BIOMETRIC-SMART CARD SYSTEM FOR AUTHENTICATION IN ELECTRONIC TRANSACTIONS

M. Şt. VLAD[1], V. SGÂRCIU[2]

Lucrarea de faţă îşi propune să prezinte un sistem integrat dezvoltat pentru obiective de înaltă securitate, cum ar fi: zone de apărare naţională, nucleară sau alte puncte critice. Sistemul de identificare personală automată beneficiază de capacităţile de securitate ale smart card-urilor, precum şi de caracteristici specifice fiecărui utilizator. Acestea din urmă pot fi: amprenta, retina sau alte elemente faciale.

Aplicatia de identificare personala va fi inglobata in cadrul unui sistem de control al accesului. Scopul acestei aplicatii este de a limita accesul personalului neautorizat intr-o locatie de inainta securitate, bazat pe drepturile de acces ale fiecarei persoane.

This paper presents an integrated system developed for high security objectives, such as: defense locations, nuclear or critical ones. The system for automated personal identification will benefit from the smart card security features and from a user specific identification components. These may be: fingerprint comparison, retina scan, or key facial elements.

Personal identification application will be embedded with an access control application. The purpose of this application is to limit the access of unauthorized personal to a high security location, based on access rights of different persons.

Keywords: Smart Card, Multi-application Concept, Java Card, Access Control, Automatic Personal Identification

1. Introduction

The problem of personal identification in the Digital Era has many aspects and many developments. Most of them are based on secure authentication, authentication over secure channels, and the physical ways of implementing these concepts are web servers, smart cards, and biometrics and so on.

The main concepts involving digital identification are based on several principles, such as:

- who you are,

[1] PhD Student, Faculty of Automatic Control and Conputer Science, University "POLITEHNICA" of Bucharest, e-mail:madalinv@ac.pub.ro,

[2] Prof., Faculty of Automatic Control and Conputer Science, University "POLITEHNICA" of Bucharest, vsgarciu@aii.pub.ro

- what you have,
- what you know.

Smartcards and biometrics by themselves each provide a considerable boost to the Identification and Authentication (I&A) mechanism of any system. Together, they can provide a comprehensive solution of the three principles described above A common understanding of the underlying technologies is required to fully grasp how each component contributes toward a comprehensive I&A solution.

The advantages of using a biometric for identification are obvious. Each of us has forgotten our password and, in an effort not to forget it the next time, written it down, or chosen one that was easy to remember. In essence we have undermined security for the sake of convenience. The use of biometrics changes all of this. Instead of using what we know to prove who we are, we use some unique feature of ourselves such as a fingerprint, handprint or the sound of our voice. A world that replaces a memory test with a fingerprint scanner is quiet attractive, and there are numerous devices available today that provide secure access based solely on a biometric

2. Automated information systems

The use of biometrics and/or smartcards must work in tandem with some form of Automated Information System (AIS) to meet a minimum level of assurance. Whether it is a workstation on a desk or an embedded system within a vending machine, strong user authentication is based on proper integration of the separate components. Use of these systems requires that it is trusted to perform the operations desired and only those specific operations. An example would be that a vending machine is expected to only debit a stored value application within a smartcard and not attempt to digitally sign legal documents. “Trust” in an AIS is earned when the AIS’s functionality is perceived to be correct with respect to an established security policy. Use of a robust multi-application smartcard with the appropriate security features can help mitigate risk when using an AIS of questionable origin.

There are several ways to establish different levels of trust in an AIS. One method is to use a Trusted Operating System (TOS). A TOS has been verified to perform correctly and if a failure occurs, it will fail safely, so that no restricted information is compromised. Verification methods of this trust include testing and formal mathematical analysis. Other less stringent methods to gain trust in a system can include physical isolation (no network or dial-up connections), purchasing products through trusted vendors, and of course physical security to prevent tampering.

The level of trust in an AIS required for a specific application is dependent on the value of the information at risk. An AIS restricting access to a classified room should not be connected to the Internet. Ensure that the platform used for your application really is “trustworthy”.

