AARMS Vol. 14, No. 2 (2015) 187–200. **10.32565/aarms.2015.2.5**

Selection of Authentication Systems for Hungarian Health Care, Based on Physiological Study

Part I.

The Biometric Systems

BARÁTH Artur[1]

The actuality of the topic indicated in the title comes from more and more events where the verification of identity might be required. Health-care is an important part of the critical national infrastructures. A primary task of the protection of critical information infrastructures consists in the access control of data managed by IT system where the identity-authentication forms an important part. For this reason, the technologies considered suitable for use and their supporting means are listed.

After examining and comparing the relevant parameters, the optimum solution for the authentication procedures in the Hungarian health care system is specified.

First of all, the modern and efficient biometric identification processes are examined; however, the possession-based Radio Frequency Identification (RFID), as an additional system, is also studied. Due to the well-known problems of passwords and chip cards, they were deliberately omitted during the system planning and efforts were made to exclude the human factors from the planned authentication system as much as possible.

Keywords*: authentication, biometry, RFID, health care, human factors*

Introduction

This study makes an effort to find a solution for identification and access management problems of the health care institutions in Hungary. As is generally known, the above indicated field faces serious problems in data security and access authorization issues that need to be remedied as soon as possible. For this, a technology that offers a proper level of protection and the introduction and operation of which fail to carry glaringly high costs is required; a further important aspects is that the authentication problems caused by people are excluded as far as possible.

The work is aimed at selecting the system from among those available that are best suited for the purpose and condition defined above. To achieve this, the procedures worth considering are listed, their properties and operation are described; finally, based on their examination and a summation of the results, the most suitable one is selected.

1 e-mail: magicman@mailbox.hu

The Importance of Data Protection and Interpretation of Related Concepts

In the 21st century, great value is attached to the protection of personal data. It cannot be accepted that our personal data is stolen by unauthorized persons. The professionals engaged in the protection of personal data should not turn a blind eye to the explosion-like growth in the number of biometric devices. The development and increasing use of such technologies relying on authentication identification needs special attention. The significant novelty in this identification system is that they can be compared not only by people but also by IT devices developed for this purpose. This service requires the cooperation of the identified person, without any other persons, as this process takes place automatically. The specific characteristics of the given person are programmed into the device that will be able to recognize and identify the person in the future, based on a chip or portrait.

In my opinion, the protection of our prized possessions is indispensable today, whether it be our data stored in the computer or physical devices. There are a lot of possibilities to protect and delimit them from certain persons. Within these, we can talk about different levels of protection. There are safe or less safe solutions; the technology to be used is determined by the importance of the data or object to be protected. First, I want to deal with the means serving the protection of physical assets, although these methods are also used to protect other data todays. This will be described later.

It is necessary to clarify certain indispensable definitions before listing possibilities.

Authentication

Authentication is a security service. It is aimed at identifying the origin of a message or request in a reliable way. The classic method is how people identify themselves to the computer (and how computers also identify each other), it consists of entering passwords. Essentially, the authentication serves the verification of individual authority and identification of the user. In other words, it determines which users (e.g. employees) have access to what information and how far their competence extends. [1] The ratios of "Security level/cost" are grouped into categories as follows:

- Low-end (low-end, low-cost): it is aimed at creating an appropriate security level by using solutions as cheap and as economical as possible.
- High-end (top of the line): it is used in systems that require a high level of security. The disadvantage is that it is considered to be an expensive solution.

Biometrics

Biometrics consists of the identification of people based on one or more essential physical or behavioral pattern. Biometrics is used as a method of identity management and access control, primarily in the field of IT. [1] Biometrics can be categorized into two main groups:

- Physiological-biometrics: perhaps, it is this that is considered to be the most popular biometric means. They are connected with the form of individual parts of the human body in all cases. These include: examination of face (geometry, skin design, heat

map, smile, dynamic characteristics), lip (figure, imprint, movement), anthropometry (physical dimensions such as height, head length, shoulder width, etc.), bioelectric field, skin spectroscopy,[2] DNA/DNS, teeth (bite, teeth X-ray photo), ear (geometry, geometry of auricular canal, echo), iris, retina, hand geometry (hands, fingers), nail (nail bed), heart rate, odor/aroma, soles, toes (ridge, phalanges, wrinkle, wrinkle joints, topography), vascular (on fingers, hands, palms, wrists).

