[www.reciis.cict.fiocruz.br]
e-ISSN 1981-6278

Original article

An application of biometrics in the web regarding health insurance

DOI: 10.3395/reciis.v4i5.333pt

Antonio Idelvane Santana Silva
Federal Institute for Education, Science and Technology of Piauí (IFPI); Infoway E-Health Co., Teresina, Brazil
idelvane@infoway-pi.com.br

Ney Paranaguá de Carvalho
Federal Institute for Education, Science and Technology of Piauí (IFPI); Infoway E-Health Co., Teresina, Brazil
ney@infoway-pi.com.br

Pedro de Alcântara dos Santos Neto
Departamento de Informática e Estatística (DIE), Federal University of Piauí (UFPI), Teresina, Brazil
pasn@ufpi.edu.br

Abstract

Biometrics is being increasingly adopted to identify people. It allows you to identify someone through physical traits (iris, fingerprint, face) or through other singularities (voice, signature). In order to identify individuals, it can be used in several ways.The Web is now one of the main focuses of biometrics. Creating a Web biometric system requires detailed study of such platform. Security, usage, and customer environment issues must be taken into account from the beginning of the project. This paper provides an overview of how a Web biometric system works, with an approach to the technical and operational aspects of its implementation and deployment. In addition to that, we present a case study of biometrics solution for a health insurance plan which is managed through the Web, as well as a general overview of how it has been deployed.

Keywords

biometrics; health insurance management; computer system; authentication; Web biometric system

Non-funded research. Period: from June to December 2009. No need for approval by the Ethics Committee. There are no conflicts of interest. There are no randomized controlled trials or clinical trials. This work has been supported by Infoway Consultoria e Soluções em Tecnologia para Gestão de Saúde.

Internet popularity has increased the number of services offered on this type of platform, and that has increased even more the need to identify and authorize access to people. Many web applications need to keep their information or services secure. In order to do so, a wide range of techniques are being developed to keep such systems more secure. Common techniques used for identification have shown some problems, such as the use of passwords being subjected to the interception of others, and also issues related to sharing or forgetting. Although such techniques have been highly developed, they do not guarantee total assertiveness of one's identity, because they present weaknesses. Due to such weaknesses, the concept of biometrics is being increasingly spread, including in web systems.

Biometrics compromises methods of recognizing humans based upon physical traits, such as iris, and fingerprint, or behavioral traits, such as voice, and signature (COSTA, 2001). Biometrics authentication occurs in two stages: on the first stage, the user's biometric trait is captured so it can be used in his or her authentication. After it has been captured, the user's trait is converted into a mathematical model, known as template, which is then submitted to authentication. On

the second stage of biometrics authentication, the user's biometric trait is compared and validated as a stored template.

Biometrics utilization in web systems requires detailed study of the platform's peculiarities.

- Performance – refers to how fast someone's authentication is made, through the transmission of the individual's information data.
- Usability – a good interface is crucial for a web application that uses biometrics, because this functionality cannot add more complexity to the system. A concise and interactive interface is an alternative for this issue.
- User environment – customer environment restrictions must be analyzed. Conducting a survey on which the operating system and hardware applied to the user, in order to avoid incompatibilities with the software used to recognize biometric traits, is extremely useful for the biometric system deployment process in the web application.

Biometrics in the context of Web has several types of applications (COSTA, 2007). On this work we present an approach to a health insurance plan system. For this purpose we developed a Java web application that seeks to meet the requirements of this platform as well as the needs of the health plan that has been developed. This project is sectioned as follows: on Section 2 we present the main concepts of biometrics, on Section 3 we describe a detailed manner of implementing biometric solution for a web platform, on Section 4 there is a case study of how to use biometrics in an application for a health plan on the web; Section 5 relates to future work and Section 6 conclusion.

Biometrics

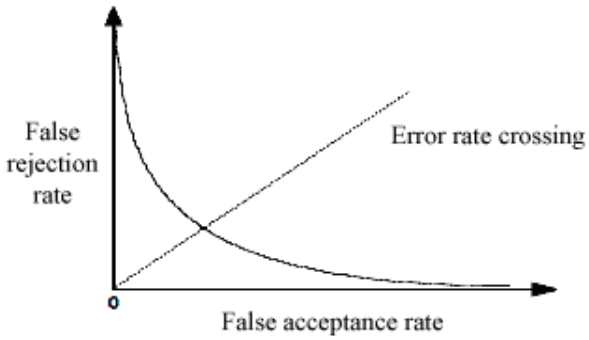
Biometrics refers to authentication techniques that rely on the use of individual traits to access information data systems (LIU *et al.*, 2001; JAIN *et al.*, 2008). With biometrics the individual becomes his own authentication mechanism. Through biometrics, there are two ways of identifying a person.

