Integrated Citizen Centered Digital Health and Social Care
A. Värri et al. (Eds.)

doi:10.3233/SHTI200701

A Secure Protocol for Managing and Sharing Personal Healthcare Data

Athanasios KIOURTIS[a,1], Argyro MAVROGIORGOU[a], Sofia-Anna MENESIDOU[b], Panagiotis GOUVAS[b] and Dimosthenis KYRIAZIS[a]
[a]*Department of Digital Systems, University of Piraeus, Piraeus, Greece*
[b]*Ubitech Ltd, Athens, Greece*

Abstract. Current technologies provide the ability to healthcare practitioners and citizens, to share and analyse healthcare information, thus improving the patient care quality. Nevertheless, European Union (EU) citizens have very limited control over their own health data, despite that several countries are using national or regional Electronic Health Records (EHRs) for realizing virtual or centralized national repositories of citizens' health records. Health Information Exchange (HIE) can greatly improve the completeness of patients' records. However, most of the current researches deal with exchanging health information among healthcare organizations, without giving the ability to the citizens on accessing, managing or exchanging healthcare data with healthcare organizations and thus being able to handle their own data, mainly due to lack of standardization and security protocols. Towards this challenge, in this paper a secure Device-to-Device (D2D) protocol is specified that can be used by software applications, aiming on facilitating the exchange of health data among citizens and healthcare professionals, on top of Bluetooth technologies.

Keywords. Device-to-Device protocol, Health Information Exchange, HL7 FHIR

1. Introduction

The current medical world is surrounded by healthcare information stored either locally (on each device) or remotely (on computer clouds) – among others, with the overall purpose of being exchanged among authorized people who can gain value from it [1]. The exchange of this data can be performed through multiple ways (wired, wireless, physical documents), at various distances, achieving different goals in terms of transmission rate, security, or platform applicability. In the electronic healthcare domain, the exchange of information between citizens - patients and healthcare practitioners (HCPs), is characterized of great importance, since a medical condition and solution can be found much faster, while the overall life quality can be improved. Currently, European Union (EU) citizens have very limited control over their own health data, despite the fact that several countries are using national or regional Electronic Health Records (EHRs) for realizing virtual or centralized national repositories of citizens' health records. Among others, what is missing is to complement and integrate the current interoperability infrastructures with new technologies for health data exchange that is

[1] Corresponding Author, Athanasios Kiourtis, 80, M. Karaoli & A. Dimitriou St., 18534 Piraeus, Greece; E-mail: kiourtis@unipi.gr.

centered on the citizen, which does not demand the coordination by a superior authority, thus leaving more control of the health data to its owner. While there are specific cases (e.g. authorization to buy a medication abroad) that demand coordination among government institutions, there are many cases (e.g. a medical visit abroad) that do not, and for which the exchange of personal health data could be better handled directly by the citizen. At present, citizens often carry their own paper medical documents for such medical visits. However, it would be more effective if citizens could carry or access their data in a digital form. This paper addresses the current lack of standardization and security, by presenting a set of integrated protocols, supporting secure data exchange and portable local storage, released as open specifications in order to perform short-range distance Health Information Exchange (HIE) [2] among the different stakeholders. Hence, a secure Device-to-Device (D2D) protocol is specified, based on small-scale wireless technologies and in particular Bluetooth technologies [3], with the overall goal to be adopted at a pan-European level for the safe exchange of medical records between a smart mobile device and a health information system.

The remainder of this paper is organized as follows. In Section 2, the methodology followed to specify the D2D protocol is being provided, while Section 3 depicts the overall evaluation results of the proposed D2D protocol. Section 4 includes a short discussion of the derived results, presenting our concluding remarks.

2. Methods

In order to conclude to the usage of the Bluetooth short range wireless communication technology in the D2D protocol, an exhaustive research took place among the most widely used short range distance communication protocols. The top-four candidates [4] for the D2D protocol were the Wi-Fi direct, Bluetooth v4.0, Bluetooth Low Energy (BLE), and Near Field Communication (NFC). In this context, since it was within our plans to exchange large files of healthcare data (e.g. medical images), for BLE and NFC we concluded that they should not be included due to their low data rates. As a result, Wi-Fi direct and Bluetooth v4.0 were the top-two choices. In that case, Wi-Fi direct had 10 times better data rate than Bluetooth, but since Wi-Fi direct supports unidirectional communication instead of the Bluetooth that supports bidirectional communication, we concluded that Bluetooth would be the best option for our needs (Table 1).

Table 1. Short-range wireless communication technologies comparison.

