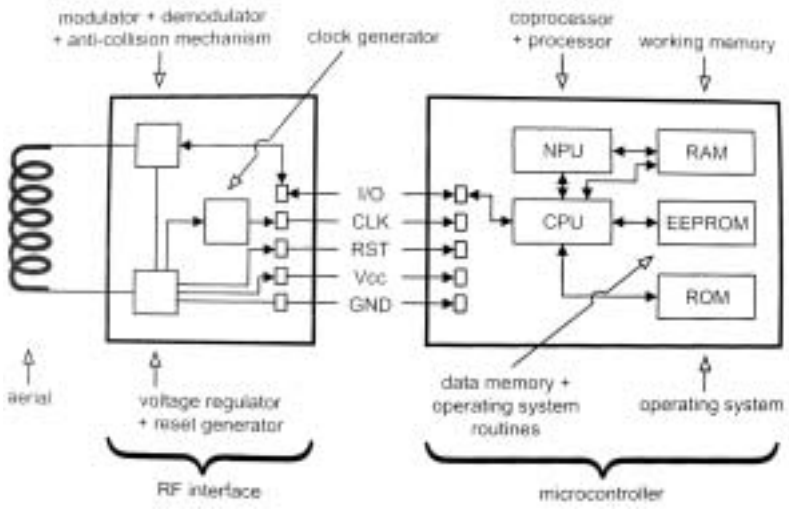


Figure 9 – Typical architecture of a contact-less microprocessor card

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

As can be seen, the added part comprises of an antenna, which is embedded in the body of the card, plus an RF interface, contacts of which are identical to that of the

microprocessor part. The power needed for contact-less cards is generated using the concept of loosely coupled transformers in the electromagnetics, by using the antenna as the electric coil. In this way, an electromagnetic field is created between the antenna and another coil in the reader device, from which electric current is generated in the card body.

Contact-less cards are preferred over contact cards because there are certain problems with respect to the contacts. Contacts are sources of failure for the cards, they might be contaminated or covered and thus prevent the card from functioning, and the microprocessor can be damaged by the electrostatic discharge. Contact-less smart cards also provide some advantages over contact cards at the human interface level. This is mostly because there is no need to enter the card into a reader slot; the RF interface can communicate with the reader interface from a distance of up to one meter. For instance, contact-less cards are preferable in applications such as customer authentication in transport sector, where many people should be authenticated in a short time. They also provide higher security as they remove the need for the reader device to be accessible to people, who may try to prevent the system from functioning by "forcing chewing gums or superglues into the reader slot." (Rankl & Effing, 2003, p. 23)

Although these cards, as well as their relevant reader devices, cost more than the contact-type cards, maturity and mass production can lower the prices up to the level of the contact-type cards.

4.2.2.4. Other cards

Besides the above-mentioned cards, there are always new types evolving. One example, which is already being used, is the optical memory card. The most important feature of these cards is that they present much more memory, compared to the other types. The memory of present optical cards, which amounts to several megabytes, is a read/write-once type, which means it is possible to add data to the

memory, but the written data can not be changed or removed. Yet, this is suitable for some applications, such as the health care information of patients. Like the magnetic-stripe card, the security argument is also valid here. However, these cards can benefit from the features of other smart cards, by employing complicated encryption methods to protect the data from being illegally accessed.

On the other hand, today's cards are rarely of one type. Card issuers usually try to get the maximum benefit out of cards by combining different methods. For example, it is quite normal to have embossed features, a magnetic stripe and a microprocessor module on one single card. This enables the card holder to use the card where magnetic-stripe readers are used, to present it where smart card encoders are present, and also whenever there is no reader machine and the conventional system of embossed cards and paper receipts is applied, e.g. onboard an airplane.

4.2.3. Card components

As already mentioned, the comprehensive description of cards is provided by the ISO in relevant standards. According to the ISO 7810 standard, ID-1 cards have the following dimensions:

Table 7 – Dimensions of standard ID-1 cards

Width	between 85.46 mm and 85.72 mm
Height	between 53.92 mm and 54.03 mm
Thickness	between 0.68 mm and 0.84 mm

Source: Derived from ISO standard number 7810

Card body

There are several components that make up a card. The first is the card body, which should be made of durable material, with enough resistance to bending, twisting, and climatic changes. Polyvinyl Chlorine or PVC is the most common material used for the card body, with suitable features, although it is considered to be harmful for the

environment. The other options are Acrylonitrile Butadiene Styrene (ABS), which is very stable and resistant to temperature extremes, Polycarbonate (PC), which is the same material used to make CDs and DVDs, with good durability, but low resistance to scratches and rather expensive, and Polyethylene Terephthalate (PET.), which is also known as Polyester. Research is on-going to find better materials.

Security measures

Cards usually have several security features, such as *signature panels*, where a sample of the holder's signature is printed, *ultraviolet text*, where control numbers are printed using ultraviolet ink, and *microtext*, which is used to print very small text. Microtexts need special magnifying glasses to be seen and are invisible to scanners used by forgers. *Holograms* and *Multiple laser images*, which are techniques used to include pictures that are visible in different lighting conditions, are also utilized to prevent easy production of fake cards. *Laser engraving*, which is used to darken a plastic layer by heating it with a laser beam, is another attempt to make cards tamper proof. This method can be used to engrave some text or even the picture of the holder on a card. Laser engraving is done in two different modes, namely raster and vector, and the engraved part can be overlaid by a foil, to make it even stronger. (Rankl & Effing, 2003, p. 35)

Chip modules

The integrated circuit or Chip module, which is the most important component of the card, is fixed on the card body using different techniques. Chip modules are usually placed under the contacts that form the visible surface on the card. This protects the chip from external interfering factors, and also provides access to the microprocessor through the contacts.

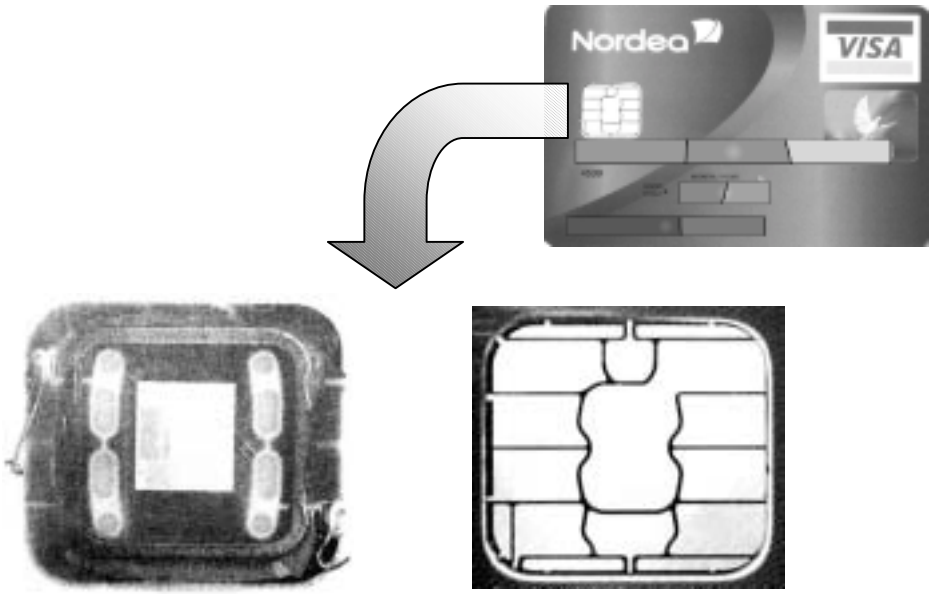


Figure 10 – Contact surface of a smart card

Source: ***Left:*** Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons., ***Right and top:*** Photographed and prepared by the author

The most widely used method to secure the chip module in the card body is called *chip-on-flex*, where an opening is punched in the card body so that the chip module can be glued into it. Figure 11 illustrates the cross section of a chip being mounted using this method.

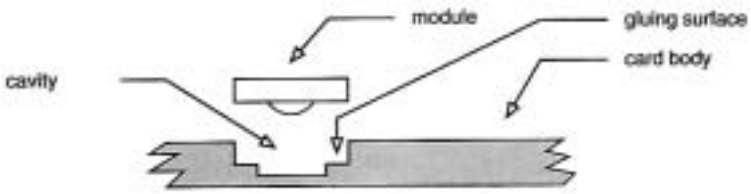


Figure 11 – Inserting the chip module in the opening in the card body

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

As this is the standard practice used in the semiconductor industry to place chips in packages, the knowledge and technology is not very expensive and thus, it is cheaper than the other methods.

4.2.4. Smart card lifecycle

Smart cards have a defined lifecycle. According to the ISO 10202-1 standard, a smart card passes five phases throughout its lifecycle, namely: production of the chip and the smart card, card preparation, application preparation, card usage, and termination. Figure 12 illustrates the phases and their interactions.

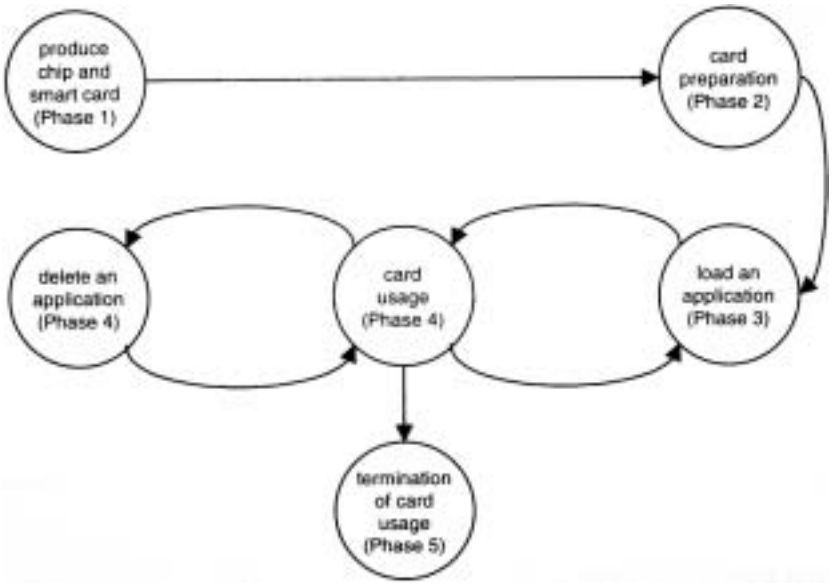


Figure 12 – The life cycle of a smart card according to the ISO 10202-1 standard

Source: Rankl, W., & Effing, W. (2003). Smart card handbook. Chichester: John Wiley & Sons.

In the first phase, the chip is designed and a suitable operating system (OS) for the chip is generated. Then the chip is fabricated and part of the OS is transferred into the ROM. The card body is also produced in this phase and, if the card is contact-less, the coils are integrated into the body. The last process in this phase is to embed the module into the card body. At the end of this phase, the 'bare' card is produced, which would be used in the second phase. To improve quality and assure that any probable error is rectified at the proper stage, there are test mechanisms in place at each phase, mostly using special machines. The tests in phase 1 are crucial, as it would be impossible to correct any mistake in the operating system or the internal communications, after the card passes this phase.

Phase 2 is where the card is further completed by adding the necessary data related to the applications, as well as the part of the OS that should be stored in the EEPROM. In this phase, all the application data and files that do not vary from card to card should be stored in the card. Thus, the card issuer should send the necessary information to the card manufacturer, including some secret keys and important data files. The data transfer channel between the issuer and the manufacturer should be secure, otherwise, the security of the card system would be compromised. The data transfer is usually done using diskettes, magnetic tapes or online communication.

After this phase, the applications should be initialized and the card should be personalized or individualized for each user. Phase 3 includes: generating card-specific secret data, transferring data to the smart card, and individualization, both visually and electronically. As this phase mostly deals with individual secret data, the operations need to be done in a secure and automated mode, with minimum human involvement.

The secret data, such as PIN codes should be generated and stored in the card using secure methods. A common way seems to be the creation of the PIN codes by the manufacturer using a random code generator, and then sending the PIN using an automated mechanism, called envelope stuffing. In this method, the PIN codes created for each user are printed and put in envelopes using a special purpose envelope printer. In this way, no one can see the PIN code except the person who receives the envelope, who is the same person to whom the card is issued. To achieve higher level of security by making sure the right person gets both, the card and the envelope are sent to the user via separate paths.

The individualization consists of visual processes such as embossing the name, engraving pictures and texts into the card, as well as the electrical process of loading personal data into the microprocessor memory (EEPROM) or the magnetic stripe. The biometric data, if applicable, is loaded into the card in this phase.

Phase 4 of the card lifecycle is the duration when the cardholder actually uses the card. During this time, the card should be managed by a system to control and perform the necessary transactions by managing the data on cards. A management system, most of all, needs a database system to control all the information related to the issued cards. On the other hand, if a card is designed for several applications, adding and removing various applications is done in this phase.

Phase 5 is the end of a card's life. In effect, the duration of a card's lifecycle depends on the policy of the card issuers. However, a period of 5 years seems to be the accepted standard for the lifetime of each card. After this period, the card should be disabled by deactivating the applications on it. This can be important due to the existence of secret information in the card. Nevertheless, issuers rarely require the card to be submitted back to them after the expiry date. This can be considered as a problem for the environment, as the cards should be recycled to prevent any hazard to the environment. For example, only "in 1997, approximately 40,000 metric tons of plastic were used in the whole world for the production of smart cards." Obviously, the increased popularity of the smart cards contributes to a bigger problem with card waste.