- Verification: it is a biometric process that verifies the effectivity of someone's identity. In other words, it can be defined as a one to one comparison process (1:1) of a captured biometric with a stored template to verify that the individual is who he claims to be. For instance, someone's right thumb fingerprint is digitally captured. In the verification process, he uses his right thumb fingerprint to compare to that which has been previously stored. As a result, there could be two responses: yes, this is him, or, no, they are two different people.
- Identification: is the biometric process that identifies people through their biometric traits against a previously registered database. It is a one to many comparison (1:N) of the captured biometric against a biometric template database in attempt to identify if an unknown individual belongs to such sample. As a result, there could be only one response: a validated individual from the provided template. The identification process may be slower than the verification process since it requires the comparison with many other registered templates.

Nowadays, there are several characteristics that are used separately or in groups to verify or authenticate an individual. Each method can be accessed through several parameters: degree of reliability, comfort level, level of acceptance and implementation costs.

Degree of reliability refers to how reliable the biometric authentication method is. It can be measured taking into account the false accept rate - FAR or false match rate - FMR, which measures the percent of invalid inputs that may access the system, and the false rejection rate - FRR, or false non-match rate - FNMR, which measures the percent of valid inputs which are incorrectly rejected. However, these variables are mutually dependable, and it is not possible to reduce the value of both. Thus, there is a need to find a balance point called Crossover Error Rate - CER (LIU *et al.*, 2001). The lower the CER, more precise is the biometric system. Figure 1 shows the relation of the variables that define the degree of reliability in a biometric authentication technology.

Figure 1 – Error rates associated to biometric systems.



Source: KAZIENKO, 2003

The comfort level is a subjective measure of how practical the chosen technology for biometric authentication is.

The acceptance level, which is also a subjective measure, regards the level of intrusion. A biometric system will be more acceptable however less intrusive it may be.

The implementation cost refers to the whole structure of hardware, software and people (software engineers, and staff), involved in the process of biometrics deployment in a given system (LIU et al., 2001).

Biometric Authentication Technologies

Face recognition

In order to recognize someone's face, the systems study the geometry and the proportions of the face. Later, facial landmarks are extracted and registered, so the proportions, distances, and shapes of each feature can be defined – mouth, nose, eyes, eyebrows, etc. Then it is possible to make the necessary comparisons (VIGLIAZZI, 2003). The main analyzed measures are:

- the distance between the eyes;
- the distances between mouth, nose, and eyes;
- the distances between eyes, chin, mouth, and hair line.

In facial recognition, the problems are essentially caused by different orientations of the individual's head, once it is freely positioned (POH et al., 2001).

Iris scan

Iris has several features that may be used for biometric recognition. The main features are related to the complexity of its tissue image and its radial form. This radial form spans 266 degrees-of-freedom, number of variations that allow different irises to be distinguished (VIGLIAZZI, 2003). The iris is covered by the cornea, that protects it from tissue damage, and also, the iris is not subjected to the effects of aging, thus it maintains a lifetime steady biometric pattern.

Voice recognition

Biometrics authentication through voice recognition is based in the fact that the physical traits of an individual entails to the singularity of the human voice as a feature. The most relevant physical aspect is the vocal tract which is made up by all the organs and cavities that articulate speech production (MAGALHAES, 2003).

The sound of the voice is captured through a microphone. Therefore, the user is supposed to recite some sort of pass phrase in the microphone, and repeat it until a harmonic pattern is extracted and stored. Speech patterns in different moments result in similarity, but they have different feature vectors.

Digital fingerprint

Fingerprints are impression on a surface of the curves formed by the ridges on a fingertip, on hands and feet. They are found on the dermis (the deep vascular inner fundamental layer of the skin, located in the epidermal), and they reproduce in the epidermis (the thin, transparent membrane that covers the dermis), generating several patterns (VIOLA, 2006).

