Improving Health Information Exchange through Wireless Communication Protocols

Athanasios Kiourtis
Department of Digital Systems
University of Piraeus
Piraeus, Greece
kiourtis@unipi.gr

Argyro Mavrogiorgou
Department of Digital Systems
University of Piraeus
Piraeus, Greece
margy@unipi.gr

Dimosthenis Kyriazis
Department of Digital Systems
University of Piraeus
Piraeus, Greece
dimos@unipi.gr

Alessio Graziani
Engineering Ingegneria Informat.
SpA - R&D laboratory
Rome, Italy
Alessio.Graziani@eng.it

Francesco Torelli
Engineering Ingegneria Informat.
SpA - R&D laboratory
Rome, Italy
Francesco.Torelli@eng.it

***Abstract*—Health Information Exchange (HIE) allows healthcare providers and citizens, to access and securely share healthcare information electronically, improving the speed, quality, safety, and cost of patient care. Exchange of this information can be achieved through a wired or wireless way, at close or long distances, achieving different goals in terms of transmission speed, exchange reliability and data transfer security. While HIE cannot replace provider-patient communication, it can greatly improve the completeness of patients' records. Most of the current research is devoted on exchanging health information among healthcare organizations, without giving the ability to the citizens on exchanging healthcare data with healthcare organizations and be able to manipulate this data, mainly due to lack of standardization and security guarantees. Towards the goal of HIE, and the ability of citizens to have access to their healthcare data, in this paper two different wireless communication protocols (Remote-to-Device (R2D) and Device-to-Device (D2D)) are specified that can be used by software applications. The goal of the R2D protocol is to facilitate the acquirement of healthcare data of a citizen from an Electronic Health Record (EHR) through internet connection, while the D2D protocol aims on facilitating the exchange of this health data among citizens and healthcare professionals, on top of Bluetooth.**

Keywords— Wireless Communication, Health Information Exchange, Device-to-Device, Remote-to-Device

I. INTRODUCTION (*HEADING 1*)

Today's digital environment is characterized by the sheer number of devices connected to the internet that produce and consume large sets of data that need to be retrieved, evaluated, and used to trigger different actions [1]. This data is stored either locally (on each device) or remotely (on computer clouds), with the ultimate goal of being exchanged among people who can extract additional knowledge from it, by analyzing or combining the extracted knowledge with other sets of information. The exchange of this information can be achieved through a wired or wireless way, at close or long distances, achieving different goals in terms of transmission speed, exchange reliability and data transfer security. In particular, in the field of electronic healthcare, the exchange of data between citizens - patients and medical staff, is characterized as vital, since in this way a medical problem can be identified faster, a medical solution can be found rapidly, and the quality of the life of the citizens can be improved. It is said that "True healthcare interoperability means that information can flow wherever it is needed, across borders and health systems" [2]. Currently, citizen's health data is stored in different systems scattered among several hospitals and healthcare providers. In order to better support the continuity of care, several countries are adopting national or regional Electronic Health Records (EHRs), so as to realize virtual or centralized national repositories of citizens' health records. In this way, healthcare operators have centralized access to medical records produced by different public or private providers. In 2015, according to WHO global survey on eHealth [3], 59% of Member States in the WHO European Regions had a national EHR system and 69% of Member States had legislation supporting the use of their national EHR systems. What is more, directive 2011/24/EU on patients' rights [4] promotes the exchange of information among European states. However, a full integration among European states is still far from being realized. There are some initiatives, such as the Connection Europe Facility (CEF) [5] and the eHealth Digital Service Infrastructure (eHDSI) [6] that are working to this end, which are however initial steps, while their integration is complicated by the EHRs of different countries adopting different regulations and modalities of integration.

Currently, European citizens have very limited control over their own health data [7]. Hence, what is missing is to complement and integrate the current interoperability infrastructures with new technologies for health data exchange centered on the citizen, that does not require the coordination by a superior authority and that leaves more control of the health data to the citizen. While there are specific situations (e.g. authorization to buy a medication abroad) that do require 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 records for just this reason. However, it would be more convenient if citizens could carry or access their data in a digital form. There exist online services offering personal health record (PHR) management, but these are typically limited to data produced by the citizen (e.g. wellness data) and/ use cloud-based storage. Nevertheless, many citizens do not want to store their data on cloud storage belonging to private organizations, since they are increasingly conscious that their data are highly sensitive and valuable, and do not want to lose control over it. At the same time, several hospitals and private healthcare providers already allow patients to access digital versions of their medical records. However, each organization uses different data formats and access modalities, which makes it difficult for the citizens to manage and exchange data with other healthcare operators.

