EUROSMART

The Voice of the Smart Security Industry

# White paper

# Smart Biometrics for Trust and Convenience

December 2010

*Disclaimer*

*Eurosmart has taken reasonable measures to ensure the quality of the information contained in this document. However, Eurosmart will not assume any legal liability or responsibility for the accuracy, reliability or completeness of any information contained herein or for any consequences of its use.*

**Index**

## *Foreword by the Eurosmart Chairman*

Our Industry has designed and developed biometric solutions for more than 10 years now. Our vision has been always that personal data and especially biometric references should be stored in a smart card.

We are now at the front of very new era with significant deployment in the eID market. And today the global privacy protection issue opens emerging opportunities in almost all Smart Security market segments.
Biometric solutions can positively contribute to reducing ID fraud or payment card skimming, reinforcing trust in electronic transactions, and improving the convenience of security solutions.

Our Biometrics Task Force has done an impressive job, gathering and formatting key expertise amongst our members and proposing many relevant use cases for the future. This White paper will become a reference document for any stakeholder or end user that wants to consider Biometric technologies.
All forms of biometrics are considered, even though some are more adapted to smart security and targeted applications. Today Eurosmart members have the capacity to industrialize the Biometric solutions described in this document, and together they have the willingness to support any interoperability definition that may be necessary.

As a natural consequence to this initiative, Eurosmart will demonstrate a host of applications at its Biometrics booth at Cartes'10!

Enjoy your reading!

Marc Bertin
EUROSMART Chairman

## *Introduction*

The development of Biometrics is a result of political, economic and technological globalisation. The world is now a global place for trade, migrations, transfers and reliable exchanges of all kind of information and values, physically and / or remotely. This can give rise to new risks, problems, fraud, illegal traffic, identity theft or even terrorism. Biometrics is seen as the best solution for identification or authentication as it is directly linked to the person (whoever he /she is). Identity theft has been classified as the fastest growing white collar crime since the mid-1990s. For goods and documents that also need to be guaranteed as genuine or identified / authenticated, some technologies may be used that can be classified as biometrics for objects.

However there are privacy and ethical concerns that must be taken into account.

In the opinion of Eurosmart, “the Voice of the Smart Security Industry”, technology does not have an intrinsic value, either good or bad. Biometric technology must both provide security benefits and ensure respect for ethical concerns and protection of privacy. This objective will be easier to manage when biometrics is combined with smart card technology.

This paper aims to make recommendations on the use of biometrics for cases of identification and authentication of individuals and goods. It is aimed at governments and organizations that have a primary role and responsibility for implementation of electronic identities, with safeguarding of privacy and to secure themselves and their people against those who seek to do harm, travel illegally, or commit fraud.

This White paper is divided into four parts. Part 1 provides general information about biometrics and gives a tour of biometrics, i.e. a presentation of the different forms of biometrics.
In Part 2, the objective is to provide detailed and comprehensive information about biometric concepts and use.
Part 3 develops biometric use cases with a focus on the most promising markets and recommendations from the Smart Security Industry.
The appendix in Part 4 provides additional information on the documentation used for the White paper, as well as a glossary about Biometrics.

# 1. Information

## *1.1. The need for biometrics*

Some thousands of years ago, Chinese pottery makers used to put their fingerprints on their products. Over a hundred years ago fingerprint analysis was introduced for criminal investigations. In the first case, the goal was to identify and authenticate the origin of the product (object), in the second case; the major concern was to identify criminals and offenders (people).

Biometrics is a characteristic of human morphology or behaviour. In the identification, or authentication process of an individual, the use of biometrics provides accuracy and eliminates many of the risks of fraud. However there may be some political, religious, public and private concerns when biometric techniques are used. Eurosmart recommends that biometrics should be used for electronic identity documents as it is certainly the most efficient technique, and also in respect of protection of privacy and other ethical concerns.

With the globalization of world trade, there is a huge flow of people and goods. In order to prevent piracy / terrorism, and counterfeiting as much as possible, there is a need to use reliable identification and authentication methods. The use of biometric techniques allows identification - for instance of one individual within a population - or authentication – that is to say verifying a claimed identity – as a result of the study of physical characteristics that vary from one individual to any other.

When we talk about biometrics, we can deal with the physical characteristics of people or objects that are used successfully, but also behavioural characteristics (for which we are more at the experimental stage).
Some are emergent like voice and smell. New technologies based on chaotic elements can be used for manufacturing what we can call the object biometrics.

In a dematerialized world the identification / authentication process is based on what you own (a key, a card …), what you know (PIN code, secret), who you are (biometric characteristics), or any combination of these. The confidence level is of course dependent on the number of methods that are used to authenticate and identify the individual. The use of one is less safe than the use of several of these methods. In general, it is better to use a combination of the "element owned and biometrics" type which gives a very high level of confidence. The use of known information can be subject to disclosure and indiscretion and is especially less reliable over time.

In this context, biometrics is emerging as essential in authentication and identification applications.

## *1.2. A tour of biometrics*

Biometrics is a characterised result from the natural chaos that authenticates and identifies individuals. There are several forms of biometrics:

- Morphological / physiological biometrics:
  These biometric methods use a biological characteristic of the individual or object. For example, fingerprints, iris texture, shape of the face or hands, wood grain or even atomic minerals in the organization.

- Behavioural biometrics:
  These are the biometrics that measure a dynamic characteristic associated with an ability to reproduce a movement, a sound or even an electromagnetic resonance. For example, writing, handwritten signature, voice or a magnetic field of particles.

- Object biometrics:
  These are the biometric methods that reproduce a natural phenomenon for elements whose characteristics are chaotic and measurable, for example, surface states, the bubbles in the material, manufacturing defects. For instance, digital watermarking, surface aspects and

bubble tags are object biometrics.

Capturing a biometric sample is generally made by live capture but some biometric characteristics methods allow identifying from traces. For instance, we all leave fingerprint traces on objects, and a hair is a trace using DNA identification.

We shall continue this tour with a focus on the main biometric techniques used.

**Fingerprints**

Fingerprint recognition is based on the analysis of the ridge patterns on the tips of fingers. This biometric technique has been used for more than a century to identify criminals. The process was purely manual, carried out by experts. But this biometric technique was the first to be automated in order to enhance criminal investigation and create civilian records in countries where no population register existed. Each finger of an individual is different and it is different from the fingers of another individual. The sensors, systems and algorithms have been refined over many years giving this technique good accuracy and performance, cost effectiveness and led to the creation of huge databases. Sensors produce images of the ridges that are scanned for the search of structural features (called minutiae) such as bifurcations or terminations. The minutiae of one fingerprint can be matched against all other fingerprints.

**Face**

Facial recognition is based on the measurement of the positions of distinctive features of the face - including the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes. The use of face recognition has been introduced for the electronic / biometric passport to the ICAO standard. As facial recognition works when images have a suitable quality, the ICAO has defined criteria that must be checked before accepting a facial image for recording. Accuracy is not considered as good as for fingerprints and the iris.

**Iris**

The iris is the coloured part of the eye that lies between the pupil and the white of the eye. It is made up of coloured tubes, each having a diameter less than the diameter of a hair. The data is so dense that individual details can only be distinguished when viewed through a microscope. The iris contains a biometric pattern. An individual's right eye is as different from his left eye as it is from the eye of another individual. The eyes of identical twins are different. The colour can vary throughout an individual's life but the pattern and the external radius do not.

Data acquisition is done by a camera. The image is filtered to remove background noise and reflection, the border of the iris is searched, and a mathematical transformation is then made. Accuracy is considered as very good.

**Hand**

Hand palm print recognition is similar to fingerprinting. It uses the same principles and techniques. Hand geometry is based on measuring the dimensions of fingers and the hand to generate descriptive templates. The sensing process is user friendly, which is the reason for its relatively widespread use in the areas of access control and time attendance monitoring.

**Vein**

Veins have also been recognised as a unique characteristic that can be applied as a biometric for verification. Veins are developed before birth and remain highly stable throughout life, even differing between twins. Vascular pattern recognition systems identify an individual by using the patterns of veins on their finger, or palm (although almost any body part with visible veins could be used). An infrared camera captures the vein pattern with a focus on the shape and location of the vein structure.

**DNA**

Deoxyribonucleic acid (DNA) may be the most accurate of all biometrics. DNA contains genetic identity information about an individual’s health as well as his identity. There are privacy concerns with the use of this biometric method and the process is inherently slow. So there is no real use of DNA other than for forensic applications

**Multimodal biometrics**
Above is a summary of the main methods of biological biometrics. Each of them has different accuracy characteristics, but it should be noted that it is more and more common to use multiple biometric techniques in systems (such as fingerprints combined with face).

Advantages of using multimodal biometrics are that overall accuracy is significantly improved and the system still works even if one of the biometric samples is damaged.

**Object biometrics**
Biometrics is fundamentally a characteristic of human morphology or behaviour. Physical processes can generate chaos elements that cannot be voluntarily reproduced. When tightly coupled with an object a chaos element can be interpreted with accuracy for the identification, or authentication of the object. This object, for instance a document, can then be preserved from the many risks of fraud. This characterised result from the natural chaos of objects or documents may be known as the object biometrics.

As an example, the type of natural 3 dimensional generated physical chaos known as a bubble tag is a natural and unique occurrence. Characteristics are complex and cannot be either reproduced or counterfeited. When the bubble tag is attached to an object or a document, that object or document becomes uniquely identifiable and authenticable as the one and only original.

### *1.3. Legal and societal aspects*

Biometric systems can, by nature, invade privacy since they make it possible for authorities to track people in all their actions and travels. Privacy concerns can be real or imagined and a user’s perception of the invasiveness of biometrics will impact on their acceptance of the system.

The right to privacy is the right to protect property against search and seizure and to control information about oneself, at all times. The Universal Declaration of Human Rights, in article 12 says that “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks* “. Privacy is a fundamental right that is recognised in many international instruments and regulations, for example, all European countries have enacted legislation safeguarding privacy and Directive 95/46/EC of the European Union (EU) focuses directly on protecting personal data. However, there is currently very little legislation in Europe which deals specifically with biometric technologies. Directive 95/46/EC is presently under revision to adapt the legal framework in Europe to the new context and the issues raised by the digital environment. Based on the results of the public consultation in 2010, the European Commission should present a revision in the first half of 2011.

Some very interesting papers have been published on biometrics and privacy by various organizations such as:

- The Irish Council for Bioethics,
- The BITE (‘Biometric Identification Technology Ethics’) project.

It is not the role of Eurosmart to introduce a new one, but it recommends either to set a task for the European Ethics Group set up by the European Commission, or to create an Ethics Committee specifically for the use of biometrics. This Ethics Committee should, in our opinion, be independent of course of any government and any industrial group. Eurosmart would be willing to answer any technological question that the group might like to ask.

In order to be constructive, Eurosmart has analyzed all its proposed use cases with regard to ethical criteria.

# 2. Education

## *2.1. Electronic Identity*

The expected benefits of electronic Identity (eID) are many: reinforced security, more privacy protection, more and better services to citizens, global interoperability, cost effectiveness, etc.

Security can be seen as protection against terrorism acts, identity theft, criminal or fraudulent acts against private interests and/or public affairs.
Privacy is the ability to reassure people that their lives and personal affairs are out of undesirable public view, that they have control of the flow of their personal information, and that their individual actions cannot be tracked. Privacy is sometimes related to anonymity and can be seen as an aspect of security.
More and better services mean confidential access to electronic services and cyberspace. Besides, global interoperability is a nationwide and cross-border necessity.
All the benefits of electronic identity must be cost effective. This is actually possible, because electronic identity allows the implementation of automated processes.

The key functionalities of electronic identity are Identification, Authentication, and electronic Signature, very often referred as IAS. They allow the protection of people’s data when a strong security level is deployed. In order to satisfy all the needs for security, privacy and interoperability, there is a requirement to define and adopt robust standards. Smart card technology associated to biometrics is the best answer. Digital identification and authentication, with or without an associated digital signature, where the biometrics feature (“I am”) reinforces the PIN (“I know”), allows secure access control to personal data by appropriate individuals. Thus, the privacy issue is managed in a secure way and can be integrated into a complete interoperable system. The European Citizen Card (ECC) standard, as well as the ICAO standard for electronic passports are reliable fundamentals for eID.

## *2.2. Concepts and basics of biometrics*

### 2.2.1. Basics of biometrics use

- **Identification**

Identifying somebody is obtaining his identity from his biometrics.

The identification system works from a collected biometric sample and compares it to all references stored in the database. The person may be known as present in the database, or not. In the first case, it is a “closed set” identification. In the second case (open set identification), the database is a watch list and then the system must determine whether the person is in the database and in case of yes provide the identity.
In terms of biometrics, it is a one-to-many matching process (1: N).

- **Authentication**

Authentication is the verification that an individual actually has the identity it claims to have. This verification process can be made by:

- Checking something the individual owns, like an Identity document with a photograph,
- Verifying something they know, a password, a PIN code, a secret,
- Verifying a biometric characteristic, such as a fingerprint (his).

The verification is said to be a 1, 2, 3 factor authentication, depending on the number of type checks made. In terms of biometrics, the authentication can be a one-to-one matching process (1:1). In this case, a new biometrics sample is taken from the individual to be authenticated and compared to one of their previously registered biometrics sample. If it matches, the user is "authenticated".

- **Electronic Signature**

Like a hand written signature, the electronic signature is used for giving irrefutable evidence of the user's approval for an electronic contract or transaction. Electronic signatures are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. Their legal validity is governed by legislation in many countries and in Europe. Electronic signatures are also referred to as "digital signatures".

It is possible to generate strong cryptographic keys from biometrics. So, a new technology known as bio-cryptography has been developed, linking the electronic signature more firmly to the user. This then makes impossible the repudiation of an agreement or a transaction thus signed.

### 2.2.2. Biometrics qualification methods

Making the selection of a biometric method for identification/authentication must take full consideration of its appropriateness for the use case with regard to fundamental criteria.

Seven main criteria are generally taken into consideration when selecting a biometric method for an identification or authentication process.

- Universality: each individual or object must possess this characteristic;
- Uniqueness: the characteristic is different for each individual or object in the considered population;
- Permanence/immutability: the characteristic should be sufficiently invariable over time;
- Measurable / scalable: it can be acquired by technology that can quantify it;
- Performance: Accuracy and speed of the authentication or identification process;
- Human acceptance: General human feeling that makes people reluctant or cooperative with the use of biometric methods;
- Non circumvention: level of difficulty for hacking the system using biometric methods.

### 2.2.3. Biometrics use: flow process

- **Overview**

Biometric techniques are used for many reasons, but the flow process, despite some variants, always include some key steps.

- The enrolment process that captures biometric data processes it in order to transform it into reference templates that will be stored for future comparisons.
- The verification or identification process, based on a matching search. A correlation score is computed between the live template and any of the stored ones. Then, the score is compared to an application threshold to make a YES / NO decision (for example: granted /denied access).

The following figure illustrates the flow process. It is relevant to every kind of biometrics.

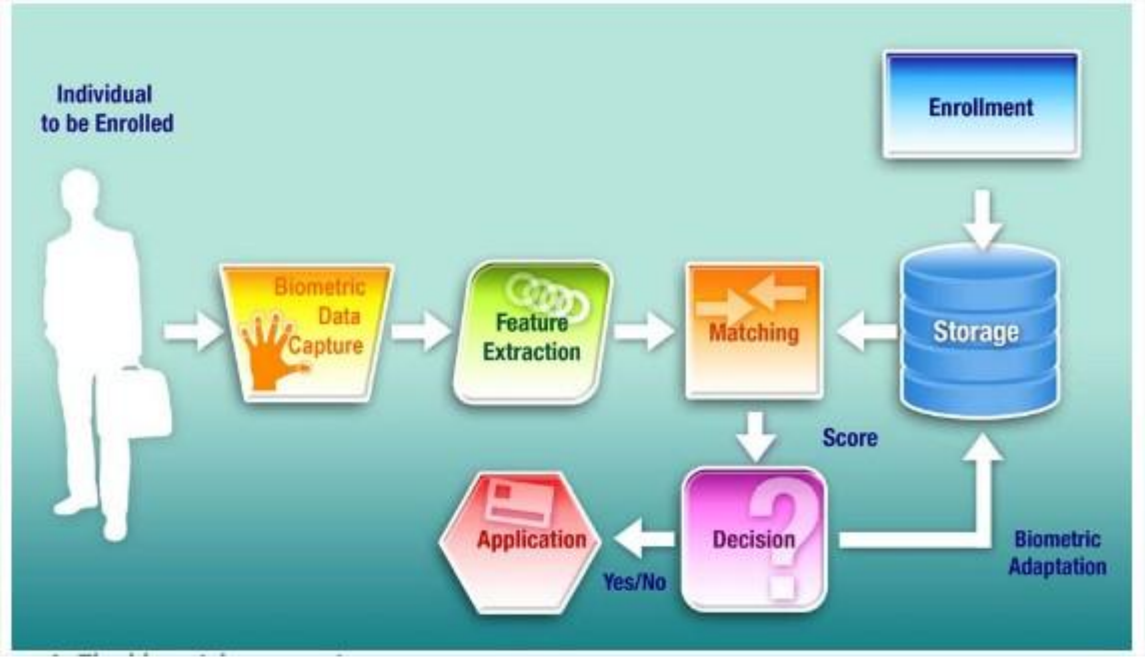


**Fig. 1: The biometrics flow process (Global Platform source)**

- **Enrolment**

The first step of the flow process of any biometric solution is the enrolment of the individual(s). The system captures biometric data, extracts unique features into a reference template and ties the reference template to the individual's identity.
The captured biometric may be recorded:

- in a large central database, such as a Automated Biometric Identification System (ABIS), that allows the performance of later operations of identification of one individual within a population or to ensure that there are no duplicated identity records and thus no identity fraud;
- In a secure individual device such as a smart card, for future 1:1 comparison (authentication).