The method that allows the identification of people through the comparison of fingerprints is called dactyloscopy. The term dactyloscopy comes from the Greek words: *"Daktylos" meaning "finger" and "skopein" meaning "to examine", suggesting therefore that it is the examination of fingers, or fingerprints (VIOLA, 2006). Regarding its constitution, the lines that compose the fingerprint may be said to be parallel lines, considering a certain orientation, and if we analyze local neighbor ridges from a given point. Such incidental details caused by local perturbations of the lines are called minutiae (REIS, 2003).* Figure 2 shows different types of minutiae used throughout the fingerprint recognition process.

Figure 2 – Different types of minutiae

A = Ending, B = Island, C = Spur, D = Lake, E = Short ridge, F = Bifurcation.
Source: REIS, 2003.

The minutiae are used as parameters for most algorithms that compare fingerprints and do not change throughout the individual's life, unless the finger is badly damaged in a way that the epidermis or dermis is compromised. The peculiarities of fingerprinting are extracted by a reader and stored for further comparison (VIGLIAZZI, 2006). The comparing process, called matching, verifies the degree of similarity among the characteristics extracted from the user's sample and the previously stored profile. This process will generate a score that represents the similarity between the two data sets. If there is more similarity than a previously established limit, known as threshold, the decision is to authorize access to the user, in other words, the authentication has been validated. However, if there is less similarity to the threshold, the user should not be granted access (REIS, 2003).

Recognition through fingerprint is the most common and most used biometric process nowadays. The main reasons for that are (COSTA, 2007):

- Reliability: the possibility that it will fail is minimum, once each individual has a singular fingerprint feature;
- Low cost: fingerprint readers are cheaper when compared to readers of other technologies;
- Low intrusive level: it only requires that the user press the fingerprint reader (biometric reader or scanner);
- Familiarity: for many years people have been collecting fingerprints for several other purposes, which makes it more acceptable when used for authentication.

Authentication in web systems

When any web-based application is being developed, it is necessary to consider security in first place. Different mechanisms were created as a way of making sure the application was going to be secure. Among them, the most common one was the use of passwords and/or key-words for the authentication of people (COSTA, 2007). When the user informs his or her access password and/or key-word, the information is compared to a database entry and then validated. The process of authentication through the use of passwords may fail for several reasons, for instance: password theft, weak passwords, bad management of passwords (with no concern that others may use them).

Another method of individual authentication is through the use of smart cards that are able to identify the user through a chip with an embedded microprocessor. The smart cards have instructions that are able to identify a user through a Personal Identification Number - PIN (MAGALHAES, 2003; FERREIRA *et al.,* 2006). However, there are problems regarding the security of the process once smart cards can be cloned or stolen.

Biometrics applied to web systems is a more secure method compared to previous ones when used appropriately. Biometrics is a great approach to be used in the validation of users in a web system, because the cost to forge any physical or behavioral human trait is too high.

Biometrics for web systems

During the development of the biometric system for a web application, it is important to consider issues related to performance, usability of application, and adverse conditions in the final user environment. During the development of the web there are two technologies that enable the development of a biometric-based application: *ActiveX* (FARRAR, 2001) and *Applets* Java (DEITEL 2005).

ActiveX is a Microsoft specification that allows regular Windows programs to work within a web page, ActiveX programs can be written in Visual Basic, and Visual C++, for instance. It is present on the server's side as well as on the client's side in a web application. The components written for *ActiveX* are executed with the client and they have some access privileges to hardware and software resources.

ActiveX allows you to create web pages with active content, which interact with the end user. They have a wide variety of previously developed components that can be integrated easily with other web applications and they have two major advantages: 1) the downloading of ActiveX components happens automatically, but this process occurs only once, 2) its components have access to resources of the Windows operating system on the client, allowing the use of various software and hardware features. The direct access to such resources facilitate the integration between the hardware that is being used to read the biometric trait and the web application that uses ActiveX.

End user direct access to the Operating System (OS) is also a great disadvantage to the ActiveX, since it is not

completely secure against attackers. In order to do so, a code is intentionally generated to be executed while an ActiveX component is in action. That way, programs can be written with the intention of erasing data from the client's Hard Disk (HD) or even with the intention of formatting the computer. Another disadvantage regarding *ActiveX* is that it is particular for Microsoft Internet Explorer, therefore it is hard to perform the portability of the applications developed with this technology.