Such fragmentation arises from the lack of a common standard for the exchange of health data between citizens and healthcare institutions. Having in mind that most of the citizens own some kind of smart device (e.g. smartphone, tablet), it would be natural to use these devices to store and exchange medical records with healthcare operators and research institutions. Unfortunately, this is likewise prohibited due to the lack of standardization and security guarantees. This paper addresses the current lack of standardization and security, by presenting a set of integrated protocols and conformance criteria for mobile applications, supporting secure data exchange and portable local storage, released as open specifications, in order to perform Health Information Exchange (HIE) [8] among the different stakeholders. For short-range distance HIE, a secure Device-to-Device (D2D) protocol is specified. This protocol is based on small-scale wireless technologies and in particular Bluetooth technologies [9], and aims 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. For long-range distance HIE, a secure Remote-to-Device (R2D) protocol that functions over the internet (i.e. HTTP protocol [10]) is specified, which is used for the import of health data from EHRs to the citizen's mobile device and for the subsequent periodic synchronization operations. Through the current research, it is provided a way for the citizens both to carry their health data with them in digital form, and to manage it easily even when they are abroad. Citizens' benefits include the obtaining of health data from a foreign healthcare provider, being able either to share their personal health data directly with a local healthcare professional (HCP) using a secure and private communication mechanism similar to contactless payments, or to download their personal health data from a distant operator using encrypted internet communication.

The remainder of this paper is organized as follows. In Section II, an analysis of different research works and projects is being provided, concerning both the D2D and the R2D protocols. Section III depicts a high-level specification of the proposed protocols, while Section IV includes an evaluation of the specified protocols, through a specific scenario. In the same section, a short discussion is being provided regarding the applicability of the specified protocols. Finally, Section V presents our next steps and concluding remarks.

II. Related Work

Before referring to the importance and originality of the current research and its related work, the following terms should be identified: the "medical application of a citizen (i.e. Smart-EHR (S-EHR) application)" and the "application of medical staff (i.e. Healthcare Professional (HCP) application)". A S-EHR app is any application installed on a personal mobile device that is able to safely store a user's personal health data. Such an application contains user health information generated and signed by the healthcare provider, but may also contain data stored and produced directly by citizens or by sensors (e.g. smartwatches). An HCP application is any software application designed to allowing the medical staff securely exchange health data (e.g. medical prescription, medical evaluation data) with any S-EHR app using the specified data exchange protocols.

A. *Device-to-Device (D2D) Related Work*

With the explosion of available wireless devices, there has also been a big increase of wireless protocols and standards to support all of that technology. Below is a short list of the most commonly used short-range wireless communication standards and technologies. ANT and ANT+ [11] are sensor network technologies used for collecting and transferring sensor data. This short-range wireless communication technology is a type of personal-area network (PAN) that features low power consumption and long battery life. Bluetooth [9] is another category of such systems, which is covered by the IEEE 802.15.1 standard. Originally created as an alternative to cabled RS-232, Bluetooth is now used to send data from PANs and mobile devices. This plug-and-play technology utilizes the 2.4-2.485 GHz band and has a standard range of 10 meters, being able to be extended to 100 meters at maximum power with a clear path. Bluetooth Low Energy (BLE) [9] has a simpler design than Bluetooth and is a direct competitor of ANT+, focusing on health and medical applications. Another category refers to the EnOcean [12], which is self-powered and able to wirelessly transmit data by using ultra-low power consumption and energy collecting technology. Instead of a power supply, EnOcean's wireless sensor technology collects energy from the air. What is more, Near Field Communication (NFC) [13] is an ultra-short-range technology created for contactless communication between devices. It is often used for secure payment applications, fast passes and similar applications. Operating on the 13.56 MHz ISM frequency, NFC has a maximum range of around 0,2 meters, which provides a more secure connection that is usually encrypted. Among others, Radio-Frequency Identification (RFID) [14] is another Device-to-Device communication protocol that uses small, flat, cheap tags that can be attached to anything and used for identification, location tracking, and inventory management. When a reader unit is nearby, it transmits a high-power RF signal to the tags and reads the data stored in their memory. ZigBee [15] should be mentioned, as the standard of the ZigBee Alliance. The path of a message in this network zig-zags like a bee. It is a software short-range wireless communication technology that uses the 802.15.4 transceiver as a base and is meant to be cheaper and simpler than other WPANs, like Wi-Fi or Bluetooth. To this end, Wi-Fi Direct [16] should be mentioned, initially called Wi-Fi P2P, which is a Wi-Fi standard enabling devices to easily connect with each other without requiring a wireless access point. Wi-Fi Direct allows two devices to establish a direct Wi-Fi connection without requiring a wireless router. Hence, Wi-Fi Direct uses a single radio hop communication, instead of multihop wireless communication that mainly use the wireless ad hoc networks and the mobile ad hoc networks. Finally, Z-Wave [17] should be mentioned as a wireless communications short-range technology that was used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance, allowing wireless control of residential appliances and other devices.

Several protocols at the application layer have been developed so far, aiming to cover all the aforementioned aspects, being potentially applicable to IoT [18-21]. One of the most popular is the Message Queuing Telemetry Transport (MQTT) [22] protocol, which is a TCP-based open-source publish-subscribe protocol developed by IBM for messaging applications. In the same concept, the Data Distribution Service (DDS) [23] protocol has been developed, a TCP-based protocol that features decentralized nodes of clients across a system and allows these nodes to identify themselves as subscribers or publishers through a localization server. Another protocol is the Constrained Application Protocol (CoAP) [24] that is a stateless protocol developed by the IETF to replace HTTP in resource-constrained devices. In 2010, IBM developed "Stream Computing" techniques [25], through which people can use the real-time analysis techniques to help intensive care patients, which it is very helpful in the healthcare area. Thus, various researchers have put their effort upon the healthcare data exchange protocols. Chen et al. [26] proposed a secure healthcare data exchange protocol based on a cloud environment, where they used mobile devices' characteristics, allowing people to use medical resources on the cloud environment and seek medical advice conveniently. Seo et al. [27] proposed a WBAN MAC protocol for contention-based medical and consumer electronics (CE) applications. Berman [28] presented a threshold protocol that can facilitate the exchange of healthcare information by splitting information into pieces, where none of which contains sufficient information to recreate the original text. Santos et al. [29, 30] presented a system that enables Personal Health Devices (PHDs), mobiles, and CE devices to share health sensor data with local and internet services using CoAP and IEEE 11073 [31], evaluating how the IEEE 11073 communication model should be adapted for CoAP. Another key technology utilized for data exchange is NFC, supported by NFC Forum [32], as it was described in Section II.