The enrolment is the foundation of a reliable identity chain, thus some very important procedures must be observed:

- Location must be secure in order to prevent individual data theft or cloning and the operation must be performed by an authorized enrolment officer;

- The captured data must have the highest available quality. This will determine the accuracy and performance of the future matching operations. With regard to this, it is highly recommended that the operation be performed in a live and well checked process by a trusted officer.

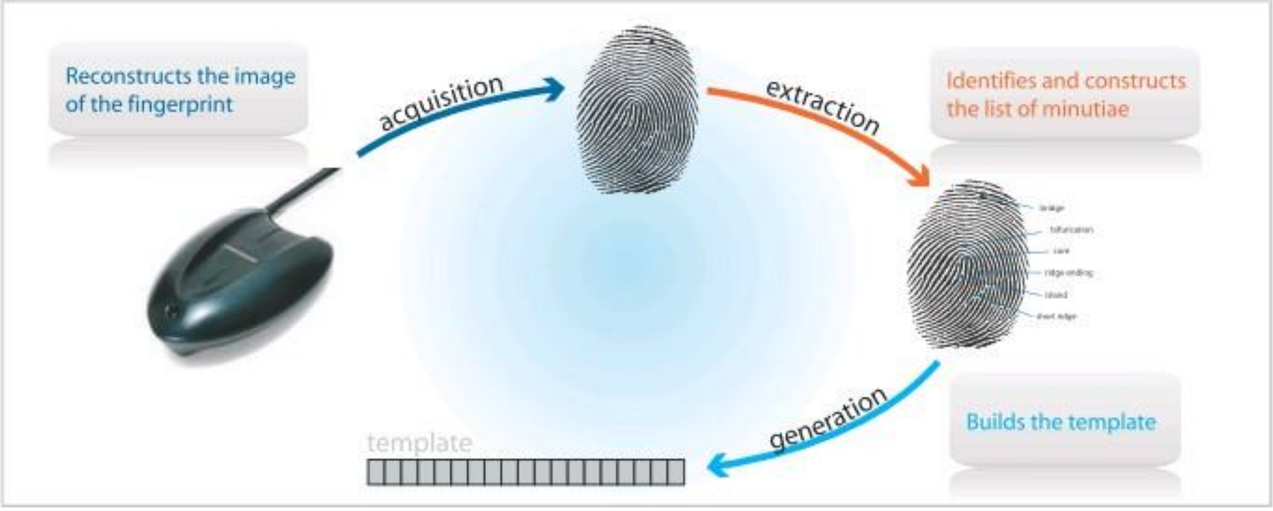


**Fig .2 Enrolment (Global Platform source)**

With regards to identification solutions, the enrolment process is made either with individual's consent (civilian applications) or not (criminal investigation), live and checked, or from biometric traces.

Biometric life enrolment means capture biometric data direct from the person, for example, obtaining the facial photo or fingerprint. With this approach, the quality of the data is under control as well as the management of the biometric data. Life detection of persons could be the second key topic with this method.

- **Identification**

Biometric systems are used to identify an individual's biometric data against a large database or watch-list of individuals in a process known as a 1: n matching. The wording "Match on System" MOS) is also used. This approach is mainly used by governments for identifying their employees, as well for identifying citizens for social benefits, or for checking the uniqueness of identity document delivery.

Automated Biometric Identification system (ABIS) is both a generic word and it is also used when using multi-biometric techniques. Many systems are based on fingerprints. Such systems are named AFIS (Automated Fingerprint Identification System).

This identification process is also used for criminal investigations, from biometric tracking.

- **Authentication**

A biometric verification process includes the following steps:

- Live data acquisition: the user presents the required biometric characteristic to the capture device, for instance a finger;
- Live feature extraction: a unique template is extracted from the previously captured image; according to the selected biometric methodology;
- Storage extraction: the reference template is retrieved from the secure storage memory. E.g. Smart card;
- Matching: a correlation score is computed between the live template and the storage template;
- Decision making: according to the score and the pre-defined policies and rules by the application, a YES / NO decision is done. Ex: granted / denied access.

The smart card technology allows performing the matching algorithm in the processor of the smart card. Then the operation is said to be "Match On Card" (MOC).

If the biometric templates are stored on a device that cannot perform the matching algorithm process, then this is a “Template On Card” case (TOC), and the templates must be transferred to a terminal / system that will carry out the matching. Depending on project type and size, this may cost less but offers a lower level of security.

- **Signature**

Digital signatures allow the user to apply an electronic stamp to a file. The file can then be sent to another person. As a result of the electronic stamp, the recipient can verify the authenticity of the file. Digital signature is part of a PKI (Public Key Infrastructure) system (infrastructure/framework that uses digital certificates as an authentication mechanism and is built to manage these certificates and their associated keys).

A PKI application (embedded on a smart card or on a PC) securely stores user’s credentials (digital certificates, keys etc.). In order to apply his signature, the user must be authenticated on the system by following the process described previously: The user is requested to enter his biometric identifier to the system and a matching is done.

Once he is authenticated, he can sign files or documents for secure data exchange. The electronic stamp contains information regarding the signatory (identity, organization...) and the signature (date, approval authority...). The recipient of the file can then verify the information (using the dedicated software) and validate the authenticity of the file.

The user's credentials can be generated from his biometric characteristics based on new technology called bio-cryptography. This reinforces the link between the user and his credentials.

### 2.2.4. Use of Biometrics with regard to security, privacy and ethics

Passwords and PINs can be forgotten, shared with others, or lost or stolen, which can compromise the integrity of a system. A biometric trait is part of an individual and as such it offers the best element of proof of identity (something you are). Consequently, biometric traits are thought to have a number of advantages over the above security measures: they cannot be lost or forgotten, they are difficult to copy, forge or share and they require the individual to be present at the time of identification.

The use of biometrics also makes it difficult for an individual to deny having accessed a physical location or a computer system, or having conducted a particular transaction. In fact, biometric traits are often portrayed as the ultimate form of identification or verification. They are used as a means of heightened security, efficiency and convenience and have been proposed as the solution to issues of identity theft and benefit fraud. Biometric systems are faster and more convenient to use, cheaper to implement and manage and more secure than traditional identification and verification methods.

Biometric data is more sensitive than private data. It must be used in a secure way. No unauthorized third party must be able to use it.

Automated Biometrics Identification Systems are key elements for security, but an uncontrolled or illegal use of them could infringe privacy. So a strict policy of use, procedures and security techniques must be put in place with such systems:

- Global examination by a Committee in charge of Civil liberties;
- Evaluation of the security mechanisms preventing hacking or illegal use of the systems;
- Audit of procedures :
    - Trusted officials and infrastructures to reassure individuals that the data cannot be compromised and information is not cloned;
    - Biometrics database is operated diligently and by competent official;
    - Use only in valid scenarios;
    - Biometrics systems may be certified by the data protection authorities of the Member States.

When biometrics is used with smart card technology, protection of privacy is easier to ensure.

- **Biometric Match on Card**

A smart card is a safe box of data. By storing biometrics on a smart card as opposed to a central database, there is less opportunity for compromising the biometrics data. In the case of a card if it were compromised, only the data of the card owner would be read. In case of system hacking, then the entire database could be compromised.

The biometric match on card can be used instead of or in addition to a PIN code check. The biometric template is not transferred outside of the card and cannot be caught by a hacker. When smart cards are used to store sensitive data such as medical or civil information, MOC authentication of the user is a far better method than PIN to unlock the card and read the information.

- **Matching off card with biometric or template  images in the card**

ePassports store biometric images. The matching is not performed in the document, but on reliable biometrics terminals.  These deployment models offer good security characteristics and accuracy, but require these terminals to be secured and attended. The model is successful as the number of checkpoints is relatively low and strict procedures are defined by the authorities which limits the risk of compromised inspection systems. As such, verification on the inspection system may be cost effective. This architecture, however, cannot be utilized in an open environment.

Other matching off card cases are made using chipless or memory cards that just store biometric templates. For instance, some welfare programs issue chipless cards with fingerprint templates registered with other data and encryption in a 2D bar code. The card reader decodes the 2D bar code and makes a match with the captured biometric sample.

- **Summary of matching processes**

| **Template on …. ➔**<br>**Match on … ↓** | **Database** | **Card** | **Terminal** |
|---|---|---|---|
| **System** | ABIS AFIS<br>Identification, forensic | Cards that can only store the template, but cannot process the matching algorithm (chipless or memory cards). | No sense |
| **Card** | No sense | The template never leaves the card | No sense |
| **Terminal** | In this case the terminal periodically receives a subset from the database (watchlist) | Cards that can only store the template, but cannot process the matching algorithm (chipless or memory cards) | Used when the expected individuals are known to be in a small database. For instance, physical access control. |

Notwithstanding the fact that Eurosmart cannot be a starting point for statements on for biometric ethics, it has analyzed all its proposed use case with regards to ethical. The following table has arisen from our analysis.

| Ethical criteria | Eurosmart technical questionnaire | Eurosmart recommendation to government, ID management and service providers |
|---|---|---|
| Role of the biometric application | Description use case per use case | Full and frank debate on the issues raised by all parties who will be involved in the proposed application, prior to establishment of the proposed programme |
| Transparency regarding use of biometric technology | Who has access to the biometric information at the different steps of the solution? | Describe in a public document the procedures that go with the technical measures |
| Relevance and necessity | *Environment*: does the nature of the workplace need a high degree of security?<br>*Purpose*: is a biometric system required to achieve the intended purpose or could a less intrusive method be used?<br>*Efficiency*: is the introduction of a biometric system needed to meet requirements. Which alternative, less intrusive methods have been unable to achieve them?<br>*Reliability*: Which other methods have failed to work? | Answer in the same questionnaire. |
| Use of only required information to achieve a clear, limited and specified purpose. | How is this technically managed? | Appropriate information and access management procedures should be established. |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Description of security objective measures and control that allow the system operator to define procedures that meet the target? | Appropriate information and access management procedures should be established. |
| Can system operators and system providers access information other than that only required to carry out their job? | Description of security objective measures and control that allow the system operator to define procedures that meet the target? | Appropriate information and access management procedures should be established. |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Description of security objective measures and control that allow the system operator to define procedures that meet the target? | Appropriate information and access management procedures should be established. |
| Can the user make the decision whether or not to participate in the programme? | | An individual should be fully and accurately informed and should understand all the issues and implications relating to the provision of his/her information. |
| What are the practical measures that ensure the integrity of an individual's personal and information privacy? | Description of technical measures. | General description and guarantee to be described in an easy to find and understand document. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Description of technical measures. | Data protection legislation should be reviewed in order to deal sufficiently with the privacy concerns presented by the use of biometrics. |
| Clear knowledge of vulnerabilities | Description of security | Describe in a public document the |

| | | |
|---|---|---|
| and protection against them. | mechanisms, countermeasures and their control. Answers to these known vulnerabilities<br>*Spoofing,* use of a fake biometric.<br>*Replay attacks,* recording an image from a legitimate user and inserting it back into the system.<br>*Substitution attacks* –overwriting a stored template and replacing it with his/her own template.<br>*Tampering-* the verification process to achieve a hit for his/her own biometric.<br>*Masquerade attacks* , by means of .<br>*Trojan horse attacks* , for instance, in order to get a hit for his/her own biometric.<br>*Overriding the yes/no response,* inserting a false hit response to bypass the biometric system. | procedures that go with the technical measures. |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Technical solution must allow the subsequent actions tyo be performed with appropriate security. | Procedures must allow the individual’s rights to be satisfied. Moreover, when context allows it; if an individual no longer wishes to utilise the biometric application or the original purpose of the application has been achieved, then any biometric and other personal information about that person should be deleted from the system. |

## *2.3. Interoperability*

In the past use was made of biometric technology mainly for criminal investigations or specific applications of physical access control or access to social benefits. This is changing now. The world is opening up with cross border agreements in the EU and worldwide, the international need to fight terrorism and the increasing need to securely verify the identity of users of e-commerce services.

International organizations have defined the use of biometrics for border controls. The ICAO has endorsed facial and fingerprint recognition for the e-passport and the EU has introduced a technical specification accordingly. The ISO is hosting sub-committees (SCs) relevant to the biometrics industry.

### 2.3.1. European Organizations Requiring Conformity and Interoperability

As a result of the freedom of movement of European citizens to live and to work across the EU, many sectors require conformity and interoperability. Here is a non exhaustive list of sectors which will require conformity and interoperability:

- Border controls and criminal justice,
- Cross border transportation,
- (e-)Healthcare,
- e-Government,
- Banking,
- Sensitive industrial site protection, such as nuclear power facilities,
- Military installations.

### 2.3.2. Barriers to consensus

The various sectors have different priorities and different timescales for cross interoperability. In addition, local-only solutions tend to get favoured and implemented. They are sometimes based on some standards, but every sector will benefit from a cross border consensus and from coordinated projects.

### 2.3.3. Current projects and Relevant Existing Standards

Here are some very important projects and infrastructures regarding EU wide interoperability of biometric systems:

- Visa Information System (VIS),
- Schengen Information System II (SIS II)
- Bio Testing Europe
- BioDev
- EURODAC (Asylum Seeker Data Base)
- Biometric passports

In the case of forensic systems that have been deployed earlier, Member States have proprietary systems. The need for standardization is not so important.

### 2.3.4. International standards

ISO sub-committee 37 (SC37) was set up in 2002 to develop formal international biometric standards for harmonization of vocabulary, biometric technical interfaces, biometric data interface formats, profiles for biometric applications, testing and reporting and cross-jurisdictional and societal aspects.

Smart card technology is well defined by many standards that enable it to be the most secure and interoperable means of setting up biometric solutions. These standards are produced by sub-committee 17 (SC17) at ISO, but other organizations have also defined the BioAPI (Java Card Forum),

and the European Citizen Card (CEN).
The ICAO's work on ePassports has been set out by the Technical Advisory Group on Machine Readable Travel Documents (TAG – MRTD) in ICAO document No 9303.

A list of standards is attached in the appendix.

## *2.4. State of the art*

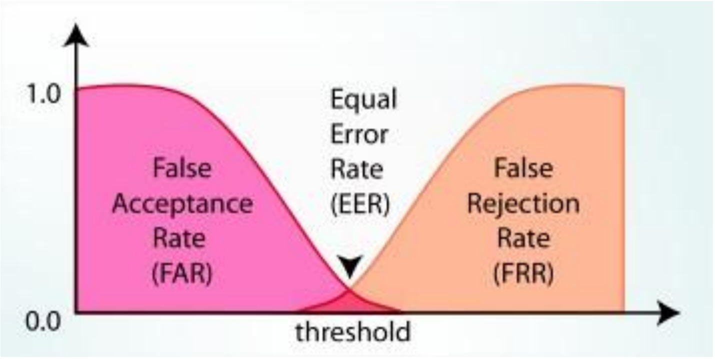
### 2.4.1. Performance: FAR, FRR and FTE

While it appears to simply give a yes or no answer, the biometric matching algorithm actually measures how similar a captured biometric data is to the stored reference. Biometrics uses score to express the similarity between a reference and a candidate biometric template. The higher the score, the higher the similarity between them.
Then it makes a decision according to a preset threshold as to whether the biometric sample comes from the same individual that provided the stored biometric template or not. That is to say, this process is statistical and although very accurate, it is not always exact. The security level is set by the threshold matching scores.

A false match is an erroneous conclusion by the biometric system that a reference template is from the same individual, when in fact, it is not. A False Acceptance Rate (FAR) or False Match Rate (FMR) is the statistical evaluation of false acceptances (wrong positive matches).

A false non-match is an erroneous conclusion by the biometric system that a reference template stored is not from the same individual, when in fact, it is. A False Rejection Rate (FRR) or False Non Match Rate (FNMR) is the statistical evaluation of false rejections (wrong no matches).

If we put together the curves of FAR and FRR, there is a point where both of them have the same value, it is called the Equal Error rate (EER). When setting the threshold value high, FAR reduces while FRR rises. When setting threshold score low, FAR rises whilst FRR reduces.



FAR and FRR are the main criteria for quality assessment of a biometric system. Their values are also related to the quality of the enrolment.

The failure to enrol rate (FTER) measures the probability that an individual will be unable to enrol in the biometric system. Failure to enrol may be due to:

- The biometric method that may not allow all individuals to permanently have distinctive enough biometric samples. For instance, the fingerprints of some manual workers are more often difficult to capture than for other people.
- The design of the system can make it difficult to get consistent biometric data.
- The quality of the enrolment system or the enrolment procedure. A commonly accepted rule

is that good quality enrolment must be live and well checked.

