Investigation of User Acceptance for Biometric Verification/Identification Methods in Mobile Units

Sandra Giarimi and Helen Magnusson

Master of Computer and Systems Sciences[1]
Department of Computer and Systems Sciences
Stockholm University/Royal Institute of Technology

[1] This thesis corresponds to 20 weeks of full-time work for each of the writers.

Abstract

Information technology widely uses Personal Identification Numbers (PIN:s) to verify a user to a system. Recognition of a PIN does not, however, mean recognition of the person's identity. Anybody can have gained access to a PIN, a card or any other 'key' that is being used to get access to a device. This means that systems that are dependent on high access security can not always rely on these kinds of tokens, since they can not ensure that a user is who s/he claims to be. Biometrics could be used to gain trust to a device instead of PIN:s or passwords.

Using biometrics raises concerns about the public's perception of a possible intrusion of their privacy. One can generally say that the less intrusive the biometric, the more likely it is that it will be accepted by the users. To increase the level of user acceptance a Personal Trusted Device (PTD)[2] can be used. The thought is that the security in a PTD should be high enough that both user and the communicating party shall feel trust. Confidentiality, integrity and accuracy shall be achieved, without any doubt.

To get access to a PTD, the user has to log on with a biometric method. For every critical transaction to be performed (bank transactions with certificates, secure email etc.), a new verification should take place.

A statistical investigation was performed to draw conclusions about user acceptance for biometric verification/identification methods in mobile units. The investigation was performed on young people living in Sweden – about 16-18 years old.

Our main conclusions are:
According to our study the most suited biometric methods for mobile units are iris scan and fingerprint technologies. These methods are the ones fulfilling the highest security expectations and the highest acceptance rate among the investigated students.

The secure services being in use today, like PKI, certificates etc. should also be used in the future. We suggest to replace PIN:s and passwords for log in to the mobile unit and the secure services with a biometric method for more secure access.

[2] The explanation to the expression PTD can be found in the glossary.

1. Introduction

1.1. Background

A few years ago not many people had access to the Internet at home. Bills were paid at the post or bank offices, shopping were made in real stores and letters were sent by ordinary mail. After the break-through of the Internet at home these services could easily be performed from the home-office at any time. Some years ago many people started to pay their bills and do at least some of their shopping on the Internet, not having to think about opening hours and being at the right location. Many people have even stopped writing 'real' letters and instead turned to email. In many cases people have also started to use email and SMS instead of telephone calls. New technologies (WAP, GPRS, blue-tooth and in the near future UMTS etc.) have developed and email, shopping and other services no longer have to be utilised from the home-office. Instead they can be made regardless of place and time using a mobile unit. The concept 'mobile unit', also called 'mobile terminal', stands for a mobile phone, a laptop, a personal digital assistant (PDA), etc, that includes Internet access.

Information technology (IT) widely uses Personal Identification Numbers (PIN:s) to verify a user to a system. Recognition of a PIN does not, however, mean recognition of the person's identity. Anybody can have gained access to a PIN, a card or any other 'key' that is being used to get access to a device. This means that systems that are dependent on high access security can not always rely on these kinds of tokens, since they can not ensure that the user is who s/he claims to be.

With a mobile unit, which contains important information and is used for secure transactions for instance, it is of extreme importance that the user trusts the device. A trusted device, also known as a Personal Trusted Device (PTD)[3], denotes in this thesis a mobile unit where the owner can store any kind of information and be sure that no one other than her/himself can get access to it. Biometrics could be used to gain trust to such a device.

Biometrics can be described as measurable physiological and/or behavioural characteristics that can be used to verify the identity of an individual to a system. Common physiological characteristics include fingerprints, hand geometry, retina and iris patterns. Behavioural characteristics include voice, signature and keystroke patterns. There are many kinds of biometric technologies, but common to them all are that they take a characteristic sample of a person, a pattern and use this to verify and/or identify that person. This biometric pattern is an example of a piece of information that can be stored in a PTD.

Using biometrics instead of PIN:s or passwords to get access to a device does not mean that services like PKI, certificates and others will or should be replaced. Such services provide security for transactions from the device to a network like Internet. However, based on our previous investigations [GIMA], [GIMA2], we draw the conclusion that the security of these services may be compromised in the accessing stage since they all rely on PIN:s and/or passwords.

[3] The expression PTD is taken from Mobile electronic Transactions [MeT], however in this thesis we have stipulated our own definition.

A problem is that people in general may feel that their privacy might be threatened by the use of biometric methods [LIU]. This concern can be reduced if the biometric samples are stored locally in the mobile unit – the PTD. Storing the templates in the mobile unit means, that the comparison is made locally and not in a database or server, which in term means that the comparison is one-to-one and not one-to-many.

"Imagine a Palm Pilot that greets its user by name as soon as it's turned on and held in the right owner's hand, or a cell-phone that won't activate unless it recognises the subscriber personally. Imagine losing any kind of mobile personal digital device and not having to worry that a techno-savvy hacker could decode the layers of passwords and network security that protect your investments." [CHI]

1.2. Problem statement

Do future users accept biometric verification/identification methods in mobile units and are there any differences in the acceptance between one-to-one and one-to-many storage?

1.3. Purpose

The major purpose of this thesis is to investigate if there is any user acceptance for biometric methods in mobile units among future users. Another purpose is to investigate and analyse the maturest[4] biometric methods, available today and in the near future. The most promising methods for PTD:s will be selected and analysed in depth.

1.4. Target group

Our target group is our sponsor – Memogram AB, people in the telecom business and persons with interest in mobile technology and security. To gain the most of this thesis, the reader is recommended to have basic knowledge in information security.

1.5. Delimitations

The focus in this thesis is on the verification/identification of users to a PTD. Security services for information transactions from end user to networks, such as PKI, certificates and others, are not considered in this report. Due to limited time, implementing and testing biometric products will be out of the scope of this thesis. The user acceptance investigation will be performed in Sweden.

1.6. Research methods

1.6.1. Background work

The background work for this thesis started in early spring 2001, when we worked with secure transactions for mobile applications [GIMA]. The conclusions were that transactions seemed to be secure, but there was nothing that assured that the person presenting the right PIN, was the right user. A correct PIN or password does not verify the identity of a person, it only verifies that the person has the right information. The next step was a study of identification and verification methods for mobile applications [GIMA2], where the conclusions were that the use of biometrics, possibly in combination with a Smart Card and PIN or password would present much higher

[4] A mature method or technology is one that is generally accepted in the IT-business sector and available for mass-production to a considerably fair price.

security to mobile units. A suggestion was made to investigate user acceptance for biometric methods, especially for mobile units.

1.6.2. Iterative work

The work in this thesis was characterised by the ongoing and fast development in the areas of mobile units and biometric techniques. Every day information has been searched for in relevant newspapers and on the Internet. As new information was released this thesis had to be modified.

1.6.3. Literature search

The research began with studies of different types of verification methods. These methods are based on something you know, something you have and something you are. Strictly speaking these methods also include 'where you are'. After this initial study the work ended up focusing on something you are – biometrics. Different biometrics includes fingerprints, iris and retina patterns, face geometry, voice, signature and keystroke patterns etc. After studying the most common and mature biometrics the objective was to find which methods that were best suited for mobile units.

The literature search was mainly performed on the Internet in an unsystematic way. Also the library and newspapers were used as information resources.

Since the two areas of main interest, biometrics and mobile technologies, can be characterised as 'moving targets' we can not know if the literature search has been thorough enough. After intensively having followed the biometrics area and the area of mobile units in open sources during most of 2001, we recognised in total what was 'new' information. We also believe that much research information still is stored as confidential information within different companies and organisations.

1.6.4. Statistical investigation

A statistical investigation was performed to draw conclusions about user acceptance for biometric verification/identification methods in mobile units. The investigation was performed on young people living in Sweden – about 16-18 years old. This selection was made because biometric methods still are quite new on the commercial market and the 16-18 year olds are probably the future users of biometric methods.

A distinction between verification on a mobile unit and verification/identification on a server was made. The aim was to see if there were any differences between the user acceptance if the biometric sample was stored locally on a PTD or globally in a database or on a server.

For a more thorough description of the statistical investigation, the reader is recommended to read chapters 6 – the method and 7 – the statistical investigation.

1.7. Sponsor

Memogram AB, a company with expert knowledge in telecommunications, sponsored this work.

1.8. Related work

Similar studies or research projects as this thesis have not been found. However, AgV and the German BioTrust project conducted a research about how to improve chances

that users will accept any given biometrics system. The results were published in Biometric Technology Today, January 2001 [BTT]. Some of the main conclusions where:

- The users wanted to have knowledge of where the biometrics data was stored
- The users wanted to have knowledge of how the biometrics data was protected and who had access to this data

before they could accept using biometric methods.

Another report on the evaluation of biometric techniques for identification and authentication [POL] provides some advice as how to increase the level of user acceptance. For example it is important where data is stored. With the use of a card to store the template, people should not fear 'Big Brother' as much as they do when the template is stored in a database. It is also of great importance to educate the users, so that they have some understanding on how biometric methods function.

During the search for research projects in the area of this thesis, a contact was made with Mr. Julian Ashbourn who is one of the very first persons to successfully design biometric systems and to integrate biometrics into other processes [ASH]. He has written a large number of technical papers and articles about biometrics. He is also a member of the Association for Biometrics. We asked him if he knew about any project that was going on in this specific area. According to Mr. Ashbourn, there were not any projects or research at all regarding the same issues as this thesis.

1.9. Definitions

The glossary, which contains the main expressions used in this thesis, can be found in appendix 1.

Nevertheless, there are some major definitions that have to be explained: identification, verification and PTD.

Identification answers the question 'who is this person?' [IBM2]. It means that the system checks all the stored identities for a match and does not know if there will be a match. This is also called a one-to-many comparison.

Verification answers the question 'are you the person you claim to be?' [IBM2]. It means that a person claims that s/he is entitled to enter the system and in this case there should be a match. In the area of biometrics the term authentication have the same meaning as verification in most cases. In this thesis we have chosen to only use the term verification to avoid confusion. This is also called a one-to-one comparison.

A Personal Trusted Device is a device that both the user and the communicating party can trust. A PTD is in this thesis a mobile unit where the owner can store any kind of information and be sure that no one other than her/himself can get access to it.

1.10. Structure of thesis

In chapter two, an overview of different types of biometric methods can be found. General drawbacks of biometrics and explanations to different error rates in biometric systems will also be found in this chapter.

In chapter three, we suggest which biometric methods to apply in mobile units and which ones to focus on in the investigation.

In chapter four, we discuss the influences on user acceptance, such as where the templates are stored, cost and education and what if the user runs out of biometrics. We also explain the meaning of a PTD.

In chapter five we have listed a few areas for consideration before applying biometric methods in mobile units.

In chapter six the investigation method can be found.

In chapter seven the reader will find the statistical investigation.

Finally, in chapter eight, the discussion, conclusions, source critics and suggestions for future work will be found.

In appendix 1-3 the reader will find the glossary, the questionnaire and the explanation to the questionnaire.

The total statistical material is not included in the thesis or its appendices for reasons of corporate confidentiality.

2. An overview of biometric methods

The aim of this chapter is first to make a short introduction to the maturest biometric methods. These methods are examined from the viewpoints of technology, procedures and user friendliness. Their strengths and weaknesses are listed. Some additional methods are also mentioned. However, these methods are not considered mature enough and will not be thoroughly examined in this thesis.

For all biometric methods, before verification or identification can be performed, the first step is to go through a registration process, also called enrolment. Enrolment means that biometric data is extracted, captured and a template is created.

2.1. Fingerprint systems

Identification of a person through a fingerprint is one of the oldest biometric sciences. There are many suggestions on where and when the first use of fingerprints as identification method appeared. For instance in France, in 1870, A. Bertillon invented a system based on finger print analysis for identifying criminals [POL]. In the USA, one of the first uses of finger print analysis conducted in 1901, was to prevent railway workers from collecting double pay [BIO].