B. Remote-to-Device (R2D) Related Work

Importing health data in a standard way from EHRs of several European countries is a very challenging subject. At the moment, each Member State has its own EHR, based on proprietary Application Programming Interfaces (APIs), proprietary data models and proprietary data representation. These EHRs have been designed in order to satisfy only requirements coming from stakeholders of the Member State itself and not to be interoperable with each other. Many steps have been performed by the European Union (EU) in order to foster interoperability between European eHealth systems, especially through the activities of the eHealth Network (established under Article 14 of Directive 2011/24/EU of the European Parliament and of the Council) and the CEF Programme [5]. The most important project regarding cross border health data exchange financed by the EU is the European eHealth Digital Services Infrastructure (eHDSI), whose objectives are the initial deployment and operation of services for cross-border health data exchange under the CEF. The architecture of eHDSI is based on a closed and trusted federation of National Contact Points (NCP) one for each Member State named eHDSI Circle of Trust, whereas a NCP is a software component representing a Member State's EHR. A NCP provides a reduced-but-common API designed for allowing EHRs of EU countries to interoperate with each other in order to exchange health data. Another important European project that supports the interoperability between European eHealth systems, through using HL7 Fast Healthcare Interoperability (FHIR) [33] or HL7 Clinical Document Architect (CDA) standards, is the International Patient Summary (IPS) project [34]. This joint project, participated by HL7 and European Committee for Standardization (CEN), has specified a European Standard for the representation of a Patient Summary, following guidelines adopted by the European eHealth Network (eHN). The project has followed two main development lines: one to define the specifications and the other one to obtain the status of standard by CEN. The project started by the initial proposition of the Patient Summary dataset proposed by eHN in 2013, and then produced the official IPS specifications adopted by eHN and published in 2019. The Argonaut project [35] is, instead, a private sector initiative aiming to advance industry adoption of modern, open interoperability standards. This project is not an organization for the definition of new standards, but its objectives are to accelerate and promote the adoption of FHIR and OAuth in healthcare provisioning and related architectural patterns. Integrating the Healthcare Enterprise (IHE) [36] is another joint initiative, globally extended, developed with the aim of creating one methodology to make systems and IT entities of the health sector interact with each other. The IHE experience saw the light in 1998 in the United States in response to growing problems of interoperability in the field of radiology. The Fatherhood of the organization is attributable to two user associations: the Radiological Society of North America (RSNA) and the Healthcare Information and Management Systems Society (HIMSS). After a few years IHE also took hold in European countries and, at present, the structure of the initiative is divided into three wide Regions of interest (North America, Europe, and Asia) in turn organized by nations. Although its committee is made up of users and manufacturers of these systems, the IHE organization was born as a non-profit organization, the main objective of its initiative is, in fact, to promote the culture of integration, through an accurate definition of clinical needs and a combined use of the most important standards. In essence, the ultimate goal of this strategy is to speed up and make health integration, and clinical practice in general, more efficient.

C. Advancements beyond the Related Work

While most research projects in the health domain exploited D2D communication mainly for monitoring and for accessing body and environmental sensors, the D2D protocol described in this paper exploits D2D communication, together with the HL7 FHIR standard, for bidirectional exchange of any kind of health data between EMRs terminals and smart devices running the S-

EHR application. The proposed D2D protocol will provide an additional option to the citizens for the exchange of data with healthcare providers, ensuring higher confidentiality than the internet-based communications' confidentiality. Using the HCP application or an extended EMR application, an authorized HCP will be able to send and receive any health data, including data produced by other cross-border healthcare organizations and collected by the patients on their S-EHR running on personal smart devices (e.g. smartphones). While most applications for mobile health adopt proprietary APIs for accessing only specific services, the R2D protocol is an open specification that describes how any EU citizen may access to any EU healthcare service to download her personal Health Records on a personal mobile device. The protocol exploits the eIDAS architecture [38] for the identification of EU citizens in compliance with current regulations and defines a specific profile of the standard HL7 FHIR API for supporting citizen's access. The R2D specification includes also a mapping of eHDSI access methods to HL7 FHIR access methods that defines how citizens may access to the same kind of standard documents provided to the HCPs by means of eHDSI NCPs. This mapping is intended to simplify the adoption of R2D by service providers that already provided an integration with eHDSI. On the other hand, the R2D protocol goes further the eHDSI capabilities as its API supports the access of any kind of health information covered by the HL7 FHIR standard, including the ones identified by the recent EU recommendation for EHR exchange [39].