- Behavioral biometrics: a less popular biometric method. Its essence is to examine the movements performed by the human body and behavior forms expressed by the individual, e.g. use of keyboard, sound (speech, laughter), gait, handwriting (dynamic signature, signature sound) and dynamics of using the mouse.

The identification systems are used to establish authority. This may be done by entering a given computer system, or accessing some critical data. The entry or access is always managed by some system that may be human resource-based or electronic, or a still more IT based one. In the following, the IT line will be followed. Obviously, there are several possible solutions to achieve our goals; these shall be arranged on the basis of several criteria in order to arrive at a correct conclusion at the end of the studies. In almost all cases, personal identification is used for releasing the protection. To do this, three methods are used apart from the vanishingly small exceptions: [2]

- knowledge-based;
- held-based object;
- biometric-feature based.

The safety in this order increases from top to bottom. As is known, there is no perfect security, but the use of these facilities enables obtaining a level of safety that is acceptable in respect to both economy and safety. The above three methods are described in detail as follows:

Knowledge-based

Some sort of user name, password, PIN combination are used to identify ourselves. A better known and more frequent solution is the use of a password that, in any case, shall include at least three ones of those listed below:

- small letters and capitals;
- number;
- special characters.

In addition, the length of the password is also an important factor, as the more characters, the more time and work are required for decoding. The minimum length generally accepted in professional circles amounts to 16 characters.

In the PIN (not the same PIN code, that is used by credit cards) identification, the secret is usually a four, six or eight-digit decimal number, possibly a five-character alphanumeric sequence. The four-character PIN represents 102, the six-character 106, and the eight-character 108 variants. The alphanumeric string is usually based on the 26 letters of the English alphabet and ten numbers, represents a five-character password with (26+10)5, that is 60,466,176 variations. From among the three identification methods, it is the last one, in that it is the feeblest.

2 Solution method of imaging technology.

Held object-based

In this case, an object can be kept to identify ourselves. In most cases, this is a chip card, less often an RFID chip; however, a more and more popular method is to insert an implant under the skin, and it may also be a device of a RFID system. [3]

A chip card is a card kept by us and presented to the reader when we want to identify ourselves. The reader identifies the card by using radio frequency technology. A 112-bit key is used nowadays with 3-DES encryption. This is included in the chip card. The system compares it to the keys stored in the SQL database; thus, the identification takes place. A weak point of such systems is the link between the reader and the database as it is susceptible to be successfully attacked by certain viruses (SQL injection).[3]

- There are many types of chip-cards and systems using this method:
- operating frequency (125 kHz, 13.56 MHz, 430 MHz, 862–956 MHz (UHF), 2.45 GHz, etc.;
- reading range (<0.05 m, 0.05–0.5 m, 0.5–2 m, >2 m);
- power supply mode (passive, active and partially passive);
- operations allowed (factory programmed, writable once, rewritable, writable/readable).

Security of chips:

- Open: simple fixed code fix, readable and interpretable (or unstructured) data content.
- Encoded: readable, cannot be interpreted, but can be copied.
- Data access protected (password protected): access using password; unable being copied in itself.
- Encrypted: it is the most secure at present.

An improvement of identification by using chip-card is to insert an implant consisting of a chip in the human body. It is the Very-Chip in the United States of America that is the only one allowed to be used as a human RFID implant. The method of identification is the same as in the case of having a card with ourselves. This includes a 16-character length code for the purpose of identification. [3]

3 http://en.wikipedia.org/wiki/SQL_injection (downloaded: 14 03 2015)

Biometric Systems – General

In respect to security, the biometric identifiers also have some kind of order shown in Figure 1.