- A system design that makes it difficult to provide consistent biometric data. For instance, retina recognition systems needs to be very accurate, so is difficult to achieve in the enrolment process.

### 2.4.2. Comparison of techniques

The following table gives some figures for FTER, FAR an FRR for fingerprint, iris and face biometrics. These rates may vary depending on the quality of the enrolment, the sensors and the parameters selected for the system. For instance, in some cases a service provider might prefer to have more false acceptances and less false rejections, in other cases false acceptances are strictly prohibited.

| | Fingerprint | Iris | Face | Face + Fingerprint |
|---|---|---|---|---|
| Failure to Enrol | 0.1% | 1-2% | 0% | 0,1% |
| False Acceptance Rate | 0.01% | 0.0001% | 1% | 1% |
| False Rejection Rate | 0,5% | 0,2% | 2-10% | 0,6% |
| | | | | |

The comparison of the techniques with regard to the qualification criteria of biometrics must be taken into account for the expected use case.

| Biometry \ characteristics | universality | uniqueness | permanence / immutability | measurable | performance | acceptance[1] | resistance to circumvention |
|---|---|---|---|---|---|---|---|
| FACE | high | medium | medium | high | low | high | low |
| FINGERPRINT | high | high | high | high | high | medium | high |
| IRIS | high | high | high | medium | high | medium/low | high |
| VEIN PATTERN | medium/high | medium/high | medium/high | medium | medium | medium | unknown |
| HAND GEOMETRY | high | low/medium | medium | medium/high | medium | medium | medium |
| BUBBLE TAG | High | high | high | high | high | high | high |
| DNA | high | high | high | low | high | low | low |
| MULTIMODAL | High | high | high | high | high | high | high |

## 2.5. *Typical architectures for biometrics*

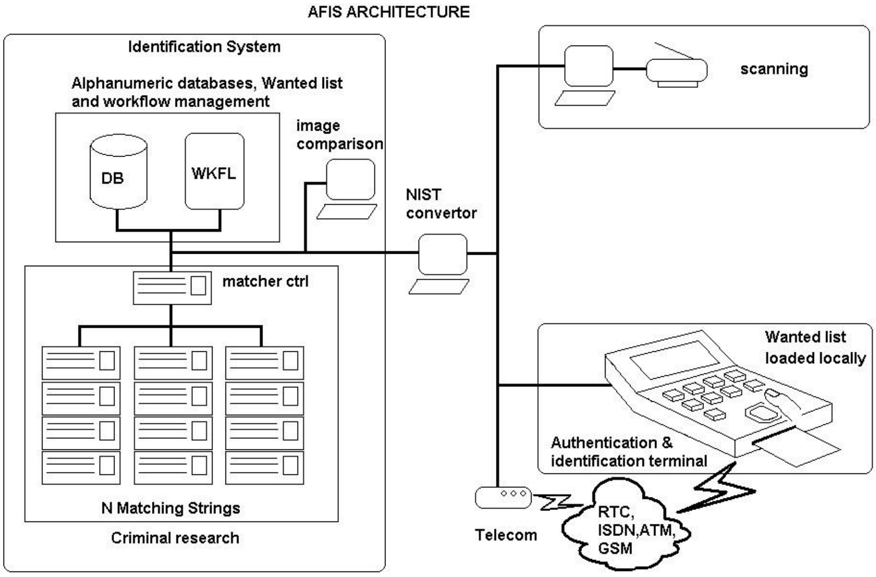
### ABIS architecture (Match on System)

The architecture of such systems is independent from the biometric technique. The biometric identification is purely based on algorithms in which quality is determinant for the performance as regards accuracy and response time. In general three types of algorithms are involved:

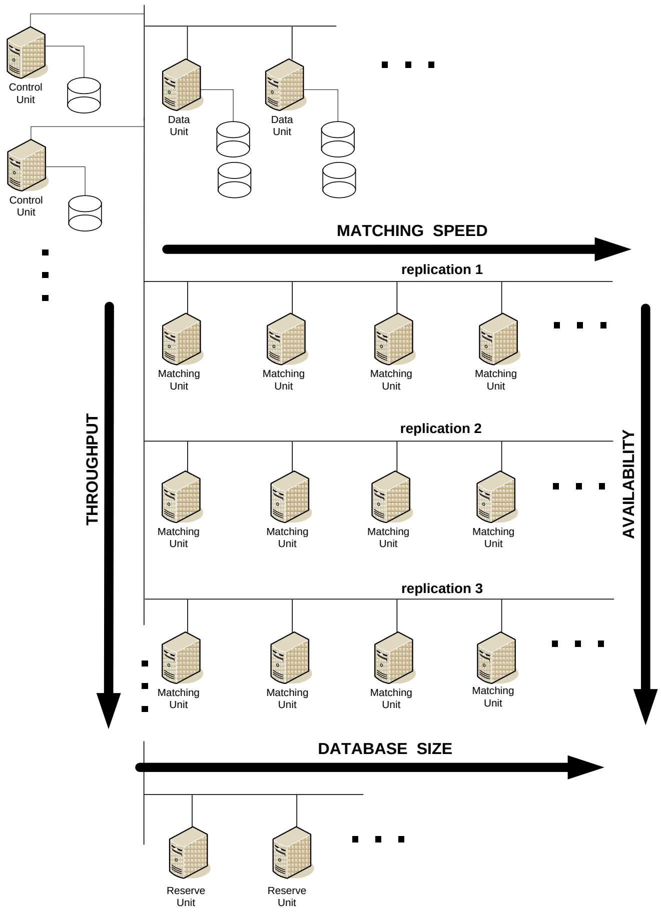
- Coding: These algorithms extract and encode information from the biometric samples, in order to prepare the next steps for high performance.
- Classification: Objective is to reduce the population of the database that will be considered for the matching process. The efficiency of these algorithms is key to the performance of a given hardware, or for the cost of the system at a given performance level.
- Matching: The aim of these algorithms, also named matchers, is to find the correct candidate for identification. For each reference they search for and evaluate the number of common minutiae and compute a score. Then the final decision will be either “no match”, “hit”, or

[1] Acceptance may vary depending on countries and culture

presentation of candidates to experts for visual inspection in the case of criminal investigations.



In order to achieve high performance when databases can be very large (millions, tens of millions, or hundreds of millions) and transaction requests numerous (tens of thousands per day), the architecture will then be based on clusters of Matching Units. This approach permits workload balancing flexibility and high reliability and availability of the system. Searches are then performed in parallel on sub-databases thus increasing the matching performance. When the search is completed on each sub-database, the results are consolidated to give the list of potential hits on the entire 1:N template database.



### Match-on-Card Architecture

On-card comparison, or Match On Card (MOC) means that the biometric sample verification is performed in the card. The smart card must have sufficient processing power to perform the matching. The biometric system captures the biometric sample and extracts biometric data. The created biometric data is then uploaded to the card for verification. The verification process is executed on-card. If the biometric verification is successful the card's security state is updated and an appropriate signal sent to the back-end system.

Match On Card may be performed for fingerprint, face, iris, and almost certainly other techniques in the future.

The storage of the biometric templates in the card memory requires a few hundred bytes only for fingerprints and iris and a few kilobytes for face.

Match-on-Card fits with all available operating systems in the market such as Java, Multos, .NET and cards with proprietary Card OS´s.

### Match-on-terminal architecture

Matching on Terminal may be made either by comparison of the captured biometric sample with a list of templates stored in the terminal memory (watch list) or by a 1:1 comparison with a template stored in a card.

Comparison to a watch list:

This watch list is downloaded and updated to the terminal by a system that owns a biometric database. This architecture is used, for instance, in some physical access controls where the terminals only get the biometric list of people who can access the protected area. In this case there is no need for employee badges.

Comparison by use of a token

The biometric template stored inside the card is then transferred to the terminal software for 1:1 comparison.

### BioAPI

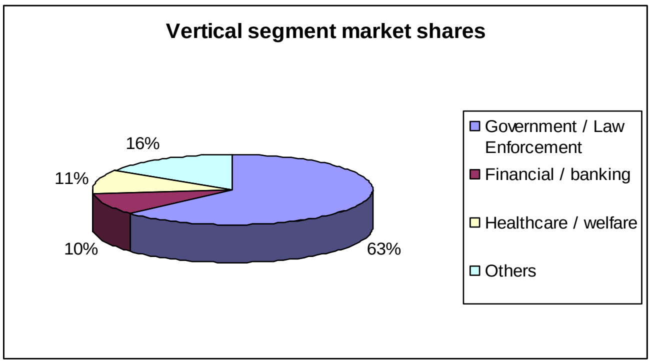
BioAPI (Biometric Application Programming Interface) is a key part of the International Standards that support systems that perform biometric enrolment and verification (or identification). It defines interfaces between modules that enable software from multiple vendors to be integrated together to provide a biometrics application within a system, or between one or more systems using a defined Biometric Interworking Protocol (BIP).

## *2.6. Market figures*

These figures are extracted from an EMEA Biometrics market study carried out by Frost & Sullivan in July 2009.

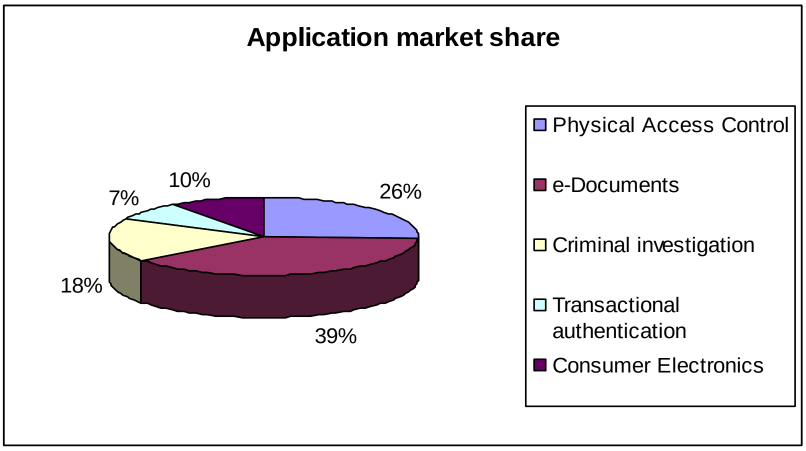
The Biometrics market in Europe is estimated at about 250 million Euros in Europe for the year 2010, with a 25% compound annual growth Rate (CAGR) from 2008 to 2015. The economic downturn in the commercial and financial segments should be counterbalanced by government projects.

Vertical markets are mainly:



- Government/Law Enforcement represents 2/3 of the market.
- Financial/Banking, at about 10%
- Healthcare, at about 10%
- Others at about 15%

Main applications are:



- Physical Access Control:
- e-Documents:
- Criminal Identification:
- Transactional Authentication
- Consumer electronics

In terms of techniques:

- Fingerprinting (non-AFIS) is the predominant biometric technology used for most applications. It is increasingly used in e-Documents like the Schengen visa and e-Passports and in consumer electronics.
- Facial recognition is linked to the adoption of biometric passports according to the International Civil Aviation Organisation (ICAO) mandate. The use of facial recognition with CCTV for security measures in the next three to five years is a potential growth area for this technique.
- Iris recognition is also likely to gain traction for airport security, registered travellers and access control in sensitive areas for airport staff.

Main market drivers are:

- Increased security concerns
- Government projects
- Use of biometrics in healthcare / welfare programs,
- Consumer electronics: Authentication of users accessing PCs, PDAs, smartphones,..

Main restraining factors are:

- Economic downturn,
- Privacy concerns and insufficient educational activity.
- Delays in government projects.

## 3. Biometrics use cases

Because it refers to intrinsic characteristics of the individual rather than to the ownership of an object or the knowledge of what is supposed to be a secret, biometrics has huge advantages for identification applications.

Some varied concrete case uses can be identified, enjoying the benefit of new possibilities introduced by biometrics:

- Identity verification is necessary in many cases. It can be citizenship identification at borders or on land by the police. It can also be the verification of the digital identity when accessing IT infrastructure or electronic services. Identity verification can be extended to some attributes other than first and last name and citizenship, in order to control the access to some benefits or rights.
- Strong and secure authentication purpose; to ensure that the identity claimed by an individual is really his or hers. This is a need for both face to face verification for citizenship or membership of a group and digital identity. Biometrics, contrary to PINs and passwords, is intrinsically linked to the individual and thus truly authenticates who the individual is.
- Digital signature, for the provision of a legally compliant irrefutable signature.
- Simplifying password management that is proven to be a weak and inconvenient authentication solution. A recent study revealed that French internet users have on average 12 accounts, that is to say even more passwords to remember and keep confidential. Human memory fails; some ailments prevent people using these properly; confidential preservation of these secrets is also difficult.
- Replacement of PIN code support, it is clear that PIN secrecy is very difficult to maintain. Environmental conditions and also technology available to hackers makes PIN theft easy.
- Product & document protection: Counterfeiting and forgery of documents and products is now so huge that new solutions must be put in place.
- Data protection that is adequate, relevant and not excessive.
- Civilian registration and criminal investigations: The use case has been developed for some time, but the market is still developing and technology provides enhancements.

### *3.1. Attempt at classification and listing of use cases*

This list of use cases is not, of course, exhaustive.

| Families of Use-Cases | Some concrete examples of use case |
|---|---|
| Identity Verification | Border controls |
| | Identity checks on land |
| | Secure chat for children |
| | Access to e-services |
| | Driver’s license |
| | Tachograph card |
| | Physical Access Control |
| Strong & Secure Authentication | Secure e-mailing |
| | e-administration (tax declaration, call for tenders) |
| | e-banking |
| | e-health |
| | e-commerce |
| | Border controls |
| Digital Signature | Notary service |
| | e-banking |
| | e-administration (tax declaration, call for tenders) |

| | |
|---|---|
| | e-health |
| | e-mailing |
| Simplify Password Management | Mobile connections to e-services sites |
| | Application management |
| Replacement of Pin code Support whenever possible | Internet/Intranet web-service connection |
| | Internet/Intranet tools usage |
| | Banking/e-banking |
| | e-administration (tax declaration, call for tenders) |
| | e-commerce |
| Product and document protection | eID card for national |
| | eResident Permit for foreigners |
| | Documents, certificates |
| | Material goods |
| | Vehicle registration |
| Civilian registration & Criminal investigations | Identification |

The following table provides another classification of the use cases:

| Use cases | Identification | Authentication | Signature | Password simplification | PIN replacement | Product Document authenticity |
|---|---|---|---|---|---|---|
| **Border controls** | X | X | | | | X |
| **On land identity document verification** | | | | | | X |
| - eID card for nationals | X | X | | | | X |
| - eResident Permit for foreigners | X | X | | | | X |
| - Driving license checking | X | X | | | | X |
| - Vehicle registration | X | X | | | | X |
| - Tachograph card and data | X | X | | | | X |
| **Payment** | | X | | | X | |
| **ID and non ID document or certificate checking** | | | | | | X |
| **Material goods checking** | | | | | | X |
| **Digital world** | | | | | | |
| **Secure emailing** | X | X | X | | | |
| **Secure chat for children** | X | X | | | | |
| **Age verification for purchases** | | X | | | | |
| **Access to e-services** | X | X | X | | | |
| - e-administration (tax declaration, call for tenders) | X | X | X | X | X | |
| e-banking | X | X | X | X | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| - e-health | **X** | **X** | **X** | **X** | **X** | |
| - e-commerce | **X** | **X** | **X** | **X** | **X** | |
| - e-billing | **X** | **X** | | **X** | **X** | |
| - Notary service | **X** | **X** | **X** | | | |
| - On-line contract (for any of the above use cases) | | | **X** | | | |
| - Mobile connections to e-services sites | **X** | **X** | | **X** | | |
| **Application management** | **X** | **X** | | **X** | | |
| **Internet/Intranet webservice connection** | **X** | **X** | | **X** | **X** | |
| **Internet/Intranet tools usage** | **X** | **X** | | **X** | **X** | |
| **Physical Access Control** | **X** | **X** | | | **X** | |

Below we give an informal description of the use case and provide further details for the most promising business use case

### 3.1.1. Civilian registration & Criminal investigation

It is often necessary to identify individuals after a crime, an accident or military action. Biometrics have been providing this type of identification for centuries. Biometric analysis can be used to identify both offenders and victims and this information can be stored on databases and used for later applications. The biometric methods used are mainly fingerprints extending to rolled fingerprints, palmprints, face, and DNA. Collection of biometric samples on crime scenes takes time of course, as well as the analysis process, and then the matching with the databases. The systems used are called ABIS (Automatic Biometric Information systems) and AFIS in the case of fingerprints.

AFIS and ABIS are used also for civilian registration and provide the assurance that a citizen is registered only once under a unique identity.

Civilian registration methods at national elections with biometric data have been made on a large scale, e.g. Bangladesh, Pakistan and the Republic of South Africa. India has started a new program of central registration in combination with fingerprint data and a UID system for 1.1 billion citizens (called UIDIA) and Brazil is also doing so for 270 Million citizens (called RIC).

