

Smart Card in Biometric Authentication

Željka Požgaj, Ph.D.
Faculty of Economics and Business
10000 Zagreb, Trg. J.F. Kennedy-a 6
E-mail: zpozgaj@efzg.hr

Ivor Đurinek, Bs.C.
10090 Zagreb, Dvoriček 1
E-mail: ivor96@gmail.com

Abstract. *Identification and authentication by individuals' biometric characteristics is becoming an accepted procedure that is slowly replacing the most popular identification procedure – passwords. Rapid progress of biometric technology and its expanded application brings new possibilities in identification process. The usage of biometric smart card in the process of identification and authentication is nothing new. What is new is that the process is expected to be used more in our environment. This paper presents basic characteristics of biometric identification, points out the specific qualities of using a smart card in biometric identification, reveals the requirements and open issues regarding the authentication process in general and the implementation of biometric smart card, and discusses possible areas where biometric identification could be put into practice.*

Keywords. Biometric authentication process, biometric smart card.

1. Introduction

Ever more frequent implementation of biometric authentication is closely connected with the development of information and Internet technologies in the United States and western European countries in the past fifteen years. In Croatia, biometric technologies are being more and more used. This is most probably connected with better access to information about implementation of biometric technologies in the rest of the world, foreign investments in Croatia where foreign companies bring not only their money but also their knowledge and experience, and companies' effort to protect the available data and their business processes more effectively. For now, biometric identification methods are mainly used in unimodal identification process, when a person enters protected premises (premises of a company), and is connected with application for work records and other applications closely connected with that. Identification via biometric smart card is

for now not being conducted. A clear indicator that biometric technologies industry is becoming a respectable branch of information technologies industry are the predicted annual revenues for 2007 and 2010 stated in Annual Biometric Industry Revenues published by International Biometric Group [2]. The predicted revenue for 2007 comes to around \$3010.7 million and in 2010 it could go up to around \$5749.2 million. This data show that biometric technologies are becoming an ever more significant part of information technologies. Although the individuals' biometric characteristics have been used in the identification process since the 2nd century BC (China) [9], the basic idea of identification has remained the same. The only thing that has changed is biometric data storage devices and the technology used in identification process.

Conventional smart card invented in 1974 [10] has gone several development phases during the years. Today it is credit-card-sized card equipped with microprocessor, memory and input/output handler. It is a portable, low cost, intelligent device capable of manipulating and storing data. Adding individuals' unique characteristics into smart card chip, smart card becomes more secure medium, suitable for use in a wide range of applications that support biometric methods of identification. There are numerous ID systems implemented worldwide based on biometric smart card and biometric technology. For example: US Department of Defense Common Access Card, Malaysia's national ID multipurpose card, UK's Asylum Seekers Card – contain photo for visual recognition and fingerprint template stored on smartcard chip for biometric identification [6]. The same method of identification is used in Netherlands' "Privium" automated border crossing system and Brunei's national ID system

[6]. Biometric smart card ID system is also implemented in various products that are used in everyday life like keyboards, door locks, safes, USB tokens, POS terminals, ATMs etc [11]. The most usable biometric smart card is MOC (Match-on-card) type. Some of their producers are: ActivCard, beTRUSTed, SAFLINK, Siemens, Philips/IBM, AFIS readers etc. [7].

In this paper authors want to presents the main characteristics of biometric and smart card technology especially biometric smart card ID system technology. As they belief, there are at the least three reasons why biometric smart card ID system will play (or already play) an important role in the process of identification and authentication. The reasons are: (1) world becomes highly networked; (2) the style of living requires mobility; (3) new procedures in business transactions supported by information and Internet technology, some applications and some products require high level of security in identification and authentication processes.

The paper is divided into six chapters. Following the introduction, methods of biometric identification are presented in the second chapter. The main characteristics of biometric smart card are explained in the third chapter. Fourth chapter points out the requirements and open issues about biometric identification process and biometric smart card. The usage of biometric smart card is presented in the fifth chapter. The conclusions follow in the sixth chapter.

2. Biometric methods of identification

2.1. Background

The word *biometrics*, an acronym of Greek origin can be literally translates as “the measure of life”. It means that biometrics is based on biological (anthropological) measurable characteristics. According to Smart Card Alliance glossary, biometrics is “a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual” [12]. Some sources directly link term “biometrics” with term “biometric technology”. In that context, Wayman defines biometric technologies as “automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristics [14].

According to IEEE (Institute of Electrical and Electronics Engineers) biometric technology is used for automatic personal recognition based on biological trait or behavioral characteristics [4]. As all definitions points out, identification and authentication process is based on individuals' unique physiological and behavioral characteristics. Physiological biometrics characteristics are: fingerprint, hand and finger geometry, vessel pattern, iris and retina pattern, face geometry, facial pattern etc., while behavioral characteristics reflect individuals' behavior regarding performing of certain actions. They are: gait, keystroke, signature, voice etc.