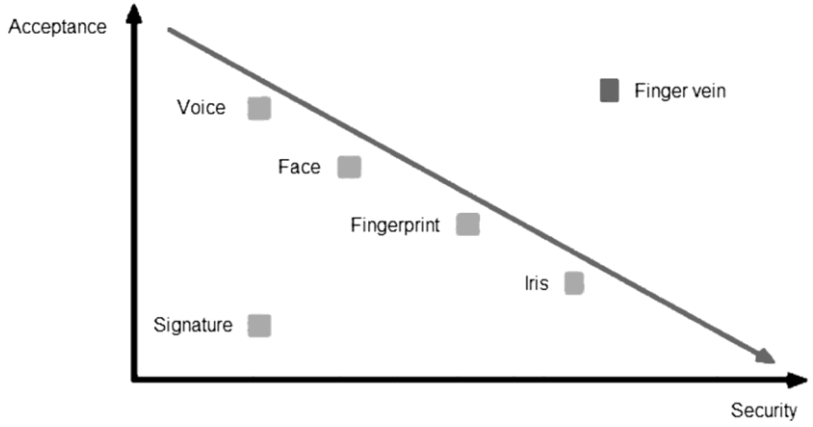

Figure 1. Security of finger vein. (Made by the author.)

The most prominent ones of these are the fingerprint and iris identification. Consequently, it is these that shall be better examined in the following. First, two questions are answered that come up in nearly all cases when using biometric methods and provide proof that the world is indeed going in this direction.

The replies to the two questions below further strengthen the legitimacy of biometric identification: Is it true whether biometric identification will become the basis of identity verification in the future?

Yes, because the traditional identification methods – such as passwords or various identity cards – are based on "what you know" or "what you have". On the other hand, the biometric identification methods are based on "what you are"; on anatomical features (face, fingerprint or iris recognition), or behavioral patterns (signatures or gate). These procedures are much safer than traditional methods. In contrast to the passwords and identification documents or cards, the biometric methods are much more difficult to be deceived by guessing, distribution, lending, copying or counterfeiting.

Why will the biometric methods spread soon in the very near future?

Still, as both the demand and supply are given. On the demand side there is a growing demand for safety and a growing fear of counterfeiting. The states want to know who crosses their borders, to which they pay social benefits. The companies want to control who enters their premises, who are allowed to access their webpages and databases. And what is of key importance: the social acceptance of technology is also growing slowly; more and more use biometric methods in order to ensure identity and to prevent theft, to protect their laptops or phones or in case of payment. On the supply side, small-size, low-cost and fast sensors were able to be developed as a result of the sudden technologic development in the recent past that can be fully automated and are suitable to be used for "real time" imaging. In the following, the functions of the individual procedures are described.

These identification systems can be defined as the totality of processes and devices that uses the physical properties of persons that can be measured by using some kind of technique with the view of determining personal identity or identification. During identification, a comparison of the body of the individual takes place. In this case, two different answers are expected of the system: yes or no. During personal identification, the system recognizes the person by distinguishing its data from stored ones of others. In the first case, two data are compared, while in the latter, one item of data is compared with other stored data.

The more and more and widening use of biometric systems is justified by the special features of biometric data. Data of people can be considered to be universal in the sense that everybody is in possession of such data. The best solution for identification or distinction is represented by DNA-samples, fingerprints and retinal images; however, the geometry of face, the hand and the voice can also be used for this purpose. Everybody has physical characteristics of this kind. These data are individual and different, so the conclusion that there are no two ones alike can be drawn. In time, these data suffer no change. Of course it is not true for all biometric data. Taking these identification systems in a broader sense, it is not only the physical properties of individuals that can be taken into account, but the behavior as well. Factors describing the behavior include e.g. the signature and movement of persons. Part of biometric identification systems combine the use of certain data types e.g. fingerprint and voice identification, while others use methods that take the knowledge of individuals into account e.g. whether they know their password or PIN code associated with their bank card etc. [4]

Basic requirements of these systems are:

- they shall be able to be interpreted and used by everybody;
- uniqueness (no two persons meet the same conditions);
- time stability (static characteristics for long time);
- measurability (preferably high-performance, fast);
- difficulty being deceived.

