# Integration of Biometrics to the E-Health

Milena Stefanova[1] and Oleg Asenov[2]

*Abstract* – **This report presents an approach for application of finger vein biometric identity management in the healthcare sector. It is emphasized that the applying of finger vein recognition and identity management is the cost effective way that ensures an incessant and integrated protection of users in e-health services. The basic concept and examples for integration of vein identity management solution into typical healthcare IT-services are presented in the paper.**

*Keywords* – **Biometrics, Finger Vein Identification, e-Health, e-Government.**

## I. Introduction

Information and Communication Technology (ICT) applications for health are referred to as "e-Health". These applications include means and services generally aiming at facilitating and improving healthcare. E-Health supports services and activities facilitating the supply of health-related goods and services. E-Health also includes the provision of health-related knowledge infrastructure and/or collaboration platforms and it depends on the existence of the necessary IT infrastructure [1].

Present-day e-Health solutions should provide for:

- Flexible and scalable web-based solutions;
- Tools to help security and privacy management;
- Integration to current clinical workflow.

By application of finger vein biometric in the health care, the approach to enable secure access is offered and in this way to improve privacy and the security management.

Predicting the development of health insurance is that people will take a more active role in managing and controlling their health record information. According to one of all the future health care network predictions, users will access their own e-health records over the Internet with secure logins and encrypted transmissions. These features readily exist at present. The possibility of their practical application is that people can consider their own medical records as important as electronic banking records.

In the paper, the place of biometric identity of e-government services access is examined. The important advantages of the finger vein over all other technologies are offered. The application model and requirements to IT-resources are described. The possible decision with biometric identification in healthcare sector is presented.

## II. E-Government And Biometric Identity

Each successful project of e-government is associated with the opportunity every citizen to be identified in order to get access to their own personal pages quickly, easily and reliably. Depending on the type of information and services offered in e-government projects usually there are two levels of identification defined:

− Identification without the need of verification of presence;

− Identification with necessity of presence confirmation.

The solutions for biometric identification are usually applied to the second scenario, they are also applicable to the first one if there is a requirement of a high level of protection. Identification of the individual where the presence is not required can be designed by a unique numeric identifier on a portable electronic carrier which is linked to the data on individuals in a secure database.

Identification, which requires obligatory presence, can be made by presenting the same unique identifier and verification of holder by an official (this brings a subjective element) or by the application of technology that requires the presence of the individual [4]. Recognition for such purposes must comply with several criteria:

− Adequate protection against violent crime: theft, forgery or counterfeiting;

− Uniqueness and consistency in time (the uniqueness is similar to those in DNA (Deoxyribonucleic acid) recognition);

− Contact-less method (convenience and hygiene reasons);

− Minimal digital size of used template;

− Ensuring the presence in the identification;

− Minimum time for identification (speed).

Biometric authentication by scanning the individual geometrical position of the veins in finger or palm of the hand is a method that meets all the **necessary criteria**:

− *Protection* – veins are hidden in the human tissue and their removal / tampering is virtually impossible, even through complex surgery, in addition, the method itself requires the presence of live (with circulation) tissue for identification, thus preventing the possibility of criminal abuse.

− *Uniqueness* – this method is second (after DNA) in terms of uniqueness in identification – It is unique even in Twins and remains constant in adults in the course of time.

− *Contactless* – the identification is done by non-contact scan image by thermal camera.

− *The smallest size* – digital imprint is stored in only 400 B.

− *Requirement of presence*. Biometric identification through this method guarantees presence. This would allow the real treatments and procedures to be controlled as well as a high level of protection to be secured in cases of identification of presence.

− *High speed of identification* – the identification time is less than 1 second for up to 20 000 users.

[1] Milena Stefanova works at the Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of V. Tarnovo, 3 G.Kozarev str., 5000 Bulgaria, E-mail: m_stefanova@abv.bg.

[2] Oleg Asenov works at the Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of V. Tarnovo, 3 G.Kozarev str., 5000 Bulgaria, E-mail: olegasenov@abv.bg.