The other possible technology to implement a web system is based on Java applets. An applet is a special kind of program that is downloaded from the Internet and runs on the end user's browser application. It is typically embedded in a webpage. Unlike ActiveX components, applets do not have permission to access the resources of the client's machine easily, since they run separately from the other browser processes through a mechanism called sandbox (DEITEL *et al.,* 2005). The sandbox refers to the set of security restrictions imposed on the applet. It was made to prevent the actions of potential harmful code that can be run on the client's computer.

One of the advantages of having an applet as technology employed for a system that uses biometrics is that they, being developed in Java, are multiplatform, and have a high level of security, features of the language. However, the applet's have some disadvantages: 1) they have great difficulty to suit the needs of applications with more elaborate interfaces (Rich Internet Applications - RIA), due to, for example, poor performance at startup (DEITEL *et al.* 2005); 2) every time the page is loaded, the applet must be downloaded, because they do not remain in cache; 3) because it is executed in the sandbox, the applet is unable to access the file system or start some process on the client, however you can grant access to certain resources through signature using a digital certificate.

Implementation

Throughout the development of a biometric system, a tool kit is normally used (Software Development Kit - SDK) for capturing and to match the patterns of a given biometric technology. In this present work, a Griaule Biometrics software called Fingerprint SDK (Software Development Kit) 2009 was chosen to be used (GRIAULE, 2009).

Fingerprint SDK 2009 is offered in two versions: Fingerprint SDK for Windows that supports multiple programming languages via Windows Dynamic Link Library (DLL), or ActiveX, and Java Fingerprint SDK that enable the development of Java software platform with access to biometric devices. Communication with the biometric reader occurs through libraries that must be installed on the client's machine. Such libraries are easily installed by running installers created for both Windows (Fingerprint_SDK_2009_Installer.exe) and Linux (Installer Fingerprint_SDK_Java_2009_. Jar) (GRIAULE, 2009).

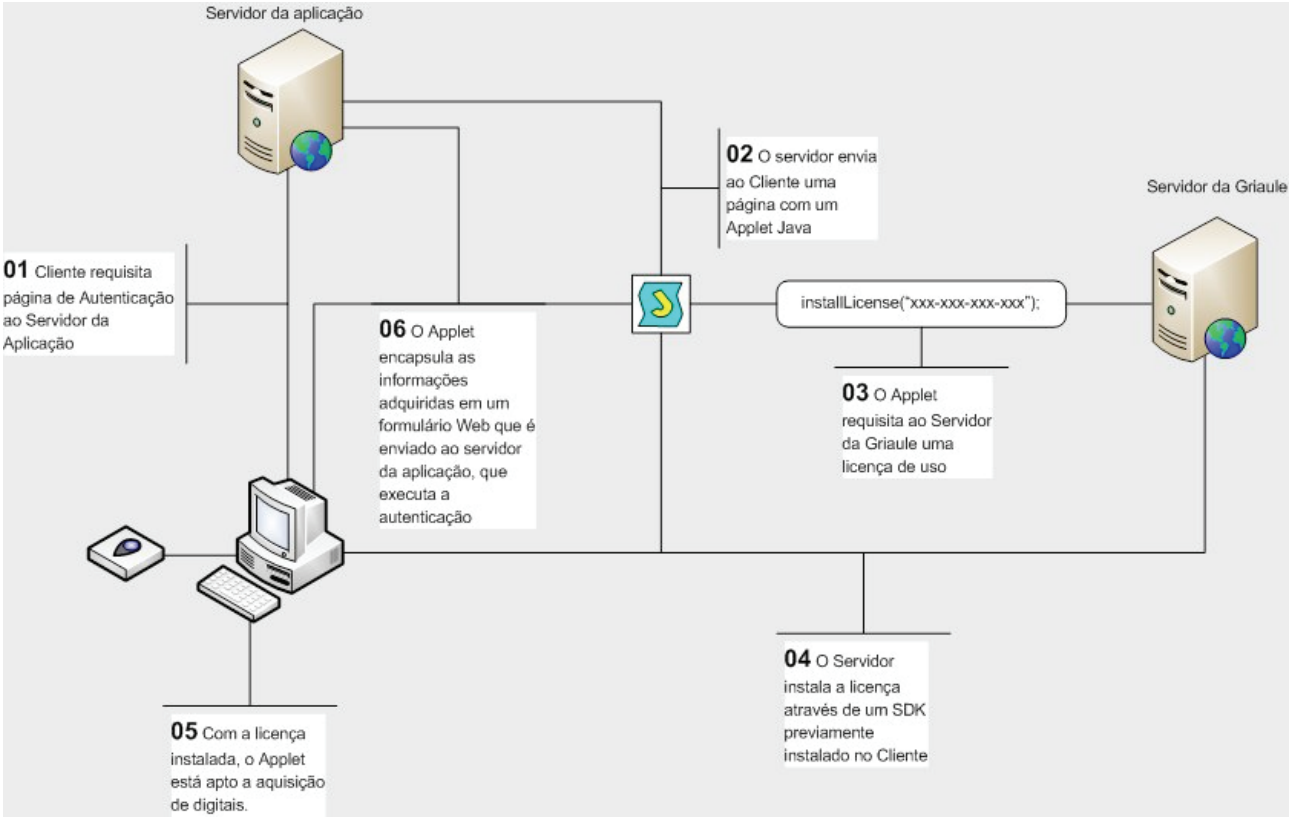
Another important feature of SDK is that it provides communication with a reasonable number of biometric readers, reducing costs for the client.

