Patients to Mobilize Their Data: Secure and Flexible mHealth Delegation

Rafael Almeida[a], Pedro Vieira-Marques[b] and Ana Ferreira[c]
CINTESIS - Centro de Investigação em Tecnologias e Serviços de Saúde, Faculty of Medicine of Porto, Porto, Portugal

Keywords: Access Control, Delegation, Data Sharing, mHealth, Token-based Authentication, mHealth App.

Abstract: This work describes the development of a prototype of a secure and flexible delegation architecture, to be applied to an mHealth scenario where a mobile app is used for monitoring and coaching asthma patients. The motivation is the fact that mHealth apps are not security prepared and patients still have no trust in using them, on a regular basis. Nonetheless, patients can acknowledge mHealth potential and see the relevance of sharing/delegating health data to others, e.g., healthcare professionals, depending not only on the necessity and security, but also on the level of control they can have over it. This proposal empowers the patient to control, in a flexible, easy and secure way, fine-grained delegation features within a real mHealth setting.

1 INTRODUCTION

Research has confirmed that mobile app users have security and privacy concerns when using mHealth apps in their daily lives (Zhou, 2019) (Kotz, 2016), something that can help justify their low usage and adherence (Papageorgiou, 2018). Zhou et al. concluded that mHealth users want to know how health care providers apply access control to their data and suggest the development of strong, but easy-to-use security features, with clear privacy policies, to encourage mHealth apps' use (Zhou, 2019).

But this is just one step in the mobile security chain. Patients should not only trust that authorized people access their records, but they also need to be able to securely share and delegate access whenever and to whomever is necessary. Prasada et al. identified that patients' ability to share their personal data collected via mHealth devices, with their friends, family, third parties and the public, could limit their willingness to use mHealth apps and reduce their adherence and long-term use (Prasad, 2012). On another study, many participants were reluctant to share personal information because people considered health-related information such as exercise and dietary patterns, as private matters (Peng, 2016). Although most of the participants were not favourable to sharing personal information, they would do it, depending on the necessity, security and proper mechanisms to control what data and with whom they would share them (Peng, 2016).

As delegation is needed to meet the requirements for flexible and responsive access to resources (Rabehaja, 2019), developers must consider that mHealth users may change their sharing decisions over time, as their privacy concerns are not static. Current research must focus on sensible default settings and flexible privacy controls for different recipients (Prasad, 2012), and provide incentives to foster continued use (Peng, 2016).

The main contribution of this work is a prototype of a secure and flexible delegation architecture, applied to a real mHealth setting for controlling and coaching asthma patients, namely AIRDOC. Patients can delegate their data with professionals in a simple yet secure and fine-grained way, providing patient empowerment to control who accesses what, in terms of delegation needs.

[a] https://orcid.org/0000-0002-5488-8450
[b] https://orcid.org/0000-0003-4174-2820
[c] https://orcid.org/0000-0002-0953-9411

Almeida, R., Vieira-Marques, P. and Ferreira, A.
Patients to Mobilize Their Data: Secure and Flexible mHealth Delegation.
DOI: 10.5220/0008972905520560
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 552-560
ISBN: 978-989-758-399-5; ISSN: 2184-4356

2 RELATED WORK

Delegation is a concept that simply translates into sharing or delegating tasks, duties, or roles (delegator) to another subject (delegatee) (Schaad, 2002), who will act on behalf of the delegator. Usually, the delegatee is a third-party outside the realm of the access control policy defined for that system. This is why delegation provides flexibility and dynamism to a fixed access control policy. In healthcare, delegation can be a necessity, for instance, for a professional to consult a colleague's opinion on a patient's diagnosis or to verify continuous monitoring of a chronic patient. Proper security and privacy must be provided for the patient to trust that transaction, or the patient's health outcomes could be seriously compromised (Boulos, 2014).

The authors did not find in the literature the implementation of delegation in real mHealth scenarios. Most delegation works focus on the formal metamodeling and/or the theoretical extension of existing access control models (Schefer-Wenzl, 2014). A general overview of the literature for the past ten years is shown in Figure 1.