3. Biometric authentification

Users’ identities are verified using one or more of three generic methods (types): something they know (PINs, passwords, memory phrases, etc.), something they have (a physical token such as a magnetic stripe card, a physical key, a smartcard, etc.), or something they are (biometric verification). If this information is gathered by a trusted process, verified, and then signed by a trusted authority, it can be considered as trusted authentication information (AI).

Biometrics are methods of measuring the inherent physical attributes of an individual. This is usually performed in order to identify an individual or to verify a claimed identity.

In the first case, a “livescan” is provided, and a database of templates is searched to determine who the scan is associated with. In the second case, a template is provided with the livescan for a direct comparison.

There are many different types of biometric attributes to identify users. They may be based upon fingerprints, hand or facial geometry, retinal or iris patterns, or even speech recognition. Each of these technologies can be obtained from multiple sources, with different algorithms and techniques for storing an individual’s features and/or comparing a “livescan” of an individual’s features to the previously stored record. The stored record is typically referred to as the “Biometric Template”. Biometrics can be best characterized as an emerging technology.

These various methods and data formats provide a challenge for those who would like to use multiple biometric systems or prevent themselves from becoming dependent upon a single proprietary solution. One solution is to wrap these proprietary interfaces and data formats with a standard interface or data format, much in the same way that the Internet uses IP (internet protocol) to wrap all of the various application data into standardized packets to provide seamless connectivity worldwide. This is the approach proposed, using certificates as the standard format.

4. Fingerprint identification

In fingerprint identification there are several aspects that must be taken in consideration, such as: fingerprint matching, enrolled image, acceptance/rejection rates or template storage, detailed below.

4.1 Fingerprint matching

Fingerprint matching determines whether two fingerprints are from the same finger or not. Many fingerprint verification methods have appeared in literature over the years. In general, the two most significant features used in fingerprint matching are ridge ending and ridge bifurcation called minutiae. The algorithm used in minutiae comparison requires a specific mode of storing features, using polar coordinates, which also brings the advantage of reducing the memory space needed. The parameters are:

- *x and y coordinate* of the minutia point
- *orientation*, defined as the local ridge orientation of the associated ridge.
- *type of the minutia point*, which is whether the minutia is ridge ending or ridge bifurcation.
- *associated ridge*.

4.2. Enrolled Image Quality

Enrollment quality is very important to achieve high operational performance. Some enrollment applications have advanced feedback dialog messages which provide useful information about poor quality scans, be it fingerprint, facial or speech. There should be a good balance between the feedback mechanism of the enrollment software and the understanding of acceptable quality by the enrollment officer.

4.3. False Acceptance/False Rejection

The False Acceptance Rate (FAR) is the rate at which an intruder can be recognized as a valid user. Many vendors quote the false acceptance rates of their devices, typically generated through mathematical extrapolation of field trial data. As a result, it's difficult to compare these technologies based on vendors' quoted FAR numbers. But it's important to remember that during user verification (a one-to-one match), false acceptance is based on imposter attempts, not on the total number of attempts by valid users. If the FAR is 1 percent, that means one out of 100 users trying to break into the system will be successful.

The False Reject Rate (FRR) is the rate at which a valid user is rejected by the system. A 1% FRR would imply the average user would fail every hundredth time. However, it is more likely that only a few individuals may fail a lot more often. These individual may be conduits for a secondary verification mechanism. Many systems, such as the fingerprint-recognition devices, may be tuned to do less strict checking at the expense of opening the system. Administrators have to

balance false acceptances versus false rejects, the possibility of fraud versus user convenience.

One method for reducing the false rejects is to use more than one template for verification. The ability to use different fingers for verification can be simply achieved by storing multiple user fingers on the smartcard.

4.4. Template Storage

Although the biometric template typically cannot be used to create an image or physiological attribute of the user, the template still is sensitive data. The digital representation of what the reader detects should be encrypted where it's stored, and protected storage locations such as smartcards can improve overall security. The size of the template may be a factor. Most fingerprint and iris templates require between 256 bytes and 1 KB per user, though some systems need up to 8 KB. Face-recognition systems can require up to 3.5 KB per user too large for some smartcards.

