Isdefe

DIRECTORATE – GENERAL FOR MOBILITY AND TRANSPORT

EPAIC II
Study for the Analysis and the Conceptual Development of a European Port Access System

PROJECT Nº: TREN/G2/180-1/2009

Final Report

Date of Deliverable : 23/12/2010

Start Date of Project : 01/01/2010 **Duration :** 12 months

Document ID : ISEPAE-111396-2RL **Revision :** Final

Executive summary

The terrorist attacks in the US, Madrid and London have shown the vulnerability of transport and the need for Europe to adopt preventive measures in this area. The European Commission thus considers that the implementation of security measures in the field of maritime transport is one of the poles to combat terrorism.

The access control requirements of an international port differ greatly from those of other infrastructures. A European Port Access System must be able to manage general access and area control, parking permits and ID cards, access for employees to the port, terminals and restaurant, access to the customs area and the terminals, commercial traffic, public traffic, red carpet customers, trailers, trains, cars, bicycles, pedestrians, ship crews, maintenance crews, taxis, and emergency vehicles, passengers and personnel. Due to the complexity and heterogeneous nature of the existing environment, a second turn on the existing study is needed.

The main objective of EPAIC II is twofold: to objectively analyse the feasibility and the current information regarding the implementation of a port access identification card from an industry – independent point of view and to propose the basic structure of such a system.

In this context, efficiency, interoperability and a modular architecture are the key features of the prototypes to be studied and proposed in the contract. These factors will make possible a system that:

1. Is easily adaptable to port infrastructure and existing port access control systems, thus reducing migration costs and negative impacts.

2. Is easily adaptable to the security level required in each port, through a configurable security layer schema.

3. Considers previously deployed technologies in its design as well as technologies based on international standards.

4. The whole community of ports within the EPAIC national system deployed can be easily integrated into a common EU-wide system in the future.

5. Functions and processes responsibilities are clearly delimited and assigned to the pertinent entities.

ISDEFE

Isdefe was created in September 1985 with the objective of providing technical support in engineering and consulting services for advanced technologies.

In the twenty-five years which have elapsed since its creation, Isdefe has demonstrated that it is the perfect ally to support the Public Administration in national and International Programmes, especially in the Security and Defence sectors.

Isdefe’s goal is to provide personalised consultancy services and technical excellence in the solutions it proposes, together with strong integration with the client’s objectives. The company’s main values are: independence with respect to industrial, commercial and financial interests, the high level of its professionals’ qualifications, excellence in technology and management, and a clear commitment to technological innovation, security and quality.

EPAIC II methodology

In order to be considered successful, any project has to fulfil its objectives and has to serve its potential users. In EPAIC II, it is clear that the potential final users are the European port community, ranging from port authorities to road hauliers, ship suppliers, terminals' staff and more. Their inputs and points of view are therefore of great value for the purposes of EPAIC II.

The information, however, cannot be collected in any way, but following a methodology. The inputs that EPAIC II considers are:

- Stakeholder's consultation. A questionnaire was carefully made, containing questions whose answers are vital to the project. The nature of them varies greatly and includes technical, societal and economical data, among others such as the perception of the stakeholder towards the adoption of a European port access system. Most of the answers came from ports and up to 26 answered the call.

- Conclusions and results from the first EPAIC study. Since the European Commission incepted EPAIC II as its continuation, the information that was generated in the former was adopted, processed and improved in the latter.

- Analysis of the relevant technologies. Since the beginning, a wide range of different technological solutions was envisaged, and shrank as the project maturated and the best ones were chosen. As examples we can cite biometrics, of which a deep study is offered or the different types of cards.

From the main inputs the requirements were established and the study started to develop, until a point was reached in which a preliminary solution could be offered to the stakeholders. That was done in October 2010 at the SAGMAS meeting in Brussels, were the project was reviewed, providing feedback for the rest of the project.

Regulation and legal issues

Several pieces of regulation affect ports. Some of them emanate from international sources, such as the IMO, while others come from European legislation. The EPAIC II study also got to the member State level.

According to the communication EU COM(2006) 786, ports may be considered as European critical infrastructures. Such infrastructures have to follow a specific regulation in the field of security where, among others, access controls and emergency plan are contemplated. EU Regulation 725/2004 has as its objective the implementation of the ISPS code. Both are identified and its requirements blended into EPAIC II.

Data protection has also to be ensured. Directive 95/46/EC establishes some of the restrictions that systems such as those proposed in EPAIC II have to comply with. The Directive provides a set of legal requirements for personal data to be processed wholly or partly by automatic means in Europe; and how all the Members States have to adopt this Directive in order to be transposed into national regulation, according to the article 4, national law applicable. The concept of personal data is broad and applies to an extensive range of information (text, sound, images) that relate to an identified or identifiable person. The Directive states principles relating to data quality which make data processing lawful and that are embodied in the EPAIC II, such as avoiding data collection on sensitive information or destroying it when it is no longer needed.

However some issues arise when dealing with personal information, such as those relating to the transmission of data. In general European States can do such a thing from one to another, but care has to be put in the generalisation. Moreover, the sources of information are not clear in this respect. The approach of EPAIC II is to collect just as much information as needed and not any more and to reduce data transmission to the minimum possible.

Stakeholders

The first EPAIC project did a good job in gathering information by preparing and sending questionnaires. These contained a large number of questions related to the policy that ports followed regarding access cards, the costs that they incurred in and some others. The aforementioned questionnaires were sent to several ports, with total of answers, and some other organisations were also contacted. However the procedure could be improved and some areas need some clarification. For instance, it is stated that a certain European Haulers Association was contacted but no further information nor contact details are provided, which leads to the fact that it is quite difficult to determine the constituents of the Association.

The approach selected by the EPAIC II project is to adopt similar practices to that of the previous study, to improve them and to add new ones. The starting point is the selection of the stakeholders whose opinions are of importance in order to contact them and, as can be easily understood, ports are among the main players. Since maritime traffic in Europe tend to follow certain routes – for example, the "motorways of the sea" that were established by an agreement between Spain and France – the work was organised around sea corridors. The main ones were selected and a sample of ports within them was contacted. These corridors and their ports are:

- Baltic corridor: located in the North East, is surrounded by many European Member States, including Sweden and Finland and some other non – member States, such as Russia and Norway. The ports selected are those of Turku, Göteborg, Stockholm, Helsinki, Fredericia, Malmö, Riga, Rauma, Århus, Ystad, Szczezin and Swinoujscie.

- North Sea corridor: located between the main European economical centres, including partially the end of the axis that runs from Milan to Stockholm and the Paris and London zones, its neighbours are the Baltic and the Atlantic corridors. Due to the size and economic importance of the cities in this area, ports in the North Sea corridor experience a large activity. The contacted ports are those of Le Havre, Hamburg, Bremen, Rotterdam, Antwerp, Liège, Felixtowe and Liverpool.

- Atlantic corridor: going also by the name of Celtic Sea corridor, it connects peripheral areas in Europe which have been historically somewhat less developed than other areas. In 2009 two motorways of the sea, the first one connecting Gijón and Nantes – St. Nazaire and the second one serving the ports of Algeciras, Vigo, Le Havre and Nantes were officially established. The selected sample for EPAIC II covers the ports of Gijón, Vigo, Dublin, Bristol and Nantes – St. Nazaire.

- Mediterranean Sea corridor: rich in history, the Mediterranean serves nowadays Southern Europe as an excellent passageway and the best solution to reach some the many islands that are surrounded by it. The ports contacted by EPAIC II are the ones of Algeciras, Barcelona. Valencia. Alicante, Tarragona, Marseilles, Genova, Livorno, Bari, Patras and Thesaloniki.

With the addition of the port of Seville, in an inland location and between the Atlantic and Mediterranean corridors, a total of 37 ports were directly contacted, as well as a number of them through indirect mechanisms, such as associations. Those ports are located in 14 European Member States (Finland, Sweden, Denmark, Latvia, Poland, Germany, France, Spain, Italy, Ireland, United Kingdom, The Netherlands, Belgium and Greece) and they returned up to 26 questionnaires, a figure that allows for an appropriate analysis.

But the opinion of ports is not the only one to be considered. Many other actors, such as road hauliers, workers associations and many others have points of view, recommendations and criticisms to make and the EPAIC II study has tried to collect as many as possible. Since targeting individual companies is too a long work to be carried out, the selected approach is to target associations and to send them questionnaires as well as concrete questions and even some of Isdefe staff could present the project during a SAGMaS meeting. The following is a list of the associations that were contacted:

- European Sea Ports Organisation (ESPO)
- Baltic Ports Organisation (BPO)
- Federation of European private Port operators (FEPORT)

- European Association of Airport and Seaport Police (EAASP)
- European Tugowners Association (ETA)
- Confederation of European Security Services (CoESS)
- Eurochambers
- European organisation for Security (EOS)
- European harbour Masters Committee (EHMS)
- European Confederation of Shipowners Associations (ECSA)
- Organisation de la Communauté Européenne des Avitailleurs de Navires (OCEAN – ship suppliers organisation)
- European Dredging Asssociation (EuDA)
- European shippers Council (ESC)
- European Transport Workers’ Federation (ETF)
- Confederation of European Shipmasters' Associations (CESMA)
- European Maritime Pilots Association (EMPA)
- European Federation of Inland Ports (EFIP)
- European Boating Association (EBA)

Port access control systems state – of – the – art

The social and economical weight that ports represent makes them critical sites that should be protected accordingly. That has led in the introduction of control access systems all over the world in a process that is still under development. EPAIC II analyses some of them, as can be seen in the following paragraphs, in order to include the best solutions into the final recommendation.

The identification system used in the maritime facilities of the United States is called Transportation Worker Identification Credential (TWIC) and is based on an identification credential for all personnel in ports requiring unescorted access to specific areas, facilities and vessels. This system is also mentioned in the first EPAIC study although some important information should be added.

TWIC identification system has been designed to fulfil the security plans defined in the MARSEC system, which represents the three-tiered United States Coast Guard Maritime Security system created to be compatible with the Homeland Security Advisory System. Thus, TWIC is structured to be compatible with several security layers. Data are stored on the surface (name, photograph, employee affiliation, expiration date, etc.) and in a chip (biometric templates, personal identification number, a security 16 byte encription key and a security object). It possesses several advantages, such as the possibility to work in two different modes; the biometric data are enciphered; no information is transmitted from the reader to external networks (a feature that European privacy protection laws would require) and personal data are signed by the authorised user. However, it also presents some disadvantages, namely the authentication of the reader is not considered and the information, although ciphered is actually sent to the reader, among others. All in all, TWIC shows some of the characteristics that the EPAIC solution should have.

Alfapass is the identification card for regular visitors developed by the Belgian port community, represented by Alfaport Antwerp. The main goal of Alfapass is to avoid frequent visitors the burden of carrying several badges, one for each port or terminal. It is currently in use in the ports of Antwerp, Zeebrugge and Ghent. On the surface there is a number of data, namely: name and surname, date of birth, coloured photography, nationality, card number, card validity date and employer. The card has an embedded chip that may be used to store holder’s biometric information, although it up to the port facilities to use it or not. The chosen biometric patterns are hand geometry and fingerprint. The technology employed in the card is completed with contactless Mifare smartcard. Alfapass is intended for several categories of regularly visitors: port labourers, lorry drivers, facilities personnel, temporary visitors and others, such as quay shipping agents. The card serves as an identification mechanism and access rights are always managed by each port facility owner, which is desired feature, as indicated in the following sections.

The port of Rotterdam employs its own card, called *XSkey PortKey*, which offers identification and access control capabilities. Data about the holder and the employer are stored within a Mifare chip, along with access rights to facilities. The card is prepared to withstand the hard physical conditions in ports.

The Seafarer’s Identity Document (SID) is backed by the homonymous international convention of 1958, although some changes have recently been implemented. It enables seafarers to go ashore in foreign ports after perhaps weeks or even months on board, and means for joining their ship or for transit across a country for professional reasons. Each ratifying member of the convention shall implement a national electronic database and designate a permanent focal point, in order to manage SID verification inquiries from competent authorities of all members, which is also a very interesting characteristic for EPAIC. The SID does not affect ports, although it possesses some characteristics of interest. However, the recent adoption of a new standard for biometric templates has brought worries to many Stares, so that only some of them have already ratified it.

The Maritime Security Identification Card (MSIC) is employed in Australia and is issued to identify people who have been subject to background checks. The holder meets minimum security requirements and may work unescorted or unmonitored. No access control is derived from this card and hence each port could request its own card, so the holder may end up having many of them, which is one of the burdens that EPAIC wants to ease.

The Marine Transportation Security Clearance Program (MTSCP) was initiated in January 2003 with a commitment to introduce background checks of workers at marine facilities and ports in Canada. The holder may have undergone a security clearance, in which case the relevant information appears in the card. The regulation also claims for the use of restricted area passes conceded to these individuals, proving they hold the needed authorization. As in the Australian case, it is only an identity and authorisation proof and not a control access technology.

The European Union has adopted a new type of electronic passport, called *ePassport*, which includes biometric prints (including finger and iris). It introduces cryptography in communications but does may be too expensive for ports to implement.

The port of Barcelona has set up a project, known as PROATRANS (Transport Access Restructuring and Regulation Plan), in order to implement a specialised plan to adapt the logistics community, and in particular the land-based container freight sector, to current legislation on competition and the free market. In this project a credential containing relevant information is produced, allowing lorry drivers an easier access to terminals while maintaining security. The effectiveness of PROATRANS should be taken into account while designing EPAIC.

EPAIC model approaches

The first EPAIC study generated a high level architecture comprising three main subsystems: a central European system, a national one and local system in each port. Those three parts have different responsibilities, duties and capabilities, depending on the relations among them. EPAIC I defined six different relationships, creating thus six different models. Each one was analysed and finally two of them were proposed as starting point: the centralised and the hybrid models. The characteristics of both are, as defined in the precious study:

In the central data, both data and logic (functionality) are concentrated in the European subsystem. National subsystems act as simple gateways to provide access to the services supported by the system and local subsystems and their end-users are connected to the system's services via their respective national systems. Benefits of the central model are the ease of administration and integration of new member States to the system, but the main disadvantages are the high cost of the communication infrastructure, a poor performance of the authentication processes due to the high traffic load within all the system, and the high dependence of a single system node.

In the hybrid model, data and business logic are shared between the central and the national infrastructures, with the European subsystem providing also interconnection capabilities for the national systems. This model decreases drastically the communication infrastructure costs with the central system and improves the authentication process efficiency, but the administration and maintenance complexity is higher. Thus, complexity of the national level systems increases significantly, dealing with bigger systems, and one per Member State. This translates into increased costs for hardware and software, biometric infrastructure, etc.

The analysis, however, may be improved, as done in the EPAIC II study. In fact, some conceptual issues need to be addressed before making any proposal, for instance, in the definition of the proposed models a clear separation between identification and access control is not found. In the present study this separation is considered a relevant factor to take into account, as each process requires different requirements and roles to be managed. The research done in both EPAIC I and EPAIC II shows that port authorities want to keep the rights to authorise entrance to their premises. That is to say, a valid card should be enough to authenticate (the card is not forged and belongs to the holder) and identify (the holder is who claims to be), but the port authorities and the facility owners should have the last word concerning who can enter and who cannot. Exceptions could be done, of course, regarding State security officers or during emergency situations, for example.

Moreover, The different approaches to the architecture presented in EPAIC I do not take into account one of the conclusions obtained from the stakeholder consultations: most of the potential users enter just one port, while only a minority visit several ports on a regular basis. Therefore it is recommended to consider a model with different user roles depending on their mobility between EPAIC system ports.

Both models will be used a basis in EPAIC II, but another feature is to be defined: biometrics. The previous study analysed four different techniques, namely fingerprint, iris recognition, hand geometry and facial scan. The present project studies them in more depth, reaching two main conclusions: biometrics should be chosen as an additional tool, as the ports operating with Alfapass already do; and hand scan is the preferred technique. Data protection, however, should be a high priority, to avoid this sensitive personal information to fall in the wrong hands. Security measures such as data ciphering, communications over secured interfaces, disclosure prevention or use of privacy enhancement technologies should be implemented when possible.

Gathering information

The present study places a great effort in obtaining new information from stakeholders and in analysing it. To achieve that objective the first step is to understand the potential users of the system. The identified stakeholders belong to the following general categories:

- Ports, belonging to the transport corridors listed in the previous sections.
- Transport companies
- Workers associations
- Maritime international organisations
- Terminal owners
- Ship suppliers

In agreement with DG-MOVE, organisations were contacted via e-mail, phone, interviews and occasional seminars, meetings and conferences. Moreover, with the purpose of gathering the highest number of answers the European Commission acted as a multiplier to contact and motivate the users. In this sense, the EC prepared a support letter for Isdefe activities in EPAIC II and facilitated access to some stakeholder groups (as FEPORT, Federation of European Private Port Operators) and working groups (SAGMaS).

Once the stakeholders were identified, the following phase involved obtaining information from them, a process that stretched up to the final days of the project. Part of the effort involved creating a questionnaire to be sent to the stakeholders, covering aspects related to the port access requirements, existing infrastructure and deployed technologies, possible EPAIC system user types, etc. In brief, the sections of the document are as follows:

- First, a general section including questions about the systems already in use and the perception of the stakeholders about a unified port access card system.
  - General questions: does the stakeholder use a similar card access system? What are its overall characteristics?
  - Display and verification. How are the cards displayed and verified, along with the identity of holder?
  - Economic part about the cost of the current system, and the benefits or possible drawbacks of a migration to a unified solution as that of EPAIC.
- Secondly, technical questions about how the system used by the stakeholder is actually employed.
  - Credential and information. How is the card designed? What kind of information is stored in it? What are the security measures implemented?
  - Card lifecycle management. How can someone enrol? Are there background checks? How is data protected? Are cards taken care of after their holder ceases to need them?

The number of responses was not as high as expected, due to a range of possible reasons such as reluctance to answer without a tangible gain or the difficulty in finding contact people in ports. However, enough answers were received to make the appropriate analysis

The responses were classified depending on their precedence (e.g. ports were grouped together and in transport corridors) and information was extracted from them. In fact, several requirements and considerations were identified among which are:

- Even when there is a common control access to the port, each terminal tends to manage another one of its own. In some cases there is not a general access control since the port trust completely those in use in the terminals.
- When several access systems are running together they generally use different technologies. For example, licence plate recognition and a PIN code.
- When cards are use, usually only one type is deployed.
- Users include port authority staff, workers from companies operating inside the port, other port workers, visitors and seafarers, although the latter should be treated separately.
- In most cases the cards for different groups are clearly separated, with the bigger difference between temporary and others. For example, different colour badges for visitors and regular staff.
- Port authorities tend to separate authentication from authorisation.
- A few ports externalise the issuance of cards to private companies, but in most cases the systems are owned and managed by ports.
- Most port accesses do not comply with SID (Seafarers Identification Document) standards.
- Most ports do not use biometrics but they are regarded as highly desirable option.
- MiFare is one of the most extended technologies for cards, although magnetic stripe is also used.
- The most common data requested to the holder during the enrolment phase are complete name, photography, work address, date of birth, identification documents (such as passport) and biometrics (when used). In addition to those, some others are stored: employer, holder role, access rights, card unique identification number and expiry date.
- The most common data on the surface of the card are complete name, photography, date of birth, employer, holder and card identification number.
- The most common data in the chip are access rights, card identification number, expiry date and biometrics (if used).
- Cards tend to be valid for about 3 years.
- Card enrolment and termination are usually initiated by the employer or by the port authority.
- About 40% of ports do not follow card audits.

42% of ports are willing to adopt a European access control system, while 33% oppose the idea and 29% did not answer. Since it is not an absolute majority and if we assume that most of the ports that did not respond to the questionnaire might dislike the idea, we would face a scenario in which the implementation of a mandatory, Europe – wide EPACI system could be almost impossible, although a gradual approach could be feasible.

The main concern about the adoption of EPAIC (52% of answers) is the migration cost. Some ports have already made an investment in access security and worry about been compelled to change everything and acquire new material and follow new operations. On the other end of the spectrum, some port authorities find access controls of no use to them (although of interest for terminals) and have no plans to set up any entrance limitation. This leads to the conclusion that opposition to EPAIC could be lowered if selected approach takes into consideration the most common current solution in order to reduce migration costs. And the foresaid opposition could diminish even further if ports are force to make just the minimum inversion necessary, leaving part of the responsibility to the terminals and facilities within them.

The questionnaires also show that complying with SID convention is not a priority among ports and is not regarded as a crucial security improvement. This situation can be due to a number of reasons, such as the fact that most access control checks for ship crew and passengers are actually performed by police, customs and port border agencies and thus port authorities are not responsible for these checks; regular documents, such as visa and passport, are enough for that purpose; ports and port facilities are focused on other types of users; and finally, current SID has only been signed by a limited number of countries.

However some ports stated that EPAIC could entail some benefits, mainly in economic terms, since they find that savings in operational daily costs (in terms both of time and money) could be attained. And going beyond ports, other stakeholders have expressed in many occasions their deep interest in the implementation of an EPAIC system. Among them road hauliers, ship suppliers and in general those having to enter more than one port are numbered.

Cost – benefit analysis and impact assessment

The cost benefit analysis constitutes a burning point of the study. As shown in the document, most ports have already implemented its own control access system, normally supported by a great investment. From the analysis a relatively low interest in a hypothetical European access system has emerged. The benefits of a new security measure is not simple to be calculated especially when the benefit itself lacks of a market value and then the cost of implementation has not a direct relation with it.

The study analyzes at a very high level the costs to be supported by the port to implement a control access system based on a European card.

The cost of migration varies from port to port and depends on the level and type of investment already done. Most of the ports already have a control access system based on cards so that the cost of migration will be limited to adapt the existing system to the new one, but there are ports which do not have any access control system or the one they have is not based on cards. There are also ports, like the port of Hamburg in which the control access system is only managed by terminals owners inside the port.

Even the port size, the volume and the type of merchandise are important variables to be considered by the time to decide on the implementation of a European access control system. Probably a port where mostly no dangerous goods are moved does not need a higher level of security and then it would not be interested in an investment of that range.

Without doubt a European card access system will bring a lot of benefits, such as:

- to better organise people, trucks, car, haulier flow with an increased logistic organization and consequently a better use of time,
- to enhance port security, minimizing the possibility to counterfeit,
- to facilitate integration between ports by using only an access card accepted and recognized by all participants which will reduce current differences
- to ease the administrative and legal work that companies have to deal with
- to make way for the foreseen increment in road traffic entering and exiting ports, since allowing for a faster entrance could also raise the capacity of ports and so more vehicles could enter them.

In some cases, however, the total cost of the investment does not justify the sum of the investment.

The data acquired shows a very different situation in which the cost of one gate can vary considerably form port to port and also shows the different interest that ports have in the implementation of a European access control system.

That is why, in ports where the investment has been considerably, the cost of migration will have to take in account all the components of the existing system which could be reutilized. Every port authority or terminal owner should be able to know more or less which of the existing fixed assets could be reutilized and then to know roughly the investment required implementing the new control access system.

The implementation of such system, besides the direct costs related to the investment, has to manage with other problem such as data protection. One of the mayor problems met in proposing the implementation of a common European card is the level by which data can be managed due to the different protection data legislation in Europe.

Currently, there are licence and security certificates that could be used as a solid foundation for a central recording and administration of system of transport providers both on member States and on an EU – basis. The great number of different personal data required and the use of so many different items in EPAIC would produce a system complex to manage with an increase in the cost of databases and in time needed during the enrolment phase.

But the legal problem is the most critical because some pieces of information, such as gender, are considered as sensitive information in some States. In case background checks should be required, there are barriers which cannot be crossed such as medical and criminal records.

For this reason a minimum set of data to meet security needs should be decided within the EPAIC system. To manage more information than the minimum required, even if could increase security level, would be too costly and maybe not so useful for the proposed aim.

Proposed conceptual development of a European port access system

An underlying principle that has driven the creation of the final model in EPAIC II is to follow, to the extent possible, the current trends in port access security and to generate the minimum trouble for ports to adapt to the new system. That is why the opinions of the stakeholders, shown above, have been taken into account for the model proposed in this section.

The main concepts could be summarised as follows:

- The access control should be applied in two different levels: at port – wide, less restrictive one (mandatory for those ports that join the EPAIC system) and at an optional and more restrictive terminal – level. This will provide flexibility to the solution.
- Card authentication is the basic factor, although it is completed with an optional biometric identification system, based on hand scan.
- Holder personal data do not have to be transmitted outside the card.
- Some information needs to be transmitted and shared among different member States. However the system is designed as to send just card – related information, and not personal data.
- The card will present the most common features among ports as well as physical and logical security measures. It will be based on *MiFare* technology.

- Card Lifecycle described in this design will require an enrolment, card production and issuing, renewal and updating, revocation and termination procedures.

The proposed architecture takes into account two important aspects: access control management and holder role nature. Regarding the former, ports and terminals keep total control on who enter their premises, although exceptions can be done to authorities and to emergency and security services. Pondering migration costs, flexibility and complexity, the best option is to outsource the service to an external company, so that the port needs to maintain a minimum infrastructure while achieving full security and confidence.

When examining holder roles, a fact emerges: most users do not enter more than one European port. That is, a big percentage of users can be regarded as local users. Others, however, need to move from port to port (lorry drivers, ship suppliers, etc.) and can enter in the category of mobile users. These two classes, local and mobile, need two different approaches, as it is shown below. Apart from them a third class can be taken into consideration, that of visitors or temporary users that go to a single port on rare occasions.

The first EPAIC study identified six different models and chose two of them as the preferred ones. In EPAIC II they have been studied and, along with our own research, a new mode of operation has been selected, one that can be named "enhanced hybrid model". It consists on an adaptable combination of distributed match – on – card and national – centralised access control system compatible with European operation, with minimal sized data transmission between systems and no holder personnel data transmission from Member State to Member State.

The final proposal consists on three different subsystems grouped in a general one called card management system. These three subsystems are:

- Local port card management system. It is mandatory (for ports inside EPAIC), own by each port authority and should be applied at least at the entrances to the port, although it can be deployed at other locations. It is intended for local users and for visitors. Each port authority shall also develop a full card lifecycle infrastructure capable of managing card application, in-house production and deliver, as well as card renewal, upgrading, revocation and termination implemented procedures. Facilities and terminals within the port can join the system while keeping authorisation rights.

- Outsourced card management system. It is intended for those ports where the current card management system is already outsourced. The aim is local users. The services are supplied by third parties to the port authority and to those terminals and facilities requesting it, although a local office shall be present at the port.

- European card management system. It is a sole European system, intended for mobile users. It will allow this kind of users for fast and easy identification at all ports in EPAIC. Either port authorities or facilities within them can ask for the deployment of the system, although the former are in charge of the card lifecycle, including enrolment and issuance of the cards. Therefore a local office is needed in each port. National systems are connected together in order to exchange information about the cards.

The cards have some mandatory features (physical security measures to avoid forgery, logical security measures to protect information within them) as well a set of common data (name, surname, photograph, etc.). They are able to introduce an optional security measure based on biometrics, specifically on hand geometry.

The data collected during enrolment are:

  - Card holder complete name

  - Card holder picture

- Card holder birth date
- Card holder nationality
- Card holder signature
- Valid identification document (passport or other)
- Card holder’s company or responsible organization
- Address of company or responsible organization
- Biometric sample to be stored inside the card, if required by applicant.
- Initial access rights, holder role type, card unique identification, expiry date, and issuer identification are set during the enrolment process, but not provided by the applicant

The data on the surface of the card are:

- Card holder complete name
- Card holder picture
- Card holder company or responsible organization
- Address of company or responsible organization
- Expiry date
- Issuer identifier
- Port identification number, outsourcer provider identification number, member state national system identification number
- Card holder role identifier
- Local user, mobile user, or visitor or temporary user

The data stored in the chip are:

- Identification of the issuer
- Card holder complete name
- Card holder employer: card holder company or responsible organization.
- Employer address: contact address for the holder's company.
- Biometric minutiae.

Finally, the data in the database are:

- Card holder complete name
- Card holder picture
- Card holder birth date

- Card holder nationality.
- Card holder employer
- Card holder company or responsible organization
- Address of company or responsible organization
- Issuer identifier
- Port identification, outsourcer provider identification, member state national system identification
- Access rights
- Card holder role type
- Card unique identification
- Expiry date

The model proposed in EPAIC II takes into consideration the work previously done, the requirements from the stakeholders, their current systems and their worries, while aiming for high security objectives. The card is for identification purposes, not for authorisation; the cost of implementation is as low as possible and uses pre – existing infrastructure where available; personal information is not transmitted across borders; and although it clearly represents a significant step in the harmonisation process, its flexibility allows for further advancements and improvements.

INDEX

1. BACKGROUND......4

1.1. European Port Access System 4
1.2. EPAIC I Study Basis 4

2. EPAIC II METHODOLOGY 4

2.1. WP1.1: Information Gathering...... 4
2.2. WP1.2: Analysis of Results and Elaboration of System Requirements...... 4
2.3. WP1.3: Second Stakeholder Consultations: Proposed Approaches Presentation. 4

3. REGULATION AND LEGAL ISSUES 4

3.1. Port Security 4

3.1.1. EU Regulation 725/2004 4
3.1.2. EU Directive 2005/65 4

3.2. Data Protection...... 4
3.3. Legal Issues On The Board 4

4. STAKEHOLDERS......4

4.1. EPAIC I Consultation Analysis and Stakeholders...... 4
4.2. Stakeholder Advanced Consultation 4

4.2.1. Ports' Consultation...... 4
4.2.2. Road Hauliers Associations 4
4.2.3. International Associations 4
4.2.4. Workers 4
4.2.5. Ship-Suppliers 4

5. PORT ACCESS CONTROL SYSTEMS STATE-OF-THE-ART 4

5.1. Transportation Worker Identification Credential (TWIC)...... 4

5.1.1. Overview...... 4
5.1.2. System Description...... 4
5.1.3. Data Stored Inside the Card...... 4
5.1.4. Card Applications...... 4
5.1.5. Card Data Object Model with Issuer Signature...... 4
5.1.6. Interfaces...... 4
5.1.7. Authentication Factors Available for Use in TWIC System 4
5.1.8. Operation Modes 4

5.1.8.1. Pros 4

5.1.8.2. Cons 4

5.2. Alfapass..... 4

5.2.1. Overview..... 4
5.2.2. Credential and Information Specifications..... 4
5.2.3. Scope – Involved Parties 4
5.2.4. Enrolment – Issuance Process 4
5.2.5. Conclusion..... 4

5.3. XSkey PortKey 4
5.4. Seafarers' Identity Document (SID) 4

5.4.1. Overview..... 4
5.4.2. Credential and Information Specifications..... 4
5.4.3. Scope – Involved Parties 4
5.4.4. Enrolment – Issuance Process 4
5.4.5. Conclusion..... 4

5.5. Maritime Security Identification Card (MSIC) 4

5.5.1. Credential and Information Specifications..... 4
5.5.2. Scope – Involved Parties 4
5.5.3. Enrolment – Issuance Process 4
5.5.4. Conclusion..... 4

5.6. Marine Transportation Security Clearance Program (MTSCP)..... 4

5.6.1. Overview..... 4
5.6.2. Credential and Information Specifications..... 4
5.6.3. Scope – Involved Parties 4
5.6.4. Enrolment – Issuance Process 4
5.6.5. Conclusion..... 4

5.7. Identification And Validation Within Second Generation ePassport..... 4

5.7.1. Overview..... 4
5.7.2. First Generation ePassport 4
5.7.3. Second Generation ePassport..... 4
5.7.4. Scope – Involved Parties 4
5.7.5. Enrolment – Issuance Process 4
5.7.6. Conclusion..... 4

5.8. PROATRANS 4

5.8.1. Overview..... 4
5.8.2. Credential and Information Spcecifications 4
5.8.3. Scope – Involved Parties 4
5.8.4. Enrolment – Issuance Process 4
5.8.5. PROATRANS Procedure 4
5.8.6. Conclusions 4

6. EPAIC MODEL APPROACHES 4

6.1. EPAIC I Model Review 4
6.2. Considerations to Candidate Models 4
6.3. Considerations About Biometrics 4

6.3.1. Additional Enquiries 4
6.3.2. Conclusion 4

7. GATHERING INFORMATION 4

7.1. Understanding The Users 4

7.1.1. Users identification 4
7.1.2. Contacting users 4
7.1.3. Users classifications 4

7.2. Understanding The User Needs 4

7.2.1. Questionnaire Structure 4

7.3. Response Rates 4
7.4. Requirements Emanating From Ports 4

7.4.1. General Requirements 4

7.4.1.1. Solo And Multiple Access Control System Approach 4
7.4.1.2. Access Control System Scope: Areas To Be Controlled 4
7.4.1.3. User Roles 4
7.4.1.4. Access Control System Management Control And Ownership 4
7.4.1.5. Access Rights Management 4
7.4.1.6. Other Security Access Control Technologies Used In Combination 4
7.4.1.7. SID Compliance 4
7.4.1.8. ISPS Code Compliance 4

7.4.2. Card Related Requirements 4
7.4.2.1. Usage of Card Access Systems 4
7.4.2.2. Checks Performed and Authentication Factors Required 4
7.4.2.3. Biometrics 4
7.4.2.4. Preferred Card Interfaces 4
7.4.2.5. Card Design Preferences 4
7.4.2.6. Card Security Measures Applied 4

7.4.3. Holder Data Usage, Storage and Protection Tendency 4

7.4.3.1. Enrolment 4
7.4.3.2. On Card Surface 4
7.4.3.3. Inside Card Chip Or Magnetic Stripe (If Available) 4
7.4.3.4. In the Card Management Systems 4

7.4.4. Card Management System and Card Lifecycle Aspects 4

7.4.4.1. Card Management System Ownership, Operation And Infrastructures 4
7.4.4.2. Card Management System Data Protection Security Measures 4
7.4.4.3. Visitor and Temporary Cards Specific Requirements 4
7.4.4.4. Audit 4

7.4.5. Port Impressions Regarding Adoption of a New System Such EPAIC 4

7.4.5.1. Port Impressions About Their Current System 4
7.4.5.2. Actual Security Level Achieved In Ports Current Systems 4
7.4.5.3. Willing of Adoption of an EPAIC Control Access System 4
7.4.5.4. Willing Of Adoption Of Other Possible Improvements 4
7.4.5.5. Common Concerns 4
7.4.5.6. Perceived Aspects and Benefits of EPAIC 4

8. COST BENEFIT ANALYSIS AND IMPACT ASSESSMENT 4

8.1. Cost Benefit Analysis 4

8.1.1. Aim of the task 4
8.1.2. Methodology 4

8.1.2.1. Benefit of the Epaic System 4
8.1.2.2. Analysis of the data acquired 4
8.1.2.3. EPAIC II access system 4

8.2. Impact Assessment 4

8.2.1. General aspects 4
8.2.2. Legal aspects 4
8.2.3. Logistics 4
8.2.4. Environmental impact 4
8.2.5. Human and Technical resources 4

9. PROPOSED CONCEPTUAL DEVELOPMENT OF A EUROPEAN PORT ACCESS SYSTEM 4

9.1. Identified Requirements for the System Model 4
9.2. System Architecture Description 4

9.2.1. Port and Facility Access Control Factors 4
9.2.2. Divergence of Holder Roles Nature and Necessities 4
9.2.3. EPAIC I Base Architecture Model 4
9.2.4. Proposed Architecture Model Key Points 4
9.2.5. Integrated Card Management Systems 4

9.2.5.1. Local Port Card Management System (CMS_L) 4
9.2.5.2. Outsourced Card Management System (CMS_O) 4
9.2.5.3. European Card Management System (CMS_EU) 4

9.2.6. Authentication Factors 4

9.2.6.1. Mandatory Authentication Factor ("What I Have") 4
9.2.6.2. Optional Authentication Factor ("What I Am") 4

9.3. Card Holder Roles 4
9.4. Data Model 4

9.4.1. General and Specific Requirements for CMS_L 4

9.4.1.1. Card Authentication 4
9.4.1.2. Biometric authentication 4

9.4.2. Requirements for CMS_O 4

9.4.2.1. Card Authentication 4

9.4.3. Requirements for CMS_EU 4

9.4.3.1. Card Authentication 4

9.4.4. Card data structure and design 4

9.4.4.1. Data inside the card chip 4
9.4.4.2. Proposed EPAIC Card Surface Data 4

9.4.5. CMS data structure 4

9.4.5.1. Data Retrieved for Enrolment 4
9.4.5.2. Data Stored in the Database. 4

9.4.6. Proposed Data Model Key Points 4

10. GLOSSARY 4

11. REFERENCES 4

LIST OF FIGURES

Figure 1 PIV Card Layout 4
Figure 2 TWIC Card Sample 4
Figure 3 CHUID Verification Flowgraph 4
Figure 4 PIV Active Card Asymmetric Authentication Flowgraph 4
Figure 5 PIV Active CHUID Verification + Biometric + PIN Authentication Flowgraph 4
Figure 6 TWIC Active CHUID Verification + TPK Enciphered Biometric Authentication Flowgraph 4
Figure 7 Alfapass Card Look and Components 4
Figure 8 Alfapass Card Issuance Process 4
Figure 9 PortKey Sample Card 4
Figure 10 C-185 Compliant SID Specimen 4
Figure 11 SID Issuance Process Flow 4
Figure 12 Maritime Security Zones 4
Figure 13 MSIC Sample Card 4
Figure 14 ePassport – BAC Session Keys Generated from MRZ Data 4
Figure 15 ePassport - Sample 4
Figure 16 ePassport – Full Data Set 4
Figure 17 ePassport - Chain of Trust 4
Figure 18 PROATRANS card sample 4
Figure 19 Fingerprint Minutiae Processing 4
Figure 20 Iris Scan Processing 4
Figure 21 Hand Geometry Processing 4
Figure 22 Facial Scan Processing 4
Figure 23 Biometric Technologies Comparative 4
Figure 24 Selected Technologies Comparison Against the Seven Pillars 4
Figure 25 Biometrics Market Share Evolution (2004 & 2009) 4
Figure 26 Advantages and Disadvantages of Biometric Technologies 4
Figure 27 Contact list 4
Figure 28 Unique ACS vs. various ACS operating at port 4
Figure 29 ACS coverage 4
Figure 30 ACS users 4
Figure 31 ACS management 4
Figure 32 Access Rights Management included in the ACS 4

Figure 33 Control access system technology....4
Figure 34 SID Compliance....4
Figure 35 ISPS Code Compliance....4
Figure 36 Implementation of Access Systems....4
Figure 37 Grant Access Form....4
Figure 38 Card interfaces....4
Figure 39 RFID interfaces....4
Figure 40 Card design preferences....4
Figure 41 Card security measures....4
Figure 42 Holder data storage....4
Figure 43 Personal data acquired in the Enrolment Process....4
Figure 44 Personal data on Card Surface....4
Figure 45 Personal data inside Card Chip or Magnetic Stripe....4
Figure 46 Personal data in the Card Management System....4
Figure 47 Responsible for card system enrolment process at port....4
Figure 48 Port's satisfaction with their current ACS....4
Figure 49 Interest in an EPAIC approach....4
Figure 50 Concerns about EPAIC system....4
Figure 51 Different Access Control System technologies....4
Figure 52 Card Issuance Authority....4
Figure 53 Overview of the Integrated Card Management Systems....4
Figure 54 Overview of the Local Port Card Management System....4
Figure 55 Overview of Outsourced Card Management System....4
Figure 56 Overview of European Card Management System....4
Figure 57 Biometric authentication procedure....4
Figure 58 Card authentication....4
Figure 59 Biometric authentication....4
Figure 60 Card authentication - CMS_O....4
Figure 61 Card authentication - CMS_EU....4
Figure 62 Glossary of terms....4

LIST OF TABLES

Table 1 Baltic corridor ports consultation 4
Table 2 North Sea corridor ports consultation 4
Table 3 Atlantic corridor ports consultation 4
Table 4 Mediterranean Sea corridor ports consultation 4
Table 5 Other ports and organisations consultations 4
Table 6 Interior ports consultation 4
Table 7 Road Hauliers Associations 4
Table 8 International associations 4
Table 9 Port workers 4

1. BACKGROUND

1.1. EUROPEAN PORT ACCESS SYSTEM

The terrorist attacks in the US, Madrid and London have shown the vulnerability of transport and the need for Europe to adopt preventive measures in this area. The European Commission thus considers that the implementation of security measures in the field of maritime transport is one of the poles to combat terrorism.

The access control requirements of an international port differ greatly from those of other infrastructures. A European Port Access System must be able to manage general access and area control, parking permits and ID cards, access for employees to the port, terminals and restaurant, access to the customs area and the terminals, commercial traffic, public traffic, red carpet customers, trailers, trains, cars, bicycles, pedestrians, ship crews, maintenance crews, taxis, and emergency vehicles, passengers and personnel. Due to the complexity and heterogeneous nature of the existing environment, a second turn on the existing study is needed.

The main objective of the current contract will be twofold: to objectively analyse the information from an-industry independent point of view and to propose the development of a prototype of a port access identification card system based on end-users requirements, the variety of specific needs depending on ISPS code requirements, and other local factors as day-to-day work, information flow, owner of the data.

In this context, efficiency, interoperability and a modular architecture are the key features of the prototypes to be studied and proposed in the contract. These factors will make possible a system that:

1. Is easily adaptable to port infrastructure and existing port access control systems, thus reducing migration costs and negative impacts.

2. Is easily adaptable to the security level required in each port, through a configurable security layer schema.

3. Considers previously deployed technologies in its design as well as technologies apt to use based on international standards.

4. The whole community of ports with the EPAIC national system deployed can be easily integrated into a common EU-wide system in the future.

5. Functions and processes responsibilities are clearly delimited and assigned to the pertinent entities.

Agreement on EU-wide valid information and legal aspects also will be taken into account.

1.2. EPAIC I STUDY BASIS

EPAIC I was a study carried out by the PortIDS consortium and focused on the possibilities for the introduction of a common identification card for all European ports. The project was executed in 2007 so that not much time for a change in the situation has elapsed.

This first EPAIC project achieved the following goals:

- Analysis of the current situation (as of 2007) in European ports of the procedures to obtain access credentials for workers and those needing ingress (truck drivers, seafarers, etc.). A total of 37 ports in the EU were questioned or visited in order to gain information about their practices and those in Norway and Iceland were also taken into account (since they also belong to the Schengen area).

- The type of identification badge in use in every port was identified, along their intended future developments and conditions of issuance. They were compared to each other and with those employed in other countries, such as the United States.

- Review of the advantages and disadvantages of implementing a unified identification system through European ports.

- Analysis of the existing options and legal constraints and propose the best solution for a unified identification system for European ports.

The first EPAIC project proposed the creation of an ID card storing several data about the holder (name, photograph, signature, biometric prints such as hand, finger and iris scans) and issued by a central authority. The possession of a valid card would be enough for the identification of the holder; the authorisation to enter the premises would be responsibility of each port.

The EPAIC I project offers two different models for the management of information and the identification system:

- A centralised one in which all the data and functions are localised at a central facility and the local services request information from it.

- A hybrid model in which some of the data are stored at a central system (e.g. indexes) while the biggest ones are located at national systems.

2. EPAIC II METHODOLOGY

Any project can only be considered successful if its outcome serves its potential users. However, the collection of information and requirements is of a special relevance in our project. This situation arises from two main sources: on the one hand, the previous project EPAIC has to constitute a sound pillar for the present initiative. Since the present project is a continuation of EPAIC, the work performed by the latter has to be taken as an input. On the other hand, it is necessary to gather information from the main stakeholders, which comprises ports and their security services, including their needs as well as their views on the different technologies and solutions proposed.

It is required the definition of a proper methodology for requirements collection, which will merge the previous work of EPAIC, the stakeholder's point of view and the efforts and skills of the staff to find all the requirements that fits a conceptual model of a European prototype in the best way possible. It is divided into three different phases where each phase is developed in a different task of this work-package WP1:

2.1. WP1.1: INFORMATION GATHERING

As explained in the Annex to the Contract, the methodology is basaed on a triangulation process, in other words, it uses more than one technique to gather requirements. The process consists in a triangulation of Stakeholders Consultations (interviews and /or questionnaires) with data from the interaction with Working Groups (as for example SAGMAS), and results from EPAIC as a fundamental pillar.

- ***Stakeholder consultations.***

  Stakeholder's necessities and recommendations are considered as great value inputs. Taking into account this approach, the first task in this phase will be further stakeholder consultations (via questionnaires) above those in EPAIC first study to gather any necessary information of all European ports considered, mainly focused on interoperability and existing system compatibility aspects (particularly, topology, structure, infrastructures, necessities and control access organisation and procedures of the ports should be considered for the study).

  More in-deep consultations (i.e. interviews) shall be done to ports of Spain, where the Barcelona port could take a relevant role because it is quite pro-active in the area of control access systems such as PROATRANS plan, and it is based near other important European ports, as Valencia or Marseille ports.

  The procedure will start with the creation of one, or more if needed, questionnaires to be sent to the stakeholders. The set of stakeholders will be composed by a large number of ports from all over Europe, fitting up to some point those selected in the past EPAIC project. The questionnaires will primarily cover aspects related to the port access requirements, existing infrastructures and deployed technologies, possible EPAIC system user types, etc. One of the main goals is to model the different port typology according to security requirements. The responses will be gathered and their information extracted to be part of the output for the next phase.

  This task will include the elaboration of questionnaires, and the processes of sending and receiving them with the results to/from stakeholders, respectively.

- ***Conclusions and results from the first EPAIC study.***

  The first EPAIC study is considered to be the baseline of the study performed in this project. So, in parallel with, or even before the stakeholders' consultations, a deep analysis of the results and conclusions of the EPAIC first study shall be done. All the information related to the proposed models and industry's and stakeholders' interests will be prioritised.

- ***Analysis of the relevant technologies state of art, normative and legal aspects.***

  This third task will deal with information gathering processes related to technological and legal aspects, to compound a map of the latest available technical specifications.