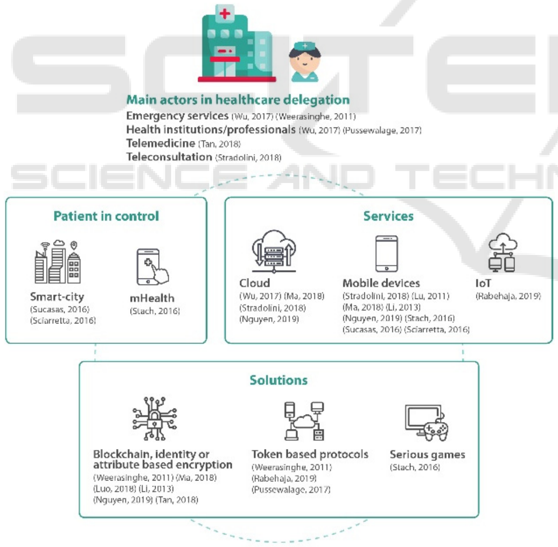

Main actors in healthcare delegation
Emergency services (Wu, 2017) (Weerasinghe, 2011)
Health institutions/professionals (Wu, 2017) (Pussewalage, 2017)
Telemedicine (Tan, 2018)
Teleconsultation (Stradolini, 2018)
Patient in control
Smart-city (Sucasas, 2016) (Sciarretta, 2016)
mHealth (Stach, 2016)
Services
Cloud (Wu, 2017) (Ma, 2018) (Stradolini, 2018) (Nguyen, 2019)
Mobile devices (Stradolini, 2018) (Lu, 2011) (Ma, 2018) (Li, 2013) (Nguyen, 2019) (Stach, 2016) (Sucasas, 2016) (Sciarretta, 2016)
IoT (Rabehaja, 2019)
Solutions
Blockchain, identity or attribute based encryption (Weerasinghe, 2011) (Ma, 2018) (Luo, 2018) (Li, 2013) (Nguyen, 2019) (Tan, 2018)
Token based protocols (Weerasinghe, 2011) (Rabehaja, 2019) (Pussewalage, 2017)
Serious games (Stach, 2016)

Figure 1: Healthcare delegation actors, used services, solutions and patient in control – review of last 10 years.

In terms of delegation architectures, those described in the most recent literature commonly include cloud services that comprise authentication, processing and storage services, and constitute also a middleware to connect both end points (e.g., an EHR with emergency medical services (Wu, 2017) or healthcare providers (Weerasinghe, 2011)). However, using cloud services can hinder a transparent view on the security controls that are (or are not) used (Stradolini, 2018). Most cloud privacy relies on cryptographic protocols but these may not be used for all services in the cloud system (Li, 2013).

For authentication of the parties and establish secure and trustable communications, the most used protocols are OAuth2 (OAUTH 2, 2019) (Sucasas, 2016) (Sciarretta, 2016) (Ferretti, 2017) and token-based. Since OAuth2 is a tested, light and still reliable protocol, together with token-based features, this can be a simple solution to establish a one-time secure communication channel for temporary delegation purposes (Weerasinghe, 2011).

For the works which empower the patient to control what data are shared to other parties, Stach et al. claims that the user defines what data and how accurate they are, can be shared with the game, providing a fine-grained and extendable permission system (Stach, 2016). However, the patient (children with diabetes) may not have the dexterity/experience to decide on what should be shared and how (especially in sharing their location as provided by the game features). Another work allows the citizen/user to authorize the mobile app to access protected resources, on their behalf (Sucasas, 2016). This work is not used in practice. Work (Sciarretta, 2016) does not focus on mHealth, but presents a delegation mechanism for Smart City mobile apps, which is used in practice. The solution is based on OAuth2, with a strong security assessment but with flat grant/deny delegation options for fixed situations.

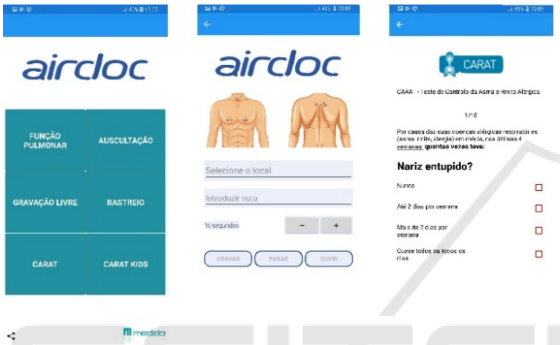
Our delegation architecture reuses available and tested solutions and protocols such as OAuth2 and openID, with token-based authentication, so it does not rely on a cloud-based architecture, and is implemented in a real mHealth setting.

3 METHODS

A literature review was performed to find techniques used to implement delegation and retrieve the requirements that could be applied to our use case scenarios. The search was performed in July 2019 in the IEEE Xplorer, ACM and Scopus online databases, of articles published after 2009 (last ten years) with search terms such as: "sharing or delegation patient and health professional mobile app"; "delegation mobile"; "delegation mobile health". Titles and abstracts were reviewed by one researcher and those which referred to sharing and/or delegation of mHealth (mobile and/or IoT) data with professionals or other health related entities, were included. Twenty papers were selected to be read fully and, after the analysis, a total of 14 papers were included in the review for further perusing secure delegation architectures to identify necessary requirements (2 papers were not directly related to the subject; 2 were similar from the same authors but published on different places; and 2 others were not describing delegation schemes but analysed mHealth and sharing perceptions and needs).

