MAGISTERARBEIT

Design and architecture of a Nationwide ID infrastructure project in Republic of Croatia

zur Erlangung des akademischen Grades

Magister

(Mag. rer. soc. oec.)

ausgeführt am

Institut für Rechnergestützte Automation

Forschungsgruppe Industrial Software

der Technischen Universität Wien

unter der Anleitung von

Univ.-Prof. Dipl.-Ing. Dr. Thomas Grechenig

durch

Tomislav Maricevic

Anschrift

Köllnerhofgasse 5/61, A-1010 Wien

Wien, 09.07.2008

Abstract

Security situation in the world drastically changed in the last few decades. Terrorism, illegal immigration, identification theft and documents falsification urged for new solutions in order for government to protect their citizens. National identification seemed to be an ideal solution for many governments. Personal identity cards and electronic passports are typical products of such projects. The different methods and mechanisms used for this purpose are strongly controversial and disputed among different interest groups. The main questions are, to which degree should the government obtain control of personal data, for how long should this information be stored and maybe the most important, who will gain access to these highly sensitive data. Another discussion point is the technology used in order to achieve certain results. Technology improves by the day but is it really fully developed to satisfy both interested parties, namely government and citizens? Based on a case study on a National ID project in Republic of Croatia, this thesis shows a concrete solution to all these issues and discusses different points of view.

Keywords: National ID, ePassport, RFID, MRTD, ICAO, Biometry, Border Control Croatia, eReissepass, Biometrie.

Kurzfassung

In den letzten Jahrzehnten hat sich die Sicherheitssituation in der Welt drastisch verändert. Terrorismus, illegale Einwanderung, Fälschung von Identifikationen und Dokumenten haben es für Regierungen notwendig gemacht, neue Lösungen zu suchen, um ihre Bürger zu schützen. National ID hat sich als ideale Lösung für viele Regierungen gezeigt. Personalausweise und elektronische Reisepässe sind typische Endprodukte von solchen Projekten. Welche Methoden und Mechanismen für diesen Zweck benutzt werden, ist umstritten. Im Mittelpunkt der Diskussion steht, in welchem Umfang die Regierung die Kontrolle über Privatdaten erhalten soll, wie lange die Daten gespeichert werden und wer den Zugriff auf diese äußerst sensitiven Daten hat. Weitere Fragen beziehen sich auf die zu verwendende Technologie. Obwohl die Technologie einen weiten Schritt gemacht hat, ist es fraglich, ob sie reif genug ist, Regierung und Bürger wirklich zufrieden zu stellen. Anhand eines konkreten National ID Projektes in Kroatien wird ein möglicher Lösungsweg im Rahmen dieser Arbeit vorgestellt und unterschiedliche Aspekte vergleichend diskutiert..

Contents

List of Figures

List of Tables

1. Introduction

United States and many other countries have raised their border security to the maximum level since the September 11th terrorist attack. The need for better border controls became the first priority for an ever increasing number of countries. In order to better control their borders a whole infrastructure had to be made that would support this huge project. This infrastructure had to unambiguously identify individuals and recognize any threats that they might pose. Furthermore it should also be able to protect individuals' civil rights and their right for privacy.

New National Identification Projects were started all over the world. Most of these projects were disputed in their countries mostly on security and privacy issues, but also on financial issues. This work should clarify the above mentioned issues and describe further features related to the implementation of National Identification Projects.

The second chapter gives the key definitions of notions related to this area of work. The following notions are presented: identity, identification, identification systems, actors and processes in identification systems.

Third and fourth chapter give detailed information about technology issues and biometric systems used in identification systems. Smart cards are reviewed on historical, technical and secure fields. Biometric systems give a full insight of technologies and schemes used in today's identification systems. The thesis compares their accuracy, methods and application fields.

The fifth chapter describes standards, organizations, history and technical issues concerning machine-readable travel documents, and more specifically, machine-readable passports and identification cards.
Last chapter offers a practical solution of such a project in Republic of Croatia.

2. National identification basic principles

2.1. The notion of identity

Since ancient times, people have used different techniques to unambiguously identify a single person or a group. Regardless if it was a tattoo that ancient humans used to mark a belonging to a certain group, or the seals that kings used when sending their messages, or the identification cards that we use in modern times to confirm our identity, the identification techniques were always an integral part of society. In order to understand the concept of identification, which is closely linked but not to be confused with identity, few statements about identity have to be clarified.

"Identity is used to refer to a set of explicit relevant attributes (permanent or temporary) of a person in the context of practical activities." [NaHi05]

However, another approach introduced by Hildebrand must also be mentioned. This model distinguishes *ipse-identity* as inner identity of a person (who the person truly is, persons individuality) and *idem-identity* as a person's external projection (subset of attributes used for identification). Ipse-identity concept is not particularly useful for information technology and automated identification process since it is based on philosophical considerations, while the second concept – idem-identity, based on external properties, is used in everyday IT processing.

Furthermore identity can be structured into different categories: [Hild05]

- Personal identity (name, location, biological attributes)
- Social identity (family, friends)
- Leisure identity (interests, activities, hobbies)
- Organizational identity (employee, business reputation)
- Citizen identity (citizenship, nationality, political preference)

- Customer or client identity (buying capacity, properties owned)
- Learning identity (competence, certification, aspirations)

Identity can also be classified from three different perspectives: [ICPP03]

- Identity from the Sociological Perspective
- Identity from the Legal Perspective
- Identity from the Technical Perspective

2.1.1. Identity from the Sociological Perspective

Identity definition from the sociological point of view was described by George H. Mead in 1934 *as an exclusive perception of life, integration into a social group and continuity, which is bound to a body and shaped by society. Such concepts of identity modify the difference between "I" and "Me"*. [MEAD34]

This definition distinguishes the identity accessible only by the individual itself, namely "I", and identity accessibly by communication, namely "Me". This identity describes the distinction between an individual and a person, which can only be determined from the perspective of a person.

There are three social systems in which people can develop and describe their identity. [ICPP03]

- Interactional systems describe recognition and participation in communication between present individuals. Typical situations are spontaneous encounters, e.g. in a subway, shopping mall or on the street. In these systems the identity has a special relevance. There is a direct contact between communicating parties (eye contact, hearing, body language). In this case the identity is a simple set of attributes. One person knows the specific character of the other; his or her attributes can be viewed as an analytically undivided whole.

- Organisational systems are based on a previous individual decision for a person to participate in certain activities and be a subject of either joining or separation. Common examples are companies, institutions, institutes, political parties, hospital, schools, army, prison etc. Organisations differ from one another in many aspects. One such instance is the empowerment inside an organisation – for example, in prisons, where the hierarchy is strict; the prisoners have a consultative role but never an executive role that could enable them to change this structure. Identity issues are much more complicated in organisational systems than in interactional systems. Each person is viewed not only as individual but as a part of a group. He / she is not only what the person might consider himself or herself to be, but is also whatever the organisation might consider him or her to be. Significant difference of the interaction system is that the difference does not necessarily result in conflict. However, being different in an organisation and not playing by the rules makes it more difficult to be a part of it.

- Four social subsystems have been identified so far. The economical system (insolvency), the legal system, the political system (voting rights) and scientific system. All of the subsystems are linked with one's identity and the lack of the common attributes means that communication is possible only in a limited way.

2.1.2. Identity from the Legal Perspective

Legal person is mostly defined as a human being onto whom the legal system confers legal rights, privileges and obligations. Current legislation has no systematic regulation for the identity of a physical person. It is a grouping of attributes and has two main functions: [ICPP03]

- To grant identification for legal purposes and
- To protect individual rights of freedom (name, self determination, freedom of speech, privacy, etc.) related to a physical person.

Legal identity consists of attributes with a function to make it unique. The attributes with the function to grant uniqueness to a personal identity are most developed in the legal system, but differ from one legal system to another. These attributes usually include:

- Gender (male/female)
- Name (given name)
- Surname (family name)
- Date of birth
- Place of birth
- Number of birth certificate
- Identity of parents
- Nationality
- Place of residence/domicile
- Profession

Some of these attributes are of a great importance in protecting one's identity. The main legal sources of the protection of individual identity are: [ICPP03]

- Constitutions
- International Treaties
  - Treaties of the European Union
  - European Convention for the Protection of Human Rights and Fundamental Freedoms
  - European Directives
- National Law
- Other national Regulations

The aspects of human personality that are protected by the above mentioned legal sources are: [ICPP03]

- One's name and the identity
- Freedom from physical constriction (habeas corpus)

- Inviolability of the domicile and right to privacy
- Freedom of speech and self expression, in particular:
  - The right to choose one's image
  - The right to protect one's honour
- Freedom of movement and freedom to settle (granted only to people of age)

2.1.3. Identity from the Technical Perspective

In technology jargon, the term "ID" is far more important than “identity”. IDs describe "technological identities" of any possible object. It could represent a name, a serial number, or some other pointer or address to the entity being identified. Even if identifiers are not directly assigned to a user, but to, e.g., pieces of his/her hardware or programmes, the specific user may often be derived.

ID examples are:

- IDs in relational databases
- MAC address
- IP address
- Cookies

Identity from the technical perspective is most interesting perspective for this work and therefore will be discussed in more detail in the following chapters.

2.1.4. Identity theft

According to the US Department of Justice identity theft and identity fraud are *“terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.”* [USDJ06]

There are two types of the known identity theft. The first one is referred to as an account takeover. In this case the identity thief tries to collect as much information as possible about the victim's existing bank account in order to take control over it. Once the information is collected it is possible for the identity thief to withdraw money, take out a cash advance, or purchase goods and services in the victim's name. It is not very often that the identity thiefs are captured, since the most of the victims usually notice the theft only after obtaining a monthly bank statement. The second type of identity theft is called application fraud, also referred to as a true name fraud. In this identity theft scenario the identity thief collects just fragments of the victim's information e.g. date of birth, social security number, personal ID number. Having collected these information fragments, the thief tries to open a new bank account or to obtain new credit cards. In the same way as with the application fraud, it might take months for the victim to recognize that he or she was subject of the identity theft. [PRCl03]

In order to acquire information needed for identity theft, various techniques are developed and are described as follows: [PRCl04]

- Stealing (physically stealing someone's wallet or documents)
- Main fraud (intercepting e-mail communication that is not using security channels)
- Dumpster diving (searching through trash cans in order to acquire personal information)
- Posing as a legitimate business person (false identification as an employer or even as a law enforcement agent)
- Home invasion (physically stealing victims computers or documents)
- Keyboard recording (logging the victim's keyboard for passwords, pins and other confidential information)
- Phishing (sending emails or asking to input sensitive data on the webpage)
- Work place theft (stealing the customer or other user information accessible at work)

In order to be protected from identity theft, people should consider few basic rules. Since banks do not ask their customers to repeat personal data, any sensitive data, such as passwords and PINs, should be sent over e-mail, phone, chat lines or SMS??. Passwords, PINs and other confidential data should not be written down or and carried around. It is highly advisable that this information is memorized and the paper evidence destroyed by shredding or burning. Consumers are encouraged to ask about information security procedures in the workplace and who has access to their personal information.

2.2. The notion of identification

If we wish to clarify and build upon the identity concept, identification can be defined as a process used to link a person with an identity:

"Identification concerns the set of approaches and mechanisms that intervene in the course of an interaction and which are very broadly related to the disclosure of Identity information (person characteristics and/or linking to a profile)." [NaHi05]

More precise definition was given by Jain, Hong, and Pankanti:

"Personal identification is the process of associating a particular individual with an identity. Identification can be in the form of verification (also known as authentication), which entails authenticating a claimed identity ("Am I who I claim I am?"), or recognition (also known as identification), which entails determining the identity of a given person from a database of persons known to the system ("Who am I?")." [JaHo00]

A distinction between identification and authentication is defined as follows: [Nguy03]

- *Identification consists in determining the identity of a person from within a given population of possible matches.*

- *Authentication consists in verifying an identity either determined by identification, or claimed by a person.*

The usage of identification has various purposes, but it is possible to categorize them into three main contexts: [NaHi05]

- Access control to restricted resources or areas (authentication)

- Exploitation of identity information
- Monitoring to enable accountability

The first concept is widely used for authentication and access management, as well as performing a personal verification and enabling access to any allowed resources and areas. The exploitation of identity information concept relies on knowing certain information which can increase the amount of interaction between communicating parties. The third concept - monitoring to enable accountability- is also sometimes called behavioral observation. It gives a certain pattern of user's actions that are useful for the user and/or other interested parties.

Two identification approaches are defined in the context of identification mechanisms: [NaHi05]

- Explicit identification
- Implicit identification

Explicit identification refers to a direct interaction between user and identification process, meaning that the user has to participate in confirming his/her identity. This is described by three different mechanisms as shown in Figure 2-1.

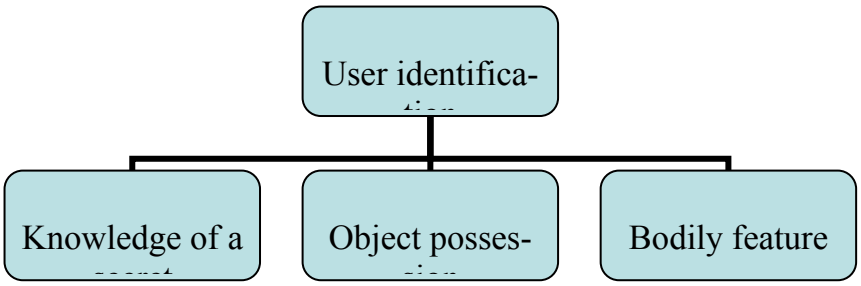

Figure 2-1: Classification of methods for person identification [RaEf03]

The first method, knowledge of a secret, refers to entering a password or in the majority of cases entering a secret number, also known as PIN (Personal Identification Number). If this process is successful it seems safe to assume that the person is likely to be whoever he or she claims to be. The second mechanism, possession of an object, is based on testing whether the person is in possession of a required object. Both of these methods of identification can be transferred to a third person. This could be considered as an advantage because of its flexibility, or a disadvantage when the identity theft occurs. The bodily feature method eliminates the possibility of identity transfer, since it is the actual human body attributes that are used in the identification process. These bodily features are based upon different measurements of human body parts, such as fingerprints, retina or iris, and are described in more detail in chapter 2.4. [RaEf03]

Unlike the explicit identification, the implicit identification is established without the explicit awareness of a person that needs to be identified. It is based on a series of available information that is extracted and filtered from the given source (RFID or IP number). Furthermore, behavioural characteristics can be captured and analysed at a later time or used in the context of data mining. [NaHi05]

The simplest physical form of identification today is a card or paper carrying the user's signature or biometric attributes (photo, fingerprint) that unambiguously identify the user and distinguish him or her from other people. Although modern computers can achieve high performances and have enhanced logical processes, they still lack, unlike humans, intelligence which is necessary for many identification tasks. Therefore, since biometrical and other human identification characteristics have to be reliable, this still presents a big challenge for developers and planners.

2.3. Identification systems

After defining identity and discussing different aspects of one's identity, as well as describing identification as a process of associating a particular individual with an identity, the next step is to define and describe a way to store and handle this information.

Identification system is defined more precisely as follows:

An identification system is a physical (paper, microfilm, computer, etc) system which can be run as a stand-alone system and implements the identification functionalities: registration, information storage/update and information revelation. An identification system can be used together with one or many other identification systems to meet the needs of an identification scheme. [Nguy03]

Identification system is in the majority of cases a system with a relational database in the background, which is able to store and update personal information for future usage. The sole purpose of an identification system is to get certain information about a chosen person. In everyday life our brain manages and saves the individuals that we met in our memory so that the next time we meet someone the "person's data" is being fetched from our memory. In order to do the same with the far larger data requirements, we use identification systems in which a person's information is stored digitally.

Each identification system should be able to perform the following actions: [Nguy03]

- Registration
- Information storage
- Information update
- Information retrieval

Registration and information storage is completed when a person is in contact with an identification system for the first time - e.g. applying for a passport. The information stored in a database differs depending on usage. In some cases only basic data, such as name, surname, address and email, is stored, while in other the more sensitive cases the more complex data, such as biometric information (face, fingerprint or iris), is stored.

Information update is a functionality used to change the person's data - for instance if the person married and changed last name, or if they moved to another address.

The main difference between a regular storage system and an identification system is that the identification system has an ability to compare the actual person or the person's identification with the data stored in the database and to unambiguously confirm or deny the person's identity. The stored information is retrieved and compared with the actual person by using different identification methods. These are described in the forthcoming chapters.

2.4. Actors in identification systems

In order to present the whole identification life cycle one must first define the involving actors. For the purpose of this discussion only the relationship between an individual and an organisation will be described. The individual – individual relationship will be ignored since typical national identification system uses individual-organisation relationship. The actors will be also described in regard to the identification system functionalities: registration, information storage, information retrieval and identification.

The actors and the roles they play in identification system differ from one identification system to another and from one scenario to another. However it is possible to narrow the actors into three main categories. Typical scenario in the category relevant for this work includes, for example, registering and issuing a valid passport, and the actors in this scenario are most common in national identification systems.

They are defined as follows:

- Private individuals
- Government (law enforcement, government agencies)

Private individuals are at the heart of the identification system because they are the reason that the identification system is developed in the first place. As already mentioned, the interaction of a private individual with the identification system is based on his/her desire to gain certain privileges or obligations. Furthermore, with an effective and secure national identification system private individual can protect his/her identity against identity fraud or identity theft.

National governments are motivated by several different factors. In some countries (e.g. France) setting up a national identification system is related to a way to prove

citizenship. In other countries its primary usage is to fight terrorism. Governments' intentions can be classified into three main categories:

- Gain more control over the citizens - As already mentioned one of the main advantages of implementing national identification systems is increasing national security, fighting terrorism and controlling illegal immigration.

- Make government administration more effective - With more control over its citizens government agencies can handle issues such as social security, taxes, immigration or customs far more effectively.

- Repaying the service to the society - With the measures, for instance, to more effectively collect taxes or to stop illegal immigration government can use those assets to build better roads or a better health system in order to raise the quality of living for its citizens.

Another similar actor classification is presented by Nguyen. The involved parties are classified by the functionality of an identification system (registration, information storage/ update, information revelation). The actors are: [Nguy03]

- Person / Registered person (a person has a digital identity while a registered person has personal data saved and attached to his/her identity)

- Identity authority (creates a person's digital identity and saves or updates information about the registered person's digital identity)

- Information authority (certifies information authenticity of a registered person's digital profile)

- Examiner (obtains digital profile of a registered person)

2.5. Processes in identification systems

This chapter describes the most relevant and common processes in national identification systems and in identification systems in general. These processes have already been mentioned in chapter 2.3, but weren't discussed in detail.