### 3.1.2. Border Controls

In the travel and tourism sector, biometrics now plays a key role in identity management. The International Civil Aviation Organisation (ICAO) set international standards for the industry and has recommended facial recognition as the primary biometric with iris and fingerprint as backup (but not compulsory). Some countries are starting border control processing by the use of eGate systems. The systems acquire, for instance, a live image of an individual's face and use facial recognition technology to match the image with the digitised image stored in the individual's ePassport. If there is a successful match, the individual is cleared to proceed through the Customs control point. If there is not a successful match they would be referred to a Customs Official for processing in the traditional, manual way. Some eGates systems use fingerprint or iris instead of face, but the general processing is the same.

eTravel documents embed many security features that are used for checking that the document is not a faked one, and has not been forged. An additional level for guaranteeing the genuineness of the document can be done by the use of biometrics of object

### 3.1.3. On land Identity document verification

- **National eID cards**

These ID documents may often be used like an e-passport in some regions of the world. They are also used for accessing eServices. Resident Permits shall offer the same features as a National eID card. Thus, in Eurosmart's opinion the use of electronic e-passport technology is recommended for the use case of citizen identity verification with these cards.
In addition, checking the genuineness of the document against a biometric document image can be an additional security against counterfeiting or forgery.
Some countries have decided to include the match on card feature to these documents. This is the case, for instance, in Spain and Portugal.

- **Driving license**

Electronic driving license: Driving license document fraud is huge in many countries. Providing electronic documents that cannot be forged or counterfeited and that allow management of respect by the driver for the safety rules is a solution that can save lives. Introducing a biometric technique that can be verified by police officers using mobile terminals with biometric ICAO checking or matching on card may well lead to a significant increase of road safety. In some countries, the driver's license has the statute of an identity document.

- **Tachograph card**

Tachograph systems record key data like driving time, speed. Respect for these by professional drivers is an important factor in guaranteeing the safety of passengers, drivers and other vehicles. This equipment uses a smart card that is general individual to a driver. Other smart cards are also distributed to authorized officials controlling the system. A level of secure authentication should be adopted equal to the one proposed for the driver's license.

- **Vehicle registration cards**

Current paper documents do not allow true authentication of the origin and history of the car (owners, accidents, periodical technical mandatory inspection results …). By preventing the possibility of shady dealing in cars, we can improve road safety. The Biometric use of document and chip technology would provide better security by ensuring the uniqueness and the integrity of the document. The solution can also be enhanced by linking object biometrics of the car to the card chip.

### 3.1.4. ID and non ID document checking

Even with more and more sophisticated security features in the e-ID and eTravel documents, it is not possible to conclude that powerful terrorist organizations cannot forge or counterfeit documents. The use of smart card technology combined with biometrics is the only means that can provide reliable identity verification.

Many other documents such as school certificates, proofs of ownership, issued by administration bodies, notaries, and even private institutions can have a high value. They are very often made of paper. Use of object biometrics can make forgery and counterfeiting of the document very difficult and their detection easy. The introduction of the owner's biometric characteristics would provide an even better level of security.

Authentication of objects solutions built around object biometrics can be applied in various sectors for victims of frauds such as forgery or counterfeiting:

- Identity Documents to: ID cards, Passports, Driving licenses, eResident permits …
- Secure access professional cards,
- Healthcare cards, Benefit cards, …
- Contracts,
- Property title
- Intellectual property

### 3.1.5. Material goods checking

In many cases it is important to be able to prove that a material good really has the claimed origin, and is not a counterfeited product. This can be for safety reasons, for instance maintenance parts for aircrafts, or IP protection for products that have required huge R&D efforts, Quality label protection.

Authentication solutions built around object biometrics can be applied to products in various sectors for victims of frauds such as forgery or counterfeiting:

The main interests of the use of the object biometrics as a seal applied to the logistics field are:

- Security of large packages (by price, know-how, confidentiality) in transportation and storage phases;
- Deterring and control of access to highly secure data (the fight against industrial espionage);
- Deterring and control of opening of the packaging.

Benefits:

- The biometric seal prevent consumers and distributors from any counterfeiting of products and brands;
- Beyond the authenticity guarantee, the Biometrics seal has a deterrent role on the opening of packages or systems;
- The biometric seal enables each package to be individually and formally identified and authenticated.

### 3.1.6. Payment

By using Match-on-Card fingerprint recognition as an alternative to PIN when verifying a purchase it is possible to avoid forgotten PINs and “shoulder surfing”. Other advantages can also be achieved using secure distribution by enabling biometric activation of the card.

The technology fits perfectly with EMV architecture, as card holder verification is still performed inside the smart card. It offers a stronger link between the card and the card holder. The use of biometrics ties the card to one specific physical individual, removing the possibility of card usage transfer or delegation, and making the card truly personal.

### 3.1.7. Physical Access Control

Physical Access control can be achieved by a human (guard...), through a device which can be a mechanical key or an electronic device which uses a token such as a smart card. In order to access a restricted area, the user needs to have a sufficient access right defined in his device. But the loss of the device by the user can be a security breach in the system. If the badge is found by someone before being deactivated in the system, intruders may be able to access a restricted area.

As a result of biometrics the user needs to be at the access control point to present his biometric credential to obtain access. Users can no longer share their device. Moreover, nowadays most of the biometric techniques can differentiate between a live and dead biometric identifier avoiding the risk of identity theft. Biometric use brings the most advanced level of security to physical access control.

### 3.1.8. Digital world

- **Secure e-mailing**

Access to mails is one of the fundamental privacy rights that must be protected. Personal computers, and also personal storage space on servers can contain the people’s entire correspondence over many years. Any attack on such a storage space may lead to serious harm.

As a secure alternative to traditional e-mailing it is possible, as a result of biometric technologies, to identify both the sender and the recipient. Usually, emails are not considered as a safe way of transmitting sensitive data. With biometric technologies associated to the secure environment of a smartcard, the e-mail is encrypted and sealed by the sender. The message can only be read by the authorized receiver who also must identify himself by fingerprint biometrics. With this solution, the authenticity and integrity of the e-mail, recipient and sender are ensured.

Another possible scenario is to drag emails to a special encrypted e-mail folder accessible only with the user’s biometrics in order to avoid anyone reading the emails in his inbox. Documents and e-mails can only be opened by means of his fingerprint, face or voice.

- **Secure chatrooms for children**

The Internet can be both good and bad. Cases of paedophiles who have been able to meet children through internet chatrooms are too numerous. This must be prevented. A smart card that can deliver a status answer about a minority / majority age is a level of protection. But children do not really understand the idea of confidentiality and may disclose passwords and PINs unintentionally. A smart card with an age status delivery function protected by a match on card is a secure solution.

- **eID Verification/Age verification for purchase**

Some purchases are dependent on the age of the buyer (e.g. Alcohol). It may be necessary to first check the age of the buyer before delivering the requested purchase. For such a use, the identification does not deal with names, surnames, etc but focuses only on age in order to validate the order (off-line or on-line). The order is accepted when the Age Verification is in line with the rules associated with the purchase; it is refused when this is not the case. The same solutions as for secure chatrooms for children should be provided.

- **Access to e-services**

These services can be:

- Public e-services (Government to citizen, government to government, government to companies)
- Private e-services (business to business, business to citizen)

<u>e-administration</u>

We can assume that nobody likes to pay taxes for someone else, or that this is not a real loss. But making false declarations in lieu of the authorized individual or organization may cause losses, financial losses, consequential losses, and many legal problems for businesses.

Administration processes can be streamlined by using a digital signature. Administration employees can digitally sign electronic documents to validate forms and make requests from citizens or within the administration. Then the document can be legally sealed by the use of certified applications compliant with standards such as the "European citizen card".

On the other hand, citizens can validate their forms such as tax declaration through a digital signature online on e-government websites. Administration processes are then faster and more secure avoiding the risk of fraud based on paper documents' lack of security.

Biometric authentication or / and digital signature based on biometrics gives a higher level of security to the transaction as the signature is based on the presentation of a biometric characteristic of the signatoryr. Fraud, misuse and even corruption can then be reduced. Rejection of the transaction becomes impossible.

<u>e-banking</u>

Banks are familiar with risk management and use it to adapt the security of their system to the best compromise between ease of access their services, security costs and the risk of fraudulent use of e-banking services. But criminal organizations are looking more and more to attack e-banking with powerful IT resources and skilled people inside their organization. Access to e-services through a weak authentication mechanism is one of the preferred ways of hacking a system.

Nowadays, banks want to offer new services such as bank transfers, subscriptions to new services and, on line contract signing. Technologies are available to secure a signature and laws in most of the countries define frameworks for a legal and qualified signature.

With the biometric technologies associated to the secure environment of a smartcard for example, the customer or the sales representative can only sign a contract after identifying himself by his biometric identifier. With this solution, the authenticity and integrity of the signature is ensured

### eHealth / eWelfare

For these application fields there is the need to both protect private data relative to the individual's health and ensure that the benefit of social insurance or welfare organization are actually provided to the right individual. The sums of money are important, the social impact is high.

Whether the reason is regulatory or financial, fraud reduction and security enhancement are the primary concerns for healthcare applications. Issues related to fraud are most commonly seen in countries and regions where healthcare insurance is widely used. Three of the main issues are:

- Phantom billing – a claim is submitted but no service is rendered and the patient is not physically present
- Coding errors – a claim that includes services that are not rendered or more services than those that were rendered.
- Card sharing and ID theft – uninsured individuals using another's valid identity

Utilizing biometrics and thereby binding transactions to an individual is a powerful tool to combat the abovementioned issues.

Using biometrics for welfare payments can efficiently fight against fraud. For instance, the payment of pensions in some countries where no real civilian registration or identity documents are available: Biometric use makes certain that the payment of pension has been made to the right individual.

A system that has to know and use an individual's unique social security number or an individual's medical history can be considered more invasive of privacy than other systems, including biometrics. Medical information can be stored in the tamper-proof environment of a smartcard which the holder can keep.

Granting access with the permission of the holder thanks to a Match on Card mechanism will certainly protect the confidentiality of this personal data... In order to reduce costs, electronic health records are currently being deployed in many countries. To ensure the authenticity of a prescription, the health professional can digitally sign the prescription using an electronic device such as a smart card. The digital seal is then integrated in the electronic prescription allowing pharmacists and other health professional easily to verify the authenticity of a prescription. Use of biometrics for digital signature avoids the risk of fraud with prescriptions by bringing a highly secure authentication method that prevents a shared use of a credential. In addition, access to health records on medical servers can be highly protected by biometric authentication.

### e-commerce

e-commerce protection is similar to e-banking. The volume of e-commerce transactions is increasing. Hence the interest in hacking into systems is also increasing for criminal organizations acting on their own behalf or seeking to sell fraudulent access to e-commerce sites to individuals. The digital economy must also seek to prevent money-laundering.

Confidence is absolutely necessary for the development of e-commerce. Government authentication of a person's identity is the best means for instilling this confidence in both customer and service provider's minds. For a government, using a sovereign identity document and biometrics is the only certain solution.

### e-billing

In almost every discussion about implementing e-billing, concerns about privacy and the protection of information quickly emerge as key issues. A company delivering invoices to its customers has the possibility to use biometric technologies in order to keep the related information confidential such as:

- Billing amounts,
- Bank accounts,
- Or the nature of the product or service bought

The chip implements some cryptographic algorithm protecting the data. The possibility of access to this sensitive information is given to the customer using biometric identification such as Match on Card fingerprint recognition.
There is no interest in stealing one invoice but attacking a server or bills website can be profitable for some hackers or some dishonest employees. Using biometrics, to sign or access this information, in such a situation, is the best way to avoid these threats.

### Notary services

A document issued by a notary office may be falsified, counterfeited, and even be a fake. Use of such documents is not in general subject to strong verification. Applying object biometrics to the document is a safer mean of document direct authentication, with even the possibility proceeding to on-line supplementary checking.

### On-line contract

Online contract signing is generally carried out in 2 steps. As long as the acceptance does not change the terms set out in the offer, the contract is concluded at the second step. In order to do so, those entering into the contract have to be sure that the data has not been altered by the other party or by a third party. Using biometric technologies makes certain that the contract content was created by the legitimate authority and has not been altered.
Only the two parties to a contract can access the contract as a result of a biometric authentication.

### Mobile connections to e-services sites

This is a relatively new market. Some smartphones and new portable computers are embedding smart card technology and biometric sensors. This will allow local secure authentication and proof of it to the e-service site. MOC in the mobile/ Match on device.

### *3.2. Analysis of use cases*

#### 3.2.1. Border controls with biometric travel documents

| **Border controls** | Biometric Travel Documents |
|---|---|
| **Status** | New World-Standard ICAO 9303; two regulations: US VISIT for 27 VISA WAIVER Countries (like Australia, Japan, and many EU-States), EU: 2252/2004 with deadlines in CY 2006 for 27 EU Member States.<br>In CY 2010, 91 of 188 states worldwide issue travel documents with biometric facial or combined with biometric fingerprint data; border control equipment is only in place in 6 states (pilot scheme); Main applications are three-way-verification of the document holder and the possibility of automatic border control (ABC). Three way verifications means:<br>- verification of document and MRZ<br>- verification optical data set versus electronic data set<br>- verification electronic biometric data set with document holder<br>ABC allows the replacement of border police by an electronic gate. This gate can take over the three way verification as well as matching a data set to a wanted list.<br>The following travel documents could be handled: a) MRP, b) RTP-tokens and c) National eID w/ biometric data, d) e-Residence Permit, e) e-Visa. |
| **Benefits** | - biometrics increases the security of the document<br>- biometrics allows better linkage between holder and travel document<br>- provides a profile of the traveller; identifies those on the “wanted list” ; a traveller profile captures data, such as name, given name, birthday, nationality, 10 fingerprint images, one facial image and other.<br>- Automation of border controls |
| **Security** | Travel documents have 5 to 10 optical security elements; with an embedded microcontroller electronic HW and SW securities are captured. |
| **Interoperability** | - done thanks to a worldwide standard ICAO 9303-1, 9 global interoperability tests in the time window CY 2004 – CY 2009, organized by the ICAO (worldwide) and BIG (Europe) and conformity tests according ISO 10373-6. A test sequence on biometrics and interoperability was not done. |
| **Privacy** | Protection of electronic data by reading MRZ and hashing the value (ICAO-BAC security). Photo image as printed and fingerprint protected by access key in DG14 (BIG-EAC security). |
| **ROI** | Re-financing of production cost by increasing the fee per travel document.<br>Automation might also reduce cost of border controls |

| | |
|---|---|
| **Recommendations** | a) Government recommendation:<br>US regulation VISIT for all VWP-states, published in CY 2004.<br>EU regulation 2252/2004 for all travel documents in EU from August 2006 onwards.<br>b) EUROSMART's recommendation:<br>New travel documents should be used at any SCHENGEN Border, to use the new security level and to protect against crime. Travel documents with biometric data have been issued for five years, but only three airports in Europe have it in use (some of them at the pilot stage), included biometric verification of the document holder. |

| Ethical criteria | Eurosmart technical questionnaire | Eurosmart recommendation to government, ID management and service providers |
|---|---|---|
| Role of the biometric application | Accurate verification of the traveller's identity, by an official or by means of automated inspection systems | EU and member states have discussed the subject and issued regulations and laws |
| Transparency regarding use of biometric technology | Enrolment: By a registration official<br>Storage : in travel document<br>Acquisition & matching by an authorized official or a closed system in a protected area | Describe the procedures in a public document |
| Relevance and necessity | This subject has been dealt with by official bodies in Europe and the Member States, and endorsed by ICAO. | |
| Use of only required information to achieve a clear, limited and specified purpose. | The only information linked to biometric is that required to obtain an accurate identity | Appropriate information available to travel document applicants and travellers should be easily accessible.<br>Access management procedures should be established and made public.<br>An individual should be fully and accurately informed and should understand all the issues and implications relating to the provision of his/her information.<br>General description and guarantee to be described in an easy to find and understand document. |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Access to information can only be made by terminals linked to a key public infrastructure | |
| Can system operators and system providers access information other than that just required to carry out their function? | No information other than that needed to carry out the function is accessible. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | The system does not record the information extracted from the travel document | |
| Can the user make the decision whether or not to participate in the programme? | Not if he wants to travel abroad. | |
| What are the practical measures to ensure the integrity of an individual's personal and information privacy? | The travel document stores raw images; but reading the chip information is protected by the BAC mechanism, and access to biometrics (finger/ iris) is protected by EAC protocol | |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | The travel document information is protected by the BAC mechanism, and access to biometrics (finger/ iris) is protected by EAC protocol | |

| | | |
|---|---|---|
| Clear knowledge of vulnerabilities and protection against them. | Identity verification is performed by an authorized official or by automated inspection terminals that are reliable, secure and attended. | Describe the procedures that go with the technical measures in a public document. |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | ? | |

### 3.2.2. National eID card with biometrics

| | |
|---|---|
| **National eID-Card** | National eID card for eGovernment Services ; biometric data for identification and/or authentication of the card holder |
| **Status** | 12 States in Europe use National eID cards (Spain, Portugal, Monaco, Italy, Belgium, Austria, Netherlands, Lithuania, Estonia, Finland, Sweden, Serbia) 6 of them use biometrics for identification, 1 uses biometrics for verification (Portugal) ; Main purpose of replacing printed ID documents with electronic ID documents is to open up this document to e-government services as well to e-business services and to increase the security of the document. Alongside this application three elements are in use: identification (with a token), authentication (with a PIN or biometric verification) and optional electronic signature. |
| **Benefits** | Benefit for the user/citizens :<br>- in the case of verification: more convenience for the user;<br>- in the case of identification: more trust in secure documents for the police<br>Benefit for the authorises:<br>- user verification at the issuing procedure |
| **Security** | - in the case of verification: Match on Card<br>- in the case of identification: protecton of the data set with access key; typically fingerprint images are stored in the 6 running national eID cards. To protect the images, the Police need the right to read the data. Typically specific access keys to this data are in use. |
| **Interoperability** | - in the case of verification: interoperability programs are not in use.<br>- in the case of identification: test program is in progress under ICT LSP STORK; 17 EU member states participate in this; life test phase for cross border services has been running since July 2010. Biometrics is not part of these cross border interoperability tests. |
| **Privacy** | - in the case of verification: no re-building of fingerprint images; biometric data will never leave the secure token.<br>- in the case of identification: only authorized persons, such as police have access to biometric data. In the case of using the ICAO framework, specific access conditions, such as ICAO-BAC are defined. |
| **ROI** | Refinancing by increasing the document fee. Example: new national eID card in Germany (nPA) costs 28,80€ compared with the current ID-card, at 8€. In the event of re-using part of the infrastructure for travel documents, such as the link to the population register, the bridge to trust center and the data capturing equipment, total cost for the infrastructure could be reduced dramatically. |

| | |
|---|---|
| **Recommendations** | a) Government’s Recommendation:<br>EU recommendation 14351/2005; this refers to ICAO 9303.<br>b) EUROSMART’s Recommendation:<br>In the case of authentication: to maintain privacy as well as security, match-on-card would be the best approach.<br>In the case of identification: the ICAO framework is well known and established. |

Eurosmart recommendations for this use case are to use ICAO 9303 specifications for citizenship identity and another application for digital identity, the analysis with regard to ethics:

- is the same as for border controls, when the ICAO 9303 application is used,
- is given in the following table for digital identity with match on card.