The following step was to define personas associated with the main use cases for the domain where those were going to be applied (section 4).

Then a new delegation approach was defined to face the specific AIRDOC requirements. A prototype was implemented and tested within a mobile app simulation (sections 4 & 5).



CARA - Teste de Controlo da Asma e Rinite Alérgica

1/10

Por causa das suas doenças alérgicas respiratórias (asma, rinite, alergia) em média, nas últimas 4 semanas quantas vezes teve:

Nariz entupido?

Nunca □

Até 2 dias por semana □

Mais de 2 dias por semana □

Quase todos ou todos os dias □

Figure 2: AIRDOC mHealth app screenshots: first menu page, symptoms location and CARAT survey (left to right).

4 AIRDOC – THE mHEALTH APP

4.1 AIRDOC - The Project

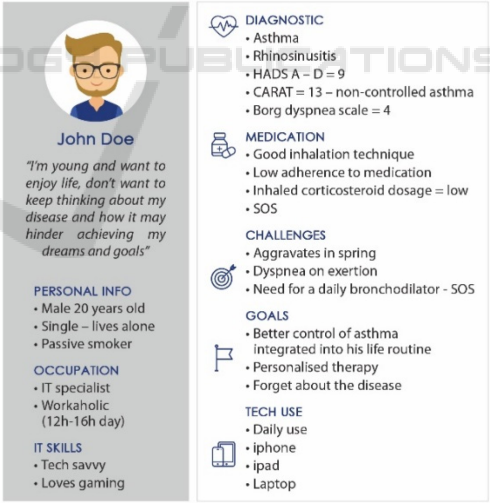
The project AIRDOC aims to develop *a Smart Mobile Application for Individualized Support and Monitoring of the Respiratory Function and Sounds of Chronic Obstructive Patients (CORD)* (AIRDOC, 2018). Current tools for CORD self-monitoring and self-managing are complex, unattractive, not individualized and require laborious analysis by health professionals, discouraging their use and integration. AIRDOC wants to make use of the ubiquitous presence of smartphones in everyday life, their embedded sensors (e.g., microphone) as well as their processing and communication abilities. AIRDOC aims also to focus on security, privacy and interoperability requirements to impact on the innovation of CORD healthcare, with increased patient involvement and empowerment (Figure 2).

4.2 Use-Case Delegation Scenario

The success of the AIRDOC project mostly depends on the simple, but also, secure and private integration and communication between patients, health professionals, family and friends, for supporting the patient in their daily health monitoring capabilities. For this, the functionality of delegation is one of the first to be integrated within its access control model. This section presents a use-case of a *persona* who needs to use the AIRDOC mHealth application (AIRDOC app) as a self-monitoring device and shares data with his/her health professional.

4.2.1 Persona

For applications to be more successful and used on a daily basis, they need to represent the users that are going to be engaged and benefit from the application, and not what the developers think is needed. A persona puts a face and personal contextual attributes to that user (all fictitious), who represents the target population (Platt, 2016). A photograph and demographic data - such as name, age, gender, marital status, occupation, education, IT skills, health history and how the mHealth application might achieve their goals - are associated to the persona. Figure 3 presents the persona for our use case (Section 4.2.2).



John Doe

"I'm young and want to enjoy life, don't want to keep thinking about my disease and how it may hinder achieving my dreams and goals"

PERSONAL INFO
- Male 20 years old
- Single – lives alone
- Passive smoker

OCCUPATION
- IT specialist
- Workaholic (12h-16h day)

IT SKILLS
- Tech savvy
- Loves gaming

DIAGNOSTIC
- Asthma
- Rhinosinusitis
- HADS A – D = 9
- CARAT = 13 – non-controlled asthma
- Borg dyspnea scale = 4

MEDICATION
- Good inhalation technique
- Low adherence to medication
- Inhaled corticosteroid dosage = low
- SOS

CHALLENGES
- Aggravates in spring
- Dyspnea on exertion
- Need for a daily bronchodilator - SOS

GOALS
- Better control of asthma integrated into his life routine
- Personalised therapy
- Forget about the disease

TECH USE
- Daily use
- iphone
- ipad
- Laptop

Figure 3: Persona describing a patient use-case for the AIRDOC mHealth application.