Figure 2 shows the general block diagram of an average biometric test. In respect of function, the steps indicated are the minimum required ones that have to take place.

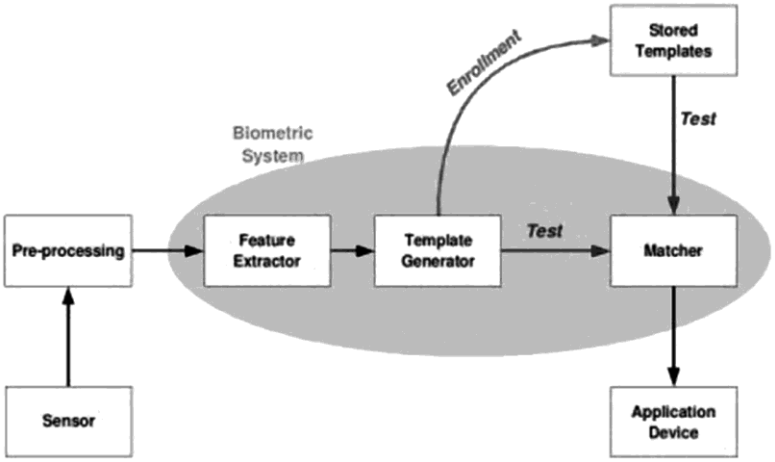

Figure 2. Biometric test's block diagram. [6]

In the block diagram, the operation of biometric identification can be followed. The sensor data are subject to pre-processing (e.g. noise filtering) and the unwanted data are filtered out of the data set (feature extraction). Based on the remaining data, a sample is made up that can be compared with the samples stored in the database; then, the results are forwarded for further processing (alarm, notification etc.). Figure 3 shows the elements that form a biometric identification system.

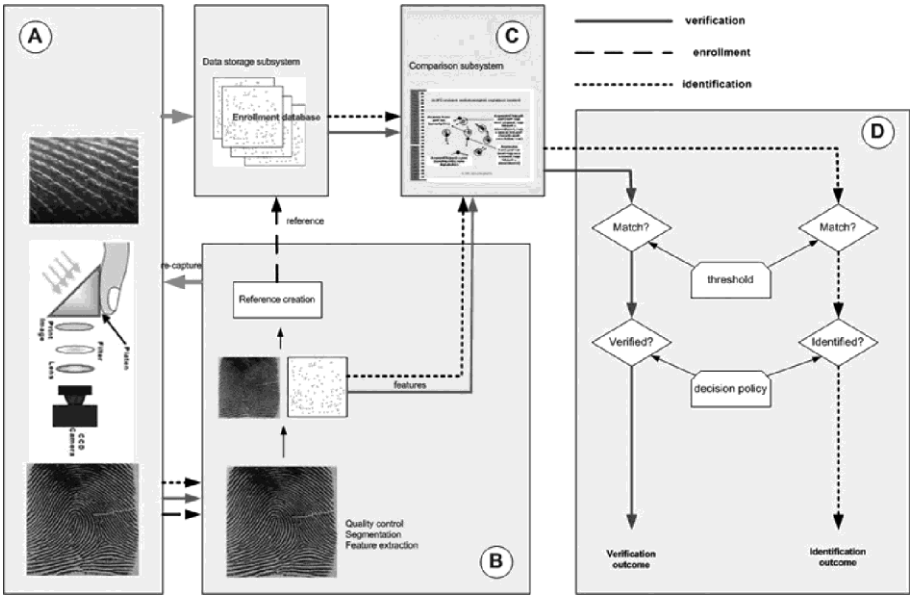

Figure 3. Elements and process of biometric identification.[4]

In general, a biometric identification system consists of four main parts. First, a sensor is required to record the biometric pattern – be it fingerprints, iris texture, handwriting, voice pattern, or whatever. Then, the specific features of the sample that facilitate the identification shall be selected; a database that includes examples characteristic to the individual biometric features is required. Finally, a device for comparison that compares the individual samples with those stored in the database is required. [5]

In terms of reliability, several studies have been done in the past that draw conclusions as follows.