4.2.5. Attacks on cards

A secure smart card is one that does not allow illicit access to its data. In other words, it should be very hard to read the data for someone who is not allowed to do so; otherwise the card would be a mere storage device. Ideally, the phrase "very hard to read" in the above sentence could be replaced with "impossible to read." In reality, however, it is impossible to have a perfect security system. Each security system might be compromised in different ways. The only possible measure is to make the system as strong as possible.

Furthermore, time is a crucial factor when considering security of the documents. When security measures used in a document are not continuously updated, forgers

have enough time to find weaknesses and effective ways to compromise security. Thus, in the continuous race between the industry and criminals, the one who has the lead is the current winner. That is why the lifetime of a smart card is generally 3 years, which can help the industry to remain ahead of the attackers.

Attacks on smart cards can be at the social, physical, or logical levels. An attack at the social level is directed at the people who deal with cards in the different phases of the card lifecycle, including the workers in the card manufacturing industry and the cardholders. Attacks at the physical level are directed at the microprocessor and require technical equipment to provide physical access to the electric circuits on the card. At the logical level, attackers try to find out the encryption techniques used by the card and the weaknesses of the system, by using software techniques such as "Trojan horses."

On the other hand, attacks may be conducted against four major parts of the cards, namely: card body, microprocessor, operating system and application. The attacks on the card body mostly involve changing the information displayed on the card body, such as the names, the validity period, etc. Such attacks are not very important, as the contents of a card always have the dominant importance. However, such attacks may be needed by forgers to harmonize the appearance of a fake card with its forged contents. The other attacks have to do with the chip and its contents. Details of the attacks against the microprocessor and the circuits on a card is a very technically specific subject, and has a lot to do with microelectronics, which does not match the scope of this dissertation. However, it is possible and desirable to briefly describe the most important attacks.

Attacks during development and production of the chip and the operating system are usually insider attacks, as access to the location is highly restricted. Moreover, as the required knowledge is private and very high level, the number of people who can perform these attacks is very small. Nevertheless, there are some measures to protect these stages from attacks, such as assigning unique numbers to chips, observation of

security measures in the design criteria, regular inspections of the whole process, distributing knowledge among several specialists (everybody does not know everything) and authentication mechanisms between the chip and the machines.

On the other hand, attacks while the card is being used are more probable, as access to the card and the chip is possible, and the required level of expertise is much lower. Static analysis of the microcontrollers is done to extract information directly from the chip memory, which can be prevented by encrypting the contents, adding protective layers and following relevant measures in the design stage. On the other hand, dynamic analysis happens while the microcontroller is operational, and thus, the measures against them are usually combined with the software. For example, several light micro sensors can be placed in different locations of the chip, which would trigger a signal to the chip software explaining that the chip might be exposed to an attack. Scrambling methods can be used to thwart illegal data access during internal data transmissions. For instance, to avoid successful access to the transmission channels between the CPU and RAM, the sequence of the channel lines can be changed for each microcontroller, or even for each transaction. Frequency and temperature monitoring techniques can also detect illegal access to the chip circuits.

4.3. Card / biometrics Combination

In the previous sections, the pros and cons of biometrics and smart cards were mentioned. These are both mechanisms to increase security of the systems. Nevertheless, they do not belong to the same group of authentication methods. As already mentioned, biometrics is “what one is”, while a smart card is “what one has” (possession-based.) In effect, the level of security of biometrics is higher, as possession-based security can be compromised by illegally accessing the proof; here the card. However, biometrics in itself is not the ultimate comprehensive solution. Thus, a combination of smart cards and biometrics might provide a good solution.

As already discussed in 4.1.2, security grows by combining two or more authentication methods. On the other hand, biometric templates should be stored somewhere, so that the system can access them at the time of performing authentications. Based on the previous discussions, a distributed database provides much more security than a centralized one. This is achieved by storing the biometric templates of each person on his or her smart card. One of the results would, then, be that the attack point 10 in Figure 4 is removed, since a centralized database of biometric templates is not needed. In effect, the database is scatter on all cards.

Actually, smart cards and biometrics can complement each other. Using the two, whenever authentication is needed, each person would present his or her smart card, as well as the biometric identifier (such as fingerprint or face) to the system. A sample of the present biometric identifier is then scanned, and then compared with the template already on the card. If the two samples match, the person is authenticated and if not, he or she is rejected. This means that even when a smart card is lost, it would not serve the finder, as the biometric sample of the bearer should match the template on the card. In practice, by adding a third item of "what one knows" (knowledge), card issuers can achieve the highest level of security. This might help the system in making sure of the genuineness of the person whenever needed.

Moreover, advanced security features of smart cards such as complicated cipher techniques can be used to protect the biometric template stored on the card from illegal access or changes. When the card allows the matcher to be run inside its chip module, the biometric template does not need to leave the card. In this way, the template is accessed only within the card, which is even more secure.

One of the common features of smart cards and biometrics is that both need databases to keep and manage the information of their users. Such a database normally contains identity information about each person, as well as the trustees and rights he or she has in the system. When combining the two, it is also possible to

integrate the databases into one. Then the biometric template is an element of the card database, and the identity information will not be kept twice, which improves the quality of the system. Besides, all the necessary information would be retrieved at once, without the need for communication between two different databases.

4.4. Critique of the ILO solution

As mentioned in chapter 3.3.2, ILO decided, in the follow-ups to its latest convention C185, to use the fingerprint as the biometric identifier and a two-dimensional barcode on a card as the storage to be used for identification of seafarers. By this selection, ILO has tried to minimize the costs of implementation and application of the SID. This is because most crew-supplying States are developing countries and it is difficult for them to set up and maintain an expensive system. The production cost of the cards is also a matter of concern for ILO, as the seafarers would probably pay for it. Thus, ILO is trying to introduce a biometrics system that is compatible with the current practice in States. Furthermore, it is trying to follow the specifications set by ICAO about inclusion of biometrics in documents, although these specifications are only ICAO recommendations.

4.4.1. The Biometric Identifier

ILO has chosen the Fingerprint as the biometric identifier for seafarers' identity document by considering several aspects. As already discussed in 4.1.5, each application has its own requirements, which should be carefully studied in order to make the best choice among biometric identifiers. Therefore, to evaluate the ILO solution, one needs first to define the requirements of the application, i.e., identification of the seafarers.

4.4.1.1. Application requirements

Authentication of seafarers is an application with its special requirements. By considering those requirements and other particulars of this process, it is possible to draw a table such as Table 3 to show the biometric features and their importance in the process of seafarers' authentication.

For the purpose of this research, a small interest group was formed within the World Maritime University, with members from the seafarers and other experienced people. The issue was briefly explained to them and then they were asked about the importance of biometric properties of the first three sections of Table 3. The result of this discussion is summarized and reflected in Table 8.

The values in the first section are similar to that of physical access. The reason is that seafarers require this authentication, and they are to certain extent, willing to accept some drawbacks, such as "Required cooperation" for authentication, e.g. in the case of contact sensors. Seafarers are against losing their privacy rights; but the issue of shore leave is so important for them that they may accept a moderate level of inconvenience, in a trade-off between privacy and facilitation of shore leave. Thus, "Social stigma", "Intrusiveness", "inconvenience" and "required proximity" are set to "medium" value. "Population missing" is not crucial here, as users of the system are specific people and do not have other choices to switch to. However, if the application of biometric cards is considered negative and undesirable, population missing can affect the industry in the long run, as it can discourage younger generations from becoming seafarers.

"Acquisition time" is not very important here as well, as the population is not very large. The slowest methods of authentication are done within a few minutes, which is an acceptable timing in the shipping industry. Like physical access, "Failure to Enrol" and "Failure to acquire" have moderate importance, as they can be solved by human intervention, although sometimes this requires extra time and effort.

Table 8 –Application requirements for authentication of seafarers

Features	Importance Weighting	Numeric equivalent
Intrinsic properties		
Required cooperation	medium	3
Social stigma	medium	3
Intrusiveness	medium	3
Population missing	low	1
Sampling properties		
Inconvenience	medium	3
Required proximity	medium	3
Acquisition time	low	1
Failure to enroll	medium	3
Failure to acquire	medium	3
1:1 matching properties		
# FA per 10K (FRR = 10%)	high	10
# FA per 10K (FRR = 1%)	high	10
Template size (bytes)	high	10
Technology properties		
Installation cost	high	10
Continual cost	medium	3
Cost per match	medium	3

Source: Compiled by the author, based on the results of the discussions with the interest group formed in the World Maritime University during the study

As security is one of the main causes of existence for seafarers' identification documents, the number of False Accepts needs to be as low as possible in both situations, thus giving a value of "high" to both relevant features, i.e., "# FA per 10K (FRR = 10%)" and "# FA per 10K (FRR = 1%)". The reason why "Template size" has a high importance is the use of distributed databases. As cards typically have limited capacity, template size should be small enough to be stored in the card memory. However, this can lose its importance as new technology increases card capacities.

"Installation cost" is an important issue. As will be examined in the next chapter, this is mainly due to the responsibility of the Nation State to issue the document, which is the most expensive part of the project and requires considerable investments in terms of software, hardware and the human element. The problem of installation costs is aggravated because major crew-supplying States are among developing

countries. Other costs can be considered as of "medium" importance because other stakeholders require much less investment, and usually have better financial position.

4.4.1.2. Which biometric identifier?

One of the ways to compare biometric identifiers is to calculate the mismatch scores. By following the method discussed in 4.1.5.3, it is possible to calculate the mismatch scores for different biometric identifiers, by using the data in two tables; Table 5 and Table 8. This gives a comparison of which biometric identifier better suits seafarers' identification.

Table 9 – Parameters needed to calculate mismatch points for six major biometric identifiers to be used in seafarers' identification document (SID)

Features	SID (W)	Finger (P_1)	Face (P_2)	Voice (P_3)	Iris (P_4)	Hand (P_5)	Signature (P_6)
Required cooperation	3	10	1	1	3	10	10
Social stigma	3	10	1	1	3	3	1
Intrusiveness	3	3	1	1	3	3	1
Population missing	1	1	1	3	1	3	3
Inconvenience	3	1	1	1	3	3	3
Required proximity	3	10	1	1	3	10	10
Acquisition time	1	1	1	3	3	3	3
Failure to enrol	3	3	1	3	10	1	1
Failure to acquire	3	3	3	3	3	1	1
#FA per 10K (FRR=10%)	10	*0*	*20*	*34.8*	*0.0*	*20*	*34.8*
#FA per 10K (FRR=1%)	10	*10*	*30*	*30*	*0.0*	*20*	*30*
Template size (bytes)	10	5	10	20	2.5	1.0	2.0
Installation cost	10	1	1	1	3	3	3
Continual cost	3	1	1	1	3	1	1
Cost per match	3	3	1	1	1	3	1

Source: Compiled and inferred by the author

After doing all the calculations, the resultant mismatch scores are as follows:

Table 10 – Mismatch scores of six major biometric identifiers for SID

Biometrics	Finger	Face	Voice	Iris	Hand	Signature
Mismatch score (X)	294	645	903	155	551	791

Source: Compiled and inferred by the author

Table 10 suggests that based on the mismatch score calculation method, Iris is the best biometric identifier for authentication of the seafarers, and Fingerprint recognition is in second position. Voice and signature seem to be the worst choices, which is a valid point compared to the previous discussions, as the two are not distinctive and scalable enough for large populations.

4.4.1.3. ILO choice

Selection of Fingerprint as the biometric identifier for seafarers has several aspects to consider. First of all, people usually do not have a good impression of Fingerprint recognition, as it has long been used by law enforcement authorities, to identify or verify criminals and lawbreakers. However, the situation is being changed. The low cost, maturity and acceptable distinctiveness of Fingerprint recognition have made it a good option for certain applications, even in daily life. For example, a well-known supermarket chain in the UK has started to test a fingerprint-based payment system at the point of sale in three of its stores. ("UK supermarket chain trials biometrics", 2004) In effect, as time goes by, application of the Fingerprint in various sectors may change the image in everyone's mind.

Scientific methods of biometric evaluation show that Fingerprint is one of the best choices. As already explained, in the evaluation of biometric identifiers using the mismatch calculation method, Fingerprint recognition has the second position for authentication of seafarers. Although this method suggests that iris scans is the first choice for the SID, maturity is the winning factor of the fingerprint recognition over the newer iris scans. In fact, fingerprint technology is given priority over others, as it is a known experience in most countries, even though in manual form and in a different application framework.

Having the circumstances in which ILO nominated fingerprint recognition as the select technology, even if a comparison method was employed, concerns about cost of production and operation were so much that the costing structure had become a

definitive factor. This caused iris, which is still a rather expensive technology, to lose its status in the minds of people who decided at ILO, which resulted in the selection of Fingerprint recognition. However, this is not a permanent situation; as technology advances, relevant costs of certain identifiers may decrease, which could considerably change the ranking positions.

4.4.1.4. Pattern-based or Minutiae-based?

Between the two major fingerprint matching techniques, the International Labour Office suggested that the pattern-based method should be selected as the solution, as it better suited the seafarers identification document in the follow-up to the seafarers' identity documents convention (revised) on 24th of February 2004. The reasons why this suggestion was made are mentioned to be:

1. The information obtained from a pattern-based method always fit into the limited memory capacity on the proposed barcode, whereas the information obtained from a minutiae-based method may not fit, thus requiring more capacity. As the capacity is limited in the proposed card, the sample may need to be truncated, which compromises accuracy of the fingerprint recognition.
2. The pattern-based method can use lower quality scanned samples, compared to what is required for the minutiae-based method. This can lower the equipment costs.