4.2.2 Use-Case Description

The persona is an Asthmatic who wants to delegate access to his health monitoring data, stored within the AIRDOC app, to the professional who has been treating him or to another professional, not directly

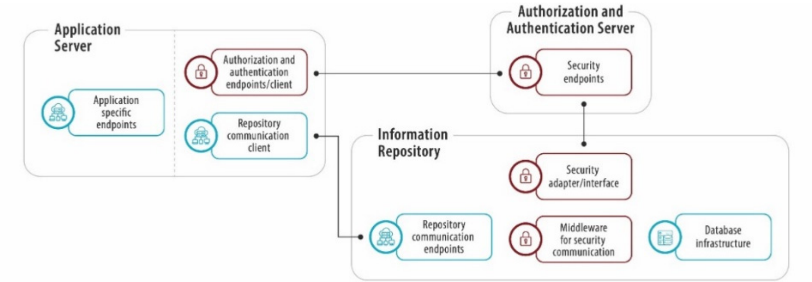

Application Server
Application specific endpoints
Authorization and authentication endpoints/client
Repository communication client
Authorization and Authentication Server
Security endpoints
Information Repository
Security adapter/interface
Repository communication endpoints
Middleware for security communication
Database infrastructure

Figure 4: Architecture of the mHealth delegation AIRDOC prototype.

related to his treatment, but who can be helpful, at a certain moment, about his condition (Figure 3).

Delegation Scenario: John is having trouble controlling asthma symptoms lately so he is going for a consultation with another specialist recommended by a friend. At the consultation, the doctor verifies that John can probably beneficiate from a tool that can be integrated into his routine activities and use of technology, in order to closely control symptoms, medication adherence and improve recommendations at any moment. She tells John to install the AIRDOC app, an asthma coaching mHealth app to help him follow medication plans and adopt suggested behaviours for controlling asthma. In order for the doctor to closely monitor the first months of Johns'new therapy, John installs the app and decides to activate the delegation feature:

1. *John opens and accesses the AIRDOC app, and starts the delegation functionality to delegate his data to a "related" professional, someone who is following him at the moment*
2. *John must insert a code in the app, given by the doctor, as a means to securely identify John to that doctor*
3. *Doctor's AIRDOC app asks if she accepts to receive data from that patient*
4. *The doctor accepts*
5. *A message is sent to both John and the doctor asking them to revise and confirm the data that are going to be shared, and with what parties*
6. *John and the doctor must agree to delegation terms and conditions to finalize the delegation process*
7. *Authentication messages and/or tokens are exchanged, and access to John's data is delegated to the doctor*
8. *Secure communications are established and delegation is set for a pre-defined period of time, or until any of the parties revoke the request.*

5 DELEGATION PROPOSAL

5.1 Delegation Architecture

Figure 4 presents the main components of the developed architecture delegation prototype. These comprise an: 1) Application Server, responsible for supplying the application with the necessary request resources and/or information; 2) Authorization and Authentication Server, the main responsible for security communications of the whole architecture; and 3) Information Repository.

The authentication procedure is implemented with the OAuth2 protocol together with the Authorization and Authentication Server, using a hybrid flow, which is a combination of implicit and authorization flow. This server contains basic user and role information (login/pass), as well as an identifier for user identification, authentication and authorization to the AIRDOC app. The Information Repository contains all medical and personal data.

When a request is received from the app, it is intercepted by the "Middleware for security communication" component, which directs the: a) authorization token, b) the type of CRUD action (e.g., create, read, update, delete, or other), c) the type of accessed resource, d) the resource identifier and e) any parameters on the request query, onto the "Security adapter/interface". This component contains: a) a client to communicate with the security server using introspect endpoints which validate the security token, and retrieve the user's ID and role; b) configurable role permissions; and c) the ownership/delegation verification pipeline process.

Security server information is used to setup the client and the general role permissions, using a Role Based Access Control model, by validating the retrieved user's role and intended action. This is required to implement the interfaces of the methods used during the ownership/delegation verification pipeline process, in order to tell the system how to search for user's security details. This verification uses context specific implementations to determine who is the data owner, and if there is any delegation using that same data, in the repository.

5.2 Delegation Prototype

Specific to the delegation prototype, the described components comprise various technologies:

- **Authorization and Authentication Server:** uses the Identity4 framework, which includes both OAuth2 and openID protocols. This is used to create our own identity server to contain core user information and recognized roles to be applied during the authorization process;
- **Application Server:** a simple NodeJS stub server was used to simulate the OAuth2 protocol steps and perform information requests to verify ownership and delegation;
- **Information Repository:** most of the work was implemented here for the storage needs of the repository to comply with the prototype goals, which the application server could request, as well as keep track of user's relations (where applicable), and between stored information. It also maintains a register of all the delegation processes.