It is important to explain the difference between fingerprints and finger-scans. Fingerprinting systems, also known as live-scan, are normally used for forensic usage [FING]. Fingerprinting systems store the whole image of a finger. The comparison is one-to-many, which means that each fingerprint is compared to the whole database of up to several millions of fingerprints, for example, the Federal Bureau of Investigation's (FBI) database contains about 70 million fingerprints [MSU]. One search takes about a couple of hours. Finger scanning on the other hand does not store the whole fingerprint, but particular data about the fingerprint. The data is stored in a template that does not require as much storing space as the whole image. Finger-scan can be used to make a one-to-many comparison, but is much more used for one-to-one verification, which takes 1-3 seconds [FING].

2.1.1. Minutiae

A human fingerprint contains of a rather smooth flow of ridges that make a pattern. A discontinuity that interrupts the flow of ridges is called a 'minutia'. There are several types of minutiae: the core, which is the inner point around which loops, arches and swirls center; dots, that are very small ridges; islands, slightly longer than dots; bridges; lakes etc. A typical fingerprint image contains 30-40 minutiae. FBI claims that no two individuals can have more than eight common minutiae [BIOC], but police procedures in other countries have other requirements for corresponding minutiae [RJA].

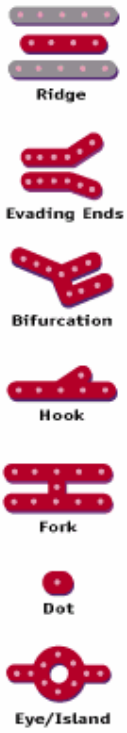


Fig. 1. Some anatomic characteristics of a fingerprint (minutiae). Source: [BIOP].

2.1.2. Technologies

There are different mechanisms to capture a fingerprint image. Today, at least three different technologies are being used: optical, silicon and ultrasound.

Optical

The most common and widespread technology is the optical. The finger is here placed on a coated platen. A charged-coupled device converts the image of the fingerprint into a digital signal. The digital signal is then adjusted to get an image. Some of the strengths of optical devices are that they are considerably cheap, they are most proven over time and they can withstand temperature fluctuations. The weaknesses with an optical device are that the platen, where one puts the finger, must be big enough to get a quality image of the fingerprint, and that the device that converts the image of the fingerprint into a digital signal can wear with age and cause errors. [FING]

Silicon

The majority of companies working with fingerprint techniques use optical devices. However many are now turning to the silicon technology. Silicon is a new technology, which became available in the late 1990's. It is based on direct current (DC) capacitance, which means that the silicon sensor acts as one plate of a capacitor and the finger as the other. Capacitance, also referred to as electrical fields, between the platen and the finger is converted to a digital image. Some of the strengths are: the image produced is of better quality than with optical technologies; silicon chips, that is where the image data is stored, are smaller than optical ones and can therefore be

used in smaller devices. One weakness, however, is that silicon devices are not proven to last, especially in conditions that are less than optimal. The reason for this is that the technology is still rather new and has not been tested enough. [FING]

Ultrasound
The third technology is ultrasound. It is considered the most accurate, however not very common yet. It transmits acoustic waves and measures the distance based on the impedance[5] of the finger, the platen, and air. One of the major strengths of this technology is that the ultrasound is capable of penetrating dirt and leftovers from other fingerprints on the platen, which optical devices can not. Ultrasound is a very new and unproven technology, though, and since it has not yet started to be used widely, its long-term performance has yet to be proven. [FING]

2.1.3. Procedure

When performing the enrolment, there are several steps to convert an image of the fingerprint to a template. This process is called 'feature extraction' and each finger-scan vendor has its own algorithm, usually a patented one.

There are a few basic steps when doing the feature extraction in finger-scan systems: if the image is greyscale, areas that are lighter than a particular point are discarded, and those darker are made black. The ridges are then thinned down to one pixel (from 5-8). The next step in the process in to localise the minutiae. Any false minutia, caused by dirt, sweat or scars, is discarded. Minutiae that do not make sense, like when a ridge is crossed by two or three other ridges (probably a scar), are also filtered out. After filtering, the next thing is to situate the minutiae. There are several ways to place a minutia – it can be placed directly on the end of the ridge, one pixel away from the ending, or one pixel within the ridge ending. Besides the placement of the minutia, the angle of it and the type and quality can be used to classify it. [FING]

2.1.4. Strengths and weaknesses

The major strength is that fingerprints are unique. No two individuals have identical ridge patterns. Ridge patterns are formed in the embryo and changed during lifetime only by injury, burns, diseases and other unnatural causes [BIO]. Even identical twins can be successfully distinguished, though with a slightly lower accuracy than non-twins can [RICH]. Another strength is that fingerprint devices can be made very small and rather cheap and can therefore be suitable for mobile units.

A major weakness with fingerprints is that a fingerprint will not be accepted if the finger is injured, for example. Further on, a weakness is also that some people can not use fingerprint methods, because they have too 'weak' ridge patterns, which means that the sensors can not 'read' their fingerprints. [RJA]

2.1.5. User friendliness

Leaving one's fingerprints is still considered connected with criminology and law-enforcement. Users might find that biometric methods based on the fingerprints intrude their privacy since a person can be identified by her/his fingerprints. Another problem is that many people think that a fingerprint can easily be forged, which is not

[5] Impedance is the electro-technical term for the total resistance between two points in an alternating current (AC)-circuit.

always true. Many systems today have a method for checking for the pulse in the finger. In spite of the above mentioned, fingerprint systems are user friendly since they are easy to use, cheap and have a quite high security level.

2.2. Hand geometry

There are several types of technologies that in some ways measure a user's hand, for instance hand scan technology and hand geometry. These methods use different distinct characteristics of the hands, which include geometry of hand and fingers, palm and fingerprints, blood vessel patterns etc. In this thesis the focus will be on hand geometry, since it is the most used method [DYS], [IRCO].

Hand geometry is a method that measures the physical characteristics of a user's hand and fingers. It is most often used in two applications, namely access control (to buildings for example) and time and attendance (time clocks). The method is sometimes mistaken for palm reading, but has nothing to do with that. Hand geometry is a method that looks at the hand and fingers from a three dimensional perspective.

2.2.1. Procedure

Enrolment is done in the following way: the user places her/his hand on a plate, which has a set of guidance pins that ensures the right position of the hand. A camera above the plate records the top and side views of the hand. A set of key measurements, length and width of the fingers for instance, are extracted from the photo image and used to categorise the user.

For the verification process the user once again positions her/his hand on the plate, the camera records the images needed. A comparison is done between the newly given sample and the previous stored template.

2.2.2. Strengths and weaknesses

One of the major strengths of hand geometry is that it is easy to use. Because of the guidance pins, the hand will always be in the right position. This means that users will probably make fewer errors. Since hand geometry devices are easy to use, they are considered user friendly.

A drawback of hand geometry is that it is not as reliable as fingerprints, iris or retina scan. However it is more reliable than behavioural biometrics, such as signature and keystroke analysis. Another major weakness is that a hand geometry device is quite large, which prevents it from being used where compact design is of crucial importance, like in mobile units. An injured hand will also influence the verification process negatively.

2.2.3. User friendliness

Hand geometry is one of the easiest biometric methods to use and therefore considered to be user friendly. However, since it is not a very reliable method, many users might feel that they could not trust it.

2.3. Iris recognition

Iris recognition is one of the most reliable biometric identification and verification methods. It is used today on a few airports instead of tickets for frequent travellers. It

is called EyeTicket and people that use it do not have to check in like other passengers, they just have to scan their iris and walk through. [MEE]

The shape of the iris is stabilised under a baby's first year and there are no further changes in lifetime [RJA]. Because of this stability, iris recognition is reliable, which could have a positive impact on the user friendliness. The mechanism that forms the iris is chaotic which leads to the fact that even identical twins have unique irises and even the right and the left iris of a person are different [RJA].

2.3.1. Technology

Iris scan is based on visible qualities of the iris like furrows, rings, freckles and the corona. Those characteristics are converted by the iris recognition technology into a code and stored for future verification attempts [IRI].

2.3.2. Procedure

The eye is scanned with a monochrome video camera. The first step in the enrolment process is to locate the iris with the camera no more than three feet (approximately 1 meter) away from the eye. When the iris is found, the outer edge and the pupil has to be located and then a complex algorithm converts parts of the iris and stores it in a hexadecimal form. [IRI]

When verification/identification is due, a comparison will be performed on the data within the hexadecimal form. This process only needs a glance at the camera and is quite simple. The iris is located within 1/4 second and the code is generated within one second. The next step in the procedure is to make a match and the time needed for that is depending on the processor speed and where the template is stored. [IRI]

2.3.3. Strengths and weaknesses

Iris scan results in unique patterns and gives also very high accuracy among users with eye diseases. Iris recognition has the lowest error rates among automated systems when measured in laboratories. The method is both easy to use and very fast. Iris recognition is reliable even if there are ongoing changes in the eye, such as the pupil's extraction and contraction. The template will always result in the same size regardless of the size of the iris.

On the negative side, the method is still rather expensive and people might be reluctant using it due to fears of eye damages. Iris scan can also be affected if the person is blinking, if the eyelashes obscure the eyes and if the person is wearing sunglasses [RJA].

2.3.4. User friendliness

Since iris scan does not require more than a glance from the user, it can very well be accepted for verification. Iris scan relies only on reading iris from the outside which means it is not necessary to use any light beam (like in retina scan). This is one reason why iris scan could be more accepted than retina scan. It can also be mentioned that it can be a very fast procedure, given that processor power is available.

For a mobile unit one can imagine that the scanning procedure takes place with a minimal camera placed somewhere among the buttons. It should be initiated when the user presses the START-button and the scanning of the iris should not require any

additional activity. However it is very important that the user has full control over the procedure initiation, since all that is needed is a glance at the camera to start the recognition process. This is not always what one wants when looking at the camera.

2.4. Retina scan

Retina scan is an 'old' biometric method and as far back as in the 1930's, research showed that the pattern of blood vessels in the eye were unique even among identical twins. Along with iris recognition, retina scan is one of the most reliable biometric methods used. The device needed to perform a retina scan is a portable unit that today weights almost one kilo. The retina scan is one of the most expensive biometric methods used today. [RET]

2.4.1. Technology

When a scan of the retina, including blood vessels, patterns etc., is done, the results make a unique sample that is stored as a template. In the process of verification/-identification, the user has to stand about 1,5 cm from the camera so that it can scan the back of the retina. Retina scan devices read through the pupil using a light beam and measure the pattern of the retina at over 400 points. This presumably gives retina scan a higher accuracy than a fingerprint which is only measured at about 30-40 points [RET].

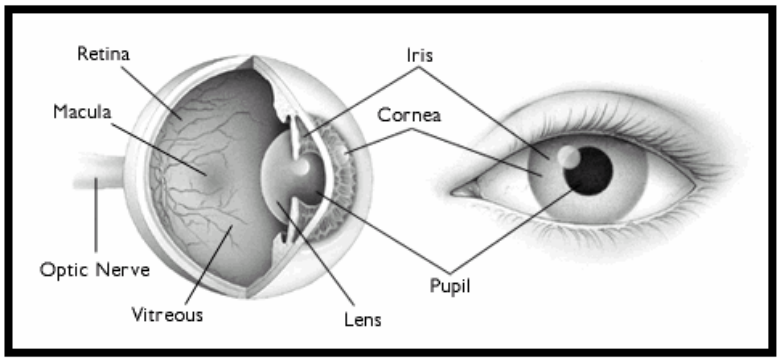


Fig. 2. Elements of the eye. Source: American Academy of Ophthalmology [RET]

2.4.2. Procedure

The enrolment requires that the user looks into the device holding the eye absolutely still, otherwise the procedure has to be repeated. The retina is scanned a number of times and the system needs several scores to make a template [RET].