The identification accuracy is determined by two indicators:

- False Accept Rate (FAR) – this index shows the frequency of admitting NON-authorized users to enter the system.
- False Reject Rate (FRR) – this index shows the frequency of rejecting authorized users to enter the system.

4 Source: unknown.

Table 1. Reliability comparison. (Made by the author.)

Face recognition	2,000:1
Voice identification	500:1
Fingertips identification	1,000,000:1
Iris scan	10,000,000:1
Retina scan	10,000,000:1

Table 1 shows a comparison of several FAR indices (how many false identification fails to a right one).

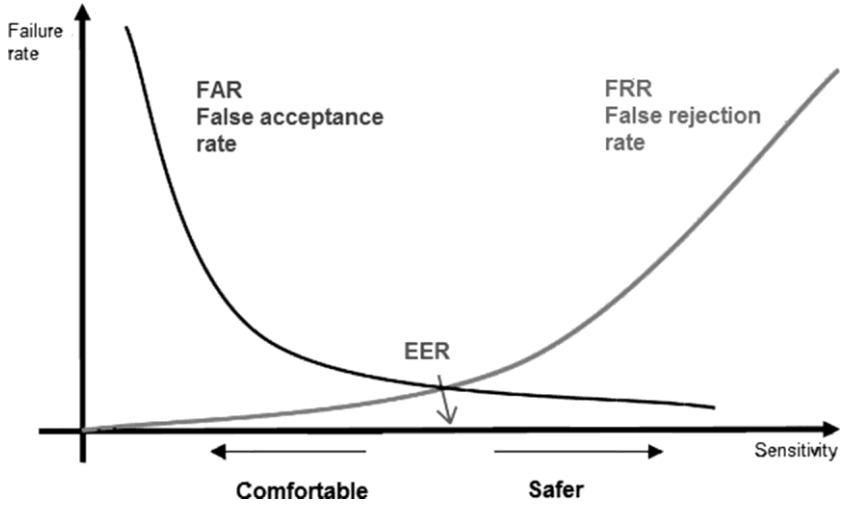

Figure 4. Equal Error Rate (EER) point declaration. (Made by the author.)

The FAR and FRR together represent two curves intersecting at a point. Figure 4 shows: this point is called EER. Table 2 shows a comparison of the relative accuracy of individual tests i.e. the EER values calculated with the FAR and FRR values.

Table 2. EER points list. (Made by the author.)

Face recognition	200:1
Voice identification	50:1
Fingertips identification	500:1
Iris scan	131,000:1
Retina scan	10,000,000+:1

The FRR value of modern fingerprint identification systems lies around 0.01 per cent (one error falls to ten thousand events); while their FAR value around 0.1 per cent (one error falls to a thousand events). Of course, the actual performance of a biometric system depends on several factors. In addition to the biometric characteristics, much depends on the sensitivity of the sensor, size of the database and a variety of other factors (temperature, humidity, indoor or outdoor use, and so on). Various aspects have importance in case of different uses. [4]

Identification of Fingerprints

The safe use of fingerprints in data protection is based on individuality and permanence. There are no two people, not even twins, with the same fingerprints. First, consider the two kinds of imprints classification structured by Henry (1900) and Galton (1892).

In the Henry structure, it is the numbers of ranges, while in the Galton structure the characteristic signs that are competent. Although the uniqueness or quality of fingerprints do not serve as a basis of Henry structure unlike ranges and unique properties. Therefore, to establish whether two fingertips are identical or not, an appropriate number of (privileged) points and/or properties should be located in the same place:

- Beginning and ending ridge;
- Bifurcation;
- Island;
- Enclosure.

This list has been expanded and refined over time. According to the proposal made by the American National Standards Institute it became as follows:

- Ending;
- Bifurcation;
- Mixing;
- Undefined.

The most common system today is the Minutiae-Coordinate model (used by the FBI). This system uses two properties i.e. ending and bifurcation for the identification. It interprets the points of properties as a coordinate each and uses them as a basis for displaying and verifying the identification.