In order to use unique physiological and behavioral characteristics of an individual in identification and authentication process, it was necessary to develop certain recognition techniques. We can distinguish between physiological techniques that include fingerprint recognition, retinal and iris recognition, hand/finger geometry, facial feature recognition and facial thermography recognition, DNA analysis, ear lobe recognition, wrist/vein recognition etc., and behavioral techniques like voice recognition, handwriting (signature) recognition, keystroke dynamic, gait (walking pattern) etc.

2.2. The identification/authentication process

The identification process includes enrollment and verification (authentication). Both processes are virtually the same for all biometrics identification methods.

Enrollment process covers the following steps:

- Taking the initial (identifying) sample
- Transforming the sample to template
- Storing the template

Verification process can be repeated in every further attempt of identification. It covers:

- Identification process (taking the new biometric sample)
- Verification of the taken and stored template
- Approval or rejection for further actions.

In taking the first sample, the person is identified through classical method of identification (identity card) in order to confirm their identity.

The biometric characteristic is taken according to selected methods and characteristics of the identification equipment. Basic elements of biometric authentication system are templates. They are created twice: in enrollment and verification phases. Initial template is stored in database, on the local reading device or on a smart card. Next time when someone wants to identify themselves they have to pass the identifying process again. The goal of verification is to confirm authentication. Process of verification is successfully completed if the template of the newly scanned part of person's body corresponds with the stored template. Depending on the result of verification, further activities are either granted or denied.

Initial template produced during the enrollment process can be stored on two ways. The ways are [3]:

- "One-to-many", or
- "One-to-one".

Method "one-to-many" means that initial template is added to already store templates in database or on local device memory. If initial template is stored on smart card (or any other floppy device), "one-to-one" method is used. It means that only one template is stored on smart card and it belongs to the owner of the smart card.

The authentication (verification) process is always based on "one-to-one" matching. It means that template created in the process of identification has to be matched with stored template (in database or on smart card). The procedure of authentication depends about the access to the stored template. There are two types of template search [3]:

- "One-to-many" or open search capable
- "One-to-one" or close search capable.

"One-to-many" search procedure is based on a sequential search of stored templates till the corresponded template is found. Search is successful if digital code of a newly formed template is identical to the stored one, or unsuccessful if there is no template in database identical to the digital code of a newly formed template. This model is suitable for physical access control with reasonable number of templates as search procedure includes matching of a newly formed template with all templates stored in sequential way.

There is also another "one-to-many" search procedure based on the numerical literal that has to be entered at the beginning of identification before the sample is taken. Numerical literal (has a role of primary key), is added to the initial template and stored together with template into database. Therefore, search process is easier, faster and allows direct access to a particular template. The model is suitable for situations where a lot of identifications have to be done in a short period.

"One-to-one" search method is used in situations when template is stored on floppy device like smart card. Procedures of identification and verification are performed one after the other nearly at the same time. If a template formed at the moment of identification is identical to the template stored on smart card, authentication is confirmed.

3. Biometric smart card

Using a card as means of identification is one of the basic forms of identification. During time, type of card identification has changed: from undefined entry like Visitor, through stating name and surname of the carrier with possible addition of photo, marking of the entry, magnetizing the entry to putting the entry on a chip. The first chip card was invented by Helmut Gröttrup and Jürgen Dethloff in 1968; Roland Moreno patented the first concept of memory card in 1974; the patent was finally improved in 1982; first mass use of the chip card was in 1983 [10]. Although the chip card is called smart card, which it really is, since it enables storage of certain contents, the more sophisticated smart cards are actually mini computers with all the necessary components (CPU, RAM, ROM, and EEPROM). According to the definition smart card is "a device that includes an embedded integrated circuit that can be either a secure microcontroller or equipment intelligence with internal memory or a memory chip alone" [12].

In biometric identification process we can distinguish between three types of smart card regarding their typical technical features and the type of authentication they support. The three types of smart card are [13]:

- Template-on-card (TOC)
- Match-on-card (MOC)
- System-on-card (SOC)

In the case of TOC, initial (original) identifying biometric template is stored on a smart card. Other procedures like data acquisition, feature extraction and matching are done at the reader side. During the authentication process, the reading device requests the identifying template from the smart card and matches it on the reader side with newly scanned template.

In MOC version, original template is stored on a smart card. Data acquisition and feature extraction are done at the reader side and the matching is done inside the smart card. During the authentication process reading device constructs the new template for identification and sends it to the smart card for matching. The final matching decision is computed inside the smart card itself.

In SOC version, smart card incorporates original template, the entire biometric sensor, processor and algorithm. All authentication procedures (data acquisition, feature extraction and matching) are done inside the smart card itself.