The procedure for verification is the same as for enrolment except for the number of images that are needed. For verification only one good image of the eye is needed to make a correct match. [RET]

2.4.3. Strengths and weaknesses

This is a stable method because the retina is normally not changed during a person's lifetime. The only way the retina can be affected is by diseases like eye catarrh or a serious head trauma. The retina is also unique for every person and this makes it secure for verification/identification.

Retina measures the inside of a body part, thus no person can obtain the biometric information without the owner's knowledge. A fingerprint can be 'lifted', everybody

can se a person's face and the voice can be recorded. A retina pattern is a secret until the owner of the pattern wants to share it. This makes the retina more resistant to fraud than fingerprints and irises, for example.

One of the most negative parts of retina scan is the difficulty to keep the eye still in the enrolment process. Another negative part is that people often think that the procedure to scan retina could be dangerous and make damage to the eye. The price of retina scan devices is also too high today, which make a commercial introduction for mass market difficult.

2.4.4. User friendliness

There are no studies that show that the light beam could cause any damage to the eyes, although, in a study 2500 persons out of 9000 participating did not even want to try retina scan [ORK]. This was probably because of the light beam that had to be directed straight into the eye. However, the participating persons in the study thought that the retina scan was a reliable technique [ORK].

Since the enrolment process requires much from the user, such as standing absolutely still and putting the eye against a device, it can affect the user friendliness negatively.

2.5. Face recognition

To recognise a person by the face is something that is known and used since ages. However, today it can be done automatically by a system.

2.5.1. Technologies

Face recognition technology relies on the comparison of different parts in the face. There are four types of face recognition technologies:

Eigenface
Eigenface means approximately 'one's own face' and this is a method where the whole face is taken under consideration. Pictures in two dimensions and greyscale are being used to recognise the most distinctive characteristics. The user's face is mapped to a series of coefficients. When it is time for verification the user's new template is compared to the enrolled template to determine coefficient variations. [FAC]

Feature analysis
Feature analysis, implies that the features of the face are being analysed. This is a more useful technology than Eigenface because of the ongoing changes in the face, as smiling, etc. No global picture of the face is compared against a template; just the extracted feature is analysed, which makes it easier to do a comparison in different angles. [FAC]

Neural Network
The Neural Network technology maps features from both the enrolled template and the 'living face' or a reference face. An algorithm, which uses as many measurable points as possible to make a comparison, determines the level of similarity. The algorithm initiates a vote on matches and if there are more mismatches than matches it has to be decided which features are most important, and then make a final vote. [FAC]

Automatic Face Processing
Automatic Face Processing is a basic technology, using distances between eyes, corners of mouth, length of the nose and other points. This is not as accurate as the other techniques. [FAC]

2.5.2. Procedure

The enrolment process takes about 20-30 seconds when several pictures are taken. The pictures should differ from each other both in positions and features for better and simpler match. It makes the verification/identification of a face in different situations easier. [FAC]

The pictures are converted into a template that can be stored in a database or on, for example, a smart card. A picture of a face can be encoded into a very small template and then recreate itself to be almost exactly like the original picture [PHI].

For verification the user claims an identity or the fact that s/he is entitled to enter the system. In a few seconds a picture is taken and compared to either the claimed identity template or all templates. If there is a match, the user is accepted.

2.5.3. Strengths and weaknesses

Existing hardware, as for example a video camera, could be used for face recognition. Demo versions of software are available for free download, which makes trials relatively cheap [FAC].

A drawback with the face recognition system is that it requires continuous updating because of the ongoing changes in a person's face. If a user has a beard for example the analysis of the features could be a very difficult process.

2.5.4. User friendliness

Face recognition could reach high user acceptance, because people are more or less familiar with having their pictures taken [POL]. The method does not require any more of the user than the fact that s/he is positive to having her/his picture taken. For the user it is a passive procedure where s/he only has to look into the camera.

2.6. Voice biometrics

To recognise a person by the voice is something that is known and used since ages, both by humans and animals. Today it can be done automatically by a system.

2.6.1 Technologies

Voice biometrics is also known as speaker recognition, but we chose to use the term voice biometrics in this thesis, denoting the use of the features of a person's voice to verify/identify the person. Voice biometrics should not be confused with speech recognition, which refers to technologies that recognise what a person is saying. There are some similarities between the two, though:

- Both techniques are sensitive to background and channel noise, hoarseness, vocal stress etc.
- Both techniques need good microphones and noise cancellation software. [MARK]

Voice biometrics is one of the few biometrics that process acoustic information most others are image based. Voice biometrics have mainly two commercialised forms, namely speaker verification and speaker identification [MARK].

2.6.2. Procedure

General steps for enrolment are:

- The user initialises the voice biometric system in some way.
- The system prompts the user to say something, a password for instance, a few times.
- The system aggregates what is said to get a more robust average voice print for the user.
- The feature extraction is done, which means that the system analyses the characteristics of the user's statements. The features are then loaded in some kind of database to be used for future verification processes.

Systems that use *speaker verification* verify that a person is who s/he claims to be. The speaker verification process is illustrated in fig. 3.

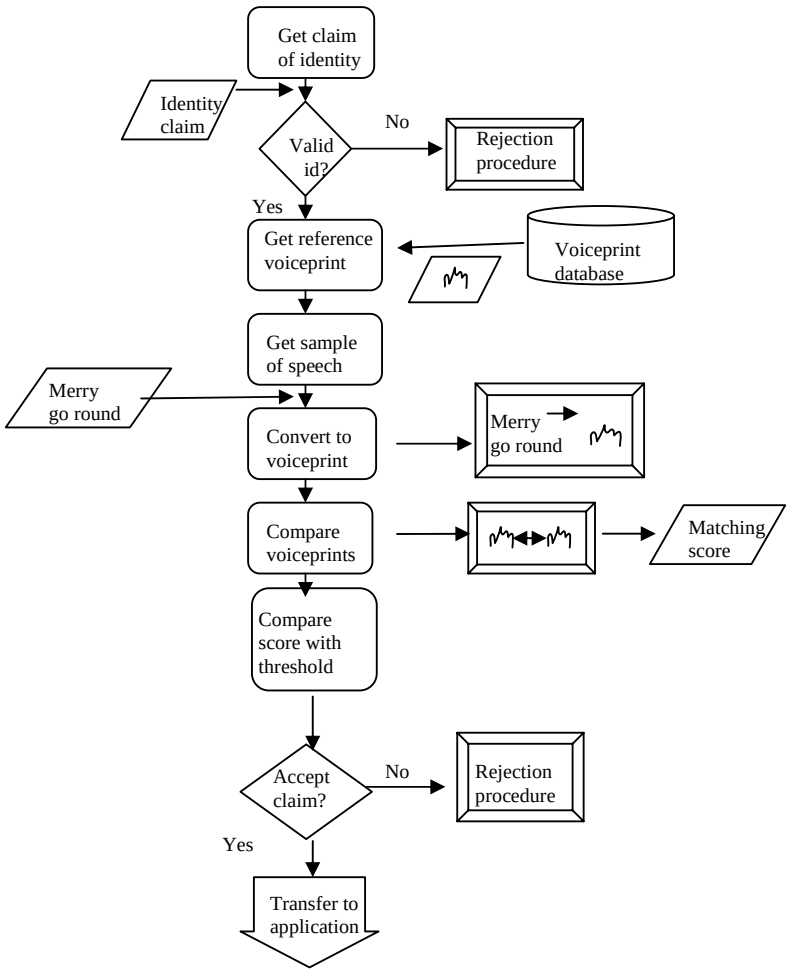


Fig. 3. Speaker verification. Source: [MARK]

Speaker identification is sometimes called speaker recognition. Speaker identification does not expect to receive a claim of identity from a person, it assigns an identity to the voice of an unknown speaker. Usually the speaker does not even know that her/his voice is being recorded. The process is illustrated in fig. 4. [MARK]

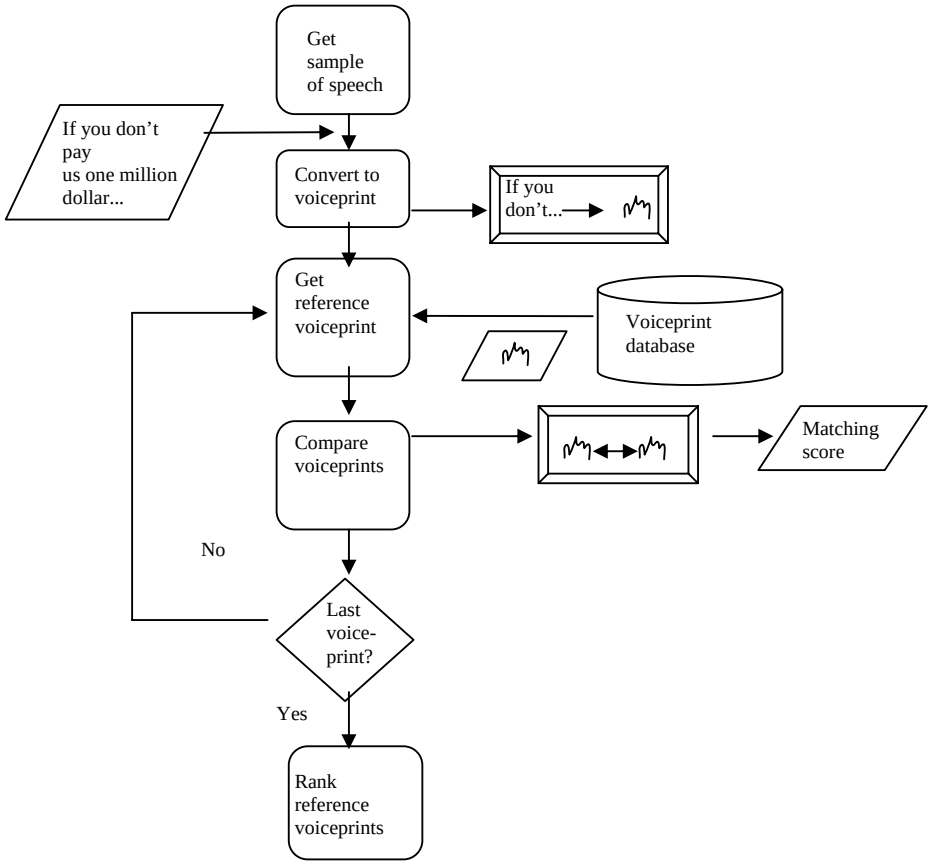


Fig. 4. Speaker identification. Source: [MARK]

2.6.3. Strengths and weaknesses

The number one strength with voice biometrics is the fact that talking is something we do every day. For the user, voice biometrics is not as intrusive as fingerprint scanning, retina scans and other physiological biometrics [OTG].

Another strength is that voice biometrics is cost effective because no special hardware is needed. If used in mobile phones, for instance, the device already has all the hardware it needs, such as microphone. Only the software is needed.

As mentioned earlier, voice biometrics is sensitive to background and channel noise, hoarseness, vocal stress etc. This is a major weakness with this method. Another weakness is that it is easy to record a person's voice and use it in a fraudulent way.

2.6.4. User friendliness

Since talking is something we do every day, voice biometrics is really not anything new. No special effort is needed from the user, apart from talking into the device. This

makes the voice biometrics method user friendly. On the other hand if there is any background noise during the enrolment, this noise must also exist during the verification process, otherwise the user will be rejected. When a user has a sore throat, that can also impact acceptance/rejection by the system.

2.7. Signature verification

For many years people have used their signatures to get verified. The main difference is that earlier, one had to be 'in place' to write the signature but today it can be done electronically.