  The main aspects to be faced in this task will focus primarily on:

  - Further technical analysis with a more in-deep focus on the chosen system model, and oriented to a national port access control system approach. This would include a necessary study of the existing national network infrastructures that could handle the proposed system network traffic and processes.
  - Find and analyse new or widely used available technologies and their standardization context related to the project that could be applied to the chosen system model functionality. This would include, for example, smartcard or card reader technologies, id card authentication schemes, etc.
  - Examine the normative and the legal aspects that could affect the manipulation of personal data that could be required by the EPAIC system to perform its functions. Confidentiality and ownership of data shall be considered, as well as the nature (private, public) of the possible entities responsible of the processes that handle this sensitive data (card registration and validation, authentication checks, etc.). The analysis shall be made from national and European perspective, concerning port security sector and protection of critical infrastructures in transport sector as well.

2.2. WP1.2: Analysis of Results and Elaboration of System Requirements

All collected data (raw initial data) from the previous phase will be the input for the current one. This will consist of data analysis and the generation of a complete set of requirements. All of this will constitute a more complete, refined and better structured input than the raw initial data for the next cost analysis (WP2) and solution proposal (WP3) work packages. The different types of requirements are shown below in next sections.

2.3. WP1.3: Second Stakeholder Consultations: Proposed Approaches Presentation

Finally, the different approaches will be presented to some end – users. The latter will be further elaborated and polished in the corresponding WP2 and WP3. The end–users will be composed of main ports as well as other potential users or clients of cards: road hauliers, terminal owners among others. This procedure will not only aid to the production of a neatly finished outcome, but it will also serve as a form of validation made with the help of end – users.

This phase will take as inputs the current proposals from WP2 and WP3 at that moment, and will generate, based on them, a executive presentation or report, in order to present the different proposed solutions to the end-users.

3. REGULATION AND LEGAL ISSUES

The creation of a unified identification system for European ports brings several legal issues to consideration. Such a system implies somewhat the distribution of personal information (e.g. fingerprints, hand and iris scans, etc.) among several port authorities, which impacts directly on privacy. And the Schengen convention, to which most European States belong to, creates constraints and opportunities for the EPAIC system.

According to the communication EU COM(2006) 786, ports may be considered as European critical infrastructures. Such infrastructures have to follow a specific regulation in the field of security where, among others, access controls and emergency plan are contemplated. This leads to the possibility of storing some personal information related to these processes as, for instance identification data of an access-card; therefore a policy of data protection must be taken into account in order to guarantee the privacy of the users.

Next section summarises the legal framework in the port security field as well as the data protection required for storing the information in the European Union.

3.1. PORT SECURITY

In order to facilitate security of ports, port facilities and ship within European Union, The European Commission has established the following regulation.

3.1.1. EU REGULATION 725/2004

In order to come into force the ISPS code, the Commission passes the Regulation 725/2004 on enhancing ship and port facility security. Consequently, this regulation only applies to the direct ship/port interface.

The International Ship and Port facility Security Code (ISPS code) established by IMO has as objectives:

- To establish an international framework involving co-operation between Contracting Governments, Governments agencies, local administrations and the shipping and port industries to detect/assess security threats and take preventive measures against.
- To establish the role and responsibilities of all parties concerned, for ensuring maritime security at international and national level.
- To ensure interchange of security-information efficiently.
- To provide a methodology for security assessment which allows to change security levels.

Designation of appropriate personnel on each ship, port facility and shipping company is necessary for putting into effect the security plans established.

ISPS code has two main parts: Part A, where the mandatory requirements regarding the provisions of chapter XI-2 of SOLAS as amended; and Part B, a guidance regarding the provisions of chapter XI-2 of SOLAS as amended and Part A of the Code.

In the Part A the next items are established:

a) types of ships and port facilities to which ISPS Code applies,

b) what the responsibilities of Contracting Government are,

c) different security levels for ships and port facilities. There are three identified:

- Security Level 1, Normal: the level at which ships and port facilities normally operate.
- Security Level 2, Heightened: the level applying for as long as there is a heightened risk of security incident.
- Security Level 3, Exceptional: the level applying for the period of time when there is a probable or imminent risk of a security incident.

d) ship security, security assessments and security plans, where is detailed

- The responsibility of the ship in relation to the security levels placed upon it by the Contracting Government.
- Information regarding the security assessment required to be undertaken
- The information required to be present in the approved Ship Security Plan

e) Port facilities, security assessments and security plans, where is detailed just the same that d. item

f) Identification of the figures:

- from the ship side: Company Security Officer who, among others responsibilities, ensures that ships security assessment and security plan implementation are carried out. Other figure is the Ship Security Officer who, among others responsibilities, maintains and supervises the implementation of the ship security plan, proposes modifications to the security plan and reports all security incidents.
- from port facility side: Port Facility Security Officer who has similar responsibilities that Company Security Officer but from port facility side

On the other hand, Part B outlines guidance on the processes envisaged in establishing and implementing measures and arrangements needed to achieve and maintain compliance with the provisions of chapter XI-2 and or Part A of the ISPS Code. Measures for different security levels are describe as well as some aspects that should be identified in the ship and port facility plans.

For instance and from the point of view of port access control, Part B points that an identification document entitled to board ships or enter port facilities is advisable; and also establishes procedures whereby the authenticity of such documents might be verified. In addition, from security level 1, Normal, the Code arranges different measures to control accesses to ships and to port facilities.

In accordance with Article 3.5 of Regulation 725/2004, Part A and some paragraphs of Part B of the ISPS Code are made mandatory for the Member States. Domestic shipping within the Community is included.

A periodic review of the port facility security assessment, at least once every five years, will be carried out in order to monitor the application of the Regulation.

Member states may determine alternative security agreements or equivalent security arrangements in order to promote intra-Community short sea shipping.

3.1.2. EU DIRECTIVE 2005/65

In this directive, the EC introduces measures to enhance port security in the face of threats of security incidents in every port located in the territory of a Member State.

It is the responsibility of the Member States to ensure that port security measures introduced by this Directive are in line with those from Regulation 725/2004, shown above.

The Directive identifies three figures:

1. Port Security Authority which will be responsible for security matters in a given port. This security port authority will carry out the minimum detail requirements laid down in the first annex.

2. Port Security Officer which will be the point of contact for port security related issues.

3. Focal Point for port security, which is designated by the Member States and will communicate to the EC the list of ports concerned by this Directive and inform it of any changes, if any.

A port security plan is required and should take into account the minimal specifications given in the second annex and must include security measures to be applied to passengers and vehicles on vessels. It will be reviewed, at least, once every five years. In addition, it will apply according to the established security level. Member States may determine the different measures to take into account in each security level.

Three security levels have been defined:

Security level 1, in which minimum security measures must be maintained at all times.

Security level 2, as consequence of an increase of the risk of a security incident, further security measures will be maintained for a period of time.

Security level 3, when a security incident is probably or imminent, further specific protective security measures will be maintained for a period of time.

The Commission, in cooperation with the focal points, will monitor the implementation of this Directive by the Member States.

Member States are in charge of ensuring that effective, proportionate and dissuasive penalties for infringements of the national provisions are adopted following this Directive.

Three annexes are included in the Directive

a) Annex1: Port Security Assessment, where the requirements for the port security plan and its implementation have been identified.

   From the point of view of port access, to highlight that the port security plan will attribute tasks and specify work plans in the following fields:

   - access requirements. In some areas requirements will only enter into force when security levels exceed minimal thresholds. All requirements and thresholds will be comprehensively included in the port security plan;

   - ID, luggage and cargo control requirements. Requirements may or may not apply to sub-areas. Persons entering or within a sub-area may be liable to control. The port security plan will appropriately respond to the findings of the port security assessment, which is the tool by which the security requirements of each sub-area and at each security level will be identified.

b) Annex2: The Port Security Plan, based on the port security assessment, sets out the port's security arrangements. An important point about identification cards in the annex2 establishes that when dedicated identification cards are developed for port security purposes, clear procedures will be established, including the use-control and the return of such documents. Such procedures will take into account the specificities of certain groups of port users allowing for dedicated measures in order to limit the negative impact of access control requirements.

It also mentions different categories that could be considered as stakeholders for EPAIC II, in particular when mentioning that the categories will at least include seafarers, authority officials, people regularly working in or visiting the port, residents living in the port and people occasionally working in or visiting the port.

c) Annex3: Basic Security Training Exercise Requirements, where various types of training exercises will be carried out at least once each calendar year with no more 18 months between the training exercises.

3.2. DATA PROTECTION

The EC, in regards of the personal data protection, established the Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

The Directive provides a set of legal requirements for personal data to be processed wholly or partly by automatic means in Europe; and how all the Members States have to adopt this Directive in order to be transposed into national regulation, according to the article 4, national law applicable.

The concept of personal data is broad and applies to an extensive range of information (text, sound, images) that relate to an identified or identifiable person. In this sense, the Directive mentions that an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number.

The Directive states principles relating to data quality which make data processing lawful. These principles are gathered in article 6 and include:

a) Personal data needs to be processed fairly and lawfully.

b) Data must be gathered for specified and explicit purpose in a legitimate process. The legitimacy of data collection is governed by article 7 of the Directive where legitimacy can be derived from a) unambiguous consent, b) the necessity of processing for the performance of a contract, c) a legal obligation of the controller, d) protection of the vital interests of the data subject, e) performance of a task carried out in the public interest or in the exercise of official authority, or f) necessity of processing for the purposes of the legitimate interests pursued by the controller.

c) Data collection must be adequate, relevant and not excessive in relation to its purpose.

d) Data should be accurate and up to date.

e) Not to be kept longer than necessary.

f) Personal data processing needs to be protected against data loss, destruction and alteration pursuant to article 17.

g) It is not permitted the processing of sensible information such racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life.

In the article 12, it mentions the right of access of the data in which is possible a rectification of data processing. In this scope, the Directive also includes the possibility to object in accordance with the data subject's right.

The Directive incorporates the possibility to transfer personal data to a third country only if it ensures the adequate level of protection.

The figure of Working party is defined in order to protect individuals with regard to the processing of personal data. Among its obligations, the working party will:

a) Exanimate any questions adopted under this Directive and the application of the national measures.

b) Give the Commission an opinion of the level of protection in the Community and in third countries.

c) Advise the Commission on any propose amendment of the present Directive.

d) Give an opinion on codes of conduct drawn up at Community level.

e) Provide an annual report on the situation regarding processing of data in the Community and in third countries.

3.3. Legal Issues On The Board

One of the most pressing issues is that of privacy protection. Several agreements, such as Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, establish the need to respect private and family life.

The right to privacy can only be disturbed, as stated in Article 8 of the ECHR, in cases dealing with national security, public health, the economic well – being of the country, the prevention of disorder or crime, for the protection of health and morals or for the protection of rights or freedom of others.

The Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) needs also to be taken into account. It prohibits the processing of data about a person's race, politics, health, religion, sexual life, criminal record and other in the potential absence of proper legal national safeguards. It also ensures the individual's right to know what information is stored about him and to have if corrected if necessary.

The information stored in the EPAIC system must respect these principles. That is to say, it has to:

- Obtain and processes personal data in a fairly and lawfully fashion. Personal information can only be used for a specific propose.
- No data recorded on the card may be used without the knowledge of the cardholder.
- The cardholder should clearly understand the card's applications.
- If the cardholder's wishes, he should have access to the data recorded on the card and they should be made accessible to him in a legible and understandable fashion. He holds the right to correct the data. The method of access will respect confidentiality and the cardholder's right to a protection of privacy.
- If there are legitimate reasons for disclosure, the cardholder must be made aware of that disclosure as soon as possible.
- Each application shall make use only of the personal data pertinent to the given application and to the extent essential for fulfil ing the purpose of the application; this means that any multiple applications

on a single card require that any personal data must be compartmentalised for the individual applications.

- ID cards are not designed to be instruments for monitoring persons or curtailing their rights in any way.
- Any discrimination must be excluded.
- If the card is "transaction – enabled" then the processor does not always need to know exactly who the cardholder is. In such cases it is sufficient for the cardholder to provide authorisation only for the given transaction.
- Personal data shall be accurate and, when necessary, kept up to date. Erroneous or inaccurate data, as well as those that no longer serve their original purpose, must be erased or rectified.
- Personal data shall be preserved in a form which permits identification of data subjects for no longer than is required for the purpose for which those data are stored.
- The card issuer and the administrator of every application shall ensure personal data protection in the event of a loss, theft, destruction or other abuse of the card, as well as protection against copying of the card.
- For a specific application, security systems shall be used that will ensure protection against copying of the card.

The Schengen Agreement is another item to be account for. The abolition of border checks within most countries in the EU, Norway, Iceland and Switzerland regulates in part the authorisation for incoming citizens in ports.

The Schengen Convention establishes common rules for visas, the right of asylum, checks at the external borders and cooperation between police forces and customs authorities. A reporting system exists for the exchange of data about the identity of individuals. The Member States that are signatories to the Schengen Agreements also now conduct closer cooperation on the abolition of internal frontiers in the European Union. The signatories to the Schengen Agreements are 22 Member States of the European Union plus Norway, Iceland, Liechenstein and Switzerland. The Member States which are not fully signataries of the Schengen Agreement are the United Kingdom, Ireland (these two countries are partial signatories), Bulgaria, Cyprus and Romania (which are expected to join in the future).

This Schengen Information System is composed of a database housed in Strasbourg, comprising records put in by its EU Member States which is then accessed by other state agencies. This database, which contains basic information, is backed up by a SIRENE bureau in each state, which can provide on request more detailed information. The sytem is able to interrogate records to identify persons which are:

- Wanted for arrest on the basis of a European arrest warrant.
- Under provisional arrest subject to possible extradition.
- Vulnerable and in need of temporary police protection.
- Wanted for judicial procedure.
- Under discrete surveillance or specific checking procedures.

However the Schengen Agreements may vary in the future. This situation, along with the fact that not all the Member States of the European Union are fully signatories to them and that some non – EU countries have however ratified them, presents a complex picture that affect the working of a system such as the one shown in this study.

One of the main questions for the EPAIC II is what kind of information may be stored in the card. Since not every country in the EU or in the Schengen area may admit the same data to be used, a common set must be chosen.

EPAIC I project failed to mention the concrete items that can appear in the cards or that can be allowed by different Member States, and the situation is a bit complex. With that information absent in the first EPAIC project, the present one can only propose solutions that may not fit completely into the real picture. However, we will seek the information that can clarify what type of data may appear in the access cards.

Nevertheless there are some items of information that seem adequate to be included in the card, such as: name, signature, photograph, personal code, etc. The EPAIC II project will propose a larger list.

4. STAKEHOLDERS

4.1. EPAIC I CONSULTATION ANALYSIS AND STAKEHOLDERS

The EPAIC I project selected several stakeholders in order to seek their views and opinions. Those stakeholders were intended to be the most relevant and, in many cases, the objective was achieved. The procedure was composed of a questionnaire, which was sent to the selected actors, interviews and visits to the ports. However we believe that the identification of the stakeholders and the questioning could be improved. The following is a brief review on the matter:

- National and port authorities were chosen. The questionnaire was sent to 35 ports from several countries, which seems to represent an appropriate action.

- Port facilities were also visited, covering a representative sample composed of several kinds.

- Hauliers were also consulted. But instead of selecting a sample – which indeed may be a too heavy task – they approached the European Haulers Association. However they do not give any other reference and the only organisation with that name that we have managed to find is also called Organisation des Transporteurs Routiers Européens (http://www.otre.org/) and all of its members seem to be French. We believe that a more ambitious approach should have been taken, trying to contact road hauliers from other areas. The study, as it is, may be biased. And what is more, the EPAIC I final report does not explicitly state whether the questionnaire was sent to this organisation or the just contacted and interviewed them, the latter being an action that has some value of its own but perhaps not as much as sending the questionnaire.

- Traders: in a similar fashion, the European Traders Organisation was contacted. However, we could not even find more details about this association.

- Law enforcement and emergency services personnel, port workers, sub-contractors personnel and regular visitors were also said to be taken into account. However, it is not stated whether some of them were sent the questionnaire or interviewed.

As we can see, some of the main stakeholders were properly questioned, as in the case of port, but some other seem to be quite absent. This situation, along with the fact that we do not know exactly what was asked in the questionnaire nor the answers received, represents a drawback for the EPAIC II project.

The questionnaires sent by the EPAIC I sent to ports were divided into the following sections:

- Details of policy(s) regarding access control procedures. In detail:
  - Is there a policy in effect?
  - Which security requirements this policy includes?
  - How this security policy is implemented?

- The policy on the security regulations for ID card use:
  - What responsibilities the policy introduces?
  - Which is the authority of the issuing body?
  - Which are the appointments of the issuing body?
  - Is there a policy on Inspections/Audits of ID card systems?
  - Is there a policy on the design of the ID cards?
  - Is there a policy on the ID card expiry?
  - What level of access is permitted for each type of ID card? Are there more than one type?
  - Is the wearing of ID cards mandatory?

- Is there any standard/best practice adopted for implementation of ID cards? Which?
- Is the security clearance of staff controlling the ID card system sought?
- Which is the application procedure for an ID card?
  - Is there a validation procedure for establishing identity?
  - Which documents are used for validation?
  - Is the use of references necessary?
  - What kind of information is held on the records of issued ID cards?
- What controls exist for the registration system (manual or/and computer based)?
- What controls exist for personal information (security controls, controls of personal information on networked systems, controls of backups containing personal information)?
- Are there any restrictions on pass production and control? Is the ID cards production outsourced? Are the black cards protected? Are the production stuff security cleared?
- Is there a procedure (reporting obligations or/and disciplinary issues) for lost ID cards?
- Are there any procedures for the destruction of ID cards?
- Are there any procedures for the revocation of ID cards?
- Are there any procedures for the audit of ID card accounting systems?
  - What is the frequency (if any) of the audits?
  - Are there any responsibilities defined?
  - What actions are taken to rectify faults?

The results from the questionnaire were processes and shown in the available documents. Several conclusions were reached, among them:

- All of the 35 interviewed had access control systems. Out of them, 26 operated those systems while 9 let third parties do that task. However, from the results it is not clear whether all those ports had card – based or other type of access control system. Therefore, more research is needed.
- Almost had of the interviewed authorities could not say if the access system was port – wide or more restricted in application (that is, used only in terminals or areas)
- 23 ports reported having audit policies. There was one which could not reveal that kind of information, so in 12 cases –that is, more than one third – there was not such a policy. Those data show that a high percentage does not possess enough control capabilities.
- Several ports have different cards in use, depending on the functions of the holder. However, it is not stated if port – wide and terminal – area cards are managed by the same authority.
- The matter around personal references is somewhat obscure. Although 26 ports required them, their exact nature is not reported. That is to say, we do not know if background checks are carried out, a necessary piece of information which will be sought in EPAIC II.
- In most cases there were procedures for the reporting of lost or revoked cards.
- Ports did not give enough economic data, which represents a lack in the study. EPACI II will request the necessary information.

The EPAIC I questionnaire represents a good source of information, although there is some information missing (a situation which will be improved by EPAIC II) and the questions were aimed at ports. Therefore the study shows the data gathered from port authorities but not from other stakeholders, such as workers, seafarers or transport companies. That constitutes a negative issue that EPAIC II will have to fix.

4.2. Stakeholder Advanced Consultation

The EPAIC II project will prepare its own questionnaires in order to retrieve information from the stakeholders. The present section is devoted to the preparation of the questions and the identification of the actors to be contacted.

As for the stakeholders, the EPAIC II has already identified several of them – although the number may be increased during the project's lifetime. Some of these stakeholders are:

- Ports. A number of ports, including those from EPAIC I but also some others, will be contacted.
- Transport companies,
- Workers associations,
- Maritime international organisations,
- Terminal owners,
- And ship-suppliers

The following sub – sections cover some of these stakeholders:

4.2.1. Ports' Consultation

The aim of the study is to cover as many ports as possible in Europe, and to accomplish this objective many questionnaires were sent, including among their recipients some sector organisations. And since maritime transport in Europe is somewhat organised along corridors, the selected sample covers the main ones. The response that were receive range from openly against EPAIC to anthusiastic about it, but some ports – not many of them, but a certain number - did not send any answer at all. The ports that were contacted and their corridors are:

- The Baltic sea, located in the North East, is surrounded by many European Member States, including Sweden and Finland and some other non – member States, such as Russia and Norway that are also in this area. It shares, along with the Nort sea corridor, the northernmost part of the European axis that goes from Milan to Stockholm.

BALTIC CORRIDOR
Port of Turku (Finland)
Port of Göteborg (Sweden)
Port of Stockholm (Sweden)
Port of Helsinki (Finland)
Port of Fredericia (Denmark)
Port of Mälmo (Sweden)
Port of Riga (Latvia)

BALTIC CORRIDOR
Port or Rauma (Finland)
Port of Århus (Denmark)
Port of Ystad (Sweden)
Port of Szczezin (Poland)
Port of Swinoujscie (Poland)

Table 1 Baltic corridor ports consultation

- The North sea area is located between the main European economical centres, including partially the end of the axis that runs from Milan to Stockholm and the Paris and London zones. Therefore, its ports are located in very populous and economically thriving areas.

NORTH SEA CORRIDOR
Port Autonomme Du Havre (France)
Port of Hamburg (Germany)
Port of Bremen (Germany)
Port of Rotterdam (The Netherlands)
Port of Antwerp (Belgium)
Port of Liege (Belgium)
Port of Felixtowe (United Kingdom)
Port of Dover (United Kingdom)

Table 2 North Sea corridor ports consultation

- The West of Europe borders the Atlantic Ocean, and therefore finds in it a natural way of communication. Several European States have been historically influenced by this ocean. However, this area, as geography shows, located in the periphery of Europe, have also tended to be somewhat less economically developed, at least compared with more "central" areas. In the past year, two "motorways of the sea" have been implemented in this area, as a bilateral agreement between the governments of Spain and France. These two motorways connect the ports of Gijón and Nantes St-Nazaire and the ports of Vigo, Algeciras, Le Havre and Nantes, respectively.

ATLANTIC CORRIDOR
Port of Gijon (Spain)
Port of Vigo (Spain)
Port of Dublin (Ireland)
Port of Bristol (UK)
Port of Nantes – Saint Nazaire (France)

Table 3 Atlantic corridor ports consultation

- The Mediterranean sea has has served as a connection area for peoples long before the dawn of written history. Nowadays it serves Southern Europe as an excellent transport corridor and the best solution to reach some of its islands. Thanks to that the West part is very well connected through cargo and passenger ships.

MEDITERRANEAN SEA CORRIDOR
Port of Algeciras Bay (Spain)
Port of Barcelona (Spain)
Port of Valencia (Spain)
Port of Alicante (Spain)
Port of Tarragona (Spain)
Port Autonome de Marseille (France)
Capitaneria di Porto di Genova (Italy)
Port of Livorno (Italy)
Port of Bari (Italy)
Port of Patras (Greece)
Port of Thesaloniki (Greece)

Table 4 Mediterranean Sea corridor ports consultation

- Some ports fall outside the main transport corridors, such as Seville, between the Atlantic and the South – West and sharing characteristics of both, but still deserve attention. In the same way, many organisations have been contacted in order to request their point of view and their needs.

OTHER PORTS AND ORGANISATIONS
Port of Seville (Spain)
Puertos del Estado (Spain)
ESPO – European Sea Ports Organisation
Ocean – European Ship Suppliers Organisation
SAGMaS – Stakeholder Advisory Group on Maritime Security

Table 5 Other ports and organisations consultations

- It should be noted that some of the ports are inland facilities, that is, are not in the sea but in rivers or artificial waterways. These deserve special attention since their needs and their conditions are not exactly the same. For example, they may have larger terminal areas although these are under pressure from cities, which seek to expand themselves. Inland ports allow sending goods to many interior cities in spite of the fact that their catchment areas tend to be smaller than those of sea ports. The interior ports that have been contacted in EPAIC II have been listed before but are worth summing them up in a separate table:

INTERIOR PORTS
Hamburg Port Authority (Germany)
Port of Rotterdam (The Netherlands)
Port of Antwerp (Belgium)
Port of Seville (Spain)
Port of Swinoujscie (Poland)

Table 6 Interior ports consultation

4.2.2. ROAD HAULIERS ASSOCIATIONS

These are some Road Hauliers Associations we consider to approach in order to get their views and opinions into EPAIC II:

ORGANISATION	TYPE	GEOGRAPHICAL COVERAGE	NUMBER	TRANSPORT TYPE	COMMENTS
IRU (INTERNATIONAL ROAD TRANSPORT UNION)	International Association of associations	International (72 countries)	600 associates	Road	_
BGL (BUNDESVERBAND GÜTERKRAFTVERKEHR LOGISTIK UND ENTSORGUNG E.V.)	Association of regional associations	Germany	12000 companies	Road and Rail	German Member of IRU
FEBETRA (FEDERATION ROYALE BELGE DES TRANSPORTEURS ET DES PRESTATAIRES DE SERVICES LOGISTIQUES)	National Association	Belgium	2050 road operators and logistic companies	Road and Rail	Member of IRU
RHA (ROAD HAULAGE ASSOCIATION)	National Association	United Kingdom	9500 members	Road	Member of IRU
VVWL (VERBAND VERKREHRSWIRTSCHAFT UND LOGISTIK NORDRHEIN-WESTFALEN E.V.)	Regional association	Germany (Nordrhein-Westfalen)	3000 companies	Road, rail, inland waterway, air	Member of BGL

Table 7 Road Hauliers Associations

The International Road Transport Union (IRU) is an association of associations representing the interest of buses, coaches, taxis and trucks, from large fleet to individual owner-operators worldwide.

Most IRU members are national federations such as Febetra in Belgium, BGL in Germany and RHA in United Kingdom.

Due to the size of the country, the German member BGL is a federation of regional associations on the level of the *Bundesländer*. In this case, it was thus also possible to contact an organisation acting on a regional level, hence a 3-layer analysis (VVWL)

BGL regroups 19 German regional associations and represents approximately 11.000 mainly medium-sized companies of the road haulage, logistics and disposal sector. VVWL represents the interests of roughly 3000 companies involved in the logistics and/or transport (only Nordrhein-Westfalen area)

Febetra is the industry association representing and defending the interests of freight transport by road in Belgium.

RHA is the main representative body for UK companies whose main business is providing road haulage and related services. Its 9,500 members run 100,000 Lorries and include owner-drivers, small and medium-sized fleets and large multi-depot operators.

4.2.3. INTERNATIONAL ASSOCIATIONS

All European and International Associations included in the SAGMaS (Stakeholder Advisory Group on Maritime Security) meetings with a special emphasis on:

ORGANISATION
European Sea Ports Organisation (ESPO)
Baltic Ports Organisation (BPO)
Federation of European private Port operators (FEPORT)
European Association of Airport and Seaport Police (EAASP)
European Tugowners Association (ETA)
Confederation of European Security Services (CoESS)
Eurochambers
European organisation for Security (EOS)
European harbour Masters Committee (EHMS)
European Confederation of Shipowners Associations (ECSA)
Organisation de la Communauté Européenne des Avitailleurs de Navires (OCEAN – ship suppliers organisation)
European Dredging Asssociation (EuDA)
European shippers Council (ESC)
European Transport Workers' Federation (ETF)
Confederation of European Shipmasters' Associations (CESMA)
European Maritime Pilots Association (EMPA)
European Federation of Inland Ports (EFIP)
European Boating Association (EBA)

Table 8 International associations

4.2.4. WORKERS

Another group of stakeholders to take account of is that formed by port workers and the people actually accessing the facilities, whether truck drivers, sub – contractors or others. Two main associations have been identified:

ORGANISATION	TYPE	GEOGRAPHICAL COVERAGE	NUMBER	TRANSPORT TYPE	COMMENTS
ITF (INTERNATIONAL TRANSPORT WORKERS' FEDERATION)	International Association of associations	International (148 countries)	700 transport unions	All modes	Representing around five million workers.

ORGANISATION	TYPE	GEOGRAPHICAL COVERAGE	NUMBER	TRANSPORT TYPE	COMMENTS
ETF - EUROPEAN TRANSPORT WORKERS' FEDERATION	International Association of Associations	Europe (40 countries)	223 transport unions	All modes	ETF represents more than 2.5 million transport workers.

Table 9 Port workers

The ETF has affiliated unions which organise workers in railways, road transport, maritime transport, ports and docks, inland navigation, civil aviation, fisheries and tourism services.

These two federations had relation with the SID (Seafarers' Identity Document), explained in Section 5.4. Lessons learnt from the SID might be taken into account into the process of creating a Euopean Port Access Identification Card.

4.2.5. SHIP-SUPPLIERS

Ship suppliers compose a large group of companies that deliver goods intended to be used on board: food, clothes, ropes and cables, paint, cleaning items… During this project, the European Ship Suppliers Organisation (OCEAN), which comprises over 750 companies with a total of more than 250,000 employees, was contacted and its point of view was added to the study.

5. PORT ACCESS CONTROL SYSTEMS STATE-OF-THE-ART

After the facts that have striken at the heart of key national bodies and infrastructures, both governments and public opinion all over the world have developed a growing concern on the impact of such incidents and the likelihood of new ones to come. Protection of welfare state against these arising threats requires among others, security measures covering a wide extent of domains such as transportation, goods supply and trading.

At this stage, ports have become considered a critical infrastructure due to the social and economical weight on society nowadays. Authorities and main port agents are thus involved on applying security principles that allow to enhance trust and ensure activities are performed on a safely and timely manner. So far there have emerged several initiatives at local, national or even broader levels to set some of these measures up.

One of the main issues to take care about is access control to port facilities and ships. Beyond the evident, this need is reflected through multiple regulation requirements that lead great stress on this point. Efforts in this field have been hence studied to understand the current state-of-the-art. The aim of this analysis was to reach a proficent knowledge about strengths and weak points related to port access systems currently in exploitation or with a matured enough projection. The chosen systems were also selected because of their similar scope and port-oriented conception. Some of these systems were already exposed on the first EPAIC study, nevertheless, it has been found that there were factors and critical issues that needed to be considered and analysed in-depth.

Following EPAIC methodology, every system is briefly introduced and its information specifications presented along with the design of the credential. Parties involved on the issuance and maintenance process as well as stakeholders on scope, are followed by the enrolment course of action. Finally, conclusions are explained on those aspects that have to do with this project's aim.

5.1. TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

5.1.1. OVERVIEW

Transportation Worker Identification Credential (TWIC) is an identification system used in USA maritime facilities. It's based on an identification credential for all personnel in ports requiring unescorted access to specific areas, facilities and vessels.

TWIC system has been already analysed in the first EPAIC study, and further details and results can be obtained from that source. However, this study of TWIC performed in EPAIC I is mainly focused on the card life cycle, and a deeper analysis should be done about the technological aspects and operation modes of TWIC system. Next, the present study will expose the main features and more interesting points regarding these technical areas of TWIC, which shall be useful in the present EPAIC II study.

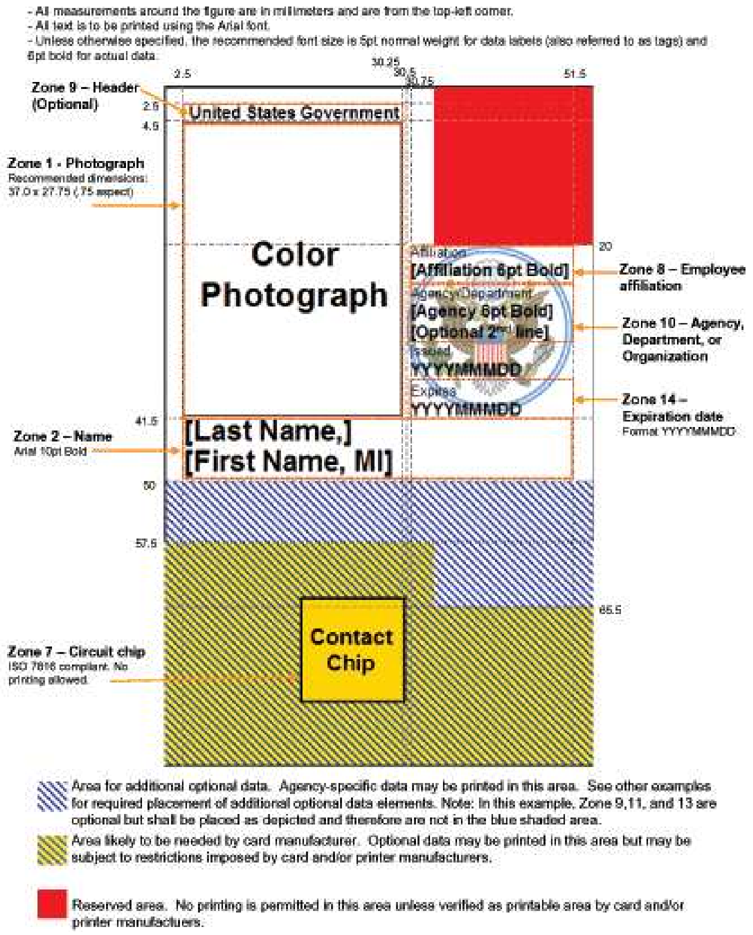
5.1.2. SYSTEM DESCRIPTION

TWIC identification system has been designed to fulfil the security plans defined in the MARSEC system. MARSEC represents the three-tiered United States Coast Guard Maritime Security system created to be compatible with the Homeland Security Advisory System (HSAS) of the Department of Homeland Security. Thus, TWIC is structured to be compatible with several security layers.

Although the system was designed to fulfil the layered security architecture of the MARSEC approach, TWIC neither establishes any security policy, nor defines control access policies of any kind for the authentication and identification processes. However, TWIC readers shall be compatible with the operation modes defined in every MARSEC security level specification.

TWIC is part of a greater control access system, the PIV (Personal Identity Verification) program. The objective of PIV is to represent an implementation of the policy for a common identification standard for Federal Employees and Contractors (HSPD-12, August 2004), and it's fully standardised in the Federal Information Processing Standard 201 (FIPS-201, February 2005). Any activity involving federal personnel or contractors may be subject to the implantation of the PIV system. Thus, different applications, departments and collectives can be found as former subsystems of the PIV program, from the Common Access Card for federal employees, to the TWIC system for transportation workers, or the PIV-pilot-testing Department of Veteran Affairs (VA).

Any card implementing the PIV program contains a computer chip, which allows receiving, storing and saving information in a secure method. The main function of the card is to encrypt or code data to strengthen the security of information and physical access to secured areas, while using a common technical and administrative process. PIV uses Public Key Infrastructure (PKI) technology which complies with all Federal security policies, and is the accepted Global Business Standard for Internet Security, providing the functionality for digital signatures as well.



- All measurements around the figure are in millimeters and are from the top-left corner.
- All text is to be printed using the Arial font.
- Unless otherwise specified, the recommended font size is 5pt normal weight for data labels (also referred to as tags) and 6pt bold for actual data.

▨ Area for additional optional data. Agency-specific data may be printed in this area. See other examples for required placement of additional optional data elements. Note: In this example, Zone 9,11, and 13 are optional but shall be placed as depicted and therefore are not in the blue shaded area.

▨ Area likely to be needed by card manufacturer. Optional data may be printed in this area but may be subject to restrictions imposed by card and/or printer manufacturers.

🟥 Reserved area. No printing is permitted in this area unless verified as printable area by card and/or printer manufactuers.

Figure 1 PIV Card Layout

As part of the PIV (Personal Identity Verification) system, TWIC card and reader are PIV cards and readers as well, and can be used as part of this identification system through a multiple application scheme that improves interoperability and compatibility between various identification systems. This factor could be a key aspect in the future EPAIC design, and will be considered as an interesting feature further on this document.

The TWIC system authentication and identification process involves a credential card and a RFID-contactless and magnetic stripe reader, which requires biometric data reading capabilities as well.

5.1.3. DATA STORED INSIDE THE CARD

The card contains the following data:

- Visual identification data printed in the front side of the card: name and a photograph of the applicant, a unique identifier for the credential, and the expiration date of the card.
- Data stored inside a MIFARE chipset (a Dual Interface Integrated Circuit Card, ICC), which contains the following information:
  - Biometric templates (minutiae) of the fingerprints of two fingers of the cardholder.
  - Personal Identification Number (PIN), which is chosen by the applicant in the final step in activation process.
  - U.S. Federal Agency Smart Credential Number (FASCN), which will act as a unique identification number for the credential (for card authentication purposes).
  - TWIC Private Key (TPK) is a 16 byte encryption key using AES algorithm to encipher or decipher the reference biometric template stored in the card (in its TWIC card application). It is encoded on the magnetic stripe in the card. It is never used by the TWIC application in the card, but the TWIC application in the readers, to decipher the biometric templates during the identification process or to encipher the, (for storage in the card).
  - A security object, consisting in the hashes of the rest of data elements stored in the card, for integrity check purposes.

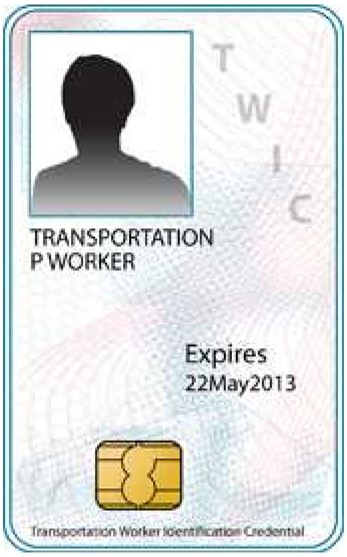


Figure 2 TWIC Card Sample

5.1.4. CARD APPLICATIONS

As it has been said, TWIC system is designed to be compatible by default with PIV system, and this compatibility could be extended with other control access card systems. This feature is achieved by defining and distinguishing different applications, to be used by each system supported. TWIC system supports at least two different types of applications to be executed in the TWIC cards and readers: PIV applications and TWIC applications. But more applications for an additional control access system could be added.

Every application is uniquely identified by an Application Identifier and the reader is able to search and launch a concrete application type inside the card. The reader can be configured to search for certain applications by default, or to iterate the available applications in the card in a predefined preference order.

TWIC system is compatible with the TWIC card, the PIV card, and the Department of Defence Common Access Card (CAC), with that priority order configured in the readers by default.

As it will be exposed, depending on the application to be used (TWIC or PIV), the operation processes and data in the card used will vary.

5.1.5. CARD DATA OBJECT MODEL WITH ISSUER SIGNATURE

The previous data elements are organised in identified data objects inside the card. For card authentication purposes, some of these objects are signed by the issuer during the issuance process. This way, the TWIC readers can check the expiry and authenticity of the card just by having the signing certificate (i.e., the public key) of the card issuer. These signatures are of type RSA 2048 SHA1. The data objects inside the card are the following:

- CHUID (Card Holder Unique Identifier): contains the FASCN and the card expiration date. It can be signed by the issuer or unsigned. In case of being signed, it also contains the issuer asymmetric signature.
- PIV Biometric object: for use in the PIV application, this object is unsigned, and contains the biometric templates not ciphered. Because of this fact, this object can not be transmitted through the contactless interface, but a magnetic stripe or contact slot card interfaces, and the PIN number will be required for input to authorise the access to this object.
- TWIC Biometric object: for use in the TWIC application, this object is TPK-enciphered, and inside it contains the fingerprint templates and FASCN number, and a digital signature of both elements signed by the issuer during the card registration.
- Security object.

5.1.6. INTERFACES

The card and card reader are compatible with the following interfaces:

- RFID contactless interface, as part of the Dual Interface ICC. The TPK and the PIV biometric object shall never be transmitted through this interface.
- Contact slot card reader interface, as part of the Dual Interface ICC.

- A magnetic strip interface, to store the TPK key.
- Bar code encoding the card identifier.

5.1.7. *Authentication Factors Available for Use in TWIC System*

- Something you have: by authenticating the card, checking its authenticity and expiry.
- Something you are: via biometric authentication of fingerprints.
- Something you know: via the PIN which shall be required in some particular processes and operations, like the biometric template retrieving in PIV application.

5.1.8. *Operation Modes*

TWIC system defines four operation modes in the authentication processes:

- CHUID verification: this data object contains the card identifier (FASCN) and the card expiration date. Because every card is uniquely assigned with its cardholder, this FASCN can be considered as a user identifier as well. However, the CHUID is freely readable and it could be easily cloned and manipulated, unless it is signed by the issuer. Thus, unsigned CHUID verification by itself can not be considered as a strong authentication factor, and shall not be used alone.

  Signed CHUID verification assures that the data contained in the retrieved CHUID is legitimate and has not been manipulated. In order to prove this, the TWIC reader must have access to the updated list of the authorised TWIC issuers signing certificates, which will be used to verify the signed CHUID, and its actual validity in terms of revocation or expiration. The signed CHUID verification consists of the following steps:

  - The reader selects the card TWIC application.
  - The reader retrieves the signed CHUID data object from the card.
  - The reader obtains the issuer signing certificate from the CHUID object and verifies it, checking the expiration, revocation and validity against its authorised issuer certificates updated list.
  - Once the CHUID objet is verified, its contents (FASCN and expiry date) are reliable and can be used.

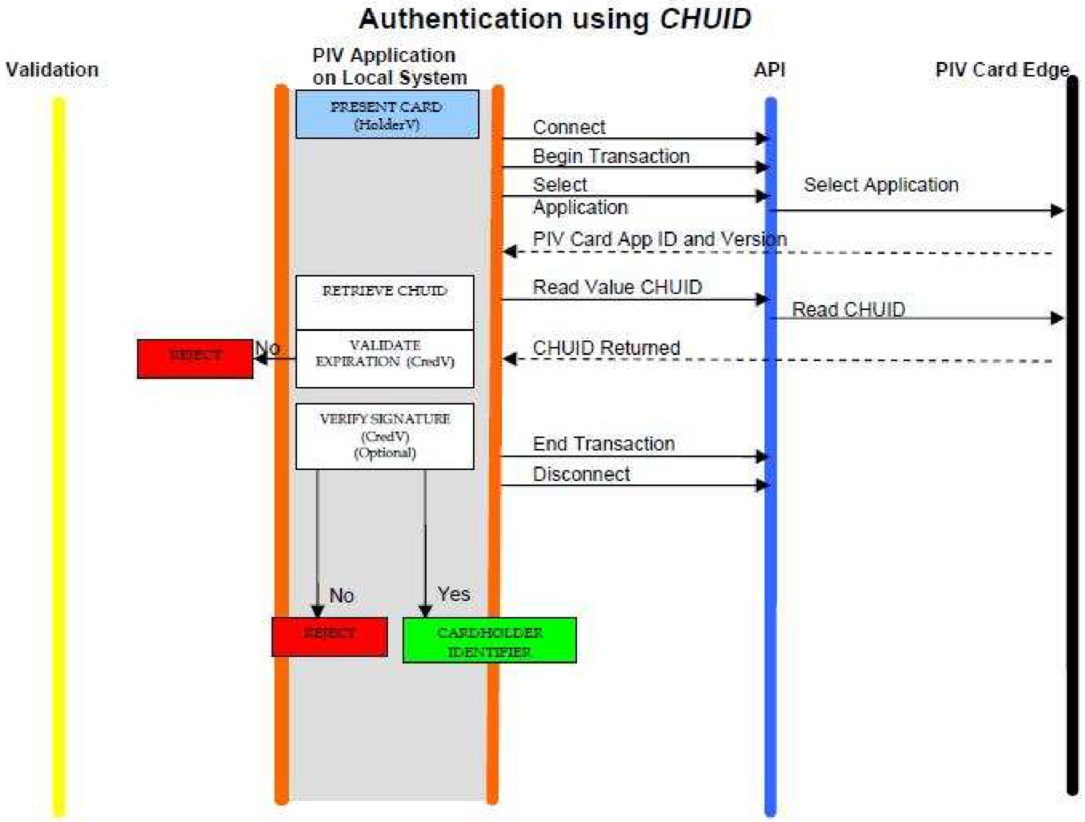


Figure 3 CHUID Verification Flowgraph

- Active Card Authentication: this is a "what you have" authentication factor defined for the PIV system, thus it is a possible authentication method in the TWIC system, but only by selecting the PIV application inside the card. The asymmetric Card Authentication Key (CAK) option has been used in TWIC, consisting in:
  - An asymmetric private key (the CAK key) unique for the card and not readable, used by the card ICC to sign data.
  - A Card Authentication Certificate (which is recommended to be signed by the same issuing authority that signed the certificate of the CHUID object), containing:
    - The asymmetric CAK public key.
    - A unique identifier for an algorithm used to create nonces to be used in an asymmetric challenge-response protocol.
    - The card FASCN identifier.
    - The expiry date.

The reader will retrieve the Card Authentication Certificate, and verify the expiration, revocation and validity against its authorised issuer updated list. Next, the reader will obtain the public CAK and the algorithm ID, and use the required algorithm to generate a nonce and send it back to the card. Then, the card will sign the nonce with its private CAK and return the signed nonce to the reader, which will decipher the nonce with the public key and check it against the original nonce sent.

Active Card Authentication is not accessible by any card application other than PIV application, but the CHUID verification TWIC process is not necessary if the PIV Card Authentication Certificate was signed by the same CA than the signed CHUID (both contains the FASCN identifier and the card expiry date).