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | Biometric application will replace PIN by matching on card | Full and frank debate on the issues raised by all parties:<br>– Government,<br>– Administrative service providers<br>– Private service providers,<br>– Citizens |
| Transparency regarding use of biometric technology | Enrolment: By a registry official<br>Storage : in eID document<br>Acquisition & matching by cardholder’s terminal and PC | Describe the procedures that go with the technical measures in a public document |
| Relevance and necessity | *Environment*: On internet nobody knows who you are. Password / PIN easy to spoof.<br>*Purpose*: Biometrics is the only technique that can authenticate who you are.<br>*Efficiency*: No existing technique can replace biometrics<br>*Reliability*: Pin and password theft Is an increasing white collar fraud. | A government policy on digital identity management should be defined, describing:<br>– Identity theft dangers for the community, for the service providers and for citizens.<br>– Along with identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities have to be relaible.<br>MOC by itself has a privacy guarantee, but governments must provide evidence that there is no biometric database, or that their use is restricted to justified known use case, using defined procedures protecting privacy.<br>General description and guarantee to be described in an easy to find and understand document. |
| Use of only required information to achieve a clear, limited and specified purpose. | MOC is the cardholder’s clear consent to access his/her data | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | No need for system operators. | |
| Can system operators and system providers access information other than that required to carry out their function? | No need for system operators. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Use of MOC does not allow this possibility. | |
| Can the user make the decision | Use of MOC for accessing e- | Availability of MOC on the eID card |

| | | |
|---|---|---|
| whether or not to participate in the programme? | services is always a voluntary act. | shall be an option decided by the citizen |
| What are the practical measures that ensure the integrity of an individual's personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data must be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | Data protection legislation should be reviewed in order to deal sufficiently with the privacy concerns presented by the use of biometrics. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password.<br>*Substitution attacks,* Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Describe in a public document the procedures that go with the technical measures.<br>Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Government must allow the individual's right to be satisfied at a cost corresponding to the legitimacy of the cardholder's claim. |

### 3.2.3. eID document authenticity as a result of object biometrics

| **e-ID document authenticity** | **e-ID document authenticity: guarantee of genuineness and uniqueness by linking chip and object biometrics(bubble tag for instance).** |
|---|---|
| **Status** | This use case has not yet been implemented, but some proof of the concept has already been developed.<br>The interest of this prospective use case is to guarantee that the chip and the body of the document have been personalized together at the same time as a unique document. It also allows control of the document even if the chip is broken by means of a database transaction |
| **Benefits** | Benefits include :<br>• Tying the medium to the chip<br>• When the chip is broken, control is possible with a bubble tag through a central anonymous database<br>• The chip and a bubble tag may moderate the number of security features<br>• avoids the theft of rights and identity because of the impossibility of duplicating the document |

| | |
|---|---|
| **Security** | The chip can confirm the authenticity of the document body when it is challenged by presentation of the physical biometrics of the object sample.<br>Reinforce the integrity check of the e-ID document: the right chip on the right medium with the right data.<br>Allows control of the e-ID even if the chip is broken in an online transaction. |
| **Interoperability** | At the moment, no standards have been defined to use object biometrics in this way. A standard must be developed. |
| **Privacy** | Object biometrics actually protect privacy by accessing the data of the e-Id without the use of the human biometrics in a database transaction. |
| **ROI** | The bubble tag has an extra cost to integrate it, and increases the price of the smartcard reader, but it may reduce the cost of the document design by reducing the number of extra security features.<br>The reading of object biometrics has an extra cost for the inspection terminal/system |
| **Recommendations** | Object biometrics is recommended to link the document with central anonymous databases and to ensure the link between the chip and the body of the card. |

For this use case, we assume that any on card verification does not infringe civil privacy. This table focuses on on-line access to a central database, if any.

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | A bubble tag closely integrated with the document is linked to the smart card chip. Optionally, in the case of a broken chip a central database can provide document authentication and identity verification | In the case of a central database, full and frank debate on the issues raised by all parties who will be involved in the proposed application, prior to the establishment of the proposed programme |
| Transparency regarding use of biometric technology | Enrolment: Object biometrics created at document personalization<br>Storage : in the document<br>Acquisition & matching by an authorized officialr or a closed system in a protected area | Describe in a public document the procedures |
| Relevance and necessity | An attempt at fraud is breaking the chip of the document, or creating a new document using a chip that was personalized for another identity.<br>*Environment*: The document requires a high degree of security<br>*Purpose*: Make document forgery impossible , by establishing a unique link between document and chip.<br>*Efficiency*: Today there is a multiplication of security features | Access to the database should be allowed in the only case of doubts over the document: Chip broken and security features difficult to verify. |

| | | |
|---|---|---|
| | engraved on or affixed to the document. There are so many that they become difficult to check, except in laboratories.<br>*Reliability*: Reliability is linked to human capacity | |
| Use of only required information to achieve a clear, limited and specified purpose. | The only information linked to the biometrics is that required to obtain an accurate identity | Appropriate information available to travel document applicants and travellers should be easily accessible.<br>Access management procedures should be established and made public.<br>An individual should be fully and accurately informed and should understand all the issues and implications relating to the provision of his/her information.<br>General description and guarantee to be described in an easy to find and understand document.<br>General description and guarantee to be described in an easy to find and understand document. |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Access to information can only be made by terminals linked to a public key infrastructure | |
| Can system operators and system providers access information other than that required to carry out their function? | No information other than that needed to carry out the function is accessible. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | The only information linked to the biometrics is the one requested for getting an accurate identity (ICAO) | |
| Can the user make the decision whether or not to participate in the programme? | Not if he wants to travel abroad. | |
| What are the practical measures that ensure the integrity of an individual's personal and information privacy? | The record in the database can be encrypted by a key extracted from the bubble tag. | |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | The record in the database can be encrypted by a key extracted from the bubble tag. The BAC protocol can also be used. | |
| Clear knowledge of vulnerabilities and protection against them. | Identity verification is performed by an authorized official or by automated inspection terminals that are reliable, secure and attended. | Describe the procedures that go with the technical measures in a public document. |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Technical solution must allow the subsequent actions to be performed with appropriate security. | Procedures must allow the individual's rights to be satisfied. |

### 3.2.4. Physical / logical access control

| **Employee ID card for physical access control** | **ID card for controlling access to restricted area, corporate or government facilities** |
|---|---|
| **Status** | Securing access to sensitive facilities has always been a concern. Video surveillance can give information after unauthorized access but security officers need to prevent unauthorized access. Access can be restricted to certain employee after authenticating themselves.<br>Today some smart solutions are used such as badges based on smart card technology. Fingerprints are also used alone or linked to a database of authorized users. Combining employee ID card and biometrics offers a more convenient and reliable solution respecting the privacy of end-users.<br>- Boeing employee card with fingerprint data (since 2007)<br>- Case Use electronic Government Employee-eID cards with biometric data, e.g. US Department of Defence, US-Army and US-Coast Guard |
| **Benefits** | More secure for security officers as biometrics allows verification of the user instead of an object owned by the user.<br>As the user cannot lose his biometric identifier, it is more secure than a PIN code for security officers and it provides more confidence and convenience for users.<br>Other applications can be accessed through employee badges after a biometric authentication. For instance, e-purse for vending machines inside the building, access to the canteen… |
| **Security** | Use of biometrics enables strong authentication as the end-user needs to be present at the control point to present his biometric identifier.<br>It reinforces the fight against fraud and unauthorized access as an employee card cannot be shared between employees and a lost card cannot be used on its own (i.e. without end-user presenting his biometrics). |
| **Interoperability** | Interoperability can be achieved using standards for biometric images and or templates (ANSI 378, ISO 19794-2, ISO 19794-4) and using standards for contactless protocols (ISO 14443). |
| **Privacy** | As a result of MoC, end-user's privacy is maintained by keeping the reference template in the proven secure environment of a smartcard.<br>Storage of end-user's biometrics (On-Card or in databases) must be done with regard to ethics & privacy committee's recommendations for each country. |
| **ROI** | No more pin code/password loss. Cost saving for card re-issues.<br>According to a cost/benefit analysis from US DoS, 200USD per user per year can be saved on password management by the use of biometrics. |
| **Recommendations** | Logical and physical access applications can be merged on a single dual employee ID card.<br>Each solution must be adapted and/or customized to the needs of the different stakeholders: Military restricted area access control vs private company employees' access control. |
| **Eurosmart Recommendations** | Combination of an access badge with MoC and biometrics for two factor identification with respect for privacy.<br>For highly sensitive areas, multimodal biometrics can be used with combination of fingerprint and iris for instance. |

| **Employee ID card for logical access control** | **Digital ID for employees enabling logical access control to sensitive data and critical IT infrastructures** |
|---|---|
| **Status** | Authentication on IT networks in companies or government agencies is mainly done through PIN code or passwords. But PIN codes and passwords are something the user knows and that he can give them to someone else or they can be retrieved against his will. As soon as someone has a password, he can be authenticated on the system with another identity until it has been deactivated by security officers.<br>Combining employee ID card and biometrics offers a more convenient and reliable solution respecting privacy of end-users. |
| **Benefits** | More secure for security officers as biometrics allows verification of the user instead of an object owned by the user and/or a password he knows.<br>As the user cannot lose his biometric identifier, it offers more security than a PIN code for security officers and it offers more confidence and convenience for users.<br>Biometric can be used to cipher and sign electronic file/documents. |
| **Security** | Use of biometrics enables a strong authentication as the end-user needs to present both his employee card and his biometric identifier to be authenticated by the system.<br>It reinforces the fight against fraud as the employee card cannot be shared between employees and a lost card cannot be used on its own (i.e. without end-user presenting his biometrics).<br>Electronic corporate data can be encoded and protected when stored and/or sent in e-mails with biometrics ensuring their integrity. E-mails can be signed by an electronic stamp ensuring authenticity of electronic communications inside the company/government agency. |
| **Interoperability** | Interoperability can be achieved by using standards for images and or templates (ANSI 378, ISO 19794-2, ISO 19794-4)<br>Currently, no standard is defined for employee digital identity. |
| **Privacy** | Thanks to MoC, end-user's biometrics remains in his card. It ensures end-user's privacy by keeping the reference template in the proven secure environment of a smartcard.<br>End-user can encode his files on his desktop with his biometric identifier and prevent access to them by another user.<br>Storage of end-user's biometrics (On-Card or in databases) must be done with regard to ethics & privacy committee's recommendations of each country. |
| **ROI** | No more pin code/password loss. Cost saving for card re-issues.<br>Reduction of calls to help desk for password resets<br>Reduce electronic data thrft.<br>According to a cost/benefit analysis from US DoS, 200USD per user per year id saved on password management by the use of biometrics. |
| **Recommendations** | Logical and physical access applications can be merged on a single dual employee ID card.<br>Each solution must be adapted and/or customized to the needs of the different stakeholders:<br>▪ High security infrastructure<br>▪ Government employee for IT network access, legal forms |

| | |
|---|---|
| | digital signature…<br>▪ Private company employees for IT network access… |
| **Eurosmart Recommendations** | Combination of an access badge with MoC and biometrics for two factor identification with respect of privacy.<br>Definition of a standard for employee digital identity on corporate networks.<br>European standard IAS-ECC can be used for digital signature application. |

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | Biometric application is to use MOC in both cases of physical access control and PIN replacement | Full and frank debate on the issues raised by all parties in the entity concerned of a public or private organization. |
| Transparency regarding use of biometric technology | Enrolment: By an appointed official<br>Storage: in the employee card only.<br>Acquisition by means of attended terminals for physical access and cardholder's terminal for logical access control.<br>Matching: On card | Describe in a document the procedures that go with the technical measures.<br>Request the legal authorizations. |
| Relevance and necessity | *Environment, purpose*, e*fficiency*: relative to the entity that must be protected<br>*Reliability*: MOC is more reliable than codes, PINs and passwords. | The ID management policy of the entity must comply with legislation, regulations. Information will describe<br>– The dangers for the entity, for the employees.<br>– The management of biometric data and procedures, confirming that no biometric database would be set up. |
| Use of only required information to achieve a clear, limited and specified purpose. | MOC is the clear cardholder's consent to be authenticated. No access to any further information. | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Biometrics does not affect in any way the management of employee's information. | |
| Can system operators and system providers access information other than that required to carry out their function? | Biometrics does not affect in any way the management of employee's information. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Biometrics does not affect in any way the management of employee's information. | |
| Can the user make the decision whether or not to participate in the programme? | Use of MOC may be not the unique identification / authentication mean. | Subject to negotiation in the entity, taking into account, relevance, necessity and acceptance by users. |
| What are the practical measures that ensure the integrity of an individual's personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | Templates are never stored or transmitted elsewhere other than inside the card. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password. | Describe in a public document the procedures that go with the technical measures. |

| | | |
|---|---|---|
| | *Substitution attacks* Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Entity must allow the individual's rights to be satisfied. |

### 3.2.5. Healthcare

| **Healthcare** | **Use of smart card + biometrics in order to enhance efficiency, prevent fraud, whilst reducing healthcare costs** |
|---|---|
| **Status** | eHealth card systems appeared in the early 90s, to streamline the infrastructure for transactions and processing. The objective was to reduce the administrative costs of health care coverage.<br>Since the new millennium, security objectives became an increasingly important aspect for protecting the personal data of users and it become crucial to enhance the security of those systems aimed at protecting against fraud, on the one hand, and abuse/excessive treatment, on the other.<br>Many European countries (France, Germany, Slovenia, Spain, Italy, etc.) have already set up modern healthcare systems. Many other initiatives are currently being pursued around the world (South Africa, Taiwan, Algeria, etc).<br>Today a new generation of systems are arriving adding new features to the infrastructure already in place, based on PKI for example, implementing ePrescriptions management, allowing online medical data... where strong authentication is needed. Biometrics is the perfect technology to achieve this goal. |
| **Benefits** | Providers<br>- Instant patient identification<br>- Rapid accessibility to patient medical history<br>- Accurate link between patients and institutional medical records<br>- Faster care delivery in emergency care situations<br>- Potential reduction in adverse events and medical errors due to lack of patient information<br>- Reduction in claims denials<br>- Integration with legacy systems with nominal IT costs<br>- Audit trail through a course of treatment across multiple organizations<br>- Reduction in unnecessary/duplicated diagnostic tests or procedures by providing results from other medical providers<br><br>Healthcare Delivery Organizations<br>- Reduction or elimination of mismanaged, lost or stolen electronic records<br>- Fraud Reduction via accurate patient identity<br>- Data Integrity -- Reduced medical record maintenance costs (duplicates/overlays) --<br>- Streamlined administrative procedures<br><br>Healthcare Employer<br>- Highly secure identity credential for both physical and logical access<br>- Single sign-on capabilities (reduction in help desk calls/password management requirements)<br>- Link to other employee services (ID badge, parking, cafeteria) |
| **Security** | - against fraud and misuse of system both from patients and health care providers<br>- patient security – enabling quick decision making based on correct facts |
| **Interoperability** | - Regulatory Compliance: HIPAA and DEA compliance for ePrescribing controlled substances<br>- Interoperability using standards for images and or templates (ANSI 378, ISO 19794-2, ISO 19794-4) |
| **Privacy** | - MoC with template stored on card possible, no database needed. |
| **ROI** | In France, with the Vitale card, annual administrative cost savings have been estimated at EUR 300 millions,<br>In Germany, the annual medical cost savings have been estimated at EUR 3 |

| | |
|---|---|
| | billions. |
| **Recommendations** | - combination of smart cards and biometrics for identification of both patients, doctors and other health care providers<br>- win-win situation<br>• Patients get more efficient and quicker help<br>• Reduced administration and higher efficiency for health care providers<br>• Reduced fraud, saving money for insurance and government |