## III. The Technology

Identification functions on the principle of finger vein structure and each finger of each person is unique [10]. Based on this discovery made in 2006, a vein-code technology for reading and recognizing people has been developed and this technology has **major advantages** in comparison with other technologies:

− Reading the vein-code is *contactless* – fingers and sensors are not in contact;

− Practical *zero-error in detection* and recognition. It does not depend on the quality of the finger skin, the dirtiness of the skin or the presence of surface injuries;

− *The time* for reading and identification (in the system with comparison by 1:1 method) *is less than one second*;

− Recognition takes place only when blood flows through the veins and this type of identification *can not be falsified* (medically proven that it is not possible to imitate the same vein-code through plastic surgery). Vein-code is recognized as a method for rapid identification of individuals by FBI in December 2009.

The presented device has been developed by Japanese-American consortium Hitachi-M2SYS. The software based on this method of biometric identification is compatible with different types of biometric devices [6] and it allows:

− Avoiding duplication of medical records and eliminating language barriers and poor literacy;

− The process of identification of the patient is optimized, and thus the work efficiency of employees in health care is improved;

− Identification of the patient and also verification of their health status;

− The use of the patient biometric identification during doctor's rounds is quicker than usual and the medics have no doubt that the prescribed treatment is for the exact patient;

− Because of the uniqueness of the individual biometric templates, the software prevents duplication of patient medical data; it alerts the medical employee that the data of the patient have already been introduced in the system;

− It integrates easily with the existing hospital-patient software; the system can work up to 24 hours without the need of new program code or integrating data base.

The technology has been developing and finger-vein reading sensor for mobile devices [8] and for tablets [7] has already been designed.

## IV. IT-Resources and Model Application

The digital template, used for biometric identification, is in size not larger than 400 bytes, which provides easy transportation including low-speed communication.

To access the system, clients should have only a web browser and biometric reader, shown on Fig.1 [5], where identification is required to verify of presence. Table I presents the fixed specifications of the biometric reader [5].

For the purposes of application the method of biometric vein-code identification in protection against illegal malicious user access with replacement of identity, when accessing personal e-health records, an architectural model for the implementation of user applications is considered [2,3]. That model [2,3] for the performance of the protection through biometric identification with vein-code for e-health applications is used.

In the presented model, there is a virtual Active X Bridge built and it runs as an executable code on the servicing Web-Server for access from the user workstation to the Host Application. In the model, Client Manager is launched as part of a web-service, supporting Active X gateway. Before the Client Manager permits or denies right of entry of the user, the e-health records are not accessed.

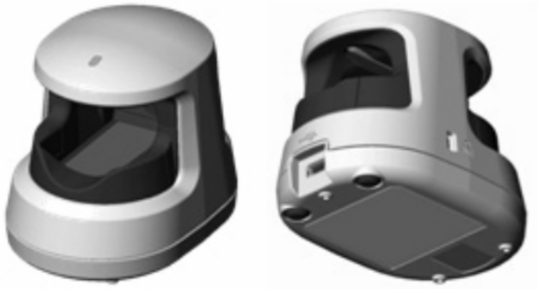


Fig. 1. The Hitachi USB Finger Vein Biometric Authentication Unit

The users must identify themselves on the client computer with biometric reader, connected by USB 2.0 port. Through ActiveX Bridge the registered biometric template is transmitted to the Bio-Plug-in Server to compare with the already stored patterns in the Finger Vein Database. Once permissions are matched and configured– the e-health record is accessible and it is interpreted by the client's browser. In case of mismatch– the application is rejected and medical data are not accessed.

TABLE I
FINGER VEIN READER SPECIFICATIONS

| Item | Specifications |
|---|---|
| Capture System | Infrared LED + Camera |
| Interface | USB 2.0 |
| Dimensions | 59 (W) x 82 (D) x 74 (H) mm |
| Weight | 96g |
| Power | DC5V +/-5% <500mA (Power from USB bus) |
| USB Cable | 1.8 m |
| Certifications | FCC, CE |

The system allows working with virtually unlimited number of people. In the presented biometric identification, the vein-code cannot be forged or faked, which means that the person is the one who actually has the right to work remotely with the information or input data. The used vein-code ensures that the user who applies for access to the resources of e-healthcare has been certified in person. No person can pass their personal vein-code to a third party. Practically it is impossible to catch the use of the template because every time a scanning over communication interface template is sent, it is encrypted with a different key.

