Mobile technologies and electronic governance

Milena Stefanova

St Cyril and St Methodius University of Veliko Turnovo, Faculty of Mathematics and Informatics, 5000 Veliko Turnovo, Bulgaria

Corresponding author's e-mail: m_stefanova@abv.bg

Received 17 March 2015, www.cmnt.lv

Abstract

This paper looks at some of the problems of electronic governance in the Republic of Bulgaria. It also provides a summary of the advantages and disadvantages of providing e-services in the e-health sector. An optimized algorithm is then drawn up, upon which a model with vein code biometric identification for web-based systems is applied in the process of providing e-services in the healthcare sector. This model provides a much higher level of authenticity in data processing in comparison with the traditional customer service procedure. A comparative analysis is built upon the various criteria of mobile websites and applications, where the choice of mobile application analysis is well-founded. The major stages of mobile application development are traced and a preliminary research on their precision and convenience is carried out.

Keywords: e-Government, e-services, biometric identification, mobile applications

1 Introduction

According to the e-Governance law (EGL): "**Art. 8, Par. 1** Within the scope of *electronic administrative services* fall those administrative services provided to citizens and organizations by the administrative bodies, the services provided by people to whom public service provision has been assigned, as well as the public services requested and/or provided distantly *by means of electronic devices"* [1].

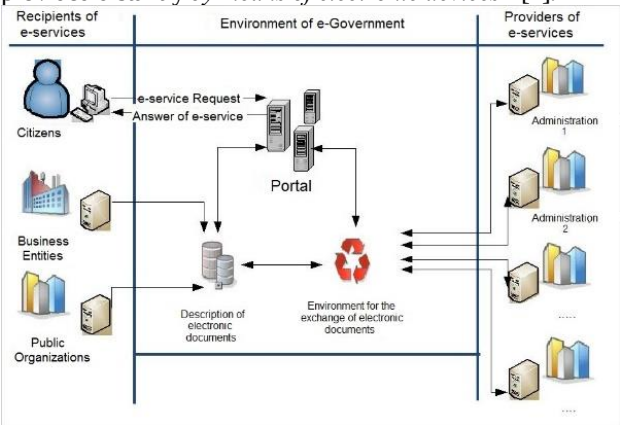

FIGURE 1 Infrastructure of unified information environment for electronic governance

It is necessary that the *administrative e-services* be delivered in a user-friendly and accessible interactive form, also for persons with disabilities. Access to e-services is based on the entitlement of each natural or legal person to all services accessible to this user category.

Key element in the *e-service provision* by means of a unified information environment (Figure 1) is the possibility for persons and organizations to access the information inserted for review at any time and from any location [3].

Figure 1 illustrates the basic components in the unified information environment infrastructure:

- *The recipients of e-services*, citizens and an organization who after confirming their identity in the unified information environment get limited access to the requested e-services;
- *Unified information environment:* – supports single portal for access to e-services; – Provides integrated interdepartmental e-services related to consolidated transactions to databases of more than one department, directorate or administration;
- *E-service providers* – information systems of the administration or of organizations which by virtue of normative act had outsourced part of the functions and activities inherent in the administration.

The providers of e-services manage the actual processing of requests for e-services, the portal and the environment being mainly responsible for the accessibility of services and the protection of information, as well as the individual access to confidential information through relevant identification of requesters.

Prior to the final identification by means of identity confirmation saved on electronic storage device, identity check with view of providing access to information within the e-governance environment can be fulfilled as follows:

Comparing between the names of the requester in the application form and the holder of the electronic signature certificate;

Check in the administration responsible for the citizen registration, whether the unique identifier of the applicant indicated in the application form corresponds to the name of a citizen holding this name;

Subject to identity check are all citizens who had claimed circumstances and possess a unique identifier;

Check of the identity of organizations is based on the respective organization registry books.

The single identification is binding if the citizen, respectively the organization had indicated a unique identifier.

After indicating the unique identifier, the e-service environment recognizes the identifier itself, not the actual service requester. The basic issue remains unresolved. If a third party acquires or becomes aware of the content of the unique identifier, that person may act as the citizen or the organization in front of the unified information environment

and get access to information and services to which he/she is not entitled.