III. SPECIFICATION OF D2D AND R2D PROTOCOLS

A. Protocols Overview

The most characteristic aspect of this research is the assumption that the HRs of a citizen are collected and integrated on her mobile device. Every exchange of health data among software applications can be realized using one of the following data exchange protocols: the D2D protocol for short-range distance transmission over Bluetooth, and the R2D protocol for remote (long-range) transmission over the internet. Both the D2D and the R2D protocols will be used for standardizing how software applications exchange health data with the mobile application (S-EHR application) of the citizen, including additionally - in the case of the D2D protocol, the application (HCP application) of the healthcare practitioner. The main focus of this section is to define the technical specifications of these two protocols, providing also detailed descriptions of their contexts of use, and overall functionality, accompanied by an explanation of their separate purposes of existence.

The D2D protocol specifies a series of Bluetooth messages for health data exchange (e.g. in terms of successful or failed health data exchange) between a healthcare practitioner (utilizing the HCP application) and a citizen (utilizing the S-EHR application), without the usage of internet connection. Differently from the D2D protocol, the R2D protocol functions over the internet and defines the set of operations for acquiring the health data of a citizen from an EHR (e.g. the national EHR, the EHRs of hospitals, laboratory results or other kind of healthcare providers' results) to her S-EHR application. It should be noted that additional variants of the R2D protocol, not detailed in this paper, are under definition, to cover other use cases, such as the uploading of health data to the Cloud (S-EHR Cloud) for periodic backup, adopting an encrypted format that the cloud service provider cannot decrypt, to fully protect the citizen's privacy. Another use case is to allow authorised hospitals to access the Cloud in case of emergency, when the citizen is unable to interact with the healthcare practitioner.

The overall data exchange options are depicted in Fig. 1. The citizen imports (using the R2D) her past health records from the EHR of one country (e.g. the National EHR system of her Country A) to the S-EHR application installed on her smart mobile device. Thanks to local storage she is able to consult any health record in any moment, transfer them to HCPs in another Country (e.g. Country B) or receive new health records from them, also when internet connection is not available (using D2D). Additionally, she (may execute a backup to the Cloud (using R2D Cloud) – which is out of the context of the current paper. All the operations are coordinated by the citizen using the S-EHR application, while the citizen is under the total control of her health data. It should be mentioned that the data exchange with R2D is possible only if the citizen owns a valid eIDAS identity [38], whilst the data exchange with D2D is possible only after the citizen has been identified by the HCP and the citizen has given the needed consent to the healthcare organization of the HCP.

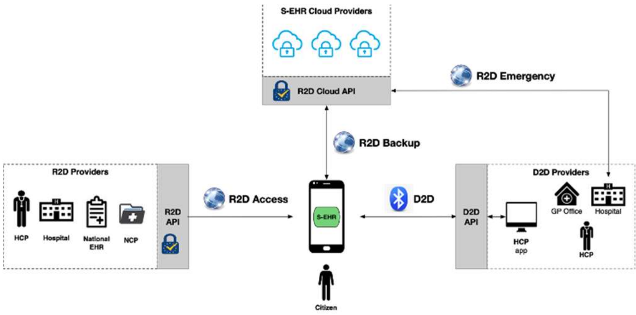


Fig. 1. Overall data exchange process.

B. D2D Protocol High-level Specification

The D2D protocol defines the Bluetooth operations represented by the interfaces that are offered by the mobile application and the healthcare's organization application speaking of the S-EHR application and the HCP application correspondingly. These interfaces are exposed and used by the two main actors of the D2D protocol, namely the citizens and the HCPs. These two actors are the only involved ones in the overall interaction, for exchanging the consent of accessing each one's personal data, the healthcare related data, and the evaluation data (i.e. healthcare data in the form of evaluation data, which are created after the examination of the HCP) accordingly. The first interface is responsible for offering the Bluetooth operations and services for the S-EHR application for interconnecting, exporting messages and receiving requests from the HCP application, while the second interface is responsible for offering the Bluetooth operations and services for the HCP application for similar types of tasks from the S-EHR application. Since, the overall communication is based on the Bluetooth short-range wireless communication technology, the initial step of the D2D protocol is the two involved applications to pair and bond their devices, prior to exchanging any messages. Fig. 2 displays the overall interactions and connection between a citizen's S-EHR application and an HCP application at conceptual level.

Following, a detailed description of the sequence diagram of Fig. 2 takes place. These steps are classified into five (5) main categories: (i) Bluetooth Connection, (ii) Demographic Data Exchange, (iii) Consent Exchange, (iv) Healthcare Data Exchange, and (v) Bluetooth Connection Closure.