2.7.1. Technologies

Signature verification measures several factors, like the pressure, rhythm, acceleration rates and stroke length, and it is based on the dynamics of making a signature [RUG]. The signature is a reflex action and not influenced by deliberate muscular control [POL]. There are different ways to capture data for analysis i.e. a special pen can be used to recognise and analyse different movements when writing a signature, the data will then be captured within the pen. Information can also be captured within a special tablet that measures time, pressure, acceleration and the duration the pen touches it [POL].

As the user writes on the tablet, the movement of the pen generates acoustic emissions that are transmitted like stress waves in the material. The sound generated when the user writes the signature is used for verification. [KOE]

2.7.2. Procedure

In the enrolment process the user has to write her/his signature a number of times so that there are several points that can be used for a measurement. The system analyses the signatures and captures characteristics into a template [DAV].

When the user needs to verify her/himself, s/he will be asked to write the signature. The system compares already stored templates with the new data captured signing on the tablet or with the pen.

If the stored template and the fresh signature match in a predetermined number of points the user will be accepted by the system. Otherwise, the user will be rejected.

2.7.3. Strengths and weaknesses

Signature biometrics are easy to use, simple to integrate with today's technique and people have a high grade of acceptance for signatures. These are methods well suited for verification combined with a personal key.

One weakness is that the signature could be affected by hand/finger injuries. Another is that the signature often changes in time, why the user might be rejected if s/he has not used the system for a long time.

2.7.4. User friendliness

People are familiar with writing their signatures and this fact leads to a very high grade of acceptance for signature verification [POL]. There are not any requirements from the user apart from using a special pen and/or tablet. This takes almost no additional time and requires no extra effort.

Since a user's signature may change in time, the system will eventually reject the user. Therefore a signature recognition system should be adaptive. [DAV]

2.8. Keystroke dynamics

Keystroke dynamics is one of the more unusual methods to verify a user. The method relies on the fact that every person has her/his own keyboard-melody, which is analysed when the user types. The process requires typing on a full keyboard, not only pressing a single button.

2.8.1. Technologies

Both digraphs and trigraphs are analysed. In digraph analysis, pairs of letters, i.e. t-h; e-s and r-e, are analysed. Trigraph analysis, that is when triples of letters are analysed, is more reliable [DYS]. Key parameters that are analysed are [BoB]:

- The time a user needs to reach a certain key.
- The time a user needs to press one key.

2.8.2. Procedure

The enrolment is done by typing the same sentence as many times as needed for an algorithm to develop the user's electronic signature based on the user's keyboard melody [BoB].

The verifying process is done continually while the user is typing.

2.8.3. Strengths and weaknesses

If the user is under stress or has injured a finger the typing melody can be different and the right user could be rejected. For keystroke dynamics to work there has to be a user-friendly keyboard. Another weakness is that this is a method more suited for verifying the identity of a person while typing. It can not replace username and password to log on a device.

It is a strength that the verification is done continually, because intrusion can be detected immediately.

2.8.4. User friendliness

People are used to typing on the keyboard, thus it may well be easily accepted. Keystroke dynamics requires no effort from the user more than typing. However, for this method to be used on mobile units, there could be problems. The keyboards on mobile units are very specific in a way that makes it difficult to perform an analysis. That could, though, change when virtual keyboards [CS] are introduced commercially. The virtual keyboard consists of two bracelets attached to the hands[6]. A sensor within the bracelet recognises what the user wants to type.

[6] See fig. 8 in chapter 3.8.

2.9. Biometric methods that we exclude

Biometric methods not mature enough or not suitable for mobile units are the following:

- Vein/vascular patterns: Analyses the veins in, for example, the hand and the face. This technique is hard to adjust to mobile units.
- Nail identification: Analyses the tracks in the nails. Not suitable for mobile units.
- DNA patterns: People have the same DNA pattern in the hair as in the blood and the DNA is unique for every person except identical twins. This is a very expensive technique; it takes a long time for verification/identification and it is not very likely that a person wants to analyse her/his blood or hair or skin every time s/he wants log on to be able to perform a transaction.
- Sweat pore analysis: Analyses the way pores on a finger are located. This method could suit mobile units because one just has to place the finger in a sensor for verification/identification. The technique is however not developed enough today.
- Ear recognition: Shape and size of an ear are unique for every person, but this is not a well-known technique and there is limited information available today about it. Ear recognition might be a suitable biometric method in the future though.
- Odour detection: Verified/identified by your smell? Interesting but not mature enough and almost no information is available about the technique.
- Walking recognition: Analyses the way a person walks. Not suitable for a mobile unit.

2.10. General advantages of biometrics

The major advantages of biometrics are the facts that they do not change over time and also that they are something that one never have to remember, like with a PIN or a password. A fingerprint, for example, is a part of the body and therefore a person will always have it with her/him. Another advantage is that biometrics make sure that a person is who s/he claims to be, as opposite to PIN:s and passwords. Recognition of a PIN or a password does not mean recognition of the person's identity. Because of that it is more secure to use a biometric method for verification/identification than a PIN or a password.

2.11. General drawbacks of biometrics

It is said that the major strength of biometrics is the fact that they do not change over time. At the same time, somewhat ironically, this is the major drawback of biometrics as well. Since a user only has a limited number of fingers, eyes, etc, if the biometric data is compromised, the user will soon run out of biometric features to use. Once a biometric data is compromised it may be useless forever.[7] So, where are the attack points in a biometrics-based system? The following attack points are described in The IBM Systems Journal [IBM]:

1. Presenting fake biometrics at the sensor.
2. Resubmitting previously stored digitised biometrics signals.
3. Overriding the feature extraction process.
4. Tampering with the biometrics feature representation.
5. Corrupting the matcher.
6. Tampering with stored templates.

[7] What to do when one runs out of biometrics, is discussed in chapter 4.

7. Attacking the channel between the stored templates and the matcher.
8. Overriding the final decision.

Attacks at point 1 can be prevented, for instance, if there is a fingerprint pulse check. At point 4 remote attacks can be prevented if encrypted communications channels are used. If the matcher and the database are in a secure location attacks at points 5, 6 and 7 can be hindered. Attacks at point 8 are prevented if cryptography is being used. [IBM]

2.12. Error types

To measure how accurate a biometric method is, mainly two error types are used. Error type 1, also called False Acceptance Rate (FAR) and error type 2, also known as False Rejection Rate (FRR). The FAR indicates the likelihood that a system will grant access to a person who is not enrolled in the system. The FRR, on the other hand, indicates the likelihood that the system denies access to a person who normally should be granted access.

The intersection of the two error types is called Equal Error Rate (EER). A very low EER indicates that there is a balance of sensitivity. Most systems have error rates around 1% [RJA]. More specifically, if the FAR is high, the FRR should be low and vice versa, to get a balance. This is usually something that can be changed in the system, according to the system manager's demands. If it is more important for a company to never give access to unauthorised persons, they might accept that people, who normally should be accepted, sometimes are rejected by the system. However, such a system will be considered not user friendly, since many authorised persons will be rejected. [ASH]

In this thesis the FAR, FRR and EER are not considered, because the biometric methods and techniques are constantly under development, which means that those rates also changes. Also, the error rates are based on tests mostly made in laboratories, which could lead to somewhat positive figures. Still, as a reader, one might want to compare the different methods: one study [BIOC] shows that retina and iris scan systems have the lowest error rates today, followed by fingerprint and hand geometry systems. According to the same study, signature verification and voice biometrics have the highest error rates among the investigated methods. Keystroke dynamics and face recognition was unfortunately not considered in the study.

3. Biometric methods applied in mobile units

In the previous chapter several different biometric methods were examined. This chapter will deal with their feasibility on mobile units. The following text is based on our own speculations, assumptions and suggestions.

3.1. Fingerprints

Fingerprint methods are the only methods developed and cheap enough to be considered as verification methods in mobile units. Today, at least one company (Swedish company Fingerprint Cards AB) has a solution for mobile units.

All information about their product is taken from the company's homepage [FIN]:

The template is stored on a Smart card, which means in the case that the mobile unit is a mobile phone, the template is stored on the SIM-card. Also the algorithm is stored here. If the mobile unit does not have an SIM-card, the template and algorithm can be stored within the system.

The algorithm consists of two steps:

1. Registration (enrolment): a number of distinct areas are extracted from the fingerprint image. They, together with their geometric relationship, form a template, unique for each fingerprint
2. Verification: the template is used as an operator acting on the fingerprint image. If the result is approved, the verification is completed.

Fig. 5. A fingerprint reading mobile phone. Source: [FIN]

3.2. Hand geometry

The device for scanning a hand is too big to use on a mobile unit in a proper way. It requires as much place as a hand takes, and is therefore not suitable for mobile units and not considered at all in the investigation.

3.3. Iris recognition

Iris recognition could very well be suitable for mobile units, but today it is too expensive. With the use of a small camera, like the ones that are already implemented in some new mobile phones, an iris could be scanned. The applicable software must also be added in the mobile unit.

The only effort required from the user is to look at the camera while pressing the START-button. A press on this button should initiate the recognition process, and before the user gets access to the application there has to be a positive verification.

Fig. 6. A mobile video conference unit including a video camera. Source: [NAT]

3.4. Retina scan

Retina scan is also too expensive to use in mobile units, but that is not the only problem. Imagine a user who wants to get access to her/his mobile unit. First it is necessary to initiate the process that will scan the blood vessels in the back of the eye, lets say even this is done by pressing the START-button. After doing that the user has to hold the scanning mechanism 1/2 inch (approximately 1,5 cm) from the eye, while keeping absolutely still. Then a light beam is directed straight into the eye. It is not a very time-consuming process but it requires a lot of effort from the user, probably too much effort to be considered for a mobile unit.

3.5. Face recognition

To make a face-recognition, a regular digital built-in camera could be used. There just has to be more software implemented in the mobile unit. During the verification the user should hold the device at a distance long enough to get the whole picture of the face. That could lower the user acceptance. Because the face recognition is not as secure as fingerprint, retina and iris scan and because it requires a little too much from the user, this is a method not considered in the investigation.

3.6. Voice biometrics

This method could be used today. There are many programs based on speaker recognition on the market. Mobile units, especially mobile phones, are already prepared for this. It is important that it is the user who initiates the recognition process, it should not be initiated only by the sound of the user's voice. A good idea is to use speaker recognition combined with speech recognition so that the user can say something predetermined and the system checks both that the user is who s/he claims to be and that what s/he is saying is correct.

Voice biometrics (or speaker recognition), though, is not a method with as high security as required for critical transactions. Because of the fact that the verification could fail when there are background noise or when the user has a cold, it should be combined with some other verification method.

3.7. Signature verification

Signature verification is a method suitable for mobile units that already are being used for writing on, like a Palm Pilot. A press on the START-button should initiate the access to the unit. After that the user should write her/his signature. If the signature matches the stored template the user should be accepted. However this is not one of the most secure methods, and maybe not suitable for all transactions.

Fig.7. A Palm Pilot that is suitable for signature recognition. Source: [MCM]

3.8. Keystroke dynamics

As mentioned earlier keystroke analysis requires an additional method for getting access to the mobile unit and a secure application. When the access is granted, the user is verified the whole time during typing.

With new technology, like the previously mentioned virtual keyboard, it could be a feasible method for mobile units. But usually, transactions are made by just a few keystrokes, which might not be enough for the verification process to work properly.

Fig. 8. The virtual keyboard; Senseboard. Source: [SEN]

Because this method is not suitable for login, it is not considered in the investigation.

3.9. Which biometrics to focus on in the investigation

In the investigation focus was on fingerprint, voice, iris/retina and signature recognition. Iris and retina have been put together, because of the purpose to see if there was any acceptance at all for biometric methods based on the eye. The time for performing the investigation was not long enough so that the differences between these two methods could be accurately explained. Fingerprint was selected for the investigation because it is a method in use already. Both signature and voice recognition are biometric methods that can be used today without any complementing hardware, thus being suitable to consider in the investigation. In the investigation hand and face recognition and keystroke dynamics were excluded.