The subsequent Sparrous model uses a structural representing mode for drawing the fingerprints, which made it possible to recognize the print even if it is distorted.

A complete fingerprint contains about 100 ridge bifurcations and endings i.e. so called minutiae points. The fingerprint identifiers compare 30 to 60 minutiae of the given pattern. The resulting image can also be used for identification either directly (global analysis) or by creating a fingerprint code based on the distance of minutiae points from each other or the angle formed by the connecting straight lines. The patterns formed may be a size between 100 and 1500 bytes, depending on the algorithm and the number of identified points; of course, they are also closely related to system reliability.

The Possible Methods of Touch Based Biometric Identification

Handprint identification: it is not as general a use in biometric identification; instead, it occurs primarily at the scenes of offences. In case of identification, the wrinkled location of main lines, the ridges and tissue samples on the palm are analyzed. Following a precise analysis, the information similar to the fingerprint sample is obtained.

The essence of hand geometry identification is that, while analyzing the samples taken of the form and surface of the hand, the length and width of fingers, the width of the hand as well as the scale of the palm and fingers are taken into account. Four positioning pins are used to place the palm in the same position for scanning. There are devices without positioning pins that examine particular specific values under microscope; systems of this kind are used e.g. in work time recording systems. Their advantage is the possibility of integrating with other systems.

Palm and finger identification is a relatively new method. Functionally the finger or palm is illuminated by infrared light that is reflected by the different tissues in different intensity due to differences in absorption. The light is absorbed by blood flowing in the veins much better that results in the exact mapping of veins. The advantage is that the operation is not affected by surface lesions of the skin and is nearly impossible to be deceived.

Fingerprint identification: the finger is placed on the scanner that, by measuring the surface temperature and moisture, verifies whether the finger is live. Then, the identification takes place.

From among the four possibilities described above, the fingerprint test system is selected. It is for reasons that the identification is intended to be used not only for access authorization but also for log-in control into computer systems. In such cases, the palm scanner raises very serious scruples in respect to practical applications. Fingerprint scanning is more appropriate even in respect to economy; in fact, purchase of physical devices represents lower costs. Last but not least, the selected procedure is more advantageous even in respect of hygiene.

According to the decision, the fingerprint test system is considered in more detail. A number of technologic solutions exist in fingerprint scanning systems. Certain identifiers are capable of examining whether the fingers belong to the hand of a living person; this is done by analyzing the temperature and humidity of fingers. The similarity between the devices consists in that the uniqueness of ridges on fingers is analyzed, stored, and finally, compared to specify that the ridges on the fingers are of the individual named and stored, and then it eventually finds the comparison identified. There are two versions of the technique, optical and non-optical methods.

Optical Devices

The fingerprint is mapped onto the surface of an image processor. The image processor is a Complementary Metal-Oxide Semiconductor (CMOS) or Charge-Coupled Device (CCD) element. LEDs are used to illuminate the ridges. Currently used types are as follows:

- Total reflection type: in this case the fingers are placed on the surface of a prism, and the picture obtained during lighting is mapped onto the surface of an image processing device.

- Diffraction type: similar to total reflection-procedure, except that the prism is replaced by a Fresnel lens.
- Chip sensor: a finger is placed onto the surface of the sensor and the signal obtained is transferred via fiber optic cable to the image processing device.
- Thermal analysis: in this case, the device shall not be touched, instead, the finger pulled away in front of it. This device reads the information broken up into slices to form the image. The built-in sensor detects the temperature difference between ridges. So far, few manufacturers have made an attempt in this field; yet, the part played by this device in the market is expected to rise and its current high price is expected to be reduced. It can also be used under extreme circumstances.