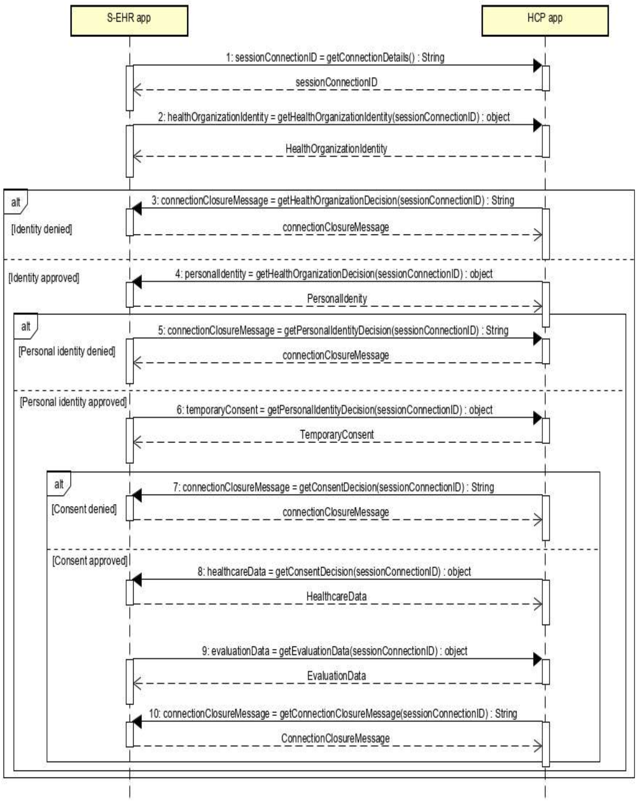


Fig. 2. D2D protocol specification.

1) Bluetooth Connection

Step 1: The S-EHR app gets the connection's unique session identifier in the form of a secret String. In order to assure that the string remains secret among the two parties, this step uses a Quick Response (QR) code generated by the HCP application, which hides the aforementioned string. Hence, this interaction is not a Bluetooth related interactions, but it is based on the visual interaction between the citizen's mobile device camera and the HCP's computer screen. This String will be used by both sides (S-EHR app and HCP application), for the current's connection identification purposes. As the D2D protocol is specified on top of the Bluetooth standard, this step also includes the standard sequence of messages for the Bluetooth connection process.

2) Demographic Data Exchange

Step 2: The next step is for the S-EHR application to get the Healthcare Organization identity.

Step 3-4: At this point the citizen checks if the Healthcare Organization is the one she intends to interact with and decides whether to approve the connection or not. As soon as the decision has been made, the HCP application gets the decision from the side of the S-EHR application. This operation will return, one either (a) a connection closure message in the form of a String, indicating that the Health Organization identity was not approved, hence the connection will be closed, or (b) the demographic data of the S-EHR application owner in the form of an Object (Patient).

Step 5-6: In the case that the Healthcare Organization identity has been approved, the S-EHR application gets the decision from the side of the HCP application, regarding whether the provided demographic data are approved or not by the HCP - i.e. if they correspond to the identity of the citizen visiting the HCP. As in the previous cases, this operation will return either (a) a connection closure message in the form of a String, indicating that the demographic data was not approved, hence the connection will be closed, or (b) the temporary consent request of the HCP application owner in the form of an Object (Consent), requesting the permission to access the health data of the citizen's S-EHR application for a specific purpose.

3) Consent Exchange

Step 7-8: In the case that the temporary consent has been requested, the HCP application gets the decision from the side of the S-EHR application, regarding whether the consent for getting the S-EHR application owner's data has been approved or not. As in the previous cases, this operation will return either (a) a connection closure message in the form of a String, indicating that the temporary consent was not approved, hence the connection will be closed, or (b) the requested healthcare data of the S-EHR application owner (i.e. data that has been approved for sharing) in the form of an Object (HealthcareData, representing a set of health records).

4) Healthcare Data Exchange

Step 9: In the case that the healthcare data has been provided, the S-EHR application gets the Evaluation Data (i.e. new health records) from the side of the HCP application (after the examination), to be stored to the S-EHR application.

5) Bluetooth Connection Closure

Step 10: The last step includes the HCP application to get the final message of the connection closure, after the overall interaction has successfully ended.

C. R2D Protocol High-level Specification

The R2D protocol is an internet based protocol that defines the set of operations used for enabling the download of health data by the S-EHR application, acting on behalf of a citizen from an EHR provider (e.g. a hospital, or a national health record system). Although R2D focuses on the exchange of healthcare data, it requires some security operations to authenticate a citizen. These security operations are the only operations that do not exchange healthcare data, and must be considered as preliminary operations invoked to enable a secure exchange of healthcare data. Authenticating to the EHR, is the only way to gain access to the core R2D functionalities for the exchange of healthcare data. R2D has two main states: (a) AUTHENTICATED, which is the state that allows the use of the operations for the exchange of healthcare data, and (b) NOT_AUTHENTICATED, which is the state that does not allow the use of the operations for the exchange of healthcare data, but allows only the use of the operations for the authentication of a citizen. Once a citizen is authenticated and the protocol is in the AUTHENTICATED state, all the R2D operations for the exchange of healthcare data can be used, without any restrictions and without the need of following restrictions in the sequence of operations. Fig. 3 illustrates the overall flow, outlining the usage of the methods getLastRecord(), getRecords(), and getRecord().

Following, a detailed description of the sequence diagram of Fig. 3 occurs, outlining the two (2) main categories of the (i) Authentication, and (ii) Healthcare Data Import.