All of these characteristics and requirements led to the decision of using the FHIR standard (FHIR, 2011). This standard allows the information regarding user, and associated roles to be stored on FHIR resources called Person, Patient, Related Person and Practitioner. To implement the delegation functionality and store related data on FHIR, a resource named Consent is created. This resource was designed to formally describe a given authorization by a resource owner, to another actor in the system, detailing what information is shared and what type of access is given. For the actual prototype implementation, the HAPI-FHIR framework (HAPI-FHIR, 2014) was chosen because it introduces most required functionalities to build a working prototype in JAVA language. As for the database, considering that FHIR naturally allows the use of JSON to describe and communicate data, we decided to use the nosql database MongoDB, in which JSON documents can be directly stored, with no extra processing work.

5.2.1 Generic Communication Flow

Figure 5 shows the communication flow and queries performed between the components of the architecture, to generally execute a resource request, as well as what differs in the communication, when the request is a delegation request (pink rectangle).

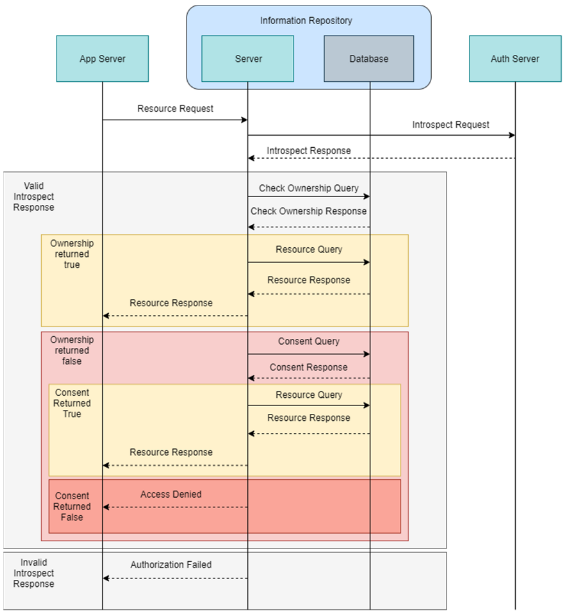


Figure 5: Generic activity diagram to perform the use-case delegation procedure described in section 4.

Steps for this execution are the following:

- **Resource Request:** the user accesses the AIRDOC app and requests access to resources – since it is using REST standard, it should contain the resource(s) ID and type, along with the security token created earlier for the user;
- **Introspect Request:** request for the security token validation, user (security) id and role information;
- **Check Ownership Query:** an implemented interface method which asks the information repository for the internal and security ID of the owner. If retrieved security ID is the same as the one retrieved from the introspect request, we can assume it is indeed the owner and proceed with the resource request. Otherwise it is required to check for delegation consent;
- **Consent Query:** another implemented interface method which uses the resource request security ID, retrieves the system ID of the user, to be used with the resource owner system ID, to verify the existence of any active delegation consent. If such consent exists, the resource request may proceed. Otherwise an unauthorized access should be issued. Later work should be done to parse the consent for specific content details authorization.

5.2.2 Delegation Communication Flow

For the delegation process to be possible, both entities (Actor A and Actor B – Figure 6) need to already be

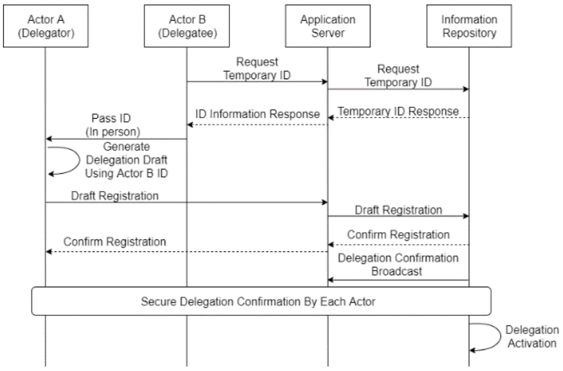
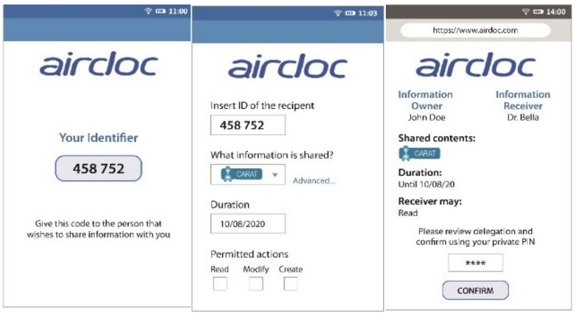


Figure 6: Activity diagram - delegation request.

recognized on the information repository, which in the context of the prototype, means to already have a Person resource created for each actor, ready to be used for delegation rights assignment. For most of this process, the application server acts only has a middlelayer, passing the requests received from the application onto the information repository.