Notwithstanding the suggestion made by the International Labour Office, as already mentioned, the Governing Body of ILO finally selected the minutiae-based matching method on 26th of March 2004. One of the major reasons behind this decision was the opposition from different States against the pattern-based method, since most of the forensic applications in various States are based on minutiae-based recognition, thus giving it priority over pattern-based method, due to the availability of the equipment, and the knowledge and experience to use it. Furthermore, as there are

many companies who produce minutiae-based matching equipment, the price of such devices is much lower than that of pattern-based method.

On the other hand, it should be considered that the above-mentioned priorities of the minutiae-based method over the pattern-based method could be removed due to the technology improvements. As the devices are continuously becoming cheaper, there is no point in using lower quality scanners to get the samples. This idea proves to be more valid by considering the fact that the biometric scanner amounts to a minor share of the total cost. The issue of costing structure is discussed in more detail in the following chapter. Moreover, considering alternative methods for the establishment of new solutions, cards are not so limited in their capacity. Therefore, it would be easy to store the minutiae-based data on cards, even if they need slightly more memory.

4.4.2. The Card

Regarding the document itself, ILO decided to ignore the application of magnetic-stripe cards or chip-cards to prevent any probable misuse of the cards against seafarers by inclusion of hidden information in the storage. This is a measure to follow the requirement set by Article 3, paragraph 9, which provides that all data concerning the seafarer recorded on the document have to be visible and where not eye-visible, seafarers should have convenient access to machines that enable them to inspect the data. (International Labour Organization, 2003)

The chosen barcode technology by ILO restricts the card to a read-only state. In fact, using barcode technology looks like writing a text on paper with a pen, without being able to change it. This is true for the cards as well; when the card is issued, it is not possible to change the information in it or add something new to it, unless the card is changed and a new card is issued. As the information is written into the card only once, it only suits SIDs that do not include CoC information.

There are certain pros and cons in this respect. For example, the potential for fraud and forgery in the documents may decrease, as the barcode section is usually protected by laminates and other security measures. Furthermore, there is a centralized control of the information written in the card, which makes it easier to handle. This also gives more confidence to seafarers who are concerned about probable inclusion of hidden information in the card that may be used against them, as there is only one authority and one stage of data storage in the card.

On the other hand, this technology prevents any probable change in the usage of the document in the future. For example, if a new instrument from ILO or IMO suggests inclusion of CoC information in the card, then the whole document should be changed.

Another point to consider regarding the ILO policy to minimize the costs is that barcode technology, magnetic-stripe or smart cards are not significantly different in terms of costing. Although this may look a little bizarre, it can be proved by taking a look at the discussions in section 5.5.1 about costing. To have a valid discussion, three main groups involved in the costing should be considered: Card readers/checkers, Card issuers/updaters and seafarers. Card readers are those who need to check the information and compare the stored biometric template with the biometric sample obtained from the seafarers, including Port State Control authorities, Flag State Inspectors, Immigration authorities and Shipowners/companies. The equipment used by these authorities is either a computer equipped with biometric scanner and card reader (encoder) or a special handheld computer specifically designed for this purpose. In either case, the card reader is a part of the machine that reads information from a card or in the case of memory or smart cards, also writes the necessary data on it. This part contributes to only a small share of the value of the whole device, not more than 10 percent. Thus, application of a higher technology, such as magnetic-stripe or smart cards, does not have a significant effect on the price of card encoders.

The second group, i.e. issuers/updaters, should spend a big portion of the money on the infrastructure, software development and maintenance, which has little to do with the type of card used. Section 5.5.1 clearly shows that for a combined SID and CoC card, the cost of the equipment is around 20% of the whole investment required. Thus, even if such equipment is 50% more expensive than what is needed for cards based on barcode technology, the total costs will not change more than 10%.

Seafarers are the third group, who will face a considerable change in the cost of cards, if they are to pay for them. Even so, the maximum cost of USD 15 for a 5-year valid card compared to the seafarers' income is not considerable at all. Thus, as will be explained later, this seems to be a pretext to oppose the application of biometrics.

Thus, the chosen card technology does not decrease costs and expenses very much.

Another issue is the seafarers' right to be aware of the information stored in their documents, which could also be provided in magnetic-stripe and smart cards. Like a barcode, whatever is stored in a magnetic-stripe or chip can also be read by the seafarer using a card reader device. The only information inaccessible in a smartcard is the cryptographic data, which is related to the methods used to code and decode the information; the same thing is valid for barcode cards, as certain codes are embedded in the barcode, which facilitate retrieval of the information.

Chapter 5

Integrated Seafarers' Identity and Certificate - SIC

5.1. Introduction

In previous chapters, the original idea of a new document for seafarers to include all information about certificates and identification of seafarers into one secure document was discussed. At least, IMO had this view, upon requesting ILO to develop "a Seafarers' Identification Document as a matter of urgency, which should cover, inter alia, a document for professional purpose, a verifiable security document and a certification information document." (ISPS conference resolution, item 1.)

This shows that IMO has been looking for a solution to overcome the problem of fraud in seafarers' certificates as well, especially after the report of the research done by SIRC in 2001. Since then, IMO has become really concerned about fraudulent practices in the certification of seafarers. However, ILO members, after all their discussions on the issue, decided to ignore the last part of the above quoted requirement of IMO, i.e. certification information. During the discussions at ILO, some members were concerned about the time factor. They wanted to have the convention adopted as soon as possible, and they concluded that inclusion of

certificate information would definitely slow down adoption and the implementation of the new convention.

Some countries such as France and Germany raised the issue of difficulties that could arise in updating the documents if the solution was to include CoC information. They believed that as it is necessary to update the information on the cards after changes of functions and qualifications of seafarers, it would not be easy to perform the updates on such a document. Other countries such as Canada, the UK and the USA favoured optional inclusion of certificates in the card depending on the decisions of individual members. (International Labour Organization, 2003b, pp. 79-84)

Nevertheless, despite all the urgency in its adoption, the C185 convention, with only three ratifications after a year from its adoption, seems to be away from being a globally accepted solution. The reason why member States do not ratify this convention could be sought in the way the USA reacts to this issue. On the one hand, the convention was customized for American needs, but on the other hand, the USA has ruled out the convention, and has announced that it will not ratify the C185 convention. ("US insists," 2004, p. 1) So, member States have hardly any incentive to ratify the convention, because even if they do, crewmembers on their vessels still need to obtain a visa to go ashore in the USA ports, and this is not possible before fulfilling all the necessary formalities, including an interview. Without the USA and other major maritime States joining, even if some other countries ratify the C185 convention, it will not be more than a regional agreement.

So far, the convention has not been successful in achieving its goal of implementing a globally accepted seafarers' identification document. On the other hand, combating fraudulent practices in the certification of seafarers is a matter of real concern for IMO. To overcome this situation, something needs to be done, whether by amending the C185 convention, adoption of a new instrument by IMO/ILO or both, or any other relevant measure to appropriately address CoCs, as well as SIDs.

Besides the position of the USA, there are some other obstacles, which prevent the C185 convention from achieving its goals. The obligation stated in Article 2 of the C185 convention to issue SIDs by the State of nationality of seafarers is one of the problems. This requires States to issue the new document only for seafarers who are nationals or permanent residents there, which may not be easy for all States, as they may not have enough resources or the necessary administrative procedures in place to implement the issuance system. On the other hand, sometimes it is not easy for such States to verify that the person asking for a SID is really a qualified seafarer. In this case, the SID would be merely an identification document like a passport. Therefore, the SID issuer needs to somehow obtain the necessary information to confirm the qualifications of claiming seafarers.

5.2. Electronic CoC

The implementation of an electronic CoC can solve some of the problems mentioned earlier. Such a document can considerably decrease fraud and forgery in the certification of seafarers. As prescribed by SIRC in their report, the use of measures such as smart cards and biometrics is a solution to prevent and combat fraudulent practices in the certification of seafarers. (Seafarers International Research Centre, 2001, p. 43)

By using an electronic CoC system, fraud in certificates would decrease, since this technology has dynamic security measures which make the documents difficult and much more expensive to forge. An efficient electronic CoC can also help successful implementation of SIDs. By making a globally accepted electronic CoC and providing a strong link between SID and CoC, all active entities in the shipping industry would be encouraged to utilize both of them to have a good system of identification and certification. Such a reasonable link would also solve the problem of the restriction of issuance of identification document only by States of nationality.

This idea can be supported by taking into account that the need for electronic CoCs is already there in the marketplace. As a pioneer in this respect, Liberia has already developed a system to issue a combined CoC and SID for seafarers. However, the procedure adopted by Liberia does not comply with the C185 convention, primarily in that Liberia issues SIDs for non-national seafarers. Although this project is still in its test phase, it shows that a big Flag State really needs to have a secure document, which covers both the identification and certification information of seafarers.

Nevertheless, application of electronic CoCs should be adapted to the current practice in the shipping industry. According to the STCW convention, the original certificates of all crewmembers should be onboard each vessel. As a measure to prevent fraudulent practices and let inspectors check the validity of the certificates, this requirement would be in place unless an amendment removes it. Thus, the electronic CoC should be considered as a supplement to the original certificates of competency. In practice, however, the positions could be the other way around; i.e., inspections would be done by checking the contents of the electronic CoCs and the originals used whenever the card contents need to be verified. In this case, the original document would be a supplement to the electronic CoC.

On the other hand, the legal aspect of using electronic CoCs should be carefully considered. This is mainly because the electronic documents are unacceptable in some juridical frameworks. As electronic documents are quite new, many judiciaries do not recognize them as valid documents like paper documents. This is a potential source of legal problems in dealing with challenges and disputes, after the implementation and actual use of the electronic CoC. In fact, as long as the legal authorities in various States refuse to accept the electronic CoC as a valid document, it cannot be successfully implemented. Nevertheless, this is not the first area of application of electronic documents. Several applications such as Banking have already employed electronic documents and considerable advancements have been reached in the legal aspects. Therefore, some countries have placed electronic documents in their legal frameworks. Yet there are many States that have not done

this. It is then necessary for them to have the electronic CoC recognized as a valid legal entity in their judicial system.

5.3. Integration of SID and CoC

Thus, the need for a unified solution seems to be obvious. This solution can be the implementation of another document for CoCs or the coming up with a single document covering both capacities. Making a comparison between the two can show that a single document is preferable.

First of all, one single document will make the whole solution much cheaper. To deal with electronic SID or CoC, different entities such as Port States, Flag States, Immigration Authorities and crew-supplying States should set up platforms and pay considerable amounts of money for hardware and software requirements. Administrative procedures, training of personnel and maintenance also contribute a lot to the total cost of realizing the solution. If there are two separate documents to be handled, most of these expenses will be twice as much, plus the time and energy needed. This is also an important issue for seafarers, as they want to pay as little as possible; obviously one card is cheaper than two cards. It would also be much more convenient to carry one card for both certification and identification.

Secondly, if another separate document is implemented, a part of the process is being repeated all the time, which incurs extra costs and efforts for seafarers and related authorities. To check the validity of a CoC, the holder of the CoC needs first to be authenticated. In fact, a secure way is needed to link the person to the document. This is usually done by checking a biometrics sample on the document and comparing it with the person's live biometrics sample at the time of authentication. The same procedure is done while checking the identification of the seafarer.

Actually, identification is a part of CoC evaluation. Therefore, the biometric sample and certain other personal information must be there in the electronic CoC document.

This means the enrolment procedure, as well as digitizing and storage of the biometrics sample must be done twice for the two documents. In doing so, different problems may occur. For example, if the two issuing authorities use different methods, there might be cases where a seafarer is authenticated with one of the documents, but rejected with the other one. This could easily happen if the relevant authorities use different values for FAR and FRR parameters.

Nevertheless, there are some difficulties in trying to setup a single document for identification and certification. The first one is the need for harmonization of all seafarers' certificates throughout all countries. This is needed because the information to be stored in the database and on the documents should have a similar format, so that different States can read and write information from/to the card in a proper and standard way. While the STCW convention has suggested certain formats for CoCs, such standards should be more precisely and pervasively defined. Obviously, such harmonization is not very easily achieved and may take some time to be implemented.

The other obstacle in building a single CoC and SID document is the coordination needed among States of nationality and the certificate issuers.

5.3.1. How SIC should work

Having discussed the necessity of a solution for SIDs and CoCs, the focus shall now be on the solution itself, which is supposed to be a single card, equipped with biometrics. As a unified electronic SID and CoC, this card could be called SIC (Seafarers' Identification and Certificate document), which is the term used hereinafter.

As this document should contain two sets of information, it will need more storage, compared to the ILO-proposed document. The document should be a card, equipped with either a magnetic-stripe or chip to hold all the necessary information.

To understand how the integrated SID/CoC (SIC) should work, the following could be considered as a possible procedural description.

Issuance

In the first stage of its lifecycle, the card should be produced. Two entities are involved in this phase: the Nation State and the Flag State. The Nation State should issue the card for its national seafarers upon their request, with information about their identity, including personal information and necessary biometric sample(s). Thus, the biometric enrolment process is done in the Nation State. At the same time, the national database of seafarers, which shall be produced by the Nation State, should be updated to include the newly enrolled seafarers. The Nation State can have certain criteria to believe that the person is a seafarer, prior to accepting the request to issue a SIC.

Then the seafarer has a partial SIC, which is not yet valid. The next step is to make the card complete by adding the information about seafarer's qualifications and certificates. Thus, the seafarer should present his/her partial SIC to the second authority, which is usually the maritime administration of a State where their certificates are issued. This authority should then add to the card all the necessary information regarding the certificates obtained by the seafarer. If the seafarer is to work onboard a vessel from this same State, the issuance phase of the card is done. Otherwise, there would be a third step that demands the State of registry of the vessel to endorse the certificates already obtained by the seafarer in other States by adding a data item to the card.