2.5.1. **Registration**

Registration is the first step towards establishing a functional identification system. Since this is the beginning of a chain process, its successful completion is crucial to the entire identification process. All further identifications in the system will rely on the authenticity of the initial information. In this process the digital identities of private individuals are created.

The first step is to unambiguously identify the person applying for registration. What information is needed for proper identification can be different for different information systems, but in the case of national identification systems it is up to lawmakers and governments to decide which information is relevant, while taking care not to encroach on individual privacy. In order to standardize this information about the registrant international organizations are setting standards in order to make the information system compatible around the globe. E.g. In case of travel documents the organization responsible for the standardisation is the International Civil Aviation Organization (ICAO).

The next step is the actual creation of a person's digital identity. Since digital identity is defined as a *part of that person's identity that it is recorded in the identification system* [Nguy03], only select information will be prepared for storage. Along with the creation of a new digital identity, the identification system should also cross-check for any earlier digital identities. The decision of how to handle multiple identities lies in the hands of lawmakers and governments.

2.5.2. Information storage / update

Each identification system requires an option to store or update the information acquired at the registration. Although the idea of storing personal, and sometimes sensitive, data is widely disputed, the need to store personal information is essential. It is likely that certain change will occur during a person's life, such as changing address, changing name or even some biometric information – e.g. height. In addition, it is important to avoid errors during the registration process.

Before storing personal information the issuing authority should check the person's information for authenticity in order to avoid false information in the system. There are three methods to accomplish this: [Nguy03]

- Verify the information in person (e.g. eye color, height)
- Check other information sources (e.g. birth certificate)
- Trust the person (only in cases where the person has no interest to falsify information)

Information can be stored in a centralised or a decentralized way. The current tendency is to keep data as centralized as possible, but some governments do not want to share their information with other countries, mostly due to privacy issues but also because of the possible security breaches. The centralized storage means that a person is identified through a unique global identifier which makes it easier to maintain such a system, thus making it cheaper. [Nguy03]

2.5.3. Information revelation

Information revelation is a key to the most widely spread identification model and is based on three levels: identification-authentication-authorization. Identification determines the identity of a person, authentication checks the identity with the identifi-

cation system and authorization allows the individual to acquire certain rights, privileges or access - e.g. entering foreign county with your passport.

Another possibility proposed by Nguyen is a modified three level identification system:
Identification-authentication-profile revelation. What is the benefit of this model? Since not all information is needed all of the time, certain profiles are provided as an information revelation instead of a whole set. Different profiles are saved for different applications. Based on an application or a situation, only the information needed (profile) is loaded and used for the identification process.

3. Technology in national identification systems

Technology developments that occurred in the second half of the 20th century made identification more reliable and secure. However the development also opened new opportunities to abuse identification documents through forgery or data manipulation. With each evolutional step both security and vulnerability become more sophisticated.

This chapter concentrates on technologies used in identification systems, including smart-cards and RFID technology. The standards given by the ICAO and the ISO, concerning the development and implementation of smart cards in national identification systems will be also described.

3.1. History

During the last 60 years, since their first appearance in the early 1950s, plastic cards have undergone a substantial evolution in design, technology and usage. At the outset everything was simple - it all started with a man eating his dinner in a restaurant, who had forgotten to take his wallet with him, leaving him without money to pay. That man was Frank McNamara, one of the co-founders of Diners Club and the pioneer of smart cards as we know them today. Diners Card was originally intended for an exclusive set of individuals and was considered a status symbol - the possession of a Diners Card was equated with an individual's "good name".

The first credit cards were quite simple. They contained data that was either printed on the card, embossed on the card, or both. In the majority of cases the card's issue name and card's number were embossed. Protection against forgery and misuse was at the visual level, meaning that any persons responsible for accepting the cards were the system's security interface, checking for security printing and other security features. In addition the majority of cards had a signature field that was used to compare it with the cardholder's signature.

As a number of users and cards expanded a machine-readable card was necessary to cut the raising administrative costs and fraud. First step toward this goal was the magnetic strip card which allowed storing data that was printed or embossed on the card in electronic form. This made the data processing faster and easier, but on the other hand security was compromised. It was possible to falsify data written on the magnetic strip by reading and re-writing new data onto the card. [RaEf03]

3.1. Card overview and components

Identification documents are available in various forms and sizes. Although physical forms and shapes can be different, there are specific standards that make these documents usable and readable all around the world. In the same way the technology used to identify a person has to be compatible in different countries. Identification documents are just one component of a complex system. In the field of smart cards, which are planned to become the most important identification carriers in the future, the ISO/IEC standards are developed to define the basic properties of smart cards. Smart cards have a defined size of 85.6mm x 53.98mm x 0.76mm. However, they can be as small as SIM (Subscriber Identity Module) cards with dimensions 25.1mm x 15.1mm x 0.76mm.

The ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) standards are especially significant for smart cards, since they define the basic properties of smart cards. The ISO and IEC had to avoid duplication of standards so the standards are developed by the joint technical committees and published as the ISO/IEC standards. The main goal of these worldwide associations counting more than 100 national standards agencies is to promote the development of standards around the world in order to simplify the international exchange of goods and services and to develop worldwide cooperation in the fields of science, technology and economy. Both, large global companies and small start-up companies profit from standardization. For global enterprises international standards are bringing additional security and protection for large investments. The small companies benefit from the opportunity to enter large markets which otherwise might have been closed to them. [ChSe93]

The Figure 3-1 presents the classification scheme for card components.

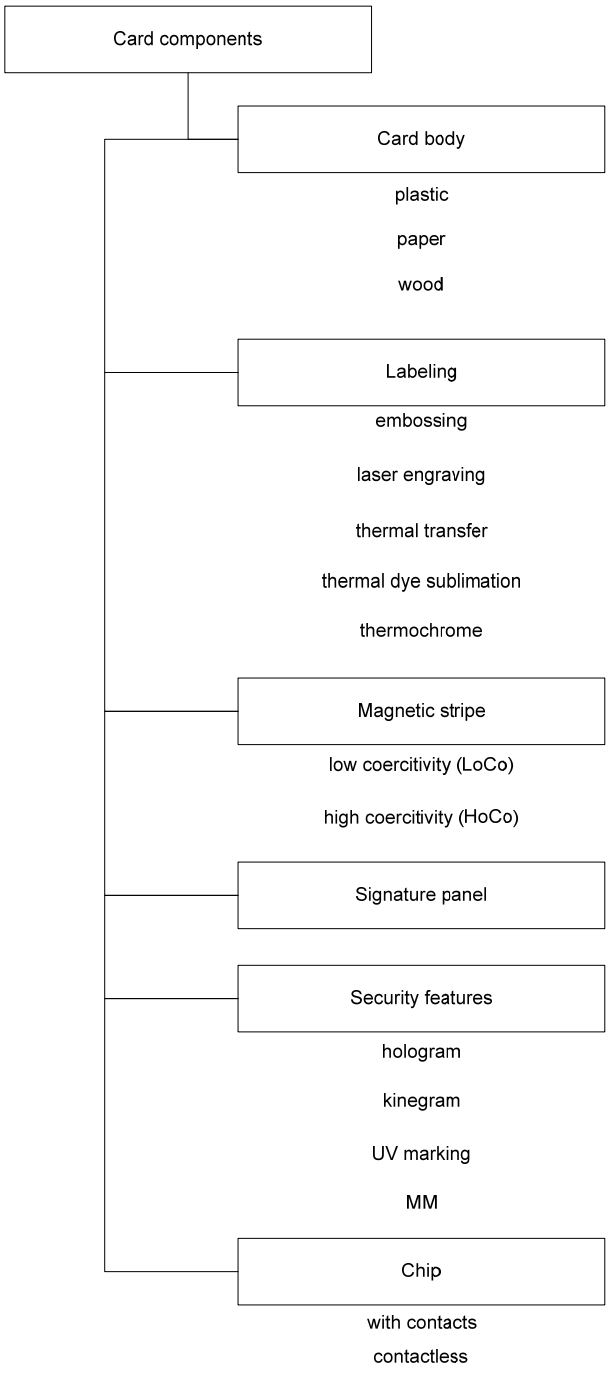

Figure 3-1: Classification scheme for card components [RaEf03]

Smart cards are the latest addition to the exiting family of identification cards that use the ID-1 format defined the by ISO standard 7810 called “Identification Cards – Physical Characteristics”. Since different technologies have been used in the past for identification purposes, the existing architecture cannot be replaced instantly. Combination of the older with the newer technologies is common in many applications

(e.g. credit cards). This is the reason why the older technologies have to be mentioned and briefly described.

3.2. Embossed and magnetic strip cards

Printing and embossing are the oldest methods for adding machine-readable features to identification cards. The embossed characters on an identification card can be easily transferred to paper using simple, inexpensive mechanical devices. Furthermore, embossed cards are easily read visually by humans and neither electrical energy nor connection to external devices is necessary. Protection against forgery and misuse is at the visual level, meaning that any persons responsible for accepting card transactions act as a system's security interface, checking for security printing and other security features. Furthermore, the majority of cards have a signature field that is used to compare it with a cardholder's signature. Although these techniques seem basic, they made the worldwide usage of credit cards possible. Form, size and height of the characters and their placement on the card are specified through the ISO 7811 standards. The embossed cards have introduced the machine-readable identification cards, but their remaining fundamental disadvantage is high cost of processing paper receipts. [RaEf03]

As a number of users and cards has expanded, it was necessary to introduce a more sophisticated card in order to cut the raising administrative costs and fraud. The first step towards this goal was the magnetic strip card which allows for storing data that is printed or embossed on the card in electronic form. This makes data processing faster and easier, but on the other hand security is still compromised. It is possible to alter data written on the magnetic strip by reading and writing new data onto the card. Another disadvantage is the usage of automated equipment which makes visual inspection, performed by human, impossible. Magnetic-strip card manufacturers have developed various techniques to improve security of the card by introducing new features such as adding invisible and unchangeable code to the card, which requires special sensor in the card terminal. This results in higher expenses for the card terminal, which makes it too expensive for establishment on the international market. [RaEf03]

3.3. Smart cards

The smart card is the latest addition to the identification cards in the ID-1 format. Since 1968, when German inventors Jürgen Dethloff and Helmut Grötrupp patented the idea of having plastic cards hold microchips, smart card made a big step toward everyday use. Former French journalist Roland Moreno filed for a patent on the IC (Integrated Circuit) card in 1974. The patent was registered in France in 1975 and 1978 in the United States. Since the technology to support his idea was not available until 1976, his patent was rather theoretical then practical research. [Huse99]

The Figure 3-2 shows a structure overview of the relevant ISO and IEC working groups and the standards under their supervision.

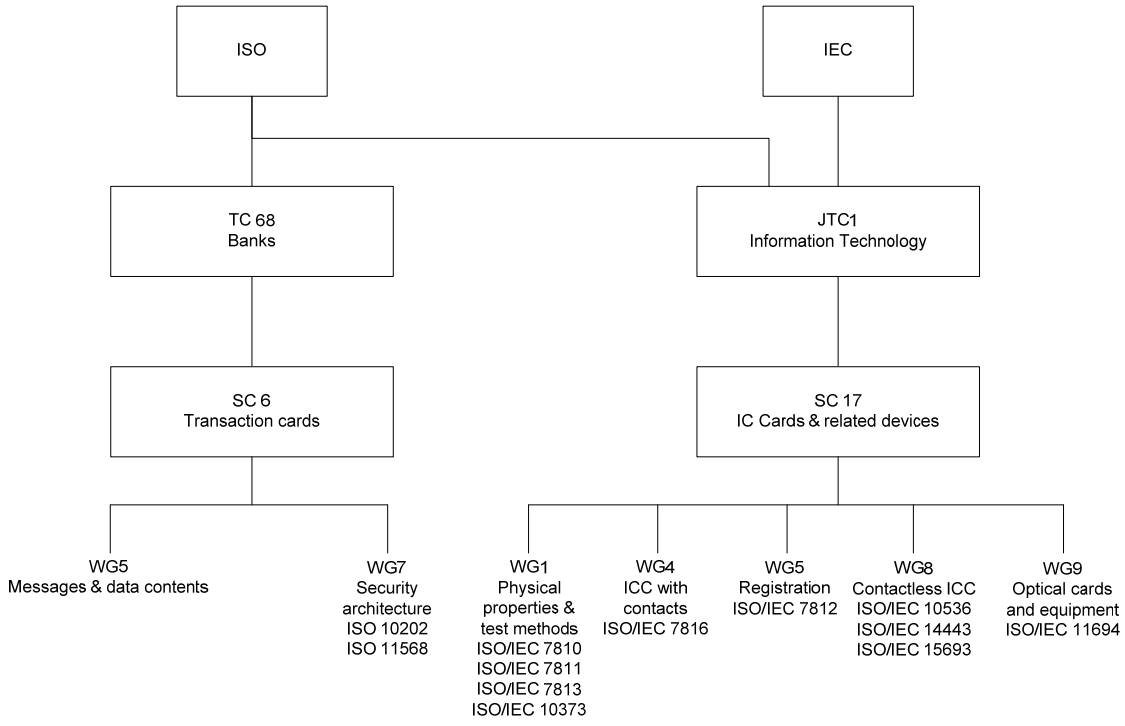

Figure 3-2: Overview of the working groups for international smart card standards [RaEf03]

Smart card according to Shelfer and Procaccino is *"any credit card-sized card with more memory than the traditional magnetic stripe (the common technology of credit cards and debit cards), but technically speaking, the "true" smart card has an on-board embedded processor, or smart chip."*[ShPr02]

More precise definition is stated by General Services Administration in their Government Smart Card Handbook, where smart card is defined as *"a credit card-sized device that contains one or more integrated circuits (ICs) and also may employ one or more of the following machine-readable technologies: magnetic stripe, bar code (linear or two-dimensional), contactless radio frequency transmitters, biometric information, encryption and authentication, or photo identification."* [Gene04]

The second definition is directed at addressing the identification cards with smart card and/or additional functionality. Although every definition of a smart card is represented with one or more Integrated Circuits (IC), it is the size that is not necessarily *"credit-card size"*. It is only ID-1 format that is standardized as credit card sized. On the other hand, formats ID-00 or ID-000 are not of the same size, but are still recognized as smart cards - e.g. SIM cards.

Fundamental characteristics and functions of smart cards with contacts are defined in the ISO 7816 standard, which contains eleven parts. Smart cards are distinguished by the type of chip that they contain and by the type of interface that they use to communicate with the reader. [Gene04]

Smart card classification is shown in the Figure 3-3.

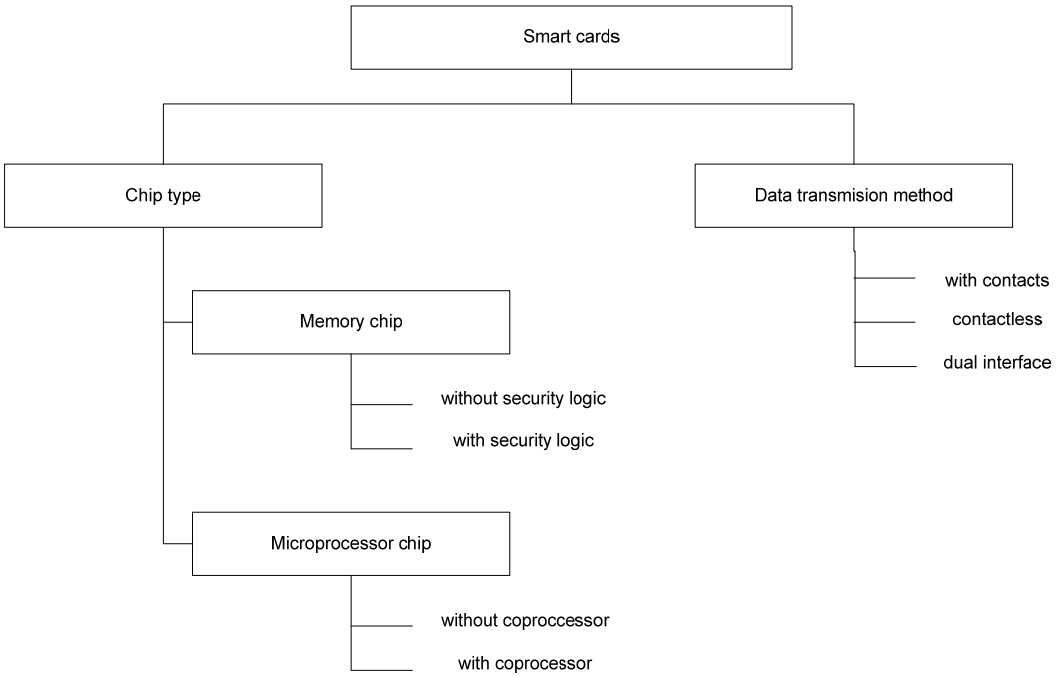

Figure 3-3: Smart cards classification [RaEf03]

Another classification states that there are three different types of chips that are associated with smart cards: memory only, which includes serial-protected memory, wired logic and microcontroller. The terms “memory only,” “wired logic” and “microcontroller” refer to the functionality that the chip provides. [Kapl96]

The following briefly introduces this categorization: [Kapl96; ZoOt94]:

The memory-only chip cards do not perform any logical or calculation operations. These cards are used only to store information. First versions of memory-only cards were read-only, low capacity, prepaid disposable cards with little security. Newer versions use read/write memory and binary counting schemes that allow the cards to have higher capacity.

A wired logic chip card contains a logic-based state machine that provides encryption and authenticated access to the memory and its contents. Wired logic cards provide a static file system supporting multiple applications, with optional encrypted

access to memory contents. Their file systems and command set can only be changed by redesigning the logic of the integrated circuit.

Microcontroller cards contain a microcontroller, which is based on semiconductor technology, an operating system, and read/write memory that can be updated many times. The secure microcontroller chip card contains and executes logical and calculation operations and stores data in accordance with its operating system. To operate it needs power and a communication terminal. Contact, contactless and dual-interface microcontroller ICs are available. Unlike memory-only products, these microcontroller ICs have been designed to meet security targets. The secure microcontroller chip card is usually referred to as the "true smart card".

Although three different types of chips are introduced, in the literature the smart cards are mostly divided into two types of chip:

- Memory cards and,
- Microprocessor cards

For this reason this type of chip categorization will be used from this point forward.