To start the delegation process, Actor B, or the delegate, the health professional, henceforward called Doctor Bella, requests a temporary ID to be issued from the application server. This ID should be human readable, since, when received by Doctor Bella, it is passed, in person, to actor A, or the delegator, in this case the patient, John Doe (Figure 7 - left). With that temporary ID, John can build a delegation draft where he gives the required permissions to the ID, given to him by the Doctor, but still, for the moment, unrecognized by the application (Figure 7 - middle). The delegation draft is then communicated to the information repository via the application server. Once on the repository, the temporary ID is replaced by Doctor Bella's formal ID and the draft is stored in the database, waiting for confirmation.


11:00

airdoc

Your Identifier

458 752

Give this code to the person that wishes to share information with you

11:03

airdoc

Insert ID of the recipent

458 752

What information is shared?

CARAT Advanced...

Duration

10/08/2020

Permitted actions

Read □ Modify □ Create □

14:00

https://www.airdoc.com

airdoc

Information Owner
John Doe

Information Receiver
Dr. Bella

Shared contents:
CARAT

Duration:
Until 10/08/20

Receiver may:
Read

Please review delegation and confirm using your private PIN

****

CONFIRM

Figure 7: AIRDOC app - Doctor Bella's temporary ID, passed on to John (left); the patient drafts the delegation consent for Doctor Bella (middle); delegation consent draft sent to all delegation parties, for confirmation with a personal PIN, previously set (right).

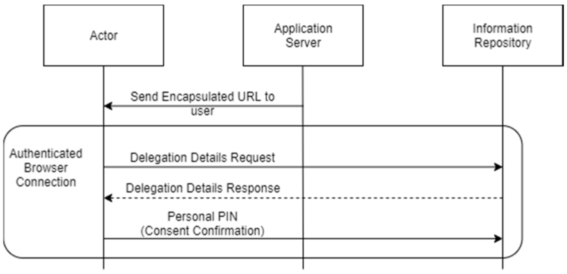

Actor
Application Server
Information Repository
Send Encapsulated URL to user
Authenticated Browser Connection
Delegation Details Request
Delegation Details Response
Personal PIN (Consent Confirmation)

Figure 8: Activity diagram – delegation confirmation.

To perform the confirmation (Figure 7 - right), an URL address pointing to the delegation draft is passed onto the application server, which is responsible to broadcast that draft to the mobile application of all the actors involved. The application should pass the URL onto the device's browser which opens a view to the delegation draft and a confirmation box to allow both the patient and the health professional to confirm or deny the operation. To do this, they use a personal pin, which allows them to validate their identities using a communication channel directly from the device, to the information repository (Figure 8). This part of the process is similar to existing OAuth2 flows of authentication, while additional security methods can also be included in this process.

6 DISCUSSION

As previous research has shown, users want more control over who accesses their health data, as well as easy to use, but also strong security features to accomplish that. The same applies to delegation situations, which are increasing in the world of mobile app with anytime/anywhere accesses. However, there is concern in not sharing out their health data to third parties, and even family and friends, by default. There is evidence that patients will want to do it, but want to delegate their data whenever they see necessary, and in a controlled manner, always verifying what and to whom they will share them with (Peng, 2016).

Most existing research in the area of mHealth delegation is just proof of concept and very few cases are tested in real scenarios. Our work is being developed in the ambit of a project which aims to implement and make use of a mobile app for monitoring and coaching chronic patients with respiratory diseases. The developed app will be available in online stores for download and use, and several studies with real patients from various healthcare organizations, will be performed within the timeframe of the project's duration.

In terms of architecture and technologies used, most are reused from existing well tested technologies, e.g., OAuth2 and openID for authentication and authorisation, which introduces the use of token-based authentication. The main advantage of token-based authentication is allowing to use a reduced amount of credentials. It does this by utilizing a single point for logging in, which generates access tokens accordingly, to be used by the application server to access the secured information repository. This is done with authorization from the user, the owner of the information, and also refreshing tokens to maintain sessions, without the use of credentials. Another advantage is the ease to make identified third-party servers communicate with the secured repository. An example is the hybrid flow which is designed to force the application server to be registered as a client in the OAuth2, implying that the user would still have to use the credentials directly with the OAuth2 server, and explicitly authorize the third-party server, to perform requests in their name.