Updating

Then the seafarer has the complete SIC in hand, which should always be kept by them. Nevertheless, the card contents may change in the second phase of the card's lifecycle. This normally happens when the seafarer obtains new certificates, when validity of a certificate should be extended or withdrawn, or when the seafarer moves

to a vessel registered in another Flag State. If the Discharge book information is also included in the SIC, the card will need more frequent updates, including the seafarer's movements to other vessels or his/her roles onboard.

For the purpose of updates, a seafarer should present the card to the relevant authorities and get it back after the card contents are revised, which brings it up-to-date and valid for use.

Checking

The other operation that seems to be much more frequent than the others is checking the validity of the card and authenticity of the seafarer. This is done by the relevant authorities whenever they need to make sure the card bearer is a genuine seafarer and the card contains valid information. The authentication process is done by obtaining a biometric sample from the seafarer and comparing it to the biometric sample on the card. Checking other information on the card may need communication with the database where the data is kept, such as the national seafarers' database.

Invalidation

After the definite validity period of the card, it should be invalidated and a new one issued. A good choice for the validity period could be 5 years, which complies with other identity documents such as a passport. Defining a reasonable validity period can also facilitate application of the forthcoming technologies for all seafarers with a maximum delay of five years.

5.3.2. Requirements

Taking into account the above-mentioned framework, the requirements for successful creation and application of the integrated SID/CoC (SIC) for seafarers should be considered.

5.3.2.1. Coordination among States

Three States need to have coordination among themselves: the State of the seafarer's nationality or permanent residence, the State of issuance of seafarer's certificate, and the State of registration of the vessel on which the seafarer is working (Flag State.)

The reason behind this requirement is the global nature of the shipping industry with its unique features; where it is quite common to see a vessel belonging to State X, registered in State Y, sailing far away from X and Y, with a crew onboard from States E and F, with certificates obtained from States G and H, and endorsed by State Y.

Considering the three States of Nationality, Certification and Flag as A, B and C, four possible situations may come about:

A = Nationality = Certification = Flag

In this situation, there is not much of a problem, as all responsible entities for the three aspects are within the same jurisdiction and follow more or less the same rules and regulations. The coordination here is normally between the maritime administration and immigration authorities of each State.

A = Nationality, B = Certification = Flag

Here, a national of one State (A) gets his certificates from another State (B) and works onboard a vessel flying the flag of the same State (B.) In this case, the two States need to coordinate activities regarding the seafarer's SID and CoC. State B should somehow get the necessary information about identification of the seafarer from State A, which is the most competent authority to deal with identification of its nationals. There should be a practical procedure in place to facilitate this cooperation.

A = Nationality = Certification, C = Flag

A national of one State with certificates obtained from the same State (A), works onboard a vessel flying the flag of another State (C). In this case, identification information is already linked to certificates through internal procedures in State A, but State C must endorse those certificates, as the Flag State is responsible for the qualification of seafarers onboard their vessels. Therefore, there should be a procedure to make endorsement of certificates possible.

A = Nationality, B = Certification, C = Flag

The most complicated case is when a national of A gets his certificates from State B and then works on a vessel flying the flag of State C. Here, both coordination and endorsement mechanisms are needed; coordination between A and B and endorsement by State C of certificates issued by State B.

Having said all this about the necessary procedures, the degree of coordination and common procedures depend a lot on the solution acquired. On the other hand, although many States have good relations and are interested in cooperation, there are instances where due to political instabilities or conflicts, such coordination cannot be achieved. Thus, it is best to choose a solution that mostly relies and depends on clear rules and procedures. In fact, even in using a single document for seafarers' certification and identification, a good solution can decrease the dependency of States on each other to a large extent.

5.3.2.2. Harmonization of certificates

If certificates are to be placed electronically on a document, data items should have standard formats, whether in databases or on the document itself. Standard methods for storage and retrieval of data are also needed. The STCW convention has introduced standard forms for certificates and endorsements by member States in section A-I/2 of the mandatory part 1 of the STCW Code. However, these forms are

designed for paper documents and are not precise enough for electronic documents. For this purpose, besides the necessary information and physical format, exact specifications of the data fields should also be defined, including their type and length. On the other hand, in an electronic CoC, only data fields should be stored and titles and other fixed texts should not be repeated.

5.3.2.3. Appropriate document

This seems to be an obvious requirement. Compared to the ILO solution for SIDs, a considerable amount of information need to be stored on a SIC document, so the card must have enough capacity. On the other hand, unlike the identification and biometrics data which are rather static, the data for certificates is not read-only; as the qualifications and certificates of seafarers may change, including the addition of a new certificate or extension or withdrawal of an existing one, the data related to certificates on the card also require updates. Thus, an appropriate card here is considered to be one with the ability to update information, enough capacity and enough security measures to protect the data in it from unauthorized access or change.

Nevertheless, the maturity of the chosen card technology should also be considered. New technology may fulfil all the above-mentioned requirements at the highest level, but at a very high price, thus making it impractical to utilize. Therefore, maturity and the price of the card technology should also be considered.

5.3.3. Who is engaged?

Having the SIC implemented, there are numerous entities involved in the process of issuance, control and use of the cards. First of all, the governments have an important role to play in different capacities; as Port State Control (PSC) Authorities, as Flag State Surveyors, as identification authority in crew-supplying States, and as issuers of certificates.

5.3.3.1. Port States - Port State Control

PSCs are directly involved in the identification and certification of seafarers. To fulfil their duty to prevent unseaworthy vessels from sailing (UNCLOS, Article 219) and relying on the enforcement right given to them by the United Nation's Convention on the Law Of the Sea (UNCLOS) in Articles 25, 216 and 218, PSC inspectors should be able to check the presence of enough competent crew (according to the applicable rules and regulations) onboard each vessel calling at their ports. They need to make sure the crew onboard the vessel under inspection are the right persons and have the right certificates. To do this, they will need devices to check the validity of the certificates, as well as the identity of the seafarers. Talking about SIC, these devices would be small hand-held computers especially made for this purpose, equipped with fingerprint scanners and card readers. Therefore, PSC inspectors will need to receive training in the new technology as well.

5.3.3.2. Flag States - Maritime Administration

Flag States, on the other hand, have certain duties regarding crewmembers onboard vessels flying their flag. Article 94 of the UNCLOS describes, inter alia, Flag State responsibilities to ensure "that each ship is in charge of a master and officers who possess appropriate qualifications …". To perform these duties and enforce jurisdiction over its ships, each Flag State needs to do surveys at appropriate intervals. Like PSC, these surveyors also involve the identification and certification of seafarers, which justifies their need for the equipment, as well as the knowledge of its use.

5.3.3.3. Crew-supplying States - Immigration Authorities

Crew-supplying States are the next in line. With a considerable number of seafarers working under other flags, they are the ultimate responsible entities for identification of their nationals and shall issue identity documents for their seafarers. In an integrated SIC, this entity is responsible for the identification part of the document.

However, it also has something to do with the CoC, since the issuing authority should be able to verify that the person who requests for the identification document is indeed a seafarer.

To this end, crew-supplying States must have appropriate equipment to issue a new SIC and register the identification information in it.

5.3.3.4. Registries - Maritime Administration, Certificates Section

After the introduction of the concept of open registers, many countries have turned to this business. One of the incentives for shipowners to register their vessels in open registers is that they usually do not have any restriction on the nationality of the crew, thus enabling them to hire inexpensive crewmembers from different countries. Open registers have become so popular that some of them have thousands of vessels from shipowners all over the world, with hundreds of thousands of seafarers from labour supplying countries.

However, the registry is responsible for the issuance of new certificates, or the endorsement of present certificates for seafarers working onboard the vessels flying its flag. Therefore, they will need equipment and knowledge to update the SIC and store the most recent information of seafarer's certificates on the document, whether it is issuance of a new certificate or extension or withdrawal of one. In an integrated document, this is the second phase of issuance of the SIC, which is done after the first one, i.e. identity phase.

5.3.3.5. Shipowners/Operators

Shipowners/Operators are also involved in checking of identity and certification of seafarers. They should employ qualified seafarers to make sure their business is safe and secure and their capital is protected. Therefore, they also need to have necessary tools and knowledge to check validity of the document and authenticity of the

seafarer. Such tools for SIC should consist of, at least, a card reader and a biometric scanner.

5.3.3.6. Seafarers

At the very basic level are the seafarers themselves, who are obviously a part of this process. They should keep the document with them, as well as their live biometrics, and present it to the appropriate authority in charge. After all, the whole process is to give a better service to seafarers. Seafarers should not be abused by the inclusion of covert information in the document against them. They have the right to know what is exactly stored in the document (International Labour Organization, 2003) and as electronics are not visible, seafarers would need devices, which let them see what is in the card. Such devices, as mentioned in ILO C185, Article 3-9, should be conveniently accessible to seafarers. These are usually simplified versions of the checking devices, which only read the SIC.

5.3.4. Beneficiaries

Several entities benefit from an integrated SIC, the most important of which are Flag States, Port States, shipowners/Operators and Seafarers.

Flag States, especially big registers, have serious problems regarding fraud and forgery in the certification of seafarers who work onboard their ships. These fraudulent practices in certification of seafarers will damage the reputation that aspiring Flag States try hard to make for themselves, which is essential for them to thrive in the market. This is mostly because shipowners have the choice to go to other registers, if they present more reliable service regarding certification of seafarers.

As an example, one could refer to the Panamanian Register, which has suffered a lot due to the high rates of fraudulent practices in the certification of seafarers, which

has led to a change in the certificate document. (“Firms Line up for Panama ID card contract”, 2004)

By having a secure SIC, Flag States can ensure, to a large extent, quality of the seafarers for whom they issue certificates or endorsements, which will, at the end of the day, give them a good reputation, and more money. Furthermore, if the SIC is successfully put into practice, open registers can register vessels with crews coming from different nationalities, without facing the problem of shore leave for seafarers.

Port States also benefit from the SIC, but in a slightly different way. With the surprising expansion of security concerns all over the world, which affect every industry, ports are also trying to protect themselves from any threat, and provide a secure and safe environment for ships.

If a globally accepted integrated SIC is in place, port authorities can make sure that the crew onboard vessels calling at their port are genuine seafarers with enough qualifications. This will make the port area and facilities a safer and more secure place for the passengers, for the people working there and for the cargo being transported, which is a good encouragement for more ships to call at the port, and finally means more money for the port. A widespread SIC will also save money for ports by lowering the demand for other security measures.

Further, shipowners are a beneficiary of safety and security resulting from a good SIC, as they will secure their vessel and the crew and cargo onboard, by having genuinely competent people in charge. Cargo owners will definitely prefer a safe and secure vessel that would be accepted in all ports. All this means a healthy business and greater benefit for shipowners.

Seafarers are probably the most important beneficiaries, though they are getting their natural rights. These rights are respect from the society, safety and security in the workplace, and facilitation of shore leave and professional movement. On the other hand, shore leave is one of the basic rights for seafarers, which they are being refused

in some ports. By having an internationally accepted document, besides safety and security in the working environment, ports and immigration authorities have fewer excuses to avoid seafarers' the right of shore leave. This may also lead to a situation where seafarers are also paid enough respect, as seen in other sectors such as aviation.

5.3.5. Costs

To implement and use a SIC, there are certain expenses to be disbursed by different authorities, namely Hardware (equipment), Software (programs and applications) and management-ware (administrative procedures to be followed to utilize the new system.) Putting them into another category, the costs are of two kinds; setup costs and maintenance charges. Setup costs are mostly done only once to launch the system, while maintenance costs are always bound to the system.

5.3.5.1. Equipment

To issue and handle cards, each entity would require different equipment, depending on the role and capacity they have in dealing with cards. The first in line is a set of equipment needed to produce cards at the very beginning, including Card printers and encoders. However, the actual production in phases 1 and 2 of the card's lifecycle is not considered here. Instead, it would be supposed that phases 1 and 2 are performed by smart card manufacturers, and only phase 3 is carried out by the card issuer. This is a valid assumption, as the number of seafarers in many States, and subsequently the number of cards they need, is not so great to financially justify establishment of a card making plant. On the other hand, some States may already have such equipment and not need to incur any cost.

Thus, card printer/encoders are devices used to perform the procedures of the phase 3, i.e. to initialize the applications, and personalize the card. Like printers, these can print information such as text, picture and barcode on cards, as well as holograms and laminates to prevent forgery. The encoder part of these devices is used to store

information in the card memory. Printers/encoders are needed by States of nationality to issue the SID, as well as Flag States, for issuance of CoC.

Card printer/encoders cost between USD 5,000 and USD 20,000 depending on their capabilities and different available options. An example of these devices is HDP600 from FARGO. (Further information could be obtained on Fargo website: www.fargo.com)

On the other hand, in a SIC system, except for its national seafarers, a Flag State is responsible only for the certification part of the document. This means just to save, retrieve or update information in the card, rather than issue a new card. For this purpose, Card Encoders are used. These let Flag States add information for new certificates, endorse a CoC obtained by a seafarer in another State, extend the validity period of an existing certificate, or withdraw one.