Non-Optical Devices

- Radio frequency signal is sent to the finger that reflects it to the receiving sensor. This procedure is also capable of forming a depth image of the fingers and the ridges.
- Principle of capacitive sensor: the finger is placed onto the surface of a sensor mounted with small capacitors. The sensor detects the capacity differences between grooves and ridges. This signal is converted into an electric signal for evaluation. The sensor consists of a conducting layer of lattice structure that generates an electromagnetic field over itself. Touching it with a finger means some of the charge is removed from the position in which it is capable of being sensed by the device.
- The sensor emits ultrasonic signals to the finger. The reflected wave signals are used to generate a depth image.
- Pressure sensor: a piezo-electric matrix is built-in below the sensor surface that detects the unevenness of the finger surface to generate an image.
- The E-field technology measures the electric field of the skin. It is suitable for everyday use and insensible to the quality of the fingerprint. This electronic reading creates an electric field between the finger and the semiconductor in contact, which takes up the grooving of the fingerprint. The resulting image is of high purity, three-dimensional, but small size.

The research and development projects affect all the elements of biometric identification systems, thus better and better, more reliable and faster sensors and algorithms are being made. One direction of development is to combine data from different, independent biometric sources, thereby reducing the error rate. The US-VISIT strategy with dual fingerprint verification is one of the possible forms of "multi-biometric" systems.

In light of the knowledge of the above let me state that the fingerprint can and should be introduced for the purpose of identification in the Hungarian health care system; still, a simpler system representing lower costs shall also be selected for areas where the high level of identification ensured by the fingerprint is not required.

In the future, the information supplied by fingerprints will be able to be completed with information supplied by face recognizing software. With this in view, the retina, iris, facial recognition systems are described in the following.

Possible Methods of Biometric Identification

The iris-recognition is made possible by the individual and time invariant pattern of the human iris. The video camera takes a picture of the eye, then following that, the pupil of the eye, eyelid and eyelashes are cut from the picture; the field of the iris is removed. The information included in the unique iris pattern is recorded in digital form. The identification requires the sequence of bits to be compared.

Iris identification is based on the iris of the eye. In this device, the possibility of errors is almost zero. The iris of the eye includes 400 different identification points. The iris never suffers any changes during life. The chance that two people have exactly the same irises is excluded. During identification, the relevant device examines the visible and invisible elements of the iris. The radial pattern of the iris with circles, ditches and crown belongs to the elements visible to the naked eye. The retina-membrane veins become visible when reading in infrared light. During identification, the pupillary reflexes can also be observed, thus the abuses of contact lenses can be excluded. The scanner of iris identification system converts the image of the iris together with all its characteristics (dimples, circles, ditches, crown, and fabric fibers) that make the eye unique into a three-dimensional contour map. After digitizing, the information thus obtained it forms a code of exactly 2,048-digits. This will be compared later on with those stored in the database. Two methods can be used during the examination. Based on taking photographs, two types of reading can be distinguished i.e. active and passive. The active reading requires the active involvement of the user as he/she shall keep his/her eye at a distance of 0.15 to 0.35 m from the camera. In contrast, the passive procedure is more pleasant in respect to the users; in this case the system first determines the position of the eyes by means of a wide-angle camera and focuses another camera on them to perform the reading at a distance of as much as 0.3 to –1 m. In both cases, the reading takes about 1 to 2 seconds, same as the time required for fingerprint identification. Unfortunately, the active devices can raise hygiene problems; while the disadvantage of passive devices is that they require highly sophisticated technical implementation, so that their price is very high.

Retina identification: the retina at the back of the eye is illuminated with infrared light. Its function is similar to the identification systems of finger and palm. The reflected infrared beams are absorbed to a different extent, so they are able to draw the fundus vasculature. Direct contact with the reader shall be established; therefore, there is a high risk of infection. This technology is very rarely used; usually in case of systems requiring high security.

Face recognition in visible light: Face recognition – associated with sample identification procedures – can serve as a good means of identification. Currently, it is used in special cases. It is unable to be used for distinction of perfectly identical twins.