Another type of smart card categorization is provided by the type of interface that they use to communicate with the reader also the called data transmission method. There are two types of the chip card interfaces in use:

- contact and,
- contactless

These terms describe the way by which electrical power is supplied to the ICC (Integrated Circuit Chip) and by which data is transferred from the ICC to a reading device and vice versa. The contact interface requires the card to be inserted into a card reader so that the reader can establish a direct electrical contact with the chip. A contactless smart card contains a chip and an antenna embedded in a plastic credit card. Communication is facilitated using Radio Frequency (RF) technology. Other types of

the chip card interfaces may contain two chips on the same card, one for a contact interface and other for a contactless interface. These two chips are not connected to each other. These cards are also referred to as hybrid cards. Furthermore, smart cards can also use a dual-interface chip, meaning that one chip is able to connect both to a contact and a contactless interface. These smart cards are also referred to as dual-interface chip smart cards or combo cards. [Gene04]

3.3.1. Memory cards

As already mentioned in the previous chapter, memory cards are often not considered to be the real smart cards. The reason for this is that they do not posses the CPU (central processor unit) that would put them in the "smart" category. The only functionality that memory cards posses, is to store information. However, although they do not posses the CPU, their advantages, when compared to magnetic-strip cards, is vast. In terms of questions capacity, memory card capacity is many times greater than that of magnetic-strip cards.

According to some smart card manufacturers, the currently available capacity for memory cards ranges from eight bytes to 2KB, while traditional magnetic strip-based cards can store approximately 220 bytes of data. [ShPr02] Furthermore, security is enhanced either by using simple security logic or more complex security logic that might include even simple encryption. [RaEf03] Another advantage compared to magnetic-strip cards is that the read/write devices are far less expensive. [Gene04]

Basic memory card architecture is shown in Figure 3-4.

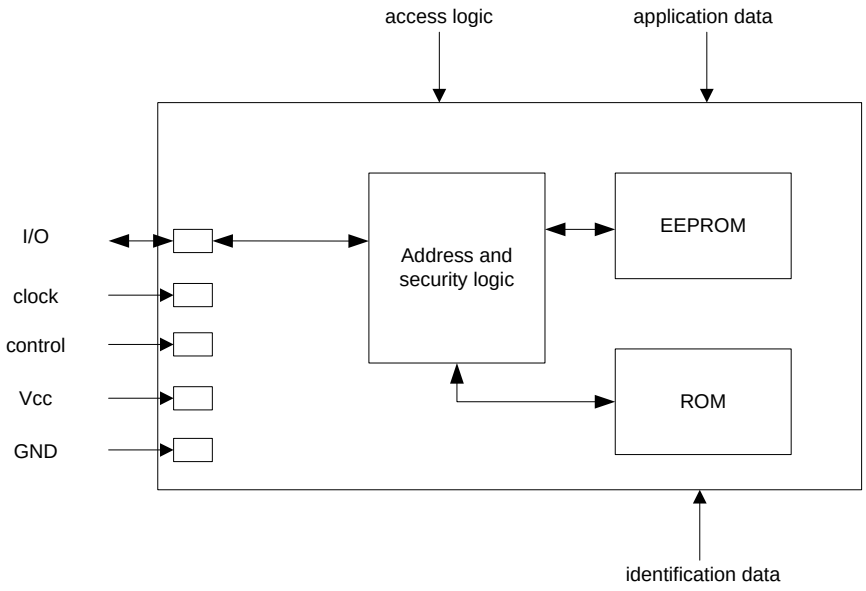

Figure 3-4: Memory card architecture [RaEf03]

Since the price of such a memory card is low, they are typically used as prepaid telephone cards. Although some literature suggests that there is a wide spread and typical usage of memory cards in health insurance [RaEf03] – e.g. the health insurance project in Austria, e-card and other health insurance projects in European Union suggest almost equal usage of memory and microprocessor cards. [Otte05]

3.3.2. Microprocessor cards

Microprocessor cards are often referred to as the "true" smart cards. Unlike the memory cards the microprocessor cards have the CPU at a heart of the chip. The information stored on this type of microprocessor card can be protected by active data encryption schemes along with some biometric identification, e.g. fingerprints. Unlike magnetic strip-based cards, which are often subject to fraud and other criminal activity, such smart cards are difficult to duplicate. [ShPr02]

The basic architecture of such a microprocessor card is presented in Figure 3-5.

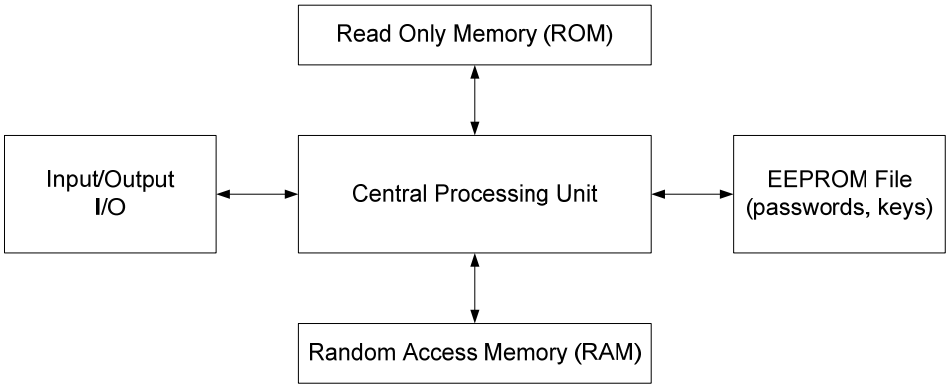

Figure 3-5: Architecture of a smart card with microprocessor [ShPr02]

A microprocessor card consists of the following main functional blocks: [Gene04]

- An 8-bit, 16-bit or 32-bit central processing unit (CPU)
- Read Only Memory (ROM)
- Random Access Memory (RAM)
- Other non-volatile memory, e.g. Electrically Erasable Programmable Read Only Memory (EEPROM), flash memory etc.
- At least one Input/Output communication port
- Mechanism against known and foreseen security threats
- Environmental sensors (e.g., voltage, frequency, temperature)
- A random number generator
- Timers
- Optional cryptography engine(s) (e.g., providing support for DES, 3DES, RSA, ECC)
- Other optional dedicated peripherals (e.g., checksum accelerator, Serial Peripheral Interface (SPI) communication port).

Three main memory types will be further discussed.

ROM contains a chip operating system, which is copied to the memory once the chip is manufactured. Since it is copied into a Read Only Memory, it cannot be deleted or changed during the chip's lifetime. [RaEf03] Chip operating system controls all communication between the chip and the outside world.

Non-volatile memory is represented by the EEPROM. This memory type allows reading and writing of the mostly application data into its storage. The EEPROM capacity ranges from typically 128 Kbytes to more that 256 Kbytes of memory. Communication with the EEPROM is done through operating system and can be written and rewritten from tens to hundreds of thousands of times. [Gene04] Another common non-volatile memory representation is flash memory with capacities up to 1 MB. [ShPr02]

RAM, which is volatile, is used as a temporary storage register by the chip micro-processor. For instance, when a PIN is being verified, the PIN sent by the terminal or a PIN pad is temporarily stored in RAM, but as soon power supply is lost, the PIN is erased from RAM. [Gene04].

3.4. Smart card systems

In order to set up a fully operational and effective smart card system, there are few pre-considerations that have to be met. When planning such a system, six important issues have to be addressed.

1. Management and organizational issues
2. Technical issues
3. Legal issues
4. Cost issues
5. Standards
6. Privacy

The first consideration concerns preparation and detailed strategic planning of the system's implementation. During the implementation phase, some processes will have to be reconsidered in order to gain efficiency and improve performance. Technical issues necessitate precise defining of the infrastructure requirements. This is one of the most critical steps in designing and deploying an effective smart card system. Legal aspects also have to be considered, especially from the user's point of view in order to maintain the individual's privacy rights. Another consideration relates to the cost that this type of project entails. With the adequate planning and the knowledge of detailed requirements, the cost overruns can be avoided. Although a smart card system is not inexpensive, it is proven to be more cost-effective than other identification technologies. As mentioned earlier, the standards are critical for the acceptance of a smart card system. It is of great importance that organizations and governments keep up with technology developments. Further developments of modern standards lead to a simple goal: any smart card should be able to be used in any reader. Privacy question is possibly the most important issue in this context. If there is no acceptance by the users or citizens the whole system will be in question. The primary users' concern is security and protection of their information stored in the smart card. [Gene04].

3.4.1. Components of a smart card system

Smart card systems are very different from each other and are application dependable. However, a most typical configuration and its components can be defined. The main components, based on the smart cards that one identification platform requires, are as follows: [Gene04]

- Cards
- Central Card Management System
- Smart Card Equipment and Software
  - Enrolment Workstation
  - Key Generation Workstation
  - Card Personalization System
  - Registration Authority System
  - Certificate/Attribute Authority System
  - Card Reader
- Applications
- Interfaces to Legacy Databases

Smart cards are able to combine multiple authentication techniques with other features, e.g. Public Key Infrastructure (PKI) and biometrics. The central card management system is the heart of smart card system and connects to all other components. It is also responsible for the management and other operations considering Life Cycle Management (LCM) of smart cards. LCM includes: pre-issuance, issuance, status, replacement, renewal, post-issuance capabilities and audit of smart cards. Smart cards equipment and software includes hardware and software necessary for gathering information processed during the smart card life cycle. [Gene04]

3.4.2. The smart card life cycle

According to the ISO 10202-1 standard, which attempts to define a card life cycle that can be applied to all manufacturing methods, the smart card life cycle has five phases:

1. Production of the chip and the smart card
2. Card preparation
3. Application preparation
4. Card usage
5. Card usage termination

The first phase describes the designing of the chip with activities like generating the smart card operating system and fabricating chips and modules. Furthermore it covers the production of the card body and embedding the module in the card body. In the second phase the loading of operating system is completed as well as implanting the chip in the prepared card bodies. The third phase of the smart card life cycle includes generating and transferring card-specific secret data (PINs, keys) and smart card personalization. Phase two and phase three are mostly completed by one manufacturer. Although the production is carried out by one company these two phases are completely separated both organizationally and physically. Phase four is used and well known in everyday life. It primarily consists of activating or deactivating specific applications. The last phase, phase five, defines all measures relating to terminating the use of a smart card. First the applications are deactivated and then the smart card is deactivated as well. The last step is very theoretical since most of the today's smart cards end up in a trash can. [RaEf03]

3.5. RFID technology

3.5.1. **Overview and components**

During the last few years automatic identification has become widely spread in many spheres of everyday life. Industry, logistics, access control and lately personal identification are all profiting from the expanding development of contactless technology. Unlike the smart cards with electrical contacts, the contactless smart cards do not need to be slid through a reader. Instead these cards access/transmit information through a transmission, such as radio frequency. The chip is powered through the card's antenna if the card is placed within 10 centimetres up to four meters from the smart card reader. [ShPr02]

Radio-based identification has become common in a variety of applications where access control and robust data carriers without electrical contacts are required - e.g. building entrance, highway toll pay etc. [Floe06]

The aim of contactless smart card technology is *"to provide low cost "no-touch" communication, which can create an authenticated, and optionally, encrypted channel of communication between the card reader and the nearest smart card."* [KfWo05]

Contactless technology using radio frequency for identification process is called Radio Frequency Identification (RFID) technology. RFID can be defined as a method that uses radio frequency in order to ensure contactless identification of objects, persons or animals. Although RFID systems have many technical characteristics, three are common for the most RFID implementations: [Bund04]

- electronic identification
- contactless data transmission
- transmission on request

Every RFID system has two main components as shown in Figure 3-6:

- Transponder
- Reading device

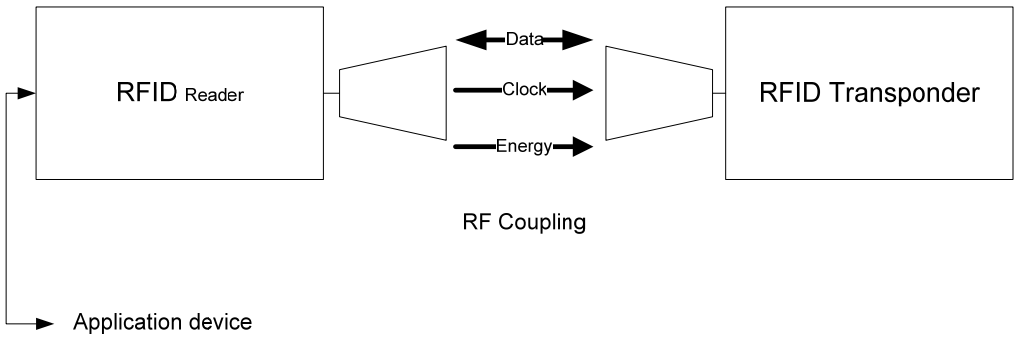

Figure 3-6: Two main components of the RFID system [Fink06]

Transponders, shortly tags, come in various shapes and forms and are not strictly bounded to the ID-1 format. The most typical tag consists of the ICC for the memory and logical performance and the RF module (antenna) for power supply.

3.5.2. Categorization

Transponders can be classified and categorized in five ways: [Bund04]

- **Form**. Different tag forms and shapes are available for different application fields. For example, smart labels are used for marking and pricing products, disk transponder can be used to access control in park garages and card transponder is typically used for personal or access control identification.

- **Frequency ranges**. Transmission frequency is based on LF (Low Frequency), HF (High Frequency), UHF (Ultra High Frequency) and Microwave technology. It defines not only the frequency, but also the reading range of transponders.

LF transmits on 125-134 kHz frequency and is described by the ISO 11784/85 and 14223 standards. This technology is used by the majority of today's access control systems. Communication range between reader and LF transponders is up to 1.2 meters.

HF transponders are mainly used for ticketing, track & trace systems and asset management. Communication frequency is 13.56 MHz and is described by the ISO 14443, 15693 and 18000 standards. This standard is worldwide accepted. The reading range is almost the same as LF transponders, namely 1.2 meters.

UHF technology operates on 868 MHz or 915 MHz depending on the country. This standard is spread mostly in EU and USA and is defined by the ISO 14443, 15693 and 18000 standards. It is typically used for shipping container track & trace systems. The range of the UHF based RFID systems is up to four meters.

Microwave transponders are still under consideration and are not widely accepted in the world. They operate on the frequencies of 2.45 GHz or 5.8 GHz and are described by the ISO 18000 standard. Their application fields are typically shipping container track and trace, and highway toll payment systems. Their range is up to 15 meters.

- **Energy supply**. Classified by energy supply, two main transponder types are available.

  Active transponders use their own power supply source (batteries) for making electromagnetic waves. They operate in stand-by modus until external activation signal is sent to start communication. The activation signal is provided by a reader unit.

Passive transponders have no internal power supply. They use external power supply which is provided by readers. As soon as the transponder is in the reader's electromagnetic field, his antenna induces power to the ICC.

- **Transmission**. Data transmission between reader and transponder is usually based on two principles. The first is inductive coupling and is described by Finkenzeller in the RFID handbook: *"The reader's antenna coil generates a strong, high frequency electro-magnetic field, which penetrates the cross-section of the coil area and the area around the coil. Because the wavelength of the frequency range used (< 135 kHz: 2400 m, 13.56 MHz: 22.1 m) is several times greater than the distance between the reader's antenna and the transponder, the electro-magnetic field may be treated as a simple magnetic alternating field with regard to the distance between transponder and antenna."* [Fink06] The second is backscatter coupling, which works on a radar principle. It is important to mention that low range RFID systems operate primarily on the inductive coupling principle while long range systems operate on the backscatter coupling principle.

- **Storage**. Based on storage technology, there are two typical transponder types: Read-only and read-write transponder. The read-only transponder is cheaper to produce and has a written serial number on it, which is used for identification. The read-write transponder is more sophisticated and its production costs are higher. However, it allows higher protection level and it offers variable data values that can be updated.

Classification of the RFID systems based on application areas is presented in Figure 3-7.

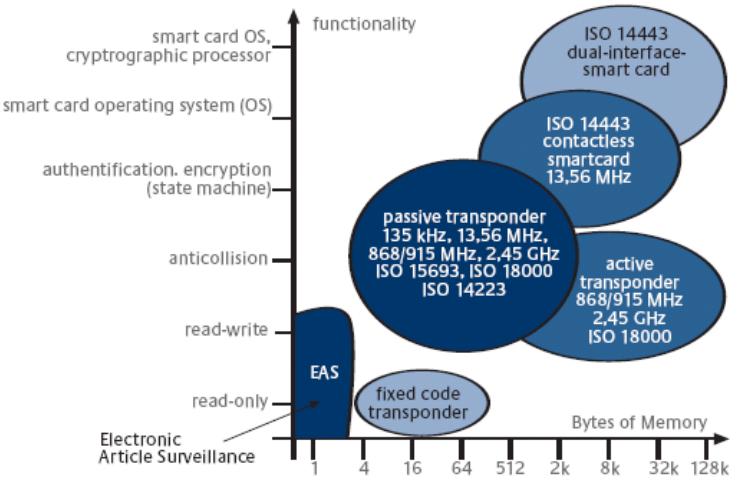

Figure 3-7: RFID system classification [Fink06]

3.5.3. Threats

Basic types of attacks on the RFID systems are presented in Figure 3-8 and are described as follows: [Bund04]

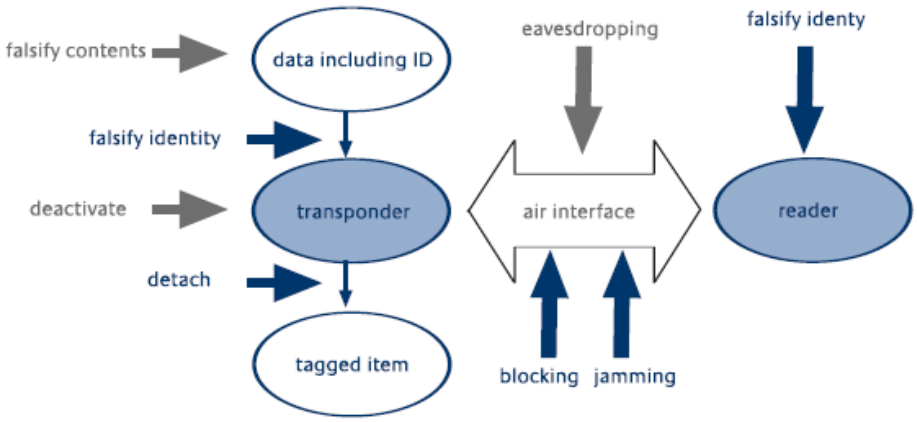

Figure 3-8: Basic attack types of on RFID systems [Bund04]

- Falsification of contents: In order to falsify the data on the transponder the attacker uses unauthorized write access to the transponder. Only under specific circumstances can this attack be classified as successful. These circumstances apply when the transponder's serial number or and other security information such as keys are unchanged, otherwise it might happen that the reader refuses

the connection to the transponder. Since serial numbers and other security relevant data are forbidden to manipulate, this kind of attack is possible only in the case of RFID systems that use transponders which store other information as well.