There are two ways of integrating the tool with a Web application developed in Java (GRIAULE, 2009):

- The client sends the digital image converted to a byte array, which was captured by the applet to the server, which owns the application that actually uses SDK. This application deals with the fingerprint that has been received, for instance: it stores it in database, compares with others that were previously stored, and extracts the template (calculates from the digital image), etc.;
- The second option is to leave the whole recognition process to be executed by the applet. It will perform the capture, template extraction, and comparison of fingerprint, only by accessing the server's database. This method has drawbacks, because the database needs to be visible to the client and the applet must have access permissions on the client machine, as opposed to the first option where only the server needs to be visible.

The first option was chosen because it offers greater security (it does not expose the server) and it requires less compromise with the clients' computers. To prevent problems when running the applet, it is necessary that the Java file (Java Archive - JAR), containing the classes of the SDK that communicates with the biometric reader, is "signed" with a digital certificate, in the public and private key model, to ensure its originality, and to guarantee security (DEITEL et al., 2005). The jar can be signed through keytool, which is included inside Sun SDK (DEITEL et al., 2005). If the application has commercial purposes, it is necessary to hire a certifying agent to purchase a certificate for the applet.

Figure 3 – Authentication/licensing process.



01.The client requires authentication page to the application server. 02. The server sends the client a page with a Applet Java. 03. Applet requires to the Griaule server a utilization license. 04. The server installs a license through a SDK previously installed on the client. 05. Now that the license has been installed, the Applet is able to acquire fingerprints.
Source: Prepared by the authors

Figure 3 shows how the authentication/licensing process works. Upon loading the applet, the licensing of the client's computer is done by the SDK, in order to do so, it accesses Griaule Web server and generates a licensing file for the client's computer. After that, the applet triggers the reader that captures the fingerprint in an array of bytes. The captured fingerprint is submitted to the application server via a web form. Once you have the information that has been captured, you can perform template storage operations in database or compare with an existing record.

Deployment

During the bibliographic development there were no references that showed the deployment process of a biometric system to web platform. This fact demonstrates the importance of this work for its innovative character.

When deploying Web application that uses biometrics, the aspects listed below must be observed:

Submit a template captured by postback - postback is the measure taken by an interactive website where the page and its contents are sent to the application server for processing information, and the same page is returned as a result (DEITEL et al., 2005). This mechanism improves applet communication as a server without the interception of data that has been collected. It is necessary because there are barriers created on the client's computer to hinder the sending and / or receiving unauthorized information, an example of that are firewalls.

Making interface interactive - one of the most important aspects to be taken into account in developing a web application is the user interaction. After capturing the fingerprint, it is interesting to show the captured image to the user, because it proves to the user that the fingerprint has been successfully captured, in addition to the assurance that the image has been sent.

Matching benchmarks - the threshold for determining whether the digital sample collected and retrieved for comparison belong to the same person, it must be thoroughly studied to avoid constraints of not recognizing the user's system. The established value directly affects the rates of false positive and false negative.

Enabling storage of biometric feature used in the process - information about which finger, hand or eye was used at the time of biometric acquisition to be used in the process as to facilitate the use of the biometric system. Therefore it provides support for the system operator at the time of authentication, because it allows the user to tell which finger to place into the device, for instance.