Key priority areas of the electronic governance are the "Safety", the "Healthcare", the "Finance and Tax Policy" [2], the three of them containing confidential information for the citizens and organizations access to which could be obtained through the e-services portal, the information could be "downloaded" only and solely upon submission of universal electronic identifier. In the sector "Finance and Tax Policy" the electronic signature is sufficient proof for the provider of certified services of the reliability of information provided by citizens and organizations, but in the reverse processing, security matters are not the responsibility of the information provider. According to the law, the person submitting the tax declaration bears responsibility for the data inserted but, if a third party could access the e-service portal or could otherwise access the aforementioned tax declaration, this counts as severe security failure. The two key characteristics of the information are its reliability and protection. With the essential help of the electronic governance portal the administration will receive more and faster information electronically, since it is expected that both the citizens and all organizations will be facilitated in issuing this type of information by authenticating its content with an electronic certificate.

From a technological point of view, an important aspect in the development of electronic governance is the placement of the two properties of information, authenticity and protection, on an equal footing of importance. At this stage the problem with the provision of authentic information is to a great extent solved, however, the problems of providing reliable electronic identity are still pressing.

2 Special features and flaws of providing electronic services in the e-healthcare sector

The Healthcare sector has priority over other sectors in terms of the need for providing electronic services. In this area a considerable progress in terms of operation information processing has been achieved with the introduction of contemporary Information and Communication Technologies (ICT). What is special about the sector is that its work is related to the provision of a special type of electronic services called electronic attendance services. An example of this kind of service is drawing money from ATM. The service is a typical e-service in itself, but the presence of the certificate holder and the authentication of their identity at the institution providing the service are key features for the healthcare sector.

In the "Healthcare" sector, patient identification plays a key role in terms of service provision and the reliability of information with the electronic method.

A main disadvantage of the instantaneous way of obtaining information is the lack of certainty in the identity validation of consumers. In the process at present, one could not otherwise be sure, than relying on the conscientiousness of general practitioners or chemists, if the patient had actually attended the general practitioner and if this particular patient had fulfilled the prescribed recipe at the pharmacy. These kinds of issues relating to identity confirmation in the delivery of information through e-services are even more conspicuous when the e-service provided results in the money transfer.

It is possible in practice, false records to be gathered on the basis of which payments are fulfilled without any guarantee whatever on the true identity of the beneficiary of the health or the e-service provided.

The application of biometric identification, in this case, is one of the possible solutions to objectify the process of inserting reliable information in the key fields of the database used.

This study is based on the algorithm of processing clinical pathways by way of tracking the patient's "route" from the general practitioner to the specialist.

Other major characteristic is the possibility of adding two additional factors for identification – time and location – in the course of identity confirmation and completion of key fields.

The technology of biometric identification implies the addition of information about the time and place of identification, which in itself solves the problem of the meaning of steps in the process of information services, i.e. it is obvious that at a given hour and date the prescription has been issued in favour of the patient who, in one's own turn, had "personally" attended one's general practitioner and after the elapse of a good time span this same patient was "actually" at the pharmacy, was identified biometrically and fulfilled the prescription.

The purpose of the optimization of the existing algorithm is turning the information processing into an objective process via a biometric identification technology, as well as to reduce the paper work related to the information processing and accounting of the process.

3 Optimized model of a web-based system for e-service provision in the healthcare sector with application of biometric identification through vein code

A new version of the base algorithm for data processing of clinical pathways is presented. The application of the optimized model aims at making the process of clinical pathway data processing more objective, by integrating a biometric identification technology. The new version marks the possibility for biometric identification to be applied as factual evidence for attendance, as well as for confirmation of the actual clinical pathway implementation.

Thus, only with the introduction of an effective enough method of biometric identification which does not entail significant information and communication resources, a number of problems had been solved and this is a precondition for further improvement in the quality of the e-service provision. Assuming that such an identification model has already been introduced and that each general practitioner and pharmacy, each inlet and outlet in the "clinical pathway" is equipped with devices and relevant program "shell" for biometric identification, then all paper recipes and medical referrals to a professional or clinical pathway could be removed. A paper authentication would not be necessary to prove that a certain person had obtained a prescription or an actual medical referral to professionals or that this same patient had "benefited" from the services and budget by virtue of the clinical pathway.

