Design and Validation of a Secure Communication Platform for Mobile Health

Beatriz Martín de Juan[1], Miguel Ángel Valero Duboy[1], Diana Soler[2], José Manuel Azorín[3], and Rafael Conde[1]

[1] T>SIC, Information & Knowledge Society Technologies,
Technical University of Madrid EUIT Telecomunicación,
Ca. Valencia, km. 7. 28031, Madrid, Spain
{bmdjuan,mavalero,rconde}@diatel.upm.es
[2] Modelos de Atención Gestionada
C. Bruc, 35, 5º, 08010 Barcelona, Spain
diana@mag.es
[3] Vodafone España
C. Grañón (Pau Las Tablas), 22, 28050 Madrid, Spain
jose-manuel.azorin@vodafone.com

Abstract. This paper focuses on the design and validation experience of an eHealth system that provides end users with web and mobile access to their personal health records (PHR). The system has been tested with different mobile devices to ensure full compliance with privacy and confidentiality requirements. As a result, both patients and medical doctors can share sensible medical data in a secure and efficient way. The pilot site has been evaluated under the cooperation of 375 volunteers from a global mobile operator, a regional medical company, a SME applications developer and a state university with deep background on eHealth. Users´ feedback has been quite satisfactory and promising.

Keywords: Mobile health, medical confidentiality, secure communications.

1 Introduction

Mobile health (mHealth) [1] requires suitable network, software and hardware technologies to provide patients with mobile health services in a flexible, realistic and usable way at the point of need [2]. Telemedicine services are meant to provide at this point not only medical care but services provision depending on the availability of reliable networks to make medical information fully accessible for clinical purposes. However, mobility goes further beyond this aim since patients' location is not restricted and they can manage clinical information.

Telemedicine and eHealth must be secure not only in terms of safety but also regarding data confidentiality and integrity. This research paper focuses on the design and validation of a secure platform to provide mobile patients with integral PHR. The experience has been trailed in Spain thanks to the participation of 375 volunteers from a global mobile operator, a regional level medical company, a SME applications developer and the research work of an estate university with wide background on eHealth and telemedicine.

K.S. Nikita et al. (Eds.): MobiHealth 2011, LNICST 83, pp. 24–31, 2012.

1.1 Background

European health care policies do always face new challenges to manage huge amounts of medical data due to the increasing penetration of PHRs. The combination of mobile and web technologies paves the way for efficient solutions to provide citizens with private access to their medical data. Since health care services are highly fragmented, patients and medical doctors have multiple difficulties to easily consult requested clinical information. The enhancement of care quality provision is directly related to the availability of ad hoc medical data. Computer and communication technology advances, mobile networks and affordable devices have made data information more manageable for patients that can now easily access to their personal information distributed in compliance with privacy and confidentiality requirements.

Although mHealth has developed a framework to allow more and more patients to benefit from ubiquitous transmission of massive medical information in a quick way, it sets up new inevitable issues such as open information exposition to malicious intruders [3]. The transmission of patients' information over wireless networks must grant confidentiality, integrity, availability and privacy as HL7/ISO standards do specify.

Several initiatives have already tackled various key problems when integrating secure PHR management with usable and efficient mobile access. However, while wireless applications for healthcare can be divided in: monitoring applications and patient communication and supporting applications [4] [5] [6], the innovative side of this proposal is the secure data exchange. Patients records security is not only based on complex mechanisms to support encryption or authentication to servers or network access, but the integration of solutions in a widespread and highly demanded device such as mobile phone from which information is potentially transferable to the social environment and widely used by citizens.

1.2 Platform Requirements

The actual system consists of a web platform that can be consulted directly or by means of a mobile application. The main goal is to promote proximity and universal access to the patient's PHR; it supports access from anywhere, at any time using standard clinical information [7] and enables interfacing communication with other systems and providers by transferring the actual contents to the patient's mobile phone. The system allows automatic updates, either by further interventions and updating their data, or by means of upgrading health advisories and alerts generated automatically by the system. It also guarantees the secure data storage and transmission ensuring the confidentiality and security of data throughout the whole process [8], in compliance with current regulations [9].

mHealth data needs to be protected against unauthorized access. The issues concerning mHealth information are mainly related to: information recollection, retention, distribution and use. In the first instance, the provider must be authorized by the user before the information is given [2]. In order to protect the access to the medical information, the patient will have the right to know if such information exists and when necessary if it has been consulted by another person. Personal identifiable

health information about individuals should also have the fully informed consent of patients [10].