Meanwhile, the use of openID frameworks, permits the creation of an identity server to be used alongside the OAuth2 protocols, adding information such as the user role in the system. Furthermore, and since interoperability in healthcare is a must requirement, FHIR, an already developed and implemented standard for health information, is used to store and communicate clinical related data. This is a step forward to communicate with other clinical information repositories, such as the ones used in hospitals, or similar health related applications, while also helping in the dissemination of standardized clinic information. Being a well-known and increasingly used standard, there is significant previous work in the stability of the standard and on the structures to contain as much as relevant and organized information, as possible.

As for the delegation process, some analysis on the security requirements and properties defined during the work, is necessary. In order to start the delegation, it is required that both parties can identify each other. Although at the beginning of the process an anonymous ID is used to link them, prior to the confirmation step, the information repository is able to replace the anonymous ID with an identification used within the system, related to the person that requested that ID. This method allows the patient for later confidently identify the person/delegatee to whom he is going to share information with. This way, there is no need to depend on sharing permanent IDs during all these communications, which could be reused on, for example, a replay attack.

Afterwards, there is the problem of allowing all parties relevant to the delegation process to confirm the delegation consent and its contents. We used a native property on FHIR resources that allows to define the active state of each instantiated resource as: draft, proposed, active, rejected, inactive or entered-in-error. At this stage, we were studying the possibility of using the draft state for when a consent defining a delegation permission is uploaded into the information repository. After this upload, we would mark the draft in the waiting state, until all involved parties confirm their authorization regarding the consent contents, which would then imply changing it to the active or rejected state. However, the confirmation step should not be performed using the application server, since confirmation of identity and authorization is critical, so it should be as secure as possible. Our proposed solution is based on how the OAuth2 protocol works, where a similar method is used in which a URL address is transmitted to the users, with the same intent as when the application server redirects authentication requests to the OAuth2 server. In practice, this opens an HTTPS connection with the information repository, which can be considered a secure channel for the user to review the consent, validate it and confirm the authorization using a previously registered PIN to confirm their identity.

Limitations. A limitation of this work is the small number of related research with applied mHealth use-cases, available for comparison and discussion. Also, due to the lack of space, it was not possible to show varied use-cases, with different *personas*, and more fine-grained delegation features. Finally, this work is still in the prototype phase and requires usability and reliability tests with end users, for its final evaluation. However, this limitation will be overcome within the lifetime of the project (AIRDOC, 2018), as already described, tests will be performed with real patients, enrolled in various healthcare organizations, before the AIRDOC app goes online.

7 CONCLUSIONS

The presented delegation prototype sets the path for a more flexible, easy and empowered way to provide secure delegation to patients, in real mHealth settings. This is a very relevant requirement with chronic disease patients, to securely share/delegate their continuous monitoring data to healthcare professionals, or others who can support them. The goal is to improve patients' adherence to medication and therapeutics to achieve better healthcare outcomes. Our solution can be applied in any similar mHealth scenario as the security framework was developed in a modular and independent way, using available and well tested standards and technologies.

As future work, the solution will be validated for its content, usability as well as legislation and privacy requirements, and will integrate into the SoTRAACE model (Moura, 2017). SoTRAACE allows to include features that take into account a risk-based personalized and contextual based decision, adapted to every mHealth interaction. Delegation can be one of those useful features on the way to a more patient empowered, dynamic, usable and secure mHealth.

ACKNOWLEDGEMENTS

This work is supported by project NORTE-01-0247-FEDER-033275, financed by the North Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, and through the European Regional Development Fund (ERDF). A. Ferreira is also with TagUBig - Taming Your Big Data (IF/00693/2015) from Researcher FCT Program funded by National Funds through FCT.

REFERENCES

AIRDOC, 2018. *AIRDOC - Smart Mobile Application for Individualized Support and Monitoring of the Respiratory Function and Sounds of Chronic Obstructive Patients.* Available at: http://cintesis.eu/en/portfolio-items/airdoc/ (Accessed: September 2019).

Boulos, M., Brewer, A., Karimkhani, C., Buller, D., Dellavalle, R., 2014. Mobile medical and health apps: state of the art, concerns, regulatory control and certification. *Online J Public Health Inform*, 5, pp. 229-229.

Ferretti, L., Marchetti, M., Colajanni, L., 2017. Verifiable Delegated Authorization for User-Centric Architectures and an OAuth2 Implementation. *In IEEE 41st Annual Computer Software and Applications Conference (COMPSAC),* pp. 718-723.

FHIR, 2011. *Fast Healthcare Interoperability Resources. Standard for health care data exchange, published by HL7®.* Available at: https://www.hl7.org/fhir/ (Accessed October 2019).

HAPI-FHIR, 2014. *Open-source implementation of the FHIR specification in Java.* Available at: https://hapifhir.io/. (Accessed October 2019).