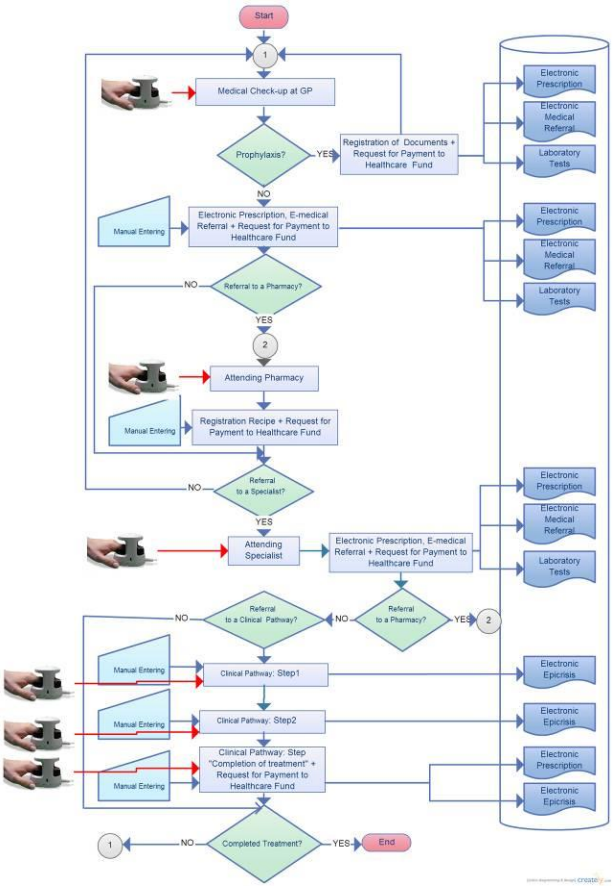

FIGURE 2 An optimized algorithm for information processing in the "clinical pathway" range in Bulgaria

Only with the application of this simple and feasible method of biometric identification could, on the one hand, *the authenticity of the user be guaranteed*, and on the other, arise opportunities for optimization and addition of new electronic services and *paper accounting be reduced*. Third, this *reduces significantly the amount of information* inserted by all operators in the information provision service, particularly those from pharmacies, and creates *opportunity for real-time processing*.

This optimized model of the "clinical pathway" information processing algorithm (Figure 2) ensures greater degree of authenticity of the data inserted compared to the traditional user service approach.

Authentication of patient availability at each step of the process is made by means of unique vein-code biometric identification of a single or several fingers. Card issuance or the application of complex identification technology is not required, the only thing to do being inserting your finger into an attester terminal and letting a vein identifier (vein ID) to be recorded.

All documents are electronically made and the next stage follows only if the vein code has been successfully detected. The registered vein code allows for spatial and temporal tracking of the patient in the process as well as his/her "physical" participation in the process. Generation of documents is not possible in the case of absence or fictive presence where valid registration of the unique finger vein code is not available.

4 Advantages of mobile applications

Mobile websites use HTML protocol and work with related websites as well as any general website. They are less integrated to the device hardware in terms of applications though the HTML protocol is a universal Internet protocol adapted to any browser. Some users prefer to access mobile websites from a tablet or a smartphone being satisfied because in this way they need no further installation but only the Internet address of the website. An additional application is not necessary because all the information required from the mobile website is available in several touches of the screen. Specialized applications, in turn, offer a more complete package of services. They are installed on devices and are much better integrated to already installed or to user selected applications. When creating an application, the website owners may require from developers the embedding of features that work equally well on any OS. Thus, the user is satisfied and keeps on using the website.

The specialized mobile applications provide much better tracking of usage, usage duration, specific position in the application and access to profiles on the social networks Facebook, Twitter, Google+, LinkedIn. In-App subscriptions and premium versions without ads are possible. The specialized applications compared to mobile websites use less system resources whereas providing more functions.