Perform simulation on the client's environment - it is important to test the application in different types of environment. When performing this procedure, you can set minimum requirements for implementing the biometric system on the client, for example, what O.S. is compatible and what version of Java should be used. Another test that should be carried out is the one that regards the compatibility with other biometric solutions, such as staff score control, that the client may have.

Difficulties

Throughout the process that was described in the previous section, some difficulties can be found. Such difficulties can be classified according to where they occur:

In the client: difficulties regarding installation of dependencies in the client

Computers that are not updated and/or have restrictions to the execution of the application can get on the way of the whole process. Another great problem is the incompatibility with biometric recognition softwares from other providers. In order to solve these problems there must be minimum requirements that the client's computer must meet, and other biometric systems that the client may need to use must be tested.

In the application: low performance in the applet load

Currently, when developing a Web page that has an applet, you have to expect the end user to have the latest version of Java Runtime Environment (JRE) or at least the version to which the applet has been developed. This problem is deeply frustrating during the development of an applet, because no matter how well designed it is, there will always be the problem of downgrading the client's JRE, or even the absence of JRE. Most of the time, the first load of the applet is very slow due to the startup of the Java Virtual Machine (JVM). The poor performance of the JVM on startup is known as Java Cold Start, which causes a bad user experience on the use of applets. With the purpose of solving this problem, the new Java Plug-in and Java Deployment Toolkit from the Java SE 6.0 update 10 was created (DEITEL et al., 2005). The Java Deployment toolkit consists of a set of JavaScript functions made to avoid incompatibilities with browsers on the client and improve the installation of the application that contains an applet or Java Web Start (DEITEL et al., 2005).

Case study: *Iapep Saúde* Health Insurance

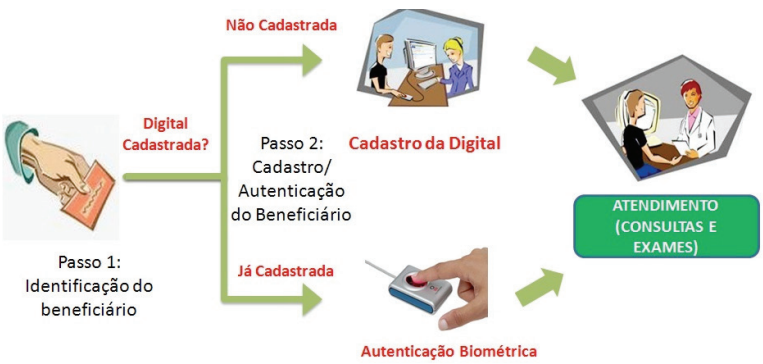
Iapep Saúde is the health plan of the Instituto de Assistência e Previdência (Institute of Assistance and Insurance) from the state of Piaui in Brazil. Iapep was created in January of 1966, with the purpose to provide services regarding health and welfare for workers from the state of Piaui. Therefore, Iapep Saúde is now responsible for ensuring quality and timely health care services to a population of 171,000 insured people.

Iapep Saúde assists more people than all other health insurance plans in Piaui. There is a monthly average of 30,000 consultations and 70,000 examinations in all medical and dental specialties, including those with continuous treatment, such as psychology, physiotherapy, hydrotherapy, nutrition, acupuncture and speech therapy.

Biometrics in the web system

In an attempt to provide greater assurance about the identity of the insured clients and thereby combat fraud by misrepresentation, we developed a biometric system that was integrated to the Iapep web system. The process of identifying the insured people was changed, and it was added to it the fingerprint requirement. The strategy for capturing the clients' fingerprints and their use is illustrated in Figure 4. The best

Figure 4 - Authentication process of Iapep Saúde.



(Step 1: Identification of the payee – Step 2: Registration/authentication of the payee – Not registered – Registered fingerprint? – Fingerprint registration – Fingerprint authentication)
Source: Prepared by the authors

way to register the fingerprints was to capture them in the particular clinic where they were going to be assisted. Another alternative would be to conduct the registration directly at the headquarters of the Iapep, but there is a large number of policyholders that would slow the registration process.

During the process of making appointments for medical examinations the clients are asked to show their insurance card. The assistant searches for the client's data in the database. Then, the assistant verifies the existence of a registered fingerprint. If so, the assistant asks for a new fingerprint scanning in order to validate it with the one that has been previously stored. Figure 5 shows a print screen of the applet for fingerprint scanning. For Iapep, this identification method, through biometric verification, is the best choice once there is a large number of clients. Through this method, they make sure the client is who he claims to be, right away, with no need to compare his fingerprint with other clients'. If the insured client has not yet registered his fingerprint, the screen will be directed to the fingerprint registration page (Figure 6).