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | Biometric application is to replace PIN by matching on card | Full and frank debate on the issues raised by all parties:<br>– Social insurance<br>– Healthcare professionals (HP)<br>– Patients |
| Transparency regarding use of biometric technology | Enrolment: By a registry official at Insurance premises.<br>Storage : on eID card only<br>Acquisition by HP's terminal for an electronic claim, or cardholder's terminal for access to a medical / health insurance server<br>Matching on card. | Describe the procedures that go with the technical measures in a public and easily accessible document |
| Relevance and necessity | *Environment*: Medical information is very sensitive. The MOC protects privacy.<br>*Purpose*: The requirement is actuallyto authenticate who you are.<br>*Efficiency*: No existing technique can replace biometrics<br>*Reliability*: Pin and password theft Is an increasing white collar fraud. | A policy on medical data and digital identity management should be defined, describing:<br>– Identity theft dangers for the community, social insurance, healthcare professionals and for patients.<br>– Along with identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities must be trusted.<br><br>MOC by itself has a privacy guarantee, but health insurance management must provide evidence that there is no biometric database.<br><br>General description and guarantee to be described in an easy to find and understand document. |
| Use of only required information to achieve a clear, limited and specified purpose. | MOC is the clear cardholder's consent to access his/her data | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Introducing biometric MOC does not particularly impact this point. | |
| Can system operators and system providers access information other than that only required to carry out their function conduct their job? | Introducing biometric MOC does not particularly impact this point. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Introducing biometric MOC does not particularly impact this point. | |
| Can the user make the decision whether or not to participate in the programme? | Use of MOC for accessing e-services is always a voluntary act. | Availability of MOC on the eID card must be an option decided by the patient. Warning of weaker protection of personal data should |

| | | |
|---|---|---|
| | | be given in case of refusal to use MOC. |
| What are the practical measures that ensure the integrity of an individual's personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | No specific concern as far as biometrics is concerned. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password.<br>*Substitution attacks* Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Describe in a public document the procedures that go with the technical measures.<br>Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Health insurance must allow the individual's right to be satisfied at costs corresponding to the legitimacy of the cardholder's claim. |

### 3.2.6. Welfare

| **Using biometrics for welfare** | **Use of smart card + biometrics in order to prevent fraud, misappropriation of welfare benefits whilst protecting privacy** |
|---|---|
| **Status** | Welfare programs provide pension payments, distribution of goods and services to poor populations. In many cases, the people who should benefit from the program do not have any ID document. It might also be the case that no civilian registration is in place. Provision of goods and services is decentralized and very often no on-line connection is available. People must be identified in order to avoid misappropriation of the benefits. Biometrics is the most secure means to identify these people. |
| **Benefits** | For welfare organizations<br>- Instant individual identification<br>- Elimination of duplicate beneficiaries<br>- Fraud Reduction via accurate patient identity<br>- Easier administrative processing<br><br>Beneficiaries<br>- Confirmation that he/she is a beneficiary of the program<br>- |
| **Security** | - against fraud and misappropriation by misuse of identity<br>- Biometrics is linked to the beneficiary not to a document that can be counterfeited, stolen or lent. |
| **Interoperability** | - Interoperability using standards for biometric images and or templates |
| **Privacy** | Non Governmental organizations are not officials. They are not entitled to manage a biometric database. Then MOC is the right solution. |
| **ROI** | In all cases, there is the need to enrol all the beneficiaries. Capturing biometric data does not represent a significant cost increase in the process. It allows prevention of duplicate identities. Issuing a document for biometric matching is cheap compared to the cost of an on-line IT infrastructure. |
| **Regulations and recommendations** | |
| **Eurosmart recommendations** | - combination of smart cards and biometrics for beneficiaries<br>- Avoid the use of biometric database for convenience and misuse by organizations that shall not be entitled to manage identities |

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | Biometric application will verify the beneficiary's identity. | Full and frank information to all parties.<br>– Government<br>– Welfare organization members<br>– Beneficiaries |
| Transparency regarding use of biometric technology | Enrolment: By an authorized official with only possibility of recording templates onto the beneficiary's | Describe in a public and easily accessible document the procedures that go with the |

| | | |
|---|---|---|
| | card.<br>Storage : on beneficiary’s card only<br>Acquisition by welfare organization terminal.<br>Matching on card. | technical measures |
| Relevance and necessity | *Environment*: No civil registry able to prevent duplicated identities<br>*Purpose*: The requirement is to authenticate who the beneficiary is<br>*Efficiency*: No existing technique can replace biometrics<br>*Reliability*: No other reliable solution for most cases | A policy on welfare benefits and digital identity management should be defined, describing:<br>– The risks that must be prevented.<br>– Alongside a clear statement on the use of biometrics<br>MOC by itself has a  privacy guarantee but welfare organization must provide evidence that there is no biometric database,<br>General description and guarantee to be described in an easy to find and understand document, for the people concerned. |
| Use of only required information to achieve a clear, limited and specified purpose. | Introducing biometric MOC does not particularly impact this point. | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Introducing biometric MOC does not particularly impact this point. | |
| Can system operators and system providers access information other than that only required to carry out their function? | Introducing biometric MOC does not particularly impact this point. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Introducing biometric MOC does not particularly impact this point. | |
| Can the user make the decision whether or not to participate in the programme? | Balanced benefits are important for beneficiaries. Biometrics is more likely to be used as a protection of privacy rather than a threat to privacy. | |
| What are the practical measures that ensure the integrity of an individual’s personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | No specific concern as far as biometrics is concerned. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password.<br>*Substitution attacks*  Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Describe in a public document the procedures that go with the technical measures.<br>Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Welfare organization must allow the individual’s rights to be satisfied corresponding to legitimate claims. |

### 3.2.7. eGovernment

| **eGovernment use case:** | **Declaration of revenues of small enterprises for calculation of company's owner social contributions** |
|---|---|
| **Status** | e-Government Services with biometric authentication are being deployed in Portugal (since 2007).<br>In France, this declaration can be made over the internet by an employee of the company. Security is carried out by an identifier + a password authentication. After the first declaration, the company receives a letter informing them of this identification.<br>In small companies, the security culture is poor. Protection of identifiers and passwords may not be observed. A malicious person could create problems for the company owner with social organizations and the legal system.<br>The use of the national eID card would make great progress in terms of security. In addition, authentication via Match On Card would provide the guarantee that the card holder is the person who made the declaration. |
| **Benefits** | For the employee: This person would feel comfortable that nobody can carry out malicious acts with his / her identity.<br>For the company owner: His delegation of duties to a person is secure.<br>For the service provider: Small companies will make more on-line declarations that will reduce its costs and enhance its own processes. Disputes are unlikely to happen. |
| **Security** | Security is enhanced by means of strong authentication. The benefit in terms of security is to avoid personal financial harm and unmerited problems with social declaration organizations and the legal system. |
| **Interoperability** | European Citizen Card (ECC) and electronic signature standards are applicable. |
| **Privacy** | Use of his/her own credentials might be seen as a privacy risk by the employee. Match On Card authentication, if well explained, would put his/her mind of rest. |
| **ROI** | No investment required: The company does not have to issue corporate cards. The security solution is effected by the use of the employee's ID card. |
| **Regulations & recommendations** | EC initiatives and directives in terms of eGovernment and electronic signature. |
| **Eurosmart recommendations** | For the adoption of the solution, there is a need to explain what Match On Card is. There is also a need for Ethical organizations to confirm that Match On Card does not infringe in any way card holder's privacy. |

With regards to privacy and ethics, this is a special use of an eID card. So the same table applies.

### 3.2.8. eBanking

| **e-Banking** | **Introducing biometric authentication for on line banking use cases** |
|---|---|
| **Status** | Banks are familiar with risk management and use in order to adapt the security of their system to the best compromise between ease of access their services, security costs and the risk of fraudulent use of e-banking services.<br>As early adopters of biometric technology for employees it is expected that this functionality also will be made available to customers. |
| **Benefits** | Biometric technology simplifies access to services while Match-on-Card ensures end-user privacy. |
| **Security** | PINs and passwords are frail links in a security chain as they are easily written down, lost, borrowed or even stolen. With biometric Match-on-Card, you tie each transaction to a physical individual, creating traceability and reducing risks of fraud. |
| **Interoperability** | N/A – closed loop system. |
| **Privacy** | Match on card ensures end-user privacy by keeping the reference template in the proven secure environment of a smartcard. |
| **ROI** | Many laptops have built in sensors but for those who does not have one there is an investment related mainly to distribution of biometric readers. These readers, when distributed to customers without support, may also provide a branding opportunity for the bank. |
| **Recommendations** | None |
| **Eurosmart Recommendations** | Match-on-Card is strongly recommended to ensure privacy of clients. The possibility of allowing the clients to self enrol solves what would otherwise be a logistical challenge in some parts of the world. |

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | Biometric application would replace PIN / secret code / password by matching on card | Application shall comply with the law, regulations, and necessary authorizations.<br>The contract between the bank and the customer m,ust provide clear information on all issues.<br>– |
| Transparency regarding use of biometric technology | Enrolment: By the customer him/herself in secure premises of the bank, in presence of a bank official.<br>Storage : on eID card only<br>Acquisition by cardholder's terminal | Describe in the contract the procedures that go with the technical measures |

| | | |
|---|---|---|
| | to access a bank server<br>Matching on card. | |
| Relevance and necessity | *Environment*: Banking information is very sensitive. The MOC protects privacy.<br>*Purpose*: The requirement is to authenticate who you are.<br>*Efficiency*: No existing technique can replace biometrics<br>*Reliability*: Pin and password theft Is an increasing white collar fraud, especially for financial transactions. | The bank policy on digital identity management should be defined, describing:<br>– Identity theft dangers for the bank, service providers and customers.<br>– Alongside identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities must be trusted.<br>MOC by itself has a privacy guarantee, but the bank must provide evidence that there is no biometric database.<br>General description and guarantee to be described in an easy to find and understand document. |
| Use of only required information to achieve a clear, limited and specified purpose. | MOC is the clear cardholder’s consent to access his/her data | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Introducing biometric MOC does not particularly impact this point. | |
| Can system operators and system providers access information other than that only required to carry out their function? | Introducing biometric MOC does not particularly impact this point. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Introducing biometric MOC does not particularly impact this point. | |
| Can the user make the decision whether or not to participate in the programme? | Use of MOC for accessing e-services is always a voluntary act. | Availability of MOC on the card must be an option decided by the customer. Warning of weaker protection of personal data should be given in case of refusal to use MOC. |
| What are the practical measures that ensure the integrity of an individual’s personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | No specific concern as far as biometrics is concerned. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password.<br>*Substitution attacks* Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Describe in the contract the procedures that go with the technical measures.<br>Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Banks must allow the individual’s rights to be satisfied at costs corresponding to the legitimacy of the cardholder’s claim. |

### 3.2.9. Vehicle Registration card

| **Electronic Vehicle Registration card** | **The EU Directive 2003/127/EC of December 2003, allows all member countries to introduce an electronic vehicle registration card as an alternative to the paper format. The card replaces previous documents dealing with registration and ownership of the vehicle concerned.** |
|---|---|
| **Status** | Electronic vehicle registration cards have been in discussion for a number of years, but up to the end of 2009, none had been introduced. Since 2009, however, member countries and their transport ministries have shown increased interest in the introduction of a highly secure electronic registration document. Slovakia, Austria and the Netherlands are leading the way and are already implementing the eVRC. Morocco has issued electronic Vehicle cards since 2007<br><br>No biometric technique is involved to date. |
| **Benefits** | For the user, for the service provider, the government, the society, …<br>Road safety is a huge concern: It is a matter of saving lives, not simply money! Card document fraud is at very high level. In France, 200 000 cars are stolen annually and most of them are reused in France or other countries. The directive allows the addition of further data or changes to be made to the data initially created in the card. An overwrite option can, for example, be useful where vehicle modifications or tuning require registration changes that are not personalized in the card. The introduction of the eVRC will not only simplify vehicle checks by the responsible authorities at home and abroad but also make them more reliable.<br>Smart card technology and security features printed or engraved in the document will provide a high level of security. A higher level of global security could be obtained by tying the vehicle to the document, using object biometrics. A bubble tag placed in the windscreen of the vehicle and identified in the chip of the eVRC would establish this strong link.<br><br>Benefits for society: fewer accidents caused by vehicles that should no longer be used. Lives saved!<br>Benefits for enforcement officers: Fast, easy and efficient checking of vehicle ownership, operational ability.<br>Benefit for car owners and insurance companies: drastic reduction in vehicle thefts. |
| **Security** | Road safety is enhanced.<br>Vehicle thefts are drastically reduced. Cost of vehicle insurance could be reduced accordingly. |
| **Interoperability** | Directive 2003/127/EC<br>A further standardization of use of object biometrics should be provided, but not impacting on previous standards. |
| **Privacy** | Reading the biometrics of the vehicle could infringe privacy by tracking vehicle trips. However using eVRC and the vehicle together does not present such risks. O line checking with a database can be strictly allowed for enforcement officers in some very specific cases. |
| **ROI** | The cost of a smart card is of course higher than the classical paper document. But fees paid for VCR by motorists are very high in comparison of the technology costs, and thus are not really linked to it. Adding object biometricswould not add a cost to the eVRC.<br>Introducing a bubble tag would affect the manufacturing of the vehicle part (windscreen as suggested here) but not significantly.<br>Identity verification, including e-passports, eID cards, Driving licenses, |

| | |
|---|---|
| | eVRCs, tachograph cards, can be done with same tools. Use of object biometrics would request an additional sensor.<br>Estimation of ROI: Most investment for eVRC can be shared by all other eID documents. Bubble tags add a marginal cost. But benefits are firstly saving of lives, and then the possibility of drastically reducing vehicle theft. |
| **Regulations & recommendations** | No regulation, no recommendation to date. |
| **Eurosmart recommendations** | Recommendations when using object biometrics are only linked to on line verification. This should be limited to police, and only in the case of non presentation of the eVRC, broken chip, or vehicle theft suspicion. Object biometrics could be used for anonymity of the data base, in this case. |

The use case of a bubble tag applied to a document with the aim of guaranteeing genuineness and uniqueness of the document is very similar to the eIdentity document authenticity use case. So the same table may be reused.
In the case of a bubble tag (or any object biometrics) installed on the vehicle, we assume that any on card verification would not infringed civil privacy. So, the following table focuses on on-line access to a central database, if any.