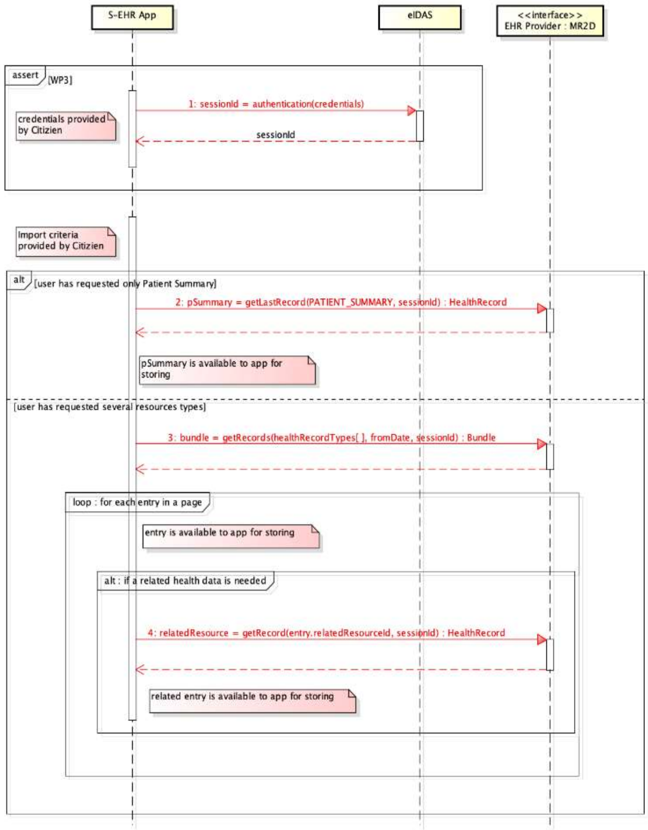


Fig. 3. R2D protocol specification.

1) Authentication

Step 1: This is a preliminary step that moves the R2D state from NOT_AUTHENTICATED to AUTHENTICATED and allows the application citizen to gain access to all the services of the R2D protocol.

2) Healthcare Data Import

Step 2 (getLastRecord): This is an optional step executed only if the citizen wants to download only the last record of a certain type (e.g. her last patient summary). In this case the S-EHR application invokes the protocol method named getLastRecord (), providing as input the type of the requested data (e.g. PATIENT_SUMMARY). The method returns to the client the most recent instance of HealthRecord of type HealthRecordType.PATIENT_SUMMARY. The patient summary is then available to the client for storing.

Step 3 (getRecords): This and the following step are an alternative to Step 2. This step is performed by the citizen to trigger the import of several health data from the remote repository. Its parameters are: (i) healthRecordTypes[] that is an array indicating the list of types (chosen from a closed enumeration of values) of health data requested by the client, and (ii) fromDate that is a date, constraining to return only the health records produced after that date. This method returns an instance of Bundle containing only the first of the overall pages that compose the entire result.

Step 4 (getRecord): At this point, the client has obtained the first page of the overall results and starts looping the items of the current page (entries of the Bundle) processing each one of them. If during this processing, the client needs to download a health data related to the one under processing, the S-EHR application will invoke the protocol method named getRecord(), passing the id of the related resource as input. After this invocation, the client can process both the primary health data and its related resource.

Each one of the R2D conceptual operations correspond to a specific operation of the standard FHIR API and to specific constraints applied to it.

D. Conceptual Data Model

This section describes the conceptual data model used by both the D2D and the R2D protocols. The following class diagram (Fig. 4) depicts this data model, showcasing the main classes and their relationships. In Table 1, a brief description of each class of the data model is provided, based on the HL7 FHIR structure. The two central classes of the data model are (i) the Patient class that represents the citizen, and (ii) the HealthRecord class that represents the health data of one of the following types: patient summary, prescriptions, dispensation, laboratory report, medical image, or discharge report (health data types indicated by EU guidelines about European Electronic Health Record exchange format [39]). In Table 1, a brief description of each class of the data model is provided, based on the HL7 FHIR structure.

TABLE I. DESCRIPTION OF THE DATA MODEL CLASSES

Data Model Class	Description
HealthRecord	It represents any possible health data of the patient (Patient Summary, laboratory analysis, set of medical images, etc.).
HealthRecordType	An enumeration representing the set of defined kinds of health data. Values of HealthRecordType have been defined to match the baseline of the EU Cross Border.
Patient	It represents an individual receiving care or other health-related services.
HealthCareProfessional	It represents an individual providing care or other health-related services to a patient.
HealthCareOrganization	It represents any organization offering health-related services.
Consent	It is used to express a consent regarding healthcare, given by a patient (grantee) to a healthcare provider (grantor).
Bundle	It is a container for sets of instances of HealthRecord class. It corresponds to an HL7 FHIR Bundle.
ResponseFormat	It represents the format required by the client S-EHR of health data to be returned.