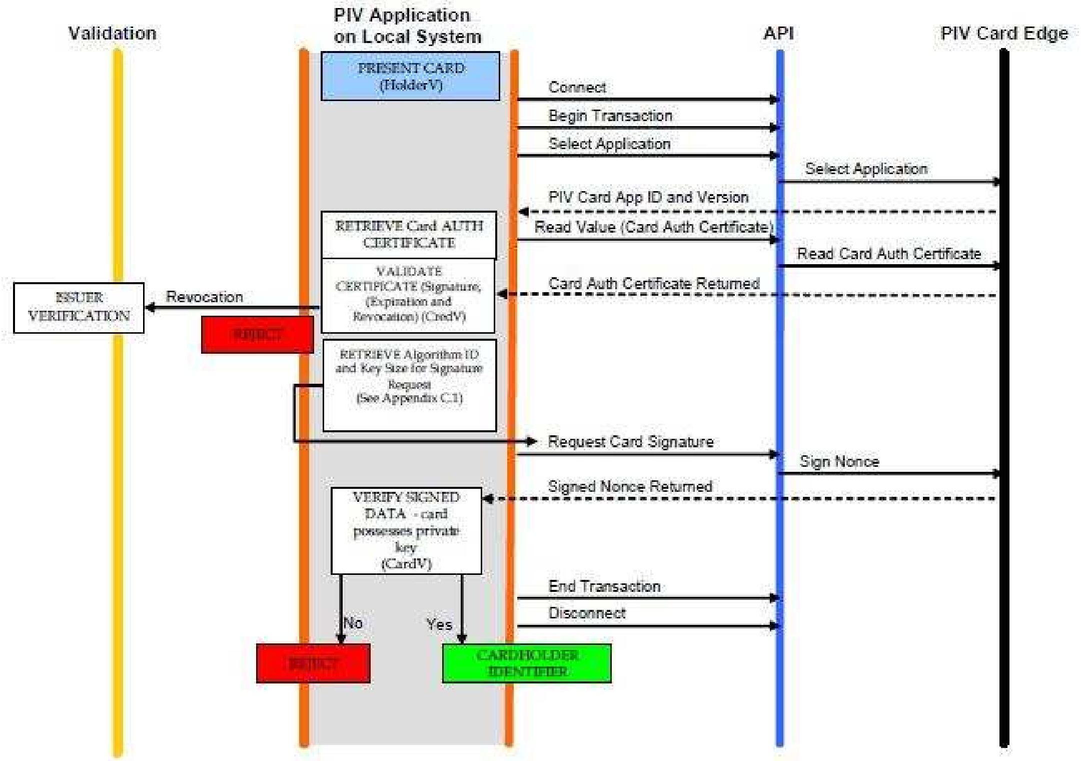

Validation
PIV Application on Local System
API
PIV Card Edge
PRESENT CARD (HolderV)
Connect
Begin Transaction
Select Application
Select Application
PIV Card App ID and Version
RETRIEVE Card AUTH CERTIFICATE
Read Value (Card Auth Certificate)
Read Card Auth Certificate
ISSUER VERIFICATION
Revocation
VALIDATE CERTIFICATE (Signature, (Expiration and Revocation) (CredV)
Card Auth Certificate Returned
REJECT
RETRIEVE Algorithm ID and Key Size for Signature Request (See Appendix C.1)
Request Card Signature
Sign Nonce
Signed Nonce Returned
VERIFY SIGNED DATA - card possesses private key (CardV)
End Transaction
Disconnect
No
Yes
REJECT
CARDHOLDER IDENTIFIER

Figure 4 PIV Active Card Asymmetric Authentication Flowgraph

- CHUID Verification + Biometric User Authentication: add a "what you are" biometric authentication factor. The biometric templates (fingerprints minutiae) are written in the TWIC card during the card issuing process, and can be retrieved by the TWIC readers. As it has been said, the biometric data is stored in a "PIV biometric object" (not enciphered) and a "TWIC biometric object" (enciphered with the TPK symmetric AES key). Both the TWIC application and PIV application inside the card will transmit the respective biometric objects, but in different ways:
  - PIV Application: only contact interfaces are permitted (magnetic stripe or chip contact slot reader), as the object is not enciphered. Also, the PIN input in the reader is required to retrieve the biometric object, adding a "what you know" authentication factor.
  - TWIC application: both the biometric object and the TPK key used to encipher it are transmitted to the reader. The biometric object can be transmitted through either contact or contactless interface, but the TPK can never be transmitted through contactless interface (it will be normally stored and retrieved from the magnetic stripe).

Once the reader retrieves (and deciphers) the biometric object, it obtains the biometric templates, the FASCN, and the digital signature of both elements signed together by the issuer. The reader must validate the authenticity of this signed data using its updated authorised issuer signing certificates list. If the checks are passed, then a fingerprint of the cardholder is taken from the TWIC fingerprint reader and matched against the templates.

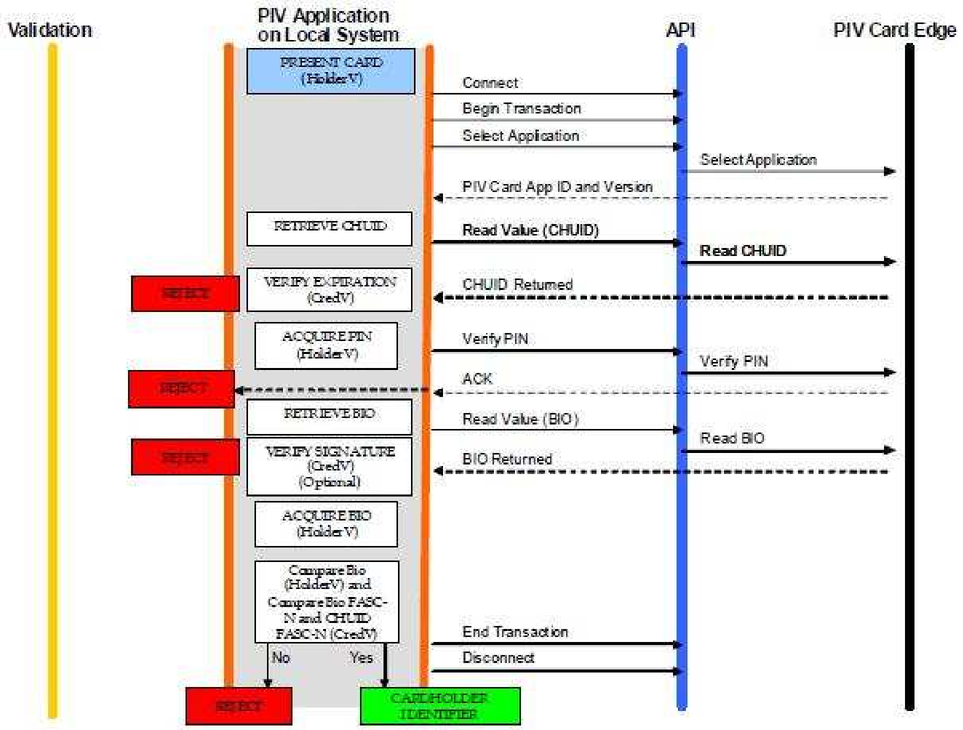


Figure 5 PIV Active CHUID Verification + Biometric + PIN Authentication Flowgraph

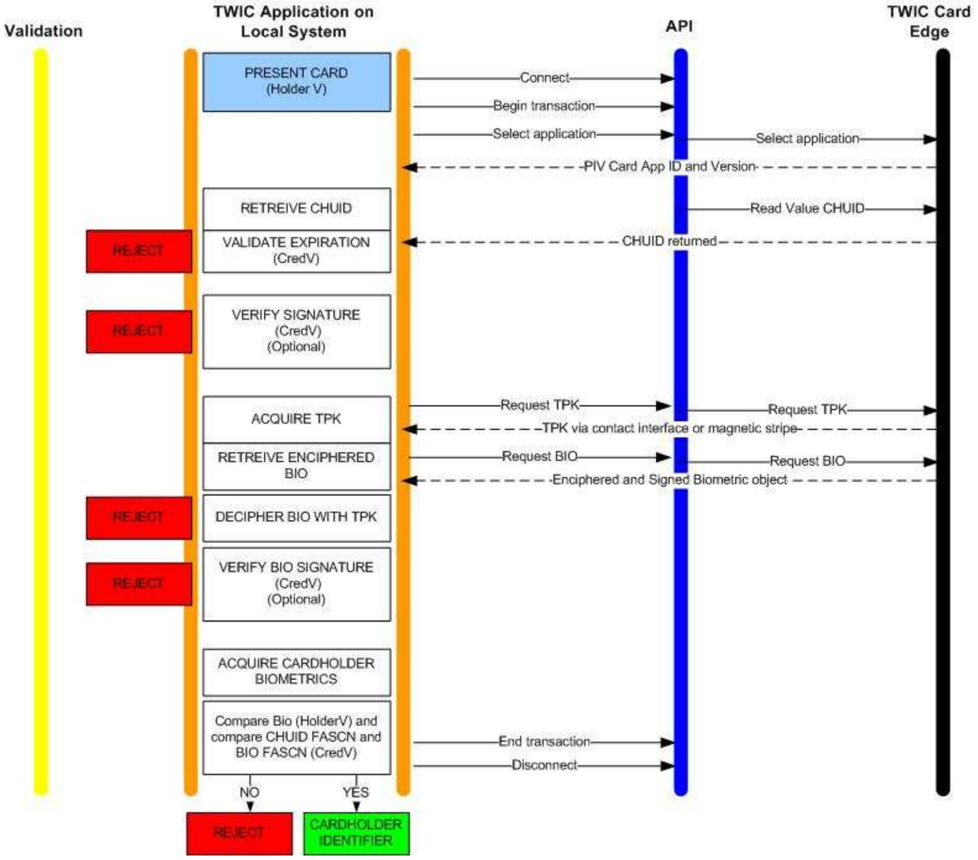

Validation
TWIC Application on Local System
API
TWIC Card Edge
PRESENT CARD (Holder V)
Connect
Begin transaction
Select application
Select application
PIV Card App ID and Version
RETREIVE CHUID
Read Value CHUID
REJECT
VALIDATE EXPIRATION (CredV)
CHUID returned
REJECT
VERIFY SIGNATURE (CredV) (Optional)
ACQUIRE TPK
Request TPK
Request TPK
TPK via contact interface or magnetic stripe
RETREIVE ENCIPHERED BIO
Request BIO
Request BIO
Enciphered and Signed Biometric object
REJECT
DECIPHER BIO WITH TPK
REJECT
VERIFY BIO SIGNATURE (CredV) (Optional)
ACQUIRE CARDHOLDER BIOMETRICS
Compare Bio (HolderV) and compare CHUID FASCN and BIO FASCN (CredV)
End transaction
Disconnect
NO
YES
REJECT
CARDHOLDER IDENTIFIER

Figure 6 TWIC Active CHUID Verification + TPK Enciphered Biometric Authentication Flowgraph

- Signed CHUID verification + Active card authentication + Biometric user Authentication: it's a combination of the previous modes, providing a two factor authentication, "something you have" and "something you are". It must be noted that both TWIC and PIV applications are being used to perform the card "something you have" authentication.

Conclusions: Pros and Cons of the TWIC Approach in the EPAIC Context

5.1.8.1. PROS

- TWIC system is able to work in two models, following the first EPAIC study criteria: networked model and standalone model. The only difference between both models is the connectivity of the reader with an external network, server or database required by the networked model to retrieve the data objects (biometric templates, identifiers, etc.). In the standalone model, data is transmitted, processed and managed between the card and the reader, and no information shall be transmitted from the reader to external networks. This model is an interesting approach when raising possible issues regarding the personal data transfer between State Members. Particularly, these key points in the TWIC standalone model should be focused on the biometric templates (which is considered the most sensible personal data used in the TWIC system, apart from those used in background checks during the issuing process):

    - Biometric data is stored in the card enciphered. It is transmitted enciphered as well, and it will be only deciphered in the reader.

    - The symmetric TPK key used to decipher the biometric data is never transmitted through the contactless interface.

    - In case of using the PIV non-ciphered biometric data object, it is never transmitted through the contactless interface, and a PIN password input is required for the reader to retrieve it.

    - Biometric matching is performed in the reader, and it will use the biometric templates acquired only for that purpose, and shall not transmit, use or store this data in any way.

    - In fact, only an inbound connection with the external system networks, servers or databases is required for retrieving the newest authorised issuer certificates, and any updated data or list necessary to check the validity, expiration and revocation of the cards. Outbound connections are not mandatory in the TWIC system approach.

    - Personal data inside the card is signed by an authorised issuer, and the reader will check these signatures to assure the authenticity of this data.

- The biometric data is bound to the card identification data by signing both the biometric templates and the FASCN identifier together during the issuing process.

- Card identification and authentication is checked through a unique identifier (FASCN number) assigned to each card (and therefore each cardholder) which is signed by the card authorised issuer. Card authentication is performed before proceeding with any biometric authentication process.

- In the case of the Active Card Authentication process, an asymmetric challenge-response algorithm against the card is additionally performed after the issuer signing certificate verification. This algorithm requires that the card ICC has capabilities to receive data (a random nonce) from the reader, and sign this data with an asymmetric unique and unreadable private key (CAK key). Card authentication is performed before proceeding with any biometric authentication process.

- The biometric data authenticity is also checked by performing this issuer signature verification.

- TWIC system is designed to accept different operation modes in the readers which are easily switched during the system operation. An operation mode is the configuration of the authentication and identification processes required (card authentication, biometric authentication, etc.), their sequence, preference of card applications to be executed, interfaces to be used, etc. The system must accept immediate changes between different operation modes, fast configuration of the new mode to be launched, without any interruption. In conclusion, the purpose of this feature is to make the system fast responsive when changing the operation mode required for each security level when an external event occurs. This is, the system is designed to be compatible with a different security level schema.

- The TWIC system also supports the execution of different card applications in the same card/reader. Each application inside the card is identified by a unique ID, and these applications can be part of different identification and authentication systems. For example, TWIC is compatible with PIV and CAC (Common Access Card) cards and readers, as the TWIC card contains the necessary TWIC, PIV and CAC applications inside. Aspects as the applications to be included, the execution preference order, and the applications executed by default can be configured.

- Multi-application compatibility and easily and fast configured operation modes are interesting features of TWIC regarding the following aspects:

  - Migration plan: possibility of doing a progressive migration of the local control access systems during the EPAIC implementation deployment.

  - Implantation of a security layered architecture approach: for example, a basic application without biometric authentication for the basic security level or non critical areas, and another application which may add a biometric authentication procedure for higher security levels or areas. On the other hand, configurable and event-triggered operation modes can be used to improve the system response when the security level is tightened due to any incident or risk.

  - Possible compatibility of the EPAIC card and reader with other identification cards used in the ports. This would avoid the problem of having multiple cards, an issue stressed by the stakeholders in the first EPAIC study.

5.1.8.2. CONS

- The TPK key is unique and constant for each card. That means that, if eventually the key is stolen, the biometric data security would be compromised. When symmetric keys are being used, transmitting the key itself between the involved parties is not a good practice. So, challenge-response algorithms or dynamic one-use key generation is recommended. Such approaches should be considered if key interchanging between card and reader is necessary. Card capabilities to dynamically generate one-time keys shall be further analysed.

- Authentication of the reader is not considered in the TWIC system. Therefore, all readable data inside the card could be retrieved by a fake or manipulated reader, even if this data is enciphered. Even if the control access area or the readers are physically protected, a social engineering attack against the cardholders to make them use their cards in fake readers could be done.

- The information inside the card, although enciphered, is actually transmitted to the reader for authentication processes. Possible legal issues regarding personal data transmission between different countries may arise from this point, and should be taken into account further in the present study.

- These legal issues regarding personal data transmission between State Members could be more complex if any personal data is required to be shared between the ports involved in the EPAIC system, more than the issuer signing certificate list, revocation and expiration list, and registered card identifier (FASCN in the TWIC system) list. If only the card identifier and its issuer certificate to authenticate the card is required for the ports to implement their control access policies, then this issue can be ignored. But, if the port control access system need to be informed of who is going to access the port facilities and when (particularly, it may be required for non frequent visitors), this point shall be further studied.

- In case of using an operation mode without biometric authentication (which may be the most probable option in basic security levels or areas), the TWIC system will only perform card authentication. Thus, in an unattended control access point, the identity of the person would not be checked, and therefore identity supplanting of the legitimate cardholder would be possible. In fact, even if a attended visual identification check is performed, if the card printed photograph and name are manipulated or forged the cardholder identification check would be fooled as well, as the TWIC card, unlike ePassport credential, does not contain the name and photograph of the cardholder stored inside the card.

5.2. ALFAPASS

5.2.1. OVERVIEW

Alfapass is an identification card for regular port visitors developed under the commitment of the Belgian port community, represented by Alfaport Antwerp. A co-operative company (Alfapass CVBA) was established along with Cepa and Seagha, becoming responsible for the development of a uniform ID system for the Antwerp port and the management of a shared database. The main goal of Alfapass was to avoid frequent visitors the burden of carrying a different access badge for every different company they had to visit. The card also offers the frequent visitor the advantage that his visits will be handled much more smoothly than those of an occasional visitor that doesn't disposes over an Alfapass card. Currently, it is being applied on the ports of Antwerp, Zeebrugge and Ghent.

Individual port terminals can voluntarily adhere and support this technology, while they will remain responsible for awarding access rights and installing the reading equipment or tuning their access control systems to the ALFAPASS ID-card, with third party suppliers' help.

AlfaPass is offered with or without biometric identification built in and with the capability of serving an Application Programming Interface (API) for integration with currently installed access control systems. In case that there are no electronic readers available, visual identification is also supported.

5.2.2. CREDENTIAL AND INFORMATION SPECIFICATIONS

The following data will be available in a legible format on the Alfapass card:

- Name and surname.
- Date of birth.
- Coloured photograph.
- Nationality.
- Card number.
- Card validity date.
- Employer.

Holder's biometric data (mainly hand geometry template or optionally fingerprints) will be electronically stored in a chip embedded within the card. An initial assessment valued hand geometry as the most suitable biometry, and lately (from 2007 on) fingerprint storage capabilities were added to the card.

The technology used consists of a contactless Mifare smartcard with a 4 kbyte memory chip. As aforementioned, the chip holds the biometric data while the other data are displayed on the surface of the card. A hologram and UV markings prevent any counterfeiting of the card, its photograph or other data, commonly used for a classic visual identification. Thus, a card whose data has been altered can be easily identified by an experienced member of the port facility personnel.

Data stored on the card is ciphered and can only be read by using public keys, distributed on the readers allowed to access sensitive data. Data changes require of the private key set that were originally used by AlfaPass CVBA when issuing the cards.

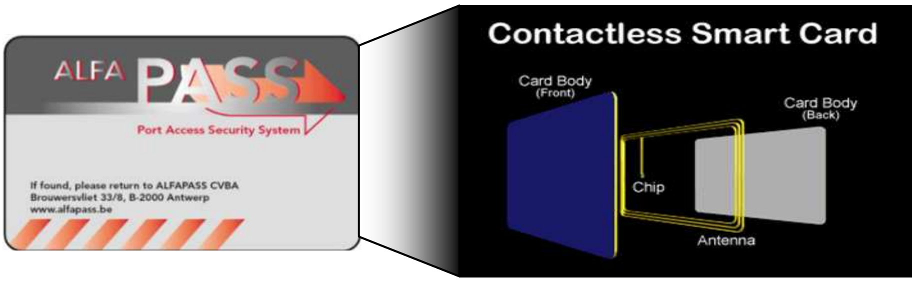

ALFA PASS
Port Access Security System
If found, please return to ALFAPASS CVBA
Brouwersvliet 33/8, B-2000 Antwerp
www.alfapass.be
Contactless Smart Card
Card Body (Front)
Card Body (Back)
Chip
Antenna

Figure 7 Alfapass Card Look and Components

In addition, the unique number of the Alfapass-card and additional data such as the holder’s telephone number and address are stored in a central database, managed by Alfapass CVBA.

Interoperability with the Belgian e-ID card was initially on the scope of Alfapass project. Yet it was discarded because e-ID made use of a contact interface, which was then considered an undesirable constraint. There were other limitations such as lack of writable memory within the e-ID.

5.2.3. Scope – Involved Parties

The following categories of regular visitors are distinguished:

- Port labourers.
- Truck drivers.
- Port Facilities personnel.
- Others (quay shipping agents, quay agents, water clerks, ship chandlers, ...)
- Temporary visitors (not frequent)

Port Facilities can voluntarily integrate this technology with their control access systems, thus converging unmanned identification and authorization on the same card.

Information regarding technical specifications on Alfapass cards and interfaces remains confidential unless a Non Disclosure Agreement is signed between Alfapass CVBA and Port Authorities, which in turn should apply this NDA to third party suppliers.

5.2.4. Enrolment – Issuance Process

The overall process of card issuance is managed by Alfapass CVBA, who first enrols an employer (company or self-employed) needing Alfapass cards for its employees due to the activities they perform, as a customer. Subsequently, the employer must submit on-line or by email an enrolment form containing the relevant employees’ personal information, job responsibilities and position, as well as company information details. The application goes through a screening phase and if accepted, cards are issued and personalised.

Card issuance time can take from 2 days to 2 weeks. Once ready, they can be collected from several issue stations that Alfapass has established, by the card holder who should provide some means of identification. In case biometrics is used, templates are then added to the card along with the holder photograph.

In order to access individual Port Facilities, the card should be further activated when accessing for first time to each facility. The activation process for each company ensures that a card is also recognised by the local access control systems of the Port Facilities and specific access rights are allocated until the card's expiry date.

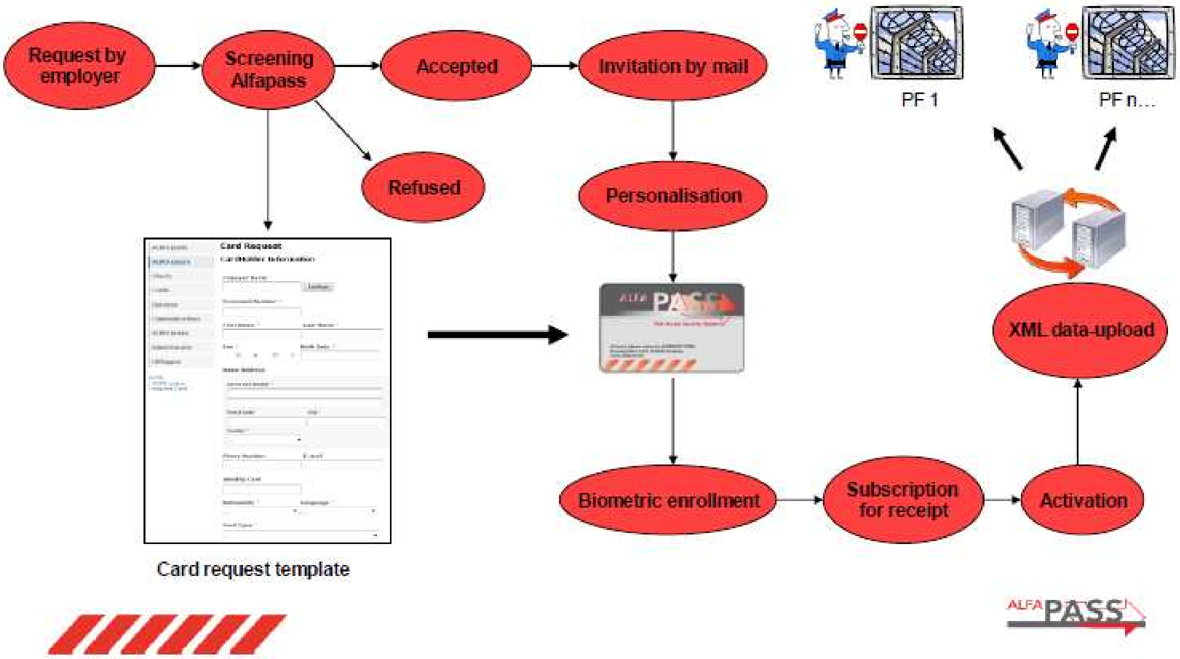


Figure 8 Alfapass Card Issuance Process

In addition to the normal Alfapass trucker card, a "starter card" concept has been developed in consultation with the transportation sector. It has been conceived in order to minimise the nuisance this card issuance process could involve to recently engaged hauliers, so that they can carry out their tasks in the port without any trouble. New drivers can hold a starter card for a period of up to 3 months while their final Alfapass card is being produced. Starter cards can be afterwards transferred to other new drivers if needed, but there can be no more than 10% starter cards (1 starter card for each 10 Alfapass cards owned by the company). There cards remains under the transport company's responsibility and supervision.

When the starter card is collected or transferred, the starter's biometric data (hand scan) will be put on the new card along with the other driver data. From then on, the starter card is fully linked to the driver's identity for regular use at the Port Facilities.

The Alfapass service has associated fees, for card production and yearly subscription, which must be afforded by the applicant. The cards have a validity period of 5 years, and then they have to be replaced.

5.2.5. CONCLUSION

Access rights to facility boundaries and premises are always managed by each Port Facility owner. Card holders have to ask each relevant facility security desk for card activation, first time accessing a specific facility or group of affiliated companies. This process comprises granting them customised right access.

Alfapass biometric technology relays on hand geometry and fingerprint. Anyway, use of strong authentication such as biometrics, is up to the Port Facility who remains responsible for issuing access policies to its own locations, and deploying the access control infrastructure.

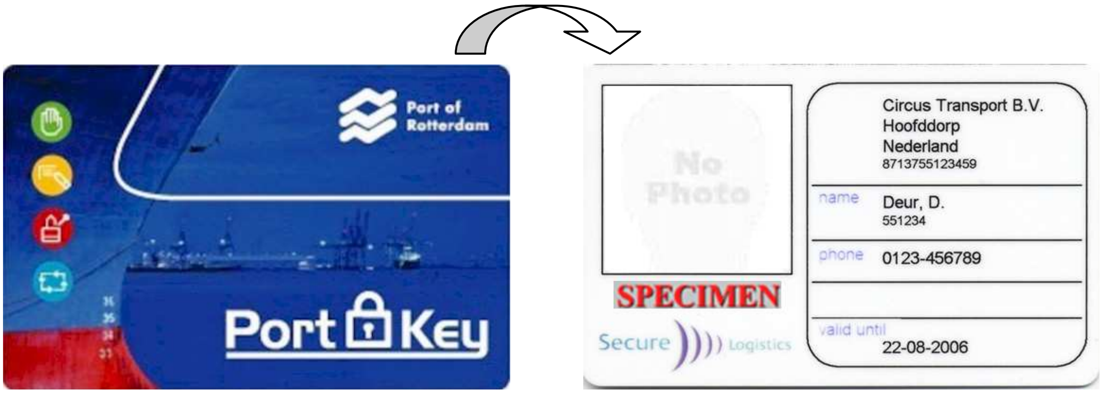
There are "starter cards" aimed to allow new drivers carry out their tasks in the port for up to 3 months, while their final Alfapass card is issued. These cards are still personalised and could hold the biometrics of the driver if required.

5.3. XSKEY PORTKEY

PortKey offers identification and access control capabilities to port facilities within Rotterdam port, and has been operational since 2004. Therefore, it has been implemented and experienced for a while becoming a stable enough technology and it is not known to have been deployed elsewhere than in the Rotterdam Port. This means no significant changes have been introduced since first EPAIC study analysed in-depth this credential, pointing out every relevant issue. Hence, we will just name the main characteristics of the product, without going further in their analysis, relying on the proficient source of information released by EPAIC study.

Summarizing, PortKey comprises data stored into a MIFARE integrated chip, regarding the employer and the card holder (or employee) as well as access rights to facilities. It depends on each facility infrastructure to make their own logical and physical access control systems compatible with the card, in order to control the access to secure and sensitive areas.

PortKey relays on hand geometry biometrics for reliable identification. Most of the data is also printed on the card surface. The card can be both used on a contactless basis or swiping the smartcard on the reader.



Circus Transport B.V.
Hoofddorp
Nederland
8713755123459

name Deur, D.
551234

phone 0123-456789

valid until 22-08-2006

Figure 9 PortKey Sample Card

The card is supposed to be specifically enhanced in order to withstand damages from the difficult port environment and harsh weather conditions.

Cards can be requested by the employee's contractor through a web based application. Secure Logistics, who remains responsible of PortKey exploitation, carries out checks regarding information and identity of the card holder and hand him the credential once produced.

Any company claiming the use of PortKey cards has to sign a Branch Security Statement with Secure Logistics. There are several clauses and data privacy statements aligned with EU data protection, included in the XS-Key Management System privacy regulations.

5.4. SEAFARERS' IDENTITY DOCUMENT (SID)

5.4.1. OVERVIEW

The "C108 Seafarers' Identity Documents Convention, 1958" was conceived as a professional identity document for Seafarers that would provide for some facilities, namely "shore leave" enabling seafarers to go ashore in foreign ports after perhaps weeks or even months on board, and facilities for joining their ship or for transit across a country for professional reasons.

The International Labour Organisation (ILO), a tripartite organisation, in which representatives of Governments, Employers and Workers take part with equal status, **adopted the Seafarers' Identity Documents Convention of 2003 (No. 185)** that revises the earlier Seafarers' Identity Documents Convention, 1958 (No. 108). The changes of 2003 relate to the identification of the seafarers. Their aim is to enhance the security features as well as the uniformity of the Seafarers' Identity Document (SID) that countries are required to issue to their seafarers, and lay down minimum requirements with respect to the countries' processes and procedures for the issuance of SIDs.

In order to successfully implement ILO Convention No. 185, Seafarers' Identity Documents (SIDs) issued in each ratifying State must be able to be used for verifying a seafarer's identity in every other State to which that seafarer travels in the course of his or her duties.

Consequently, because of several reasons, it is worth the review of the current situation in which this project remains. Main motivations are:

- EPAIC and SID share a common operational environment (port proximities, docks, shores, etc.) and are exposed to the same hazards and limitations, such as humidity, water and salt threatening the technology, as well as seafarers performing jobs which could affect their biometric factors.

- SID scope was regarded as a worldwide identity card, so it has to deal with troubles related to those EPAIC has to face. Interoperability and regulation rise as two of the most cumbersome issues to be resolved in both cases.

5.4.2. CREDENTIAL AND INFORMATION SPECIFICATIONS

a) *Legacy C108-SID.*

The "C108 Seafarers' Identity Documents Convention, 1958" stated on its Article 4, that the SID shall be designed in a simple manner, be made of durable material, and be so fashioned that any alterations are easily detectable. In accordance with [1] it shall be conceived to display:

- Full name (first and last names where applicable)
- Date and place of birth.
- Nationality.
- Physical characteristics.
- Photograph.
- Signature or, if bearer were unable to sign, a thumbprint.

Finally, the seafarer's identity document shall contain following information about the issuance process:

- The name and title of the issuing authority.

- The date and place of issue.

- A statement that the document is a seafarer's identity document for the purpose of this Convention.

b) New C185-SID.

In addition to the normal physical features for a modern machine-readable identity document, the new SID (defined through Convention No. 185) carries a **fingerprint-based biometric template**, which was adopted with the agreement of the world's shipowner and seafarer organisations. This template must conform to an international standard enabling the biometric templates on a SID issued by one country to be correctly read by devices used in other countries.

Seafarers' fingerprint biometric data comprising two-fingerprint templates shall be recorded using the standardised format, known as BioAPI compliant format (defined under the ILO SID-0002 standard) and embedded in a two dimensional barcode displayed on the card (or passport form booklet) surface. The barcode is to be encoded and printed using the PDF 417 barcode symbology specification defined in ISO/IEC 15438 [12], being readable with commercial hand held barcode readers.

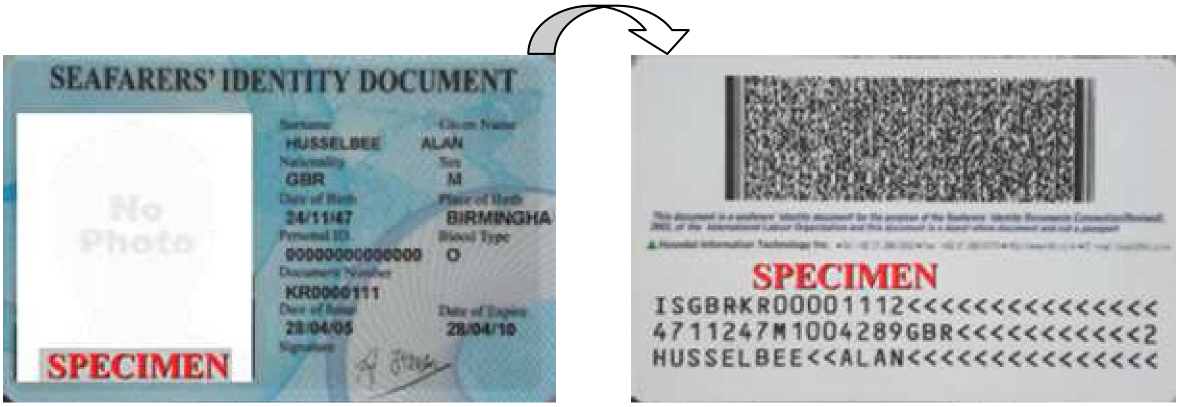
Additionally, the data requirements stated by ILO [3] correspond to the following fields that are both printed on the surface of the SID in plain text and appended to a machine-readable zone conforming to ICAO specifications, in order to support seafarer authentication:

- Full name of seafarer (first and last names where applicable).
- Nationality.
- Place of birth.
- Date of birth.
- Gender.
- Signature
- Date of issue.
- Place of issue.
- Issuing authority: country code of the issuing authority.
- Document number.
- Personal identification number.
- Expiration date.

The Convention also includes "any special physical characteristics that may assist identification" and the holder's signature among the data to be incorporated into the SID in accordance with [2].

Data on the document shall be protected by a laminate or overlay, or by applying an imaging technology and substrate material that provide an equivalent resistance to substitution of the portrait and other biographical data. The materials used, dimensions and placement of data shall conform to the International Civil Aviation Organisation (ICAO) specifications, mainly regarding compliance with Machine Readable Zone (MRZ) [9]. By contrast, biometric templates storage is not intended to comply with ICAO standards as further explained.

Other security features shall include at least one of the following features: Watermarks, ultraviolet security features, use of special inks, special colour designs, perforated images, holograms, laser engraving, micro-printing, and heat-sealed lamination.



SEAFARERS' IDENTITY DOCUMENT

Surname: HUSSELBEE
Given Name: ALAN
Nationality: GBR
Sex: M
Date of Birth: 24/11/47
Place of Birth: BIRMINGHA
Personal ID: 000000000000000
Blood Type: O
Document Number: KR0000111
Date of Issue: 28/04/05
Date of Expiry: 28/04/10
Signature

SPECIMEN

SPECIMEN

```
ISGBRKR00001112<<<<<<<<<<<<<<<
4711247M1004289GBR<<<<<<<<<<<2
HUSSELBEE<<ALAN<<<<<<<<<<<<<<<
```

Figure 10   C-185 Compliant SID Specimen

The ILO SID-0002 standard was meant to provide for an interoperable biometric template as required by Convention No. 185, covering fingerprint data capture, template generation and bar code storage. It was based on draft ISO standards dated October 2003 (ISO 19794-2 [11]), but modifications were made to satisfy the requirements of storing two fingerprint templates on a two-dimensional barcode. No manufacturers were known to have products that supported this new standard; consequently, modifications to commercial products were necessary.

Since 2004, the ILO has been performing tests on several biometric products, deployed on board cruise ships. The aim of these tests was to determine, in a realistic seafaring environment, whether they could meet the technical requirements of the ILO SID-0002 standard or not. The ILO’s stated performance criteria were a 1 per cent false rejection rate (or less) at a 1 per cent false acceptance rate.

After allowing vendors to modify software to resolve interoperability issues, three biometric products were found to meet the performance criteria while being able to interoperate correctly, processing fingerprint templates created by the other products. Lately, other biometric providers products have been added to the list of ILO SID-0002 standard compliant, after going through new test process, reaching up to 12 interoperable sensor devices from manufacturers in eight different countries available nowadays [4].

It is noticeable that information in the card, even biometrics, is stored unencrypted. In fact, the amended ILO SID-0002 standard (November 2005) states that data security should rely on cryptographic means through the data transference phase between card and service systems, by using secure messaging functions according to ISO/IEC 7816-4. This is not fully congruent since the ISO/IEC 7816-4:2005 is an “Identification card” standard focused on Integrated circuit cards, and consequently based on features far from SID capabilities.

On July 2009, the ISO and the IEC approved ISO/IEC 24713-3 standard [10], which is technically compatible with ILO Convention No. 185. It includes additional details in the standardization of the bar-code content, the biometric data, the national databases and the infrastructure needed for communication between different issuing authorities and those who may wish to verify the authenticity of a SID. Nevertheless, it also points out several technological recommendations to be adopted by ILO in a future, while maintaining backwards compatibility. Main references suggest to:

- Became compliant with the final published version of ISO/IEC 19794-2, instead of the older draft version profiled in ILO SID-0002 standard.

- Make use of contactless integrated circuits, following the specification for an ePassport. These contactless ICs shall allow the storage of fingerprint minutiae records (but not finger image data) and a digital representation of the photograph printed on the document, conformant to ISO/IEC 19794-2 and19794-5 respectively.

- Apply Basic Access Control features, such as those used in ePassport, when using contactless IC in order to read fingerprint minutiae data. Briefly, this means no encryption should be needed although ensuring a higher degree of data protection.

- Use a Public Key Infrastructure (PKI) that allows verification of data reliability against the issuing authority. It would relay on digital signature of MRZ and barcode contents and a PKI such as the ICAO Public Key Directory being used for ePassports. Where on-line access via a PKI secured infrastructure is not available, the verification station should download and refresh information cached from the trusted third party whenever on-line access become ready. Anyway, the stored information (including SID revocations) should be refreshed no less frequently than once a month.

- Consider the deletion of sensitive data, used by components during enrolment or verification processes, which should remain no longer accessible once processes are completed.

5.4.3. Scope – Involved Parties

Each ratifying member shall implement a **national electronic database** and designate a permanent focal point, in order to manage SID verification inquiries from competent authorities of all Members of the Organisation. The Convention requirements on security and personal data protection are aligned with main EU Directives on the matter (procedures to allow holders to check or modify their data, no data exchange or use against the purposes it was collected for, etc.).

The information stored within the database, shall be restricted to:

- Issuing authority named on the identity document.
- Full name of seafarer as written on the identity document.
- Unique document number of the identity document.
- Date of expiry or suspension or withdrawal of the identity document.
- Biometric template appearing on the identity document.
- Photograph.
- Details of all inquiries made concerning the seafarers' identity document.

Due to the evolutions already presented, a conflict of interests has arisen among countries which hence have rarely adopted the C185 so far. ILO asserts in [6] that only 18 countries have ratified it at the present time, most notably France, Nigeria and recently the Russian Federation, contrary to the 59 ratifying the previous convention [5].

Ratifying countries shall be able to:

- Issue national Seafarer ID against the ILO C185 published compliance criteria.

- Validate queries against any issued SID by reference to a national electronic database in which each issued, suspended or withdrawn SID must be registered.

- Verify Seafarer IDs issued by other member States through the national focal point of the country of issuance, who must be available 24 hours a day, seven days a week.

Thereafter, this Convention shall come into force for any Member six months after the date on which its ratification has been registered. In some cases, this might lead to change requirements on national legislation.

Main claims against the new document adoption are focused on legal aspects related to personal data treatment, interoperability or technical issues posed by the new biometrics format which doesn't follow

ICAO or other widespread approaches, and the costs associated to such a nation-wide infrastructure. Finally, most countries are reluctant to adopt this convention until the majority has already done.

Regarding SID users community, this document would only apply for seafarers, when this term is applied to any person who is employed or is engaged or works in any capacity on board a vessel, other than a ship of war, ordinarily engaged in maritime navigation. Therefore, it doesn't take into account any other of the individuals involved on daily activities inside or around ports.

5.4.4. Enrolment – Issuance Process

Seafarers may only apply for a SID to the Member state they belong to. Each Member for which the Convention (C185) is in force shall issue a SID to each of its nationals or to those who have been granted the status of permanent resident in its territory, who are seafarer and make an application to that effect. The application is registered on a personalization centre where the document is pre-produced and sent to one of the application stations supplied with fingerprint capture and barcode reader devices. There the applicant registers its biometrics in the document and databases, retrieving afterwards its final SID document.

The issuance of SID may be subject to the same conditions as those prescribed by national laws and regulations for the issuance of travel documents. Applications go through the proper screening process by the corresponding authority that could reject the application, although the Seafarer must have the chance of an administrative appeal in that case.

The maximum validity of a seafarers' identity document shall be determined in accordance with the laws and regulations of the issuing State and shall in no case exceed ten years, subject to renewal after the first five years.

The country issuing SIDs must in addition arrange for an independent evaluation of the administration of its issuance system to be carried out at least once every five years. The evaluation report is reviewed in the framework of the ILO with a view to the maintenance of a list of the countries that fully meet the minimum requirements laid down by the Convention.

The SID shall be promptly withdrawn by the issuing State if it is ascertained that the seafarer no longer meets the conditions for its issue under Convention C185. Procedures for suspending or withdrawing seafarers' identity documents shall be drawn up in consultation with the representative shipowners' and seafarers' organisations and shall include procedures for administrative appeal.

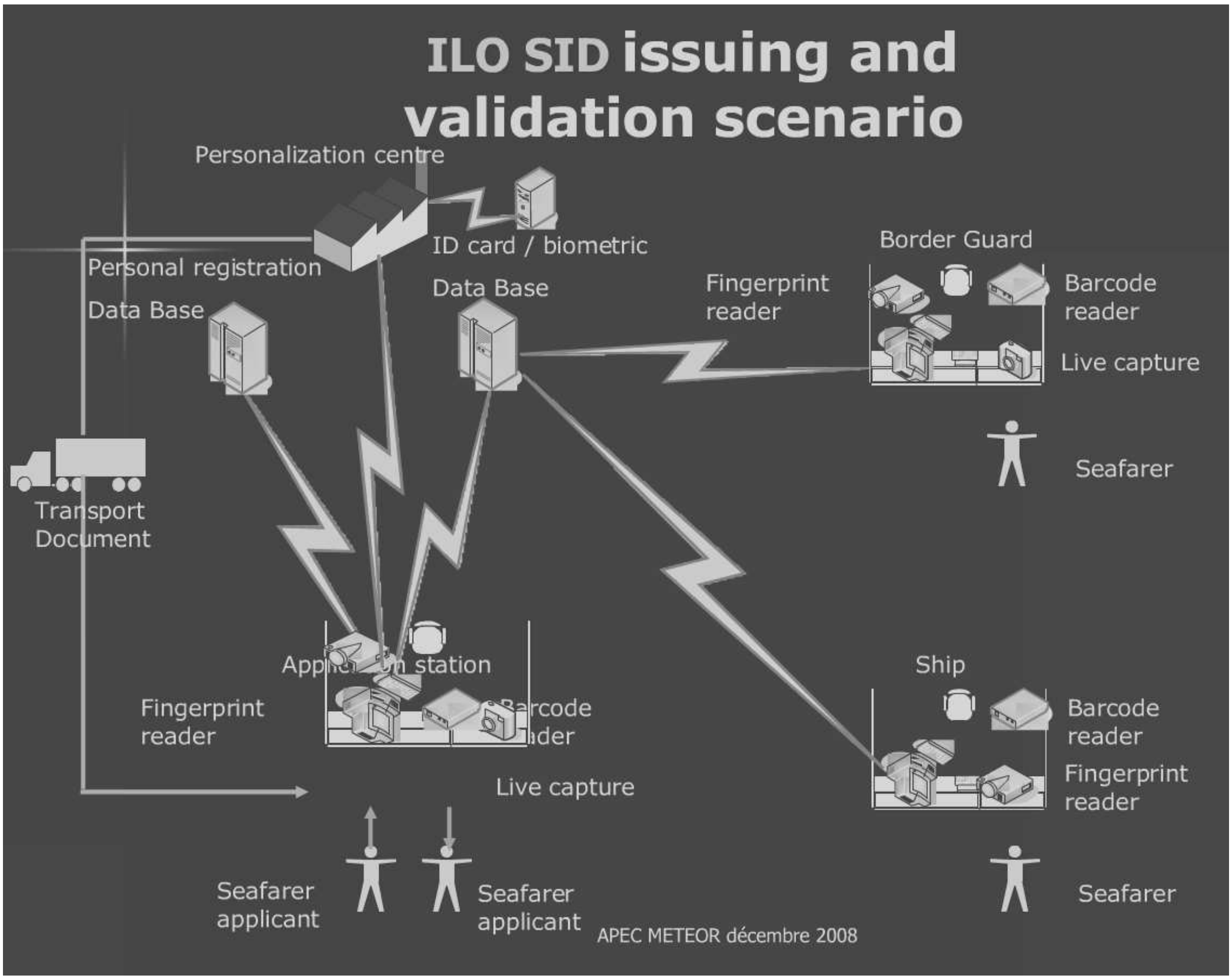


Figure 11 SID Issuance Process Flow

The Convention C185 points out the requirement of implementing security around the SID issuance and management practices, supplying ratifying members with guidance on implementing an issuance system. Through several mandatory results, as well as recommended procedures and practices, it will assist to achieve a reliable and more secure identification documents management. These results and procedures are focused on:

- Production and delivery of blank SIDs
- Custody, handling and accountability for blank and completed SIDs
- Processing of applications; suspension or withdrawal of SIDs; appeal procedures
- Operation, security and maintenance of the database
- Quality control of procedures and periodic evaluations

Finally, no background checks are requested as part of the SID issuance process. However, this is a practice that is being reinforced in other environments closely related as evidenced by the Crew Member Certificate (CMC). CMC is a pre-designed MRZ readable credential supported by ICAO, and used in the aviation sector similarly to SID in the navigation one. Statutory use of CMC falls under the scope of Convention on International Civil Aviation [13] and its issuance is subject to a background check completion, carried out by or on behalf of the relevant government office [14].

5.4.5. CONCLUSION

The Seafarer Identity Document is, as its own name states, only focused on seafarer individuals omitting other port user categories which fall under the European Community worries when protecting ports and facilities within. Besides, the SID is solely concerned about verification and identification, with no access control features in its conception.

This Convention tries to set a global mechanism to verify seafarers' identity even in real time, with the provision of focal points and nation-wide databases, able to perform validation checks against centralised data under request. In some cases, use and interchange of biometric data as well as centralised personal information storage (including biometric templates) might push ratifying Members from all over the world to introduce national regulatory changes, thus hindering its general adoption.

The development of a new standard for biometric data storage, instead of the adoption of a widespread accepted one such as ISO/IEC 19794-2, played an important role against the general ratification of the Convention and consequently of the improved SID. Manufacturers were forced to develop new solutions delaying any implementation of infrastructures, and contributing to a lack of maturity in the available products that may threaten some countries. Furthermore, the fact biometric templates within SID documents are unencrypted and effortless readable (using commercial devices as fake barcode readers) may likely cause distrust and uneasiness among stakeholders. However, recent publication of the ISO/IEC 24713-3 standard gives a valuable support to SID implementation, even though it raises several areas in need of improvement, such as data protection and enhanced technological alternatives (mainly contactless integrated circuits).