The price of card encoders varies from USD 2,000 to USD 5,000 based on their quality and capabilities. For instance, the smart card encoder packages from CARDWERK are capable of performing smart card personalization, application loading and card customization. (www.cardwerk.com)

After issuing the card, there are some authorities in charge of checking its validity, the most important ones being Flag State surveyors, PSC inspectors and Immigration authorities. Compared to the issuance and revision of information in the card, this is a more frequent operation. On the other hand, as this is only an inspection, the information in the card need not be changed. Here, the biometrics information stored in the card is compared with live samples of the seafarer's biometrics. The information about certificates would also be checked through another comparison, by communicating valid databases of seafarers' certificates maintained by Flag States. This communication could be in different forms, such as a simple dialup Internet connection or a wireless connection to the central station in the port for handheld devices used by inspectors.

Thus, relevant authorities need suitable devices to read card contents, as well as scanning biometric samples of the seafarers and comparing them. These devices cost around USD 2,000 on the market today. Two examples of such devices are DSVII-SC and DSVerify2D from DATASTRIP, which are portable card readers equipped with fingerprint scanners. (www.datastrip.com)

In addition to FS surveyors, PSC inspectors and Immigration authorities, shipowners, Shipping companies and any other authority dealing with security measures may require these devices.

As already mentioned, seafarers should have easy access to devices which let them see what is stored on their cards. To provide the seafarers with this basic right, issuing States and maybe shipowners/operators will need simplified card readers. The price of such readers is approximately USD 500 to USD 1,000 today. As an example, one could refer to the PCRead2D from DATASTRIP, which is a reader device that connects to any computer. (www.datastrip.com)

5.3.5.2. Platform

Besides all the above-mentioned equipment needed, issuing States will have to build robust IT (Information Technology) platforms. These are mainly computer networks with good communications capabilities to act as the backbone of the system to securely generate and issue cards and maintain credible databases with global accessibility using communications channels such as the Internet.

Although some of the equipment described so far function as a standalone device, software plays a crucial role in the whole system. The cipher algorithms, which code and decode information, communications modules, database management programs and design and control software, are integral parts of the system in different stages of issuance and use of the cards.

As the chosen and acquired platforms and software depend a lot on the State's present IT infrastructure and policies of the related entity, it is not easy to evaluate related costs in this respect.

5.3.5.3. Human resource

Provision of all hardware and software components does not necessarily guarantee an efficient or even working system; management policies and administrative procedures play a big role. If a very good system is in place, but the legislator does not support it, the system will never be used. On the other hand, if the system is not well customized to meet the special requirements of individual States, it may become a total failure. Therefore, the necessary rules and regulations should be formulated or revised to recognize smart cards and the information therein as valid documents in each State's national jurisdiction. Besides the legal framework, there should be clear and efficient administrative procedures with necessary considerations of the situations in each State to support the utilization of new documents.

Training is another aspect of this nature. During the setup and maintenance phases, well-trained people should be in charge of the system. They should be proficient in the new technology, as well as current practices regarding identification and certification of seafarers in the State. The relevant authorities should also be trained on how to operate the equipment and devices. Public knowledge about cards and biometrics also needs an upturn.

5.3.5.4. Maintenance

After the system starts to work, the setup costs are almost complete, but to operate it in the proper way, software and hardware equipment needs to be maintained. This will incur a continuous cost to related entities, especially to issuing States who have a big share of the whole investment. Maintenance costs are also hard to estimate, as they depend on other factors.

5.3.5.5. Cards

Seafarers should receive and hold the card as proof of their identity. Creation of each card has certain costs, between USD 1 and USD 15 depending on its type, which should be paid by the seafarers, or otherwise by the issuing authority. The higher the technology used in a card, the more expensive it will be. For example, cards with barcodes are much cheaper than cards equipped with microchips. However, like many other IT innovations, as time goes by, the cost of issuing each card will decrease.

5.3.6. Obstacles

Several problems could be foreseen underway when talking about the creation of a new entity called SIC. These range from the beginning stages of designing the system to the final steps of implementation, but two obstacles seem to be more significant, as already experienced in the case of ILO's SID.

5.3.6.1. Seafarers' influence

As the new document has to do with the identification and certification of seafarers, one should consider their important role in this respect. The fact that the industry has already experienced opposition against the SID implies that seafarers would not be happy if they were to pay for the card. As GREGORIO OCA, president of the Associated Marine Officers' and Seamen's Union of the Philippines (AMOSUP) said at the Fifth Asia-Pacific Manning & Training conference in Manila, "… the cost of such an initiative was always a major issue in countries such as the Philippines, the world's largest supplier of seafarers." He also proposes "some arrangements should be done to allow State subsidy and cost sharing between employers, manning agents and seafarers". ("Union demands action on ID cards", 2003)

On the other hand, this controversial issue shows that seafarers are discontented by the use of biometrics in the new document. This is rooted in the idea that biometrics

are intrusive and act in the way that human beings lose their privacy rights. Otherwise, the price of USD 1 for a 5-year valid identity card is not a major problem for any seafarer. Even if the more expensive smart cards, costing USD 15 maximum, were employed, each seafarer would have to pay roughly USD 0.25 per month during the 5-year validity period. This is not an expensive service for seafarers, compared to the level of safety, security and services they would benefit from. Yet the workers' federations are probable to raise the problem of card costs on behalf of the seafarers.

5.3.6.2. Costing

One of the obstacles, which usually causes problems in the implementation of new standards is the financial considerations; SIC (or even SID) is no exception. Having realized different stages of the implementation and their relevant costs, it should be obvious that certain entities are greatly concerned with the money they should pay. While it is not difficult for a shipowner or operator to equip their vessels with a couple of devices for the price of USD 2,000, half a million dollars to set up the issuance system is definitely a big deal for some developing countries, many of which supply large numbers of seafarers to the world market.

Therefore, costing would be a big obstacle in the movement of the industry towards a successful SIC. If this problem is not resolved and only a few States get involved, the result will be a multilateral or regional agreement among certain States, rather than a globally accepted solution for seafarers' certification and identification. Implementing a successful international SIC is possible only through active participation of all the related entities.

5.3.6.3. Position of the USA

It should be remembered that the standpoint of the USA against the document is a very important factor. However strong the solution is in terms of security and however reasonable it is designed, if the USA does not accept it, the chances of

global acceptance and implementation will diminish significantly. This is already one of the major obstacles for the ILO proposed SID.

If the USA fails to ratify the relevant instruments and continues to insist on its visa policy for seafarers, which requests individual seafarers to apply for, hang around a certain amount of waiting time and finally get a visa prior to calling at a US port, the SIC could experience the same fate as that of the SID. However, the SIC is far more comprehensive than the SID, and there are certain features in it, such as its pervasive nature, that can encourage the USA to look at it in a different way.

5.4. Implementation of the SIC

Implementation of the SIC is not an easy task, neither is it a short-term project. It is a global endeavour that involves several entities and should be carefully studied, planned and accomplished. To this end, one of the important issues to consider is the document type and biometrics to be employed. As already argued, there is no unique solution with regard to card technology or biometrics; each application in each location may require a special combination of card and biometrics. However, to come up with a global solution for identification and certification of seafarers, a common point should be reached, where most of the requirements, if not all, are satisfied.

At least two entities are involved in the issuance of the seafarers' identification and certification document (SIC): the Nation State and the Flag State. The former is responsible for identity information, while the latter has to do with certificates of competency (CoC) and other documents related to the qualifications of seafarers. Thus, an important part of the job is to define how the two parts will coexist on the same document, with regard to certain differences between the two.

First of all, the identity information is usually static and does not need updates. Name, date of birth, nationality, etc., as well as biometric templates of a person are

rarely changed and so, they are regarded as read-only information. For this reason, the identity data can be stored on a read-only storage like a two-dimensional barcode, as well as on read/write storages. The certification part, however, is quite dynamic; a seafarer may get new certificates or may lose one, many certificates need revalidation after some time, and if the Discharge Book is included in the SIC, continuous updates are needed as seafarers move to other vessels or their role is changed. This makes it impractical to store information related to certificates on a read-only storage. In effect, they need a read/write storage like the magnetic-stripe or microchip.

Secondly, the information related to the certificates is mostly text based, which occupies a small portion of card memory and can be compressed very well using software techniques to occupy even less. However, the identification information also includes pictures and biometric templates, which need more capacity and compress less.

Considering the above situations, it is possible for the two items to coexist in one storage medium by assigning separate parts to each, which would be dealt with by the different entities in charge. As a substitute, it is also possible to use two separate storage media, one read-only for identity and one read/write for certificates. The latter solution may have an advantage over the former, for its potential compatibility with the current standards. For example, if the SIC needs to be compatible with the SID cards proposed by ILO, employing a two-dimensional barcode to keep identity information and a magnetic-stripe or microchip to store certificate information can provide the required compatibility. This may allow the SIC card to be, though partially, recognized by those who are already using the SID. Moreover, it can enable ratifying States and other entities to upgrade their existing systems, instead of starting from scratch.

On the other hand, having two storage media on a card means higher costs, resulting in extra expenses for those who do not have systems in place. Thus, it can be said

that the type of combination of the two data sets also depends on the number of States ratifying the C185 convention. To make it more realistic, one should consider the actual implementation of the SID by countries, rather than the ratification status.

In any case, as two different entities in different States are to handle the SIC cards, there should be clear instructions and complete technical definitions on the rights and responsibilities of each State regarding the storage media.

Considering the identity and certificate information as two separate entities, there are some common items in both, such as name, date of birth, nationality, etc. In a combined document like SIC, such data items should be stored only once. Thus, shared items should be specifically assigned to one category, either identity or certificates, which will then make a particular State eligible to deal with it.

5.4.1. Card

As discussed in section 4.2, cards have different levels of security. To achieve the goals of the SIC and especially to prevent fraudulent practices in the certification of seafarers, it is necessary to choose a secure card for the SIC. The best choice for this purpose seems to be smart cards equipped with microprocessors and built-in security logic.

These cards, as explained in section 4.2.2, provide high levels of security by using complicated cryptography methods to encode information in the card, which prevent access to the data in the card's memory. Some models even allow data operations to be done inside the card, instead of reading the card contents into a reader machine, which makes the card even more secure, and fraud and tampering much more difficult. Notwithstanding the high security they can provide, the cost of using these cards may rise as an obstacle. However, alongside the technological improvements in microelectronics, the reduction in the price of IT equipment is anticipated.

As an alternative, simpler and cheaper versions of smart cards such as memory cards can be used. Although these cards do not offer all the security measures present in the microprocessor cards, they have the potential to be reliably used if relevant security measures are observed. These measures include employing powerful ciphering methods and the use of a secure communication channel between the card, the reader device and the databases.

A third choice can be the magnetic-stripe card, which is not as secure as the smart card, because the information in it can easily be read and even modified by anyone who has access to a reader/writer. Nevertheless, it is still possible to use these cards to store and retrieve seafarers' identity and certificate information in a relatively secure mode. Here, employing powerful ciphering techniques can be a reasonable measure to code the data on the card, but this is not a perfect security measure, as there is always a risk for cryptograms to be hacked. The advantage of magnetic-stripe cards over smart cards is that they are considerably cheaper to produce and operate. This is because of the simpler technology of magnetic stripes, which has turned these cards into a low-cost solution.

5.4.2. Biometrics

Selection of the biometric identifier is an important issue for any application. As can be seen in Table 10, the Iris and Fingerprint are the first and second best choices for authentication of the seafarers. So, one may decide that Iris recognition should be used for this purpose. However, it should be noted that the resultant scores in this method are not enough to choose the right biometric identifier. The mismatch calculation method can give a general idea of which biometric identifier may be better than the others. Besides, by altering some of the parameters, or even by changing the scores used to digitize the analogue values of "low", "medium" and "high", the final mismatch scores may change. In effect, some of the parameters used to calculate the mismatch scores may considerably change depending on the time and place of the application.

However, Iris and Fingerprint are the two top choices. Iris, as described earlier, is still non-mature and thus, expensive to implement and use. Fingerprint is mature and much cheaper, but still considered as obtrusive by most people.

Fingerprint recognition can be a good choice for two reasons. Firstly, ILO has already discussed the use of fingerprints. This, along with the other applications of the fingerprint in daily life, can rectify the negative perceptions about it and introduce this biometric identifier as a good measure to enhance security. On the other hand, compatibility with ILO's decision to use fingerprint recognition is a measure to avoid the change for those who have already started to use or develop their authentication system based on the ILO standards.

Secondly, in the case of seafarers, fingerprint samples can be acquired more easily, compared to the other biometric identifiers. For example, in comparison with iris scanning, fingerprint sampling is done much faster and with less effort.

Considering the conditions in the aviation industry, which is ahead of the shipping world in the field of biometrics, can also be useful. This sector of transport has chosen face recognition as its select biometric identifier. This seems to be in contrast with scientific findings, which suggest that face recognition is not distinctive enough for large populations and so, its scalability gets a low score. An important point to notice about aviation is that besides face recognition, ICAO has authorized individual States to choose another biometric identifier, such as fingerprint to be used in conjunction with face recognition.

This highlights the idea of strengthening the whole system by combining two (or more) biometric identifiers. In this way, the two biometric identifiers can complement each other and result in a more secure system. However, it is obvious that using more than one biometric identifier adds to the costs, requires more time and effort and can complicate the situation. While this appears to be a good solution

for extremely high security applications, using more than one biometric identifier to verify the identity of seafarers can be more problematic than useful.

5.4.3. Combination

Considering a combination of cards and biometrics, there are some interrelated aspects that should be considered. First of all, the biometric sample is stored in a memory structure on the card. As the memory has a limited capacity, the digital representation of the sample (the biometric template) should not take up more than a certain amount. This also depends on the card type. For example, as the capacity of barcode and magnetic-stripe card is much less than the chip cards, a suitable biometric template for them should be as small as possible.