4. Influences on user acceptance

Using biometrics raises concerns about the public's perception of a possible intrusion of their privacy. One can generally say that the less intrusive the biometric, the more likely it is that it will be accepted by the users. However, the users are asked to give away images of body parts, and these images are often stored in digital form in different databases. The users have no control over who has access to those databases. This is a big concern. Other issues that have influence on user acceptance are: the cost of the new technology, if any education is needed before the new technology can be used and what happens if one runs out of biometrics – can this happen? The above mentioned issues are the most important, according to us.

4.1. Storing templates

One of the main issues that influences the user's acceptance is where the template is stored [BTT].

4.1.1. In a database

The biometric template can be stored in an external database. In that case the biometric information has to be sent over the net every time the user wants to be verified. During transport the information is encrypted, which makes external database storing rather secure. The problem is that the user has no control over her/his own biometric pattern. The information could be stolen from the database and tampered with, or used in one fraudulent way or another.

Another problem is the response time: it can take long time to perform verification when information is sent over the net because of net overloading and the size of the file.

On the positive side, it does not require as much memory in the mobile unit if the template is stored on an external database as if it is stored within the unit.

4.1.2. In the mobile unit

Storing the template in the unit or on a Smart card leads to the fact that the user has control over her/his biometric information. The biometric verification should take place when the user wants to log in to the mobile unit, and when the user wants to perform a critical transaction or send a secure email, for example. The verification process should be executed on the unit, and give the user access to secure services. These services include PKI, digital signatures, certificates etc.

A drawback is that it will require quite a lot of memory to store the template in the unit. Today the template sizes varies from 9 bytes (hand geometry) to approximately 1000 bytes (fingerprints) [BIOC], [RET]. Most template sizes can be found somewhere in the middle. If the template is to be stored on an SIM-card that could mean problems, since today's SIM-cards might not have enough memory capacity. Today the memory of an SIM-card is between 12 and 64 kB [MEM].

4.2. Cost and education

Some people are always attracted to new techniques. The price is not an issue. However, this group of users is probably not large. People in general will probably not pay

much for a new technique, if they are not sure that it is really useful. The extra cost for a biometric method has to be in proportion with the outcome of it – in this case higher security.

Another issue with new techniques is that they should be easy to use. Naturally all new technical devices need a manual, but it is important that it is relatively easy to learn how to use this new 'thing' without becoming frustrated. If the user can not get the device started or use it in a satisfying way s/he will probably get tired of trying and eventually find the device useless. So, the users need some kind of education to get started. The level of education will probably not be the same for all users.

A distinction between a professional user of a biometric system and a general, 'man-on-the-street'-user is suggested as necessary [ASH]:

The professional user is a system administrator or somebody else that uses a specialist application as part of her/his job. This person is probably eager to use a new technology and s/he usually has a special interest in technical issues.

The 'general' user is a person who is required to interact with the system in an every day situation. S/he can be a person with very little interest in the technique itself. Maybe s/he does not even want this new technique at all and might feel forced to use it. This is, of course, not always the case – the general user can very well be a person who is very interested in new technology and wants to use it. However, the education for these two groups of people is different and must be adjusted to their needs.

4.3. What to do when one runs out of biometrics?

What to do when one runs out of biometrics is a big question that has to be solved, before using biometric methods for verification. This is especially important if the templates are stored in a database and because of that are exposed to several people.

Cancellable biometrics is a method that can be used to solve this problem. Instead of enrolling with a true biometric, the biometric is intentionally distorted in a repeatable manner and this new print is used. If somebody gets hold of a fingerprint, for example, a 'new' fingerprint, to be used as template, can be issued by changing the parameters of the distortion process. This leads to enhanced privacy for the user since the true biometric is never used anywhere, and different distortions can be used for different types of accounts. [IBM2]

4.4. The purpose of a PTD

"A password does not authenticate a person: successful authentication only implies that the user knew a particular secret. There is no way of telling the difference between the legitimate user and an intruder who has obtained that user's password." [GOL, p. 28]

To increase the level of user acceptance a PTD can be used. The thought is that the security in a PTD should be high enough that both the user and the communicating party shall feel trust. To get access to a PTD the user has to log on with a biometric method. For every critical transaction to be performed (bank transactions with certificates, secure email etc.), a new verification should take place. There are relatively secure services, like certificates, today that fit mobile units and the aim is to use these

services and just change the way the user gets access to them. That could mean replacing PIN/password with a biometric method as a ‘protecting shield’.

When a PTD is used to make a request for a money transaction the bank should not doubt who has initiated the request. The reason for this is that the bank should get some kind of indication that it communicates with a PTD and therefore knows that the user has been verified with a biometric method.

If a PTD is lost or stolen, while it is open, some non-critical information might be misused. However, since the critical information is protected by yet another verification process, this information is very hard to steal. It should be up to the user to decide which applications and files etc. that should be protected by ‘double verification’.

5. To make biometric methods in mobile units happen

To introduce biometric methods in mobile units instead of or as a complement to PIN:s or passwords is a major step. It is a big change – a shift of paradigm one could say and it needs a lot of adjustments. Legislation is one area that has to be considered and the same goes for technology, for instance the SIM-card. Another important issue is patents. Are they inhibitors to commercialisation? And finally, standardisation - still an open issue. In this chapter some enablers and inhibitors are briefly mentioned. However, the time given for this thesis was not enough to consider these areas in more detail. Nevertheless, they are worth mentioning since they all are important issues.

5.1. Legislation

Today, a person's signature on paper is an accepted legal verification method. For instance, when one uses a credit card, the signature given is compared with the one on the card and no other identification document is required in most countries. The signature is accepted and forgery is punishable.

If biometric methods are to be accepted as verification/identification methods, the law must accept them equally. Probably not until then will banks and other institutions accept biometrics.

One may compare this to the legal stand of digital signatures using cryptography and all the work that it took to accept those.

5.2. The SIM-card and the Mobile equipment

The SIM Application Toolkit (which specifies the API and functional capabilities in SIM) will certainly need additional functionality to interact with biometric information. The mobile equipment will probably need to accommodate new hardware and software for integral support of biometric processes. [MEM]

5.3. Patented technology and algorithms

Due to lack of open and generally available information on biometric methods, broad commercial introductions and product innovations might be slow.

Most of the algorithms and technologies are patented, which could lead to high costs when licensing these technologies. This may be one of the reasons why there are no more techniques adjusted for mobile units than fingerprint scan. Eventually, future progress in hardware and software development could bring solutions based on algorithms similar to the patented ones, thus lowering the costs considerably.

5.4. Standardisation

A global standard is needed to provide common software interfaces and features. Standardisation is needed to be able to share biometric templates and to permit effective comparison and evaluation of biometric methods and technologies.

The BioAPI standard is an open system standard developed by a consortium of vendors, biometric developers and government agencies. It defines a common method for interfacing with a given biometric application. The BioAPI consists of function calls

(written in C) to perform basic actions, like enrolment, authentication (verification) and identification, that are common to all biometric technologies. [LIU]

According to the BioAPI Consortium, implementation of the BioAPI will enable [BIOA]:

- Rapid development of applications employing biometrics.
- Flexible deployment of biometrics across platforms and operating systems.
- Improved ability to exploit price performance advances in biometrics.
- Enhanced implementation of multiple biometric alternatives (fingerprint, voice, face, iris, etc.).

Also Microsoft, a former member of the BioAPI consortium, has developed a biometric API (BAPI), to speed development of standardised hardware drivers. BAPI is included in the BioAPI specification. [RAI]

However, existing standards might need more extensive functionality and common understanding to be adopted by all vendors and developers.

6. Method

The work with this thesis started after a brief research on the topics secure electronic transactions in mobile units [GIMA], and how to get access to mobile services [GIMA2]. The conclusions from the later work were that it seemed to be too little consideration taken to the fact that PIN:s and passwords are easy to forget and quite simple to crack, why maybe biometrics could be a solution. The big question was, though, if people would consider using biometric methods in mobile units. A search began to find an interested company, to sponsor a project concerning this topic. In May 2001 we got in contact with Memogram AB, and a co-operation started. Memogram was interested in having a statistical investigation done to see if there was any user acceptance for biometric methods in mobile units. The investigation was to be performed on future users in Sweden.

6.1. Investigation method

The investigation is a cross-section[8] survey [LEWA] performed on a sample chosen from a population of students in the gymnasiums[9] in the county of Stockholm. The purpose was to investigate a small number of people in a chosen population, and then draw conclusions from the results and apply these on a larger population. The advantage of examining a sample is reduced costs, less time and that it is easier to perform.

The sample was chosen partly by a cluster-choice [DAH] and partly by a self-choice. A number of schools were chosen (cluster-choice) for the investigation and then the principals in these schools could chose (self-choice) which classes should be a part of the investigation. In these classes, all present students were investigated.

Since the number of participating students was over 200, the investigation is considered to be quantitative.

6.2. Which were the main questions?

Along with the sponsor of this project some main questions were listed. It was decided that the most important question to answer was if the users of mobile units would accept biometric verification/identification methods. Which methods users thought were the best was also of importance, in addition to the question whether the acceptance depends on where the biometric template is stored.

6.3. Who should be investigated?

The reason to perform an investigation on future users was that using biometrics in mobile units is a very new and not yet commercialised area. There are only a few mobile units with a biometric technique implemented on the market today, and those are based on fingerprint technologies. Today most biometric techniques are not developed to be used on small units and even if they were, they are too expensive for the average user. This will probably change in the near future.

Another reason is the importance of increasing the level of security and integrity thinking with young people. They will have use for this in the future. It is also pro-

[8] A cross-section of a group of people or things is a sample of them containing examples of everything within the group. [CHA]

[9] A ‘gymnasium’ is an upper secondary school with grades ten through twelve.

bably easier to have young people to use new techniques, than older people. Young people are often more curious about new things, they are not afraid of new technologies and they might even find it fun. Young people usually have not used old technique very long, so they will not find it difficult to change to a new one as compared to some older people. As the saying goes: “You can’t teach an old dog new tricks”.

Future users were decided to be people in their upper teens, which means approximately 16-18 years old.

6.4. The selection

To make the selection among people in their upper teens it was decided that the population should consist of all students in the gymnasium in the county of Stockholm. If the population was any bigger than this including all the gymnasiums in Sweden, the work would be impossible to perform in twenty weeks. The county of Stockholm had 104 gymnasiums all together at the time and among them 97 were picked out to make the population. Seven schools were excluded, they were French, German or other foreign language schools and schools for children with special needs. The exclusion of these schools was made because of hesitation on whether we could make ourselves completely understood or not.

A sample from the population was picked out through a lottery. This sample included six schools. We got in contact with the principal of each of these six schools and requested to be allowed to make the investigation in one to three classes. It was decided that about 200 students should be enough for the investigation and hoped for positive answers from at least four schools.

6.5. How to perform the investigation

A questionnaire was used, see appendix 2, to investigate the level of user acceptance for biometric methods. We chose to make a triangulation[10] to get good reliability. This means that, in each class were we handed out the questionnaire, we also picked one person for an interview. We chose to use a questionnaire because our goal was to investigate about 200 students. The only way to handle that much data for us in the given time was to store the information in a database. This required a questionnaire with predetermined answers.

Even the interviews were based on the questionnaire, and the aim was to see if there were any differences in the answers from the interviews and the questionnaires. If there were great differences it had to be questioned why, and how reliable the investigation really was.

A presentation of the investigation and us, as students from the University of Stockholm, was done on each appointment, prior to performing the investigation. The students got a very brief introduction to what biometrics is, how the storage could be done, threats and different security solutions. The aim was that the introduction should be as objective as possible and not coloured by our opinions. After our presentation, the questionnaires were handed out to all the students. Together with the questionnaire, the students also got a paper with explanations, see appendix 3. The

[10] A triangulation means that two or more methods are mixed in an investigation. In this case a questionnaire and an interview.

meaning of this was to help the students to remember the key facts from our presentation. One of the questionnaires was marked with an X, and the student who got this one was taken out of the classroom for an interview. During the investigation, it was possible for the students to ask questions if there was something they did not understand.