However, the pool of tests carried out on behalf of SID fingerprint compliant readers, is priceless. Some of the tests took place on real port environment conditions (performed on board cruise) and were tested on a key population such as seafarers, showing that biometric technologies are able to operate properly on EPAIC II scenarios alike.

The Convention No. 185 also stresses the importance of policies and procedures (some of them are mandatory requirements) that may guarantee a security baseline, throughout the SID lifecycle management..

5.5. MARITIME SECURITY IDENTIFICATION CARD (MSIC)

The Maritime Security Identification Card (MSIC) is an Australian identification card which is issued to identify a person who has been the subject of a background check. It shows that the holder has met the minimum security requirements and needs to work unescorted or unmonitored in a maritime security zone.

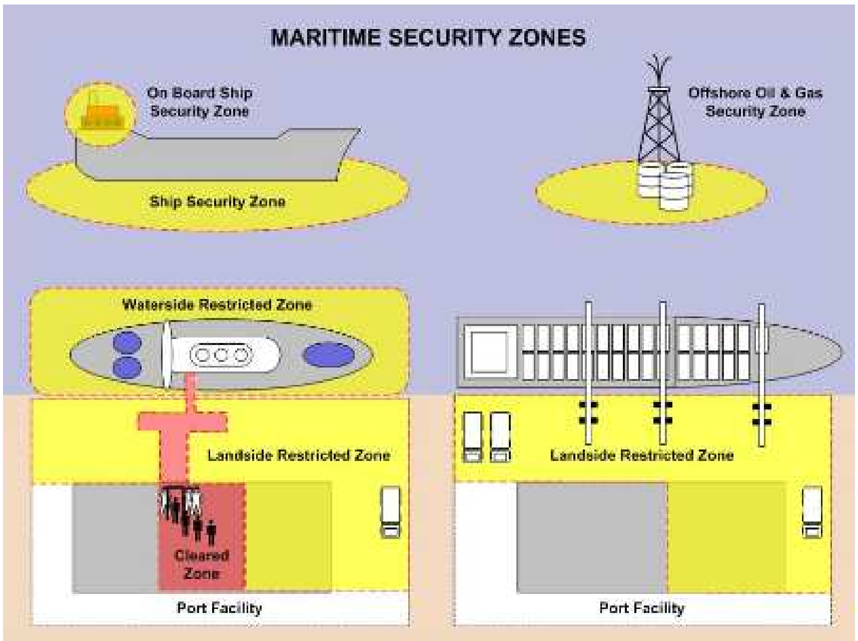


Figure 12 Maritime Security Zones

The Maritime Security Identification Card, is as its own name claims just an identification card the Australian Department of Infrastructure, Transport, Regional Development and Local Government has sponsored. That means, no access control is derived from the use of this technology and the relevant authority at each port or facility still controls access to its maritime security zones. That could lead to a burden of cards, as the requirement of a control access card still remains wholly distributed.

Nevertheless, some of the features this MSIC holds are aligned with EPAIC goals, thus deserving to be considered herein.

Legal requirements have been implemented in Australia, through the Maritime Transport Security Act 2003. Several reviews have been undertaken and have led to a number of legislative and other regulatory changes. Finally, in June 2005, the Maritime Transport Security Act was amended to cover Australia's offshore oil and gas facilities and was renamed the Maritime Transport and Offshore Facilities Security Act 2003. Both acts aim to safeguard against unlawful interference with maritime transport or offshore facilities, by establishing one security regulatory framework. One of the major provisions in the legislation was the introduction of a new security identification card for Maritime workers.

5.5.1. CREDENTIAL AND INFORMATION SPECIFICATIONS

The regulation thoroughly establishes the requirements for both the cards (size, shape, data, etc.) and the background check process. Regarding the card appearance and data displayed, it has to be told that the MSIC has neither information storage component nor electronic device (RFID, magnetic band or smart chip are not integrated). It is **only useful for visual examination and non-automated validation**. The design of the card aims to ease the distinction between permanent worker (background colour is blue) and temporary ones (background colour is orange). MSIC are valid for up to five years, unless cancelled.

The only information gathered over the card is the one showed on its surface, as it is shown below, comprising:

- First and last name.
- A recent photograph with tampering-protection.

- An expiry date.
- A unique identifying number.

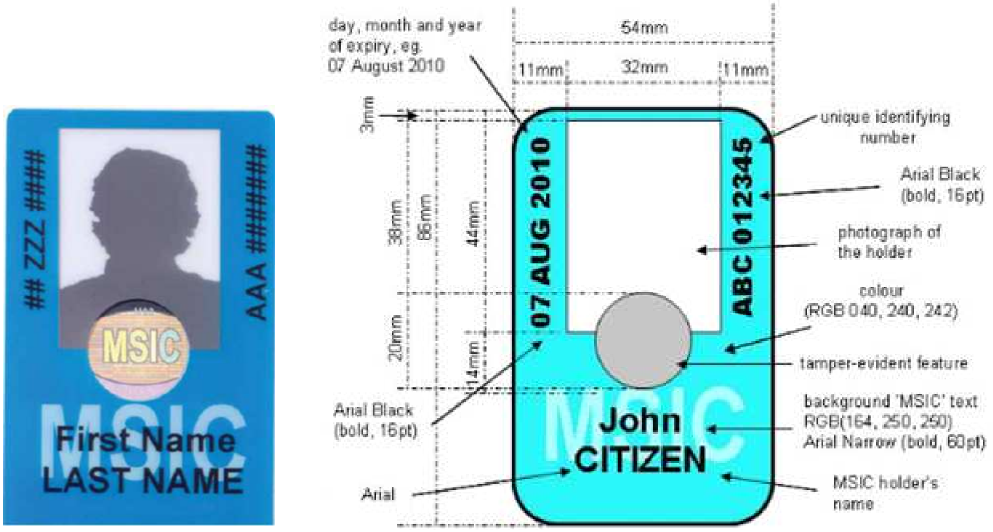


Figure 13 MSIC Sample Card

5.5.2. SCOPE – INVOLVED PARTIES

The requirement of having a MSIC card in order to access facilities applies to:

- Port, port facility and port service workers;
- All waterfront workers;
- Offshore industry participants;
- Seafarers on Australian regulated ships;
- Maritime industry participants or employees of a maritime industry participant such as:
- Contract workers and labour hire firms;
- Agents (including freight forwarders and cargo agents);
- Security contractors;
- Maintenance staff;
- People working on or providing services to ships and offshore oil and gas facilities, including catering and maintenance companies;
- Supply ships and maritime rescue services;
- Helicopter and amphibious pilots transporting personnel to ships and offshore facilities; and
- Transport operators such as train and truck drivers.

By contrast, emergency personnel such as Defence Forces, law enforcement officers or ambulance, rescue or fire service officers who are responding to an emergency are not requested to hold any MISC.

5.5.3. ENROLMENT – ISSUANCE PROCESS

There are two main requirements to get a MSIC. First one is the need for unescorted access to a security zone. The second one is to have been the subject of a **background check**. The whole MSIC application goes through three phases, involving different official bodies. The process is as follows:

1. The individual must apply for an MSIC through an approved MSIC issuing body, whose duties are to confirm the applicant's identity, confirm the applicant’s operational need for an MSIC, and if necessary, confirm the applicant’s right to work in Australia. In the meantime, the issuing body also submits a request for a background check of the applicant by AusCheck (branch of the National Security Law and Policy Division within the Australian Attorney-General's Department).

2. The first background check step is an assessment of a criminal records check undertaken by the Australian Federal Police, which is used to determine if an applicant has an adverse criminal record. A person has an adverse criminal record if he or she has been convicted of a Maritime-security-relevant offence (MSRO) and sentenced to imprisonment (including a suspended sentence, periodic detention, home-based detention, and detention until the rising of the court). The list of Maritime-security-relevant offences is defined within regulation.

3. A security assessment conducted by the Australian Security Intelligence Organisation.

Ignoring the requirement of holding the card always visible, as well as every misuse of the card or any other related offence, is liable to a fine.

5.5.4. CONCLUSION

MSIC sets an example of a port oriented protection effort, based upon legal requirements not far from EU ones. Its main aim is identification of people accessing maritime security zones, and a prior assessment of the security threat they represent by means of a complete background check.

Checks are initially delegated to approved issuing bodies who then, ask the appropriate agencies to get their support in the task.

Nevertheless, the drawback of MSIC is that it is not regarded as a control access card, and it has no technology items (RFID, magnetic strip or chip) that could allow neither the addition of a control access oriented feature nor unmanned identity validation.

5.6. MARINE TRANSPORTATION SECURITY CLEARANCE PROGRAM (MTSCP)

5.6.1. OVERVIEW

The Marine Transportation Security Clearance Program (MTSCP) was initiated in January 2003 with a commitment to introduce background checks of workers at marine facilities and ports, conducted by the Transport Canada, who is responsible for transportation policies and programs in Canada. It answers to the requirements covered under the 1994 Marine Transportation Security Act, further defined by the Marine Transportation Security Regulations.

One of the provisions of this regulation is to introduce a clearance program (MTSCP) in order to reduce the risk of security threats by preventing unlawful interference with the marine transportation system by conducting background checks on marine workers who perform certain duties or who have access to certain restricted areas. The regulation also claims for the use of restricted area passes conceded to these individuals, proving they hold the needed authorization.

Under the program, port workers will require a transportation security clearance to gain access to certain restricted areas. The designated restricted areas include:

- Areas in the marine facilities that contain the central controls for security and surveillance equipment;
- Areas that contain the central lighting system controls;
- Areas that are designated for the loading or unloading of cargo and ships’ stores at cruise ship terminals; and
- Land adjacent to vessels interfacing with cruise ship terminals.

5.6.2. Credential and Information Specifications

The Marine Transportation Security Regulations asks for the existence of a restricted area pass that an individual accessing a restricted area should hold. Furthermore it establishes the requirements this pass shall be compliant with.

The mandatory data this pass should include is:

- Name.
- Height.
- Eye colour.
- Photograph.
- Expiry date.

If the pass owner holds a security clearance, both expiry dates should be coincident, and the pass shall bear a mark that clearly distinguishes it from restricted area passes issued to persons who are not security clearance holders.

Biometrics is only pointed out as best practice recommendations. The same happens with interoperability with other systems within the facility and/or nationally, which is considered a best practice by the program, thus not mandatory. Several references are done to the aviation system that has implemented a national pass system for a Restricted Area Identity Cards (RAIC) based on Smart Cards, ICLASS contactless technology, with embedded biometric templates to allow for confirmation of the individual’s identity; (i.e. the card holder is the person to whom the card was issued) and confirmation that the cardholder still has a valid clearance.

Temporary restricted area passes need not meet the requirements previously stated but they shall also bear a mark that clearly distinguishes them as a temporary passes.

The holder of a restricted area pass shall, when they enter or remain in a restricted area, display the pass on their outer clothing and above their waist with, except in the case of a temporary restricted area pass, their photograph or other facial image visible at all times.

5.6.3. Scope – Involved Parties

The requirement of going through a security clearance in order to access facilities applies to port workers occupying certain positions or responsible for specific duties have been designated as requiring a transportation security clearance. Designated positions and duties include the following:

- Licensed ship pilots;

- Harbour master or wharfingers;
- Security responsibilities, including authorised screening and security guard functions;
- Access to a cruise ship that is interfacing with a restricted area two, to provide services, supplies or equipment to the cruise ship or a member of the complement of the cruise ship;
- Seafarers who have submitted an application for a Seafarer's Identification Document; and
- Those which could cause the failure of preventative measures, delay the response to a security incident or adversely affect the recovery from a security incident as a result or being assigned or performing any of the following duties, responsibilities or functions:
  - access to security information at the marine facility or port;
  - supervision of the marine facility operations;
  - creation, alteration, control or maintenance of cargo documentation for crew or passenger lists by a person who is present at the marine facility or port or who has advance access to the documentation or lists; or
  - planning or directing of the movement of cargo or containers at a container terminal, including their loading and unloading into and from vessels.

Nonetheless, any police force in Canada, the Canadian Security Intelligence Service, the Canadian Forces or a provider of emergency services who is on duty are neither expected to hold any restricted area pass nor a clearance.

Commercial truck drivers are exempt to get the clearance in case they are required to enter a restricted area two at a marine facility or port as part of their commercial activities, and provided that they hold alternative authorizations such as a valid FAST/EXPRESS card.

5.6.4. Enrolment – Issuance Process

In order to obtain a transportation security clearance, applicants will report to an enrolment site at the appropriate port administration to submit an application package. The enrolment site will be responsible for submitting the application to Transport Canada. Transport Canada will then conduct a background check, in concert with the appropriate agencies. The process is as follows:

- The Royal Canadian Mounted Police (RCMP) investigates criminal records and relevant files of law enforcement agencies, including intelligence gathered for law enforcement purposes.
- The Canadian Security Intelligence Service (CSIS), performs an indices check and, if necessary, a CSIS security assessment.
- The Citizenship and Immigration Canada checks the applicant's immigration and citizenship status, if required.

Once satisfied that the applicant does not pose a risk to marine transportation security, Transport Canada will approve the application for a transportation security clearance and notify the respective port. A restricted area access pass will then be issued to the individual by the port's pass control office. Ports or enrolment sites does not keep or use the information for any other purpose. The information (data, documents, photographs or fingerprints gathered to support the background check process) is transmitted electronically to Transport Canada through secured channels. Paper copies of the application form and documents are sent to Transport Canada for processing.

The Marine Transportation Security Clearance Program also includes a reconsideration process for marine workers. An applicant whose transportation security clearance has been refused or cancelled can apply to the Office of Reconsideration (OOR), which will arrange for an independent assessment of the case and make a recommendation. The OOR is independent of the office that made the original evaluation and recommendation. Information on the OOR will be made available to applicants at the enrolment sites, and additional details are available on Transport Canada's website.

5.6.5. CONCLUSION

The MTSCP is a Canadian country-wide program intended to obtain a security assessment for those individuals accessing without due escort to maritime restricted areas, by means of a complete background check, that involves security forces and intelligence services.

Canadian maritime regulation claims for the use of passes (giving local/port authorities enough freedom to design them by themselves) in order to access restricted areas, and also for background checks to be performed when the area to be accessed is highly sensitive. Passes delivered to clearance holders should be easily to recognise. Once again it is not a control access technology in itself but rather an identity and authorization proof, as it happens with Australian MSIC.

5.7. IDENTIFICATION AND VALIDATION WITHIN SECOND GENERATION EPASSPORT

5.7.1. OVERVIEW

In the aftermath of September 11, 2001, the US changed its entry requirements and obliged all countries participating in the Visa Waiver Program to start deploying electronic passports as of October 26, 2006. As a result, European Commission (EC) passed the (EC) 2252/2004 regulation, calling for common technical specifications to enable biometric markers on travel documents. First approach, claimed to include facial biometric image in all ePassport with deadline August 2006, in what is called first generation ePassport.

The second phase of the technical specifications from (EC) 2252/2004, which called for the use of fingerprints as a second biometric marker in ePassports, was adopted by the European Commission on June 28, 2006. This time, deadline for compliance was set for June 28, 2009.

While it may be thought ePassport has no apparent connection with port access control, the main reason why it has been taken into consideration, is that it raised similar issues to those faced in EPAIC such as use of biometrics (both facial and fingerprints), connectionless communications (mainly RFID), time response thresholds and European wide infrastructure. Certainly, it also has to deal with legal issues around data privacy and data security.

Credential and Information Specifications.

5.7.2. FIRST GENERATION EPASSPORT

Data stored in the first generation ePassports comprised the holder's biographic data like their name, date and country of birth, as well as the holder's face image as biometric data.

This ePassport relied on three security measures, in order to validate the authenticity of data stored and provide protection against eavesdropping or ePassport cloning. So, they were carefully designed to be tamper- and forgery-proof. Those measures were:

Basic Access Control (BAC). It enables an inspection system to read the data from the chip only if it proves it has physical access to the Passport using a challenge-response protocol including data from the optically read Machine Readable Zone (MRZ), avoiding skimming attacks. Cryptographic session keys are generated enabling subsequent data communications between the chip and the inspection system to be encrypted by Secure Messaging to protect against eavesdropping.

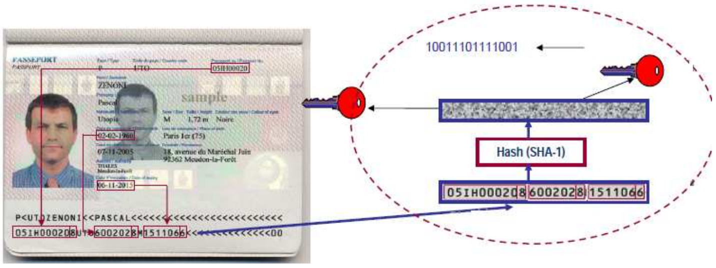

PASSEPORT
ZENONI
Pascal
sample
P<UTOZENONI<<PASCAL<<<<<<<<<<<<<<<<<<<<<<<<<<
051H000208UTO6002028M1511066<<<<<<<<<<<<<<00
10011101111001
Hash (SHA-1)
051H000208 6002028 1511066

Figure 14 ePassport – BAC Session Keys Generated from MRZ Data

- *Passive Authentication*. It is meant to authenticate the data that is read from the ePassport by validating the signature of that data, using the appropriate Public Key certificates from the Issuing State. There are 16 slots of data which hash is signed with the Private Key from the issuing state, thus allowing checking its integrity and0 authenticity.

- *Active Authentication*. This was an OPTIONAL protection, whereas BAC and Passive Authentication were mandatory. Active Authentication aim was to avoid chip cloning, by verifying that the chip itself is genuine. This check is achieved by means of a challenge-response protocol based on a unique secret key stored in a protected memory which can't be read nor cloned.

5.7.3. SECOND GENERATION EPASSPORT

The addition of fingerprints or even iris biometrics to the new (or second) generation ePassports drove to a security improvement need in order to better protect this highly sensitive information. Thus the second generation of ePassport defines new security measures, known as *Extended Access Control (EAC)*. EAC is intended to restrict access to sensitive data to the issuing country and countries that have permission from the issuing country.

EAC overall approach introduces additional certificates and another hierarchy of Certification Authorities over and above those defined in the previous specifications to support Passive Authentication. This gives the means to authenticate an Inspection System and determine that the system is authorised to read its sensitive data. But EAC also provides enhanced chip authentication and secure messaging features:

- *Chip Authentication*. It is an alternative to Active Authentication and the Secure Messaging implemented as part of Basic Access Control. It proves the microprocessor is genuine relying on secret key and shared secret technology, and thus protecting the electronic passport against cloning. It also improves the BAC security mechanism by replacing the encryption key (located within the MRZ code) with a totally random key.

- *Terminal Authentication*. It is mandatory whenever an access to sensitive data is performed. It aims to prove to the microprocessor that the terminal is allowed to access the data on the microprocessor. This access is granted through a chain of certificates, the root of which is the passport issuer. In other words, only the issuer of the passport controls who can access the data on the document

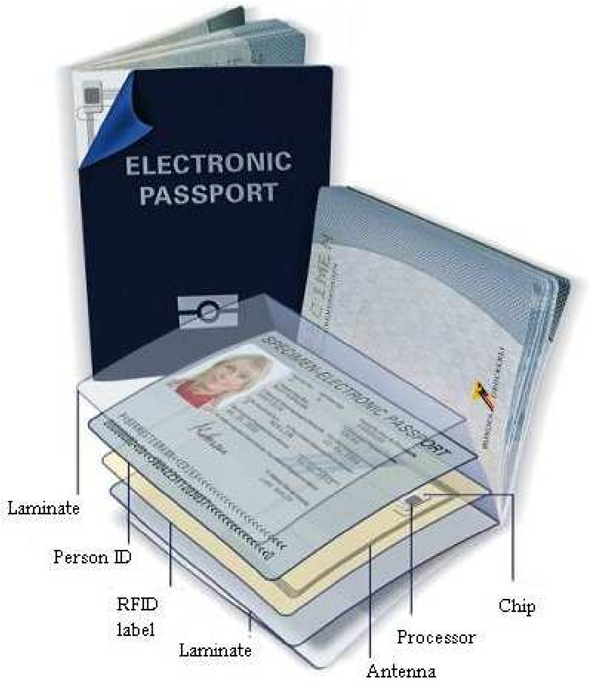


Figure 15 ePassport - Sample

The passport visible data content is shown below:

- Issuing state organisation
- Name of document
- Type of document
- Issuing state organisation code
- Passport number
- Name-Primary identifier
- Name-Secondary identifier
- Nationality
- Date of birth
- Personal number
- Sex
- Place of birth
- Date of issue
- Authority issuing office
- Date of expiry
- Holder's signature
- Holder's portrait

Additionally, the information stored on the Machine Readable Zone (MRZ) contains some of the previous data as well as control and check digits. Lastly, the chip holds the most sensitive information such as Face, Fingerprint and Eyes biometrics properly encoded within, besides personal data details.

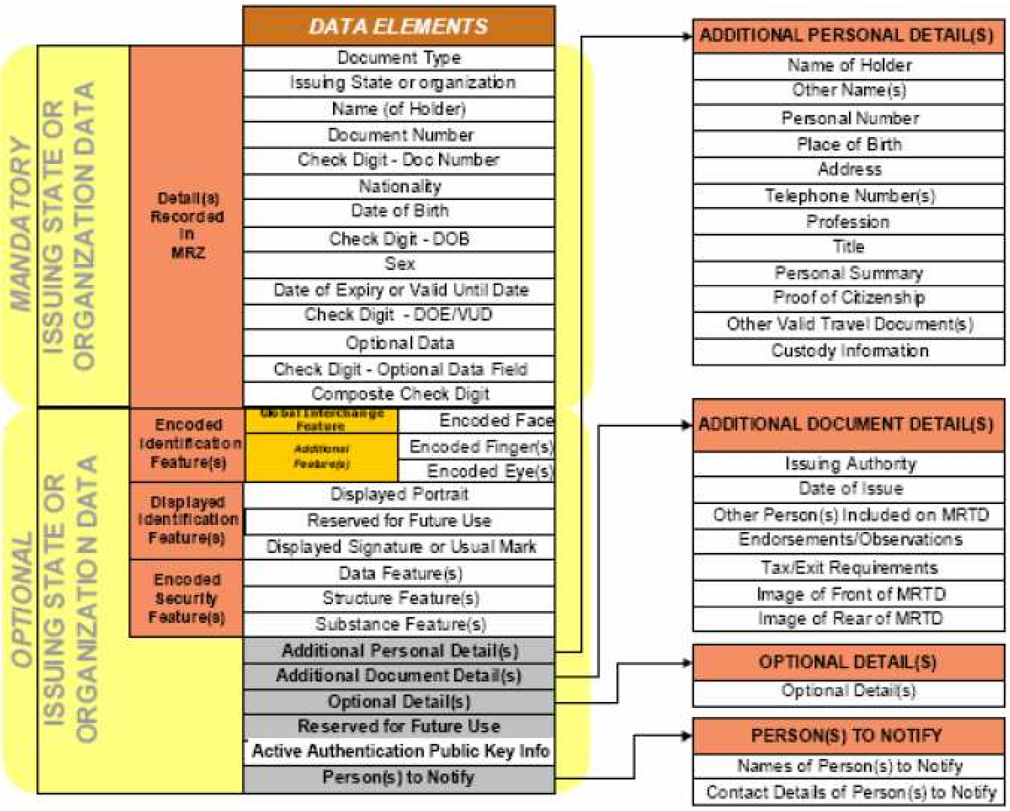


Figure 16 ePassport – Full Data Set

5.7.4. SCOPE – INVOLVED PARTIES

Terminal Authentication requires an EU-wide chain of trust, where the passport issuer (CVCA) concedes permissions through international agreements to foreign Document Verifiers, and ultimately to foreign Inspection Systems, to read sensitive data of its self-issued ePassports.

Below it is graphically represented this chain of trust between two countries and their own elements, where C, DV and IS stands for Certificate, Document Verifier and Inspection System respectively. In this case IS-B2 will be allowed to read sensitive data form Country A ePassports, while IS-B3 won’t.

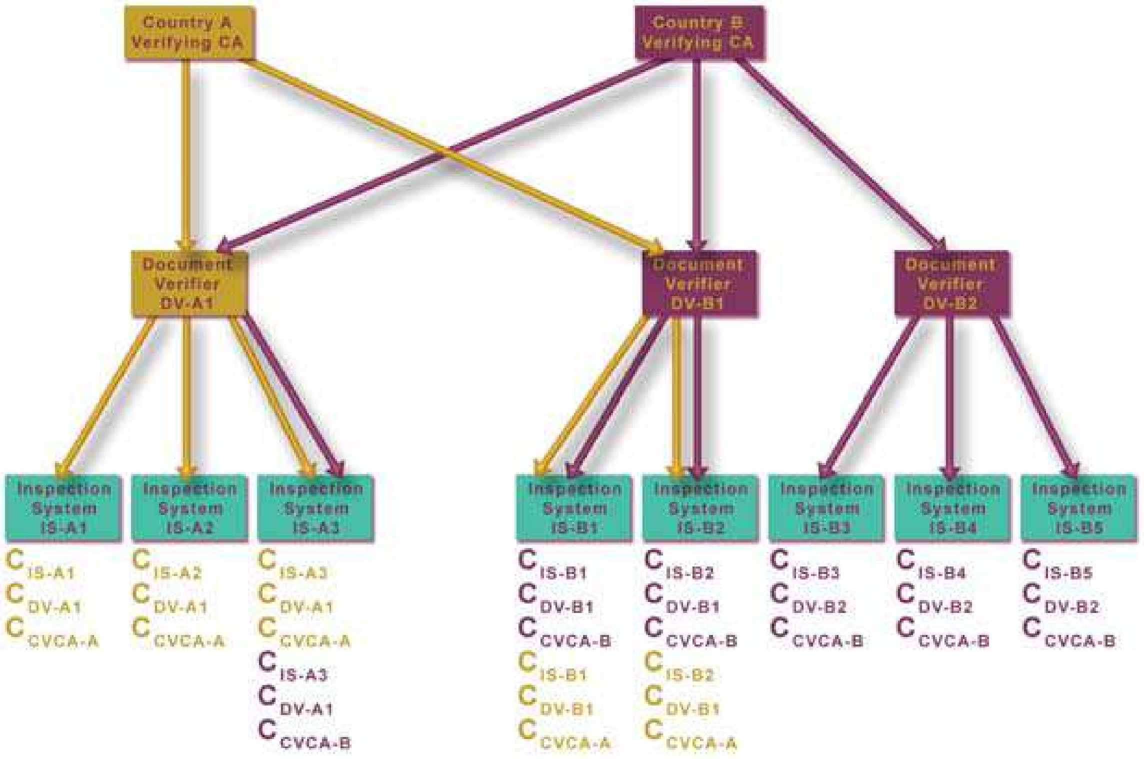

Country A Verifying CA
Country B Verifying CA
Document Verifier DV-A1
Document Verifier DV-B1
Document Verifier DV-B2
Inspection System IS-A1
Inspection System IS-A2
Inspection System IS-A3
Inspection System IS-B1
Inspection System IS-B2
Inspection System IS-B3
Inspection System IS-B4
Inspection System IS-B5
C_{IS-A1} C_{DV-A1} C_{CVCA-A}
C_{IS-A2} C_{DV-A1} C_{CVCA-A}
C_{IS-A3} C_{DV-A1} C_{CVCA-A} C_{IS-A3} C_{DV-A1} C_{CVCA-B}
C_{IS-B1} C_{DV-B1} C_{CVCA-B} C_{IS-B1} C_{DV-B1} C_{CVCA-A}
C_{IS-B2} C_{DV-B1} C_{CVCA-B} C_{IS-B2} C_{DV-B1} C_{CVCA-A}
C_{IS-B3} C_{DV-B2} C_{CVCA-B}
C_{IS-B4} C_{DV-B2} C_{CVCA-B}
C_{IS-B5} C_{DV-B2} C_{CVCA-B}

Figure 17 ePassport - Chain of Trust

5.7.5. Enrolment – Issuance Process

One of the main legal and data security issues, is the need to put in place both high security standards and strict privacy policies for biometric data capture, storage and matching. A system securing privacy for the whole issuing chain from enrolment to personalization, called end-to-end-privacy, is designed around the process. There is also a requirement from EU which stipulates that the operating system on the microprocessor must be security certified. The security certification must be done following the international Common Criteria process designed for evaluating secure IT.

The changes introduced by the second generation ePassport to the document inspection process, set the following ordered checklist of actions, taking into account that some of them could be optional or conditional:

a) Select ePassport application (REQUIRED)

b) Basic Access Control (REQUIRED): If successful, the MRTD chip starts Secure Messaging, and grant access to less-sensitive data.

c) Chip Authentication (REQUIRED): If successful, the MRTD chip restart Secure Messaging, with new shared secret.

d) Passive Authentication (REQUIRED): This authentication process, though initialised here is applied all along the data interchange.

e) Active Authentication (OPTIONAL)

f) Terminal Authentication (REQUIRED only to access sensitive ePassport data): If successful the MRTD chip grants access to sensitive data according the inspection system's access rights.

g) Read and authenticate data: The inspection system reads and verifies by passive authentication the data groups, according to the inspection system’s access rights.

5.7.6. *CONCLUSION*

Introduction of cryptography in communications and terminal authentication are important features in order to protect sensitive information, specially once biometric information has been included among data required to implement this document.

EU-wide “Chain of Trust” infrastructure deployment is a challenge likely to be succesful among national administrative bodies. However, developement of this concept on an international port authority level, though technically feasible, might not be so supportively afforded.

5.8. PROATRANS

5.8.1. *OVERVIEW*

The Port Authority of Barcelona (APB), in its on going efforts to maintain an operational framework for logistics community companies, has set up a project, as known as PROATRANS (Transport Access Restructuring and Regulation Plan), in order to implement a specialised plan which establishes the regulatory framework for the provision of road freight services.

The primary objective of PROATRANS is to adapt the logistics community and, in particular, the land-based container freight sector associated with the Port of Barcelona, to current legislation on competition and the free market.

Within PROATRANS framework and in order to enhance security, APB installed a traffic system management based on the identification of vehicles and drivers situated in different points inside the port. These checkpoints are located in:

1. Access gate to the port, where the vehicles do not stop and vehicle identification is registered through TAG’s antenna reading.

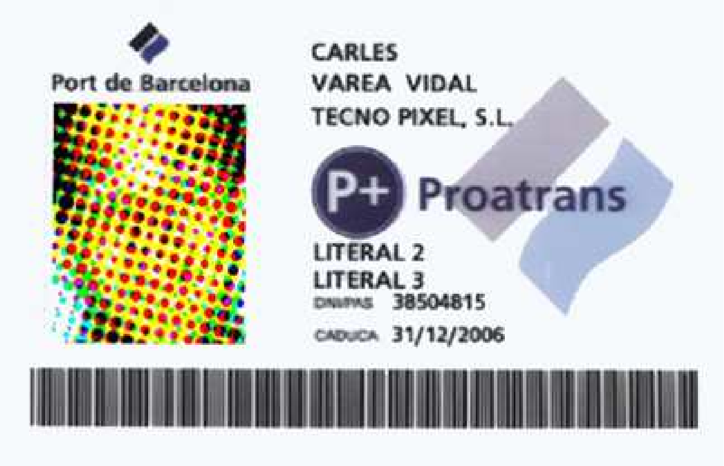
2. Terminals. Driver and vehicle identification is required and compared with the information stored in the port data base.

3. Parking lot. Driver or vehicle identification is required.

5.8.2. *CREDENTIAL AND INFORMATION SPCECIFICATIONS*

Driver identification is checked through PROATRANS card. The following data is available in the card:

- Name and surname of employer.
- Company.
- Character Identification (P, regular operator or E, eventual operators).
- ID number/passport.
- Expiry date.
- Issuing authority.
- Coloured photograph.



Port de Barcelona

CARLES
VAREA VIDAL
TECNO PIXEL, S.L.

P+ Proatrans

LITERAL 2
LITERAL 3
DNI/PAS 38504815
CADUCA 31/12/2006

Figure 18 PROATRANS card sample

None biometric data is stored. The card includes a bar codes and magnetic stripe.

5.8.3. Scope – Involved Parties

The APB created this plan and established itself as the coordinating body for the different agents tasked with carrying it out, whether APB departments and/or sector organisations, for instance:

- Shippers
- Subcontractor carriers
- Transport operators
- Road-freight and multimodal transport companies
- Shipping agents
- Shipping companies
- Forwarding agents
- Customs brokers
- Inland maritime terminals
- Container depots

5.8.4. Enrolment – Issuance Process

Effectiveness of the system is based on PROATRANS card, obtained with a previous registration via FAX or telematic message sent to Portic, which is the e-commerce platform of the Logistic Community of the Port of Barcelona. The card is provided by the APB who is the only one that may dispatch it.

Portic was created to offer the users, agents and bodies operating in the Port of Barcelona e-commerce services among companies, and between administrations and companies. Portic offers the electronic commerce tools necessary for simplifying, speeding up and bringing down the costs of exchanges of documents, invoices and payments associated to the transport of goods in order to increase the competitiveness of the logistics environment of the Barcelona port.

Once received the message registration, data from drivers and vehicles are stored in the APB database. A PROATRANS non-contact smart card is provided to the user, and a message (Portic message) is sent to the terminal who gathers all the transit information that shall be sent to the APB. Cost of the card is paid by the transport company who receives a serial of benefits just for registration, for instance free parking, in addition to save time in facility accesses.

A driver or container truck that does not have a PROATRANS card must go to CISAU (User Support Service Identification Centre) where a temporal card is facilitated by the APB and a Portic message is sent to the facility required. Temporal card is printed just for one access to the facility.

5.8.5. PROATRANS PROCEDURE

In the facility accesses there are barriers where driver and vehicle identification are mandatory. In the checkpoints, number plates are taken by cameras and are compared against the information registered in the database and also compared with the TAG antenna reading. The driver inserts the card into the reader and in the case the present card is valid (information agrees with database info), truck can go inside; otherwise, truck and driver must go to CISAU for identification process.

Outgoing is not controlled, just monitoring for statistics.

Non-fulfilment with PROATRANS instructions will be rule according to article 113 of 27/1992 Law of Spanish Port States and Merchant Marine (Spanish Maritime Authority).

5.8.6. CONCLUSIONS

Thanks to PROATRANS, the port of Barcelona has grown in effectiveness looking for the balance between security measures, through the identification of drivers and trucks in the access to port; and the container movements, speeding up the inbound/outbound traffic in facilities associated to port of Barcelona.

EPAIC should go in this line, increasing the security measures with not losing contact with the port's commercial activity.

6. EPAIC MODEL APPROACHES

EPAIC I study proposes a high level architecture which comprises three main types of subsystems: a central system at European level, a national system that exposes EPAIC services at National Level, and local systems at Port Authority level. These three subsystems shall distribute the functions and data needed for the EPAIC system operation.

EPAIC I assigns to the local port system the responsibilities or functions for applicant data capturing for issuing new cards: EPAIC application document, digital photograph, biometrics, and any other personal data required. The national system and central system shall store, process and transmit the data across the system, depending on the function and data distribution of each generic model presented.

6.1. EPAIC I MODEL REVIEW

The EPAIC I project presents six different models:

1. ***Central model.***

   Data and logic (functionality) is centralised in the central subsystem. National subsystems act as simple gateways to provide access to the services supported by the system and local subsystems and their end-users are connected to the system's services via their respective national systems. Benefits of the central model are the ease of administration and integration of Member States to the system, but the main disadvantages are the high cost of the communication infrastructure, a poor performance of the authentication processes due to the high traffic load within all the system, and the high dependence of a single system node.

2. ***Distributed model.***

   Data and business logic are held at the national level, while the central system provides only interconnection capabilities for the national systems. This model decreases drastically the communication infrastructure costs with the central system and improves the authentication process efficiency, but the administration and maintenance complexity is higher. Thus, complexity of the national level systems increases significantly, having to deal with fully sized systems, one per Member State. This translates into increased costs for hardware and software, biometric infrastructure, etc. In the first EPAIC study, distributed model is not considered suitable due to poor response times estimated.

3. ***Replicated model.***

   Data and logic resides at National as well as at Central level. Again, complexity of the national level systems increases, as well as a complex central system. This replication incurs in very high data storage and bandwidth requirements, like in the distributed model. On the other hand, search is centralised, authentication processes are more efficient, and the replication can serve as a proper security measure against availability threats. This model has been discarded in the study due to the high global data storage requirements, the complexity of system administration and maintenance and very high communication infrastructure requirements to handle voluminous data, as biometrics or images.

4. ***Hybrid model.***

   Data and functions can be stored in the different levels according to the selected configuration. Advantages and disadvantages depend on the configuration applied.

5. ***Mesh model.***

   Data and business logic (functionality) are decentralised at national level. However, some common data (which may vary depending on the selected configuration) are replicated in all the national systems, improving search and consultation processes, but making more difficult updating or adding new data into the system. The selected configuration can vary, from the "minimal" (where only a alphanumerical index is replicated to facilitate searching processes) to the "maximal" (where almost all the data are replicated in all the national systems). Such configurations would result in reduced telecommunication costs at the expense of increasing several system complexities due to data replication. In this model the central system acts as simple gateway. This model has been discarded in EPAIC I arguing the same reasons exposed in the distributed model, which outperforms its sole benefit, the response time.

6. ***Standalone model.***

   Personal data is stored on the card, and at national level for archiving purposes. Authentication process is simple and efficient, requiring just a card reader, and is easy to introduce new Member States to the system. However, the EPAIC I study discards the model due to the total lack of ID card life cycle capabilities.

6.2. CONSIDERATIONS TO CANDIDATE MODELS

The first study proposes two models as candidates for EPAIC system: central and hybrid. However, the selection criteria followed to evaluate each model, the EPAIC I study doesn’t have taken into account some facts that have been considered relevant.

For **both candidate models,** the following aspects have been considered:

- In the definition of the proposed models, a clear separation between identification and access control has not been found. In the present study, this separation is considered a relevant factor to take into account, as each process requires different requirements and roles to be managed. In fact, the stakeholder consultations from EPAIC I showed that Port Authorities will not agree about losing control of the access control management and policies.

- As a consequence of the previous point, a model separated from the control access management processes would require a review of the requirements presented in the first study. This implies that the data required to be handled within the system:

  - Access rights and permissions for each cardholder shall not be mandatory.

  - Transmission of personal data through the system network infrastructure, in case of a decentralised model, shall not be necessary as well.

  - In consequence, heavily sized data as photograph, images or permission documents would not be necessary to be processed in the system network, resulting in a lighter and less demanding set of technical requirements.

- The different approaches in the architecture of the models presented in EPAIC I do not take into account one of the conclusions obtained from the stakeholder consultations, that is, the lack of need for visiting or working in other ports for most of the staff susceptible to need an access card in the port facilities. This fact shows that considering a model with different user roles depending on their mobility between EPAIC system ports is recommended.

- As a consequence of the previous point, the card management and life cycle considered for most of the models in the first study are heavily oriented to centralization, thus incurring in increased costs and technical complexity in the system. However, as only a small percentage of EPAIC users would actually move between more than one port, it shall be more adequate to consider a local approach of the card life cycle management, with interaction and communication capabilities with the similar management systems in the rest of the ports of the EPAIC system when necessary (new applications, revocations and validity information, or identification of those cardholders who should require to other ports).

- EPAIC I studied and considered the different authentication factors typically present in access systems (card authentication, user identity authentication, and passwords or PIN), as well as the different security layer schema to be implemented in ports security. However, these aspects are not reflected in the models approaches described in the first study. The use of one or more authentication factors shall be necessary and useful when defining the security layer or level architecture defined in the Directive 2005/65/EC of 26 October 2005 on enhancing port security.

Regarding the **centralised model**:

- The centralization of the logic and data in a unique, central system for all ports of State Members poses many disadvantages, as stated by the first EPAIC study:

  - High infrastructure costs.
  - High system performance requirements.
  - High dependence of a single critical node.

- Additionally to this, the present study raises new issues regarding to this centralised model, specially the legal aspects regarding personal data transmission which could be required in all processes, between State Members, due to the different normative and legislation applied to them.

- Finally, the current project approach of designing a national level EPAIC system, for a further European wide approach in the future based on the national system solution adopted, seems to be incompatible with, or hard to migrate to a centralised model.

Regarding the **hybrid model**:

- It is a flexible approach, but an improvement in the authentication process shall be considered, confining these use case events to the local systems. This approach would have the same advantages as the standalone model in the first study (light authentication process and easy new Member State incorporation), with a common, non-isolated card life cycle capabilities. This enhanced architecture would be similar to a PKI model, which is widely used in other card control access systems.

6.3. Considerations About Biometrics

One of the points EPAIC was greatly concerned about was the research of the most suitable biometrics to be used within this project, in case some was required. In an information technology environment, biometrics refers to technologies that measure and analyse human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Thus they are useful to prove that someone is who he says he is.

Accuracy, when authenticating individuals depends on the factors we count on. The three existing factors are defined as “something you know”, “something you have” and “something you are” meaning anyone could prove his identity by being the only one who knows a secret (i.e. a password), having something he only could have (i.e. token or personal card) or presenting a biometry unique to that individual (iris, fingerprint and so on). First two factors are usually easier to fool than biometrics. Anyway, best practice when protecting access to critical areas, is the use of two or even the three factors, thus enhancing trust in a correct authentication of an individual.

EPAIC I analyses mainly 4 biometric techniques that are the most commonly deployed:

- Fingerprint: Fingerprints are made up of ridge endings and bifurcations exhibited by friction ridges and other detailed characteristics called minutiae. It is the distinctiveness of these minutiae that gives each individual a unique fingerprint. An individual places his finger on a device that reads the details of the fingerprint and compares this to a reference file.

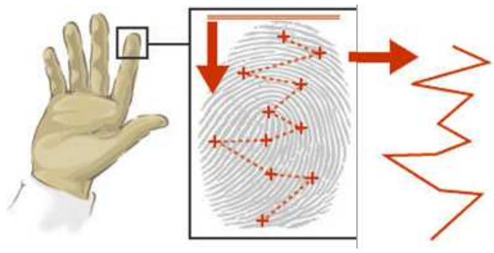


Figure 19 Fingerprint Minutiae Processing

- Iris Recognition: The iris is the coloured portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colours, rings, coronas and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the template of the user. Sampling the iris offers more coordinates than any other type of biometric. Mathematically, this means it has a higher accuracy potential than any other type of biometric.

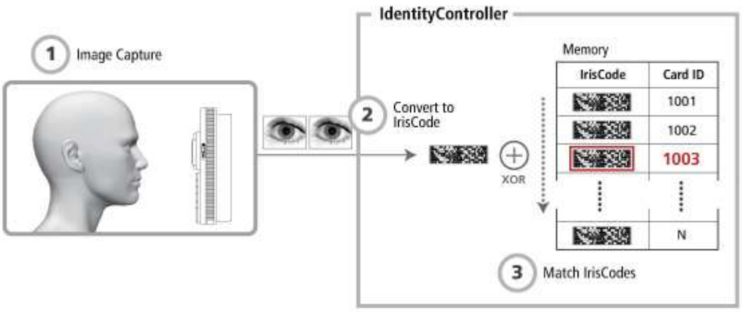


Figure 20 Iris Scan Processing

- Hand Geometry: The shape of a person's hand (the length and width of the hand and fingers) defines hand geometry. This trait differs significantly between people and is widely used for applications in physical access to verify identity. A person places her hand on a device that has grooves for each finger. The system compares the geometry of each finger, and the hand as a whole against the known reference template to verify that person's identity.

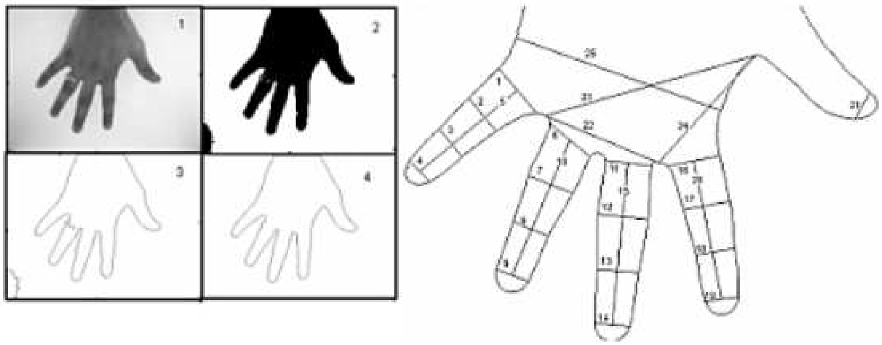


Figure 21 Hand Geometry Processing

- Face/Facial Scan: A system that scans a person's face takes many attributes and characteristics into account. People have different bone structures, nose ridges, eye widths, forehead sizes, and chin shapes. These are all captured during a facial scan and compared to an earlier captured scan held within a reference record. Face recognition is characterised by its theoretical potential to operate at a distance, with or without user cooperation.