5. System risks due to the smartcard

The risks of frauding the system are imminent, and they appear due to smart card. But the application or the data on the smart card have the same risk of being copied or altered as the other application stored there.

The specific sensitive data placed on the smart card will consist of:

- Private signature key of the user.
- Private key exchange key of the user
- The authentication certificate
- Other sensitive information such as account balances, security codes, etc.
- The data on the smart card can be lost in the following ways:
- Physical attack on the smartcard
- Incorrect implementation of an algorithm
- Back doors and implementation flaws due to poorly designed/test implementation of the smartcard.
- Placing a “Trojan Horse” application in the host PC to capture I/O information
- Tapping the line between the host and the smartcard
- Providing a bogus host to capture the information from the smartcard

To break a smart card it is a must to break the private key. Most smartcards do not allow private keys to be obtained directly from the interface. The most likely way of obtaining the private key is via a physical attack.

6. Structure of the application

We propose an integrated system for automatic identification, using smart card and fingerprint features. The goal of the application is to do both a biometric verification and identification, with the personal data stored on the smart card.

In this way, the first important step is considered to be the enrollment. Therefore, a new user, who will be involved in the system, comes to an authority and gets his finger scanned for several times (usually 3-5 times), in order to get the best fingerprint. From the images captured by the biometric sensor, the features are extracted, and the best feature string, with maximum number of minutiae will be stored on the smart card.

The algorithm of extracting minutia for enrollment phase is similar with the one used either in verification or in identification. Sending and storing the minutiae string on the smart card are done in a secure way, with several mechanism of authentication, in order for the personal data to be perfectly protected.

After the enrollment has been successfully done, the used has the ability of using the system for further verification, such as access control or personal identification.

The use of the system permits, as mentioned above, two actions to be undertaken: identification and verification. Depending on the specific type of comparison, there are several modules in the application that interact with each other, as in Fig 1.

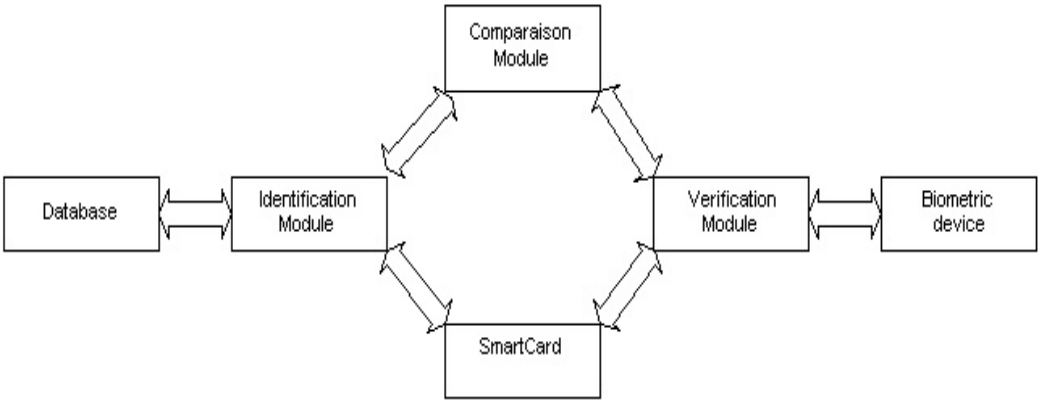

Fig.1. The modules of the integrated system

In development framework, two subsystems were considered:

- on-card application, which stores the minutiae string, and have several methods for restricting access to them
- off-card application, the client part of the system, responsible for several activities, such as:
  - establish secure connection and communication with the smart card
  - establish secure connection and communication with the database
  - reading information from the biometric sensor
  - comparing the minutiae string

The application runs on an experimental embedded system, formed by specific components:

- Computer: Pentium III, 1,2 GHz, 384 Mb RAM
- Biometric sensor: Digital Persona U.are.U 4000, 500 dpi
- Smart card reader: Gemplus GCR 410, Serial Connection
- Smart cards Gemplus GemXpresso PK 211, with 16 KB RAM