Figure 5 – Fingerprint capture screen.

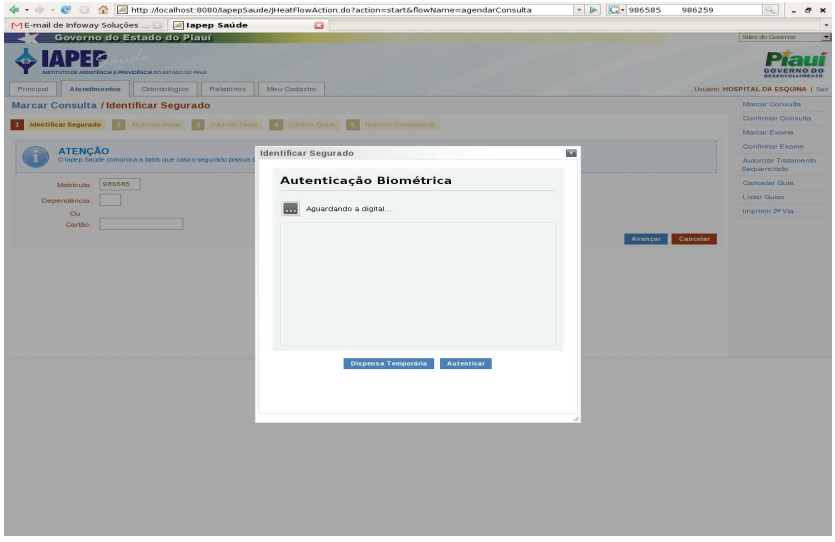
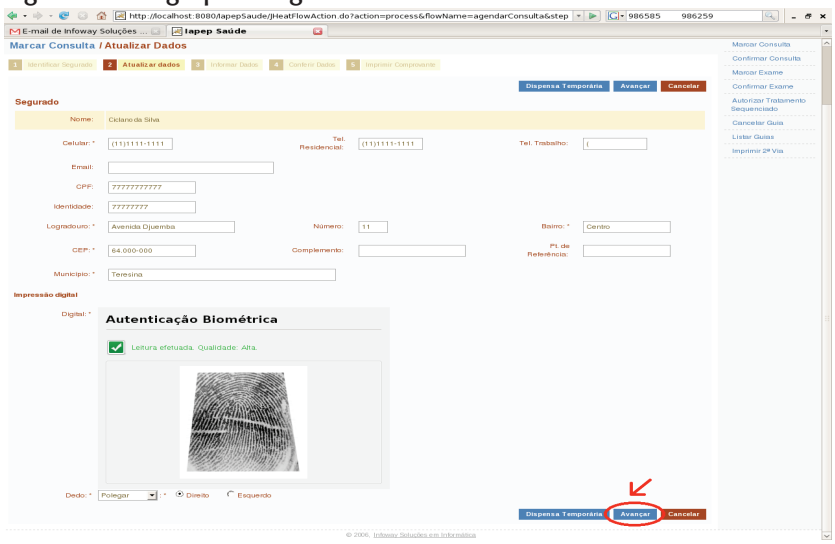


Figure 6 – Fingerprint registration screen.



Source: Prepared by the authors

Difficulties

During the process of deployment of the biometric system for Iapep Saúde, we found some difficulties which motivated us on the making of this present work. The main difficulties found were related to the following aspects:

- The client's environment was not tested – according to item 3.3.5 the client's environment must be tested. Such measure was not taken early in the process which led to a new deployment strategy, thus delaying the initial schedule of installation.
- Parameterization problem of variable in the SDK – item 3.3.3 speaks of the necessity of adjusting the threshold of the biometric solution. The fact that it has not been changed since the beginning has generated a high number of false negatives, failure to recognize the person that is registered, a problem that was solved with the adequacy of the value.
- Incompatibility with other biometric solution - stems from failure to observe item 3.3.5 of this present work. In some cases the client had to use a new computer, in other cases, we found a way to make biometric systems compatible;
- Need for installation on the client - the need for such dependencies caused the creation of an installation package to be used by each end user. Up to now we have found no solution to this problem.