4. Requirements and open issues

Requirements and open issues regarding biometric identification process, especially if it involves smart card refer to:

- Standardization
- Mobility
- Privacy – availability of a sample
- Procedure security

Standardization

The issue of standardisation is generally present in biometric identification process. In biometric identification via smart card the need for standardisation primarily refers to the smart card itself, the procedure of identification, and configuration of the card reading device. Some of the standards referring to the area of biometric smart card implementation include [5],[12]: ISO/IEC 7810 (a series of international standards describing the characteristics of identification cards, including physical characteristics, sizes, thickness, dimension, construction, materials and other requirements); ISO/IEC 7816 (the international standard for integrated circuit cards with contact, as well as command set for all smart cards); ISO/IEC 14443 (international

standard for contactless smart chips and cards that operate at a distance less than 10 centimeters); ISO/IEC 15693 (international standard for contactless smart chips and cards that operate at a great distance then ISO/IEC 7816).

Mobility

The only limit in finding new areas for implementing biometric identification is storage of biometric samples into samples database. In order to avoid that, the possibility of moving biometric samples to portable devices has been introduced. One of the solutions to storing biometric samples onto portable devices is using a smart card. If an identification sample is stored on a card, there is no need to connect the identification site to the biometric samples database in order to check the authenticity of the user. In that way, cardholders control their identification sample which enables them maximum mobility in using biometric identification and autonomy in choosing authentication site.

Privacy – availability of a sample

Availability of a sample represents the basic issue of privacy. Issues arising here refer to the possibility of reconstructing the original sample, unauthorized use of stored samples and other, as well as the possibilities of protection against such activities. The possibility of reconstructing the original sample from the identification sample is the basic issue of privacy and individual's identity preservation. The issue of protecting the privacy of biometric sample is solved via the process of creating identification sample. Namely, with the help of appropriate algorithm, in the process of creating identification sample only certain key features of the original sample are extracted. The selected key features are enough to reconstruct the identification sample, but insufficient to reconstruct the original sample.

The issue of unauthorized access to biometric samples database is solved via rigorous authentication procedures. As there is no perfectly safe biometric system, the goal of each biometric system is to develop security measures which are considered to be optimal at a given moment and in current conditions. In that sense the moving of biometric samples from biometric

database to smart card can be seen as a way of protection from unauthorized use. In the case of biometric sample being stored on a smart card, the card and the privacy of the biometric sample are the responsibility of a cardholder. They decide who they will give the card to and in that way enable access to the identification sample.

One of the ways to protect the privacy is the possibility of cryptographic protection of card contents. There is a wide choice of cryptographic algorithms embedded into cryptographic tools used for encoding digital entry of the identification sample at the moment of creation and storing it into selected storage device. Most biometric smart cards support PKI (Public Key Infrastructure) as a form of protecting biometric contents.

Procedure security

From the aspect of security there are two key moments in the authentication process: feature extraction and matching. By analyzing authentication process characteristics [5], [8] for three types of smart cards (TOC, MOC and SOC) it can easily be seen that SOC offers the highest level of security. In the case of SOC, all processes needed for authentication are done inside the smart card and there is no need for biometric data to be transferred out of the smart card.

TOC offers the least security level. As it was already stated, the card holds only the sample, while the other authentication processes are conducted at the reader side. During the process of authentication, reader requires smart card to release the stored identifying template and send it to the reader. In that way the identification sample travels through the network and no matter how high the security measures are, there is always the risk of an impostor invading the network and replacing the original sample. In the case of possible switch of samples a new, replaced sample can be used in authentication process which completely mars the integrity of the comparison process.

Taking into consideration the security level it provides in authentication process, MOC system is somewhere between SOC and TOC systems. The most important fact regarding security with MOC system is that the identification sample stays on the card and a newly taken sample is

transferred through the network. In this case, the impostor's intervention makes no sense at all.

5. Using smart card in identification system

According to the findings of the author, at this moment identification system based on biometric smart card has no wide use in Croatia although the identification systems based on TOC and MOC smart cards are available on the market. The good thing is that a lot of Croatian companies have already introduced biometric identification when entering their premises so products like portable computers and USB with fingerprint identification can already be found on the market. This makes users become aware of the existence of biometric equipment, which is good considering that biometric smart card will become widely accepted means of identification in the near future.

SOC ID systems as the safest form of biometric identification have yet no wider commercial use even in the countries where identification via biometric smart card is already present for a longer period of time. This situation is mainly supported by high costs of mass production of additional equipment for the smart card (sensor and powerful microprocessor).

Throughout the world, MOC ID systems are most frequently used when it comes to biometric smart card identification. Their technical features and form of authentication process provide relatively high security level. The authentication process is mainly based on recognizing fingerprints. According to the International Biometric Group data [2], fingerprinting is also the most common identification method. The share of revenue for biometric technology based on fingerprinting compared with other biometric systems came to 43.6 % in 2006.