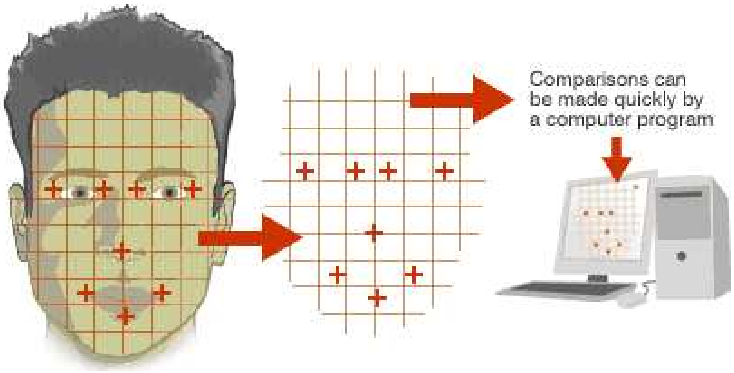


Figure 22 Facial Scan Processing

The four values that were used in EPAIC I study as usability and performance indicators were:

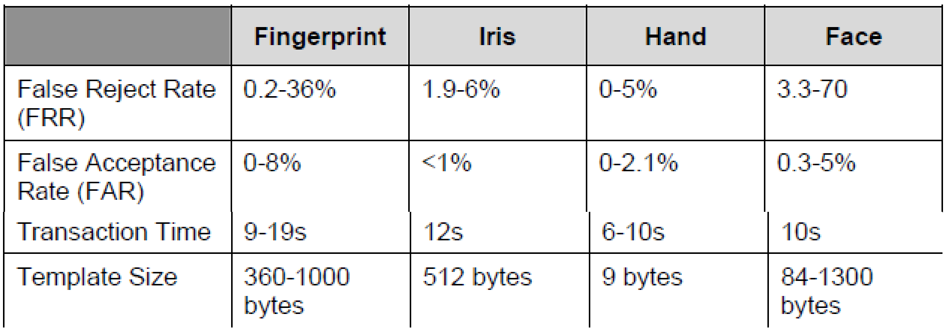
- False Reject Rate (FRR): is the proportion of genuine verification transactions incorrectly denied. It is displayed as a percentage over total transactions.

- False Acceptance Rate (FAR): is the proportion of zero-effort non-genuine transactions incorrectly accepted. It is displayed as a percentage over total transactions.

- Transaction Time: time elapsed to complete a biometric measurement, process the match function and return the result. It is displayed as seconds.

- Template Size: storage volume needed to record one single biometric template. It is displayed as bytes.

The table below has been taken from the EPAIC I analysis and illustrates a comparison between the main biometrics technologies, based on the four indicators aforementioned.



	Fingerprint	Iris	Hand	Face
False Reject Rate (FRR)	0.2-36%	1.9-6%	0-5%	3.3-70
False Acceptance Rate (FAR)	0-8%	<1%	0-2.1%	0.3-5%
Transaction Time	9-19s	12s	6-10s	10s
Template Size	360-1000 bytes	512 bytes	9 bytes	84-1300 bytes

Figure 23 Biometric Technologies Comparative
Source: *United States General Accounting Office Technology/Assessment*

EPAIC I analysis also shows that Hand recognition leads this assessment with the lowest FRR, FAR (except for the Iris FAR which is still lower) and transaction time ranges. The template size for Hand biometry is fairly smaller than any other one. Besides, Iris recognition technology is also well positioned, in spite of having one of the highest transaction times.

Nevertheless, EPAIC I already points out the main issue while using Hand recognition. That is, this technology has good accuracy while making a 1 to 1 match, but it is no so trustworthy when comparing 1 to N templates. Briefly, it should be really useful when verifying someone identity (matching his biometric measure just against his recorded template) but not as useful when trying to identify someone out of the blue.

Regarding biometric encryption, EPAIC I presents two alternative architectures. Both of them rely on a ciphered template inserted into the card which could be transmitted over the contactless interface. Private Key management is the difference. This key needed to decipher the template could be stored in the network (centrally or distributed over relevant facilities) and retrieved using the individual or card identifier. Otherwise, Private Key will stay also stored in the card (standalone architecture) and will only leave through the contact interface for security reasons in order to avoid eavesdropping.

Finally, EPAIC I raises questions to be further studied related to the likely slowdown in access control on peak times, intrusiveness and intensive testing. Due to the alleged robustness the study tends to consider Iris recognition as the better solution, but it opts for excluding any biometric field from the card except for the printed photograph and signature. Thus they will only be useful for a manual and non-automated verification.

6.3.1. ADDITIONAL ENQUIRIES

ESRIF [7] refers to biometrics technology pointing out that there are mainly two classes of attacks, by which an attacker can breach the security of a biometric system or fool the system to gain access to the biometric data of a legitimate user:

- *External attacks*: the attacker tries to fool the acquisition device by showing a fake image (like a copy of a fingerprint of a legitimate user). Such attacks can be prevented with appropriate anti spoofing mechanisms.

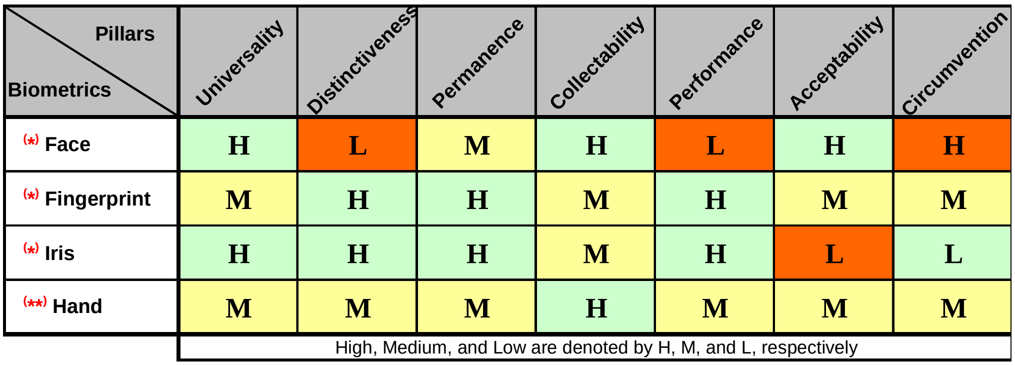
- *Internal attacks*: the attacker is able to retrieve the template of a genuine user that has already enrolled onto the system. This can be done by spoofing the system while the legitimate user uses the system or by hacking the database where the biometric data are stored or simply by access not being adequately protected or restricted. The attacker then injects the template directly into the matching algorithm. This solution is more complex to implement as the attacker needs to interfere with components within the system perimeter.

ESRIF also emphasises that due to such threats, biometric data of citizens must be protected to a high level. This issue is addressed by the Personal Data Protection legislation but further measures or standards for secure deployment are required. It focuses on issues related to unauthorised use, abuse or misuse of data.

When trying to envision an infrastructure deployment throughout several facilities in a widespread scale, technical issues are likely to arise. One of the concerns could be the need of agreement with regard to data format, especially when speaking about biometrics. ESRIF as well as other studies (see Seafarer' Identity Document for further discussion) complaint about the relatively immature situation of the market in this field and the common adoption of proprietary solutions instead of standards already developed. The Joint Technical Committee on Information Technology (ISO/IEC JTC 1/SC 37) is the main body in charge of this standardization, having issued the ISO 19794 family. The 19794 series Part2, Part5, Part6 and Part10 cope with data standards for fingerprint minutiae, face image, iris image and hand geometry respectively.

As ESRIF states, although there is still a long way to go towards achieving interoperability in terms of technical specifications, it is important to note that these standards exist and they should be promoted and developed.

The **European technical report** [8] developed for the European Parliament was focused on three of the technologies aforementioned (Face, Fingerprint and Iris) and a final fourth that was DNA. There also included references to Hand Geometry technology along the report. This report introduced a comparison based on the concept of the "Seven Pillars of Biometric Wisdom" that provides a framework with which to evaluate biometric technologies. The colour scheme (green for positive, red for negative) allows an immediate impression of the areas of strength and weakness for each technology, showing overall better results for Iris and Fingerprint. Below there is a definition about each pillar meaning.



Pillars / Biometrics	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
(*) Face	H	L	M	H	L	H	H
(*) Fingerprint	M	H	H	M	H	M	M
(*) Iris	H	H	H	M	H	L	L
(**) Hand	M	M	M	H	M	M	M

High, Medium, and Low are denoted by H, M, and L, respectively

Figure 24 Selected Technologies Comparison Against the Seven Pillars
Source (*): *Biometrics at the Frontiers: Assessing the Impact on Society (2005)*
Source (**): *The Challenge of Biometrics (Laurence Edge)*

- *Universality*: All human beings are endowed with the same physical characteristics - such as fingers, iris, face, DNA – which can be used for identification.

- *Distinctiveness*: For each person these characteristics are unique, and thus constitute a distinguishing feature.

- *Permanence*: These characteristics remain largely unchanged throughout a person's life.

- *Collectability*: A person's unique physical characteristics need to be collected in a reasonably easy fashion for quick identification.

- *Performance*: The degree of accuracy of identification must be quite high before the system can be operational.

- *Acceptability*: Applications will not be successful if the public offers strong and continuous resistance to biometrics.

- *Circumvention*: In order to provide added security, a system needs to be harder to circumvent than existing identity management systems.

This report also shows a meaningful biometrics market share graph from 2004, were Fingerprint is undoubtedly the best positioned (48%) far above all the others technologies. That trend is corroborated according to a current survey from 2009 on the same matter, were the share is still bigger for Fingerprint technology (66,7%), taking into consideration both Fingerprint and AFIS systems. Face recognition is the second one, followed nowadays by Iris recognition and lastly Hand Geometry.

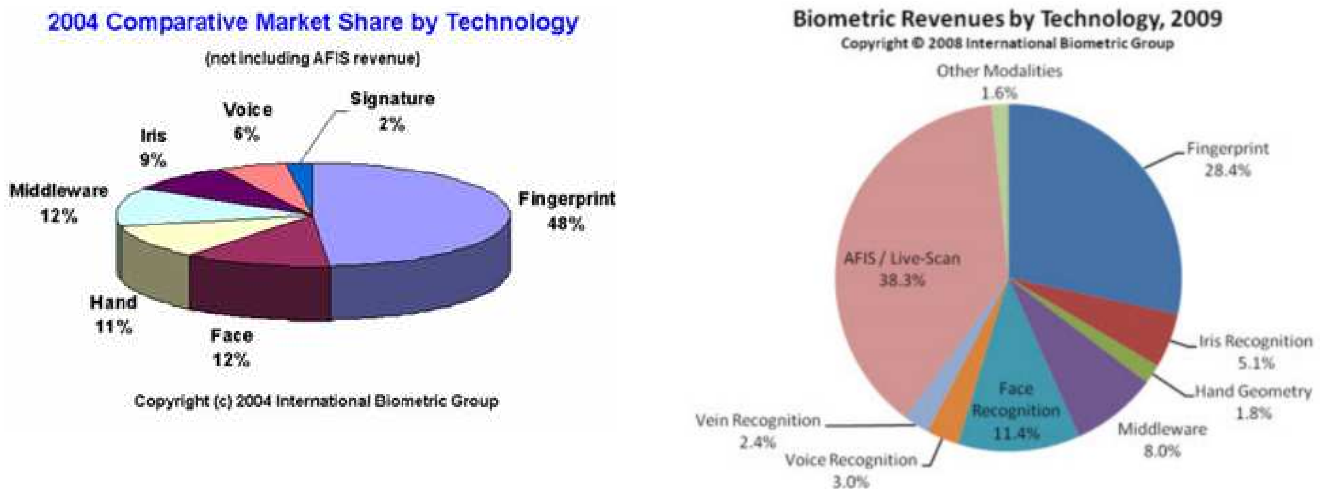


Figure 25 Biometrics Market Share Evolution (2004 & 2009)

All through the analysis, several advantages and disadvantages inherently attached to each technology have been found. Gathering them herein could help, on the one hand to better understand the previous evaluation against the seven pillars, and on the other hand to find the technology that fits the best with requirements that could further arise.

HAND GEOMETRY	
ADVANTAGES	**DISADVANTAGES**
❖ Ease of use. ❖ Very good performance in 1 to 1 match (verification) ❖ Small template size. ❖ Relatively simple and cost effective setup. ❖ Generates less privacy concerns. ❖ Readers tend to be durable and operate in hostile environments.	❖ Hand changes and severe injuries can vary the geometry. ❖ Accuracy limits its application to identity verification rather than identification. ❖ Costs could be higher than other technologies. ❖ Readers are unlikely to be portable. ❖ Hygiene concerns, from multiple users touching the reader. ❖ Few suppliers of these technologies available. ❖ Readers require a large amount of physical space.
COMMERCIAL AND GOVERNMENT SECTORS EXAMPLES OF USE	❖ Alfapass along with Fingerprint biometric. ❖ XSKey PortKey. ❖ RHIDES. ❖ US Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) ❖ Several airports as stated in the technical report Biometrics at the Frontiers: Assessing the Impact on Society (2005)

FINGERPRINTS	
ADVANTAGES	DISADVANTAGES
Extensive experience with fingerprint technology. Good performance. Costs are lower than most of the other technologies. Portable reader devices can be used by security personnel on the field. Multiplicity of fingers that can be engaged.	Estimated 5% of people are not able to enrol. Lack of interoperability in an open commercial context. Susceptible to environmental changes (e.g. if an individual performs intensive manual work over a sustained period, fingerprints can easily become worn and difficult to read) Considerable template size. Hygiene concerns and dirt interference, from multiple users touching the reader.
COMMERCIAL AND GOVERNMENT SECTORS EXAMPLES OF USE	Alfapass along with Hand Geometry biometric. TWIC. Seafarers' Identity Document (SID) European ePassport. Spanish identity card (eDNI)
IRIS	
ADVANTAGES	DISADVANTAGES
Highly unique even for twins. Iris is a characteristic which does not alter dramatically over the course of a lifetime. Protected internal organ. Less prone to injury. Mature enough to be used commercially in high-security applications. Excellent performance results in both identification and verification modes. An iris scan can be performed from about 10cm to a few meters away, avoiding contact with any surface.	Produce a sense of discomfort as users are not certain as to where to focus when providing a sample. Relatively higher failure-to-enrol rate. Controlled light exposure. Potentially affected by occlusion due to eyelids and eyelashes. It tends to have the highest costs. Cannot be verified by a human.
COMMERCIAL AND GOVERNMENT SECTORS EXAMPLES OF USE	A number of US and Canadian airports (NEXUS program) Several Canadian airports (CANPASS Air program)
FACE	
ADVANTAGES	DISADVANTAGES
Considered less intrusive than all other technologies. Theoretical potential to operate at a distance, with or without user cooperation. Second position in market share. Commonly available sensors (cameras) Easy for humans to verify results.	Still very weak technically in terms of performance and accuracy. Faces change over time. Controlled light exposure. Sensitive to changes in expression or pose. Face can be obstructed by hair, glasses, hats, etc.
COMMERCIAL AND GOVERNMENT SECTORS EXAMPLES OF USE	Australian automated border processing system (SmartGate) German Federal Police system for fully automated border controls at Frankfurt.

Figure 26 Advantages and Disadvantages of Biometric Technologies

Sources: Biometrics at the Frontiers: Assessing the Impact on Society (2005); ESRIF Final Report 2009; EPAIC I Final Report; NSTC – U.S. National Science and Technology Council, Subcommittee on Biometrics and Identity Management, Foundation Documents; and Biometrics Task Force Biometric Standards Development Status (Update January - March 2009)

6.3.2. CONCLUSION

Biometrics should just be used when or where there is a real need of strong authentication. Thus, collection and use of biometrics should be restricted to a limited set of individuals and places reducing the infrastructure investment. It would also help to a better acceptance of the EPAIC solution proposals among users and stakeholders.

Regarding biometric technologies, Hand Geometry should be foreseen as a good option in case verification is the only matter to care about. Nevertheless, if identification of individuals was a requirement, Fingerprint should be more desirable. Both of them could allow integration with existing systems located in port facilities where those technologies have already been deployed and tested.

Standards shall be taken into account when designing the infrastructure in order to allow interoperability of biometric data, whatever provider or system has to deal with the templates. Otherwise, the use of proprietary solutions will compel to work with a limited set of providers whose systems are able to interoperate.

Security on biometrics is a great concern all over the EU, thus they need strong protection. Security measures such as data ciphering, communications over secured interfaces, disclosure prevention or use of privacy enhancement technologies should be pondered, and whenever possible settled as a requirement. Additionally, collected biometric data should be used only for the purpose technically and legally associated with the data at the enrolment stage.

7. GATHERING INFORMATION

Once analysed the state of the art of different card systems and reviewed the architectures from EPAIC I, stakeholders participation will be crucial in order to obtain their necessities to be included in the future EPAIC system.

In this section, it has been shown the work taken into account.

7.1. UNDERSTANDING THE USERS

The participation of users is fundamental for the success of EPAIC II study because they are the best positioned to identify the needs, gaps, constraints and improvements of the current Access Identification System because of their job.

Their intervention is also decisive in order to know the deployed technology in the accesses to port. There will be valuable information taken into account for cost benefit analysis and migration cost.

7.1.1. USERS IDENTIFICATION

In order to reach the objectives of EPAIC II study, several stakeholders have been identified, as it was mentioned in section 4.2 These stakeholders answer to the following communities:

- Ports,
- Transport companies,
- Workers associations,
- Maritime international organisations,
- Terminal owners,
- And ship-suppliers.

7.1.2. CONTACTING USERS

In agreement with DG-MOVE, organisations were contacted via e-mail, phone, interviews and occasional seminars, meetings, conferences etc. Main ideas of the EPAIC II study, objectives, and descriptions were presented in order to receive comments, suggestions and recommendations in the EPAIC II framework beyond to require their participation in the questionnaire fulfilment.

With the purpose of gathering the highest number of answers, the European Commission acted as a multiplier to contact and motivate the users. In this sense, The EC prepared a support letter (or letter of recommendation) for Isdefe activities in EPAIC II project. Furthermore, The EC facilitated access to some stakeholder groups (as FEPORT, Federation of European Private Port Operators) and existing working groups (as SAGMAS,)

EPAIC II requested participation to the following experts and end users:

ORGANISATION
Port of Turku (Finland)
Port of Göteborg (Sweden)
Port of Stockholm (Sweden)
Port of Helsinki (Finland)
Port of Fredericia (Denmark)
Port of Mälmo (Sweden)
Port of Riga (Latvia)
Port or Rauma (Finland)
Port of Århus (Denmark)
Port of Ystad (Sweden)
Port of Szczezin (Poland)
Port of Swinoujscie (Poland)
Port Autonomme Du Havre (France)
Port of Hamburg (Germany)
Port of Bremen (Germany)
Port of Rotterdam (The Netherlands)
Port of Antwerp (Belgium)
Port of Liege (Belgium)
Port of Felixtowe (United Kingdom)
Port of Dover (United Kingdom)
Port of Gijon (Spain)
Port of Vigo (Spain)
Port of Dublin (Ireland)
Port of Bristol (UK)
Port of Nantes – Saint Nazaire (France)
Port of Algeciras Bay (Spain)
Port of Barcelona (Spain)
Port of Valencia (Spain)
Port of Alicante (Spain)
Port of Tarragona (Spain)
Port Autonome de Marseille (France)
Capitaneria di Porto di Genova (Italy)
Port of Livorno (Italy)
Port of Bari (Italia)
Port of Patras (Greece)
Port of Thesaloniki (Greece)
Port of Seville (Spain)
Puertos del Estado (Spain)
ESPO – European Sea Ports Organisation

ORGANISATION
Ocean – European Ship Suppliers Organisation
IRU (International Road Transport Union)
BGL (Bundesverband Güterkraftverkehr Logistik und Entsorgung e.V.)
FEBETRA (Fédération Royale Belge des Transporteurs et des Prestataires de Services Logistiques)
RHA (Road Haulage Association)
VVWL (Verband Verkrehrswirtschaft und Logistik Nordrhein-Westfalen e.V.)
BPO (Baltic Ports Organisation)
FEPORT (Federation of European private Port operators)
SAGMaS (Stakeholder Advisory Group on Maritime Security)

Figure 27 Contact list

7.1.3. USERS CLASSIFICATIONS

Once identified the users and contacted them, users have been classificated in line with the following groups:

- Ports, which includes end users, experts and entities in charge of the security measures in port.
- Terminal Owner. Due to some ports around Europe are open ports with public roads crossing the port areas (for instance port of Antwerp in Belgium); it established this community because they are in charge of the security measures to be implemented in their facilities.
- Other, which embraces those end users and experts included at international associations, road hauliers, shipping companies, ship owners…

These groups are represented from two points of view: on the one hand ports and terminals who establish the control and monitoring through security measures and, on the other hand, users that have to use them. For this reason it is important to understand their work environments and their daily problems in order to obtain a catalogue of requirements to all communities involved.

7.2. UNDERSTANDING THE USER NEEDS

The objectives of EPAIC II are twofold: to objectively analyse the information from an-industry independent point of view, and to propose the development of a prototype of a port access identification card system based on end-users requirements, the variety of specific needs depending on ISPS code requirements, and other local factors as day-to-day work, information flow, owner of the data, etc.

In order to achieve the second objective, a questionnaire was realised to have a deep knowledge of the current systems around Europe. It is important to know what the worries of the user are, what they need and what they expect.

7.2.1. QUESTIONNAIRE STRUCTURE

The questionnaires will primarily cover aspects related to the port access requirements, existing infrastructures and deployed technologies, possible EPAIC system user types, etc. One of the main goals is to model the different port typologies according to security requirements. The responses will be gathered and their information extracted to be part of the output for the next phase.

The questionnaire is composed of several sections (See Annex B), and each one may be address to different users. The structure is as follows:

1. First, a general section including questions about the systems already in use and the perception of the stakeholders about a unified port access card system.

   General questions: does the stakeholder use a similar card access system? What are its overall characteristics?

   Display and verification. How are the cards displayed and verified, along with the identity of holder?

   Economic part about the cost of the current system, and the benefits or possible drawbacks of a migration to a unified solution as that of EPAIC.

2. Secondly, technical questions about how the system used by the stakeholder is actually employed.

   Credential and information. How is the card designed? What kind of information is stored in it? Which are the security measures implemented?

   Card lifecycle management. How can someone enrol? Are there background checks? How is data protected? Are cards taken care of after their holder ceases to need them?

There is more information in Annex B containing the concrete questionnaire.

7.3. RESPONSE RATES

The overall response rate was lower than expected. There are several reasons to this fact:

- There might be a reluctance to respond to any kind of questionnaire (and survey) and apply resources without a real incentive.
- Sensitivity regarding confidentiality, despite the inclusion in the questionnaire of a note explaining that data were going to be used in an aggregate manner and a disclaimer, may have been a demotivating factor.
- Requested figures (specially those related to costs) from some Stakeholders were not readily available; often the data (if recorded at all) is distributed among several departments and there is no standard procedure to collect the information. This obviously increases the effort needed to give a comprehensive answer, thereby lowering the response rate.
- Obtaining direct e-mail address proved difficult. An effort was made by Isdefe to develop an address list to overcome the lack of availability of direct points of contact, at an additional cost in both time and budget.

7.4. REQUIREMENTS EMANATING FROM PORTS

Technical Requirement Analysis.

The following section analyses the results of the questionnaires and the port requirement tendencies. Based on this analysis, the technical requirement for a common access control system approach are set, based on a start point of minimal cost migration and operational impact criteria, and from there, remarking which security aspects shall be improved, proposing several possible options, and the technical requirements of each of them, to achieve a proper security level. These different options shall be further discussed to find the most suitable one to maintain the security level required minimizing costs and impact as much as possible.

Requirements set for the possible EPAIC proposed approaches are noted with:

- ***"Requirement"***

7.4.1. General Requirements

7.4.1.1. Solo And Multiple Access Control System Approach

There is not a clear tendency on how many access control systems are operating simultaneously in the ports. However, in most cases there is a main system, supported or complemented by secondary systems, which always differ from the main control access system in, at least, two different criteria:

- Control access system ownership and range: when there is a main system owned and managed by the port authority, a common case is to find secondary access control systems owned by private companies operating inside port facilities (terminal operators, etc.), not replacing but adding a security layer to the main access control system for some specific areas. In some cases, port authorities consider the secondary access control system secure enough to be used instead of the main access control system, but the most common scenario is a main system with freedom to deploy private control access system for those private operated port facilities which may require extra security, or those specific critical facilities and infrastructures the ports may consider (authority and port officer buildings, dangerous cargo terminals, etc.). In conclusion, the tendency in this case is the use of a main system with optional secondary systems deployed in specific areas, due to the extra security measures required by ports or operating companies.

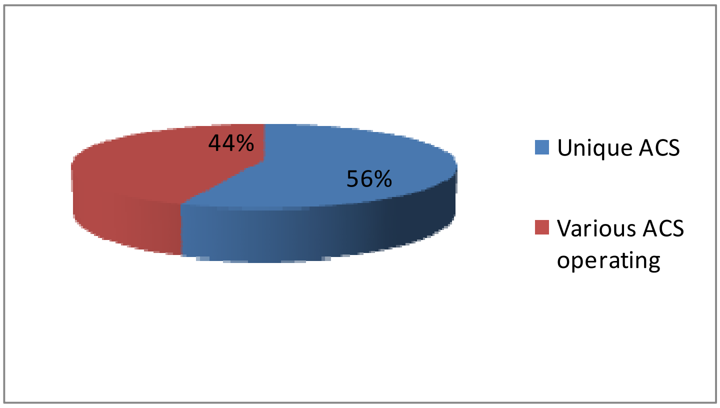


Figure 28 Unique ACS vs. various ACS operating at port

- Control access system technology: when several access control systems are operating simultaneously and in the same areas (same gates) or managed by the same entity, is a rare case that these system are based on the same technology. The most common scenario is that one where the security level is enhanced by using several different technologies together. For example, a control access system based on cards can be running together with a license plate recognition control access system for vehicles and cargo trucks (a very frequent case in the ports consulted), a PIN numerical code control access system, etc.

The principal point to be remarked is that in most cases, when cards access systems are used, the tendency is to have only one common main card system deployed, and in case that more than one card is used, these will be secondary/other purpose card systems, with a different scope (guest card system for one-time-pass visitors, specific private or restricted area cards, private companies cards, etc).

- ***A main card control access system is preferred, but compatibility with additional security layers provided by secondary card control access systems may be desirable.***

Other remarkable aspect is that any card access system deployed will be required to run together with other type of control access mechanisms and technologies. So, any approach to be proposed will have to be compatible and adaptable to/with other control access systems of different nature, especially with license plate recognition systems and visual verification systems.

- ***Any approach developed should offer compatibility with other, non card based control access systems, such as license plate recognition.***

7.4.1.2. Access Control System Scope: Areas To Be Controlled

There is not a clear tendency of which areas should control access system cover, but near the 48% of ports use their systems to control access to both port entrance and specific port facilities which require access control. Due to this divergence in the port requirements in this subject, the proposed approaches shall be versatile enough to be deployable both in a port wide scenario and in specific port facilities.

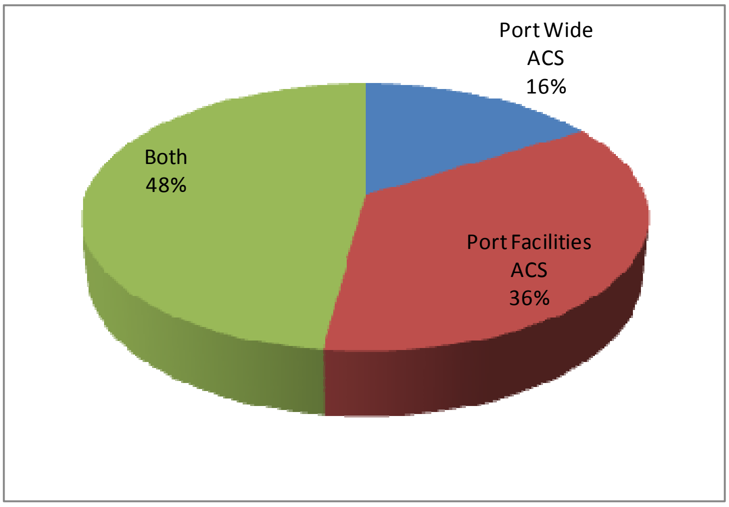


Figure 29 ACS coverage

- ***Any approach developed will permit to implement the card control access system in a port wide approach, specific port facilities approach, or both.***

7.4.1.3. User Roles

Most roles defined in the questionnaire match with the port user role requirements, as it is seen in the results. Seafarers are the role less considered in the port access control systems.

- ***Users shall include:***
  - **Port authority staff.**
  - **Other port workers.**

- **Workers form private companies operating in the port.**
- **Visitors or short-term temporary workers.**
- **Seafarers should be further discussed.**

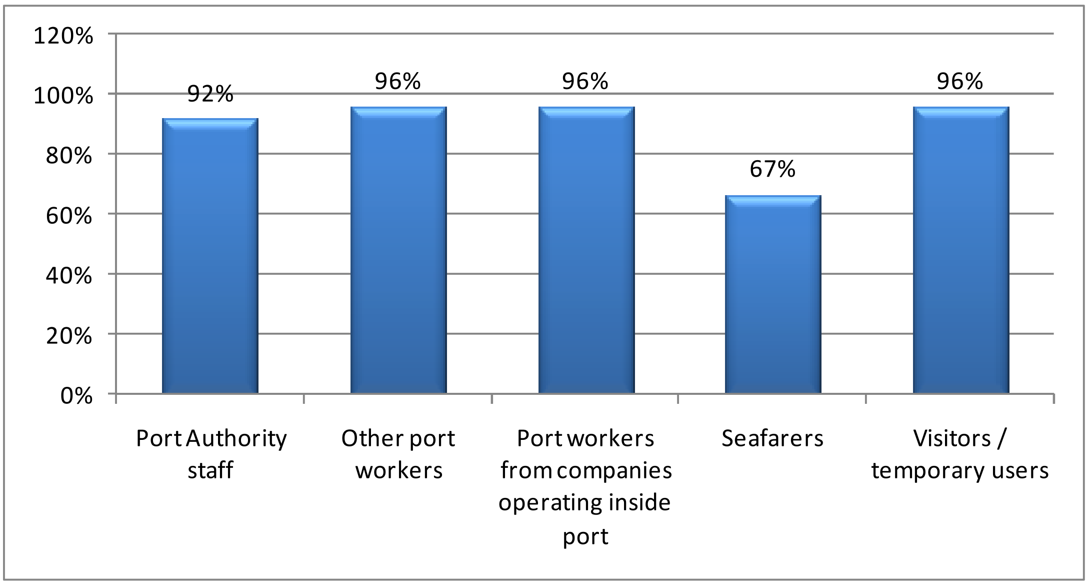


Figure 30 ACS users

- ***People living in the port are rarely applicable as a card user, as most ports do not have permanent residents in the areas under the reach of the control access system.***

Visitors or short term temporary workers tends to be considered as the same type of user. As security measures differ from these kind of user from the rest (it is commonly required that they are escorted, expiry time is much shorter, cards use to be dumb cards which can be instantly issued and quickly discarded, etc.), they are often dependant of secondary card control access system, for temporary/guest/visitor cards.

- ***The proposed card control access systems will have different requirements for one time users or visitors. For these users, cards must be issued almost instantly and may not require electronic authentication techniques or persistent holder data registration/storing, as other security measures can be applied instead (commonly, users require permanent port security escort when accessing restricted areas, or visual identification checks are performed). The proposed approaches shall be able to adapt to this special card lifecycle requirements for these kind of users, or offer a secondary card control access system for this purposes.***

Holder roles defined vary from one port to another, but the most remarkable points found are these:

- In most cases, temporary/guest/visitor card holders are clearly identified and differenced from persistent/regular users.
- In most cases, port staff and private companies' staff are separately considered as different holder types.
- Same happens between regular workers and port authority or port officer staff.
- In various ports truck drivers are defined as a separate holder type.

- Only a few ports make a further detailed division between holder types.

Based on the previous facts, the following requirements regarding card holder roles have been identified:

- ***Regular or persistent users shall be clearly distinguished from temporary short term or visitor holders.***
- ***Same is recommended when distinguishing between staff from the different companies operating in the port and the port staff itself. This classification will provide good compatibility for ports requiring different access rights for workers based on the firm they work for.***
- ***A holder role for security, port authority personnel or officers is desirable; as these users may need special access right requirements (restricted area access, etc.).***
- ***A holder role for cargo transportation workers (truckers) should be further discussed, as they can be, in general terms, considered as a generic port worker. However, in some ports this kind of holders are the group using control access systems more often, and trans-European port access needs could be expected from them (or at least access needs to several ports in the same corridor or area). This, with the fact that a few ports have an actual holder role applied for truckers and transportation workers, makes necessary to seriously consider the inclusion of a separate holder role for this user type.***

7.4.1.4. Access Control System Management Control And Ownership

There is a clear tendency in this subject: port and port authorities are the entities responsible of the control access system. In the case of the card control access systems, this includes card enrolment, production, issuing and renewal and termination management processes. The systems and infrastructures of the control access management system are property of ports and are administrated by port authorised personnel.

The next common approach is to outsource the control access system deployment, management and lifecycle processes to a trusted and contracted third party specialised in this matter (for example, Secure Logistics), or furthermore, to adopt an existing control access solution (as Alfapass system). The main benefit of these outsourced option is that a more secure and modern technology seems to be applied to perform the control access system procedures. Alfapass and Secure Logistic outsourced systems are the only one in the consulted ports including a user authentication factor through biometrics, while any of the port owned control access system included any user authentication mechanism other than manual visual verification checks of cardholders.

Finally, a few ports delegates completely all the existing control access systems to the private companies operating in the port facilities/terminals, and in those cases any further details are given. This approach shall not be regarded as a possible option for an EPAIC system, as implies a poor control of the actual security level implemented in the ports, and makes harder the compatibility between port control access systems, because of their inherited divergence.

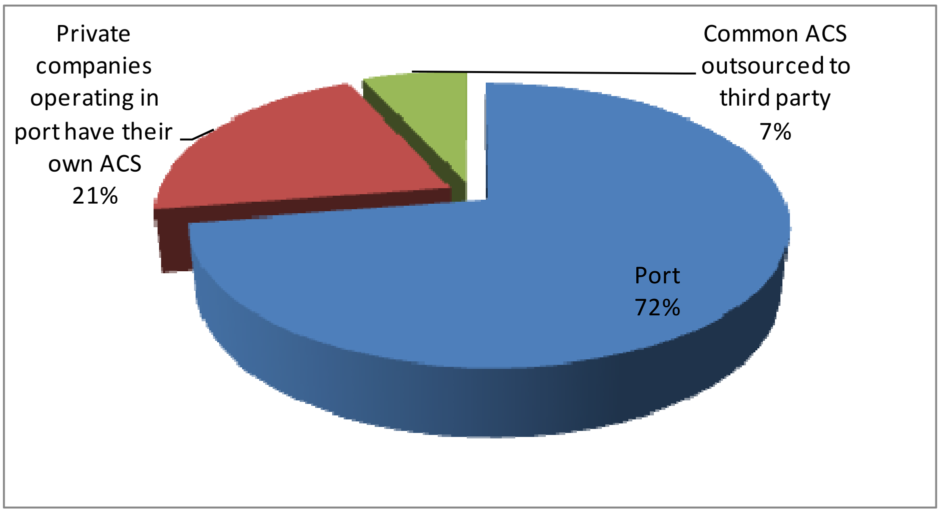


Figure 31 ACS management

When questioning which approach would be more adequate for EPAIC proposals, the following facts must be taken into account:

- In most cases, the systems are owned and managed by the ports.
- In all the cases, these port-owned systems are not as secure as the outsourced ones. Any of the systems owned and managed by the ports uses biometric authentication procedures, digital signature of contents, or similar technical improvements available.
- Migration costs and issues can be a true problem if an outsourced, or non port-managed system is proposed, because most of the ports consulted do not use this kind of approach.
- Technological investments and costs could be high if additional user authentication procedures are implemented in the proposed system, as any of the port-managed systems count with this technology.
- In all port-managed systems, no automated/electronic user authentication can be performed. Instead of this, manual visual verification checks are performed.
- The previous point implies that any control access point would require to be manned, which shall require an additional cost and probably operative time delay compared to an automated unattended system.
- Outsourced and non port-managed solutions could be perceived as a loss of the actual access control from the port point of view.

Based on these facts, two different approaches, with different requirements, shall be considered:

- ***Port-managed and port-owned system: would suppose a less costly and easier migration, and would keep the system management under port control. This seems to be the most suitable option.***
- ***Outsourced system: would provide an opportunity to delegate the system responsibility and procedures to others, and to adopt better technical solutions, as they are provided by a specialised third party dedicated to security and control access solutions. It would be, as well, compatible with ports where control access are privately owned and managed by the companies operating in port facilities. This approach is likely to be less compatible with the***

present situation, but may be a deep change of the control access approaches could be considered as an interesting option for the ports.

The aspects regarding user authentication issues obtained from the previous analysis will be studied in point 2.3 (Biometrics) of this document.

7.4.1.5. ACCESS RIGHTS MANAGEMENT

Almost all of the ports consulted include the access right management as a part of the control access system. This is, card lifecycle, stored data, and management system include the access rights of the cardholder, and the control and use or modification of them.

However, EPAIC I study clearly concluded that ports shall not agree to lose control of the access right management, and thus, a separated authentication/identification system and actual control access system based on access right management must be the correct focus of the approaches to be proposed.

This apparent contradiction is explained because most of the access control systems are fully owned and managed by the entities managing access rights (this is, in most cases, port authority). In conclusion: in the present situation, both authentication/identification system and access right management is under control of the same party, and probably a separated access rights management system would be more costly than an integrated, unique control access system including authentication, identification, and actual control access based on access rights given to the system users.

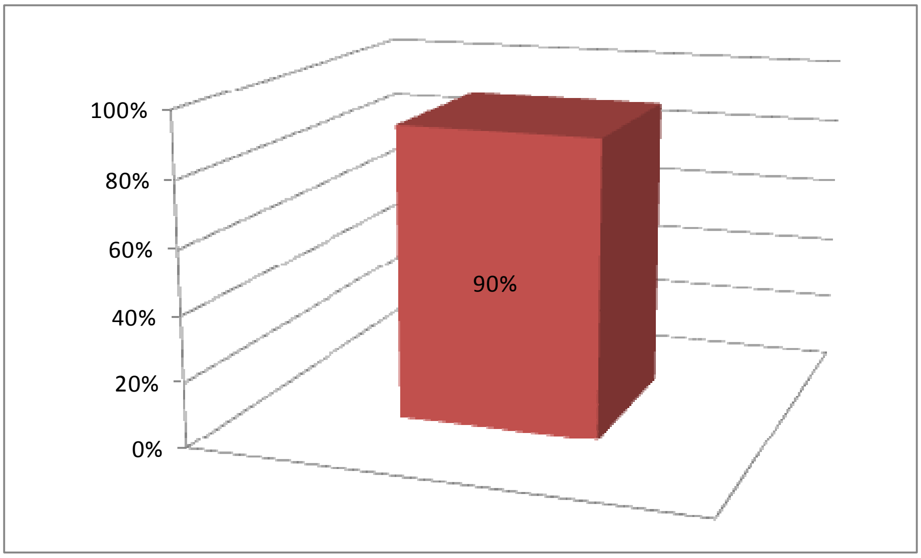


Figure 32 Access Rights Management included in the ACS

- ***Based on the results obtained, and for port owned and managed system approaches, the best access right management policy is to integrate it with the authentication and identification processes in the whole control access system.***

- ***For an alternative, outsourced system, the opposite requirement would be preferred: access rights management shall be isolated and fully managed and controlled by the port authority.***

7.4.1.6. OTHER SECURITY ACCESS CONTROL TECHNOLOGIES USED IN COMBINATION

Vehicle access to ports seems to be an obvious need. Thus, most of them implements license plate registration and recognition systems to control and restrict access of the vehicles accessing the controlled areas. CCTV is present as well in most ports consulted.

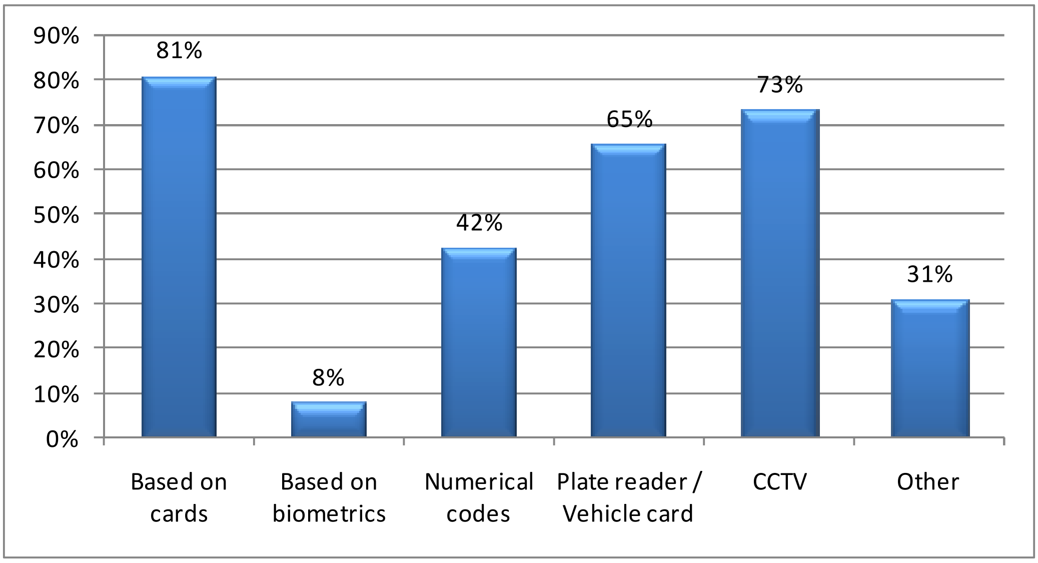


Figure 33 Control access system technology

- ***Any approach shall be compatible with license plate recognition and CCTV systems, and may consider the synergic and combined use with them to improve the access control system overall security levels.***

- ***Other technologies other than card access systems used in a few ports (for example, RFID tags), will have to integrate with and adopt the EPAIC card system proposed.***

7.4.1.7. SID COMPLIANCE

Most of the port's access control systems do not comply with the SID (Seafarers Id Document) standards. And, as it will be remarked in point 5.4, this compliance is poorly seen as necessary. This is because seafarers are, in most cases, a user type with little or no interaction with the control access systems, and police checks and regular ID documents (passport, etc.) are considered enough for identification purposes of this collective.

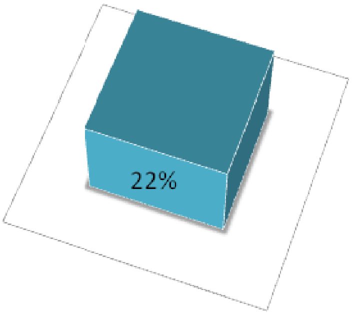


Figure 34 SID Compliance

- ***SID compliance shall not be raised in this EPAIC study.***

7.4.1.8. ISPS Code Compliance

Almost all the ports consulted have implemented extra security measures for levels two and three, as it is remarked in the ISPS code. However, the answers are not detailed enough to propose a specific set of technical requirements for each level.

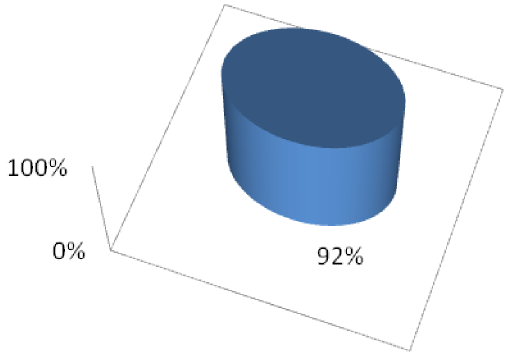


Figure 35 ISPS Code Compliance

The most common extra security measures adopted include police control, tightened access right requirements, and permanent manned access points. Anyhow, the EPAIC system approaches must be easy to adapt to this extra measures quickly if the situation is required, so the following requirements can be proposed:

- ***Police and local/government authorities shall be eligible as authorised administrator users of the control access management system if it is needed. They could be considered as a port authority holder type user.***
- ***Access right management inclusion in the EPAIC management system, as seen in point 1.5, is preferred.***
- ***Gates and control access point must be able to be manned.***

7.4.2. Card Related Requirements

7.4.2.1. Usage of Card Access Systems

Most of the port current control access systems already use cards. This is an advantage when trying to impulse and adopt a common card system as EPAIC.

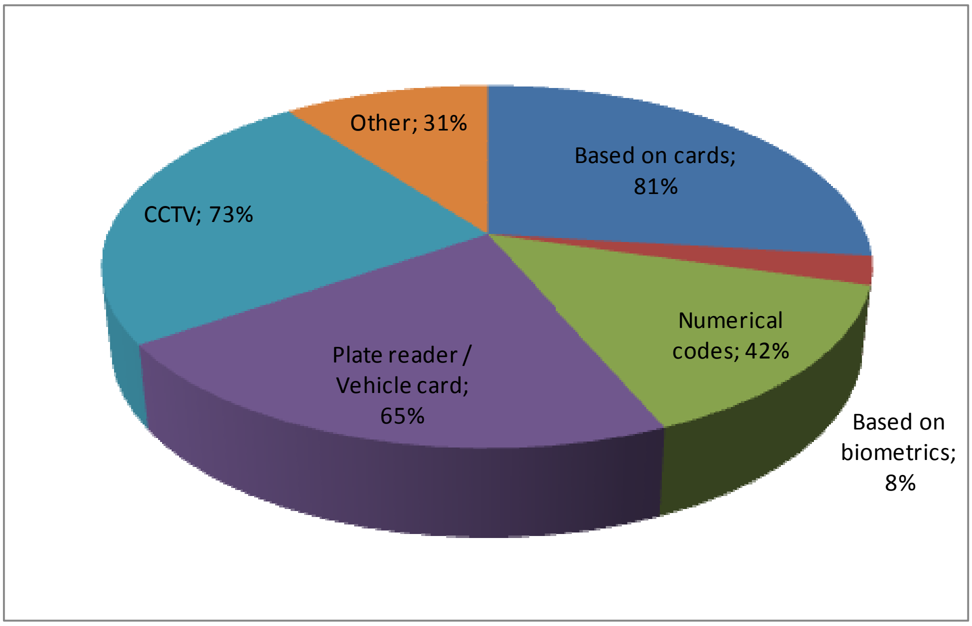


Figure 36 Implementation of Access Systems

7.4.2.2. Checks Performed and Authentication Factors Required

Most of the card control access systems perform electronic validation. Dumb/empty cards are more commonly used for one-time-use guest and visitor cards.