- Falsification of transponder identity: In this case the attacker deceives a reader into accepting the false transponder identity by obtaining the serial number and any security information of the real transponder. This means, using this technique it is possible to emulate or duplicate any kind of transponder. This kind of attack results in several transponders with the same identity being in circulation.

- Deactivation: This type of attack makes the transponder usable for detection or communication with the reader. The transponder is deactivated either through commands from terminal (delete or kill commands), or by physical destruction. Depending on the scale of the damage, the reader is not able to detect or to establish communication channel with the transponder in field.

- Detaching the tag: This attack is typically used for switching prices in stores. A transponder is separated physically from the tagged item and may subsequently be associated with a different item. Even though it may appear trivial at first sight, this type of attack poses a serious security problem, since the RFID systems are completely dependent on the unambiguous identification of the tagged items by the transponders.

- Eavesdropping: The communication between reader and transponder via the air interface is monitored by intercepting and decoding the radio signals. This is one of the most specific threats to the RFID systems [FiKe04].

- Blocking: So-called blocker tags simulate to the reader the presence of any number of transponders, thereby blocking the reader. A blocker tag must be configured for the respective anti-collision protocol that is used.

- Jamming: Data exchange via the air interface can be disrupted by passive means such as shielding or by active means (jamming transmitters). As the air interface is not very robust, even simple passive measures can be very effective.

- Falsifying reader identity: In a secure RFID system the reader must prove its authorization to the tag. If an attacker wants to read the data with his own reader, he must fake the identity of an authorized reader. Depending on the security measures in place, such an attack can be "very easy" to "practically impossible" to carry out. The reader might need access to the backend in order, for example, to retrieve keys that are stored there.

Another attack method is presented by Kfir and Wool. The “Relay attack” causes the reader to identify a remote card, which is not the device that is presented. This fact breaks the hidden assumption that the physical medium is secure and that the identified card must be very close to the reader device. Extending the reader to the card range using ghost and leech devices allows for the victim’s card to be at an unlimited distance. Ghost is a device which fakes a card to the reader, and leech is a device which fakes the reader to the card. Additionally, extending the reader to ghost range and the leech to card range significantly increase the attacker’s options: Larger distances mean no physical contact and no eye contact or security-camera exposure.

The authors of this study believe that attackers will appear whenever the financial gain is high enough. Low cost NFC technology will be on the shelves soon, and the upcoming credit cards based on contactless smartcard present a real temptation and high gain for attackers. The combination of high availability, low cost and easy profits may well cause the “Virtual Pick Pocket” attack to appear “in the wild” before long.

4. Biometric identification schemes and systems

The term biometrics is derived from the Greek words 'bios', which means life, and "*metrikos*", which means measure. People have used bodily attributes, such as voice and facial features for centuries in order to recognize each other. As technology is advancing, people are using more and more body characteristics for recognition and identification.

Most well known types of biometric identification schemes are listed below: [GaMe05]

- Facial geometry: analyses distance between facial features (eyes, nose, mouth)
- Voice: analyses the tone, pitch, cadence and frequency of a person's voice
- Fingerprint: analyses finger lines, pore structure
- Hand geometry: analyses the length of the fingers and shape of the hand
- Iris: analyses the coloured ring surrounding the pupil of the eye
- Retina: analyses the capillary vessels at the back of the eye
- Vein: analyses the patterns of veins, traces and shapes in the back of the hand and the wrist using infra-red light
- Ear form: measures dimensions of the ear
- DNA: carrier of human hereditary characteristics
- Signature: analyses writing using pressure and speed differentials
- Keystroke dynamics: analyses rhythm of keyboard strokes

The usual person identification requires a possession of an object or the knowledge of a specific secret. Identification with biometrics does not require these kinds of methods, since the secret and specific object is the human body with its characteristics. Flexibility, and the fact that it is much harder to forge bodily characteristics, gives the biometrics great advantage when compared with standard identification

procedures. However, lack of accuracy and complexity in some cases, makes it necessary to combine standard identification methods with biometrics.

Biometric system can be used either for identification or verification of a person as shown in Figure 4-1. Identification consists of recognizing the person by searching all saved biometric data in the system database. Verification involves the process of comparing the person's biometric data with a singe previously saved reference template. [JaRo04]

More precise definition was given by the ICAO in which verification is described as confirming identity by comparing identity details of the person claiming to be a specific living individual against details previously recorded on that individual, and identification as determining possible identity by comparing identity details of the presenting person against details previously recorded on a number of living individuals. [ICAO]

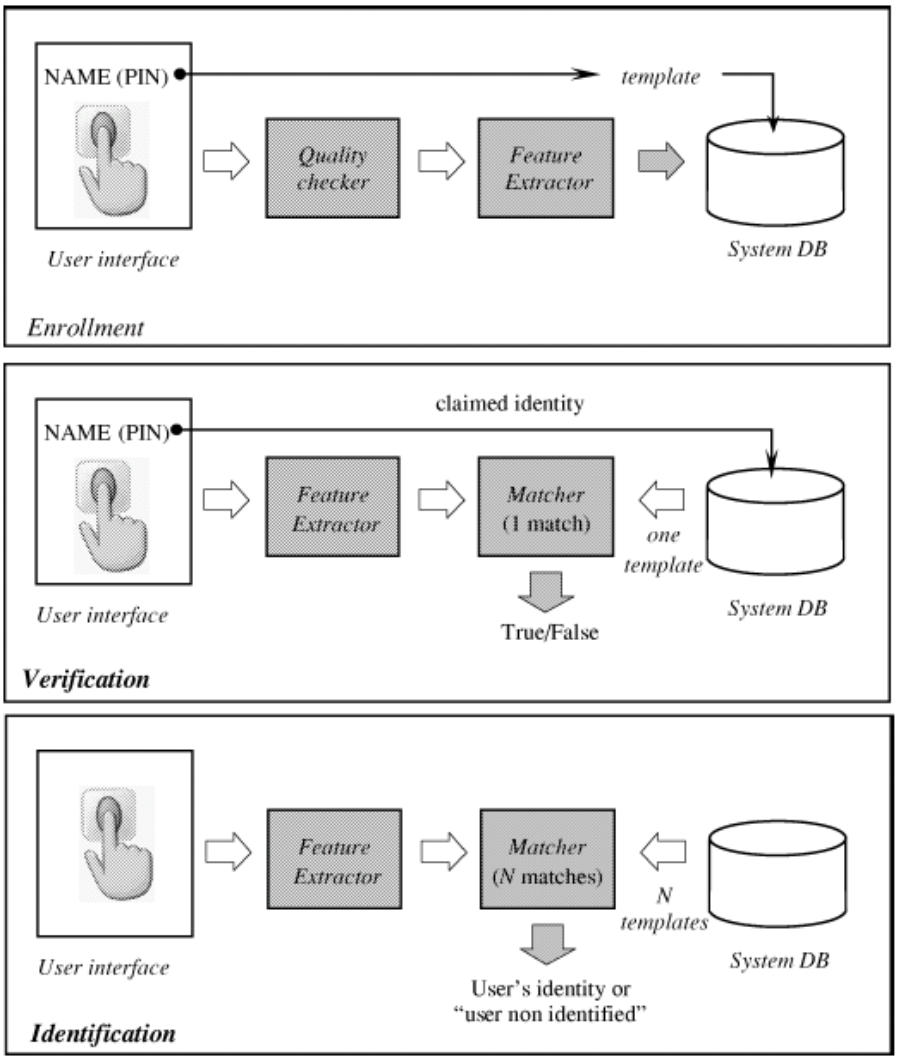

Figure 4-1: Enrolment, verification and identification in a biometric system

As shown almost every physiological or behavioural characteristic can be used as long as few ground principles are fulfilled: [JaRo04]

- Universality: each person should have the characteristic.
- Distinctiveness: any two people should be sufficiently different in terms of the characteristic.
- Permanence: the characteristic should be sufficiently invariant over a period of time.
- Collectability: the characteristic can be measured quantitatively.

These statements are more theoretical than practical. For the realization of practical biometric systems there are additional rules that need to be considered: [JaHo00]

- Performance, that is, a system's accuracy, speed, robustness and storage
- Acceptability, or the extent to which people are willing to accept a particular biometric identifier in their daily lives
- Circumvention, how easy it is to fool the system through fraudulent methods.

4.1. Legislative issues

There are many reasons for introducing national identification systems as previously discussed; especially the September 11the terrorist attacks made the whole world realize the presence of a new, more global threat. The September 11th events made governments and lawmakers around the globe address the implementation of national identification systems with new urgency in order to enhance their national security. Immediately after this tragic event the European Commission made a set of legal acts that will protect its interests. [PeSa02] These legal acts were designed to impose more control and security in the fields of illegal immigration, visa system and border control.

The EU Data Protection Directive is the legal basis for protecting personal data. This term is defined by the Article 2a of the EU Data Protection directive as „*any information relating to an identified or identifiable natural person ('data subject'), while an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". [EURO95]

The legal issues concerning biometric systems can be divided into the following categories: [Horn04]

- Choice of biometric identifier: Biometric methodology has to be universal and the system has to operate with high accuracy, false acceptance rate (FAR) and false recognition rate (FRR) should be less than 1 %. *See Chapter 4.2. for further information.*

- The issue of central database: As already mentioned, the majority of countries tend to use central, nationwide database containing all personal information. The goal of this type of structure is to prevent double identities and possible inconsistence in the databases.

- Use in private applications: Private institutions or individuals should not have access to biometric data without explicit consent of the holder.

- Back-up procedures: There is, and there will probably always be, a certain percentage of individuals that are unable to present the required biometric feature. Because of this countries have to *install back-up procedures to both ensure the secure identification of all persons, and avoid discrimination of those unable to enrol in the system.* [Horn04]

- Matching on the document: This possibility enables the document holder to verify himself with the document. This option is possible only with finger-printing and the controlling authority still has to trust that the document itself is not forged.

- Contactless interfaces: The use of a contactless chip has many advantages, such as durability, and it is therefore preferred by the ICAO for long-term identification documents. However, the document holder is at risk since he/she is not aware if the sensitive data is being loaded by unauthorized party.

- Usage of templates: Templates are being used in order to save storage space. Although this might be a preferable way of identification, since not all data is being read, it still comes with a risk of incompatibility with other countries and the templates they might be using.

- Use of encryption: Encryption is one of the ways to protect personal data. Although it is not completely safe and it cannot protect from a highly motivated attacker it can still prevent random persons from gaining personal biometric data.

4.2. Performance measuring

Performance of biometric systems is defined through their accuracy, speed, storage, usability and costs. Several error rates have been developed in order to quantify the performance of these systems. Because biometric systems are not perfect, some deviation concerning the accuracy and other parameters is to be expected. In example of fingerprint identification systems, two types of error decisions, i.e. two types of mistake, can be made by biometric systems: [BfSI04]

1. False Match – Two fingerprint images of different fingers are categorized as being identical.
2. False Non-Match – Two fingerprints of the same finger are categorized as being different.

False Match and False Non-Match errors are also referred to as the False Acceptance and the False Rejection.

These error rates are described in more detail below: [BfSI04; Brom02; GaMe05]

- **False Acceptance Rate (FAR)** measures the frequency with which a non authorized person is accepted as authorized. Since FAR is considered to be the most serious security error of a biometric system, it is important to take actions in order to prevent or minimize the damage. FAR can be also defined as:

$$FAR = \frac{\text{Number of comparisons of different fingers resulting in a match}}{\text{Total number of comparisons of different fingers}}$$

- **False Rejection Rate (FRR)** is the frequency with which an authorized person is rejected access. This is considered to be more annoying than dangerous. It is obviously recommended to keep the both values as low as possible.

Although the manufacturers claim that the value of the both measurements is as low as 0.0001%, the practical solutions show a much higher level. FRR can be also defined as:

$$FRR = \frac{\text{Number of comparisons of the same fingers resulting in a non - match}}{\text{Total number of comparisons of the same fingers}}$$

- **False Match Rate (FMR)** indicates a proportion of persons who, in the attribute comparison, were falsely accepted. Those attempts that were previously rejected due to a low quality (e.g. of the image) are, in contrast to FAR, not taken into consideration. Whether a falsely accepted attribute contributes to increasing the FAR or the FRR depends on the application

- **False Non-Match Rate (FNMR)** indicates a proportion of persons who, when comparing attributes, were falsely not accepted. Those attempts that were previously rejected due to a low quality (e.g. of the image) are, in contrast to the FRR, not taken into consideration. In the same way as with the FMR, whether a falsely non-accepted attribute contributes to increasing the FRR or the FAR, depends on the application.

- **Equal Error Rate (EER)** is defined at an operating point where the condition FMR = FNMR. The EER cannot be determined exactly. However, an EER range in which the error rates match can be established. This means that if the system is set accordingly, the same number of people will be falsely accepted and falsely rejected. Depending on the application, it can be useful to fix this operating point in such a way that different error rates are generated.

- **Failure To Acquire Rate (FTA)** specifies the rate at which a certain attribute cannot be acquired by the sensor in automatic mode. For example, the scanning of a fingerprint might be rejected even though the finger was placed on the sensor. The higher the measured value, the less the sensor is suited for acquiring the fingerprint. This means that this error rate becomes a parameter for evaluating the sensor.

- **Failure To Enroll Rate (FER)** refers to the ability of the system to successfully enrol biometric characteristics for a person. The FTE rates occur often in connection with systems which, by checking the fingerprint image quality, decide whether or not a template will be generated. This means that low quality fingerprint images will not be enrolled in the system. In this sense, the FTE is a parameter evaluating the capability of the algorithm to process low quality fingerprint images.

- **Failure To Match Rate (FTM)** indicates the percentage of enrolled biometric attributes which can neither be matched nor generally processed with the stored biometric templates. This shows the incapability of the system to make a decision, i.e. unlike in the case of false matches there is no result in which a wrong decision could be made.

In order to use biometric systems for different application areas, different settings for the FMR and the FNMR are used. For example, high security systems operate at a small FMR, while forensic applications operate at a high FMR. On the other hand civilian applications try to operate at both low FMR and low FNMR. The system's performance at all operating points can be shown in a ROC (Receiver Operating Characteristic) curve as shown in Figure 4-2.

This curve plots the FRR versus the FAR. The ROC curves are the standard approach for evaluating the performance of pattern recognition systems. They provide for objective comparisons in decision systems. Hence, they can be applied when comparing biometric systems in general and fingerprint recognition systems in particular.

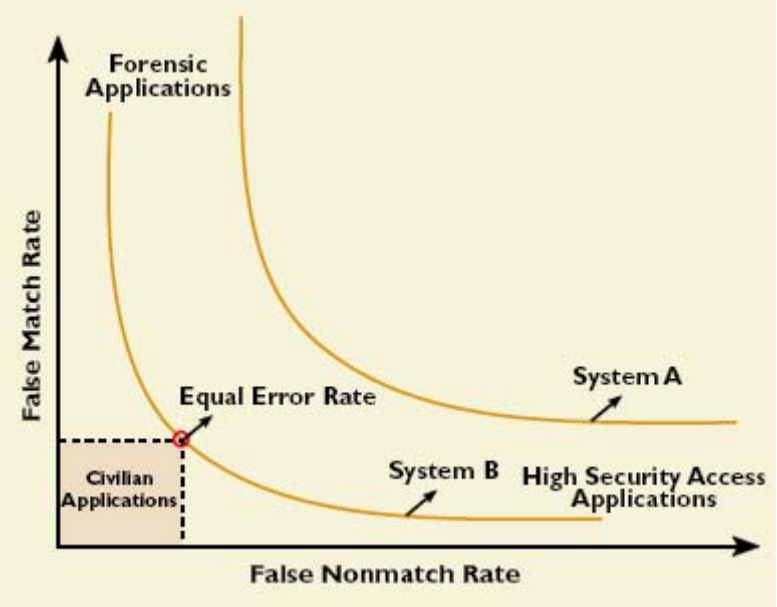

Figure 4-2: Receiver Operating Characteristic for different application areas [JaHo00]

4.3. Leading biometric technologies

Feature development of biometric characteristics of a person is defined through three factors; genetics, random development and behavioural development. Biometric methods that are based on genetics are face, hand geometry, finger geometry, DNA and voice. Random development is typical for fingerprint, iris, retina and vein structure biometric measurements, while behavioural development is applicable for signature and keyboard dynamics biometric methods.

Biometric technology is based on the collection of digital representations of physiological features unique to an individual as already stated above. This digital representation of biometric data is then usually transformed via specific algorithm to produce a template. It is security relevant issue that this algorithmic transformation is irreversible in order to stop possible forgers from obtaining the actual biometric attribute. These templates are then stored either in a centralized database that is accessed in order to compare the relevant biometric attributes, or they are stored in a decentralized way, e.g. on a smart card. The advantage is that no password has to be remembered since the authentication object is the actual body part. This option does not require a central database with all the user information, which is usually one of the greatest issues regarding privacy concerns. [Ploe99]

4.3.1. **Face recognition**

Among various biometric methods the previously mentioned facial images are probably the most common biometric characteristic used for personal identification. Another form of biometric measurement based on a human face is facial recognition. It is a non-intrusive, implicit identification method, measuring specific facial characteristics like a distance between eyes, nose or mouth. Because this method is non-intrusive it can be performed without awareness of a person to be identified. Potential application fields for effective facial recognition systems can be seen in many areas, e.g. law enforcement for mug-shot identification, verification and access con-

trol for personal identification such as driving licenses and credit cards, surveillance of crowd behaviour, anti-terrorism, as well as enhanced human computer interaction. [GaMe05]

The usage of the face recognition method can occur either in controlled or uncontrolled environment. In a controlled environment, the images are taken in a similar position (frontal, profile) and with a similar background colour so that a certain grade on standardization is achieved. The more interesting area of face recognition occurs in uncontrolled environment where the image capture conditions are far away from perfect. Different lightning, occluded faces, different poses, positions and face expressions, complex back-and foreground, more than one face in a single shot are just some of the conditions and disturbances that such a recognition system has to be able to process. [GaMe05]

Typical face recognition algorithm is described below: [Bund05]

- Create template
  - Make image
  - Find the face
  - Find the eyes
  - Find other attributes
  - Normalize the face
  - Extract attributes
  - Create template

- Create reference dataset
  - Quality check (Are there enough attributes)
  - Save the template

- Compare

Although the extensive studies were made regarding the automatic face recognition and there are numerous face-recognition systems available, it has still not been

proven that a human face can be used to reliably identify or verify an individual. Even though the manufacturers of automatic face recognition systems are specifying the FAR as low as 0.0001%, the field tests conducted by independent agencies show a much higher FAR level, meaning that this method is less accurate than described by the manufacturers. [JaHo97]

4.3.2. Fingerprinting

Fingerprint recognition has been developing for centuries, but it is officially used since the early 20th century and has replaced the Bertillon system which used skeletal features for personal identification. To understand the technique of fingerprint identification, first of all the biological principle has to be defined. A fingerprint is a pattern of individual epidermal ridges and furrows (valleys) and is been formed during the first seven months of pregnancy. The first application areas of automatic fingerprint- identification systems (AFIS) were law-enforcement agencies. In the 1960, the Federal Bureau of Investigation (FBI), United Kingdom Home Office and the Paris Police Department invested a large amount of effort in developing these systems and were so successful that automatic fingerprint-identification systems found their way into other sectors for civilian application. Since their first appearance automatic fingerprint- identification systems have greatly improved the effectiveness and reduced the costs for law-enforcement agencies. However, a number of design factors are still presenting obstacles in achieving desired performance. Also, these systems require a large amount of computational resources, especially in the identification mode. [JaHo97]

Various fingerprint types and a fingerprint classification schema of six categories is presented in Figure 4-3: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop.