Secure Systems of Information should incorporate politics, standards and procedures that can assure data confidentiality, integrity and availability. The current legislation must be obeyed and be aware of potential digital danger to face up to. Furthermore, information needs to be shared between different systems, so it will be a must to guarantee and enable secure communication and protection by means of secure communication channels and integration platforms between systems [11]. A mHealth application must also ensure that data remain confidential, integrity is always guaranteed throughout the whole process and only authorized personnel can have access to it [12]. There are mainly four requirements that such a system has to fulfil:

I. Anonymity – in this kind of service anonymity is essential, since users' personal data cannot be linked with their identity while are being transmitted. The system must protect participants' anonymity throughout the whole process. Occasionally, it could be relevant to request users' personal data, as sex, age, occupation, etc so it is essential that they can assure their confidential information is absolutely anonymous and there isn't any way to verify their truthfulness. Consequently, if users think their data may have been incorrectly treated, they could always decline to include their true information.

II. Confidentiality - Along with anonymity, the application must guarantee that there is no way to link health information with the actual source as well as data confidentiality in transmission. An unauthorized source should never access to the content.

III. Authentication – Health information needs to be authenticated at both the user and application source level in response to the need to ensure anonymity. This service must guarantee that mobile application installed in the mobile is only received by the patient.

IV. Integrity – It's essential the information has not been manipulated in their way from the provider server to the patient's mobile.

2 Design and Implementation

The deployed architecture consists of a mobile device in which a mHealth application is installed; a Proxy Server carries out the security function; a portal web; and a Provider's Server for data management. The web platform offers a management tool for the patient's medical history and active processes. Further, it enables proximity and trustworthiness throughout the interaction with the health workers and providers involved in the process. It also includes a subsystem to be adapted to different mobile phone models in order to achieve a fair presentation of the record in the mobile phone. Due to the use of a transparent proxy security server the functionality is not affected by the incorporation of the proposed security mechanisms to the web platform.

Data have to be protected in each and every phase of the process: storage, updating, search and retrieval. The system has to assure that data are accurate, correct, and valid and that they have not been modified in the whole process. The mechanism developed to carry out this function is the digital signature that is also used to validate the identity of the user. Cryptography is meant to ensure the network traffic integrity and confidentiality so as the communication between the user and the service provider. The provider-side is validated by means of certificates and SSL protocol guaranteeing that authenticity is always verified [13].

The mHealth application has been developed using J2 Micro Edition (J2ME) technology. This technology is mainly supported by Symbian and BlackBerry which own a high percentage of the market. This is the main reason to develop the security library in this language. Since BlackBerry is not fully compatible with all the security libraries like J2ME, it was required to avoid obfuscation and others methods like socket push-registry that are not supported. Figure 3 points out the Global statics of the different mobile OSs in the last 2 years. These data reveal that handsets with J2ME, Symbiam OS, BB OS, Sony Ericsson and some Samsung devices cover more than 50% of the market [14], although Android devices are gaining ground with a 16,23% in the last year. Data are based on mobile web usage and not on physical handsets. Once the operation in J2ME compatible devices was validated, the Android version was fully developed. This platform has been also verified with testing applications and it is actually being integrated within the mHealth service.

The library of security has been implemented using the BouncyCastle lightweight API that works as with J2ME and JDK 1.6. Android has its own libraries of security used to the implementation. Android is a software stack for mobile devices that includes an operating system, middleware and key applications. The Android SDK provides the essential tools and APIs to begin developing applications on the Android platform, using the Java programming language. Each Android application has its own security sandbox once it's been installed on a device.

2.1 Security Mechanisms

The security mechanisms carried out by the security library are the keys generation and storage, the ciphered and signed of the information. Encryption is the main tool used to prevent from reading confidential information. The keys used are RSA. The generation time is a key factor to be considered for usability reasons since a user could become impatient if the application spends too much time in this process. Table 1 shows the measured results of these tests in a common smartphone.

Table 1. Time keys' generation

Size	Time
4096 bits	>5 minutes
2048 bits	approx. 4 min and 30 sec.
1024 bits	approx. 40 sec.
512 bits	approx. 15 sec.