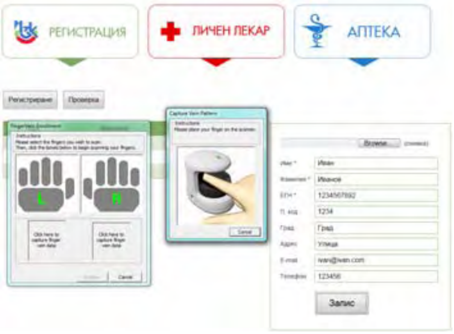
## V. Decision on Health Care

The suggested solution is due to a detailed survey and analytical research of the active regulation algorithm of processing of health clinical paths in the healthcare sector in Bulgaria. The analysis is carried out from the point of view of tracing “the way” of the patient from the GP-doctor to the specialist. An optimized model of algorithm for health clinical path information processing, which provides considerably greater extent of authenticity of input data, has been offered. At each phase of the process the presence of the patience is certified by an identification of unique vein-code of one or more fingers of the hand. The registering of the vein-code gives an opportunity to monitor the time and place of patient movement in the process as well as their real “physical” participation in this process.

Thus the application that has been worked out makes the process of information processing of health clinical paths more objective by applying the technology of biometric identification; it leads to decreasing the amount of “paper” documents for processing and giving accounts of this process. The application contains three fundamental items for managing the main activities in the healthcare by biometric identification with the help of the vein-code:

### A. Registration of patients in the uniform database (Fig. 2):

− The necessary data in predefined fields are completed;
− The picture is added – from a file or from connected to the place of work camera;
− The input data are recorded;
− For better security, two fingers are registered;
− The input information is recorded once again.



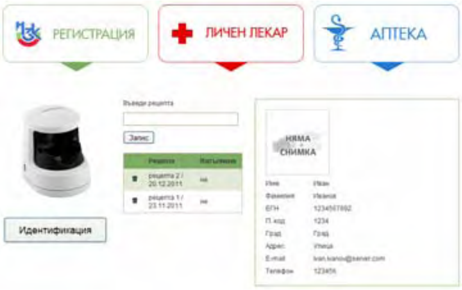
Име * Иван
Фамилия * Иванов
ЕГН * 1234567892
П. код 1234
Град Град
Адрес Улица
E-mail ivan@ivan.com
Телефон 123456

Fig. 2. Patient’s registration

### B. Registered patient visits their GP-doctor:

− After the identification and examination treatment and a recipe are prescribed;
− In addition to records of recipes details of conditions, drug intolerance, treatments performed, etc can be kept;
− It allows verification of the recipe situation for the registered patient: which have been fulfilled and which have not.

### C. Registered patient visits Pharmacy (Fig. 3):



Име Иван
Фамилия Иванов
ЕГН 1234567892
П. код 1234
Град Град
Адрес Улица
E-mail ivan.ivanov@server.com
Телефон 123456

Fig. 3. Patient visits Pharmacy

− After identification of the patient, fulfillment of recipe is registered;
− Similarly, records of any treatment can be implemented, monitored and kept.

## VI. Conclusion

Using the highly secure authentication principle of finger vein verification, corporations and healthcare institutions can ensure user identity and data security and minimize data security breaches and cyber crimes taking place at enterprise worldwide [9]. Biometrics can play an important role in authentication applications, since they are strongly linked to the holder, and difficult to forget, lose or give away. It is important that the biometric systems are designed in the way, which can resist the attacks, working in security-critical applications, especially in unattended remote applications such as e-health sector.

## References

[1] Progress Consulting S.r.l. and Living Prospects Ltd., *Dynamic health systems and new technologies: e-Health solutions at local and regional levels*, Comittee of the Regions of the European Union, 2011.
[2] M. Stefanova, “Model for user’s identity protection by access to web-applications,” V International scientific conference “Innovations in technology and education”, Kemerovo / Belovo, May 2012.
[3] M. Stefanova, T. Stefanov, and O. Asenov, “Access to e-government’ services through vein-code biometric identification,” CISTI'2012 (7th Iberian Conference on Information Systems and Technologies), Madrid, June, 2012.
[4] W. Chuck, *Vein pattern recognition: a privacy-enhancing biometric*, CRC Press Taylor & Francis Group, 2010.
[5] http://m2sys.com/finger-vein-reader.htm
[6] http://m2sys.com/rightpatient-biometric-patient-identification.htm
[7] http://www.biometrictribe.com/?p=471
[8] http://www.fujitsu.com/global/news/pr/archives/month/2011/20110419-01.html
[9] http://www.hitachi.com/rd/yrl/conf/2011/ijcb/index.html
[10] http://www.hitachi.eu/veinid/documents/veinidwhitepaper.pdf