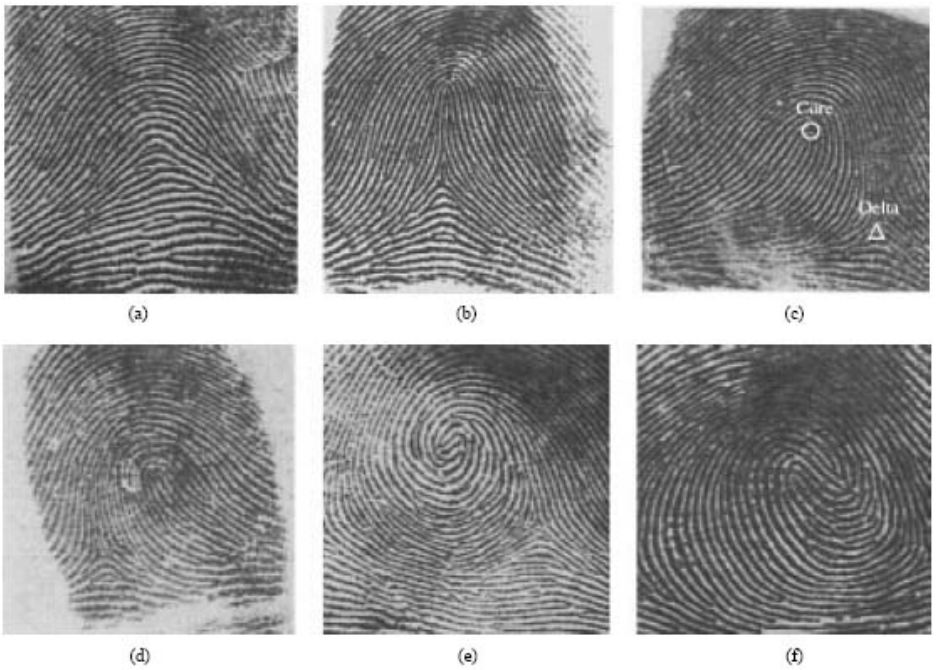

Figure 4-3: Six different fingerprint types [JaHo97]

An automatic fingerprint identity authentication system has four main design components:

- Acquisition
- Representation (template)
- Feature extraction
- Matching

More precise description can be given through the six steps for analysis of fingerprints proposed by the German Federal Office for Information Security in 2004 as shown in Figure 4-4: [BfSI04]

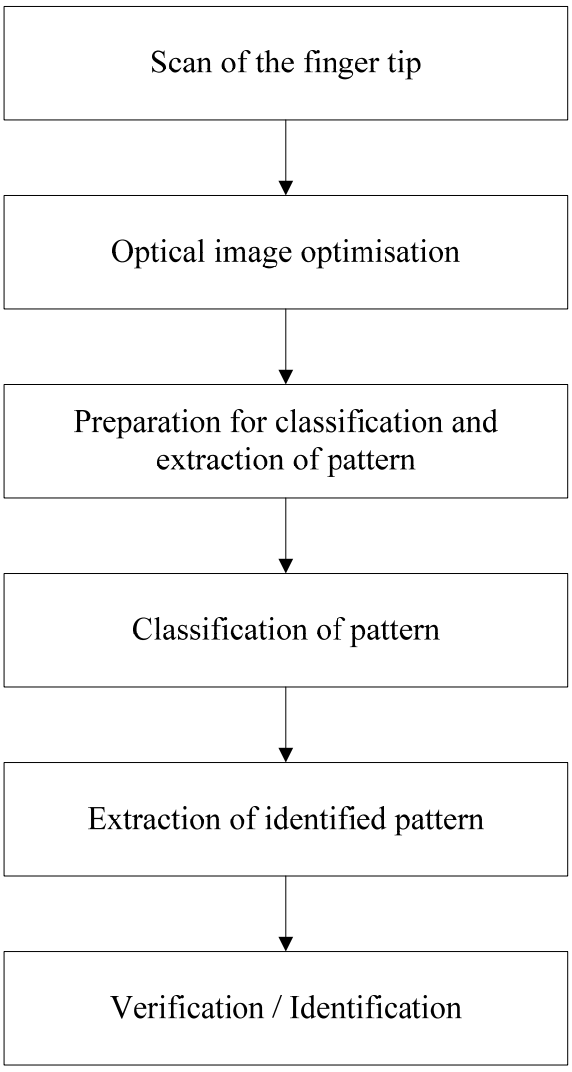

Figure 4-4: Fingerprint analysis procedure [BfSI04]

1. The first step is crucial for an automatic fingerprint identity system. The higher and better the image quality of a fingerprint, the less complicated are the following steps. The use of high-definition scanners, which are able to tolerate different skin types, damages, dryness, as well as the humidity of a finger surface, is highly recommended. The traditional offline method of scanning a picture of a fingerprint is rarely used. Various sensors for taking image of a fingerprint include: optical sensors, electromagnetic field sensors, polymeric thin film transistor sensors, thermal sensors, capacitive sensors, pressure sensors, ultrasonic sensors.
2. The second step is an optical improvement of the structures (ridges) on the scanned image, and this is done by optimizing contrast, light and other dis-

turbances. If the image, despite the effort to improve the quality, is still unusable, a new scan should be performed.

3. Preparation for classification and extraction of pattern or image processing represents the preparation phase for feature extraction and classification purposes.
4. In the fourth step, the pattern classification of a fingerprint is classified into one of the three principal fingerprint classes; loop, whorl or arch.
5. The fifth step is feature extraction. In this phase the location of the minutiae (ridge bifurcations and ridge endings) in a fingerprint is detected and extracted by using different algorithms. Ridge ending is defined as the end of a line, while ridge bifurcation is defined as a point in the ridge where the line is separated into two branches.
6. The sixth step entails performing matching check of the results from the step five with one or more stored templates.

4.3.3. Iris

The first usable iris biometric algorithm was developed and introduced in the early 1990s by John Daugman at the University of Cambridge. This method analyses individual patterns of iris. Iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side and is developed from between third and eight month of pregnancy. Since it is randomly and not genetically developed, each iris is unique and even irises of identical twins are different. Another important iris characteristic is time stability, meaning that the changes with time are minor. Iris identification systems are mostly equipped with monochrome camera and near infrared light source for better visibility of the iris structure. [NeCh00] Iris pattern example can be seen in Figure 4-5.

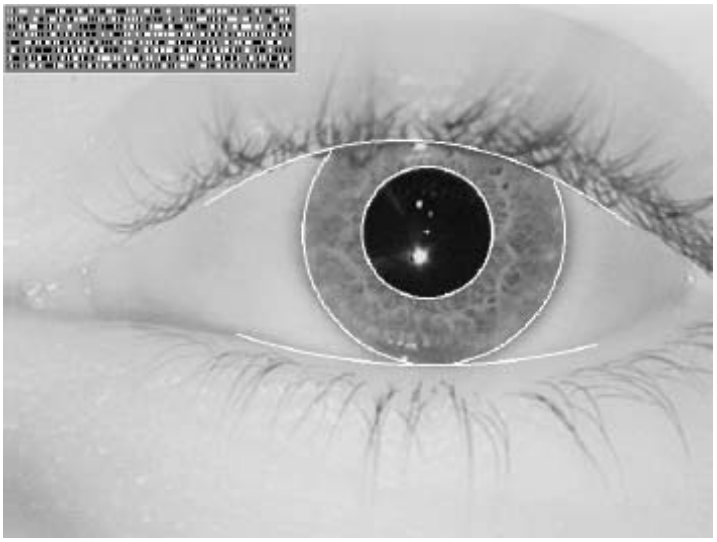

Figure 4-5: Example of iris pattern [Daug03]

Iris recognition is performed by converting an iris image into a numeric code which is essential for further use. For proper iris recognition it is necessary to have good-quality iris images with the person's iris in focus and correctly positioned. The iris code is calculated using eight circular bands that have been adjusted to conform to the iris and pupil boundaries. The entire method is presented in the Figure 4-6: [GaMe05]

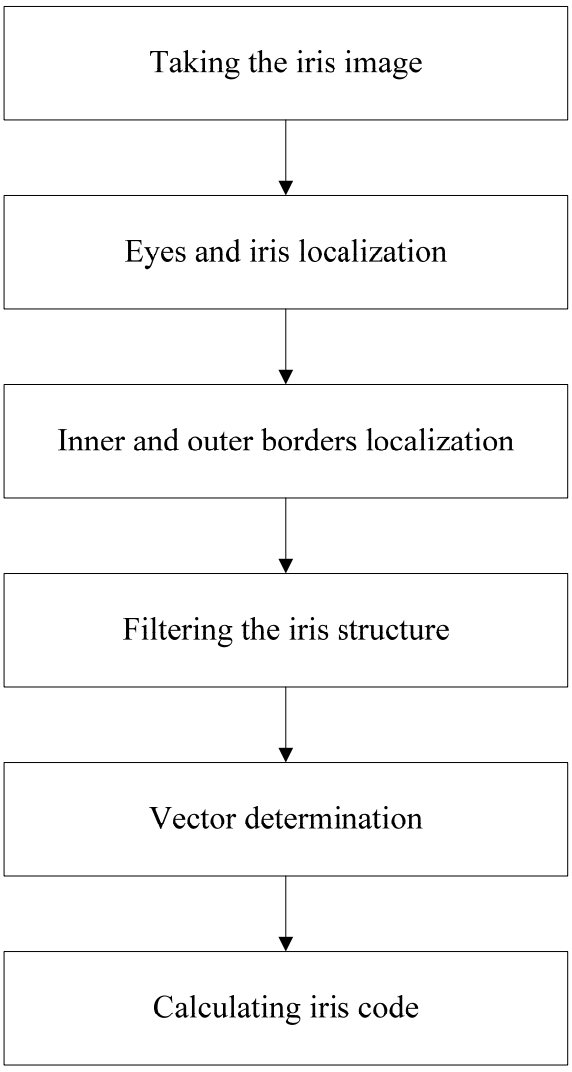

Figure 4-6: Iris analysis procedure [AmFi03]

The first step of this method is taking an iris image. This is conducted by using a pair of stereo wide-field-of-view (WFOV) cameras with near infrared light at a distance of 0.1 to 1 meter. The camera locates the eyes and iris of the subject to be scanned. Before taking the picture the visual obstacles, such as reflections, shadows or covered parts, have to be removed. Also the picture is rotated to compensate for a tilted head. Successful identification can be made through glasses and contact lenses, and at night, which offers higher flexibility and accuracy of the system. The resolution of the taken picture varies from 50 to 140 dpi. The next step defines the inner and outer borders of the iris. There are eight circular bands that have to be adjusted to conform to the iris and its inner and outer boundaries. Compared to other biometrical approaches, iris recognition has a high level of symmetry. This feature makes the crea-

tion of a template much easier because various deformations, such as iris contraction under the influence of light, are mathematically easily corrected. [NeCh00]

The circular structure is converted into lines filled with squares for easier extraction. In the next step the system looks at the patterns of light and dark iris areas and their distribution inside the grid. Each square that is lighter that a medium value is assigned value "1", and each square darker that medium value is assigned value "0". This process makes it possible to generate a 512-byte human bar code for that person. [GaMe05]

In order to verify specific subject, iris codes derived from this process are compared with the previously generated iris codes. The difference between two iris codes is expressed as a fraction of mismatched bits, named a Hamming distance. Hamming distance for two identical iris codes is 0. For two completely unmatched iris codes the Hamming distance is 1. For unmatched irises, the average Hamming distance is about 0.5, which indicates a 50 percent difference in the codes. For two different images from the same iris, the Hamming distance ranges from approximately 0.05 to 0.1. A Hamming distance of 0.32 can reliably differentiate authentic users from impostors. [NeCh00]

4.3.4. Other

Since the ICAO recommended primarily the usage of the above described biometric methods for implementing the MRTDs, other biometric methods are jointly described in this chapter.

Hand geometry. A variety of measurements of the human hand can be used as biometric attributes as its shape, length, widths and bending of the fingers are unique. This method has been used in the last 20 years, mostly in the USA. The method starts with taking an image of the subject's hand. If the image is lower quality or some disturbances are visible, algorithm should neutralize them. The referring points are found and finally the calculation of the reference points is conducted. The current

systems reach the FAR between 0.0001% and 0.1% and the FRR between 0.0007% and 1.0%. An equal error rate (ERR) 0.1% has been reported. [GaMe05; JaRo04]

Retinal scan. The pattern formed by retinal vasculature is stable and unique and is considered to be the most secure biometric method, since it is not easy to change or replicate the retinal vasculature. It is a characteristic of each individual and each eye. *"A digital image of retinal vasculature can be acquired by projecting a low-intensity beam of visual or infrared light into the eye and capturing an image of the retina using optics similar to a retina scope."* [JaHo00] The image acquisition requires a high cooperation of the person, since the person has to focus on a specific spot, which affects the public acceptance of this method.

Signature is considered to be a trusted method for user verification. It is used in many application areas, including legal, financial and government agencies. Each person has a unique style of signing. However, the variations from a typical signature also depend upon the physical and emotional state of a person. Signature identification can be static or dynamic. Static signature identification uses geometric forms for signature verification, while dynamic signature identification uses dynamic features, such as pressure, acceleration and velocity, to determine the authenticity of the signature. Advantage of such a system is a wide population acceptance. [GaMe05]

Voice print represents a combination of physiological and behavioural biometrics. Although voice print of a person is distinctive, it may not contain sufficient invariant information to offer large-scale recognition. A disadvantage of voice-based recognition systems is that speech features are sensitive to a number of factors such as background noise. [Mark00]

A brief comparison of biometric techniques categorized based on these ground principles are presented in the Table 4-1.

Biometrics	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Iris	high	high	high	medium	high	low	high
Hand geometry	medium	medium	medium	high	medium	medium	medium
Hand vein	medium	medium	medium	medium	medium	medium	high
Retinal scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice print	medium	low	low	medium	low	high	low

Table 4-1: Comparison of biometric technologies [JaHo97]

However, the categorisation of biometric techniques can be based on different criteria, as introduced by Scheuermann and shown in Table 4-2

Biometrics	Expense	User friendliness	Maintenance level
Face	medium	high	medium
Face Thermograph	medium	high	medium
Fingerprint	medium	low	medium to high
Iris	high	high	medium
Hand geometry	high	medium	medium
Hand vein	medium	low	medium
Retinal scan	high	high	medium
Signature	medium	low	medium
Voice print	low	low	low

Table 4-2: Alternative comparison of biometric technologies [Sche00]

It is of the outmost importance to point out that all of the comparisons stated above are to be taken with a great reserve since they tend to be incomplete, preliminary or even subjective due to a fact that their accuracy is sometimes not testable and given by the manufacturer.

The summary of all the technologies listed and described, as well as an overview of their pros and cons is shown in the following table. Please note that the warning given previously also applies for this comparison.

Biometrics	Pros	Cons
Face	➢ contactless ➢ use of standard devices ➢ party compatible with paper documents ➢ continuous control	➢ inconsistent with aging ➢ light and temperature dependable ➢ party positioning needed ➢ privacy issues
Fingerprint	➢ unique ➢ consistent ➢ easy to use ➢ low-cost	➢ skin condition dependent ➢ positioning needed ➢ system incompatibility ➢ no life detection ➢ low public acceptance
Iris / retina	➢ unique ➢ consistent ➢ contactless	➢ positioning needed ➢ cost-intensive ➢ possible health issues
Hand geometry	➢ no skin condition de-pendency ➢ low FER ➢ easy to use ➢ fast	➢ low accuracy ➢ applicable only on adults ➢ no life detection ➢ cost-intensive
Signature	➢ compatible w. standard devices ➢ public acceptance ➢ statement of intention	➢ low accuracy ➢ inconsistent ➢ time-consuming enrol-ment
Voice print	➢ no physical presence needed ➢ easy to use ➢ use of standard devices ➢ statement of intention	➢ low accuracy ➢ inconsistent ➢ time-consuming enrol-ment ➢ easy to manipulate

Table 4-3: Pros and cons of selected biometric systems [BeRo00]

4.4. Privacy issues

Storing biometric data is the most controversial part of the whole national identification implementation process. Some privacy organizations see these actions solely as an opportunity for governments to collect a huge amount of personal data for intelligence and surveillance purposes. If we add in the fact that the effectiveness of biometrics is highly debatable, the privacy concerns become even more reasonable. The main question is how to preserve individual privacy, while continuing to protect national security.

Many international discussions that are led about biometrics have defined a set of categories that need to be applied in order to protect one's privacy and still provide security for the whole society. These categories include the following: [GaMe05]

- Biometric system should be transparent and any participation should be on a voluntary basis: Making a system transparent is not a sensitive issue, but the whole concept of national identification cannot be only on a voluntary basis. Individuals with bad intentions are not likely to register themselves voluntarily.

- Only information needed for specific application should be collected and no raw data should be saved. In order to avoid racial and discrimination profiling no raw data should be saved since it is not necessary for the verification or identification process.

- Biometric data and personal information should be kept separate: Biometric data should be secured and encrypted during the registration and storage. Also personal information, such as name or address, should not be linked to biometric data.

- Bodily privacy should be protected (health information): For instance during an iris scan certain health issues can be revealed, e.g. alcoholism

- Secret data assessment should be forbidden: One of the biggest controversies was the identification system in Tampa, Florida during the American Football Super Bowl in 2001 where almost every visitor was scanned, identified and stored.