Comparing mobile website to mobile application considering the following criteria:

Accessibility

– A mobile website is immediately accessible to users through the browser which all mobile devices are nowadays adapted to use.

– The applications shall be installed by the user to be able to see the website content.

Scope

– Mobile websites have a broader scope, because they are available for different platforms and easy sharing among users.

– The application functionality is limited to the operation system for which they are designed.

Update

– A mobile website is much more dynamic in terms of flexibility for updating the content. The mobile website design or content could be changed by making corrections in the code, the update being immediately visible.

– The update of a mobile application requires dissemination of the available updates to the users, as the application update shall be made on every type of device.

Searchability

– The mobile websites are easy to find via Google or Bing search engines.

– The applications' visibility is limited to a great degree within the specific App Store of the specific OS (WP, Android, iOS).

Compatibility

– A mobile website is accessible to users with different mobile devices. Its URL could be easily integrated into other mobile technologies, such as SMS, QRcodes and NFC (Near Field Communication).

– The Apps require development of specific version for different types of devices.

Website Sharing

– The mobile websites could be easily shared in

developer to user and user to user manner.

– The applications could also be easily shared by means of multiple related online services but they are not always multi-platform.

Duration of availability

– The mobile websites are available as long as the main website exists.

– The majority of Apps have short life unless they are constantly maintained by developers. This maintenance is closely connected to the constant update and monitoring of the new versions of operation systems so that outdatedness and the risk of user mobile device's inability to access to the selected mobile application could be avoided.

Costs

– The mobile websites are cheaper because the Application stores are free of charge.

– Investments with mobile applications are not limited to their initial start-up. Proper support and development of an application (update, testing, compatibility issues and continuous development) is much more expensive.

Despite the obvious advantages of mobile websites, applications are quite popular due some special characteristics, making the use of a single application the better option:

– *Interactivity* – this index makes the use a single application the more suitable choice than the website.

– *Power* – as applications are directly linked to the operating system, they can use its available resources.

– *Personalization* – if the target consumers want to personalize a given service in accordance with their preferences, the contemporary applications provide a suitable method of doing so.

– *Offline maintenance* – if when a specific service is needed but there is no access to the internet, the mobile website becomes unreliable, while a single application can provide offline access whatever the circumstances.

5 Stages in the development and testing of mobile applications

This section looks at the creation and usage of two mobile applications for access to the centralized system. The functionality of the first application is realized by conventional access, with a consecutive pair: "name : password", and the "M-Zdrave.apk" mobile application is used to create a virtual channel that connects a biometric sensor, working with Windows XP operating system, with the mobile device of the consumer via QR code.

The creation of each mobile application for Android OS goes through the following sequence of ***stages***:

- S1: Development of the conceptual design – formulating the initial requirements for the application.

- S2: Context-based design – research on the user needs and requirements in terms of the operative working environment.

- S3: User Environment Design (UED) – introduction of the system functions and their organizing in a user friendly way. At this stage, the settings of the application working environment are made; also, adding and adjustment of the PHP framework and libraries.

- S4: Development – writing, editing, testing and correcting the source code.

- S5: Mobile App testing. Corrections of the source code follow, subsequently implementation and testing.

- S6: Introduction of the developed application. At this stage, the implementation is under way. A preliminary research on the applications is conducted.