Face thermogram: A photo made by an infrared camera that shows the thermal pattern of the face. The image is unique and combined with a pattern identification algorithm of high complexity – that verifies the relative temperature differences on the face – it offers a technique that is independent of age and health, but the temperature of the body as well. By means of taking nineteen thousand "data points", the method offers an exceptionally safe procedure provided that the costs of process are reduced to an acceptable level. It is of high accuracy and capable of distinguishing seemingly perfectly identical twins even in the dark. Another advantage is its complete discretion. The development of this technology is direct-

ed today to reduce the costs in order to become widely applicable in the identification and authentication procedures. The facial thermogram is the most promising method at present.

Similarly to the other biometric procedures, the processing begins with noise filtering. Noise and disturbing factors include: eyelashes, eyelids, pupils, reflections. Then, the recognition of structure and the generation of code take place. This data set consists of a sequence of properties described in a polar coordinate system taken concentrically with outward motion starting from the pupil of the eye. As a camera that is capable of taking as many as ten pictures in a second at nearly the same focus, it is used to take pictures, it is possible to select the "best" picture with the lowest noise level (eyelashes, eyelids, reflections).

Iris identification has caught up to fingerprint identification in a short time, and became clearly a complement to finger at present. This is because multimodal identification offers higher security (lower false rejection, greater selectivity) on the one hand, and if the fingerprint testing is the primary one, it provides an alternative identification method, on the other hand.

Neither glasses nor contact lenses interfere with the black and white picture. The aging of the template can be compensated for by a simple re-recording (because of aging, illness: cataract, diabetes). It is important that the final image shall be sufficiently detailed so as to make the features used for identification well visible.

Iridology can help to survey the health of the person examined. By means of pupil control, it is possible to demonstrate whether a person is tired, consumed alcohol or used any drug. In addition to its quickness, the key advantage of iris identification is the accuracy – thanks to the iris stability – because the eye is an internal organ, protected, yet visible from outside. Several countries use iris identification. Millions are included in an iris identification system throughout the world for reasons of convenience, which enables them to cross borders without passport.

In the light of the knowledge described above in can be stated that it is the iris identification that would be the best choice at present. Both considering the ratio of price/value and taking the reliability parameters into account, there are currently no better alternatives. Yet, it can be said that its use in a healthcare environment might be problematic, except for identification at a critical level. On the other hand, it is not competitive against the costs of fingerprint testing systems. The development and spread of this technology result in positive changes in this respect, however, I think it unable to be introduced at present.

For this reason, the search for an additional system to the fingerprint testing shall be continued in order to achieve the appropriate level of security. In the second part, an important consideration for the selection is the ease of use, the acceptable cost level and, of course, the proper level of functionality. I consider it worth directing the development towards the RFID technology. By using this, a multi-level identification system could be implemented, that would perform the identification at a standard level by means of RFID while the high-priority access control would use the fingerprint test and RFID in combination.

References

[1] IMRE S. et al.: *Examination of RFID Systems In Terms Of Consumption and Technology.* (In Hungarian), www.rfid.answare.hu:8080/site/kutatasi-erdmenyeink/radios-megoldasok/2006/rfid-rendszerek-vizsgalata-felhasznalas-es-technologia-szempontjabol.pdf/view (downloaded: 12 02 2012)

[2] VARGA D., OLÁH A.: Biometric identification systems. (In Hungarian), *Híradástechnika*, 7 (2004). www.hiradastechnika.hu/data/upload/file/2004/2004_07/HT0407-8.pdf (10 10 2013) [3] BUNYITAI Á.: Today and Tomorrow's Automatic Identification Procedures for Access Control Security Systems Perspective. (In Hungarian), *Hadmérnök*, VI 1 (2011), 22–35. www.hadmernok.hu/2011_1_bunyitai.pdf (downloaded: 11 08 2013)

[4] SZABÓ M. D.: *Biometric Identification and Data Protection*. (In Hungarian), http://szabomat.hu/tanulmany/biometria.pdf (downloaded: 16 08 2013)

[5] KOVÁCS T.: *Biometric Identification*. (In Hungarian), Budapest: BMF, 2009. (College digital note)

[6] http://upload.wikimedia.org/wikipedia/commons/3/3c/Biometric_system_diagram.png (downloaded: 12 10 2014)