Future works

We plan to apply some changes to the applet code in order to improve the loading process. We plan to use resources from *Java Deployment Toolkit* and new *Java Plug-in*, to solve the problem related to Java *Cold start*. We also plan to remake the whole applet code for platform JavaFX (DEITEL et al., 2005). JavaFX is a multimedia software platform developed by *Sun Microsystems* Java based for the creation and availability

of applications by RIA (*Rich Internet Applications*) that may be executed in several different devices. JavaFX is completely integrated with JRE. To build applications in JavaFX, the developers use a static language called JavaFX Script. Static typing languages are those which a variable type is important to the context where it is used (DEITEL et al., 2005).

We will also study the possibility of downloading all dependencies of Griaule SDK on the client, so it will be not necessary to use a support team to perform the installation manually.

Conclusion

Biometrics refers to the use of physical traits (iris, fingerprint) or behavioral (voice, writing) of an individual for the authentication in a computer system. It is now used as a means of ensuring safety in different types of applications, including web applications. In this present work we exhibited a guide to the implementation and deployment of a biometric system based on experiences in developing a solution for a health plan in the internet. We discussed the concerns about security, interaction with the end user operating environment that must be observed during the process of developing and installing the system in the operating environment. This work was developed precisely because of the difficulty in deploying biometrics in a management system running on the web. The purpose of this work was to make this task easier for those who have to implement it, since the main issues are cited, demonstrating possible alternatives to be followed, forms of implementation and reasons for choosing one of the options.

Regarding the biometric applications on the web, we have demonstrated its use in the identification of the clients that were insured by a health insurance plan, trying to avoid frauds and identity theft. In this case study we have exposed problems that occurred during the deployment of the system, which also motivated the development of this work, and the conclusions of this study led to the creation of a generic model that can help on the creation of biometric systems on the web.

References

COSTA, L. **Um modelo para autenticação biométrica para web banking**. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal de Santa Catarina. 2007.

COSTA, S.M.F. Classificação e verificação de impressões digitais. 2001. 193p. Dissertação (Mestrado em Sistemas Elétricos) – Escola Politécnica da Universidade de São Paulo. Available at: <http://www.teses.usp.br/teses/disponiveis/3/3140/tde-18032002-102113/>. Access in: 21 jan. 2010.

DEITEL, H. M.; DEITEL, P.J. **Java como programar**. 6. ed. [S.l.]: Prentice-Hall, 2005.

FARRAR, B. **Usando Active X.** [S.l.]: Campus, 2001. 424p.

FERREIRA, C.R.; SANTOS, M.R.; SOUSA, E.F. **Identificação biométrica**. 2006. Available at: <http://www.frb.br/ciente/Impressa/Info/Identificacao>. Access in: 21 may 2009.

GRIAULE. Fingerprint SDK 2009. Available at: http://www.griaulebiometrics.com/page/pt-br/fingerprint_sdk/overview. Access in: 19 may 2009.

JAIN, A.K.; FLYNN, P.; ROSS, A.A. (Eds.). **Handbook of biometrics.** Berlin: Springer, 2008.

LIU, S.; SILVERMAN, M. A practical guide to biometric security technology. **IT Professional**,v.3, n.1, p.27–32, 2001. [doi: http://dx.doi.org/10.1109/6294.899930].

MAGALHAES, P.S. **Biometria e autenticação**. 2003. Available at: <https://repositorium.sdum.uminho.pt/bitstream/1822/2184/1/capsi.pdf>. Access in: 17 may 2009.

PERSON AUTHENTICATION AVBPA 3., 2001, Halmstad. **Proceedings**... Berlin: Springer-Verlag, 2001. p.348-353.

POH, N.; KORCZAK, J. Hybrid biometric person authentication using face and voice features. In: INTERNATIONAL CONFERENCE, AUDIO AND VIDEO-BASED BIOMETRIC

REIS, C.M.S. dos. **Autenticação com impressão digital**. Available at: http://www.deetc.isel.ipl.pt/comunicacoesep/disciplinas/pfc/fingerprint/files/carlos.pdf. Access in: 17 may 2009.

VIGLIAZZI, D. Biometria: medidas de segurança. 2 ed. [S.l.]: Visual Books, 2006.

VIOLA, F.M. **Estudo sobre formas de melhorias na identificação de características relevantes em imagem de impressão digital.** 2006. Dissertação (Mestrado) – Universidade Federal Fluminense. 2006. Available at: http://www.ic.uff.br/PosGraduacao/Dissertacoes/298.pdf. Access in: 17 may 2009.