- Unique identifier should not be directly linked to a person: Every state can decide which biometric technology to use but fingerprints can be considered as a general purpose identifier. Links between unique identifiers and personal databases should be avoided.

- Biometric data should be strictly protected: Governments must take all necessary technical and organisational measures to protect personal data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access.

- Accuracy of the biometric systems should be high: the false acceptance rate (FAR) and the false recognition rate (FRR) should be less than 1 %.

Finally, one should mention some of the current programs and organizations monitoring and consulting governments with privacy issues:

- The International Biometric Group
- BioPrivacy
- PRIME project

5. Travel Documents in National Identification Systems

After presenting an overview regarding functionality of different technologies and biometric methods used in identification systems, the MRTD (Machine Readable Travel Documents) and the MRP (Machine Readable Passports) and TD-1 and TD-2 (Size 1 and Size 2 Machine Readable Official Travel Documents), present a concrete implementation of all the above mentioned technologies.

In order to able to understand the MRTD, it is advisable to look into the definitions of the few important terms.

MRTD (Machine Readable Travel Documents) is an *official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine.* [ICAO06]

MRZ (Machine Readable Zone) is a *fixed-dimensional area located on the MRTD data page, containing mandatory and optional data formatted for machine reading using OCR methods.* [ICAO06]

As already stated before the main purpose of the national identification systems, where the MRP and TD-1 and TD-2 represent one part of the system, is to on one hand protect the citizens form various threats and abuse of their identity and on the other to give government more control over the state and people living in it. The balance between these two parties is very important and sometimes very hard to achieve, especially when it comes to issues like privacy.

In order to accomplish certain standardization in travel documents international organizations have prepared the guidelines and technical requirements for all the member states. In many cases these guidelines are not mandatory. However no large scale disputes have been noted between the member states. It is in every state's interests to issue a valid and worldwide readable travel document.

Different techniques are available to read the MRTD. Techniques presented in this work offer automatic person identification. This makes the whole identification process faster, more reliable and comfortable. Furthermore the standardization process is much easier to implement. Available techniques shall be discussed in more detail further on.

5.1. Standards and organizations

5.1.1. **ICAO**

The International Civil Aviation Organization (ICAO), an agency of the United Nations, codifies the principles and techniques of international air navigation and fosters the planning and development of international air transport to ensure safe and orderly growth.[WWW1]

The ICAO was founded in 1944 at the Chicago Convention and today it is a specialized agency incorporated in the United Nations. It has 190 member states and its main activity is to develop standards for international civil aviation. Its headquarters are located in the Quartier International of Montreal, Canada.

The ICAO defines and standardizes the following functions for use in the airline industry: [WWW2]

- Aeronautical Message Handling System
- International Standard Atmosphere
- Machine-Readable Travel Documents

The organisation has developed the following Strategic Objectives for the period 2005-2010: [WWW2]

- Safety - Enhance global civil aviation safety
- Security - Enhance global civil aviation security
- Environmental Protection - Minimize the adverse effect of global civil aviation on the environment
- Efficiency - Enhance the efficiency of aviation operations
- Continuity - Maintain the continuity of aviation operations
- Rule of Law - Strengthen law governing international civil aviation

The core of the ICAO work concerning MRTDs is done by the Technical Advisory Group on Machine Readable Travel Documents TAG/MRTD, which was established in 1984. In 1998, the New Technologies Group of the TAG/MRTD started developing more effective systems for biometric identification in MRTDs. Their earlier TAG/MRTD work was assembled and published in a document with their reference DOC 9303. This document represents a starting point for every state intending to introduce a state of the art travel documents and presents de facto a standard for MRTDs. The DOC 9303 consists of three parts: [WWW3]

- Part 1 - Machine Readable Passport - Volume 1; Passports with Machine Readable Data Stored in Optical Character Recognition Format
- Part 1 - Machine Readable Passport - Volume 2; Specifications for Electronically Enabled Passports with Biometric Identification Capabilities
- Part 2 - Machine Readable Visas
- Part 3 - Size 1 and Size 2 Machine Readable Official Travel Documents

5.1.2. ISO / IEC

Another organization responsible for issuing standards and guidelines in the field of MRTD is jointly operated by the ISO, the International Organization for Standardization, and the IEC - the International Electrotechnical Commission. The standard concerning travelling documents is defined by the ISO/IEC Joint Technical Committee 1, which is responsible for Information Technology. The subcommittee 17 as a part of the JTC1 has developed the standard for Cards and Personal Identification and consists of the following standards: [WWW4]

- ISO/IEC 7501-1:2005, Identification cards - Machine readable travel documents - Part 1: Machine readable passport

- ISO/IEC 7501-2:1997, Identification cards - Machine readable travel documents - Part 2: Machine readable visa

- ISO/IEC 7501-3:2005, Identification cards - Machine readable travel documents - Part 3: Machine readable official travel documents

- ISO/IEC 14443, Identification cards -- Contactless integrated circuits

The standard ISO/IEC 7501 is an endorsement in a short form of the specific parts of the International Civil Aviation Organization (ICAO) Doc 9303. The ISO/IEC JTC 1 will undertake its consideration for endorsement as a new fifth edition of ISO/IEC 7501.

5.2. Identification methods used for travel documents

This chapter undertakes a short overview of the available and standardized automatic identification methods. The following figure illustrates these methods and their relationship to each other.

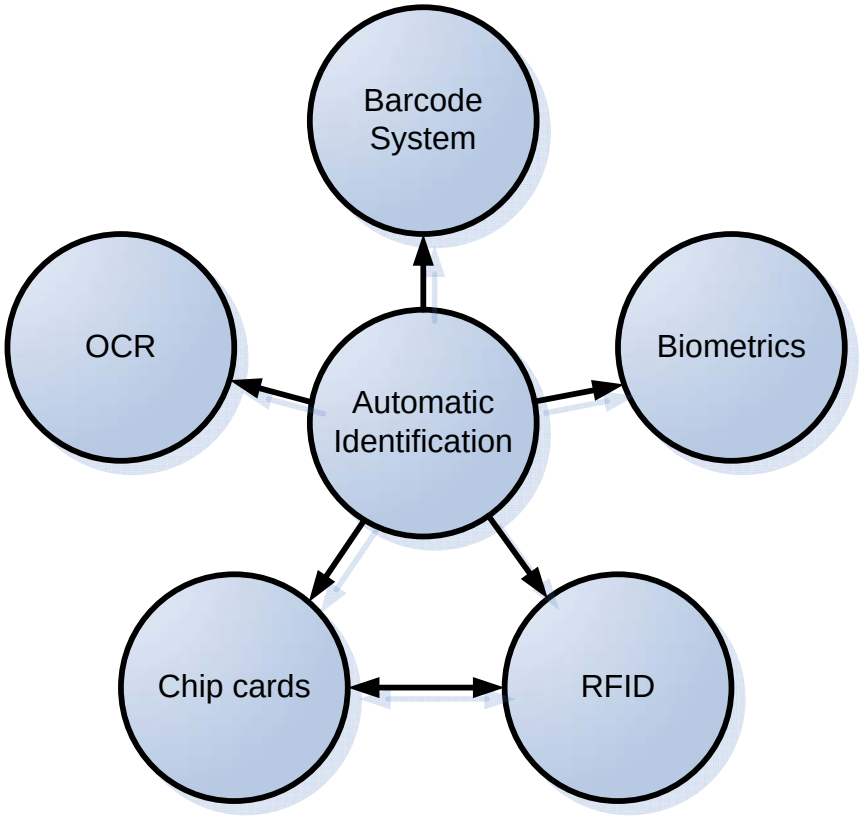

Figure 5-1: Automatic Identification Systems [Fink06]

5.2.1. Barcode systems

A barcode represents machine-readable information in a form of dark lines on light background. The pattern of dark lines and white spaces in a specific order represents numeric or alphanumeric information. Barcodes are read using optical scanners which register a different reflection of dark lines and light spaces. Originally barcodes used only lines to encode information but today they also come as a pattern of

dots, concentric circles and as text codes hidden within the image. Another version of barcode is a matrix code also known as a 2D barcode. This code also consists of dark and light areas but it can store far more data on the same amount of space. [Fink06]

5.2.2. Optical Character Recognition (OCR)

OCR is usually an electronic translation of images into usable data. In the OCR process optical devices, such as cameras or optical readers, make an image of a document or another object that needs to be identified. They transform this image into data that can be saved or edited. The OCR is used in MRTDs and this will further discussed in the following chapters.

Other systems such as biometric systems, chip cards or the RFID systems have been described in detail in the earlier chapters and therefore will not be further discussed. Table 5-1 shows a comparison of the above mentioned identification systems.

System/Parameter	Barcode	OCR	Biometrics	Chip card	RFID
Amount of data/ Bytes	1~100	1~100	depends	16~64k	16~64k
Data density	low	low	high	very high	very high
Machine readability	good	good	complex	good	Good
Person readability	limited	easy	difficult	hard	hard
Environmental influence (dirt, humidity)	very high	very high	depends	possible (contacts)	none
Device cover	total failure	total failure	depends	depends	none
Influence by position and side	low	low	depends	high	none
Abrasion	limited	limited		limited (contacts)	none
Acquisition cost	very low	medium	very high	low	medium
Operation expenses	low	low	none	medium	none
Unauthorized coping	easy	easy	hard	hard	hard
Reading speed	low ~ 4 s	low ~ 3 s	very low > 5 s	Low ~ 4 s	fast
Max distance (reader – item)	0 - 50cm	< 1cm	direct contact	direct contact	0 - 10m

Table 5-1: ID systems comparison [Fink06]

5.3. Machine readable passports

MRP (Machine Readable Passport) is *a passport conforming with the specifications contained in Doc 9303 normally constructed as an ID-3 size book containing pages with information on the holder and the issuing State or organization and pages for visas and other endorsements. Machine readable information is contained in two lines of OCR-B text, each with 44 characters. These specifications permit the MRP to be in the form of a free-standing card of ID-1 size.* [ICAO06]

MRPs' data page consists of two major parts. The first part is called VIZ (Visual Inspection Zone) and the second part is called MRZ (Machine Readable Zone). The VIZ is divided into five zones and contains mandatory elements in a standard sequence which represent the minimum requirements for the MRP data page. The zones are as follows: [ICAO06]

- Zone 1: Mandatory header
- Zone 2: Mandatory and optional personal data elements
- Zone 3: Mandatory and optional document data elements
- Zone 4: Mandatory holder's signature or usual mark (original or reproduction)
- Zone 5: Mandatory identification feature
- Zone 6: Optional data elements.
- Zone 7: Mandatory machine readable zone

Zone 1

- Issuing state or organization
- Name of document
- Type of document
- Issuing state or organization code
- Passport number

Zone 3

- Date of issue
- Authority of issuing office
- Date of expiry
- Optional document data elements

Zone 2

- Name – primary identifier
- Name – secondary identifier
- Nationality in full
- Date of birth
- Personal number
- Sex
- Place of birth
- Optional personal data elements

Zone 4

- Holders signature or usual mark

Zone 5

- Holder's portrait

The MRZ contains two lines, each holding 44 characters. The first line holds information about the holder, such as their first and second name, issuing state and document art. The second line holds holder's date of birth, sex, expiry date and various check digits. In the Figure 5-2 the green area represents the VIZ and the red area the MRZ.

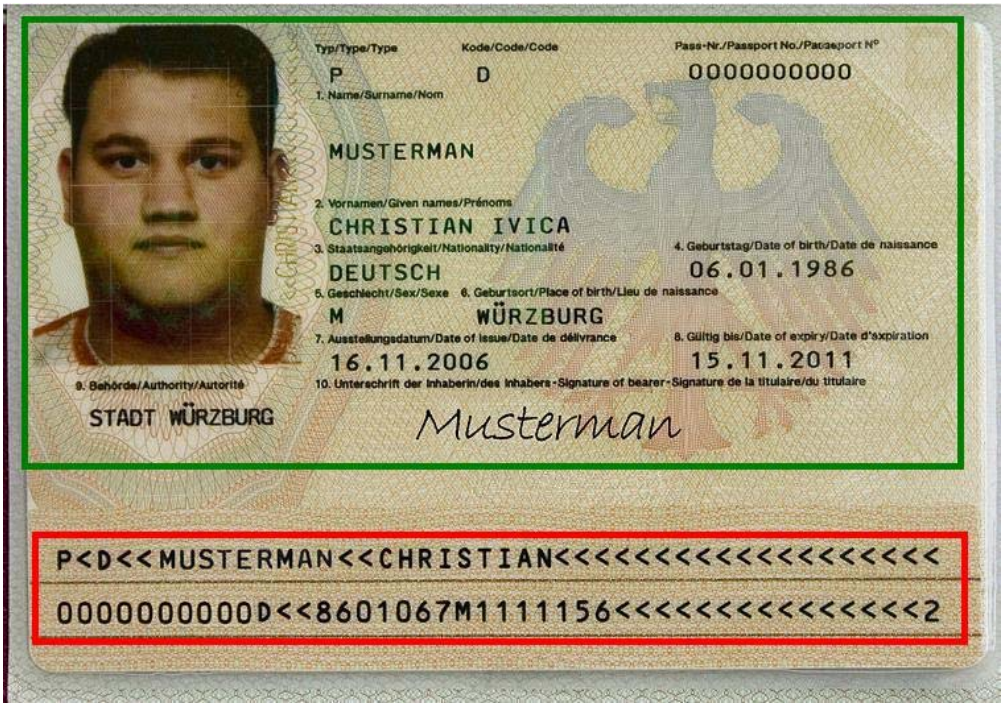

Figure 5-2: Passport front page [WWW5]

5.3.1. **Issuing passports**

Passport issuing process can be different from state to state, but some similarities can be drawn for all states. The first stage is application process when, depending on the state, certain documents have to be provided. The second phase is checking and verifying applicant's identity and provided documents. Assuming all checks are successfully concluded the last phase takes place when the passport is printed and issued to the applicant. In order to guarantee passport security features and to prevent identity forgery, it is very important to undertake various security measures during this process. This ensures that the potential for later security risks is significantly reduced. The following figure represents the passport issuing process in the United States. [GAO02]

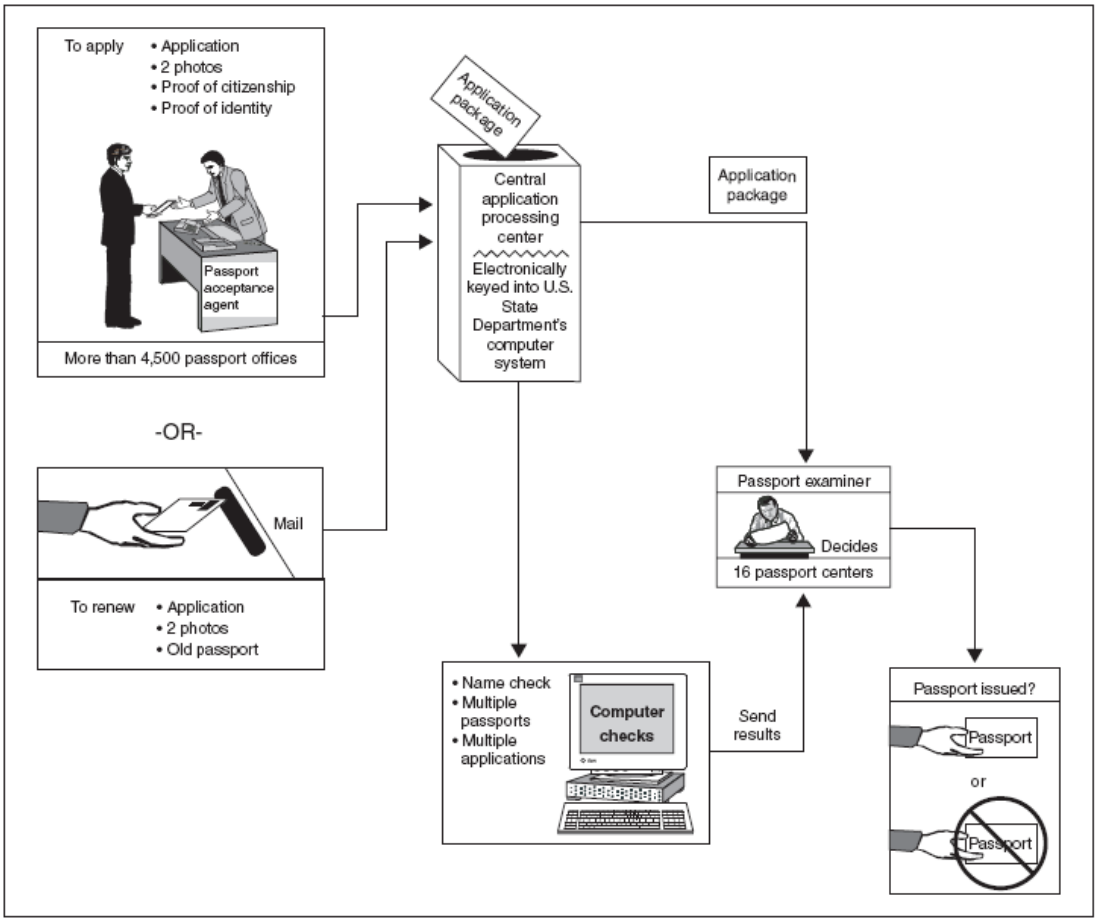

Figure 5-3: Passport issuing process [GAO02]

5.3.2. **Electronic Passport**

Electronic Passport *is a machine readable passport containing a contactless Integrated Circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder, and a security object to protect the data with PKI cryptographic technology, and which conforms to the specification of Doc 9303, Part 1*. [ICAO06]

Figure 5-4: Austrian Electronic Passport

Every Electronic Passport must have an appropriate symbol on its covers in order to identify it as such. Figure 5-4 shows Austrian Electronic Passport with a special symbol at the bottom of the page. Only a MRP with a contactless chip and memory capacity of at least 32kB may carry this symbol. Through the years of research the ICAO came with a list of accepted biometric features.

The primary biometric identifier is a high quality digital image saved on a chip. The secondary biometric identifiers are fingerprint and iris images, also saved on a chip as high quality images. The primary identifier is mandatory while the secondary

identifiers are optional. Another information stored on a chip is a copy of the MRZ with basic information about issuing state, issue date etc. These elements are defined through the Logical Data Structure (LDS) for Electronic Passports, which is also a part of the ICAO's Doc 9303. The LDS covers topics about mandatory and optional data elements, ordering and grouping of data elements, format of data elements and security principles concerning reading and writing data elements into a contactless IC.

The first considerations that the TAG/MRTD was given from the ICAO member states can be summarized in five points: [ICAO06]

- Global interoperability
- Uniformity
- Technical reliability
- Practicality
- Durability

The Doc 9303 gives a detailed description on image storage, compression and cropping, storage of the biometric and other data in a logical format in a contactless IC, placement of the contactless IC in the MRP etc.