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | A bubble tag integrated in the vehicle is linked to the chip of the car registration smart card.<br>Optionally, in the case of a broken chip a central database can provide document authentication and vehicle data. | In the case of a central database, full and frank debate on the issues raised by all parties who will be involved in the proposed application, prior to the establishment of the proposed programme |
| Transparency regarding use of biometric technology | Enrolment: The biometrics of object is created at document personalization<br>Storage : in the document<br>Acquisition & matching by an authorized official or a closed system in a protected area | Describe the procedures in a public document |
| Relevance and necessity | An attempted fraud is breaking the document chip,<br>*Environment*: The document requires a high degree of security<br>*Purpose*: Make impossible to have fakes or forged documents for bad deals of vehicles.<br>*Efficiency*: Today no real security feature exists.<br>*Reliability*: No equivalent solution in terms of reliability | Access to the database should be allowed in well defined case uses: Upload of data, or check in the case of doubts on the document: Chip broken and security features difficult to verify. |
| Use of only required information to achieve a clear, limited and specified purpose. | Introducing of object biometrics does not particularly impact this point. | Appropriate information available to vehicle owners should be easily accessible. .<br>Access management procedures should be established and made public.<br><br>An individual should be fully and accurately informed and should |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Introducing of object biometrics does not particularly impact this point. | |

| | | |
|---|---|---|
| Can system operators and system providers access information other than that only required to carry out their function? | Introducing of object biometrics does not particularly impact this point. | understand all the issues and implications relating to the provision of his/her information.<br>General description and guarantee to be described in an easy to find and understand document. |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Introducing of object biometrics does not particularly impact this point. | |
| Can the user make the decision whether or not to participate in the programme? | Introducing of object biometrics does not particularly impact this point. | |
| What are the practical measures that ensure the integrity of an individual's personal and information privacy? | Introducing of object biometrics does not particularly impact this point. | |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Object biometrics of is not linked to a person. | |
| Clear knowledge of vulnerabilities and protection against them. | Identity verification is performed by an authorized official or by automated inspection terminals that are trusted, secured and attended. | Describe in a public document the procedures that go with the technical measures. |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Technical solution must allow the performance of the subsequent actions, with suitable security. | Procedures must allow the individual's rights to be satisfied. |

### 3.2.10. Payments, cash withdrawals

| **Payments, cash withdrawals: use of biometrics instead of PIN or as a complement.** | **Tailored payment solutions depending on the user Identity As aresult of biometrics, we can now adapt and tailor the payment solution for each citizen category.** |
|---|---|
| **Status** | Access to smartcards has historically been controlled by a simple authentication method: the PIN (Personal Identification Number).<br>As a result of the right PIN, the cardholder has access to the card functionalities. This solution is relatively weak because the code can be easily forgotten and quickly recoverable.<br>Biometric technologies can improve these authentication mechanisms. Indeed, a combination of both PIN and biometrics will easily improve security and privacy.<br>Another solution is only to use biometrics to verify the user identity depending on the application.<br>In some countries, many citizens can enjoy tax exemption on purchases. In this situation, the vendor or the authority need to verify the identity to adapt the payment. This is typically the type of application where MoC adds value. |
| **Benefits** | For the user, for the service provider, the government, the society, …<br>- Avoids card sharing: only the cardholder can use it. Transaction only possible for the cardholder.<br>- Easy to use and impossible to forget compared to a PIN code.<br>- Strong authentication: the card and the cardholder are at the same place at the same time.<br>- Easy to integrate into current systems.<br>- Improves user confidence.<br>- Cost saving for issuer due to the pin code loss and card reissue.<br>- Possibility to adapt the payment as a result of the User Identity, tailored payment solution depending on the type of user. Authentication is done in advance to adapt the method of payment to the user's profile.<br>- No database, no constraining maintenance |
| **Security** | How is security enhanced? Protection against terrorism, fraud, counterfeiting, identity theft, theft of money, …<br>- Strong cardholder authentication<br>- No skimming<br>- Impossible to use a stolen payment card<br>- Avoids people looking over the shoulder |
| **Interoperability** | done thanks to standards? Regulation, …<br>- EMV<br>- ISO<br>- NFC |
| **Privacy** | What are the privacy concerns?<br>- No database.<br>- Only the cardholder has the record of his fingerprints.<br>- Fingerprints secured in the tamper-proof environment of the smart card. |

| | |
|---|---|
| | - Impossibility of card sharing. |
| **ROI** | Estimate of ROI: Investment, extra recurrent costs, measurable benefits<br>- Cost saving for issuers due to pin code loss and card reissue.<br>- No costs for database maintenance.<br>- Costs due to fingerprint reader to be integrated at the point of sale. |
| **Recommendations** | For adoption of the solution, for programs, support procedures, advices to regulation<br>- Add biometric functionality when a payment solution needs to be adapted due to the user identity.<br>- Work closer with Visa/MasterCard to integrate the Biometric PIN. |

| **Ethical criteria** | **Eurosmart technical questionnaire** | **Eurosmart recommendation to government, ID management and service providers** |
|---|---|---|
| Role of the biometric application | Biometric would replace PIN / secret code / password by matching on card | Application shall comply with the law, regulations, and necessary authorizations.<br>The contract between the bank and the customer must provide clear information on all issues. |
| Transparency regarding use of biometric technology | Enrolment: By the customer him/herself in secure premises of the bank, in presence of a bank official.<br>Storage : on eID card only<br>Acquisition by payment terminal or an ATM for a payment or a cash withdrawal<br>Matching on card. | Describe in the contract the procedures that go with the technical measures |
| Relevance and necessity | *Environment*: Spoofing a PIN at payment terminal or ATM is easy.<br>*Purpose*: The requirement is to replace the PIN weakness.<br>*Efficiency*: No existing technique can replace biometrics<br>*Reliability*: false or true PIN theft Is increasing. | The bank policy on biometric use should be defined, describing:<br>– Risks for the bank, retailers and customers.<br>– Use of biometrics should not be imposed, but given as a more secure and convenient possibility when digital identities must be trusted.<br>MOC by itself has a privacy guarantee, but the bank must provide evidence that there is no biometric database,<br>General description and guarantee to be described in the contract. |
| Use of only required information to achieve a clear, limited and specified purpose. | Introducing biometric MOC does not particularly impact this point. | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | Introducing biometric MOC does not particularly impact this point. | |
| Can system operators and system | Introducing biometric MOC does | |

| | | |
|---|---|---|
| providers access information other than that only required to carry out their function? | not particularly impact this point. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Introducing biometric MOC does not particularly impact this point. | |
| Can the user make the decision whether or not to participate in the programme? | Use of MOC for accessing e-services is always a voluntary act. | Availability of MOC on the card must be an option decided by the customer. Warning of weaker protection must be given in case of refusal to use MOC. |
| What are the practical measures that ensure the integrity of an individual’s personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | No specific concern as far as biometrics is concerned. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password.<br>*Substitution attacks* Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Describe in the contract the procedures that go with the technical measures.<br>Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Banks must allow the individual’s rights to be satisfied at costs corresponding to the legitimacy of the cardholder’s claim. |

### 3.2.11. Protection of children: Safe Chat

| **Chat** | **Access control of participants to a children's chat room, by biometric authentication, in order to avoid participation by undesirable adults.** |
|---|---|
| **Status** | Users are not all familiar with risk management and there is the need to adapt the security of their system to the best compromise between ease of access to chatroom services, security cost and the risk of fraudulent chat.<br>Teenagers do not perceive the risks connected with chatrooms.<br>As early adapters to biometric technology for adults it is expected that this functionality will also be made available to teenagers. |
| **Benefits** | Biometric technology simplifies access to services while Match-on-Card ensures end-user privacy.<br>The strong secure authentication reinforces the age validation and guarantees that teenagers are talking with appropriate persons in term of age. |
| **Security** | PINs and passwords are weak links in a security chain as they are easily written down, lost, borrowed or even stolen. With biometric Match-on-Card, you tie each chatroom to a physical individual, creating traceability and reducing risks of fraud. |
| **Interoperability** | Biometrics are not part of these cross border/systems interoperability tests. Bu, the approach as in e-Passports could be reused here. |
| **Privacy** | Match on card ensure end-user privacy by keeping the reference template in the proven secure environment of a smartcard.<br>- in the case of verification: no re-building of fingerprint images<br>- in the case of identification: only authorized person have access to biometric data |
| **ROI** | Many laptops have built in sensors but for those who does not have one there is an investment related mainly to distribution of biometric readers |
| **Recommendations** | The approach as in e-Passports could be reused here. |
| **Eurosmart Recommendations** | Match-on-Card strongly recommended. |

| Ethical criteria | Eurosmart technical questionnaire | Eurosmart recommendation to government, ID management and service providers |
|---|---|---|
| Role of the biometric application | Biometric application will replace PIN by matching on card | Full and frank debate on the chatroom misuses raised by all parties:<br>– Government,<br>– Administrative service providers<br>– Private service providers,<br>– Citizens |
| Transparency regarding use of biometric technology | Enrolment: By a registry official<br>Storage : on eID document<br>Acquisition & matching by | Describe in a public document adapted to teenagers the procedures that go with the |

| | | |
|---|---|---|
| | cardholder’s terminal and PC | technical measures |
| Relevance and necessity | *Environment*: On internet nobody knows who you are. Password / PIN easy to spoof.<br>*Purpose*: Biometrics is the only technique that can authenticate who you are.<br>*Efficiency*: No existing technique can replace biometrics<br>*Reliability*: Pin and password theft Is an increasing white collar fraud. | A government policy on digital identity management should be defined, describing:<br>– Identity theft dangers for the community, for the service providers and for teenagers.<br>– Along with identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities must be trusted.<br>MOC by itself has a privacy guarantee, but governments must provide evidence that there is no biometric database, or that their use is restricted to justified known use caseuse cases, using defined procedures protecting privacy.<br>General description and guarantee to be described in a document easy to find and understand forteenagers. |
| Use of only required information to achieve a clear, limited and specified purpose. | MOC is the clear cardholder’s consent to access his/her chat | |
| Are system operators and system providers properly trained with regard to their obligations to respect and protect the information? | No need of system operators. | |
| Can system operators and system providers access information other than that only required to carry out their function? | No need of system operators. | |
| Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately? | Use of MOC does not give any possibility to do so. | |
| Can the user make the decision whether or not to participate in the programme? | Use of MOC for accessing e-services is always a voluntary act. | Availability of MOC on the eID teenager’ card must be an option decided by the citizen |
| What are the practical measures that ensure the integrity of an individual’s personal and information privacy? | Templates and MOC are the best measures for ensuring both integrity and privacy of information | No specific concern as far as biometrics is concerned. |
| The biometric data should be classified as sensitive personal information and as such afforded greater protection. | Templates are never transmitted outside of the card. | Data protection legislation must be reviewed in order to deal sufficiently with teenagers privacy concerns presented by the use of biometrics. |
| Clear knowledge of vulnerabilities and protection against them. | *Spoofing,* Less easy than with PIN / password<br>*Replay attacks,* Less easy than with PIN / password.<br>*Substitution attacks* Not possible*.<br>*Tampering* not possible*.<br>*Masquerade attacks* not possible*<br>*Overriding the yes/no response,* Not possible*.<br>* within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum | Describe in a public document the procedures that go with the technical measures.<br>Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum) |
| An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary, | Possibility to cancel a card and issue a new one. | Government must allow the individual teenager’s rights to be satisfied at costs corresponding to the legitimacy of the cardholder’s claim. |

### 3.2.12. Notary Acts

| **Notary acts** | **Use of object biometrics for authentication of documents** |
|---|---|
| **Status** | This solution is to use object biometrics and is already up and running in some countries to certify and authenticate original notary deeds as land titles. One reference solution is Benin where now object biometrics are systematically attached to the issued documents. |
| **Benefits** | Land title used to be falsified, counterfeited, and illegally delivered. Consequently the documents were questionable and lost value Offering the possibility to prove that one is in possession of the one and only unique original gives value to the documents. Benefits are many; for the benefit of the citizen, who can negotiate an investment loan with banks for his land, for the city that can identify the rightful owners, and for the economy of the society because of the trustworthy environment.<br>The most convenient solution is to use a bubble SmartCard and an Authentication Cloud services. The bubble SmartCard allows the owner to certify the current use of the notary deed to prove and apply the right attached to the bubble SmartCard and the Authentication Cloud services with the bubbleTag reinforce the long term verification of the document. |
| **Security** | Security is enhanced by having the token proving that the document is genuine and that the information is accurate and not altered in any way. Additionally security is durable because no information is stored in the biometric element, it is just a unforgeable optical key linked to managed security information stored on an electronic medium as a Bubble SmartCard for years |
| **Interoperability** | The system is web based and accessible to all citizens according to local rules and regulations |
| **Privacy** | None, it obeys local laws and can be changed should privacy issues change |
| **ROI** | The cost of using a bubble SmartCard and Authentication Cloud services is higher than a paper document but the return on the investment lies in reducing paper document storage for the notary, reducing the cost of verifying the document and increasing the confidence in the document leading to a reduction in the financial risk. |
| **Recommendations** | Documents with high longevity (over 5 years) should carry a visible optical object biometricacting as an unforgeable optical key to access the file stored in either local or remote information storage facilities. This object biometric should ideally be linked to a human biometric when the protected information is linked to one or more individuals involved in the certification process. |

### 3.2.13. Driving licenses

| **e-Driving License** | **Extended EU regulations are expected in November 2010; these regulations refer to new application standards ISO 18013, as well as a harmonized document in format, security and driving class.** |
|---|---|
| **Status** | In CY 2010 e-Driving License are in use in 10 states outside Europe. Many programs run with biometric data stored on the document, such as in Japan, Hong Kong, India, Morocco, and El Salvador. The new extended EU regulations would foster more programs in Europe.<br>Facial images are in use in Japan (tested in Russia), fingerprint data is in use in India and Morocco and both biometric data are used in El Salvador and Hong Kong. |
| **Benefits** | - increasing the security of the document<br>- better tie between holder and license document<br>- increase in road safety |
| **Security** | New EU driving licenses have a minimum of 5 optical security elements, defined by the EU Commission; with an embedded microcontroller electronic securities in HW and SW are captured. |
| **Interoperability** | If the EU-specification defines all key elements, such as data set on card, access to the data set on card, communication protocol between card and reader, interoperability should be possible, similar to the programs running for EU-Tachographs, which run today in 32 states. |
| **Privacy** | Protection of electronic data by access key. Fingerprint images must be protected by an additional access key. Card-to-Card Authentication and PIN verification by authorized persons, such as the police, should be used. |
| **ROI** | Re-financing of production costs by increasing the fee per driving license document. |
| **Recommendations** | a) Government's Recommendation<br>EU regulation 2006/126/EC for all driving license documents in EU from 2012 onwards ID1-format, Polycarbonate, 5 optical security elements, uniform design)<br>b) EUROSMART's Recommendation<br>In some EU states driving licenses are equivalent to ID-cards, because ID-cards are not in use (e.g. UK, Norway, Denmark) or ID cards are voluntary (e.g. in Sweden, Finland, France). With the migration to e-Driving License a contribution to national security would be achievable. |

With regard to privacy and ethics, the eDriver's license is similar to an eID card. So the same tables apply, for either identification or authentication.

### 3.3. Eurosmart general recommendations and position

Community and individual security risks that exist and are growing fast are not well identified and evaluated:

- Terrorism, acts of piracy are increasing,
- Illegal immigration,
- Identity theft,
- Social insurance, welfare benefit Fraud,
- White collar, organized crime,
- Misappropriation of documents, intellectual property,
- ….,

A global response for drastically reducing all of these is to reinforce identification of people and objects. Biometrics is the only means of identification that is linked to the individual or the object itself. Thus it is natural to consider its use.

Generally, the man in the street thinks that biometrics is a threat to his own privacy and an ethical risk for people.

**The first recommendation of Eurosmart is to provide education:**

- On security risks: nature, seriousness of harm to the community and individuals, impact on economy, growth,

- On solutions that can combat the risks, whatever they are, on the evaluation of their efficiency, costs, side effects, their intrinsic security, the misuses they can give rise to.

- On privacy: What it is, perceived and effective privacy, on proportionality: security vs privacy.

- On what is identification, digital economy, digital identity,

- On smart card technology, biometrics,

This is similar to the OECD’s promotion of a security culture.

**Associated with this recommendation, Eurosmart would like an Ethics Committee to** elaborate and validate impartially these education documents. In a globalized world, we can assist in preventing non-use of good solutions because of unverified threats as reagrds privacy and ethics, and also in the uncontrolled use of inappropriate solutions. With regards to that, we recall the paradox of people who are afraid of sending their personal data to reliable organisations when they disclose it all to the planet via social networks on the internet.

**The second recommendation of Eurosmart is to classify use cases we have tried in this document, in order to analyse and compare solutions on the basis of pragmatic criteria.**

These criteria will relate to security, privacy protection, efficiency, convenience, ease of use, benefits, costs and ROI.

**The third recommendation is to roll out solutions that comply with EU regulations, governmental laws, and authorizations issued by ethics committees**. In our opinion, technology does not intrinsically have value, either good or bad. The proposed solution must provide countermeasures to the identified misuses that represent threats.

**Linked to the third recommendation, our fourth one is to recommend the association of both smart card technology and biometrics, and in particular the use of Match On Card.**

**As a fifth recommendation, we note that the security of IT solutions can be evaluated and certified.** The common criteria methodology has been used extensively used for smart card technology and is being adopted for Match On Card. The objective of an evaluation document forming part of the method can define what has to be protected in terms of security and in terms of privacy.

**Better integration of biometrics in smart card standardization is our 6th recommendation.** The European Citizen card (ECC) standard should perform this action. This will enhance interoperability at card level.

**Integration recommendations deal with:**

- The selection of the biometric technique according to the use case,
- The use of multimodal biometrics where necessary,
- The definition of procedures for system operators and system providers.

# 4. Appendix

## *4.1. Sources and references*

- European Biometrics Portal (EBP) Trend report, “Biometrics in Europe”, Unisys, 2006.
- “EMEA Biometrics market” Frost and Sullivan, July 2009.
- [FGB09] Report on a biometric profile specific to cross-border interoperability of biometrics applicable to e-identity, 1.0, Focus Group on Biometrics, CEN, 2009.
- [TR09] Technical Report : a consensus on conformity and interoperability mechanisms; both for applications and sensors, in order to achieve security evaluated interoperable solutions between European Union Member States, v1.01, Focus Group on Biometrics, CEN, 2009.
- [IDMT07] The Global Platform Value Proposition for Identity Management, Global Platform, White Paper September 2007.
- [MOC09] The Global Platform for Biometric Match-on-Card Verification, Global.
- “The GlobalPlatform value proposition for biometrics match on card verification”, GlobalPlatform, white paper 2009.
- “Smart cards and biometrics in privacy-sensitive secure personal identification systems”, Smart Card Alliance, May 2002.
- “Biometrics enhancing security or invading privacy?” Irish Council for Biometrics, 2009.
- Ethical practices in the use of biometrics identifiers within the EU, Anne-Marie Sprokkereef and Paul de Hert.

## *4.2. Glossary*

These definitions are part of the Eurosmart glossary (www.eurosmart.com).