Kotz, D., Gunter, C., Kumar, S., Weiner, J., 2016. Privacy and security in mobile health: a research agenda. *Computer*, 49(6):22-30.

Li, L., Huang, D., Shen, Z., Bouzefrane, S., 2013. A Cloud based Dual-Root Trust Model for Secure Mobile Online Transactions. *In IEEE Wireless Communications and Networking Conference (WCNC),* pp. 4404-4409.

Lu, J., Zhou, J., 2011. Preventing delegation-based mobile authentications from man-in-the-middle attacks. *Computer Standards & Interfaces*, 34, pp. 314-326.

Luo, J., Dong, Q., Huang, D., Kang, M., 2018. Attribute Based Encryption for Information Sharing on Tactical Mobile Networks. *In IEEE Military Communications Conference (MILCOM),* pp. 1-9.

Ma, H., Zhang, R., Yang, G., Song, Z., He, K., Xiao, Y., 2018. Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices. *In IEEE Transactions on Dependable and Secure Computing*, pp. 1-1.

Moura, P., Fazendeiro, P., Vieira-Marques P., Ferreira, A., 2017. SoTRAACE — socio-technical risk-adaptable access control Model. *In 2017 International Carnahan Conference on Security Technology (ICCST),* pp. 1–6.

Nguyen, D., Pathirana, P., Ding, M., Seneviratne, A., 2019. Blockchain for secure EHRs sharing of mobile cloud based ehealth systems. *IEEE Access*, 7, pp. 66792-66806.

OAUTH 2, 2019. *OAuth 2.0 [online]*. Available at: https://oauth.net/2/ (Accessed: August 2019).

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C., 2018. Security and privacy analysis of mobile health applications: the alarming state of practice. *IEEE Access*, 6:9390-9403.

Peng, W., Kanthawala, S., Yuan, S., Hussain, S., 2016. A qualitative study of user perceptions of mobile health apps. *BMC Public Health*, 16.

Platt, D., 2016. The Joy of UX – User Experience and Interactive Design for Developers. *Addison-Wesley*.

Prasad, A., Sorber, J., Stablein, T., Anthony, D., Kotz, d., 2012. Understanding sharing preferences and behavior for mHealth devices. *In Proceedings of the 2012 ACM workshop on Privacy in the electronic society,* pp. 117-128.

Pussewalage, H., Oleshchuk, V., 2017. Attribute based access control scheme with controlled access delegation for collaborative E-health environments. *Journal of Information Security and Applications*, 37, pp. 50-54.

Rabehaja, T., Pal, S., Hitchens, M., 2019. Design and implementation of a secure and flexible access-right delegation for resource constrained environments. *Future Generation Computer Systems,* 99, pp. 593-608.

Schaad, A., Moffett, J., 2002. Delegation of Obligations. In *Proc. of the 3rd International Workshop on Policies for Distributed Systems and Networks*, pp. 25-35.

Schefer-Wenzl, Sigrid., Bukvova, H., Strembeck, Mark., 2014. A Review of Delegation and Break-Glass Models for Flexible Access Control Management. *Lecture Notes in Business Information Processing*, 183.

Sciarreta, G., Carbone, R., Ranise, S., 2016. A delegated authorization solution for smart-city mobile applications. *In IEEE 2nd International Forum on*

Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), pp. 1-6.

Stach, C., 2016. Secure Candy Castle - A Prototype for Privacy-Aware mHealth Apps. *In 17th IEEE International Conference on Mobile Data Management (MDM),* pp. 361-364

Stradolini, F., Tamburrano, N., Modoux, T., Tuoheti, A., Demarchi, D., Carrara, S., 2018. IoT for Telemedicine Practices enabled by an Android™ Application with Cloud System Integration. *In IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1-5.

Sucasas, V., Mantas, G., Radwan, A., Rodriguez, J., 2016. An OAuth2-based protocol with strong user privacy preservation for smart city mobile e-Health apps. *In IEEE International Conference on Communications (ICC),* pp. 1-6.

Tan, Z., 2018. Secure Delegation-Based Authentication for Telecare Medicine Information Systems. *IEEE Access*, 6, pp. 26091-26110.

Weerasinghe, D., Muttukrishnan,R., et. al., 2011. Secure Trust Delegation for Sharing Patient Medical Records in a Mobile Environment. *In Proceedings of 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4.

Wu, X., Dunne, R., Yu, Z., Shi, W., 2017. STREMS: A Smart Real-Time Solution toward Enhancing EMS Prehospital Quality. *In IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE),* pp. 365-372.

Zhou, L., Bao, J., Watzlaf, V., Parmanto, B., 2019. Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study. *JMIR Mhealth Uhealth,* 7(4): e11223.