Besides its effects on the selection of biometric identifiers, the limited capacity of the cards is also linked with the feature extraction techniques. Emerging software technologies make biometric templates smaller, which allow storage of bigger samples on smaller memories. However, some of these methods may reduce security by losing details of the biometric sample, which can result in bigger values of FAR, and thus, lower accuracy.

Moreover, the card type can directly affect the biometrics used, in terms of security. In barcode or magnetic-stripe cards, almost all the operations are done in the reader device. Thus, the authentication process requires the template to be transferred from the card memory to the reader device, which is a potential for interception by forgers. On the contrary, chip cards equipped with processors can provide higher levels of security, by preventing the original biometric template from leaving the card. In other words, instead of exporting the biometric template to a reader machine and matching it against the sensed biometric sample, the scanned biometric sample data enters the card and the comparison is done on the card. This can, to a large extent, prevent illegal access to the original biometric template on the card.

5.4.4. Databases and their interconnection

Like the requirement set in ILO C185 convention, the creation of the seafarers' databases is a necessity for the successful implementation of the SIC. This should be done, both by the Nation State and the Flag State, to keep valid information about seafarers for checking the validity of the documents and authenticity of the seafarers.

Although the application of smart cards and biometrics can provide a reasonable level of security, it is always possible to have fraudulent cards, as there is no absolute solution for forgery. Therefore, it may be necessary to check the validity of the card contents by comparing them with the real information. This real information should, thus, be stored and updated in a database by the issuing State when the card is issued or updated. In this way, it would be possible for the relevant authorities to access the database and check the validity of the information.

Regarding the SIC, there are two databases involved; one for identification information and one to keep information about seafarers' qualifications, neither of which is new to the shipping world; the latter has already been addressed by IMO for CoCs and the former has been introduced by ILO for SIDs.

The STCW convention requires all parties to "maintain a register or registers of all certificates and endorsements … which are issued, have expired or have been revalidated, suspended, cancelled …" and also to "make available information on the status of such certificates, endorsements and dispensations to other Parties and companies which request verification of the authenticity and validity of certificates produced to them by seafarers…."

The ILO C185 convention obliges members to "ensure that a record of each seafarers' identity document issued, suspended or withdrawn by it is stored in an electronic database…" and to "designate a permanent focal point for responding to inquiries, from the immigration or other competent authorities of all Members of the

Organization, concerning the authenticity and validity of the seafarers' identity document issued by its authority…."

However, the important point regarding the SIC is that it needs both databases, one for verification of the seafarers' identity and the other for checking the validity of their certificates. Thus, there should be either a single database covering both categories, or two separate databases with an interconnection.

The first one does not seem to be practical, as the SIC is produced and issued by - at least – two authorities in two phases: phase 1 by the Nation State and phase 2 by the Flag State. Subsequent updates may be done by both, or even by third party authorities. If all seafarers get their certificates from their Nation State and work there, it would be possible to have a common database for the identity and certificate parts, but this does not usually happen. Thus, to have a common database, there should be a shared entity between all the States, as each State has relations with a number of others. This is not an easy goal to achieve, as there might be many conflicts of interests.

Therefore, the second choice should be considered; each crew-supplying State should create and maintain a database for its seafarers regarding their identity and each Register should make and maintain a database for the seafarers onboard its vessels concerning their certificates. The databases should be structured so that the relevant authorities can easily access to verify both the information about identity and the certificates of the seafarers. The structure should also guarantee uniqueness of the information stored for each seafarers. This can be done by assigning each seafarer a unique identifier in the databases. For example, a combination of the seafarer's name, date of birth and nationality can be a good identifier. Another choice can be a unique code made up of a country code, for the issuing State, plus the serial number on the card. By using this method, it would be possible to address a specific seafarer in all existing databases all over the world.

It is the duty of the DataBase Management System (DBMS), used to maintain certificate databases, to check the validity of the identity information prior to enrolling a new seafarer in its database, or while updating the data for an existing seafarer. The certificate DBMS should also communicate with other certificate databases when a certificate issued by another State is being endorsed. Therefore, communications among databases is an important requirement of the system.

Thanks to the Internet, communication among databases can be established at a reasonable cost. The connection channel could be provided by the port facilities, by the ship data communications itself or by the checking devices equipped with wireless communications.

Nevertheless, one of the most important points in relation to the databases and their communications is protection against unlawful access, which can threaten the security of the whole system. Without secure communication channels, the data can be hacked and illegally used by hackers. Thus, all possible measures should be employed to ensure that only authorized entities could access the databases.

5.5. Removing the obstacles

As mentioned in earlier discussions, the two major obstacles for implementing SIC would be the seafarers' negative influence and costing. Regarding the former, it should be noted that opposition to change in an existing system, especially by those who are closely involved in the system, is an identified issue. However, this resistance usually decreases when they properly understand the change and its pros and cons. For this reason, dealing with the opposition against identity/certificate cards by seafarers requires training, as seafarers need to know the benefits they would gain from the new system. In today's shipping world, where there are several news items everyday about the problem of shore leave, seafarers would be in favour of the SIC if they realized its potential to solve the problem of shore leave, as well as the other benefits it can give them.

In order to help seafarers understand the system and its benefits, it is necessary to first convince seafarers' unions through seminars and workshops. Actually, the more seafarers know about the system, the higher is the chance for the SIC to succeed. In this respect, priority should be given to major crew-supplying States.

Regarding the influence of the USA on this system, there are some measures to be taken. For example, inclusion of certain information such as the Discharge Book can provide more valid background information for the immigration authorities. On the other hand, a step further is to negotiate the relevant authorities in the USA prior to the adoption of any new instrument, to realize the situations that could actually satisfy the needs of the USA and lead to the acceptance of the SIC.

In effect, part of the opposition of the American authorities is because of the current widespread security problems they face, with a feeling that American interests are being threatened by different modes of transport. If this problem is resolved, or at least moderated in the future, acceptance of the new documents by the USA can be expected.

Notwithstanding the importance of other obstacles, costing could be considered as the most demanding problem in the actual implementation of the SIC, which needs to be studied in more detail. The following discussions try to analyze the issue and examine possible solutions for it.

5.5.1. Costing

Notwithstanding the importance of other factors, the more demanding obstacle regarding the SIC would be costing. To come up with any solution for this problem, one needs to carefully consider different stakeholders and their relationships. As already described, there are several entities that need to pay for hardware, software and human element. Some of these entities are able and willing to invest in the SIC, while some others may be either unable or not willing to pay.

The amount of money stakeholders should invest depends on their role in the whole process. This can be measured by considering the operations they would perform on the SIC cards, biometrics and the seafarers' database. Table 11 shows the stakeholders and their respective roles.

As identity checking is a combination of card operation (Read) and scanning the biometric sample, it requires additional equipment or peripherals. On the other hand, as each State should create a database containing valid information for checking validities and the authenticity of seafarers, stakeholders should also deal with this issue. For most of the entities, which only need to access the database to read information, this is not very costly, especially by considering cheap communication methods available. However, two entities will have to create the database and keep it up-to-date, which demands considerable amounts of money.

Table 11 – Role of SIC stakeholders

Operation on the card / Stakeholder	Create and update card	Read card contents	Check identity	Create and update database	Read database contents
Port State Control	×	✓	✓	×	✓
Flag State Surveyors	×	✓	✓	×	✓
Shipowners/companies	×	✓	✓	×	✓
Immigration authorities	×	✓	✓	×	✓
Crew-supplying States	✓	✓	✓	✓	✓
Registers	✓	✓	✓	✓	✓
Seafarers	×	✓	×	×	✓

Source: Compiled and inferred by the author

As can be observed in Table 11, crew-supplying States and registers are the two stakeholders with the maximum role, and consequently, more burdens on their shoulders.

5.5.1.1. Estimated costs

To go further to the issue of costing, there should be an estimate of the amount of money that each stakeholder should invest to enter this business. As there are different devices with varying prices for each purpose in the market, in calculating the costs, the higher price threshold is considered. This is to have all potential requirements of the relevant entity covered, without any shortcoming in security.

Besides, the estimation does not cover training and maintenance required for actual operation of the system. The main focus of this section is the implementation phase.

Port States

To perform the inspections each PSC inspector needs to have a hand-held device to check the cardholder's biometrics and card contents, approximately ***USD 2,000*** each. The important point here is that PSC inspections are usually delegated by authorities to Recognized Organizations (RO); yet, the ultimate responsibility lies with maritime administrations. Therefore, they need to have the required equipment and knowledge to observe the inspections to ensure the quality of the RO's job. Considering an average number of 5 inspectors for each port, then:

Equipment Cost = 5 x 2,000 = 10,000 USD

Flag State surveyors

Similar equipment is needed here, approximately ***USD 2,000*** for each surveyor. Flag State surveys are usually delegated to Classification Societies (CS), but the maritime administration is responsible for making sure this is being done properly. Thinking about roughly 20 surveyors to each maritime administration, the cost would be:

Equipment Cost = 20 x 2,000 = 40,000 USD

Shipowners/companies

At least one system is needed, either a computer equipped with the necessary peripherals or a standalone system for authentication of the seafarers and checking their certificates. These devices would cost less than ***USD 2,000*** for each ship. As an example, the same considered for Port State Control can also be used here. Moreover, ships may also require an Internet connection to access the seafarers' databases, but as the checking is usually done when the ships are in ports, this is not a significant cost for ships.

If it is required by the Flag State, ships should also set up a card reader device onboard to let seafarers read their cards. This would cost each ship an extra ***USD 1,000***. Thus, the total cost for each ship could amount to:

Equipment Cost = 1,000 + 2,000 = 3,000 USD

Immigration authorities

What immigration authorities usually need to do is to make sure of the seafarers' identity, which is done by biometric authentication of the cardholder. Thus they will need devices for this purpose, of a cost of about ***USD 2,000*** each. While immigration authorities can use portable machines, they are also capable of using cheaper devices that are not standalone, but connect to a computer, since they usually have their offices equipped with computers.

Crew-supplying States

The most complicated costing structure belongs to the crew-supplying States. As these should issue the cards, they need to have the platform and all necessary equipment to produce blank cards, then to personalize them and subsequently to issue each seafarer a card. In addition, they need to enrol seafarers in a biometric system, transfer biometric templates to the cards, and create and continuously update a national database of seafarers.

For this reason, it is not very easy to estimate the costs for this stakeholder, although rough figures can be calculated. As already mentioned, for the purpose of this study, the process of creating blank cards (phases 1 and 2 of the smart card life cycle) is put aside. Thus, it is supposed that the crew-supplying States will use 3rd party, ready-made blank cards and would not involve in the process of producing blank cards. In this condition, only card printer/encoders are needed, which cost maximum ***USD 20,000*** each. Approximately 5 such devices might be needed for each crew-supplying maritime administration.

On the other hand, the establishment of a platform for issuing SIDs will need a computer network linked to the Internet, as well as a database management system to handle seafarers' database, which would cost around ***USD 200,000*** to set up and make operational.

Equipment Cost = 200,000 + 10 x 10,000 = 300,000 USD

Registers

A simplified system as described for crew-supplying States is needed for Registers. To deal with cards, registers need card encoder devices, which cost around ***USD 5,000*** each, as they should update card contents regarding seafarers' certificates.

Each Flag State would require around 10 devices of this kind. The required platform for Registers should include a network linked to the Internet, as well as a database management system to keep and handle information about certificates issued by that State. Such a platform would cost registers roughly ***USD 100,000***.

Equipment Cost = 100,000 + 10 x 5,000 = 150,000 USD

Seafarers

Seafarers may or may not need to pay for their card, depending on the regulations set by individual governments. The cost of issuing the most expensive card for each seafarer would be around ***USD 15*** for a five-year period.

5.5.1.2. Acceptability

Port State control inspections are mainly done by ROs as a service for money paid by Port States. Thus, ROs should also enter this business. Nevertheless, this could be considered as an upgrade to the service they provide for Port States, which could be compensated by an increase in the prices. As a result, Port States pay only a fraction of the real cost they would have paid without using ROs. In effect, the investment of Port States for the SIC, which is estimated around USD 20,000 for each port (refer to section 5.5.1.1), is not a big deal.

This is also a valid discussion regarding Flag State Inspections; maritime administrations that delegate the job to Recognized Organizations will pay only a fraction of the actual cost. Thus, albeit they are not as rich as ports, they will not be in trouble to pay the one time cost of USD 40,000. For shipowners/companies, USD 3,000 is an acceptable cost, compared to the other expenses of having a vessel in service.

Immigration authorities are the next in line. Logically, they will have to pay for the necessary equipment, as they are the ones who wish to authenticate seafarers. Otherwise, they may decide not to use biometric identity cards, and verify the identity of seafarers based on passports or other identity documents. However, this is not the expected approach, as one of the main reasons for the creation of SID or SIC is the fact that seafarers are refused to go ashore is that some States do not accept the current documents. So, upon the creation of a globally acceptable document, most immigration authorities seem to be willing to pay for equipment that will help them authenticate seafarers more easily and with higher levels of security.

Crew-supplying States have the most challenging situation. In effect, these States should pay the biggest share among all stakeholders. On the other hand, most of them are developing countries, which makes it hard for them to justify the expenses and eventually pay for the equipment and human element required to set up the document issuance system. Thus, while most industrialized countries can afford to do the job on their own, developing countries will experience major problems to catch up with the standards.