Not all students had enough time to fill in the questionnaire, even if that was the purpose. External circumstances resulted in that some of the classes had less time to perform the investigation than others. The investigation was planned to take fifteen to twenty minutes. Those who had longer time could of course ask more questions and have more time to read each question more thoroughly.

If there was any time left, we explained the purpose of the investigation. This was not done before the investigation, because we did not want the students to know how we felt about using PIN:s or passwords. That could have influenced the results.

6.5.1. The questionnaire

The development of the questionnaire was of an iterative kind. Along with the contact person on Memogram AB, questions were designed and redesigned continuously. One of the major purposes was to make the questions as neutral as possible. A problem with making a questionnaire is to know how to ask questions that give relevant answers and also to limit the number of questions. A test period for the questionnaire began when it seemed to contain all the questions we wanted to ask and the questions were relevant for the problem statement in this thesis.

6.5.2. The explanation to understand the questionnaire

There had to be definitions and explanations of the words being used in the investigation about biometrics and mobile units. Especially when the students are not studying computer science or biology. To find out how to explain complicated information in a simple way, was also a work of iterative kind. To become as clear as possible, the explanation document was redesigned several times.

6.5.3. Testing the questionnaire

About ten people in different age groups and with different backgrounds were testing the questionnaire including the explanation, and they all gave their point of view. As the tests were performed the questionnaire and the explanation were redesigned. The language used had to be suitable for the population. The aim was to make them all understand the questions and how to answer them.

7. The statistical investigation

It is recommended to look at the questionnaire in appendix 2 before reading this chapter.

7.1. How was the response from the schools?

Previously it was decided that four schools were a minimum for this investigation. The decision had also been taken that about 200 students would be enough. Four schools took contact with us and allowed us to perform the investigation. When the investigation was at the end, a fifth school contacted us and invited us there. However because it was late in the investigation and the number of investigated students were already above 200, we declined the invitation. The response to the letters with the request was good, five out of six schools were positive.

7.2. Falling-off

There are two different types of falling-off in this investigation. The total falling-off includes students who were not in school when it was time to perform the investigation and those who handed in a blank paper. The partial falling-off includes questions that are not answered. The total falling-off was almost 16% (34 students) and the single reason was that the students were absent that day. No one handed in a blank paper.

The partial reduction was small, except from two questions (6,10) where the falling-off was around 2,5 %. Approximately 1,4% did not answer three questions (8b, 9, 11). The conclusion can be drawn that the questionnaire was quite well designed.

7.3. Results from the investigation

Out of 213 investigated students, there were only 4% (8 students) who did not have mobile phone. Almost everyone uses their mobile phone to create and send SMS and there were only a few using WAP. Many of the students answered that they are using the mobile phone to play games, that seems though to be games integrated in the mobile unit, since they are not using WAP.

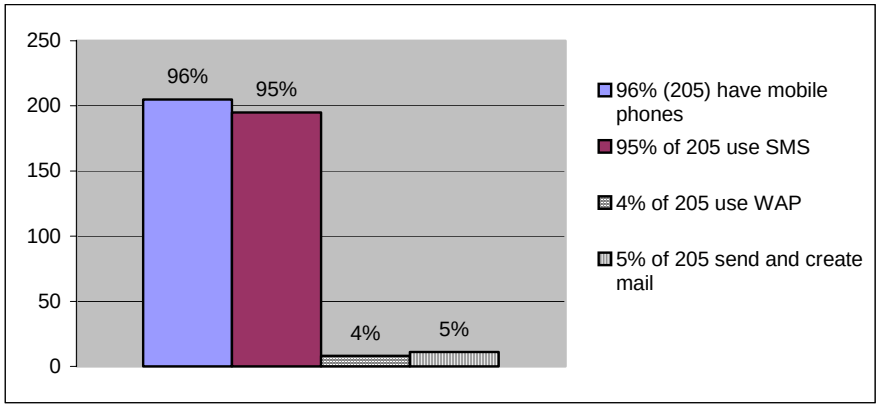


Fig. 9. What is the mobile phone used for?

The question about if they had any other mobile terminal in addition to a mobile phone resulted in 15% (32) positive answers. There were only 1% (2 students) who did not use Internet and 99% (211 students) who did. The Internet was mostly used for getting information, sending and picking up email, chatting, downloading programs, playing games and listening to music. Only 23 % (49 students) that use the Internet, use it for shopping.

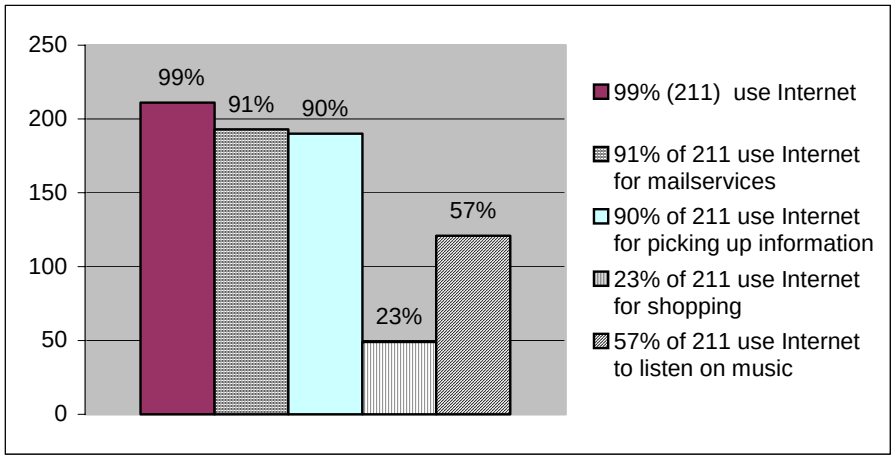


Fig. 10 What is the Internet used for?

As many as 56% (120 students) have lent their PIN or password some time. The follow-up question asking for what purpose they lent their PIN/password, was answered mostly as to get access to the computer and to get access to the mobile phone.

7.3.1. The attitudes to biometrics

There were surprisingly many students who could bare the thought of using biometrics. Of 213 students, 93% (199 students) answered that they could consider to use a biometric method depending on different circumstances. The results show that it is a remarkable difference in acceptance depending on where the storage is done. In cases where the user is the only one having access to the biometric pattern, the positive responses varied from 72% (activate services with a biometric method) to 83% (log in to the mobile unit with a biometric method).

The question regarding if the biometric patterns were stored on an external database also gave high acceptance levels, but not at all as high as if the storing was done in the mobile unit. In the question if one wants to use a biometric method to buy/order something, and send the biometric pattern over the net, there were 44% (94 students) who were positive. To use the same method for performing bank transactions gave better results, 58% (122 students) were positive. This is illustrated below.

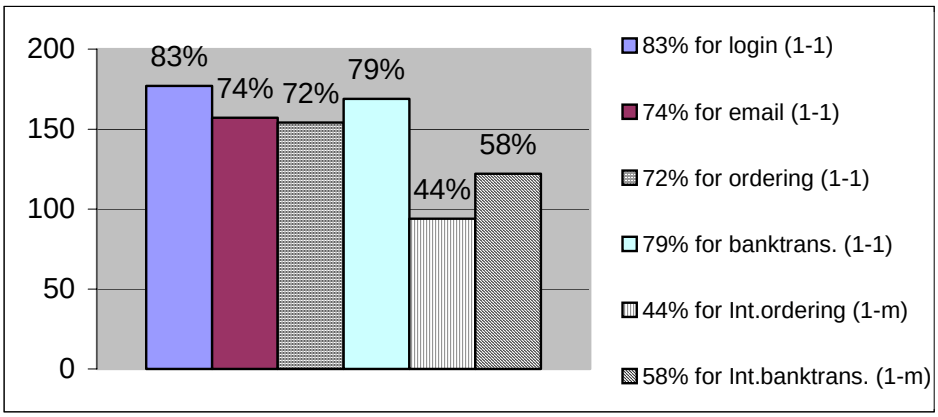


Fig. 11. How many are positive to using biometrics?

Attitudes towards different biometrics

Fingerprinting and biometric methods based on the eyes had the most support in the investigation. 95% (168 students) of those who were positive to use biometrics preferred fingerprints and 62% (109 students) were positive to use iris and/or retina scan. 44% (78 students) were positive to voice biometrics and 30% (53 students) to signature verification.

7.3.2. Biometrics or PIN/password

17% (36 students) did not have any preference on which verification methods should be used, but almost 44% (91 students) would prefer a biometric method. 27% (57 students) wanted to continue with PIN/password. 10% (22 students) thought that both biometrics and PIN/password seemed to be all right.

7.3.3. Are people willing to pay for biometric methods?

To begin with, this study showed that it was only 26% (55 students) who could consider paying for getting a biometric technique in a mobile unit. 70% (149 students) did not at all want to pay and 4% (9 students) did not answer either yes or no.

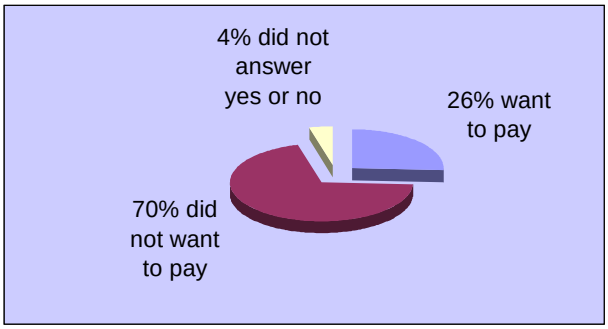


Fig. 12. Do people want to pay for biometrics or not?

The students who were willing to pay answered that they would pay quite a lot. From 20 SEK to 5000 SEK, and there were more who answered the higher price than the lower. However, the most answers where around 100-200 SEK.

7.4. Who shall have access to the biometric template?

Who shall have access to the biometric template? That question was probably a bit hard to understand and resulted in contradicting answers. Students who answered that they did not want to make their biometric information available to anyone else than themselves, should not answer that they want to have a biometric technique for verification on an external database, but that has happened. We have excluded this question in our conclusions, since it was not clearly worded and therefore misunderstood.

6. If You should use a *biometric method*, who do You think should have access to Your biometric pattern? (Several choices are allowed)

☐ only Yourself or

☐ Yourself and ☐ Your telephone/Internet operator ☐ Your employer/school

☐ Your bank office ☐ the government/the county council/the county

☐ whoever You buy something from ☐ other_____

Fig. 13. Question no. 6 in the questionnaire.

The idea was also that the students should understand that they could answer either me (first alternative) or myself and for example the bank office (second alternative), should have access to the template. But some of the respondents answered that only they self should have access to the template, but after that they even answer that somebody else could have access to it.

7.5. Difference in the answers between the questionnaires and the interviews

There was no significant difference between the answers in the questionnaires and the interviews. The only question where it seemed to be a possible difference was the one asking whether the respondent ever had lent her/his PIN/password.

One difference was the fact that there was no falling-off in the interviews, as was the case in the questionnaires.

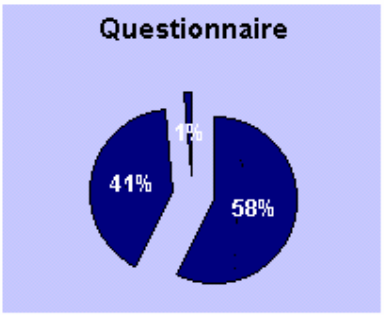


Fig. 14. 58% has lent their PIN/password and 41% had not. One percent did not answer

Fig. 15. 30% has lent their PIN/password and 70% had not.