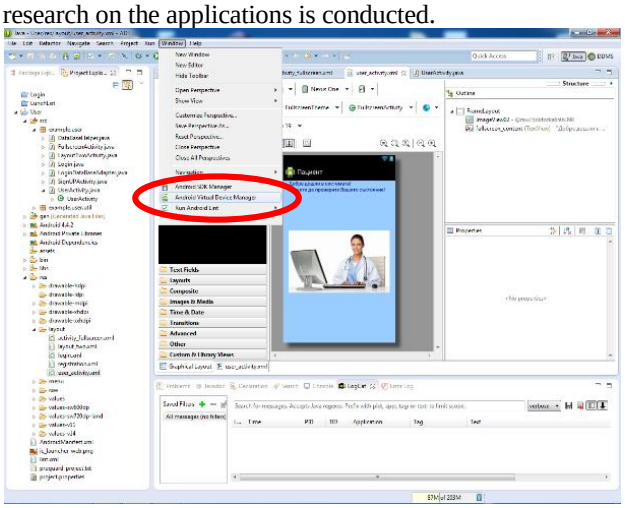

FIGURE 3 Menu for work with virtual device manager Android SDK

The applications are developed with Eclipse IDE (Integrated Development Environment) and Android SDK (Software Development Kit). Eclipse IDE is an open code programming environment [7]. Android SDK is a free-of-charge toolkit creating applications for Android mobile operating system [5]. The programming environment maintains the testing of developed applications with the help of a virtual device, simulated and adjusted in "Android Virtual Device Manager" mode (Figure 3).

Figure 4 – a visualization of an instant of the functionality and the proper behaviour check of the mobile application "M-Zdrave.apk", test conducted on the virtual device "5554: LG4", simulating work with Nexus 4 device in Google – screen size 4.7 inch, resolution 768 x 1280: xhdpi, SD Card 1 GiB and RAM 768 MiB, emulation of both device cameras.

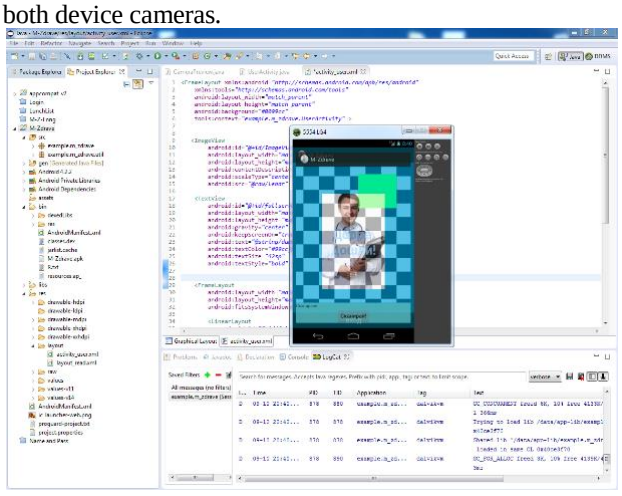

FIGURE 4 Test of the mobile App "M-Zdrave.apk" on a virtual device

The actual feel of comfort, applicability or difficulties on the part of the consumer when working with this application are impossible to define with the help of a virtual device, whose interface is managed from the keyboard and mouse of the computer system. The purpose of this operational mode is mostly to detect code errors or an unpredicted

unexpected behaviour of the mobile application. What is important is the impression gained from the end result of the actual handling of the user interface by touching the screen of the device and by working with its main functional keys, rather than the choice of elements made by pointing with a mouse or using a keyboard, as is the management and user dialogue of a virtual devise.

Prior to the introduction stage, it is necessary to test the application functionality using various mobile devices with Android operating system, including those ones different versions of the platform.

The functioning of the mobile application "***M-Zdrave.apk***" has been studied and tested in practice – on different devices and different versions of the mobile operation system – *Gingerbread, Jelly Bean and KitKat.* The results from the preliminary study of the application's proper behaviour and user friendly interface are shown in Table 1.

TABLE 1 Functionality of the mobile application "M-Zdrave.apk"

OS Android Version	**Samsung devices**	**Screen characteristics**		**M-Zdrave.apk**	
		Size	Resolution	Login (sec.)	Convenience
2.3.7. *Gingerbread*	S5300 Galaxy Pocket	2.80"	240 x 320	-	-
4.1.2. *Jelly Bean*	I8260 Galaxy Core	4.30"	480 x 800	4.2	+
4.3. *Jelly Bean*	I9250 Galaxy Nexus	4.65"	720 x 1280	3.1	+
4.4.2. *KitKat*	I9505 Galaxy S4	4.99"	1080 x 1920	2.5	+

6 Comparative technology analysis and methods for identification with remote access

The proposed model is a result of the detailed research and analytical study of the existing legal algorithm for processing clinical pathways in the healthcare sector in Bulgaria. A series of counselling has been conducted with medical staff working as general practitioners. The analysis is based on the tracking the patient "route" from the general practitioner to the medical professional. An optimized model of the algorithm for clinical pathway information processing is being suggested which ensures much greater authenticity of the data provided. Patient availability at every stage of the process is verified through unique finger vein code method of identification.