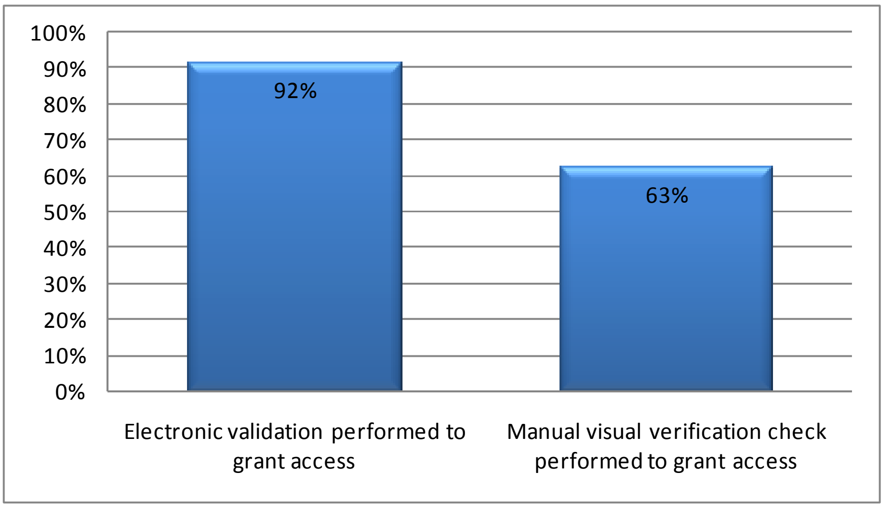


Figure 37 Grant Access Form

Visual verification checks are performed in most ports, but it is not said if it is always checked during normal system operation in the control access points (which requires them to be manned), or if it is only required under certain circumstances (ISPS higher levels, or whenever security personnel or police consider it necessary). *This information would be very valuable in order to find the actual need for an electronic or automated user authentication measure, which is not available in any system not using biometrics*.

Regarding technical requirements:

- ***Cards must permit both electronic validation and visual verification checks.***

7.4.2.3. BIOMETRICS

Only the ports using outsourced approaches performs biometric authentication, making them the only ports performing user authentication. This lack of user authentication factor (“what I am”) is a serious issue for the security level offered by the current systems.

Card authentication factor alone is not considered secure enough, and should be, at least, complemented with an additional authentication factor, which depending on its nature could be:

- **What I know**: card holder must authenticate the card and also input a numerical code or password that only the legitimate holder should know. As physical control access is performed when accessing port areas, a “What I am” factor would be more secure and possible in any use case: holder is always physically present in the control access. A “what I know” authentication factor would require password input compatible and secured readers and the systems responsible for checking those passwords.

- **What I am**: as said before, this option is preferred, as the user is physically present during the check. Three alternatives are found:

  - Biometrics: unattended and automated solution. It is the most secure alternative, as can also provide strong card counterfeit protection by using encrypted and hashed biometric templates (minutiae patterns). It would surely cut the user authentication check delay as well, and it saves the cost of having manned access control points. Most ports does not use biometrics in their current access control systems, so cons would include the implementation and deployment cost, and probably, a complicated user adoption of this kind of checks. It also supposes that at least enrolment and the card chip would require registration and store of the holder biometric data, which can be considered as sensitive personal data.

    Most suitable biometric technology for this kind of use and environment requirements is hand-scan and fingerprint checks.

  - Permanent manned control access points (local or remote): in person face to face visual verification of holder against the holder photo on surface or displayed from card chip. Check must be done by authorised personnel (port authority staff for example), and it could be performed in the actual access point, or remotely through CCTV or similar image transmission system.

    Ports may be better adapted to implement this approach, as most of them already perform this kind of checks, although it is not said if in a permanent basis or following different criteria, as seen on point 2.2. Due to this good start point, adoption cost could be lower than in the biometric approach. However, this method could be slower in practical operation, and does not provide a strong protection against card counterfeit, which should require security measures to avoid this kind of threats:

    - For holder photo imprinted on surface check: counterfeit measures that physically makes the card unique (holograms, guilloches, UV markings, microtext, etc.).

    - For holder photo displayed from card chip to screen: electronic card authentication methods, and data protection through encryption and trusted issuer signature on enrolment.

    If holder photo is not obtained from card, but from inside the management system, card counterfeit would not suppose a threat, but systems, networks and terminals storing and managing the displayed picture shall be secured.

  - Other automated visual check technologies: face recognition: would suppose an unattended and automated solution, but technology is not mature enough to reach the security level of a biometric approach like fingerprint or hand-scan.

- ***A biometric user authentication factor is strongly recommended to improve the current security in the ports. However, high deployment cost and user adoption issues are expected. Proposed approach could include some solutions based on biometrics, and other using other, less advanced but better adaptable methods as described above. Or, if possible, an adaptable approach that could support biometric and non-biometric operation modes could be the best option.***

- ***In all cases, card counterfeit measures are a strong requirement to guarantee a proper security level, as it will be discussed in point 2.6.***

7.4.2.4. PREFERRED CARD INTERFACES

About 50% of ports use contactless RFID interfaces. A 29% of them specifically remarked the use of MiFare products, and other 19% of the rest use ISO 14443A compatible RFID interfaces. The non contactless interface most used is the magnetic stripe.

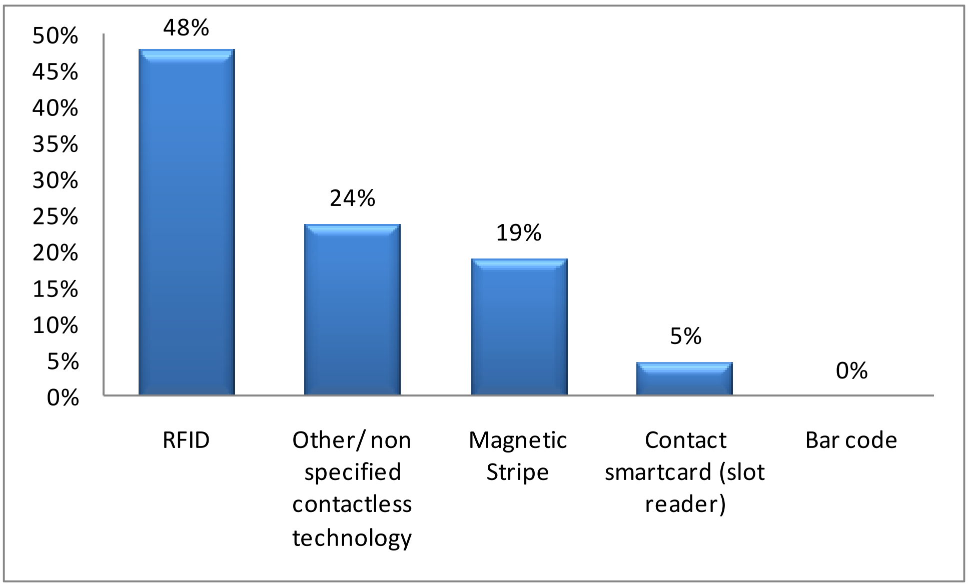


Figure 38 Card interfaces

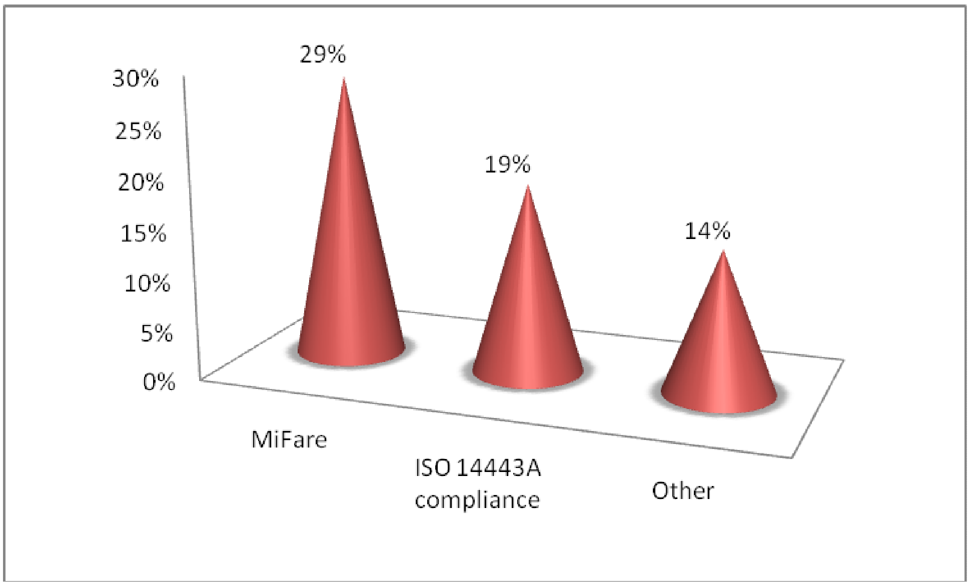


Figure 39 RFID interfaces

- ***MiFare standard is one of the most extended options for cards. However, magnetic stripe shall be considered as a secondary interface to improve compatibility with ports with no possibility or will to deploy contactless technologies. Secondary non contactless interfaces would suppose a good option to improve the security when sharing data between card and reader, as it can be used as a separated transmission connection, with no possibility of wireless data threats (good option for encryption shared key transmission between card and reader, for example).***

7.4.2.5. CARD DESIGN PREFERENCES

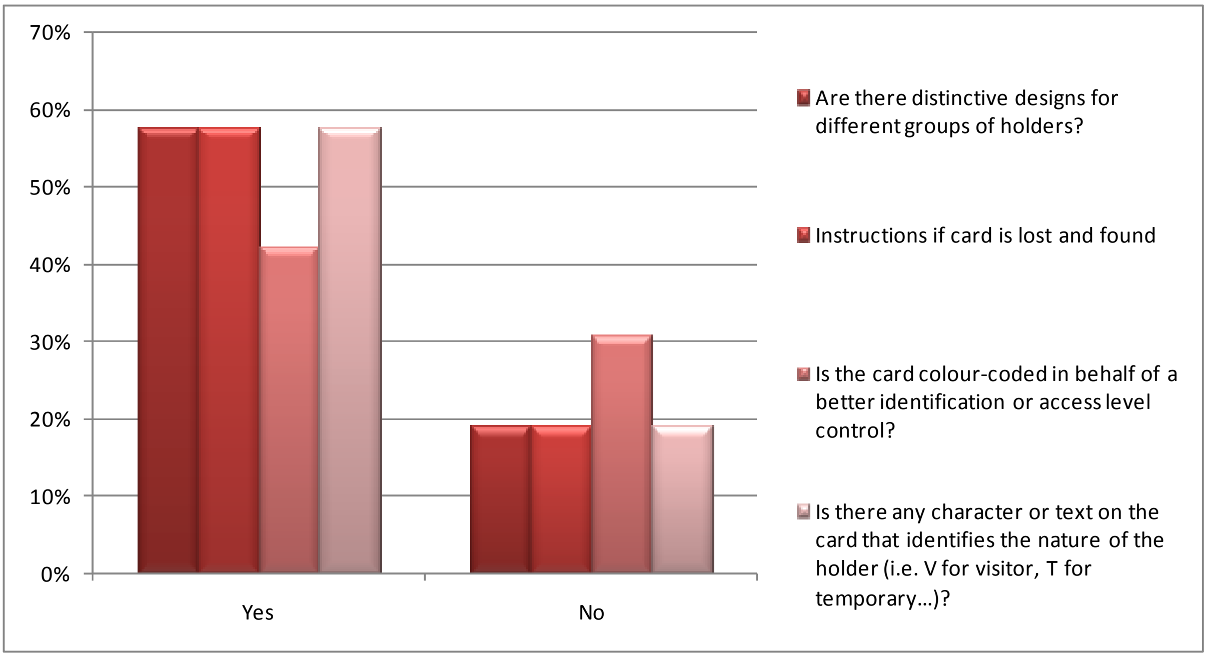


Figure 40 Card design preferences

Based on the tendency present in most ports, card design should meet the following requirements:

- ***Different designs for each user role, explicitly identifying the holder role type. In the case of private companies operating in the port, this shall include a distinctive sign that identifies the card holder employer.***
- ***Instructions for lost and found cards must be included.***

7.4.2.6. CARD SECURITY MEASURES APPLIED

Many ports do not apply any security measure to their cards. This supposes a big impact in the card authenticity security aspects.

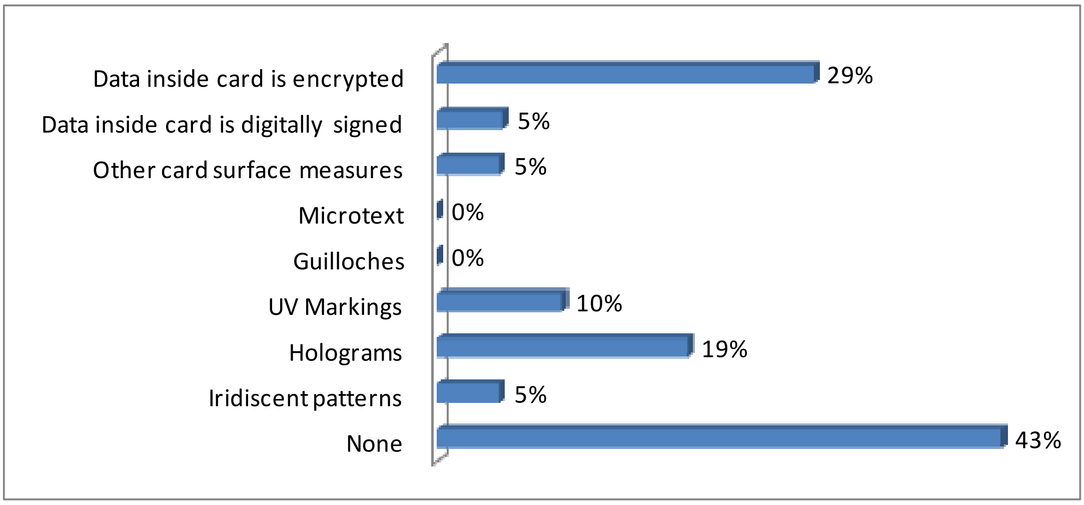


Figure 41 Card security measures

If no security measures are applied, cards could be cloned or counterfeited, making any card authentication method not reliable.

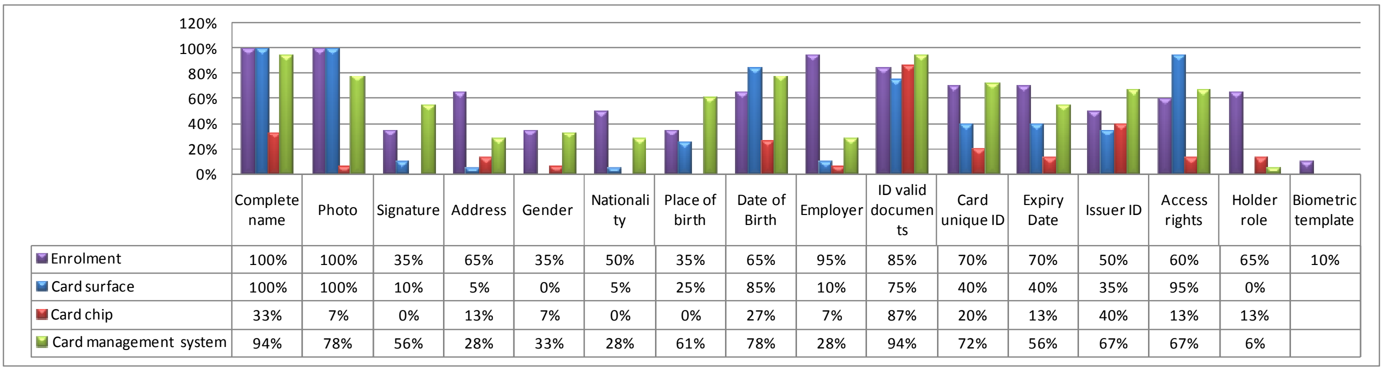
- ***One or more counterfeit measure quoted in the questionnaire should be applied, as well as data encryption.***

Data stored inside the card chip could be subjected to unauthorised access and modifications, by using illegitimate readers with stolen cards, or sniffing data from wireless connections in the contactless interfaces for example.

- ***Data encryption with robust algorithms and/or digital signature of the legitimate issuer assures that data inside cards is properly secured.***

Card security measures are a key factor that needs to be improved in order to assure a proper security level. These requirements shall be considered as a priority.

7.4.3. HOLDER DATA USAGE, STORAGE AND PROTECTION TENDENCY



	Complete name	Photo	Signature	Address	Gender	Nationality	Place of birth	Date of Birth	Employer	ID valid documents	Card unique ID	Expiry Date	Issuer ID	Access rights	Holder role	Biometric template
🟪 Enrolment	100%	100%	35%	65%	35%	50%	35%	65%	95%	85%	70%	70%	50%	60%	65%	10%
🟦 Card surface	100%	100%	10%	5%	0%	5%	25%	85%	10%	75%	40%	40%	35%	95%	0%	
🟥 Card chip	33%	7%	0%	13%	7%	0%	0%	27%	7%	87%	20%	13%	40%	13%	13%	
🟩 Card management system	94%	78%	56%	28%	33%	28%	61%	78%	28%	94%	72%	56%	67%	67%	6%	

Figure 42 Holder data storage

7.4.3.1. ENROLMENT

The enrolment process is the one requiring more personal data from holder. This should not suppose a legal problem, as the enrolment can be performed without any personal data transmission between different countries, unless background checks are required and holders are applying for the card in a country different from theirs.

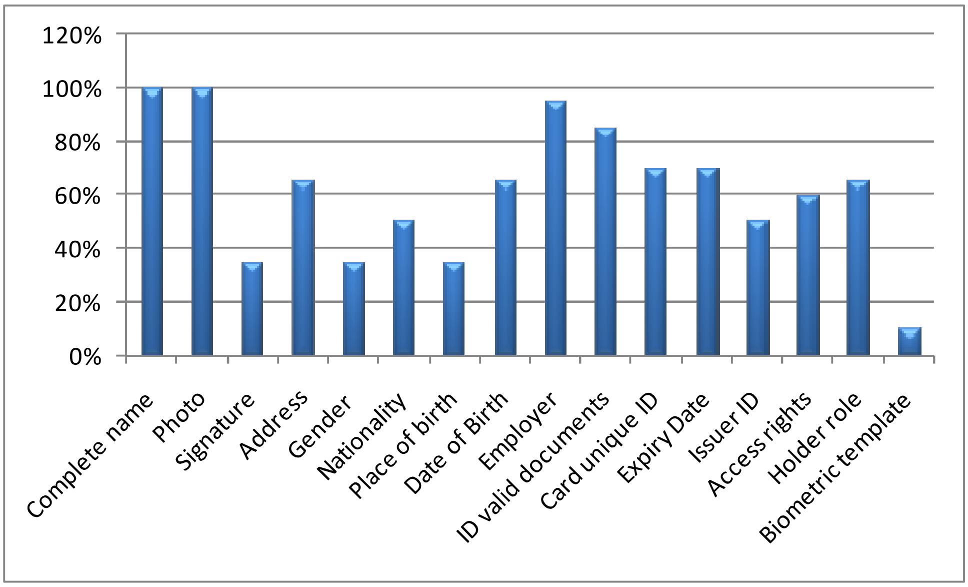


Figure 43 Personal data acquired in the Enrolment Process

The most common personal data requirements found are the following:

- ***Complete name.***
- ***Photography.***
- ***Address (work address).***
- ***Date of birth.***

- ***ID valid documents (passport, etc.).***
- ***Biometrics (only in case of using biometric authentication)***

The most common non-personal data requirements found are the following:

- ***Employer.***
- ***Holder role to be assigned.***
- ***Access rights to be given.***
- ***Card unique ID is created during the process.***
- ***Expiry date is defined during the process.***

7.4.3.2. On Card Surface

No sensible personal data is required to be present on the card surface. The most common personal data requirements found are the following:

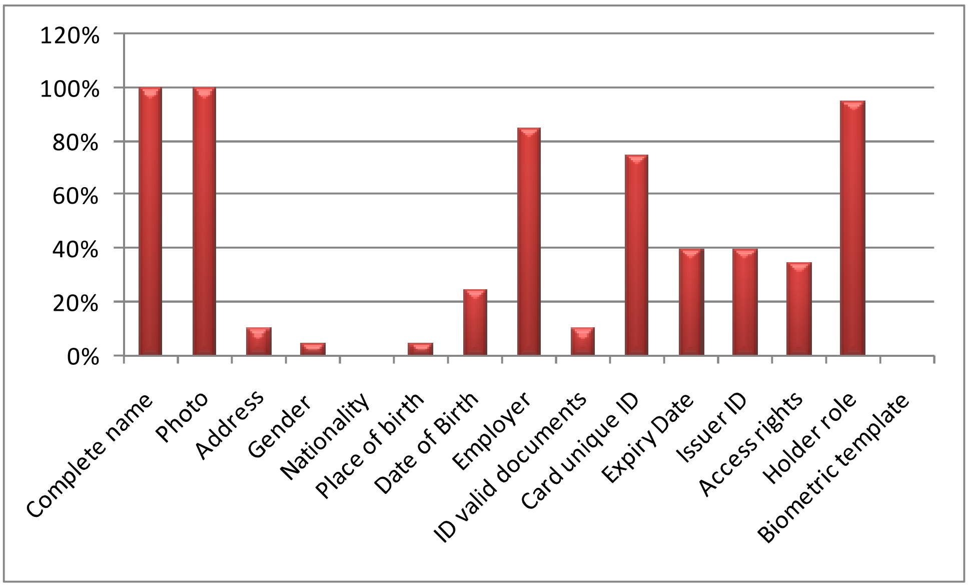


Figure 44 Personal data on Card Surface

- ***Complete name.***
- ***Photography.***
- ***Date of birth.***

The most common non-personal data requirements found are the following:

- ***Employer.***
- ***Holder role to be assigned.***
- ***Card unique ID.***

7.4.3.3. INSIDE CARD CHIP OR MAGNETIC STRIPE (IF AVAILABLE)

Unless biometric authentication is used, no personal data is required to be stored inside the card electronic chip or memory. The most common personal data requirements found are the following:

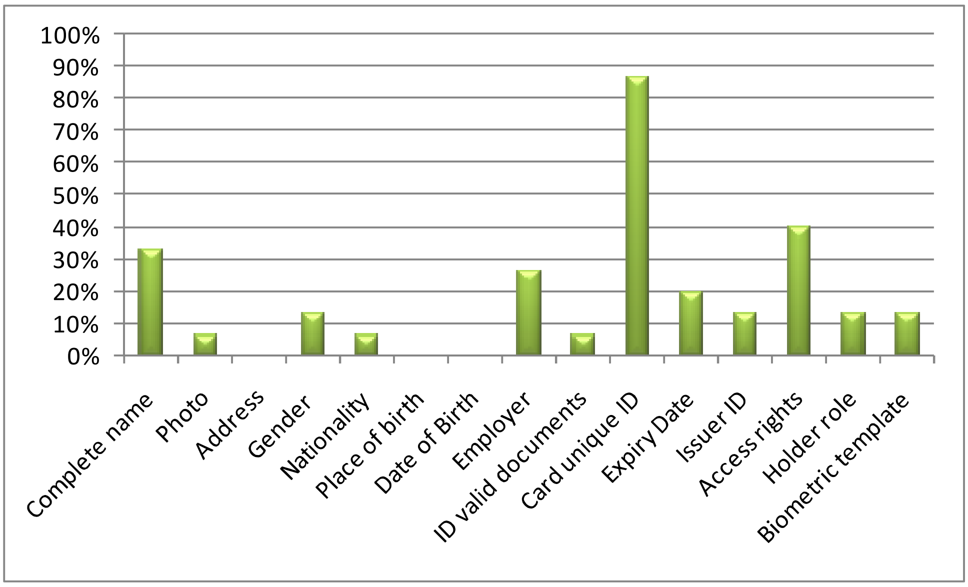


Figure 45 Personal data inside Card Chip or Magnetic Stripe

- ***Biometrics (only in case of using biometric authentication)***

The most common non-personal data requirements found are the following:

- ***Access rights to be given.***
- ***Card unique ID.***
- ***Expiry date.***

7.4.3.4. IN THE CARD MANAGEMENT SYSTEMS

In most cases, the card management system requires, after the enrolment procedure, to manage and store a bigger number of personal data. However, in technical terms, it is not strictly necessary for the management system to count with some of this data, and the main reasons for keeping this information stored in those systems may be:

1. That the management system owner (port authority in most cases) desires to store and keep track of the personal data of holders as a method to have more control over the control access system users, creating a not necessarily true feeling of improved security.

2. That data collected during the enrolment process is automatically stored in the management system, just in case it could result necessary.

The truth is, that for actual system operation in technical terms, no personal data is required, unless the management system need to transmit this data (complete name and picture) to remote terminals for a manual check (visual verification as approach for user authentication procedures). If the systems is well designed, biometric templates can be stored exclusively in the card chip.

However, there are various valid reasons to keep stored some personal data in the management system: backup security measures, keeping a complete user profile activity registry for incident handling and forensics, speeding up renewal, upgrade, revocation and termination processes, etc.

- The proposed approach should start from a model where any personal data is actually required for ***system operation, and from that starting point, the need for include additional personal data in the system for those justified purposes quoted above shall be proposed.***

- ***In addition, this additional personal data can be actually considered as non sensible information in most cases, and its inclusion in the management system does not need to arise any legal issue between state members. This non sensible data could include the following:***

  - ***Holder complete name.***

  - ***Holder photography.***

  - ***Date of birth.***

The most common non-personal data requirements found are the following:

- ***Access rights to be given.***

- ***Card unique ID.***

- ***Expiry date.***

- ***Holder role.***

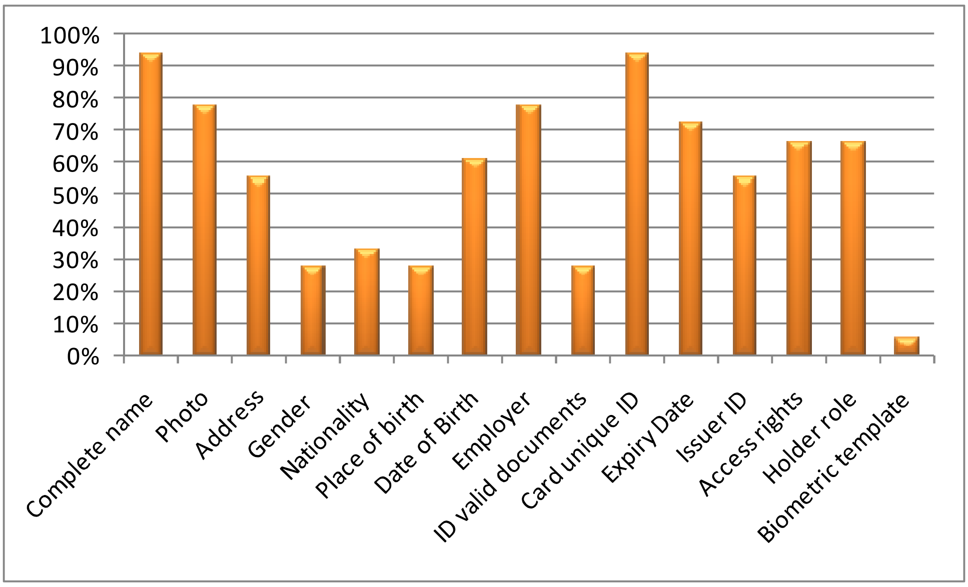


Figure 46   Personal data in the Card Management System

Finally, in case that biometric authentication approach is preferred:

- ***Biometric templates are not required to be stored or used by the card control access management system, but the card reader.***

7.4.4. *Card Management System and Card Lifecycle Aspects*

7.4.4.1. Card Management System Ownership, Operation And Infrastructures

As it has been seen before, most ports have control of the main access control system operating in the port. Other approaches, like outsourcing the authentication and identification system to a third security specialised party, or give the private companies operating in port facilities freedom to use their own, unique access control system, are minimal in comparison with the port owned and port managed approach.

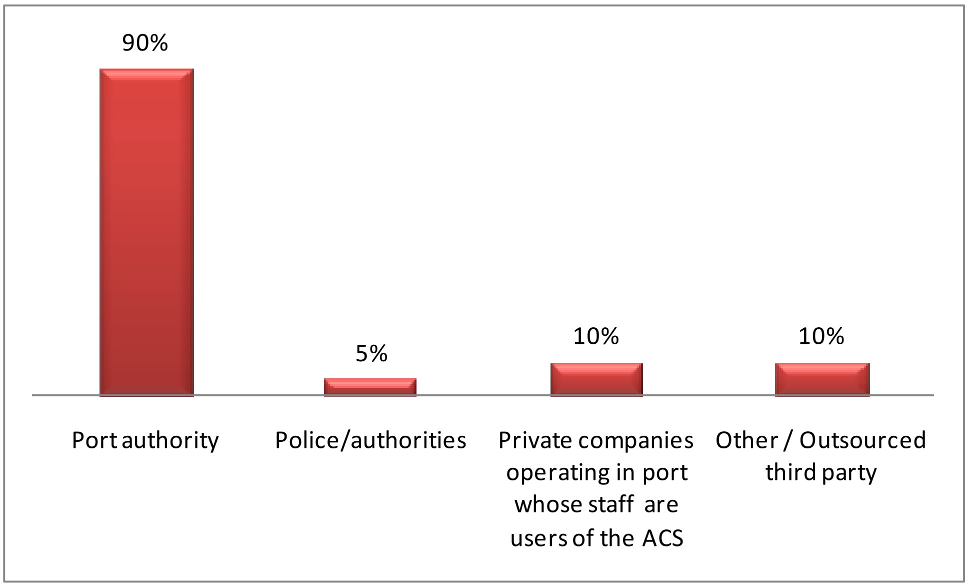


Figure 47 Responsible for card system enrolment process at port

As consequence of this, card lifecycle related procedures are performed and managed by port authorities as well. Based on this fact, the following proposed requirements have been created to reach a minimal cost migration for most ports consulted, as they follow the common lines of convergence found in the questionnaire results.

- ***Port authority staff or authorised personnel shall perform the enrolment process.***
- ***An office or similar adequate point must be available inside the port for applying for a new card. This office will be also available for new and renewed card claiming.***
- ***Card holder or his employer can request the enrolment, under the following requirements:***
  - ***Holder must complete an in-person face to face verification during application.***
  - ***A formal operational need statement must be included to justify the need for a card for the card applicant. Holder employer shall perform this task.***
- ***The following background checks are required:***
  - ***The holder company must be checked before starting its operations in a port facility.***
  - ***Individuals applying for a card could be checked if:***
    - ***Their task to be performed in the port is related to port security aspects.***

    - *Their task to be performed takes place in restricted or dangerous port areas or facilities.*

- *Background checks shall only be performed by Police if the port authority does not have access and permission to access to the data to be checked (criminal records, etc.).*

- *Background checks shall last from 1 to 3 weeks.*

- *Card production procedures and infrastructures are managed and owned by the port authority authorised own personnel, which must be security cleared. Card actual production shall not be outsourced, so a production infrastructure will be required. Only card holders shall claim their cards, or they can be sent to the holder company for distribution to their holders.*

- *Without background check delays, total card application and production time shall be no more than three days.*

- *Card expiration time span may vary from 1 to 3 years.*

- *Card renewal will require that holder return the expired card at the card issuing office and a new card is produced. In person face to face verification of the holder is required.*

- *Any expired or terminated card must be automatically blocked. This means that the following requirements mentioned before must be met:*

    - *Access right management must be integrated in the card management system.*

    - *Expiry date must be stored and checked in the card management system.*

- *Card termination shall be initiated by port authority or by holder employer, with a justified reason.*

- *When a card is terminated, the holder data must be erased from any system in the card access control system, and if card is not physically destroyed, erased from the card as well. Data deletion procedures must be secure and guarantee that data can not be accessible anymore.*

- *Only non sensible holder personal data (complete name) can be further retained in the system after card termination, exclusively stored in the existing system registry for auditing purposes or if needed in legal issues.*

- *The following data inside cards and management system could require modifications during card lifecycle:*

    - *Holder photo (if required).*

    - *Expiry date.*

    - *Access rights.*

    - *Biometric templates (if required).*

    - *Holder role.*

- *These modifications shall be performed only by port authority authorised personnel through secure means and procedures.*

7.4.4.2. Card Management System Data Protection Security Measures

Any holder data managed and stored inside the card and the access control management system shall require protection. Most ports apply some security measures to their systems, but the following shall be applied for any proposed approach:

- ***Card readers must be secured: physical security measures to prevent reader manipulations, secured administrative interfaces, protection against information sniffing, and reader counterfeit protection.***

- ***Card access control management system shall be an isolated system, and any data must be transmitted to external systems, with the exception of other port EPAIC card access system for the following purposes:***

  - ***Expiry date checks.***

  - ***Update of any id data regarding card authentication procedures: this shall not include any personal data, but card unique id, authorised issuer certificates updates, card blacklisting and status, etc.***

  - ***Update or notification of validity and registration of a new EPAIC card holder. This shall not include any sensible personal data, neither holder photo if remote on screen visual verification checks are not performed.***

  - ***Update of holder photo, only in case of approaches requiring it for remote on screen visual verification checks in ports (not necessary if biometrics is used).***

  - ***Update of holder role and access rights for the card holder in that port. This shall not include any personal data.***

- ***For these punctual transmissions between ports, communications must be secured.***

- ***Police shall have access to the data inside the management system. This shall be achieved by granting authorised police officers access to the system as port authority administrative user holder role. This is police staff responsible of EPAIC system access shall apply for this administrative user role.***

- ***Management system data back up must be performed periodically.***

- ***Terminals, servers and databases must be protected with user control access under login and password authentication.***

- ***System networks shall be protected through firewalls and IDS/IPS elements.***

7.4.4.3. Visitor and Temporary Cards Specific Requirements

Visitor and temporary card holders have special needs that entail different requirements for this type of cards.

- ***Card production of visitor/temporary cards must be performed instantly in the previously quoted issuing office.***

- ***Enrolment would not require any personal data but complete name should be included.***

- ***Card shall consist on a dumb card displaying only the holder complete name, card ID, holder role, validity time or expiry time, and employer.***
- ***If required, card electronic interfaces (RFID) shall only contain a predefined visitor card unique ID (this may cut card issuing time) and card expiry. During enrolment and card issuing, this new visitor card ID must be mapped to certain access rights.***
- ***The previous requirement is not needed if visitor escorting is mandatory.***
- ***Card expiry time shall be defined during issuing, and would be obviously shorter than the average expiry time of normal cards.***
- ***Card must be terminated and destroyed once expired. There is not a renewal process.***

7.4.4.4. AUDIT

System audit should be a mandatory action to maintain and guarantee that the system meets the security requirements and quality standards. About 40% of ports consulted have not implemented an audit plan or procedures.

- ***Any proposed approach must include an audit plan or procedure, which shall include security audits at least. The audit would be performed annually, and can be performed by external professionals or internal system staff suitable for these tasks.***

7.4.5. PORT IMPRESSIONS REGARDING ADOPTION OF A NEW SYSTEM SUCH EPAIC

7.4.5.1. PORT IMPRESSIONS ABOUT THEIR CURRENT SYSTEM

Most ports are satisfied with their current system, and also plan to make future improvements. This can lead to a lack of agreement and support from ports to adopt a new system such EPAIC if migration cost and operation impact is not as low as possible.

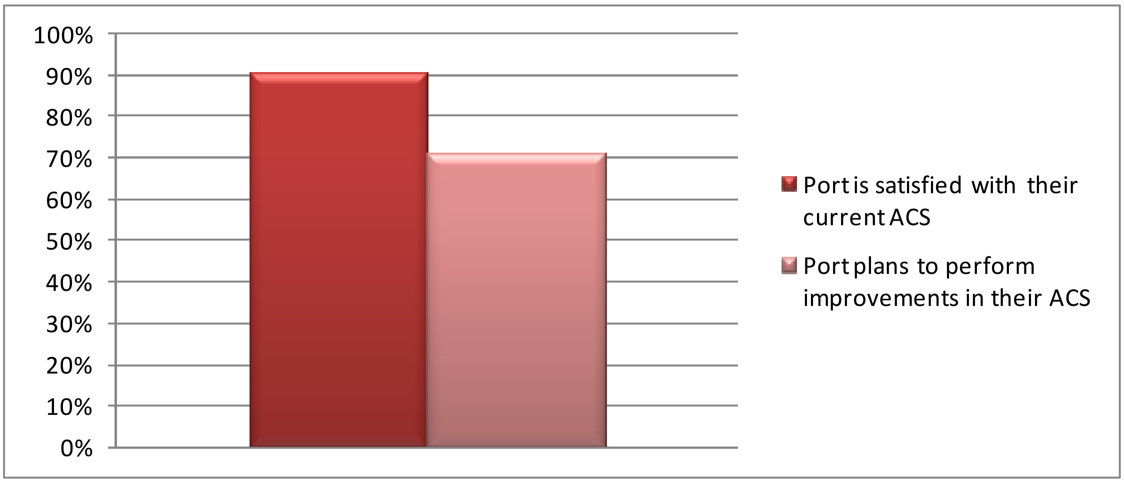


Figure 48 Port's satisfaction with their current ACS

Therefore, any approach should be based on the model that will suppose the minimal migration cost for most ports, and from that point, discuss which new security requirements are actually needed. New security improvements must be necessary enough to justify the increase of the migration cost and operation impact that their inclusion in the proposal will suppose. Fortunately, all ports consulted have a lot of common requirements, and their control access systems converge in many aspects.

7.4.5.2. ACTUAL SECURITY LEVEL ACHIEVED IN PORTS CURRENT SYSTEMS

The main lack of technical security measures in the current port access control systems are, basically, two:

- Lack of user authentication factor: only card is authenticated. The optimal solution for this is the use of biometrics. However, other options have been discussed in this document as well (permanent manual visual verification control checks, etc.).
- Lack of card protection and security measures: card could be easily counterfeited and their content illegitimately obtained. Card counterfeit physical protection measures (holograms, UV markings, etc.), and data encryption to avoid unauthorised access to data inside the cards. Issuer digital signature of card data (as a PKI) would be both a counterfeit and data confidentiality protection mechanism.

7.4.5.3. WILLING OF ADOPTION OF AN EPAIC CONTROL ACCESS SYSTEM

Results on this subject reflect that only about 42% of ports would be interested in the adoption of an access control system approach such EPAIC. However, this percentage could be actually lower, if ports that have not even send the answered questionnaire are taken into account. Thus, the conclusion is that a full support and willing of adoption of the EPAIC system approach will not be possible. This makes the reduction of migration cost and operational impact even more critical.

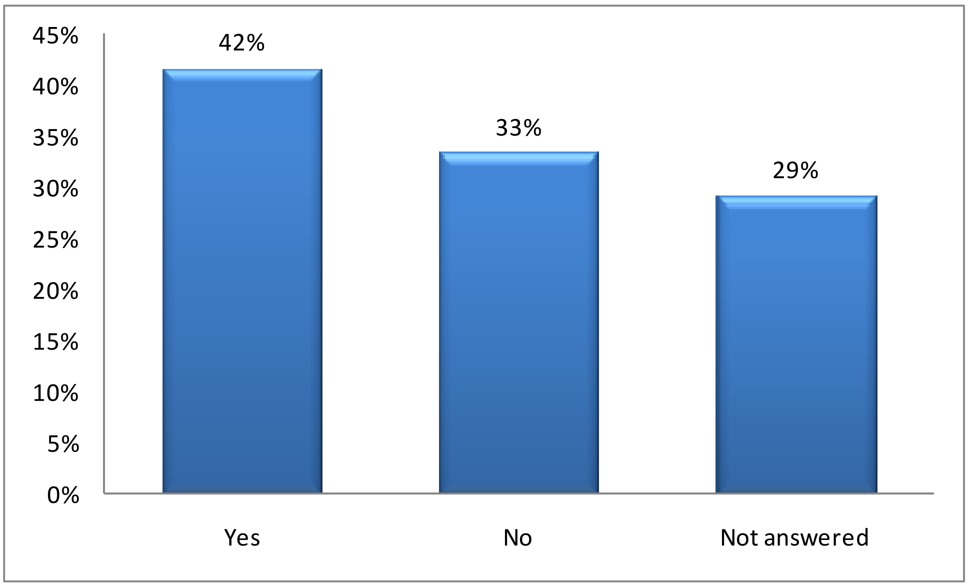


Figure 49 Interest in an EPAIC approach

7.4.5.4. WILLING OF ADOPTION OF OTHER POSSIBLE IMPROVEMENTS

SID document compliance is poorly supported, as most ports do not consider it as a critical security improvement. This is due to the following facts:

- Most access control checks for ship crew and passengers are actually performed by police, customs and port border agencies. Port authority is not responsible for these checks.
- For police and custom checks, identity documents, as passports and visa, are enough to their purpose.
- Aligned with the first point, port and port facilities access control systems are more focused on other type of users, mainly port workers, port operating private companies' workers and visitors.
- That in the present day, SID has only a few supporting countries ratifying it (Nigeria, France and Jordan).

7.4.5.5. Common Concerns

Port main concerns about EPAIC system adoption are:

1. Migration cost.
2. Access control system and access right management actual control and management.
3. Port operational needs divergence.

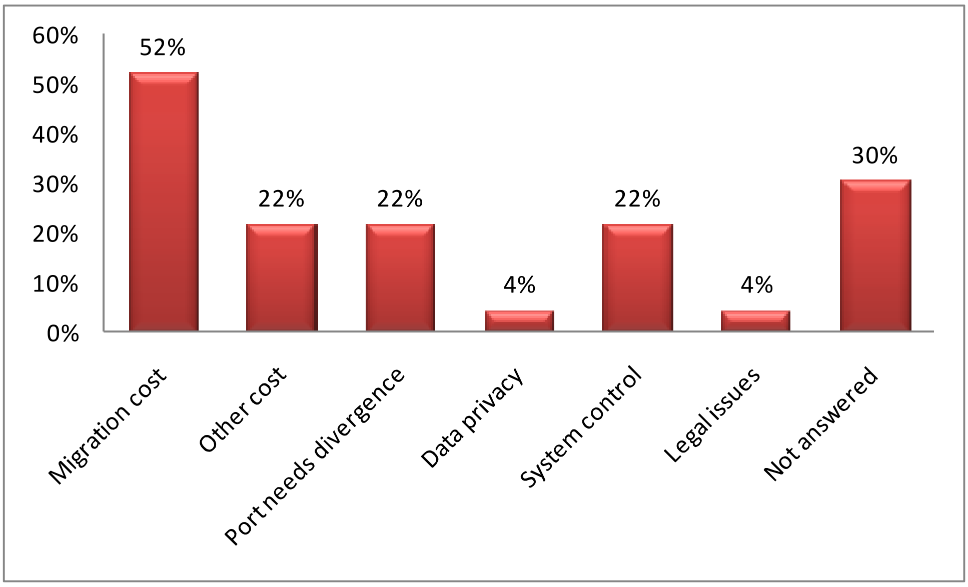


Figure 50 Concerns about EPAIC system

7.4.5.6. Perceived Aspects and Benefits of EPAIC

Only a few ports have remarked one or more benefits about a system approach like EPAIC. The main benefit remarked is the operational daily cost in time and money for those users requiring to access to various ports (transportation workers, mainly).

8. COST BENEFIT ANALYSIS AND IMPACT ASSESSMENT

8.1. COST BENEFIT ANALYSIS

8.1.1. AIM OF THE TASK

Nowadays the European ports have different access systems which require for people working inside or who have commercial relationships with it, the use of different way of access to go through port sites.

The need to introduce a common identification card has been the object of the analysis of EPAIC I project in which the creation of an ID card storing several data of the card owner and issued by a central authority was raised.

The EPAIC I analysis proposed five candidate models which main differences were basically in the way of storing data and functions:

- The Central Model where data and functions are stored at a Central Level.
- The Distributed Model where data and functions are stored at a National Level.
- The Replicated Model where data and functions are stored replicated at national systems and stored at national level.
- The Hybrid Model where data and functions are stored part at Central Level and part at National Level.
- The Mesh Model where some data and functions are stored at National Level while the rest are copied to a National Level.

After having analysed the five candidate models and taking into consideration the storage, processing and communication requirements for each type of data that would be stored and processed by EPAIC, two models were proposed as candidate for the EPAIC system: the central and the hybrid model.

- Central Model: the centralization of the logic and data in a unique system including all ports of state members has the disadvantage of a high communication infrastructure cost and the benefit of an ease administration and integration of the Member States to the system.
- Hybrid Model: data and functions can be stored at different level according to the selected configuration. The costs and benefit of the model varies depending on the selected configuration (especially telecommunication costs)

The aim of this task is to assess the costs and benefits of a European Port Access System to be adopted from the European ports as resulted of the EPAIC II study.

Cost is defined as the total sum of any monies, time, resources or other relevant determinable valuable feature that has or can in given circumstances have a negative or reductive financial impact on the specific decision contemplated. Costs are normally defined as reduction in human well-being

Benefits is defined as the total sum of any monies, time, resources or other determinable valuable feature that has or can in given circumstances have a positive or accretive financial impact on the specific decision contemplated. Benefits are normally defined as increases in human well being.

Benefit - cost analysis is a "tool" to support decision makers whether a regulation is efficient or not. In this context we can say that a regulation is justified if the incremental cost of implementing or adapting the actual system to a safer one is exceeded by the incremental benefit generated by the regulation.

The incremental cost of implementation is the difference between cost incurred from the proposed access system and the cost incurred for the current system with no action.

8.1.2. METHODOLOGY

The methodology to be followed in the study will analyse:

- Benefit of the common European Port Access System as conceived in the EPAIC I.
- The data acquired with the questionnaires with special attention to economic data.
- The access system as conceived in the EPAIC II trying to give a list of the related cost needed to implement the system (in a first step we hypothesise costs in a Spanish market):
  - CAPEX costs. Capital expenditures (CAPEX) are expenditures creating future benefits. A capital expenditure is incurred when a business spends money either to buy fixed assets or to add to the value of an existing fixed asset with a useful life that extends beyond the taxable year. CAPEX are used by a company to acquire or upgrade physical assets such as equipment, property or industrial buildings.
  - OPEX costs. Operational expenditures (OPEX) are ongoing costs for running a product, business, or project. In summary, OPEX costs are the sum of a project's operational expenditures for a period of time, such as a month or year, and can be fixed or variable.