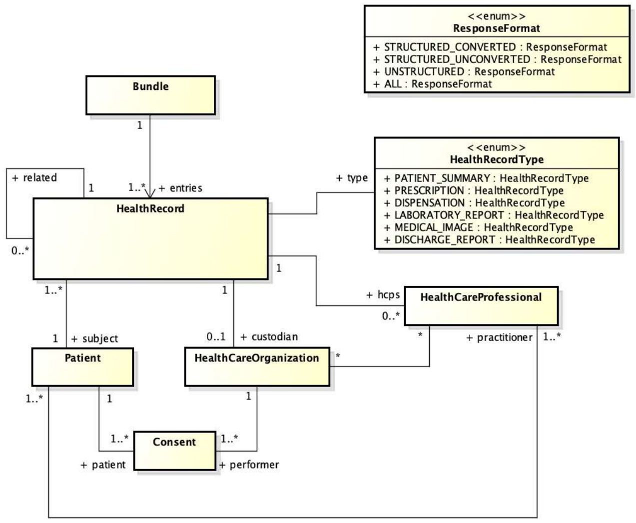


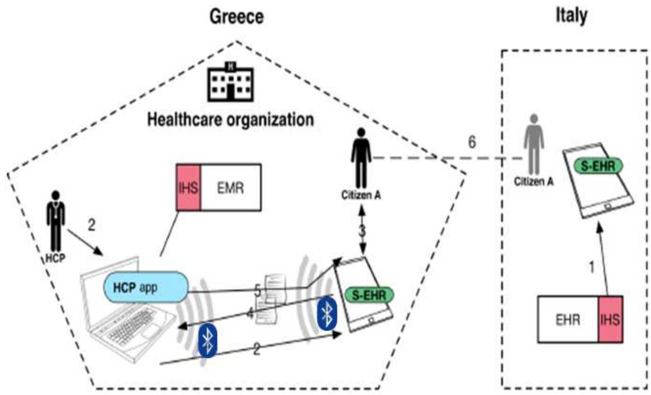
Fig. 4. D2D and R2D conceptual data model.

IV. PRELIMINARY EVALUATION

An open source reference implementation as a set of Java libraries for Windows and Android, has been realised for both the D2D and R2D protocol. As the protocols are based on an open specification, alternative interoperable implementations for other platforms are possible as well. In order to test the overall specification of the protocols, as well as the reference implementation, the libraries have been integrated into three testing applications (a representing model of an EHR, a S-EHR application and an HCP application) have been developed. They offer a basic interface just for testing purposes. The model of the S-EHR application runs on Android v4.3.1, while the model of the HCP application and the EHR have been developed in Java v8.0 They are also based on the Java reference implementation of HL7 FHIR (HAPI).

For both protocols, the following testing scenario was followed: "In Italy data are imported from an Italian EHR on the S-EHR application of a citizen using the R2D protocol. Afterwards, the same citizen travels abroad (in Greece), and must visit a healthcare organization. An HCP requests the authorization to access the citizen's healthcare data through her S-EHR. The citizen authorizes the HCP - using the S-EHR application by exploiting the D2D protocol, to access a portion (e.g. allergies, adverse effects to drugs etc.) of her health data. The authorization is temporary (i.e. it will be automatically removed as soon as the edge to edge connection will not be available anymore). The HCP accesses the shared data from the HCP application and after the evaluation of the received healthcare data, the HCP prescribes a new therapy plan for the citizen. In the end, the citizen receives the new prescription on her S-EHR application, again exploiting the D2D protocol. The citizen leaves the office and the HCP cannot access the citizen's data anymore (the authorization of the HCP is automatically removed). Fig. 5 illustrates the aforementioned scenario.

For the experimentation purposes, the overall process described in the specification of the protocols (Section III) regarding the operations to be invoked was successfully followed. Since the applications were only developed for evaluation purposes, with a very basic User Interface, in the current document it is avoided depicting specific figures of the applications' interfaces during the HIE process, since both applications display only the content of the exchanged messages in XML format. According to the overall results, the protocols' specification and the sequence of the exchanged messages was strictly followed, thus providing the capabilities offered by the two protocols. Through this way it was provided to the citizens the ability using only their smart mobile devices to securely travel along with their healthcare data, and exchange it with the interacting healthcare practitioners, even in the cases where no internet connection is available.



Evaluation scenario of a medical visit.

V. CONCLUSIONS

Secure HIE can allow healthcare providers and citizens-patients, to access and share the latter's vital healthcare information electronically, improving the speed, quality, safety and cost of patient care. While HIE cannot replace provider-patient communication, it can greatly improve the completeness of patients' records. Towards the goal of HIE, in this paper two different protocols have been described that can be used by software applications facilitating (i) the acquirement of healthcare data of a citizen from an EHR, and (ii) the exchange of this data among citizens and healthcare professionals. With the implementation of the D2D protocol it becomes feasible to achieve the exchange of healthcare related data between a healthcare practitioner and a mobile application of a citizen, without the usage of internet connection, whereas with the implementation of R2D it becomes feasible to exchange healthcare related data between any EHR and a mobile application of a citizen, with the usage of internet.

The benefits of these two protocols became clear upon the implementation of a specific healthcare data exchange scenario, where both protocols were utilized for downloading and transferring healthcare data among the authorized stakeholders. It should be noted that through these protocols, the citizen is given the opportunity to have her healthcare data in her possession, being able not only to manage it as she wants, but also to transfer / exchange them wherever she is, avoiding the transfer of paper based documents as an evidence of her current state of health. Both the D2D and R2D protocols specify the communication interfaces, but they are not creating any constraints at the programming interfaces. Different libraries based on different APIs and for different platforms may interoperate. Concerning future research on the D2D protocol, the possibility to exploit different D2D communication technologies other than Bluetooth is under investigation. Regarding the specification of the R2D protocol, the focus is on the transfer of multiple types of healthcare data, which is continuously increasing. In the upcoming versions of both protocols, it is within our goals to adjust their specifications for additional types of medical and non-medical data (e.g. different kind of medical images), to perform comparisons with similar implementations, and to evaluate the specified protocols in additional scenarios. Through the latter, improvements and updates can be made on their specification, to facilitate and improve the HIE, so to realise the vision of Smart EHRs in people's hands across the EU.