The differences between the two groups could, though, depend on the small number of students that were interviewed and maybe due to the fact that it can be embarrassing to confess that one has lent her/his PIN or password.

7.6. Our influence on the investigation

Prior to and during the investigation we tried to present the material in an objective way, so that the students would not be influenced by our thoughts about biometrics. We were very careful about presenting threats against both biometric methods and PIN:s/passwords. We also explained the difference between storing the biometric template on the mobile unit and in a database as objective as possible. However, we can not eliminate the risk that we might have influenced the students, even though we tried not to.

8. Discussion and conclusions

8.1. Source critics

The literature existing today in the biometrics area is out of date. There is no literature that deals with both biometrics and mobile units. The main information in this thesis comes from the Internet. However, there is no guarantee that this information is fully correct and objective. Many of the sources in this thesis have the same references, which shows that there are not many papers/reports etc. published on the Internet. There is more information about biometrics and probably even about biometrics and mobile units, but this is classified. We also know that there are projects in the military area, but also that is out of our reach. Due to the fact that some of the information in this thesis is taken from developers, vendors and other parties with economic interests, it may not be as objective as we would wish.

8.2. Discussion

Reliable?

Industry people representing different biometric methods, talk about how secure the methods are. Probably that is true, but one has to keep in mind that to know for sure that, for example, all retina patterns are unique all retinas have to be scanned. That is not the case, since most studies are made in laboratories or in groups of limited sizes. It should also be noted that no system can ever be 100% secure!

Extraordinary cases?

There are some other issues to consider, for example how it is with identical twins and their samples? Are they unique? Some biometrics, like fingerprints and iris patterns, are said to be different for all people, including identical twins. On the other hand, DNA patterns for identical twins are the same. But what about if we start to clone human beings? Will they have unique or common biometric patterns? These questions are outside of the scope of this thesis, however, they may be worth thinking about.

One method fits all?

The biometric method selected for verification and identification has to fit as many as possible. Today the only mature enough verification/identification method based on biometrics for a mobile unit is fingerprint. The fingerprint method, however, is not very suitable either for older people with dry skin or for people whose fingerprints are not distinct enough.

Bypassing security?

The use of a PTD should also increase the level of security so that all involved parties shall feel trust. Confidentiality, integrity and accuracy shall be achieved without any doubt. This, however, can only be done if the users understand the importance of security thinking. This is not the case today, when for instance 56% of the students in our investigation admit that they have, at some time for some reason, lent their PIN or password to someone else.

Best case scenario?

Choosing such an open-minded young group could imply that the results could be seen as a best case scenario on acceptance. The reason for this is that young people often are curious and are not afraid to use new technologies. If the population had

been another, the results could have been different. But in this thesis, we were interested in future users, why we think the results are of interest.

Identification or verification?
Even if we have mentioned identification in this thesis, it is really verification that is treated here. As explained in chapter one, identification answers the question "who is this person?" meaning that the system checks all stored identities for a match and not knowing beforehand if there will be one. This is never the case, when using a mobile unit for getting access to the secure services. If the matching is performed on the mobile unit it will always be a question of verification, "are you the person you claim to be?".

8.3. Conclusions

The results from our investigation clearly show that future users are positive to biometric methods. More exactly, 93% of the students in the study could consider themselves using some kind of biometric method in mobile units. 43% of the students preferred to use a biometric method instead of a PIN-code or password. Only 27% thought that PIN/password was better than biometrics, which can be an indicator that many students are aware that biometrics are more secure.

One part of the problem statement was to find out if there was any difference in the user acceptance, depending on where the biometric template was stored. The study shows that there is a remarkable difference in the user acceptance depending on if the template is stored in the mobile unit or in a database. 77% in average were prepared to use a biometric method if the storing was done on the mobile unit. 51% could consider using biometric methods if the template was stored somewhere else.

The secure services being in use today, like PKI, certificates etc. should also be used in the future. We suggest to replace PIN:s and passwords for log in to the mobile unit with a biometric method for more secure access. We do not want the biometric template to be stored on a database and this is not necessary if the matching procedure is performed on the mobile unit. The biometric method, with the given biometric sample, should initiate secure services and therefore the templates never have to be sent over the net.

According to this study the most suited biometric methods for mobile units are iris scan and fingerprint technologies. These methods are the ones fulfilling the highest security expectations and the highest acceptance rate among the investigated students. The two methods also have a very easy login process and do not require any special efforts from the user. Retina scan is less suited because we believe that it is a difficult process, requires much from the user and also it is too expensive. There was a low acceptance rate among the investigated students for signature verification and that is why we excluded this method too. Because voice biometrics has many drawbacks, we do not think that it is one of the most suited methods for mobile units.

To illustrate our vision, the following example is given:

Anna wants to perform a bank transaction with her PTD. She opens the PTD by pressing the START-button and at the same time she glances at the built in camera and thereby leaves her biometric sample, in this case the iris pattern. The system captures

the newly given sample and compares it to the earlier stored template. Anna is now granted access, which means that the PTD is now open. At the same time the newly given sample is erased from the temporary memory. Anna now opens a browser to enter her bank. At the bank Anna opens her certificate, which is stored in her PTD, by pressing the START-button and again glancing at the camera. A new biometric verification process is performed and if there is a match, the opening process for the certificate starts. The whole process is not visible for Anna, but basically works as certificates work today with username and PIN/password, however they are pre-given. This means that the certificate information sent from the PTD does not contain the biometric sample.

The bank will receive information from the certificate together with a flag indicating that biometrics has been used to open the certificate. In this way the bank system will know that an authorised person has performed the transaction.

If the biometric method works as a protecting shield it can co-operate with today's securing services. This means that the same certificate can be used whether or not biometric methods are being used.

Finally, our investigation shows that users might not want to pay for getting a biometric technique into their mobile unit. We recommend that the costs for introducing such functionality should rather be 'hidden' for example paid by sponsoring banks, authorities, etc. due to higher security levels.

8.4. Suggestions for future work

One suggestion for future work is to perform a survey among companies that work with different security solutions in mobile units, to investigate their attitudes towards biometric methods. It is also interesting to see what they think on the matter of integrating biometric methods with already existing security solutions.

Another proposal for future work is to investigate the legal framework. The purpose would be to clarify what changes are required in order to introduce biometrics as a legally bound verification/identification method.

Acknowledgements

First of all we would like to thank our sponsor Memogram AB, that believed in our ideas and wanted to be a part of this work. We would also like to thank the schools that wanted to participate in our investigation and give us the time needed. Then we want to thank the students that were willing to listen to us and fill in the questionnaires. Thanks also to the people that agreed to test the questionnaire and make it understandable for teenagers.

Last, but not least, we would like to thank our advisor at the Department of Computer and Systems Sciences, Louise Yngström.

References

[ASH] J. Ashbourn, User Psychology and Biometric Systems Performance. 2000

[ASH2] J. Ashbourn, The Biometric White Paper. 1999

[BTT] A. Albrecht, Understanding the issues behind user acceptance. Biometric Technology Today, January 2001

[CHA] Chambers Essential English Dictionary. Chambers Harrap Publishers Ltd., 1998

[CHI] S. Chiose, Financial Services, your own body may be your best electronic shield Biometrics may solve security concerns as financial services increasingly go mobile. The Globe and Mail, October 2000

[CS] M. Ricknäs, Senseboard skriver utan tangentbord. Computer Sweden, November 2001

[DAH] K. Dahmström, Från datainsamling till rapport – att göra en statistisk undersökning. Studentlitteratur, Lund, 1996

[DAV] D.W.Davies & W.L.Price, Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer. John Wiley & Sons, second edition, 1997

[DYS] A. Dysart, Biometrics. EECS 598 University of Michigan, 1998

[GIMA] S.Giarimi & H. Magnusson, Olika betalningssätt för transaktioner över mobilt Internet, samt säkerhetsaspekter för dessa. DSV, SI2, 2001

[GIMA2] S.Giarimi & H. Magnusson, En studie av identifieringsmetoder för mobila tillämpningar. DSV, SI4, 2001

[GOL] D. Gollman, Computer Security. John Wiley & Sons, 1999

[IBM] N.K. Ratha, J.H. Connell and R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, Vol. 40, no. 3, 2001

[IBM2] R.M. Bolle et al, Biometric Technologies…Emerging Into the Mainstream. IBM Research Report, IBM Research Division, October 2001

[KOE] V. Koerper, Biometrics: A Brief Introduction. CSC 490 – Security Seminar, 1998

[LEWA] P. Lekwall, C. Wahlbin, Information för marknadsföringsbeslut. IHM förlag, 1993

[LIU] S. Liu & M. Silverman, A Practical Guide to Biometric Security Technology. IEEE Computer Society, 2000

[MARK] J.A. Markowitz, Voice Biometrics, who are you? Your voice alone can be used to verify your personal identity – unobtrusively and invisibly. Communications of the ACM, Vol.43. No. 9, 2000

[MEE] M. Meehan, Iris scans take off at airports. Computerworld, July 2000

[MeT] MeT WAP Banking, Version A. Mobile electronic Transaction, February 2001

[MSU] Fingerprint Identification. Pattern Recognition and Image Processing Lab, Dep. Of Computer Science and Engineering, Michigan State University

[ORK] Orkand Corporation, Personal Identifier Projekt: Final Report. State of California Department of Motor Vehicles report DMV88-89, reprinted by the U.S. National Biometric Test Center, April 1990

[POL] D. Polemi, Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable. Institute of Communication and Computer Systems National Technical University of Athens, 1997

[RAI] D. Raikow, The Myth of Fingerprints. The Biometricgroup/Smart Partner, March 2001

[RICH] E.P.Richards, Phenotype v.Genotype: Why Identical Twins Have Different Fingerprints. UMKC School of Law

[RJA] R.J.Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons, Inc. 2001

[RUG] T. Ruggles, Comparision of Biometric Techniques. For The California State Legislature, 1996

[SÄL] F & M. Sällström, Face Recognition. Umeå Universitet, 1996

Links:

[ASH] http://homepage.ntlworld.com/avanti

[BIOA] www.bioapi.com

[BIOC] http://biometric-consulting.com

[FING] www.finger-scan.com

[FAC] www.facial-scan.com

[FIN] www.fingerprint.se

[HAND] www.hand-scan.com

[IBM2] www.research.ibm.com

[IRCO] www.irco.com

[IRI] www.iris-scan.com

[LT] http://library.thinkquest.org

[MCM] www.mcmahonworldwide.com

[MEM] www.memogram.com

[NAT] www.national.com

[OTG] www.otg.ca

[PHI] www.symbions.org

[RET] www.retina-scan.com

[SEN] www.senseboard.com

Appendix 1: Glossary

Bluetooth	Short range radio standard for terminal to terminal connectivity. Can replace cables between terminals.
Enrolment	The initial process of collecting biometric data from a user and then storing as a template for later comparison.
GPRS	General Packet Radio Services: a packet data network in GSM that makes mobile Internet access faster and cost efficient for mobile terminals. The terminals can be online continuously.
GSM	Global System for Mobile communication: today's mobile network; most used system globally.
PTD	A personal trusted device is a device that both the user and the communicating party can trust.
SIM	Subscriber Identification Module is a Smart Card containing a chip with algorithms, functions and subscription data used in GSM and 3G mobile units for verification of a subscriber.
SMS	Short Message Service: text-based messaging used by mobile terminals in GSM.
Template	A mathematical representation of biometric data.
UMTS	Universal Mobile Telecommunication System: a third generation (3G) mobile systems providing much faster access to multimedia services including telephony and Internet.
WAP	The Wireless Application Protocol: the protocol used to browse the Internet using mobile terminals

Appendix 2a: Questionnaire (Swedish version)

Undersökning om användaracceptans

Allt som är skrivet i kursiv stil i rött förklaras i medföljande bilaga.