Registers also have a significant share of the costs, but unlike crew-supplying States, most of them are not in trouble to meet their share of the costs. These are one of the primary beneficiaries of the SIC system and are willing to pay for the implementation of the system that will benefit them more. The activities already done by some open registers such as Liberia to implement a similar system can further support this idea.

Finally, the maximum of USD 15 for each card is much less than what a seafarer would have to pay for a visa application for one of the countries he is going to visit. As already explained, considering a 5-year valid card, a seafarer pays around 25 cents of a US dollar per month, which seems to be tolerable. However, it may cause some resistance in the beginning.

5.5.2. Solutions

As a result, there are some stakeholders with lower levels of expenses, who are willing and likely to pay, and some others with a bigger share, who are either not willing or unable to pay. Thus, a solution is needed to solve the problem by bringing the latter entities in. The most important entities in this group are the crew-supplying States and seafarers. To this end, several solutions could be suggested, with their specific strengths and weaknesses.

5.5.2.1. Only Flag States

One possible solution is to ignore the whole idea of obliging Nation States to issue identity documents for their national seafarers. Then, Flag States would be responsible for issuing the SIC themselves. As Flag States were already responsible for issuance of the CoC, the only added responsibility for them would be to include the identity information into the document. In practice, however, the change is more demanding for Flag States, as they would have to do the first phase of the SIC as well, which is to issue the card. This is much more than what they had to do in the proposed shared SIC system, i.e., to update the issued card with the certificate information. Yet, most Flag States, especially open registers, would be willing to pay the costs of implementing a nationwide SIC system, as they are the major beneficiaries.

If this method is to be followed, as the Nation States are accountable for identity documents they will have no responsibility to set up the platforms and pay for the equipment. On the other hand, as already explained, the costing structure suggests that the other stakeholders can afford to pay for the required expenses. In effect, such a solution could change the whole concept of the SIC, and all previous discussions should be revised. For example, as only one State is involved, there is no need for coordination between two States. Many of the requirements would also be satisfied with simple solutions, as they exist merely in the national spectrum.

However, this solution will face a real problem regarding the identity of seafarers. As already discussed, Nation States are the most competent entity to decide on the identity of the seafarers. Although it is possible to check seafarers' identities through negotiations with the Nation States, Flag States cannot achieve the same level of confidence with regard to the seafarers' identity. Thus, the resultant document would not be as strong with respect to the identity section. Furthermore, some Flag States may decide not to join, as they may see their current systems as being quite successful.

5.5.2.2. An international electronic card company

There are several big electronic card companies, which are already in the business, mostly for banking applications. Some of them like the HSBC, which has over 50 times the whole international maritime workforce in its card carrying customers, are believed to be able to do the job very easily for the whole international maritime workforce. (Grey, 2004)

This suggests that instead of implementing the system in all crew-supplying States and Flag States, the job could be delegated to a company, which would then issue the documents and keep them up-to-date. This removes the need for States to buy and install various sets of equipment, as well as the necessary knowledge to acquire such; all the States would make use of the services provided by the relevant company. This, in itself results in a much shorter time for the implementation of the SIC, as well as a higher level of efficiency, due to the existing experiences of the company.

The solution is not free, as no company would give a service for free. However, as only one entity is to set up the issuance system, a few installations at certain focal points in different parts of the world would be enough. Thus, the total cost of implementing the system would considerably decrease, and thus, the service provided by the company could be much cheaper.

However, because of the limited number of installations, for many States, the cards should be posted to the States after the card is issued or updated. Thus, there would be a time gap between the request by a State and the actual delivery of the card, which is a potential source of problems.

On the other hand, it is arguable whether all States accept the solutions proposed by a company, especially in the case of security measures, such as the encryption algorithms and other security measures used to protect the data on the card and in the databases. This is a controversial issue, as many States prefer to have exclusive methods regarding security measures. Design and maintenance of the databases that

contain information about a State's nationals may also be a matter of concern. From the privacy rights point of view, this solution potentially leads to complex situations, as the firm that has control over the biometric, as well as certificate data, can use them for commercial purposes. There is also a lasting concern about the unanticipated use of the seafarers' data, as it might be directed to certain authorities that are not meant to access such information. These are also relevant issues at the national level, but when an international company is to set up the whole system, there may turn out to be major problems, especially by adding the political interactions and disputes to the picture.

5.5.2.3. A fund

Another solution to consider is to set up a fund, primarily to help developing countries to set up platforms, buy software and hardware equipment and implement the issuance system. Providing these States with financial aids and expert knowledge will give them the opportunity to set up the platform, implement the system and maintain it successfully, thus strengthening the global system. The question then is "who should contribute to this fund?"

Logically, those who benefit from the successful implementation of the system are the best choice. As already mentioned, Registries and shipowners have considerable interests in the successful application of a global SIC. Port States are also interested, since such a document contributes to higher levels of safety and security in port facilities, and would save them time and money. Hence, big Registers, shipowners and Port States are potential contributors to a SIC fund.

5.5.3. The SIC Fund

In setting up a fund, the most important issue is to define contribution criteria, based on which, various contributors and their shares are determined. While careful examinations prior to this determination can bring about successful establishment of a fund, inappropriate conditions and unsuitable factors will result in problematic

situations. In setting the conditions, one should have a practical approach, in that some stakeholders, despite their crucial role, may not be willing to contribute, which can adversely affect the whole system. Thus, acceptability is a vital factor to consider.

On the other hand, the receiving entities and the payment criteria should be clearly identified, to determine who and how much should be received. There should also be an estimation of the total amount of money that should be paid by the fund.

5.5.3.1. Donors / Recipients

In the case of the SIC Fund, as already discussed, major eligible receivers from the SIC Fund are crew-supplying States in developing countries, which, despite their specific economical problems, need to pay the biggest sum to implement and maintain the issuance system. Nevertheless, some Flag States also face difficulties with respect to setting up the card updating system. To make the SIC more successful, inclusion of such Flag States also seems to be a wise decision.

Potential contributors of the SIC Fund are big Registers (Flag States), shipowners and Port States. Among the three, the latter is not easy to include in the list. As Port States indirectly benefit from the SIC, through improvements in the safety and security of the vessels calling at their ports, they may not be willing to contribute unless they experience the system and its actual success.

Shipowners are the next, with a good level of acceptability. However, it would not be easy to enforce the fund with direct involvement of the shipowners, as they are big in number and scattered in location, which can cause many problems in the practical implementation of the SIC. As an example, collecting the contributions from the shipowners, itself, would be a big problem. Thus, they should be involved indirectly, probably through a different entity. Big Flag States and especially open Registers are the most practical stakeholders to be directly involved. With high acceptability due to their direct connection with seafarers, big Registers are

potentially interested in the successful implementation of the SIC. As already described, the SIC can benefit Registers by helping them overcome fraudulent certificates, as well as by enabling the vessels under their flag to comfortably employ crews from various nationalities, without the apprehension of facing problems regarding shore leave and professional movement. On the other hand, most of the Flag States are members of IMO and ILO, which makes it easier to have them involved in the system, through ratification of the relevant instrument by the State. This is not true of shipowners, who do not have such a straightforward link to the law-making bodies.

Considering the above-mentioned issues, in order to have a more focused discussion, it is supposed, hereinafter, that the contributing entities are the Flag States that allow foreign crews onboard their registered vessels. As already mentioned, these are the most probable stakeholders to pay for the fund.

5.5.3.2. Total value of the fund

Earlier discussions show that the focus of the SIC Fund should be on the establishment of card issuance systems in developing countries, mainly for crew-supplying States and Flag States (registers), which can not afford to pay for it. Thus, an estimate of the total cost for each country is required.

Considering the cost structure mentioned in section 5.5.1.1, each crew-supplying State would need at around USD 300,000 to have the system implemented. If 100 States were supposed to need help from the fund to set up the issuance system, the sum would be USD 30,000,000. On the other hand, Registers require USD 150,000 each. Considering the same number of 100 countries, the total would be USD 15,000,000. The total estimate would then be roughly USD 45 million, which should be provided by the SIC Fund.

If the matter of seafarers turns into a crucial issue, it is possible to add another item to the fund as a special feature to compensate seafarers for the first card issued to

them. As already mentioned, the card cost will amount to a maximum of USD 15 for each seafarer. Having around 1.2 million seafarers all over the world, the maximum amount of money required would be USD 15 x 1,200,000 = USD 18,000,000. The total value of the fund, including this special item, would total USD 63 million.

5.5.3.3. Contribution bases

The amount of money to be paid by each contributing entity needs a calculation basis. Such a basis should be rational, so that different stakeholders find it fair and also can satisfactorily participate in it. Obviously, an appropriate basis is necessary for a fund to be successful.

One simple way is to divide the total value by the number of contributors and demand equal shares from each, but this may cause an imbalance due to the different financial capacities of various entities. An alternative can be to base the contributions on the economic power of the States, namely the Gross Domestic Product (GDP.) In this way, regardless of the situations of the shipping industry in each State, the richer countries should pay the bigger share. In effect, the States' economic strength is definitive in this method, i.e., even if a country is very strong in the shipping business, but not very wealthy, it will pay the lesser amount.

The alternative solution can be to base the contributions on the number of registered vessels. This is a different method, in that it demands more active maritime States to pay more, regardless of the economical power of the country in charge. A potential negative outcome of this method is that it may put an extra burden on the aspiring maritime States, like some open registers, which are trying to develop through the shipping sector.

Another potential basis for calculation is the number of foreign seafarers onboard each State's registered vessels. The rationale behind this criterion is to oblige the States that employ a cheaper work force to pay for the benefits they get out of it. Obviously, the shipowners earn more from this opportunity, and the Registers can

demand a share from them, through the registration fee. To justify this criterion, another argument can also be made: Flag States normally have the responsibility to issue documents for the seafarers working onboard their registered vessels, but as some of them use foreign seafarers, they are actually shifting part of their duty (the identity part of the SIC) to the Nation States; thus they should contribute to the fund, so that the Nation States can implement the system and issue the document instead of them.

Nonetheless, it is possible to get better alternatives by combining some of the above-mentioned bases. As an example, the combination of a State's GDP with its number of registered vessels can result in a basis that addresses both the economic power of the State and the benefits it gets out of the shipping industry. To make the calculation basis even more comprehensive, one can add the number of foreign crews onboard a State's registered vessels to the combination. This leads to the consideration of all advantageous involvements of a Flag State in the shipping business.

Therefore, the contribution of each State can be defined as a function of a its GDP, number of registered vessels, and the number of foreign crews onboard its registered vessels.

$$C = f\left(T, S, V, GDP\right)$$

C = Contribution of the State
T = Total Value of the fund
S = Number of foreign crew employed by the State
V = Number of registered vessels in the State

As a result, each State would have to pay an amount of money to the SIC Fund, which would then be distributed to eligible crew-supplying States and Flag States.

Further description of the contribution criteria and a sample formula is presented in 0.

5.5.3.4. Seafarers to pay

Besides the contribution criteria already mentioned, a second option could also be chosen by the industry. As already mentioned, seafarers are one of the primary beneficiaries of the SIC. Thus, it is possible to have them pay for it. This solution would please the owners and other stakeholders, as they who would not need to pay, but may also lead to opposition by the seafarers.

If this is to happen, total value of the fund should be shared among paid by all seafarers of the States which receive money from the SIC Fund. Share of each seafarer can be defined by dividing total value of the fund, estimated around USD 63 million, to the number of seafarers in such States. If, for example, the number of seafarers from crew-supplying States was around 1 million seafarers, each seafarer would have to pay around USD 63 when he/she receives the new document.

In this way, seafarers would pay after the system is implemented in their country, while the implementation needs money beforehand. Thus, a loan may be needed for the fund, to be remunerated after the systems are in place in each country, and seafarers pay for the cards.

5.5.3.5. Implementation

Although the SIC Fund is aimed at helping developing States to implement the SIC issuance system, maintenance of the system is also a matter of concern for some States. Thus, the maintenance costs should also be considered. In fact, the fund should be clear on what aspects it covers and what it does not. If the SIC Fund is to cover only implementation of the SIC issuance system, each State should receive the money once in a lifetime. Thus, the contributors may also pay only once.

Conversely, if the fund is to cover maintenance costs, the contributions may need to be paid on a continuous basis.

Furthermore, it is not possible to have the system implemented at once, all over the world. It will take some time until the States can actually have the system established. Likewise, States also join the fund gradually. Thus, even if the fund covers only implementation costs, it should be operational for several years. To this end, an organization should be created to manage the fund in harmony with its mandates.

One of the responsibilities of this organization would be to determine the amounts of money to be paid to different States. This could be done by acquiring a group of experts in biometrics, IT and card technology, or by receiving professional advise from third party organizations. If the latter is chosen, the issue of conflicting interests should be carefully considered.

Besides, there are various procedures that, if precisely defined and followed, can make the fund more efficient. For example, although it is preferable that each State has its own card production standard and ciphering method for the purpose of better nationwide security, by using a shared method among several States, the costs would credibly decrease. In determining the best procedures to be followed for this purpose, expert knowledge should be used to make sure the security and integrity of the whole system is not compromised. As a supplementary measure, the system can be more efficient if the States receive consultations on how to implement and maintain the system. These can be other duties of the organization in charge.

5.5.3.6. Problems and implications

The biggest problem in front of the SIC Fund would be non-participation of the States. The problem may deteriorate if the calculation of the contributions is not on a globally agreed basis. Like any other fund, collection of the money from contributors is another problem, which demands considerable amounts of time and

energy from the fund organization to have the due contributions paid. Political problems also play a role here, where some States may oppose the payments by the fund to certain States, due to the existing disputes or for other political reasons.