Both J2ME computer simulators and real market devices allowed the generation of keys up to 4096 bits**,** although their generation took too much processing time. Consequently, we opted for using a size of 1024 bits since the keys have an adequate size, compared with other security services and the waiting time for the patient isn't excessive. The size of the server's key is 2048 bits. The keys are stored as in Base64 as Byte arrays in a database with the purpose of being recovered later. Every time the application is open, the system checks those keys that have been stored which means the application has been correctly installed. If the keys weren't stored should be generated and stored in the device database.

2.1.1 Configuration and Information Storage

The configuration of the library is made based on a file sent to the mobile along with the installation file. This file contains the address of the Security Server ciphered with an AES key that is well-known by the mobile application.

There is a register of the different communication that occurs between the server and application. Each register consists of a nickname of the communication initiator, the date and part of the information that has been exchanged. This information is stored inside the mobile device after being ciphered with the same AES key that was used to decipher the configuration file.

2.1.2 Keys Generation and Storage

The library uses two different couples of keys to sign, cipher, and decipher the data and to verify the signature during the user's authentication process in front of the Security Server.

Access to data stored in the Record Management System of the application is granted only if the authorization mode of the RecordStore allows access by the current MIDlet suite. In our case, the access is limited through the parameter "authmode" which is private. The information is also stored ciphered using AES. When some of the information is sent, it will be ciphered and signed in this case with the set of RSA keys and the server public's key so a malware won't be able to interpret it.

The application stores the public key's modules and exponent while the recovering of the private keys is necessary to store modulus, public exponent, private exponent, prime1, prime2, exponent1, exponent2 and coefficient. Each parameter is ciphered with the AES key before being stored.

2.1.3 Cipher and Digital Signature

The data sent from the application to the Security Server are ciphered using the server's public key to ensure that only the Security Servers can access to the information. The confidentiality requirement is fulfilled since the information can only be deciphered by the Security Server. The cipher is made by using the algorithm RSA, in mode Electronic Code Book (ECB) and the padding PKCS1Padding. The signature is made up of the SHAwithRSA algorithm that has been implemented by the BouncyCastle libraries. The digital signature ensures the authentication and integrity requirements.

2.1.4 Security Server

Secure information submission by the application requires a proxy server whose functions are signing/verification and encryption/decryption of information. This server is also in charge of transferring information requests to the Provider's Server, receiving and ensuring the security of the data given as a response.

The requested tasks of the Security Server are identified subsequently:

I. To send public key contains in its certificate.

The server sends data needed to the application in order to rebuild the server's public key that will be used to the ciphered of the information. Data sent are the module and the exponent of the RSA key of 2048 bits.

II. To transfer the information to the destiny:

Once the information is received, the application has to verify the digital signature and, if it is valid, it will later decipher the information since the mobile application sends its public key to the server. All data involved in the process have to be signed; as a result it will be necessary to implement a specific method capable of verifying such a signature and another in charge of carrying out the digital signature and sending it to the mobile application. The Security Server contains also one method to cipher the data sent to the mobile application and another to decipher the information received from it.

Once the Security Server has verified and recovered the information, it's the right time to send the information to the destiny. The destiny can be either the mobile application or the Provider's Server depending on which one was the emitter. The address of the Provider's Server is part of the cipher information that the Security Server receives from the mobile application. The address of the Security Server is included in the configuration file that is then sent to the mobile along with the installation file.

3 Validation

Reliable tests were performed within 40 mobile devices of 5 different brands: Nokia, BlackBerry, Samsung, Sony Ericsson and LG, with a percentage of compatibility of 85%. A device is compatible providing it passes the following tests: a WAP Push SMS reception; the installation file download; the full installation; the initial launch; the keys generation and initial data load; the manual launch; the test of navigability and visualization; the update starting; the data updating and the automatic close. Nowadays, the test application is also compatible with tactile devices. However, some devices have failures in the visualization because of the presentation of base64 characters that are incorrectly showed. This is another source of incompatibility in devices as KU990 Viewty or Samsung M1.

The pilot site of the eHealth platform is being carried out amongst 375 registered volunteers of Vodafone Spain. The pilot will have 9 month of duration. After two months of pilot over 90% of the volunteers have already introduced their data in the web platform and the 34% of them have downloaded the mobile application. The

application's installation success rate is 90% and the failures 10% that were caused by non-compatible devices like iPhone or Android.

A sociological study is also taking place with a double methodology, quantitative, the surveys, and qualitative, the face interview and profiles. An initial survey was carried out amongst volunteers from the age of 17 up to 55, before the platform was tested. This survey has identified different profiles between the registered users and an exhaustive evaluation of the usage reasons will be also conducted within a short period of time. The reasons are mainly: hardly go to the doctor; the possible impact of the application over their health; the time factor the future problems prevention and pregnant.