Criterion	Wi-Fi Direct	Bluetooth v4.0	BLE	NFC
Range	Up to 180m	Up to 100m	Up to 10m	Up to 4cm
Data Rate	Up to 250 Mbps	Up to 25 Mbps	Up to 200 kbps	Up to 424 kbps
Security	High	High	High	Medium
Power Consum	High	Medium	Low	Low
Communication	Unidirectional	Bidirectional	Bidirectional	Unidirectional

Regarding the D2D protocol, it can be best described as a series of different Bluetooth messages that contain the information that is being exchanged, in terms of healthcare related data, between an HCP and a citizen, without using internet connection. Before continuing the description of the D2D protocol, the following terms should be identified: “medical application of a citizen (smart Electronic Health Record application (S-EHR-app))” and “application of medical staff (Healthcare Practitioner application (HCP-app))”. A S-EHR-app is any application installed on a personal mobile device that

can store a user's personal health data securely (encrypted). Such an application may contain user health information generated and signed by the healthcare provider, but may also contain data stored and produced directly by citizens or sensors (e.g. smartwatches). An HCP-app is a software application designed to provide medical staff with access to and use of patient data from a S-EHR-app, with the goal of securely exchanging health data with any S-EHR-app, using different protocols. The overall specification of the D2D protocol is based on exchanging HL7 FHIR healthcare data [5], following the steps of Fig. 1, that occur between the citizen and the HCP, using their S-EHR-app and HCP-app.

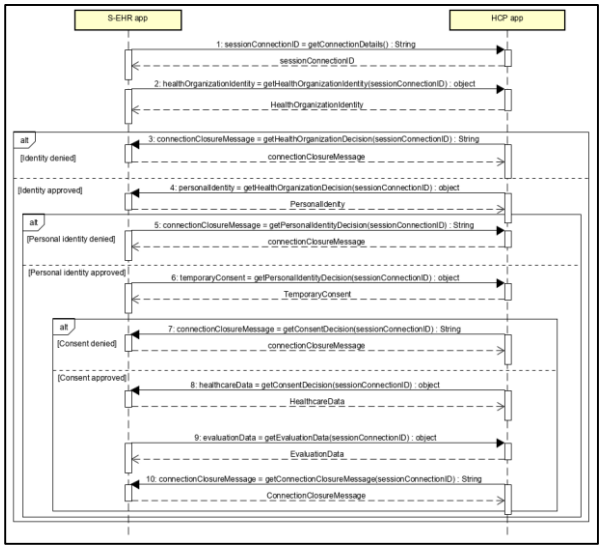

Figure 1. Data exchange phases of the D2D protocol.

In deeper detail, the steps of the D2D protocol have been categorized into five main phases, based on the different functionalities that they offer: (i) in the Connection phase, the HCP-app gets the advertised connection request from the side of the S-EHR-app so as to initiate the Bluetooth connection, (ii) in the Demographic Data Exchange phase, as soon as the connection has been done, the S-EHR-app gets the Healthcare Organization identity in order to identify the HCP and the Healthcare Organization. After that, in the case that the citizen approves the Healthcare Organization identity, the HCP-app gets the Personal Identity data from the side of the citizen, in order for the HCP to identify the citizen. Again, in the case that the HCP approves the Personal Identity data of the citizen, the S-EHR-app receives a consent request from the side of the HCP-app, in order for the HCP-app to have access to the citizens' healthcare data, (iii) in the Consent exchange phase, it is included the approval of the consent from the side of the S-EHR-app, and as a result the exchange of Healthcare Data. Hence, if the S-EHR-app approves the consent, then the HCP-app receives as a reply the requested healthcare data. On the contrary, if the consent request is not approved, the connection terminates, (iv) in the Data Exchange phase, as described before, the reply to the consent request is the healthcare related data from the side of the S-EHR-app. Hence, the HCP examines this data, and sends back to the citizen her consultation results, (v) in the Connection Closure phase, the S-EHR-app, as soon as the consultation results' data has been received, sends to the HCP-app a specific connection closure message, in order for the Bluetooth connection to terminate.

On top of the D2D protocol phases, a security protocol has been specified for performing encryption in transit, consisting of five phases, towards establishing an encrypted communication channel (Fig. 2). More particularly, the existing phases are as follows: (i) in the Bootstrap phase, the prerequisites regarding certificate acquisition on both entities are performed, (ii) in the Identity Management (IDM) phase, each entity verifies the identity of the other entity by certificate exchange and signature verification, (iii) in the Consent Management phase, the citizen gives her consent for process upon her data, (iv) in the Key Establishment phase, a symmetric key establishment happens for secure communication, while (v) in the Encrypted Communication phase, both parties use the established symmetric key to transfer data in an encrypted form.