Another relevant issue is related to the policies of individual States regarding the payment of contributions. As already mentioned, some States, more likely the open Registers, may decide to demand a portion of their share of the SIC Fund contribution from their registered vessels, by including a new item in the registration fee. This is a measure to help States satisfy their commitment, while making profit in the market. However, some States may choose another way; for example, a State with a defined contribution of USD 5 million may decide not to join the fund, and instead, invest a portion of the money to set up the system for a major crew-supplying State, from which most of its vessels employ seafarers. This allows the State to pay much less, and at the same time, gives it a better position in the market, due to the fact that it can avoid demanding anything from the shipowners for the purpose of the SIC.

Chapter 6

Conclusion

6.1. Conclusion

In today's world, identification of seafarers is crucial to satisfy security requirements. Moreover, seafarers' certification is a matter of real concern, especially from the safety point of view. These two aspects have recently become more important due to the increasing focus on security and the fraudulent practices in the certification of the seafarers. The result is a negative consequence for the seafarers, who are being refused their vital right of shore leave. Although the two relevant UN organizations, namely IMO and ILO have tried to address the issue in different ways, the problems persist. Even the urgent initiative of ILO is suspended because the member States do not ratify the new convention, even though it was adopted on a consensus basis. Yet, the ILO proposed solution, by ignoring the issue of certification, leaves part of the problem in place.

To overcome the above-mentioned problems, a proper solution should be established, capable of addressing both relevant aspects; i.e. identification and certification. This study tries to find a solution, by examining different aspects of the seafarers' identity and certificates, the new technology in IT and biometrics, and the integration of the seafarers' identity documents and certificates of competency.

The study's objectives are attained by introducing a new combined document for Seafarers' Identity and Certificates, or the SIC, and subsequently examining its different aspects. The SIC is a smart card in combination with a biometric identifier, to be initially issued by the States of nationality of seafarers, completed and subsequently updated by the Flag State, and be used by all relevant entities such as the immigration authorities and PSC inspectors, to authenticate seafarers and check their qualifications.

This document is, to a large extent, capable of solving the problems of fraudulent practices in the certification of seafarers and refusal of shore leave by some States. However, this can happen only if the major stakeholders accept and ratify it, which is a known requirement for any rule or regulation developed for international implementation. In particular, success of the SIC depends on how the USA treats it, as a big part of the problem is rooted in the refusal of shore leave in USA ports. This has already been experienced, regarding the non-ratification of the ILO C185 convention by the USA, which is clearly in contrast with the fact that "the quest for an internationally approved, universally recognized identity document for seafarers was launched at the behest of the US." (Grey, 2004)

Due to the continuous improvement of IT and microelectronics, it is very difficult to find a comprehensive and permanent solution as the suitable technology for the SIC. This can also influence implementation and other relevant issues. For example, all the expenses allotted to a SIC project may need to be paid again, to acquire the newly arrived technology. Frequent changes in the equipment and methodology can also lead to major problems in maintenance, training and support of the systems. Nevertheless, it is always possible to choose flexible methods, which allow gradual upgrades whenever necessary, without having to change the whole system at once.

The results of this study suggest that using fingerprints in combination with microchip smart cards can be a suitable solution for the time being. In order to be compatible with the ILO proposed solution, the card can contain a barcode to store

identity information on it. The proposed solution is also flexible in using other biometric identifiers as a supplement to the main one.

However, probable opposition of the seafarers is not a trivial issue. As the SIC intends to serve seafarers, the first step is to meet their satisfaction. This is possible by assuring them that the pros exceed the cons. Yet many seafarers do not know what a smart card is and what biometrics means. There are also some misconceptions that can worsen the situation, such as the idea that biometrics means DNA sampling and authentication using biometrics would require a piece of the body. False impressions like this can also have an impact on deterioration of the shortage of seafarers, by discouraging potential seafarers from going to sea.

To overcome these problems, necessary training should be delivered to seafarers and even to ordinary people, especially those in the crew-supplying States. Considering the practical application of the SIC, seafarers should be well aware of what they are using, what are the weaknesses of the system and how to combat potential attacks against their biometrics and the attacks on their cards at the social level.

Notwithstanding the significance of training, when it comes to the actual implementation of the SIC, costing is a major issue. This is especially important by considering that ICAO has proposed a different identifier, i.e. face recognition, as some States may need to spend twice as much to have both systems.

As most major crew-supplying States are developing countries, they might face serious problems in setting up and maintaining the card issuance system. Yet, they should have the expensive system in hand, as each State is the most competent authority to issue an identity document for its nationals. On the other hand, Flag States have already faced the requirement for an integrated solution such as the SIC; some have even started to test a similar system, before an actual implementation in near future. However, there are other views that disapprove of this system, due to the incompetence of the Flag State regarding the identity information.

Thus, there are some major beneficiaries such as open registers, who are willing to undergo the necessary costs to have the system implemented, and on the other hand, there are some major crew-supplying States with financial problems, which prevent them from establishing the system. A reasonable solution should yield a balance between these two interests. While there can be several answers to this problem, the study suggests a fund to be established. The main contributors of the fund could be the Flag States that employ foreign crews onboard their ships, and the main receivers would be the crew-supplying States.

The fund is focused only on the implementation of the system and does not consider the training and maintenance. However, for practical implementation of the system, these aspects should also be addressed, either by adding their relevant costs to the fund value or by any other measure, such as encouraging States to assist others attain an appropriate level of knowledge and experience.

In conclusion, the SIC may be a good idea. To make it a good solution, all the stakeholders in the shipping industry should take an active part, and be vigilant in having it implemented.

6.2. Further studies

The focus of this dissertation is on examining the combination of the seafarers' identity documents and their certificates of competency, and possible solutions for this purpose. Obviously, actual implementation of the idea requires more detailed investigation in some fields. As explained in 5.3.2.1, the involved States should be coordinated. The applicable methods of that coordination should be studied and analyzed. Harmonization of certificates is the next issue, which is a requirement for the actual implementation of the SIC. The harmonization should be thoroughly studied, and the resultant solution should allow all the involved States to practically deal with the cards, both in issuance and updating the SIC and in checking the CoCs on each card.

Moreover, acceptability of biometrics and cards by seafarers, from the social point of view, is a credible subject to elaborate on, as this can significantly affect the success of the SIC among seafarers. In such a study, practical methods of improving the seafarers' knowledge about biometrics and cards and their pros and cons should be considered.

The idea of the SIC FUND should also be investigated in more detail, especially the contribution basis, the contributing stakeholders and the method of contribution, which are matters worth expanding more.

Why does the USA not ratify a USA-customized convention? This question needs to be academically answered. The answer could then be used in the development of future conventions, to give them a better chance of success.

Finally, the actual methods of implementing the project, including the technical aspects related to both biometrics and smart cards, should be examined and focused on in a separate comprehensive study.

References

Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. *Ethics and Information Technology, 5*, 139-150.

Ashbourn, J. (2004). *Practical biometrics: From aspiration to implementation*. New York: Springer-Verlag.

BIMCO, ISF, & U. Warwick (2000). *The BIMCO/ISF 2000 manpower update: the world-wide demand for and supply of seafarers: main report*. Coventry: University of Warwick.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). *Guide to biometrics*. New York: Springer-Verlag.

Doumbia-Henry, C. (2000). *Background paper on the International Labour Organization and on its maritime activities*. Geneva: International Maritime Law Institute.

Doumbia-Henry, C. (2003). Current maritime labour law issues – an internationally uniform identity document for seafarers. *WMU Journal of Maritime Affairs, 2*(2), 129-148.

Firms Line up for Panama ID card contract. (3 May 2004). *Lloyd's List*, p.3.

Grey, M. (2004 August 2). Check out this check-in common sense … and let's have some of it for seafarers. *Lloyd's List*, p.7.

International Labour Office. (2003). *Effect to be given to resolutions adopted by the International Labour Conference at its 91st Session (2003)* (GB 288/3/2, 288th session). Geneva: International Labour Office.

International Labour Office. (2004). *Follow-up to the Seafarers' Identity Documents Convention (Revised) 2003 (No. 185)* (GB 289/7, 289th session). Geneva: International Labour Office.

International Labour Organization. (1958). *Seafarers' Identity Documents Convention*. Retrieved June 20, 2004 from the World Wide Web: http://www.ilo.org/ilolex/english/convdisp1.htm

International Labour Organization. (1959). *Record of proceedings, 41st session of the International Labour Conference, 1958.* Geneva: International Labour Office.

International Labour Organization. (1976). *The impact of international labour Conventions and Recommendations*. Geneva: Author.

International Labour Organization. (2003). *Seafarers' Identity Documents Convention (Revised 2003)*. Retrieved June 20, 2004 from the World Wide Web: http://www.ilo.org/ilolex/english/convdisp1.htm

International Labour Organization. (2003a). *Report VII (1): Improved security of seafarers' identification, Proceedings of 91st session of the International Labour Conference, 2003*. Geneva: International Labour Office.

International Labour Organization. (2003b). *Report VII (2A): Improved security of seafarers' identification, Proceedings of 91st session of the International Labour Conference, 2003*. Geneva: International Labour Office.

International Labour Organization. (2004 March 26). *ILO takes major step to ensure security of seafarers*. Retrieved May 25, 2004 from the World Wide Web: http://www.ilo.org/public/english/bureau/inf/pr/2004/12.htm

International Labour Organization. (2004). *ILO Conference Adopts Convention on Identity of Seafarers: Balances Security and Seafarers' Rights*. Retrieved July 15, 2004 from the World Wide Web: http://www.us.ilo.org/labor/conventions/seafarers_id_oked.cfm

International Maritime Organization. (1965). *Convention on Facilitation of International Maritime Traffic (FAL), 1965*. London: Author.

International Maritime Organization. (2001). International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978 as amended in 1995 and 1997. London: Author.

International Maritime Organization. (2003). *International Ship & Port Facility Security Code and SOLAS amendments.* London: Author.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of fingerprint recognition.* New York: Springer-Verlag.

McLaughlin, J. (2004 July 22). US State Department pushes on with ban on crew list visa. *Lloyd's List*, p.7.

Philippine Embassy in Stockholm. (2004). *Crew list visa*. Retrieved July 12, 2004 from the World Wide Web: http://www.philembassy.se/consulr/crevs.htm

Rankl, W., & Effing, W. (2003). *Smart card handbook*. Chichester: John Wiley & Sons.

Schröder, J. U. (2004). *The IMO/ILO approach to human element*. Unpublished lecture notes, World Maritime University, Malmö, Sweden.

Seafarers International Research Centre (SIRC). (2001). *A study on fraudulent practices associated with certificates of competency and endorsements*. Cardiff, Wales: Author.

UK Immigration & Nationality Directorate. (2004). *Control of Seamen: Practical Considerations*. Retrieved July 12, 2004 from the World Wide Web: http://www.ind.homeoffice.gov.uk/ind/en/home/laws___policy/policy_instructions/table_of_contents/chapter_16_-_seamen/annexes__a_-_e/annex_a_-_control.html

UK supermarket chain trials biometrics. (2004, June). *Biometric Technology Today*, 1.

Union demands action on ID cards. (2003, November 26). *Fairplay Daily News*. Retrieved July 20, 2004 from the World Wide Web: http://www.fairplay.co.uk

US insists that crew list visas must end. (2004, May/June). *The Sea, 169*, 1.

US State Department pushes on with ban on crew list visa. (22 July 2004). *Lloyd's List*, p.7.

Woodward, J. D., Horn, C., Gatune, J., & Thomas, A. (2003). *Biometrics: A look at facial recognition.* Santa Monica, CA.: RAND Public Safety and Justice.

Appendix 1

Sample contribution criteria for the SIC Fund

As explained in 5.5.3.3, the contributions can be calculated by using a formula, which defines the amount of money based on several factors.

$$C = f\left(T, S, V, GDP\right)$$

Supposing that each seafarer would pay the cost of his/her card, total value of the fund calculated in section 5.5.3.2 is USD 45 million. This is the money that SIC Fund needs to earn. Therefore, the factors in the above formula should be designed in a way that the money can be shared among States that employ foreign crews. A sample formula could be as follows:

$$C = T \times \left(\frac{S_f}{2 \times S_t} + \frac{V_f}{2 \times V_t} + GDP\ Factor \right)$$

C = Contribution of the State
T = Total Value of the fund = 45,000,000
S_t = Total number of seafarers = 1,200,000
V_t = Total number of merchant vessels = 50,000
S_f = Number of foreign crew employed by the State
V_f = Number of registered vessels in the State
GDP factor = (GDP per capita – 15,000) / 1,000,000

In the above formula, the two major factors are the number of foreign seafarers, and number of registered vessels. However, the GDP factor plays a moderating role, by adding to or deducting from a State's share, based on its economic power. Those with GDP per capita of more than USD 15,000, which is an average base value, would have to pay more, while the States with lower GDP per capita should pay less.

Some examples:

S_f = 30,000

V_f = 5,000

GDP per capita = 30,000 ⇨ GDP factor = 0.015

C = 45,000,000 x (1/80 + 5/100 + 0.015) = 3,487,500

S_f = 10,000

V_f = 2,000

GDP per capita = 5,000 ⇨ GDP factor = – 0.01

C = 45,000,000 x (1/240 + 2/100 – 0.01) = 637,500

S_f = 100,000

V_f = 8,000

GDP per capita = 15,000 ⇨ GDP factor = 0

C = 45,000,000 x (1/24 + 8/100) = 5,475,000