A face to face interview, whose main goal is to find out volunteers' prospects regarding this kind of systems, will be carried out. At last, a use case survey is carried out each three months to improve the application's features based on volunteers' opinion. This specific survey has three parts related to the web application, mobile application and fulfilled prospects.

The results of the first use case survey shows the rate of acceptance by the users. The Table 2 also reveals the answer of the users to the question: Is it worth having your medical information in the mobile phone? More than 60% of the volunteers agree that the mobile phone application is worth versus the 6% who disagree.

Table 2. Is it worth having your medical information in the mobile phone?

Fully disagree	Disagree	Indifferent	Agree	Fully agree	Total
2,73%	2,73%	28,18%	38,18%	28,18%	100,00%

4 Conclusions and Future Research

The developed architecture provides usable security mechanism in the exchanging process of sensible data between devices and external entities. Both the device used, a smartphone, and the technology chosen for the developed platform allow to integrate mHealth application with other existing network technologies. It is portable and operational in a timely appropriate period and also compatible with a high rate of available devices of the market regardless of the operating system: RIM or Symbian that covers most of mobile devices.

For the time being, the conclusions drawn, considering the analysis of data and statistical association tests (Chi2, C Pearson and V Kramer), state that: gender and age don't influence the inserted data; having a chronic pain may raise the prospects, but the number of data inserted: maternity/paternity can also gradually/highly increase the interest towards the platform, even as a service for children.

Work is in progress on the Android version mobile application integration within the eHealth platform and on the development of new features to improve the system interactivity.

Acknowledgements. This research has been supported by the Ministerio de Industría, Turismo y Comercio under project TSI-020302-2009-85 and the Ministerio de Ciencia e Innovación of Spain under project TIN2010-20510-C04-01. The authors would like to acknowledge the contribution of the volunteers from Vodafone Spain.

References

1. Tessier, C.: Management and Security of Health Information on Mobile Devices. American Health Information Management Association (AHIMA), Chicago (2010)
2. Huang, X., Jiang, Y., Liu, Z., Kanter, T., Zhang, T.: Privacy for mHealth presence. International Journal of Next-Generation Networks (IJNGN) 2(4), 33–44 (2010)
3. Ren, Y., Werner, R., Boukerche, A.: Monitoring Patients via a Secure and Mobile Healthcare System. Wireless Technologies for EHealthcare. IEEE Wireless Communications, 59–65 (2010)
4. Alasaarela, E., Nemana, R., DeMello, S.: Drivers and challenges of wireless solutions in future healthcare. In: 2009 IEEE International Conference on eHealth, Telemedicine, and Social Medicine, pp. 19–21 (2009)
5. Curioso, W.H., Karras, B.T., Campos, P.E., Buendía, C., Holmes, K.K., Kimball, A.M.: Design and Implementation of Cell-PREVEN: A Real-Time Surveillance System for Adverse Events Using Cell Phones in Peru. In: AMIA Annu. Symp. Proc. 2005, pp. 176–180 (2005)
6. Kumar, A., Chen, J., Paik, M., Subramanian, L.: ELMR: Efficient Lightweight Mobile Records. In: MobiHeld 2009, Barcelona, Spain, pp. 69–70 (2009)
7. Health Level Seven International, http://www.hl7.org
8. GSMWorld: GSMA Mobile Privacy Initiative Discussion Document: Privacy Design Guidelines For Mobile Application Development (2011)
9. Ministerio del Interior. Gobierno de España: Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (1999), http://www.mir.es/SGACAVT/derecho/lo/lo15-1999.html
10. Papadopoulos, H., Pappa, D., Gortzis, L.: Legal & Clinical Risk Assessment Guidelines in Emerging m-Health Systems. In: Itab 2006, Congress Center Du Lac, Ioannina (2006)
11. Rubin, A.D.: Security Considerations for remote electronic voting. Communications of the ACM 45(12), 39–40 (2002)
12. Report of the WHO Global Observatory for eHealth, World Health Organization (2006)
13. Smith, M., Buchanan, W., Thuemmer, C., Hazelhoff Roelfzema, N.: Analysis of Information governance and patient data protection within primary health care. International Journal for Quality in Health Care, 1353–4505 (2010)
14. StatCounter Global Stats. Worldwide Mobile OS, http://gs.statcounter.com/