Furthermore, the ICAO in its Doc 9303 also gives a typical business process for reading Electronic Passports. This process can be adapted for each state's needs but the basic diagram can be seen in Figure 5-5.

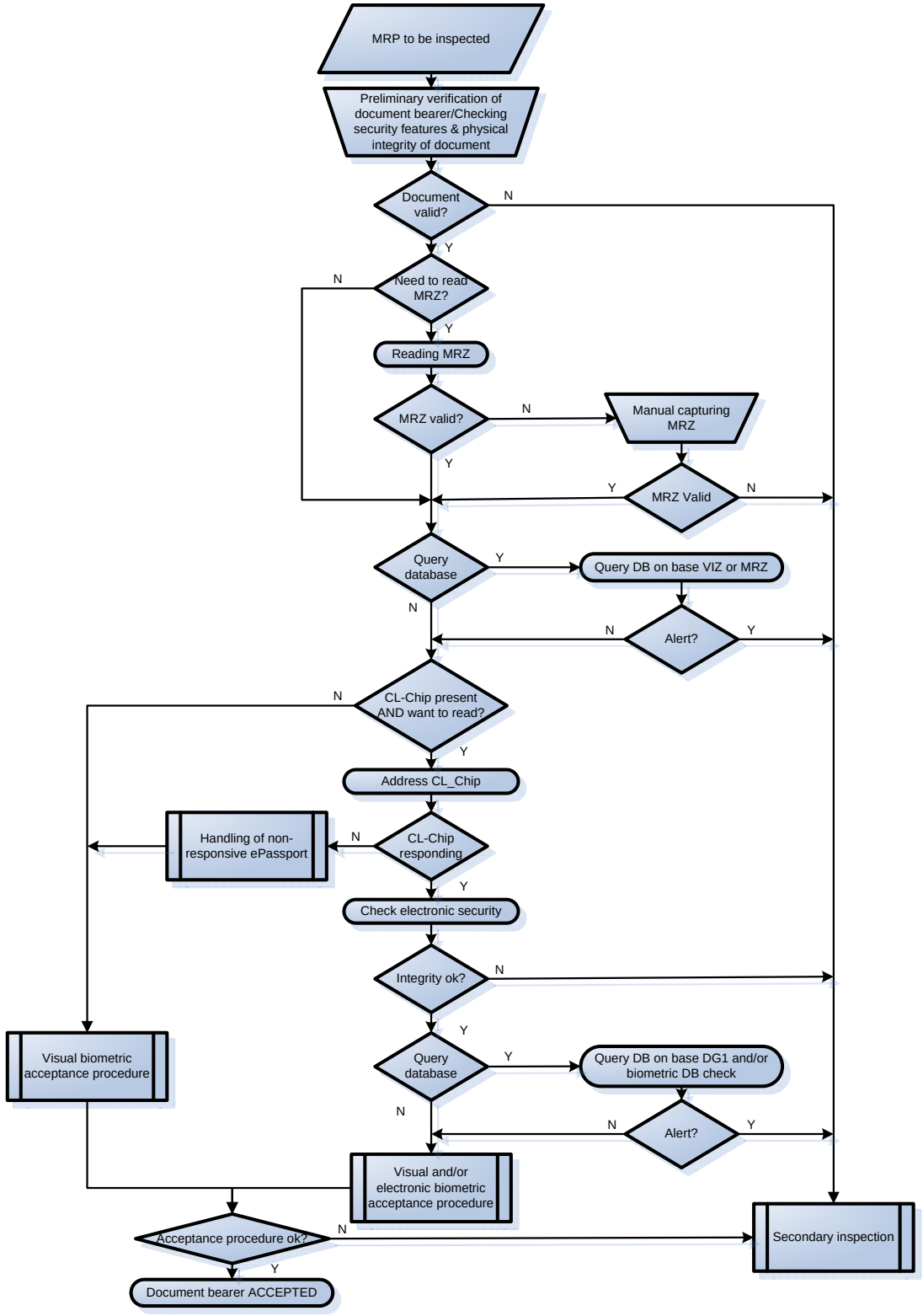

Figure 5-5: Typical Business Process for reading Electronic Passports [ICAO06]

5.4. Machine readable ID cards

Identification cards are also defined in the ICAO's Doc 9303 as size 1 and size 2 machine readable official travel document (TD-1 and TD-2). This is a *card with nominal dimensions guided by those specified for the ID-1 and ID-2 type card (ISO/IEC 7810) (excluding thickness). In the case of a plastic card which carries any optional, additional data storage technology, the reading of which requires it to be inserted into a slot reader (i.e. magnetic stripe, optical memory or integrated circuit with contacts), the TD-1 and TD-2 conforms to the precise dimensions and tighter tolerances specified in ISO/IEC 7810.* [ICAO02]

Similar to machine-readable passports are machine-readable official travel documents that also have a machine-readable zone and a visual inspection zone. TDs are also as in the MRPs divided into seven zones, where the seventh zone represents the MRZ. The zones contain the following information: [ICAO02]

Zone 1

- Issuing state or organization
- Type of document

Zone 2

- Name – primary identifier
- Name – secondary identifier
- Sex
- Nationality
- Date of birth
- Optional personal data elements

Zone 3

- Document number
- Date of expiry
- Optional document data elements

Zone 4

- Holders signature

Zone 5

- Holder's portrait

Zone 6

- Optional data elements

In Figure 5-6 the front side of an Estonian Size 1 machine readable official travel document is presented. This ID card also contains a chip (red area) that can contain biometric data. The green area represents a scanned signature. Front side contains zones from 1-5.

Figure 5-6: Estonian ID Card, front side

The back of an Estonian Size 1 machine readable official travel document is presented in Figure 5-7. The back contains zones six and seven. It is also important to mention that the member states are allowed to implement further security features such as holograms or special printing techniques as represented in the green area. The red area represents the MRZ. In the case of TD-1 and TD-2 the MRZ contains three machine-readable lines, unlike the MRP which contains only two machine-readable lines.

Figure 5-7: Estonian ID Card, back side

5.5. Security and privacy issues

The ICAO as a leading organisation for implementing the standards for the machine readable travel documents identified the following threats to documents security, its issuance, use and fraud possibilities: [ICAO06]

- Counterfeiting a complete travel document
- Photo-substitution
- Deletion/alternation of text in the visual or machine readable zone of the MRP data page
- Construction of a fraudulent document, of parts thereof, using materials from legitimate documents
- Removal and substitution of entire page or visas
- Deletion of entries on visa pages and the observations page
- Theft of genuine document blanks
- Impostors (assumed identity; altered appearance)

As a countermeasure to the threats mentioned above the ICAO made a list of basic security measures that each member state should implement. Furthermore, the advanced measures have been defined and it is recommended to the member states to apply these measures as well. The countermeasures are listed below and Table 5-2 shows the threats and the basic security solutions: [ICAO06]

- Substrate materials
- Security printing
- Protection against copying
- Personalization technique
- Additional security measures for travel documents
- Quality control
- Security control of production and product

Threats	Security solutions
Photo-substitution	➢ Integrated biodata page ➢ Guilloche overlapping portrait ➢ Secure laminate or equivalent
Alternation of the biodata	➢ Reactive inks ➢ Secure laminate or equivalent
Page substitution	➢ Lock stitch or equivalent ➢ Unique biodata page design
Deletion or removal of stamps and labels	➢ Reactive inks ➢ Chemical sensitizers ➢ High-tack adhesives (labels) ➢ Permanent inks (stamps)
Document theft	➢ Good physical security arrangements ➢ Control of all security components ➢ Serial numbers on blank documents ➢ Secure transport of blank documents ➢ Internal fraud protection system ➢ International exchange on lost and stolen documents

Table 5-2: Threats and basic solutions [ICAO06]

Kc and Karger identified in their Research Report the security vulnerabilities that lead or could lead to privacy issues. The focus of their work is on the machine readable passports with integrated IC, (so called?) electronic passports. Their study does not involve political or civil liberties issues concerning privacy, but only technical issues. Although the new electronic passports brought many advantages they still have some problems, especially regarding the actual design decisions made in the standards. They defined the primary security deficit as follows:

The primary breach in the security of the electronic passports arises from the invalid assumption that all communications in which a passport chip may participate are secure and legitimate. [KcKa05]

Furthermore they identified the following privacy issues: [KcKa05]

- Stalking selected passport holders
- Identity theft
- Unauthorized distribution of sensitive data
- Movement pattern - which countries did the passport holder visited

Due to the security vulnerabilities there are several privacy issues arising. Juels, Molnar and Wagner came to the following conclusion:

The secrecy requirements for biometric data imply that unauthorized reading of e-passport data is a security risk as well as a privacy risk. The risk will only grow with the push towards unsupervised use of biometric authentication. [JuMo05]

The conclusion that Kc and Karger proved is that carefully planed and implemented cryptographic and other security measures will significantly enhance security of electronic passports and make them practically forge-proof. It is never possible to guarantee 100% security but the current ICAO's plans include especially weak protection measures that make the security and privacy issues still a weak spot of the new electronic passport. [KcKa06]

6. Identification infrastructure project in the Republic of Croatia

6.1. National Border Management Information System

As a part of the Stabilisation and Association Process, which represents the European Union Framework support for peace, stability and prosperity in South-East Europe, Croatia has become a part of the CARDS assistance programme. The CARDS (Community Assistance for Reconstruction, Development and Stabilisation) programme should help Croatia to bring its structures closer to those of the European Union. The CARDS program supports the overall economic and social development in order for Croatia to fulfil its obligation to the Stabilisation and Association Process.

The budget for the CARDS assistance for Croatia in the period 2001-2004 was € 249 million. The beneficiary of the CARDS program was the Croatian Border Police. The following projects were realized: [CAIM05]

- CARDS 2001 "Integrated Border Management (IBM) - Border Police" Twinning (Budget: € 500.000):

- CARDS 2001 "Integrated Border Management-Interagency Co-operation" (Budget: € 6.800.000):

- CARDS 2002: "Development and Implementation of a National Border Management Information System" (Budget: 2.500.000 €):

- CARDS 2003: "National Border Management Information System – Phase 2" (budget: € 2.000.000)

- CARDS 2003: "Continued Support and Capacity Building for the Border Police" (Budget: € 500.000)

- CARDS 2003 "Capacity Building in the area of illegal migration" (Budget: € 1.150.000)

This discussion will focus on two projects from the CARDS program:

- CARDS 2002: "Development and Implementation of a National Border Management Information System" (Budget: 2.500.000 €):
- CARDS 2003: "National Border Management Information System – Phase 2" (budget: € 2.000.000)

These two projects were to bring Croatia in-line with the leading countries in this area and to fulfil the requirements for the European Union and the Schengen Information System. It is based on the state-of-the-art technologies including fingerprint reader, passport reader, RFID-chip handling and several vehicle observation modules. The goal was to contribute to public safety and migration control in Croatia and its European neighbour countries and is a part of the establishment of a modern information society in the country.

Typical border control framework is presented in Figure 6-1:

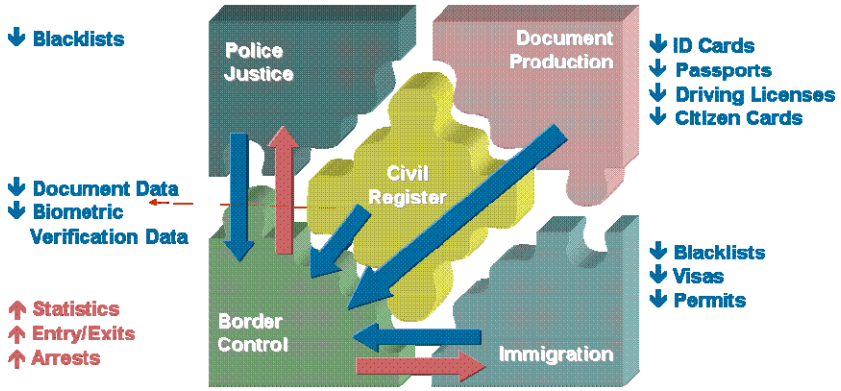

Figure 6-1: Border Control Framework

6.1.1. Project description

The goal of the NBMIS (National Border Management Information System) is to aid border control police officials to execute their daily tasks on border crossings. These daily activities include control of passengers, control of travel documents, objects and vehicles at entering and leaving of the country.

The NBMIS should be able to ensure automatic query in the existing centralized database of the Ministry of the Interior information system as well as to store the collected data. Furthermore, the NBMIS must contain a centralized database under the authority of the Border police Directorate.

The NBMIS must ensure the following basic functions: [RCMI05]

- Scanning of the travel document
- Verification of passengers and travel documents and search in the centralized database.
- Verification of protection elements of the travel documents
- Verification of the visas validity
- Verification of fingerprints
- Verification of photographs
- Scanning of the vehicle license plates
- Verification of vehicles in databases
- Verification of the registration documents of the vehicle
- Counting and classification of vehicles crossing the state border
- Verification of objects and search in the centralized database (weapons, works of art etc)
- Issuing of documents on the border crossing
- Update of the collected data
- Supervision activities
- Reports and statistics

The NBMIS is a state-of-the-art border control solution. It is based on open standards such as SOAP, XML, HTTP(S), HTML, JDBC, LDAP etc. The usage of the IBM DB2 database is used to take advantage of a reliable, high-end RDBMS and to provide large scale transaction processing, speed and reliability.

The central and the local databases have compatible structures. This enables the following:

- Seamless migration of data between databases, which means that data, edited centrally, is distributed to local databases and vice versa
- Significant reduction of the chances for replication failures
- Enhanced scalability (new databases can be added without significantly affecting the existing ones).

The projects security features provide means for preventing unauthorized access, system integrity protection and secure and reliable data transfer. The internal protection of the system is achieved by using usernames/passwords and the user roles. The NBMIS enables administrators to add new or redefine existing user security roles. All user activities performed in the NBMIS are being logged and saved to the database.

6.1.2. **Phase I**

Phase l of the NBMIS project included installation and calibration of the passport and fingerprint readers, hardware and software installation, network development and other activities needed to start-up the first phase of the project. In the central location a new application server and a new storage system were to be installed. The following boarder crossing were affected in Phase l: [RCMI02]

- Central location (Police HQ)
- Bajakovo border crossing (land)
- Airport Pleso border crossing (air)
- Police academy

The corresponding system architecture is shown in Figure 6-2.

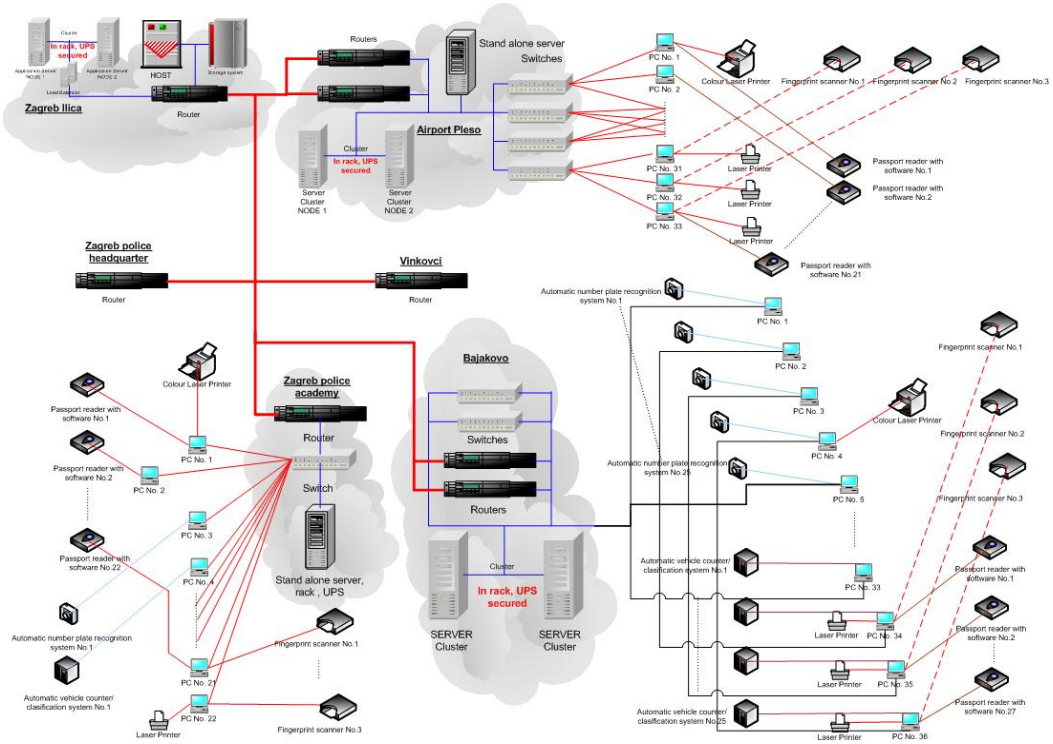

Figure 6-2: IT-Hardware Architecture [RCMI02]

6.1.3. **Phase II**

In the second phase the NBMIS project was extended to six road border crossing points (Stara Gradiška, Slavonski Brod, Slavonski Šamac, Županja, Gunja, Karasovići), one air border at the international airport Split, to the regional police headquarters in the towns of Dubrovnik, Vinkovci, Slavonski Brod and Split and the Ministry of Interior central system in Zagreb. The complete infrastructure is constructed into three levels and is similar to the organizational structure of Ministry of Interior. The hardware architecture is shown in Figure 6-3: [RCMI05]