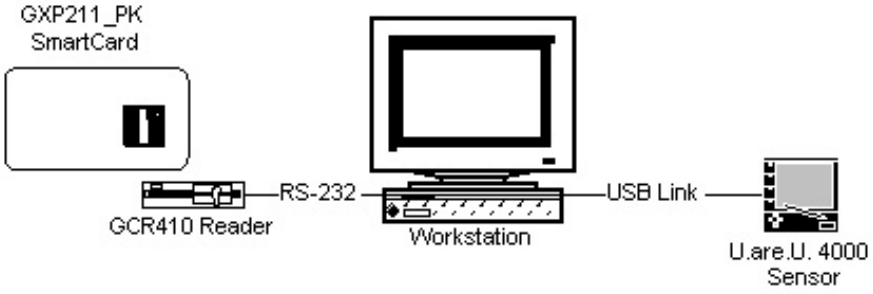

Fig. 2. The integrated system

Software used consists of the development environment, which was Borland Java Builder 4.0, with Java JDK 1.3. On-card application is written using Java Card 2.1.1 and Open Card 2.0.1 standards and it is compliant with OCF and Visa Open Platform. Communication with smart card was ensured by libraries developed by Gemplus and included in the Gemplus RAD III package, while the capture and the process of the fingerprint was done with VeriFinger 4.2 package from Neurotehnologija. The database used in identification part of the application was developed in Microsoft Access XP.

7. Client application

As mentioned above, from user point of view, the client performs two actions: verification and identification.

For experimental reasons, there is only a single application, which can perform the two types of identification. From the menu it can be chosen what kind of action it will do.

7.1 Verification System

Verification is used mainly for access control into specific location. The system, through the both subsystems – the biometric sensor and the smart card reader, waits for an external event. When one is produced, the user is prompted for the complementary action. After the two conditions were satisfied, the computer side applications starts to extract the minutiae from the image acquired through the U.are.U sensor. This step is performed using the VeriFinger methods. The steps of the application can be seen in Fig. 2.

Upon extraction of the fingerprint features, the minutia string stored on the smart card is read. Then, the two strings are compared, and if a percent of matching is met, the access is granted, otherwise is denied. The percent of matching, called threshold can be established within the program, depending on the FAR/FRR rate required at the specific location where access control takes place. If we want to use the system for a security objective, the typical threshold is 85%, which is the usual in biometric identification system. For improvement of security, a higher threshold can be set, which means that more minutiae must be extracted from the image acquired from the biometric sensor, when a user wants to authenticate. That procedure usually involves many retry of user fingerprint read, because the image is altered by external factors, such as dust, wet, or degrading of the fingerprint, due to a hard work.