TABLE 2 Mobile applications – comparative analysis

OS Android Version	**Reg_patient.apk**		**M-Zdrave.apk**	
	Time to login with password	Convenience	Login time with QR code (sec.)	Convenience
2.3.7. Gingerbread	42	-	-	-
4.1.2. Jelly Bean	23	-	4.2	+
4.3. Jelly Bean	19	-	3.1	+
4.4.2. KitKat	21	-	2.5	+

Comparing the mobile application functioning. The idea behind comparing two applications with different mechanism of functioning is to highlight the advantages of the identification model using biometric terminal. This model is applied to get access to a requested database of a centralized system that fulfils biometric control of its users.

Table 2 illustrates a resume of the rates of the comparison drawn as a result of the work and experience of users having different versions of Android operation system.

7 Advantages and disadvantages of the identification model

The mobile applications are hereby compared so as to highlight the advantages of the identification model with M2SYS biometric reader [6]. After the testing and analysis of the precision of the personal mobile applications have been carried out, some of the main advantages and disadvantages of working with the biometric identification system for centralized database access of the e-healthcare sector and of mobile device control access have been summed up.

Advantages:

- The registration of the vein-code allows for patient control in the process in terms of "time and location" as well as control of the user "real attendance" during the process.
- The developed application makes the processing of information within clinical pathways impartial through applying the biometric identification technology and reduces the volume of "paper work" by information processing and accounting.
- Registration of an electronic health status file according to this model enhances the medical service efficiency:
- Gives reliable information to the medical professional about all past diseases and treatments prescribed;
- Reduces the service administration time.

Disadvantages of the presented model:

- Entails Internet connection.
- Requires the availability of a well-working biometric sensor. For registration of the finger vein biometric in the database, a proper interaction with the software governing the specialized biometric registration hardware is required.
- The medical healthcare service for children under-age is not regulated and therefore, it could not be provided only on the basis of the proposed identification model.
- The use of the system is difficult when serving immobile patients.

8 Conclusions

This paper provides a research of a model for biometric identification in the public informational system and a secondary control access from a mobile device. It traces the major stages in the development of mobile applications for a web-based system with centralized database, biometric control and mobile device access, as well as its compatibility when working and gaining access from various devices. Preliminary study of the proper behaviour and user-friendly work of the mobile applications has been carried out.

The designed system is subject to further developments with view to solve the disadvantages of the present model. The development of mobile applications for various operation systems is under way, which will be user-friendly, reliable and will bring user satisfaction when making inquiries to the information service system in the healthcare sector.

Acknowledgments

This work was supported by a grant from the project №09-590-13/10.04.2013, Integrated electronic services for the citizens and the business of St.Ciryl and St.Methodius University of Veliko Turnovo, Bulgaria.

References

[1] Electronic Governance Act, promulgated *State Gazette*, *Issue 46 from 12.06.2007, as of 13.06.2008*
[2] Common Strategy for Electronic Governance in the Republic of Bulgaria 2011-2015 http://www.mtitc.government.bg/upload/docs /Obshta_Strategia_eGovernment_2011_2015.pdf
[3] http://computerworld.bg/32934
[4] http://creately.com/
[5] http://developer.android.com/tools/sdk/eclipse-adt.html
[6] http://m2sys-biotracker-finger-vein.software.informer.com/
[7] https://eclipse.org/downloads

Author

Milena Stefanova, 7 December 1971, Pleven, Bulgaria

Current position, grades: chief assistant professor, PhD in Informatics and Computer science of Department of Computer Systems and Technologies, St Cyril and St Methodius University of Veliko Turnovo
University studies: St Cyril and St Methodius University of Veliko Turnovo.
Scientific interest: Computer Network Administration, Programming, Computer Security, Biometrics, Integration of the ICT in eBusiness and eGovernment
Publications: 23 papers.