8.1.2.1. BENEFIT OF THE EPAIC SYSTEM

The strengths of adopting a European common Port Access system can be describe as follows:

- to enhance port security, minimizing the possibility to counterfeit
- reduce vulnerability of transport
- to meet the need to adopt preventive measures at a European level
- to facilitate integration between ports by using only an access card accepted and recognised by all participants which will reduce current differences
- to better organise people, trucks, car, haulier flow with an increased logistic organisation

However the adoption of a common port access system presents weaknesses such as:

- The right to privacy and national data protection rules.
- Social and behavioural consequences of the different kind of control which could affect human rights. A recent study of RAND "applying for a passport" case study demonstrate "a general discomfort in the provision of advanced forms of biometric information such as DNA as part of the process of passport application. Responders were only willing to accept (i.e. they derived negative utility form) the collection of DNA and photograph data at the point of application for a passport only if there was a subsidy of 19 pounds on the cost of the passport"[1].

[1] RAND Technical Report "security at what cost? Quantifying people's trade offs across liberty, privacy and security"

- Ports have different needs so that actually the access controls are based on the diversity of each of them. A harmonization does not mean a better and safety environment
- The cost implications could be higher than the expected benefit.
- Many ports have already implemented their own access control according to ISPS code and they have invested large sum of money for implementing it.

8.1.2.2. ANALYSIS OF THE DATA ACQUIRED

The data collected until now with the questionnaire has highlighted the following:

- Most of the feedback came from the ports. There is only one questionnaire from Coast Guards.
- Based on the questionnaire results, the access control systems are mostly based on:
  - Cards (81%)
  - Biometrics (8%)
  - Numerical codes (42%)
  - Plate Readers (65%)
  - CCTV (73%)
  - Others (31%)

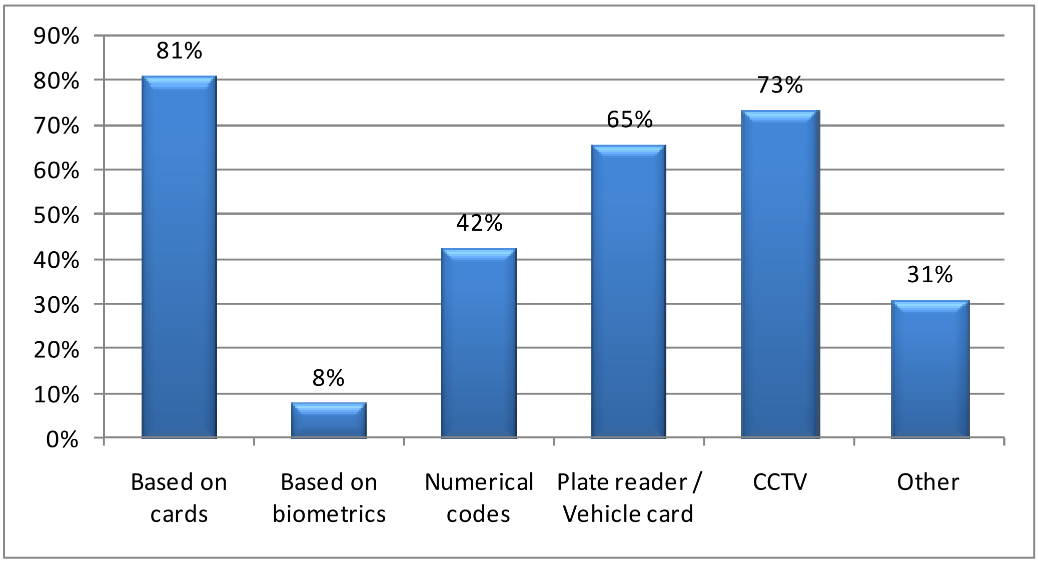


Figure 51 Different Access Control System technologies

- The number of existing control access gates vary considerably from port to port. On one side there are ports which lack of a wide port access system while port facilities located inside the port operate with its own control access system as required by the ISPS code whose management is in charge of the port facilities operators as well. On the other side there are ports that do not have any sensitive port facilities and consequently there's not any wide port access system or facilities port access system. Finally there are ports which consider the port access system proposed in the project not able to improve security.

- Data related to costs are not readily available; the collection of information is often distributed among several departments and there is no a standard procedure to gather the information. This obviously increases the effort needed to give a comprehensive answer, thereby lowering the response rate.

The cost of an access gate varies considerably from port to port. Such difference could be ascribed to different reasons.

On one side it could be hard for a security department to know and collect data which normally depend on other departments. Economic and accounting data are often provided from the accounts department and in an aggregated form which need to be performed.

On the other side, it could be possible that such differences are real and the existing gap depends on different technologies used in port access system. This analysis implies a good knowledge of the different existing market on security technologies. Prices of security devices can vary considerably within European countries.

Another important variable to consider in the cost assessment is the number of security personnel employed. The cost of personnel is a considerably part of the "gate" total costs, considering that the gross wage, income taxes and other concepts differs from state to state. A port which for instance has simply an access gate without security personnel in charge can reduce a lot the cost of the access system.

Normally the training cost must be considered as part of the start-up cost, but in this case only the cost of fixed assets have been considered because on our opinion, the cost of personal training seems to be too out of proportion for the purpose of the analysis.

The total cost of the gate includes not only the card access system but the whole control system (CCTV, card plate reader, numerical codes) implemented in every gate. The EPAIC II control access system is only based on cards. The compatibility and interoperability with other access control systems besides cards could be considered in the migration cost. There will be parts of the existing system which could be reutilised in case of migration.

8.1.2.3. EPAIC II ACCESS SYSTEM

- ***ENROLMENT PHASE***
  - An application request is sent usually by the individual or the employer to a named office which could be located inside the port;
  - The proposed model distinguish between fixed and movable workers which difference is reflected in data storage (a local data base for fixed workers, a national data base for movable ones)
  - The management could be outsourced to an external company
  - During enrolment, several pieces of information are to be requested and stored in the card, namely:
    - Holder name
    - Photograph
    - Address
    - Employer

    - ID valid documents (e.g. national identification number, passport number, social security number, etc.)
    - Card unique identification number, created during the production of the card.
    - Expiry date
    - Holder role

- ***CARD SURFACE***
  - The card is used only for authentication purposes
  - Depending on the security level, the reader of the card may be a human being (if only photograph and name is required) or an electronic device
  - On the surface of the card, some elements could appear to allow for identification by human operators such as
    - Holder name
    - Photograph
    - Employer
    - Card unique identification number
    - Holder role
    - Expiry date

- ***CARD SECURITY***

  The following **physical counterfeits** have been proposed:

  - Biometric (basically based on hand geometry)
  - PIN code
  - Encryption of communication between the card and the card reader in order to avoid card cloning (contactless card technology MIFARE DESfire, as planned in some ports). Another option is to encrypt data of the card. In this case communications are also encoded.

- ***CARD LIFECYCLE***
  - It starts with their issuance.
  - Data can be changed after their production.
  - Each card would have an expiry date after which it should be renewed or destroyed, in case its holder does not need it anymore.
  - In any case, cards should be returned to avoid the existence of non – authorised cards which could end up in the wrong hands.
  - Expiration dates differ greatly from one port to another (from three months up to ten years).

- An expiration time of three years is recommended.
- In case card lifecycle will be managed inside the port an appropriate office will be needed.

TEMPORAL CARDS

- Temporal cards may be issued for those who need to enter ports during short periods of time (one or two days).
- These cards can be produced faster and require a fewer number of data but they may be more limited.

CARD ISSUANCE AUTHORITY

In almost all cases the port authority is in charge of enrolment (90 %) and the production of the cards (85 %). This may be due to different factors, such as the lack of a European normative that could specify a different issuance authority.

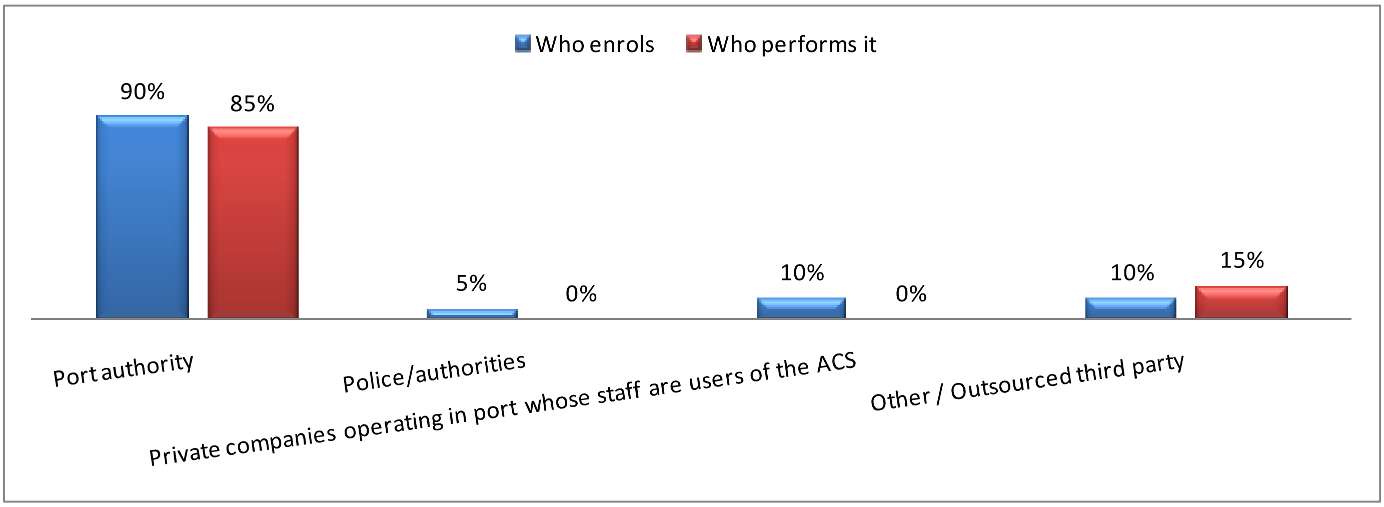


Figure 52 Card Issuance Authority

However:

- Some ports are determined to keep total control over the issuance process.
- Others would be glad to handle over that responsibility to an external agent. In this case the enrolment and issuing phases are managed by an external company but:
  - The technology used should be compatible with port wide system technology, including terminals.
  - Minimum security requirements must be agreed between local port authority and the external company.
  - Card holders can only enter in the ports which join the initiative.

DATA STORAGE

According to the enrolment phase:

- A **local data base** for port workers who don't need to move from a port to another and whose activities are limited to the port area.
- A **national data base** for those workers who need to enter different ports (truckers, ship suppliers, etc...).

MINIMUM INVESTMENT (COST BREAKDOWN)

Cards Cost

Almost all ports whose access control is based on cards use the MIFARE DESfire technology**.** The cost breakdown will be based on that technology in order to mitigate the cost of migration.

- **Internal issuing:**
  - From **10 EUR to 15 EUR** per card
  - About **5 EUR** per card for temporary reusable cards
- **External companies:**
  - **35 EUR** card issuing.
  - **30 EUR** annual fee for card management.
- **Card Reader**
  - Vicinity card reader MIFARE DESfire from **110 EUR to 150 EUR**
  - Biometric and fingerprint reader from **500 EUR to 700 EUR**
  - Every 2 card readers a card reader controller is needed whose price is about from **800 EUR to 1,100 EUR.**
- **Terminal:**
  - Fingerprint reader plus card reader from **600 EUR to 800 EUR.**
  - ID national card or passport reader from **2,800 EUR to 3,200 EUR.**
- **Software** to manage the enrolment and verification phase from **3,500 EUR to 4,500 EUR.**
- **Server data base** from **7,500 EUR to 8,500 EUR.**
- **Computer** from **800 EUR to 1,200 EUR**.
- **Card issuer machine** from **1,500 EUR to 1,900 EUR.**
- **Cable network.** This data is not predictable depending on the size of the area to be assessed.
- **Integration with other existing control access systems (plate Readers, CCTV, etc).** Normally there is not any problem to integrate new technologies with existing ones. It depends on the terminal owner or port authority decision and the cost of integration depends on the number of existing technologies to be integrated.

- **Implementation of an administrative office and related personnel.** In the case that the enrolment and issuing phases are carried out inside the port, then the implementation of an administrative office will be necessary. Besides the fixed assets costs, already mentioned above, at least one person in charge of administrative tasks must be accounted. Referred to the Spanish market, an administrative gross wage could vary from **20,000 EUR to 25,000 EUR** per year.

- **Security Personnel.** Not all gates inside ports need to have a security employer at the entrance. If the port decides to contract security service then the gross wage for that kind of worker can vary from **20,000 EUR to 25,000 EUR** per year. If the security service will be contracted for 24 hours a day then the gross wage will be multiply by three being a normal shift of 8 hours per day (Spanish market).

- **Annual maintenance Cost** the annual maintenance cost of the system can vary form **4,000 EUR to 6,000 EUR**.

  Other fixed assets costs like crash barriers, turnstile, traffic light, panels, etc will not be considered. In most cases all this kind of assets can be reutilised in the implementation of the new access system.

COST OF MIGRATION

The choice about migrating from one access system to another, includes many reasons to be considered which are not only limited to the value of the current technology. Since ports will be free to decide whether to move or not to another security access system, which means they don’t have any obligation laid by the law, the variables could be more than one.

Each decision has an associated risk, cost and value.

The return on investment of each decision is the incremental value divided by the incremental cost. Evaluate the risk, and add it to the cost.

A decision about the implementation of new security measures is not so simple. Most of the benefits are not easy to be directly calculated because of the lack of a market value. Let’s think for example to human lives. There is not a direct “price” in the market to compare with the cost needed for the investment. When considering this kind of investment, there are several indirect benefits to be considered even if the evaluation is more difficult.

Once we have all the economic data necessary to know the OPEX and CAPEX costs of the European Ports Access System, we’ll be able to know, at a very high level, how much the migration or the adaptation to the new system costs, taking in account:

- Components of the existing system which could be reutilised. Every port authority or terminal owner should be able to know more or less which of the existing fixed assets could be reutilised and then to know roughly the investment required implementing the new control access system.

- New investment needed to implement the new security system.

Cost of migration varies from port to port depending on the magnitude of the investment needed to adapt the current access system to the new one.

8.2. IMPACT ASSESSMENT

It is obvious that the impact that a system as the one proposed in the present project may have on European ports is of large magnitude. The EPAIC II project could not be completed without an assessment of such impact, and to that aim is this section devoted.

The most significative inputs for the completion of our task is constituted by the responses to the questionnaire. In its last section, called "future considerations", several questions regarding the impact are raised. Up to the present moment, several answers have been received and some of them contain very precious pieces of information. As said in previous sections, the questionnaires will bring the point of view of different stakeholders, mainly ports but also others.

But the search of information will not be limited to the questionnaires. Several questions will be proposed at the meetings that Isdefe's staff will attend to. And other sources, such as the dedicated literature, will also be used.

The impact assessment will consider several key areas, as was stated in the inception report and which appear in the following paragraphs, expanded to include new aspects.

8.2.1. GENERAL ASPECTS

Some principles will guide EPAIC preparation. Among them, the idea of "trade facilitation" or, more generally, of "operation facilitation" is one of the most important. EPAIC should help professionals working in ports and should ease their work while avoiding imposing new burdens and costs. New procedures should be easier to understand and implement.

The EPAIC system does also fit the demands from many different types of stakeholders. European organisations, international bodies and public security bodies, to list a few, rank among those who at some point have asked for a system such as the one described in the present project. To start with, the International Maritime Organisation has stated that its member States should consider entering into reciprocal agreements to recognise clearances and identity card systems and, moreover, should work towards a common set of characteristics for the cards [20].

The Commission of the European Communities proposed in 2006 the creation of a new figure, that of "secure operator" that would help to enhace security in the supply chain [21]. The status of security operator would be given to firms and individuals capable of complying with some objectives in a similar fashion to EPAIC, in which cards are not given to anyone but to those that show to meet some characteristics.

Public security bodies also highlight the need for systems such as EPAIC. For example, the National Coordinator for Counterterrorism in the Netherlands states that the security chain comprises five links, of which prevention is one of them [22]. Preventive measures avoid direct causes of insecurity, helping organisations to become a less easy target. Some of those preventive initiatives include opening and closing procedures and access policies; limiting the number of entrance points and drawing a key – holder plan, assuring that not everybody can access the premises; electronic access systems and background checks, among many others. As can be easily seen, these recommendations are matched by EPAIC.

The analysis would no be completed without mentioning another groups: projects that had already explained the necessity for acces controls, such as Counterect (funded by the 6th Framework Programme).

8.2.2. LEGAL ASPECTS

The implementation of a system such as the one proposed in EPAIC has many potential legal implications. The EPAIC I project stated many of them so that a great part of the work is already done. However, some remains to be completed, namely questions regarding the use and distribution of personal information.

Part of the legal issues are already solved, since some ports in most countries have already adopted, at least to some extent, the directives about port security or at least are very close to it. Therefore, the possible legal problems arising from the building of physical access systems have already been solved, including those about background checks. But the issues regarding personal data may pose difficulties. Following European directives on data protection, the Member States have set up different agencies and laws that in some cases may be too restrictive for the purposes of a unified access system. For example, some Member States may impose restriction on the distribution to another country of personal information collected within them, so that the creation of a single, unified register might be compromised.

Currently, there are licence and security certificates required for any transport operator all over Europe [23] that can be used as a solid foundation for a central recording and administration of system of transport providers both on member States and on a EU – basis. EPAIC matches such a description and handles certain information for each card holder. From the information acquired through the questionnaire, a conclusion can be drawn: ports in Europe employ a great number of different personal data. The use of so many different items in EPAIC would not only render it too big and too complex to manage, increasing also costs (at least when the databases are considered) and time during enrolment, but they would also bring legal problems. For instance, some pieces of information, such as gender, could be considered as sensitive information in some States. And while some posts and security levels could requiere background checks, there are indeed some barriers which cannot be crossed: medical and criminal records, for example, are non – disclosable to the future employer [24]. Those are the reasons that has driven the decision to include in the EPAIC system the minimum set of data to meet security needs. Adding more information would bring redundances and perhaps a somewhat increased security level, but the associated burdens would be too costly.

EPAIC is also intended to ease the administrative and legal work that companies have to deal with. Let us illustrate this with the following example: if a French road haulier opens a subsidiary in Rome and employs a Maltese driver in a truck with a licence plate from Sweden, many ports would ask for at least three official documents just to test the origin of each of the aforementioned elements and persons, not to talk of the additional papers that could ask for. And this operation might need to be repeated for each different port or even for each time a port is entered. By using Epaic, only some documents would be needed for the registration of the driver, andjust on one occasion, that of the enrolment. From that moment onwards, the card could be used to convey all the necessary information. And some similar initiatives are already in place: Directive 2003/59/EC introduces a compulsory certificate of profesional competence and obligatory additional training once every five years. The similarities between a compulsory certificate and a compulsory card to access ports are striking.

A concrete issue that has been raised on several occasions is that of privacy, mainly in its connection with data transfer among member States. Although in general there is no problem concerning the delivery of individuals' information from member State to member State, somo people could find it not appropriate. There are, however, several European Union – wide systems that already share and store information as that of EPAIC. For example, the visa information system, intended for inmigration purposes and which records alphanumeric data on the applicant, including digitised photographs and biometric prints.

As discussed in the present study, a decision should be taken between establishing a national databases or a single, central one. The former increases costs (up to 27 or even more, with their cost of maintenance and an associated increase in security risks, since there are many more database to attack in order to steal information); the latter could bring about privacy issues as stated above. However there are examples that show that those concerns could be avoided. Eurodac, a system intended to assist in determinig which member State is responsible for examining an asylum application under the Dublin II regulation, bears some resemblance to EPAIC. It is comprised of a unit within the Commission equipped with a computerised central database for comparing the fingerprints of asylum applicants and a system for electronic data transmission between member States and the database. Eurodac stores several items of information for each asylum seeker: fingerprints (as stated before), member State of origin, place and date of the asylum application, sex, reference number, date on which the fingerprints were taken and the date on which data were forwarded to the central unit. That information is sent by the member States to the Commission and entered directly in the database by the central unit. The information that it stores is thus very similar to that of EPAIC and its use is similar to the one proposed in this project.

As can be said, there is a number of legal issues that could put extra complexity on the EPAIC system; however, most of them can be either solvable or have been solved in previous initiatives.

8.2.3. LOGISTICS

The European logistic networks may be benefited from the implementation of a unified access system to ports. To start with, truck drivers would only need to carry – and pay for – a single card, instead of having many for the different ports they visit. That would save the transport industry money and time. It would also broaden the number of ports that a single transport worker may visit and it would also avoid having to undergo several security clearances. And the movement of goods within the European Union could also be improved thanks to a simplified access policy.

However, many questions remain unanswered. For instance, some ports have their own train stations – how should railroad workers be considered? Once more, the questionnaire will be a vital tool in order to find an answer. Its last section will be carefully reviewed in order to extract the position of ports and other stakeholders.

The EPAIC systems aims at bringing easier and faster entry solutions, solving some of the current problems. For example, shipsuppliers, who are the professionals that bring to ships goods to be consumed in them, complain through the Organisation of the European Community Shipsuppliers [19] that security and access requirements vary greatly from port to port. Thus, in some sites when a truck needs to enter the port the driver and the vehicle details have to be provided, while in others it is not necessary. That leads shipsuppliers to ask about the information they have to deliver in each port, wasting precious time. By using the EPAIC system, however, each truck driver would only need to employ a single card in order to give all the relevant information, saving thus time and effort. However, EPAIC should be completed, if possible, with a wider normative in order to specify the procedures. For example, the sema shipsuppliers organisation points out that they have to give notice of their coming to specific ports within a certain amount of time that varies from place to place. EPAIC, as it is currenctly conceived does not give a response to this kind os issue, so that its employ should be completed with a further homogeneisation.

8.2.4. ENVIRONMENTAL IMPACT

A unified European port access system could also have an impact in environment. To start with, the needed infrastructures (card readers, cameras, barriers, etc) represent construction works that in some cases may have a negative impact. But there can also be other effects stemming from the foreseen increment in road traffic entering and exiting ports, since allowing for a faster entrance could also rise the capacity of ports and so more vehicles could enter them.

Apart from fixed assets in each port and the increased traffic, another main issue would be on the vert cards. Although a single one does not bring much trouble, millions of them would be issued each year and, what represents a very high quantity of plastic and other materials that are nor re-used recyclated.

And the database to store the information brings also a certain comsumption of resources (e.g. electricity), much bigger if the decentralised solution is preferred over the central one, since up to 27 databases would be set.

8.2.5. HUMAN AND TECHNICAL RESOURCES

As mentioned before, the access system under study may have a clear impact on the people working in ports. From the lorry driver who will need to undergo a security clearance – neither many, as in the current situation, nor none, as for those who visit non – restricted ports – to the staff that ports will need to hire, many professionals will be affected.

The creation of new access systems and the possible substation of current ones represent a change in technological needs and resources and current employees will have to adapt. Some opposition form the part of those that have done things in different ways for many years can be expected. In fact, the analysis of the questionnaires shows that some ports do not seem inclined towards the adoption of an EPAIC system and some are openly against it. Althoug several reasons may account for, including the fear that ports might lose the authority to deny or allow access (understandable although groundless, since in the proposed model ports retain fully control over those issues) some oppose due to economic matters. Some places have already invested great deals of money on access systems and switching to new ones would increase costs unnecesarily, or so they fear. Some obvious advantages, to name a few, would be an easier interoperability and a lowering of operative burdens for road transport and other stakeholders, which would extent to the whole of the European port community. These and other advantages should be presented to ports reluctant to implementig an EPAIC system.

As has been shown in this study, cards, hardware, software and many other resources would be required or transformed. All of these represent new bussiness opportunities. Some jobs would be created directly (e.g., the officials in charge of card issuance) but the real beneficiaries of the new system would be companies, which would save time and money in administrative issues. The enrolment of personnel and the daily operations would be eased and time would be saved, as many of them demand [19]. This can expectedly lead to a stronger trade system and the possibility for companies to expand their staff, creating new jobs in Europe.

9. Proposed Conceptual Development of a European Port Access System

9.1. Identified Requirements for the System Model

An exhaustive analysis of the main requirements has been performed, taking into consideration the first EPAIC study, the present state of art technologies and products. It has also included consultation results from the port authorities, port facilities parties, transportation and cargo partners and other stakeholders, for instance, SAGMaS meeting which was held in Brussels on October 2010.

The main requirements and conclusions can be summarised in the following guidelines:

- The access control system should be applicable both in a port wide (mandatory and less restrictive) and port facilities level (optional and more restrictive). This will provide a good flexibility when adopting the access control system according to each port necessities, as well as a "Defence in Depth" oriented topology.

- In order to follow the main tendency in most ports, card authentication ("what-I-have factor") is the basic authentication factor. However this basic security level shall be complemented with an extra, optional biometric authentication ("what-I-am" factor) based on hand-scan technologies. This will provide a cost and security requirement flexible approach: only critical port areas and facilities demanding more security shall invest in this extra biometric authentication factor. To make this flexibility possible, all EPAIC cards will be compatible with biometric template digital recording.

- Regarding the card data model:

  - For the optional biometric authentication, holder personal data will not need to be transmitted outside the card, because authentication procedure is match-on-card based.

  - Any further holder personal data will need to be transmitted through card management systems across different countries. System is designed in a way that only card related (and not user related) data need to be transmitted between management systems, being avoided any international personal data transmission.

- Regarding card design:

  - As the base authentication factor is card authentication ("what-I-have" factor), the card design will include physical and logical security measures in order to avoid any card tamper-proofing and cloning technique and card chip data integrity and confidentiality.

  - Card layout will include the most common designs identified in the port consultations performed.

  - The card will be based on MiFare technology, as it is widely used in most ports, and provides a contact less interface as well as compatibility with secure card chip data storage and channel 128 bit AES encryption, with CC EAL4+ Certification.

- Card Lifecycle described in this design will require an enrolment, card production and issuing, renewal and updating, revocation and termination procedures. As it will be seen in the following sections, there will be various differently focused and owned card access control management systems within the present model, but all of them shall fulfil the previous card lifecycle requirements.

- The philosophy of the system model is a collection of integrated access control systems where the security requirements are harmonised and the user only will need one identification card, named EPAIC.

9.2. System Architecture Description

The proposed system architecture comes up from two different aspects deeply analysed during the project: access control system management and holder role nature according to stakeholders’ necessities.

9.2.1. Port and Facility Access Control Factors

Around 85% of ports have port authorities managing and controlling the card access control system. The remaining ports delegate it to private operating port facilities companies or outsource the entire access control system to third parties.

In the latter case, not only one but various ports can be included in the card management system. Moreover, these particular cases of outsourced solutions have been identified in the project as the most reliable and security advanced of all in comparison with port owned systems, offering card control access systems with biometric authentication.

The conclusion of these factors is that forcing a port owned system design as this model system would promote the disappearance of these fully functional, secure outsourced solutions that are working properly nowadays, as well as it would endanger the business continuity of these outsourced parties.

The European model proposal shall achieve flexibility to an easy adaptable system that can be adopted by any port without big impact and migration costs, and maintaining if not improving their current operational performance.

In the same way must be focused on aspects regarding port-wide versus port facility access control system approaches. About half of the consulted ports use both port wide and port facility access control systems; they perform control access to the port and to certain or all port facilities within the port as well.

Thus, both management options shall be available in the proposed architecture: a mandatory port wide access control system point as a first security tier less restrictive, and, for port facilities requiring it, a port-facility-wide access control system point more restrictive.

9.2.2. Divergence of Holder Roles Nature and Necessities

A very important fact that arises from the analysis and feedback received from stakeholder is that most card holders rarely work in two or more different ports, much less in different ports across different EU Member States. A big percentage of users are permanent port workers, being mainly port staff and operating companies’ staff. So the question coming up is, if an European wide access control system - and its bigger cost and investment requirements associated - are really required when a big percentage of users do not really work in several ports, but only in one single port. These users will be referred as “local users”.

On the other hand, there is one holder role left that is considered as very important by stakeholders: transportation workers (cargo truck haulers). These particular users could require access to two or more ports within the EU, which will be referred as “mobile users”. Thus, at least a solution for this particular type of users shall be included in the proposed architecture. The solution can be shared with other mobile profile users, as authorities.

9.2.3. EPAIC I Base Architecture Model

The EPAIC first study analysed different architectures for a European wide system, and selected two candidates to be the most adequate topologies:

- A purely centralised model, where all the data is stored at a central system.
- A hybrid model, combining a central and distributed approach, where data is stored both in central and national systems.

The central model has been discarded due to the following reasons:

- It is not compatible with the development of an initial national system as first step to a European system.
- With the data model proposed in this model, it is required that personal data is transmitted across different EU countries, arising legal issues regarding personal data protection.

Thus, the hybrid model will be the base of the architecture proposal in this study. However, this model will be enhanced and modified in order to fulfil all the requirements identified during the project. In conclusion, this "enhanced hybrid model" can be described as follows:

> *"An adaptable combination of distributed match-on-card and national-centralised access control system compatible with European operation, providing minimal sized data transmission between systems and no holder personnel data transmission between countries."*

9.2.4. PROPOSED ARCHITECTURE MODEL KEY POINTS

The enhanced hybrid model selected as the proposed architecture model is based on the following key aspects:

1. All the authentication process is match-on-card, including biometric authentication, if available. This means that personal data will not be transmitted from the card-reader to any external system in the authentication process.
2. Ports have a Defence-in-Depth based control access systems conformed by two tiers: a mandatory port-wide tier less restrictive and optional port-facility-wide tiers for each port facility operating party requiring extra security measures.
3. The architecture is based mainly in two different and integrated card management systems: local port system (local users aimed) and European system (mobile users aimed). It will be allowed an outsourced card management system that could manage the ID card for a close group of ports including their local users and even some of their mobile users. This outsourced system can be viewed as an aggregated ports system.
4. Access rights management will be kept solely under responsibility of port authorities (port wide access control tier) and port facilities operating companies (any existing port facility wide access control tiers).
5. Every member state will count with a national system used in the European card management system. These national systems will be interconnected, but personal data of the car holders stored in these systems will not be transmitted between member states.
6. Furthermore, card holder data doesn't need to be transmitted from central systems to any other external system.

9.2.5. Integrated Card Management Systems

The proposed architecture is based on three different and integrated card management systems: local port system (local users aimed), outsourced system (close group of local users and mobile users aimed) and European system (for mobile users aimed). These systems will be referred in the present document as Card Management System (CMS).

The complete architecture of this three way CMS's approach can be found in the following figure:

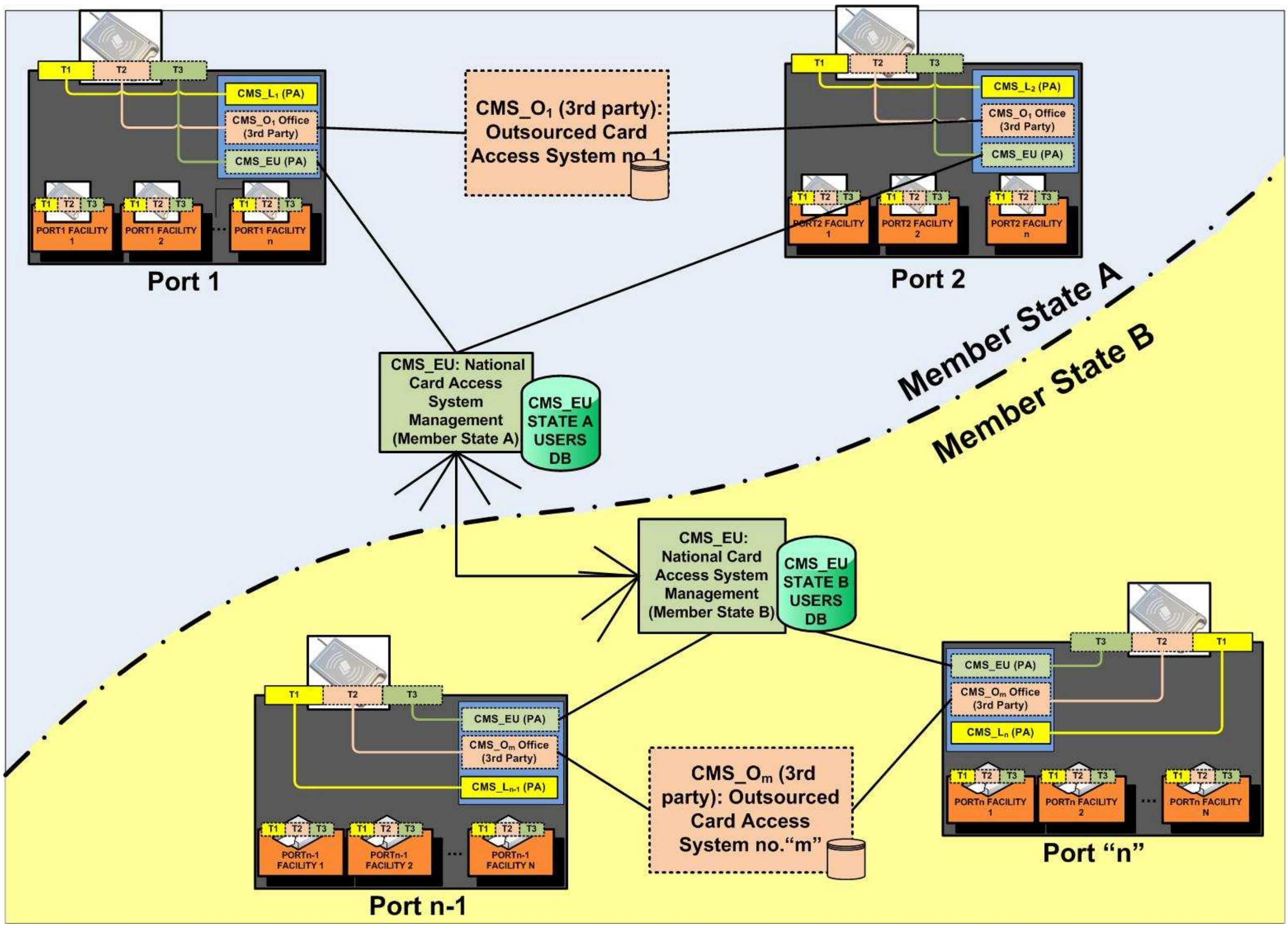


Figure 53 Overview of the Integrated Card Management Systems

9.2.5.1. Local Port Card Management System (CMS_L)

Port CMS (named CMS_L) is mandatory, and it is owned and managed by Port Authority. This access control system will be at least applied on the port entrance perimeter (port-wide security tier). However, any port facility requiring further access control points can deploy CMS_L compatible readers and request card application for their users (port staff or company workers which require access to that facility), conforming a second, port-facility-wide tier. This second tier is, therefore, optional.

Port Authority, responsible of CMS_L operation, shall develop not only a card operational access control system (operational authentication and right access processes), but also a card lifecycle infrastructure capable of managing card application, in-house production and deliver, as well as card renewal, upgrading, revocation and termination implemented procedures. This arise the following requirements that a Port Authority owned CMS_L shall met:

- Port Authority needs a IT infrastructure capable of:
  - Maintaining a secure cardholder user database system that ensures personal data confidentiality, integrity and required availability.
  - Processing new user registrations and deletions. Any user deletion shall imply automatic secure deletion of user holder personal data from any system of this infrastructure.
  - Providing the system administrators (port authority for port-wide tier and facility administrator for port-facility-wide tier) an interface capable of managing and modifying holder user access rights in every applicable area.
  - Automatically check cards expiration state and block any expired card.
  - Assuring that only authorised administrators can access to their assigned data and management capabilities.
  - Allowing authorised staff to modify only pertinent data inside card chip due to card renewal or upgrading needs.
- Personal data stored in cards shall not be transmitted from readers to external CMS_L system (or any other external system), particularly in case of biometric templates, as biometric authentication must be performed in a match-on-card authentication model.
- Port authority shall provide a physical point nearby, where card related request could be performed: new enrolment requests and registration, card renewal, replacement and upgrading, and card termination and revocation requests.
- Port authorities need an infrastructure for card production and issuing capable of:
  - Complete the entire card issuing process within two working days.
  - Produce or print cards with physical security measures that minimise any tamper proof or cloning attack procedure.
  - Guarantee that only authorised and security checked port staff can access to these infrastructures and the produced cards.
  - Storing and deliver cards in a secure way.
  - Instantly produce one day use cards, applicable for visitors and those users whose card has been stolen, forgotten or damaged.
- For port-wide access control tier, access rights must be managed only by port authority responsible personnel. Valid and non expired cards shall permit port access to any user under normal circumstances. However access rights could be temporary or permanently modified when:
  - Card has expired and access rights must be consequently revoked. This change shall be automatically performed when card expiration limit is reached.
  - Card has been renewed and access rights must be consequently restored. These changes shall be automatically performed once the renewed card has been delivered to the holder.

   - Holder is not a user anymore, and card is terminated, so access rights must be consequently revoked. This change shall be automatically performed when card termination/revocation procedure is executed.
   - Card is upgraded or modified in some authorised way, and this upgrade/modification implies access rights updating as well. These changes do not need to be automatically performed.
   - Port access policies changes (non normal operation is set, as for example ISPS Code 2 and 3 security levels measures). This operational context (emergencies or unusual situations) may require access right restrictions for many if not all users. Card access rights management can be a useful tool to fast and effectively apply and execute these security restrictions measures. Moreover, these port emergency awareness access rights restrictions could be automated.

- For port-facility-wide secondary access control tier, access rights must be managed only by those entities responsible of the security of the covered area (this is, the facility operating company security responsible or port authority security responsible for that port area). In case that access rights are being managed by port facility operating companies, they shall not use any private CMS, but the port internal CMS_L, by registering their security responsible personnel as administrators of their particular user's access rights in the CMS_L. In other words, port facility administrators authorised by the facility operating company can manage access right of users accessing that facility. Port authority may be, if agreed by all parties, a second administrator entity of these access rights, if preferred.

  Any holder user whose card permits to access a port facility MUST have valid access rights to access the port (this is, must have port-wide -tier 1- valid access rights).

  Valid and non expired cards shall permit port facility access to any authorised user under normal circumstances. However access rights could be temporary or permanently modified when:

   - Card has expired and access rights must be consequently revoked. This change shall be automatically performed when card expiration limit is reached.
   - Card has been renewed and access rights must be consequently restored. These changes shall be automatically performed once the renewed card has been delivered to the holder.
   - Holder is not a user anymore, and card is terminated, so access rights must be consequently revoked. This change shall be automatically performed when card termination/revocation procedure is executed.
   - Card is upgraded or modified in some authorised way, and this upgrade/modification implies access rights updating as well. These changes do not need to be automatically performed.
   - Port or Port facility access policies changes (non normal operation is set, as for example ISPS Code 2 and 3 security levels measures). This operational context (emergencies or unusual situations) may require access right restrictions for many if not all users accessing the port facility. Card access rights management can be a useful tool to fast and effectively apply and execute these security restrictions measures. Moreover, these port emergency awareness access rights restrictions could be automated.

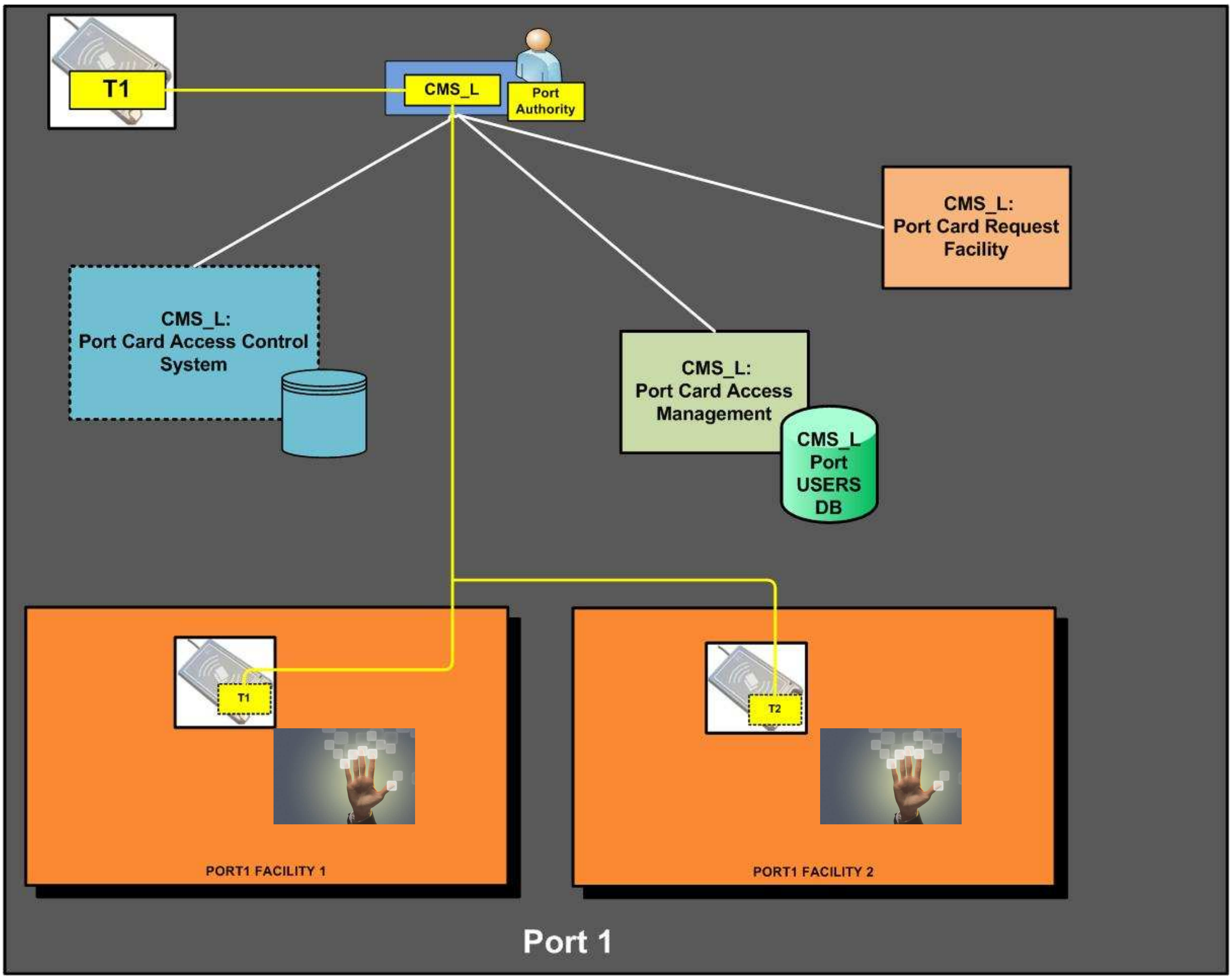

T1
CMS_L
Port Authority
CMS_L: Port Card Request Facility
CMS_L: Port Card Access Control System
CMS_L: Port Card Access Management
CMS_L Port USERS DB
T1
T2
PORT1 FACILITY 1
PORT1 FACILITY 2
Port 1

Figure 54 Overview of the Local Port Card Management System

9.2.5.2. OUTSOURCED CARD MANAGEMENT SYSTEM (CMS_O)

The outsourced CMS (CMS_O) is optional, and it is intended for those ports where currently the card management system is outsourced to third parties. CMS_O is owned and managed by third parties. This system will be supplied by these third parties to either port authorities (to be applied in port-wide tier or port authority dependant facilities) or private companies operating in port facilities that request the service. These two parts will be referred as users of the providing CMS_O party.

Also, the outsourced solution could be applicable to more than one port alone, and be used by several ports nearby, or even distant ports requesting the service, if the organisation providing it is capable of so.

To synthesise, the key factor in CMS_O is that ports and companies operating in port facilities can outsource, as clients of third parties, the deployment of the Card Management System, as long as the system provided fulfil the requirements described in this document (which are applicable to all CMS defined in this section by default), and summarised in the following points:

- CMS_O must use EPAIC cards, and all the security, design, interface and operational specifications defined in this proposal for these cards.

- CMS_O providing party shall develop not only a card operational access control system (operational authentication and right access processes) according with port authority and port facilities needs, but also a card lifecycle infrastructure capable of managing card application, production and deliver, as well as card renewal, upgrading, revocation and termination implemented procedures.
- Providing party must rely the CMS_O on a IT infrastructure capable of:
  - Maintaining a secure card holder database system that ensures personal data confidentiality, integrity and required availability.
  - Processing new card holder registrations and deletions. Any user deletion shall imply automatic secure deletion of user holder personal data from any system of this infrastructure.
  - Providing the authorised users (port authorities and facility operating companies) an interface capable of managing and modifying holder user access rights in every applicable area (port wide tier and port facility tiers).
  - Automatically check cards expiration state and block any expired card until it is renewed.
  - Assuring that only authorised administrators can access to their assigned data and management capabilities.
  - Allowing user's authorised staff to manage or request modification of only pertinent data inside card chip due to card renewal or upgrading needs.
- Sensible holder data stored in cards shall not be transmitted from readers to external CMS_O systems or any other external system, particularly in case of biometric templates, as biometric authentication must be performed in a match-on-card authentication model.
- CMS_O providers shall count with a physical point nearby in every port where service is deployed. In this provider facilities card related request can be performed: new enrolment requests and registration, card renewal, replacement and upgrading, and card termination and revocation requests.
- CMS_O providers need an infrastructure for card production and issuing capable of, for each port served:
  - Complete the entire card issuing process within two working days.
  - Produce or print cards with physical security measures that minimise any tamper proof or cloning attack procedure, as defined in this proposal later.
  - Guarantee that only authorised and security checked own staff can access to these infrastructures and the produced cards.
  - Store, transport and deliver cards in a secure way.
  - Instantly produce one day use cards, applicable for visitors and those card holders whose card has been stolen, forgotten or damaged.
- Port-wide access control tier can be only provided to port authority users.
- Valid and non expired cards shall permit port access to any card holder under normal circumstances. However access rights could be temporary or permanently modified when:
  - Card has expired and access rights must be consequently revoked. This change shall be automatically performed when card expiration limit is reached.