ACKNOWLEDGMENT

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

REFERENCES

[1] Number of connected devices reached 22 billion, where is the revenue?, https://www.helpnetsecurity.com/2019/05/23/connected-devices-growth/

[2] IHE Developing Integration Profile for the International Patient Summary, https://www.ihe.net/news/ihe-developing-integration-profile-for-the-international-patient-summary/

[3] Status of eHealth in the WHO European Region, http://www.euro.who.int/__data/assets/pdf_file/0013/303322/fact-sheet-status-of-ehealth-in-who-european-region.pdf?ua=1

[4] DIRECTIVE 2011/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0024

[5] Connecting Europe Facility, https://ec.europa.eu/inea/en/connecting-europe-facility

[6] Governance model for the eHealth Digital Service Infrastructure during the CEF funding, https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+GOVERNANCE

[7] S. Courbier, et al., "Share and protect our health data: an evidence based approach to rare disease patients' perspectives on data sharing and data protection-quantitative survey and recommendations", Orphanet journal of rare diseases, vol. 14(1), 2019, p. 175.

[8] M. Soto, C. Sicotte, and A. Motulsky, "Using Health Information Exchange: Usability and Usefulness Evaluation", Studies in health technology and informatics, vol. 264, 2019, pp. 1036-1040.

[9] Bluetooth Core, https://www.bluetooth.com/specifications/bluetooth-core-specification/

[10] HTTP Specifications and Draft, https://www.w3.org/Protocols/Specs.html

[11] ANT+, Website: https://www.thisisant.com/consumer/ant-101/what-is-ant

[12] EnOcean Self-powered IoT, Website: https://www.enocean.com/en/

[13] NFC forum, Website: https://nfc-forum.org/

[14] How RFID Works: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm

[15] Zigbee alliance: https://www.zigbee.org/

[16] Wi-Fi Direct: https://www.wi-fi.org/discover-wi-fi/wi-fi-direct

[17] Z-wave: https://www.z-wave.com/

[18] R. Sutaria, and R. Govindachari, "Making sense of interoperability: Protocols and Standardization initiatives in IOT". In 2nd Int Workshop on Computing and Networking for Internet of Things, 2013, p. 7.

[19] Z. Sheng, et al., "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities". IEEE wireless communications, vol. 20(6), 2013, pp. 91-98.

[20] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey. Computer networks", vol. 54(15), 2010, pp. 2787-2805.

[21] A. Asensio, A. Marco, R. Blasco, and R. Casas, "Protocol and architecture to bring things into internet of things", Int Journal of Distributed Sensor Networks, vol. 10(4), 2014, pp. 158-252.

[22] MQTT protocol specification, http://mqtt.org

[23] DDS protocol specification, http://www.omg.org/spec/DDS

[24] Constrained Application Protocol, http://coap.technology

[25] IBM web site, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/streamcomputing/

[26] C. L. Chen, T. T. Yang, and T. F. Shih, "A secure medical data exchange protocol based on cloud environment". Journal of medical systems, vol. 38(9), 2014, p. 112.

[27] Y. S. Seo, et al., "OCDP: A WBAN MAC protocol for contention-based medical and CE applications". 4th International Conference on Ubiquitous Information Management and Communication, 2010, p. 12.

[28] J. J. Berman, "Threshold protocol for the exchange of confidential medical data". BMC Med research methodology, vol. 2(1), 2020, p. 12.

[29] D. F. Santos, et al. "A personal connected health system for the Internet of Things based on the Constrained Application Protocol". Computers & Electrical Engineering, vol. 44, 2015, pp. 122-136.

[30] D. F. Santos, et al., "Integrating IEEE 11073 and constrained application protocol for personal health devices". 29th Annual ACM Symposium on Applied Computing, 2014, pp. 466-467.

[31] IEEE. ISO/IEEE 11073-20601: Health informatics - Point-of-care medical device communication – Part 20601: Optimized exchange protocol Standards, first edition.

[32] NFC forum, https://nfc-forum.org/

[33] HL7 FHIR, https://www.hl7.org/fhir/

[34] IPS Project, http://international-patient-summary.net/mediawiki/index.php?title=Main_Page

[35] Argonaut Project, https://argonautwiki.hl7.org/Main_Page

[36] Integrating the Healthcare Enterprise, https://www.ihe.net/

[37] European guidelines for cross border exchange of patients' health data, https://ec.europa.eu/digital-single-market/en/news/european-guidelines-cross-border-exchange-patients-health-data-considered-leading-reference-set

[38] Discover eIDAS, https://ec.europa.eu/digital-single-market/en/discover-eidas

[39] Exchange of Electronic Health Records across the EU, https://ec.europa.eu/digital-single-market/en/exchange-electronic-health-records-across-eu