Födelseår:_____ **Kön:** ☐ man ☐ kvinna

1. Har du en mobiltelefon? ☐ ja ☐ nej, om nej gå till fråga 3.

2. Vad använder du mobiltelefonen till förutom att ringa? (flera kryss tillåtna)

☐skicka SMS ☐Wap ☐läsa/skicka email ☐annat_____

3. Använder du Internet? ☐ ja ☐ nej, om nej gå till fråga 5.

4. Vad använder du Internet till? (flera kryss tillåtna)

☐läsa/skicka email ☐ leta efter information ☐ handla ☐ lyssna på musik

☐ annat_____

5. Använder du någon annan *mobil terminal* än mobiltelefon?

☐ ja, vilken_____ ☐ nej

6. Om du skulle använda dig av en *biometrisk metod*, vem tycker du ska ha tillgång till ditt biometriska mönster? (flera kryss tillåtna)

☐ endast du själv eller

☐ du själv och ☐ tele/Internet operatör ☐ arbetsgivare/skola ☐ banken

☐ staten/landsting/kommun ☐ den du köper någonting från

☐ övriga_____

7. Skulle du kunna tänka dig att använda dig av en biometrisk metod (dvs istället för PIN-kod):

a) för att logga in på din mobila terminal? *(en till en)*

☐ ja, vilken/vilka: ☐fingeravtryck ☐röst ☐ögonbotten/iris ☐ signatur

☐ nej kommentar:_____

b) för att få tillgång till säkra sätt att skicka email? (en till en)

☐ ja, vilken/vilka: ☐fingeravtryck ☐röst ☐ögonbotten/iris ☐ signatur

☐ nej kommentar:_____

c) för att aktivera *tjänster* som gör det säkert att köpa/beställa något över nätet? (en till en)

☐ ja, vilken/vilka: ☐fingeravtryck ☐röst ☐ögonbotten/iris ☐ signatur

☐ nej kommentar:_____

d) för att aktivera tjänster som gör det säkert att utföra banktjänster över nätet? (en till en)

☐ ja, vilken/vilka: ☐fingeravtryck ☐röst ☐ögonbotten/iris ☐ signatur

☐ nej kommentar:_____

8. Skulle du kunna tänka dig att använda dig av en biometrisk metod (istället för PIN-kod/lösenord):

a) för att köpa/beställa något från din mobila terminal?
Alltså skicka ditt biometriska mönster krypterat över nätet för att bli identifierad i affärens/biografens etc. databas *(en till många)*

☐ ja, vilken/vilka: ☐fingeravtryck ☐röst ☐ögonbotten/iris ☐ signatur

☐ nej kommentar:_____

b) för att betala räkningar och utföra andra banktjänster från din mobila terminal?
Alltså skicka ditt biometriska mönster krypterat över nätet för att bli identifierad i bankens databas? (en till många)

☐ ja, vilken/vilka: ☐fingeravtryck ☐röst ☐ögonbotten/iris ☐ signatur

☐ nej kommentar:_____

9. Vilken identifieringsmetod skulle du vilja ha för att skydda personlig och viktig information (t ex email, koder, kontoinformation etc.) i din mobila terminal?

☐ PIN/lösenord ☐biometrik ☐spelar ingen roll ☐annat:_____

10. Är du villig att betala mer för att få en biometrisk identifieringsmetod i din mobila terminal istället för PIN/lösenord?

☐ ja, hur mycket mer?_____kronor ☐nej kommentar_____

11. Har du någonsin lånat ut din PIN kod eller ditt lösenord?

☐ ja, i vilket syfte åtkomst till: ☐ dator ☐ bankomat ☐ mobiltelefon

☐ annat:_____

☐nej

12. Övriga kommentarer:

_____
_____
_____
_____

Som tack för din medverkan är du med i ett lotteri, där priset är biocheckar.

Appendix 2b: Questionnaire (English version)

Investigation about user acceptance

Everything written in italics and red is explained in the appendix

Birth year:_____ **Sex:** ☐ male ☐ female

1. Do You own a mobile phone? ☐ yes ☐ no, if no go to question 3

2. What other services do You use other than telephony ? (several choices are allowed)

☐send SMS ☐Wap ☐read/send email ☐other_____

3. Are You using Internet? ☐ yes ☐ no, if no go to question 5

4. What are You using Internet for? (several choices are allowed)

☐read/send email ☐ searching for information ☐ shopping ☐ listen to music

☐ other_____

5. Are You using any other *mobile terminal* than a mobile phone?

☐ yes, which_____ ☐ no

6. If You should use a *biometric method*, who do You think should have access to Your biometric pattern? (several choices are allowed)

☐ only Yourself or

☐ Yourself and ☐ Your telephone/Internet operator ☐ Your employer/school

☐ Your bank office ☐ the government/the county council/the county

☐ whoever You buy something from ☐ other_____

7. Could You imagine using a biometric method (instead of PIN/password):

a) to log onto Your mobile terminal? *(one to one)*

☐ yes, which: ☐fingerprint ☐voice ☐retina/iris ☐ signature

☐ no comment:_____

b) to gain access to secure services to send email? (one to one)

☐ yes, which: ☐fingerprint ☐voice ☐retina/iris ☐ signature

☐ no comment:_____

c) to activate *services* that makes it secure to buy/order something over the net? (one to one)

☐ yes, which: ☐fingerprint ☐voice ☐retina/iris ☐ signature

☐ no comment:_____

d) to activate services that makes it secure to perform bank sevices over the net? (one to one)

☐ yes, which: ☐fingerprint ☐voice ☐retina/iris ☐ signature

☐ no comment:_____

8. Could You imagine using a biometric method (instead of PIN /password):

a) to buy or order something using Your mobile terminal?
Sending Your biometric pattern encrypted over the net to be identified in the store's/the cinema's etc, databases? *(one to many)*

☐ yes, which: ☐fingerprint ☐voice ☐retina/iris ☐ signature

☐ no comment:_____

b) to pay bills and perform other services using Your mobile terminal?
Sending Your biometric pattern encrypted over the net to be identified in the bank's database? (one to many)

☐ yes, which: ☐fingerprint ☐voice ☐retina/iris ☐ signature

☐ no comment:_____

9. Which identification method would You like to have to protect private and important information (like email, codes, account information etc.) in Your mobile terminal?

☐ PIN/password ☐biometrics ☐it does not matter ☐other:_____

10. Are You prepared to pay more money to have a biometric identification method in Your mobile terminal instead of PIN/password?

☐ yes, how much more?_____SEK ☐no comment_____

11. Have You ever lent your PIN code or your password?

☐ yes, in which purpose to get access to: ☐ computer ☐ ATM

☐ mobile phone ☐ other:_____

☐no

12. Other comments:

_____
_____
_____
_____

To show our appreciation You are a participant in a lottery where the price is cinema cheques.

Appendix 3a: Explanation to the questionnaire (Sw. version)

Bakgrundsinformation och förklaring till enkätundersökningen

Mobil terminal

En mobil terminal är mobiltelefon, laptop, handdator och liknande bärbara enheter med möjlighet att använda Internet.

Biometrik - metod och mönster

En biometrisk metod kan användas för att identifiera en person med hjälp av ett biometriskt mönster. Ett sådant mönster är unikt för varje människa och svårt att förfalska. Exempel på dessa är fingeravtryck, röst, ögonbotten och iris samt signatur dvs. handskrift.

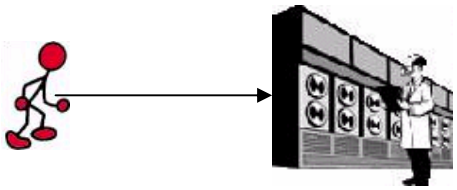
en till en

Det unika mönstret kan sparas i Din egen mobila terminal och då kontrolleras det bara att Du är Du och inte någon annan. Detta kallas en till en förhållande och innebär att det biometriska mönstret endast innehas av Dig, som ägare av terminalen. Vid inloggning jämförs det mönstret som lämnas då med det som redan finns lagrat. Om det är samma mönster kommer inloggningen lyckas, annars nekas Du tillträde.

Tjänster

Säkra överföringar av pengar, mail och information kan idag göras med olika tjänster som redan finns. Gemensamt för dessa är att åtkomsten till dessa tjänster kräver PIN eller lösenord. Ett alternativ till PIN eller lösenord skulle kunna vara en biometrisk metod. Exempelvis kan man tänka sig att man efter att ha loggat in med sitt biometriska mönster på sin mobila terminal automatiskt får tillgång till de olika tjänster som finns.

en till många



Mönstret kan också sparas i en databas, som kan ägas av t ex en affär, staten, banken etc, och då jämförs Ditt mönster med många andra för att kolla vem Du är. Detta kallas en till många förhållande och innebär att Du innan en jämförelse blir aktuell har lämnat Ditt biometriska mönster till tex. banken, staten eller någon som Du vill köpa tjänster eller varor ifrån. När jämförelsen görs lämnar Du ett nytt biometriskt mönster som kollas mot ett flertal mönster i en databas. Om mönstret överrensstämmer med något som redan finns, lyckas inloggningen och innehavaren av databasen vet vem Du är.

Hot biometri

Hot mot biometriska metoder finns även om det är mycket svårt att förfalska ett biometriskt mönster. Dessa hot uppkommer om någon obehörig får tillgång till ditt lagrade mönster.

Hot PIN/lösenord

Hot mot PIN kod och lösenord som finns är bla.att de är förhållandevis enkla att knäcka. PIN-koder/lösenord kan också vara svåra att komma ihåg. Detta leder ganska ofta till att man skriver ned dessa koder/lösenord vilket gör att andra lätt kan få tag på dem. Det kan också leda till att man använder sig av samma kod till alla kort/tjänster.

Appendix 3b: Explanation to the questionnaire (Eng. version)

Background information and explanations to the questionnaire

Mobile terminal

A mobile terminal is a mobile phone, a laptop, a personal digital assistant (PDA) and other mobile devices that includes Internet access.

Biometrics - methods and patterns

A biometric method can be used to identify a person with the help of a biometric pattern. A biometric pattern is unique for every human being and is very difficult to forge. Examples of patterns are: fingerprint, voice, retina and iris and also signature, that is handwriting.

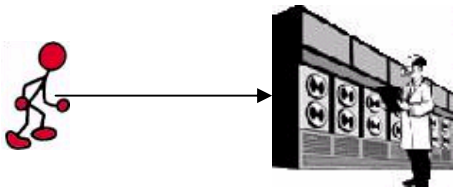
One-to-one

The unique pattern can be saved in Your own mobile terminal and in that case there is only one check that You are You and nobody else. This is called a one-to-one relationship and it means that the biometric pattern is owned by Yourself, as a owner of the terminal. When You log on, the pattern given is compared to the pattern that is stored in Your device. If there is a match, You are granted access, otherwise access is denied.

Services

Secure transactions of money, mail and information can today be done with existing techniques. Common to these techniques is that access to them requires a PIN or a password. An alternative to PIN:s/passwords could be a biometric technique. For instance after logging on to Your device with Your biometric pattern You should automatically get access to those techniques.

One-to-many



The pattern can also be stored in a database, that is owned by a store, the state (government), the bank, etc, and in that case Your pattern is compared to many others to check who You are. This is called a one-to-many relationship and it means that You, prior to a comparison have given Your biometric pattern to the bank, state or any other organisation/person that You want to buy services or merchandise from. When the comparison is made You leave a new biometric pattern that is compared to several others in a database. If there is a match, the login is successful and the owner of the database knows who You are.

Threats - biometrics

Threats to biometric methods exist even if it is very difficult to forge a biometric pattern. The threats occur when an unauthorised gets access to Your biometric pattern.

Threats – PIN/password

Threats to PIN:s and passwords are that they are considerably easy to crack. PIN:s and passwords can also be hard to remember. This often leads to the fact that owners very often writes these codes down, which makes them easy to get access to. It can also lead to the fact that many people use the same code to all cards/services.