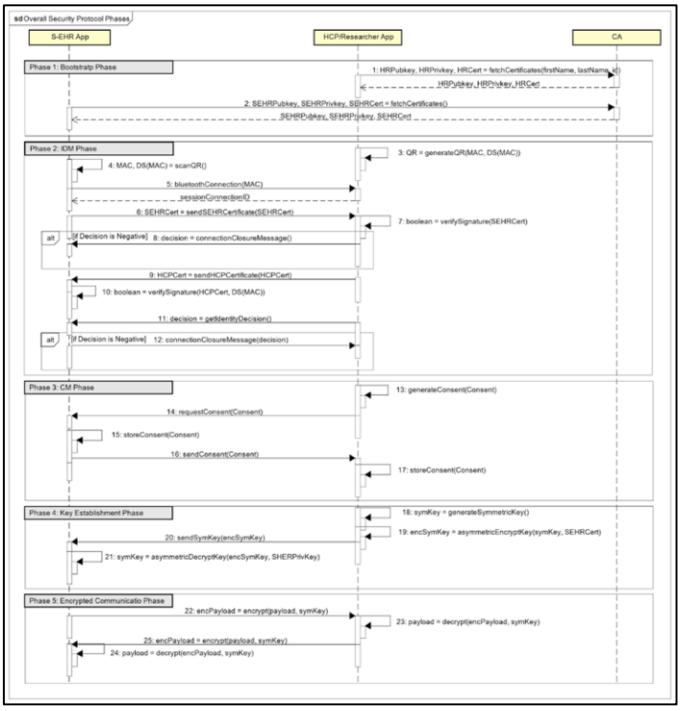

Figure 2. Security phases of the D2D protocol.

3. Results

In order to evaluate the proposed overall protocol, two applications were created in Java for Android and Windows, using Android Studio and NetBeans accordingly, for sending and receiving healthcare data based on the described flow. The scenario on top of which we have based in order to specify the D2D protocol and implement its functionality, was the one of a medical visit abroad. Shortly, in this scenario it is assumed that an Italian citizen who already has her data stored on her S-EHR-app, is visiting an HCP in Greece. Hence, these two parties have to connect to each other, identify themselves, and finally exchange healthcare related data. The overall flow of Fig. 1 was followed, providing us with the expected results. Fig. 3 displays a few screenshots of the developed applications that confirm the functionality of the protocol on top of the medical visit scenario,

showcasing the scanning of a Quick-Read (QR) code for performing the Bluetooth connection, the personal details of the HCP, and the closure of the Bluetooth connection.

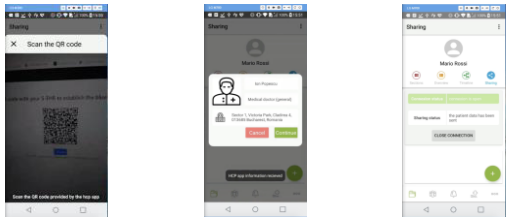

Figure 3. Medical visit abroad scenario.

4. Discussion & Conclusions

In this paper, a secure protocol was specified, based on small-scale wireless technologies (Bluetooth) that aims to be adopted at a pan-European level. The current specification is based on a globally used short-range distance data exchange protocol, being compatible by the main market operating systems (e.g. Android, Apple, Windows). Among the most innovative novelties is the fact that through the D2D protocol, it happens a secure data exchange process with minimum user interactions and fast response times, while the citizens are given the ability to manage their own healthcare data, with consultation data being provided back to them, without the interaction of any other third party.

For our next goals, we are planning to redesign some operations on exchanging health data, to provide the option for the citizen to send partial information (upon request) of a HL7 FHIR resource, to add operations for transmitting additional types of health data, and finally to perform evaluations with different communication technologies (e.g. Wi-Fi Direct), respecting privacy issues, based on the mechanism developed in [6].

Acknowledgment

The research has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106 (InteropEHRate project).

References

[1] Ezekiel E, Wachter R. Artificial intelligence in health care: will the value match the hype?. Journal of the American Medical Association. 2019;321(23):2281-2282.
[2] Mello M, et al. Legal barriers to the growth of health information exchange−boulders or pebbles?. The Milbank Quarterly. 2018;96(1):110-143.
[3] Zeadally S, et al. 25 years of Bluetooth technology. Future Internet. 2019;11(9):194.
[4] Abdulnabi M, et al. A distributed framework for health information exchange using smartphone technologies. Journal of biomedical informatics. 2017;69:230-250.
[5] Saripalle R, et al. Using HL7 FHIR to achieve interoperability in patient health record. Journal of biomedical informatics, 2019;94:103188.
[6] Kiourtis A, et al. Towards a Secure Semantic Knowledge of Healthcare Data Through Structural Ontological Transformations. Joint Conf. on Knowledge-Based Software Engineering. 2018;178-188.