**ABC** **A**utomatic **B**order **C**ontrol.

**ABIS** Automated Biometric Identification System. Such a system compares captured biometric samples to a database of records in order to determine the identity of an individual.

**Accuracy** The accuracy of a biometric procedure or system gives the level of precision reached in the actions.

**AFIS** Automated Fingerprint Identification System. Automated Biometric System that compares a submitted fingerprint record (single or multiple) to a database of records in order to determine the identity of an individual.

**Authentication** A cryptographic process that validates the claimed origin of data or an identity [EMV].In biometric technique the authentication process compares the captured biometric sample with the biometric information’s previously stored on a smart secure device (epassport, smart card,…)

**Biometrics** Measurable, distinct physical characteristics or personal traits that can be used to recognize the identity or verify the claimed identity of an enrolled person.

**BioAPI (Biometrics Application Programming Interface)** Define the programming interface and service provider interface in order to facilitate the integration of biometric devices into the overall system architecture.

**Biometric Data** A general term used to refer to any computer data that is created during a biometric process. More precisely two kinds of biometrics data can be used :
* Collected Biometric Data : raw data get out of the sensors named Biometric Samples
* Compressed or computed Biometric Data : in order to accelerate the automated biometric process or reduce size needed by the records in memory, raw Data are “compiled” or “compressed” by dedicated algorithms that keep accuracy while decreasing drastically size of records.

**Biometrics** A general term to describe either a characteristic or a process :
* A measurable biological and behavioral characteristic that can be used for automated recognition
* In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

**Biometric Sample** Raw data originating from the sensors.

**Biometric template** Representations of a fingerprint or other biometrics using series of numbers and letters.

**BIP** **B**iometric **I**nterworking **P**rotocol.

**BITE** The BITE (‘Biometric Identification Technology Ethics’) project set out to promote research on the bioethical and ethical implications of emerging biometric identification technologies and initiate an international, public debate on the subject. The project brought together nine partners, including bioethicists and representatives of the biometric industries, from five European countries, including four EU Member States.

**Capture** Process of collecting biometric samples from an individual via a sensor.

**CBEFF** A standard that provides the ability for a system to identify and interface with multiple biometrics systems and to exchange data between system components.

**Comparison** Process of comparing a biometric sample with a previously stored reference or references, in order to make an identification, or a verification.

**Digital signature** Digital signatures are used to establish the authenticity of electronic messages and documents. They are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. The legal validity of digital signatures is governed by legislation in many countries and in Europe. Digital signatures are sometimes referred to as ‘electronic signatures’.

**DNA** **D**eoxyribo**n**ucleic **A**cid.

**ECC** **E**uropean **C**itizen **C**ard.

**EER (Equal Error Rate)** Statistic evaluation of the biometric performance of the system where FAR and FFR are equal. In general the lower the EER is, the more accurate the biometric system is.

**Enrolment** The initial process of collecting biometric data from a user and then storing it in a template for later comparison. As far as smartcard are concerned the process of originally acquiring the biometric data of a cardholder and entering it into the corresponding smart card. The data stored in the smart card then form the basis for subsequent biometric user identification.

**e-Services** Or "eServices" is a highly general/generic term usually referring to the provision of services via the Internet (the prefix 'e' standing for "electronic", as it does in many other uses). It is true Web jargon, meaning just about anything done online. e-Services include "e-commerce," although they may also include non-commercial services. Non-ecommerce e-services include (at least some) "eGovernment" services.

**eVRC** **e**lectronic **V**ehicle **R**egistration **C**ard.

**Extraction** In a biometric security system, the process of converting a captured biometric sample into data that can be compared to a reference template and possibly stored.

**Face Recognition** Biometric modality that uses an image of the visible physical structure of an individuals' face for recognition purposes.

**FAR - False Acceptance Rate** A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometrics.

**Fingerprint Recognition** Biometric modality that uses the physical structure of the User fingerprint for recognition. In most of Fingerprint recognition the Biometric Samples are compressed in Minutiae points that reduce the size of data and accelerate the process.

**FTA ( Failure To Acquire or FMR)** Failure of a biometric system to capture and/or extract usable information from a biometric sample.

**FRR - False Rejection Rate** A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false reject, which occurs when an individual is incorrectly matched to his/her own existing biometrics.

**FRR Rate** Statistic evaluation of the FRR of a biometric system.

**FTE - Failure To Enrol** Failure of a biometric system to form a proper enrolment reference for an end user. Common failures include end users who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or the sensor data insufficient quality to develop a template.

**FTE Rate** Statistic evaluation of the FTE of a biometric system.

**Global Platform** A non-profit organization founded in 1999 aiming at Smart Card infrastructure development to support multi-application, multi-actor and multi-business models implementations. At the end of 2008, the Global Platform association had more than 50 members.

**Hacker** A person who attempts to break into computers that he or she is not authorized to use.

**Hand Geometry Recognition** Biometric modality that uses the physical structure of the user's hands for recognition

**HPC (Health Professional Card)**
The Healthcare Professional Card (HPC) is a person specific ID Card, which allows health professionals to access to the Patient Card (PC) data and IT infrastructure available for healthcare and health insurance services.

**IAS ( Identification, Authentication & Signing)**
The three main pillars for a 2-factor user authentication combined with electronic signature useful for all online services such as e-Government, e-Business and e-Procurement services. A smartcard with MoC (Match on Card) capability ideally provides all the necessary ingredients for identification including with biometrics and authentication (PIN verification).

**IAS-ECC**
Technical specification for smart card based on the European Citizen Card (ECC) standard which is a CEN standard

**ICAO**
**I**nternational **C**ivil **A**viation **O**rganization.

**Identification**
* The process, generally employing unique machine-readable names, that enables recognition of users or resources as identical to those previously described to the computer system
* The assignment of a name by which an entity can be referenced. The entity may be high level (such as a user) or low level (such as a process or communication channel
* In a biometric system, a task where the system searches a database for a reference matching a submitted sample, ad if found, returns a corresponding identity.

**Identification card**
Card identifying its holder and issuer which may carry data required as input for the intended use of the card and for transactions based thereon. [ISO 7810]

**Identity**
Two definitions:
* Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.
* Representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE. An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym.

**Integrity**
* The accuracy, completeness and validity of information in accordance with business values and expectations. The property that data or information has not been modified or altered in an unauthorized manner
* A security service that allows verification that an unauthorized modification (including changes, insertions, deletions and duplications) has not occurred either maliciously or accidentally.

**Interoperability**
The ability to exchange requests between entities. Objects interoperate if the methods that apply to one object can request services of another object. Example: ePassports from different vendors must be readable at any border control terminal from various vendors.

**Iris Recognition**
Biometric modality that uses an image of the physical structure of an individual’s iris (the iris muscle which is the colored portion of the eye surrounding the pupil) for recognition purposes. Only the iris structure is used by the recognition process, not the color of the iris.

**ISO (International Organization for Standardization)** ISO was founded in 1947 and is based in Geneva, Switzerland. Its function is to support the generation of international standards in order to promote the free exchange of goods and services. Many ISO standards are used by the Smartcard Industry and Smart technology Industry such as
* ISO 7816 series for contact card products & systems
* ISO 14443 series for contactless smartcard products & systems
* ISO 15693 series for “vicinity” cards
* ISO18092 for the NFC interface and protocol communication modes
* ISO 15408 series for IT security evaluation
* Etc.
Conversely “ISO” is not an acronym, but the Greek word for “equal.”

**JTC** **J**oint **T**echnical **C**ommittee.

**LSP ( Large Scale Pilot)** In the areas of electronic identity and online public procurement, many initiatives have been launched at national level to develop solutions. Bringing these sometimes divergent approaches into line and making them interoperable at European level is the focus of a series of Large-Scale Pilots (LSP) being launched with the support of the European Commission? STORK, PEPPOL, epSOS are such pilots.

**Masquerade** A masquerade is where one entity pretends successfully to be a different entity. A masquerade is usually used with some form of an active attack such as replay and modification of messages or data.

**Match** Decision that the biometric sample and a stored template comes from the same human source. The decision is made on the level of similarity (difference or hamming distance).

**Matching** The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. The system makes decisions based on this score and its relationship (above or below) with a predetermined threshold.

**Match on Card (MOC)** The process of matching a biometric sample against a previously stored template on the same smartcard. MOC is the best known approach to underwrite cardholder’s privacy protection.

**Match On System (MOS)** The process of matching a biometric sample against a previously stored template, performed on a system.

**Match off Card** The process of matching a biometric sample against a previously stored template outside of card or any portable personal object.

**Minutia (e) Point** Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae are compared for recognition purposes. It accelerates the matching and can be done using a smaller memory footprint for storing them.

**MRTD** **M**achine **R**eadable **T**ravel **D**ocuments.

**MRZ (Machine Readable Zone)** Data on the identity page is encoded in optical character recognition (called OCR) format. Many states began to issue Id documents with MRZs in the 1980. The standardization was done by the International Civil Aviation Organization (ICAO), with the document ICAO 9303.

**Multimodal Biometric System** System that uses two or more modality components (biometric characteristic, sensor type, or feature extraction algorithm) occurs in multiple. (For example: fingerprints and iris recognition).

**Non-repudiation** The author of a message cannot deny an operation.

**nPA** **n**euer **P**ersonal**a**usweis (German new eID card).

**Objects Biometrics** A natural phenomenon of elements which characteristic is chaotic and measurable, for example, surface states, bubbles in a material, manufacturing defects, can be used a biometric characteristic of the element.

**OECD** **O**rganisation for **E**conomic **C**o-operation and **D**evelopment.

**One to Many, One to n** In a biometric system describes the comparison of one reference to many enrolled references. One to Many is used for identification or by watch list tasks.

**One to One** In a biometric system describes the comparison of one reference to one enrolled reference to make a decision .One to One is used for authentication particularly by Match on Card.

**Palm Print Recognition** Biometric Modality that uses the physical structure on an invidual's palm print for recognition purposes.

**Performance** When applied to a biometric process or algorithm, this word means a measurement of a single or mixed characteristics, such as accuracy, speed, throughput.

**Phishing** Phishing' refers to emails that trick people into giving out their personal and banking information; they can also be sent by SMS. These messages seem to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers.

**PI** Personal identification.

**PIN (Personal Identification Number)** A security method used to show "what you know". Depending on the system a PIN could be used to either or verify a claimed identity.

**PIV (Personal ID-Verification)** In response to HSPD 12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. The PIV-Card is a secure token for logical and physical access.

**PKI** Public Key Infrastructure A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

**Population** The set of people that can be concerned by a biometric application.

**Replay attack** A replay attack occurs when a message, or a part of a message, is repeated to produce an authorized effect.

**ROI** **R**eturn **O**n **I**nvestment.

**SC** **S**ub-**C**ommittee.

**Security**

This term has different generic definitions:
• Freedom from undesirable events, such as malicious and accidental misuse; how well a system resists penetrations by outsiders and misuse by insiders:
• The protection of system resources from accidental or malicious access, use, modification, destruction, or disclosure.
• The protection of resources from damage and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction.
Security concerns transcend the boundaries of an automated system.

**Security feature**

Technical mean which permits raising the effort of exploiting a threat, or even making it impossible to exploit. It can be implemented at software, hardware or protocol level.

**Sensor**

Hardware of a biometric device that is able to capture a biometric sample, for instance iris, fingerprint, or face.

**SIS**

**S**chengen **I**nformation **S**ystem.

**Skimming**

Card skimming’ is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam. In biometrics and ID it could be the act of obtaining data from an unknowing end user who is not willing to submit the sample at that time. An example could be secretly reading while in close proximity to user on a bus.

**Smart Card (Smartcard)**

Generally used to name a card containing a chip or an Integrated Circuit (strictly a secure microcontroller). A Smart Card is an ICC

**Spoofing**

Commonly used technique to break inside a network. The packets are building so that they seem to come from inside the network whereas they come from the outside. This kind of attack can be blocked by firewalls.

**Tachograph**

Device combining the functions of a clock and a speedometer. Fitted to a motor vehicle, a tachograph records the vehicle's speed whether it is moving or stationary. In order to avoid tampering analogue tachographs are now being replaced by digital tachographs which records data on Smart Security Devices (smartcards or other form factor).The signals from the vehicle’s axle-tree sensor are encrypted which makes tampering much more difficult.

**Tamper**

To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

**Template**

A digital representation of an invidual’s characteristics representing information extracted from a biometric sample and calculated at the enrollment phase. Accuracy of algorithm that generates Templates is the key point of the complete system.

**Terminal**

The device used in conjunction with the ICC at the point of transaction to perform a financial transaction. The terminal incorporates the interface device and may also include other components such as host communications [EMV].

**Threat**

A threat consists of an adverse action performed by a threat agent on an asset [CC]
Examples of threats are:
* a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network or from card;
* a worm seriously degrading the performance of a wide-area network;
* a system administrator violating user privacy;
* someone on the Internet listening in on confidential electronic communication.

**Treshold** Setting for a biometric system. The acceptance or rejection is determined by the fact that the comparison process provides a score that is above or below the treshold.

**Trojan horse** When a software program that performs a legitimate function contains a hidden unauthorized function that exploits the legitimate function, the unauthorized function is called Trojan horse.

**True Rejection Rate** i.e. the percentage of times a system (correctly) rejects false claim identity. The TAR is one of the components which measures the performance of a biometric system when operating in the verification task.

**Trust** A firm belief or confidence in the honesty, integrity, justice, reliability, etc., of a person, company, etc. In the security engineering, a trusted system is a system that is relied upon to a specified extent to enforce a specified security policy. As such, a trusted system is one which failure may break a specified security policy.

**Trusted channel** A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

**Verification** A task where a biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample to one or more previously enrolled templates.

**VIS** **V**isa **I**nformation **S**ystem.

**VISIT (USA) / US-VISIT** The U.S. Department of Homeland Security's US-VISIT program provides visa-issuing posts and ports of entry with the biometric technology that enables the U.S. government to establish and verify your identity when you visit the United States

**Vulnerability** A flaw or weakness in a product and/or system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

**Watch list** Biometric database / list consisting of biometric data that has to be used for an identification purpose. Watch list may be a black of white list.

**Web services** These are software applications running via the internet (as opposed to Client software installed on one particular platform). The main advantage is that they do not require any software installation on the user’s computer. All what is needed is a web browser. Web Services work seamlessly across all platforms and all Operating Systems because they only interact with the web browser. The benefits for the users are numerous

* According to W3C: A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically an XML based format named WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

* When mentioned in the plural ("Web services”, the term often refers to an interface for a service oriented architecture (SOA), in which Web-based applications dynamically interact with other Web applications using open standards that include XML running over HTTP, UDDI and SOAP. Such applications typically run behind the scenes, one program "talking to" another (server to server). Microsoft's .NET and Sun's Java System (J2EE) are the major development platforms that natively support these standards

### *4.3. Standards*

- ISO/IEC JTC[2] 1 SC[3] 37 “Biometrics”, which deals exclusively with biometrics standardization includes several Working Groups

  WG1 Harmonized biometrics vocabulary
  WG2 Biometric Technical interfaces
  WG3 Biometric data interface formats
  WG4 Profiles for biometric applications
  WG5 Biometric testing & reporting
  WG6 Cross jurisdictional and societal aspects

- ISO/IEC JTC 1 SC 27 “IT Security Techniques”, which deals with specific questions on securing biometric data and on general IT security topics,
- ISO/IEC JTC 1 SC 17 “Cards and Individual Identification” deals in Working Group 3 “Machine Readable Travel Documents” with standardization of passports, ID cards, visa, and other travel documents in cooperation with the International Civil Aviation Organization (ICAO),
- ISO/IEC JTC 1 SC 17 also deals in its Working Group 11 “Application of biometrics to cards and individual identification” with topics such as comparison of biometric data on a smartcard;
- ISO TC68/SC 2 “Security management and general banking operations” offers guidelines that have already been applied to large scale heterogeneous banking systems and might also be useful in the context of biometric technology

Standards:

ISO/IEC 19794-1 Biometric data interchange formats
ISO/IEC 19794-2 Finger Minutiae Data
ISO/IEC 19794-3 Finger pattern spectral data
ISO/IEC 19794-4 Finger Image Data
ISO/IEC 19794-5 Facial image Data
ISO/IEC 19794-6 Iris image Data
ISO/IEC 19794-9 Vascular image Data
ISO/IEC 19794-10 Hand geometry silhouette data
ISO/IEC 19785 CBEFF Common Biometric Exchange Framework format
ISO/IEC 19784 BioAPI
ISO/IEC 19795 Biometric testing and reporting
  Part 1: Evaluation of biometric systems in terms of error and throughput rates
  Part 2 Technology and scenario evaluation
  Part 3 Modality specific testing
  Part 4 Interoperability and performance testing

ISO 24708, under development: syntax, semantics and encoding of messages for BIO APIs

[2] Joint Technical Committee
[3] SubCommittee

EUROSMART
The Voice of the Smart Security Industry

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work in dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospective emerging markets).

Eurosmart is acknowledged as representing "The Voice of the Smart Security Industry" and is heavily involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Bruxelles
Tel. (+32) 2 506 88 38 / Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com