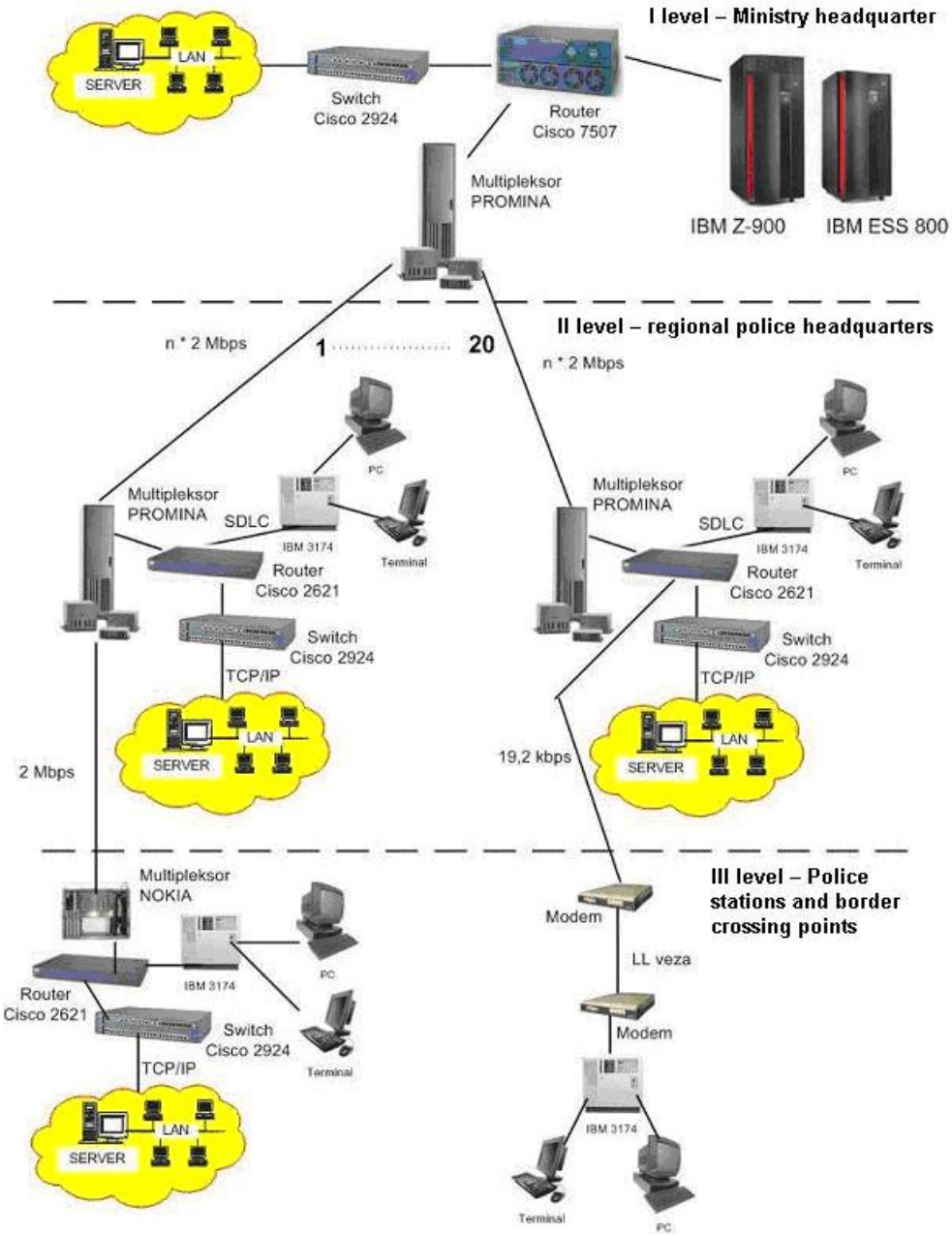

Figure 6-3: IT-Hardware Architecture Phase II [RCMI05]

6.2. Croatian Personal Identity Card

6.2.1. **Project description**

In accordance with the international standards relating to personal and travel documents (ICAO Doc 9303), the Parliament of the Republic of Croatia passed a "Law on Personal Identity Card" on 23 January 2002, establishing the content and the shape of the new personal identity card. The law envisages that the new identity card can be produced centrally in one place, while the requests for its issue can be placed in the place of applicants' residence.

The project "New Personal Identity Card" bridges the gap between traditional information technologies and new technologies. By using all the positive values of the mainframe computer (stability, scalability, high degree of availability and safety) it upgrades the existing solutions using Web, Intranet/Internet and Java technologies and an asynchronous transaction server.

6.2.2. **Process description**

- The citizen submits a request for an identity card at the police administration or station in the place of residence (front office)
- The request is received and recorded in the central base of the MUP RH. Subsequently, a form is made with the submitter's personal data.
- The data is written in the Latin alphabet and in the alphabet of a national minority if the submitter requires it
- The submitter's photo is placed on the form and the print of his/her index finger's papillary lines is taken
- The submitter's photo is glued on the written form and the submitter signs his name on the form
- The submitter is issued with a receipt confirming that he has submitted a request and his existing identity card remains with him

- The request is filed in the work order and is passed on for further processing
- The form is scanned and all the data from the form are stored in the local relation database (DB2 UDB) in a police station. This is done without the presence of the party (back office).
- When the papers of the work order have been scanned, their transfer to the central computer of the MUP RH (mainframe) is initiated (textual and pictorial data). This process is automated with the support of the IBM WebSphere MQ software product. The pictures are stored in the DB2 database on the mainframe. The Data transfer is confirmed to the data sender, that is, to the police administration, with the WebSphere MQ
- . Text and pictures are sent from the MUP RH to the authorized legal person responsible for the production of identity cards (Commercial Affairs Agency, Zagreb - AKD). The delivery must be confirmed to the MUP RH via the WebSphere MQ.
- Based on the received data, the AKD commences the production of identity cards.
- . After identity cards have been produced, a message is sent to the MUP RH using the WebSphere MQ detailing which identity cards have been made.
- The citizen comes to the police station, takes the new identity cards in person and leaves the old one to be invalidated. The whole process of identity card issue is done electronically, which enables permanent supervision over the entire procedure.

The hardware architecture for this process is shown in Figure 6-4.

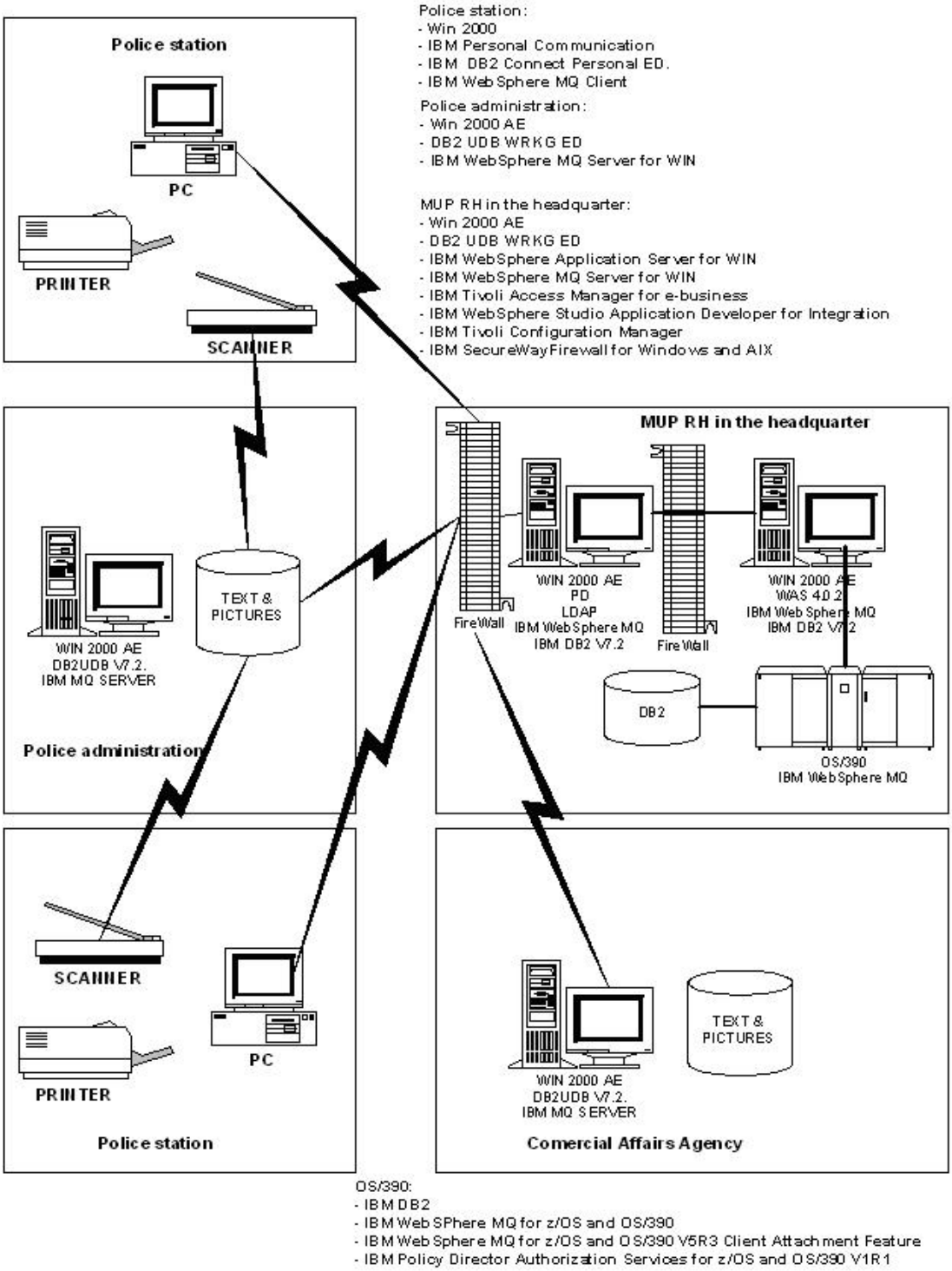

Figure 6-4: Hardware Architecture for issuing ID cards

7. Conclusion

After an initial defining of the notions relevant to this work, the smart cards and RFID are described in detail since they represent the key stone of the new identification processes. Different smart cards variations are available and their classification is described in detail. A special place was given to the RFID systems because of their great role in the new machine readable passports, so called electronic passport. Biometric methods are directly relevant to the RFID technology because biometric information found on electronic passports is stored and read from a contactless integrated circuit. Functionality, characteristics and threats to RFID systems should help reader to better understand this topic.

Which biometric identifiers are used is defined by the international organizations ICAO and ISO. Their work defines the new machine readable passports and size 1 and size 2 machine readable official travel document (TD-1 and TD-2). The summary of their research is published in the Doc 9303 which provides all the information needed for the member states to implement these standards. It is very important for all member states to use the guidelines given by these organisations in order to keep travel documents standardized and readable all over the world. Three main biometric measurements are accepted as a standard in machine readable travel documents; fingerprint, facial recognition and iris scan. Furthermore, performance measuring showed which biometric technologies are suitable for which application fields. In the first phase is expected that many countries will implement only fingerprint measurement and later on additional safety features.

It was clear from the beginning that the national identification projects are going to be controversial. Privacy and security issues are the biggest area of dispute. Civil rights organizations claim that these measures implemented by governments are just an opportunity to establish more control over their citizens. Furthermore, they claim that security leaks directly endanger privacy of individuals. These claims are in part correct since the security measures are not ideal. However, all the innovations im-

plemented in the new machine readable travel documents represent enormous improvements compared to the old passports. The ICAO and the ISO are constantly developing new standards in order to improve the security situation.

As already mentioned ICAO set standards for Machine Readable Travel Documents. This thesis showed different identification methods used for travel documents as well as detailed description of the new electronic passports. Furthermore, the processes concerning issuing and reading electronic passports are presented graphically and verbally.

To sum up, the electronic passports, biometric technology and national identification projects in general need time to adapt to the users' expectations. This thesis presented a relatively undisputed National Identification project in Republic of Croatia (National Border Management Information System). The Croatian government saw this project as an opportunity to enhance their border security and at the same time make one more step towards European Union. It was also in the EUs interest to strengthen their borders to the South East Europe. This project was developed in two phases. First phase was CARDS 2002 project: "Development and Implementation of a National Border Management Information System" and its successor was CARDS 2003 project: "National Border Management Information System – Phase 2" with total budget of € 4.500.000.The presented thesis clearly shows …. 1 Abschlußsatz!

Bibliography

[AmFi03] Amberger, M., Fischer, S., Rößler, J., *Biometrische Verfahren – Studie zu State of the Art*, Erlangen, 2003.

[BeRo00] Behrens M., Roth, R. (2000): *Sind wir zu vermessen, die PIN zu vergessen?* In Datenschutz und Datensicherheit, 2000

[BfSI04] Bundesamt für Sicherheit in der Informationstechnik, *Study: "Evaluation of Fingerprint Recognition Technologies – BioFinger"*, 2004

[Bund04] Bundesamt für Sicherheit in der Informationstechnik, *Risiken und Chancen des Einsatzes von RFID-Systemen*, 2004

[Bund05] Bundesamt für Sicherheit in der Informationstechnik, *Gesichtserkennung*, 2004

[Brom02] Bromba, M., *BioIdentifikation*, 2002

[CAIM05] Centre for Administrative Innovation in the Euro Mediterranean Region, Administrative *Reform, Innovation and Maintenance in Croatia*, 2005

[ChSe93] Chow Sherman, Serinken Nur, Shlien Seymour, *Forgery and tamper-proof identification document*, IEEE, 1993

[Daug03] Daugman John, *How Iris Recognition Works*, 2003

[EURO95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Official Journal L 281, p. 31, available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

[FiKe04] Finke, T., Kelter, H., *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*. BSI, 2004

[Fink06] Finkenzeller Klaus, *RFID Handbook*, John Wiley & Son Ltd., 2006.

[Floe06] Floerkemeier Christian, *Infrastructure Support for RFID Systems*, 2006

[GaMe05] Gasson, M., Meints, M., Warwick, K. (Eds.), FIDIS Deliverable 3.2, *Study on PKI and Biometrics*, Frankfurt a. M. 2005. See http://www.fidis.net/487.0.html

[GAO02] United States General Accounting Office, *Technology Assessment, Using Biometrics for Border Security*, 2002

[Gene04] General Services Administration, *Government smart card handbook*, 2004

[Hild05] Hildebrandt Mireille (2005), *Privacy and Identity*; in: Erik Claes and Antony Duff (ed.), Privacy and the Criminal Law, proceedings of the Conference on Privacy and the Criminal Law 14th-15th May 2004, to be published 2005

[Horn04] Hornung Gerrit, *Biometric Identity Cards: Technical, Legal, and Policy Issues*, 2004

[Huse99] Husemann, D, *The smart card: don't leave home without it*, IEEE Concurrency 7, 2 (April–June 1999), 24–27.

[ICAO06] Doc 9303, *Part 1 - Machine Readable Passport - Volume 1; Passports with Machine Readable Data Stored in Optical Character Recognition Format and Volume 2; Specifications for Electronically Enabled Passports with Biometric Identification Capabilities, Sixth Edition*, ICAO, 2006

[ICAO02] Doc 9303, *Part 3 - Size 1 and Size 2 Machine Readable Official Travel Documents, Second Edition*, ICAO, 2006

[JaHo00] Jain Anil, Hong Lin, and Pankanti Sharath, *Biometric identification*, February 2000/Vol. 43, No. 2 Communications of the ACM, 2000

[JaHo97] Jain Anil, Hong Lin, Pankanti Sharath and Bolle Ruud, *An Identity-Authentication System Using Fingerprints*, Proceedings of the IEEE, Vol. 85, No. 9, September 1997

[JaRo04] Jain Anil, Ross Arun, and Prabhakar Salil, *An Introduction to Biometric Recognition*, IEEE transactions on circuits and systems for video technology, Vol. 14, No. 1, January 2004

[JuMo05] Juels A, Molnar D, Wagner D, *Security and Privacy Issues in E-passports*, 2005

[Kapl96] Kaplan Jack M., Smart Cards, *The Global Information Passport* (New York: International Thomson Computer Press, 1996), 69-75.

[KcKa05] Kc Gaurav, Karger Paul, *Security and Privacy Issues in Machine Readable Travel Documents (MRTDs)*, IBM Research Report, 2005

[KcKa06] Kc Gaurav, Karger Paul, *Preventing Attacks on Machine Readable Travel Documents (MRTDs)*, IBM Research Report, 2006

[KfWo05] Kfir Ziv and Wool Avishai, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005

[Mark00] Markowitz Judith, *Voice biometrics*, Communication of the ACM, Vol. 43, No. 9, September 2000

[Mead34] George H. Mead, *Mind, Self and Society*; Chicago Press 1934.

[NaHi05] Nabeth, T., Hildebrandt, M. (Eds.), FIDIS Deliverable D2.1, *Inventory of topics and clusters*, Frankfurt a.M., 2005. See http://fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf.

[NeCh00] Michael Negin, Thomas A. Chmielewski Jr., Marcos Salganicoff, Theodore A.Camus, Ulf M. Cahn von Seelen, Péter L. Venetianer, Guanghua G.Zhang, *An Iris Biometric System for Public and Personal Use*, IEEE, 2000

[Nguy03] Thien-Loc Nguyen, *National Identification Systems*, MIT 2003

[Otte05] Otter Heinz, *Die e-card im internationalen Vergleich*, 2005.

[PeSa02] Petermann Thomas, Sauter Arnold, *Biometrische Identifikationssysteme*, 2002

[Ploe99] Van der Ploeg Irma, *Written on the Body: Biometrics and Identity*, Computers and Socety, March 1999

[PRCl03] Privacy Rights Clearinghouse, *Reducing the risk of identity theft*, 2003, see also: http://www.privacyrights.org

[PRCl04] Privacy Rights Clearinghouse, *Identity theft victims guide*, 2004, see also: http://www.privacyrights.org

[RaEf03] Rankl Wolfgang, Effing Wolfgang, *Smart Card Handbook*, 3rd Edition, 2003

[RCMI02] Republic of Croatia, Ministry of Interior, *CARDS 2002 – NBMIS – Phase I, Technical specifications*, 2002

[RCMI05] Republic of Croatia, Ministry of Interior, *CARDS 2003 – NBMIS – Phase II, Technical specifications*, 2005

[Sche00] Scheuermann D, *Usability of Biometrics in Relation to Electronic Signatures*. GMD-Report 118, 2000

[ShPr02] Shelfer Katherine M. and Procaccino J. Drew, *Smart card evolution*, Communications of the ACM, July 2002/Vol. 45, No. 7.

[SCAl03] Smart Card Alliance, *Privacy and secure identification systems: The role of smart cards as a privacy-enabling technology*. A Smart Card Alliance White Paper, Feb. 2003. http://www.smartcardalliance.org/.

[USDJ06] US Department of Justice, *Identity theft and fraud*, 2006, see also: http://www.usdoj.gov/criminal/fraud/idtheft.html

[ZoOt94] Zoreda Jose Luis and Oton Jose Manuel, *Smart Cards*, Artech House, Inc., 1994, 5-6.

[ICPP03] Independent Centre for Privacy Protection, *Identity Management Systems (IMS): Identification and Comparison Study*, 2003

Web links

[WWW1] en.wikipedia.org/wiki/International_Civil_Aviation_Organization, visited on 21.04.2008

[WWW2] http://www.icao.int/icao/en/strategic_objectives.htm, visited on 23.04.2008

[WWW3] http://mrtd.icao.int/content/view/33/202/, visited on 23.04.2008

[WWW4] http://www.iso.org/, visited on 23.04.2008

[WWW5] http://de.wikipedia.org/wiki/Reisepass/, visited on 25.04.2008