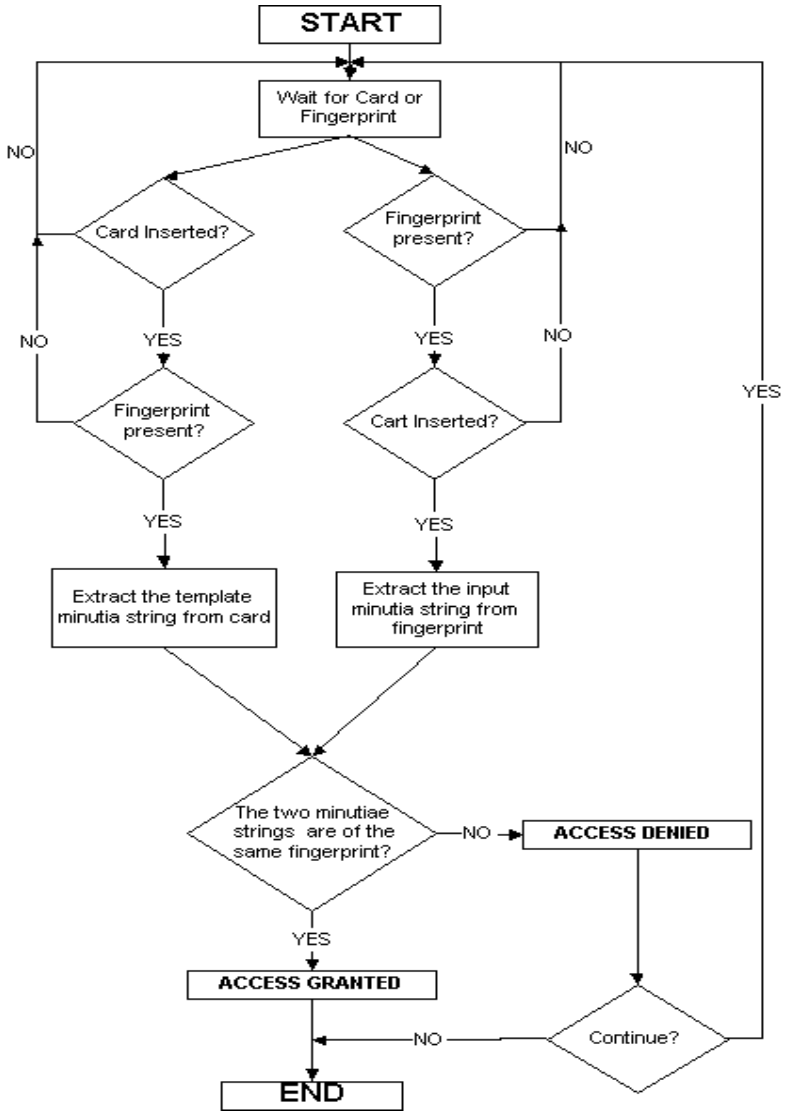

Fig.3. The verification steps of the application

7.2 Identification

The identification part of the application performs several steps, in order to find an owner of a card in the database. First of all a verification is done, in order for the user to be authenticated towards his card.

Application is connected to a database, where personal detail of a user are stored. The details include fields like: Name, Address, etc, and also a picture of

the user. Upon successful completeness of the user fingerprint verification towards his/her smart card, the channel to the smart card is closed. The minutia sting took from the smart card is already stored in a variable inside the program. This string is searched in a database, and if found, a window with his/her personal data is shown.

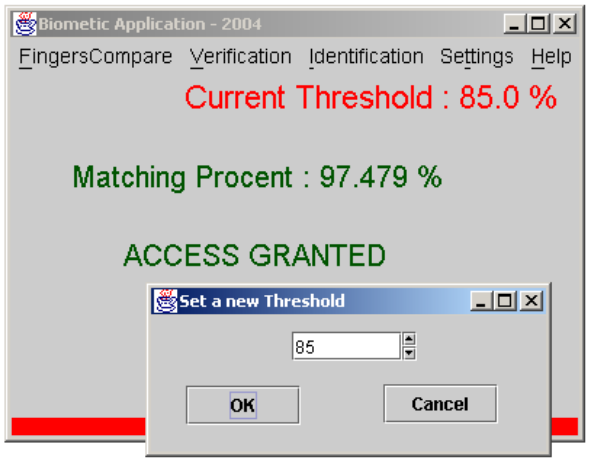

Fig. 3. The main window of the application.

8. Conclusions

Biometric identification is preferred over the traditional methods because the person to be identified is required to be physically present at the point of identification and also identification based on biometric techniques obviates the need to remember a password. Along with a smart card, there can be designed access control systems which can have a higher immunity to frauds.

In embedded systems, based on biometrics and smart cards, the personal features can be used in authentication to the smart card. In this way, better security to smart card stored data is provided, compared with the current security, provided by a PIN number, who can be easily subtracted.

REFERENCES

[1]. *Zanero, S.* Smart Card Content Security, 2002
[2]. *Pankanti, S., Prabhakar, S., and Jain, A.* On the individuality of fingerprints. IEEE Transactions on PAMI 24, 2002
[3]. *Hendry, M.* Smart Card Security and Applications, Second Edition, Artech House, 2001
[4]. *Davida, G., Frankel, Y., and Matt, B.* On enabling secure applications through off-line biometric identification, IEEE Symposium on Privacy and Security, 1998.
[5]. *GSA Government Group*, Guideline for placing biometrics in smart cards, 1998
[6]. *Zhang, W., Wang, S. and Wang, Y.* Structure matching algorithm of fingerprint minutiae-based on core point, 2003