  - Card has been renewed and access rights must be consequently restored. These changes shall be automatically performed once the renewed card has been delivered to the holder.

  - Card holder has not access anymore, and card is terminated, so access rights must be consequently revoked. This change shall be automatically performed when card termination / revocation procedure is executed.

  - Card is upgraded or modified in some authorised way, and this upgrade/modification implies access rights updating as well. These changes do not need to be automatically performed.

  - Port access policies changes (non normal operation is set, as for example ISPS Code 2 and 3 security levels measures). This operational context (emergencies or unusual situations) may require access right restrictions for many if not all users. Card access rights management can be a useful tool to fast and effectively apply and execute these security restrictions measures. Moreover, these port emergency awareness access rights restrictions could be automated.

- For port-facility-wide secondary access control tier, access rights management must be performed or requested only by those client entities responsible of the security of the covered area (this is, the facility operating company security responsible or port authority security responsible for that port area). In other words, port facility CMS_O administrator users authorised by the facility operating company and the provider party can manage access rights of users accessing that facility. As a special type of client, only Port authority can be, if agreed by all parties, a second CMS_O user administrator of these access rights, if preferred.

  Valid and non expired cards shall permit port facility access to any authorised card holder under normal circumstances. However access rights could be temporary or permanently modified when:

  - Card has expired and access rights must be consequently revoked. This change shall be automatically performed when card expiration limit is reached.

  - Card has been renewed and access rights must be consequently restored. These changes shall be automatically performed once the renewed card has been delivered to the holder.

  - Card holder has not access anymore, and card is terminated, so access rights must be consequently revoked. This change shall be automatically performed when card termination / revocation procedure is executed.

  - Card is upgraded or modified in some authorised way, and this upgrade/modification implies access rights updating as well. These changes do not need to be automatically performed.

  - Port or Port facility access policy changes (non normal operation is set, as for example ISPS Code 2 and 3 security levels measures). This operational context (emergencies or unusual situations) may require access right restrictions for many if not all users accessing the port facility. Card access rights management can be a useful tool to fast and effectively apply and execute these security restrictions measures. Moreover, these port emergency awareness access rights restrictions could be automated.

- Card holder data between CMS_O clients (port authorities and operating companies) shall be never shared, or accessible by any other client than the legitimate card holder responsible client entities. For example, if two port facilities in the same or different ports are users of a CMS_O, data of card holders of each one must be secured to assure management independence, confidentiality and integrity.

- Regarding the previous point, the only exceptions shall be permitted when:
  - Card holders are accessing to various client ports.
  - Card holders are accessing to various client port facilities operating companies in the same or different ports.
  - There is an agreement between clients that permits card holder data sharing/management through CMS_O.
- Responsibility or cost assumption of any other infrastructures required by the system (basically, card readers installation and its IT and network infrastructure associated) are not scoped by this model. However, these infrastructures must meet the requirements:
  - EPAIC CMS_O card compatible.
  - If used, biometric compatible with biometric authentication procedures and design used in the present proposal (hand-scan technologies, match-on-card model, etc.).
  - Security measures required: readers must not transmit any personal data to external systems of any kind.
- If the party providing the CMS access control system has clients in more than one EU member state, same requirements as the CMS_EU system about European holder data transmission will apply. These are fully detailed in the data model section of this proposal.

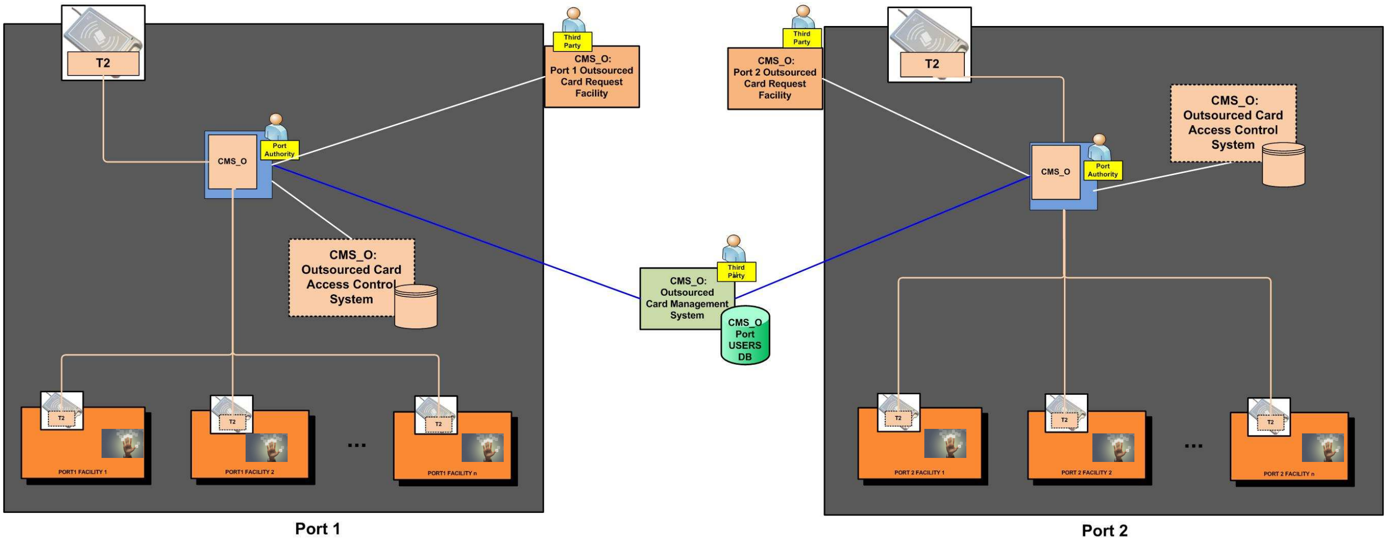


Figure 55 Overview of Outsourced Card Management System

9.2.5.3. EUROPEAN CARD MANAGEMENT SYSTEM (CMS_EU)

The European CMS (CMS_EU) is mandatory and unique. This system is European scoped, and is intended for mobile EPAIC card holder users needing to move frequently from/to distant ports. Thus, a CMS_EU will permit a mobile user to be authenticated by any port which has adopted this system.

Again, either port authorities (to be applied in port-wide tier or port authority dependant facilities) or private companies operating in port facilities can request to deploy and use a CMS_EU based control access system. These two parts will be referred as clients or users of the CMS_EU control access system.

Although CMS_EU existence is mandatory, ports and port facilities operating companies do not need to associate to it as users. This is recommended for ports where there is not any mobile card holder type. For port facilities operating companies willing to use CMS_EU, they can apply for being CMS_EU user only if the port itself is an associated CMS_EU user. This is because CMS_EU system architecture end points are the ports themselves, and this point are managed by port authorities as part of the CMS_EU system.

A collateral benefit of the CMS_EU design is that it is not only applicable to ports, but to any infrastructure requiring control access for mobile card holders. Thus, for example, a cargo truck hauler could be authenticated through CMS_EU in ports, logistic companies, products manufacturers, or any party involved in the cargo transportation chain, all them distributed anywhere in the EU, just by being CMS_EU associated users.

The CMS_EU architecture design is outlined in the following figure:

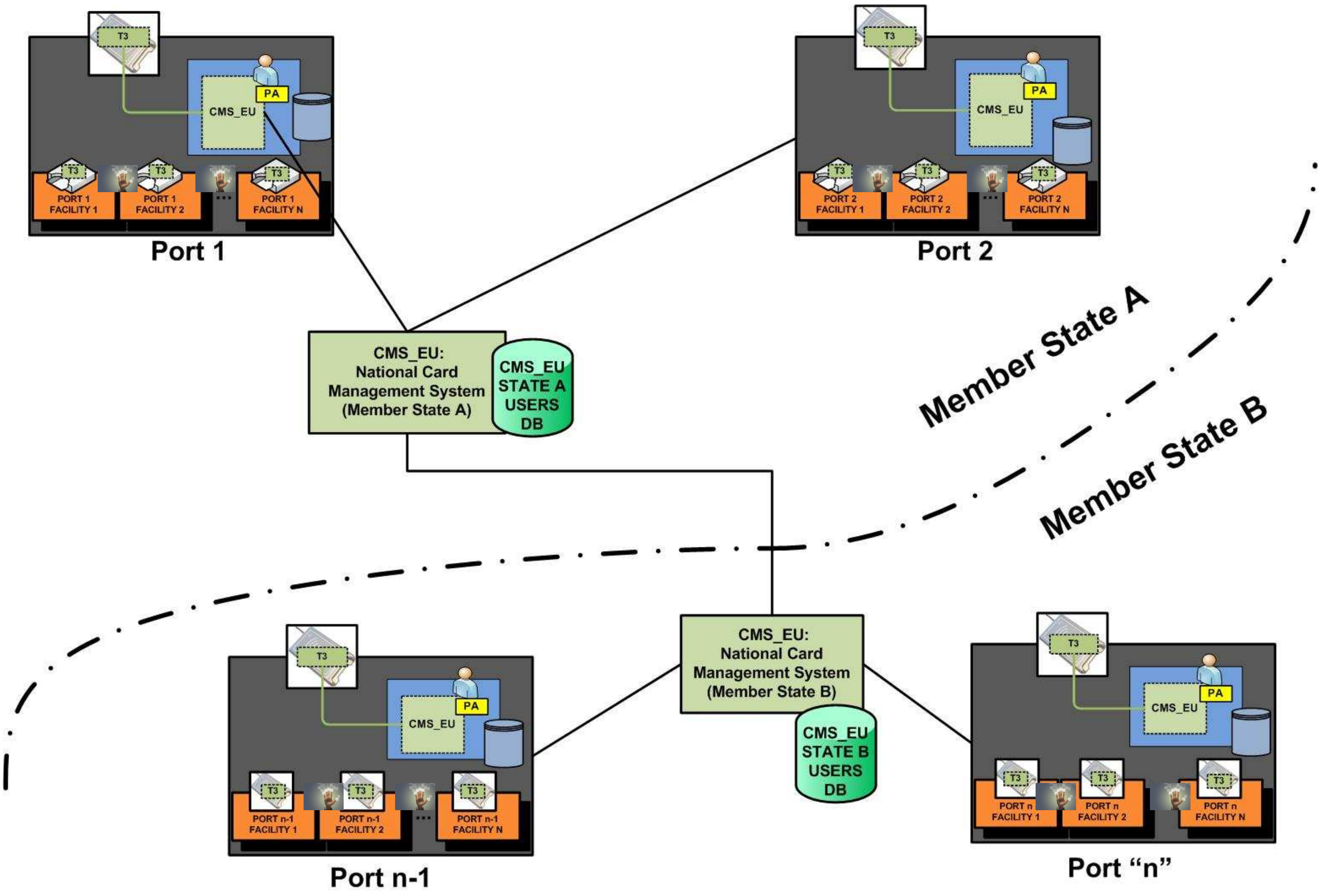


Figure 56 Overview of European Card Management System

CMS_EU shall meet the following requirements:

- As it was said before, in the model proposed, all CMS_EU associated users (ports and companies operating in their facilities) will manage and use the system through a port placed CMS_EU end point which will be under the own port authority responsibility. Port can be seen as a CMS_EU user (port card holders using the system) and as a CMS_EU conforming part (port authority managing the CMS_EU endpoint in the port).

- CMS_EU will be applicable in both port-wide perimeter tier and port-facility-wide secondary tiers.

- All port CMS_EU endpoint systems will be connected with one (or more, if replication is needed due to performance or backup purposes) national systems. Those national systems are the only point where personal data of card holders of that member state will be stored.

- All national systems will be connected together. The network topology could be as follows:

  - Distributed national systems connections: distributed point to point topology model.

  - All national systems connected with a central node: centralised topology model.

- Data and functional models are not affected by choosing one specific topology model, as the central node in the centralised topology alternative shall only work as a forwarding point, with no data storage, management or functionality at all.

- CMS_EU shall not transmit any card holder personal data to any external system: card holder data is securely stored in the CMS_EU national database of the EU state member where the card holder applied for the card. This personal data is exclusively and securely transmitted from the port CMS_EU endpoint to its national database system during the enrolment process, once.

- Access right management is completely up to users (port authorities and port operating companies). CMS_EU will only provide authentication procedures.

Port authority is responsible of the CMS_EU port end point operation, and shall develop not only a card operational access control system (operational authentication and right access processes), but also a CMS_EU card lifecycle infrastructure capable of managing card application, in-house production and deliver, as well as card renewal, upgrading, revocation and termination implemented procedures, that shall be initiated in the port endpoint and further processed in the necessary national systems. This arise the following requirements that a Port Authority owned CMS_EU endpoint shall met:

- Port authorities need a IT infrastructure capable of:

  - Initiating new user registrations and deletions procedures and get acknowledge of the procedure result from national systems. Any user deletion shall imply automatic secure deletion of user holder personal data from any system of this infrastructure.

  - Providing the system administrators (port authorities for port-wide tier and facility administrators for port-facility-wide tier) an interface capable of managing and modifying holder user access rights in every applicable area.

  - Automatically check cards expiration state through national system information request and block any expired card until it is renewed.

  - Assuring that only authorised administrators can access to their assigned data and management capabilities.

  - Allowing authorised staff to modify only pertinent data inside card chip due to card renewal or upgrading needs.

  - Establish communications or transmit the required data (see data model section) to national systems in a secure way that ensure confidentiality, availability and integrity of data.

  - Establish communications or transmit the required data (see data model section) to national systems with the speed and latency required to a proper system operation.

- Sensible holder data stored in cards shall not be transmitted from readers to external CMS_EU systems (or any other external system), particularly in case of biometric templates, as biometric authentication must be performed in a match-on-card authentication model.

- Port authorities, as CMS_EU end point responsible owner, shall provide a physical point nearby, where card related request could be performed: new enrolment requests and registration, card renewal, replacement and upgrading, and card termination and revocation requests.

- Port authorities need an infrastructure for card production and issuing capable of:

  - Complete the entire card issuing process within two working days.

  - Produce or print cards with physical security measures that minimise any tamper proof or cloning attack procedure, as defined in this proposal later.

  - Guarantee that only authorised and security checked port staff can access to these infrastructures and the produced cards.

  - Storing and deliver cards in a secure way (protected storing and logistics for cards).

  - Instantly produce one day use cards, applicable for visitors and those users whose card has been stolen, forgotten or damaged.

Regarding access rights management (which is not part of the CMS_EU access control system), same requirements set for CMS_L shall be applied:

- For port-wide access control tier, access rights must be managed only by port authority responsible personnel. Access rights could be temporary or permanently modified when:

  - Card has expired and access rights must be consequently revoked. This change shall be automatically performed when card expiration limit is reached.

  - Card has been renewed and access rights must be consequently restored. These changes shall be automatically performed once the renewed card has been delivered to the holder.

  - Holder is not a user anymore, and card is terminated, so access rights must be consequently revoked. This change shall be automatically performed when card termination/revocation procedure is executed.

  - Card is upgraded or modified in some authorised way, and this upgrade/modification implies access rights updating as well. These changes do not need to be automatically performed.

  - Port access policies changes (non normal operation is set, as for example ISPS Code 2 and 3 security levels measures). This operational context (emergencies or unusual situations) may require access right restrictions for many if not all users. Card access rights management can be a useful tool to fast and effectively apply and execute these security restrictions measures. Moreover, these port emergency awareness access rights restrictions could be automated.

  - Also, access rights could be set specifically upon card holder arrival to port whenever it is necessary. The card holder access must be expected and access rights shall be set to granted prior to actual arrival to port. In the same way, access right could be set to “access denied” state once the card holder has finished tasks and leaved the port.

- For port-facility-wide secondary access control tier, access rights must be managed only by those entities responsible of the security of the covered area (this is, the facility operating company security responsible or port authority security responsible for that port area). Port facility administrators authorised by the facility operating company can manage access right of users accessing that facility. Port authority may be, if agreed by all parties, a second administrator entity of these access rights, if preferred.

Any holder user whose card permits to access a port facility MUST have valid access rights to access the port (this is, must have CMS_EU port-wide -tier 1- valid access rights).

Valid and non expired cards shall permit port facility access to any authorised user under normal circumstances. However access rights could be temporary or permanently modified when:

- Card has expired and access rights must be consequently revoked. This change shall be automatically performed when card expiration limit is reached.
- Card has been renewed and access rights must be consequently restored. These changes shall be automatically performed once the renewed card has been delivered to the holder.
- Holder is not a user anymore, and card is terminated, so access rights must be consequently revoked. This change shall be automatically performed when card termination/revocation procedure is executed.
- Card is upgraded or modified in some authorised way, and this upgrade/modification implies access rights updating as well. These changes do not need to be automatically performed.
- Port or Port facility access policies changes (non normal operation is set, as for example ISPS Code 2 and 3 security levels measures). This operational context (emergencies or unusual situations) may require access right restrictions for many if not all users accessing the port facility. Card access rights management can be a useful tool to fast and effectively apply and execute these security restrictions measures. Moreover, these port emergency awareness access rights restrictions could be automated.
- Also, access rights could be set specifically upon card holder arrival to port facility whenever it is necessary. The card holder access must be expected and access rights shall be set to granted prior to actual arrival to port. In the same way, access right could be set to "access denied" state once the card holder has finished tasks and leaved the port facility.

9.2.6. AUTHENTICATION FACTORS

Based on the port necessities identified during the stakeholder consultations, the following key aspects have been concluded:

- Most ports and facilities rely on single card authentication ("what-I-have" factor).
- Most ports do not have biometric authentication infrastructures available, as they do not see biometrics as necessary, in general terms, for a secure operation.
- However, biometric authentication or any other authentication factor layer is seen as a good improvement for critical areas or facilities (for instance, restricted areas).
- A secure single card authentication system requires security measures which ensure that card can not be cloned, tamper-proofed or spoofed by any means. Card data stored in chip must be protected as well, ensuring its confidentiality and integrity.

- Most ports rely on card that does not meet the previous requirement: card security measures are, therefore, a critical factor. Requirements for this are fully detailed in the Card design and security requirements.

- Based on the firs EPAIC study, the current port applying biometric authentication, the study of impact of port environment in biometric devices and card holder use operational an personal impact, the most suitable biometric authentication for this purpose seems to be the hand-scan, and fingerprint reader as secondary option.

These points have led to a two layer authentication factor design that will be described in the following subsections.

9.2.6.1. Mandatory Authentication Factor ("What I Have")

The EPAIC card will be presented during the checks is a currently valid, authentic EPAIC access card. However, this will not validate that the person holding the card is the legitimate card holder. For this task, additional authentication or validation procedures and checks shall be performed, as for example biometric authentication or visual verification through card surface holder picture check or video surveillance images.

Card authentication factor is performed through a card unique ID assigned and recorded inside card chip during the issuing process. When checking against a card reader, card will provide its unique ID, whose validity will be requested to the pertinent CMS card holder database. This request will be responded with the information regarding card authenticity and current validity (i.e., card is registered, no expired and currently activated and not blacklisted). This authentication factor will be mandatory for any control access system deployed in the port-wide tier.

This EPAIC CMS database can be considered as a secure and trusted source, so this information received is reliable enough to guarantee card authenticity and validity, as long as this database or card itself has not been manipulated or cloned in some way.

The first assumption is unlikely to be possible if the CMS infrastructure is tied to a basic set of security measures, which will be described later in this proposal.

The second assumption, card manipulation, tamper-proofing or card cloning, arises a higher and more probable risk for the system security. Thus, specific security requirements and measures for the card are a must in the design proposed. These measures will be:

- Card physical security measures to avoid card tamper-proofing or physical cloning.

- Card data logical security measures to protect, through encryption, data stored inside card chip (card unique ID included) and all the transmission interfaces (contact less encrypted transmission channels).

9.2.6.2. Optional Authentication Factor ("What I Am")

This additional factor is optional and intended for those CMS users requiring improved security access control (restricted areas, hazardous cargo, etc.). In combination with the mandatory card authentication, both of them provide a very secure two-factor authentication access control.

Biometric user authentication compatibility requires two requirements for any EPAIC card to be issued:

- Card chip will contain at least one biometric minutia.

- This biometric data will be securely stored in card chip and transmitted to reader through secure encryption. Biometric minutiae shall be kept always encrypted, included during the biometric authentication procedure taken place in the card reader.

And, for any party deploying an EPAIC access control system with biometric authentication factor will require:

- Card readers with EPAIC card compatible biometric readers. Shall be capable of establishing secure channels to retrieve biometric minutiae hashes from card, and perform the check without decrypting the minutiae. This is, reader shall hash and encrypt the person’s biometric sample taken from the biometric reader, and compare it with the already hashed and encrypted minutiae.

- Security measures applied to readers in order to avoid any biometric data leakage to external systems during authentication process.

- For card production and enrolment process responsible: biometric readers and systems capable of reading biometric samples, hashing them into biometric minutiae and recording them inside the card chip.

Biometric authentication procedure will follow these steps:

1. Card authentication takes place. Card is successfully checked.

2. Without releasing the card out from the reader range, card holder biometrics is asked to be acquired. Holder provides the sample in the card reader biometric reader. Sample is hashed into an encrypted minutia with the proper CMS EPAIC key (see sections 6 and 7 for further information), conforming the first required data element in the process.

3. Card reader establishes a secure encrypted channel with card (if not already established in the previously performed card authentication procedure). Biometric minutiae hash is retrieved as the second data element.

4. Both data elements are compared for match. If elements match, the person is authenticated as the legitimate card holder.

5. Both data elements are securely erased from the card reader.

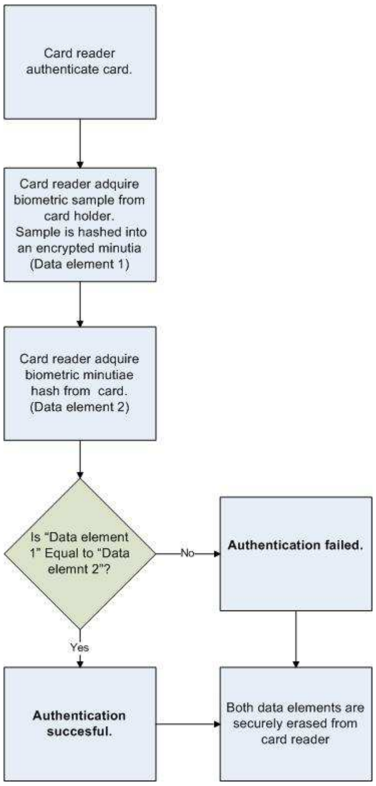

Card reader authenticate card.
Card reader adquire biometric sample from card holder. Sample is hashed into an encrypted minutia (Data element 1)
Card reader adquire biometric minutiae hash from card. (Data element 2)
Is "Data element 1" Equal to "Data elemnt 2"?
No
Authentication failed.
Yes
Authentication succesful.
Both data elements are securely erased from card reader

Figure 57 Biometric authentication procedure

Hand scan is selected as the more proper technology for biometric authentication processed in the context of maritime control access system. The first EPAIC study already pointed hand scan as one of the most adequate alternative to the design.

The main reasons for choosing hand scan as the most adequate alternative in biometrics are:

1. It is compatible with harsh environments like those present in most ports.
2. Authentication procedures and readers are fast enough to be applied for cargo gate control access.
3. It is user friendly and minimally invasive for the individuals using it (unlike iris scan).
4. It is surprisingly accurate even in the worst operation conditions (humidity, greasy or dirty hands, etc.), unlike the fingerprint scanner.

9.3. CARD HOLDER ROLES

Each user will be a card holder of a different CMS, and only one, depending on the required profile:

1. Local port card holder (CMS_L and CMS_O)
2. It is a profile that requires access to a single port. Port staff, port authority personnel, people employed by port facility operating companies.
3. Aggregated ports card holder (CMS_O)
4. It is a profile that requires access to a closed group of ports. Some port staff, some people employed by port facility operating companies and some transportation workers.

5. Mobile card holder (CMS_EU)

6. It is a profile that requires access to several ports in a frequent basis, including ports placed in different countries within Europe. Transportation workers and national / European authorities.

9.4. DATA MODEL

9.4.1. GENERAL AND SPECIFIC REQUIREMENTS FOR CMS_L

A CMS_L local office facility shall be available in the port perimeter, or nearby, to perform enrolments, card renewal, card updates, card termination and card revocation procedures. Only during the enrolment process the holder personal data is transmitted from the CMS_L local office system to holder database inside the port.

Update process is not intended to change any holder personal data, unless mistakes or data corruption which may have happened during the enrolment procedure.

Requests for renewal, termination and revocation do not imply transmission of any kind of holder personal data, just the holder card unique id and any document or information required by the card lifecycle procedures.

Card revocation and termination must imply the deletion of any holder personal data from all systems in the CMS_L. This is, from the holder database and any backup database it could have.

For further information about the holder data required in the enrolment process, see section 9.4.5.1 about enrolment holder data requirements.

9.4.1.1. CARD AUTHENTICATION

1. Card is presented at the card reader by holder.

2. Card and card reader authenticate each other through a pre-shared symmetric key challenge response procedure. A secure encrypted channel is created.

3. Card unique ID is retrieved from card. Optionally, further data stored inside the card shall be retrieved upon user requirements: card holder name, card holder employer, expiry date, etc.

4. Reader request access permission for that card ID to the pertinent CMS in the port:

   - For CMS_L, the management system and holder database owned by port authorities.

   - For CMS_O, the management system owned by the outsourced party providing the card management system. See section 9.4.2 for further details.

   - For CMS_EU, the CMS_EU management system owned by the port authorities. See section 9.4.3 for further details.

5. Reader receives response from the pertinent CMS local system allowing or denying access to that card ID. Optionally, status message could be attached. Examples:

   - Access granted: OK

   - Access denied: invalid card ID.

- Access denied: card does not have permissions to access to that area.
- Access denied: expired card.
- Access denied: CMS error.

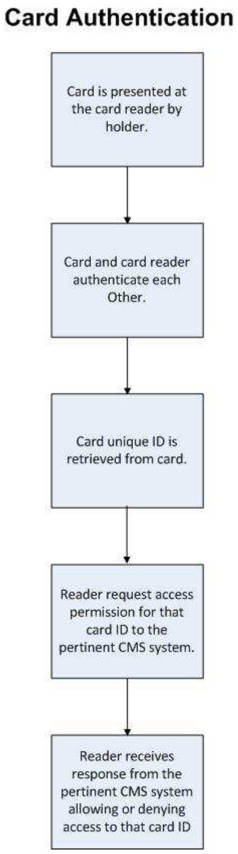

Card Authentication
Card is presented at the card reader by holder.
Card and card reader authenticate each Other.
Card unique ID is retrieved from card.
Reader request access permission for that card ID to the pertinent CMS system.
Reader receives response from the pertinent CMS system allowing or denying access to that card ID

Figure 58 Card authentication

9.4.1.2. BIOMETRIC AUTHENTICATION

1. Card authentication is performed before.
2. Reader retrieves biometric sample from holder, through biometric reader interface.
3. Reader retrieves biometric minutiae from card through the contact less secure encrypted channel between card and card reader.
4. Matching and authentication is performed.
5. Once finished, all the data is erased from reader.

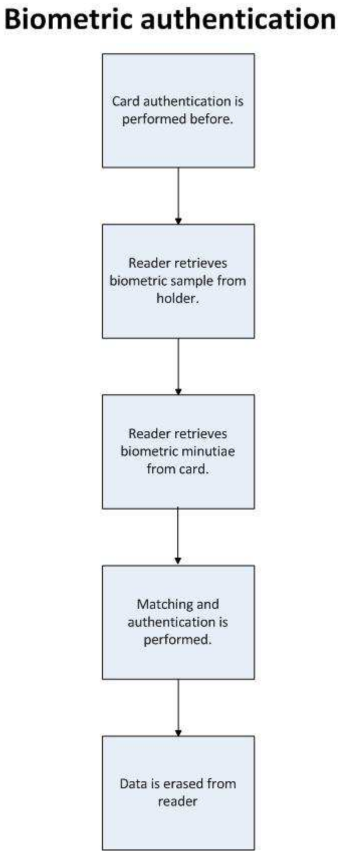

Biometric authentication
Card authentication is performed before.
Reader retrieves biometric sample from holder.
Reader retrieves biometric minutiae from card.
Matching and authentication is performed.
Data is erased from reader

Figure 59 Biometric authentication

9.4.2. REQUIREMENTS FOR CMS_O

A CMS_O local office facility shall be available in the port perimeter, or nearby, to perform enrolments, card renewal, card updates, card termination and card revocation procedures. Only during the enrolment process the holder personal data is transmitted from the CMS_O local office system to the outsourced service provider holder database.

Update process is not intended to change any holder personal data, unless mistakes or data corruption which may have happened during the enrolment procedure.

Requests for renewal, termination and revocation do not imply transmission of any kind of holder personal data, just the holder card unique id and any document or information required by the card lifecycle procedures.

Card revocation and termination must imply the deletion of any holder personal data from all systems in the CMS_O. This is, from the provider holder database and any backup database it could have.

For further information about the holder data required in the enrolment process, se section 4.5.1 about enrolment holder data requirements.

9.4.2.1. CARD AUTHENTICATION

When reader request access permission for a card ID, the CMS_O local system deployed in the port will act as a forwarding point to the CMS_O system where the holder database is actually held (typically, the

CMS_O provider company databases). In this database is stored all data about card holder, currently assigned access rights, and card expiry and validity information; and where a response and status message can be generated.

This proposed data model searches to be as similar as possible for the three EPAIC CMS. Thus, the data transmissions from the CMS_O local port system and CMS_O main provider party system (holder database) must meet the same security requirements set for CMS_L data transmissions.

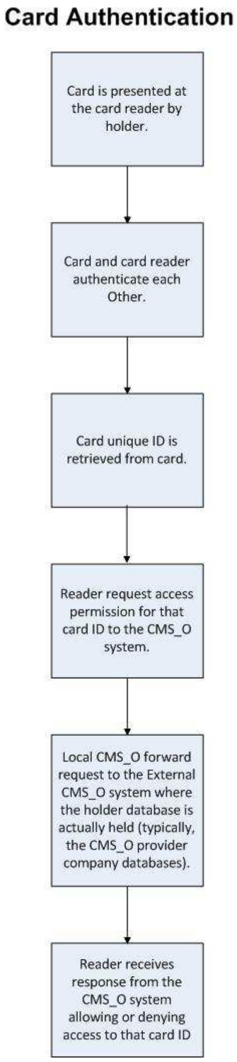

Card Authentication
Card is presented at the card reader by holder.
Card and card reader authenticate each Other.
Card unique ID is retrieved from card.
Reader request access permission for that card ID to the CMS_O system.
Local CMS_O forward request to the External CMS_O system where the holder database is actually held (typically, the CMS_O provider company databases).
Reader receives response from the CMS_O system allowing or denying access to that card ID

Figure 60 Card authentication - CMS_O

9.4.3. Requirements for CMS_EU

A CMS_EU local office facility shall be available in the port perimeter, or nearby, to perform enrolments, card renewal, card updates, card termination and card revocation procedures. Only during the enrolment process the holder personal data is transmitted from the CMS_EU local office system to it assigned national system holder database.

Update process is not intended to change any holder personal data, unless mistakes or data corruption which may have happened during the enrolment procedure.

Requests for renewal, termination and revocation do not imply transmission of any kind of holder personal data, just the holder card unique id and any document or information required by the card lifecycle procedures.

Card revocation and termination must imply the deletion of any holder personal data from all systems in the CMS. This is, from the proper national holder database and any backup database it could have.

For further information about the holder data required in the enrolment process, see 9.4.5.1 about enrolment holder data requirements.

9.4.3.1. CARD AUTHENTICATION

When reader request access information about a card ID, the CMS_EU local system deployed in the port will act as a forwarding point to the CMS_EU system where the holder database may be actually held: a CMS_EU national system. In this point, two different situations may arise:

1. The card ID requested is present in the holder database in this central system. This means that the holder enrolled in the same country as the port requesting for card ID access permission.

2. The card ID requested is not found assigned to any holder in the holder database in this central system. The request is forwarded to the pertinent CMS_EU national system.

In both cases, the CMS_EU databases will not contain data about access rights of users to port areas. CMS_EU holder databases in the national systems are slightly different to CMS_L and CMS_O holder databases. The first are intended to provide holder blacklists to the control access points.

A blacklisted holder is a card holder whose card, for some reason, is no longer valid for the system: card expiration, revocation, termination, etc. Blacklists have no relation with each port's access right policy on CMS_EU card holders. Thus, the access right data and management is out of the scope of the national systems and their databases.

CMS_EU national databases can be very useful for cargo transportation security. For example, if the national database stores a list of plate numbers of the vehicles that a holder uses for transportation, those plate numbers could be included in the national CMS_EU response. Taking into consideration that most ports already have plate number readers for cargo haulers, this extra information could be extremely useful in order to improve the port cargo areas security.

Additionally, as CMS_EU card holders are expected to travel long distances between ports, a previous "authentication" request can be performed prior to the actual card holder arrival if the port has knowledge of the card id for any reason (for example, a previous notification from the hauler's company to inform the port authorities about which of his employees are going to transport the cargo to the port, just by sending their EPAIC card ID numbers). This feature can help the port authorities (or the facility control access responsible) to schedule, program and plan their access control policies for particular EPAIC CMS_EU cards, dates or even hours of granted access.

This proposed data model searches to be as similar as possible for the three EPAIC CMS's. Thus, the data transmissions from the CMS_EU local port system and CMS_EU national systems (holder database) must meet the same security requirements set for CMS_L data transmissions. Same applies with any transmissions between national CMS_EU systems of different countries.

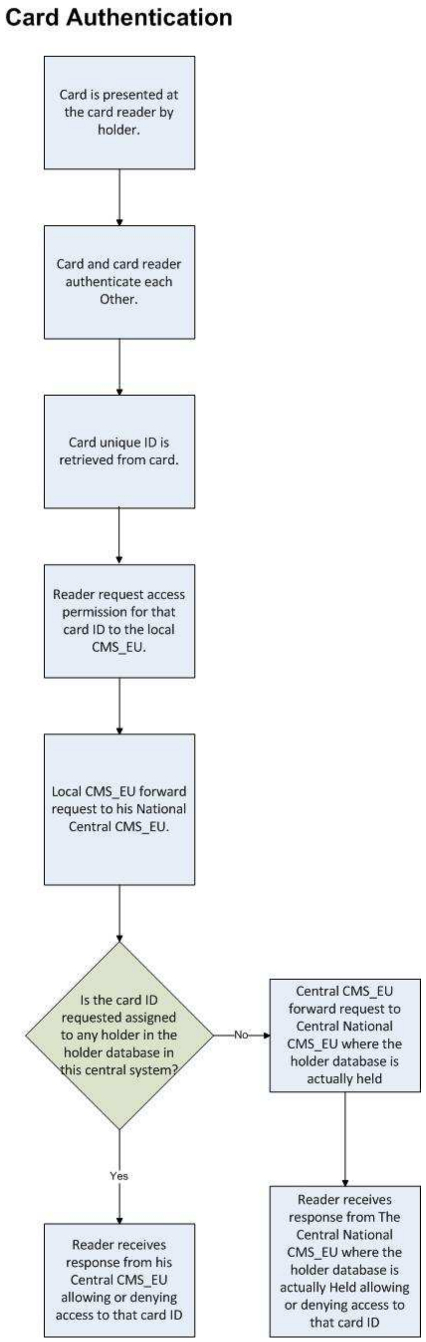

Card Authentication
Card is presented at the card reader by holder.
Card and card reader authenticate each Other.
Card unique ID is retrieved from card.
Reader request access permission for that card ID to the local CMS_EU.
Local CMS_EU forward request to his National Central CMS_EU.
Is the card ID requested assigned to any holder in the holder database in this central system?
No
Central CMS_EU forward request to Central National CMS_EU where the holder database is actually held
Yes
Reader receives response from his Central CMS_EU allowing or denying access to that card ID
Reader receives response from The Central National CMS_EU where the holder database is actually Held allowing or denying access to that card ID

Figure 61 Card authentication - CMS_EU

9.4.4. CARD DATA STRUCTURE AND DESIGN

All three EPAIC CMS's follows the following card data structure.

9.4.4.1. DATA INSIDE THE CARD CHIP

1. Card unique ID: must be a unique alphanumerical number assigned to each card during the issuing process. This number must not have any kind of relationship with any holder personal data. The ID format is as follows:

[CMS][PAYLOAD1]

Where [CMS] identifies which type is the CMS issuing the card. This is, CMS_L, CMS_O and CMS_EU.

<u>For CMS_L cards:</u>

[PAYLOAD1] = [PORT-ID][CARD-ID]

Where PORT-ID is an identifier for the port managing the CMS1 system and CARD-ID is the card identifier. CARD-ID length must be long enough to meet the card availability requirements of any European port. Note that the PORT-ID field is equivalent to an ISSUER-ID.

<u>For CMS_O cards:</u>

[PAYLOAD1] = [PROVIDER-ID][CARD-ID]

Where PROVIDER-ID is an identifier for the outsourced party managing the CMS2 system and CARD-ID is the card identifier. CARD-ID length must be long enough to meet the card availability requirements of any outsourced provider. Note that the PROVIDER-ID field is equivalent to an ISSUER-ID.

<u>For CMS_EU cards:</u>

[PAYLOAD1] = [COUNTRY][CARD-ID]

Where COUNTRY is an identifier for the CMS_EU national system where card holder data is stored and CARD-ID is the card identifier. CARD-ID length must be long enough to meet the card availability requirements of all CMS_EU European port users. Note that the COUNTRY field is equivalent to an ISSUER-ID.

2. Card holder complete name.
3. Card holder employer: card holder's company or responsible organisation.
4. Employer's address: contact address for the holder's company.
5. Biometric minutiae.

9.4.4.2. Proposed EPAIC Card Surface Data

1. Card holder complete name.
2. Card holder picture.
3. Employer's address

   Contact address for the holder's company.

4. Card holder employer

   Card holder's company or responsible organisation.

5. Expiry date.

6. Issuer identifier

   Port ID, outsourcer provider ID, member state national system ID.

7. Holder role identifier

   Local user, mobile user, visitor/temporary user.

9.4.5. CMS DATA STRUCTURE

Every CMS will follow the card data structure as it is explained in the following subsections.

9.4.5.1. DATA RETRIEVED FOR ENROLMENT

1. Card holder complete name.
2. Card holder picture.
3. Holder birth date
4. Holder nationality.
5. Holder signature.
6. Valid ID documents (passport, etc.)
7. Employer's address

   Contact address for the holder's company.

8. Card holder employer

   Card holder's company or responsible organisation.

9. Biometric sample to be stored inside the card, if required by applicant.
10. Initial access rights, holder role type, card unique ID, expiry date, and issuer ID are set during the enrolment process, but not provided by the applicant.

9.4.5.2. DATA STORED IN THE DATABASE.

1. Card holder complete name.
2. Card holder picture.
3. Holder birth date
4. Holder nationality.
5. Employer's address

   Contact address for the holder's company.

6. Card holder employer

Card holder's company or responsible organisation.

7. Issuer identifier

   Port ID, outsourcer provider ID, member state national system ID.

8. Access rights (except CMS_EU)

9. Holder role type

10. Card unique ID

11. Expiry date

9.4.6. PROPOSED DATA MODEL KEY POINTS

1. Size of data transmitted is minimal. This was a considerable concern in the first EPAIC study. In this technical proposal, only a small data structure is sent and received between local port systems and further centralised systems (provider party for CMS_O or national systems for CMS_EU).

2. No personal holder data is transmitted from the CMS databases. It is only stored once, during the enrolment procedure.

3. Any biometric data issue is resolved through the match-on-card model approach.

4. The data structure and model from all the ports consulted during the study follows a clear tendency that is represented by this data model proposal.

10. GLOSSARY

List of acronyms	
Acronym	Meaning
APB	Port Authority of Barcelona
BAC	Basic Access Control
BGL	Bundesverband Güterkraftverkehr Logistik Und Entsorgung E.V.
BPO	Baltic Port Organisation
CAC	Common Access Card
CAK	Card Authentication Key
CAPEX	Capital expenditures
CCTV	Closed Circuit TeleVision
CESMA	Confederation of European Shipmasters' Associations"
CHUID	Card Holder Unique Identifier
CISAU	User Support Service Identification Centre
CMC	Crew Member Certificate
CMS	Card Management System
CMS_EU	European CMS
CMS_L	Local CMS
CMS_O	Outsourced CMS
CoESS	Confederation of European Security Services
CSIS	Canadian Security Intelligence Service
DNA	DeoxyriboNucleic Acid
EAASP	European Association of Airport and Seaport Police
EAC	Extended Access Control
EBA	European Boating Association
ECHR	European Convention for the protection of Human Rights and Fundamental Freedoms
ECI	European Critical Infrastructure
ECSA	European Confederation of Shipowners Associations
EFIP	European Federation of Inland Ports
EHMS	European harbour Masters Committee
EMPA	European Maritime Pilots Association
EMSA	European Maritime Safety Agency
EOS	European organisation for Security
EPAIC	European Port Access Identification Card
ESC	European shippers Council
ESPO	European SeaPorts Organisation
ESRIF	European Security Research and Innovation Forum
ETA	European Tugowners Association
ETF	European Transport Workers’ Federation
EuDA	European Dredging Asssociation

FAR	False Acceptance Rate
FASCN	U.S. Federal Agency Smart Credential Number
FEBETRA	Federation Royale Belge Des Transporteurs Et Des Prestataires De Services Logistiques
FEPORT	Federation of European Private Port Operators
FIPS	Federal Information Processing Standard
FRR	False Reject Rate
HSAS	Homeland Security Advisory System
ICAO	International Civil Aviation Organisation
ICC	Integrated Circuit Card
ILO	International Labour Organisation
IRU	International Road Transport Union
ISPS code	International Ship and Port Facility Security Code
ITF	International Transport Workers' Federation
MARSEC	Maritime Security Group
MRZ	Machine Readable Zone
MSIC	Maritime Security Identification Card
MTSCP	Marine Transportation Security Clearance Program
OCEAN	European Ship Suppliers Organisation
OOR	Office of Reconsideration
OPEX	Operational expenditures
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PROATRANS	Transport Access Restructuring and Regulation Plan linked to Barcelona Port
RAIC	Restricted Area Identity Cards
RCMP	Royal Canadian Mounted Police
RFID	Radio Frequency Identification
RHA	Road Haulage Association
SAGMaS	Stakeholder Advisory Group on Maritime Security
SID	Seafarers' Identity Document
SWOT	Strengths, Weaknesses, Opportunities and Threats
TPK	TWIC Private Key
TWIC	Transportation Worker Identification Credential
VVWL	Verband Verkrehrswirtschaft Und Logistik Nordrhein-Westfalen E.V.

Figure 62 Glossary of terms

11. REFERENCES

[1] C108 Seafarers' Identity Documents Convention, 1958
http://www.ilo.org/ilolex/cgi-lex/convde.pl?C108

[2] C185 Seafarers' Identity Documents Convention (Revised), 2003
http://www.ilo.org/ilolex/cgi-lex/convde.pl?C185

[3] ILO SID-0002 Finger Minutiae-Based Biometric Profile for Seafarers' Identity Documents
standard adopted by the Governing Body at its 289th Session (March 2004) and amended at its 294th Session (November 2005)

[4] Ninth Supplementary Report: Follow-up to the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)

[5] Convention No. C108 Ratifying Countries
http://www.ilo.org/ilolex/cgi-lex/ratifce.pl?C108

[6] Convention No. C185 Ratifying Countries
http://www.ilo.org/ilolex/cgi-lex/ratifce.pl?C185

[7] ESRIF Final Report 2009

[8] Biometrics at the Frontiers: Assessing the Impact on Society (2005)

[9] ICAO document 9303 standard

[10] ISO/IEC 24713-3:2009 Information technology – Biometric profiles for interoperability and data interchange – Part 3: Biometrics based verification and identification of seafarers

[11] ISO/IEC 19794-2:2005 Information technology – Biometric data interchange formats -- Part 2: Finger minutiae data

[12] ISO/IEC 15438:2006 Information technology – Automatic identification and data capture techniques -- PDF417 bar code symbology specification

[13] ICAO Annex 9 to the Convention on International Civil Aviation - Facilitation

[14] ICAO Annex 9 to the Convention on International Civil Aviation amendments - FALP/5-WP/18

[15] Joint communication from the governments of Spain and France, February 27th 2009.

[16] Acuerdo entre el Reino de España y la República Francesa sobre la selección, puesta en marcha y financiación de dos proyectos de autopistas del mar entre España y Francia en la fachada atlántica – La Mancha – mar del Norte. BOE, 4 de junio de 2010. (Agreement between the Kingdom of Spain and the French Republic on the selection, setting and funding for two motorways of the sea projects between Spain and France in the Altlantic area – the Channel – North sea. Spanish Official Gazette, June 4th, 2010)

[17] Response of the European Federation of Inland Ports to the Commission's Action plan on Urban Mobility, COM (2009) 490.

[18] Response of the European Federation of Inland Ports to the Communication from the European Commission on a European Ports Policy. Brussels, December 2007.

[19] Organisation of EC-Shipsuppliers: *Contribution to the European Port Access Identity Card consultation*, 2007.

[20] International Maritime Organisation: *Measures to enhace maritime security – Best practices for clearance programmes of international and domestic transportation*, 2010.

[21] Commission of the European Communities: *Proposal for a regulation of the European Parliament and of the Council on enhacing supply chain security*, COM(2006)79 final, 2006.

[22] National Coordinator for Counterterrorism from the Netherlands: *What steps can your company take to counter terrorism?*, available at http://www.nederlandtegenterrorisme.nl/bedrijven/publicaties

[23] Counteract project: *Deliverable 2, State of the art*, 2007.

[24] Counteract project: *Final report*, 2007