Very interesting example of biometric smart card is BAI Authenticator Smart Card [1]. It is a type of MOC ID system that has a built-in sensor for taking fingerprints next to the chip (Fig. 1). BAI Authenticator Smart Card presents a complete fingerprint identification system that can be inserted into most smart card readers requiring user authentication (Fig.2). It performs all sensor, processor and decision-making functions within the smart card. Card's sensor is completely self-contained in a self-authentication subsystem.

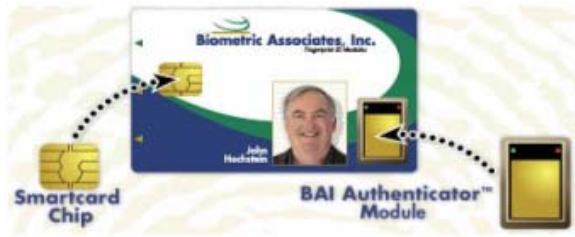


Figure 1. BAI Authenticator Smart Card [1]



Figure 2. Process of authentication [1]

It detects and creates three-dimension electrical image on the fingerprint's unique sample. These signals are verified and then programmed into protected memory on the module. When the enrollment process is finished, the module is locked and subsequent placement of any finger on the sensor triggers the verification process. Matching process is under a special programmed algorithm.

Some relevant BAI Authenticator v1.6 Biometric Subsystem Specifications are presented as follow [1]:

- Overall Dimension: 23.0 x 16.0 x 1.5 mm
- Protective Coasting: Exceeds ISO 7816 requirements
- Active Sensing Area: 14.00 x 10.64
- Recognition Speed: Approximately 0.8 sec.
- False Accepted Rate: < 0.001%
- False Rejection Rate: < 0.008%
- Interoperable With Major 7816 Smart Chips.

Biometric smart cards are being ever more used in identification process, and the identification system itself is being built-in into more and more products. Biometric smart card can be used for e-commerce transactions, facility entry, network access, laptop PC protection, identity cards, electronic payment authorization, portable medical records and next generation credit cards.

6. Conclusions

Identification systems based on recognizing individuals' biometric characteristics are

becoming widely accepted and are slowly replacing traditional identification methods of which identification via password is still most widely spread. Using biometric identification systems in products like mobile phones, USBs, computer keyboards, but also ATMs, cars (door, i.e. ignition mechanisms), entrance doors, check points at airports and other, doesn't represent a novelty in the world today. It is all done to enhance security levels, i.e. to better protect people and assets.

In the future biometric identification forms will develop in two directions: the first refers to further standardization of equipment and identification procedures, and the need for storing biometric identification samples onto portable devices such as smart card or USB. Standardization and mobility are prerequisites for further development of biometric identification methods and their implementation into all aspects of human life.

The other direction refers to further development of multimodal biometric systems (identification via more biometric characteristics at once, i.e. combination of biometric and logical identification forms) because of the expressed need for protection and raising of security and privacy levels in performing business activities as well as in personal life.

The aim of this paper was to point out the basic characteristics and possibilities of using smart card in biometric identification system in a way that it becomes a carrier of biometric sample and procedures needed for identification and authentication processes.

7. References

1. BAI Authenticator SmartCard (2007): <http://biometricassociates.com>
2. Biometric statistic in focus (2006): <http://www.sciencedirect.com>
3. Biometric Technical Assessment (2001): <http://biometric-consulting.com>
4. IEEE: Biometrics (2007): <http://www.ieee.org/portal/site/emergingtech/index.jsp?techId=623>
5. Jutant, A. (2007): The Magic Touch, <http://stevenspublishing.com>
6. Hi-Tech Security Solutions: The Industry Journal for Security & Business Professionals (2007): <http://www.securitysa.com>

7. MOC providers (2007):
<http://www.biometrics.org>
8. Pohlman, N. (2002): Forget About PINs,
<http://itsecurity.com/papers/utimaco1.thl>
9. Požgaj, Ž.(2002): Biometrics and New Technology, Proceedings of International Conference “An Enterprise Odyssey: Economics and Business in the New Millennium”, Zagreb, 2002, 75-98.
10. Rankl, W. Effing, W. (1999): Smart card – Hand Book, Wiley & Sons, New York.
11. Smart card Alliance: Smart card Reader Catalog (2007): <http://www.smartcardalliance.org/catalog>
12. Smart Card Alliance Identity Council (2007): Identity and Smart Card Technology and Application Glossary,
<http://www.smartcardalliance.org>
13. Yun, Y.W., Pang, Ch. T.(2005): An Introduction to Biometric Match-On-Card,
<http://www.itsc.org.sg>
14. Wayman, J. Jain, A., Maio, D. (2005): Biometric Systems, Springer, London.